ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น

CAUSAL FACTORS OF PRIVACY DATA PROTECTION BEHAVIORS ON ELECTRONICS TRANSACTIONS IN FIRST JOBBERS

ธีรศักดิ์ พลพันธ์

บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ

2564

ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น

ธีรศักดิ์ พลพันธ์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปรัชญาดุษฎีบัณฑิต สาขาวิชาการวิจัยพฤติกรรมศาสตร์ประยุกต์
สถาบันวิจัยพฤติกรรมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ
ปีการศึกษา 2564

CAUSAL FACTORS OF PRIVACY DATA PROTECTION BEHAVIORS ON ELECTRONICS TRANSACTIONS IN FIRST JOBBERS

THEERASAK PONEPAN

A Dissertation Submitted in Partial Fulfillment of the Requirements

for the Degree of DOCTOR OF PHILOSOPHY

(Applied Behavioral Sc.Research)

BEHAVIORAL SCIENCE RESEARCH INSTITUTE, Srinakharinwirot University

2021

ปริญญานิพนธ์
เรื่อง
ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์
ในกลุ่มวัยทำงานตอนต้น
ของ
ธีรศักดิ์ พลพันธ์

ได้รับอนุมัติจากบัณฑิตวิทยาลัยให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาปรัชญาดุษฎีบัณฑิต สาขาวิชาการวิจัยพฤติกรรมศาสตร์ประยุกต์
ของมหาวิทยาลัยศรีนครินทรวิโรฒ

(รองศาสตราจารย์ นายแพทย์ฉัตรชัย เอกปัญญาสกุล)
คณบดีบัณฑิตวิทยาลัย

คณะกรรมการสอบปากเปล่าปริญญานิพนธ์

..... ที่ปรึกษาหลัก
(ผู้ช่วยศาสตราจารย์ ดร.ศรัณย์ พิมพ์ทอง)

..... ประธาน
(ศาสตราจารย์ ดร.ดุจเดือน พันธุมนาวิน)

..... ที่ปรึกษาร่วม
(ผู้ช่วยศาสตราจารย์ ดร.กาญจนา ภัทราวิวัฒน์)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.นำชัย ศุภฤกษ์ชัยสกุล)

ชื่อเรื่อง	ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ในกลุ่มวัยทำงานตอนต้น
ผู้วิจัย	ธีรศักดิ์ พลพันธ์
ปริญญา	ปรัชญาดุษฎีบัณฑิต
ปีการศึกษา	2564
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์ ดร. ศรัณย์ พิมพ์ทอง
อาจารย์ที่ปรึกษาร่วม	ผู้ช่วยศาสตราจารย์ ดร. กาญจนา ภัทราวิวัฒน์

การวิจัยนี้มีวัตถุประสงค์เพื่อทดสอบและพัฒนาแบบจำลองความสัมพันธ์โครงสร้างเชิงเส้นของปัจจัยที่มีอิทธิพลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น จากการศึกษาภายใต้ทฤษฎีแรงจูงใจเพื่อการป้องกันร่วมกับแบบจำลองการยอมรับการใช้เทคโนโลยี กลุ่มตัวอย่างเป็นวัยทำงานตอนต้นจำนวน 418 คนในเขตกรุงเทพมหานครและปริมณฑล ใช้วิธีการสุ่มตัวอย่างแบบกลุ่ม 2 ขั้นตอน ตามเกณฑ์จัดกลุ่มพื้นที่ของการแบ่งเขตการปกครองกระทรวงมหาดไทย เครื่องมือที่ใช้เก็บรวบรวมข้อมูลเป็นแบบสอบถามจำนวน 12 ตอน มีค่าความเชื่อมั่นระหว่าง 0.72-0.85 และวิเคราะห์ข้อมูลโดยใช้วิธีการวิเคราะห์แบบจำลองสมการโครงสร้าง ผลการวิจัยพบว่าการพัฒนาแบบจำลองความสัมพันธ์โครงสร้างเชิงเส้นของปัจจัยที่มีอิทธิพลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยมีค่าดัชนี = 684.99, df = 173, p-value < 0.01, RMSEA = 0.075, SRMR = 0.055, NNFI = 0.96, CFI = 0.97 and GFI = 0.90. และพบว่าพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ได้รับอิทธิพลทางบวกโดยตรงจากปัจจัยความตั้งใจในการปกป้องข้อมูลส่วนบุคคล และได้รับอิทธิพลทางบวกโดยอ้อมจากปัจจัยการรับรู้ถึงโอกาสเสี่ยงบนธุรกรรมทางอิเล็กทรอนิกส์ ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล และการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ตามลำดับ

คำสำคัญ : พฤติกรรมการปกป้องข้อมูลส่วนบุคคล, ธุรกรรมทางอิเล็กทรอนิกส์, กลุ่มวัยทำงานตอนต้น

Title	CAUSAL FACTORS OF PRIVACY DATA PROTECTION BEHAVIORS ON ELECTRONICS TRANSACTIONS IN FIRST JOBBERS
Author	THEERASAK PONEPAN
Degree	DOCTOR OF PHILOSOPHY
Academic Year	2021
Thesis Advisor	Assistant Professor Saran Pimthong , Ph.D.
Co Advisor	Assistant Professor Dr. Kanchana Pattrawiwat

This study aims to test and develop a structural equation model of the factors influencing personal data protection behaviors in first jobbers during electronic transactions. The participants were 418 first-time jobbers living in the Bangkok metropolitan area. The two-stage cluster sampling was applied to randomize the sample group within the administrative zone. The theoretical foundations of the current study was Protection Motivation Theory and an expanded Technology Acceptance Model. The data were collected using twelve constructs of reliable and valid questionnaires and with alpha coefficients ranging from 0.72 to 0.85. The results showed that the developed structural equation model was consistent with the empirical data, as measured by the goodness of fit indices: = 684.99, df = 173, p-value < 0.01, RMSEA = 0.075, SRMR = 0.055, NNFI = 0.96, CFI = 0.97 and GFI = 0.90. The findings revealed that intentions had a direct effect on privacy data protection behaviors, while perceived vulnerability, self-efficacy and subjective norms had an indirect effect on privacy data protection behaviors respectively.

Keyword : privacy data protection behaviors, electronic transactions, first jobbers

กิตติกรรมประกาศ

ผู้วิจัยขอกราบขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร. ศรัณย์ พิมพ์ทอง และ ผู้ช่วยศาสตราจารย์ ดร. กาญจนา ภัทราวิวัฒน์ ซึ่งเป็นอาจารย์ที่ปรึกษาหลักและอาจารย์ที่ปรึกษาร่วมปริญญานิพนธ์ที่คอยให้ความช่วยเหลือ สนับสนุน ให้คำปรึกษา แนวคิดและคำแนะนำ ปรับปรุงแก้ไขตลอดช่วงเวลาในการวิจัยครั้งนี้ รวมทั้งขอกราบขอบพระคุณ ศาสตราจารย์ ดร. ดุจเดือน พันธุมนาวิน ประธานสอบปากเปล่าปริญญานิพนธ์ และผู้ช่วยศาสตราจารย์ ดร.นำชัย ศุภฤกษ์ชัยสกุล กรรมการสอบปากเปล่าปริญญานิพนธ์ ที่ให้ความเมตตา ให้ความเห็นคำแนะนำที่เป็นประโยชน์และการปรับปรุงแก้ไขข้อมูลเชิงการวิจัยพฤติกรรมศาสตร์ ทำให้ปริญญานิพนธ์ฉบับนี้มีความสมบูรณ์มากยิ่งขึ้น

ขอกราบขอบพระคุณอาจารย์คณะกรรมการสอบเค้าโครงการวิจัยทุกท่าน ที่ให้คำแนะนำเพื่อให้งานวิจัยนี้มีความชัดเจน ถูกต้องและเป็นไปได้ในทางการวิจัยพฤติกรรมศาสตร์ และขอกราบขอบพระคุณอาจารย์ผู้ทรงคุณวุฒิและผู้เชี่ยวชาญทุกท่าน ที่กรุณาให้คำปรึกษาและสละเวลาตรวจคุณภาพของเครื่องมือ ทำให้เครื่องมือ/แบบวัดในงานวิจัยนี้ มีความถูกต้องและสามารถสำหรับนำไปใช้ในการวิจัยได้อย่างมีประสิทธิภาพ

ขอขอบพระคุณคณาจารย์สถาบันวิจัยพฤติกรรมศาสตร์ ที่ให้ความรู้เชิงทฤษฎี คำแนะนำเชิงปฏิบัติ และประสบการณ์ทางการวิจัยทางพฤติกรรมศาสตร์ในระหว่างที่ทำการศึกษาที่สถาบันแห่งนี้ รวมทั้งเจ้าหน้าที่สถาบันวิจัยพฤติกรรมศาสตร์ทุกท่าน ที่มีส่วนช่วยเหลือในการดำเนินการจัดทำปริญญานิพนธ์ฉบับนี้ให้เป็นไปอย่างรวดเร็วและถูกต้องตามรูปแบบของบัณฑิตวิทยาลัย

ขอขอบคุณหน่วยงานและองค์กรที่เกี่ยวข้องที่ให้ความร่วมมือ ช่วยประสานงานเอกสาร ประชาสัมพันธ์และอนุญาตให้ดำเนินการเก็บรวบรวมข้อมูลเพื่อการวิจัย รวมทั้งกลุ่มพนักงานที่เป็นวัยทำงานตอนต้นและเป็นกลุ่มตัวอย่างการวิจัยครั้งนี้ที่ให้ความร่วมมือเป็นอย่างดีและเสียสละเวลาในการตอบแบบสอบถามงานวิจัย

ขอกราบขอบพระคุณบิดา มารดาและสมาชิกครอบครัวพลพันธ์ทุกคน ที่ให้กำลังใจและสนับสนุนการศึกษาต่อครั้งนี้ ขอบคุณเพื่อนร่วมชั้นเรียนแบบมีวิชาเรียน รุ่น 12 ทุกคนที่คอยแนะนำ ข้อมูลข่าวสารและให้กำลังใจกันมาตลอด รวมทั้งพี่ๆ และเพื่อนร่วมงานจากสถาบันการจัดการปัญญาภิวัฒน์ ซึ่งเป็นทั้งพี่เลี้ยงในการศึกษาต่อและกัณยาณมิตรที่ดีมาโดยตลอด

สุดท้ายผู้วิจัย ขอขอบพระคุณสถาบันการจัดการปัญญาภิวัฒน์ ที่มอบทุนสนับสนุนการศึกษาและคอยสอบถามความเป็นไปของการศึกษาต่อในครั้งนี้ จนประสบความเร็จในการศึกษาตามที่ตั้งใจไว้

ธีรศักดิ์ พลพันธ์

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญรูปภาพ

หน้า

บทที่ 1
บทนำ

ที่มาและความสำคัญของปัญหา

ปัจจุบันความก้าวหน้าทางด้านเทคโนโลยีการสื่อสารผ่านทางเครือข่ายอินเทอร์เน็ต (Internet) ได้เข้ามามีอิทธิพลต่อการดำเนินชีวิตประจำวันของบุคคลในสังคมเป็นอย่างมาก เป็นที่นิยมใช้ในการติดต่อสื่อสารและการมีปฏิสัมพันธ์โต้ตอบกัน (Interaction) เช่น การสนทนาออนไลน์กับบุคคลอื่นที่อยู่ห่างไกลกันหรือข้ามประเทศ การเข้าดูรายละเอียดสินค้าและบริการต่างๆ และการซื้อ-ขายสินค้าออนไลน์หรือการพาณิชย์อิเล็กทรอนิกส์ (E-Commerce) โดยไม่จำเป็นต้องเดินทางไปยังร้านค้าหรือห้างสรรพสินค้า (Berendt et al., 2005; ขจรศักดิ์ รุ่งศรีรัตนวงศ์ และคณะ, 2550; สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2561) รวมทั้งการโฆษณาและประชาสัมพันธ์สินค้าออนไลน์ที่ต้องการให้กลุ่มเป้าหมายรับทราบก็สามารถทำได้อย่างรวดเร็ว (Wu, 2003; จีราภรณ์ สุธัมมสภา, 2555) เป็นต้น จากความก้าวหน้าทางด้านเทคโนโลยีการสื่อสารผ่านทางเครือข่ายอินเทอร์เน็ตนี้ ทำให้ทุกคนต้องมีการปรับตัวให้ทันต่อพัฒนาการและการเปลี่ยนแปลงของเทคโนโลยีการสื่อสาร

ด้วยความก้าวหน้าทางด้านเทคโนโลยีการสื่อสารผ่านทางเครือข่ายอินเทอร์เน็ต ได้ถูกนำมาใช้งานในการประกอบธุรกิจอย่างแพร่หลาย สำหรับธุรกิจประเภทสถาบันทางการเงินและธนาคารได้มีการปรับตัวเพื่อรองรับธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions) หรือการทำธุรกรรมทางการเงินออนไลน์ (ธนาคารแห่งประเทศไทย, 2561; สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2559; ธนาคารอาคารสงเคราะห์, 2562) โดยการเพิ่มช่องทางในการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่สามารถดำเนินการได้ด้วยตนเองเพื่อให้มีความสอดคล้องกับพฤติกรรมของผู้บริโภคที่ต้องการความสะดวกและรวดเร็วมากขึ้น โดยไม่จำต้องเสียเวลาในการเดินทางไปยังธนาคารหรือไปยังตู้เอทีเอ็ม (Automatic Teller Machine: ATM) เหมือนในอดีตที่ผ่านมา ในปัจจุบันพบว่ารูปแบบการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์จำแนกตามช่องทางในการให้บริการออกเป็น 2 ช่องทาง (ธนาคารแห่งประเทศไทย, 2561; Digital Ventures, 2017) ได้แก่ 1) อินเทอร์เน็ตแบงก์กิ้ง (Internet Banking) เป็นบริการของธนาคารที่เปิดให้ลูกค้าสามารถทำธุรกรรมทางอิเล็กทรอนิกส์ได้เองเช่น การฝาก-ถอนเงิน การโอนเงิน การตรวจสอบยอดเงินคงเหลือ การชำระค่าสาธารณูปโภค เป็นต้น ผ่านทางเว็บไซต์ (Website) ของธนาคาร และ 2) โมบายแบงก์กิ้ง (Mobile Banking) เป็นบริการของธนาคารที่เปิดให้ลูกค้าการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารที่เปิดให้บริการผ่านทางสมาร์ทโฟน (Smartphone) และ

แท็บเล็ต (Tablet) จากการใช้งานผ่านแอปพลิเคชัน (Application) ของแต่ละธนาคารหรือสถาบันทางการเงินที่มีลักษณะและรูปแบบหน้าจอที่แตกต่างกันออกไป สอดคล้องกับผลสำรวจพฤติกรรมการใช้สมาร์ทโฟนปี พ.ศ. 2560 ที่พบว่าคนไทยใช้สมาร์ทโฟนในการชำระเงินและทำธุรกรรมทางอิเล็กทรอนิกส์เพิ่มมากขึ้น (การซื้อสินค้าออนไลน์ของคนไทยในยุค Thailand 4.0, สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2561, น. 78) และจากสถิติการทำธุรกรรมทางอิเล็กทรอนิกส์ผ่านทางโมบายแบ้งก์กิ้ง (ธนาคารแห่งประเทศไทย, 2560) พบว่าได้รับความนิยมเพิ่มขึ้นอย่างต่อเนื่อง โดยในปี พ.ศ. 2559 มีอัตราเพิ่มขึ้น คิดเป็นร้อยละ 95.57 เมื่อเปรียบเทียบกับปี พ.ศ. 2558 และเนื่องจากได้รับการส่งเสริมในการใช้บริการจากธนาคารพาณิชย์หลายแห่ง ส่งผลทำให้ผู้ใช้บริการปรับเปลี่ยนพฤติกรรมในการทำธุรกรรมทางอิเล็กทรอนิกส์มากขึ้น ประกอบกับธนาคารพาณิชย์ได้มีประกาศยกเลิกค่าธรรมเนียมการเงินบนช่องทางอิเล็กทรอนิกส์ (ธนาคารแห่งประเทศไทย, 2560) ทำให้ยอดการโอนเงินข้ามระหว่างธนาคารมีอัตราการเติบโตเพิ่มขึ้นถึงร้อยละ 239 และจำนวนหมายเลขบัญชีการใช้งานธุรกรรมทางอิเล็กทรอนิกส์ผ่านช่องทางโมบายแบ้งก์กิ้งเพิ่มขึ้นกว่า 38 ล้านบัญชี (BLTBangkok, 2018 อ้างใน ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย, 2561)

เนื่องจากบริการธุรกรรมทางอิเล็กทรอนิกส์ ส่งผลให้ผู้ใช้บริการได้รับความสะดวกสบายและรวดเร็ว และสามารถทำธุรกรรมทางการเงินได้ทุกที่ทุกเวลา (ธนาคารแห่งประเทศไทย, 2561; สถาบันวิจัยและบริการวิชาการ มหาวิทยาลัยอัสสัมชัญ, 2559) รวมทั้งธนาคารพาณิชย์หลายแห่งได้มีการส่งเสริมและกระตุ้นให้ลูกค้าให้เข้ามาใช้บริการธุรกรรมทางอิเล็กทรอนิกส์มากขึ้น เพื่อลดจำนวนสาขาของธนาคารและเป็นการประหยัดงบประมาณและทรัพยากรบุคคล ในปัจจุบันพบว่าการแข่งขันในการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ของแต่ละธนาคารมีแนวโน้มการแข่งขันกันที่สูงขึ้น มีความหลากหลายและเฉพาะเจาะจงมากขึ้นเช่นกัน (ธนาคารกสิกรไทย 2560; MoneyGuru, 2018) ซึ่งการที่แต่ละธนาคารมีการพัฒนาด้านการใช้บริการผ่านแอปพลิเคชันจึงเป็นทางเลือกที่ช่วยให้ลดต้นทุนในการให้บริการและเพิ่มความสะดวกให้แก่ลูกค้ามากขึ้น ประกอบกับธุรกิจสื่อสารโทรคมนาคม ในการให้บริการเครือข่ายอินเทอร์เน็ตความเร็วสูงที่มีความก้าวหน้าในการรับส่งข้อมูลต่างๆ (Aghaei et al., 2012; Moneyhub, 2017) ทำให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารได้รับประโยชน์จากการพัฒนาเทคโนโลยี ส่งผลให้ปริมาณการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารเพิ่มขึ้นตามไปด้วย รวมไปถึงการพาณิชย์อิเล็กทรอนิกส์ (E-Commerce) ถือได้ว่าเป็นธุรกรรมทางอิเล็กทรอนิกส์รูปแบบหนึ่ง ซึ่งเป็นธุรกรรมผ่านทางเครือข่าย

อินเทอร์เน็ตจากการซื้อและขายสินค้าหรือบริการทางอิเล็กทรอนิกส์ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2561)

สำหรับการใช้บริการเครือข่ายอินเทอร์เน็ตในประเทศไทยที่ผ่านมา จะเห็นว่าเข้ามามีบทบาทในชีวิตประจำวันมากขึ้นเรื่อยๆ เกือบทุกครัวเรือนมีการใช้บริการอินเทอร์เน็ต (สมาร์ทเอสเอ็มอี, 2560) รวมทั้งการได้รับการสนับสนุนจากหน่วยงานของกรุงเทพมหานคร ที่ให้บริการอินเทอร์เน็ตไร้สายแบบไม่เสียค่าใช้จ่ายหรือกรีน แบงค็อก วายฟาย (Green Bangkok Wi-Fi) รวมไปถึงศูนย์การค้า โรงแรม สถานที่ท่องเที่ยว สนามบิน ร้านอาหารและร้านกาแฟต่างๆ ที่เริ่มมีพื้นที่ให้บริการอินเทอร์เน็ตไร้สายแบบไม่เสียค่าใช้จ่าย ซึ่งมีส่วนช่วยให้ผู้ใช้บริการอินเทอร์เน็ตได้รับความสะดวก และสามารถที่จะเข้าถึงบริการอินเทอร์เน็ตเพื่อบริการธุรกรรมทางอิเล็กทรอนิกส์ได้ง่ายขึ้น (MoneyGuru, 2018; สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2561) จากการศึกษาช่วงอายุของผู้ใช้บริการเครือข่ายอินเทอร์เน็ตพบว่ากลุ่มอายุระหว่าง 21-30 ปีมีการใช้บริการอินเทอร์เน็ตเพิ่มขึ้นคิดเป็นร้อยละ 88.4 (การมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน สำนักงานสถิติแห่งชาติ, 2561, น. 5) โดยให้ความสนใจในกิจกรรมการซื้อขายสินค้าออนไลน์มากกว่ากลุ่มอายุอื่นๆ เนื่องจากเป็นกลุ่มที่เริ่มมีกำลังซื้อสินค้าตามกระแสสื่อสังคมออนไลน์และเป็นกลุ่มอายุที่มีความเสี่ยงต่อการถูกล่วงละเมิดข้อมูลส่วนบุคคลที่เพิ่มขึ้น (ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย, 2563; ศูนย์การเรียนรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล, 2563) และแม้ว่าการพาณิชย์อิเล็กทรอนิกส์ จะเป็นช่องทางที่ช่วยส่งเสริมในด้านความสะดวกสบายสำหรับการซื้อขายสินค้าและบริการออนไลน์ ที่ผู้บริโภคสามารถซื้อสินค้าได้ทุกที่ทุกเวลา แต่ในทางตรงกันข้ามช่องทางเหล่านี้อาจทำให้คนอีกประเภทหนึ่งแฝงตัวมาในรูปแบบมิจฉาชีพที่สร้างความไม่ปลอดภัยทางด้านการเงินให้กับผู้ซื้อสินค้าและบริการ (Gupta et al., 2006; สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2563) เช่น การลักลอบนำข้อมูลส่วนบุคคลของผู้บริโภคไปใช้งานหรือนำไปขายให้กับหน่วยงานต่างๆ ตลอดจนการโจรกรรมที่อาจนำมาซึ่งความเสียหายต่อทรัพย์สินและชีวิตได้ จากการศึกษางานวิจัยที่เกี่ยวข้องกับการพาณิชย์อิเล็กทรอนิกส์ พบว่าผู้บริโภคให้ความสำคัญระบบการป้องกันข้อมูลส่วนบุคคลและการเก็บข้อมูลเป็นความลับในการสั่งซื้อสินค้าออนไลน์ (ปวุฒิ บุนนาค, 2557; ณัฐศักดิ์ วรวิทยานนท์, 2555) อย่างไรก็ตามในกระบวนการซื้อขายสินค้าออนไลน์ ผู้บริโภคจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลบางอย่างให้กับร้านค้าหรือผู้ขายสินค้าออนไลน์ ทำให้ผู้ซื้อสินค้าออนไลน์มีโอกาสสูญเสียความเป็นส่วนตัวได้โดยง่าย

สอดคล้องกับรายงานผลการวิจัยต่างประเทศ *"Stranger danger: the connection between sharing online and losing the data we love"* (Kaspersky Lab, 2019) พบว่ากลุ่มวัยรุ่นอายุระหว่าง 18-26 ปี จำนวนร้อยละ 93 มีพฤติกรรมการเปิดเผยข้อมูลส่วนบุคคลสู่สาธารณะและร้อยละ 59 ตกเป็นเหยื่อการจารกรรมข้อมูลส่วนบุคคล โดยการเอาข้อมูลส่วนบุคคลไปแอบอ้างเพื่อหาผลประโยชน์ และการโจมตีทางการเงินซึ่งเกิดจากการเปิดเผยรายละเอียดทางการเงินและการชำระเงินทางอิเล็กทรอนิกส์ ดังนั้นจะเห็นว่าข้อมูลส่วนบุคคลนั้นมีสถานะไม่ต่างไปจากทรัพย์สินส่วนบุคคล และหากผู้ใช้บริการอินเทอร์เน็ตไม่ระมัดระวังในการใช้งานกิจกรรมออนไลน์ต่างๆ และเมื่อข้อมูลส่วนบุคคลได้เข้ามาสู่โลกออนไลน์ ข้อมูลส่วนบุคคลอาจจะไม่เป็นความลับอีกต่อไป กลายเป็นข้อมูลสาธารณะที่ไม่สามารถลบออกไปได้หมด (Feng & Xie, 2014; Ernst et al., 2015; สุภารัตน์ แก้วสุทธิ 2553; วสันต์ ลิ่วลมไพศาลและสฤณี อาชวานันทกุล , 2556; สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2563) และหากข้อมูลส่วนบุคคลเหล่านั้นมีความสำคัญมาก เช่น หมายเลขบัตรประจำตัวประชาชน รหัสบัตรเครดิต เลขที่บัญชีธนาคาร หมายเลขโทรศัพท์ วันเดือนปีเกิด เป็นต้น หากมีบุคคลอื่นทำการขโมยข้อมูลส่วนบุคคลเหล่านี้ไปอาจสร้างปัญหาต่างๆ ตามมา ซึ่งข้อมูลส่วนบุคคลหากถูกขโมยตัวตน (Identity Theft) อาจถูกนำไปใช้เพื่อการจารกรรมข้อมูลทางการเงิน การก่ออาชญากรรม การสะกดรอยตามเพื่อใช้ประโยชน์ทางการตลาดหรือทางการเมืองจากการขายข้อมูลส่วนบุคคลไปยังบุคคลที่สาม (Third-Party) ก็เป็นไปได้

หลายครั้งที่เราได้ทราบเรื่องราวการรายงานข่าวของสื่อต่างๆ เกี่ยวกับภัยบนโลกออนไลน์หรือภัยในยุคดิจิทัลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ โดยจำเป็นต้องกรอกข้อมูลส่วนบุคคลเพื่อเข้าใช้งาน และจะพบข่าวการถูกขโมยข้อมูลส่วนบุคคลโดยเจ้าของข้อมูลไม่รู้ตัว (เพจเฟซบุ๊กศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ, 2563; ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย, 2563; ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย, 2562) เช่น การถูกขโมยข้อมูลส่วนบุคคลเพื่อเข้าทำธุรกรรมทางอิเล็กทรอนิกส์แทนเจ้าของบัญชีธนาคาร กลุ่มมิจฉาชีพทางการเงินในรูปแบบต่างๆ จากการซื้อขายสินค้าออนไลน์หรือการพาณิชย์อิเล็กทรอนิกส์ การขโมยเงินผ่านช่องทางกระเป๋าเงินอิเล็กทรอนิกส์ (E-Wallet) การขโมยบัญชีเฟซบุ๊กเพื่อหลอกให้เพื่อนโอนเงินมาให้ เป็นต้น ซึ่งการรายงานข่าวปัญหาการถูกขโมยข้อมูลส่วนบุคคลสำหรับธุรกรรมทางอิเล็กทรอนิกส์ในประเทศไทยนั้นยังคงปรากฏให้เห็นอย่างต่อเนื่อง อีกทั้งยังคงเป็นปัญหาอยู่และมีแนวโน้มเพิ่มสูงขึ้น (ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย, 2563; สมาคมผู้ดูแลเว็บไทย, 2562)

จากการศึกษารายละเอียดข้อมูลเกี่ยวกับรายงานข่าวปัญหาการถูกขโมยข้อมูลส่วนบุคคลสำหรับธุรกรรมทางอิเล็กทรอนิกส์ข้างต้น พบว่าผู้เสียหายจะอยู่ในฐานะผู้บริโภคที่นิยมซื้อสินค้าและบริการออนไลน์และมีอายุระหว่าง 23-29 ปี ซึ่งจัดอยู่ในกลุ่มเจเนอเรชั่นวาย (Generation Y) สอดคล้องกับรายงานผลสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทยของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (2563) ในกลุ่มเจเนอเรชั่นวายเกี่ยวกับพฤติกรรมสุ่มเสี่ยงในการถูกขโมยข้อมูลส่วนบุคคลและการละเมิดข้อมูลส่วนบุคคลที่เพิ่มสูงขึ้นและมากกว่ากลุ่มเจเนอเรชั่นอื่น เนื่องจากการมีเอกสารส่วนตัวในการทำธุรกรรมทางอิเล็กทรอนิกส์และการซื้อสินค้าออนไลน์ที่เพิ่มขึ้น เช่น บัตรเครดิต บัญชีธนาคาร หมายเลขประกันสังคม เป็นต้น โดยพบว่าร้อยละ 42.3 เสี่ยงต่อการถูกขโมยตัวตนและข้อมูลทางธุรกรรมออนไลน์ จากการไม่ทันสังเกตเครื่องหมายความปลอดภัยในการเข้าใช้งาน และร้อยละ 35.8 เสี่ยงต่อการถูกเข้าถึงอุปกรณ์และข้อมูลโดยผู้อื่น จากการใช้อุปกรณ์คนอื่นทำธุรกรรมทางการเงินและการบอกรหัสผ่านเข้าอุปกรณ์ให้เพื่อนสนิทหรือคนรู้ใจ สะท้อนให้เห็นว่าผู้เสียหายในฐานะผู้บริโภคยังไม่ให้ความสำคัญและตระหนักในการปกป้องข้อมูลส่วนบุคคลเท่าที่ควร และจะเห็นได้ว่าผู้เสียหายซึ่งมักจะขอความช่วยเหลือหรือหวังพึ่งพาจากหน่วยงานที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี อาจเนื่องมาจากขาดความรู้ ความเข้าใจในการปกป้องและการรักษาความปลอดภัยของข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ การขาดแคลนบุคลากรที่ให้ความรู้และขาดการประชาสัมพันธ์ถึงปัญหาอาชญากรรมทางเทคโนโลยี รวมไปถึงขอบเขตของกฎหมายการคุ้มครองข้อมูลส่วนบุคคลที่อาจยังไม่ชัดเจนในรายละเอียดเชิงปฏิบัติ ซึ่งแนวทางการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ คงไม่ใช่การยกเลิกใช้บริการไปเลย เพราะยังมีประโยชน์ค่อนข้างมากจากบริการธุรกรรมทางอิเล็กทรอนิกส์ เช่น ผู้ซื้อสินค้าออนไลน์สามารถเข้าถึงสินค้าที่ต้องการได้สะดวกและรวดเร็ว เป็นต้น (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2563)

ในปัจจุบัน วิธีการปกป้องความปลอดภัยในข้อมูลส่วนบุคคลของผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ ได้มีการจัดทำเป็นนโยบายความเป็นส่วนตัว (Privacy Policy) หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลบนเว็บไซต์และแอปพลิเคชันก่อนเข้าใช้บริการ เพื่อสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ซึ่งเป็นเพียงแนวทางปกป้องข้อมูลส่วนบุคคลรูปแบบหนึ่งเท่านั้น และในทางกฎหมายนโยบายการคุ้มครองข้อมูลส่วนบุคคลบนเว็บไซต์และแอปพลิเคชัน มีสถานะเป็นเพียงคำมั่นเท่านั้น (ธนัท สุวรรณปริญญา, 2550) อย่างไรก็ตาม หากศึกษาถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคล ในปัจจุบันประเทศไทย ได้มีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ที่ประกาศขึ้นเมื่อวันที่ 27 พฤษภาคม 2562 (ราชกิจจานุเบกษา, 2562, น. 52) ทั้งนี้

ยังไม่มีการปฏิบัติใช้คุ้มครองข้อมูลส่วนบุคคล เนื่องจากจำเป็นต้องจัดตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และให้เวลาผู้ควบคุมข้อมูลจัดเตรียมระบบให้พร้อมเป็นเวลา 1 ปี นับจากวันประกาศ และจะต้องมีการออกประกาศขั้นตอนระเบียบปฏิบัติต่างๆ อีกประมาณ 30 ฉบับเพื่อเป็นแนวทางปฏิบัติต่อไป (มติชนออนไลน์, 27 พฤษภาคม 2562) และเมื่อศึกษาในรายละเอียดข้อมูลของกฎหมายดังกล่าวไม่ได้คุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมการกระทำผิดและการร้องเรียนเกี่ยวกับข้อมูลส่วนบุคคลทั้งหมด เพียงแต่ให้ความคุ้มครองเฉพาะบางเรื่อง ดังนั้นผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ยังจำเป็นต้องให้ความสำคัญในการเปิดเผยข้อมูลส่วนบุคคล การปกป้องและรักษาความปลอดภัยของข้อมูลส่วนบุคคลสู่สาธารณะ (สถาบันวิจัยเพื่อการพัฒนาประเทศไทย, 2562)

ในขณะที่หลายๆ ประเทศ การเปิดเผยข้อมูลส่วนบุคคลถือเป็นเรื่องที่มีความสำคัญ ได้มีแนวทางมาตรการเพื่อป้องกันและตระหนักถึงปัญหาการให้ความคุ้มครองข้อมูลส่วนบุคคลเพื่อคุ้มครองสิทธิความเป็นส่วนตัว เนื่องจากบุคคลอื่นอาจนำข้อมูลส่วนบุคคลไปแสวงหาผลประโยชน์ในรูปแบบต่างๆ ได้ และเมื่อมีการจัดเก็บอยู่ในระบบคอมพิวเตอร์หรือเอกสารอิเล็กทรอนิกส์ (e-Document) ทำให้การนำไปใช้ต่อและการเผยแพร่ถึงบุคคลจำนวนมากสามารถทำได้โดยง่ายและรวดเร็ว อย่างเช่นกลุ่มประเทศในสหภาพยุโรป (European Union: EU) ได้ออกกฎหมายใหม่เพื่อปกป้องข้อมูลส่วนบุคคลมีชื่อว่า General Data Protection Regulation (GDPR) และมีผลบังคับใช้กับประเทศสมาชิก 28 ประเทศเมื่อวันที่ 25 พฤษภาคม ค.ศ. 2018 แทนที่กฎหมายฉบับเดิม Data Protection Directive 1995 (Directive95/46/EC) ซึ่งเป็นกฎหมายมุ่งเน้นถึงการคุ้มครองสิทธิความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคลโดยเฉพาะ และกฎหมายดังกล่าวไม่ได้มีผลกับบริษัททางด้านเทคโนโลยีสารสนเทศเท่านั้น แต่ยังรวมไปถึงผู้ให้บริการด้านสุขภาพ โรงแรม การคมนาคม ธนาคารและบริษัทประกันภัยรูปแบบต่างๆ รวมไปถึงอีกหลายผู้ให้บริการที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนและการรับโทษนั้นจะมีอัตราค่าปรับที่สูงลิ่ว (สมาคมผู้ดูแลเว็บไทย, 2561) ถือได้ว่าเป็นเพิ่มสิทธิ์ในการคุ้มครองและควบคุมข้อมูลส่วนบุคคลจากผู้ให้บริการออนไลน์ต่างๆ ที่มากขึ้น ทำให้เจ้าของข้อมูลสามารถควบคุมข้อมูลของตนได้อย่างมีประสิทธิภาพมากขึ้น

จากความก้าวหน้าทางด้านเทคโนโลยีการสื่อสารผ่านทางเครือข่ายอินเทอร์เน็ต ที่มีการพัฒนาอย่างต่อเนื่องและรวดเร็ว สิ่งที่จำเป็นต้องคำนึงถึงควบคู่ไปกับความก้าวหน้าทางด้านเทคโนโลยีการสื่อสารคือ การปกป้องและรักษาความปลอดภัยของข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ เนื่องจากการจัดเก็บข้อมูล การเปิดเผยและการเผยแพร่ข้อมูลส่วนบุคคลได้อยู่

ในรูปแบบของเอกสารอิเล็กทรอนิกส์ ที่มีความสะดวกและรวดเร็วมากขึ้นกว่าในอดีต ประกอบกับเมื่อศึกษาถึงกลุ่มบุคคลที่ได้รับผลกระทบ จากการสังเคราะห์ข่าวเกี่ยวกับปัญหาการถูกขโมยข้อมูลส่วนบุคคล จะพบว่าเป็นผู้ที่ใช้หรือเคยใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ และเป็นกลุ่มบุคคลที่เริ่มเข้าสู่การทำงานหรือวัยทำงานตอนต้น (First Jobber) หรือนักศึกษาจบใหม่ที่เริ่มต้นชีวิตการทำงาน ที่มีการปรับตัวออกสู่โลกของการทำงาน ซึ่งเป็นกลุ่มบุคคลที่เริ่มมีรายได้เป็นของตนเอง และต้องรับผิดชอบตนเองโดยเฉพาะด้านการจัดการและการวางแผนทางการเงินในฐานะผู้ใหญ่คนหนึ่ง (MoneyandBanking, 2019) ที่สามารถใช้จ่ายได้ด้วยเงินของตนเอง ทำให้สามารถเข้าถึงบริการทางการเงินต่างๆ ได้ เริ่มมีพฤติกรรมการใช้บัตรเครดิตและสินเชื่อส่วนบุคคลเพื่อการซื้อสินค้าและบริการออนไลน์ รับประทานอาหารนอกบ้านและการท่องเที่ยว (บริษัทข้อมูลเครดิตแห่งชาติ, 2562; โครงการฉลาดคิด ฉลาดใช้ ธนาคารกรุงศรีอยุธยา, 2562) และจากรายงานของศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย (2563) และศูนย์วิจัยเศรษฐกิจธุรกิจและเศรษฐกิจฐานราก ธนาคารออมสิน (2562) ได้ให้ข้อมูลพฤติกรรมกลุ่มวัยทำงานตอนต้นว่ามีการเปลี่ยนแปลงตามกระแสของเทคโนโลยี กล่าวคือกลุ่มวัยทำงานตอนต้นมีความนิยมในการซื้อขายสินค้าออนไลน์และการใช้โมบายแบ้งก์กิ้งเป็นช่องทางในการชำระค่าสินค้า ทางอิเล็กทรอนิกส์ที่เพิ่มมากขึ้น ซึ่งกลุ่มวัยทำงานตอนต้นถือว่าจัดอยู่ในกลุ่มเจเนอเรชั่นวาย เป็นกลุ่มบุคคลที่มีขนาดใหญ่ที่สุดของประเทศไทย คิดเป็นร้อยละ 28.00 ของประชากรทั้งหมด (โครงการสุขภาพคนไทย, 2560; ฐานเศรษฐกิจ, 2562) และเป็นกลุ่มบุคคลที่เกิดและเติบโตมาพร้อมกับการพัฒนาเทคโนโลยีการสื่อสาร ทำให้เป็นกลุ่มมีความสนใจและสามารถใช้งานเทคโนโลยีได้อย่างคล่องแคล่ว รวมไปถึงเป็นกลุ่มบุคคลที่ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์และซื้อสินค้าผ่านช่องทางออนไลน์มากกว่ากลุ่มอื่นๆ (นุศรา ทองรอด, 2555; อุไรพร ชลสิริรุ่งสกุล, 2554; Kim et al., 2015) ซึ่งทำให้โอกาสในการเปิดเผยข้อมูลส่วนบุคคลออนไลน์และพฤติกรรมสุ่มเสี่ยงต่อการถูกขโมยข้อมูลส่วนบุคคลจากการทำธุรกรรมทางอิเล็กทรอนิกส์ก็มากขึ้นตามไปด้วย (สมาคมประชาสัมพันธ์ไทย, 2563; ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย, 2563; สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2563) ดังนั้นงานวิจัยนี้มุ่งศึกษากลุ่มตัวอย่างวัยทำงานตอนต้นที่จัดอยู่ในกลุ่มเจเนอเรชั่นวาย โดยใช้กรอบการจัดแบ่งช่วงวัยทำงานของกรมอนามัย กระทรวงสาธารณสุข (2559) คือบุคคลที่มีอายุระหว่าง 20-29 ปี เมื่อพิจารณาจะเห็นว่าเป็นกลุ่มวัยเริ่มทำงานและเป็นช่วงอายุที่สำคัญเกี่ยวกับการบริหารจัดการด้านการเงิน หากสามารถเริ่มมีการปกป้องข้อมูลส่วนบุคคลจากการทำธุรกรรมทางอิเล็กทรอนิกส์ที่ดี จะทำให้รูปแบบการดำเนินชีวิตทางการเงินมีความปลอดภัยจากกลุ่มมิจฉาชีพ แต่ถ้าตั้งหลักหรือเริ่มต้นไม่

ดีเกี่ยวกับการปกป้องข้อมูลส่วนบุคคลจากการทำธุรกรรมทางอิเล็กทรอนิกส์ อาจทำให้รูปแบบการดำเนินชีวิตทางการเงินมีความเสี่ยงและเดือดร้อนได้ (The Standard, 2020)

จากประเด็นปัญหาดังกล่าวมาข้างต้น ผู้วิจัยจึงมีความสนใจศึกษาปัจจัยที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้นจากการให้ข้อมูลส่วนบุคคลที่สามารถเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์และเป็นการให้ข้อมูลส่วนบุคคลอย่างระมัดระวัง เพื่อให้เห็นถึงความจำเป็นที่จะต้องเร่งส่งเสริมและปลูกฝังให้กลุ่มวัยทำงานตอนต้นให้มีความรู้ ความเข้าใจที่ถูกต้องและกลวิธีในการปกป้องเกี่ยวกับการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ และเป็นที่น่าสนใจว่าในพื้นที่กรุงเทพมหานครและเขตปริมณฑลมีบุคคลที่ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์และการพาณิชย์อิเล็กทรอนิกส์จำนวนมากและมีอัตราที่เพิ่มขึ้นทุกปี และเป็นเขตที่มีจำนวนการจดทะเบียนของผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์รายปีสูงขึ้นอย่างต่อเนื่อง (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2561; กรมพัฒนาธุรกิจการค้า, 2562) ทั้งนี้จากการทบทวนและค้นคว้างานวิจัยในอดีตที่เกี่ยวข้องกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ในฐานข้อมูลงานวิจัยต่างประเทศ ได้แก่ ProQuest Dissertation & Thesis, Social Sciences Citation Index (Web of Science) และ Scopus (Elsevier) ตั้งแต่ปี พ.ศ. 2550-2562 พบว่าเริ่มให้ความสำคัญและศึกษาถึงแนวทางการปกป้องและรักษาความปลอดภัยของข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (Chellappa, 2008; Fernandes, 2013; Isaac & Sherali, 2014; Boerman et al., 2018) สำหรับประเทศไทยนั้นพบว่ามีงานวิจัยที่ผ่านมามีการศึกษาเรื่องนี้ค่อนข้างน้อยและเป็นเพียงงานวิจัยเชิงการสำรวจ (Survey) ในพฤติกรรมการยอมรับเทคโนโลยีและการตัดสินใจใช้บริการบนธุรกรรมทางอิเล็กทรอนิกส์เท่านั้น (ธนวรรณ สำนวนกลาง, 2559; สุรัสสา ลิมปพานนท์, 2561; วิวัฒณ์ ขันธเขตต์ และ สิงหา ฉวีสุข, 2562). และหากเป็นองค์ความรู้จากการบันทึกเป็นหนังสือคู่มือเพื่อใช้งานธุรกรรมทางอิเล็กทรอนิกส์อย่างปลอดภัยนั้นยังมีการเผยแพร่ข้อมูลไม่มากนักและไม่ปรับให้ใช้งานได้ทันต่อสถานการณ์ในปัจจุบันที่เริ่มมีการใช้งานธุรกรรมทางอิเล็กทรอนิกส์ผ่านแอปพลิเคชันจำนวนมากขึ้น นอกจากนี้ จากการค้นคว้างานวิจัยที่เกี่ยวข้องยังไม่พบการทำวิจัยในรูปแบบความสัมพันธ์โครงสร้างเชิงเส้นของการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น เนื่องจากรูปแบบความสัมพันธ์โครงสร้างเชิงเส้นเป็นวิธีการทางสถิติที่สามารถใช้ในการยืนยันโครงสร้างทฤษฎีว่าสามารถนำไปใช้กับข้อมูลเชิงประจักษ์ และเป็นเทคนิควิธีการวิเคราะห์ข้อมูลทางสถิติสำหรับงานวิจัยที่มุ่งศึกษารูปแบบความสัมพันธ์เชิงเหตุระหว่างตัวแปรแฝงเชิงทฤษฎี (Constructs) ที่มีความสัมพันธ์ต่อกัน

หลายๆ ตัวแปร ได้ทำให้ผลการวิเคราะห์ข้อมูลมีความถูกต้องมากยิ่งขึ้น (Schumacker & Lomax, 2010)

จากการทบทวนวรรณกรรมที่เกี่ยวข้องข้างต้น พบว่าปัญหาการถูกขโมยข้อมูลส่วนบุคคลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่เพิ่มมากขึ้นในสังคมปัจจุบัน ซึ่งลักษณะของสังคมของประเทศไทยกำลังเข้าสู่สังคมไร้เงินสด (Cashless Society) ที่ลดการใช้เงินสดและรูปแบบการชำระเงินที่มีการเปลี่ยนแปลงไปจากเดิม (สถาบันวิทยาการตลาดทุน, 2560; ธนาคารแห่งประเทศไทย, 2561) รวมทั้งรายงานสถานการณ์เกี่ยวกับโรคติดเชื้อไวรัสโคโรนาสายพันธุ์ใหม่ 2019 (COVID-19) ที่เกิดขึ้น (World Health Organization, 2020a; กรมควบคุมโรค กระทรวงสาธารณสุข, 2563) ที่รณรงค์ลดพฤติกรรมการใช้เงินสด ธนบัตรและเหรียญซึ่งอาจจะเป็นสื่อในการแพร่เชื้อโรคได้ เพราะมีการเปลี่ยนผ่านหลายมือจากบุคคลหนึ่งไปยังบุคคลหนึ่งอย่างรวดเร็ว และส่งเสริมการใช้จ่ายแบบไร้เงินสดรูปแบบต่าง ๆ โดยเฉพาะอย่างยิ่ง การจ่ายเงินผ่านบริการธุรกรรมทางอิเล็กทรอนิกส์บนสมาร์โฟน ซึ่งเป็นวิธีการชำระเงินที่ไม่จำเป็นต้องสัมผัสกับวัตถุใด ๆ นอกจากสมาร์ทโฟนของตนเอง ซึ่งเป็นทางเลือกที่เสี่ยงจากเชื้อโรคน้อยกว่ามาก ทำให้ผู้วิจัยเห็นว่าจำเป็นต้องศึกษาปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้นในเขตกรุงเทพมหานครและปริมณฑล เพื่อหาข้อเท็จจริงสำคัญที่แสดงถึงความสัมพันธ์ของตัวแปรเชิงเหตุและผลระหว่างตัวแปรได้อย่างครอบคลุมและมีความชัดเจนที่สามารถนำไปสู่แนวทางปฏิบัติในการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ที่ถูกต้องและเหมาะสม ผลจากงานวิจัยนี้จะเป็นแนวทางป้องกันจากการถูกขโมยข้อมูลส่วนบุคคลในกลุ่มผู้บริโภค ข้อควรปฏิบัติที่เหมาะสมในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งปัจจุบันสมาร์ทโฟนมีการใช้งานกันอย่างแพร่หลายผ่านทางแอปพลิเคชันต่างๆ และกลายเป็นส่วนหนึ่งของชีวิตประจำวัน ดังนั้นควรมีศึกษาถึงพฤติกรรมการปกป้องข้อมูลส่วนบุคคลและการตระหนักถึงภัยในยุคดิจิทัลจากการขโมยข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ที่อาจเกิดขึ้นต่อไป

วัตถุประสงค์การวิจัย

เพื่อทดสอบแบบจำลองรูปแบบความสัมพันธ์โครงสร้างเชิงเส้นของปัจจัยทางจิตวิทยาและสังคมที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้นในเขตกรุงเทพมหานครและปริมณฑล

ประโยชน์ของการวิจัย

ผลจากการศึกษาก่อให้เกิดคุณค่าด้านวิจัยและการนำไปใช้ ดังนี้

1. **ด้านการวิจัย**

ทำให้เกิดความเข้าใจในรูปแบบความสัมพันธ์โครงสร้างเชิงเส้นของปัจจัยทางจิตวิทยาและสังคมที่มีผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น จากการนำทฤษฎีแรงจูงใจเพื่อการป้องกัน (Protection Motivation Theory: PMT) ของ Rogers (1983) ที่นำมาใช้ในการศึกษาทางด้านสุขภาพสำหรับการป้องกันโรค ร่วมกับแบบจำลองการยอมรับการใช้เทคโนโลยี (Technology Acceptance Model: TAM) ของ Davis et al. (1989) ซึ่งจากการทบทวนวรรณกรรมและงานวิจัยที่ผ่านมายังไม่ปรากฏของการนำทฤษฎีแรงจูงใจเพื่อการป้องกันร่วมกับแบบจำลองการยอมรับการใช้เทคโนโลยีมาใช้ศึกษาในบริบทสังคมไทย โดยเฉพาะอย่างยิ่งการศึกษาในกลุ่มวัยทำงานตอนต้น ดังนั้นการนำทฤษฎีแรงจูงใจเพื่อการป้องกันร่วมกับแบบจำลองการยอมรับการใช้เทคโนโลยีมาประยุกต์ใช้ในงานวิจัยนี้ จะทำให้ทราบว่าแบบจำลองที่งานวิจัยนี้ได้พัฒนาขึ้นจากบริบทสังคมตะวันตกนั้น จะสามารถอธิบายปัจจัยทางจิตวิทยา สังคมและพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้นในบริบทสังคมไทยที่แตกต่างกันออกไปได้หรือไม่ อย่างไร รวมไปถึงการศึกษาในกลุ่มวัยทำงานตอนต้นที่มีความเฉพาะเจาะจง ที่แตกต่างไปจากกลุ่มวัยทำงานโดยทั่วไป ซึ่งจะทำให้เกิดความเข้าใจและอธิบายปรากฏการณ์ของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้นได้อย่างชัดเจนมากขึ้น อีกทั้งเป็นการต่อยอดและเพิ่มพูนองค์ความรู้ในทฤษฎีแรงจูงใจเพื่อการป้องกันและแบบจำลองการยอมรับการใช้เทคโนโลยี

2. **ด้านการนำไปใช้**

หน่วยงานที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์ การคุ้มครองข้อมูลส่วนบุคคล การละมิดความเป็นส่วนตัวบนธุรกรรมทางอิเล็กทรอนิกส์และอาชญากรรมทางเทคโนโลยี ทำให้เข้าใจถึงความสัมพันธ์ในเชิงเหตุและผลของตัวแปรต่างๆ และสามารถนำไปประยุกต์ใช้เป็นแนวทางในการส่งเสริม ประชาสัมพันธ์ สนับสนุนและแนวปฏิบัติในการปกป้องข้อมูลส่วนบุคคลให้กับผู้ใช้บริการ ตระหนักถึงความปลอดภัยและใช้บริการธุรกรรมทางอิเล็กทรอนิกส์อย่างระมัดระวัง รวมไปถึงหน่วยงานด้านการพัฒนาระบบสารสนเทศและเทคโนโลยี ใช้เป็นข้อมูลสู่การพัฒนานวัตกรรมเพื่อตอบสนองให้ผู้ใช้บริการเกิดการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ขอบเขตของการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงปริมาณ เพื่อทดสอบแบบจำลองรูปแบบความสัมพันธ์โครงสร้างเชิงเส้นของปัจจัยทางจิตวิทยาและสังคมที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ในฐานะที่เป็นกลุ่มผู้บริโภคหรือผู้ซื้อสินค้าและบริการออนไลน์ (Customer/Buyer) จากการให้ข้อมูลส่วนบุคคลและเพื่อการใช้งานธุรกรรมทางอิเล็กทรอนิกส์อย่างระมัดระวัง ได้แบ่งขอบเขตของการศึกษาวิจัย ดังนี้

ขอบเขตด้านตัวแปรที่ศึกษา

ตัวแปรที่ใช้ศึกษาในงานวิจัยนี้ ประกอบด้วยตัวแปรแฝงภายนอก (Exogenous Variables) และตัวแปรแฝงภายใน (Endogenous Variables) ดังนี้

ตัวแปรแฝงภายนอก ได้แก่

ตัวแปรทางสังคม จำนวน 1 ตัวแปร ได้แก่

การคล้อยตามกลุ่มอ้างอิง (Subjective Norms)

ตัวแปรสาเหตุทางจิต จำนวน 6 ตัวแปร ได้แก่

คุณลักษณะของระบบ (System Characteristics)

การรับรู้ถึงโอกาสเสี่ยง (Perceived Vulnerability)

การรับรู้ถึงความรุนแรง (Perceived Severity)

ความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล (Response Efficacy)

ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล (Self-efficacy)

ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคล (Response Cost)

ตัวแปรแฝงภายใน ได้แก่

ตัวแปรสาเหตุทางจิต จำนวน 5 ตัวแปร ได้แก่

การรับรู้ถึงประโยชน์ในการตั้งค่าการปกป้องข้อมูลส่วนบุคคล (Perceived Usefulness)

การรับรู้ถึงความง่ายในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล (Perceived Ease of Use)

ทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคล (Attitude)

ความตั้งใจในการปกป้องข้อมูลส่วนบุคคล (Intention)

และพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (Privacy Data Protection Behaviors)

ขอบเขตด้านวิธีดำเนินการวิจัย

1) ขอบเขตด้านพื้นที่

แหล่งพื้นที่ในการเก็บรวบรวมข้อมูลในงานวิจัยนี้คือ สถานที่ทำงานของหน่วยงานทั้งภาครัฐและภาคเอกชน ในเขตกรุงเทพมหานครและปริมณฑล ที่ได้รับอนุญาตและให้ความร่วมมือในการรวบรวมเก็บข้อมูล

2) ขอบเขตด้านประชากรและกลุ่มตัวอย่าง

ประชากรที่ศึกษาคือ กลุ่มผู้บริโภคที่ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเป็นวัยทำงานตอนต้น (First Jobbers) ที่มีอายุระหว่าง 20-29 ปี โดยใช้กรอบการจัดแบ่งช่วงวัยทำงานของกรมอนามัย กระทรวงสาธารณสุข (2559)

กลุ่มตัวอย่าง งานวิจัยนี้แบ่งกลุ่มพื้นที่ในการเก็บรวบรวมข้อมูลออกเป็นเขตกรุงเทพมหานคร จำนวน 5 กลุ่ม และปริมณฑล จำนวน 5 จังหวัด จากนั้นทำการสุ่มกลุ่มตัวอย่างโดยวิธีการสุ่มตัวอย่างแบบกลุ่ม 2 ขั้นตอน (Two-stage Cluster Sampling) ประกอบด้วย ขั้นตอนที่ 1 การสุ่มเลือกตามการแบ่งเขตการปกครองของกรุงเทพมหานครและการสุ่มเลือกจังหวัดของปริมณฑล โดยวิธีการจับสลาก และขั้นตอนที่ 2 การสุ่มเลือกเขตในกรุงเทพมหานครและการสุ่มเลือกอำเภอสำหรับกลุ่มตัวอย่างปริมณฑล โดยวิธีการจับสลาก จากนั้นสอบถามไปยังหน่วยงานในพื้นที่ที่ให้ความร่วมมือในการรวบรวมเก็บข้อมูลและคัดเลือกกลุ่มตัวอย่าง (Screening Question) โดยมีเงื่อนไขว่ามีช่วงอายุ 20-29 ปีและมีความถี่ในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์มากกว่า 5 ครั้งต่อเดือนในรอบ 6 เดือนที่ผ่านมา สำหรับการศึกษาที่มีการวิเคราะห์องค์ประกอบ (Factor Analysis) จากข้อเสนอแนะเกี่ยวกับขนาดตัวอย่างที่เหมาะสมของ Kline (2010) ที่สามารถเป็นตัวแทนของประชากรและมีจำนวนเพียงพอที่ทำให้ผลการวิจัยเชื่อถือได้ ควรให้มีขนาดตัวอย่างในการศึกษาวิจัยไม่ต่ำกว่า 200 ตัวอย่าง และการวิเคราะห์แบบจำลองสมการโครงสร้าง (Structure Equation Modeling) ขนาดของตัวอย่างควรมีจำนวน 15-20 เท่าของตัวแปรสังเกต (Hair, et al., 2010) ในการวิจัยครั้งนี้ผู้วิจัยกำหนดขนาดตัวอย่างเป็นกลุ่มวัยทำงานตอนต้นในเขตกรุงเทพมหานครและปริมณฑล จำนวน 400 คน ขึ้นไป

นิยามศัพท์เฉพาะ

ข้อมูลส่วนบุคคล หมายถึง ข้อมูลของบุคคลธรรมดาที่สามารถระบุหรือเชื่อมโยงถึงตัวบุคคลในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ไม่ว่าจะทางตรงหรือทางอ้อม และแสดงถึงการเป็นเจ้าของข้อมูล เช่น ชื่อจริง นามสกุลจริง หมายเลขบัตรประจำตัวประชาชน วันเดือนปีเกิด หมายเลขโทรศัพท์ หมายเลขบัญชีธนาคาร อีเมล์ รูปถ่าย ที่อยู่ ประวัติทางการศึกษา หมายเลขบัตรเงินอิเล็กทรอนิกส์ ความสนใจและพฤติกรรมการซื้อสินค้าและบริการออนไลน์ผ่านร้านค้าการพาณิชย์อิเล็กทรอนิกส์

ธุรกรรมทางอิเล็กทรอนิกส์ หมายถึง การเข้าใช้งานธุรกรรมทางการเงินผ่านช่องทางอิเล็กทรอนิกส์ที่มีการระบุตัวตนของผู้ใช้งานและสามารถดำเนินการทำธุรกรรมทางการเงินได้ด้วยตนเองในฐานะผู้บริโภค จำแนกอุปกรณ์อิเล็กทรอนิกส์ในการใช้บริการเป็น 2 ช่องทาง ได้แก่ 1) เครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งรวมไปถึงคอมพิวเตอร์แบบพกพา (Laptop) และคอมพิวเตอร์แบบรับข้อมูลด้วยการเขียนบนจอภาพ (Tablet) และ 2) สมาร์ทโฟน (Smart Phone)

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

ในการวิจัยครั้งนี้ เป็นการศึกษารูปแบบความสัมพันธ์เชิงเหตุของปัจจัยทางจิตและสังคมที่ส่งผลต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ผู้วิจัยได้ศึกษาแนวคิดทฤษฎี เอกสารและงานวิจัยที่เกี่ยวข้อง ดังต่อไปนี้

1. พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

1.1 ความหมายและประเภทของข้อมูลส่วนบุคคล

1.2 ความหมายและประเภทของธุรกรรมทางอิเล็กทรอนิกส์

1.3 แนวคิดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

1.4 ความหมายของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

1.5 องค์ประกอบของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

1.6 การวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

1.7 งานวิจัยที่เกี่ยวข้องพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

2. ทฤษฎีและแนวคิดเกี่ยวกับสาเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

2.1 การวิเคราะห์สาเหตุพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

2.2 ทฤษฎีแรงจูงใจเพื่อการป้องกัน (The Protection Motivation Theory: PMT)

2.3 แบบจำลองการยอมรับการใช้เทคโนโลยี (Technology Acceptance Model: TAM)

2.4 ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

3. กรอบแนวคิดในการวิจัย

4. แบบจำลองและสมมติฐานการวิจัย

5. นิยามปฏิบัติการตัวแปร

1. พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

1.1 ความหมายและประเภทของข้อมูลส่วนบุคคล

ความหมายของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล (Personal Information) หมายถึง ข้อความที่เกี่ยวข้องกับบุคคล สามารถระบุถึงตัวบุคคลนั้นได้ไม่ว่าจะโดยตรงหรือโดยอ้อม ซึ่งอาจกระทำได้โดยการอ้างอิงหมายเลขบัตรประจำตัว หรือลักษณะเฉพาะอย่างอื่นของบุคคลนั้นๆ ไม่ว่าจะเป็นลักษณะทางกายภาพ ฐานะทางเศรษฐกิจ หรือเอกลักษณ์ทางสังคม (EU Directive 95/46/EU, 1995) สำหรับ Federal Data Protection Act (2001) ได้ให้ความหมายข้อมูลส่วนบุคคลว่าเป็นสารสนเทศที่เกี่ยวข้องกับบุคคล ซึ่งบุคคลนั้นเป็นเจ้าของข้อมูล รวมไปถึงพฤติกรรมที่สามารถชี้เฉพาะตัวบุคคลนั้นได้

ศูนย์วิจัยกฎหมายและการพัฒนา จุฬาลงกรณ์มหาวิทยาลัย (2561: 24-25) ได้นิยามข้อมูลส่วนบุคคลว่าเป็นข้อมูลใดๆ ที่ระบุถึงเจ้าของข้อมูลได้ และอาจเป็นข้อมูลที่มนุษย์เข้าใจได้หรือไม่ก็ได้ โดยเป็นข้อมูลที่คอมพิวเตอร์หรืออุปกรณ์ต่างๆ สามารถเข้าถึงได้โดยอัตโนมัติ และได้ให้ตัวอย่างข้อมูลที่เป็นข้อมูลส่วนบุคคลดังนี้ 1) ชื่อ-นามสกุล หรือชื่อเล่น 2) เลขประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร เลขบัตรเครดิต รวมถึงการเก็บเป็นภาพสำเนาจากเลขที่กล่าวมา 3) ที่อยู่ อีเมล์ เลขโทรศัพท์ 4) ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP Address, MAC Address, Cookie ID 5) ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า ลายนิ้วมือ ฟิล์มเอกซเรย์ ข้อมูลพันธุกรรม 6) ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์ โฉนดที่ดิน 7) ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิด สถานที่เกิด สัญชาติ น้ำหนัก ส่วนสูง ตำแหน่งที่อยู่ ข้อมูลการศึกษา ข้อมูลทางการเงิน 8) ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม แม้ไม่สามารถระบุไปถึงตัวบุคคลได้แต่หากใช้ร่วมกับระบบดัชนีข้อมูลอีกระบบหนึ่งก็จะสามารถระบุไปถึงตัวบุคคลได้ 9) ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง 10) ข้อมูลบันทึกต่างๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่างๆ ของบุคคล เช่น log file และ 11) ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

โดยสรุป แต่ละประเทศมีคำนิยามของข้อมูลส่วนบุคคลที่แตกต่างกันออกไป ซึ่งส่วนใหญ่จะหมายถึงข้อมูล สารสนเทศที่สามารถระบุและเชื่อมโยงถึงเฉพาะบุคคลนั้นๆ ได้ ในงานวิจัยนี้จะหมายถึงข้อมูลของบุคคลที่สามารถระบุหรือเชื่อมโยงถึงตัวบุคคลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์

ประเภทของข้อมูลส่วนบุคคล

จากการศึกษาของศิริกุล ภู่พันธ์ และนคร เสรีรักษ์ (2544) สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (2557) และธาริณี มณีรอด (2559) ได้จัดข้อมูลส่วนบุคคลออกเป็น 2 ประเภท คือ ข้อมูลส่วนบุคคลทั่วไป (Non-Sensitive Data) และข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) โดยข้อมูลส่วนบุคคลทั้งสองประเภทมีความแตกต่างกันดังนี้ 1) ข้อมูลส่วนบุคคลทั่วไป เป็นข้อมูลข่าวสารใดๆ ที่เกี่ยวข้องกับบุคคล สามารถบ่งชี้เฉพาะตัวบุคคลและนำมาประมวลผลเป็นข้อเท็จจริงที่บ่งชี้ลักษณะเฉพาะตัวบุคคลได้ ได้แก่ ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์และลักษณะทางกายภาพของบุคคล โดยสภาพของข้อมูลเหล่านี้เป็นข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้ และ 2) ข้อมูลส่วนบุคคลที่มีความอ่อนไหว เป็นข้อมูลที่เป็นความลับ ไม่พึงประสงค์ที่จะให้เปิดเผย ได้แก่ ข้อมูลที่เกี่ยวกับเชื้อชาติ สถานะทางการเงิน ความเชื่อในลัทธิศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ประวัติสุขภาพ หรือข้อมูลอื่นที่กระทบต่อความรู้สึกของผู้อื่น

ทั้งนี้ การแบ่งประเภทข้อมูลส่วนบุคคลในประเด็นความอ่อนไหวที่อาจส่งผลกระทบต่อเจ้าของข้อมูล หากมีการเปิดเผยข้อมูลนั้น สามารถแบ่งออกได้เป็น 3 ระดับ (ปิยะพร วงศ์เบี้ยสัจจ์, 2552; Chang & Heo, 2014; สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2562) ดังนี้ 1) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับต่ำ (Low-Sensitivity) เป็นข้อมูลที่เกี่ยวข้องกับบุคคลที่มีความอ่อนไหว เนื่องมาจากข้อมูลเหล่านี้อาจช่วยทำให้ได้มาซึ่งข้อมูลที่มีระดับความอ่อนไหวสูงขึ้น 2) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับปานกลาง (Moderate-Sensitivity) เป็นข้อมูลบุคคลที่มีความอ่อนไหวมาก ในแง่ที่มีโอกาสที่จะก่อให้เกิดความเสียหาย เมื่อข้อมูลถูกนำเอาไปใช้ในทางที่ผิดอยู่ในระดับสูง ครอบคลุมถึงข้อมูลประเภทที่เกี่ยวกับความคิดเห็นของบุคคล และ 3) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับสูง (High-Sensitivity) เป็นข้อมูลรายละเอียดส่วนตัวของบุคคล ในส่วนที่เกี่ยวข้องกับประวัติทางการแพทย์ พฤติกรรมทางเพศ หรือข้อเท็จจริงด้านอื่นๆ ในชีวิตของบุคคล ซึ่งเป็นเรื่องลับเฉพาะและไม่ควรถูกเก็บรวบรวมไว้โดยสิ้นเชิง

1.2 ความหมายและประเภทของธุรกรรมทางอิเล็กทรอนิกส์

ความหมายของธุรกรรมทางอิเล็กทรอนิกส์

ธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions) เป็นกิจกรรมที่กระทำขึ้นระหว่างหน่วยธุรกิจ บุคคล รัฐบาล ตลอดจนองค์กรเอกชนหรือองค์กรของรัฐใดๆ เพื่อวัตถุประสงค์ทางธุรกิจ การค้า การบริการและการติดต่องานราชการ โดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือบางส่วน ซึ่งไม่จำเป็นต้องรวมถึงขั้นตอนการจ่ายเงิน (พระราชบัญญัติว่าด้วยธุรกรรมทาง

อิเล็กทรอนิกส์, 2544 อ้างใน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2558) และจากการศึกษาในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (2544) แก้ไขเพิ่มเติมฉบับที่ 2 (2551) พบว่าธุรกรรมทางอิเล็กทรอนิกส์ หมายถึงธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน ซึ่งเป็นการกระทำที่เกี่ยวข้องกับการค้าขายโดยอาศัยอิเล็กทรอนิกส์อย่างโทรศัพท์ อีเมล์ เป็นสื่อ โดยไม่จำเป็นต้องเป็นการกระทำตลอดทั้งกระบวนการก็ได้ เพียงแต่ให้มีส่วนหนึ่งในขั้นตอนการค้าขายหรือการติดต่อที่ใช้สื่ออิเล็กทรอนิกส์ก็เพียงพอ เช่น หากใช้อีเมล์ในขั้นตอนการสั่งซื้อสินค้าเพียงขั้นตอนเดียว แต่ขั้นตอนอื่นๆ อย่างการออกใบเสร็จรับเงิน การส่งสินค้า ไม่ได้ใช้สื่อหรือระบบอิเล็กทรอนิกส์ ถือได้ว่ากระบวนทั้งหมดนั้นเป็นธุรกรรมทางอิเล็กทรอนิกส์ด้วย ดังนั้นการสั่งซื้อสินค้าทางอินเทอร์เน็ตจะถือเป็นธุรกรรมทางอิเล็กทรอนิกส์ รวมถึงการตกลงทำสัญญาซื้อขายบนอินเทอร์เน็ต การโอนเงินด้วยระบบอัตโนมัติ การสมัครสมาชิกและการสอบถามข้อมูลผ่านระบบออนไลน์ (สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, 2557; ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย 2561)

ในงานวิจัยนี้ ธุรกรรมทางอิเล็กทรอนิกส์จะหมายถึงกิจกรรมของบุคคลในฐานะผู้บริโภค จากการเข้าใช้บริการทางการเงินต่างๆ ในการซื้อขายสินค้าและบริการออนไลน์ผ่านสื่ออิเล็กทรอนิกส์ จะทั้งหมดหรือเพียงบางส่วนของกระบวนการก็ได้

ประเภทของธุรกรรมทางอิเล็กทรอนิกส์

เอกสารจากประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ราชกิจจานุเบกษา (2555: 39-41) เรื่องประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย ได้แบ่งประเภทของธุรกรรมทางอิเล็กทรอนิกส์ออกเป็น 6 ประเภท ดังนี้ 1) ด้านการชำระเงินทางอิเล็กทรอนิกส์ ตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 2) ด้านการเงินของธนาคารพาณิชย์ ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน 3) ด้านประกันภัย ตามกฎหมายว่าด้วยประกันชีวิตและประกันวินาศภัย 4) ด้านหลักทรัพย์ของผู้ประกอบธุรกิจหลักทรัพย์ตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์ 5) ธุรกรรมทางอิเล็กทรอนิกส์ที่จัดเก็บรวบรวมและให้บริการข้อมูลของบุคคล หรือทรัพย์สินหรือทะเบียนต่างๆ ที่เป็นเอกสารมหาชนหรือที่เป็นข้อมูลสาธารณะ และ 6) ธุรกรรมทางอิเล็กทรอนิกส์ในการให้บริการด้านสาธารณูปโภคและบริการสาธารณะ ที่ต้องดำเนินการอย่างต่อเนื่องตลอดเวลา

จากรายงานธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์สำหรับการให้บริการการเงิน (E-Banking) และการชำระเงินทางอิเล็กทรอนิกส์ (E-Payment) ของสายกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย (2557) ได้กำหนดขอบเขตกระบวนการทำธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์สำหรับลูกค้ารายย่อย ดังต่อไปนี้ 1) การให้บริการธุรกรรมผ่านทางอินเทอร์เน็ตแบ้งก์กิ้ง (Internet Banking) 2) การให้บริการธุรกรรมผ่านทางโมบายแบ้งก์กิ้ง (Mobile Banking) 3) การให้บริการธุรกรรมด้วยบัตรเงินอิเล็กทรอนิกส์ (E-Money) ทั้งประเภทบัตรเงินอิเล็กทรอนิกส์ (Card Based) และสื่อการชำระเงินที่ไม่ใช่บัตร (Non-Card Based) หรือกระเป๋าเงินอิเล็กทรอนิกส์ (E-Wallet/E-Purse) 4) การรับชำระการซื้อสินค้าและบริการผ่านร้านค้าการพาณิชย์อิเล็กทรอนิกส์ (Payment Gateway) และ 5) การให้บริการรายการชำระเงินระหว่างธนาคาร ประกอบด้วยจุดเชื่อมต่อของการรับส่งข้อมูลรายการชำระเงินทางอิเล็กทรอนิกส์ (Switching) ให้กับผู้ให้บริการตามที่ได้ตกลงกันไว้ และบริการหักบัญชี (Clearing) ซึ่งเป็นบริการรับส่งข้อมูล ตรวจสอบและยืนยันตามคำสั่งของการชำระเงิน

งานวิจัยนี้ผู้วิจัยมุ่งศึกษาธุรกรรมทางอิเล็กทรอนิกส์ ประเภทการชำระเงินทางอิเล็กทรอนิกส์ในฐานะผู้บริโภค ที่ให้บริการธุรกรรมผ่านทางอินเทอร์เน็ตแบ้งก์กิ้งและโมบายแบ้งก์กิ้งรวมไปถึงบัตรเงินอิเล็กทรอนิกส์และกระเป๋าเงินอิเล็กทรอนิกส์

ประโยชน์ของธุรกรรมทางอิเล็กทรอนิกส์

จากความก้าวหน้าของเทคโนโลยีการสื่อสารทางเครือข่ายอินเทอร์เน็ต ในปัจจุบันบริการธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์ได้รับความนิยมใช้บริการอย่างแพร่หลายและมีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง ธนาคารพาณิชย์หลายแห่งได้มีบริการธนาคารอิเล็กทรอนิกส์ทั้งช่องทางอินเตอร์เน็ตแบ้งก์กิ้งและโมบายแบ้งก์กิ้ง (ธนาคารแห่งประเทศไทย, 2560) รวมทั้งผู้ใช้บริการสามารถเลือกทำธุรกรรมทางอิเล็กทรอนิกส์บนผ่านอุปกรณ์คอมพิวเตอร์ประเภทต่างๆ ได้ เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล สมาร์ทโฟน แท็บเล็ต จากรายงานของธนาคารกสิกรไทย (2560) และธนาคารไทยพาณิชย์ (2560) กล่าวถึงข้อดีของการโอนเงินออนไลน์ดังนี้ 1) สามารถทำได้สะดวก รวดเร็ว ประหยัดเวลาโดยไม่จำเป็นต้องไปเข้าแถวเพื่อโอนเงินที่ตู้เอทีเอ็มหรือหน้าเคาน์เตอร์ (Counter) ธนาคารสาขา รวมไปถึงการประหยัดค่าใช้จ่ายในการเดินทาง 2) ไม่จำเป็นต้องพกเงินสดจำนวนมาก ในปัจจุบันหลายร้านค้าได้ร่วมรายการส่งเสริมการขายกับธนาคารพาณิชย์ต่างๆ เพื่อให้สามารถใช้วิธีการโอนเงินออนไลน์หรือใช้กระเป๋าเงินอิเล็กทรอนิกส์ได้แทนการจ่ายเงินสด 3) มีโอกาสได้รับสิทธิพิเศษ เช่น การรับเงินคืนจากการซื้อสินค้าและบริการผ่านแอปพลิเคชัน สิทธิ์แลกซื้อสินค้าในราคาพิเศษ เป็นต้น และ 4) ไม่เสีย

ค่าธรรมเนียมหากทำการโอนเงินผ่านพร้อมเพย์ (Promtpay) ซึ่งเป็นบริการรับและโอนเงินแบบใช้หมายเลขบัตรประชาชนหรือหมายเลขโทรศัพท์ แทนการใช้เลขที่บัญชีธนาคาร

อีกทั้งบริการของธนาคารทางอินเทอร์เน็ต ได้มีการพัฒนาให้เข้าถึงผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์มากขึ้นไปอีก โดยการใช้โมบายแบ้งก์กิ้งที่ให้บริการธุรกรรมทางการเงินผ่านแอปพลิเคชันของธนาคารเข้ามาใช้ในสมาร์ทโฟนของตัวเอง และสามารถใช้เป็นการแจ้งเตือนเพื่อให้ชำระเงินค่าสินค้าและบริการตามวันและเวลาที่กำหนด และสามารถตั้งโอนเงินล่วงหน้าได้ (ธนาคารกสิกรไทย, 2560) ซึ่งข้อดีของโมบายแบ้งก์กิ้ง ได้แก่ 1) ความสะดวกสบายในการทำธุรกรรมทางการเงิน ที่ไม่จำกัดด้านเวลาและสถานที่ 2) ไม่เสียเวลาในการเดินทางไปธนาคารสาขาหรือตู้เอทีเอ็ม ทำให้ประหยัดเวลาและค่าใช้จ่าย และ 3) ลดปัญหาอาชญากรรม การปล้นจี้จากการพกเงินสดเพื่อนำเงินไปฝากธนาคารสาขาหรือตู้เอทีเอ็ม และด้านการพาณิชย์อิเล็กทรอนิกส์ เมื่อศึกษาถึงระบบการชำระเงินทางอิเล็กทรอนิกส์ผ่านทางสมาร์ทโฟน จะเห็นว่าพฤติกรรมของผู้บริโภคได้มีการเปลี่ยนแปลงจากการซื้อสินค้าจากร้านค้าไปเป็นการสั่งซื้อสินค้าผ่านทางระบบออนไลน์มากขึ้นไม่ว่าจะเป็นหน้าเว็บไซต์ทั้งในประเทศและต่างประเทศ และระบบการชำระเงินของการพาณิชย์อิเล็กทรอนิกส์ได้มีหลากหลายรูปแบบมากขึ้น (ธนาคารแห่งประเทศไทย, 2560) เช่น การตัดเงินผ่านบัตรเครดิต การชำระเงินผ่านอินเทอร์เน็ตแบ้งก์กิ้งและโมบายแบ้งก์กิ้ง กระเป๋าเงินอิเล็กทรอนิกส์ เป็นต้น ซึ่งช่องทางการชำระเงินเหล่านี้ช่วยเพิ่มความสะดวกสบายให้กับผู้ใช้งานเป็นอย่างดี เช่นเดียวกับข้อดีของการโอนเงินออนไลน์

แม้ว่าปัจจุบันประเทศไทยยังไม่ได้เข้าสู่สังคมไร้เงินสดอย่างแท้จริง แต่รัฐบาลเริ่มมีการผลักดันที่จะนำประเทศเข้าสู่สังคมไร้เงินสดตามนโยบาย 4.0 ซึ่งจะเห็นได้จากธนาคารพาณิชย์ได้มีการปรับลดจำนวนธนาคารสาขาและจำนวนพนักงาน เนื่องจากการทำธุรกรรมทางอิเล็กทรอนิกส์นั้น สามารถช่วยอำนวยความสะดวกในการใช้ชีวิต ช่วยให้ทุกคนมีเวลาให้กับตนเองมากขึ้น มีเวลาให้กับครอบครัวและมีเวลาเพื่อเพิ่มพูนทักษะความรู้ใหม่ๆ ได้มากขึ้น เช่น การโอนเงินสามารถทำได้อย่างรวดเร็วโดยไม่ต้องเดินทางไปธนาคารสาขาและสามารถทำธุรกรรมทางการเงินผ่านทางสมาร์ทโฟนได้ และไม่เสียค่าธรรมเนียมการโอน (สถาบันวิทยาการตลาดทุน, 2560; ธนาคารแห่งประเทศไทย, 2561) จากการเปลี่ยนแปลงสภาพทางสังคมทางด้านธุรกรรมทางการเงิน สามารถสรุปข้อดีของสังคมไร้เงินสด ได้ดังนี้ 1) ลดต้นทุนการผลิตธนบัตรและเหรียญกษาปณ์ 2) ไม่เสียเวลาเดินทางไปยังธนาคารสาขา และมีความสะดวกในการชำระเงินจากการซื้อขายสินค้าและบริการออนไลน์ ที่มีรูปแบบการชำระเงินที่หลากหลาย และ 3) ลดปัญหาอาชญากรรม จากการที่ใช้เงินลดน้อยลงมีส่วนช่วยในการลดอัตราการฉกชิงวิ่งราวได้

1.3 แนวคิดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

แนวคิดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ เป็นแนวคิดที่มีรากฐานมาจากความเป็นส่วนตัวของข้อมูล (Privacy Information) ในประเด็นด้านจริยธรรม (Ethical Issues) ของยุคข้อมูล ข่าวสารหรือยุคสารสนเทศ (Information Age) เกี่ยวกับความกังวลข้อมูลด้านความเป็นส่วนตัว (Information Privacy Concerns) ที่เพิ่มขึ้นของชาวอเมริกัน จากการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ในองค์กร (Smith et al., 1996) หลังจากนั้น Cate (1997, p.33) ได้นำเสนอแนวคิดความเป็นส่วนตัวในยุคสารสนเทศ จากการที่มีการใช้งานคอมพิวเตอร์อย่างแพร่หลายในช่วง ค.ศ. 1980 โดยมีการพัฒนาเป็นกฎหมายคุ้มครองส่วนบุคคลที่คำนึงถึงสิทธิในข้อมูลของประชาชนที่เพิ่มมากขึ้น ซึ่งต่อมา Youn (2005) มีการเสนอแนวคิดของพฤติกรรมการรับรู้และการรับมือของความเป็นส่วนตัวออนไลน์ในกลุ่มวัยรุ่น อีกทั้งแนวคิดของ Moscardelli & Divine (2007) ที่กล่าวถึงความกังวลในกลุ่มวัยรุ่นต่อความเป็นส่วนตัวเมื่อมีการใช้งานอินเทอร์เน็ต โดยได้ศึกษารูปแบบทำนายการวิเคราะห์เชิงประจักษ์และความสัมพันธ์กับพฤติกรรมการปกป้องความเป็นส่วนตัว (Empirical Analysis Predictors and Relationships with Privacy Protecting Behaviors)

จะเห็นว่า แนวคิดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์นั้นมีส่วนเกี่ยวข้องกับพฤติกรรมการปกป้องความเป็นส่วนตัวผ่านทางเครือข่ายอินเทอร์เน็ต จากการศึกษาของ Son & Kim (2008) ได้นำเสนอการปกป้องข้อมูลส่วนบุคคลของผู้ใช้งานอินเทอร์เน็ต (Internet User's Information Privacy-Protective Responses) จากความนิยมในการใช้เครือข่ายอินเทอร์เน็ตและการพาณิชย์อิเล็กทรอนิกส์ที่เพิ่มขึ้น ที่ผู้ใช้งานสามารถเปิดเผยข้อมูลส่วนบุคคลได้มากขึ้น จนเป็นเหตุให้เกิดระดับความเสี่ยงและภัยคุกคาม เช่น การสวมรอย การโจรกรรมข้อมูลทางการเงิน การแอบอ้างเพื่อหาผลประโยชน์ทางการตลาด เป็นต้น รวมทั้งแนวคิดของ Lee et al. (2008) ซึ่งได้เสนอรูปแบบพฤติกรรมการปกป้องข้อมูลส่วนบุคคลออนไลน์ จากการศึกษาพฤติกรรมการปกป้องไวรัสคอมพิวเตอร์ (Virus Protection Behavior) และภัยคุกคามจากไวรัสคอมพิวเตอร์ (Computer Virus) เพื่อการใช้งานเครือข่ายอินเทอร์เน็ตอย่างปลอดภัย ดังนั้นแนวคิดพฤติกรรมการปกป้องข้อมูลส่วนบุคคล เป็นผลมาจากพฤติกรรมของผู้ใช้บริการอินเทอร์เน็ต การเปลี่ยนผ่านการใช้ชีวิตประจำวันไปสู่ชีวิตดิจิทัลที่เพิ่มขึ้นอย่างต่อเนื่อง ซึ่งความหลากหลายของกิจกรรมบนเครือข่ายอินเทอร์เน็ตส่งผลให้มีความเสี่ยงในการถูกละเมิด

ข้อมูลส่วนบุคคล รวมไปถึงความปลอดภัยของข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์

1.4 ความหมายของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ เป็นแนวคิดที่พัฒนามาจากพฤติกรรมการปกป้องความเป็นส่วนตัวผ่านทางเครือข่ายอินเทอร์เน็ต จากการทบทวนเอกสารที่เกี่ยวข้องพบผู้ให้ความหมายที่สามารถเทียบเคียงกับงานวิจัยนี้คือ Milne et al. (2004) ซึ่งได้ให้ความหมายไว้ว่าพฤติกรรมการปกป้องข้อมูลส่วนบุคคลในฐานะผู้บริโภค (Consumer's protection of online privacy) คือการหลีกเลี่ยงต่อความเสียหายและการถูกโจรกรรมข้อมูลส่วนบุคคลและข้อมูลทางการเงินผ่านทางอุปกรณ์อิเล็กทรอนิกส์

1.5 องค์ประกอบของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

การศึกษาองค์ประกอบพฤติกรรมการปกป้องข้อมูลส่วนบุคคล ได้มีนักวิชาการที่ศึกษาและจำแนกองค์ประกอบพฤติกรรมการปกป้องข้อมูลส่วนบุคคล เช่น การศึกษาของ Son & Kim (2008) ได้จำแนกองค์ประกอบพฤติกรรมการปกป้องข้อมูลส่วนบุคคลของผู้ใช้บริการเครือข่ายอินเทอร์เน็ต (Types of Information Privacy-Protective Reponses: IPPR) ในฐานะที่เป็นผู้บริโภคไว้ 3 องค์ประกอบ ได้แก่ องค์ประกอบที่หนึ่ง พฤติกรรมการให้ข้อมูลส่วนบุคคล (Information Provision) ประกอบด้วยการเลี่ยง (Refusal) ให้ข้อมูลส่วนบุคคลบนเว็บไซต์ และการให้ข้อมูลส่วนบุคคลที่เป็นเท็จหรือการบิดเบือนข้อมูลความจริง (Misrepresentation) องค์ประกอบที่สอง การกระทำเพื่อป้องกันปัญหาที่อาจเกิดขึ้น ประกอบด้วยการลบข้อมูล (Removal) ที่เกี่ยวข้องกับความเป็นส่วนตัวในกิจกรรมต่างๆ จากการใช้งานเครือข่ายอินเทอร์เน็ต เช่น การเลือกไม่เข้าร่วมรับข่าวสารออนไลน์ทางอีเมล์จากการสมัครเป็นสมาชิก และองค์ประกอบที่สาม การกระทำเพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการซื้อสินค้าออนไลน์ ประกอบด้วยการร้องเรียนหรือไม่พึงพอใจเกี่ยวกับสินค้าและบริการ ควรติดต่อหรือแจ้งไปยังร้านค้าออนไลน์โดยตรง ไม่ควรแสดงความคิดเห็นส่วนตัวที่ไม่พอใจบนเว็บไซต์

การศึกษาของ Buchanan et al. (2007) เกี่ยวกับองค์ประกอบของการปกป้องความเป็นส่วนตัวจากการใช้งานเครือข่ายอินเทอร์เน็ตทั่วไปและการพาณิชย์อิเล็กทรอนิกส์ โดยสรุปองค์ประกอบของพฤติกรรมการปกป้องความเป็นส่วนตัวเป็น 2 ด้าน ได้แก่ การปฏิบัติในข้อควรระวังทั่วไปและการปฏิบัติในข้อควรระวังด้านเทคนิค มีรายละเอียดดังนี้ 1) ด้านการปฏิบัติในข้อควรระวังทั่วไป (General Caution) เป็นการปฏิบัติตามข้อบังคับตามหลักการปกป้องข้อมูลส่วน

บุคคลทั่วไป เพื่อป้องกันปัญหาที่จะส่งผลกระทบกับตนเองหากเข้าใช้งานบริการออนไลน์ ทั้งนี้ เนื้อหาองค์ประกอบสอดคล้องกับองค์ประกอบด้านการปฏิบัติตนเมื่อเข้าใช้งานเครือข่ายอินเทอร์เน็ตโดยทั่วไป (Malhotra et al., 2004) เช่น เมื่อมีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตควรทำลายข้อมูลส่วนบุคคลหากสามารถเผยแพร่ข้อมูลไปยังบุคคลอื่นให้รับรู้ได้ การพยายามซ่อนหมายเลขบัตรเครดิตธนาคาร เมื่อเข้าใช้บริการซื้อสินค้าการพาณิชย์อิเล็กทรอนิกส์ การเข้าใช้งานหรือลงทะเบียนในเว็บไซต์นั้นก็ต่อเมื่อมีการแจ้งนโยบายความเป็นส่วนตัว การอ่านนโยบายความเป็นส่วนตัวทุกครั้งก่อนเข้าใช้งานเว็บไซต์นั้น การมองหาใบประกาศรับรองความเป็นส่วนตัว (Privacy Certification) หรือการแจ้งไม่ละเมิดความเป็นส่วนตัวจากเว็บไซต์ต่างๆ ก่อนที่จะลงทะเบียนเข้าใช้งานในเว็บไซต์นั้น และการอ่านข้อตกลง (License Agreement) ร่วมกันเกี่ยวกับความเป็นส่วนตัวของผู้ใช้งาน ก่อนที่จะทำการยอมรับเข้าใช้งานเว็บไซต์ เป็นต้น และ 2) การปฏิบัติในข้อควรระวังเพื่อปกป้องข้อมูลส่วนบุคคลด้านเทคนิค (Technical Protection) เป็นการปฏิบัติตามข้อบังคับตามหลักการปกป้องข้อมูลส่วนบุคคลทางด้านเทคนิค เพื่อป้องกันปัญหาที่จะส่งผลกระทบกับตนเองหากเข้าใช้งานบริการออนไลน์ โดยมีเนื้อหาองค์ประกอบสอดคล้องกับองค์ประกอบทางด้านเทคนิคเมื่อเข้าใช้งานเครือข่ายอินเทอร์เน็ต (Paine et al., 2007) เช่น การควบคุมช่องทางการสื่อสารออนไลน์จากการเป็นสมาชิกหรือการส่งเสริมการตลาดจากร้านค้าออนไลน์ต่างๆ (Opt-out) การลบคุกกี้ (Cookies) บนเว็บบราวเซอร์ (Web Browser) การพยายามปิดหน้าต่างป๊อบอัพ (Pop-up Window Blocked) เมื่อเข้าใช้งานเว็บไซต์ การติดตั้งโปรแกรมป้องกันไวรัส (Antivirus Program) เมื่อมีการเข้าใช้งานเว็บไซต์ควรทำการลบประวัติการใช้งาน (Clear Your Browser History) และเมื่อมีข้อความหรืออีเมล์เข้ามาจะได้ทำการตั้งค่าบล๊อก (Blocked) ข้อความหรืออีเมล์นั้นหากเป็นบุคคลที่ไม่รู้จักกันมาก่อน เป็นต้น

ในงานวิจัยของ Youn (2009) ได้กล่าวถึงปัจจัยที่เกี่ยวข้องกับความกังวลและอิทธิพลของการปกป้องความเป็นส่วนตัวบนโลกออนไลน์ในกลุ่มวัยรุ่น โดยแบ่งองค์ประกอบของพฤติกรรมการปกป้องความเป็นส่วนตัวบนโลกออนไลน์เป็น 3 องค์ประกอบ ได้แก่ องค์ประกอบที่หนึ่ง พฤติกรรมการให้ข้อมูลส่วนบุคคลที่ไม่ตรงกับความเป็นจริง (Fabricate) เป็นการกระทำที่แสดงถึงการเข้าใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ด้วยความตั้งใจใช้ชื่อปลอม (False Name) และการให้ข้อมูลส่วนบุคคลที่ไม่สมบูรณ์ (Incomplete Information) องค์ประกอบที่สอง พฤติกรรมการค้นคว้าและแสวงหา (Seek) ความรู้ เป็นการกระทำที่มุ่งพัฒนาความรู้ของตนเอง รวมทั้งการแสวงหาโอกาสจากการสอบถามหรือปรึกษาจากผู้รู้ เช่น บุคคลในครอบครัว อาจารย์ เป็นต้น ก่อนเข้าใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ รวมไปถึงการเข้าไปศึกษาและอ่าน

ประกาศเกี่ยวกับนโยบายความเป็นส่วนตัว (Privacy Statement) บนเว็บไซต์ก่อนเข้าใช้งานเครือข่ายอินเทอร์เน็ต และองค์ประกอบที่ 3 พฤติกรรมการละเว้น การปฏิเสธในการให้ข้อมูลส่วนบุคคล (Refrain) เป็นการกระทำเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการเรียกร้องขอข้อมูลส่วนบุคคลจากผู้ให้บริการเว็บไซต์ โดยการจะเข้าใช้บริการกับเว็บไซต์นั้นๆ หากไม่สอบถามข้อมูลส่วนบุคคลที่มากจนเกินไป และหากมีการสอบถามข้อมูลส่วนบุคคลเพิ่มเติมจะทำการขอยกเลิกและออกจากการเข้าใช้บริการอินเทอร์เน็ต

การศึกษาของ Boerman et al. (2018) ซึ่งได้ศึกษาองค์ประกอบของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลและความเป็นส่วนตัวจากการใช้งานอินเทอร์เน็ต (Privacy on the Internet) สามารถจำแนกเป็นองค์ประกอบเป็น 10 พฤติกรรมจากการใช้งานอินเทอร์เน็ต ได้แก่ 1) การปิดกั้นโฆษณา (Use an ad blocker) 2) การลบคุกกี้ (Delete cookies) 3) การไม่เข้าเยี่ยมชมเว็บไซต์ หากเว็บไซต์นั้นให้ทำการยอมรับเงื่อนไขการใช้งานคุ๊กกี้ (Accept cookies) หรือการเก็บประวัติหรือข้อมูลของผู้ใช้งานเมื่อเข้าเยี่ยมชมเว็บไซต์ผ่านทางเว็บเบราว์เซอร์ 4) การปฏิเสธที่จะยอมรับการใช้งานคุกกี้ (Decline to accept cookies) หากเว็บไซต์นั้นเสนอทางเลือกมาให้ 5) การเข้าใช้งานโหมดท่องเว็บไซต์แบบส่วนตัว (Private mode) 6) การลบประวัติหรือข้อมูลการท่องเว็บไซต์ผ่านทางเว็บเบราว์เซอร์ (Delete browser history) 7) การไม่เข้าร่วมในรายการส่งเสริมการขาย การตลาดของร้านค้าออนไลน์ (Opt-out) 8) การท่องเว็บไซต์ผ่านทางเว็บบราวเซอร์โดยเปิดใช้งานแบบ Do not track เพื่อป้องกันการติดตาม สะกดรอยและเก็บข้อมูลจากผู้ให้บริการอินเทอร์เน็ต 9) การใช้โปรแกรมลักษณะพิเศษ (Special software) เช่น Ghostery และ Abine Taco เพื่อป้องกันการเก็บข้อมูลการเข้าใช้งานบนเว็บไซต์ และ 10) การให้ข้อมูลส่วนบุคคลที่เป็นเท็จ (Wrong information) อาทิเช่น ชื่อปลอม อีเมล์ปลอม หากมีการสอบถามจากผู้ให้บริการอินเทอร์เน็ต

จากรายงานพฤติกรรมเกี่ยวกับวิธีการป้องกันจากการซื้อสินค้าออนไลน์บนสมาร์ทโฟน อย่างปลอดภัย (กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, 2561) เสนอแนวทางพฤติกรรมการป้องกันข้อมูลส่วนบุคคลจากการซื้อสินค้าออนไลน์บนสมาร์ทโฟน จำแนกเป็น 7 เรื่องดังนี้ 1) เมื่อเข้าซื้อสินค้าและบริการออนไลน์ผ่านทางเว็บไซต์ เว็บไซต์เหล่านั้นจะต้องขึ้นต้นด้วย HTTPS (Hypertext Transfer Protocol Secure) รวมไปถึงการทำธุรกรรมทางการเงินด้วย ซึ่งเว็บไซต์ที่หลอกลวงให้ทำธุรกรรมทางการเงินมักจะไม่มีตัว S (Secure) เกี่ยวกับความปลอดภัยของข้อมูลส่วนบุคคล 2) ควรมีการปรับปรุงรุ่นของโปรแกรมป้องกันไวรัสคอมพิวเตอร์ให้เป็นปัจจุบัน เพื่อเป็นการลบช่องว่างที่จะเปิดโอกาสให้ไวรัส

คอมพิวเตอร์หรือกลุ่มมิจฉาชีพเข้ามาโจมตีหรือล้วงข้อมูลส่วนบุคคลจากสมาร์ทโฟนได้ 3) ควรใช้ระบบวายฟาย (Wi-Fi) ที่มีระบบป้องกัน เนื่องจากหลายคนนิยมมองหาการเชื่อมต่อระบบวายฟายซึ่งจะช่วยลดค่าใช้จ่ายบริการเครือข่ายอินเทอร์เน็ตบนสมาร์ทโฟนได้ แต่นั่นก็สามารถทำให้กลุ่มมิจฉาชีพเข้าถึงข้อมูลส่วนบุคคลได้ง่ายเช่นกัน 4) สังเกตสัญลักษณ์ด้านความปลอดภัย นอกจาก HTTPS ที่ให้สังเกตตัว S แล้ว หลายครั้งที่กลุ่มมิจฉาชีพพยายามเจาะระบบเข้าเว็บไซต์เพื่อจารกรรมข้อมูลทางการเงิน ดังนั้นหลายเว็บไซต์จึงได้ทำการสร้างระบบความปลอดภัยอีกอีกชั้น โดยเว็บไซต์ที่มีความปลอดภัยสามารถสังเกตได้จากสัญลักษณ์รูปแม่กุญแจ ที่อยู่ใกล้กับ HTTPS ซึ่งจะเป็นตัวบ่งบอกว่าเว็บไซต์นี้ปลอดภัย 5) ไม่นำข้อมูลส่วนบุคคลที่สามารถเชื่อมโยงไปถึงข้อมูลทางการเงินลงในสื่อสังคมออนไลน์ต่างๆ เนื่องจากกลุ่มมิจฉาชีพสามารถนำข้อมูลส่วนบุคคลเหล่านั้นไปสวมรอยแอบอ้างเป็นเหยื่อก่อนที่จะสามารถเข้าถึงข้อมูลทางการเงินได้ 6) ไม่เก็บข้อมูลส่วนบุคคลที่สำคัญไว้ในสมาร์ทโฟน ข้อมูลส่วนบุคคลนั้นสามารถถูกกลุ่มมิจฉาชีพนำไปแอบอ้างได้ แม้ว่าจะไม่มีการปล่อยข้อมูลเหล่านั้นออกสู่เครือข่ายอินเตอร์เน็ต แต่การเก็บข้อมูลเหล่านั้นไว้ในสมาร์ทโฟนก็ยังถือว่าเป็นสิ่งที่อันตราย และ 7) ตั้งรหัสผ่านให้ยุ่งยาก ซึ่งปัจจุบันสมาร์ทโฟนรุ่นใหม่จะมีการให้เข้ารหัสเพื่อรักษาความปลอดภัย การตั้งรหัสผ่านให้มีความยุ่งยาก ซับซ้อนถือเป็นหนึ่งวิธีที่สามารถช่วยปกป้องข้อมูลส่วนบุคคลได้

จากหนังสือคู่มือใช้เน็ตอย่างไร ให้ปลอดภัยและสร้างสรรค์ เรื่อง “รู้ทันภัยไซเบอร์ ทำธุรกรรมออนไลน์อย่างไรให้หายห่วง” ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (2560) ได้นำมาศึกษาเป็นแนวทางเกี่ยวกับองค์ประกอบของพฤติกรรมการป้องกันข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ดังต่อไปนี้ 1) จำกัดวงเงินทำธุรกรรมทางอิล็กทรอนิกส์ ไม่ว่าจะเป็นการโอน หรือการจ่ายสินค้าหรือบริการออนไลน์ ให้อยู่ในงบประมาณที่เหมาะสม เพื่อจำกัดความเสี่ยงของจำนวนเงิน 2) ระมัดระวังเว็บไซต์ประเภทฟิชชิง (Phishing) เช่น อีเมล์ปลอม ที่มีลักษณะอีเมล์คล้ายกับสถาบันการเงินที่มีชื่อเสียง เว็บไซต์เลียนแบบธนาคารออนไลน์ และโทรศัพท์แอบอ้างเป็นเจ้าหน้าที่ราชการ ธนาคาร เพื่อล้วงหรือให้เปิดเผยข้อมูลบุคคล 3) เว็บไซต์ที่ใช้บริการควรมีการเข้ารหัสเสมอ โดยให้สังเกตสัญลักษณ์กุญแจล็อกที่อยู่บนบราวเซอร์ เมื่อทำการคลิกที่สัญลักษณ์จะเห็นใบรับรองอิเล็กทรอนิกส์ (Secured Socket Layer: SSL Certificate) และ 4) การตั้งรหัสผ่าน ควรตั้งให้ยุ่งยากไว้ก่อน ไม่เลือกรูปแบบการจำรหัสผ่านอัตโนมัติ (Auto Password) และไม่ควรใช้รหัสผ่านเดียวเข้าทั้งอีเมล์และทำธุรกรรมทางอิเล็กทรอนิกส์ ถ้าจำเป็นต้องทำธุรกรรมทางอิเล็กทรอนิกส์ผ่านคอมพิวเตอร์

สาธารณะให้เปลี่ยนรหัสผ่านทันที และหมั่นเปลี่ยนรหัสผ่านทุก 30-45 วัน รวมทั้งใช้ตัวอักษรผสมทั้งตัวพิมพ์เล็กและพิมพ์ใหญ่ มีตัวเลขและอักขระเป็นส่วนประกอบ

เอกสารการใช้ธนาคารออนไลน์ให้ปลอดภัยบนสมาร์ทโฟนจากศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย (2561) แบ่งองค์ประกอบของพฤติกรรมการปกป้องข้อมูลในบัญชีธนาคารออนไลน์บนสมาร์ทโฟนเป็น 2 องค์ประกอบ ได้แก่ องค์ประกอบที่หนึ่ง พฤติกรรมก่อนใช้งานแอปพลิเคชันของธนาคาร เกิดจากการตั้งรหัสผ่านบนหน้าจอสำหรับเข้าใช้งานสมาร์ทโฟนและเป็นรหัสผ่านที่คาดเดาได้ยาก ทำการติดตั้งโปรแกรมหรือแอปพลิเคชันสำหรับตรวจสอบไวรัสคอมพิวเตอร์ที่ถูกกฎหมาย ไม่ทำการดัดแปลงหรือแก้ไข (Jailbreak/Root) ระบบปฏิบัติการหรืออุปกรณ์ภายในสมาร์ทโฟน เนื่องจากอาจเกิดความเสี่ยงในการถูกทุจริตด้านข้อมูล จำกัดวงเงินในการทำธุรกรรมทางการเงินต่อวัน เพื่อป้องกันกลุ่มมิจฉาชีพแอบขโมยผ่านการโอนเงินจำนวนมาก และผู้ใช้บริการต้องทราบข้อมูลว่าแต่ละธนาคารไม่มีนโยบายส่งเอสเอ็มเอส (SMS) หรืออีเมล์ เพื่อให้ติดตั้งโปรแกรมหรือแอปพลิเคชันหรือลิงก์ (Link) เข้าสู่ระบบผ่านทางออนไลน์โดยตรง และองค์ประกอบที่สอง พฤติกรรมขณะใช้งานแอปพลิเคชันของธนาคาร เกิดจากการเปลี่ยนรหัสผ่านที่สม่ำเสมอ หลังใช้งานเสร็จควรเปลี่ยนรหัสผ่านของแอปพลิเคชันธนาคารอย่างสม่ำเสมอ ทำการกดปุ่ม Logout/Log off เมื่อต้องการออกจากระบบทุกครั้งหลังเสร็จสิ้นการใช้บริการธุรกรรมทางการเงินผ่านสมาร์ทโฟน ไม่ใช้เครือข่ายไร้สายประเภทวายฟายสาธารณะ (Public/Free Wi-Fi) ในการทำธุรกรรมทางการเงิน หมั่นตรวจสอบการทำธุรกรรมทางการเงินว่ามีรายการใดผิดปกติ เช่น รายการโอนเงิน ยอดเงินคงเหลือในบัญชี เป็นต้น ทำการพิมพ์ URL (Uniform Resource Locator) หรือชื่อของเว็บไซต์ของธนาคารด้วยตนเอง และติดต่อกับธนาคารโดยตรงหากพบข้อความหรือลิงก์ที่น่าสงสัย

จากการทบทวนเอกสารและงานวิจัยที่เกี่ยวข้องข้างต้น ทั้งในประเทศและต่างประเทศที่มีการจำแนกองค์ประกอบพฤติกรรมการปกป้องข้อมูลส่วนบุคคลจากการพาณิชย์อิเล็กทรอนิกส์และการใช้งานเครือข่ายอินเทอร์เน็ตที่เกี่ยวข้อง งานวิจัยนี้ผู้วิจัยได้นำองค์ประกอบของพฤติกรรมการปกป้องความเป็นส่วนตัวของ Buchanan et al. (2007) มาปรับใช้ในแบ่งองค์ประกอบของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ในฐานะที่เป็นกลุ่มผู้บริโภค จากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วยการปฏิบัติในข้อควรระวังทั่วไปและการปฏิบัติในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลด้านเทคนิค

1.6 การวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

จากการทบทวนงานวิจัยที่เทียบเคียงกับงานวิจัยเรื่องนี้พบว่า การประเมินพฤติกรรมการปกป้องข้อมูลส่วนบุคคล ในงานวิจัยโดยส่วนใหญ่ใช้แบบสอบถามเป็นเครื่องมือวัด และใช้แหล่งข้อมูลมาจากผู้ที่ใช้บริการเครือข่ายอินเทอร์เน็ตโดยเฉพาะกลุ่มวัยรุ่น ตั้งแต่ช่วงอายุระหว่าง 16-30 ปี ซึ่งขึ้นอยู่กับข้อคำถามในการวิจัยและความสอดคล้องกับตัวแปรที่เกี่ยวข้องในการศึกษา ในงานวิจัยนี้เป็นการศึกษาพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้นที่มีอายุระหว่าง 20-29 ปี จึงได้ทบทวนงานวิจัยแบบวัดที่ถูกพัฒนาขึ้น พบแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลที่เกี่ยวข้องกับงานวิจัยนี้ ดังนี้

ฉบับที่หนึ่ง เป็นการพัฒนาแบบวัดจากความกังวลและการปกป้องความเป็นส่วนตัวจากการใช้งานเครือข่ายอินเทอร์เน็ตของ Buchanan et al. (2007) จากแนวคิดเกี่ยวกับทักษะความรู้ ความเข้าใจเรื่องความเป็นส่วนตัว จากการศึกษางานวิจัยฉบับนี้ เป็นข้อคำถามจำนวน 12 ข้อ จำแนกองค์ประกอบของพฤติกรรมการปกป้องความเป็นส่วนตัวจากการใช้งานเครือข่ายอินเทอร์เน็ตจำนวน 2 ด้าน ได้แก่ ด้านการปฏิบัติในข้อควรระวังทั่วไปและการปฏิบัติในข้อควรระวังเพื่อปกป้องข้อมูลส่วนบุคคลด้านเทคนิค โดยมีขั้นตอนในการพัฒนาแบบวัด ดังนี้

ขั้นตอนที่หนึ่ง เป็นการสังเคราะห์งานวิจัยที่เกี่ยวข้องกับทักษะความรู้ ความเข้าใจเรื่องความเป็นส่วนตัว ตามแนวคิดของนักวิชาการหลายท่าน (Burgoon et al, 1989; DeCew, 1997; Fox et al, 2000; Stark, 2004) ประกอบด้วยความเป็นส่วนตัวจำนวน 3 ด้าน ได้แก่ 1) ความเป็นส่วนตัวด้านสารสนเทศ (Informational Privacy) ซึ่งเป็นข้อมูลเกี่ยวกับตัวบุคคล เช่น ชื่อ-นามสกุล ที่อยู่ หมายเลขโทรศัพท์ หมายเลขบัตรเครดิต และเลขที่บัญชีธนาคาร เป็นต้น ที่บุคคลอื่นห้ามนำไปเปิดเผย 2) ความเป็นส่วนตัวด้านการแสดงออกบนเครือข่ายอินเทอร์เน็ต (Expressive Privacy) เช่น การส่งต่อข้อมูลทางอีเมล์ไปยังบุคคลอื่น และ 3) ความเป็นไปได้ในการให้ข้อมูลส่วนบุคคลเพื่อแลกกับผลประโยชน์ที่จะได้รับ (Possible Benefits of Surrendering Privacy) เช่น การลงทะเบียนให้ข้อมูลส่วนบุคคลไว้เพื่อให้สามารถทำการเข้าสู่ระบบการสั่งซื้อสินค้าออนไลน์ที่รวดเร็วขึ้น เป็นต้น ได้ข้อคำถามเกี่ยวกับทักษะความรู้ ความเข้าใจความเป็นส่วนตัวจำนวน 82 ข้อ ใช้ลักษณะเป็นมาตราส่วนประมาณค่า 6 ระดับ ศึกษากับกลุ่มตัวอย่างที่เป็นนักศึกษาในมหาวิทยาลัยเปิด (Open University) ของประเทศอังกฤษ ที่รวมไปถึงกลุ่มนักศึกษาในระบบการเรียนทางไกล และนักศึกษาที่มีรายได้ระหว่างเรียนมี จำนวน 515 คน ผลการศึกษาแบบจำลองการวัดสามารถจำแนกเป็นองค์ประกอบ 2 ด้านได้แก่ การปฏิบัติในข้อควรระวังทั่วไปและการปฏิบัติในข้อควรระวังเพื่อปกป้องข้อมูลส่วนบุคคลด้านเทคนิค อย่างละ 6

ข้อ พบค่าความเชื่อมั่นรายด้านมีค่าเท่ากับ 0.75 และ 0.74 ตามลำดับ และพบค่าความเชื่อมั่นของแบบวัดทั้งฉบับเท่ากับ 0.93

ขั้นตอนที่สอง นำข้อคำถาม 12 ข้อเกี่ยวกับพฤติกรรมความเป็นส่วนตัว (Privacy Behavior Items) ในรูปแบบของแบบสอบถามบนเว็บไซต์ (Web-based Questionnaire) และข้อคำถามเกี่ยวกับความกังวลด้านความเป็นส่วนตัว (Privacy Concern) จำนวน 16 ข้อ ไปทดลองใช้กับกลุ่มตัวอย่างซึ่งเป็นนักศึกษาในมหาวิทยาลัยเปิด แบ่งเป็น 2 กลุ่ม คือ กลุ่มนักศึกษาที่มีความรู้ทางด้านเทคโนโลยีกับกลุ่มนักศึกษาที่ไม่มีความรู้พื้นฐานทางเทคโนโลยี จำนวนทั้งสิ้น 69 คน ผลการศึกษาค่าความเที่ยงตรง (Scale Validity) โดยการเปรียบเทียบคะแนนรายบุคคลพบว่าทั้งสองกลุ่มมีแนวโน้มที่แตกต่างกันในพฤติกรรมการปกป้องข้อมูลส่วนบุคคลจากการใช้งานเครือข่ายอินเทอร์เน็ต

ขั้นตอนที่สาม นำแบบวัดในรูปแบบของแบบสอบถามบนเว็บไซต์ไปใช้กับกลุ่มตัวอย่างซึ่งเป็นนักศึกษาในมหาวิทยาลัยเปิด จำนวน 1,122 คน เป็นข้อคำถาม 28 ข้อ มีลักษณะเป็นมาตราส่วนประมาณค่า 7 ระดับ จำแนกเป็นองค์ประกอบ 3 ด้านได้แก่ 1) พฤติกรรมความกังวลด้านความเป็นส่วนตัว 2) การปฏิบัติในข้อควรระวังทั่วไป และ 3) การปฏิบัติในข้อควรระวังเพื่อปกป้องข้อมูลส่วนบุคคลด้านเทคนิคจากการใช้งานเครือข่ายอินเทอร์เน็ตเพื่อการลงทะเบียนเข้าใช้บริการอีเมล์และการสั่งซื้อสินค้าและบริการออนไลน์ ผลการศึกษาความเที่ยงตรงเชิงโครงสร้าง (Construct Validity) พบค่าความสัมพันธ์ระหว่างองค์ประกอบทั้ง 3 ด้าน มีค่าเท่ากับ 0.25, 0.17 และ 0.09 ตามลำดับ

ฉบับที่สอง แบบวัดที่พัฒนาขึ้นเกี่ยวกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลของผู้ใช้บริการเครือข่ายอินเทอร์เน็ตในฐานะผู้บริโภคสินค้าและบริการจากร้านค้าออนไลน์หรือการพาณิชย์อิเล็กทรอนิกส์ของ Son & Kim (2008) ตามแนวคิดความตั้งใจเกี่ยวกับความเชื่อเชิงพฤติกรรม (Belief-Behavioral Intention Link) ของนักวิชาการหลายท่าน ประกอบด้วยแบบจำลองการยอมรับการใช้เทคโนโลยี (Davis, 1989; Davis et al., 1989) ความไว้วางใจเกี่ยวกับการพาณิชย์อิเล็กทรอนิกส์ (McKnight et al., 2002) และความเป็นส่วนตัวด้านสารสนเทศ (Dinev & Hart, 2006; Malhotra et al., 2004) ซึ่งอยู่ภายใต้ทฤษฎีการกระทำด้วยเหตุผล (Theory of Reasoned Action) ของ Fishbein & Ajzen (1975) เป็นข้อคำถามจำนวน 38 ข้อ มีลักษณะเป็นมาตราส่วนประมาณค่า 7 ระดับ ศึกษากับกลุ่มตัวอย่างที่เป็นนักศึกษามหาวิทยาลัยในประเทศสหรัฐอเมริกาและมีคุณสมบัติเป็นผู้ใช้บริการเครือข่ายอินเทอร์เน็ตจำนวน 523 คน ในรูปแบบของแบบสอบถามบนเว็บไซต์ ซึ่งผลจากการวิเคราะห์องค์ประกอบ สามารถจัด

กลุ่มองค์ประกอบของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลของผู้ใช้บริการเครือข่ายอินเทอร์เน็ต เป็น 3 องค์ประกอบ พบค่าความเชื่อมั่นของแบบวัดทั้งฉบับเท่ากับ 0.87 และผลการศึกษาการวิเคราะห์ปัจจัยอันดับสอง (The Second–Order Factor Analysis) พบว่าแบบจำลองกลมกลืนกับข้อมูล มีค่าดัชนีความกลมกลืนได้แก่ ค่า TLI เท่ากับ 0.96 ค่า CFI เท่ากับ 0.95 และพบค่าความเชื่อมั่นอยู่ระหว่าง 0.85 ถึง 0.97

ฉบับที่สาม เป็นแบบวัดที่พัฒนาขึ้นโดย Youn (2009) ซึ่งได้พัฒนาตามแบบวัดพฤติกรรมการปกป้องความเป็นส่วนตัวจากการให้ข้อมูลส่วนบุคคลเพื่อเข้าใช้บริการเครือข่ายอินเทอร์เน็ต ตามแนวคิดของนักวิชาการหลายท่าน (Sheehan & Hoy, 1999; Milne & Culnan, 2004; Youn, 2005; Moscardelli & Divine, 2007) เป็นข้อคำถามจำนวน 6 ข้อ มีลักษณะเป็นมาตราส่วนประมาณค่า 5 ระดับ จำแนกองค์ประกอบของพฤติกรรมการปกป้องความเป็นส่วนตัวจากการให้ข้อมูลส่วนบุคคลเพื่อเข้าใช้บริการเครือข่ายอินเทอร์เน็ตจำนวน 3 ด้านได้แก่ 1) พฤติกรรมการให้ข้อมูลส่วนบุคคลที่ไม่ตรงกับความเป็นจริง (Fabricate) 2) พฤติกรรมการค้นคว้าและแสวงหา (Seek) ความรู้ และ 3) พฤติกรรมการละเว้น การปฏิเสธในการให้ข้อมูลส่วนบุคคล (Refrain) โดยใช้เทคนิคการวิเคราะห์องค์ประกอบเชิงสำรวจ ศึกษากับกับกลุ่มตัวอย่างที่เป็นนักเรียนระดับมัธยมศึกษาตอนต้นในเขตภาคตะวันออกเฉียงเหนือ สหรัฐอเมริกา จำนวน 148 คน ผลการศึกษาพบค่าความสัมพันธ์ระหว่างองค์ประกอบทั้ง 3 ด้าน มีค่าอยู่ระหว่าง 0.41 ถึง 0.44

ฉบับที่สี่ เป็นแบบวัดในการศึกษาของ Büchi et al. (2016) เกี่ยวกับความสำคัญในทักษะการใช้งานอินเทอร์เน็ตสำหรับการปกป้องความเป็นส่วนตัว โดยพัฒนาโดยปรับปรุงจากแบบวัดตามแนวคิด Debatin et al. (2009) และ Dienlin & Trepte (2015) เป็นข้อคำถาม 10 ข้อ มีลักษณะเป็นมาตราส่วนประมาณค่า 4 ระดับ จำแนกองค์ประกอบจำนวน 5 ด้าน ได้แก่ 1) พฤติกรรมการเปลี่ยนแปลงตั้งค่าความเป็นส่วนตัว 2) พฤติกรรมการติดตาม สังเกตการณ์เกี่ยวกับข้อมูลส่วนบุคคลบนหน้าจอ 3) พฤติกรรมการให้ข้อมูลส่วนบุคคลที่เป็นเท็จ 4) พฤติกรรมเกี่ยวกับการจัดการคุกกี้ (Cookies) และ 5) พฤติกรรมการลบข้อมูลส่วนบุคคล เพื่อป้องกันบุคคลที่ไม่รู้จักหรือจากผู้ให้บริการเครือข่ายอินเทอร์เน็ต ศึกษากับกลุ่มตัวอย่างที่เป็นชาวสวิส ที่สามารถสื่อสารภาษาเยอรมัน ภาษาฝรั่งเศสหรือภาษาอิตาลีได้ จำนวน 970 คนที่มีการใช้บริการเครือข่ายอินเทอร์เน็ต โดยใช้เทคนิคการวิเคราะห์องค์ประกอบเชิงยืนยัน ผลจากการศึกษาพบว่าแบบจำลองกลมกลืนกับข้อมูล ซึ่งแบบจำลองมีค่าดัชนีความกลมกลืน TLI เท่ากับ 0.96 ค่า CFI เท่ากับ 0.97 และพบค่าความเชื่อมั่นอยู่ระหว่าง 0.83 ถึง 0.91

ฉบับที่ห้า เป็นแบบวัดที่พัฒนาขึ้นโดย Boerman et al. (2018) ซึ่งได้พัฒนาตามแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคล (To Protect One's Personal Information) และความเป็นส่วนตัวจากการใช้งานเครือข่ายอินเทอร์เน็ต ตามแนวคิดของนักวิชาการหลายท่าน (Balebako et al., 2012; Büchi et al., 2016; McDonald & Cranor ,2010; Milne et al., 2009) เป็นข้อคำถาม 10 ข้อ มีลักษณะเป็นมาตราส่วนประมาณค่า 6 ระดับ จำแนกองค์ประกอบจำนวน 10 พฤติกรรมการปกป้องข้อมูลส่วนบุคคลจากการใช้บริการเครือข่ายอินเทอร์เน็ต ได้แก่ การปิดกั้นโฆษณา (Use an ad blocker) การลบคุกกี้ (Delete Cookies) การตัดสินใจไม่เข้าเยี่ยมชมเว็บไซต์ หากเว็บไซต์นั้นให้ทำการยอมรับเงื่อนไขการใช้งานคุ๊กกี้ (Accept cookies) หรือการเก็บประวัติหรือข้อมูลของผู้ใช้งานเมื่อเข้าเยี่ยมชมเว็บไซต์ผ่านทางเว็บเบราว์เซอร์ การปฏิเสธที่จะยอมรับการใช้งานคุกกี้ (Decline to accept cookies) หากเว็บไซต์นั้นเสนอทางเลือกมาให้ การเข้าใช้งานโหมดท่องเว็บไซต์แบบส่วนตัว (Private mode) การลบประวัติหรือข้อมูลการท่องเว็บไซต์ผ่านทางเว็บเบราว์เซอร์ (Delete browser history) การไม่เข้าร่วมในรายการส่งเสริมการขาย การตลาดของร้านค้าออนไลน์ (Opt-out) การท่องเว็บไซต์ผ่านทางเว็บเบราว์เซอร์โดยเปิดใช้งานแบบไม่สะกอดรอยตาม (Do not track) เพื่อป้องกันการติดตาม สะกดรอยและเก็บข้อมูลจากผู้ให้บริการอินเทอร์เน็ต การใช้โปรแกรมลักษณะพิเศษ (Special software) เช่น Ghostery และ Abine Taco เพื่อป้องกันการเก็บข้อมูลการเข้าใช้งานบนเว็บไซต์ และการให้ข้อมูลส่วนบุคคลที่เป็นเท็จ เช่น ชื่อปลอม อีเมล์ปลอม หากมีการสอบถามจากผู้ให้บริการอินเทอร์เน็ต โดยศึกษากับกลุ่มตัวอย่างในประเทศเนเธอร์แลนด์ ส่วนใหญ่มีการศึกษาระดับปริญญาตรีหรือสูงกว่า โดยมีขั้นตอนการพัฒนาเป็นแบบการวิจัยเชิงสำรวจระยะยาวหรือช่วงยาว (Longitudinal survey) แบ่งเป็น ระยะที่หนึ่ง (Wave 1) และระยะที่สอง (Wave 2) รวมทั้งสิ้นจำนวน 928 คน พบค่าความเชื่อมั่นแต่ละระยะมีค่าเท่ากับ 0.80 และ 0.82 ตามลำดับ

จากการศึกษาแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลที่เกี่ยวข้องกับงานวิจัยนี้ทั้ง 5 ฉบับข้างต้น พบว่าแต่ละฉบับมีการจัดกลุ่มตัวแปรและนิยามเกี่ยวกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลที่ไม่เหมือนกัน แต่ท้ายที่สุดแล้วแบบวัดทุกฉบับเป็นแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคล และเมื่อศึกษาในรายละเอียดได้พบว่า แบบวัดแต่ละฉบับมีความเหมือนกันดังนี้ 1) เป็นแบบวัดที่มีแนวคิดมาจากความกังวลด้านความเป็นส่วนตัว (Privacy Concerns) จากการใช้งานเครือข่ายอินเทอร์เน็ต 2) นำข้อมูลที่ใช้ศึกษามาวิเคราะห์ด้วยหลักเกณฑ์ทางสถิติและจัดกลุ่มตัวแปร ทำให้มีความน่าเชื่อถือของข้อมูลมากขึ้น และ 3) แบบวัดทุกฉบับเป็นแบบวัดที่ใช้วัด

ในเรื่องเดียวกันคือแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคล มีลักษณะใกล้เคียงกันและคล้ายคลึงกัน ซึ่งแตกต่างกันไปตามนิยามของแต่ละแบบวัด

ดังนั้นการวิจัยครั้งนี้ ผู้วิจัยสร้างแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์โดยการประยุกต์แบบวัดของทั้ง 5 ฉบับ มาเป็นแนวทางในการสร้างแบบวัดโดยให้เป็นไปตามขอบเขตเนื้อหาและนิยามปฏิบัติการของตัวแปร ทั้งนี้จะเป็นแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ตามลำดับ สำหรับวิธีการให้คะแนน สำหรับคำถามทางบวก ผู้ที่ตอบจริงที่สุดจะได้ 6 คะแนน จริงจะได้ 5 คะแนน ค่อนข้างจริงจะได้ 4 คะแนน ค่อนข้างไม่จริงจะได้ 3 คะแนน ไม่จริงจะได้ 2 คะแนน และไม่จริงเลยจะได้ 1 คะแนน สำหรับคำถามทางลบผู้วิจัยให้คะแนนตรงกันข้าม ทั้งนี้กลุ่มตัวอย่างที่ได้คะแนนเฉลี่ยสูงกว่าจะมีพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์สูงกว่ากลุ่มตัวอย่างที่ได้คะแนนเฉลี่ยต่ำกว่า

1.7 งานวิจัยที่เกี่ยวข้องกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

จากการทบทวนงานวิจัยที่ศึกษาพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ส่วนใหญ่เป็นการศึกษาเพื่อการปกป้องข้อมูลส่วนบุคคลบนเครือข่ายอินเทอร์เน็ตและการพาณิชย์อิเล็กทรอนิกส์ ดังนี้

งานวิจัยที่เกี่ยวข้องกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในการเลือกเปิดเผยข้อมูลส่วนบุคคลและการตั้งค่าความเป็นส่วนตัว เช่น งานวิจัยของ Boerman et al., (2018) ศึกษาการปกป้องข้อมูลส่วนบุคคลและความเป็นส่วนตัวจากการใช้งานเครือข่ายอินเทอร์เน็ต ซึ่งพบว่าทักษะในการใช้งานเว็บไซต์ การติดตั้งโปรแกรมที่ใช้งานและการตั้งค่าทางเทคนิคเกี่ยวกับเว็บไซต์เป็นตัวแปรที่สำคัญต่อการปกป้องข้อมูลส่วนบุคคล เช่นเดียวกับงานวิจัยของ Malhotra et al. (2004); Feng & Xie (2014) และ Büchi et al. (2016) ศึกษาพฤติกรรมการปกป้องความเป็นส่วนตัวเมื่อเข้าใช้งานเว็บไซต์ พบว่าทักษะและความสามารถในการใช้งานเครือข่ายอินเตอร์เน็ตบนเว็บไซต์เป็นปัจจัยที่สำคัญต่อการปกป้องข้อมูลส่วนบุคคลและสามารถลดความเสี่ยงความเป็นส่วนตัวได้

งานวิจัยที่เกี่ยวข้องกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ด้านการอ่านและศึกษาข้อมูลด้านนโยบายความเป็นส่วนตัว และการใช้งานธุรกรรม

ทางอิเล็กทรอนิกส์อย่างระมัดระวัง เช่น ในงานวิจัย Youn (2005); Youn (2009) และ Dienlin & Trepte (2015) พบว่าการค้นคว้าและแสวงหาความรู้ การสอบถามผู้มีประสบการณ์มีส่วนสำคัญในการปกป้องความเป็นส่วนตัวจากการให้ข้อมูลส่วนบุคคลเมื่อเข้าใช้บริการเครือข่ายอินเทอร์เน็ต และงานวิจัยเกี่ยวกับการใช้งานธุรกรรมทางอิเล็กทรอนิกส์อย่างระมัดระวัง เช่น Jiang et al. (2013) และ McGuinness & Simon (2018) เกี่ยวกับการเข้าเว็บไซต์ด้วย HTTPS (Secure) การสังเกตสัญลักษณ์ด้านความปลอดภัยและการระมัดระวังเว็บไซต์ประเภทฟิชชิง นอกจากนี้งานวิจัยของพรพรรณ ช้างงาเนียม (2553) ศึกษาพฤติกรรมการใช้บริการธุรกรรมทางการเงินผ่านโทรศัพท์มือถือพบว่าได้รับการยอมรับมากขึ้น แต่ยังมีข้อจำกัดทางด้านความไม่มั่นใจในระบบรักษาความปลอดภัยการทำธุรกรรมทางการเงิน และงานวิจัยของนิภาพร แสงทวีและสมนึก พ่วงพรพิทักษ์ (2558) ได้วิเคราะห์ความปลอดภัยและความมั่นคงสำหรับระบบธนาคารผ่านโทรศัพท์มือถือในประเทศไทย ได้พบจุดอ่อนของระบบ M-Banking หลายอย่าง ยังมีช่องโหว่ที่ทำให้มิจฉาชีพเข้ามาจารกรรมข้อมูลได้ ส่วนใหญ่เป็นการสวมรอยเป็นเจ้าของบัญชีและพฤติกรรมผู้ใช้สมาร์ทโฟนที่ส่งผลต่อมัลแวร์ (Malware)

งานวิจัยที่เกี่ยวข้องกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์การควบคุมการเข้าถึงข้อมูลส่วนบุคคลบนเครื่องคอมพิวเตอร์และบัญชีผู้ใช้งาน และการละเว้น ลดกิจกรรมที่ส่งผลต่อการให้ข้อมูลส่วนบุคคล จากการชำระเงินซื้อสินค้าและบริการผ่านร้านค้าการพาณิชย์อิเล็กทรอนิกส์และการชำระเงินผ่านบัตรเงินอิเล็กทรอนิกส์ เช่น งานวิจัยของ Buchanan et al. (2007) และ Son & Kim (2008) ศึกษาพฤติกรรมการปกป้องข้อมูลส่วนบุคคลของผู้ใช้บริการอินเทอร์เน็ตจากการพาณิชย์อิเล็กทรอนิกส์พบว่า การหลีกเลี่ยงให้ข้อมูลส่วนบุคคล การลบข้อมูลที่เกี่ยวข้องกับความเป็นส่วนตัวในกิจกรรมจากการใช้งานเครือข่ายอินเทอร์เน็ตและการระมัดระวังการแสดงความคิดเห็นส่วนตัวบนเว็บไซต์ต่อการใช้สินค้าและบริการเป็นตัวแปรที่สำคัญต่อการปกป้องภัยคุกคามความเป็นส่วนตัวจากการซื้อขายสินค้าและบริการจากร้านค้าออนไลน์ ในงานวิจัยของสุรัสสา ลิมปพานนท์ (2561) ศึกษาพฤติกรรมผู้บริโภคเจนเนอเรชันวายในการเปิดใช้งานการชำระสินค้าและบริการผ่านอีวอลเลท (e-Wallet) ในเขตพื้นที่กรุงเทพมหานคร พบว่ามีผู้บริโภคมีพฤติกรรมการปรับเปลี่ยนสู่ระบบการชำระเงินผ่านโทรศัพท์มือถือมากขึ้น และให้ความสำคัญด้านความปลอดภัยกับการใช้จ่ายเงินผ่านบัญชีแอปพลิเคชันอีวอลเลท โดยให้ความสำคัญกับการออกจากระบบ (Logout) เมื่อเลิกใช้งานและการไม่บันทึกรหัสผู้ใช้งานเพื่อป้องกันการจารกรรมข้อมูลทางการเงินอิเล็กทรอนิกส์

2. ทฤษฎีและแนวคิดเกี่ยวกับสาเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

2.1 การวิเคราะห์สาเหตุพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

การศึกษาถึงสาเหตุของพฤติกรรมการป้องกันข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ เพื่อเชื่อมโยงข้อค้นพบไปยังการศึกษาแนวคิดทฤษฎีที่เกี่ยวข้องกับการป้องกันข้อมูลส่วนบุคคลธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งในปัจจุบันเป็นสังคมยุคข้อมูลข่าวสารหรือยุคดิจิทัล (Digital Age) เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญและส่งผลต่อการดำรงชีวิตประจำวัน ไม่ว่าจะด้วยประสิทธิภาพ ความทันสมัย ความสะดวกและรวดเร็ว และการนำมาประยุกต์ใช้งานในด้านต่างๆ เมื่อเทคโนโลยีมีความก้าวหน้ามากขึ้นเท่าใด ความเป็นส่วนตัว ข้อมูลส่วนบุคคลย่อมมีความเสี่ยงต่อการถูกล่วงละเมิดได้ง่ายมากขึ้นเท่านั้น (ศูนย์การเรียนรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล, 2561) โดยเฉพาะบริการทางธุรกรรมทางอิเล็กทรอนิกส์ กำลังได้รับความนิยมอย่างแพร่หลายและมีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง ธนาคารพาณิชย์แต่ละแห่งจึงมีการปรับกลยุทธ์ขยายการให้บริการธุรกรรมผ่านช่องทางอิเล็กทรอนิกส์เพิ่มมากขึ้น เพื่อที่จะสามารถเข้าถึงกลุ่มลูกค้าได้มากขึ้นและยังเป็นการช่วยลดต้นทุนด้านบริการ อย่างไรก็ตาม แม้ว่าการทำธุรกรรมทางอิเล็กทรอนิกส์จะมีความสะดวก สบายและรวดเร็ว แต่ก็แฝงไว้ซึ่งภัยคุกคามที่มีแนวโน้มสูงขึ้นเนื่องจากการเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้งานเพื่อให้สามารถเข้าถึงการใช้บริการได้ (Chellappa & Pavlou, 2002; Isaac & Sherali, 2014)

หากพิจารณาถึงความสัมพันธ์ระหว่างข้อมูลส่วนบุคคล ธุรกรรมทางอิเล็กทรอนิกส์ สถาบันการเงินและเทคโนโลยี จะพบว่าในปัจจุบันการปรับลดค่าธรรมเนียมจะเป็นปัจจัยหนึ่งที่ทำให้การโอนเงินธนาคารเดียวกันผ่านเครือข่ายอินเทอร์เน็ตและสมาร์ทโฟนเพิ่มขึ้น (รายงานผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตประเทศไทย สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์, 2557) รวมถึงปัจจัยสิ่งแวดล้อมอื่นๆ ที่ช่วยให้พฤติกรรมของผู้บริโภคเปลี่ยนไป เช่น จำนวนผู้ใช้สมาร์ทโฟนเพิ่มขึ้นจากราคาอุปกรณ์ที่ถูกลง ธนาคารพาณิชย์หลายแห่งมีการให้บริการผ่านแอปพลิเคชันที่ใช้งานง่ายและสะดวกมากขึ้น การให้บริการโอนเงินโดยกรอกหมายเลขโทรศัพท์ของผู้รับแทนหมายเลขบัญชีธนาคาร เป็นต้น ดังนั้นจะเห็นว่า ธุรกรรมทางอิเล็กทรอนิกส์ที่มีการเติบโตเพิ่มสูงขึ้นผ่านเครือข่ายอินเทอร์เน็ตและสมาร์ทโฟนเพื่ออำนวยความสะดวกต่อการใช้งาน และความรวดเร็วต่อผู้บริโภค ส่งผลต่อการยินยอมเปิดเผยข้อมูลส่วนบุคคลมากขึ้นตามไปด้วย

อีกทั้ง ข้อมูลส่วนบุคคลถือได้ว่าเป็นทรัพย์สินที่มีราคา มีการแลกเปลี่ยนเพื่อผลประโยชน์อย่างใดอย่างหนึ่ง ซึ่งในปัจจุบันข้อมูลส่วนบุคคลโดยเฉพาะข้อมูลผู้บริโภคจากการซื้อสินค้าและบริการออนไลน์ มักมีการแลกเปลี่ยนระหว่างผลตอบแทนกับความเสี่ยงในการเปิดเผยข้อมูลส่วนบุคคล (Gandomi & Haider, 2015; วสันต์ ลิ่วลมไพศาลและสฤณี อาชวานันทกุล, 2556; ศูนย์การเรียนรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล, 2561) เช่น การสมัครใช้บริการอีเมล์ การสมัครสมาชิกเพื่อใช้ในการเข้าถึงข้อมูลข่าวสารและการส่งเสริมการขาย เป็นต้น โดยผู้ขายสินค้าและบริการออนไลน์หรือร้านค้าจากการพาณิชย์อิเล็กทรอนิกส์จะใช้ข้อมูลส่วนบุคคลหรือข้อมูลของผู้บริโภคนี้ในการวิเคราะห์ความต้องการทางธุรกิจและวางแผนกลยุทธ์ทางการตลาด ซึ่งจากข้อมูลประวัติการเข้าดูและการซื้อสินค้าและบริการออนไลน์ของผู้บริโภคล้วนมีค่าและมีมูลค่าในการขับเคลื่อนการพาณิชย์อิเล็กทรอนิกส์ เพื่อเป็นแนวทางส่งเสริมการขาย (Promotion) ที่ตรงใจกลุ่มผู้บริโภค รวมทั้งลักษณะของสังคมในประเทศไทยกำลังจะเป็นสังคมไร้เงินสด (Cashless Society) ที่รูปแบบการชำระเงินมีการเปลี่ยนแปลงไปจากเดิม หน่วยงานที่เกี่ยวข้องไม่ว่าจะเป็นหน่วยงานภาครัฐ สถาบันการเงิน ธนาคารและผู้ประกอบหรือร้านค้าออนไลน์ สามารถเข้าถึงข้อมูลส่วนบุคคล ทำให้ผู้บริโภคเกิดความสูญเสียความเป็นส่วนตัวในธุรกรรมทางอิเล็กทรอนิกส์ได้ ซึ่งหากบุคคลมีแรงจูงใจในการปกป้องข้อมูลส่วนบุคคลและตระหนักถึงความปลอดภัยเกี่ยวกับความเป็นส่วนตัวมากขึ้นก็จะสามารถป้องกันภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ได้ (Tu & Yuan, 2012; Park & Lee, 2014; Srisawang et al., 2015; Chen et al., 2016) รวมไปถึงทัศนคติและความตั้งใจในการปกป้องข้อมูลส่วนบุคคลออนไลน์ด้วย (Yao & Linz, 2008; Saeri et al., 2014)

จากเหตุผลข้างต้น ในงานวิจัยนี้ ผู้วิจัยมุ่งศึกษาเกี่ยวกับทฤษฎีแรงจูงใจเพื่อการป้องกัน (The Protection Motivation Theory: PMT) ร่วมกับแบบจำลองการยอมรับการใช้เทคโนโลยี (Technology Acceptance Model: TAM) เพื่อเป็นแนวทางในการศึกษาปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

2.2 **ทฤษฎีแรงจูงใจเพื่อการป้องกัน** (The Protection Motivation Theory: PMT)

ทฤษฎีแรงจูงใจเพื่อการป้องกัน หรือทฤษฎีแรงจูงใจในการปกป้องตนเอง (The Protection Motivation Theory: PMT) เริ่มมีการศึกษาขึ้นโดย Rogers (1975) เกี่ยวกับความหวาดกลัวและการเปลี่ยนแปลงเจตคติ ซึ่งต่อมา Rogers (1983) ได้ทำการปรับปรุงและถูกนำมาใช้ในกระบวนการกระตุ้นด้วยความกลัวและการเปลี่ยนแปลงทัศนคติคติ (Processes in fear appeals and attitude change) ซึ่งเป็นทฤษฎีร่วมระหว่างแบบแผนความเชื่อด้านสุขภาพ

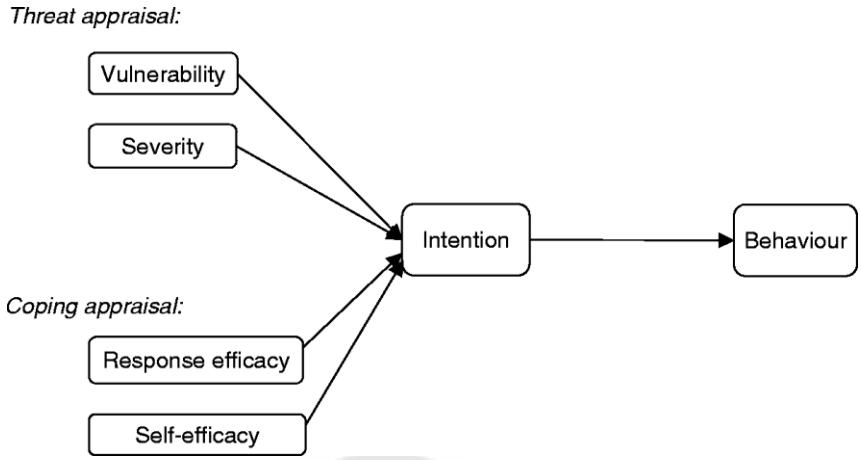
(Health Belief Model) (Rosenstock, 1974) และทฤษฎีการรับรู้สมรรถนะแห่งตนหรือทฤษฎีความคาดหวังในความสามารถของตนเอง (Self-efficacy Theory) ของ Bandura (1977) ซึ่งทฤษฎีแรงจูงใจเพื่อการป้องกันเป็นการศึกษาถึงทฤษฎีจิตวิทยาสุขภาพ (Health Psychology Theory) เกี่ยวกับแรงขับเคลื่อนภายในตัวบุคคล ที่เห็นว่าความน่ากลัวที่เกิดขึ้นกับสุขภาพนั้นรุนแรงและรู้สึกถึงอันตรายนั้น หากมีการเปลี่ยนแปลงความน่ากลัวนั้นให้ดีขึ้นได้ จะทำให้บุคคลมีความเชื่อมั่นว่าเขามีความสามารถพอที่จะตอบสนองให้เหมาะสมได้เพื่อไม่ให้เกิดอันตรายที่มาคุกคามนั้น ซึ่งเป็นทฤษฎีที่ได้รับการพัฒนาขึ้นเพื่อสร้างความเข้าใจที่เกิดจากความกลัวในตัวบุคคล ซึ่งองค์ประกอบของทฤษฎีแรงจูงใจเพื่อการป้องกัน ที่ทำให้ตัวบุคคลเกิดความกลัว ประกอบด้วย (1) การรับรู้ถึงความรุนแรง (Perceived Severity) หรือสิ่งที่กำลังคุกคาม (Noxiousness) (2) การรับรู้โอกาสเสี่ยงต่อการถูกคุกคาม (Perceived Vulnerability) และ (3) ความคาดหวังในผลลัพธ์ (Response efficacy) ร่วมการศึกษาถึงความสามารถของตนเอง (Self-efficacy) โดยแบ่งกรอบการศึกษาของกระบวนการประเมินที่ทำให้เกิดการรับรู้ (Cognitive Process) ออกเป็นการประเมินภัยคุกคาม (Threat appraisal) และการประเมินการเผชิญปัญหา (Coping Appraisal) เพื่อใช้เชื่อมโยงไปยังแรงจูงใจในการปกป้องตนเองและพฤติกรรมการระวังป้องกันภัย

การพิจารณาเหตุผลของทฤษฎีแรงจูงใจเพื่อการป้องกัน (PMT) มาประยุกต์ใช้ในงานวิจัยนี้

จากการศึกษาถึงการใช้แนวคิดเศรษฐศาสตร์เชิงพฤติกรรม (Behavioral Economics) (Thaler & Benartzi, 2004; Frank, 2004; Diamond & Vartiainen, 2012; Wilkinson, & Klaes 2017) เพื่อสังเคราะห์ข้อมูลไปสู่ทฤษฎีที่นำมาใช้ในงานวิจัยนี้ พบว่าเศรษฐศาสตร์เชิงพฤติกรรมเป็นการศึกษาถึงกระบวนการตัดสินใจของบุคคลเพื่อศึกษาถึงปัจจัยเหตุที่ทำให้เกิดการตัดสินใจที่ถูกต้อง และการตัดสินใจของบุคคลไม่ได้อาศัยเฉพาะเหตุผล แต่รวมถึงอารมณ์ ความรู้สึกและประสบการณ์ซึ่งเป็นความลำเอียงหรืออคติในการตัดสินใจ (Bias in decision making) และอธิบายถึงสาเหตุที่บุคคลประสบปัญหาในการปรับเปลี่ยนพฤติกรรมมาจากความลำเอียงในเชิงบวกหรือความลำเอียงในการสนับสนุนฝ่ายตน (Optimistic bias) ซึ่งส่งผลให้เกิดปัญหาพฤติกรรมการตัดสินใจที่ไม่สมเหตุสมผล มีพฤติกรรมเอนเอียงไปตามสถานการณ์ความรู้สึกส่วนตัวและสิ่งแวดล้อมรอบตัว

ในงานวิจัยนี้เกี่ยวกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์นั้น หากบุคคลตัดสินใจศึกษาเฉพาะการปกป้องข้อมูลส่วนบุคคลที่เกิดขึ้นและยังคงเป็นปัญหาอยู่ในปัจจุบัน (Present bias) หรือในระยะสั้นซึ่งมองเห็นแต่ประโยชน์ใกล้ตัว โดยไม่สนใจถึงผลประโยชน์ที่จะเกิดขึ้นในระยะยาวหรือในอนาคต ซึ่งอาจมองว่าเป็นสิ่งที่ยังไม่เกิดขึ้นจริงและเป็นสิ่งที่จับต้องไม่ได้จึงถูกลดทอนความสำคัญลงไป เนื่องจากผลประโยชน์ที่จะได้รับนั้นต้องใช้ระยะเวลานาน ซึ่งอาจทำให้บุคคลนั้นไม่ทันระมัดระวังในการปกป้องข้อมูลส่วนบุคคลเกิดความเสียหายด้านทรัพย์สินและความไม่ปลอดภัยจากการใช้งานธุรกรรมทางอิเล็กทรอนิกส์ได้ เช่นเดียวกับเศรษฐศาสตร์เชิงพฤติกรรมทางสุขภาพที่มองว่า การออกกำลังกายเป็นประจำ การเลิกสูบบุหรี่ การรับรู้ว่ารับประทานอาหารเพื่อสุขภาพ มังสวิรัติจะช่วยให้มีสุขภาพดีขึ้นในอนาคต โดยบุคคลนั้นรับรู้ถึงประโยชน์และเป็นสิ่งดีแต่ไม่ปฏิบัติตาม เลือกที่จะผลัดวันประกันพรุ่งและใช้เป็นข้ออ้างในการดูแลสุขภาพ และหากไม่ได้รับการแก้ไขอาจทำให้บุคคลนั้นมีพฤติกรรมการทำร้ายสุขภาพและเจ็บป่วยได้ในอนาคต ดังนั้นแนวคิดเศรษฐศาสตร์เชิงพฤติกรรมจำเป็นต้องศึกษาและทำความเข้าใจวิธีการคิดและการตัดสินใจของบุคคล โดยอาศัยการเปลี่ยนพฤติกรรมและแรงจูงใจในระยะยาว (Frank, 2004; Diamond & Vartiainen, 2012) ซึ่งถือได้ว่าเป็นการมุ่งสนับสนุนให้บุคคลมีการปรับเปลี่ยนพฤติกรรมที่ถูกต้อง ในระยะยาวและรักษาพฤติกรรมให้มีความยั่งยืน โดยการใช้แรงจูงใจในการกระตุ้นซึ่งอาจช่วยลดความรุนแรงของปัญหาเหล่านั้นได้ ในงานวิจัยนี้จึงได้นำทฤษฎีแรงจูงใจเพื่อการป้องกัน (Protection Motivation Theory) มาใช้ในการศึกษาเพื่อพิจารณาถึงแรงจูงใจและการรับรู้โอกาสเสี่ยงของแต่ละบุคคล อันจะนำไปสู่พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ดังนี้

ทฤษฎีแรงจูงใจเพื่อการป้องกัน (Protection Motivation Theory: PMT) ของ Rogers (1983) ได้นำมาศึกษาถึงกระบวนการกระตุ้นให้เกิดความหวาดกลัวและการเปลี่ยนแปลงทัศนคติ ซึ่งเป็นทฤษฎีร่วมระหว่างแบบแผนความเชื่อด้านสุขภาพ (Health Belief Model) (Rosenstock, 1974) และทฤษฎีความคาดหวังในความสามารถของตนเอง (Self-efficacy Theory) (Bandura, 1977) โดยมีความเชื่อว่าการสื่อสารเป็นการกระตุ้นให้เกิดความหวาดกลัวจะส่งผลต่อความคิด แบบแผนและพฤติกรรม และเป็นแนวคิดเกี่ยวกับการปรับตัวเมื่อตกอยู่ในสภาวะการถูกคุกคาม โดยบุคคลหากได้รับข้อมูล ข่าวสารทางด้านลบหรือที่เป็นอันตราย จะเกิดการตอบสนองทางความคิด 2 แบบ คือ การประเมินภัยคุกคาม (Threat Appraisal) และการประเมินการเผชิญปัญหา (Coping Appraisal) ซึ่งการประเมินทั้งสองแบบจะส่งผลต่อการปรับตัวที่ความเหมาะสมและไม่เหมาะสม ดังภาพประกอบ 1



ภาพประกอบ 1 แนวคิดการวิจัยจากการนำทฤษฎีแรงจูงใจเพื่อกันป้องกันมาใช้

ที่มา: Rogers, R. W. (1983) cited Plotnikoff et al. (2010)

การประเมินภัยคุกคาม ประกอบด้วย การรับรู้ถึงโอกาสเสี่ยง (Perceived Vulnerability) และการรับรู้ถึงความรุนแรง (Perceived Severity) ซึ่งเป็นการยับยั้งการตอบสนองต่อการปรับตัวที่ไม่เหมาะสม

การรับรู้ถึงโอกาสเสี่ยง เป็นความเชื่อของบุคคลเกี่ยวกับความเป็นไปได้ที่จะถูกคุกคาม ซึ่งขึ้นอยู่กับการตัดสินใจของแต่ละบุคคลว่าหากไม่ปฏิบัติตนเพื่อหลีกเลี่ยงอันตรายที่จะเกิดขึ้น จะทำให้บุคคลนั้นมีโอกาสเสี่ยงต่อการเกิดภัยคุกคามหรืออันตรายได้ และหากบุคคลนั้นรับรู้ถึงโอกาสเสี่ยงสูงจะส่งผลให้ความตั้งใจและพฤติกรรมที่จะปฏิบัติตามสูงขึ้นตามไปด้วย ในงานวิจัยของ Shklovski et al., (2014) พบว่าผู้ใช้งานแอปพลิเคชันมีความรู้สึกเสี่ยงต่อการเกิดความเสียหายจากข้อบกพร่องหรือข้อผิดพลาดของระบบในการใช้งาน โดยผู้ไม่หวังดีที่สามารถเข้ามาใช้งานแทน (Invasion) ทำให้ผู้ใช้งานมีสภาพจิตใจที่อ่อนแอ (Vulnerable) และหมดหวัง (Hopeless) เมื่อต้องทำการปกป้องความเป็นส่วนตัวบนสมาร์ทโฟน

การรับรู้ถึงความรุนแรง เป็นการได้รับข้อมูล ข่าวสารที่ทำให้บุคคลนั้นเกิดการรับรู้ว่าภัยคุกคามที่เกิดขึ้นนั้นเกิดความเสียหายหรืออันตรายถึงชีวิตหรือไม่ หากข้อมูล ข่าวสารที่ทำให้เกิดความหวาดกลัวสูงจะส่งผลให้เกิดการเปลี่ยนทัศนคติและพฤติกรรมมากกว่าข้อมูลข่าวสารที่ทำให้เกิดความหวาดกลัวเพียงเล็กน้อย

การประเมินการเผชิญปัญหา ประกอบด้วย ความคาดหวังในผลลัพธ์ (Response Efficacy) ความคาดหวังในความสามารถของตนเอง (Self-efficacy) และความ

คาดหวังจากต้นทุนที่จ่ายไป (Response Costs) หากความสามารถที่จะปฏิบัติตามและผลลัพธ์ที่จะเกิดขึ้นของการปฏิบัติตามสูง จะส่งผลต่อความตั้งใจในการปฏิบัติตามคำแนะนำสูงตามไปด้วย

ความคาดหวังในผลลัพธ์ เป็นความคาดหวังของบุคคลว่า เมื่อทำการปฏิบัติตามคำแนะนำแล้วจะสามารถลดภัยคุกคามและโอกาสเสี่ยงที่อาจเกิดขึ้นได้ ในรูปแบบของการให้ข้อมูล ข่าวสารที่เฉพาะเจาะจงและเห็นความชัดเจนของผลที่จะเกิดขึ้น เพื่อให้บุคคลนั้นปฏิบัติตามคำแนะนำช่วยให้เกิดความเข้าใจ ตั้งใจที่จะปรับเปลี่ยนพฤติกรรมและรู้สึกในการปฏิบัติตนตามคำแนะนำมากขึ้น และหากบุคคลมีความคาดหวังในผลลัพธ์ของการปฏิบัติตนตามคำแนะนำน้อยจะทำให้บุคคลนั้นไม่มีแรงจูงใจที่จะปฏิบัติตนเพื่อลดภัยคุกคาม

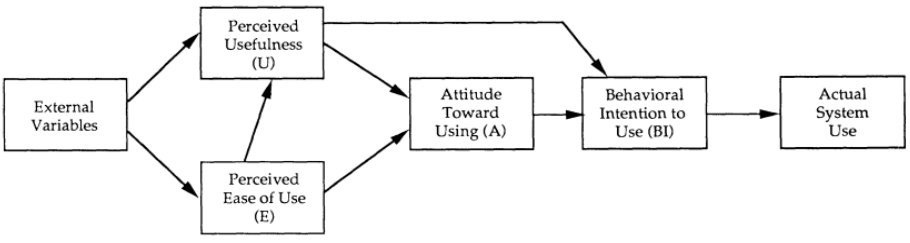
ความคาดหวังในความสามารถของตนเอง เป็นความเชื่อในความสามารถของตนเอง ว่าตนสามารถที่จะปฏิบัติตามคำแนะนำและนำไปสู่ผลลัพธ์ที่คาดหวังไว้ เป็นการนำทฤษฎีการเรียนรู้ทางสังคม (Social Learning Theory) (Bandura, 1977;1986) มาใช้ศึกษา โดยเชื่อว่าบุคคลจะมีความสามารถในการปฏิบัติตนให้ประสบผลสำเร็จในสิ่งที่ตั้งใจไว้ได้ หากบุคคลมีความสามารถที่จะปฏิบัติตามในระดับสูงและผลดีของการปฏิบัติตามสูงด้วย จะทำให้ความตั้งใจในการปฏิบัติตามคำแนะนำมีเพิ่มขึ้นตามไปด้วย ในงานวิจัยของ Chen & Chen (2015) พบว่ากลุ่มตัวอย่างที่รับรู้ความสามารถในการใช้เครือข่ายอินเทอร์เน็ตระดับสูง ส่งผลให้การจัดการเพื่อปกป้องความเป็นส่วนตัว (Privacy Management) สูงตามไปด้วย

ความคาดหวังจากต้นทุนที่จ่ายไป เป็นการรับรู้ของแต่ละบุคคลเกี่ยวกับต้นทุนหรือค่าใช้จ่ายที่เสียไปในการปฏิบัติตนเพื่อลดภัยคุกคามและโอกาสเสี่ยงที่อาจเกิดขึ้น ซึ่งต้นทุนอาจจะเป็นเงินที่ต้องจ่ายไป ค่าเสียเวลา ความพยายาม ผลกระทบที่มีต่อสภาพร่างกายและจิตใจ หากบุคคลรับรู้ว่าต้นทุนในการลดภัยคุกคามนั้นสูงเมื่อเปรียบเทียบกับผลลัพธ์ที่จะได้ จะส่งผลให้บุคคลนั้นไม่มีแรงจูงใจที่จะปฏิบัติตนเพื่อลดภัยคุกคาม ในงานวิจัยของ LeFebvre (2012) พบว่าความคาดหวังจากต้นทุนที่จ่ายไป มีอิทธิพลทางลบต่อแรงจูงใจและพฤติกรรมของผู้ใช้งานเครือข่ายอินเทอร์เน็ตเพื่อการปกป้องความเป็นส่วนตัวที่ปลอดภัย

งานวิจัยนี้ได้นำทฤษฎีแรงจูงใจเพื่อการป้องกันมาประยุกต์ใช้ โดยทำการศึกษาจำนวน 5 ตัวแปรเหตุ เพื่อให้สามารถอธิบายความตั้งใจและพฤติกรรมในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ได้ละเอียดถี่ถ้วนยิ่งขึ้น และมีการกล่าวถึงในงานวิจัยที่เกี่ยวข้องและเป็นที่ยอมรับงานวิจัย (Milne et al., 2000; Woon et al., 2005; Ifinedo, 2012)

2.3 แบบจำลองการยอมรับการใช้เทคโนโลยี (Technology Acceptance Model: TAM)

แบบจำลองการยอมรับการใช้เทคโนโลยี (Technology Acceptance Model: TAM) (Davis, 1989) ถูกนำมาศึกษาเพื่ออธิบายพฤติกรรมของผู้ใช้งานทางเทคโนโลยีเกี่ยวกับการทำนายในการยอมรับเพื่อการใช้งานด้านเทคโนโลยี ซึ่งแบบจำลองนี้ได้พัฒนามาจากทฤษฎีการกระทำอย่างมีเหตุผล (Theory of Reasoned Action) (Fishbein & Ajzen, 1975) ได้อธิบายว่าพฤติกรรมและความตั้งใจของบุคคลนั้นจะมาจากความเชื่อของบุคคล ประกอบด้วย 1) ความเชื่อเกี่ยวกับทัศนคติต่อพฤติกรรม (Attitude toward behavior) จากการประเมินถึงผลลัพธ์ของบุคคลเพื่อนำไปสู่การเกิดพฤติกรรม และ 2) การคล้อยตามกลุ่มอ้างอิง (Subjective norm) หรือบุคคลใกล้ชิดที่มีความสำคัญต่อบุคคลนั้น โดยในแบบจำลองการยอมรับการใช้เทคโนโลยี (Davis, 1989) ได้มีการปรับใช้แนวคิดจากทฤษฎีการกระทำอย่างมีเหตุผล เพื่อศึกษาการยอมรับการใช้เทคโนโลยีของแต่ละบุคคล ซึ่งต่อมา Davis et al. (1989) ได้อธิบายถึงความสัมพันธ์ว่าตัวแปรภายนอก (External variables) หรือปัจจัยภายนอกในการสร้างความรับรู้ของบุคคล เช่น ลักษณะทางประชากรศาสตร์ (Demographic) ประสบการณ์ (Previous experience) โครงสร้างองค์กร เป็นต้น ส่งผลต่อการรับรู้ผู้ใช้งานเทคโนโลยี ประกอบด้วย การรับรู้ถึงประโยชน์ (Perceived usefulness) ที่แสดงถึงระดับความเชื่อของผู้ใช้งานที่รับรู้ได้ว่าเทคโนโลยีที่พัฒนาขึ้นมีส่วนช่วยทำให้การทำงานมีประสิทธิภาพเพิ่มขึ้น และมีอิทธิพลต่อความตั้งใจในการใช้งานด้านเทคโนโลยี และ 2) การรับรู้ถึงความง่ายต่อการใช้งาน (Perceived ease of use) แสดงระดับความเชื่อของผู้ใช้งานที่รับรู้ได้ว่าเทคโนโลยีที่พัฒนาขึ้นมีความง่ายต่อการเรียนรู้ที่จะใช้งานและผู้ใช้งานไม่ต้องใช้ความพยายามมากนักในการใช้งาน จากแบบจำลองการยอมรับการใช้เทคโนโลยี หากผู้ใช้งานรับรู้ถึงประโยชน์และเทคโนโลยีที่นำมาใช้นั้นสามารถใช้งานได้ง่าย จะส่งผลต่อทัศนคติที่ดีต่อการใช้งาน (Attitude toward using) ซึ่งก่อให้เกิดความตั้งใจเชิงพฤติกรรมในการใช้งาน การยอมรับการใช้งานและส่งผลการนำเทคโนโลยีมาใช้ปฏิบัติจริง ดังภาพประกอบ 2



ภาพประกอบ 2 แบบจำลองการยอมรับการใช้เทคโนโลยี

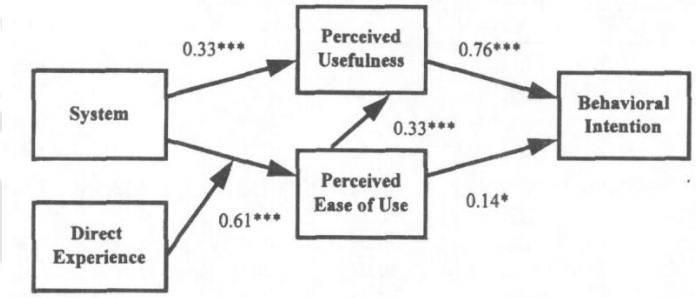
ที่มา: Davis et al. (1989). *Management science*, *35*(8), p.985

การพิจารณาเหตุผลของแนวคิดแบบจำลองการยอมรับการใช้เทคโนโลยี (TAM) มาประยุกต์ใช้

เหตุผลที่นำแนวคิดแบบจำลองการยอมรับการใช้เทคโนโลยี (TAM) มาใช้ประยุกต์ในงานวิจัยนี้ เนื่องจากจุดเริ่มต้นของแบบจำลองการยอมรับการใช้เทคโนโลยี (Davis, 1985) มาจากแนวคิดรูปแบบจำลองสิ่งกระตุ้น-ระบบ-พฤติกรรมการตอบสนอง (Stimulus-Organism-Response: S-O-R Model) (Mehrabian & Russell, 1974) ซึ่งพัฒนามาจากจิตวิทยาสิ่งแวดล้อมเกี่ยวกับการประเมินการรับรู้จากระบบภายในของแต่ละบุคคล อธิบายได้ว่าคุณลักษณะของระบบ (System feature) ของเทคโนโลยีซึ่งถือเป็นปัจจัยภายนอกหรือสิ่งกระตุ้นสิ่งเร้าทางกายภาพ ที่มีอิทธิพลต่ออารมณ์และความรู้สึกของบุคคล ในการตอบสนองต่อการรับรู้แรงจูงใจที่จะใช้งาน (User's motivation to use system) โดยถือเป็นระบบการประเมินการรับรู้ (Organism) และจะส่งให้เกิดการใช้งานระบบ (Actual system use) ซึ่งถือเป็นพฤติกรรมการตอบสนอง (Behavioral response) ต่อมา Davis (1989) ; Davis et al. (1989) จึงได้นำแนวคิดรูปแบบจำลองนี้ไปพัฒนาและเชื่อมโยงกับทฤษฎีการกระทำอย่างมีเหตุผล (Fishbein & Ajzen, 1975) ในการศึกษาและทำนายการยอมการใช้เทคโนโลยีของแต่ละบุคคลเกี่ยวกับความตั้งใจเชิงพฤติกรรมที่เกิดจากทัศนคติและส่งผลต่อการใช้งานเทคโนโลยี ดังนั้นในงานวิจัยนี้ได้นำแนวคิดแบบจำลองการยอมรับการใช้เทคโนโลยีของ Davis et al. (1989) มาใช้ประกอบศึกษาถึงพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้สามารถอธิบายความตั้งใจในการปกป้องข้อมูลส่วนบุคคลได้ละเอียดถี่ถ้วนยิ่งขึ้น และเมื่อในรายละเอียดแบบจำลองการยอมรับการใช้เทคโนโลยีจะเห็นว่าเป็นแนวคิดที่ใช้ศึกษาเชิงพฤติกรรมของมนุษย์และใช้อธิบายถึงการตัดสินใจและเหตุผลของแต่ละบุคคล (Individual person) ในการยอมรับการใช้เทคโนโลยีสารสนเทศ นอกจากนี้ในงานวิจัยของ Venkatesh et al. (2003; 427) ได้กล่าวว่าเป็นการตัดสินใจและการพิจารณาการใช้งานเบื้องต้นเกี่ยวกับปฏิกิริยาของแต่ละบุคคลที่มีต่อการใช้งานด้านเทคโนโลยีสารสนเทศ (Individual reactions to using information technology) สอดคล้องกับการศึกษาการวิเคราะห์บทความและงานวิจัยที่เกี่ยวข้องแบบจำลองการยอมรับการใช้เทคโนโลยีในอดีต (Lee et al., 2003) พบว่าการศึกษาส่วนใหญ่มุ่งเน้นในลักษณะการรายงานผลด้วยตนเองของการใช้งานเทคโนโลยี (Self-reported usage) และได้กล่าวถึงข้อจำกัดของแบบจำลองการยอมรับการใช้เทคโนโลยีว่างานวิจัยส่วนใหญ่จะมุ่งศึกษาและอธิบายความแปรปรวนของตัวแปรหลักที่ปรากฏในแบบจำลองการยอมรับการใช้เทคโนโลยี ไม่ได้มุ่งเน้นการอธิบายผลเกี่ยวกับตัวแปรภายนอก ที่ส่งผลต่อการยอมรับการใช้เทคโนโลยี ดังนั้นงานวิจัยนี้จึงไม่ได้นำตัวแปรภายนอก

ที่มีการกล่าวถึงข้างต้น เช่น ลักษณะทางประชากรศาสตร์ ประสบการณ์ โครงสร้างองค์กร เข้ามาร่วมพิจารณา

จากข้อจำกัดของแบบจำลองการยอมรับการใช้เทคโนโลยีเกี่ยวกับตัวแปรภายนอกนี้ ผู้วิจัยเห็นว่า นอกเหนือจากตัวแปรการรับรู้ถึงประโยชน์เกี่ยวกับตั้งค่าในการปกป้องข้อมูลส่วนบุคคลและตัวแปรการรับรู้ถึงความง่ายต่อการทำความเข้าใจเพื่อปกป้องข้อมูลส่วนบุคคล ในการร่วมอธิบายถึงทัศนคติ ความตั้งใจและพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ จึงได้ศึกษาถึงตัวแปรภายนอกที่อาจเกี่ยวข้องกับงานวิจัยนี้ ดังต่อไปนี้ จากการศึกษาเอกสารและงานวิจัยเพิ่มเติม พบว่าในงานวิจัยของ Venkatesh & Davis (1996) จากการพัฒนาและทดสอบเกี่ยวกับปัจจัยที่ส่งผลต่อการรับรู้ถึงความง่ายในการใช้ (Perceived ease of use) ในโปรแกรมด้านกราฟิกของกลุ่มนักศึกษา ได้มีกล่าวถึงตัวแปรภายนอกที่อาจส่งผลต่อการยอมรับการใช้งานโปรแกรมให้มีความชัดเจนขึ้น ซึ่งหมายรวมถึงคุณลักษณะของระบบ (Usability/System characteristics) การมีส่วนร่วมของผู้ใช้งานในการออกแบบระบบ (User participation in design) และกระบวนการนำไปประยุกต์ใช้ (Implementation process) ดังภาพประกอบ 3

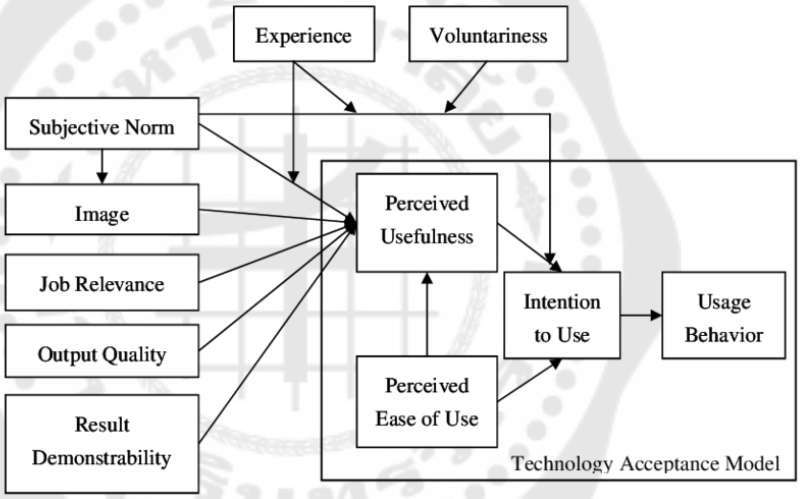


ภาพประกอบ 3 ตัวแปรภายนอกที่ส่งผลต่อการรับรู้ใช้ถึงประโยชน์และความง่ายในการใช้งานโปรแกรม

ที่มา: Venkatesh & Davis (1996). *Decision sciences*, *27*(3), p.462

ต่อมา Venkatesh & Davis (2000) ได้พัฒนาส่วนขยายแบบจำลองการยอมรับการใช้เทคโนโลยี (Extension of the Technology Acceptance Model: TAM 2) เพื่อให้สามารถทำนายพฤติกรรมการใช้ระบบสารสนเทศได้ชัดเจนขึ้น โดยทำการเก็บข้อมูลช่วงยาว (Longitudinal data collected) ในการใช้งานระบบที่แตกต่างกันจำนวน 4 ระบบ และใช้กลุ่มตัวอย่างองค์กรหรือหน่วยงานที่แตกต่างกันจำนวน 4 องค์กร (Four different systems at four

organizations) จากการศึกษาตัวแปรภายนอกที่สามารถในการอธิบายหรือมีอิทธิพลต่อการรับรู้ประโยชน์ที่ได้รับ (Perceived usefulness) และความตั้งใจในการใช้งานระบบ จากการพัฒนาส่วนขยายและผลการวิจัยได้พบว่า กระบวนการของอิทธิพลทางสังคม (Social Influence process) ประกอบด้วย การคล้อยตามกลุ่มอ้างอิง (Subjective norm) การช่วยเพิ่มภาพลักษณ์ทางสังคม (Image) และกระบวนการในการรู้คิด (Cognitive instrumental process) ได้แก่ ความเกี่ยวข้องและสนับสนุนประสิทธิภาพการทำงาน (Job relevance) คุณภาพของผลลัพธ์ที่ได้เกี่ยวกับการปฏิบัติงานได้ตามวัตถุประสงค์ (Output quality) ผลงานที่ประจักษ์ ซึ่งเป็นระบบที่สามารถจับต้องได้และสังเกตเห็นได้ (Result demonstrability) และการรับรู้ถึงความง่ายในการใช้ต่างส่งผลต่อการยอมรับในการใช้งานระบบสารสนเทศในองค์กร ดังภาพประกอบ 4



ภาพประกอบ 4 ส่วนขยายแบบจำลองการยอมรับการใช้เทคโนโลยี

ที่มา: Venkatesh & Davis (2000). *Management science*, *46*(2), p.188

จากแนวคิดแบบจำลองการยอมรับการใช้เทคโนโลยี (TAM) ที่กล่าวถึงข้างต้น จึงได้ทำการสังเคราะห์ตัวแปรเหตุและนำมาประยุกต์ใช้ในงานวิจัยนี้ ประกอบด้วยจำนวน 4 ตัวแปร ดังนี้

คุณลักษณะของระบบ เป็นระดับความเชื่อของบุคคลต่อคุณสมบัติลักษณะของระบบ รูปแบบการใช้งานของโปรแกรมต่อการทำความเข้าใจในการปกป้องข้อมูลส่วนบุคคลจากการเข้าใช้งานธุรกรรมทางอิเล็กทรอนิกส์

การคล้อยตามกลุ่มอ้างอิง เป็นระดับความเชื่อของบุคคลที่มีต่อกลุ่มบุคคลรอบข้างที่ตนยอมรับและมีความสำคัญเกี่ยวกับความคิดเห็นถึงประโยชน์ในการปกป้องข้อมูลส่วนบุคคลจากการเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์

การรับรู้ถึงประโยชน์ เกี่ยวกับการตั้งค่าในการปกป้องข้อมูลส่วนบุคคลจากการเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์

การรับรู้ถึงความง่ายในการใช้งาน ที่ไม่ต้องอาศัยความพยายามมากนักต่อการทำความเข้าใจ ทางด้านการเรียนรู้การตั้งค่าวิธีการปกป้องข้อมูลส่วนบุคคลให้มีความปลอดภัยบนเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์

2.4 ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

จากการประมวลเอกสารและการสังเคราะห์งานวิจัยที่เกี่ยวข้อง พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์เกิดจากตัวแปรเชิงสาเหตุ ซึ่งสามารถแบ่งออกเป็น 2 กลุ่มทฤษฎี ประกอบด้วย กลุ่มที่ 1 ทฤษฎีแรงจูงใจเพื่อการป้องกัน และกลุ่มที่ 2 แบบจำลองการยอมรับการใช้เทคโนโลยี เพื่อศึกษาถึงตัวแปรเหตุที่เกี่ยวข้องกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งมีรายละเอียดดังนี้

การประเมินภัยคุกคาม (Threat Appraisal)

2.4.1 **การรับรู้ถึงโอกาสเสี่ยง** (Perceived Vulnerability)

ความหมายและองค์ประกอบ

จากทฤษฎีแรงจูงใจเพื่อกันป้องกัน ซึ่งในการศึกษาทางด้านสุขภาพของ Rogers et al. (1997) ได้กล่าวถึงการรับรู้ถึงโอกาสเสี่ยงต่อการเกิดโรค ว่าเป็นความเชื่อของบุคคลว่าเกี่ยวกับความเป็นไปได้ว่ามีโอกาสจะเกิดโรค หากไม่มีการปรับพฤติกรรมด้านสุขภาพที่ถูกต้อง และการรับรู้ถึงโอกาสเสี่ยงต่อการเป็นโรคขึ้นอยู่กับการตัดสินใจของแต่ละบุคคล หากโอกาสเสี่ยงต่อการเกิดโรคสูงจะส่งผลต่อความตั้งใจในการปฏิบัติตนเพื่อลดความเสี่ยงนั้น (Rogers, 1983; Maddux & Rogers., 1983) นั่นหมายความว่าการรับรู้โอกาสเสี่ยงต่อการเกิดโรคสูงจะเป็นผลดีในการปฏิบัติตนด้วยความตั้งใจเพิ่มขึ้นตามไปด้วย ซึ่งหากนำทฤษฎีแรงจูงใจเพื่อกันป้องกันเกี่ยวกับปัจจัยการรับรู้ถึงโอกาสเสี่ยงมาประยุกต์ใช้ทางการปกป้องข้อมูลส่วนบุคคล ในงานวิจัยของ Lee & Larsen (2009) และ Bulgurcu et al., (2010) จะหมายถึงการรับรู้ความเสี่ยงด้านระบบสารสนเทศและความปลอดภัยของข้อมูล ที่ไม่สามารถปกป้องให้เกิดความปลอดภัยได้และทำให้ข้อมูลที่มีความสำคัญรั่วไหล เช่น ข้อมูลด้านการเงิน ข้อมูลประวัติของลูกค้า เป็นต้น ซึ่งเป็นความ

เสี่ยงที่เกี่ยวข้องกับความปลอดภัยข้อมูลในลักษณะเชิงลบ มีความสัมพันธ์กับความเชื่อมั่นและความตั้งใจในการกระทำ และงานวิจัยของ Dinev & Hart (2006) การรับรู้ความเสี่ยงหมายถึงความสูญเสียที่อาจเกิดขึ้นจากการเปิดเผยข้อมูลส่วนบุคคนบนเครือข่ายอินเทอร์เน็ตจากการเข้าใช้งานเพื่อการพาณิชย์อิเล็กทรอนิกส์และความเป็นส่วนตัว ซึ่งสอดคล้องกับความหมายในงานวิจัยของ Tingchi et al. (2013)

องค์ประกอบของการรับรู้ความเสี่ยงที่มีเกี่ยวข้องกับการใช้งานบนเครือข่ายอินเทอร์เน็ต จากการทบทวนวรรณกรรมได้มีนักวิชาการที่ศึกษาและจำแนกองค์ประกอบการรับรู้ความเสี่ยงด้านความเป็นส่วนตัวที่เกี่ยวข้องกับการใช้งานบนเครือข่ายอินเทอร์เน็ตที่สำคัญดังนี้ จากการศึกษาของ Doherty et al. (2006) เกี่ยวกับการรับรู้เสี่ยงกับแบบจำลองการยอมรับทางเทคโนโลยี แบ่งองค์ประกอบการรับรู้ความเสี่ยงของผู้ใช้บริการออกเป็น 2 ด้าน ได้แก่ 1) การรับรู้ความเสี่ยงเกี่ยวกับข้อมูลส่วนบุคคลของผู้ใช้บริการ เป็นการละเมิดหรือการลักลอบนำข้อมูลส่วนบุคคลของผู้ใช้บริการไปใช้งานโดยไม่ได้รับการอนุญาตหรือยินยอม และ 2) การรับรู้ความเสี่ยงด้านความปลอดภัย เป็นการสูญเสียที่ผู้ใช้บริการอาจได้รับจากความไม่ปลอดภัยของระบบคอมพิวเตอร์ เช่นเดียวกับ Dinev & Hart (2006) ได้มีการศึกษาเกี่ยวกับการรับรู้ความเสี่ยงจากการเปิดเผยข้อมูลส่วนบุคคนบนเครือข่ายอินเทอร์เน็ตและจำแนกองค์ประกอบเป็น 4 องค์ประกอบได้แก่ การส่งต่อข้อมูลส่วนบุคคลไปยังบุคคลที่สาม (Third Parties) การนำข้อมูลส่วนบุคคลไปใช้ในทางที่ไม่ถูกต้องจากการชำระเงิน การไม่ได้รับอนุญาตหรือบอกกล่าวว่านำข้อมูลส่วนบุคคลไปใช้งาน และการส่งข้อมูลส่วนบุคคลไปยังหน่วยงานภาครัฐ ส่วน Doolin et al., (2005) จำแนกองค์ประกอบการรับรู้ความเสี่ยงจากประสบการณ์ซื้อสินค้าออนไลน์ (Internet Shopping Experience) ออกเป็น 4 ด้าน ได้แก่ การรับรู้ความเสี่ยงด้านประสิทธิภาพของสินค้า ด้านจิตวิทยา ด้านเวลาและด้านการเงิน

สำหรับงานวิจัยนี้ ได้ให้ความหมายของ การรับรู้ถึงโอกาสเสี่ยง หมายถึงความเชื่อของบุคคลเกี่ยวกับความเป็นไปได้ในความไม่ปลอดภัยของเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ที่ใช้บริการนั้น มีข้อบกพร่องในการใช้งานหรือมีจุดอ่อนของระบบการปกป้องข้อมูลส่วนบุคคล ซึ่งเป็นข้อบกพร่องที่อาจมาจากขั้นตอนการออกแบบระบบ ข้อผิดพลาดจากการเขียนโปรแกรม ระบบคอมพิวเตอร์ของผู้ให้บริการ เป็นต้น ทำให้ระบบอนุญาตให้บุคคลอื่นหรือหน่วยงานภายนอกสามารถเข้ามาใช้งานแทนหรือบุกรุกความเป็นส่วนตัว โดยการนำเอาข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาต ซึ่งการรับรู้ถึงโอกาสเสี่ยงจะส่งผลทางบวกต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลให้มีความปลอดภัยจากการเข้าใช้งานเว็บไซต์หรือแอปพลิเค

ชันธุรกรรมทางอิเล็กทรอนิกส์ และแบ่งองค์ประกอบการรับรู้ความเสี่ยงที่บุคคลอื่นจะเข้าใช้งานแทนตน เป็นจำนวน 2 ด้าน โดยการประยุกต์ใช้งานวิจัยของ Doherty et al. (2006) ได้แก่ ได้แก่ การรับรู้โอกาสเสี่ยงที่อาจมาจากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์และการรับรู้โอกาสเสี่ยงจากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์

การวัดการรับรู้ถึงโอกาสเสี่ยง

ในการศึกษางานวิจัยที่เกี่ยวข้อง พบว่างานวิจัยของ Dinev & Hart (2006) ได้ทำแบบวัดการรับรู้ความเสี่ยงด้านความเป็นส่วนตัวจากการใช้บริการบนเว็บไซต์และการพาณิชย์อิเล็กทรอนิกส์ จำนวน 4 ข้อ ซึ่งเกี่ยวข้องกับการรับรู้ความเสี่ยงในการส่งต่อข้อมูลส่วนบุคคลไปยังบุคคลที่สาม การนำข้อมูลส่วนบุคคลไปใช้ในทางที่ไม่ถูกต้อง ซึ่งอาจเกิดความเสียหายต่อผู้ใช้งาน การนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาตและหน่วยงานภาครัฐสามารถเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับการยินยอม มีลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 5 ระดับ โดยใช้มาตราส่วนประมาณค่าของ Likert (1932) จาก “เห็นด้วยอย่างยิ่ง” (Strongly Agree) ถึง “ไม่เห็นด้วยอย่างยิ่ง” (Strongly Disagree) และงานวิจัยของ Moloney & Poti (2013) ซึ่งทำการศึกษาแบบวัดด้านรับรู้ความเสี่ยงในการเปิดเผยข้อมูลส่วนบุคคล จำนวน 6 ข้อ เกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคลเพื่อการแลกเปลี่ยนในการได้มาซึ่งผลประโยชน์ที่จะได้รับบนเครือข่ายอินเทอร์เน็ต มีแบบวัดเป็นมาตราวัดประเมินค่า 7 ระดับ จาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง”

สำหรับงานวิจัยเรื่องนี้ ผู้วิจัยใช้แบบวัดซึ่งพัฒนาและปรับปรุงจากแบบวัดการรับรู้ความเสี่ยงของ Dinev & Hart (2006) และ Moloney & Poti (2013) จำนวน 10 ข้อ โดยให้เป็นไปตามขอบเขตเนื้อหาและนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ตามลำดับ ส่วนข้อความทางลบเป็นการให้คะแนนในทางตรงกันข้าม

งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยที่เกี่ยวข้องกับการรับรู้ความเสี่ยง ในการศึกษาของ Dinev & Hart (2006) พบว่าระดับการรับรู้ความเสี่ยงด้านความเป็นส่วนตัวเกี่ยวข้องกับการส่งต่อข้อมูลส่วนบุคคลไปยังบุคคลที่สาม การนำข้อมูลส่วนบุคคลไปใช้ในทางที่ไม่ถูกต้อง การไม่ได้รับอนุญาตหรือบอกกล่าวว่านำข้อมูลส่วนบุคคลไปใช้งาน และการส่งข้อมูลส่วนบุคคลไปยัง

หน่วยงานภาครัฐที่มีส่วนเกี่ยวข้อง จากธุรกรรมการพาณิชย์อิเล็กทรอนิกส์ที่เพิ่มขึ้นส่งผลทำให้ระดับความตั้งใจที่จะให้ข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ลดลง สอดคล้องกับงานวิจัยของ Keith et al. (2013) จากการศึกษาพฤติกรรมการเปิดเผยข้อมูลส่วนบุคคลผ่านอุปกรณ์พกพา (Mobile Devices) พบว่าการรับรู้ความเสี่ยงด้านความเป็นส่วนตัวของผู้ใช้งานเครือข่ายอินเทอร์เน็ตผ่านอุปกรณ์พกพาเป็นปัจจัยสำคัญที่ส่งผลต่อระดับการเปิดเผยข้อมูลส่วนบุคคล ทั้งด้านการรับรู้ความเสี่ยงด้านการชำระเงินและการรับรู้ความเสี่ยงด้านความปลอดภัยในข้อมูลส่วนบุคคล รวมทั้งงานวิจัยของสัญชัย อุปะเดีย (2553) พบว่าปัจจัยการรับรู้เกี่ยวกับระบบพาณิชย์อิเล็กทรอนิกส์ด้านการรับรู้ความเสี่ยงความเป็นส่วนตัว ประกอบด้วย การนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาตและข้อมูลส่วนบุคคลอาจถูกนำไปขายต่อให้กับบุคคลอื่นทางธุรกิจและด้านการชำระเงิน มีผลต่อการตัดสินใจใช้บริการชำระเงินผ่านระบบพาณิชย์อิเล็กทรอนิกส์อย่างมีระดับนัยสำคัญ 0.05

ดังนั้น จากการทบทวนเอกสารและงานวิจัยที่เกี่ยวข้อง ผู้วิจัยจึงคาดว่า การรับรู้ความเสี่ยงมีอิทธิพลทางตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ และมีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

2.4.2 **การรับรู้ถึงความรุนแรง** (Perceived Severity)

ความหมายและองค์ประกอบ

จากการศึกษาในมุมมองความเชื่อด้านข้อมูล สารสนเทศกับพฤติกรรมการปกป้องข้อมูล พบว่าจากการศึกษาของ Lee & Larsen (2009) หมายถึงความไม่ปลอดภัยของข้อมูลที่ส่งผลต่อผู้ใช้งาน ทำให้ผู้ใช้งานมีการปรับเปลี่ยนพฤติกรรมเพื่อป้องกันความรุนแรงที่อาจเกิดขึ้นกับอุปกรณ์อิเล็กทรอนิกส์ และหากบุคคลรับรู้ถึงผลกระทบที่อาจขึ้นจากภัยคุกคามด้านความไม่ปลอดภัยของข้อมูลส่วนบุคคลจากการใช้งานคอมพิวเตอร์ จะทำให้เกิดความหวาดกลัวและวิตกกังวลขึ้น และความไม่ปลอดภัยของข้อมูลส่วนบุคคลจะส่งผลในการรับรู้ถึงความรุนแรงของแต่ละบุคคลที่แตกต่างกันไป (Ng et al., 2009)

องค์ประกอบของการรับรู้ถึงความรุนแรง จากการทบทวนวรรณกรรมได้มีนักวิชาการที่ศึกษาและจำแนกองค์ประกอบการรับรู้ถึงความรุนแรงกับการใช้งานบนเครือข่ายอินเทอร์เน็ตที่สำคัญคือ จากงานวิจัยของ Woon et al., (2005) ที่ ได้จัดแบ่งองค์ประกอบของการรับรู้ถึงความรุนแรงด้านความไม่ปลอดภัยในการใช้งานคอมพิวเตอร์เครือข่ายเป็น 2 ด้าน ได้แก่ 1) การบุกรุกความเป็นส่วนตัวหรือการถูกขโมยตัวตน (Online Identity Stolen) จากผู้ไม่ได้รับ

อนุญาติให้ใช้งาน ซึ่งมาจากการเจาะระบบเครือข่ายคอมพิวเตอร์ (Hacking) และ 2) การใช้งานซอฟต์แวร์ที่ไม่ปลอดภัยหรือเป็นอันตราย (Malicious Software) ซึ่งเป็นภัยคุกคามเกี่ยวกับความปลอดภัยทางด้านซอฟต์แวร์ เช่น ไวรัสคอมพิวเตอร์ สปายแวร์ (Spyware) การหลอกลวงข้อมูลทางอินเทอร์เน็ต (Phishing) จนทำให้เกิดการสูญเสียข้อมูลที่เป็นความลับ

สำหรับงานวิจัยนี้ ได้ให้ความหมายของการรับรู้ถึงความรุนแรง หมายถึง การประเมินการรับรู้ของบุคคลต่อข้อมูล ข่าวสารที่เกิดขึ้นว่าเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ที่ใช้บริการนั้น มีข้อบกพร่องในการใช้งานหรือมีจุดอ่อนของระบบการปกป้องข้อมูลส่วนบุคคล หากมีบุคคลอื่นหรือหน่วยงานภายนอกสามารถเข้ามาใช้งานแทนหรือบุกรุกความเป็นส่วนตัว จะก่อให้เกิดความเสียหายและอันตรายโดยการนำเอาข้อมูลส่วนบุคคลไปใช้ เช่น ความเสียหายด้านทรัพย์สิน จำนวนเงินที่สูญเสียไป รูปแบบการดำเนินชีวิต การถูกทำร้ายด้านร่างกายและสุขภาพ การไม่สามารถเข้าใช้งานธุรกรรมทางอิเล็กทรอนิกส์ต่อไปได้ ความสับสนและยุ่งยากในการใช้งานธุรกรรมทางอิเล็กทรอนิกส์ โดยแบ่งองค์ประกอบการรับรู้ถึงความรุนแรงด้านไม่ความปลอดภัยของข้อมูลส่วนบุคคลเป็นจำนวน 2 ด้าน จากการประยุกต์ใช้งานวิจัยของ Woon et al., (2005) ประกอบด้วย การบุกรุกความเป็นส่วนตัวเกี่ยวกับการรับรู้ถึงความรุนแรงด้านทรัพย์สินและการรับรู้ถึงความรุนแรงด้านอันตรายที่อาจเกิดขึ้นกับตัวบุคคล

การวัดการรับรู้ถึงความรุนแรง

จากการค้นคว้าและศึกษางานวิจัยที่เกี่ยวข้องได้พบว่า มีงานวิจัยจำนวนหนึ่งได้นำองค์ประกอบของการรับรู้ถึงความรุนแรงด้านความไม่ปลอดภัยในการใช้งานคอมพิวเตอร์เครือข่ายของ Woon et al., (2005) มาประยุกต์ใช้เป็นแบบวัด เช่น ในงานวิจัยของ Ifinedo (2012) ได้ทำแบบวัดการรับรู้ถึงความรุนแรงในการไม่ปฏิบัติตามนโยบายความปลอดภัยด้านระบบสารสนเทศจำนวน 7 ข้อ เกี่ยวกับการรับรู้ถึงความรุนแรงจากความสูญหายของข้อมูลและความไม่ปลอดภัยจากการถูกโจมตีทางด้านระบบคอมพิวเตอร์ในองค์กร มีแบบวัดเป็นมาตราวัดประเมินค่า 7 ระดับ จาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง” ส่วนงานวิจัยของ Klein & Luciano (2016) ศึกษาปัจจัยการรับรู้ถึงความรุนแรงในพฤติกรรมการปกป้องข้อมูลส่วนบุคคลในกลุ่มผู้ใช้งานในประเทศบราซิล ซึ่งจัดทำแบบวัดจำนวน 3 ข้อ จากการใช้งานซอฟต์แวร์ที่ไม่ปลอดภัย มีลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 5 ระดับ จาก “เห็นด้วยอย่างยิ่ง” (Strongly Agree) ถึง “ไม่เห็นด้วยอย่างยิ่ง” (Strongly Disagree) และงานวิจัยของ Boerman et al., (2018) เป็นปัจจัยการรับรู้ถึงความรุนแรงจากการถูกคุกคามความเป็นส่วนตัว (Perceived severity to online

privacy threats) จากการใช้งานอินเทอร์เน็ตในชีวิตประจำวัน จำนวน 5 ข้อ มีแบบวัดเป็นมาตราวัดประเมินค่า 7 ระดับ จาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง”

สำหรับงานวิจัยเรื่องนี้ ผู้วิจัยใช้แบบวัดซึ่งพัฒนาและปรับปรุงจากแบบวัดการรับรู้ถึงความรุนแรงจากการถูกคุกคามความเป็นส่วนตัวของ Boerman et al., (2018) และ Klein & Luciano (2016) จำนวน 7 ข้อ โดยให้เป็นไปตามขอบเขตเนื้อหาและนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ตามลำดับ ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม

งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยของ Boerman et al., (2018) พบว่าการรับรู้ถึงความรุนแรงจากการถูกคุกคามความเป็นส่วนตัวเกี่ยวกับการถูกขโมยตัวตนออนไลน์ และข้อมูลส่วนบุคคลจากการเข้าใช้งานอินเตอร์เน็ตเป็นประจำ เช่น การซื้อสินค้าและบริการออนไลน์ การใช้งานอีเมล์และสื่อสังคมออนไลน์ การดาวน์โหลดข้อมูล เป็นต้น เป็นปัจจัยที่สำคัญกับความตั้งใจและการปรับพฤติกรรมการปกป้องความเป็นส่วนตัว เช่นเดียวกับงานวิจัยของ Ng et al., (2009) และ Youn (2009) และในงานวิจัย Woon et al., (2005) พบว่าการถูกขโมยตัวตน และการใช้งานซอฟต์แวร์ที่ไม่ปลอดภัยจากความรุนแรงจากการถูกคุกคามบนเครือข่ายอินเทอร์เน็ต ส่งผลต่อความตั้งใจในการรักษาความปลอดภัยในการใช้งานเครือข่ายไร้สายภายในบ้าน

ดังนั้น จากการทบทวนเอกสารและงานวิจัยที่เกี่ยวข้อง ผู้วิจัยจึงคาดว่า การรับรู้ถึงความรุนแรงมีอิทธิพลทางตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ และมีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

การประเมินการเผชิญปัญหา (Coping Appraisal)

2.4.3 **ความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล** (Response Efficacy)

ความหมายและองค์ประกอบ

ในมุมมองด้านข้อมูล สารสนเทศ จากการศึกษาของ Ng et al., (2009) และ Srisawang et al. (2015) เกี่ยวกับปัจจัยที่ส่งผลพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ ว่าความคาดหวังในผลลัพธ์จากการปฏิบัติตามวิธีการเพื่อป้องกันภัยจาก

อาชญากรรมคอมพิวเตอร์เป็นความเชื่อมั่นของบุคคลต่อประสิทธิภาพของมาตรการในการป้องกันภัยที่ได้รับการแนะนำ เช่น การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ การปิดการใช้งานคุ๊กกี้ (Internet Cookies) ในขณะเข้าใช้งานอินเทอร์เน็ต เป็นต้น และจากการศึกษาของ Chenoweth et al., (2009) จะหมายถึงระดับความเชื่อมั่นของผู้ใช้งานในเครือข่ายคอมพิวเตอร์ที่มีต่อความสามารถในการดำเนินการแก้ไขปัญหาที่เกิดขึ้น ซึ่งอาจจะมาจากติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ จะเห็นว่าความคาดหวังในผลลัพธ์จากการปฏิบัติตามวิธีการเพื่อป้องกันภัยทางเครือข่ายคอมพิวเตอร์จะส่งผลให้เกิดความตั้งใจในการป้องกันภัยทางเครือข่ายคอมพิวเตอร์

องค์ประกอบความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล จากการทบทวนวรรณกรรมที่เกี่ยวข้อง พบว่าในงานวิจัยของ Workman et al. (2008) และ Yoon et al. (2019) ได้จำแนกองค์ประกอบความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการในการป้องกันภัยจากการศึกษาปัจจัยที่ส่งผลต่อพฤติกรรมในการปกป้องและความปลอดภัยข้อมูล (Behaviors in information security) โดยใช้ทฤษฎีแรงจูงใจในการป้องกันจำนวน 2 ด้าน ประกอบด้วย 1) ความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการป้องกันภัยจากวิธีการปฏิบัติทางด้านซอฟต์แวร์ที่ไม่ปลอดภัย (Malicious software) รวมไปถึงการใช้งานบนระบบเครือข่ายอินเทอร์เน็ตและอุปกรณ์คอมพิวเตอร์ และ 2) ความคาดหวังในผลลัพธ์ของการปฏิบัติตามผู้มีความรู้และเชี่ยวชาญทางด้านคอมพิวเตอร์

จากการทบทวนวรรณกรรมที่เกี่ยวข้องข้างต้น สำหรับงานวิจัยนี้ ได้ให้ความหมายของความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล จะหมายถึง ความเชื่อ ความรู้สึกนึกคิด การรับรู้และการคาดการณ์ของเฉพาะบุคคลว่า การปฏิบัติตามขั้นตอน ระเบียบปฏิบัติ มาตรการ คำแนะนำ เอกสารหรือคู่มือข้อควรปฏิบัติในการดูแล รักษาข้อมูลส่วนบุคคล จะสามารถลดโอกาสเสี่ยงและปกป้องข้อมูลส่วนบุคคลจากการเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ได้ โดยมีองค์ประกอบความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลจำนวน 2 ด้าน จากการประยุกต์ใช้งานวิจัยของ Workman et al. (2008) และ Yoon et al. (2019) ประกอบด้วยความคาดหวังในผลลัพธ์ตามวิธีการปฏิบัติตนตามคำแนะนำที่ควรปฏิบัติโดยทั่วไป และความคาดหวังในผลลัพธ์ตามวิธีการปฏิบัติตนตามคำแนะนำที่ควรปฏิบัติแบบขั้นสูง

การวัดความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล

จากการศึกษางานวิจัยที่เกี่ยวข้อง ในงานวิจัยของ Chenoweth et al., (2009) ได้ศึกษาแบบวัดความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลจากการประยุกต์ใช้ทฤษฎีแรงจูงใจในการป้องกัน เพื่อการปกป้องภัยคุกคามทางด้านเทคโนโลยีที่มีจากสปายแวร์ (Spyware) ซึ่งเป็นซอฟต์แวร์แฝงเข้ามาในขณะใช้งานอินเทอร์เน็ต จำนวน 4 ข้อ ลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 5 ระดับจาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง” โดยใช้มาตราส่วนประมาณค่าของ Likert (1932) และในงานวิจัยของ Workman et al. (2008) มีการจัดทำแบบวัดความคาดหวังในผลลัพธ์ของการปฏิบัติตามการป้องกันความปลอดภัยของข้อมูล (Information security measures) ซึ่งเกี่ยวข้องกับการขโมยข้อมูลส่วนบุคคลและการใช้งานด้านซอฟต์แวร์ จำนวน 6 ข้อ มีลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 5 ระดับจาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง”

สำหรับงานวิจัยเรื่องนี้ ผู้วิจัยใช้แบบวัดซึ่งพัฒนาและปรับปรุงจากแบบวัดของ Workman et al. (2008) จำนวน 6 ข้อ โดยให้เป็นไปตามขอบเขตเนื้อหาและนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ตามลำดับ ส่วนข้อความทางลบเป็นการให้คะแนนในทางตรงกันข้าม

งานวิจัยที่เกี่ยวข้อง

ในงานวิจัยของ Crossler (2009) ได้พบว่าความคาดหวังในผลลัพธ์ของการปฏิบัติตามการป้องกันความปลอดภัยของข้อมูลที่มาจากการโจมตีของบุคคล ส่งผลต่อความตั้งใจและพฤติกรรมในการรักษาความปลอดภัยของบุคคล (Individual Secuiry Bahavior) ซึ่งสอดคล้อดคล้องกับงานวิจัยของ Yoon et al. (2019) ซึ่งหากบุคคลเชื่อว่ามีเครื่องมือที่สามารถป้องกันภัยทางเทคโนโลยีได้ จะทำให้สามารถรับรู้ถึงประสิทธิภาพในการป้องกันความปลอดภัยของข้อมูล และงานวิจัยของ Ifinedo (2012) พบว่าปัจจัยด้านความคาดหวังในผลลัพธ์ของการปฏิบัติตามการป้องกันความปลอดภัยของข้อมูลส่งผลต่อความตั้งใจในการปฏิบัติตนตามนโยบายความปลอดภัยด้านสารสนเทศ

ดังนั้น จากการทบทวนเอกสารและงานวิจัยที่เกี่ยวข้อง ผู้วิจัยจึงคาดว่าความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ และมีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

2.4.4 **ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล (Self-Efficacy)**

ความหมายและองค์ประกอบ

ความคาดหวังในความสามารถของตนเองหรือการรับรู้ความสามารถของตนเป็นความเชื่อในความสามารถของตนเองว่า ตนเองสามารถกระทำหรือปฏิบัติตามคำแนะนำเพื่อนำไปสู่ผลลัพธ์ที่คาดไว้ (Outcome expectations) และบุคคลที่รับรู้ในความสามารถของตนเองสูงจะส่งผลต่อความสำเร็จสูงตามไปด้วย (Bandura, 1977) ซึ่งการรับรู้ความสามารถของตนเองไม่ได้ขึ้นอยู่กับทักษะที่บุคคลมีเพียงอย่างเดียว ยังขึ้นอยู่กับการตัดสินว่าตนจะสามารถทำอะไรได้จากทักษะที่มี ซึ่งส่งผลต่อความพยายามและความอดทนต่ออุปสรรคขัดขวางต่างๆ ในมุมมองความเชื่อด้านข้อมูล สารสนเทศ พบว่าในงานวิจัย Compeau & Higgins (1995) และ Sedek et al., (2018) จะหมายถึงความเชื่อและความสามารถของบุคคล (Individual's belief and capability) ทางด้านคอมพิวเตอร์ (Computer self-efficacy) ต่อแรงจูงใจและพฤติกรรมการปกป้องความเป็นส่วนตัวจากการใช้งานเครือข่ายอินเทอร์เน็ต

องค์ประกอบความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล จากการทบทวนวรรณกรรมที่เกี่ยวข้อง ได้มีนักวิชาการที่มีการศึกษาถึงองค์ประกอบความคาดหวังในความสามารถของตนเองที่เกี่ยวข้องด้านคอมพิวเตอร์ ซึ่งจากการวิจัยของ Rhee et al., (2009) จากการศึกษาการรับรู้ในความสามารถของตนในความปลอดภัยด้านข้อมูล (Self-efficacy in information security) ที่ส่งผลต่อการปฏิบัติตนของผู้ใช้งาน ได้จัดแบ่งองค์ประกอบความคาดหวังความสามารถของตนเองในความปลอดภัยด้านข้อมูลเป็น 3 องค์ประกอบ ได้แก่ 1) ประสบการณ์ในการใช้งานคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต ซึ่งรวมไปถึงความเชื่อมั่นในตนเองด้านการมีทักษะ (Skills) และความเชี่ยวชาญ 2) การแก้ไขสถานการณ์หากมีการละเมิดความเป็นส่วนตัว (Security Breach Incidents) ซึ่งเป็นการเตรียมความพร้อมในการรับมือหรือเผชิญปัญหากับภัยคุกคามทางด้านเทคโนโลยีที่อาจเกิดขึ้นได้ และ 3) ความรู้โดยทั่วไปที่สามารถควบคุมสถานการณ์ได้ (General Controllability) เกี่ยวข้องกับการรับรู้ของบุคคลในการควบคุมภัยคุกคามทางด้านเทคโนโลยีที่อาจเกิดขึ้น หรือแนวปฏิบัติโดยทั่วไปเพื่อรักษาความปลอดภัยและควบคุมความเสี่ยงทางเทคโนโลยี ซึ่งสอดคล้องกับงานวิจัยของ Yoon et al., (2019) สำหรับ

งานวิจัยของ Workman et al. (2008) องค์ประกอบความคาดหวังความสามารถของตนเองในความปลอดภัยด้านข้อมูลว่าเป็นเรื่องของทักษะและความสามารถของบุคคลด้านความปลอดภัยของข้อมูล (Abilities) โดยทั่วไปและทักษะที่จำเป็นในการใช้งานอินเทอร์เน็ต

สำหรับงานวิจัยนี้ ได้ให้ความหมายของความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลจะหมายถึง การประเมินความสามารถและการรับรู้ของเฉพาะบุคคลว่า ตนเองสามารถที่จะปกป้องข้อมูลส่วนบุคคล มีความสามารถที่จะการควบคุมการเปิดเผยข้อมูล (Disclosure) และการเก็บบันทึกข้อมูลส่วนบุคคลได้อย่างถูกต้อง เหมาะสมและปลอดภัย เมื่อเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ รวมไปถึงความสามารถในการใช้งานเครือข่ายอินเทอร์เน็ตเพื่อการปกป้องข้อมูลส่วนบุคคล โดยศึกษาองค์ประกอบความคาดหวังความสามารถของตนเอง จากการประยุกต์ใช้งานวิจัยของ Rhee et al., (2009) จำนวน 3 องค์ประกอบ ได้แก่ 1) ประสบการณ์ในการใช้งานคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต การมีทักษะ (Skills) และความเชี่ยวชาญ 2) การเตรียมความพร้อมในเผชิญปัญหากับภัยคุกคามทางด้านเทคโนโลยี และ 3) ความสามารถในการควบคุมสถานการณ์ได้ เมื่อเกิดภัยคุกคามทางด้านเทคโนโลยี

การวัดความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล

จากการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง พบว่าจากการศึกษาของ Compeau & Higgins (1995) เกี่ยวกับความคาดหวังความสามารถของตนเองทางด้านคอมพิวเตอร์ ได้จัดทำแบบวัดและแบบทดสอบเบื้องต้นจำนวน 10 ข้อ ลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 7 ระดับ จาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง” และงานวิจัยของ Workman et al. (2008) ได้สร้างและพัฒนาแบบวัดความคาดหวังความสามารถของตนเองจากการใช้งานอินเทอร์เน็ต (Internet self-efficacy) มาจาการศึกษาทฤษฎีแรงจูงใจเพื่อการป้องกัน (Rogers, 1983) และทฤษฎีความคาดหวังในความสามารถของตนเอง (Bandura, 1977) พบข้อคำถามจำนวน 7 ข้อ มีลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 5 ระดับจาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง”

สำหรับงานวิจัยเรื่องนี้ ผู้วิจัยใช้แบบวัดซึ่งพัฒนาและปรับปรุงจากแบบวัดของ Compeau & Higgins (1995) และ Workman et al. (2008) จำนวน 7 ข้อ โดยให้เป็นไปตามขอบเขตเนื้อหาและนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการ

ตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ตามลำดับ ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม

งานวิจัยที่เกี่ยวข้อง

ในงานวิจัยของ Eastin & LaRose (2000) พบว่าความคาดหวังความสามารถของตนเองจากการใช้งานอินเทอร์เน็ตและดิจิทัล ซึ่งเป็นความเชื่อของบุคคลทางด้านทักษะ ประสบการณ์และความสามารถ (Capabilities) เป็นปัจจัยที่ส่งผลต่อความตั้งใจของพฤติกรรมในการใช้งานอินเทอร์เน็ต สำหรับงานวิจัยของ Rhee et al., (2009) ความคาดหวังความสามารถของตนเองในความปลอดภัยด้านข้อมูลของผู้ใช้งานในชีวิตประจำวัน เช่นเดียวกับ Chen et al., (2017) ได้พบว่าความคาดหวังความสามารถของตนเองทางด้านระบบคอมพิวเตอร์ ความรู้ด้านความเป็นส่วนตัว (Privacy knowledge) ประสบการณ์ใช้งานอินเทอร์เน็ตและการเผชิญปัญหาที่เกิดขึ้นกับความปลอดภัยของข้อมูล ส่งผลทางบวกต่อความตั้งใจและพฤติกรรมในการปกป้องข้อมูลจากการใช้งานอินเทอร์เน็ต

ดังนั้น จากการทบทวนเอกสารและงานวิจัยที่เกี่ยวข้อง ผู้วิจัยจึงคาดว่าความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ และมีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

2.4.5 **ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อการปกป้องข้อมูลส่วนบุคคล** (Response Costs)

ความหมายและองค์ประกอบ

จากการศึกษาของ Boehmer et al., (2015) จะหมายถึงการรับรู้เกี่ยวกับค่าใช้จ่ายที่สูญเสียไปเพื่อการยอมรับในการปรับเปลี่ยนพฤติกรรมด้านความปลอดภัยจากการใช้งานเครือข่ายอินเทอร์เน็ต ส่วนงานวิจัยของ Ifinedo (2012) หมายถึงความเป็นไปได้ในด้านค่าใช้จ่าย และเวลาในการที่จะปฏิบัติตามความปลอดภัยด้านข้อมูล

องค์ประกอบความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อการปกป้องข้อมูลส่วนบุคคล จากการทบทวนวรรณกรรมที่เกี่ยวข้องพบว่า Lee et al., (2008) ได้จำแนกต้นทุนที่จ่ายไปในการปกป้องพฤติกรรมจากการใช้งานเครือข่ายอินเทอร์เน็ตจำนวน 3 องค์ประกอบ ได้แก่ ค่าใช้จ่าย เวลาและความพยายาม ส่วนงานวิจัยของ Ifinedo (2012) แบ่ง

การศึกษาเป็น 2 องค์ประกอบเกี่ยวกับค่าใช้จ่าย และอุปสรรคด้านเวลาที่ต้องสูญเสียไปในการปฏิบัติตนเพื่อปกป้องข้อมูลส่วนบุคคล

สำหรับงานวิจัยนี้ ได้ให้ความหมายของความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อการปกป้องข้อมูลส่วนบุคคล จะหมายถึงการประเมินและการรับรู้ของเฉพาะบุคคลว่าต้นทุน ผลตอบแทนหรือความคุ้มค่า ซึ่งอาจอยู่ในรูปของเงินที่ต้องจ่ายเพิ่ม เวลาที่ต้องเสียไป ความพยายาม และความยากลำบากเพื่อลดโอกาสเสี่ยงและการปกป้องข้อมูลส่วนบุคคล จะสามารถปกป้องข้อมูลส่วนบุคคลให้ปลอดภัยจากการเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ได้ โดยมีองค์ประกอบจำนวน 2 ด้าน จากการประยุกต์และปรับใช้งานวิจัยของ Ifinedo (2012); Lee et al., (2008) เพื่อให้เป็นการศึกษาที่เข้าใจง่ายและเป็นเชิงเศรษฐศาสตร์พฤติกรรมได้แก่ ความคาดหวังในความคุ้มค่าของต้นทุนหรือค่าใช้จ่ายที่อยู่ในรูปตัวเงิน (Tangible Costs) และต้นทุนหรือค่าใช้จ่ายที่ไม่ได้อยู่ในรูปตัวเงิน (Intangible Costs)

การวัดความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อการปกป้องข้อมูลส่วนบุคคล

จากการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง พบว่างานวิจัยของพบว่าจากการศึกษาของ Boehmer et al., (2015) เกี่ยวกับความคาดหวังจากต้นทุนที่จ่ายไปเพื่อความปลอดภัยทางด้านคอมพิวเตอร์ ได้จัดทำแบบวัดจำนวน 6 ข้อ ลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 7 ระดับ จาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง” และงานวิจัยของ Ifinedo (2012) ได้สร้างและพัฒนาแบบวัดความคาดหวังจากต้นทุนที่จ่ายไปเพื่อการปฏิบัติตามความปลอดภัยด้านข้อมูล พบข้อคำถามจำนวน 5 ข้อ มีลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 7 ระดับ จาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง”

สำหรับงานวิจัยเรื่องนี้ ผู้วิจัยใช้แบบวัดซึ่งพัฒนาและปรับปรุงจากแบบวัดของ Boehmer et al., (2015) และ Ifinedo (2012) จำนวน 7 ข้อ โดยให้เป็นไปตามขอบเขตเนื้อหาและนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ตามลำดับ ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม

งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยที่เกี่ยวข้อง พบว่างานวิจัยของ LeFebvre (2012) เกี่ยวกับความคาดหวังจากต้นทุนที่จ่ายไปมีอิทธิพลทางลบต่อแรงจูงใจและพฤติกรรมของผู้ใช้งานเครือข่ายอินเทอร์เน็ตในการปกป้องความเป็นส่วนตัว ซึ่งสอดคล้องกับงานวิจัยของ Lee et al., (2008) และ Boehmer et al., (2015)

ดังนั้น จากการทบทวนเอกสารและงานวิจัยที่เกี่ยวข้อง ผู้วิจัยจึงคาดว่าความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์และมีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

2.4.6 ตัวแปรแบบจำลองการยอมรับการใช้เทคโนโลยี

จากแนวคิดแบบจำลองการยอมรับการใช้เทคโนโลยี งานวิจัยนี้เป็นการสังเคราะห์ตัวแปรเหตุจากวรรณกรรมที่เกี่ยวข้องและนำมาประยุกต์ใช้ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ จึงได้ทำการให้ความหมาย องค์ประกอบและแบบวัดที่สอดคล้องกับงานวิจัยนี้ ดังนี้

คุณลักษณะของระบบ (System Characteristics) เป็นการรับรู้และความคิดเห็นของบุคคลต่อคุณสมบัติ การประมวลผล การนำเสนอและรูปแบบการใช้งานของโปรแกรมคอมพิวเตอร์หรือแอพพลิเคชันในภาพรวมต่อการทำความเข้าใจในการปกป้องข้อมูลส่วนบุคคลจากการเข้าใช้งานธุรกรรมทางอิเล็กทรอนิกส์ การมีปฏิสัมพันธ์โต้ตอบที่ดีระหว่างระบบกับผู้ใช้งานที่ส่งผลถึงประโยชน์และการรับรู้ถึงความง่ายต่อการทำความเข้าใจในการปกป้องข้อมูลส่วนบุคคลจากการเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ สำหรับงานวิจัยนี้ผู้วิจัยพัฒนาและปรับปรุงจากแบบวัดของ Venkatesh & Davis (1996) จำนวน 6 ข้อ จำแนกเป็น 2 องค์ประกอบได้แก่ คุณลักษณะเฉพาะของโปรแกรม (Features) และส่วนติดต่อกับผู้ใช้งาน (User interface) ที่น่าสนใจในการปกป้องข้อมูลส่วนบุคคล โดยให้เป็นไปตามขอบเขตเนื้อหาและนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ตามลำดับ ส่วนข้อความทางลบเป็นการให้คะแนนในทางตรงกันข้าม

การคล้อยตามกลุ่มอ้างอิง (Subjective Norms) เป็นระดับความเชื่อ การรับรู้ของบุคคลที่มีต่อความคิดเห็นกลุ่มบุคคลรอบข้างที่ตนยอมรับและมีความสำคัญเกี่ยวกับความคิดเห็นถึงประโยชน์และความสำคัญจากการตั้งค่าในการปกป้องข้อมูลส่วนบุคคลผ่านเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ สำหรับงานวิจัยนี้เป็นการศึกษาพฤติกรรมการตัดสินใจและเหตุผลของแต่ละบุคคล ดังนั้นจึงเลือกศึกษาเฉพาะกระบวนการของอิทธิพลทางสังคม (Social Influence process) เกี่ยวกับตัวแปรการคล้อยตามกลุ่มอ้างอิง เช่น เพื่อนร่วมงาน ครอบครัว ผู้เชี่ยวชาญและมีอิทธิพลทางเทคโนโลยีบนสื่อสังคมออนไลน์ (IT Bloggers/Influencers) ที่อธิบายเกี่ยวกับความสำคัญและประโยชน์จากการตั้งค่าในการปกป้องข้อมูลส่วนบุคคล สำหรับงานวิจัยนี้ ผู้วิจัยสร้างและปรับปรุงแบบวัดโดยใช้แนวคิดของ Fishbein & Ajzen (1975: 73-76) จำนวน 6 ข้อ จำแนกเป็น 2 องค์ประกอบได้แก่ การคล้อยตามกลุ่มบุคคลรอบข้างที่ใกล้ชิด และการคล้อยตามผู้ทรงอิทธิพลทางเทคโนโลยีบนสื่อสังคมออนไลน์ในการปกป้องข้อมูลส่วนบุคคล โดยให้เป็นไปตามขอบเขตเนื้อหาและนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ตามลำดับ ส่วนข้อความทางลบเป็นการให้คะแนนในทางตรงกันข้าม

การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล (Perceived Usefulness) เป็นระดับความเชื่อ การรับรู้ของบุคคล ที่ผู้ใช้งานสามารถรับรู้ถึงประโยชน์ ข้อดีของการตั้งค่าในการปกป้องข้อมูลส่วนบุคคลจากการเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ ว่ามีประโยชน์อย่างมากในการปกป้องข้อมูลส่วนบุคคลให้มีความปลอดภัยและมีประสิทธิภาพเพื่อการใช้งาน ซึ่งจะส่งผลต่อทัศนคติที่ดีต่อการปกป้องข้อมูลส่วนบุคคล สำหรับงานวิจัยนี้ ผู้วิจัยพัฒนาและปรับปรุงจากแบบวัดของ Davis et al. (1989: 982-1003) จำนวน 8 ข้อ จำแนกเป็น 2 องค์ประกอบได้แก่ การก่อให้เกิดประโยชน์ต่อตนเอง (Useful) และการเพิ่มประสิทธิผล (Increase Productivity) ในความปลอดภัยของข้อมูลส่วนบุคคล โดยให้เป็นไปตามขอบเขตเนื้อหาและนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ตามลำดับ ส่วนข้อความทางลบเป็นการให้คะแนนในทางตรงกันข้าม

การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล (Perceived Ease of Use) เป็นระดับที่ผู้ใช้งานเชื่อว่าไม่ต้องอาศัยความพยายามมากนักต่อการทำความเข้าใจ ขั้นตอนทางด้านการเรียนรู้วิธีการปกป้องข้อมูลส่วนบุคคลให้มีความปลอดภัยบนเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ เป็นเรื่องง่าย สะดวก ไม่ซับซ้อนและสามารถเข้าใจง่ายอย่างรวดเร็ว และส่งผลต่อทัศนคติที่ดีต่อการปกป้องข้อมูลส่วนบุคคล สำหรับงานวิจัยนี้ผู้วิจัยพัฒนาและปรับปรุงจากแบบวัดของ Davis et al. (1989: 982-1003) จำนวน 6 ข้อ จำแนกเป็น 2 องค์ประกอบได้แก่ ความง่ายต่อการเรียนรู้ (Easy to Learn) และความไม่ซับซ้อนของระบบ (Simplicity) ในวิธีการและขั้นตอนของการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล โดยให้เป็นไปตามขอบเขตเนื้อหาและนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ตามลำดับ ส่วนข้อความทางลบเป็นการให้คะแนนในทางตรงกันข้าม

2.4.7 ทัศนคติที่มีต่อการปกป้องข้อมูลส่วนตัวบนธุรกรรมทางอิเล็กทรอนิกส์ (Attitude)

ความหมาย

ทัศนคติ เป็นความเชื่อของบุคคลเกี่ยวกับผลที่ตามมาจากการกระทำ (Behavioral Beliefs) โดยเป็นการประเมินของบุคคล ซึ่งอาจเป็นไปได้ทั้งทางบวกและทางลบทางด้านความรู้สึก หรือเป็นไปในทิศทางที่พอใจหรือไม่พอใจก็ได้ต่อการกระทำนั้นๆ (Ajzen, 1991) ซึ่งเป็นปัจจัยส่วนบุคคลและเป็นหนึ่งในปัจจัยที่มีอิทธิพลต่อความตั้งใจที่จะแสดงพฤติกรรมนั้น หากบุคคลทราบว่าได้กระทำพฤติกรรมใดแล้วที่ได้รับผลเชิงบวก จะทำให้เกิดทัศนคติที่ดีต่อการกระทำพฤติกรรมนั้น ในมุมมองความเชื่อด้านข้อมูล สารสนเทศ พบว่าในงานวิจัย Bulgurcu et al., (2010) ทัศนคติจะหมายถึงการประเมินของบุคคลที่มีต่อประสิทธิภาพในปฏิบัติตามด้านความปลอดภัยของข้อมูล และหากมีทัศนคติที่ดีหรือทางบวกจะทำให้บุคคลนั้นเกิดความตั้งใจที่จะกระทำหรือปฏิบัติตามในการปกป้องข้อมูล และงานวิจัยของ Büchi et al., (2016) จะหมายถึงบุคคลที่พิจารณาเห็นถึงความสำคัญในการปกป้องความเป็นส่วนตัวจากการใช้งานอินเทอร์เน็ตและเป็นทัศนคติที่เกี่ยวข้องกับความเป็นส่วนตัว (Privacy attitude)

สำหรับงานวิจัยนี้ ได้ให้ความหมายของทัศนคติในการปกป้องข้อมูลส่วนตัวบนธุรกรรมทางอิเล็กทรอนิกส์ หมายถึงความเชื่อ ความคิดเห็น สภาพความคิด ความเข้าใจและความรู้สึกเชิงประเมินที่มีต่อการปฏิบัติตนตามวิธีการ และขั้นตอนการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลเมื่อเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ ของแต่ละบุคคลในการปฏิบัติตนตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

การวัดทัศนคติในการปกป้องข้อมูลส่วนตัวบนธุรกรรมทางอิเล็กทรอนิกส์

จากการค้นคว้าและศึกษางานวิจัยที่เกี่ยวข้องกับแบบวัดทัศนคติ พบว่าในงานวิจัยของ Woon & Kankanhalli (2007) ที่ศึกษาเกี่ยวกับความตั้งใจของผู้เชี่ยวชาญด้านระบบสารสนเทศในการฝึกปฏิบัติตนด้านความปลอดภัยจากการพัฒนาแอปพลิเคชัน ซึ่งเป็นแบบวัดด้านทัศนคติเกี่ยวกับความคิดเห็นในการปฏิบัติตนที่ปลอดภัยจากการพัฒนาแอปพลิเคชัน จำนวน 5 ข้อ มีลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 5 ระดับจาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง” ซึ่งมีลักษณะเช่นเดียวกับงานวิจัยของ Bulgurcu et al., (2010) ที่ศึกษาแบบวัดเกี่ยวกับทัศนคติในการปฏิบัติตนตามนโยบายด้านความปลอดภัยของข้อมูล จำนวน 4 ข้อ มีลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 7 ระดับ จาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง”

สำหรับงานวิจัยเรื่องนี้ ผู้วิจัยใช้แบบวัดซึ่งพัฒนาและปรับปรุงจากแบบวัดของ Woon & Kankanhalli (2007) และ Bulgurcu et al., (2010) จำนวน 5 ข้อ โดยให้เป็นไปตามขอบเขตเนื้อหาและนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ตามลำดับ ส่วนข้อความทางลบเป็นการให้คะแนนในทางตรงกันข้าม

งานวิจัยที่เกี่ยวข้อง

งานวิจัยของ Ifinedo (2012) พบว่าปัจจัยด้านทัศนคติ เกี่ยวกับเหตุผลความจำเป็น ผลประโยชน์และการเป็นแนวคิดที่ดีส่งผลต่อความตั้งใจในการปฏิบัติตนตามนโยบายความปลอดภัยด้านสารสนเทศ เช่นเดียวกับงานวิจัยของ Herath & Rao (2009) และ Bulgurcu et al., (2010) ที่พบว่าปัจจัยด้านทัศนคติส่งผลการปฏิบัติตามนโยบายด้านความปลอดภัยของข้อมูล รวมทั้งในงานวิจัยของ Woon & Kankanhalli (2007) พบว่าปัจจัยด้านทัศนคติส่งผลทางบวกต่อความตั้งใจในการฝึกปฏิบัติตนด้านความปลอดภัยของผู้เชี่ยวชาญระบบสารสนเทศ

ดังนั้น จากการทบทวนเอกสารและงานวิจัยที่เกี่ยวข้อง ผู้วิจัยจึงคาดว่าทัศนคติในการปกป้องข้อมูลส่วนตัวบนธุรกรรมทางอิเล็กทรอนิกส์ มีอิทธิพลทางตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ และมีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

2.4.8 **ความตั้งใจในการปกป้องข้อมูลส่วนบุคคล** (Intention to protect personal information)

ความหมาย

ในงานวิจัยของ Foltz et al., (2016) กล่าวว่าความตั้งใจหมายถึง จำนวนของความพยายาม (Amount of effort) ในแต่ละบุคคลซึ่งเป็นความมุ่งหมายเพื่อนำไปสู่การเปลี่ยนแปลงและการแสดงพฤติกรรมตามที่กำหนดไว้ รวมทั้งในงานวิจัยของ Bulgurcu et al., (2010) และ Ho et al., (2017) เป็นกล่าวถึงความตั้งใจที่จะปฏิบัติตาม (Intention to comply) ว่าเป็นความมุ่งมั่นและการวางแผนที่จะมีส่วนร่วมในพฤติกรรมการปกป้องความเป็นส่วนตัว ซึ่งในงานวิจัยนี้ความตั้งใจในการปกป้องข้อมูลส่วนบุคคลจะหมายถึง เจตนาการแสดงออก ความพยายาม ความมุ่งมั่น ความพร้อม และความยินดีที่จะปฏิบัติตนในการจัดการตั้งค่าข้อมูลส่วนบุคคล

การวัดความตั้งใจในการปกป้องข้อมูลส่วนบุคคล

ในการรวบรวมเอกสารและงานวิจัยที่เกี่ยวข้องกับแบบวัดความตั้งใจเกี่ยวกับการปกป้องความเป็นส่วนตัวและความปลอดภัยทางด้านข้อมูล พบว่างานวิจัยของ Bulgurcu et al., (2010) ได้ทำแบบวัดความตั้งใจที่จะปฏิบัติตามนโยบายด้านความปลอดภัยของข้อมูล จำนวน 3 ข้อ มีลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 5 ระดับจาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง” ในงานวิจัยของ Foltz et al., (2016) จากการศึกษาปัจจัยที่ส่งผลต่อพฤติกรรมของบุคคลต่อการเปลี่ยนแปลงในการตั้งค่าเพื่อความปลอดภัยในเครือข่ายสังคมออนไลน์ ได้จัดแบบวัดความตั้งใจเชิงพฤติกรรม (Behavioral Intention) จำนวน 4 ข้อ มีลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 5 ระดับจาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง” สำหรับงานวิจัยของ Woon & Kankanhalli (2007) พบแบบวัดความตั้งใจเชิงพฤติกรรมในการฝึกปฏิบัติตนด้านความปลอดภัยจากการพัฒนาแอปพลิเคชัน จำนวน 2 ข้อ มีลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 5 ระดับจาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง” และงานวิจัยของ Ifinedo (2012) ได้สร้างแบบวัดความตั้งใจเชิงพฤติกรรมที่จะปฏิบัติตามนโยบายด้านความปลอดภัยของข้อมูลในองค์กร จำนวน 6 ข้อ ลักษณะของแบบวัดเป็นมาตราวัดประเมินค่า 7 ระดับจาก “เห็นด้วยอย่างยิ่ง” ถึง “ไม่เห็นด้วยอย่างยิ่ง”

สำหรับงานวิจัยเรื่องนี้ ผู้วิจัยใช้แบบวัดซึ่งพัฒนาและปรับปรุงจากแบบวัดของ Bulgurcu et al., (2010) และ Foltz et al., (2016) จำนวน 5 ข้อ โดยให้เป็นไปตามขอบเขตเนื้อหาและนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ตามลำดับ ส่วนข้อความทางลบเป็นการให้คะแนนในทางตรงกันข้าม

งานวิจัยที่เกี่ยวข้อง

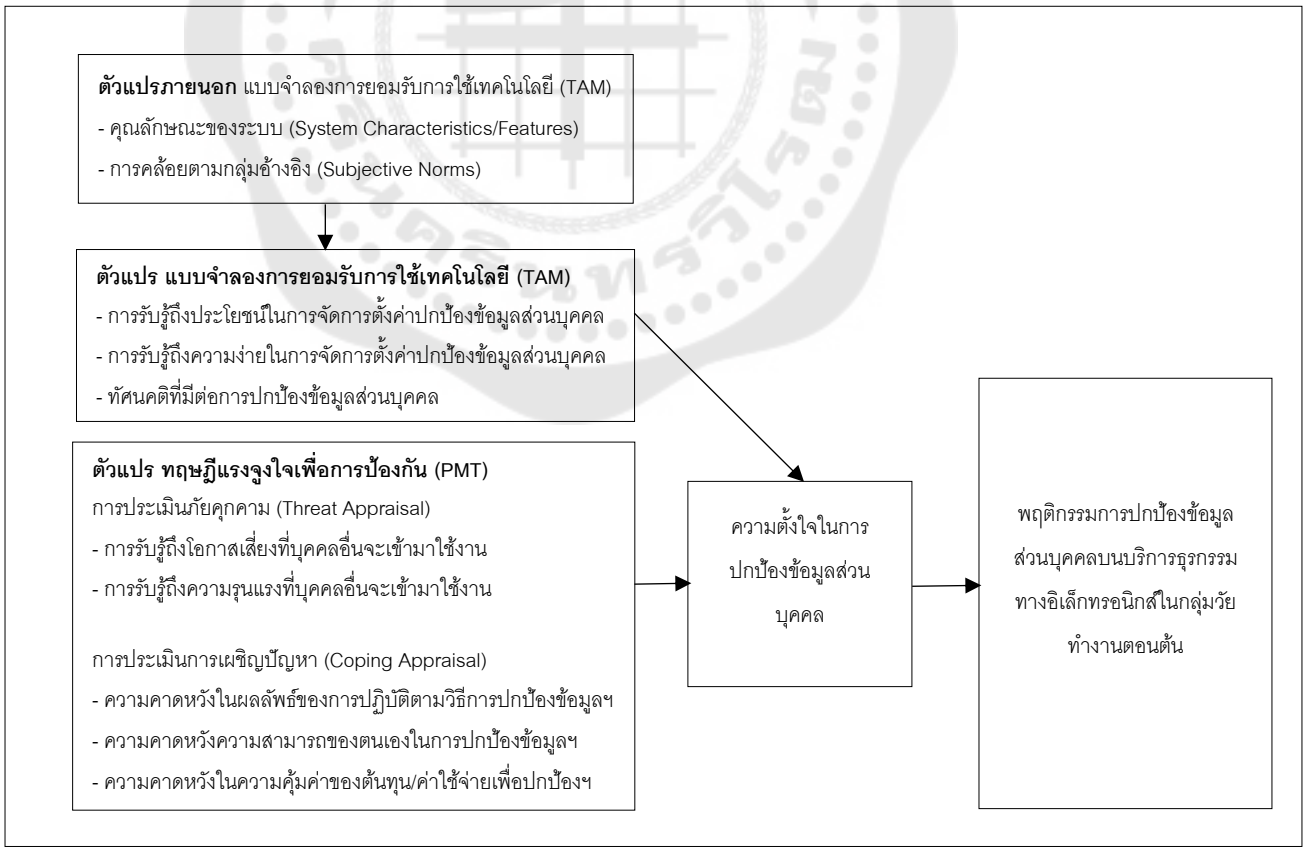
จากการศึกษางานวิจัยของ Yao & Linz (2008) พบว่าความตั้งใจของแต่ละบุคคลที่จะใช้กลยุทธ์หรือเทคนิควิธี (Intention to adopt strategies) ในการปกป้องความเป็นส่วนตัวซึ่งเป็นปัจจัยที่มีอิทธิพลในการปรับพฤติกรรมการใช้กลยุทธ์เพื่อการปกป้องความเป็นส่วนตัว (Adoption of online privacy protections) เช่นเดียวกับงานวิจัยของ Yoon et al., (2019) พบว่าความตั้งใจเชิงพฤติกรรมเกี่ยวกับการระมัดระวังตนและความกระตือรือร้น (Actively) ต่อการละเมิดข้อมูลส่วนบุคคล ส่งผลต่อพฤติกรรมด้านความปลอดภัยของข้อมูล ในงานวิจัยของ Srisawang et al., (2015) และ Ho et al., (2017) พบว่าความพยายามและความตั้งใจในการวางแผนอย่างมีส่วนร่วมที่จะปฏิบัติตามคำแนะนำ เป็นปัจจัยที่สำคัญต่อพฤติกรรมการปกป้องความเป็นส่วนตัว และงานวิจัยของ Foltz et al., (2016) พบว่าความตั้งใจเชิงพฤติกรรมที่อิทธิพลทางบวกต่อการเปลี่ยนแปลงในการตั้งค่าเพื่อความปลอดภัยในเครือข่ายสังคมออนไลน์

ดังนั้น จากการทบทวนเอกสารและงานวิจัยที่เกี่ยวข้อง ผู้วิจัยจึงคาดว่าความตั้งใจในการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางตรงต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

3. กรอบแนวคิดการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงปริมาณ เพื่อทดสอบและพัฒนารูปแบบความสัมพันธ์เชิงสาเหตุที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น จากการให้ข้อมูลส่วนบุคคลและเพื่อการใช้งานธุรกรรมทางอิเล็กทรอนิกส์อย่างระมัดระวัง จากการประมวลเอกสารและสังเคราะห์งานวิจัยที่เกี่ยวข้อง ผู้วิจัยประยุกต์ใช้กรอบทฤษฎีแรงจูงใจเพื่อการป้องกัน (Protection Motivation Theory: PMT) ของ Rogers (1983) ซึ่งให้ความสำคัญกับแรงจูงใจในการพัฒนาตัวแปรทางจิตด้านการรับรู้ที่สามารถนำไปประยุกต์ใช้ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งประกอบด้วย ตัวแปรสาเหตุทางจิต

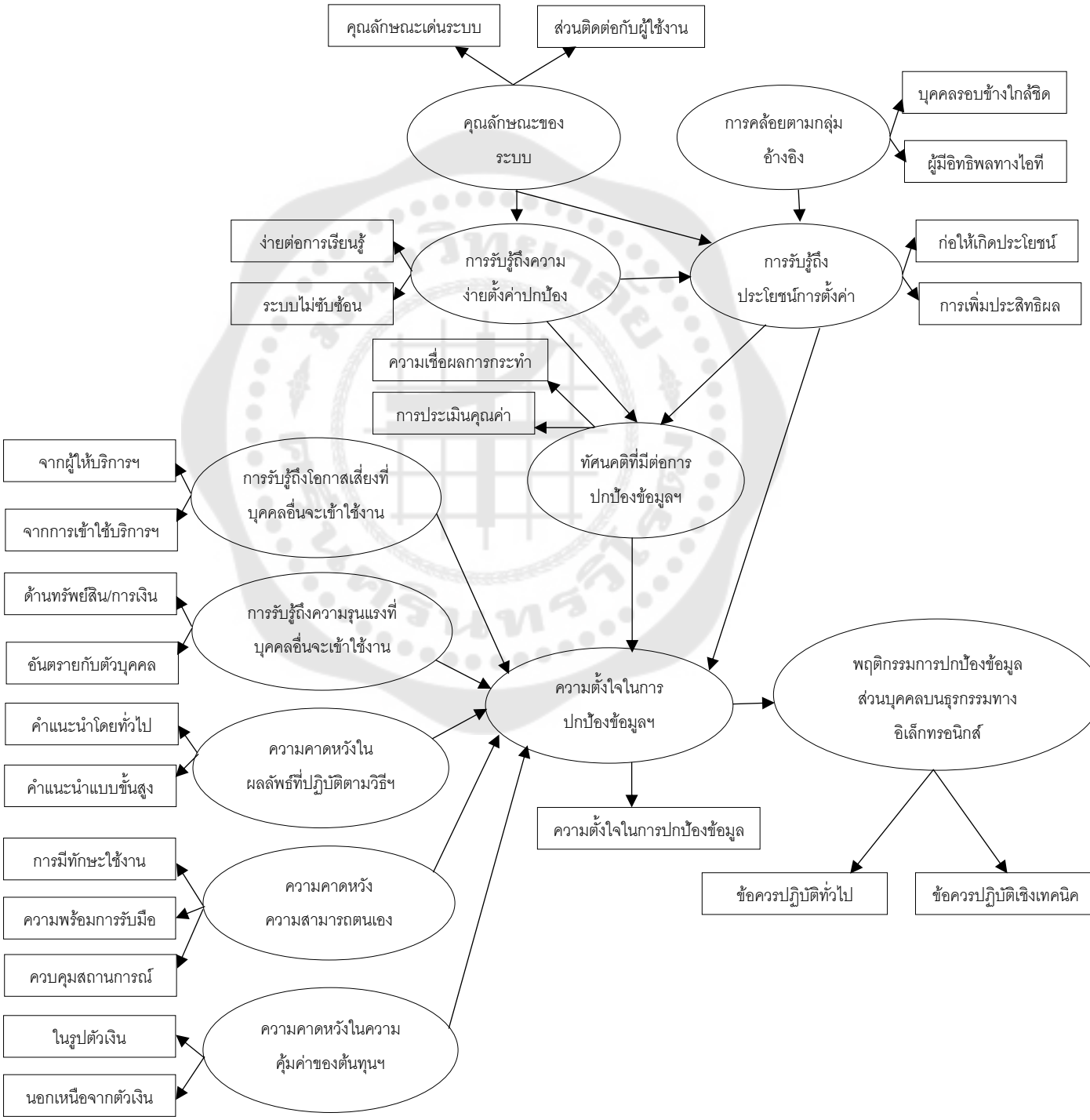
ได้แก่ การรับรู้ถึงโอกาสเสี่ยง การรับรู้ถึงความรุนแรง ความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล และความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อการปกป้องข้อมูลส่วนบุคคล รวมทั้งการศึกษาเพิ่มเติมแนวคิดและทฤษฎีที่นอกเหนือจากกรอบทฤษฎีแรงจูงใจเพื่อการป้องกัน เพื่อให้สามารถอธิบายพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ได้สมบูรณ์ยิ่งขึ้น ได้แก่ แบบจำลองการยอมรับการใช้เทคโนโลยี (Technology Acceptance Model: TAM) (Davis et al., 1989) ซึ่งพัฒนามาจากทฤษฎีการกระทำด้วยเหตุผล (Theory of Reasoned Action) (Fishbein & Ajzen, 1975) เป็นแนวคิดเกี่ยวกับการรับรู้ถึงประโยชน์จากการใช้งานและการใช้งานง่าย ส่งผลต่อทัศนคติ ความตั้งใจและพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วยตัวแปรทางสังคมได้แก่ การคล้อยตามกลุ่มอ้างอิง และตัวแปรสาเหตุทางจิต ได้แก่ คุณลักษณะของระบบ การรับรู้ถึงประโยชน์ในการตั้งค่าการปกป้องข้อมูลส่วนบุคคลและการรับรู้ถึงความง่ายในการทำความเข้าใจเพื่อการปกป้องข้อมูลส่วนบุคคล ดังภาพประกอบ 5



ภาพประกอบ 5 กรอบแนวคิดในการวิจัย

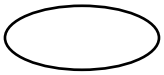
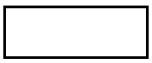
4. แบบจำลองและสมมติฐานการวิจัย

จากกรอบแนวคิดในการวิจัย ผู้วิจัยได้พัฒนาแบบจำลองสมมติฐานการวิจัยซึ่งเป็นรูปแบบความสัมพันธ์โครงสร้างเชิงเส้นของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น ดังภาพประกอบ 6



ภาพประกอบ 6 รูปแบบความสัมพันธ์โครงสร้างเชิงเส้นของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ จากการทบทวนเอกสารและงานวิจัยที่เกี่ยวข้อง

คำอธิบายสัญลักษณ์ที่ใช้ในรูปแบบความสัมพันธ์โครงสร้างเชิงเส้นตามสมมติฐานการวิจัย

สัญลักษณ์	คำอธิบาย
	วงกลมหรือวงรี แทนตัวแปรแฝง (Latent Variables)
	สี่เหลี่ยม แทนตัวแปรสังเกต (Observed Variables)
	ลูกศร แทนความสัมพันธ์เชิงเหตุระหว่างตัวแปรอิสระกับตัวแปรตาม และหัวลูกศรแสดงทิศทางของอิทธิพล (Direct Effect)
	แทนตัวแปรแฝง A เป็นสาเหตุ (Cause) ของตัวแปรแฝง B (Effect)
	แทนตัวแปรสังเกต B (Effect) ของตัวแปรแฝง A (Cause)

สมมติฐานการวิจัย

จากแบบจำลองสมมติฐานการวิจัยเรื่องนี้ ผู้วิจัยมีสมมติฐานการวิจัยว่ารูปแบบความสัมพันธ์โครงสร้างเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น จะมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ซึ่งได้กำหนดสมมติฐานการวิจัยย่อย (Hypotheses) ดังนี้

1. การรับรู้ถึงโอกาสเสี่ยง มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล (H1)

2. การรับรู้ถึงความรุนแรง มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล (H2)

3. ความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล (H3)

4. ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล (H4)

5. ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล (H5)

6. คุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล (H6) และการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (H7)

7. การคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (H8)

8. การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคล (H9) และความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น (H10)

9. การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล (H11) และทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคล (H12)

10. ทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล (H13)

11. ความตั้งใจในการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น (H14)

5. นิยามปฏิบัติการตัวแปร

พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ หมายถึง การระมัดระวังตนเพื่อรักษาความเป็นส่วนตัว การควบคุมเปิดเผยข้อมูลส่วนบุคคลและการจัดการตั้งค่าข้อมูลส่วนบุคคลให้มีความปลอดภัยด้วยตนเองจากอันตรายที่อาจเกิดขึ้นจากการให้ข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในฐานะที่เป็นกลุ่มผู้บริโภคหรือผู้ใช้บริการเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งผู้วิจัยนำองค์ประกอบของพฤติกรรมการปกป้องความเป็นส่วนตัวจากการใช้งานเครือข่ายอินเทอร์เน็ตและการพาณิชย์อิเล็กทรอนิกส์ของ Buchanan et al. (2007) มาปรับใช้ในงานวิจัยนี้ สามารถแบ่งแนวทางการศึกษาพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์เป็น 2 องค์ประกอบคือ องค์ประกอบที่ 1 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป (General Caution) และองค์ประกอบที่ 2 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค (Technical Protection)

องค์ประกอบที่ 1 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป หมายถึง การรายงานของกลุ่มวัยทำงานตอนต้นเกี่ยวกับการปฏิบัติตนเพื่อหลีกเลี่ยงที่อาจก่อให้เกิดความเสียหายจากการถูกโจรกรรมข้อมูลส่วนบุคคลและการปกป้องข้อมูลทางการเงินจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่มีการระบุตัวตนของผู้ใช้บริการ โดยอาศัยความเข้าใจเรื่องการเก็บรักษาความลับข้อมูลส่วนบุคคลทางการเงินและความเป็นส่วนบุคคลต่อการดำเนินชีวิตยุคดิจิทัลในสังคมไทย ที่ไม่จำเป็นต้องอาศัยความรู้ทางด้านการใช้งานเทคโนโลยีสารสนเทศมากนัก

พิจารณาจากการกระทำเพื่อการปกป้องข้อมูลส่วนบุคคลด้านข้อมูลและสารสนเทศ จากการปฏิบัติตนตามมาตรการขั้นพื้นฐานในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ เช่น การกำหนดหรือตั้งค่ารหัสผ่าน (Password) การเก็บรักษารหัสผ่านและข้อมูลส่วนบุคคล การศึกษาเงื่อนไขนโยบายคุ้มครองความเป็นส่วนตัว (Privacy Policy) ของผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ การตั้งค่าจำกัดวงเงิน การตรวจสอบการทำรายการธุรกรรมทางอิเล็กทรอนิกส์ย้อนหลัง เป็นต้น รวมไปถึงการควบคุมข้อมูลส่วนบุคคลและการเลือกเปิดเผยเฉพาะข้อมูลส่วนบุคคลที่มีความจำเป็นต่อการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ การกำหนดสิทธิ์ในเข้าถึงข้อมูลส่วนบุคคล การเลือกเข้าร่วมกิจกรรมส่งเสริมการขายและการตลาด (Opt-out) การไม่เข้าร่วมกิจกรรมประเภทเกมตอบคำถามชิงรางวัล (Quiz with

Prizes) การทดสอบเกม (Quiz Games) และเกมทายใจจากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่อาจก่อให้เกิดการให้ข้อมูลส่วนบุคคล

องค์ประกอบที่ 2 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค หมายถึง การรายงานของกลุ่มวัยทำงานตอนต้นเกี่ยวกับการปฏิบัติตนเพื่อหลีกเลี่ยงที่อาจก่อให้เกิดความเสียหายจากการถูกโจรกรรมข้อมูลส่วนบุคคลและการปกป้องข้อมูลทางการเงินจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่มีการระบุตัวตนของผู้ใช้บริการ โดยอาศัยทักษะความรู้และความเข้าใจเรื่องการเก็บรักษาความลับข้อมูลส่วนบุคคลทางการเงินและความเป็นส่วนบุคคลต่อการดำเนินชีวิตยุคดิจิทัลในสังคมไทย จากการยอมรับการใช้งานเครื่องคอมพิวเตอร์ความชำนาญในการใช้งานเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

พิจารณาจากการใช้เทคโนโลยีด้านฮาร์ดแวร์ (Hardware Technology) ซึ่งเป็นอุปกรณ์ทางอิเล็กทรอนิกส์หรือเครื่องคอมพิวเตอร์ชนิดต่างๆ ที่สามารถมองเห็นและสัมผัสได้ ประกอบด้วยเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา (Laptop) เครื่องคอมพิวเตอร์แบบรับข้อมูลด้วยการเขียนบนจอภาพ (Tablet) และสมาร์ทโฟน (Smart Phone) และการใช้งานด้านซอฟต์แวร์ (Software) สำหรับดำเนินงานขั้นพื้นฐานของระบบในเครื่องคอมพิวเตอร์ ประกอบด้วยซอฟต์แวร์ระบบ (System Software) ซึ่งเป็นระบบปฏิบัติการ (Operating System) ตัวแปลภาษาคอมพิวเตอร์และโปรแกรมที่ช่วยเพิ่มประสิทธิภาพให้กับระบบปฏิบัติการ (Utility Programs) และซอฟต์แวร์ประยุกต์ (Application Software) เป็นโปรแกรมคอมพิวเตอร์ซึ่งถูกพัฒนาขึ้นตามวัตถุประสงค์ในการใช้งาน โดยเป็นโปรแกรมสำเร็จรูปหรือแอปพลิเคชันที่ได้ถูกพัฒนาขึ้นสำหรับงานธุรกรรมทางการเงิน ซึ่งผู้ใช้บริการสามารถเลือกโปรแกรมหรือแอปพลิเคชันเหล่านั้นมาใช้ร่วมกับการจัดการข้อมูลทางการเงินส่วนบุคคลได้ด้วยตนเอง รวมไปถึงด้านระบบเครือข่ายคอมพิวเตอร์ (Network Systems) เป็นการใช้งานผ่านเครือข่ายอินเทอร์เน็ตและการใช้ทรัพยากรร่วมกันในธุรกรรมทางอิเล็กทรอนิกส์ จากการนำอุปกรณ์คอมพิวเตอร์มาเชื่อมต่อกันเพื่อให้ผู้ใช้บริการในเครือข่ายสามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและใช้คอมพิวเตอร์ในเครือข่ายร่วมกันได้ โดยการใช้งานผ่านโปรแกรมหรือแอปพลิเคชันที่ได้ถูกพัฒนาขึ้น

ผู้วิจัยได้ศึกษาแนวทางและพัฒนาจากแบบวัดพฤติกรรมการปกป้องความเป็นส่วนตัวจากการใช้งานเครือข่ายอินเทอร์เน็ตและการพาณิชย์อิเล็กทรอนิกส์ที่เกี่ยวข้อง (Buchanan et al., 2007; Son & Kim ,2008; Youn, 2009; Büchi et al., 2016; Boerman et al., 2018) รวมไปถึงหนังสือคู่มือเกี่ยวกับการทำธุรกรรมออนไลน์ให้ปลอดภัยและสร้างสรรค์ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ องค์การมหาชน, 2560) และเอกสารการใช้ธนาคารออนไลน์ให้ปลอดภัยบน

สมาร์ทโฟน (ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย, 2561) มาเป็นหลักในการวัดและพัฒนาเครื่องมือ โดยนำมาปรับใช้เป็นแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้มีความสอดคล้องและเหมาะสมในบริบทสังคมไทยและกลุ่มตัวอย่างที่เป็นกลุ่มวัยทำงานตอนต้น ตามขอบเขตเนื้อหาและนิยามปฏิบัติการของตัวแปรนี้ เป็นคำถามปลายปิด สอบถามพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ที่ให้กลุ่มตัวอย่างแสดงความคิดเห็นที่ตรงกับสภาพความเป็นจริงมากที่สุดเพียงข้อเดียว ซึ่งเป็นแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป และการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค

การรับรู้ถึงโอกาสเสี่ยง (Perceived Vulnerability) **บนธุรกรรมทางอิเล็กทรอนิกส์** หมายถึง การรับรู้ของกลุ่มวัยทำงานตอนต้นถึงความไม่ปลอดภัยของข้อมูลและความเป็นไปได้ว่าเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ที่ใช้บริการนั้น มีข้อบกพร่องในการใช้งานหรือมีจุดอ่อนของระบบในการปกป้องข้อมูลส่วนบุคคล ซึ่งเป็นข้อบกพร่องที่อาจมาจากขั้นตอนการออกแบบระบบ ข้อผิดพลาดจากการเขียนโปรแกรม ระบบคอมพิวเตอร์ของผู้ให้บริการ เป็นต้น รวมไปถึงการไม่ปฏิบัติตนตามการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ทำให้ระบบอนุญาตให้บุคคลอื่น ซึ่งอาจเป็นผู้ไม่หวังดีหรือหน่วยงานภายนอกสามารถเข้ามาใช้งานแทนหรือบุกรุกความเป็นส่วนตัว การถูกละเมิดโดยการนำเอาข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาต แบ่งองค์ประกอบการรับรู้ถึงโอกาสเสี่ยงที่บุคคลอื่นจะเข้าใช้งานแทนตน เป็นจำนวน 2 ด้าน ได้แก่ การรับรู้โอกาสเสี่ยงที่อาจมาจากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์และการรับรู้โอกาสเสี่ยงจากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์

การรับรู้โอกาสเสี่ยงที่อาจมาจากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ หมายถึง ปริมาณการรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับความวิตกกังวล ความไม่สบายใจ ความไม่ปลอดภัยของข้อมูลและความเป็นไปได้ถึงข้อบกพร่องของโปรแกรมที่ใช้งานธุรกรรมทางอิเล็กทรอนิกส์และหน่วยงานของผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ทั้งกิจการภาครัฐและเอกชน การที่หน่วยงาน

ของผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์สามารถเข้าถึงข้อมูลส่วนบุคคล ซึ่งทำให้เกิดโอกาสในการละเมิดหรือลักลอบนำข้อมูลส่วนบุคคลของผู้ใช้บริการไปใช้งานโดยไม่ได้รับอนุญาตหรือการยินยอม การทำให้ข้อมูลส่วนบุคคลที่มีความสำคัญรั่วไหล ถูกเปิดเผยและถูกส่งต่อข้อมูลไปยังบุคคลที่สามหรือหน่วยงานภายนอก รวมไปถึงการนำข้อมูลส่วนบุคคลของผู้ใช้บริการไปใช้งานในทางที่ไม่ถูกต้อง

การรับรู้โอกาสเสี่ยงจากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ หมายถึงปริมาณการรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่มีความไม่ปลอดภัยของข้อมูล และการที่ไม่ปฏิบัติตนตามการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งอาจก่อให้เกิดความเสียหายและอันตรายต่อเจ้าของข้อมูลหรือผู้ใช้บริการ และอาจทำให้บุคคลอื่นสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน

ผู้วิจัยได้ศึกษาจากแบบวัดการรับรู้ถึงโอกาสจากการถูกคุกคามความเป็นส่วนตัวออนไลน์ของ Dinev & Hart (2006); Moloney & Poti (2013); Boerman et al., (2018) และ Klein & Luciano (2016) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดการรับรู้ถึงโอกาสเสี่ยงที่บุคคลอื่นจะเข้าใช้งานแทนตนบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีการรับรู้ถึงโอกาสเสี่ยงที่บุคคลอื่นจะเข้าใช้งานแทนตนบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็น การรับรู้โอกาสเสี่ยงที่อาจมาจากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ และการรับรู้โอกาสเสี่ยงจากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์

การรับรู้ถึงความรุนแรง (Perceived Severity) **บนธุรกรรมทางอิเล็กทรอนิกส์** หมายถึง การรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับข้อมูล ข่าวสารที่เกิดขึ้น ถึงความเป็นไปได้ว่าเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ที่ใช้บริการนั้น มีข้อบกพร่องในการใช้งานหรือมีจุดอ่อนของระบบในการปกป้องข้อมูลส่วนบุคคล ส่งผลทำให้ระบบอนุญาตให้บุคคลอื่นซึ่งอาจเป็นผู้ไม่หวังดีหรือหน่วยงานภายนอกสามารถเข้ามาใช้งานแทนตนและการบุกรุกความเป็น

ส่วนตัว รวมไปถึงการไม่ปฏิบัติตนตามการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งอาจก่อให้เกิดความเสียหายและอันตรายต่อเจ้าของข้อมูลโดยการนำเอาข้อมูลส่วนบุคคลไปใช้ เช่น จำนวนเงินออมในบัญชีธนาคารที่สูญเสียไปจากการถูกโจรกรรมข้อมูลทางการเงิน รูปแบบการดำเนินชีวิตจากการถูกทำร้ายด้านร่างกายและสุขภาพ การไม่สามารถเข้าใช้งานธุรกรรมทางอิเล็กทรอนิกส์ต่อไปได้ ความสับสนและยุ่งยากในการใช้งานธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น แบ่งการศึกษาองค์ประกอบการรับรู้ถึงความรุนแรงที่บุคคลอื่นจะเข้าใช้งานแทนตน จำนวน 2 ด้าน ได้แก่ การรับรู้ถึงความรุนแรงด้านทรัพย์สิน และการรับรู้ถึงความรุนแรงด้านอันตรายที่อาจเกิดขึ้นกับตัวบุคคล

การรับรู้ถึงความรุนแรงด้านทรัพย์สิน หมายถึง ปริมาณการรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับความเป็นไปได้ถึงข้อบกพร่องของโปรแกรมที่ใช้งานธุรกรรมทางอิเล็กทรอนิกส์และการไม่ปฏิบัติตนตามการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งอาจทำให้บุคคลอื่นหรือหน่วยงานภายนอกสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน ส่งผลทำให้ข้อมูลทางการเงินออนไลน์มีการเปลี่ยนแปลงข้อมูลและตัวเลข ทำให้บุคคลอื่นทราบถึงรูปแบบการดำเนินชีวิตทางการเงิน สถานะทางการเงินและทรัพย์สิน ที่อาจก่อให้เกิดการปลอมแปลงเป็นเจ้าของข้อมูล การหลอกลวงให้บุคคลรอบข้างที่ใกล้ชิด สนิทสนมโอนเงินเข้ามาให้ และการถูกขโมยทรัพย์สินที่มีค่าที่จำเป็นต่อการดำรงชีวิตประจำวันและการทำงาน เช่น เงินออมในบัญชีธนาคาร สมาร์ทโฟน อุปกรณ์คอมพิวเตอร์ บัตรอิเล็กทรอนิกส์ต่างๆ เป็นต้น

การรับรู้ถึงความรุนแรงด้านอันตรายที่อาจเกิดขึ้นกับตัวบุคคล หมายถึง ปริมาณการรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับความเป็นไปได้ถึงข้อบกพร่องของโปรแกรมที่ใช้งานธุรกรรมทางอิเล็กทรอนิกส์ และการไม่ปฏิบัติตนตามการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งอาจทำให้บุคคลอื่นสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน ส่งผลทำให้บุคคลอื่นทราบถึงข้อมูลที่อยู่และสถานที่ทำงาน ที่อาจก่อให้เกิดการบุกรุกความเป็นส่วนตัว การสะกดรอยตาม การถูกทำร้ายด้านร่างกาย การเจ็บป่วย ประสบอันตรายจนถึงขั้นทุพพลภาพและมีโอกาสเสียชีวิตจากการปกป้องการถูกขโมยทรัพย์สินที่มีค่า รวมไปถึงข้อมูลทางสุขภาพอาจถูกเปิดเผยได้

ผู้วิจัยได้ศึกษาจากแบบวัดการรับรู้ถึงความรุนแรงที่บุคคลภายนอกเข้ามาใช้งานแทนตนบนเครือข่ายอินเทอร์เน็ตและการใช้งานคอมพิวเตอร์ของ Woon et al., (2005); Moloney & Poti (2013); Boerman et al., (2018) และ Klein & Luciano (2016) โดยนำมาปรับใช้และพัฒนาเป็น

แบบวัดการรับรู้ถึงความรุนแรงที่บุคคลอื่นจะเข้าใช้งานแทนตนบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีการรับรู้ถึงความรุนแรงที่บุคคลอื่นจะเข้าใช้งานแทนตนบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นการรับรู้ถึงความรุนแรงด้านทรัพย์สิน และการรับรู้ถึงความรุนแรงด้านอันตรายที่อาจเกิดขึ้นกับตัวบุคคล

ความคาดหวังในผลลัพธ์ (Response Efficacy) **ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์** หมายถึง การคาดการณ์ของกลุ่มวัยทำงานตอนต้นถึงความเป็นไปได้เมื่อทำการปฏิบัติตนตามขั้นตอน ระเบียบปฏิบัติ มาตรการ คำแนะนำ เอกสารหรือคู่มือในข้อควรปฏิบัติในการดูแลรักษาข้อมูลส่วนบุคคล จากเอกสารเผยแพร่ ข่าวสาร คลังความรู้ของหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้อง ซึ่งเป็นหน่วยงานที่มีความรู้ ความเชี่ยวชาญเฉพาะด้านและเป็นแหล่งข้อมูลที่น่าเชื่อถือ อ้างอิงได้ เช่น สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์คุ้มครองผู้ใช้บริการทางการเงินของธนาคารแห่งประเทศไทย ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีของสำนักงานตำรวจแห่งชาติ สถาบันทางการเงินและธนาคารพาณิชย์ต่างๆ สถาบันการศึกษา สมาคมผู้ดูแลเว็บไทย เป็นต้น ซึ่งจะเป็นประโยชน์ มีความรู้ความเข้าใจต่อผู้อ่าน สามารถลดโอกาสที่บุคคลอื่นหรือผู้ไม่หวังดีเข้าใช้งานแทนตนและสามารถปกป้องข้อมูลส่วนบุคคลจากการเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันบนธุรกรรมทางอิเล็กทรอนิกส์ได้ แบ่งการศึกษาองค์ประกอบความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ จำนวน 2 ด้าน ได้แก่ ความคาดหวังในผลลัพธ์ตามวิธีการปฏิบัติตนตามคำแนะนำที่ควรปฏิบัติโดยทั่วไป และความคาดหวังในผลลัพธ์ตามวิธีการปฏิบัติตนตามคำแนะนำที่ควรปฏิบัติแบบขั้นสูง

ความคาดหวังในผลลัพธ์ตามวิธีการปฏิบัติตนตามคำแนะนำที่ควรปฏิบัติโดยทั่วไป หมายถึง การคาดการณ์ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับความคาดหวังว่า หากปฏิบัติตนตามคำแนะนำ คู่มือและวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขั้นพื้นฐานอย่างตั้งใจ ซึ่งเป็นการปฏิบัติตามข้อกำหนด ข้อตกลงเบื้องต้นและการให้ความร่วมมือของวิธีการปกป้องข้อมูลส่วนบุคคลในการใช้งานธุรกรรมทางอิเล็กทรอนิกส์ ที่สามารถปฏิบัติตามลำดับ

สามารถนำไปใช้ปฏิบัติได้จริง เป็นมาตรฐานในการใช้งานและเป็นที่ยอมรับอย่างกว้างขวาง จากแหล่งข้อมูลที่น่าเชื่อถือและอ้างอิงได้ซึ่งเป็นหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้อง เกี่ยวกับการกำหนดหรือการจัดการตั้งค่ารหัสผ่าน การเก็บรักษารหัสผ่านที่เหมาะสม การตั้งค่าจำกัดวงเงิน การหมั่นตรวจสอบในการทำรายการธุรกรรมทางอิเล็กทรอนิกส์ย้อนหลัง และการเลือกเปิดเผยข้อมูลส่วนบุคคลเฉพาะที่จำเป็นต่อการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จะเป็นประโยชน์ มีความรู้ ความเข้าใจช่วยลดโอกาสที่บุคคลอื่นสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตนได้

ความคาดหวังในผลลัพธ์ตามวิธีการปฏิบัติตนตามคำแนะนำที่ควรปฏิบัติแบบขั้นสูง (Advanced Practice) หมายถึง การคาดการณ์ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับความคาดหวังว่า หากปฏิบัติตนตามคำแนะนำ คู่มือ ข่าวสารที่ทันสมัยกับเหตุการณ์ที่เป็นปัจจุบัน และวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ทางเทคโนโลยีหรือทางเทคนิคอย่างตั้งใจ ซึ่งเป็นการศึกษาในรายละเอียดลึกซึ้งและเฉพาะทางด้านคอมพิวเตอร์ ความชำนาญในการใช้งานเครื่องคอมพิวเตอร์ชนิดต่างๆ รวมทั้งสมาร์ทโฟน ระบบปฏิบัติการและการใช้โปรแกรมหรือแอปพลิเคชันสำหรับธุรกรรมทางการเงิน และการใช้งานบนเครือข่ายคอมพิวเตอร์ จากแหล่งข้อมูลที่น่าเชื่อถือและอ้างอิงได้ซึ่งเป็นหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้อง จะเป็นประโยชน์ช่วยลดโอกาสที่บุคคลอื่นสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตนได้มากขึ้นและเพิ่มความปลอดภัยของข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ผู้วิจัยได้ศึกษาจากแบบวัดความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องความปลอดภัยของข้อมูลในการใช้งานด้านซอฟต์แวร์ของ Workman et al. (2008) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นความคาดหวังในผลลัพธ์ตามวิธีการปฏิบัติตนตาม

คำแนะนำที่ควรปฏิบัติโดยทั่วไป และความคาดหวังในผลลัพธ์ตามวิธีการปฏิบัติตนตามคำแนะนำที่ควรปฏิบัติแบบขั้นสูง

ความคาดหวังความสามารถของตนเอง (Self-efficacy) **ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์** หมายถึง การรายงานของกลุ่มวัยทำงานตอนต้นในการประเมินความสามารถ การกระทำของตน และพฤติกรรมเกี่ยวกับการปกป้องข้อมูลส่วนบุคคล การควบคุมการเปิดเผยข้อมูลส่วนบุคคลและการเก็บบันทึกข้อมูลส่วนบุคคลให้มีความปลอดภัยจากการเข้าใช้บริการเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ เพื่อลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน แบ่งการศึกษาองค์ประกอบความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ จำนวน 3 ด้าน ได้แก่ การมีทักษะในการใช้งานเครือข่ายคอมพิวเตอร์ ความพร้อมในการรับมือ และความสามารถในการควบคุมสถานการณ์หากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยีที่บุคคลอื่นอาจเข้าถึงข้อมูลส่วนบุคคล (Identity Theft) ซึ่งเป็นภัยที่สร้างความเสียหายทางการเงินและทรัพย์สิน

การมีทักษะในการใช้งานเครือข่ายคอมพิวเตอร์ หมายถึง การรายงานของกลุ่มวัยทำงานตอนต้นในความสามารถของตนเกี่ยวกับการใช้งานเครือข่ายคอมพิวเตอร์สำหรับธุรกรรมทางอิเล็กทรอนิกส์ได้อย่างคล่องแคล่วและถูกต้อง จากประสบการณ์ในอดีตในการเรียนรู้และศึกษาข้อมูลเพิ่มเติมที่จำเป็น การฝึกปฏิบัติจนเกิดความเข้าใจและมีความเชี่ยวชาญต่อการปกป้องข้อมูลส่วนบุคคลให้ปลอดภัยบนธุรกรรมทางอิเล็กทรอนิกส์ รวมไปถึงการแนะนำ ช่วยเหลือบุคคลอื่นในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ เพื่อลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน

ความพร้อมในการรับมือ หากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยีที่บุคคลอื่นอาจเข้าถึงข้อมูลส่วนบุคคลหมายถึง การรายงานของกลุ่มวัยทำงานตอนต้นเกี่ยวกับการประเมินความสามารถของตนเองในการจัดทำบันทึกแผนการกระทำขึ้นไว้ล่วงหน้าเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเป็นการเตรียมความพร้อมรับมือเกี่ยวกับทักษะในการใช้งานเครือข่ายคอมพิวเตอร์ในกรณีที่ไม่ทราบเหตุการณ์ได้ล่วงหน้า การจัดทำแผนสำรอง/ฉุกเฉิน คู่มือปฏิบัติแผนและการฝึกซ้อมแผนกิจกรรมเพื่อลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน เช่น การขอเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคล การเปลี่ยนแปลงรหัสผ่าน การยืนยันตัวบุคคล อีเมล์สำรอง การระงับและการขอยกเลิกบริการจากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น

ความสามารถในการควบคุมสถานการณ์ หากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยีที่บุคคลอื่นอาจเข้าถึงข้อมูลส่วนบุคคล หมายถึง การรายงานของกลุ่มวัยทำงานตอนต้นเกี่ยวกับการประเมินความสามารถในการแก้ไขปัญหา อุปสรรค การคิดวิเคราะห์ การควบคุมอารมณ์และการตัดสินใจในกรณีที่ไม่ทราบเหตุการณ์ได้ล่วงหน้าได้อย่างรวดเร็วและถูกต้อง ซึ่งเป็นวิธีการและแนวทางปฏิบัติเมื่อต้องเผชิญกับสถานการณ์หรือความเปลี่ยนแปลงที่อาจเกิดขึ้นในการควบคุมการเข้าถึงข้อมูลส่วนบุคคล เพื่อลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน

ผู้วิจัยได้ศึกษาจากแบบวัดความคาดหวังความสามารถของตนเองทางด้านคอมพิวเตอร์และการใช้งานอินเทอร์เน็ตของ Compeau & Higgins (1995) และ Workman et al. (2008) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็น การมีทักษะในการใช้งานเครือข่ายคอมพิวเตอร์ ความพร้อมในการรับมือหากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยี และความสามารถในการควบคุมสถานการณ์หากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยีที่บุคคลอื่นอาจเข้าถึงข้อมูลส่วนบุคคล

ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่าย (Response Costs) เพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ หมายถึง การคาดการณ์ของกลุ่มวัยทำงานตอนต้นในการประเมินเรื่องของความคุ้มค่าและผลตอบแทนจากต้นทุน จำนวนเงินค่าใช้จ่าย ความพยายาม อุปสรรคและเวลาที่ต้องสูญเสียไปในการปฏิบัติตนเพื่อปกป้องข้อมูลส่วนบุคคลให้ปลอดภัยจากการเข้าใช้บริการเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ โดยคาดหวังถึงประโยชน์ที่จะได้รับในการปกป้องข้อมูลส่วนบุคคลที่เหมาะสม การลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน เมื่อเปรียบเทียบกับต้นทุนหรือค่าใช้จ่ายที่จะต้องเสียไป แบ่งการศึกษาองค์ประกอบ ความ

คาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ จำนวน 2 ด้าน ได้แก่ ความคาดหวังในความคุ้มค่าของต้นทุนหรือค่าใช้จ่ายที่อยู่ในรูปตัวเงิน (Tangible Costs) และความคาดหวังในความคุ้มค่าของต้นทุนหรือค่าใช้จ่ายที่ไม่ได้อยู่ในรูปตัวเงิน หรือนอกเหนือจากในรูปตัวเงิน (Intangible Costs)

ความคาดหวังในความคุ้มค่าของต้นทุนหรือค่าใช้จ่ายที่อยู่ในรูปตัวเงินเพื่อปกป้องข้อมูลส่วนบุคคล หมายถึง การคาดการณ์ของกลุ่มวัยทำงานเกี่ยวกับความคาดหวังว่า หากตนมีการจ่ายเงินในจำนวนที่เพิ่มขึ้น ได้มีการจัดสรรงบประมาณ หรือมีการแบกรับค่าใช้จ่ายที่เกี่ยวข้องกับการปกป้องข้อมูลส่วนบุคคลให้ปลอดภัยและมีประสิทธิภาพมากขึ้น รวมไปถึงการซื้อเครื่องคอมพิวเตอร์หรือสมาร์ทโฟนใหม่ การซื้อโปรแกรมคอมพิวเตอร์หรือซอฟต์แวร์ที่มีค่าใช้จ่ายเพื่อเพิ่มความปลอดภัยให้กับข้อมูลส่วนบุคคล การปรับปรุงโปรแกรมป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และการนำเทคโนโลยีดิจิทัลที่เป็นมาตรฐานในการเข้ารหัสและยืนยันตัวตนที่มีความปลอดภัยค่อนข้างสูงมาใช้งาน ซึ่งสามารถลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตนได้

ความคาดหวังในความคุ้มค่าของต้นทุนหรือค่าใช้จ่ายที่ไม่ได้อยู่ในรูปตัวเงินเพื่อปกป้องข้อมูลส่วนบุคคล หมายถึง การคาดการณ์ของกลุ่มวัยทำงานเกี่ยวกับความคาดหวังว่า หากตนต้องใช้เวลา ความพากเพียร ความพยายามอย่างเต็มที่ และความตั้งใจจริงในการเรียนรู้วิธีการและขั้นตอนการปฏิบัติตนปกป้องข้อมูลส่วนบุคคล เพื่อลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน จะเป็นประโยชน์ในการปกป้องข้อมูลส่วนบุคคลที่เหมาะสมและเพิ่มความปลอดภัยบนธุรกรรมทางอิเล็กทรอนิกส์ เมื่อเปรียบเทียบกับต้นทุนหรือค่าใช้จ่ายที่ไม่ได้อยู่ในรูปตัวเงินที่จะต้องสูญเสียไป

ผู้วิจัยได้ศึกษาจากแบบวัดความคาดหวังจากต้นทุนที่จ่ายไปที่มีอิทธิพลต่อแรงจูงใจและพฤติกรรมของผู้ใช้งานอินเทอร์เน็ตในการปกป้องความเป็นส่วนตัวของ Lee et al., (2008); Boehmer et al., (2015); LeFebvre (2012) และ Ifinedo (2012) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเชิงเศรษฐศาสตร์พฤติกรรมเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1

คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นความคาดหวังในความคุ้มค่าของต้นทุนหรือค่าใช้จ่ายที่อยู่ในรูปตัวเงินและไม่ได้อยู่ในรูปตัวเงินเพื่อปกป้องข้อมูลส่วนบุคคล

คุณลักษณะของระบบ (System Characteristics) **เพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์** หมายถึง การรับรู้และความคิดเห็นของกลุ่มวัยทำงานตอนต้นเกี่ยวกับระบบหรือโปรแกรมคอมพิวเตอร์หรือแอปพลิเคชันในภาพรวมและมีการใช้งานอยู่ในปัจจุบัน ที่ผู้ใช้งานสามารถกำหนดการจัดการตั้งค่าข้อมูลส่วนบุคคลในธุรกรรมทางการเงินได้ด้วยตนเอง และการควบคุมการเปิดเผยข้อมูลส่วนบุคคลให้มีความปลอดภัยจากการเข้าใช้บริการเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ โดยผู้ใช้งานสามารถทำความเข้าใจได้โดยง่ายในการเข้าใช้งาน การมีปฏิสัมพันธ์โต้ตอบที่ดีระหว่างระบบกับผู้ใช้งาน การให้ผลลัพธ์ที่ถูกต้องตามความต้องการของผู้ใช้งาน การมีรูปแบบการประมวลผลที่ถูกต้องและรวดเร็ว การมีรูปแบบการนำเสนอและความน่าสนใจของระบบ เพื่อลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน แบ่งการศึกษาองค์ประกอบคุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ จำนวน 2 ด้าน ได้แก่ คุณลักษณะเด่นของระบบ (Features) และส่วนติดต่อกับผู้ใช้งาน (User Interface)

คุณลักษณะเด่นของระบบ หมายถึง ปริมาณการรับรู้และความคิดเห็นของกลุ่มวัยทำงานตอนต้นในคุณลักษณะเฉพาะและรูปแบบการใช้งานภายในระบบหรือโปรแกรมคอมพิวเตอร์หรือแอปพลิเคชันในภาพรวมและมีการใช้งานอยู่ในปัจจุบัน สำหรับการจัดการตั้งค่าข้อมูลส่วนบุคคลในธุรกรรมทางการเงินได้ด้วยตนเอง และการควบคุมการเปิดเผยข้อมูลส่วนบุคคล ให้มีความปลอดภัยบนธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งผู้ใช้งานสามารถทำความเข้าใจได้โดยง่าย ความรวดเร็วในการประมวลผล รูปแบบการนำเสนอเนื้อหาทันสมัย ความไม่ซับซ้อนภายในระบบ และการให้ผลลัพธ์ที่ถูกต้องตามความต้องการเฉพาะเจาะจง การกำหนดระดับการเข้าถึงและตรวจสอบข้อมูล รวมไปถึงการเป็นที่ยอมรับและประสิทธิภาพเกี่ยวกับคุณภาพของระบบด้านความปลอดภัยบนธุรกรรมทางอิเล็กทรอนิกส์

ส่วนติดต่อกับผู้ใช้งาน หมายถึง ปริมาณการรับรู้และความคิดเห็นของกลุ่มวัยทำงานตอนต้นเกี่ยวกับการออกแบบบนหน้าจอการใช้งานภายในของระบบหรือโปรแกรมคอมพิวเตอร์หรือแอปพลิเคชันในภาพรวมและมีการใช้งานอยู่ในปัจจุบัน ซึ่งอำนวยความสะดวกให้กับผู้ใช้งาน

ที่สวยงามและเป็นที่ดึงดูดใจต่อการใช้งาน มีการนำเสนอที่น่าสนใจในรูปแบบกราฟิกเชิงสัญลักษณ์ การใช้คำอธิบายและคำศัพท์ที่เข้าใจง่าย การออกแบบสีและขนาดตัวอักษรที่เหมาะสม และภาพการแสดงตัวอย่างที่ชัดเจนสำหรับการจัดการตั้งค่าข้อมูลส่วนบุคคลในธุรกรรมทางการเงินได้ด้วยตนเอง และการควบคุมการเปิดเผยข้อมูลส่วนบุคคลให้มีความปลอดภัยบนธุรกรรมทางอิเล็กทรอนิกส์

ผู้วิจัยได้ศึกษาจากแบบวัดคุณลักษณะของระบบ รูปแบบการใช้งานภายในระบบเกี่ยวกับการทำความเข้าใจถึงวิธีการใช้งานที่มีอิทธิพลต่อการยอมรับการใช้เทคโนโลยีกับผู้ใช้งานของ Venkatesh & Davis (1996) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดคุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีความเข้าใจในวิธีการเข้าใช้งานคุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นคุณลักษณะเด่นของระบบและส่วนติดต่อกับผู้ใช้งาน

การคล้อยตามกลุ่มอ้างอิง (Subjective Norms) **ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์** หมายถึง การรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับการคล้อยตามความคิดเห็นกลุ่มบุคคลรอบข้างที่ตนยอมรับทางสังคมและให้ความสำคัญ ประกอบไปด้วยบุคคลในครอบครัว ญาติสนิท เพื่อนสนิท เพื่อนร่วมงาน และหัวหน้างาน รวมทั้งบุคคล กลุ่มบุคคลหรือหน่วยงานที่มีการเขียนเรื่องราว ข้อมูลแนะนำ การแบ่งปันแลกเปลี่ยนความคิดเห็นจากประสบการณ์ ข้อมูลที่น่าสนใจ การคล้อยตามทางความคิดและเป็นประโยชน์ต่อผู้อื่น จนเป็นที่รู้จักและได้รับการยอมรับว่าเป็นผู้เชี่ยวชาญและมีอิทธิพลทางเทคโนโลยีบนสื่อสังคมออนไลน์ต่างๆ ซึ่งเรียกว่าไอที บล็อกเกอร์ (IT Bloggers) และอาจพัฒนาเป็นอินฟลูเอนเซอร์ (Influencers) หรือผู้ทรงอิทธิพลทางเทคโนโลยีบนสื่อสังคมออนไลน์ได้ เกี่ยวกับความสำคัญ ข้อดีและสนับสนุนการจัดการตั้งค่าข้อมูลส่วนบุคคล การปกป้องข้อมูลส่วนบุคคลและการควบคุมการเปิดเผยข้อมูลส่วนบุคคลให้มีความปลอดภัยจากการเข้าใช้บริการเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ เพื่อลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งาน

ธุรกรรมทางอิเล็กทรอนิกส์แทนตน แบ่งการศึกษาองค์ประกอบการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ จำนวน 2 ด้าน ได้แก่ การคล้อยตามกลุ่มบุคคลรอบข้างที่ใกล้ชิด และการคล้อยตามผู้ทรงอิทธิพลทางเทคโนโลยีบนสื่อสังคมออนไลน์

การคล้อยตามกลุ่มบุคคลรอบข้างที่ใกล้ชิด หมายถึง ปริมาณการรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับการคล้อยตามความคิดเห็นกลุ่มบุคคลรอบข้างที่ตนรู้จัก ให้ความสำคัญและยอมรับในสังคม ประกอบด้วย บุคคลในครอบครัว ญาติสนิท เพื่อนสนิท เพื่อนร่วมงานและหัวหน้างาน ที่มีอิทธิพลต่อพฤติกรรมการจัดการตั้งค่าข้อมูลส่วนบุคคล การปกป้องข้อมูลส่วนบุคคลและการควบคุมการเปิดเผยข้อมูลส่วนบุคคลให้มีความปลอดภัยบนธุรกรรมทางอิเล็กทรอนิกส์ จากคำแนะนำ การชักชวน พูดคุยแลกเปลี่ยนความคิดเห็น การเห็นถึงความสำคัญ ประโยชน์ ความนิยมในการใช้งานในวงกว้าง ความต้องการและการสนับสนุนในการจัดการตั้งค่าข้อมูลส่วนบุคคล

การคล้อยตามผู้ทรงอิทธิพลทางเทคโนโลยีบนสื่อสังคมออนไลน์ หมายถึง ปริมาณการรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับการคล้อยตามความคิดเห็น ทัศนคติและพฤติกรรมของบุคคล กลุ่มบุคคลหรือหน่วยงานที่มีความรู้ แหล่งข้อมูลน่าเชื่อถือ มีความเชี่ยวชาญเฉพาะด้านและมีอิทธิพลในการใช้งานอุปกรณ์อิเล็กทรอนิกส์และเทคโนโลยีบนสื่อสังคมออนไลน์ในรูปแบบต่างๆ เช่น เฟซบุ๊ก เว็บบล็อก ยูทูป ทวิตเตอร์ เป็นต้น ซึ่งจะเรียกว่าไอที บล็อกเกอร์ (IT Bloggers) โดยเป็นที่รู้จักทางสังคมอย่างกว้างขวาง จากคำแนะนำ การกระตุ้น ชักชวน โฆษณาและประชาสัมพันธ์ การเห็นถึงความสำคัญ ประโยชน์ และการสนับสนุนในการจัดการตั้งค่าข้อมูลส่วนบุคคล การปกป้องข้อมูลส่วนบุคคลและการควบคุมการเปิดเผยข้อมูลส่วนบุคคลให้มีความปลอดภัยบนธุรกรรมทางอิเล็กทรอนิกส์ เช่น เว็บไซต์ IT24hrs.com, เพจ LDA ลดา, Beartai: แบไต๋, ธนาคารแห่งประเทศไทย, สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, เพจเฟซบุ๊กศูนย์ปราบปรามอาชญากรรมทางเทคโลโลยี สำนักงานตำรวจแห่งชาติ เป็นต้น

ผู้วิจัยได้ศึกษาจากแบบวัดการคล้อยตามกลุ่มอ้างอิงในการกระทำพฤติกรรมโดยใช้แนวคิดของ Fishbein & Ajzen (1975: 73-76) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงาน

ตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นการคล้อยตามกลุ่มบุคคลรอบข้างที่ใกล้ชิด และการคล้อยตามผู้ทรงอิทธิพลทางเทคโนโลยีบนสื่อสังคมออนไลน์

การรับรู้ถึงประโยชน์ (Perceived Usefulness) **ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์** หมายถึง การรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับข้อดีของการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล ที่ก่อให้เกิดประโยชน์ในชีวิตของตนเอง การช่วยเพิ่มประสิทธิผลในความปลอดภัยของข้อมูลส่วนบุคคลมากขึ้น และการรับรู้ถึงคุณค่าที่ได้จากการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลเมื่อเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ เพื่อลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน แบ่งการศึกษาองค์ประกอบการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ จำนวน 2 ด้าน ได้แก่ การก่อให้เกิดประโยชน์ต่อตนเอง (Useful) และการเพิ่มประสิทธิผล (Increase Productivity) ในความปลอดภัยของข้อมูลส่วนบุคคล

การก่อให้เกิดประโยชน์ต่อตนเอง หมายถึง ปริมาณการรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล จะส่งผลให้การวางแผนชีวิตทางการเงินมีความปลอดภัย สร้างวินัยทางการเงินในการปกป้องข้อมูลส่วนบุคคล และช่วยลดความตึงเครียด ลดความกังวลเกี่ยวกับโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน รวมไปถึงการอำนวยความสะดวกในการใช้บริการทางการเงินได้อย่างปลอดภัย การเพิ่มขีดความสามารถในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์และเทคโนโลยีทางการเงินให้เกิดประโยชน์สูงสุด และการลดระยะเวลาขอคำปรึกษาหรือคำแนะนำจากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์

การเพิ่มประสิทธิผลในความปลอดภัยของข้อมูลส่วนบุคคล หมายถึง ปริมาณการรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับผลที่จะเกิดขึ้นเมื่อจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์เพื่อลดจำนวนของโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน โอกาสที่จะถูกการโจรกรรมข้อมูลส่วนบุคคลลดลง การช่วยเพิ่มความพึงพอใจในการใช้บริการบนธุรกรรมทางอิเล็กทรอนิกส์ให้ปลอดภัยในระยะยาว การมีคุณภาพชีวิตด้านความปลอดภัยข้อมูลส่วนบุคคลที่ดีขึ้น การเป็นผู้ใช้งานในบริการธุรกรรมทางอิเล็กทรอนิกส์ที่ดีและมีความปลอดภัยข้อมูล การมีโอกาสได้รับบริการด้านความ

ปลอดภัยข้อมูลส่วนบุคคลจากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ในระดับที่สูงขึ้นและเพิ่มระดับความปลอดภัยข้อมูลทางการเงินในอนาคตได้

ผู้วิจัยได้ศึกษาจากแบบวัดการรับรู้ประโยชน์ของการยอมรับการใช้เทคโนโลยี โดยใช้แนวคิดของ Davis et al. (1989: 982-1003) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นการก่อให้เกิดประโยชน์ต่อตนเอง และการเพิ่มประสิทธิผลในความปลอดภัยของข้อมูลส่วนบุคคล

การรับรู้ถึงความง่าย (Perceived Ease of Use) **ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์** หมายถึง การรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับการเรียนรู้วิธีการ และขั้นตอนของการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลเมื่อเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์นั้น สามารถกระทำการตั้งค่าปกป้องข้อมูลส่วนบุคคลได้ง่าย สะดวก ไม่ต้องใช้ความพยายามในการเรียนรู้วิธีการและขั้นตอนมาก ไม่มีความซับซ้อนรับรู้ว่าขั้นตอนการตั้งค่าปกป้องข้อมูลส่วนบุคคลมีความชัดเจนและเข้าใจง่าย และมีความเป็นไปได้สูงในการยอมรับจากผู้ใช้งาน เพื่อลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน แบ่งการศึกษาองค์ประกอบการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ จำนวน 2 ด้าน ได้แก่ ความง่ายต่อการเรียนรู้ (Easy to Learn) และความไม่ซับซ้อนของระบบ (Simplicity) ในวิธีการและขั้นตอนของการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล

ความง่ายต่อการเรียนรู้ หมายถึง ปริมาณการรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับวิธีการ และขั้นตอนของการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ใช้งานง่าย มีคำอธิบายที่ชัดเจน เป็นเรื่องง่ายในการเรียนรู้ สามารถทำความเข้าใจได้ด้วยตนเอง สามารถปฏิบัติตามวิธีการได้อย่างรวดเร็วและสะดวกต่อการตั้งค่าปกป้องข้อมูลส่วนบุคคล เพื่อลด

โอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน

ความไม่ซับซ้อนของระบบ หมายถึง ปริมาณการรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับการไม่ต้องใช้ความพยายามมากของการเรียนรู้วิธีการและขั้นตอนในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ความไม่ยุ่งยาก ตรงไปตรงมา ไม่มีขั้นตอนที่ซับซ้อน ไม่ต้องใช้ความพยายามมากนัก สามารถตั้งค่าการใช้งานได้ตามความต้องการของตนเอง การใช้งานตามวัตถุประสงค์และการมีระบบคอยช่วยเหลือ (Help) ตามความจำเป็น เพื่อลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน รวมไปถึงการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์โดยไม่ต้องใช้ความพยายามด้านจิตใจ เช่น การรู้สึกท้อแท้ ความเบื่อหน่ายในการตั้งค่าปกป้องข้อมูลส่วนบุคคล เป็นต้น

ผู้วิจัยได้ศึกษาจากแบบวัดการรับรู้การใช้งานง่ายของการยอมรับการใช้เทคโนโลยี โดยใช้แนวคิดของ Davis et al. (1989: 982-1003) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นความง่ายต่อการเรียนรู้และความไม่ซับซ้อนของระบบในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ทัศนคติ (Attitude) **ที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์** หมายถึง การรับรู้ของกลุ่มวัยทำงานตอนต้นในความเชื่อ ความคิดเห็น สภาพความคิด ความเข้าใจและความรู้สึกเชิงประเมินที่มีต่อการปฏิบัติตนตามวิธีการ และขั้นตอนการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลเมื่อเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ เพื่อลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน แบ่งการศึกษาองค์ประกอบของทัศนคติที่มีต่อการปกป้อง

ข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ จำนวน 2 ด้าน ได้แก่ ความเชื่อในผลของการกระทำ (Behavioral Belief) และการประเมินคุณค่าการกระทำ (Evaluation of Outcome) ในวิธีการและขั้นตอนของการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ความเชื่อในผลของการกระทำ หมายถึงปริมาณการรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับความรู้สึกในเชิงบวกในลักษณะเห็นด้วย สนับสนุน ความพึงพอใจ เป็นสิ่งที่ควรกระทำ สิ่งจำเป็นและควรปฏิบัติตนตามวิธีการ และขั้นตอนการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลเมื่อเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์

การประเมินคุณค่าการกระทำ หมายถึงปริมาณการรับรู้ของกลุ่มวัยทำงานตอนต้นเกี่ยวกับความคาดหวัง ความรู้สึกที่มีต่อผลลัพธ์ที่อาจเกิดขึ้น และการประเมินในการตัดสินใจของผลที่จะได้รับหรือผลที่ตามมา จากการปฏิบัติตนตามวิธีการ และขั้นตอนการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลเมื่อเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ ในแง่มุมของความปลอดภัยในข้อมูลส่วนบุคคล ประโยชน์ที่คาดว่าจะได้รับ ความเข้าใจ วิจารณญาณและการมีเหตุผลในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มากขึ้น

ผู้วิจัยได้ศึกษาจากแบบวัดทัศนคติของการปฏิบัติตนตามนโยบายในการรักษาและปกป้องข้อมูลในองค์กรของนักพัฒนาแอปพลิเคชันจากงานวิจัยของ Woon & Kankanhalli (2007) และ Bulgurcu et al., (2010) โดยนำมาสร้างและพัฒนาเป็นแบบวัดทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีทัศนคติต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นความเชื่อในผลของการกระทำ และการประเมินคุณค่าการกระทำในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ความตั้งใจ (Intention) ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ หมายถึง การรับรู้ของกลุ่มวัยทำงานตอนต้นในเจตนาการแสดงออก ความพยายาม ความมุ่งมั่น ความพร้อม และความยินดีที่จะปฏิบัติตนในการจัดการตั้งค่าข้อมูลส่วนบุคคล การปกป้องข้อมูลส่วนบุคคลและการควบคุมการเปิดเผยข้อมูลส่วนบุคคลให้มีความ

ปลอดภัยจากการเข้าใช้บริการเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ เพื่อลดโอกาสที่บุคคลอื่นจะสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน

ผู้วิจัยได้ศึกษาจากแบบวัดของ Foltz et al., (2016) และ Bulgurcu et al., (2010) เกี่ยวกับพฤติกรรมของผู้ใช้งานต่อการเปลี่ยนแปลงในการตั้งค่าเพื่อความปลอดภัยจากเครือข่ายสังคมออนไลน์ โดยนำมาสร้างและพัฒนาเป็นแบบวัดความตั้งใจเชิงพฤติกรรม (Behavioral Intention) ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปรนี้ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก

บทที่ 3
วิธีดำเนินการวิจัย

งานวิจัยนี้เป็นงานวิจัยเชิงปริมาณ (Quantitative Research) มีพื้นฐานแนวคิดปรัชญาแบบปฏิฐานนิยม (Positivism) เพื่อศึกษารูปแบบความสัมพันธ์เชิงเหตุของปัจจัยทางจิตวิทยาและสังคมที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ที่พัฒนาขึ้นจากการสังเคราะห์เอกสาร การพิจารณาเหตุผลและงานวิจัยที่เกี่ยวข้องทางด้านแนวคิดเศรษฐศาสตร์เชิงพฤติกรรมและการใช้งานเทคโนโลยีเชิงพฤติกรรมการตอบสนอง โดยการพิจารณาและประยุกต์ใช้ตามกรอบทฤษฎีแรงจูงใจเพื่อการป้องกัน (The Protection Motivation Theory: PMT) ร่วมกับแนวคิดแบบจำลองการยอมรับการใช้เทคโลยี (Technology Acceptance Model: TAM) ซึ่งมีรายละเอียดวิธีการดำเนินการวิจัย ดังนี้

1. ประชากรและขนาดกลุ่มตัวอย่าง
2. การสุ่มกลุ่มตัวอย่าง
3. การสร้างและตรวจสอบคุณภาพของเครื่องมือที่ใช้ในการวิจัย
4. เครื่องมือที่ใช้ในการวิจัย
5. การเก็บรวบรวมข้อมูล การจัดกระทำและการวิเคราะห์ข้อมูล

1. ประชากรและขนาดกลุ่มตัวอย่าง

ประชากรในงานวิจัยนี้ คือกลุ่มวัยทำงานตอนต้นหรือกลุ่มที่เริ่มเข้าสู่วัยทำงาน (First Jobber) โดยใช้กรอบการจัดแบ่งช่วงวัยของกรมอนามัย กระทรวงสาธารณสุข (2559) คือบุคคลที่มีอายุระหว่าง 20-29 ปี และเป็นผู้ที่ใช้หรือเคยทำธุรกรรมทางอิเล็กทรอนิกส์

ผู้วิจัยได้กำหนดขนาดกลุ่มตัวอย่างโดยใช้กฎแห่งความชัดเจน (Rule of Thumb) ซึ่งเป็นการกำหนดขนาดตัวอย่างที่นิยมใช้กันอย่างแพร่หลาย ได้รับการยอมรับและการกำหนดขนาดตัวอย่างสำหรับการศึกษาที่มีการวิเคราะห์องค์ประกอบ (Factor Analysis) จากข้อเสนอแนะเกี่ยวกับขนาดตัวอย่างที่เหมาะสมของ Kline (2010) ที่สามารถเป็นตัวแทนของประชากรและมีจำนวนเพียงพอที่ทำให้ผลการวิจัยเชื่อถือได้ ควรให้มีขนาดตัวอย่างในการศึกษาวิจัยไม่ต่ำกว่า 200 ตัวอย่าง รวมทั้งการพิจารณาขนาดกลุ่มตัวอย่างที่เหมาะสมในงานวิจัยจากข้อแนะนำ (นงลักษณ์ วิรัชชัย, 2542; Hair et al., 2010) ควรมีขนาดกลุ่มตัวอย่าง 15-20 เท่าของจำนวนตัวแปรสังเกต (Observed Variables) ในงานวิจัย งานวิจัยนี้มีจำนวนตัวแปรสังเกต 24 ตัวแปร ควรมี

จำนวนกลุ่มตัวอย่าง 360-480 ตัวอย่าง ดังนั้นผู้วิจัยได้กำหนดขนาดกลุ่มตัวอย่างจำนวน 400 คน ขึ้นไป

ทั้งนี้ ผู้วิจัยได้กำหนดกลุ่มตัวอย่างซึ่งเป็นวัยทำงานตอนต้นที่มีสถานที่ทำงานในเขตกรุงเทพมหานครและปริมณฑล (ประกอบด้วย 5 จังหวัดได้แก่ นครปฐม นนทบุรี ปทุมธานี สมุทรปราการและสมุทรสาคร) ซึ่งกลุ่มวัยทำงานตอนต้นที่ผู้วิจัยเลือกศึกษานี้ เนื่องจากเป็นกลุ่มที่เริ่มมีรายได้เป็นของตนเอง เริ่มมีพฤติกรรมการใช้งานบัตรเครดิต การซื้อสินค้าออนไลน์และการชำระเงินผ่านทางอิเล็กทรอนิกส์มากขึ้นเมื่อเปรียบเทียบกับกลุ่มวัยทำงานกลุ่มอื่น จำเป็นที่ต้องเริ่มมีการวางแผนให้ข้อมูลแนวทางการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ที่ดีและเหมาะสมต่อสถานการณ์ปัจจุบัน เพื่อให้มีรูปแบบการดำเนินชีวิตทางการเงินที่ปลอดภัย รวมทั้งในเขตกรุงเทพมหานครและปริมณฑลมีบุคคลรายย่อยใช้บริการธุรกรรมทางอิเล็กทรอนิกส์จำนวนมากและมีอัตราที่เพิ่มขึ้นทุกปี และเป็นเขต/จังหวัดที่มีจำนวนการจดทะเบียนของผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์รายปีสูงขึ้นอย่างต่อเนื่อง (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2563; กรมพัฒนาธุรกิจการค้า, 2562) ในการวิจัยครั้งนี้ผู้วิจัยจึงได้กำหนดกลุ่มตัวอย่างเป็นกลุ่มวัยทำงานตอนต้นในเขตกรุงเทพมหานครและปริมณฑล และเป็นผู้ที่ใช้หรือเคยใช้บริการธุรกรรมทางอิเล็กทรอนิกส์

นอกจากนี้ เพื่อให้เป็นไปตามวัตถุประสงค์ของการวิจัยนี้และได้กลุ่มตัวอย่างที่ศึกษามีลักษณะเฉพาะ จะมีการสอบถามคัดเลือก (Screening Question) เกี่ยวกับช่วงอายุต้องอยู่ในกลุ่มวัยทำงานตอนต้นระหว่าง 20-29 ปีและกำหนดความถี่การใช้บริการที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์มากกว่า 5 ครั้งต่อเดือนในรอบ 6 เดือนที่ผ่านมา (รายงานผลการสำรวจพฤติกรรมผู้ใช้งานอินเทอร์เน็ต กลุ่มเจเนอเรชันวาย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2561) หากกลุ่มตัวอย่างผ่านเกณฑ์การสอบถามคัดเลือกเกี่ยวกับช่วงอายุและความถี่การใช้บริการที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์ตามที่กำหนดไว้ ผู้วิจัยจึงจะทำการขอความร่วมมือและเก็บรวบรวมข้อมูลตัวอย่างจนครบจำนวนที่กำหนดกลุ่มตัวอย่างไว้

2. การสุ่มกลุ่มตัวอย่าง

งานวิจัยนี้ ได้ใช้เหตุผลของการสุ่มกลุ่มตัวอย่างจากการเริ่มต้นพื้นที่ขนาดใหญ่ที่สุดจากจังหวัด ไปสู่อำเภอ/เขต ด้วยการสุ่มตัวอย่างแบบกลุ่มจำนวน 2 ขั้นตอน (Two-stage Cluster Sampling) ซึ่งเป็นการสุ่มกลุ่มตัวอย่างโดยอาศัยความน่าจะเป็น จากนั้นไปยังหน่วยงานที่ได้รับอนุญาตในการเก็บรวบรวมข้อมูล ด้วยการสุ่มกลุ่มตัวอย่างแบบไม่อาศัยความน่าจะเป็น ซึ่งเป็นการสุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) ประกอบด้วย

ขั้นตอนที่ 1 ใช้วิธีการสุ่มตัวอย่างแบบกลุ่ม (Custer Random Sampling) เพื่อเลือกกลุ่มตัวอย่างจากการจัดกลุ่มพื้นที่ตามการแบ่งเขตการปกครองกรุงเทพมหานครจำนวน 5 กลุ่มและเลือกจังหวัดในเขตปริมณฑลจำนวน 5 จังหวัด

ขั้นตอนที่ 2 ใช้วิธีการสุ่มตัวอย่างแบบกลุ่ม เพื่อเลือกกลุ่มตัวอย่างของเขตพื้นที่ในกรุงเทพมหานครและอำเภอสำหรับตัวอย่างในปริมณฑล เนื่องจากกลุ่มย่อยมีความชัดเจนในการแบ่งกลุ่มและความแตกต่างระหว่างกลุ่มย่อยมีจำนวนน้อย (Homogeneous) (อุทัยทิพย์ เจี่ยวิวรรธน์กุล, 2558)

จากนั้นใช้การสุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) โดยทำการสอบถามไปยังสถานที่ทำงานทั้งภาครัฐและภาคเอกชน ที่ได้รับอนุญาตและให้ความร่วมมือในการเก็บรวบรวมข้อมูล รวมไปถึงการสอบถามคัดเลือก (Screening Question) ต้องเป็นกลุ่มตัวอย่างกลุ่มวัยทำงานตอนต้น ในลักษณะงานประจำประเภทเต็มเวลา (Full-time) ที่มีพฤติกรรมใช้บริการธุรกรรมทางอิเล็กทรอนิกส์และสอดคล้องกับงานวิจัยนี้ กล่าวคือเป็นกลุ่มวัยทำงานตอนต้นระหว่าง 20-29 ปีและมีความถี่การใช้บริการที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์มากกว่า 5 ครั้งต่อเดือนในรอบ 6 เดือนที่ผ่านมา

สำหรับรายละเอียดของการสุ่มตัวอย่างแบบกลุ่ม 2 ขั้นตอน เป็นดังนี้

ขั้นตอนที่ 1 ใช้วิธีการสุ่มตัวอย่างแบบกลุ่ม เพื่อเลือกเขตพื้นที่ทำการศึกษาวิจัยโดยวิธีการจับสลาก ผู้วิจัยใช้เกณฑ์การแบ่งเขตการปกครองกรุงเทพมหานคร ตามสำนักยุทธศาสตร์และประเมินผล กรุงเทพมหานคร (2560) ซึ่งสามารถแบ่งเขตการปกครอง จำนวน 5 กลุ่มได้ดังนี้

กลุ่มที่ 1 กรุงเทพเหนือ ประกอบด้วยเขตจตุจักร บางซื่อ ลาดพร้าว หลักสี่ ดอนเมือง สายไหมและบางเขน

กลุ่มที่ 2 กรุงเทพกลาง ประกอบด้วยเขตพระนคร ดุสิต ป้อมปราบศัตรูพ่าย สัมพันธวงศ์ ดินแดง ห้วยขวาง พญาไท ราชเทวีและวังทองหลาง

กลุ่มที่ 3 กรุงเทพตะวันออก ประกอบด้วยเขตบางกะปิ สะพานสูง บึงกุ่ม คันนายาว ลาดกระบัง มีนบุรี หนองจอก คลองสามวาและประเวศ

กลุ่มที่ 4 กรุงเทพใต้ ประกอบด้วยเขตปทุมวัน บางรัก สาทร บางคอแหลม ยานนาวา คลองเตย วัฒนา พระโขนง สวนหลวงและบางนา

และกลุ่มที่ 5 กรุงธนเหนือและใต้ ประกอบด้วยเขตธนบุรี คลองสาน จอมทอง บางกอกใหญ่ บางกอกน้อย บางพลัด ตลิ่งชัน ทวีวัฒนา ภาษีเจริญ บางแค หนองแขม บางขุนเทียน บางบอน ราษฎร์บูรณะและทุ่งครุ

ในเขตกรุงเทพมหานคร ผู้วิจัยใช้วิธีการสุ่มอย่างง่าย เพื่อเลือกกลุ่มตามการแบ่งเขตการปกครองโดยวิธีการจับสลาก ซึ่งผู้วิจัยได้กำหนดเลือกกลุ่มเป็นตัวแทนจำนวน 2 กลุ่ม จากทั้งหมด 5 กลุ่มตามการแบ่งเขตการปกครอง ผลการจับสลากเพื่อสุ่มเลือก 2 กลุ่มเป็นตัวแทน ได้แก่ กรุงเทพกลาง และกรุงเทพใต้ สำหรับเขตปริมณฑล ผู้วิจัยใช้วิธีการสุ่มอย่างง่ายเช่นเดียวกับวิธีการสุ่มเขตกรุงเทพมหานคร เพื่อเลือกจังหวัดที่ทำการศึกษาโดยวิธีการจับสลาก ผู้วิจัยได้กำหนดเลือกจังหวัดเป็นตัวแทนจำนวน 2 จังหวัด จากทั้งหมด 5 จังหวัด ประกอบด้วย นครปฐม นนทบุรี ปทุมธานี สมุทรปราการและสมุทรสาคร ผลการจับสลากเพื่อสุ่มเลือกเขตปริมณฑล 2 จังหวัดเป็นตัวแทน ได้แก่ นนทบุรีและปทุมธานี

ขั้นตอนที่ 2 ใช้วิธีการสุ่มตัวอย่างแบบกลุ่ม เพื่อเลือกกลุ่มตัวอย่างของเขตพื้นที่ในกรุงเทพมหานครและอำเภอสำหรับตัวอย่างในปริมณฑล โดยวิธีการจับสลาก ซึ่งผู้วิจัยได้กำหนดเลือกเขตพื้นที่ของแต่ละกลุ่มตามการแบ่งเขตการปกครองกรุงเทพมหานครเพื่อมาเป็นตัวแทนจำนวนเขตละ 3 ของแต่ละกลุ่ม สำหรับปริมณฑลได้กำหนดเลือกอย่างละ 2 อำเภอของแต่ละจังหวัดเพื่อเป็นตัวแทน

ผลการจับสลากเพื่อสุ่มเลือก 2 กลุ่มและเขตเป็นตัวแทนของกรุงเทพมหานคร ได้แก่ กรุงเทพกลาง ประกอบด้วยเขตพระนคร พญาไทและราชเทวี ส่วนกรุงเทพใต้ ประกอบด้วยเขตยานนาวา สาทรและปทุมวัน สำหรับปริมณฑล ได้แก่จังหวัดนนทบุรี ประกอบด้วยอำเภอปากเกร็ดและอำเภอเมือง ส่วนจังหวัดปทุมธานี ประกอบด้วยอำเภอคลองหลวงและลาดหลุมแก้ว รวมทั้งสิ้น 10 เขตพื้นที่ สรุปได้ดังนี้

เขตการปกครองกรุงเทพมหานคร ผลการสุ่มเลือกกลุ่มตัวแทน ขั้นตอนที่ 1 ประกอบด้วย กรุงเทพกลาง และกรุงเทพใต้ ส่วนขั้นตอนที่ 2 กรุงเทพกลาง (ผลการสุ่มเลือกตัวแทนเขตพระนคร พญาไท และราชเทวี) และกรุงเทพใต้ (ผลการสุ่มเลือกตัวแทนเขตยานนาวา สาทร และปทุมวัน)

จังหวัดในเขตปริมณฑล ผลการสุ่มเลือกกลุ่มตัวแทน ขั้นตอนที่ 1 ประกอบด้วย นนทบุรี และปทุมธานี ส่วนขั้นตอนที่ 2 นนทบุรี (ผลการสุ่มเลือกตัวแทนอำเภอปากเกร็ดและอำเภอเมือง) และปทุมธานี (ผลการสุ่มเลือกตัวแทนอำเภอคลองหลวงและอำเภอลาดหลุมแก้ว)

จากการออกหนังสือรับรองจากบัณฑิตวิทยาลัย และโครงการวิจัยนี้ผ่านการพิจารณาจริยธรรมสำหรับโครงการวิจัยที่ทำในมนุษย์แล้วหมายเลข SWUEC-G-299/2563X (ภาคผนวก ค หนังสือรับรองจริยธรรมในงานวิจัย) สำหรับขอความอนุเคราะห์เก็บข้อมูลเพื่อการวิจัยตั้งแต่เดือนสิงหาคม 2564 ถึงเดือนตุลาคม 2564 โดยวิธีการเก็บรวบรวมข้อมูลออนไลน์ ในรูปแบบสอบถามเพื่อการวิจัยเรื่องปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ดังภาพประกอบ 7

ภาพประกอบ 7 วิธีการเก็บรวบรวมข้อมูลออนไลน์ แบบสอบถามเพื่อการวิจัย

พบว่าวิธีการเก็บรวบรวมข้อมูลออนไลน์ในรูปแบบสอบถามเพื่อการวิจัย มีหน่วยงานทั้งภาครัฐและเอกชนที่ได้รับอนุญาติและให้ความร่วมมือในการเก็บรวบรวมข้อมูลออนไลน์ในกลุ่มวัยทำงานตอนต้น ในลักษณะงานประจำประเภทเต็มเวลาที่มีพฤติกรรมใช้บริการธุรกรรมทางอิเล็กทรอนิกส์และสอดคล้องกับงานวิจัยนี้ ตั้งแต่เดือนสิงหาคม 2564 ถึงเดือนตุลาคม 2564 ตามเขตพื้นที่และหน่วยงานของการสุ่มกลุ่มตัวอย่าง (ภาคผนวก ง หนังสือขอความอนุเคราะห์เก็บข้อมูลเพื่อการวิจัย)

กลุ่มตัวอย่างที่ใช้ในการวิจัยนี้ เป็นกลุ่มวัยทำงานตอนต้นในเขตกรุงเทพมหานครและปริมณฑล มีลักษณะเฉพาะโดยจะมีการสอบถามคัดเลือก (Screening Question) เกี่ยวกับช่วงอายุต้องอยู่ในกลุ่มวัยทำงานตอนต้นระหว่าง 20-29 ปีและกำหนดความถี่การใช้บริการที่เกี่ยวข้อง

กับธุรกรรมทางอิเล็กทรอนิกส์มากกว่า 5 ครั้งต่อเดือนในรอบ 6 เดือนที่ผ่านมา ภายหลังจากการเก็บข้อมูลจากกกลุ่มตัวอย่างในช่วงวันและเวลาข้างต้น พบกลุ่มตัวอย่างจำนวนทั้งสิ้น 434 คนที่ให้ความร่วมมือในการตอบแบบสอบถามโครงการวิจัยนี้

ทั้งนี้ผู้วิจัยได้จัดกระทำข้อมูลโดยการใช้วิธีคัดเลือกค่าสุดโต่ง (Outlier) ออกไป ซึ่งเป็นข้อมูลที่มีค่าผิดปกติ อาจมีผลต่อการวิเคราะห์ข้อมูล การตรวจสอบความเหมาะสมของข้อมูลสำหรับการวิเคราะห์ด้วยค่าสถิติให้เป็นไปตามข้อตกลงเบื้องต้น ได้แก่ การตรวจสอบการแจกแจงโค้งปกติของข้อมูล (Normality) ค่าความเบ้ (Skewness) ค่าความโด่ง (Kurtosis) ค่าระดับนัยสำคัญทางสถิติ (p-value) ของการทดสอบไคสแควร์ (χ^2) และการทดสอบความสัมพันธ์ระหว่างสองตัวแปร (Bivariate Relationship) ทำให้ได้แบบสอบถามจำนวน 418 ชุด เพื่อใช้เป็นผลการวิเคราะห์ข้อมูลในโครงการวิจัยนี้ต่อไป

3. การสร้างและตรวจสอบคุณภาพของเครื่องมือที่ใช้ในการวิจัย

สำหรับตัวแปรที่ใช้ศึกษาในงานวิจัยนี้ ประกอบด้วยตัวแปรอิสระ (ตัวแปรเชิงเหตุ) และตัวแปรตาม ดังนี้

ตัวแปรอิสระ ได้แก่

1. ตัวแปรเหตุทางสังคม จำนวน 1 ตัวแปร ได้แก่ การคล้อยตามกลุ่มอ้างอิง
2. ตัวแปรเหตุทางจิต จำนวน 10 ตัวแปร ได้แก่
   - 2.1 คุณลักษณะของระบบ
   - 2.2 การรับรู้ถึงโอกาสเสี่ยงที่บุคคลอื่นจะเข้าใช้งานแทนตน
   - 2.3 การรับรู้ถึงความรุนแรงที่บุคคลอื่นจะเข้าใช้งานแทนตน
   - 2.4 ความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล
   - 2.5 ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล
   - 2.6 ความคาดหวังในความคุ้มค่าต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคล
   - 2.7 การรับรู้ถึงประโยชน์ในการตั้งค่าการปกป้องข้อมูลส่วนบุคคล
   - 2.8 การรับรู้ถึงความง่ายในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล
   - 2.9 ทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคล
   - 2.10 ความตั้งใจในการปกป้องข้อมูลส่วนบุคคล

ตัวแปรตาม คือ พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (Privacy Data Protection Behaviors) ประกอบด้วยการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไปและการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค

ในงานวิจัยนี้ ผู้วิจัยได้กำหนดลำดับขั้นตอนย่อยของการสร้างและตรวจสอบคุณภาพของเครื่องมือที่ใช้ในการวิจัย ดังนี้

3.1 กำหนดวัตถุประสงค์ของแบบสอบถามในการทำวิจัยนี้ เกี่ยวกับปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น

3.2 ทำการศึกษาเอกสาร ทฤษฎีและงานวิจัยที่เกี่ยวข้อง เพื่อเป็นแนวทางในการสร้างแบบสอบถามปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น และมีความสอดคล้องกับนิยามเชิงปฏิบัติการ

3.3 การสร้างเครื่องมือในการวิจัย โดยทำการสร้างมาตรวัดจากตัวแปรอิสระและตัวแปรตามที่ใช้ในการศึกษางานวิจัยนี้ ในรูปแบบการกระทำ บริบทและเป้าหมายให้สอดคล้องกับนิยามเชิงปฏิบัติการ เพื่อนำไปใช้ในการเป็นแบบสอบถามสำหรับกลุ่มวัยทำงานตอนต้น โดยแต่ละข้อมีลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ตั้งแต่ “จริงที่สุด” ไปถึง “ไม่จริงเลย” และในการสร้างข้อคำถามในแต่ละตัวแปรตามนิยามเชิงปฏิบัติการ หากตัวแปรที่มีเครื่องมืออยู่แล้ว ผู้วิจัยจะนำเครื่องมือนั้นมาปรับและประยุกต์ใช้ให้เหมาะสมกับบริบทที่ได้ทำการศึกษา และหากเครื่องมือเป็นภาษาต่างประเทศ ผู้วิจัยจะทำการแปลเป็นภาษาไทยที่เหมาะสมแล้วนำเสนอต่ออาจารย์ที่ปรึกษา เพื่อขอคำแนะนำเกี่ยวกับความถูกต้อง ความเหมาะสมของภาษา ข้อคำถามและการครอบคลุมในเนื้อหา เพื่อนำมาปรับปรุงเป็นเครื่องมือฉบับร่าง

3.4 ผู้วิจัยนำแบบสอบถามที่เกี่ยวข้องกับปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้นที่สร้างขึ้นจากการศึกษาเอกสาร ทฤษฎีและงานวิจัยที่เกี่ยวข้อง เสนอให้อาจารย์ที่ปรึกษาตรวจสอบและทำการ

ปรับปรุงแก้ไขตามข้อเสนอแนะเพื่อความถูกต้อง ความสมบูรณ์ของเนื้อหาและความสอดคล้องกับนิยามเชิงปฏิบัติการ

3.5 ตรวจสอบความเที่ยงตรงเชิงเนื้อหา (Content Validity) ของแบบวัด เพื่อพิจารณาถึงความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ ความเหมาะสมของการเรียบเรียงข้อคำถามทั้งคำถามหลักและคำถามรอง โดยผ่านการตรวจสอบคุณภาพเบื้องต้นด้านความเที่ยงตรงเชิงเนื้อหาจากผู้เชี่ยวชาญด้านพฤติกรรมศาสตร์จำนวน 3 ท่าน และผู้ทรงคุณวุฒิทางด้านระบบสารสนเทศ และ/หรือเทคโนโลยีสารสนเทศ จำนวน 2 ท่าน รวมทั้งสิ้น 5 ท่าน เพื่อความครอบคลุม ความชัดเจนและความถูกต้องทางภาษาของข้อคำถาม จากนั้นนำข้อเสนอแนะของทุกท่านไปปรับปรุงแบบวัด ซึ่งผู้วิจัยใช้เกณฑ์วิธีการคำนวณค่าดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ (Index of Item Objective Congruence: IOC) โดยทุกข้อคำถามจะต้องผ่านเกณฑ์ค่าดัชนีความสอดคล้องที่มากกว่าหรือเท่ากับ 0.60 จึงจะถือว่ามีความสอดคล้องกับเนื้อหา (ดวงกมล ไตรวิจิตรคุณ, 2550; สมชาย วรกิจเกษมสกุล, 2554) รวมไปถึงการเรียบเรียงภาษาในข้อคำถามตามข้อเสนอของผู้เชี่ยวชาญเพื่อความถูกต้องและสมบูรณ์ยิ่งขึ้น

3.6 นำแบบวัดไปตรวจสอบคุณภาพของเครื่องมือ โดยการนำไปทดลองใช้ (Try-out) เพื่อทดสอบความเหมาะสมของแบบสอบถามกับกลุ่มที่มีลักษณะคล้ายคลึงกับกลุ่มตัวอย่างที่เป็นกลุ่มวัยทำงานตอนต้นจำนวน 100 คนขึ้นไป เพื่อทำการประเมินถึงความเข้าใจและความยากง่ายของคำถาม จากนั้นนำมาการวิเคราะห์หาค่าความเชื่อมั่น (Reliability) ซึ่งผู้วิจัยใช้เกณฑ์ค่าสัมประสิทธิ์อัลฟ่าของครอนบาค (Cronbach's Alpha Coefficient) โดยเกณฑ์ที่ใช้ยอมรับค่าความเชื่อมั่นคือมีค่าสัมประสิทธิ์อัลฟ่าของครอนบาคมากกว่า 0.70 (Hair et al., 2010) สำหรับการตรวจสอบความสอดคล้องภายใน (Internal Consistency) และการวิเคราะห์รายข้อ (Item Analysis) จะใช้การหาค่าสหสัมพันธ์ระหว่างคำถามแต่ละข้อกับคะแนนรวมทั้งฉบับ (Corrected Item-Total Correlation: r) หรือค่าอำนาจจำแนกของข้อคำถาม โดยใช้เกณฑ์ค่าสหสัมพันธ์ระหว่างคะแนนแต่ละข้อคำถามกับคะแนนรวมต้องมีค่าเป็นบวกและมากกว่า 0.20 ขึ้นไป

3.7 การตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้าง (Construct Validity) ของเครื่องมือวัดตัวแปรต่างๆ โดยการวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis: CFA) เพื่อทดสอบความสัมพันธ์เชิงการวัดระหว่างตัวแปรแฝง (Latent Variables) กับตัวแปรสังเกต (Observed Variables) เกณฑ์ที่ใช้ตรวจสอบความเที่ยงตรงเชิงโครงสร้าง จะพิจารณาจากแบบจำลองมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ซึ่งผู้วิจัยใช้ค่าสถิติและเกณฑ์พิจารณาในการตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง

(Goodness-of-Fit Index) ของ Byrne, (2001); Schumacker & Lomax (2004: 82) และ Hair et al. (2010) ดังตาราง 1

ตาราง 1 เกณฑ์พิจารณาตรวจสอบความเที่ยงตรงเชิงโครงสร้าง

ค่าสถิติของการตรวจสอบความกลมกลืน	เกณฑ์ระดับความสอดคล้องกลมกลืน
(1) Chi-Square test (χ^2)	ไม่มีนัยสำคัญทางสถิติ (p-value > 0.05)
(2) χ^2/df	< 2.00 มีความสอดคล้องกลมกลืนดี
	2.00-5.00 มีความสอดคล้องกลมกลืนพอใช้
(3) Comparative Fit Index (CFI)	≥ 0.95 มีความสอดคล้องกลมกลืนดี
	0.90-0.94 มีความสอดคล้องกลมกลืนพอใช้
(4) Goodness of Fit Index (GFI)	≥ 0.95 มีความสอดคล้องกลมกลืนดี
	0.90-0.94 มีความสอดคล้องกลมกลืนพอใช้
(5) Adjusted Goodness of Fit Index (AGFI)	≥ 0.95 มีความสอดคล้องกลมกลืนดี
	0.90-0.94 มีความสอดคล้องกลมกลืนพอใช้
(6) Root Mean Squared Error of Approximation	< 0.05 มีความสอดคล้องกลมกลืนดี
(RMSEA)	0.05-0.08 มีความสอดคล้องกลมกลืนพอใช้

การตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้าง ถือเป็นการประเมินความถูกต้องของแบบจำลอง มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยค่าสถิติทดสอบไคสแควร์ (Chi-Square test) จะใช้ทดสอบสมมติฐานว่าผู้วิจัยต้องการยืนยันสมมติฐานว่างหรือสมมติฐานหลัก (Null Hypothesis: H_0) หากการทดสอบไคสแควร์ไม่มีนัยสำคัญทางสถิติ (p-value > 0.05) จะบ่งชี้ว่าแบบจำลองมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ หรืออัตราส่วนระหว่างค่าสถิติทดสอบไคสแควร์ กับจำนวนองศาอิสระ (χ^2/df) ควรมีค่าน้อยกว่า 5.00 (Byrne, 2001; Schumacker & Lomax, 2004) สำหรับดัชนีวัดระดับความกลมกลืนเปรียบเทียบ (Comparative Fit Index : CFI) ดัชนีวัดระดับความกลมกลืน (Goodness of Fit Index : GFI) และดัชนีวัดระดับความกลมกลืนที่ปรับแก้ไขแล้ว (Adjusted Goodness of Fit Index : AGFI) ทั้ง 3 ดัชนีควรมีค่ามากกว่า 0.90 และค่ารากที่สองของค่าเฉลี่ยกำลังสองความคลาดเคลื่อนโดยประมาณ (Root Mean Squared Error of Approximation : RMSEA) ควรมีค่าน้อยกว่า 0.08

ทั้งนี้ หากพบว่าแบบจำลองไม่มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ หรือค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนไม่เป็นไปตามเกณฑ์ที่กำหนดไว้ ผู้วิจัยจะดำเนินการปรับแบบจำลองและวิเคราะห์ข้อมูลใหม่ภายใต้พื้นฐานของแนวคิดทฤษฎีที่เกี่ยวข้อง โดยอาศัยเหตุผลเชิงทฤษฎีและค่าดัชนีการปรับแต่งแบบจำลอง (Model Modification Indices) จนกว่าจะได้แบบจำลองที่มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ จากการศึกษาของ Schumacker & Lomax (2004: 100) เกี่ยวกับค่าสถิติไคสแควร์ (χ^2) ให้มีข้อยกเว้นว่าอาจมีนัยสำคัญทางสถิติได้ แม้ว่าแบบจำลองจะมีความความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์แล้วก็ตาม เนื่องจากขนาดของกลุ่มตัวอย่างที่มีจำนวนค่อนข้างมาก รวมทั้งผู้วิจัยได้วิเคราะห์หาความเชื่อมั่นแบบวัดและการวิเคราะห์ค่าความเที่ยงตรงในการวัด (Construct Reliability and Validity) จากการดำเนินการประเมินคุณภาพของตัวบ่งชี้ว่าตัวแปรสังเกตของตัวแปรแฝงมีความเชื่อมั่นและความเที่ยงตรงในการวัดตัวแปรแฝง ดังนี้ 1) การประเมินค่าความเชื่อมั่นของตัวแปรแฝง (Construct Reliability: CR) จากการคำนวณค่าน้ำหนักองค์ประกอบ (Indicator Loadings) ซึ่งเกณฑ์ในการพิจารณาควรมีค่ามากกว่า 0.70 และมีนัยสำคัญสำคัญทางสถิติ 0.05 หมายความว่า ตัวแปรสังเกตของตัวแปรแฝงมีความเชื่อมั่นในการวัดตัวแปรแฝงหรือตัวแปรสังเกตมีความสัมพันธ์เฉพาะกับตัวแปรแฝงในด้านที่ตัวแปรสังเกตนั้นจะวัด (Hair et al., 2010: 710) และ 2) การประเมินความตรงเชิงเหมือน (Convergent Validity) จากการคำนวณหาค่าเฉลี่ยความแปรปรวนของข้อคำถามหรือตัวชี้วัด (Average Variance Extracted: AVE) ที่ตัวแปรแฝงสามารถอธิบายได้ ซึ่งเกณฑ์ในการพิจารณาควรมีค่ามากกว่า 0.50 (Fornell & Larcker, 1981; Hair et al., 2010, p.777)

4. เครื่องมือที่ใช้ในการวิจัย

รายงานผลประเมินตรวจสอบความเหมาะสม ความตรงด้านเนื้อหา (Content Validity)

ผลการตรวจประเมินความเหมาะสมของความตรงด้านเนื้อหา สำนวนภาษา ความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ และคุณภาพของเครื่องมือวัดงานวิจัย เรื่องปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น ซึ่งผู้วิจัยได้นำเสนอเครื่องมือวัดงานวิจัยต่ออาจารย์ที่ปรึกษาและผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญ เพื่อทำการตรวจสอบความครบถ้วน ความเหมาะสมของความตรงด้านเนื้อหาของเครื่องมือวัดงานวิจัย โดยมีผู้ทรงคุณวุฒิจำนวน 5 ท่าน ได้พิจารณาเครื่องมือวัดงานวิจัย (ภาคผนวก ข รายงานผลประเมินการตรวจสอบความเหมาะสม ความตรงด้านเนื้อหา)

วิธีการและขั้นตอนการประเมินความเหมาะสมของความตรงด้านเนื้อหา

วิธีการและขั้นตอนการประเมินความเหมาะสมของความตรงด้านเนื้อหา มีดังนี้

1. ผู้วิจัยได้จัดกระทำโดยการนำนิยามเชิงปฏิบัติการ (Operational Definition) และข้อคำถามที่ได้สร้างขึ้นส่งไปยังผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญ เพื่อพิจารณาตรวจสอบความครบถ้วน ความเหมาะสมของความตรงด้านเนื้อหา สำนวนภาษา และความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ของเครื่องมือวัดงานวิจัย ซึ่งมีเกณฑ์การให้คะแนน/คะแนนการพิจารณาดังนี้

ให้คะแนน -1 หมายถึง แน่ใจว่าข้อคำถามนั้นไม่เหมาะสม/ไม่สอดคล้องกับวัตถุประสงค์

ให้คะแนน 0 หมายถึง ไม่แน่ใจว่าข้อคำถามนั้นเหมาะสม/สอดคล้องกับวัตถุประสงค์หรือไม่

ให้คะแนน +1 หมายถึง แน่ใจว่าข้อคำถามนั้นมีความเหมาะสม/สอดคล้องกับวัตถุประสงค์

นอกจากนี้ หากข้อคำถามใดที่ไม่แน่ใจหรือไม่ตรงกับนิยามเชิงปฏิบัติการ และ/หรือไม่สอดคล้องกับวัตถุประสงค์ที่ใช้ในการวิจัยนี้ สามารถแสดงความคิดเห็น โดยเขียนข้อเสนอแนะหรือแก้ไขข้อคำถามนั้นๆ ได้

2. ผู้วิจัยใช้เกณฑ์วิธีการคำนวณค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย (Index of Item - Objective Congruence: IOC) โดยทุกข้อคำถามต้องผ่านเกณฑ์ค่าดัชนีความสอดคล้องที่เท่ากับหรือมากกว่า 0.60 จึงจะถือว่ามีความสอดคล้องความตรงด้านเนื้อหา โดยการนำคะแนนที่ประเมินจากผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญ มาหาค่า IOC รายข้อ โดยใช้สูตรของ Hambleton & Rovinelli (1986) ดังนี้

จากสูตร $$IOC = \frac{\sum R}{N}$$

เมื่อ IOC คือ ค่าดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ของเครื่องมือวัด

$\sum R$ คือ ผลรวมของคะแนนจากผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญทั้งหมด

N คือ จำนวนผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญ

ทั้งนี้ รายงานผลประเมินตรวจสอบความเหมาะสม ความตรงด้านเนื้อหาของค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ในแต่ละตอนของงานวิจัยนี้ ผู้วิจัยได้จัดทำไว้ในภาคผนวก ข รายงานผลประเมินการตรวจสอบความเหมาะสม ความตรงด้านเนื้อหา สำนวนภาษา และความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ตามวัตถประสงค์ของงานวิจัย และสรุปผลประเมินตรวจสอบความเหมาะสม ความตรงด้านเนื้อหา เพื่อนำไปตรวจสอบและหาคุณภาพของเครื่องมือวัดในงานวิจัยนี้โดยนำไปทดลองใช้ (Try out) กับกลุ่มตัวอย่างที่มีลักษณะใกล้เคียงกับงานวิจัยนี้ต่อไป

รายงานผลการตรวจสอบค่าความเชื่อมั่น (Reliability) ของเครื่องมือวัดงานวิจัย

ผลการตรวจสอบประเมินคุณภาพความเที่ยง ความคงเส้นคงวา (Consistency) และความน่าเชื่อถือของเครื่องมือวัดของผลที่ได้ ถึงแม้จะมีการวัดซ้ำหรือวัดจำนวนหลายๆ ครั้งซึ่งผลที่ได้มีความคงที่ไม่เปลี่ยนแปลงไปจากเดิม รวมไปถึงเพื่อให้แน่ใจว่ากลุ่มตัวอย่างเมื่อได้อ่านในเนื้อหาจะมีความเข้าใจที่ตรงกันและสามารถตอบคำถามได้ตามความเป็นจริงทุกข้อ จากการนำเครื่องมือวัด/แบบสอบถามงานวิจัยไปทดลองใช้กับกลุ่มตัวอย่างที่มีลักษณะใกล้เคียงกับกลุ่มตัวอย่างในงานวิจัยนี้จำนวน 100 ชุด ด้วยวิธีการประมาณค่าความเชื่อมั่นแบบสอดคล้องและความสัมพันธ์ภายใน (Internal Consistency Reliability) ระหว่างข้อคำถามหรือตัวชี้วัด จากการหาค่าสัมประสิทธิ์แอลฟ่าของครอนบาค (Cronbach's Alpha Coefficient: α) เพื่อตรวจสอบความสอดคล้องของข้อคำถามในเครื่องมือวัด/แบบสอบถาม

ภายหลังจากขั้นตอนผลการประเมินความเหมาะสมของความตรงด้านเนื้อหา (Content Validity) สำนวนภาษา และความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ของผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญจำนวน 5 ท่าน ที่ได้พิจารณาเครื่องมือวัดงานวิจัย และการหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย (Index of Item - Objective Congruence: IOC) โดยทุกข้อคำถามต้องผ่านเกณฑ์ค่าดัชนีความสอดคล้องที่มากกว่าหรือเท่ากับ 0.60 จากการนำคะแนนที่ประเมินจากผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญ มาหาค่า IOC รายข้อ รวมไปถึงข้อเสนอแนะที่เป็นประโยชน์ จากการนำคำแนะนำมาปรับปรุงและประยุกต์ใช้กับเครื่องมือในงานวิจัยให้มีความเหมาะสมและมีความชัดเจนกับเนื้อหาที่ต้องการสอบถามให้มากยิ่งขึ้น ซึ่งเป็นเครื่องมืองานวิจัยที่มีการปรับปรุงแก้ไขเป็นที่เรียบร้อยแล้ว

วิธีการและขั้นตอนการตรวจสอบค่าความเชื่อมั่น (Reliability) ของเครื่องมือวัดงานวิจัย

วิธีการและขั้นตอนการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัดงานวิจัย มีดังนี้

1. การเก็บรวบรวมข้อมูลและการเตรียมข้อมูลกลุ่มทดลองใช้โดยการนำเครื่องมือวัด/แบบสอบถามงานวิจัยที่ได้ดำเนินการปรับปรุงแก้ไขเป็นที่เรียบร้อยแล้ว จากการประเมินความเหมาะสมของความตรงด้านเนื้อหา ไปหาค่าความเชื่อมั่น (Reliability) ของเครื่องมือวัด โดยจัดทำเป็นแบบสอบถามออนไลน์ เพื่อเป็นการรวบรวมข้อมูลทดลองใช้ (Try out) ในงานวิจัยนี้ตั้งแต่วันที่ 3-25 กรกฎาคม 2564 ซึ่งจัดทำแบบสอบถามออนไลน์และการเก็บรวมรวบรวมข้อมูลจากกลุ่มทดลองใช้มีลักษณะใกล้เคียงกับกลุ่มตัวอย่าง ยกเว้นเขตพื้นที่ปฏิบัติงานของงานวิจัยนี้ โดยเก็บรวมรวบข้อมูลจากกลุ่มทดลองใช้และสามารถให้ข้อมูลทดลองในงานวิจัยนี้ได้ในจังหวัดสมุทรปราการ สมุทรสาคร นครปฐม ฉะเชิงเทราและชลบุรี ซึ่งจะเห็นว่ามีเขตพื้นที่ปฏิบัติงานใกล้เคียงกับกลุ่มตัวอย่างในงานวิจัยนี้

ผลจากการเก็บรวมรวบรวมข้อมูลจากกลุ่มทดลองใช้ พบว่ากลุ่มทดลองใช้ให้ข้อมูลมาทั้งสิ้น 126 ชุด ทั้งนี้ผู้วิจัยได้คัดเลือกข้อมูลการตอบแบบสอบถามที่มีความสมบูรณ์ คัดเลือกค่าสุดโต่ง (Outlier) หรือการทิ้งดิ่งของการให้คะแนนออกไป และใช้เป็นข้อมูลทดลองใช้ของการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัดงานวิจัยนี้ จำนวนทั้งสิ้น 100 ชุด

2. การเตรียมการวิเคราะห์ข้อมูลเพื่อหาค่าความเชื่อมั่น การวิเคราะห์หาค่าความเชื่อมั่นของเครื่องมือวัด หรือวิธีการประมาณค่าความเชื่อมั่นแบบสอดคล้องและความสัมพันธ์ภายใน (Internal Consistency Reliability) ระหว่างข้อคำถามหรือตัวชี้วัด เพื่อตรวจสอบความสอดคล้องของข้อคำถามในเครื่องมือวัด งานวิจัยนี้ใช้วิธีการหาค่าสัมประสิทธิ์แอลฟ่าของครอนบาค (Cronbach's Alpha Coefficient : α) ซึ่งเป็นเครื่องมือวัดทางพฤติกรรมศาสตร์ที่นิยมโดยส่วนใหญ่และมักใช้กับระบบการให้คะแนนแบบมาตรประมาณค่า (Rating Scale) (ศรัณย์ พิมพ์ทอง, 2564) และการหาค่าความเชื่อมั่นของเครื่องมือวัด/แบบสอบถามได้ดำเนินการใช้โปรแกรมสำเร็จรูปทางสถิติ

3. เกณฑ์ที่ใช้พิจารณา ช่วงสัมประสิทธิ์ความเชื่อมั่น (Reliabilty Coefficent) คือ ค่าคะแนน 0-1 หากเข้าใกล้ 1 แสดงว่าเครื่องมือวัด/แบบสอบถามมีความน่าเชื่อถือสูง (Iacobucci & Duhachek, 2003; Taber, 2018) และหากเป็นค่าความเชื่อมั่นแบบสัมประสิทธิ์แอลฟ่าของครอนบาค ควรมีค่าตั้งแต่ 0.70 ขึ้นไปสำหรับแบบวัดจากแนวคิดที่พัฒนาขึ้นมาใหม่ จึงจะถือว่าแบบวัดนั้นๆ มีความน่าเชื่อถือได้สูง ข้อคำถามมีความสอดคล้องกันและความสัมพันธ์

ภายใน ค่าความเชื่อมั่นแบบสอดคล้องภายใน (Internal Consistency Reliability) ระหว่างข้อคำถามสูง (DeVellis & Thorpe, 2021) นอกจากนี้เกณฑ์การประเมินความเที่ยงสัมประสิทธิ์แอลฟ่าของครอนบาคของ ศิริชัย กาญจนวาสี (2556) โดยพิจารณาค่าสัมประสิทธิ์แอลฟา (α) มีการแปลความหมายระดับความเที่ยงดังนี้ มากกว่า 0.9 = ดีมาก, มากกว่า 0.8 = ดี, มากกว่า 0.7 = พอใช้, มากกว่า 0.6 = ค่อนข้างพอใช้, มากกว่า 0.5 = ต่ำ และน้อยกว่าหรือเท่ากับ 0.5 = ไม่สามารถรับได้ ซึ่งงานวิจัยนี้พิจารณาโดยใช้เกณฑ์ค่าความเชื่อมั่นแบบสัมประสิทธิ์แอลฟ่าของครอนบาค ควรมีค่ามากกว่า 0.70 ขึ้นไป รวมทั้งค่าอำนาจจำแนกของข้อคำถาม (Corrected Item-Total Correlation: r) ที่มีค่ามากกว่า 0.20 ขึ้นไป

ทั้งนี้ รายงานผลการตรวจสอบค่าความเชื่อมั่น (Reliability) ของเครื่องมือวัดงานวิจัยนี้ ผู้วิจัยได้จัดทำเป็นภาคผนวก จ รายงานผลการวิเคราะห์ข้อมูลเพื่อหาค่าความเชื่อมั่นของแต่ละแบบวัดและภาพรวมทั้งฉบับและนำผลการวิเคราะห์ข้อมูลเพื่อหาค่าความเชื่อมั่นนี้ไปเขียนในรายงานในหัวข้อเครื่องมือที่ใช้วัดตัวแปรในการวิจัยนี้ต่อไป

เครื่องมือที่ใช้ในการวิจัย

เครื่องมือในการใช้วัดตัวแปรในงานวิจัยเรื่องนี้ เป็นแบบสอบถาม (Questionnaire) เกี่ยวกับปัจจัยที่เกี่ยวข้องกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ในภาคผนวก ก เครื่องมือที่ใช้ในการวิจัย ประกอบด้วย 3 ตอนและแต่ละชุดของแบบวัดมีรายละเอียด ดังนี้

ตอนที่ 1 แบบสอบถามข้อมูลทั่วไปของผู้ตอบแบบสอบถาม เป็นข้อมูลส่วนบุคคลของกลุ่มวัยทำงานตอนต้นเป็นข้อคำถามเพื่อให้ทราบข้อมูลชีวสังคมของกลุ่มตัวอย่าง รวมทั้งสิ้น 8 ข้อคำถามประกอบด้วย คุณลักษณะเฉพาะของผู้ตอบแบบสอบถามจากการสอบถามคัดเลือก (Screening Question) ซึ่งเป็นคำถามคัดกรองเพื่อให้เป็นไปตามวัตถุประสงค์ของงานวิจัยนี้ ประกอบด้วยข้อคำถามเฉพาะเจาะจง จำนวน 2 ข้อ ได้แก่ ช่วงอายุ 20-29 ปี และความถี่ในการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ โดยเฉลี่ยมากกว่า 5 ครั้ง/เดือน ในรอบ 6 เดือนติดต่อกันที่ผ่านมา และข้อคำถามสำหรับเก็บข้อมูลพื้นฐานของผู้ตอบแบบสอบถามอีกจำนวน 6 ข้อ ได้แก่ เพศ ระดับการศึกษาสูงสุด สถานภาพสมรส เขตพื้นที่ปฏิบัติงาน ประเภทของหน่วยงาน และระดับเงินเดือนปัจจุบัน เพื่อนำข้อมูลพื้นฐานนี้มาวิเคราะห์ทางสถิติเชิงบรรยาย (Descriptive Statistics) ของลักษณะกลุ่มตัวอย่าง ซึ่งมีลักษณะคำถามที่กลุ่มตัวอย่างสามารถเลือกตอบจากคำตอบที่กำหนดไว้

ตอนที่ 2 แบบสอบถามพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ เป็นแบบสอบถามเพื่อวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งผู้วิจัยได้มาจากการทบทวนเอกสารและงานวิจัยที่เกี่ยวข้อง ศึกษาแนวทางและพัฒนาจากแบบวัดพฤติกรรมการปกป้องความเป็นส่วนตัวจากการใช้งานเครือข่ายอินเทอร์เน็ตและการพาณิชย์อิเล็กทรอนิกส์ที่เกี่ยวข้อง (Buchanan et al., 2007; Son & Kim ,2008; Youn, 2009; Büchi et al., 2016; Boerman et al., 2018) รวมไปถึงหนังสือคู่มือเกี่ยวกับการทำธุรกรรมออนไลน์ให้ปลอดภัยและสร้างสรรค์ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ องค์การมหาชน, 2561) และเอกสารการใช้ธนาคารออนไลน์ให้ปลอดภัยบนสมาร์ทโฟน (ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย, 2563) มาเป็นหลักในการวัดและพัฒนาเครื่องมือ โดยนำมาปรับใช้เป็นแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้มีความสอดคล้องและเหมาะสมในบริบทสังคมไทยและกลุ่มตัวอย่างที่เป็นกลุ่มวัยทำงานตอนต้น ตามขอบเขตเนื้อหาและนิยามปฏิบัติการของตัวแปร เป็นคำถามปลายปิด สอบถามพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ที่ให้กลุ่มตัวอย่างแสดงความคิดเห็นที่ตรงกับสภาพความเป็นจริงมากที่สุดเพียงข้อเดียว

ทั้งนี้ แต่ละแบบวัดจะเป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว เป็นการสอบถามการกระทำหรือการปฏิบัติตนเกี่ยวกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ที่ให้กลุ่มตัวอย่างแสดงความคิดเห็นตามการปฏิบัติตนที่ตรงกับสภาพความเป็นจริงมากที่สุดเพียงข้อเดียว ซึ่งเป็นแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ตามลำดับ หรือมีลักษณะมาตร 6 ระดับ ตั้งแต่ระดับ “ปฏิบัติเป็นประจำ” ถึง “ไม่เคยปฏิบัติเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกจากผู้ที่ตอบ ปฏิบัติทุกครั้งได้ 6 คะแนน ปฏิบัติเป็นประจำได้ 5 คะแนน ปฏิบัติบ่อยครั้งได้ 4 คะแนน ปฏิบัตินานๆ ครั้งได้ 3 คะแนน ปฏิบัติบางครั้งได้ 2 คะแนน และไม่เคยปฏิบัติเลยได้ 1 คะแนน ตามลำดับ สำหรับข้อความหรือคำถามทางลบผู้วิจัยให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป (General Caution) จำนวน 15 ข้อ

และการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค (Technical Protection) จำนวน 14 ข้อ

ตัวอย่างข้อคำถาม

องค์ประกอบที่ 1 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป

1. ฉันเลือกใช้รหัสผ่านที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น วัน/เดือน/ปีเกิด หมายเลขโทรศัพท์ (-)

จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. ฉันมองบุคคลรอบตัวและใช้มือปกปิดการกรอกข้อมูลระหว่างทำรายการธุรกรรมอิเล็กทรอนิกส์ (+)

จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

องค์ประกอบที่ 2 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค

1. ฉันหมั่นตรวจสอบและลบแอปพลิเคชันที่ไม่มีการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ (+)

จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. ฉันเปิดใช้ธุรกรรมทางอิเล็กทรอนิกส์ด้วยบริการวายฟายสาธารณะ (Public/Free Wi-Fi) (-)

จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การหาคุณภาพแบบวัด

ภายหลังจากการประเมินความเหมาะสมของความตรงด้านเนื้อหา และเมื่อนำไปทดลองใช้ไปเพื่อหาค่าความเชื่อมั่น (Reliability) ของเครื่องมือวัดและตรวจสอบคุณภาพรายข้อคำถาม ซึ่งจากรายงานผลการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัดงานวิจัยนี้ พบว่ามีค่าความเชื่อมั่นทั้งฉบับ 0.941 และจากการตรวจสอบโดยพิจารณาแบ่งพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์เป็น 2 องค์ประกอบ พบว่าองค์ประกอบที่ 1 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป มีค่าอำนาจจำแนกของข้อคำถาม (Corrected Item-Total Correlation: r) ระหว่าง 0.243-0.670 และค่าความเชื่อมั่นของเครื่องมือ/แบบวัด 0.730 สำหรับองค์ประกอบที่ 2 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค ค่าอำนาจจำแนกของข้อคำถาม ระหว่าง 0.231-0.609 และค่าความเชื่อมั่น ของเครื่องมือ/แบบวัด 0.719 ทั้งนี้ หากพบว่าค่าอำนาจจำแนกของข้อคำถามมีค่าต่ำกว่าเกณฑ์ที่กำหนดไว้ของงานวิจัยนี้ค่อนข้างมาก ผู้วิจัยจะพิจารณาเป็นรายข้อคำถามและตัดข้อคำถามนั้นๆ ออก ก่อนนำไปใช้ในการเก็บรวบรวมข้อมูลฉบับจริง จากการนำไปเก็บข้อมูลฉบับจริงพบค่าความเชื่อมั่นขององค์ประกอบที่ 1 เท่ากับ 0.706 และค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.208-0.784 และค่าความเชื่อมั่นขององค์ประกอบที่ 2 เท่ากับ 0.701 และค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.202-0.673

จากการวิเคราะห์และตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้าง (Construct Validity) โดยการวิเคราะห์องค์ประกอบเชิงยืนยัน เพื่อทดสอบความสัมพันธ์เชิงการวัดระหว่างตัวแปรแฝงกับตัวแปรสังเกตและพิจารณาแบบจำลองมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ซึ่งจากรายงานผลการใช้โปรแกรม LISREL เพื่อตรวจสอบคุณภาพเครื่องมือ/แบบวัด พบว่าแบบจำลองพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ทั้ง 2 องค์ประกอบยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ พิจารณาจากค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนไม่เป็นไปตามเกณฑ์ที่กำหนดไว้ ผู้วิจัยดำเนินการปรับแบบจำลองจากการตัดข้อคำถามที่มีค่าน้ำหนักขององค์ประกอบหรือแต่ละข้อถาม (Factor Loading: λ) หรือค่า Standardized Solution ที่มีค่าจำนวนน้อยประกอบกับการพิจารณาข้อคำถามที่อาจมีข้อความหรือประโยคที่ซ้ำซ้อนกับข้อคำถามอื่นๆ โดยการตัดข้อคำถามออกทีละข้อ จนกว่าแบบจำลองมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผลจากการพิจารณาค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนพบว่า องค์ประกอบที่ 1 แบบวัดการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป (General Caution)

ผ่านเกณฑ์การตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง ประกอบด้วยค่าสถิติทดสอบไคสแควร์ χ^2= 2.51, df= 5, p-value = 0.77, RMSEA = 0.000, CFI= 1.00, GFI = 1.00, AGFI = 0.99 สามารถสรุปได้ว่าแบบจำลองนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยให้ค่าน้ำหนักองค์ประกอบ (Indicator Loadings/Factor Loading: λ) หรือค่า Standardized Solution ระหว่าง 0.47-0.86 และเมื่อพิจารณาจำนวนข้อคำถามจะพบว่าจากข้อคำถามเดิมจำนวน 15 ข้อ คงเหลือข้อคำถามที่นำมาวิเคราะห์ข้อมูลจำนวน 8 ข้อ สำหรับองค์ประกอบที่ 2 แบบวัดการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค (Technical Protection) ผ่านเกณฑ์การตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง ประกอบด้วยค่าสถิติทดสอบไคสแควร์ χ^2= 7.08, df= 5, p-value = 0.21, RMSEA = 0.032, CFI= 0.99, GFI = 0.99, AGFI = 0.98 สามารถสรุปได้ว่าแบบจำลองนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยให้ค่าน้ำหนักองค์ประกอบระหว่าง 0.41-0.78 และเมื่อพิจารณาจำนวนข้อคำถามจะพบว่าจากข้อคำถามเดิมจำนวน 14 ข้อ คงเหลือข้อคำถามที่นำมาวิเคราะห์ข้อมูลจำนวน 7 ข้อ รวมทั้ง 2 องค์ประกอบเพื่อจัดทำเป็นตัวแปรแฝงพฤติกรรมการปกป้องข้อมูลส่วนบุคคล ซึ่งมีค่าน้ำหนักองค์ประกอบระหว่าง 0.43-0.84

การวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง (Composite Reliability: CR) และค่าเฉลี่ยความแปรปรวนของข้อคำถามหรือตัวชี้วัด (Average Variance Extracted: AVE)

รายงานผลการพิจารณาค่า CR, AVE

การตรวจสอบค่าความเชื่อมั่นของตัวแปรแฝง (Composite Reliability: CR) เพื่อแสดงข้อคำถามหรือตัวชี้วัดที่มีความสัมพันธ์ภายในของข้อคำถามที่ดีต่อกัน หรือเป็นการตรวจสอบดัชนีชี้วัด (Measurement Item) ตัวแปรสังเกตของตัวแปรแฝงถึงความน่าเชื่อถือและความสัมพันธ์เฉพาะของตัวชี้วัดว่าสามารถอธิบายข้อเท็จจริงของข้อคำถามนั้นมากน้อยเพียงใด ซึ่งไม่สามารถวัดค่า CR โดยตรงผ่านโปรแกรม LISREL แต่สามารถจัดการคำนวณเองได้ โดยค่า CR ที่ยอมรับได้ไม่ควรต่ำกว่า 0.70 (Hair et al., 2010)

$$CR = \frac{(\sum \lambda)^2}{(\sum \lambda)^2 - \sum(\varepsilon)}$$

เมื่อ λ คือค่าน้ำหนักของแต่ละองค์ประกอบหรือแต่ละข้อคำถาม (Factor Loading) หรือค่าสัมประสิทธิ์มาตรฐานสัมบูรณ์ของตัวชี้วัด ซึ่งได้มาจากวิธีการวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis) จากค่า Standardized Solution

ε คือค่าความคลาดเคลื่อนมาตรฐานสัมบูรณ์ของตัวชี้วัด (Error Variance) หรือ $1 - \lambda^2$

สำหรับการตรวจสอบค่าเฉลี่ยความแปรปรวนของข้อคำถามหรือตัวชี้วัด (Average Variance Extracted: AVE) ที่ตัวแปรแฝงสามารถอธิบายได้ เป็นการเปรียบเทียบค่า AVE กับความสัมพันธ์ของข้อคำถามเมื่อค่าความสัมพันธ์ยกกำลังสอง (Squared Correlations) ซึ่งเป็นการวัดค่าความเที่ยงตรงภายใน (Convergent Validity) และค่าความเที่ยงตรงเชิงจำแนก (Discriminant Validity) ของข้อคำถามหรือตัวชี้วัด โดยเป็นการตรวจสอบดัชนีชี้วัดถึงความน่าเชื่อถือของข้อคำถาม ว่าข้อคำถามหนึ่งจะสามารถอธิบายข้อเท็จจริงของข้อคำถามนั้นมากน้อยเพียงใด ซึ่งไม่สามารถวัดค่า AVE โดยตรงผ่านโปรแกรม LISREL แต่สามารถจัดการคำนวณเองได้ เช่นเดียวกับค่า CR โดยค่า AVE ที่ยอมรับไม่ควรต่ำกว่า 0.50 (Hair et al., 2010; Jöreskog, Sörbom & Du Toit, 2001) ทั้งนี้หาก ค่า AVE ต่ำกว่าเกณฑ์ 0.50 อาจใช้การพิจารณาค่าความเชื่อมั่นของตัวแปรแฝงที่มีค่ามากกว่า 0.70 หรือค่าน้ำหนักองค์ประกอบอย่างมีนัยสำคัญทางสถิติทดแทน (Hair et al., 2010, p.777; Fornell & Larcker, 1981)

$$AVE = \frac{\sum \lambda^2}{n}$$

เมื่อ λ คือค่าน้ำหนักของแต่ละองค์ประกอบหรือแต่ละข้อคำถาม (Factor Loading) หรือค่าสัมประสิทธิ์มาตรฐานสัมบูรณ์ของตัวชี้วัด ซึ่งได้มาจากวิธีการวิเคราะห์องค์ประกอบเชิงยืนยันจากค่า Standardized Solution

n คือจำนวนของตัวแปรสังเกต (Number of Observed Variables) ที่นำมาร่วมพิจารณา

ขั้นตอนการคำนวณค่าความเชื่อมั่นของตัวแปรแฝงและค่าเฉลี่ยความแปรปรวนของข้อคำถามหรือตัวชี้วัดด้วยสูตรคำนวณดังกล่าว ภายหลังจากการตรวจสอบคุณภาพเครื่องมือ/แบบวัด โดยการใช้การวิเคราะห์องค์ประกอบเชิงยืนยัน ผู้วิจัยได้นำค่าน้ำหนักองค์ประกอบของแต่ละแบบวัดมาพิจารณาค่า CR และ AVE มาคำนวณจากสูตรข้างต้น ทั้งนี้ รายงานผลการคำนวณเพื่อพิจารณาค่า CR และ AVE และนำผลการวิเคราะห์ข้อมูลนี้ไปเขียนในรายงานการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถามของแต่ละแบบวัดในการวิจัยนี้ต่อไป

ผลการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝงและค่าเฉลี่ยความแปรปรวนของข้อคำถาม ของแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลรวมทั้ง 2 องค์ประกอบ มีค่า CR = 0.782 และค่า AVE = 0.552 ซึ่งแสดงว่าข้อคำถามหรือตัวแปรสังเกตนั้นมีความน่าเชื่อถือและมีความสัมพันธ์เฉพาะกับตัวแปรแฝงหรือตัวชี้วัด

ตอนที่ 3 แบบสอบถามความรู้สึก ความคิดเห็นที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น เป็นมาตรวัดตัวแปรอิสระที่เกี่ยวข้องกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ มีจำนวนทั้งสิ้น 11 ชุด ดังนี้

ชุดที่ 1 แบบวัดการรับรู้ถึงโอกาสเสี่ยงบนธุรกรรมทางอิเล็กทรอนิกส์

ชุดที่ 2 แบบวัดการรับรู้ถึงความรุนแรงบนธุรกรรมทางอิเล็กทรอนิกส์

ชุดที่ 3 แบบวัดความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล

ชุดที่ 4 แบบวัดความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล

ชุดที่ 5 แบบวัด ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคล

ชุดที่ 6 แบบวัดคุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ชุดที่ 7 แบบวัดการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ชุดที่ 8 แบบวัดการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล

ชุดที่ 9 แบบวัดการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล

ชุดที่ 10 แบบวัดทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ชุดที่ 11 แบบวัดความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

โดยเครื่องมือ/แบบวัดทั้ง 11 ชุดมีรายละเอียดการวัด ประเภทแบบวัด การปรับใช้และพัฒนาเครื่องมือ ตัวอย่างข้อคำถามและการหาคุณภาพแบบวัด ดังนี้

ชุดที่ 1 แบบวัดการรับรู้ถึงโอกาสเสี่ยง (Perceived Vulnerability) **บนธุรกรรมทางอิเล็กทรอนิกส์** ผู้วิจัยได้ศึกษาจากแบบวัดการรับรู้ถึงโอกาสจากการถูกคุกคามความเป็นส่วนตัวออนไลน์ของ Dinev & Hart (2006); Moloney & Poti (2013); Boerman et al., (2018) และ Klein & Luciano (2016) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดการรับรู้ถึงโอกาสเสี่ยงที่บุคคลอื่นจะเข้าใช้งานแทนตนบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปร เป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว เป็นการสอบถามความรู้สึก ความคิดเห็นที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีการรับรู้ถึงโอกาสเสี่ยงที่บุคคลอื่นจะเข้าใช้งานแทนตนบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็น การรับรู้โอกาสเสี่ยงที่อาจมาจากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ จำนวน 5 ข้อ และการรับรู้โอกาสเสี่ยงจากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จำนวน 3 ข้อ รวมทั้งหมด 8 ข้อคำถาม

ตัวอย่างข้อคำถาม

การรับรู้โอกาสเสี่ยงที่อาจมาจากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์

1. ผู้ประกอบธุรกิจบริการธุรกรรมทางอิเล็กทรอนิกส์ อาจเก็บรักษาข้อมูลส่วนบุคคลของฉันไม่เหมาะสม (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. ฉันไม่มั่นใจมาตรการรักษาข้อมูลและนโยบายความเป็นส่วนตัวจากผู้ประกอบธุรกิจบริการธุรกรรมทางอิเล็กทรอนิกส์ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การรับรู้โอกาสเสี่ยงจากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์

1. การเข้าใช้งานร่วมกันหลายแอพพลิเคชัน มีโอกาสที่บุคคลอื่นนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. ฉันมีโอกาสตกเป็นผู้เคราะห์ร้าย ถูกขโมยข้อมูลส่วนบุคคลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การหาคุณภาพแบบวัด

การตรวจสอบและหาคุณภาพแบบวัดการรับรู้ถึงโอกาสเสี่ยงบนธุรกรรมทางอิเล็กทรอนิกส์ ได้ดำเนินการในลักษณะเช่นเดียวกับการตรวจสอบและหาคุณภาพของแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ดังนี้ ภายหลังจากการประเมินความเหมาะสมของความตรงด้านเนื้อหาของผู้ทรงคุณวุฒิ และหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย พบข้อคำถามที่ผ่านเกณฑ์ค่าดัชนีความสอดคล้องของงานวิจัยนี้รวมทั้งสิ้น 13 ข้อ และเป็นข้อคำถามที่ได้ดำเนินการปรับแก้ไขความชัดเจนเนื้อหา การเรียบเรียงภาษาตามข้อเสนอแนะของผู้เชี่ยวชาญและอาจารย์ที่ปรึกษาตรวจสอบเรียบร้อยแล้ว และเมื่อนำไปทดลองใช้ไปเพื่อหาค่าความเชื่อมั่น (Reliability) ของเครื่องมือวัดและตรวจสอบคุณภาพรายข้อคำถาม ซึ่งจากรายงานผลการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัดงานวิจัยนี้ พบว่ามีค่าความเชื่อมั่นของแบบวัดนี้ 0.724 และมีค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.238-0.696 ทั้งนี้ หากพบว่าค่าอำนาจจำแนกของข้อคำถามมีค่าต่ำกว่าเกณฑ์ที่กำหนดไว้ค่อนข้างมาก ผู้วิจัยจะพิจารณาเป็นรายข้อคำถามและตัดข้อคำถามนั้นๆ ออก ก่อนนำไปใช้ในการเก็บรวบรวมข้อมูลฉบับจริง จากการนำไปเก็บข้อมูลฉบับจริงพบค่าความเชื่อมั่นเท่ากับ 0.716 และค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.203-0.855

จากการวิเคราะห์และตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้าง โดยการวิเคราะห์องค์ประกอบเชิงยืนยัน จากรายงานผลการใช้โปรแกรม LISREL เพื่อตรวจสอบคุณภาพเครื่องมือ/แบบวัด พบว่าแบบจำลองการรับรู้ถึงโอกาสเสี่ยงบนธุรกรรมทางอิเล็กทรอนิกส์ยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผู้วิจัยดำเนินการปรับแบบจำลองจากการตัดข้อคำถามที่มีค่าน้ำหนักขององค์ประกอบหรือแต่ละข้อถามที่มีค่าจำนวนน้อย ประกอบกับการพิจารณาข้อคำถามที่อาจมีข้อความหรือประโยคที่ซ้ำซ้อนกับข้อคำถามอื่นๆ โดยการตัดข้อ

คำถามออกทีละข้อ จนกว่าแบบจำลองมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผลจากการพิจารณาค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนพบว่า แบบจำลองการรับรู้ถึงโอกาสเสี่ยงที่บนธุรกรรมทางอิเล็กทรอนิกส์ ผ่านเกณฑ์การตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง ประกอบด้วยค่าสถิติทดสอบไคสแควร์ χ^2 = 2.72, df= 2, p-value = 0.26, RMSEA = 0.029, CFI= 1.00, GFI = 1.00, AGFI = 0.98 สามารถสรุปได้ว่าแบบจำลองนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยให้ค่าน้ำหนักองค์ประกอบระหว่าง 0.42-0.91 และเมื่อพิจารณาจำนวนข้อคำถามจะพบว่าจากข้อคำถามเดิมจำนวน 8 ข้อ คงเหลือข้อคำถามที่นำมาวิเคราะห์ข้อมูลจำนวน 5 ข้อ

การวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถามหรือตัวชี้วัด จากรายงานผลการคำนวณเพื่อพิจารณาค่า CR และ AVE พบว่าผลการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถาม แบบวัดการรับรู้ถึงโอกาสเสี่ยงที่บนธุรกรรมทางอิเล็กทรอนิกส์ มีค่า CR = 0.751 และค่า AVE = 0.559 แสดงว่าข้อคำถามหรือตัวแปรสังเกตนั้นมีความน่าเชื่อถือและมีความสัมพันธ์เฉพาะกับตัวแปรแฝง

ชุดที่ 2 แบบวัดการรับรู้ถึงความรุนแรง (Perceived Severity) บนธุรกรรมทางอิเล็กทรอนิกส์ ผู้วิจัยได้ศึกษาจากแบบวัดการรับรู้ถึงความรุนแรงที่บุคคลภายนอกเข้ามาใช้งานแทนตนบนเครือข่ายอินเทอร์เน็ตและการใช้งานคอมพิวเตอร์ของ Woon et al., (2005); Moloney & Poti (2013); Boerman et al., (2018) และ Klein & Luciano (2016) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดการรับรู้ถึงความรุนแรงที่บุคคลอื่นจะเข้าใช้งานแทนตนบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปร เป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว เป็นการสอบถามความรู้สึก ความคิดเห็นที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีการรับรู้ถึงความรุนแรงที่บุคคลอื่นจะเข้าใช้งานแทนตนบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นการรับรู้ถึงความรุนแรงด้านทรัพย์สิน จำนวน 4 ข้อ และการรับรู้ถึงความรุนแรงด้านอันตรายที่อาจเกิดขึ้นกับตัวบุคคล จำนวน 5 ข้อ รวมทั้งหมด 9 ข้อคำถาม

ตัวอย่างข้อคำถาม

การรับรู้ถึงความรุนแรงด้านทรัพย์สิน

1. การที่บุคคลอื่นเข้าถึงข้อมูลส่วนบุคคลของฉันจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ อาจนำเงินออกจากบัญชีธนาคาร ทำให้ฉันสูญเสียรายได้ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. การลงทุนผ่านบริการธุรกรรมทางอิเล็กทรอนิกส์อาจถูกปรับเปลี่ยนแก้ไขและทำให้ฉันเข้าใช้งานธุรกรรมไม่ได้ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การรับรู้ถึงความรุนแรงด้านอันตรายที่อาจเกิดขึ้นกับตัวบุคคล

1. การที่บุคคลอื่นเข้าถึงข้อมูลส่วนบุคคลของฉันจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ทำให้ทราบถึงข้อมูลที่พักหรือสถานที่ทำงานของฉันได้ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. ฉันอาจถูกร้ายร่างกายเพื่อปกป้องทรัพย์สินที่มีค่า หากสามารถบุคคลอื่นเข้าถึงข้อมูลส่วนบุคคลของฉันจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การหาคุณภาพแบบวัด

การตรวจสอบและหาคุณภาพแบบวัดการรับรู้ถึงความรุนแรงบนธุรกรรมทางอิเล็กทรอนิกส์ ได้ดำเนินการในลักษณะเช่นเดียวกับการตรวจสอบและหาคุณภาพของแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ดังนี้ ภายหลังจากการประเมินความเหมาะสมของความตรงด้านเนื้อหาของผู้ทรงคุณวุฒิ และหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย พบข้อคำถามที่ผ่านเกณฑ์ค่าดัชนีความสอดคล้องของงานวิจัยนี้รวมทั้งสิ้น 13 ข้อ และเป็นข้อคำถามที่ได้ดำเนินการปรับแก้ไขความชัดเจนเนื้อหา การเรียบเรียงภาษาตามข้อเสนอแนะของผู้เชี่ยวชาญและอาจารย์ที่ปรึกษาตรวจสอบเรียบร้อยแล้ว และเมื่อนำไปทดลองใช้ไปเพื่อหาค่าความเชื่อมั่นของเครื่องมือวัดและตรวจสอบคุณภาพรายข้อคำถาม ซึ่งจากรายงานผลการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัด

งานวิจัยนี้ พบว่ามีค่าความเชื่อมั่นของแบบวัดนี้ 0.737 และมีค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.209-0.706 ทั้งนี้ หากพบว่าค่าอำนาจจำแนกของข้อคำถามมีค่าต่ำกว่าเกณฑ์ค่อนข้างมาก ผู้วิจัยจะพิจารณาเป็นรายข้อคำถามและตัดข้อคำถามนั้นๆ ออก ก่อนนำไปใช้ในการเก็บรวบรวมข้อมูลฉบับจริง จากการนำไปเก็บข้อมูลฉบับจริงพบค่าความเชื่อมั่นเท่ากับ 0.697 และค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.205-0.793

จากการวิเคราะห์และตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้าง โดยการวิเคราะห์องค์ประกอบเชิงยืนยัน ซึ่งจากรายงานผลการใช้โปรแกรม LISREL เพื่อตรวจสอบคุณภาพเครื่องมือ/แบบวัด พบว่าแบบจำลองการรับรู้ถึงความรุนแรงที่บนธุรกรรมทางอิเล็กทรอนิกส์ยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผู้วิจัยดำเนินการปรับแบบจำลองจากการตัดข้อคำถามที่มีค่าน้ำหนักขององค์ประกอบที่มีค่าจำนวนน้อย ประกอบกับการพิจารณาข้อคำถามที่อาจมีข้อความหรือประโยคที่ซ้ำซ้อนกับข้อคำถามอื่นๆ โดยการตัดข้อคำถามออกทีละข้อ จนกว่าแบบจำลองมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผลจากการพิจารณาค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนพบว่า แบบจำลองการรับรู้ถึงความรุนแรงบนธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วยค่าสถิติทดสอบไคสแควร์ χ^2 = 0.60, df= 2, p-value = 0.74, RMSEA = 0.000, CFI= 1.00, GFI = 1.00, AGFI = 1.00 สรุปได้ว่าแบบจำลองนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยให้ค่าน้ำหนักองค์ประกอบระหว่าง 0.43-0.78 และเมื่อพิจารณาจำนวนข้อคำถามจะพบว่าจากข้อคำถามเดิมจำนวน 9 ข้อ คงเหลือข้อคำถามที่นำมาวิเคราะห์ข้อมูลจำนวน 4 ข้อ

การวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝงและค่าเฉลี่ยความแปรปรวนของข้อคำถามหรือตัวชี้วัด จากรายงานผลการคำนวณเพื่อพิจารณาค่า CR และ AVE พบว่าผลการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถาม แบบวัดการรับรู้ถึงความรุนแรงบนธุรกรรมทางอิเล็กทรอนิกส์ มีค่า CR = 0.732 และค่า AVE = 0.524 แสดงว่าข้อคำถามหรือตัวแปรสังเกตนั้นมีความน่าเชื่อถือและมีความสัมพันธ์เฉพาะกับตัวแปรแฝงหรือตัวชี้วัด

ชุดที่ 3 แบบวัดความคาดหวังในผลลัพธ์ (Response Efficacy) **ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์** ผู้วิจัยได้ศึกษาจากแบบวัดความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องความปลอดภัยของข้อมูลในการใช้งานด้านซอฟต์แวร์ของ Workman et al. (2008) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทาง

อิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปร เป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว เป็นการสอบถามความรู้สึก ความคิดเห็นที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นความคาดหวังในผลลัพธ์ตามวิธีการปฏิบัติตนตามคำแนะนำที่ควรปฏิบัติโดยทั่วไป จำนวน 3 ข้อ และความคาดหวังในผลลัพธ์ตามวิธีการปฏิบัติตนตามคำแนะนำที่ควรปฏิบัติแบบขั้นสูง จำนวน 4 ข้อ รวมทั้งหมด 7 ข้อคำถาม

ตัวอย่างข้อคำถาม

ความคาดหวังในผลลัพธ์ตามวิธีการปฏิบัติตนตามคำแนะนำที่ควรปฏิบัติโดยทั่วไป

1. หากฉันกำหนดรหัสผ่านที่คาดเดาได้ยากบนธุรกรรมทางอิเล็กทรอนิกส์ จะทำให้บุคคลอื่นเข้าถึงข้อมูลส่วนบุคคลของฉันยากขึ้นเช่นกัน (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. การหมั่นตรวจสอบการทำรายการธุรกรรมย้อนหลัง ช่วยลดโอกาสที่บุคคลอื่นจะเข้าถึงข้อมูลส่วนบุคคลของฉันได้ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

ความคาดหวังในผลลัพธ์ตามวิธีการปฏิบัติตนตามคำแนะนำที่ควรปฏิบัติแบบขั้นสูง

1. การที่ฉันมีความรู้เกี่ยวกับการดูแลรักษาเครื่องคอมพิวเตอร์ชนิดต่างๆ มีส่วนช่วยลดโอกาสที่บุคคลอื่นจะเข้าถึงข้อมูลส่วนบุคคลของฉันได้ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. การไม่ใช้บริการวายฟายสาธารณะ (Free Wi-Fi) เช่น ภายในห้างสรรพสินค้า ร้านอาหาร ร้านกาแฟ เป็นต้น เป็นวิธีการปกป้องข้อมูลส่วนบุคคลของฉันให้ปลอดภัย (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การหาคุณภาพแบบวัด

การตรวจสอบและหาคุณภาพแบบวัดความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้ดำเนินการในลักษณะเช่นเดียวกับการตรวจสอบและหาคุณภาพของแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ดังนี้ ภายหลังจากการประเมินความเหมาะสมของความตรงด้านเนื้อหาของผู้ทรงคุณวุฒิ และหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย พบข้อคำถามที่ผ่านเกณฑ์ค่าดัชนีความสอดคล้องรวมทั้งสิ้น 12 ข้อ และเป็นข้อคำถามที่ได้ดำเนินการปรับแก้ไขความชัดเจนเนื้อหา การเรียบเรียงภาษาตามข้อเสนอแนะของผู้เชี่ยวชาญและอาจารย์ที่ปรึกษาตรวจสอบเรียบร้อยแล้ว และเมื่อนำไปทดลองใช้ไปเพื่อหาค่าความเชื่อมั่นของเครื่องมือวัดและตรวจสอบคุณภาพรายข้อคำถาม จากรายงานผลการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัด พบว่ามีค่าความเชื่อมั่นของแบบวัดนี้ 0.730 และมีค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.210-0.704 ทั้งนี้ หากพบว่าค่าอำนาจจำแนกของข้อคำถามมีค่าต่ำกว่าเกณฑ์ที่กำหนดค่อนข้างมาก ผู้วิจัยจะพิจารณาเป็นรายข้อคำถามและตัดข้อคำถามนั้นๆ ออกก่อนนำไปใช้เก็บรวบรวมข้อมูลฉบับจริง เมื่อนำไปเก็บข้อมูลจริงพบค่าความเชื่อมั่นเท่ากับ 0.702 และค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.201-0.672

ในการวิเคราะห์และตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้างโดยการวิเคราะห์องค์ประกอบเชิงยืนยัน จากรายงานผลการใช้โปรแกรม LISREL เพื่อตรวจสอบคุณภาพเครื่องมือ/แบบวัด พบว่าแบบจำลองความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผู้วิจัยดำเนินการปรับแบบจำลองจากการตัดข้อคำถามที่มีค่าน้ำหนักขององค์ประกอบหรือแต่ละข้อถามที่มีค่าจำนวนน้อย ประกอบกับการพิจารณาข้อคำถามที่อาจมีข้อความหรือประโยคที่ซ้ำซ้อนกับข้อคำถามอื่นๆ โดยการตัดข้อคำถามออกทีละข้อ ผลจากการพิจารณาค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนพบว่า แบบจำลองความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ผ่าน

เกณฑ์การตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง ประกอบด้วยค่าสถิติทดสอบไคสแควร์ χ^2= 0.72, df= 2, p-value = 0.70, RMSEA = 0.000, CFI= 1.00, GFI = 1.00, AGFI = 1.00 สามารถสรุปได้ว่าแบบจำลองนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยให้ค่าน้ำหนักองค์ประกอบระหว่าง 0.41-0.83 เมื่อพิจารณาจำนวนข้อคำถามพบว่าจากข้อคำถามเดิมจำนวน 7 ข้อ คงเหลือข้อคำถามที่นำมาวิเคราะห์ข้อมูลจำนวน 4 ข้อ

การวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝงและค่าเฉลี่ยความแปรปรวนของข้อคำถามหรือตัวชี้วัด จากรายงานผลการคำนวณ เพื่อพิจารณาค่า CR และ AVE พบว่าผลการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝงและค่าเฉลี่ยความแปรปรวนของข้อคำถาม แบบวัดความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ มีค่า CR = 0.718 และค่า AVE = 0.516 แสดงว่าข้อคำถามหรือตัวแปรสังเกตนั้นมีความน่าเชื่อถือและมีความสัมพันธ์เฉพาะกับตัวแปรแฝงหรือตัวชี้วัด

ชุดที่ 4 แบบวัดความคาดหวังความสามารถของตนเอง (Self-efficacy) ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ผู้วิจัยได้ศึกษาจากแบบวัดความคาดหวังความสามารถของตนเองทางด้านคอมพิวเตอร์และการใช้งานอินเทอร์เน็ตของ Compeau & Higgins (1995) และ Workman et al. (2008) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปร เป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว เป็นการสอบถามความรู้สึก ความคิดเห็นที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็น การมีทักษะในการใช้งานเครือข่ายคอมพิวเตอร์ จำนวน 3 ข้อ ความพร้อมในการรับมือหากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยี จำนวน 5 ข้อ และความสามารถในการควบคุมสถานการณ์หากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยีที่บุคคลอื่นอาจเข้าถึงข้อมูลส่วนบุคคล จำนวน 5 ข้อ รวมทั้งหมด 13 ข้อคำถาม

ตัวอย่างข้อคำถาม

การมีทักษะในการใช้งานเครือข่ายคอมพิวเตอร์

1. ฉันสามารถใช้เครื่องคอมพิวเตอร์เพื่อเชื่อมต่อกับบริการธุรกรรมทางอิเล็กทรอนิกส์ได้ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. ฉันปฏิบัติตามขั้นตอนการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ได้คล่องแคล่ว รวดเร็ว (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

ความพร้อมในการรับมือหากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยี

1. ฉันได้จัดทำบันทึกแผนฉุกเฉินในฉบับที่ฉันเข้าใจได้ง่าย เช่น ขั้นตอนการเปลี่ยนรหัสผ่าน การขอระงับบริการจากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. ฉันสามารถควบคุมตนเองให้ปฏิบัติตามแผนฉุกเฉินหรือแผนสำรองที่ได้ทำการบันทึกไว้ได้ เพื่อรักษาข้อมูลส่วนบุคคลให้ปลอดภัย (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

ความสามารถในการควบคุมสถานการณ์หากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยีที่บุคคลอื่นอาจเข้าถึงข้อมูลส่วนบุคคล

1. ฉันสามารถใช้สติแก้ไขปัญหาเพื่อปกป้องข้อมูลส่วนบุคคลให้ปลอดภัยจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ได้ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. หากมีบุคคลอื่นอาจเข้าถึงข้อมูลส่วนบุคคล ฉันสามารถวิเคราะห์สาเหตุและลำดับเหตุการณ์ได้ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การหาคุณภาพแบบวัด

การตรวจสอบและหาคุณภาพแบบวัดความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้ดำเนินการในลักษณะเช่นเดียวกับการตรวจสอบและหาคุณภาพของแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ภายหลังจากการประเมินความเหมาะสมของความตรงด้านเนื้อหาของผู้ทรงคุณวุฒิ และหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย พบข้อคำถามที่ผ่านเกณฑ์ค่าดัชนีความสอดคล้องรวมทั้งสิ้น 19 ข้อ และเป็นข้อคำถามที่ได้ดำเนินการปรับแก้ไขความชัดเจนเนื้อหา การเรียบเรียงภาษาตามข้อเสนอแนะของผู้เชี่ยวชาญและอาจารย์ที่ปรึกษาตรวจสอบเรียบร้อยแล้ว และเมื่อนำไปทดลองใช้ไปเพื่อหาค่าความเชื่อมั่นของเครื่องมือวัดและตรวจสอบคุณภาพรายข้อคำถาม จากรายงานผลการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัด พบว่ามีค่าความเชื่อมั่นของแบบวัดนี้ 0.754 และมีค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.215-0.727 ทั้งนี้ หากพบว่าค่าอำนาจจำแนกของข้อคำถามมีค่าต่ำกว่าเกณฑ์ที่กำหนดค่อนข้างมาก ผู้วิจัยจะพิจารณาเป็นรายข้อคำถามและตัดข้อคำถามนั้นๆ ออกก่อนนำไปใช้ในการเก็บรวบรวมข้อมูลฉบับจริง เมื่อนำไปเก็บข้อมูลจริงพบค่าความเชื่อมั่น 0.711 และค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.226-0.814

จากการวิเคราะห์และตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้าง โดยการวิเคราะห์องค์ประกอบเชิงยืน และจากรายงานผลการใช้โปรแกรม LISREL เพื่อตรวจสอบคุณภาพเครื่องมือ/แบบวัด พบว่าแบบจำลองความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผู้วิจัยดำเนินการปรับแบบจำลองจากการตัดข้อคำถามที่มีค่าน้ำหนักขององค์ประกอบหรือแต่ละข้อถามที่มีค่าจำนวนน้อย ประกอบกับการพิจารณาข้อคำถามที่อาจมีข้อความหรือประโยคที่ซ้ำซ้อนกับข้อคำถามอื่นโดยการตัดข้อคำถามออกทีละข้อ ผลจากการพิจารณาค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนพบว่า แบบจำลองความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ผ่านเกณฑ์การตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง ประกอบด้วยค่าสถิติทดสอบไคสแควร์ χ^2 = 16.15,

df= 9, p-value = 0.06, RMSEA = 0.044, CFI= 0.98, GFI = 0.99, AGFI = 0.97 สรุปได้ว่าแบบจำลองนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยให้ค่าน้ำหนักองค์ประกอบระหว่าง 0.43-0.92 และเมื่อพิจารณาจำนวนข้อคำถามจะพบว่าจากข้อคำถามเดิมจำนวน 13 ข้อ คงเหลือข้อคำถามที่นำมาวิเคราะห์ข้อมูลจำนวน 8 ข้อ

ในการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝงและค่าเฉลี่ยความแปรปรวนของข้อคำถาม จากรายงานผลการคำนวณพิจารณาค่า CR และ AVE พบว่าผลการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถาม แบบวัดความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ มีค่า CR = 0.745 และค่า AVE = 0.529 แสดงว่าตัวแปรสังเกตนั้นมีความน่าเชื่อถือและมีความสัมพันธ์เฉพาะกับตัวแปรแฝง

ชุดที่ 5 แบบวัดความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่าย (Response Costs) เพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ผู้วิจัยได้ศึกษาจากแบบวัดความคาดหวังจากต้นทุนที่จ่ายไปที่มีอิทธิพลต่อแรงจูงใจและพฤติกรรมของผู้ใช้งานอินเทอร์เน็ตในการปกป้องความเป็นส่วนตัวของ Lee et al., (2008); Boehmer et al., (2015); LeFebvre (2012) และ Ifinedo (2012) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเชิงเศรษฐศาสตร์พฤติกรรมเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปร เป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว เป็นการสอบถามความรู้สึก ความคิดเห็นที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นความคาดหวังในความคุ้มค่าของต้นทุนหรือค่าใช้จ่ายที่อยู่ในรูปตัวเงิน (Tangible Costs) จำนวน 3 ข้อ และไม่ได้อยู่ในรูปตัวเงินเพื่อปกป้องข้อมูลส่วนบุคคล (Intangible Costs) จำนวน 4 ข้อ รวมทั้งหมด 7 ข้อคำถาม

ตัวอย่างข้อคำถาม

ความคาดหวังในความคุ้มค่าของต้นทุนหรือค่าใช้จ่ายที่อยู่ในรูปตัวเงิน (Tangible Costs)

1. การสมัครเป็นสมาชิกผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ในระดับที่สูงขึ้น เช่น ระดับ VIP, Platinum เป็นต้น ทำให้ฉันได้สิทธิพิเศษและประโยชน์ในการดูแลรักษาข้อมูล (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. ฉันควบคุมค่าใช้จ่ายที่เพิ่มขึ้นในแต่ละเดือนเพื่อปกป้องข้อมูลส่วนบุคคลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ได้ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

ความคาดหวังในความคุ้มค่าของต้นทุนหรือค่าใช้จ่ายที่ไม่ได้อยู่ในรูปตัวเงิน (Intangible Costs)

1. การติดตามข่าวสาร อาชญากรรมทางอเล็กทรอนิกส์ ทำให้ฉันลดโอกาสเสี่ยงที่ข้อมูลส่วนบุคคลถูกนำไปใช้โดยไม่ได้รับอนุญาต (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. หากฉันตั้งใจศึกษาถึงวิธีการและขั้นตอนปกป้องข้อมูลส่วนบุคคล จะเพิ่มความมั่นใจและความปลอดภัยจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การหาคุณภาพแบบวัด

การตรวจสอบและหาคุณภาพแบบวัดความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้ดำเนินการในลักษณะเช่นเดียวกับการตรวจสอบและหาคุณภาพของแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่ง ภายหลังจากการประเมินความเหมาะสมของความ

ตรงด้านเนื้อหาของผู้ทรงคุณวุฒิ และหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย พบข้อคำถามที่ผ่านเกณฑ์ค่าดัชนีความสอดคล้องรวมทั้งสิ้น 12 ข้อ และเป็นข้อคำถามที่ได้ดำเนินการปรับแก้ไขความชัดเจนเนื้อหา การเรียบเรียงภาษาตามข้อเสนอแนะของผู้เชี่ยวชาญและอาจารย์ที่ปรึกษาตรวจสอบเรียบร้อยแล้ว และเมื่อนำไปทดลองใช้ไปเพื่อหาค่าความเชื่อมั่นของเครื่องมือวัด จากรายงานผลการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัด พบว่ามีค่าความเชื่อมั่นของแบบวัดนี้ 0.734 และมีค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.243-0.699 หากพบว่าค่าอำนาจจำแนกของข้อคำถามมีค่าต่ำกว่าเกณฑ์ที่ค่อนข้างมาก ผู้วิจัยจะพิจารณาเป็นรายข้อคำถามและตัดข้อคำถามนั้นๆ ออก ก่อนนำไปใช้ในการเก็บรวบรวมข้อมูลจริง จากการนำไปเก็บข้อมูลจริงพบค่าความเชื่อมั่น 0.703 และค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.206-0.765

ในการวิเคราะห์และตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้างโดยการวิเคราะห์องค์ประกอบเชิงยืนยัน ซึ่งจากรายงานผลการใช้โปรแกรม LISREL เพื่อตรวจสอบคุณภาพเครื่องมือ/แบบวัด พบว่าแบบจำลองความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผู้วิจัยดำเนินการปรับแบบจำลองจากการตัดข้อคำถามที่มีค่าน้ำหนักขององค์ประกอบหรือแต่ละข้อถามที่มีค่าจำนวนน้อย ประกอบกับการพิจารณาข้อคำถามที่อาจมีข้อความหรือประโยคที่ซ้ำซ้อนกับข้อคำถามอื่นโดยการตัดข้อคำถามออกทีละข้อ จนกว่าแบบจำลองมีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผลจากการพิจารณาค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนพบว่า ผ่านเกณฑ์การตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง ประกอบด้วยค่าสถิติทดสอบไคสแควร์ χ^2 = 3.63, df= 2, p-value = 0.16, RMSEA = 0.044, CFI= 0.99, GFI = 1.00, AGFI = 0.98 สรุปได้ว่าแบบจำลองนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยให้ค่าน้ำหนักองค์ประกอบระหว่าง 0.44-0.79 และเมื่อพิจารณาจำนวนข้อคำถามจะพบว่าจากข้อคำถามเดิมจำนวน 7 ข้อ คงเหลือข้อคำถามที่นำมาวิเคราะห์ข้อมูลจำนวน 4 ข้อ

การวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝงและค่าเฉลี่ยความแปรปรวนของข้อคำถาม จากรายงานผลการคำนวณเพื่อพิจารณาค่า CR และ AVE พบว่าผลการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถาม แบบวัดความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ มี

ค่า CR = 0.724 และค่า AVE = 0.511 แสดงว่าตัวแปรสังเกตนั้นมีความน่าเชื่อถือและมีความสัมพันธ์เฉพาะกับตัวแปรแฝง

ชุดที่ 6 แบบวัดคุณลักษณะของระบบ (System Characteristics) เพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ผู้วิจัยได้ศึกษาจากแบบวัดคุณลักษณะของระบบ รูปแบบการใช้งานภายในระบบเกี่ยวกับการทำความเข้าใจถึงวิธีการใช้งานที่มีอิทธิพลต่อการยอมรับการใช้เทคโนโลยีกับผู้ใช้งานของ Venkatesh & Davis (1996) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดคุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปร เป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว เป็นการสอบถามความรู้สึก ความคิดเห็นที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีความเข้าใจในวิธีการเข้าใช้งานคุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก ในลักษณะโดยภาพรวมของแอพพลิเคชันธุรกรรมทางเล็กทรอนิกส์เพื่อการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลที่มีอยู่ในปัจจุบัน แบ่งเป็นคุณลักษณะเด่นของระบบ (Features) จำนวน 4 ข้อ และส่วนติดต่อกับผู้ใช้งาน (User Interface) จำนวน 4 ข้อ รวมทั้งหมด 7 ข้อคำถาม

ตัวอย่างข้อคำถาม

ภาพรวมของแอพพลิเคชันธุรกรรมทางเล็กทรอนิกส์เพื่อจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลที่มีอยู่ในปัจจุบัน ด้านคุณลักษณะเด่นของระบบ (Features)

1. มีข้อมูลเนื้อหาเกี่ยวกับการตั้งค่าปกป้องข้อมูลส่วนบุคคลด้วยตนเองที่ครบถ้วนสมบูรณ์และน่าเชื่อถือ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. มีการพัฒนาให้ผู้ใช้งานการตั้งค่าปกป้องข้อมูลส่วนบุคคล โดยสามารถปรับแต่งและเข้าถึงความต้องการเฉพาะของฉันได้ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

ภาพรวมของแอพพลิเคชันธุรกรรมทางเล็กทรอนิกส์เพื่อจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลที่มีอยู่ในปัจจุบัน ด้านส่วนติดต่อกับผู้ใช้งาน (User Interface)

1. มีการออกแบบหน้าจอสวยงาม ทันสมัยและดึงดูดสายตาต่อการตั้งค่าข้อมูลส่วนบุคคล (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. ใช้การโต้ตอบกับผู้ใช้งานด้วยภาพกราฟิกเชิงสัญลักษณ์และมีปุ่มกดที่สามารถเข้าใจง่าย (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การหาคุณภาพแบบวัด

การตรวจสอบและหาคุณภาพแบบวัดคุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้ดำเนินการในลักษณะเช่นเดียวกับการตรวจสอบและหาคุณภาพของแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ภายหลังจากการประเมินความเหมาะสมของความตรงด้านเนื้อหาของผู้ทรงคุณวุฒิและหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย พบข้อคำถามที่ผ่านเกณฑ์ค่าดัชนีความสอดคล้องรวมทั้งสิ้น 12 ข้อ และเป็นข้อคำถามที่ได้ดำเนินการปรับแก้ไขความชัดเจนเนื้อหา การเรียบเรียงภาษาตามข้อเสนอแนะของผู้เชี่ยวชาญและอาจารย์ที่ปรึกษาตรวจสอบเรียบร้อยแล้ว และเมื่อนำไปทดลองใช้ไปเพื่อหาค่าความเชื่อมั่นของเครื่องมือวัดและตรวจสอบคุณภาพรายข้อคำถาม จากรายงานผลการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัดพบว่ามีค่าความเชื่อมั่นของแบบวัดนี้ 0.725 และมีค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.224-0.645 ทั้งนี้ หากพบว่าค่าอำนาจจำแนกของข้อคำถามมีค่าต่ำกว่าเกณฑ์ที่กำหนดไว้ค่อนข้างมาก ผู้วิจัยจะพิจารณาเป็นรายข้อคำถามและตัดข้อคำถามนั้นออก ก่อนนำไปใช้ในการเก็บรวบรวม

ข้อมูลจริง เมื่อนำไปเก็บข้อมูลจริงพบค่าความเชื่อมั่น 0.710 และค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.207-0.812

ในการวิเคราะห์และตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้าง โดยการวิเคราะห์องค์ประกอบเชิงยืนยัน จากรายงานผลการใช้โปรแกรม LISREL เพื่อตรวจสอบคุณภาพเครื่องมือ/แบบวัด พบว่าแบบจำลองคุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผู้วิจัยดำเนินการปรับแบบจำลองจากการตัดข้อคำถามที่มีค่าน้ำหนักขององค์ประกอบหรือแต่ละข้อถามที่มีค่าจำนวนน้อย ประกอบกับการพิจารณาข้อคำถามที่อาจมีข้อความหรือประโยคที่ซ้ำซ้อนกับข้อคำถามอื่น โดยการตัดข้อคำถามออกทีละ ผลจากการพิจารณาค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนพบว่า แบบจำลองคุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ผ่านเกณฑ์การตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง ประกอบด้วยค่าสถิติทดสอบไคสแควร์ χ^2 = 1.60, df= 2, p-value = 0.45, RMSEA = 0.000, CFI= 1.00, GFI = 1.00, AGFI = 0.99 สามารถสรุปได้ว่าแบบจำลองนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยให้ค่าน้ำหนักองค์ประกอบระหว่าง 0.46-0.93 และเมื่อพิจารณาจำนวนข้อคำถามจะพบว่าจากข้อคำถามเดิมจำนวน 7 ข้อ คงเหลือข้อคำถามที่นำมาวิเคราะห์ข้อมูลจำนวน 4 ข้อ

การวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝงและค่าเฉลี่ยความแปรปรวนของข้อคำถามหรือตัวชี้วัด จากรายงานผลการคำนวณ พิจารณาค่า CR และ AVE พบว่าผลการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถาม แบบวัดคุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มีค่า CR = 0.787 และค่า AVE = 0.530 แสดงว่าข้อคำถามหรือตัวแปรสังเกตนั้นมีความน่าเชื่อถือและมีความสัมพันธ์เฉพาะกับตัวแปรแฝง

ชุดที่ 7 แบบวัดการคล้อยตามกลุ่มอ้างอิง (Subjective Norms) ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ผู้วิจัยได้ศึกษาจากแบบวัดการคล้อยตามกลุ่มอ้างอิงในการกระทำพฤติกรรมโดยใช้แนวคิดของ Fishbein & Ajzen (1975: 73-76) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปร เป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว เป็นการสอบถามความรู้สึกความคิดเห็นที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ใน

ลักษณะแบบวัดประเภทมาตรประเมินรวมค่า มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นการคล้อยตามกลุ่มบุคคลรอบข้างที่ใกล้ชิด จำนวน 4 ข้อ และการคล้อยตามผู้ทรงอิทธิพลทางเทคโนโลยีบนสื่อสังคมออนไลน์ (IT Bloggers/ Influencers) จำนวน 5 ข้อ รวมทั้งหมด 9 ข้อคำถาม

ตัวอย่างข้อคำถาม

การคล้อยตามกลุ่มบุคคลรอบข้างที่ใกล้ชิด

1. บุคคลรอบข้างที่ฉันใกล้ชิด เช่น บุคคลในครอบครัว ญาติสนิท เพื่อสนิท เพื่อนร่วมงาน มักจะแสดงให้ฉันรู้ว่าการตั้งค่าข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ เป็นสิ่งที่มีคุณค่าและควรปฏิบัติ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. บุคคลรอบข้างที่ฉันใกล้ชิด คอยตักเตือนและแนะนำให้ฉันตั้งค่าปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ เมื่อให้ฉันละเลย ไม่ปฏิบัติตาม (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การคล้อยตามผู้ทรงอิทธิพลทางเทคโนโลยีบนสื่อสังคมออนไลน์ (IT Bloggers/ Influencers)

1. การติดตามข่าวสารจากไอทีบล็อกเกอร์ เช่น IT24hrs.com, LDA ลดา, Beartai แบไต๋ ทำให้ฉันสนใจจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. ฉันทำการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ตามที่ไอทีบล็อกเกอร์ให้ความเห็นว่าเป็นประโยชน์ทางการเงินส่วนบุคคล (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การหาคุณภาพแบบวัด

การตรวจสอบและหาคุณภาพแบบวัดการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้ดำเนินการในลักษณะเช่นเดียวกับการตรวจสอบและหาคุณภาพของแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ภายหลังจากการประเมินความเหมาะสมของความตรงด้านเนื้อหาของผู้ทรงคุณวุฒิ และหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย พบข้อคำถามที่ผ่านเกณฑ์ค่าดัชนีความสอดคล้องรวมทั้งสิ้น 13 ข้อ และเป็นข้อคำถามที่ได้ดำเนินการปรับแก้ไขความชัดเจนเนื้อหา การเรียบเรียงภาษาตามข้อเสนอแนะของผู้เชี่ยวชาญและอาจารย์ที่ปรึกษาตรวจสอบเรียบร้อยแล้ว และเมื่อนำไปทดลองใช้ ไปเพื่อหาค่าความเชื่อมั่นของเครื่องมือวัดและตรวจสอบคุณภาพรายข้อคำถาม จากรายงานผลการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัด พบว่ามีค่าความเชื่อมั่นของแบบวัดนี้ 0.721 และมีค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.228-0.688 ทั้งนี้ หากพบว่าค่าอำนาจจำแนกของข้อคำถามมีค่าต่ำกว่าเกณฑ์ที่กำหนดไว้ค่อนข้างมาก ผู้วิจัยจะพิจารณาเป็นรายข้อคำถามและตัดข้อคำถามนั้นออก ก่อนนำไปใช้ในการเก็บรวบรวมข้อมูลจริง จากการนำไปเก็บข้อมูลจริงพบค่าความเชื่อมั่น 0.718 และค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.253-0.820

ในการวิเคราะห์และตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้าง โดยการวิเคราะห์องค์ประกอบเชิงยืนยัน จากรายงานผลการใช้โปรแกรม LISREL เพื่อตรวจสอบคุณภาพเครื่องมือ/แบบวัด พบว่าแบบจำลองการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผู้วิจัยดำเนินการปรับแบบจำลองจากการตัดข้อคำถามที่มีค่าน้ำหนักขององค์ประกอบหรือแต่ละข้อถามที่มีค่าจำนวนน้อย ประกอบกับการพิจารณาข้อคำถามที่อาจมีข้อความหรือประโยคที่ซ้ำซ้อนกับข้อคำถามอื่น โดยการตัดข้อคำถามออกทีละข้อ ผลจากการพิจารณาค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนพบว่า แบบจำลองการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ผ่านเกณฑ์การตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง ประกอบด้วยค่าสถิติทดสอบไคสแควร์ χ^2 = 5.52, df= 2, p-value = 0.06,

RMSEA = 0.065, CFI= 0.98, GFI = 0.99, AGFI = 0.97 สรุปได้ว่าแบบจำลองนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ให้ค่าน้ำหนักองค์ประกอบระหว่าง 0.47-0.94 และเมื่อพิจารณาจำนวนข้อคำถามจะพบว่าจากข้อคำถามเดิมจำนวน 9 ข้อ คงเหลือข้อคำถามที่นำมาวิเคราะห์ข้อมูลจำนวน 5 ข้อ

การวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝงและค่าเฉลี่ยความแปรปรวนของข้อคำถามหรือตัวชี้วัด จากรายงานผลการคำนวณ พิจารณาค่า CR และ AVE พบว่าผลการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถาม แบบวัดการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ มีค่า CR = 0.779 และค่า AVE = 0.546 แสดงว่าข้อคำถามหรือตัวแปรสังเกตนั้นมีความน่าเชื่อถือและมีความสัมพันธ์เฉพาะกับตัวแปรแฝง

ชุดที่ 8 แบบวัดการรับรู้ถึงประโยชน์ (Perceived Usefulness) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ผู้วิจัยได้ศึกษาจากแบบวัดการรับรู้ประโยชน์ของการยอมรับการใช้เทคโนโลยี โดยใช้แนวคิดของ Davis et al. (1989: 982-1003) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปร เป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว เป็นการสอบถามความรู้สึก ความคิดเห็นที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นการก่อให้เกิดประโยชน์ต่อตนเอง (Useful) จำนวน 3 ข้อ และการเพิ่มประสิทธิผลในความปลอดภัยของข้อมูลส่วนบุคคล (Increase Productivity) จำนวน 3 ข้อ รวมทั้งหมด 6 ข้อคำถาม

ตัวอย่างข้อคำถาม

การตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ด้านการก่อให้เกิดประโยชน์ต่อตนเอง

1. การตั้งค่าปกป้องข้อมูลส่วนบุคคล ช่วยให้ฉันลดความกังวลที่บุคคลอื่นสามารถเข้าถึงข้อมูลได้ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. การตั้งค่าปกป้องข้อมูลส่วนบุคคล ช่วยให้ฉันได้เรียนรู้ เข้าใจและรักษาความเป็นส่วนตัวที่ทันกับเหตุการณ์ในปัจจุบัน (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ด้านการเพิ่มประสิทธิผลในความปลอดภัยของข้อมูล

1. การตั้งค่าปกป้องข้อมูลส่วนบุคคล ช่วยลดจำนวนการถูกโจรกรรมข้อมูลส่วนบุคคลในปัจจุบันได้ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. การตั้งค่าปกป้องข้อมูลส่วนบุคคล ช่วยรักษาระดับความปลอดภัยในข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การหาคุณภาพแบบวัด

ในการตรวจสอบและหาคุณภาพแบบวัดการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้ดำเนินการในลักษณะเช่นเดียวกับการตรวจสอบและหาคุณภาพของแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ภายหลังจากการประเมินความเหมาะสมของความตรงด้านเนื้อหาของ

ผู้ทรงคุณวุฒิ และหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย พบข้อคำถามที่ผ่านเกณฑ์ค่าดัชนีความสอดคล้องรวมทั้งสิ้น 12 ข้อ และเป็นข้อคำถามที่ได้ดำเนินการปรับแก้ไขความชัดเจนเนื้อหา การเรียบเรียงภาษาตามข้อเสนอแนะของผู้เชี่ยวชาญและอาจารย์ที่ปรึกษาตรวจสอบเรียบร้อยแล้ว และเมื่อนำไปทดลองใช้ไปเพื่อหาค่าความเชื่อมั่นของเครื่องมือวัดและตรวจสอบคุณภาพรายข้อคำถาม ซึ่งจากรายงานผลการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัดงานวิจัยนี้ พบว่ามีค่าความเชื่อมั่นของแบบวัดนี้ 0.722 และมีค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.242-0.649 หากพบว่าค่าอำนาจจำแนกของข้อคำถามมีค่าต่ำกว่าเกณฑ์ที่กำหนดไว้ค่อนข้างมาก ผู้วิจัยจะพิจารณาเป็นรายข้อคำถามและตัดข้อคำถามนั้นออก ก่อนนำไปใช้ในการเก็บรวบรวมข้อมูลจริง จากการนำไปเก็บข้อมูลจริงพบค่าความเชื่อมั่น 0.704 และค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.202-0.774

ในการวิเคราะห์และตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้าง โดยการวิเคราะห์องค์ประกอบเชิงยืนยัน ซึ่งจากรายงานผลการใช้โปรแกรม LISREL เพื่อตรวจสอบคุณภาพเครื่องมือ/แบบวัด พบว่าแบบจำลองการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผู้วิจัยดำเนินการปรับแบบจำลองจากการตัดข้อคำถามที่มีค่าน้ำหนักขององค์ประกอบหรือแต่ละข้อถามที่มีค่าจำนวนน้อย ประกอบกับการพิจารณาข้อคำถามที่อาจมีข้อความหรือประโยคที่ซ้ำซ้อนกับข้อคำถามอื่น โดยการตัดข้อคำถามออกทีละข้อ ผลจากการพิจารณาค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนพบว่า แบบจำลองการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ผ่านเกณฑ์การตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง ประกอบด้วยค่าสถิติทดสอบไคสแควร์ χ^2 = 1.41, df= 2, p-value = 0.49, RMSEA = 0.000, CFI= 1.00, GFI = 1.00, AGFI = 0.99 สรุปได้ว่าแบบจำลองนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยให้ค่าน้ำหนักองค์ประกอบระหว่าง 0.44-0.85 และเมื่อพิจารณาจำนวนข้อคำถามจะพบว่าจากข้อคำถามเดิมจำนวน 6 ข้อ คงเหลือข้อคำถามที่นำมาวิเคราะห์ข้อมูลจำนวน 4 ข้อ

การวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝงและค่าเฉลี่ยความแปรปรวนของข้อคำถามหรือตัวชี้วัด จากรายงานผลการคำนวณ พิจารณาค่า CR และ AVE พบว่าผลการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถาม แบบวัดการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ มีค่า

CR = 0.727 และค่า AVE = 0.534 แสดงว่าตัวแปรสังเกตนั้นมีความน่าเชื่อถือและมีความสัมพันธ์เฉพาะกับตัวแปรแฝง

ชุดที่ 9 แบบวัดการรับรู้ถึงความง่าย (Perceived Ease of Use) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ผู้วิจัยได้ศึกษาจากแบบวัดการรับรู้การใช้งานง่ายของการยอมรับการใช้เทคโนโลยี โดยใช้แนวคิดของ Davis et al. (1989: 982-1003) โดยนำมาปรับใช้และพัฒนาเป็นแบบวัดการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปร เป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว เป็นการสอบถามความรู้สึก ความคิดเห็นที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นความง่ายต่อการเรียนรู้ (Easy to Learn) จำนวน 3 ข้อ และความไม่ซับซ้อนของระบบในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (Simplicity) จำนวน 3 ข้อ รวมทั้งหมด 6 ข้อคำถาม

ตัวอย่างข้อคำถาม

วิธีการ/ขั้นตอนการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ด้านความง่ายต่อการเรียนรู้

1. วิธีการและการชี้แจงขั้นตอนการตั้งค่าปกป้องข้อมูล เป็นเรื่องง่ายที่จะเรียนรู้สำหรับฉัน (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. ฉันสามารถทำความเข้าใจวิธีการและขั้นตอนการตั้งค่าปกป้องข้อมูลได้ด้วยตนเอง (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

วิธีการ/ขั้นตอนการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ด้านความไม่ซับซ้อนของระบบในการจัดการตั้งค่าปกป้องข้อมูล

1. ฉันไม่ต้องใช้ความพยายามมากนัก ในการศึกษาขั้นตอนการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. หากฉันพบความยุ่งยากในการตั้งค่าปกป้องข้อมูลส่วนบุคคล ฉันสามารถขอความช่วยเหลือได้จากระบบซึ่งมีคำอธิบายที่ชัดเจน (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การหาคุณภาพแบบวัด

ในการตรวจสอบและหาคุณภาพแบบวัดการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้ดำเนินการในลักษณะเช่นเดียวกับการตรวจสอบและหาคุณภาพของแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ภายหลังจากการประเมินความเหมาะสมของความตรงด้านเนื้อหาของผู้ทรงคุณวุฒิ และหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย พบข้อคำถามที่ผ่านเกณฑ์ค่าดัชนีความสอดคล้องของงานวิจัยนี้รวมทั้งสิ้น 12 ข้อ และเป็นข้อคำถามที่ได้ดำเนินการปรับแก้ไขความชัดเจนเนื้อหา การเรียบเรียงภาษาตามข้อเสนอแนะของผู้เชี่ยวชาญและอาจารย์ที่ปรึกษาตรวจสอบเรียบร้อยแล้ว และเมื่อนำไปทดลองใช้เพื่อหาค่าความเชื่อมั่น ของเครื่องมือวัดและตรวจสอบคุณภาพรายข้อคำถาม จากรายงานผลการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัด พบว่ามีค่าความเชื่อมั่นของแบบวัด 0.837 และมีค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.329-0.740 หากพบว่าค่าอำนาจจำแนกของข้อคำถามมีค่าต่ำกว่าเกณฑ์ที่กำหนดไว้ค่อนข้างมาก ผู้วิจัยจะพิจารณาเป็นรายข้อคำถามและตัดข้อคำถามนั้นๆ ออก ก่อนนำไปใช้ในการเก็บรวบรวมข้อมูลฉบับจริง เมื่อนำไปเก็บข้อมูลจริงพบค่าความเชื่อมั่น 0.736 และค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.251-0.796

จากการวิเคราะห์และตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้าง โดยการวิเคราะห์องค์ประกอบเชิงยืนยัน ซึ่งจากรายงานผลการใช้โปรแกรม LISREL เพื่อตรวจสอบคุณภาพเครื่องมือ/แบบวัด พบว่าแบบจำลองการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิง

ประจักษ์ ผู้วิจัยดำเนินการปรับแบบจำลองจากการตัดข้อคำถามที่มีค่าน้ำหนักขององค์ประกอบหรือแต่ละข้อถามที่มีค่าจำนวนน้อย ประกอบกับการพิจารณาข้อคำถามที่อาจมีข้อความหรือประโยคที่ซ้ำซ้อนกับข้อคำถามอื่นๆ โดยการตัดข้อคำถามออกทีละข้อ ผลจากการพิจารณาค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนพบว่า แบบจำลองการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ผ่านเกณฑ์การตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง ประกอบด้วยค่าสถิติทดสอบไคสแควร์ χ^2 = 3.52, df= 2, p-value = 0.17, RMSEA = 0.043, CFI= 0.99, GFI = 1.00, AGFI = 0.98 สรุปได้ว่าแบบจำลองนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยให้ค่าน้ำหนักองค์ประกอบระหว่าง 0.50-0.86 และเมื่อพิจารณาจำนวนข้อคำถามจะพบว่าจากข้อคำถามเดิมจำนวน 6 ข้อ คงเหลือข้อคำถามที่นำมาวิเคราะห์ข้อมูลจำนวน 4 ข้อ

การวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถาม จากรายงานผลการคำนวณ เพื่อพิจารณาค่า CR และ AVE พบว่าผลการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถาม แบบวัดการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ มีค่า CR = 0.748 และค่า AVE = 0.551 แสดงว่าตัวแปรสังเกตนั้นมีความน่าเชื่อถือและมีความสัมพันธ์เฉพาะกับตัวแปรแฝง

ชุดที่ 10 แบบวัดทัศนคติ (Attitude) ที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ผู้วิจัยได้ศึกษาจากแบบวัดทัศนคติของการปฏิบัติตนตามนโยบายในการรักษาและปกป้องข้อมูลในองค์กรของนักพัฒนาแอปพลิเคชันจากงานวิจัยของ Woon & Kankanhalli (2007) และ Bulgurcu et al., (2010) โดยนำมาสร้างและพัฒนาเป็นแบบวัดทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขึ้นใหม่ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปร เป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว เป็นการสอบถามความรู้สึก ความคิดเห็นที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีทัศนคติต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก แบ่งเป็นความเชื่อในผล

ของการกระทำ (Behavioral Belief) จำนวน 4 ข้อ และการประเมินคุณค่าการกระทำในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (Evaluation of Outcome) จำนวน 4 ข้อ รวมทั้งหมด 8 ข้อคำถาม

ตัวอย่างข้อคำถาม

ความเชื่อในผลของการกระทำในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล

1. ฉันคิดว่าการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล เป็นสิ่งที่ควรประพฤติปฏิบัติตน (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. ฉันคิดว่าการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล เป็นเรื่องที่ยินดีปฏิบัติตาม (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การประเมินคุณค่าการกระทำในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล

1. การจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล ทำให้ความปลอดภัยในข้อมูลของฉันมีมากขึ้น (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. การจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล ช่วยให้ฉันได้ศึกษาความรู้ด้านเทคโนโลยีใหม่ๆ (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การหาคุณภาพแบบวัด

การตรวจสอบและหาคุณภาพแบบวัดทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้ดำเนินการในลักษณะเช่นเดียวกับการตรวจสอบและหาคุณภาพของแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ภายหลังจากการประเมินความเหมาะสมของความตรงด้านเนื้อหาของผู้ทรงคุณวุฒิ และหาค่า

ดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย พบข้อคำถามที่ผ่านเกณฑ์ค่าดัชนีความสอดคล้องรวมทั้งสิ้น 13 ข้อ และเป็นข้อคำถามที่ได้ดำเนินการปรับแก้ไขความชัดเจนเนื้อหา การเรียบเรียงภาษาตามข้อเสนอแนะของผู้เชี่ยวชาญและอาจารย์ที่ปรึกษาตรวจสอบเรียบร้อยแล้ว และเมื่อนำไปทดลองใช้เพื่อหาค่าความเชื่อมั่นของเครื่องมือวัดและตรวจสอบคุณภาพรายข้อคำถาม จากรายงานผลการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัดงานวิจัยนี้ พบว่ามีค่าความเชื่อมั่นของแบบวัดนี้ 0.753 และมีค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.212-0.674 ทั้งนี้ หากพบว่าค่าอำนาจจำแนกของข้อคำถามมีค่าต่ำกว่าเกณฑ์ที่กำหนดไว้ค่อนข้างมาก ผู้วิจัยจะพิจารณาเป็นรายข้อคำถามและตัดข้อคำถามนั้นออก ก่อนนำไปใช้ในการเก็บรวบรวมข้อมูลฉบับจริง จากการนำไปเก็บข้อมูลจริงพบค่าความเชื่อมั่น 0.688 และค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.204-0.751

ในการวิเคราะห์และตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้าง โดยการวิเคราะห์องค์ประกอบเชิงยืนยัน จากรายงานผลการใช้โปรแกรม LISREL เพื่อตรวจสอบคุณภาพเครื่องมือ/แบบวัด พบว่าแบบจำลองทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผู้วิจัยดำเนินการปรับแบบจำลองจากการตัดข้อคำถามที่มีค่าน้ำหนักขององค์ประกอบหรือแต่ละข้อถามที่มีค่าจำนวนน้อย ประกอบกับการพิจารณาข้อคำถามที่อาจมีข้อความหรือประโยคที่ซ้ำซ้อนกับข้อคำถามอื่น โดยการตัดข้อคำถามออกทีละข้อ ผลจากการพิจารณาค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนพบว่า แบบจำลองทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ผ่านเกณฑ์การตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง ประกอบด้วยค่าสถิติทดสอบไคสแควร์ χ^2= 2.34, df= 5, p-value = 0.80, RMSEA = 0.000, CFI= 1.00, GFI = 1.00, AGFI = 0.99 สรุปได้ว่าแบบจำลองนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยให้ค่าน้ำหนักองค์ประกอบระหว่าง 0.42-0.86 และเมื่อพิจารณาจำนวนข้อคำถามจะพบว่าจากข้อคำถามเดิมจำนวน 8 ข้อ คงเหลือข้อคำถามที่นำมาวิเคราะห์ข้อมูลจำนวน 5 ข้อ

ในการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถามหรือตัวชี้วัด จากรายงานผลการคำนวณพิจารณาค่า CR และ AVE พบว่าผลการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถาม แบบวัดทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ มีค่า CR = 0.733 และค่า AVE = 0.528 แสดงว่าตัวแปรสังเกตนั้นมีความน่าเชื่อถือและมีความสัมพันธ์เฉพาะกับตัวแปรแฝงหรือตัวชี้วัด

ชุดที่ 11 แบบวัดความตั้งใจ (Intention) ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ผู้วิจัยได้ศึกษาจากแบบวัดของ Foltz et al., (2016) และ Bulgurcu et al., (2010) เกี่ยวกับพฤติกรรมของผู้ใช้งานต่อการเปลี่ยนแปลงในการตั้งค่าเพื่อความปลอดภัยจากเครือข่ายสังคมออนไลน์ โดยนำมาสร้างและพัฒนาเป็นแบบวัดความตั้งใจเชิงพฤติกรรม (Behavioral Intention) ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้เป็นไปตามขอบเขตเนื้อหาและครอบคลุมกับนิยามปฏิบัติของตัวแปร เป็นคำถามแบบให้เลือกตอบเพียงคำตอบเดียว เป็นการสอบถามความรู้สึก ความคิดเห็นที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในลักษณะแบบวัดประเภทมาตรประเมินรวมค่า (Summated Rating Scale) มีมาตร 6 ระดับ ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนสำหรับข้อความทางบวกมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อความทางลบจะเป็นการให้คะแนนในทางตรงกันข้าม ทั้งนี้ กลุ่มวัยทำงานตอนต้นที่ได้คะแนนเฉลี่ยจากแบบวัดนี้มาก แสดงว่ามีความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก จำนวน 5 ข้อคำถาม

ตัวอย่างข้อคำถาม

ความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

1. ฉันตั้งใจจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล เมื่อมีโอกาสอย่างแน่นอน (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

2. ฉันมีแนวโน้มปฏิบัติตามขั้นตอนจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล (+)

.....	.....	.....	.....	.....	.....
จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย

การหาคุณภาพแบบวัด

การตรวจสอบและหาคุณภาพแบบความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้ดำเนินการในลักษณะเช่นเดียวกับการตรวจสอบและหาคุณภาพของแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์

ภายหลังจากการประเมินความเหมาะสมของความตรงด้านเนื้อหาของผู้ทรงคุณวุฒิ และหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย พบข้อคำถามที่ผ่านเกณฑ์ค่าดัชนีความสอดคล้องรวมทั้งสิ้น 8 ข้อ และเป็นข้อคำถามที่ได้ดำเนินการปรับแก้ไขความชัดเจนเนื้อหา การเรียบเรียงภาษาตามข้อเสนอแนะของผู้เชี่ยวชาญและอาจารย์ที่ปรึกษาตรวจสอบเรียบร้อยแล้ว และเมื่อนำไปทดลองใช้เพื่อหาค่าความเชื่อมั่นของเครื่องมือวัดและตรวจสอบคุณภาพรายข้อคำถาม จากรายงานผลการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัด พบว่ามีค่าความเชื่อมั่นของแบบวัดนี้ 0.847 และมีค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.350-0.756 หากพบว่าค่าอำนาจจำแนกของข้อคำถามมีค่าต่ำกว่าเกณฑ์ที่กำหนดไว้ค่อนข้างมาก ผู้วิจัยจะพิจารณาเป็นรายข้อคำถามและตัดข้อคำถามนั้น ออก ก่อนนำไปใช้ในการเก็บรวบรวมข้อมูลฉบับจริง เมื่อนำไปเก็บข้อมูลจริงพบค่าความเชื่อมั่น 0.734 และค่าอำนาจจำแนกของข้อคำถามระหว่าง 0.228-0.749

จากการวิเคราะห์และตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้าง โดยการวิเคราะห์องค์ประกอบเชิงยืนยัน จากรายงานผลการใช้โปรแกรม LISREL เพื่อตรวจสอบคุณภาพเครื่องมือ/แบบวัด พบว่าแบบจำลองความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ยังไม่สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ผู้วิจัยดำเนินการปรับแบบจำลองจากการตัดข้อคำถามที่มีค่าน้ำหนักขององค์ประกอบหรือแต่ละข้อถามที่มีค่าจำนวนน้อย ประกอบกับการพิจารณาข้อคำถามที่อาจมีข้อความหรือประโยคที่ซ้ำซ้อนกับข้อคำถามอื่น โดยการตัดข้อคำถามออกทีละข้อ ผลจากการพิจารณาค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนพบว่า แบบจำลองความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ผ่านเกณฑ์การตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง ประกอบด้วยค่าสถิติทดสอบไคสแควร์ χ^2= 1.94, df= 2, p-value = 0.38, RMSEA = 0.000, CFI= 1.00, GFI = 1.00, AGFI = 0.99 สรุปได้ว่าแบบจำลองนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยให้ค่าน้ำหนักองค์ประกอบระหว่าง 0.57-0.91 และเมื่อพิจารณาจำนวนข้อคำถามจะพบว่าจากข้อคำถามเดิมจำนวน 5 ข้อ คงเหลือข้อคำถามที่นำมาวิเคราะห์ข้อมูลจำนวน 4 ข้อ

ในการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถามหรือตัวชี้วัด จากรายงานผลการคำนวณ พิจารณาค่า CR และ AVE พบว่าผลการวิเคราะห์ค่าความเชื่อมั่นของตัวแปรแฝง และค่าเฉลี่ยความแปรปรวนของข้อคำถาม แบบวัดความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ มีค่า CR = 0.804 และค่า AVE

= 0.618 แสดงว่าตัวแปรสังเกตนั้นมีความน่าเชื่อถือและมีความสัมพันธ์เฉพาะกับตัวแปรแฝงหรือตัวชี้วัด

5. การเก็บรวบรวมข้อมูล การจัดกระทำและการวิเคราะห์ข้อมูล

การเก็บรวบรวมข้อมูลและการจัดกระทำข้อมูล

ภายหลังจากได้รับหนังสือรับรองจากบัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ การพิจารณาจริยธรรมสำหรับโครงการวิจัยที่ทำในมนุษย์หมายเลข SWUEC-G-299/2563X (ภาคผนวก ค หนังสือรับรองจริยธรรมในงานวิจัย) และหนังสือขอความร่วมมือในการเก็บรวบรวมข้อมูล (ภาคผนวก ง หนังสือขอความอนุเคราะห์เก็บข้อมูลเพื่อการวิจัย) สำหรับขอความอนุเคราะห์เก็บข้อมูลเพื่อการวิจัยตั้งแต่เดือนสิงหาคม 2564 ถึงเดือนตุลาคม 2564 ผู้วิจัยนำหนังสือขอความอนุเคราะห์เก็บข้อมูลเพื่อการวิจัย ตามวิธีการ ขั้นตอนและเขตพื้นที่การสุ่มกลุ่มตัวอย่างแบบกลุ่ม 2 ขั้นตอน(Two-stage Cluster Sampling) ของงานวิจัยนี้ ไปติดต่อหน่วยงานทั้งภาครัฐและเอกชนที่ได้รับอนุญาตและให้ความร่วมมือสำหรับการเก็บรวบรวมข้อมูลในกลุ่มวัยทำงานตอนต้น ทั้งนี้ผู้วิจัยได้แนะนำตัว อธิบายวัตถุประสงค์และชี้แจงรายละเอียดงานวิจัยนี้ และประสานงานกับผู้บริหาร เจ้าหน้าที่เกี่ยวข้องและกลุ่มตัวอย่างเพื่อนัดหมายช่วงวันและเวลาที่สามารถเก็บรวบรวมข้อมูลได้ รวมทั้งการติดตามแบบสอบถามความก้าวหน้าในการตอบแบบสอบถามออนไลน์จากกลุ่มตัวอย่าง

การเก็บข้อมูลจากกกลุ่มตัวอย่างในช่วงวันและเวลาข้างต้น พบกลุ่มตัวอย่างจำนวน 434 คนที่ให้ความร่วมมือในการตอบแบบสอบถามโครงการวิจัยนี้ ทั้งนี้ในการตรวจสอบความสมบูรณ์ของแบบสอบถาม ผู้วิจัยได้จัดกระทำข้อมูลโดยการใช้วิธีคัดเลือกค่าสุดโต่ง (Outlier) ออกไป ซึ่งเป็นข้อมูลที่มีค่าผิดปกติ อาจมีผลต่อการวิเคราะห์ข้อมูล การตรวจสอบความเหมาะสมของข้อมูลสำหรับการวิเคราะห์ด้วยค่าสถิติให้เป็นไปตามข้อตกลงเบื้องต้น ได้แก่ การตรวจสอบการแจกแจงโค้งปกติของข้อมูล (Normality) ค่าความเบ้ (Skewness) ค่าความโด่ง (Kurtosis) ค่านัยสำคัญทางสถิติ (p-value) ของการทดสอบไคสแควร์ (χ^2) และการทดสอบความสัมพันธ์ระหว่างสองตัวแปร (Bivariate Relationship) ทำให้ได้แบบสอบถามจำนวน 418 ชุด รวมไปถึงการให้คะแนน การลงรหัส และการบันทึกข้อมูลในโปรแกรมสำเร็จรูปทางสถิติ เพื่อใช้เป็นผลการวิเคราะห์ข้อมูลในโครงการวิจัยนี้ต่อไป

การวิเคราะห์ข้อมูล

ภายหลังการเก็บรวบรวมข้อมูลและจัดกระทำข้อมูลเพื่อตรวจสอบถูกต้องและความสมบูรณ์ของแบบสอบถาม และการนำโปรแกรมสำเร็จรูปทางสถิติมาช่วยประมวลผลข้อมูล ในงานวิจัยนี้ผู้วิจัยแบ่งการวิเคราะห์ข้อมูล ดังนี้

1. การวิเคราะห์ข้อมูลทั่วไปของกลุ่มตัวอย่างและค่าสถิติพื้นฐาน เป็นการวิเคราะห์ข้อมูลโดยใช้สถิติเชิงบรรยาย (Descriptive Statistics) อธิบายข้อมูลลักษณะทั่วไปของผู้ตอบแบบสอบถามและการแจกแจงของตัวแปร ประกอบด้วย ความถี่ (Frequency) ค่าร้อยละ (Percentage) ค่าเฉลี่ยเลขคณิต (Mean) และส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation)

2. การตรวจสอบข้อตกลงเบื้องต้นของการวิเคราะห์แบบจำลองโครงสร้างความสัมพันธ์เชิงเหตุ ประกอบด้วย ระดับนัยสำคัญทางสถิติ (p-value) ของค่าความเบ้ (Skewness) และความโด่ง (Kurtosis) ระดับนัยสำคัญทางสถิติของการทดสอบไคสแควร์ (Chi-Square Test) ของความเบ้และความโด่ง (Skewness & Kurtosis) และการแจกแจงปกติของข้อมูล (Normal Distribution) ของตัวแปรสังเกต (Observed Variables) ที่นำมาศึกษาจากการรวมกลุ่มตัวแปรรายด้านของแต่ละข้อคำถาม หากตัวแปรสังเกตที่นำมาศึกษาในงานวิจัยนี้ไม่มีระดับนัยสำคัญทางสถิติ ($p > 0.05$) แสดงว่าตัวแปรสังเกตมีลักษณะการแจกแจงข้อมูลแบบโค้งปกติ

3. การศึกษาความสัมพันธ์ระหว่างตัวแปรสังเกตเกี่ยวกับการไม่เกิดปัญหาภาวะร่วมเส้นตรงพหุ (Multicollinearity) ใช้การตรวจสอบค่าสัมประสิทธิ์สหสัมพันธ์ของเพียร์สัน (Pearson's Product-Moment Correlation Coefficient: r) ซึ่งผู้วิจัยใช้เกณฑ์การไม่เกิดปัญหาภาวะร่วมเส้นตรงพหุ จากการพิจารณาค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปร $r \leq 0.85$ (Kline, 2010) ซึ่งเป็นเกณฑ์เหมาะสมสำหรับวิเคราะห์ข้อมูลที่จะนำไปใช้ในการวิเคราะห์รูปแบบความสัมพันธ์เชิงเหตุต่อไป

4. ศึกษารูปแบบความสัมพันธ์เชิงเหตุของตัวแปรอิสระที่มีอิทธิพลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ โดยใช้โปรแกรมสำเร็จรูปทางสถิติทำการตรวจสอบความสอดคล้องกลมกลืนระหว่างแบบจำลองตามสมมติฐานกับข้อมูลเชิงประจักษ์ (Goodness of Fit Measures) ซึ่งเป็นการวิเคราะห์องค์ประกอบเชิงยืนยันตามแนวคิดของ Schumacker & Lomax (2004) และ Hair et al., (2010) จากการคำนวณค่าสัมประสิทธิ์การทำนาย (Coefficient of Determination: R^2) และค่าสัมประสิทธิ์ความถูกต้องของการทำนายที่ปรับแล้ว ($R^2{}_{adj}$) หากมีค่าสัมประสิทธิ์สูง แสดงว่าแบบจำลองที่นำมาศึกษามีสอดคล้อง

กลมกลืนกับข้อมูลเชิงประจักษ์ และมีคุณภาพและหากมีค่าตั้งแต่ 0.75 ขึ้นไปแสดงว่าแบบจำลองมีคุณภาพสูง

5. การวิเคราะห์อิทธิพลเชิงเหตุหรือการวิเคราะห์เส้นทาง (Path Analysis) เพื่อศึกษาความสัมพันธ์เชิงเหตุ การตรวจสอบความสอดคล้องกลมกลืนระหว่างแบบจำลองตามสมมติฐานกับข้อมูลเชิงประจักษ์ การวิเคราะห์อิทธิพลทางตรง (Direct Effect) อิทธิพลทางอ้อม (Indirect Effect) และอิทธิพลรวม (Total Effect) ของตัวแปรเชิงเหตุ ผู้วิจัยใช้การประมาณค่าพารามิเตอร์ของแบบจำลอง (Parameter Estimation) ด้วยวิธีความน่าจะเป็นสูงสุด (Maximum Likelihood : ML) จากการคำนวณค่าสัมประสิทธิ์อิทธิพล (Path Coefficient: β) ควรมีค่าไม่น้อยกว่า 0.10 และมีนัยสำคัญทางสถิติ 0.05 (Hair et al., 2010)

6. การพิจารณาตรวจสอบระดับความสอดคล้องกลมกลืนของแบบจำลองกับข้อมูลเชิงประจักษ์ ซึ่งผู้วิจัยใช้ค่าสถิติและเกณฑ์พิจารณาในการตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง (Goodness-of-Fit Index) ของ Byrne, (2001); Schumacker & Lomax (2004: 82) และ Hair et al. (2010) แบ่งออกเป็น ส่วนที่ 1 การพิจารณาระดับความสอดคล้องกลมกลืนของแบบจำลองเชิงสัมบูรณ์ (Measure of Absolute Fit) ได้แก่ค่า p-value, χ^2/df, ค่ารากที่สองของค่าเฉลี่ยกำลังสองความคลาดเคลื่อนโดยประมาณ (Root Mean Squared Error of Approximation: RMSEA) และค่ารากที่สองของค่าเฉลี่ยกำลังสองของส่วนที่เหลือ (Standard Root Mean Squared Residual: SRMR) และส่วนที่ 2 การพิจารณาระดับความสอดคล้องกลมกลืนของแบบจำลองเชิงเปรียบเทียบ (Comparative Fit Index/Increment Fit Measure) ได้แก่ ค่าดัชนีวัดระดับความกลมกลืนแบบไม่อิงเกณฑ์ (Non-normed Fit Index: NNFI หรือ Tucker-Lewis Index: TLI), ดัชนีวัดระดับความกลมกลืนเปรียบเทียบ (Comparative Fit Index: CFI) และดัชนีวัดระดับความกลมกลืน (Goodness of Fit Index: GFI) ดังตาราง 2

ตาราง 2 เกณฑ์พิจารณาตรวจสอบระดับความสอดคล้องกลมกลืนของแบบจำลองกับข้อมูลเชิงประจักษ์

ค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืน	เกณฑ์ระดับความสอดคล้องกลมกลืน
Measure of Absolute Fit	
(1) Chi-Square test (χ^2)	ไม่มีนัยสำคัญทางสถิติ (p-value > 0.05)
(2) χ^2/df	< 2.00 มีความสอดคล้องกลมกลืนดี
	2.00-5.00 มีความสอดคล้องกลมกลืนพอใช้
(3) Root Mean Squared Error of Approximation (RMSEA)	< 0.05 มีความสอดคล้องกลมกลืนดี
	0.05-0.08 มีความสอดคล้องกลมกลืนพอใช้
(4) Standard Root Mean Squared Residual (SRMR)	< 0.05 มีความสอดคล้องกลมกลืนดี
	0.05-0.08 มีความสอดคล้องกลมกลืนพอใช้
Comparative Fit Index	
(5) Non-normed Fit Index: NNFI	$\geq$ 0.95 มีความสอดคล้องกลมกลืนดี
	0.90-0.94 มีความสอดคล้องกลมกลืนพอใช้
(6) Comparative Fit Index (CFI)	$\geq$ 0.95 มีความสอดคล้องกลมกลืนดี
	0.90-0.94 มีความสอดคล้องกลมกลืนพอใช้
(7) Goodness of Fit Index (GFI)	$\geq$ 0.95 มีความสอดคล้องกลมกลืนดี
	0.90-0.94 มีความสอดคล้องกลมกลืนพอใช้

7. การปรับแบบจำลอง หากพบว่าแบบจำลองไม่มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ หรือค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนไม่เป็นไปตามเกณฑ์ที่กำหนดไว้ ผู้วิจัยจะดำเนินการปรับแบบจำลองและวิเคราะห์ข้อมูลใหม่ภายใต้พื้นฐานของแนวคิดทฤษฎีที่เกี่ยวข้อง โดยอาศัยเหตุผลเชิงทฤษฎีและรายงานผลค่าดัชนีการปรับแต่งแบบจำลอง (Model Modification Indices) จนกว่าจะได้แบบจำลองที่มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ จากการศึกษาของ Schumacker & Lomax (2004: 100) เกี่ยวกับค่าสถิติไคสแควร์ (χ^2) ให้มีข้อยกเว้นว่าอาจมีนัยสำคัญทางสถิติได้ แม้ว่าแบบจำลองจะมีความความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์แล้วก็ตาม เนื่องจากขนาดของกลุ่มตัวอย่างที่มีจำนวนค่อนข้างมาก

บทที่ 4
ผลการวิเคราะห์ข้อมูล

การวิจัยเรื่อง ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น แบ่งตัวแปรที่ศึกษาออกเป็นตัวแปรสังเกต (Observed Variable) จำนวน 24 ตัวแปร ตัวแปรแฝงภายนอก (Exogenous Variables) จำนวน 7 ตัวแปร ประกอบด้วย การรับรู้ถึงโอกาสเสี่ยง การรับรู้ถึงความรุนแรง ความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคล การคล้อยตามกลุ่มอ้างอิง และคุณลักษณะของระบบ และตัวแปรแฝงภายใน (Endogenous Variables) จำนวน 5 ตัวแปร ประกอบด้วย การรับรู้ถึงประโยชน์ในการตั้งค่าการปกป้องข้อมูลส่วนบุคคล การรับรู้ถึงความง่ายในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล ทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคล ความตั้งใจในการปกป้องข้อมูลส่วนบุคคล และพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (Privacy Data Protection Behaviors) ซึ่งผู้วิจัยแบ่งการนำเสนอผลการวิเคราะห์ข้อมูล ดังนี้

1. การกำหนดสัญลักษณ์และอักษรย่อที่ใช้ในการวิเคราะห์ข้อมูล
2. ลักษณะข้อมูลทั่วไปของผู้ตอบแบบสอบถาม/กลุ่มตัวอย่าง
3. ผลการวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรที่ใช้ในการศึกษา
4. ผลการวิเคราะห์แบบจำลองโครงสร้างความสัมพันธ์เชิงเหตุ
5. ผลการวิเคราะห์ข้อมูลเพื่อทดสอบสมมติฐานการวิจัย

1. การกำหนดสัญลักษณ์และอักษรย่อที่ใช้ในการวิเคราะห์ข้อมูล

ผู้วิจัยกำหนดสัญลักษณ์ และความหมายที่ใช้ในการวิเคราะห์ข้อมูล เพื่อให้เกิดความเข้าใจตรงกันและใช้ในการแปลผลตัวแปรของงานวิจัย ดังนี้

สัญลักษณ์	English	ความหมาย
n	Numbers	ขนาด/จำนวนของกลุ่มตัวอย่าง
$\bar{x}$	X-bar/Mean	ค่าเฉลี่ยเลขคณิต
SD	Standard Deviation	ส่วนเบี่ยงเบนมาตรฐาน
Sk	Skewness	ค่าความเบ้
Ku	Kurtosis	ค่าความโด่ง
SE	Standard Error	ค่าความคลาดเคลื่อนมาตรฐาน
r	Pearson's Product Moment Correlation Coefficient	ค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สัน
χ^2	Chi-Square	ค่าสถิติไคสแควร์
p	p-value	ค่านัยสำคัญทางสถิติ
df	Degree of Freedom	ค่าองศาความเป็นอิสระ
RMSEA	Root Mean Squared Error of Approximation	ค่ารากที่สองของค่าเฉลี่ยกำลังสองความคลาดเคลื่อนโดยประมาณ
SRMR	Standard Root Mean Squared Residual	ค่ารากที่สองของค่าเฉลี่ยกำลังสองของส่วนที่เหลือ
NNFI/TLI	Non-normed Fit Index/ Tucker-Lewis Index	ค่าดัชนีวัดระดับความกลมกลืนแบบไม่อิงเกณฑ์
CFI	Comparative Fit Index	ค่าดัชนีวัดระดับความกลมกลืนเปรียบเทียบ
GFI	Goodness of Fit Index	ค่าดัชนีวัดระดับความกลมกลืนสอดคล้อง
DE	Direct Effect	อิทธิพลทางตรง
IE	Indirect Effect	อิทธิพลทางอ้อม
TE	Total Effect	อิทธิพลรวม
β	Path Coefficient	ค่าสัมประสิทธิ์อิทธิพล

สำหรับการวิเคราะห์แบบจำลองโครงสร้างความสัมพันธ์เชิงเหตุ ปัจจัยทางจิตวิทยาและสังคมที่มีอิทธิพลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น ผู้วิจัยกำหนดอักษรย่อเพื่อใช้แทนตัวแปร ดังนี้

ตัวแปรแฝง	อักษรย่อ	ตัวแปรสังเกต	อักษรย่อ
พฤติกรรมการปกป้องข้อมูลส่วนบุคคล (Privacy Data Protection Behaviors)	PDPB	การปกป้องข้อมูลส่วนบุคคลทั่วไป	General
		การปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค	Tecnica
การรับรู้ถึงโอกาสเสี่ยงที่บุคคลอื่นเข้าใช้งานแทนตน (Perceived Vulnerability)	VULN	จากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์	VUL1
		จากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์	VUL2
การรับรู้ถึงความรุนแรงบุคคลอื่นเข้าใช้งานแทนตน (Perceived Severity)	SEVE	ด้านทรัพย์สิน/ข้อมูลทางการเงินออนไลน์	SEV1
		ด้านร่างกาย/อันตรายที่อาจเกิดขึ้นกับตัวบุคคล	SEV2
ความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล (Response Efficacy)	EFFI	ตามคำแนะนำที่ควรปฏิบัติโดยทั่วไป	EFF1
		ตามคำแนะนำที่ควรปฏิบัติแบบขั้นสูง	EFF2
ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล (Self-Efficacy)	SELF	การมีทักษะในการใช้งานเครือข่ายคอมพิวเตอร์	SELF1
		ความพร้อมในการรับมือภัยคุกคามด้านเทคโนโลยี	SELF2
		ความสามารถควบคุมสถานการณ์หากเกิดปัญหา	SELF3
ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคล (Response Cost)	COST	ต้นทุนหรือค่าใช้จ่ายที่อยู่ในรูปตัวเงิน/งบประมาณ	COST1
		ต้นทุนหรือค่าใช้จ่ายที่ไม่ได้อยู่ในรูปตัวเงิน	COST2
คุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคล (System Characteristics)	SYST	ด้านคุณลักษณะเด่นของระบบ (Features)	SYS1
		ส่วนติดต่อกับผู้ใช้งาน (User Interface)	SYS2
การคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคล (Subjective Norms)	SUBJ	ตามกลุ่มบุคคลรอบข้างที่ใกล้ชิด	SUB1
		ตามผู้ทรงอิทธิพลทางเทคโนโลยี (Influencers)	SUB2
การรับรู้ประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล (Perceived Usefulness)	USEF	การก่อให้เกิดประโยชน์ต่อตนเอง	USE1
		การเพิ่มประสิทธิผลในความปลอดภัยของข้อมูล	USE2
การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล (Perceived Ease of Use)	EASE	ความง่ายต่อการเรียนรู้ด้วยตนเอง	EASE1
		ความไม่ซับซ้อนของระบบ	EASE2
ทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (Attitude)	ATTI	ความเชื่อในผลของการกระทำ	ATT1
		การประเมินคุณค่าของการกระทำ	ATT2
ความตั้งใจในการปกป้องข้อมูลส่วนบุคคล (Intention)	INTN	ความตั้งใจในการปกป้องข้อมูลส่วนบุคคล	INT1

2. ลักษณะข้อมูลทั่วไปของผู้ตอบแบบสอบถาม/กลุ่มตัวอย่าง

กลุ่มตัวอย่างที่ใช้ในการวิจัยนี้เป็นกลุ่มวัยทำงานตอนต้นในเขตกรุงเทพมหานครและปริมณฑล จำนวนตัวอย่าง 418 คน สรุปเป็นตารางลักษณะข้อมูลทั่วไปของผู้ตอบแบบสอบถาม (n= 418) ได้ดังตาราง 3 ดังนี้

ตาราง 3 จำนวนและร้อยละของผู้ตอบแบบสอบถามจำแนกตามคุณลักษณะ

ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม		จำนวน/ความถี่	ร้อยละ (%)
อายุ	21	7	1.70
	22	17	4.10
	23	27	6.50
	24	62	14.80
	25	77	18.40
	26	59	14.10
	27	67	16.00
	28	60	14.40
	29	42	10.00
ความถี่ในการใช้บริการฯ	โดยเฉลี่ย 11-15 ครั้ง/เดือน	46	11.00
	โดยเฉลี่ย มากกว่า 15 ครั้ง/เดือน	372	89.00
เพศ	ชาย	130	31.10
	หญิง	255	61.00
	เพศทางเลือก	33	7.90
ระดับการศึกษาสูงสุด	ต่ำกว่าปริญญาตรี	36	8.60
	ปริญญาตรี	373	89.20
	ปริญญาโทหรือสูงกว่า	9	2.20
สถานภาพสมรส	โสด	316	75.60
	สมรส	23	5.50
	หย่าร้าง	8	1.90
	อยู่ร่วมกันโดยไม่ได้แต่งงาน	71	17.00
เขตพื้นที่ปฏิบัติงาน	กรุงเทพมหานคร	263	62.90
	นนทบุรี	122	29.20
	ปทุมธานี	33	7.90

ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม		จำนวน/ความถี่	ร้อยละ (%)
ประเภทหน่วยงาน	ราชการ/รัฐวิสาหกิจ	75	17.90
	องค์กรธุรกิจเอกชน	343	82.10
ระดับเงินเดือนปัจจุบัน	น้อยกว่าหรือเท่ากับ 15,000 บาท	26	6.20
	15,001-20,000 บาท	216	51.70
	20,001-25,000 บาท	130	31.10
	25,001-30,000 บาท	46	11.00

จากตาราง 3 ลักษณะข้อมูลทั่วไปของกลุ่มตัวอย่าง จำนวน 418 คน พบว่าโดยส่วนใหญ่ผู้ตอบแบบสอบถามมีอายุ 25 ปี (จำนวน 77 คน คิดเป็นร้อยละ 18.40) และรองลงมามีอายุ 27 ปี (จำนวน 67 คน คิดเป็นร้อยละ 16.00) และอายุ 24 ปี (จำนวน 62 คน คิดเป็นร้อยละ 14.80) ตามลำดับ ซึ่งคิดเป็นอายุเฉลี่ยเท่ากับ 25.83 ปี ส่วนใหญ่มีความถี่ในการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ โดยเฉลี่ยมากกว่า 15 ครั้ง/เดือน (จำนวน 372 คน คิดเป็นร้อยละ 89.00) เป็นกลุ่มวัยทำงานตอนต้นเพศหญิง (จำนวน 255 คน คิดเป็นร้อยละ 61.00) รองลงมาคือเพศชาย ร้อยละ 31.10 มีระดับการศึกษาสูงสุดในระดับปริญญาตรี (จำนวน 373 คน คิดเป็นร้อยละ 89.20) รองลงมาคือต่ำกว่าปริญญาตรี ร้อยละ 8.60 ซึ่งมีสถานภาพโสด (จำนวน 316 คน คิดเป็นร้อยละ 75.60) รองลงมาคืออยู่ร่วมกันโดยไม่ได้แต่งงาน ร้อยละ 17.00 สำหรับพื้นที่การปฏิบัติงานอยู่ในเขตกรุงเทพมหานคร (จำนวน 263 คน คิดเป็นร้อยละ 62.90) รองลงมาคือนนทบุรี ร้อยละ 29.20 โดยหน่วยงานส่วนใหญ่เป็นองค์กรธุรกิจเอกชน (จำนวน 343 คน คิดเป็นร้อยละ 82.10) รวมทั้งกลุ่มวัยทำงานตอนต้นจะมีระดับเงินเดือนปัจจุบันระหว่าง 15,001-20,000 บาท (จำนวน 216 คน คิดเป็นร้อยละ 51.70) รองลงมาคือระดับเงินเดือน 20,001-25,000 บาท ร้อยละ 31.10

3. ผลการวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรที่ใช้ในการศึกษา

ภายหลังจากขั้นตอนการตรวจสอบคุณภาพเครื่องมือด้านความเที่ยงตรงเชิงโครงสร้าง (Construct Validity) ของเครื่องมือวัดตัวแปร โดยการวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis) เพื่อทดสอบความสัมพันธ์เชิงการวัดระหว่างตัวแปรแฝง (Latent Variables) กับตัวแปรสังเกต (Observed Variables) ผู้วิจัยได้รวมกลุ่มตัวแปรหรือข้อคำถาม (Compute Variables) โดยจัดทำเป็นค่าเฉลี่ยเลขคณิตเพื่อนำไปสร้างเป็นตัวแปรสังเกตของแต่ละองค์ประกอบสำหรับการวิเคราะห์องค์ประกอบ รวมทั้งสิ้น 24 ตัวแปรสังเกต จากนั้นนำตัวแปรสังเกตไปตรวจสอบข้อตกลงเบื้องต้น (Assumption) ของการวิเคราะห์แบบจำลองโครงสร้างความสัมพันธ์เชิงเหตุ ดังนี้

ลักษณะการแจกแจงปกติของข้อมูล (Normal Distribution) ของตัวแปรสังเกต

การวิเคราะห์ข้อมูลสำหรับการตรวจสอบลักษณะการแจกแจงข้อมูลของตัวแปรสังเกต ใช้การพิจารณาค่าเฉลี่ยเลขคณิต ส่วนเบี่ยงเบนมาตรฐาน ค่าความเบ้ (Skewness) ค่าความโด่ง (Kurtosis) ค่าระดับนัยสำคัญทางสถิติ (p-value) ของการทดสอบไคสแควร์ (χ^2) ของความเบ้และความโด่ง (Skewness & Kurtosis) จากการใช้โปรแกรม LISREL (Linear Structural Relations) เพื่อตรวจสอบการแจกแจงของข้อมูลให้เป็นไปตามข้อตกลงเบื้องต้น (Assumption) ของการวิเคราะห์แบบจำลองโครงสร้างความสัมพันธ์เชิงเหตุ ซึ่งเป็นการตรวจสอบการแจกแจงปกติของค่าต่อเนื่อง (Test of Univariate Normality for Continuous Variables) จากการปรับข้อมูล (Transform) ให้เป็นค่าคะแนนมาตรฐาน (Z-Score) เสียก่อนแล้วจึงนำมาตรวจสอบการแจกแจงลักษณะของข้อมูล หากผลการตรวจสอบไม่มีค่านัยสำคัญทางสถิติ ($p > 0.05$) แสดงว่าตัวแปรที่ใช้ในการวิจัยมีลักษณะการแจกแจงของข้อมูลเป็นโค้งปกติ (Joreskog et al., 2016) ผลการวิเคราะห์ข้อมูลแสดงในตาราง 4

ตาราง 4 ค่าสถิติทดสอบสำหรับการตรวจสอบลักษณะการแจกแจงข้อมูลแบบโค้งปกติของตัวแปรสังเกต

ตัวแปรสังเกต	$\bar{x}$	SD	Skewness		Kurtosis		Skewness & Kurtosis	
			Z-Score	p-value	Z-Score	p-value	Chi-Square	p-value
พฤติกรรมการปกป้องข้อมูลส่วนบุคคลฯ (PDPB)								
- การปฏิบัติตนในข้อควรระวังทั่วไป (General)	3.746	0.890	-1.665	0.096	-0.394	0.694	2.927	0.231
- การปฏิบัติตนเชิงเทคนิค (Technical)	3.755	0.865	1.209	0.227	-0.143	0.886	1.482	0.477
การรับรู้โอกาสเสี่ยงที่บุคคลอื่นเข้าใช้งาน (VULN)								
- จากผู้ให้บริการธุรกรรมฯ (VUL1)	3.678	0.990	-0.658	0.510	-1.675	0.093	5.309	0.091
- จากการเข้าใช้บริการธุรกรรมฯ (VUL2)	3.679	1.075	-1.672	0.095	-1.649	0.099	5.315	0.093
การรับรู้ความรุนแรงที่บุคคลอื่นข้าใช้งาน (SEVE)								
- ด้านทรัพย์สิน (SEV1)	3.708	1.062	-1.752	0.080	-1.552	0.121	5.278	0.125
- ด้านตัวบุคคล (SEV2)	3.652	1.083	-0.301	0.764	-2.041	0.065	5.113	0.178
ความคาดหวังในผลลัพธ์การปฏิบัติตามฯ (EFFI)								
- การปฏิบัติตามโดยทั่วไป (EFF1)	3.687	1.069	-1.313	0.189	-1.874	0.061	5.136	0.173
- การปฏิบัติตามแบบขั้นสูง EFF2)	3.605	0.996	-1.629	0.103	-0.757	0.449	3.225	0.199
ความคาดหวังความสามารถตนเองฯ (SELF)								
- การใช้งานเครือข่ายคอมพิวเตอร์ (SELF1)	3.743	1.038	0.052	0.982	-1.934	0.093	3.740	0.154
- ความพร้อมในการรับมือกับปัญหา (SELF2)	3.586	1.023	-0.053	0.958	-2.047	0.079	5.210	0.096
- ความสามารถควบคุมสถานการณ์ (SELF3)	3.714	1.065	-1.294	0.196	-1.478	0.139	3.859	0.145
ความคาดหวังในความคุ้มค่าต้นทุนฯ (COST)								
- ในรูปตัวเงิน (COST1)	3.853	1.055	-1.518	0.129	-1.378	0.168	4.203	0.122
- ไม่ใช่ในรูปตัวเงิน (COST2)	3.736	0.968	-0.907	0.364	-1.947	0.059	4.612	0.100
คุณลักษณะของระบบเพื่อปกป้องข้อมูลฯ (SYST)								
- คุณลักษณะเด่น (SYS1)	3.664	1.128	-0.156	0.876	-1.178	0.129	4.467	0.106
- ส่วนติดต่อกับผู้ใช้งาน (SYS2)	3.535	1.026	-0.807	0.420	-2.034	0.080	4.674	0.097
การคล้อยตามกลุ่มอ้างอิงปกป้องข้อมูล (SUBJ)								
- บุคคลรอบข้างที่ใกล้ชิด (SUB1)	3.952	1.098	-1.564	0.118	-1.419	0.156	4.460	0.108
- ผู้ทรงอิทธิพลทางเทคโนโลยี (SUB2)	3.778	0.864	-0.705	0.481	-1.830	0.067	3.847	0.146
การรับรู้ประโยชน์ในการตั้งค่าปกป้องฯ (USEF)								
- การก่อประโยชน์ต่อตนเอง (USE1)	3.641	1.052	-1.142	0.253	-1.921	0.058	4.596	0.099
- การเพิ่มประสิทธิผลความปลอดภัย (USE2)	3.766	1.044	-0.137	0.891	-1.188	0.235	1.431	0.489

ตาราง 4 (ต่อ)

การรับรู้ถึงความง่ายในการตั้งค่าปกป้องฯ (EASE)								
- ความง่ายต่อการเรียนรู้ (EASE1)	3.785	1.046	-1.927	0.054	0.121	0.904	3.727	0.155
- ความไม่ซับซ้อนของระบบ (EASE2)	3.843	0.934	-0.747	0.455	-1.109	0.267	1.789	0.409
ทัศนคติมีต่อการปกป้องข้อมูลส่วนบุคคล (ATTI)								
- ความเชื่อผลของการกระทำ (ATT1)	3.731	0.936	-1.950	0.051	-0.488	0.626	4.039	0.133
- การประเมินคุณค่าของการกระทำ (ATT2)	3.719	0.960	-0.777	0.437	-1.081	0.280	1.772	0.412
ความตั้งใจในการปกป้องข้อมูลส่วนบุคคล (INTN)								
- ความตั้งใจในการปกป้องข้อมูลส่วนบุคคล (INT1)	3.686	0.824	-0.463	0.643	-0.418	0.676	0.389	0.823

จากตาราง 4 เมื่อพิจารณาค่าระดับนัยสำคัญทางสถิติ (p-value) ของความเบ้ (Skewness) ความโด่ง (Kurtosis) และค่าระดับนัยสำคัญทางสถิติของการทดสอบไคสแควร์ (χ^2) ของความเบ้และความโด่ง (Skewness & Kurtosis) พบว่าตัวแปรสังเกตที่นำมาศึกษาในงานวิจัยนี้ทุกตัวไม่มีค่าระดับนัยสำคัญทางสถิติ ($p > 0.05$) ซึ่งมีค่าระหว่าง 0.091 - 0.823 นั่นหมายความว่าการแจกแจงลักษณะข้อมูลของตัวแปรสังเกต มีการแจกแจงลักษณะของข้อมูลเป็นโค้งปกติ เป็นไปตามข้อตกลงเบื้องต้นของการวิเคราะห์แบบจำลองโครงสร้างความสัมพันธ์เชิงเหตุ นอกจากนี้ เมื่อพิจารณาค่าสถิติทดสอบสำหรับการตรวจสอบลักษณะการแจกแจงข้อมูลแบบโค้งปกติของแต่ละตัวแปรสังเกต มีลักษณะดังนี้

ตัวแปรสังเกตของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ พบว่าการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป (General Caution) มีค่าเฉลี่ยเลขคณิต เท่ากับ 3.746 ค่าระดับนัยสำคัญทางสถิติของการทดสอบไคสแควร์ของความเบ้และความโด่ง (Skewness & Kurtosis) เท่ากับ 0.231 ซึ่งมีค่าความเบ้ทางลบ (-1.665) นั่นหมายความว่ากลุ่มตัวอย่างโดยส่วนใหญ่มีคะแนนการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไปสูงกว่าค่าเฉลี่ยเลขคณิต ($\bar{x}$ < Mode) และค่าความโด่งทางลบ (-0.394) หมายความว่ารูปร่างลักษณะการแจกแจงข้อมูลมีความโด่งน้อย (Platykurtic) กว่าลักษณะการแจกแจงของข้อมูลแบบโค้งปกติ ส่วนการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค (Technical Protection) อิเล็กทรอนิกส์ พบว่าการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค มีค่าเฉลี่ยเลขคณิต เท่ากับ 3.755 ค่าระดับนัยสำคัญทางสถิติของการทดสอบไคสแควร์ของความเบ้และความโด่ง (Skewness & Kurtosis)

เท่ากับ 0.477 ซึ่งมีค่าความเบ้ทางบวก (1.209) นั่นหมายความว่ากลุ่มตัวอย่างโดยส่วนใหญ่มีคะแนนการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิคต่ำกว่าค่าเฉลี่ยเลขคณิต (Mode < $\bar{x}$) และค่าความโด่งทางลบ (-0.143) หมายความว่ารูปร่างลักษณะการแจกแจงข้อมูลมีความโด่งน้อย (Platykurtic) กว่าลักษณะการแจกแจงของข้อมูลแบบโค้งปกติ

ตัวแปรเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ พบว่าทุกตัวแปรสังเกต ผ่านเกณฑ์การแจกแจงลักษณะของข้อมูลเป็นโค้งปกติ โดยมีค่าระดับนัยสำคัญทางสถิติของการทดสอบไคสแควร์ของความเบ้และความโด่ง (Skewness & Kurtosis) ระหว่าง 0.091 - 0.823 และพบว่ามีค่าความเบ้ทางลบ นั่นหมายความว่ากลุ่มตัวอย่างโดยส่วนใหญ่มีคะแนนแต่ละตัวแปรสังเกตสูงกว่าค่าเฉลี่ยเลขคณิต ($\bar{x}$ < Mode) ยกเว้นตัวแปรสังเกตของความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ด้านการมีทักษะในการใช้งานเครือข่ายคอมพิวเตอร์ที่มีค่าความเบ้ทางบวก (0.052) นั่นหมายความว่ากลุ่มตัวอย่างโดยส่วนใหญ่มีคะแนนแต่ละตัวแปรสังเกตการมีทักษะในการใช้งานเครือข่ายคอมพิวเตอร์ต่ำกว่ากว่าค่าเฉลี่ยเลขคณิต (Mode < $\bar{x}$) สำหรับค่าความโด่ง พบว่าทุกตัวแปรเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์มีค่าความโด่งทางลบ หมายความว่ารูปร่างลักษณะการแจกแจงข้อมูลมีความโด่งน้อย (Platykurtic) กว่าลักษณะการแจกแจงของข้อมูลแบบโค้งปกติ ยกเว้นตัวแปรสังเกตการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ด้านความง่ายต่อการเรียนรู้มีค่าความโด่งทางบวก (0.121) หมายความว่ารูปร่างลักษณะการแจกแจงข้อมูลมีความโด่งมาก (Leptokurtic) กว่าลักษณะการแจกแจงของข้อมูลแบบโค้งปกติ

การตรวจสอบความสัมพันธ์ระหว่าง 2 ตัวแปร (Bivariate Relationship)

ผู้วิจัยใช้ค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สัน (Pearson's Product Moment Correlation Coefficient: r) ทำการตรวจสอบและวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรสังเกต ดังตาราง 5

ตาราง 5 แสดงค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรสังเกต

Variables	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1. General	1																							
2. Technica	.755**	1																						
3. VUL1	.576**	.492**	1																					
4. VUL2	.694**	.635**	.499**	1																				
5. SEV1	.551**	.522**	.307**	.334**	1																			
6. SEV2	.506**	.629**	.520**	.623**	.388**	1																		
7. EFF1	.598**	.554**	.415**	.446**	.359**	.647**	1																	
8. EFF2	.678**	.491**	.579**	.408**	.630**	.426**	.351**	1																
9. SELF1	.654**	.735**	.366**	.372**	.386**	.353**	.391**	.362**	1															
10. SELF2	.542**	.583**	.505**	.388**	.454**	.406**	.373**	.565**	.332**	1														
11. SELF3	.658**	.762**	.534**	.740**	.387**	.755**	.559**	.411**	.437**	.409**	1													
12. COST1	.708**	.735**	.578**	.563**	.359**	.543**	.593**	.402**	.628**	.387**	.738**	1												
13. COST2	.729**	.594**	.708**	.450**	.566**	.499**	.477**	.777**	.405**	.712**	.493**	.527**	1											
14. SYS1	.585**	.598**	.586**	.532**	.417**	.724**	.647**	.473**	.360**	.436**	.632**	.624**	.554**	1										
15. SYS2	.511**	.399**	.523**	.361**	.426**	.395**	.341**	.584**	.289**	.707**	.374**	.376**	.696**	.410**	1									
16. SUB1	.671**	.725**	.738**	.603**	.485**	.678**	.604**	.548**	.484**	.522**	.729**	.780**	.688**	.787**	.492**	1								
17. SUB2	.343**	.163**	.569**	.202**	.152**	.240**	.155**	.443**	.102*	.353**	.225**	.234**	.573**	.250**	.423**	.210**	1							
18. USE1	.520**	.530**	.475**	.481**	.272**	.458**	.420**	.346**	.287**	.353**	.579**	.603**	.441**	.702**	.304**	.440**	.242**	1						
19. USE2	.573**	.624**	.459**	.435**	.533**	.474**	.421**	.496**	.489**	.524**	.489**	.666**	.631**	.521**	.455**	.688**	.063**	.694**	1					
20. EASE1	.076	.113*	.122*	.045	.016	.102*	.078	.048	.060	.097*	.099*	.100*	.071	.099*	.026	.140**	.076**	.087	.167**	1				
21. EASE2	.246**	.278**	.215**	.244**	.196**	.296**	.249**	.165**	.143**	.226**	.309**	.273**	.249**	.328**	.158**	.384**	.247**	.250**	.283**	.423**	1			
22. ATT1	.071	.170	.158**	.117	.050	.276	.048	.065	.108	.105*	.084	.094	.124*	.194	.063	.136**	.400**	.131**	.148**	.406**	.342**	1		
23. ATT2	.173**	.177**	.186**	.100*	.166**	.201**	.166**	.159**	.094	.155**	.201**	.159**	.176**	.181**	.087	.267**	.231**	.126**	.193**	.620**	.613**	.488**	1	
24. INT1	.745**	.722**	.759**	.691**	.587**	.673**	.601**	.592**	.410**	.438**	.545**	.688**	.718**	.655**	.508**	.745**	.427**	.534**	.531**	.092	.295**	.106*	.193**	1

.Correlation is significant at the 0.01 level (2-tailed). (มีระดับนัยสำคัญทางสถิติ 0.01)

.Correlation is significant at the 0.05 level (2-tailed). (มีระดับนัยสำคัญทางสถิติ 0.05)

จากตาราง 5 แสดงการวิเคราะห์ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรสังเกต โดยใช้การตรวจสอบค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สัน (Pearson's Product Moment Correlation Coefficient: r) พบว่าความสัมพันธ์ระหว่าง 2 ตัวแปรสังเกตทุกตัวมีค่าความสัมพันธ์เชิงบวก (Positive Correlation) ซึ่งโดยส่วนใหญ่มีระดับนัยสำคัญทางสถิติ 0.01 และไม่พบค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรสังเกตที่มีค่าสูงเกิน 0.85 ซึ่งอาจทำให้เกิดปัญหาภาวะร่วมเส้นตรงเชิงพหุ (Multicollinearity) และทำให้การประมาณค่าพารามิเตอร์เกิดความคลาดเคลื่อน (Kline, 2010) เมื่อนำข้อมูลไปใช้ในการวิเคราะห์แบบจำลองโครงสร้างความสัมพันธ์เชิงเหตุ

ผลการวิเคราะห์ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรสังเกต พบว่าค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรสังเกตที่มีความความสัมพันธ์เชิงบวกและมีระดับนัยสำคัญทางสถิติอยู่ระหว่าง 0.097 ถึง 0.787 ซึ่งความสัมพันธ์ระหว่าง 2 ตัวแปรสังเกตที่มีความสัมพันธ์เชิงบวกกันมากที่สุด 3 อันดับแรก ได้แก่ คุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคลด้านคุณลักษณะเด่นของระบบ (SYS1) กับการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลด้านการคล้อยตามกลุ่มบุคคลรอบข้างที่ใกล้ชิด (SUB1) (r = 0.787) การคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลด้านการคล้อยตามกลุ่มบุคคลรอบข้างที่ใกล้ชิด (SUB1) กับความคาดหวังในความคุ้มค่าของต้นทุน ค่าใช้จ่ายเพื่อการปกป้องข้อมูลด้านงบประมาณ ในรูปตัวเงิน (COST1) (r = 0.780) และความคาดหวังในความคุ้มค่าของต้นทุน ค่าใช้จ่ายเพื่อการปกป้องข้อมูลที่ไม่ได้อยู่ในรูปตัวเงิน (COST2) กับความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลแบบขั้นสูง (EFF2) (r = 0.777) ตามลำดับ สำหรับค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรสังเกตที่มีความความสัมพันธ์เชิงบวกและมีระดับนัยสำคัญทางสถิติน้อยที่สุด 3 อันดับแรก ได้แก่ การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ด้านความง่ายต่อการเรียนรู้ (EASE1) กับความคาดหวังในความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลจากความสามารถด้านความพร้อมในการรับมือหากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยี (SELF2) (r = 0.097) การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ด้านความง่ายต่อการเรียนรู้ (EASE1) กับความคาดหวังในความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลจากความสามารถในการควบคุมสถานการณ์หากเกิดปัญหาภัยคุกคามด้านเทคโนโลยี (SELF3) (r = 0.099) และการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ด้านความง่ายต่อการเรียนรู้ (EASE1) กับคุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคลด้านคุณลักษณะเด่นของระบบ (SYS1) (r = 0.099) ตามลำดับ

นอกจากนี้ พบว่าค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรสังเกตที่มีความความสัมพันธ์เชิงบวกและไม่มีระดับนัยสำคัญทางสถิติที่มีค่าน้อยที่สุด 3 อันดับแรก ได้แก่ การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ด้านความง่ายต่อการเรียนรู้ (EASE1) กับการรับรู้ถึงความรุนแรงที่บุคคลอื่นจะเข้าใช้งานแทนตนบนธุรกรรมทางอิเล็กทรอนิกส์ด้านทรัพย์สิน (SEV1) (r = 0.016) การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ด้านความง่ายต่อการเรียนรู้ (EASE1) กับการรับรู้ถึงความรุนแรงที่บุคคลอื่นจะเข้าใช้งานแทนตนบนธุรกรรมทางอิเล็กทรอนิกส์ด้านร่างกาย อันตรายที่อาจเกิดขึ้นกับตัวบุคคล (VUL2) (r = 0.045) และการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ด้านความง่ายต่อการเรียนรู้ (EASE1) กับความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลแบบขั้นสูง (EFF2) (r = 0.048) ตามลำดับ

รวมทั้ง ในการตรวจสอบความตรงเชิงจำแนก (Discriminant Validity) ผู้วิจัยดำเนินการโดยใช้ผลการวิเคราะห์เปรียบเทียบค่ารากที่ 2 ของค่าเฉลี่ยความแปรปรวนของตัวชี้วัด ($\sqrt{AVE}$) ของค่าสหสัมพันธ์แต่ละโครงสร้างหรือตัวแปรแฝง จากแนวคิด Fornell & Larcker (1981) เกี่ยวกับการเปรียบเทียบค่ารากที่ 2 ของค่าเฉลี่ยความแปรปรวนของตัวชี้วัดกับความสัมพันธ์ระหว่างองค์ประกอบ ผลจากการศึกษาพบว่า ค่ารากที่ 2 ของค่าเฉลี่ยความแปรปรวนของตัวชี้วัดในแต่ละแถวตามแนวทแยงมุมมีค่าสูงกว่าค่าสหสัมพันธ์ของตัวแปรแฝงอื่นๆ (Cross construct correlation) ทั้งในแนวตั้งและแนวนอน ซึ่งมีค่าอยู่ระหว่าง 0.695-0.736 กล่าวได้ว่าแบบจำลองมีความตรงเชิงจำแนก สามารถนำไปใช้ในการวิเคราะห์แบบจำลองสมการเชิงโครงสร้างต่อไปได้

4. ผลการวิเคราะห์แบบจำลองโครงสร้างความสัมพันธ์เชิงเหตุ

การพิจารณาตรวจสอบระดับความสอดคล้องกลมกลืนของแบบจำลองกับข้อมูลเชิงประจักษ์ ซึ่งผู้วิจัยใช้ค่าสถิติทดสอบและเกณฑ์พิจารณาในการตรวจสอบความสอดคล้องกลมกลืนของแบบจำลอง (Goodness-of-Fit Index) ของ Byrne, (2001); Schumacker & Lomax (2004) และ Hair et al. (2010) การวิเคราะห์อิทธิพลทางตรง (Direct Effect) อิทธิพลทางอ้อม (Indirect Effect) และอิทธิพลรวม (Total Effect) ของตัวแปรเชิงเหตุจากการประมาณค่าพารามิเตอร์ของแบบจำลอง (Parameter Estimation) ด้วยวิธีความน่าจะเป็นสูงสุด (Maximum Likelihood: ML) ทั้งนี้ หากพบว่าแบบจำลองไม่มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ หรือค่าสถิติของการตรวจสอบความสอดคล้องกลมกลืนไม่เป็นไปตามเกณฑ์ที่

กำหนดไว้ ผู้วิจัยดำเนินการปรับแบบจำลองและวิเคราะห์ข้อมูลใหม่ภายใต้พื้นฐานของแนวคิดทฤษฎีที่เกี่ยวข้อง โดยอาศัยเหตุผลเชิงทฤษฎีและรายงานผลค่าดัชนีการปรับแต่งแบบจำลอง (Model Modification Indices) จนกว่าจะได้แบบจำลองที่มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ซึ่งเป็นรายงานผลการวิเคราะห์ข้อมูลในแต่ละครั้ง

จากการพิจารณาตรวจสอบระดับความสอดคล้องกลมกลืนของแบบจำลองกับข้อมูลเชิงประจักษ์ โดยตรวจสอบความสัมพันธ์เชิงเส้นตรงระหว่างตัวแปรของแบบจำลองที่ได้พัฒนาขึ้นจากแนวคิดทฤษฎีว่ามีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ โดยการพิจารณาค่าดัชนีความสอดคล้องกลมกลืน (Goodness-of-Fit Index) ซึ่งรายงานผลการใช้โปรแกรม LISREL การตรวจสอบระดับความสอดคล้องกลมกลืนของแบบจำลอง พบว่าค่าดัชนีวัดระดับความสอดคล้องกลมกลืนของแบบจำลองเชิงสัมบูรณ์ (Measure of Absolute Fit) มีค่า p-value = 0.000, χ^2= 1,803.44, df= 218, ค่ารากที่สองของค่าเฉลี่ยกำลังสองความคลาดเคลื่อนโดยประมาณ (Root Mean Squared Error of Approximation: RMSEA) เท่ากับ 0.139 และค่ารากที่สองของค่าเฉลี่ยกำลังสองของส่วนที่เหลือ (Standard Root Mean Squared Residual: SRMR) เท่ากับ 0.089 สำหรับกลุ่มค่าดัชนีวัดระดับความสอดคล้องกลมกลืนของแบบจำลองเชิงเปรียบเทียบ (Comparative Fit Index/Increment Fit Measure) มีค่าระดับความกลมกลืนแบบไม่อิงเกณฑ์ (Non-normed Fit Index: NNFI หรือ Tucker-Lewis Index: TLI) เท่ากับ 0.88 , ดัชนีวัดระดับความกลมกลืนเปรียบเทียบ (Comparative Fit Index: CFI) เท่ากับ 0.90 และดัชนีวัดระดับความกลมกลืน (Goodness of Fit Index: GFI) เท่ากับ 0.75 เมื่อนำไปตรวจสอบจากเกณฑ์พิจารณาตรวจสอบระดับความสอดคล้องกลมกลืนของแบบจำลองกับข้อมูลเชิงประจักษ์ (ตาราง 6) สามารถวิเคราะห์ข้อมูลได้ว่าแบบจำลองยังไม่มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ในเกณฑ์หรือระดับที่สามารถยอมรับได้ จำเป็นต้องดำเนินการปรับแบบจำลองความสัมพันธ์ให้สอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์

แนวทางการปรับแบบจำลองความสัมพันธ์ ซึ่งผลจากการพิจารณาตรวจสอบระดับความสอดคล้องกลมกลืนของแบบจำลองกับข้อมูลเชิงประจักษ์ในครั้งแรก แบบจำลองยังไม่มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ในเกณฑ์หรือระดับที่สามารถยอมรับได้ และค่าดัชนีต่างๆ ของระดับความสอดคล้องกลมกลืนแบบจำลองนั้นมีค่าเข้าใกล้เกณฑ์ความสอดคล้องกลมกลืนพอใช้ (Fair) ดังนั้น ผู้วิจัยทำการพิจารณาการปรับแบบจำลองจากการยินยอมให้ความคลาดเคลื่อนในการวัดตัวแปรสังเกตของตัวแปรแฝง (Latent Variables) มีความสัมพันธ์กัน โดยศึกษาจากรายงานผลค่าดัชนีการปรับแต่งแบบจำลอง (Model Modification Indices: MI) ซึ่งเป็น

การพิจารณาจากคำแนะนำในการปรับค่าพารามิเตอร์โดยยินยอมให้ผ่อนคลายข้อตกลงเบื้องต้นที่ให้ค่าความคลาดเคลื่อนมีความสัมพันธ์กันได้ จนกระทั่งค่าดัชนีต่างๆ มีระดับความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ในงานวิจัยนี้เริ่มจากการพิจารณาการยินยอมให้ค่าความคลาดเคลื่อนในการวัดตัวแปรสังเกตของตัวแปรแฝง (Latent Variables) ในลักษณะตัวเดียวกันมีความสัมพันธ์กันได้ จำนวน 8 คู่ ประกอบด้วย กลุ่มตัวแปรแฝงภายใน (Endogenous Variables) จำนวน 3 คู่ ได้แก่ การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ด้านการก่อให้เกิดประโยชน์ต่อตนเอง (USE1) กับด้านการเพิ่มประสิทธิผลในความปลอดภัยของข้อมูลส่วนบุคคล (USE2), การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ด้านง่ายต่อการเรียนรู้ (EASE1) กับด้านความไม่ซับซ้อนของระบบในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล (EASE2) และทัศนคติต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ด้านความเชื่อในผลของการกระทำ (ATT1) กับด้านการประเมินคุณค่าการกระทำในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล (ATT2) และ กลุ่มตัวแปรแฝงภายนอก (Endogenous Variables) จำนวน 5 คู่ ได้แก่ การรับรู้ถึงความรุนแรงที่บุคคลอื่นจะเข้าใช้งานแทนตนบนธุรกรรมทางอิเล็กทรอนิกส์ด้านการรับรู้ถึงความรุนแรงด้านทรัพย์สิน (SEV1) กับด้านการรับรู้ถึงความรุนแรงด้านอันตรายที่อาจเกิดขึ้นกับตัวบุคคล (SEV2), ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ด้านการมีทักษะในการใช้งานเครือข่ายคอมพิวเตอร์ (SELF1) กับด้านความพร้อมในการรับมือหากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยี (SELF2), ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ด้านความพร้อมในการรับมือหากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยี (SELF2) กับด้านความสามารถในการควบคุมสถานการณ์หากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยี (SELF3), ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ด้านความคาดหวังในความคุ้มค่าของต้นทุนหรือค่าใช้จ่ายที่อยู่ในรูปตัวเงิน (COST1) กับด้านไม่ได้อยู่ในรูปตัวเงินเพื่อปกป้องข้อมูลส่วนบุคคล (COST2) และการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์กลุ่มบุคคลรอบข้างที่ใกล้ชิด (SUB1) กับการคล้อยตามผู้ทรงอิทธิพลทางเทคโนโลยีบนสื่อสังคมออนไลน์ (SUB2) หลังจากนั้น ผู้วิจัยได้พิจารณาการยินยอมให้ค่าความคลาดเคลื่อนในการวัดตัวแปรสังเกตของตัวแปรแฝง (Latent Variables) ในลักษณะคนละตัวหรือนอกเหนือกลุ่มตัวแปรแฝงเดียวกันมีความสัมพันธ์กันได้อีก จำนวน 18 คู่ ซึ่งจัดกระทำการ

ปรับแบบจำลอง จะมีลักษณะเช่นกับพิจารณาการยินยอมให้ค่าความคลาดเคลื่อนในการวัดตัวแปรสังเกตของตัวแปรแฝงในลักษณะตัวเดียวกันมีความสัมพันธ์กันได้

ผลการพิจารณาตรวจสอบระดับความสอดคล้องกลมกลืนของแบบจำลองกับข้อมูลเชิงประจักษ์ ภายหลังการปรับแบบจำลองความสัมพันธ์จากการยินยอมให้ความคลาดเคลื่อนในการวัดตัวแปรสังเกตของตัวแปรแฝง (Latent Variables) มีความสัมพันธ์กันได้ พบว่า ค่าดัชนีต่างๆ ของระดับความสอดคล้องกลมกลืนแบบจำลองนั้นมีค่าอยู่ในเกณฑ์ความสอดคล้องกลมกลืนพอใช้ (Fair) ไปจนถึงระดับดี (Good) ได้แก่ ค่าดัชนีวัดระดับความสอดคล้องกลมกลืนของแบบจำลองเชิงสัมบูรณ์ (Measure of Absolute Fit) มีค่า p-value = 0.000, χ^2= 684.99, df= 173, RMSEA = 0.075, SRMR = 0.055 ทั้งนี้ ถึงแม้ว่าการทดสอบไคสแควร์ (Chi-Square test) จะปรากฏค่า p-value มีระดับนัยสำคัญทางสถิติ ซึ่งเป็นไปได้ว่าการทดสอบไคสแควร์ดังกล่าวอาจมีระดับนัยสำคัญทางสถิติได้เนื่องจากงานวิจัยใช้กลุ่มตัวอย่างที่มีขนาดใหญ่ รวมทั้งหากพิจารณาค่า χ^2/df = 3.959 ถือได้ว่าแบบจำลองอยู่ในเกณฑ์ความสอดคล้องกลมกลืนพอใช้ สำหรับกลุ่มค่าดัชนีวัดระดับความสอดคล้องกลมกลืนของแบบจำลองเชิงเปรียบเทียบ (Comparative Fit Index/Increment Fit Measure) มีค่า Non-normed Fit Index (NNFI) หรือTucker-Lewis Index (TLI) = 0.96 , Comparative Fit Index (CFI) = 0.97 , Goodness of Fit Index (GFI) = 0.90 โดยแบบจำลองภายหลังจากการปรับแก้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ในเกณฑ์หรือระดับที่สามารถยอมรับได้ ซึ่งหมายความว่าแบบจำลองของงานวิจัยนี้ สามารถนำไปอธิบายปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ได้ ดังตาราง 6

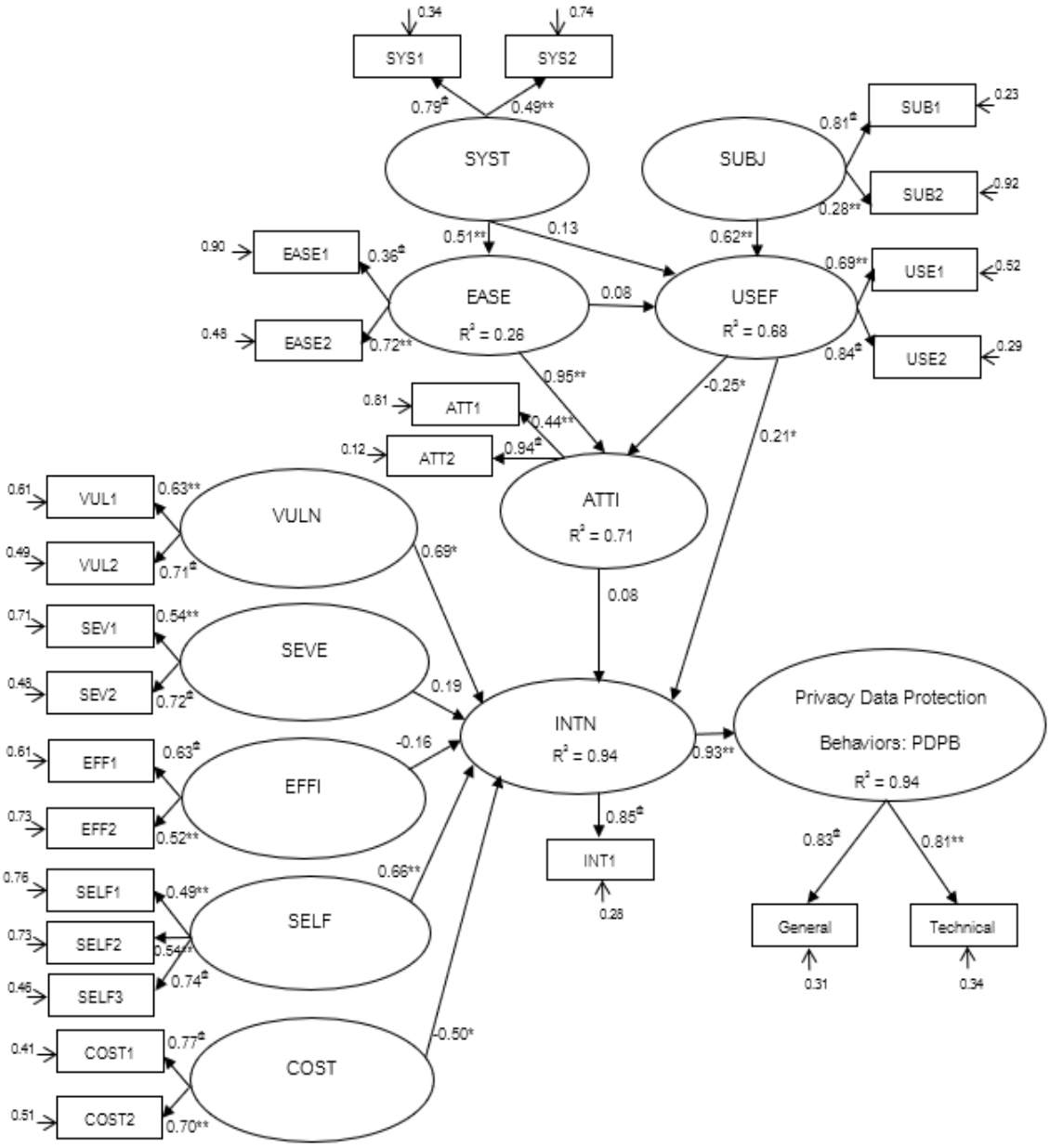
ตาราง 6 ผลการเปรียบเทียบค่าดัชนีความสอดคล้องกลมกลืนก่อนและหลังการปรับแบบจำลอง

ค่าสถิติทดสอบ	**เกณฑ์ความสอดคล้องกลมกลืน**	**ผลการวิเคราะห์ก่อนปรับ**	**ผลการปรับแบบจำลอง**
(1) Chi-Square test (χ^2) (2) χ^2/df	ไม่มีนัยสำคัญทางสถิติ (p-value > 0.05) < 2.00 มีความสอดคล้องกลมกลืนดี 2.00-5.00 มีความสอดคล้องกลมกลืนพอใช้	p-value = 0.000 χ^2= 1,803.44 df= 218	p-value = 0.000 χ^2= 684.99 df= 173
(3) RMSEA และ (4) SRMR	< 0.05 มีความสอดคล้องกลมกลืนดี 0.05-0.08 มีความสอดคล้องกลมกลืนพอใช้	RMSEA = 0.139, SRMR = 0.089	RMSEA = 0.075 SRMR = 0.055

ตาราง 6 (ต่อ)

(5) NNFI, (6) CFI และ (7) GFI	$\geq$ 0.95	มีความสอดคล้องกลมกลืนดี	NNFI = 0.88, CFI = 0.90, GFI = 0.75	NNFI = 0.96, CFI = 0.97, GFI = 0.90
	0.90-0.94	มีความสอดคล้องกลมกลืนพอใช้		

จากตาราง 6 ผลการเปรียบเทียบค่าดัชนีความสอดคล้องกลมกลืนก่อนและหลังการปรับแบบจำลอง จะเห็นได้ว่า ภายหลังปรับแบบจำลองความสัมพันธ์มีค่าดัชนีต่างๆ ของระดับความสอดคล้องกลมกลืนแบบจำลองมีค่าอยู่ในเกณฑ์ความสอดคล้องกลมกลืนพอใช้ (Fair) ไปจนถึงระดับดี (Good) แสดงว่าแบบจำลองของงานวิจัยนี้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ในเกณฑ์หรือระดับที่สามารถยอมรับได้ ซึ่งผลการวิเคราะห์อิทธิพลเชิงเหตุหรือการวิเคราะห์เส้นทาง (Path Analysis) จากการปรับแบบจำลองให้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์ ภายหลังจากการศึกษาผลของแบบจำลองภายหลังการปรับแก้มีความสอดคล้องกลมกลืนกับข้อมูลเชิงประจักษ์และรายงานผลการวิเคราะห์ข้อมูล (Output) เพื่อวิเคราะห์เส้นทาง (Path Analysis) และประมาณค่าขนาดของอิทธิพลความสัมพันธ์เชิงเหตุที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น จากการพิจารณาค่าน้ำหนักองค์ประกอบ (Indicator Loadings/Factor Loading) หรือค่าสัมประสิทธิ์อิทธิพลมาตรฐาน (Standardized Solution) จากข้อมูลตาราง Completely Standardized Solution, LAMBDA-Y, LAMBDA-X, BETA, GAMMA รวมทั้งค่าความคลาดเคลื่อนมาตรฐาน (Standard Error) และค่าสถิติทดสอบ t-value เพื่อพิจารณาระดับนัยสำคัญทางสถิติ และค่าสัมประสิทธิ์การพยากรณ์ (R^2) ที่เกิดจากการทำนายตัวแปรแฝงภายใน (Endogenous Variables) ด้วยตัวแปรแฝงภายนอก (Exogenous Variables) มาจากข้อมูลตาราง Squared Multiple Correlations for Structural Equations ซึ่งผู้วิจัยได้สร้างแบบจำลองภายหลังการปรับแก้ เพื่อให้ง่ายต่อการอ่านและวิเคราะห์ข้อมูล ดังภาพประกอบ 8 แบบจำลองแสดงเส้นทางอิทธิพลและค่าสัมประสิทธิ์อิทธิพลมาตรฐาน



** มีระดับนัยสำคัญทางสถิติ 0.01 ($p < 0.01$), * มีระดับนัยสำคัญทางสถิติ 0.05 ($p < 0.05$)

กำหนดให้ทุกตัวแปรแฝงมีหน่วยวัดเดียวกับตัวแปรสังเกตของตัวแปรแฝงนั้นๆ จึงไม่มีการทดสอบนัยสำคัญทางสถิติของค่าน้ำหนักองค์ประกอบ

ภาพประกอบ 8 แบบจำลองแสดงเส้นทางอิทธิพลและค่าสัมประสิทธิ์อิทธิพลมาตรฐาน

จากภาพประกอบ 8 แบบจำลองแสดงเส้นทางอิทธิพลและค่าสัมประสิทธิ์อิทธิพลมาตรฐาน เมื่อพิจารณาค่าน้ำหนักองค์ประกอบของตัวแปรสังเกตที่ใช้วัดตัวแปรแฝง ผู้วิจัยกำหนดให้ทุกตัวแปรแฝงมีหน่วยการวัดลักษณะเช่นเดียวกับตัวแปรสังเกตของตัวแปรแฝง ซึ่งทำให้

ตัวแปรสังเกตนั้นไม่มีการทดสอบระดับนัยสำคัญทางสถิติของค่าน้ำหนักองค์ประกอบ ทั้งนี้ตัวแปรแฝงเป็นตัวแปรที่ไม่สามารถวัดได้โดยตรง แต่เป็นตัวแปรที่เกิดจากการประมาณค่าด้วยตัวแปรสังเกตซึ่งเป็นตัวแปรที่สามารถวัดค่าได้

สำหรับตัวแปรแฝงที่มีเพียงตัวแปรสังเกตเดียวหรือองค์ประกอบเดียว คือความตั้งใจในการปกป้องข้อมูลส่วนบุคคล (INT1) ทำให้ไม่สามารถประมาณค่าความคลาดเคลื่อนจากการวัดได้ (The error variance of single variable) ดังนั้นผู้วิจัยจึงได้กำหนดการประมาณค่าความคลาดเคลื่อนในการวัดสำหรับตัวแฝงที่มีตัวแปรสังเกตเดียวมีค่าน้ำหนักองค์ประกอบของตัวแปรสังเกตเป็นค่าคงที่ มาจากการพิจารณาใช้สูตรคำนวณ (1-reliability)*variance (Schumacker & Lomax, 2004) ทำให้ไม่มีการทดสอบระดับนัยสำคัญทางสถิติของค่าน้ำหนักองค์ประกอบด้วยเช่นกัน

ทั้งนี้ เมื่อพิจารณาค่าน้ำหนักองค์ประกอบของตัวแปรสังเกต สำหรับที่มีการทดสอบระดับนัยสำคัญทางสถิติ จะพบว่าค่าน้ำหนักองค์ประกอบของทุกตัวแปรสังเกตมีระดับนัยสำคัญทางสถิติ 0.01 และจากการพิจารณาแต่ละตัวแปรแฝง สามารถนำมาอธิบายค่าสัมประสิทธิ์อิทธิพลระหว่างตัวแปรซึ่งเป็นค่าน้ำหนักองค์ประกอบของตัวแปรสังเกต จากเกณฑ์การพิจารณาค่าน้ำหนักองค์ประกอบ (Indicator Loadings/Factor Loading) หรือค่าสัมประสิทธิ์อิทธิพลมาตรฐาน (Standardized Solution) ของตัวแปรสังเกตที่ใช้วัดตัวแปรแฝงของ Comrey & Lee (2013) ควรมีค่าน้ำหนักองค์ประกอบเท่ากับหรือมากกว่า 0.32 ขึ้นไป ซึ่งแบ่งเกณฑ์การพิจารณาออกเป็น ค่าน้ำหนักองค์ประกอบระหว่าง 0.32-0.44 อยู่ในระดับต่ำหรือค่อนข้างน้อย (Poor), ค่าน้ำหนักองค์ประกอบระหว่าง 0.45-0.54 อยู่ในระดับปานกลางหรือเพียงพอต่อการนำไปใช้ (Fair), ค่าน้ำหนักองค์ประกอบระหว่าง 0.55-0.62 อยู่ในระดับดี (Good), ค่าน้ำหนักองค์ประกอบระหว่าง 0.63-0.70 อยู่ในระดับดีมาก (Very Good) และหากค่าน้ำหนักองค์ประกอบเท่ากับหรือมากกว่า 0.71 อยู่ในระดับดีเยี่ยม (Excellent) ซึ่งผลการศึกษาค่าน้ำหนักองค์ประกอบหรือค่าสัมประสิทธิ์อิทธิพลมาตรฐานของตัวแปรสังเกตที่ใช้วัดตัวแปรแฝง เป็นดังนี้

พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (Privacy Data Protection Behaviors: PDPB) พบว่าตัวแปรสังเกตทุกตัวสามารถใช้ทดแทนตัวแปรแฝงได้ดี ซึ่งมีค่าน้ำหนักองค์ประกอบ 0.83 (General) อยู่ในระดับดีเยี่ยมและ 0.81 (Technical) อยู่ในระดับดีเยี่ยมเช่นเดียวกัน นั่นหมายความว่าตัวแปรสังเกตทั้งสองตัวมีความสัมพันธ์กับตัวแปรแฝงพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ โดยตัวแปรสังเกตด้านการปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไปซึ่งมีค่าน้ำหนักองค์ประกอบมาก

แสดงว่ามีความสำคัญต่อตัวแปรแฝงพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มาก

การรับรู้ถึงโอกาสเสี่ยง (Perceived Vulnerability: VULN) บนธุรกรรมทางอิเล็กทรอนิกส์ พบว่าตัวแปรสังเกตทุกตัวสามารถใช้ทดแทนตัวแปรแฝงได้ ซึ่งมีค่าน้ำหนักองค์ประกอบ 0.63 (VUL1) อยู่ในระดับดีมาก และ 0.71 (VUL2) อยู่ในระดับดีเยี่ยม นั่นหมายความว่าตัวแปรสังเกตทั้งสองตัวมีความสัมพันธ์กับตัวแปรแฝงการรับรู้ถึงโอกาสเสี่ยง โดยตัวแปรสังเกตด้านการรับรู้โอกาสเสี่ยงที่อาจมาจากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ซึ่งมีค่าน้ำหนักองค์ประกอบมาก แสดงว่ามีความสำคัญต่อตัวแปรแฝงการรับรู้ถึงโอกาสเสี่ยงที่บุคคลอื่นจะเข้าใช้งานแทนตนมาก

การรับรู้ถึงความรุนแรง (Perceived Severity: SEVE) บนธุรกรรมทางอิเล็กทรอนิกส์ พบว่าตัวแปรสังเกตทุกตัวสามารถใช้ทดแทนตัวแปรแฝงได้ดี ซึ่งมีค่าน้ำหนักองค์ประกอบ 0.54 (SEV1) อยู่ในระดับปานกลางและ 0.72 (SEV2) อยู่ในระดับดีเยี่ยม นั่นหมายความว่าตัวแปรสังเกตทั้งสองตัวมีความสัมพันธ์กับตัวแปรแฝงการรับรู้ถึงความรุนแรงที่บุคคลอื่นจะเข้าใช้งานแทนตน โดยตัวแปรสังเกตด้านการรับรู้ถึงความรุนแรงด้านตัวบุคคลซึ่งมีค่าน้ำหนักองค์ประกอบมาก แสดงว่ามีความสำคัญต่อตัวแปรแฝงการรับรู้ถึงความรุนแรงที่บุคคลอื่นจะเข้าใช้งานแทนตนมาก

ความคาดหวังในผลลัพธ์ (Response Efficacy: EFFI) ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ พบว่าตัวแปรสังเกตทุกตัวสามารถใช้ทดแทนตัวแปรแฝงได้ดี ซึ่งมีค่าน้ำหนักองค์ประกอบ 0.63 (EFF1) อยู่ในระดับดีมากและ 0.52 (EFF2) อยู่ในระดับปานกลาง นั่นหมายความว่าตัวแปรสังเกตทั้งสองตัวมีความสัมพันธ์กับตัวแปรแฝง ความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล โดยตัวแปรสังเกตด้านความคาดหวังในผลลัพธ์ตามวิธีการปฏิบัติตนตามคำแนะนำที่ควรปฏิบัติทั่วไปซึ่งมีค่าน้ำหนักองค์ประกอบมาก แสดงว่ามีความสำคัญต่อตัวแปรแฝงความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลมาก

ความคาดหวังความสามารถของตนเอง (Self-efficacy: SELF) ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ พบว่าตัวแปรสังเกตสามารถใช้ทดแทนตัวแปรแฝงได้ ซึ่งมีค่าน้ำหนักองค์ประกอบ 0.49 (SELF1), 0.54 (SELF2) ซึ่งอยู่ในระดับปานกลางและ 0.74 (SELF3) อยู่ในระดับดีเยี่ยม ทั้งนี้ตัวแปรสังเกตทั้งสามตัวมีความสัมพันธ์กับตัวแปรแฝง ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล โดยตัวแปรสังเกตด้านความสามารถในการควบคุมสถานการณ์หากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยีที่บุคคลอื่นอาจเข้าถึงข้อมูล

ส่วนบุคคลซึ่งมีค่าน้ำหนักองค์ประกอบมาก แสดงว่ามีความสำคัญต่อตัวแปรแฝงความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลมาก

ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่าย (Response Costs: COST) เพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ พบว่าตัวแปรสังเกตทุกตัวสามารถใช้ทดแทนตัวแปรแฝงได้ดี ซึ่งมีค่าน้ำหนักองค์ประกอบ 0.77 (COST1) อยู่ในระดับดีเยี่ยม และ 0.70 (COST2) ซึ่งอยู่ในระดับดีมาก หมายความว่าตัวแปรสังเกตทั้งสองตัวมีความสัมพันธ์กับตัวแปรแฝงความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคล โดยตัวแปรสังเกตด้านความคาดหวังในความคุ้มค่าของต้นทุนหรือค่าใช้จ่ายที่อยู่ในรูปตัวเงิน (COST1) ซึ่งมีค่าน้ำหนักองค์ประกอบมาก แสดงว่ามีความสำคัญต่อตัวแปรแฝงความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคลมาก

คุณลักษณะของระบบ (System Characteristics: SYST) เพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ พบว่าตัวแปรสังเกตทุกตัวสามารถใช้ทดแทนตัวแปรแฝงได้ดี ซึ่งมีค่าน้ำหนักองค์ประกอบ 0.79 (SYS1) อยู่ในระดับดีเยี่ยมและ 0.49 (SYS2) อยู่ในระดับปานกลาง นั่นหมายความว่าตัวแปรสังเกตทั้งสองตัวมีความสัมพันธ์กับตัวแปรแฝงคุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคล โดยตัวแปรสังเกตด้านคุณลักษณะเด่นของระบบซึ่งมีค่าน้ำหนักองค์ประกอบมาก แสดงว่ามีความสำคัญต่อตัวแปรแฝงคุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคลมาก

การคล้อยตามกลุ่มอ้างอิง (Subjective Norms: SUBJ) ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ พบว่าตัวแปรสังเกตทุกตัวสามารถใช้ทดแทนตัวแปรแฝงได้ ซึ่งมีค่าน้ำหนักองค์ประกอบ 0.81 (SUB1) อยู่ในระดับดีเยี่ยมและ 0.28 (SUB2) อยู่ในระดับค่อนข้างน้อย หมายความว่าตัวแปรสังเกตทั้งสองตัวมีความสัมพันธ์กับตัวแปรแฝงการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคล โดยตัวแปรสังเกตด้านการคล้อยตามกลุ่มบุคคลรอบข้างที่ใกล้ชิด (SUB1) ซึ่งมีค่าน้ำหนักองค์ประกอบมาก แสดงว่ามีความสำคัญต่อตัวแปรแฝงการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลมาก

การรับรู้ถึงประโยชน์ (Perceived Usefulness: USEF) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ พบว่าตัวแปรสังเกตทุกตัวสามารถใช้ทดแทนตัวแปรแฝงได้ดี ซึ่งมีค่าน้ำหนักองค์ประกอบ 0.69 (USE1) อยู่ในระดับดีมาก และ 0.84 (USE2) อยู่ในระดับดีเยี่ยม นั่นหมายความว่าตัวแปรสังเกตทั้งสองตัวมีความสัมพันธ์กับตัวแปรแฝงการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล โดยตัวแปรสังเกตด้านการเพิ่มประสิทธิผลในความ

ปลอดภัยของข้อมูลส่วนบุคคลซึ่งมีค่าน้ำหนักองค์ประกอบมาก แสดงว่ามีความสำคัญต่อตัวแปรแฝงการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลมาก

การรับรู้ถึงความง่าย (Perceived Ease of Use: EASE) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ พบว่าตัวแปรสังเกตทุกตัวสามารถใช้ทดแทนตัวแปรแฝงได้ดี ซึ่งมีค่าน้ำหนักองค์ประกอบ 0.36 (EASE1) อยู่ในระดับค่อนข้างน้อย และ 0.72 (EASE2) อยู่ในระดับดีเยี่ยม นั่นหมายความว่าตัวแปรสังเกตทั้งสองตัวมีความสัมพันธ์กับตัวแปรแฝงการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล โดยตัวแปรสังเกตด้านความไม่ซับซ้อนของระบบในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล (EASE2) ซึ่งมีค่าน้ำหนักองค์ประกอบมาก แสดงว่ามีความสำคัญต่อตัวแปรแฝงการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลมาก

ทัศนคติ (Attitude: ATTI) ที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ พบว่าตัวแปรสังเกตทุกตัวสามารถใช้ทดแทนตัวแปรแฝงได้ดี ซึ่งมีค่าน้ำหนักองค์ประกอบ 0.44 (ATT1) อยู่ในระดับค่อนข้างน้อย และ 0.94 (ATT2) อยู่ในระดับดีเยี่ยม หมายความว่าตัวแปรสังเกตทั้งสองตัวมีความสัมพันธ์กับตัวแปรแฝงทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคล โดยตัวแปรสังเกตด้านการประเมินคุณค่าการกระทำในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล (ATT2) ซึ่งมีค่าน้ำหนักองค์ประกอบมาก แสดงว่ามีความสำคัญต่อตัวแปรแฝงทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคลมาก สำหรับความตั้งใจ (Intention: INTN) ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ พบว่าตัวแปรสังเกตที่ใช้ทดแทนตัวแปรแฝงมีค่าน้ำหนักองค์ประกอบ 0.85 (INT1) อยู่ในระดับดีเยี่ยม

อิทธิพลของตัวแปรเชิงเหตุที่ส่งผลต่อตัวแปรผล

การศึกษาค่าสัมประสิทธิ์อิทธิพล (Path Coefficient) ของแบบจำลองพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น ผู้วิจัยใช้ผลการวิเคราะห์อิทธิพลทางตรง (Direct Effect) อิทธิพลทางอ้อม (Indirect Effect) และอิทธิพลรวม (Total Effect) รวมทั้งค่าความคลาดเคลื่อนมาตรฐาน (Standard Error) และค่าสถิติทดสอบ t-value เพื่อพิจารณาระดับนัยสำคัญทางสถิติ จากตารางผลการวิเคราะห์ข้อมูล Total and Indirect Effects โดยใช้ข้อมูลตารางผลการวิเคราะห์ข้อมูลอิทธิพลรวมและอิทธิพลทางอ้อมของคะแนนมาตรฐาน (Standardized Total and Indirect Effects) มาสรุปเป็นตารางผลการวิเคราะห์อิทธิพลทางตรง อิทธิพลทางอ้อม และอิทธิพลรวมของงานวิจัยนี้ ดังตาราง 7

ตาราง 7 ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรง อิทธิพลทางอ้อมและอิทธิพลรวมของคะแนนมาตรฐาน

ตัวแปรเชิงเหตุ	ตัวแปรผล														
	INTN			USEF			EASE			ATTI			PDPB		
	DE	IE	TE	DE	IE	TE	DE	IE	TE	DE	IE	TE	DE	IE	TE
VULN	0.69*	-	0.69*	-	-	-	-	-	-	-	-	-	-	0.67*	0.67*
SEVE	0.19	-	0.19	-	-	-	-	-	-	-	-	-	-	0.18	0.18
EFFI	-0.16	-	-0.16	-	-	-	-	-	-	-	-	-	-	-0.16	-0.16
SELF	0.66**	-	0.66**	-	-	-	-	-	-	-	-	-	-	0.64**	0.64**
COST	-0.50*	-	-0.50*	-	-	-	-	-	-	-	-	-	-	-0.48*	-0.48*
SUBJ	-	0.22*	0.22*	0.62**	-	0.62**	-	-	-	-	-0.15**	-0.15**	-	0.22*	0.22*
SYST	-	0.03	0.03	0.13	0.04	0.17	0.51**	-	0.51**	-	0.44**	0.44**	-	0.03	0.03
USEF	0.21*	-0.01	0.20*	-	-	-	-	-	-	-0.25*	-	-0.25*	-	0.20*	0.20*
EASE	-	0.03	0.03	0.08	-	0.08	-	-	-	0.95**	-0.02	0.93**	-	0.03	0.03
ATTI	0.08	-	0.08	-	-	-	-	-	-	-	-	-	-	0.08	0.08
INTN	-	-	-	-	-	-	-	-	-	-	-	-	0.93**	-	0.93**
R^2		0.94			0.68			0.26			0.71			0.94	

** มีระดับนัยสำคัญทางสถิติ 0.01 ($p < 0.01$), * มีระดับนัยสำคัญทางสถิติ 0.05 ($p < 0.05$)

จากตาราง 7 ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรง อิทธิพลทางอ้อมและอิทธิพลรวมของคะแนนมาตรฐาน สามารถอธิบายได้ดังนี้

อิทธิพลตัวแปรเหตุที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (Privacy Data Protection Behaviors: PDPB) ได้รับอิทธิพลทางตรง (Direct Effect) จากตัวแปรปัจจัยความตั้งใจ (Intention: INTN) ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ โดยมีค่าสัมประสิทธิ์อิทธิพล (Path Coefficient) เท่ากับ 0.93 อย่างมีระดับนัยสำคัญทางสถิติ 0.01

สำหรับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้รับอิทธิพลทางอ้อม (Indirect Effect) ที่มีค่าบวกของปัจจัยการรับรู้ถึงโอกาสเสี่ยง (VULN) ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล (SELF) การคล้อยตามกลุ่มอ้างอิง (SUBJ) และการรับรู้ถึงประโยชน์ (USEF) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล โดยมีค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.67, 0.64, 0.22 และ 0.20 ตามลำดับ อย่างมีระดับนัยสำคัญทางสถิติ สำหรับอิทธิพลทางอ้อมที่มีค่าลบมาจากความคาดหวังในความคุ้มค่าของ

ต้นทุนและค่าใช้จ่าย (COST) เพื่อปกป้องข้อมูลส่วนบุคคล มีค่าสัมประสิทธิ์อิทธิพล เท่ากับ -0.48 อย่างมีระดับนัยสำคัญทางสถิติ 0.05

เมื่อพิจารณาค่าสัมประสิทธิ์อิทธิพลรวม (Total Effect) พบว่าตัวแปรปัจจัยความตั้งใจ (INTN) ในการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ถึง 0.93 รองลงมาคือ การรับรู้ถึงโอกาสเสี่ยง ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล การคล้อยตามกลุ่มอ้างอิง และการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล โดยมีค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.67, 0.64, 0.22 และ 0.20 ตามลำดับ สำหรับค่าสัมประสิทธิ์อิทธิพลรวมจากความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่าย เพื่อปกป้องข้อมูลส่วนบุคคล มีค่าสัมประสิทธิ์อิทธิพลรวม เท่ากับ -0.48

ทั้งนี้ เมื่อพิจารณาถึงค่าสัมประสิทธิ์การพยากรณ์จะพบว่าตัวแปรเชิงเหตุประกอบด้วย การรับรู้ถึงโอกาสเสี่ยง การรับรู้ถึงความรุนแรง ความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคล การคล้อยตามกลุ่มอ้างอิง คุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคล การรับรู้ถึงประโยชน์ การรับรู้ถึงความง่ายในการตั้งค่าปกป้องข้อมูล ทัศนคติและความตั้งใจในการปกป้องข้อมูลส่วนบุคคล สามารถร่วมกันอธิบายความแปรปรวนของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ได้ร้อยละ 94 ($R^2 = 0.94$)

อิทธิพลตัวแปรเหตุที่ส่งผลต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ความตั้งใจ (Intention: INTN) ในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ได้รับอิทธิพลทางตรง (Direct Effect) จากตัวแปรปัจจัยการรับรู้ถึงโอกาสเสี่ยง (VULN) ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล (SELF) และการรับรู้ถึงประโยชน์ (USEF) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล โดยมีค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.69, 0.66 และ 0.21 ตามลำดับ อย่างมีระดับนัยสำคัญทางสถิติ สำหรับอิทธิพลทางตรงที่มีค่าลบมาจากความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่าย (COST) เพื่อปกป้องข้อมูลส่วนบุคคล มีค่าสัมประสิทธิ์อิทธิพล เท่ากับ -0.50 อย่างมีระดับนัยสำคัญทางสถิติ 0.05 ส่วนตัวแปรที่มีอิทธิพลทางอ้อม (Indirect Effect) ต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล ได้แก่ การคล้อยตามกลุ่มอ้างอิง (SUBJ) ในการปกป้องข้อมูลส่วนบุคคล มีค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.22 อย่างมีระดับนัยสำคัญทางสถิติ 0.05

เมื่อพิจารณาค่าสัมประสิทธิ์อิทธิพลรวม (Total Effect) พบว่าตัวแปรปัจจัยการรับรู้ถึงโอกาสเสี่ยงอิทธิพลต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลสูงสุด มีค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.69 รองลงมาคือ ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล การคล้อยตามกลุ่มอ้างอิง และการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล มีค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.66, 0.22 และ 0.20อย่างมีระดับนัยสำคัญทางสถิติ ส่วนค่าสัมประสิทธิ์อิทธิพลรวมจากความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่าย เพื่อปกป้องข้อมูลส่วนบุคคล มีค่าสัมประสิทธิ์อิทธิพลรวม เท่ากับ -0.50 อย่างมีระดับนัยสำคัญทางสถิติ 0.05

ทั้งนี้ เมื่อพิจารณาถึงค่าสัมประสิทธิ์การพยากรณ์จะพบว่าตัวแปรเชิงเหตุประกอบด้วย การรับรู้ถึงโอกาสเสี่ยง การรับรู้ถึงความรุนแรง ความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคล การคล้อยตามกลุ่มอ้างอิง คุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคล การรับรู้ถึงประโยชน์ การรับรู้ถึงความง่ายในการตั้งค่าปกป้องข้อมูลและทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคล สามารถร่วมกันอธิบายความแปรปรวนของความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ได้ร้อยละ 94 ($R^2 = 0.94$)

อิทธิพลตัวแปรเหตุที่ส่งผลต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

การรับรู้ถึงประโยชน์ (Perceived Usefulness: USEF) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้รับอิทธิพลทางตรง (Direct Effect) จากตัวแปรปัจจัยการคล้อยตามกลุ่มอ้างอิง (SUBJ) ในการปกป้องข้อมูลส่วนบุคคล ซึ่งมีค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.62 อย่างมีระดับนัยสำคัญทางสถิติ 0.01

ทั้งนี้ เมื่อพิจารณาถึงค่าสัมประสิทธิ์การพยากรณ์จะพบว่าตัวแปรเชิงเหตุประกอบด้วย การคล้อยตามกลุ่มอ้างอิง คุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคลและการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล สามารถร่วมกันอธิบายความแปรปรวนของการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลได้ร้อยละ 68 ($R^2 = 0.68$)

อิทธิพลตัวแปรเหตุที่ส่งผลต่อการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

การรับรู้ถึงความง่าย (Perceived Ease of Use: EASE) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้รับอิทธิพลทางตรง (Direct Effect) จากตัวแปรปัจจัยคุณลักษณะของระบบ (SYST) เพื่อปกป้องข้อมูลส่วนบุคคล ซึ่งมีค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.51 อย่างมีระดับนัยสำคัญทางสถิติ 0.01 สามารถร่วมกันอธิบายความแปรปรวนของการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลได้ร้อยละ 26 ($R^2 = 0.26$)

อิทธิพลตัวแปรเหตุที่ส่งผลต่อทัศนคติมีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ทัศนคติ (Attitude: ATTI) ที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้รับอิทธิพลทางตรง (Direct Effect) จากตัวแปรปัจจัยการรับรู้ถึงความง่าย (EASE) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล มีค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.95 อย่างมีระดับนัยสำคัญทางสถิติ 0.01 สำหรับอิทธิพลทางตรงที่มีค่าลบมาจากการรับรู้ถึงประโยชน์ (USEF) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลมีค่าสัมประสิทธิ์อิทธิพล เท่ากับ -0.25 อย่างมีระดับนัยสำคัญทางสถิติ 0.05

สำหรับตัวแปรที่มีอิทธิพลทางอ้อม (Indirect Effect) ต่อทัศนคติในการปกป้องข้อมูลส่วนบุคคล ได้แก่ คุณลักษณะของระบบ (SYST) เพื่อปกป้องข้อมูลส่วนบุคคล ซึ่งมีค่าสัมประสิทธิ์อิทธิพล เท่ากับ 0.44 อย่างมีระดับนัยสำคัญทางสถิติ 0.01 ส่วนอิทธิพลทางอ้อมที่มีค่าลบมาจากการคล้อยตามกลุ่มอ้างอิง มีค่าสัมประสิทธิ์อิทธิพล เท่ากับ -0.15 อย่างมีระดับนัยสำคัญทางสถิติ ทั้งนี้ เมื่อพิจารณาถึงค่าสัมประสิทธิ์การพยากรณ์จะพบว่าตัวแปรเชิงเหตุประกอบด้วย การคล้อยตามกลุ่มอ้างอิง คุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคล การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลและการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล สามารถร่วมกันอธิบายความแปรปรวนของทัศนคติในการปกป้องข้อมูลส่วนบุคคลได้ร้อยละ 71 ($R^2 = 0.71$)

5. ผลการวิเคราะห์ข้อมูลเพื่อทดสอบสมมติฐานการวิจัย

จากผลการศึกษาค่าสัมประสิทธิ์อิทธิพล (Path Coefficient: β) ของแบบจำลองพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น การวิเคราะห์อิทธิพลทางตรง (Direct Effect) อิทธิพลทางอ้อม (Indirect Effect) และอิทธิพลรวม

(Total Effect) เกี่ยวกับอิทธิพลของตัวแปรเชิงเหตุที่ส่งผลต่อตัวแปรผล สามารถนำมาสรุปผลเพื่อทดสอบสมมติฐานการวิจัย ซึ่งมีสมมติฐานการวิจัยย่อย ดังนี้

สมมติฐานย่อย 1 การรับรู้ถึงโอกาสเสี่ยง มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรงและอิทธิพลทางอ้อม พบว่า การรับรู้ถึงโอกาสเสี่ยง มีอิทธิพลทางอ้อม (IE = 0.67) ต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น และมีอิทธิพลทางตรง (DE = 0.69) กับความตั้งใจในการปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ 0.05 สรุปได้ว่า เป็นไปตามสมมติฐานการวิจัย/สนับสนุนสมมติฐานการวิจัย

สมมติฐานย่อย 2 การรับรู้ถึงความรุนแรง มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรงและอิทธิพลทางอ้อม พบว่า การรับรู้ถึงความรุนแรง ไม่มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ อย่างมีระดับนัยสำคัญทางสถิติ 0.05 โดยพบค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.18 และไม่มีอิทธิพลทางตรงกับความตั้งใจในการปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ 0.05 โดยพบค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.19 สรุปได้ว่า ผลการวิจัยไม่เป็นไปตามสมมติฐาน/ปฏิเสธสมมติฐานการวิจัย

สมมติฐานย่อย 3 ความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรงและอิทธิพลทางอ้อม พบว่า ความคาดหวังในผลลัพธ์ไม่มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ อย่างมีระดับนัยสำคัญทางสถิติ 0.05 โดยพบค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.16 และไม่มีอิทธิพลทางตรงกับความตั้งใจในการปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ 0.05 โดยพบค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.16 สรุปได้ว่า ผลการวิจัยไม่เป็นไปตามสมมติฐาน/ปฏิเสธสมมติฐานการวิจัย

สมมติฐานย่อย 4 ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรงและอิทธิพลทางอ้อม พบว่า ความคาดหวังในความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางอ้อม (IE = 0.64) ต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ และมีอิทธิพลทางตรง (DE = 0.66) กับความตั้งใจในการปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ 0.01 สรุปได้ว่า เป็นไปตามสมมติฐานการวิจัย/สนับสนุนสมมติฐานการวิจัย

สมมติฐานย่อย 5 ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรงและอิทธิพลทางอ้อม พบว่า ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายมีอิทธิพลทางอ้อม (IE = -0.48) ต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ และมีอิทธิพลทางตรง (DE = -0.50) กับความตั้งใจในการปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ 0.05 สรุปได้ว่า เป็นไปตามสมมติฐานการวิจัย/สนับสนุนสมมติฐานการวิจัย

สมมติฐานย่อย 6 คุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรง พบว่า คุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรง (DE= 0.51) กับการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ 0.01 สรุปได้ว่า เป็นไปตามสมมติฐานการวิจัย/สนับสนุนสมมติฐานการวิจัย

สมมติฐานย่อย 7 คุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรง พบว่า คุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคล ไม่มีอิทธิพลทางตรง อย่างมีระดับนัยสำคัญทางสถิติ 0.05 โดยพบค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.13 สรุปได้ว่า ผลการวิจัยไม่เป็นไปตามสมมติฐาน/ปฏิเสธสมมติฐานการวิจัย

สมมติฐานย่อย 8 การคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรง พบว่า การคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรง (DE= 0.62) กับการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ 0.01 สรุปได้ว่า เป็นไปตามสมมติฐานการวิจัย/สนับสนุนสมมติฐานการวิจัย

สมมติฐานย่อย 9 การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรง พบว่า การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรง (DE= 0.21) กับความตั้งใจในการปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ 0.05 สรุปได้ว่า เป็นไปตามสมมติฐานการวิจัย/สนับสนุนสมมติฐานการวิจัย

สมมติฐานย่อย 10 การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อทัศนคติในการปกป้องข้อมูลส่วนบุคคล

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรง พบว่า การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรง อย่างมีระดับนัยสำคัญทางสถิติ 0.05 แต่พบว่าเป็นค่าสัมประสิทธิ์อิทธิพลทางลบเท่ากับ -0.25 สรุปได้ว่า ผลการวิจัยไม่เป็นไปตามสมมติฐาน/ปฏิเสธสมมติฐานการวิจัย

สมมติฐานย่อย 11 การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรง พบว่า การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล ไม่มีอิทธิพลทางตรง อย่างมีระดับนัยสำคัญทางสถิติ 0.05 โดยพบค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.08 สรุปได้ว่า ผลการวิจัยไม่เป็นไปตามสมมติฐาน/ปฏิเสธสมมติฐานการวิจัย

สมมติฐานย่อย 12 การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อทัศนคติในการปกป้องข้อมูลส่วนบุคคล

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรง พบว่า การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรง (DE= 0.95) กับทัศนคติในการปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ 0.01 สรุปได้ว่า เป็นไปตามสมมติฐานการวิจัย/สนับสนุนสมมติฐานการวิจัย

สมมติฐานย่อย 13 ทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรง พบว่า ทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคล ไม่มีอิทธิพลทางตรง อย่างมีระดับนัยสำคัญทางสถิติ 0.05 โดยพบค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.08 สรุปได้ว่า ผลการวิจัยไม่เป็นไปตามสมมติฐาน/ปฏิเสธสมมติฐานการวิจัย

สมมติฐานย่อย 14 ความตั้งใจในการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ผลการวิเคราะห์ข้อมูลอิทธิพลทางตรง พบว่า ความตั้งใจในการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรง เท่ากับ 0.93 อย่างมีระดับนัยสำคัญทางสถิติ 0.01 ต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ สรุปได้ว่า เป็นไปตามสมมติฐานการวิจัย/สนับสนุนสมมติฐานการวิจัย

บทที่ 5
สรุปผล อภิปรายผล และข้อเสนอแนะ

การวิจัยเรื่อง ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น มีจุดมุ่งหมายการวิจัยเพื่อทดสอบและพัฒนาแบบจำลองรูปแบบความสัมพันธ์โครงสร้างปัจจัยทางจิตวิทยาและสังคมที่มีอิทธิพลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น โดยใช้แนวคิดเศรษฐศาสตร์เชิงพฤติกรรม (Behavioral Economics) เพื่อสังเคราะห์ข้อมูลไปสู่ทฤษฎีที่นำมาใช้ในงานวิจัยนี้ ประกอบด้วยทฤษฎีแรงจูงใจเพื่อการป้องกัน (The Protection Motivation Theory: PMT) ร่วมกับแบบจำลองการยอมรับการใช้เทคโนโลยี (Technology Acceptance Model: TAM) นำมาพัฒนาเป็นแนวทางในการศึกษาปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ กลุ่มตัวอย่างที่ใช้งานวิจัยเป็นกลุ่มวัยทำงานตอนต้นมีอายุระหว่าง 20-29 ปี จำนวน 418 คนในเขตกรุงเทพมหานครและปริมณฑล ใช้การสุ่มกลุ่มตัวอย่างแบบกลุ่ม (Custer Random Sampling) จำนวน 2 ขั้นตอนตามพื้นที่การแบ่งเขตการปกครอง เครื่องมือที่ใช้ในการวิจัยเป็นแบบสอบถาม (Questionnaire) ที่ผ่านตามเกณฑ์การตรวจสอบคุณภาพแบบวัดและมีหนังสือรับรองจริยธรรมในงานวิจัยเรียบร้อยแล้ว จากนั้นจึงทำการเก็บรวบรวมข้อมูลกับกลุ่มตัวอย่าง โดยการจัดทำหนังสือขอความร่วมมือในการเก็บรวบรวมข้อมูลไปยังหน่วยงานทั้งภาครัฐและเอกชนที่ได้รับอนุญาตและให้ความร่วมมือในการเก็บรวบรวมข้อมูลในกลุ่มวัยทำงานตอนต้น และใช้การวิเคราะห์ข้อมูลทางสถิติด้วยโปรแกรมสำเร็จรูปแบบจำลองสมการโครงสร้าง ในการพิจารณาตรวจสอบระดับความสอดคล้องกลมกลืนของแบบจำลองกับข้อมูลเชิงประจักษ์และเพื่อทดสอบสมมติฐานการวิจัย สามารถสรุปผลการศึกษาดังนี้

สรุปผลการวิจัย

ผลการวิเคราะห์ลักษณะข้อมูลทั่วไปของกลุ่มตัวอย่าง

ลักษณะข้อมูลทั่วไปของกลุ่มวัยทำงานตอนต้น จำนวน 418 คน พบว่าโดยส่วนใหญ่ผู้ตอบแบบสอบถามมีอายุ 25 ปี (ร้อยละ 18.40) และรองลงมามีอายุ 27 ปี (ร้อยละ 16.00) และอายุ 24 ปี (ร้อยละ 14.80) ตามลำดับ ซึ่งคิดเป็นอายุเฉลี่ยเท่ากับ 25.83 ปี โดยส่วนใหญ่เป็นกลุ่มวัยทำงานตอนต้นเพศหญิง (ร้อยละ 61.00) รองลงมาคือเพศชาย ร้อยละ 31.10 และเพศทางเลือก ร้อยละ 7.90 มีระดับการศึกษาสูงสุดในระดับปริญญาตรี (ร้อยละ 89.20) รองลงมาคือต่ำกว่า

ปริญญาตรี ร้อยละ 8.60 ซึ่งมีสถานภาพโสด (ร้อยละ 75.60) รองลงมาคืออยู่ร่วมกันโดยไม่ได้แต่งงาน ร้อยละ 17.00 สำหรับพื้นที่การปฏิบัติงานอยู่ในเขตกรุงเทพมหานคร (ร้อยละ 62.90) รองลงมาคือจังหวัดนนทบุรี ร้อยละ 29.20 โดยหน่วยงานส่วนใหญ่เป็นองค์กรธุรกิจเอกชน (ร้อยละ 82.10) รวมทั้งกลุ่มวัยทำงานตอนต้นจะมีระดับเงินเดือนปัจจุบันระหว่าง 15,001-20,000 บาท (ร้อยละ 51.70) รองลงมาคือระดับเงินเดือน 20,001-25,000 บาท คิดเป็นร้อยละ 31.10 ตามลำดับ

ผลการวิเคราะห์ค่าสถิติพื้นฐานของตัวแปรที่ใช้ในการศึกษา

ข้อตกลงเบื้องต้นของการวิเคราะห์แบบจำลองโครงสร้างความสัมพันธ์เชิงเหตุประกอบด้วย 1) การตรวจสอบลักษณะการแจกแจงข้อมูล (Normal Distribution) ของตัวแปรสังเกตจำนวน 24 ตัวแปร พบว่าค่าความเบ้และความโด่ง (Skewness & Kurtosis) ของตัวแปรสังเกตที่นำมาศึกษาในงานวิจัยนี้ ไม่มีนัยสำคัญทางสถิติ ($p > 0.05$) ซึ่งมีค่าระหว่าง 0.091 - 0.823 นั่นหมายความว่าการแจกแจงลักษณะข้อมูลของตัวแปรสังเกตมีการแจกแจงลักษณะของข้อมูลเป็นโค้งปกติ เป็นไปตามข้อตกลงเบื้องต้นของการวิเคราะห์แบบจำลองโครงสร้างความสัมพันธ์เชิงเหตุ รวมทั้งเมื่อพิจารณารายด้านของการแจกแจงข้อมูลจากค่าคะแนนมาตรฐาน (Z-Score) จะพบว่าตัวแปรสังเกตโดยส่วนใหญ่ (จำนวน 22 ตัวแปร) มีค่าความเบ้ทางลบ (Negatively Skewed Distribution) ซึ่งมีค่าระหว่าง -1.950 ถึง -0.053 หมายความว่ากลุ่มตัวอย่างมีคะแนนในแต่ละด้านสูงกว่าค่าเฉลี่ยเลขคณิต ($\bar{x}$ < Mode) และตัวแปรสังเกตโดยส่วนใหญ่ (จำนวน 23 ตัวแปร) มีค่าความโด่งทางลบ (Negative Kurtosis Distribution) ซึ่งมีค่าระหว่าง -2.047 ถึง -0.418 หมายความว่ารูปร่างลักษณะการแจกแจงข้อมูลตัวแปรสังเกตมีความโด่งน้อย (Platykurtic) กว่าลักษณะการแจกแจงของข้อมูลแบบโค้งปกติ ซึ่งเป็นค่าช่วงที่สามารถยอมรับได้ของการแจกแจงข้อมูลแบบโค้งปกติ และ 2) การตรวจสอบความสัมพันธ์ระหว่าง 2 ตัวแปร (Bivariate Relationship) พิจารณาจากค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สัน (Pearson's Product Moment Correlation Coefficient: r) ทำการตรวจสอบและวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรสังเกต พบว่าความสัมพันธ์ระหว่าง 2 ตัวแปรสังเกตทุกตัวมีค่าความสัมพันธ์เชิงบวก (Positive Correlation) ซึ่งโดยส่วนใหญ่มีนัยสำคัญทางสถิติที่ระดับ 0.01 ซึ่งมีค่าสัมประสิทธิ์สหสัมพันธ์ระหว่าง 0.097 ถึง 0.787 และพบความสัมพันธ์ระหว่าง 2 ตัวแปรบางคู่ที่มีค่าความสัมพันธ์เชิงบวก แต่ไม่มีระดับนัยสำคัญทางสถิติ ซึ่งมีค่าสัมประสิทธิ์สหสัมพันธ์ระหว่าง 0.016 ถึง 0.094 ทั้งนี้ ไม่พบค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรสังเกตที่มีค่าสูงเกิน 0.85 ซึ่งอาจทำให้เกิดปัญหาภาวะร่วมเส้นตรงเชิงพหุ (Multicollinearity) และเป็นไปตามเกณฑ์การ

ตรวจสอบความตรงเชิงจำแนกจากการพิจารณารากที่สองของค่าเฉลี่ยความแปรปรวนของตัวชี้วัดกับค่าสหสัมพันธ์ของตัวแปรแฝง เมื่อนำข้อมูลไปใช้ในการวิเคราะห์แบบจำลองโครงสร้างความสัมพันธ์เชิงเหตุ

ผลการวิเคราะห์ข้อมูลเพื่อการทดสอบสมมติฐานการวิจัย

ผลการพิจารณาตรวจสอบระดับความสอดคล้องกลมกลืนของแบบจำลองกับข้อมูลเชิงประจักษ์ ภายหลังการปรับแบบจำลองความสัมพันธ์ พบว่าค่าดัชนีของระดับความสอดคล้องกลมกลืนแบบจำลองนั้นมีค่าอยู่ในเกณฑ์ความสอดคล้องกลมกลืนพอใช้ (Fair) ไปจนถึงระดับดี (Good) ได้แก่ ค่าดัชนีวัดระดับความสอดคล้องกลมกลืนของแบบจำลองเชิงสัมบูรณ์ (Measure of Absolute Fit) มีค่า χ^2= 684.99, df= 173, RMSEA = 0.075, SRMR = 0.055 ทั้งนี้ ถึงแม้ว่าการทดสอบไคสแควร์ (Chi-Square test) ปรากฏค่า p-value มีระดับนัยสำคัญทางสถิติ (p-value < 0.000) ซึ่งเป็นไปได้ว่าการทดสอบไคสแควร์ดังกล่าวอาจมีระดับนัยสำคัญทางสถิติได้เนื่องจากงานวิจัยใช้กลุ่มตัวอย่างที่มีขนาดใหญ่ รวมทั้งหากพิจารณาค่า χ^2/df = 3.959 ถือได้ว่าแบบจำลองอยู่ในเกณฑ์ความสอดคล้องกลมกลืนพอใช้ สำหรับกลุ่มค่าดัชนีวัดระดับความสอดคล้องกลมกลืนของแบบจำลองเชิงเปรียบเทียบ (Comparative Fit Index/Increment Fit Measure) มีค่า Non-normed Fit Index (NNFI) หรือ Tucker-Lewis Index (TLI) = 0.96 , Comparative Fit Index (CFI) = 0.97 , Goodness of Fit Index (GFI) = 0.90 ซึ่งหมายความว่าแบบจำลองของงานวิจัยนี้ สามารถนำไปอธิบายปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในระดับที่ยอมรับได้

จากผลการพิจารณา การวิเคราะห์แบบจำลองโครงสร้างความสัมพันธ์เชิงเหตุที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ได้แสดงให้เห็นว่าพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (PDPB) ได้รับอิทธิพลทางบวกโดยตรง อย่างมีระดับนัยสำคัญจากความตั้งใจการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ โดยมีค่าสัมประสิทธิ์อิทธิพลมาตรฐานเท่ากับ 0.93 รวมทั้งพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ยังได้รับอิทธิพลทางบวกโดยอ้อม อย่างมีระดับนัยสำคัญจากการรับรู้ถึงโอกาสเสี่ยง ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล การคล้อยตามกลุ่มอ้างอิงและการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล โดยมีค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.67, 0.64, 0.22 และ 0.20 ตามลำดับ สำหรับอิทธิพลทางลบโดยอ้อมมาจากความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่าย เพื่อปกป้องข้อมูลส่วนบุคคล มีค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.48 ทั้งนี้ตัวแปรสาเหตุทั้งหมดที่นำมา

การศึกษาสามารถร่วมกันอธิบายความแปรปรวนของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ได้ถึงร้อยละ 94

จากการพิจารณา ผลการวิเคราะห์ข้อมูลเพื่อการทดสอบสมมติฐานการวิจัย ในงานวิจัยนี้มีจำนวน 14 สมมติฐานการวิจัยย่อย ผลการวิเคราะห์ข้อมูลพบว่ามีจำนวน 8 สมมติฐานการวิจัยย่อยที่เป็นไปตามสมมติฐานการวิจัย และจำนวน 6 สมมติฐานการวิจัยย่อยที่ไม่เป็นไปตามสมมติฐานการวิจัย สามารถสรุปผลการทดสอบสมมติฐานการวิจัยดังตาราง 8

ตาราง 8 ผลการทดสอบสมมติฐานการวิจัย

สมมติฐานการวิจัย	**ผลการทดสอบสมมติฐาน**
H1: การรับรู้ถึงโอกาสเสี่ยง มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคล ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล	เป็นไปตามสมมติฐาน
H2: การรับรู้ถึงความรุนแรง มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล	*ไม่เป็นไปตามสมมติฐาน*
H3: ความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูล มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคล ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล	*ไม่เป็นไปตามสมมติฐาน*
H4: ความคาดหวังความสามารถของตนเอง มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคล ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล	เป็นไปตามสมมติฐาน
H5: ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อการปกป้องข้อมูล มีอิทธิพลทางอ้อมต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคล ผ่านความตั้งใจปกป้องข้อมูลส่วนบุคคล	เป็นไปตามสมมติฐาน
H6: คุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล	เป็นไปตามสมมติฐาน
H7: คุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล	*ไม่เป็นไปตามสมมติฐาน*
H8: การคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล	เป็นไปตามสมมติฐาน
H9: การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล	เป็นไปตามสมมติฐาน
H10: การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อทัศนคติในการปกป้องข้อมูลส่วนบุคคล	*ไม่เป็นไปตามสมมติฐาน*

ตาราง 8 (ต่อ)

สมมติฐานการวิจัย	ผลการทดสอบสมมติฐาน
H11: การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูลส่วนบุคคล	*ไม่เป็นไปตามสมมติฐาน*
H12: การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อทัศนคติในการปกป้องข้อมูลส่วนบุคคล	เป็นไปตามสมมติฐาน
H13: ทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล	*ไม่เป็นไปตามสมมติฐาน*
H14: ความตั้งใจในการปกป้องข้อมูลส่วนบุคคล มีอิทธิพลทางตรงต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์	เป็นไปตามสมมติฐาน

อภิปรายผลการวิจัย

งานวิจัยนี้แบ่งการอภิปรายผลการวิจัยออกเป็น 2 ส่วน ประกอบด้วย ส่วนที่ 1 การอภิปรายผลเพื่อตอบสมมติฐานการวิจัย และส่วนที่ 2 การอภิปรายผลตามแนวคิด ทฤษฎีที่นำมาประยุกต์ใช้ มีรายละเอียดดังนี้

ส่วนที่ 1 การอภิปรายผลการวิจัยเพื่อตอบสมมติฐานการวิจัย

ผลการวิจัยนี้แสดงให้เห็นว่า การรับรู้ถึงโอกาสเสี่ยงและความคาดหวังความสามารถของตนเองมีอิทธิพลทางบวกต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล ในขณะที่ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายมีอิทธิพลทางลบต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล ซึ่งส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้ง การคล้อยตามกลุ่มอ้างอิงมีอิทธิพลทางบวกต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าการปกป้องข้อมูล และการรับรู้ถึงประโยชน์ส่งผลต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล ซึ่งส่งถึงพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ นอกจากนี้ คุณลักษณะของระบบมีอิทธิพลทางบวกต่อการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูล ซึ่งส่งผลต่อทัศนคติในการปกป้องข้อมูลส่วนบุคคล และพบว่าความตั้งใจในการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางบวกโดยตรงต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ โดยผลจากการทดสอบสมมติฐานการวิจัยย่อย พบประเด็นที่สำคัญในการอภิปรายตามสมมติฐาน ดังนี้

1. ผลการศึกษาอิทธิพลของการรับรู้โอกาสเสี่ยงที่ส่งผลต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล

ผลการวิจัยแสดงให้เห็นว่า ตัวแปรการรับรู้โอกาสเสี่ยงมีอิทธิพลทางบวกกับความตั้งใจในการปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ หมายความว่า กลุ่มวัยทำงานตอนต้นที่มีการรับรู้โอกาสเสี่ยงที่บุคคลอื่นจะเข้าใช้งานแทนตนสูง ซึ่งได้แก่การรับรู้โอกาสเสี่ยงที่อาจมาจากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ และโอกาสเสี่ยงจากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จะมีผลของความตั้งใจในการปกป้องข้อมูลส่วนบุคคลสูง ทั้งนี้เนื่องจากการได้รับรู้ข่าวสารเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลของผู้ใช้บริการโดยไม่ได้รับการยินยอม การถูกเปิดเผยและส่งต่อข้อมูลส่วนบุคคลไปยังบุคคลที่สาม (Third party) และการรับรู้โอกาสเสี่ยงเมื่อไม่ปฏิบัติตนตามการจัดการตั้งค่าข้อมูลส่วนบุคคลจากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเป็นสิ่งที่จำเป็นและมีความสำคัญต่อความปลอดภัยของข้อมูลส่วนบุคคล เมื่อบุคคลมีการรับรู้ข่าวสารในปริมาณที่มาก ด้านความวิตกกังวล ความไม่ปลอดภัยของข้อมูล ความเป็นไปได้ที่ผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์สามารถเข้าถึงข้อมูลส่วนบุคคลและมีโอกาสนำข้อมูลส่วนบุคคลของผู้ใช้บริการไปใช้งานและถูกเปิดเผยโดยไม่ได้รับอนุญาตหรือการยินยอม และการไม่ปฏิบัติตามการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล ซึ่งอาจก่อให้เกิดความเสียหายและบุคคลอื่นสามารถเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน จึงส่งผลให้ความตั้งใจในการปกป้องข้อมูลส่วนบุคคลสูงขึ้น ผลการวิจัยนี้สอดคล้องกับการศึกษาของ Chenoweth et al. (2009) กล่าวถึงปัจจัยการรับรู้ความเสี่ยงของการใช้โปรแกรมคอมพิวเตอร์และเครือข่ายอินเตอร์เน็ตจากผู้ให้บริการว่าจะมีโปรแกรมแฝงเข้ามาในคอมพิวเตอร์ขณะที่ใช้งานอินเตอร์เน็ตในรูปแบบสปายแวร์ (Spyware) ซึ่งเป็นไวรัสคอมพิวเตอร์ประเภทหนึ่งที่อนุญาตให้แฮ็กเกอร์ (Hacker) เข้าถึงข้อมูลส่วนตัวของคุณได้ ซึ่งส่งผลทางบวกต่อความตั้งใจในการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-spyware software) นอกจากนี้ Ifinedo (2012) ได้ระบุถึงอิทธิพลของตัวแปรการรับรู้ถึงโอกาสเสี่ยงจากหน่วยงานภายนอกที่อาจเข้าถึงข้อมูล สารสนเทศภายในองค์กร ว่าส่งผลทางบวกต่อความตั้งใจในการปฏิบัติตนตามนโยบายการรักษาความปลอดภัยระบบสารสนเทศ (Information System Security Policy)ในกลุ่มพนักงานระดับผู้จัดการ สำหรับงานวิจัยของ Workman et al. (2008) และ Lee & Larsen (2009) ตามกรอบแนวคิดทฤษฎีแรงจูงใจเพื่อการป้องกัน พบว่าปัจจัยด้านการประเมินภัยคุกคาม (Threat appraisal) ของการรับรู้ถึงโอกาสเสี่ยงของข้อมูลส่วนบุคคลภายในองค์กร การสำรองข้อมูลไว้ในแหล่งจัดเก็บข้อมูลที่ไม่ปลอดภัย พบว่ามีอิทธิพลทางบวกกับความตั้งใจในการรักษาความปลอดภัยของระบบสารสนเทศ (Information System Security) ในกลุ่มพนักงานแต่ละบุคคลด้วยเช่นกัน รวมทั้ง

งานวิจัย Boehmer et al. (2015) ซึ่งศึกษาปัจจัยเชิงเหตุของพฤติกรรมความปลอดภัยออนไลน์ในการใช้งานเครือข่ายอินเตอร์เน็ต โดยใช้การศึกษาตามกรอบแนวคิดทฤษฎีแรงจูงใจเพื่อการป้องกันเพื่อนำไปสู่การวิจัยเชิงทดลอง (Intervention and Experimental) พบว่าความอ่อนไหวต่อภัยคุกคาม (Threat susceptibility) ของแต่ละบุคคล การตั้งรหัสผ่านที่ไม่เหมาะสม คาดเดาง่ายที่ข้อมูลส่วนบุคคลอาจถูกเปิดเผยและรั่วไหล (Data Breach) ส่งต่อไปยังบุคคลอื่น มีความสัมพันธ์และสามารถทำนายผลความตั้งใจเชิงป้องกันจากการเข้าใช้งานได้

นอกจากนี้ จากการศึกษาอิทธิพลทางอ้อมที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคล พบว่าในงานวิจัยของ Yoon et al. (2012) กล่าวถึงปัจจัยการรับรู้ความเสี่ยงที่มาจากแฮ็กเกอร์ (Hacker) เพิ่มขึ้นซึ่งเป็นผู้ไม่หวังดีสามารถเข้ามาใช้งานแทนตนบนบริการอินเตอร์เน็ตในกลุ่มนักศึกษา ส่งผลทางอ้อมต่อพฤติกรรมกระตุ้นให้นักศึกษามีการรักษาความปลอดภัยของข้อมูล (Information security behaviors) ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล ซึ่งเป็นไปตามสมมติฐานการวิจัย และ Wottrich et al. (2019) พบว่า การรับรู้โอกาสเสี่ยงที่บุคคลอื่นจะเข้าใช้งานแทนตนจากการวางโทรศัพท์เคลื่อนที่ไว้ในที่ไม่ปลอดภัย มีอิทธิพลทางตรงต่อแรงจูงใจและพฤติกรรมการปกป้องข้อมูลบนโทรศัพท์เคลื่อนที่ (Privacy protection in mobile application) ในขณะที่การศึกษาของ Workman et al. (2008) พบว่าการรับรู้โอกาสเสี่ยงที่บุคคลอื่นจะเข้าใช้งานแทนตน ของระบบข้อมูลที่สามารถเข้าถึงได้ง่าย ทำให้เกิดการละเมิดความเป็นส่วนตัวและความปลอดภัยของข้อมูล มีอิทธิพลทางลบโดยต่อพฤติกรรมการละเลยรักษาความปลอดภัยข้อมูล (Ommission of information security)

2. ผลการศึกษาอิทธิพลของความคาดหวังความสามารถของตนเองที่ส่งผลต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล

ในผลการวิจัยชี้ให้เห็นว่า ตัวแปรความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางบวกกับความตั้งใจในการปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ หมายความว่า กลุ่มวัยทำงานตอนต้นที่ประเมินความสามารถการกระทำของตน การควบคุมการเปิดเผยข้อมูลส่วนบุคคลและการเก็บบันทึกข้อมูลส่วนบุคคลให้มีความปลอดภัยจากการเข้าใช้ธุรกรรมทางอิเล็กทรอนิกส์สูง ซึ่งมาจากการศึกษาองค์ประกอบการมีทักษะในการใช้งานเครือข่ายคอมพิวเตอร์ ความพร้อมในการรับมือและความสามารถในการควบคุมสถานการณ์หากเกิดปัญหาภัยคุกคามทางเทคโนโลยี จะมีผลของความตั้งใจในการปกป้องข้อมูลส่วนบุคคลสูงตามไปด้วย ทั้งนี้เป็นเพราะความสามารถของตนในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ความคล่องแคล่ว ความเชี่ยวชาญ ประสบการณ์การเรียนรู้ที่ไม่เปิดเผยรหัสผ่านให้บุคคลอื่นทราบ การเตรียมความพร้อม การแก้ไขปัญหา การควบคุมอารมณ์และการ

ตัดสินใจหากเกิดปัญหาภัยคุกคามจากการเข้าใช้ธุรกรรมทางอิเล็กทรอนิกส์ที่บุคคลอื่นอาจเข้าถึงข้อมูลส่วนบุคคล ซึ่งมีความสำคัญต่อความปลอดภัยของข้อมูลส่วนบุคคล เมื่อกลุ่มวัยทำงานตอนต้นประเมินความสามารถการกระทำของตน ความคาดหวังจากการมีความรู้ความเข้าใจที่สูงขึ้นเกี่ยวกับการปกป้องข้อมูลส่วนบุคคลของการมีทักษะในการใช้งานเครือข่ายคอมพิวเตอร์ ความพร้อมในการรับมือและความสามารถในการควบคุมสถานการณ์หากเกิดปัญหาภัยคุกคามทางด้านเทคโนโลยี จึงส่งผลให้ความตั้งใจในการปกป้องข้อมูลส่วนบุคคลสูงขึ้น ผลการวิจัยครั้งนี้สอดคล้องกับ Chenoweth et al. (2009) กล่าวถึงปัจจัยความสามารถในการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์และการเลือกใช้ซอฟต์แวร์ที่เหมาะสมเพื่อปกป้องสปายแวร์ของผู้ใช้บริการอินเตอร์เน็ต ส่งผลทางบวกต่อความตั้งใจในการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ สำหรับงานวิจัย Giwah et al. (2019) พบว่าบุคคลที่มีอายุ 18 ขึ้นไปที่มีทักษะความสามารถในการใช้โทรศัพท์เคลื่อนที่สูง (The higher mobile self-efficacy) ในเชิงปกป้องข้อมูลส่วนบุคคลจากการรั่วไหลของข้อมูล (Data Breach) และการไม่เก็บข้อมูลสำรองไว้ในที่จัดเก็บแหล่งเดียวกัน จะส่งผลทางบวกต่อความตั้งใจปกป้องข้อมูลส่วนบุคคลบนอุปกรณ์เคลื่อนที่ (Mobile device) สูงตามไปด้วย เช่นเดียวกับการศึกษาของ Verkijika (2018) กล่าวถึงการรับรู้ของบุคคลเกี่ยวกับทักษะและความสามารถระบบการจัดเก็บข้อมูลบนคลาวด์ (Cloud Storage) ที่ปลอดภัย รวมทั้งความเชี่ยวชาญ และประสบการณ์จากการใช้สมาร์ทโฟนในระดับสูงมีความสัมพันธ์เชิงบวกและสามารถทำนายผลความตั้งใจในการรักษาข้อมูลส่วนบุคคลให้มีความปลอดภัยบนสมาร์ทโฟนได้ รวมทั้ง Yoon et al. (2012) และ Lee & Larsen (2009) พบว่าตัวแปรความสามารถของบุคคลในการเตรียมความพร้อมและการควบคุมภัยคุกคามจากการที่แฮ็กเกอร์สามารถเข้าถึงข้อมูลส่วนตัวที่มีประสิทธิภาพของการเข้าใช้บริการอินเตอร์เน็ต จะส่งผลทางบวกต่อความตั้งใจที่จะฝึกการรักษาให้ข้อมูลส่วนบุคคลมีความปลอดภัย และงานวิจัย Chen et al. (2017) ภายใต้กรอบแนวคิดทฤษฎีการควบคุมตนเอง (Self-control Theory) และทฤษฎีแรงจูงใจเพื่อการป้องกันและใช้การศึกษาแบบจำลองสมการโครงสร้างจากผู้ใช้บริการพาณิชย์อิเล็กทรอนิกส์ พบว่าการมีความรู้ความเข้าใจเกี่ยวกับความเป็นส่วนตัวทางอินเตอร์เน็ต (Knowledge about Internet Privacy) มีอิทธิพลทางบวกต่อความตั้งใจปกป้องข้อมูลส่วนบุคคล และการศึกษาของ Ifinedo (2012) พบว่าอิทธิพลของตัวแปรความคาดหวังความสามารถของตนเองโดยส่งผลทางบวกต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบสารสนเทศที่สูงขึ้นเช่นกัน ดังนั้น ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลนั้นมีความสัมพันธ์กันเชิงบวก หากบุคคลมีความ

ตั้งใจ ความหวังและความมั่นใจว่าตนสามารถที่จะปกป้องข้อมูลส่วนบุคคล ควบคุมการเปิดเผยข้อมูลส่วนบุคคลได้จะช่วยปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์และลดปัญหาภัยคุกคามทางด้านเทคโนโลยีได้

นอกจากนี้ จากการศึกษาอิทธิพลทางอ้อมที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคล พบว่าในงานวิจัยของ Wottrich et al. (2019) กล่าวถึงความสามารถในการโทรศัพท์เคลื่อนที่และการควบคุมการเปิดเผยข้อมูลส่วนบุคคล ไม่เปิดเผยรหัสผ่านต่อบุคคลอื่นจากการใช้งานแอปพลิเคชัน ซึ่งส่งผลทางอ้อมต่อพฤติกรรมพฤติกรรมการปกป้องข้อมูลบนโทรศัพท์เคลื่อนที่ (Privacy protection in mobile application) ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล ซึ่งเป็นไปตามสมมติฐานการวิจัย และ Boehmer et al. (2015) พบว่าทักษะสติปัญญาและความสามารถการใช้งานโปรแกรมคอมพิวเตอร์เชิงป้องกันจากโลกออนไลน์มีอิทธิพลทางตรงต่อพฤติกรรมความปลอดภัยบนโลกออนไลน์ (Online safety behavior) ในขณะที่การศึกษาของ Workman et al. (2008) พบว่าความสามารถของตนเองของการมีทักษะที่จำเป็นในการรักษาความปลอดภัยข้อมูล เทคนิดการเข้าถึงข้อมูลและรหัสผ่าน การมีทักษะที่จะใช้มาตรการป้องกันที่มีอยู่เพื่อไม่ให้ผู้อื่นเข้าถึงข้อมูลที่เป็นความลับของฉัน มีอิทธิพลทางตรงต่อพฤติกรรมการละเลยรักษาความปลอดภัยข้อมูล (Ommission of information security) ด้วยเช่นกัน

3. ผลการศึกษาอิทธิพลของความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคลที่ส่งผลต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล

ผลการวิจัยแสดงให้เห็นว่า ตัวแปรความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางลบกับความตั้งใจในการปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ หมายความว่า กลุ่มวัยทำงานตอนต้นที่มีการคาดการณ์และประเมินถึงความคุ้มค่า ผลตอบแทน ค่าใช้จ่าย ความพยายามและเวลาที่ต้องสูญเสียไปในการปฏิบัติตนเพื่อปกป้องข้อมูลส่วนบุคคลให้ปลอดภัย เมื่อเปรียบเทียบกับต้นทุนหรือค่าใช้จ่ายที่ต้องเสียไป ซึ่งได้แก่ความคาดหวังในความคุ้มค่าของค่าใช้จ่ายที่อยู่ในรูปจำนวนเงิน (Tangible costs) และนอกเหนือจากในรูปจำนวนเงิน (Intangible costs) สูง จะมีผลของความตั้งใจในการปกป้องข้อมูลส่วนบุคคลต่ำ ทั้งนี้เนื่องจาก ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคล เป็นสิ่งที่ต้องใช้เวลาศึกษา ความพยายาม มีค่าใช้จ่ายที่เพิ่มขึ้นและมีความสำคัญต่อความปลอดภัยของข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ เมื่อบุคคลคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วน

บุคคลสูง การแบกรับค่าใช้จ่ายที่เกี่ยวข้องกับการปกป้องข้อมูลส่วนบุคคลให้ปลอดภัยและมีประสิทธิภาพมากขึ้น การซื้อสมาร์ทโฟนใหม่ การซื้อโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่มีประสิทธิภาพสูงและรุ่นใหม่ล่าสุด รวมไปถึงเวลาที่สูญเสียในเรียนรู้ขั้นตอนปฏิบัติตนเพื่อปกป้องข้อมูล จึงส่งผลให้ความตั้งใจในการปกป้องข้อมูลส่วนบุคคลลดลง ผลการวิจัยนี้สอดคล้องกับ Chenoweth et al. (2009) พบว่าต้นทุนจากการซื้อโปรแกรมป้องกันไวรัสสปายแวร์ (Anti-spyware) และความพยายามในการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่มีประสิทธิภาพสูงจะส่งผลทางลบต่อความตั้งใจที่จะติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ของผู้ใช้งานอินเตอร์เน็ต ทั้งนี้จากงานวิจัยของ Verkijika (2018) และ Tsai et al. (2016) พบว่าต้นทุนค่าใช้จ่ายอาจเป็นเรื่องการเงิน เวลา ความพยายาม เมื่อผู้ใช้งานสมาร์ทโฟนรับรู้ต้นทุนสูงในการรักษาข้อมูลส่วนบุคคล จะทำให้ความตั้งใจที่จะมีส่วนร่วมในพฤติกรรมการรักษาความปลอดภัยผู้ใช้งานสมาร์ทโฟนน้อยลง สอดคล้องกับข้อค้นพบในงานวิจัยของ Boehmer et al. (2015) ซึ่งศึกษาปัจจัยเชิงเหตุของพฤติกรรมความปลอดภัยออนไลน์ (Determinants of online safety behavior) ในการใช้งานเครือข่ายอินเตอร์เน็ต พบว่าความคาดหวังในความคุ้มค่าของต้นทุน (Response costs) เกี่ยวกับการใช้เวลาและค่าใช้จ่ายที่มากเกินไปในการซื้อซอฟต์แวร์คอมพิวเตอร์โดยเฉพาะเพื่อรักษาความปลอดภัยของข้อมูล (Computer security software) เช่น โปรแกรมป้องกันไวรัสคอมพิวเตอร์จำนวนหลายรุ่น โปรแกรมคอมพิวเตอร์ที่ถูกลิขสิทธิ์ เป็นต้น มีอิทธิพลทางลบต่อความตั้งใจในการรักษาความปลอดภัยของข้อมูล เช่นเดียวกับงานวิจัยของ Woon et al. (2005) ซึ่งพบว่าต้นทุนของการรักษาความปลอดภัยข้อมูลเครือข่ายไร้สายภายในบ้าน (Home wireless networks) หรืออินเตอร์เน็ตภายในบ้าน ได้แก่ ค่าใช้จ่ายที่เพิ่มขึ้น ความพยายามและเวลาที่มากขึ้นกับการรักษามาตรการความปลอดภัย การตั้งรหัสผ่านที่คาดเดายากซับซ้อนและการเปิดใช้งานเพื่อการรักษาความปลอดภัยเครือข่ายไร้สาย พบว่ามีอิทธิพลทางลบต่อความตั้งใจปกป้องข้อมูลส่วนบุคคล รวมทั้งจากการศึกษาแบบจำลองสมการโครงสร้างด้านการรับรู้ความสามารถในการจัดการภัยคุกคามของศิริรัตน์ ศรีสว่าง (2558) พบว่าค่าใช้จ่ายในการป้องกันภัยบนเครื่องคอมพิวเตอร์เกี่ยวกับการติดตั้งซอฟต์แวร์หรือเครื่องมือด้านความปลอดภัยเป็นภาระและมีราคาแพงเกินไปส่งผลทางลบต่อความตั้งใจเชิงการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ แสดงให้เห็นว่าความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคลมีความสัมพันธ์กันเชิงลบต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคล

นอกจากนี้ จากการศึกษาอิทธิพลทางอ้อมที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคล พบว่าในงานวิจัยของ Yoon et al. (2012) กล่าวถึงตัวแปรความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลว่า การที่ต้องใช้เวลามากเพื่อเปลี่ยนรหัสผ่านและการศึกษาข้อมูลทางด้านเทคโนโลยีใหม่ๆ เพื่อรักษาความปลอดภัยของข้อมูล ส่งผลทางอ้อมเชิงลบ (Negative effect) ต่อพฤติกรรมกระตุ้นให้นักศึกษามีการรักษาความปลอดภัยของข้อมูล ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล ซึ่งเป็นไปตามสมมติฐานการวิจัย และ Boehmer et al. (2015) พบว่า การสละเวลาและค่าใช้จ่ายเกี่ยวกับการติดตั้งซอฟต์แวร์เพื่อการป้องกันการเข้าถึงข้อมูลส่วนบุคคลนั้นเป็นภาระ มีอิทธิพลทางตรงเชิงลบต่อพฤติกรรมความปลอดภัยบนโลกออนไลน์ (Online safety behavior)

4. ผลการศึกษาอิทธิพลของคุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนที่ส่งผลต่อการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล

ในผลการวิจัยชี้ให้เห็นว่า ตัวแปรคุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์มีอิทธิพลทางบวกกับการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ หมายความว่า กลุ่มวัยทำงานตอนต้นรับรู้ว่าโปรแกรมคอมพิวเตอร์หรือแอปพลิเคชัน (Applications) ที่มีการใช้งานอยู่ในปัจจุบัน ผู้ใช้สามารถกำหนดการจัดการตั้งค่าข้อมูลส่วนบุคคลในธุรกรรมทางการเงินได้ด้วยตนเอง ควบคุมการเปิดเผยข้อมูลให้มีความปลอดภัยจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์สูง จากการศึกษาองค์ประกอบคุณลักษณะเด่นของระบบ (Feature) เช่น ความรวดเร็วในการประมวลผล ความถูกต้อง คุณภาพและการกำหนดระดับการเข้าถึงของข้อมูล และส่วนติดต่อกับผู้ใช้งาน (User Interface) เช่น การนำเสนอในรูปแบบกราฟิกเชิงสัญลักษณ์ คำศัพท์ที่ใช้ การออกแบบสีและขนาดตัวอักษรสำหรับการจัดการตั้งค่าข้อมูลได้ด้วยตนเอง จะมีผลของการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลสูงตามไปด้วย ทั้งนี้เป็นเพราะการรับรู้ว่าโปรแกรมคอมพิวเตอร์หรือแอปพลิเคชัน เพื่อจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลสามารถทำความเข้าใจในการใช้งานได้ง่าย มีปฏิสัมพันธ์โต้ตอบที่ดีระหว่างโปรแกรมกับผู้ใช้งาน ให้ผลลัพธ์ที่ถูกต้องและมีหน้าจอที่ใช้งานซึ่งอำนวยความสะดวกกับผู้ใช้ ในปริมาณที่สูงขึ้น จึงส่งผลให้รับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลสูงขึ้น ผลการวิจัยครั้งนี้สอดคล้องกับ Giovanis et al. (2012) ภายใต้กรอบแนวคิดส่วนขยายของแบบจำลองการยอมรับการใช้เทคโนโลยีและทฤษฎีการแพร่กระจายนวัตกรรม (Diffusion of Innovation Theory) พบว่าการใช้งานในระบบที่เข้ากันได้กับผู้ใช้งานของแต่ละบุคคล (Program compatibility mode with preferred work style) ส่งผลทางบวกต่อการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลให้ความปลอดภัยจากการใช้

บริการธนาคารทางอินเทอร์เน็ต เช่นเดียวกับงานวิจัยของ Gupta & Chennamaneni (2018) ซึ่งพบว่าการใช้งานในระบบที่เข้ากันกับผู้ใช้งานด้านการรับรู้ประสบการณ์ของผู้ใช้งาน (Prior digital usage experience) และการมีปฏิสัมพันธ์ (Interaction) โต้ตอบระหว่างแอปพลิเคชันกับผู้ใช้งานจะส่งผลการรับรู้ถึงความง่ายในเชิงปกป้องข้อมูลส่วนบุคคลยุคดิจิทัลในกลุ่มผู้สูงอายุ นอกจากนี้งานวิจัยของ Shen & Chiou (2010) พบว่ารูปแบบหน้าจอและการออกแบบเว็บไซต์ (Website design style) เพื่อการพาณิชย์อิเล็กทรอนิกส์ มีอิทธิพลทางบวกต่อการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลสำหรับใช้บริการชำระเงินผ่านโทรศัพท์มือถือ

5. ผลการศึกษาอิทธิพลของการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลที่ส่งผลต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล

ผลการวิจัยแสดงให้เห็นว่า การคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ มีอิทธิพลทางบวกกับการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ หมายความว่า กลุ่มวัยทำงานตอนต้นที่คล้อยตามความคิดเห็นกลุ่มบุคคลรอบข้างที่ตนยอมรับทางสังคมและให้ความสำคัญถึงข้อดี และสนับสนุนให้ตั้งค่าข้อมูลส่วนบุคคลให้มีความปลอดภัยจากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์สูง จากการศึกษาองค์ประกอบการคล้อยตามกลุ่มบุคคลรอบข้างที่ใกล้ชิด เช่น ครอบครัว ญาติ เพื่อนสนิท เพื่อนร่วมงาน และการคล้อยตามผู้ทรงอิทธิพลทางเทคโนโลยีบนสื่อสังคมออนไลน์ จะส่งผลการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลสูงตามไปด้วย ทั้งนี้เป็นเพราะการคล้อยตามความคิดเห็นกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลที่ตนรู้จัก จากคำแนะนำ พูดคุยแลกเปลี่ยนความคิดเห็นถึงประโยชน์และสนับสนุนในการจัดการตั้งค่าข้อมูลส่วนบุคคลที่สูงขึ้น จึงส่งผลกระตุ้นให้การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลสูงขึ้นด้วย ผลการวิจัยครั้งนี้สอดคล้องกับ Hsu & Shih (2009) ที่ศึกษาพบว่าเพื่อนสนิทที่คอยแนะนำ ชักชวนถึงวิธีการและพฤติกรรมการปกป้องข้อมูลจากการใช้บริการธุรกรรมออนไลน์ส่งผลต่อการรับรู้ประโยชน์ในการตั้งค่าความเป็นส่วนตัว และการศึกษาของ Ifinedo (2012) พบว่าอิทธิพลของตัวแปรการคล้อยตามกลุ่มอ้างอิงระหว่างกลุ่มหัวหน้างานด้วยกัน (Peers) ผู้ใต้บังคับบัญชา (Subordinates) และผู้บังคับบัญชา (Superiors) กระตุ้นให้ส่งผลทางบวกต่อกลุ่มหัวหน้างานให้การรับรู้ถึงประโยชน์ในการปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบสารสนเทศที่สูงขึ้นภายในหน่วยงาน รวมทั้งในงานวิจัย Ho et al. (2017) พบว่าอิทธิพลทางสังคมอย่างเพื่อนสนิทและข้อมูลจากผู้เขียนในเว็บบล๊อก (Web blogs) ช่วยสนับสนุนและมีอิทธิพลทางบวกกับการรับรู้ถึงประโยชน์ในการใช้บริการเทคโนโลยีคลาวด์ (Cloud Technologies) อย่าง

ปลอดภัย และในการศึกษาของศิริรัตน์ ศรีสว่าง (2558) กล่าวถึงเพื่อนสนิท บุคคลในครอบครัว หัวหน้างาน บุคคลที่น่าเชื่อถือและหน่วยงานด้านความปลอดภัย ส่งผลทางบวกการรับรู้ประโยชน์ต่อการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์

นอกจากนี้ จากการศึกษาอิทธิพลทางอ้อมที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคล พบว่าในงานวิจัยของ Yoon et al. (2012) กล่าวถึงอิทธิพลของกลุ่มเพื่อนและตามความนิยมของคนส่วนใหญ่ (Most of people) ที่ใช้งานด้านเทคโนโลยีความปลอดภัยข้อมูลทางอินเตอร์เน็ต ซึ่งส่งผลทางอ้อมต่อพฤติกรรมกระตุ้นให้นักศึกษามีการรักษาความปลอดภัยของข้อมูล ผ่านความตั้งใจในการปกป้องข้อมูลส่วนบุคคล เช่นเดียวกับ Giwah et al. (2019) พบว่าการคล้อยตามเพื่อนสนิท บุคคลในครอบครัว หัวหน้างาน บุคคลที่น่าเชื่อถือและหน่วยงานด้านความปลอดภัยส่งผลทางอ้อมและสนับสนุนพฤติกรรม การป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ ผ่านทัศนคติ ความตั้งใจและแรงจูงใจในการปกป้องข้อมูลส่วนบุคคล (Alnajrani & Norman, 2020; Srisawang, 2015)

6. ผลการศึกษาอิทธิพลของการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลที่ส่งผลต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล

ผลการวิจัยได้ชี้ให้เห็นว่า ตัวแปรการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางบวกกับความตั้งใจในการปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ หมายความว่า กลุ่มวัยทำงานตอนต้นที่มีการรับรู้ถึงข้อดีในการตั้งค่าปกป้องข้อมูลส่วนบุคคล รับรู้ถึงคุณค่าที่ได้จากการตั้งค่าข้อมูลส่วนบุคคลเมื่อเข้าใช้งานเว็บไซต์หรือแอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งได้แก่การก่อให้เกิดประโยชน์แก่ตนเองและการเพิ่มประสิทธิผลในความปลอดภัยของข้อมูลสูง เมื่อบุคคลรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลในปริมาณที่สูงขึ้น จึงส่งผลให้ความตั้งใจในการปกป้องข้อมูลส่วนบุคคลสูงขึ้นด้วย ผลการวิจัยนี้สอดคล้องกับ Shropshire et al. (2015) พบว่าการรับรู้ถึงประโยชน์ของซอฟต์แวร์เพื่อรักษาความปลอดภัย (Security software adoption) มีความสัมพันธ์ทางบวก (Positively associated) กับความตั้งใจที่จะนำซอฟต์แวร์เพื่อรักษาความปลอดภัยมาใช้ และ Mican et al. (2020) พบว่าการรับรู้ประโยชน์ของระบบที่ช่วยแนะนำสิ่งที่เหมาะสมกับผู้ใช้ (Recommendation System) ซึ่งเป็นเครื่องมือที่ใช้สำหรับการพาณิชย์อิเล็กทรอนิกส์และธุรกิจออนไลน์ที่มีความเป็นระบบสากลและมีความปลอดภัยด้านข้อมูลสูง ส่งผลต่อความตั้งใจที่จะนำเครื่องมือนี้มาใช้ในกลุ่มอุตสาหกรรมบริการและช่วยทำให้ลูกค้าใช้งานระบบมากขึ้น

7. ผลการศึกษาอิทธิพลของการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลที่ส่งผลต่อทัศนคติในการปกป้องข้อมูลส่วนบุคคล

ผลการวิจัยแสดงให้เห็นว่าตัวแปรการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางบวกกับทัศนคติในการปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ หมายความว่า กลุ่มวัยทำงานตอนต้นที่มีการรับรู้เกี่ยวกับการเรียนรู้วิธีการ ขั้นตอนของการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล สามารถกระทำได้ง่าย ไม่ซับซ้อน ไม่ต้องใช้ความพยายามมากในการเรียนรู้ขั้นตอน ซึ่งได้แก่ ความง่ายต่อการเรียนรู้ และความไม่ซับซ้อนของระบบ สามารถตั้งค่าใช้งานที่ไม่ยุ่งยากเพื่อความปลอดภัยข้อมูลสูง จะมีผลของทัศนคติในการปกป้องข้อมูลส่วนบุคคลสูงขึ้น ทั้งนี้เนื่องจากตัวแปรการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล มีความสำคัญต่อความปลอดภัยของข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ เมื่อบุคคลรับรู้ว่าขั้นตอนการตั้งค่าปกป้องข้อมูลส่วนบุคคลนั้นใช้งานง่าย มีคำอธิบายชัดเจน สามารถปฏิบัติตามวิธีการได้อย่างรวดเร็ว รวมไปถึงไม่มีขั้นตอนที่ซับซ้อนและการมีระบบค่อยช่วยเหลือกับผู้ใช้ที่สูงขึ้น จึงส่งผลให้ทัศนคติในการปกป้องข้อมูลส่วนบุคคลสูงขึ้นด้วย ผลการวิจัยนี้สอดคล้องกับ Shropshire et al. (2015) พบว่าการรับรู้ขั้นตอนการใช้ซอฟต์แวร์เพื่อรักษาความปลอดภัย (Security software adoption) ที่เป็นระบบ ไม่ซับซ้อน มีข้อกำหนดเป็นมาตรฐานสากล ส่งผลต่อทัศนคติในการปกป้องข้อมูลต่อความปลอดภัยของทรัพยากรข้อมูลองค์กรที่มากขึ้น ซึ่งมีลักษณะเช่นเดียวกับตัวแปรการรับรู้ประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูล สำหรับ Taufik & Hanafiah (2019) พบว่าผู้โดยสารสนามบินที่เช็คอินที่นั่งด้วยตนเองผ่านตู้คิออส (Self-check-in Kiosk service) ที่มีขั้นตอนใช้งานง่าย สะดวก รวดเร็วโดยไม่ต้องแสดงข้อมูลส่วนบุคคลกับเจ้าหน้าที่ ส่งผลต่อทัศนคติเชิงบวกด้านความปลอดภัยในการใช้บริการเทคโนโลยีด้วยตนเอง (Self-service technology)

8. ผลการศึกษาอิทธิพลของความตั้งใจในการปกป้องข้อมูลส่วนบุคคลที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ตัวแปรความตั้งใจในการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางบวกกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคล อย่างมีระดับนัยสำคัญทางสถิติ หมายความว่า กลุ่มวัยทำงานตอนต้นที่มีความพยายาม เจตนาแสดงออก ความมุ่งมั่นและยินดีที่จะปฏิบัติตนในการจัดการตั้งค่าข้อมูลส่วนบุคคล ควบคุมการเปิดเผยข้อมูลส่วนบุคคลให้มีความปลอดภัยเมื่อเข้าใช้งานธุรกรรมทางอิเล็กทรอนิกส์สูงจะมีผลของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลที่สูงขึ้น ทั้งนี้เนื่องจากตัวแปรความตั้งใจในการปกป้องข้อมูลส่วนบุคคลเป็นสิ่งที่จำเป็นและมีความสำคัญต่อความปลอดภัยของข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ เมื่อบุคคลมีความตั้งใจในการ

ปกป้องข้อมูลส่วนบุคคล ความพยายามและยินดีที่จะปฏิบัติตนในการจัดการตั้งค่าข้อมูลส่วนบุคคลมากขึ้น จึงส่งผลให้พฤติกรรมการปกป้องข้อมูลส่วนบุคคลมากขึ้นด้วย ผลการวิจัยนี้สอดคล้องกับ Yoon et al. (2012) พบว่าตัวแปรความตั้งใจในการปกป้องและรักษาข้อมูลจากแฮ็กเกอร์ในกลุ่มนักศึกษาที่เข้าใช้บริการอินเตอร์เน็ต ส่งผลทางบวกต่อพฤติกรรมการรักษาข้อมูลส่วนบุคคลให้มีความปลอดภัย (Behavior in information security) และ Srisawang (2015) พบว่าความตั้งใจและแรงจูงใจส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ทั้งที่บ้านและที่ทำงาน

ผลการศึกษาอิทธิพลของตัวแปรปัจจัยที่ไม่เป็นไปตามสมมติฐานการวิจัย

จากรายงานผลการวิเคราะห์ข้อมูลเพื่อทดสอบสมมติฐานการวิจัย พบว่าการทดสอบสมมติฐานย่อยที่ไม่เป็นไปตามสมมติฐานการวิจัย มีรายละเอียดดังนี้

ผลการศึกษาอิทธิพลของการรับรู้ถึงความรุนแรงที่ส่งผลต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล ซึ่งไม่เป็นไปตามสมมติฐานการวิจัย พบว่าตัวแปรการรับรู้ถึงความรุนแรงมีความสัมพันธ์ทางบวกกับความตั้งใจในการปกป้องข้อมูลส่วนบุคคล แต่ไม่พบระดับนัยสำคัญทางสถิติ ซึ่งเป็นไปได้ว่าการรับรู้ถึงความรุนแรงบนธุรกรรมทางอิเล็กทรอนิกส์ จะมีผลของความตั้งใจในการปกป้องข้อมูลส่วนบุคคลไม่มากนัก ทั้งนี้อาจเป็นเพราะการรับรู้ข่าวสารที่เกิดขึ้นของกลุ่มวัยทำงานตอนต้น เกี่ยวกับระบบอนุญาตให้บุคคลอื่นหรือหน่วยงานภายนอกที่อาจเข้าถึงข้อมูลส่วนบุคคลและเข้ามาใช้งานธุรกรรมทางอิเล็กทรอนิกส์แทนตน จะส่งผลถึงข้อมูลทางการเงินออนไลน์มีการปรับเปลี่ยนตัวเลข สูญหาย การปลอมแปลงเป็นเจ้าของข้อมูล ทราบถึงสถานะทางการเงิน ที่อยู่และสถานที่ทำงานที่ก่อให้เกิดการบุกรุกความเป็นส่วนตัว รวมไปถึงการสะกดรอยตาม การขโมยทรัพย์สินที่มีค่าและการถูกทำร้ายด้านร่างกาย ซึ่งส่งผลให้ความตั้งใจในการปกป้องข้อมูลส่วนบุคคลอยู่ในระดับค่อนข้างน้อย ผลการวิจัยครั้งนี้สอดคล้องกับ Kim and Kim (2016) จากการศึกษาปัจจัยที่มีอิทธิพลต่อความตั้งใจที่จะใช้บริการป้องกันการโจรกรรมข้อมูลส่วนบุคคล (The intention to adopt identity theft protection services) พบว่าตัวแปรความรุนแรงมีความสัมพันธ์ทางบวกกับความตั้งใจที่จะใช้บริการป้องกันการโจรกรรมข้อมูลส่วนบุคคล มีค่าสัมประสิทธิ์อิทธิพล 0.08 และค่าสถิติทดสอบ t-value เท่ากับ 1.022 ซึ่งไม่เป็นไปตามสมมติฐานการวิจัย

ผลการศึกษาอิทธิพลของความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลที่ส่งผลต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล ซึ่งไม่เป็นไปตามสมมติฐานการวิจัย พบว่าตัวแปรความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลมี

ความสัมพันธ์ทางลบกับความตั้งใจในการปกป้องข้อมูลส่วนบุคคล และไม่มีระดับนัยสำคัญทางสถิติ อาจเนื่องจากความเชื่อ การคาดการณ์ถึงความเป็นไปได้ในกลุ่มวัยทำงานตอนต้น เมื่อปฏิบัติตนตามวิธีการดูแลรักษาข้อมูลส่วนบุคคล นโยบายการรักษาความปลอดภัยข้อมูล สารสนเทศความเป็นมาตรฐานในแนวปฏิบัติความปลอดภัยของข้อมูล และการเป็นที่ยอมรับของการปฏิบัติตามเหตุการณ์ในปัจจุบัน ส่งผลต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลที่ลดลง การวิจัยนี้สอดคล้องกับการศึกษาความตั้งใจในกลุ่มพนักงานที่มีต่อพฤติกรรมการรักษาความปลอดภัยบนสมาร์ทโฟน (Employees' behavioural intention to smartphone security) ของ Ameen et al. (2020) และงานวิจัย Anwar et al (2017) พบว่าตัวแปรความคาดหวังในผลลัพธ์ของการปฏิบัติตามนโยบายการรักษาความปลอดภัยบนสมาร์ทโฟนจะช่วยลดภัยคุกคามต่อข้อมูลส่วนบุคคลที่มีต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลนั้น ไม่เป็นไปตามสมมติฐานการวิจัยตามที่คาดการณ์ไว้

ผลการศึกษาอิทธิพลของคุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคลที่ส่งผลต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล ซึ่งไม่เป็นไปตามสมมติฐานการวิจัย พบว่าตัวแปรคุณลักษณะของระบบเพื่อการปกป้องข้อมูลมีความสัมพันธ์ทางบวกกับการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล แต่ไม่พบระดับนัยสำคัญทางสถิติ ซึ่งเป็นไปได้ว่าคุณลักษณะของระบบจะมีผลของการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลไม่มากนัก อาจเป็นเพราะการรับรู้ว่าโปรแกรมคอมพิวเตอร์หรือแอปพลิเคชัน เพื่อจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลที่อำนวยความสะดวกกับผู้ใช้งาน จะมีผลของการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลในระดับค่อนข้างน้อย ทั้งนี้เนื่องจาก ตัวแปรคุณลักษณะของระบบเป็นตัวแปรภายนอกของแบบจำลองการยอมรับการใช้เทคโนโลยี เมื่อนำมาประยุกต์ใช้กับการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล อาจส่งผลให้การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลในระดับค่อนข้างน้อยก็เป็นไปได้ ซึ่งงานวิจัย Basak et al. (2016) พบว่าการออกแบบเว็บไซต์ (Web design) เป็นปัจจัยที่ช่วยกำหนดในการเข้าถึงข้อมูลส่วนบุคคลระหว่างใช้เข้าบริการการพาณิชย์อิเล็กทรอนิกส์และมีความสัมพันธ์ทางบวกกับการรับรู้ประโยชน์การใช้งานเชิงป้องกันของข้อมูล แต่ไม่มีระดับนัยสำคัญทางสถิติ ดังนั้นจึงไม่เป็นไปตามสมมติฐานการวิจัย

ผลการศึกษาอิทธิพลของการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลที่ส่งผลต่อทัศนคติในการปกป้องข้อมูลส่วนบุคคล ซึ่งไม่เป็นไปตามสมมติฐานการวิจัย พบว่าตัวแปรการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลมี

ความสัมพันธ์ทางลบกับทัศนคติในการปกป้องข้อมูลส่วนบุคคล เป็นไปได้ว่าการรับรู้ถึงข้อดีในการตั้งค่าปกป้องข้อมูลส่วนบุคคล ในความปลอดภัยของข้อมูลสูง จะมีผลของทัศนคติในการปกป้องข้อมูลส่วนบุคคลเชิงลบ ทั้งนี้อาจเป็นเพราะความคาดหวัง ความคิดเห็นและความเชื่อของแต่ละบุคคลในเชิงประเมินถึงการรับรู้ประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล ยังไม่เป็นเรื่องที่มีความสำคัญและยินดีเรียนรู้ในการปกป้องข้อมูลส่วนบุคคล ซึ่งการศึกษาเชิงสำรวจของ Sun Pan (2019) นั้นการรับรู้ถึงประโยชน์ด้านการรักษาความเป็นส่วนตัวในกลุ่มวัยทำงาน จากการใช้บริการเทคโนโลยีคลาวด์ผ่านโทรศัพท์เคลื่อนที่ มีผู้ใช้งานส่วนน้อยที่เห็นความสำคัญตระหนักถึงการปฏิบัติตนตามนโยบายการรักษาความเป็นส่วนตัว แม้ว่าการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลนั้น เป็นเรื่องที่มีความน่าสนใจและเป็นประโยชน์มาก แต่อาจเป็นข้อจำกัดในด้านข้อมูล การสื่อสาร ที่ยังไม่แพร่หลาย และกลุ่มวัยทำงานที่เข้าใจถึงประโยชน์ของการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลยังอยู่ในวงจำกัด และอาจส่งผลให้มีทัศนคติทางลบด้านความรู้สึกต่อข้อมูล ประโยชน์ของข่าวสารในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล จึงไม่เป็นไปตามสมมติฐานการวิจัย

ผลการศึกษาอิทธิพลของการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลที่ส่งผลต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล ซึ่งไม่เป็นไปตามสมมติฐานการวิจัย พบว่าตัวแปรการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลมีความสัมพันธ์ทางบวกกับการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล แต่ไม่พบระดับนัยสำคัญทางสถิติ ซึ่งเป็นไปได้ว่าการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลจะมีผลของการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลไม่มากเท่าที่ควร ทั้งนี้อาจเป็นเพราะแต่ละบุคคลรับรู้ว่าขั้นตอนการตั้งค่าปกป้องข้อมูลส่วนบุคคลนั้นใช้งานง่าย มีคำอธิบายชัดเจน ไม่มีขั้นตอนที่ซับซ้อน และการมีระบบค่อยช่วยเหลือให้กับผู้ใช้งานที่แตกต่างกันอาจส่งผลให้การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลในระดับค่อนข้างน้อยก็เป็นได้ ผลการวิจัยนี้สอดคล้องกับ Roca et al (2009) พบว่าการรับรู้ถึงความง่ายของการเข้าใช้ระบบการซื้อขายออนไลน์ (Online trading systems) ที่สามารถปรับระดับความปลอดภัยและมาตรการรักษาความเป็นส่วนตัวให้กับผู้ใช้งานได้ตามความต้องการในแต่ละช่วงวัย ส่งผลทางบวกต่อการรับรู้ประโยชน์ของระบบการซื้อขายออนไลน์ที่มีประสิทธิภาพที่แตกต่างกัน ดังนั้นจึงไม่เป็นไปตามสมมติฐานการวิจัย

ผลการศึกษาอิทธิพลของทัศนคติต่อการปกป้องข้อมูลส่วนบุคคลส่งผลต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล ซึ่งไม่เป็นไปตามสมมติฐานการวิจัย พบว่าตัวแปรทัศนคติที่มีต่อการปกป้องข้อมูลมีความสัมพันธ์ทางบวกกับความตั้งใจในการปกป้องข้อมูลส่วนบุคคล แต่ไม่พบระดับนัยสำคัญทางสถิติ ซึ่งเป็นไปได้ว่าบุคคลมีความเชื่อในผลของการกระทำ ความคิดเห็น ความรู้สึกเชิงประเมินที่มีต่อการปฏิบัติตามวิธีการ ขั้นตอนการตั้งค่าปกป้องข้อมูลเมื่อเข้าใช้งานธุรกรรมทางอิเล็กทรอนิกส์ ความรู้สึกที่มีต่อผลลัพธ์จากการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลให้มีความปลอดภัย จะมีผลของความตั้งใจในการปกป้องข้อมูลส่วนบุคคลในระดับค่อนข้างน้อย อาจเนื่องจากตัวแปรทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคล แต่ละบุคคลให้ความสำคัญต่อความปลอดภัยของข้อมูลที่แตกต่างกัน เมื่อบุคคลมีความเข้าใจและสนับสนุนในการปกป้องข้อมูลส่วนบุคคล จึงส่งผลต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล ซึ่งในการศึกษาของ Shropshire et al. (2015) พบว่าการประเมินการตัดสินใจซื้อซอฟต์แวร์เพื่อรักษาความปลอดภัยของข้อมูล ส่งผลทางบวกกับความตั้งใจที่จะนำซอฟต์แวร์เพื่อรักษาความปลอดภัยมาใช้ แต่ไม่พบระดับนัยสำคัญทางสถิติ ดังนั้นจึงไม่เป็นไปตามสมมติฐานการวิจัย

ส่วนที่ 2 การอภิปรายผลการวิจัยตามแนวคิดและทฤษฎีที่นำมาใช้

งานวิจัยนี้ ภายใต้การใช้แนวคิดเศรษฐศาสตร์เชิงพฤติกรรม (Behavioral Economics) ในการสังเคราะห์ข้อมูลไปสู่การประยุกต์ใช้แบบจำลองทฤษฎีแรงจูงใจเพื่อการป้องกัน (The Protection Motivation: PMT) ร่วมกับของแบบจำลองการยอมรับการใช้เทคโนโลยี (Technology Acceptance Model: TAM) จากผลการวิจัยครั้งนี้ แสดงให้เห็นว่า

ส่วนหนึ่งสนับสนุนตามทฤษฎีแรงจูงใจเพื่อการป้องกัน โดยตัวแปรความตั้งใจในการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางบวกโดยตรงต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์สูงถึงร้อยละ 93 ทั้งนี้ เป็นผลมาจากการพัฒนาเส้นทางความสัมพันธ์ของความตั้งใจในการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางบวกต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคล และอาจเป็นเพราะการที่กลุ่มวัยทำงานตอนต้นมีความพยายามควบคุมการเปิดเผยข้อมูลและยินดีที่ปฏิบัติการตั้งค่าปกป้องข้อมูลส่วนบุคคล มีส่วนสนับสนุนให้กลุ่มวัยทำงานตอนต้นเกิดความรู้สึกที่ดีกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ตามทฤษฎีแรงจูงใจเพื่อการป้องกัน ได้ชี้ให้เห็นว่าตัวแปรกลุ่มประเมินภัยคุกคาม (Threat appraisal) พบว่า การรับรู้โอกาสเสี่ยงบนธุรกรรมทางอิเล็กทรอนิกส์มีอิทธิพลทางบวกโดยตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล อาจเป็นเพราะการที่กลุ่มวัยทำงานตอนต้นมีการรับรู้ข่าวสารในความไม่ปลอดภัยของข้อมูล มีส่วนสนับสนุนให้กลุ่มวัยทำงานตอนต้นเกิด

ความรู้สึกที่ดีกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ และตัวแปรกลุ่มการประเมินเผชิญปัญหา (Coping appraisal) พบว่า ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลมีอิทธิพลทางบวกโดยตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล ซึ่งเป็นไปได้ว่าการมีทักษะและความสามารถใช้งานคอมพิวเตอร์ที่ปลอดภัยด้านข้อมูล การจัดการปกป้องข้อมูลส่วนบุคคลและการป้องกันภัยคุกคามทางคอมพิวเตอร์ มีส่วนสนับสนุนให้กลุ่มวัยทำงานตอนต้นเกิดความรู้สึกที่ดีกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคล และความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางลบโดยตรงต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล เป็นไปได้ว่าการต้องเสียเวลาและค่าใช้จ่ายไปกับการรับมือเพื่อปกป้องข้อมูล ส่วนสนับสนุนให้กลุ่มวัยทำงานตอนต้นเกิดความรู้สึกด้านลบกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ สำหรับการประยุกต์ใช้แบบจำลองการยอมรับการใช้เทคโนโลยี พบว่าส่วนหนึ่งสนับสนุนผลการวิจัยนี้ คุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางบวกโดยตรงต่อการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล อาจเป็นเพราะ การที่กลุ่มวัยทำงานตอนต้นรับรู้ว่าโปรแกรมหรือแอปพลิเคชันเพื่อการตั้งค่าข้อมูลใช้งานง่าย อำนวยความสะดวกกับผู้ใช้ มีส่วนสนับสนุนให้กลุ่มวัยทำงานตอนต้นเกิดความรู้สึกที่ดีกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ การคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางบวกโดยตรงต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล อาจเป็นเพราะ การที่กลุ่มวัยทำงานตอนต้นมีความคิดเห็นคล้อยตามกับบุคคลที่ใกล้ชิด สนิทสนม กระตุ้นให้เห็นถึงข้อดีของการตั้งค่าปกป้องข้อมูลส่วนบุคคลให้ปลอดภัยเมื่อเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ มีส่วนสนับสนุนให้กลุ่มวัยทำงานตอนต้นเกิดความรู้สึกที่ดีกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ดังนั้น ผลการวิจัยครั้งนี้มีส่วนสนับสนุนตามทฤษฎีแรงจูงใจเพื่อการป้องกันและแบบจำลองการยอมรับการใช้เทคโนโลยี ถือได้ว่าเป็นการบูรณาการระหว่าง 2 แบบจำลอง ต่อความตั้งใจเชิงพฤติกรรมและพฤติกรรมการปกป้องข้อมูลส่วนบุคคล แสดงให้เห็นถึงแบบอย่างที่ดีเหมาะสมกับการทำนายพฤติกรรมการปกป้องข้อมูลบนธุรกรรมทางอิเล็กทรอนิกส์ และเป็นแนวทางในการกำหนดปัจจัยเชิงเหตุที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น สามารถนำมาศึกษาและใช้อธิบายในบริบทสังคมไทยได้ ซึ่งนับเป็นองค์ความรู้ใหม่ (Explicit knowledge) จากการวิเคราะห์ สังเคราะห์ข้อมูลมีกระบวนการวิจัยและพิสูจน์ สู่การพัฒนาเป็นแนวปฏิบัติที่ดีต่อการปกป้องข้อมูลส่วนบุคคล ทั้งนี้

ได้มีงานวิจัยอื่นๆ ที่มีการศึกษาและกล่าวถึงแบบจำลองข้างต้น แต่สำหรับการศึกษาครั้งนี้ได้รวมเอา 2 ทฤษฎีเข้าด้วยกัน (Integrated theories) โดยใช้การศึกษาครบทุกตัวแปรในแบบจำลองและเสนอแนวทางใหม่ที่ไม่เคยมีมาก่อน เพื่อการทำนายพฤติกรรมปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น มีผลมาจากความตั้งใจในการปกป้องข้อมูลส่วนบุคคล ถึงแม้ว่าพฤติกรรมการปกป้องข้อมูลส่วนบุคคล อาจเริ่มมาจากการตระหนักถึงภัยคุกคามจากภายนอก แรงกดดันต่อความปลอดภัยของข้อมูล หากบุคคลมีพยายามควบคุมการเปิดเผยข้อมูลและสนใจปฏิบัติดูแลรักษาข้อมูลส่วนบุคคลเป็นประจำ เมื่อเวลาผ่านไปตามประสบการณ์ ก็จะมีแนวโน้มปฏิบัติตามขั้นตอนการจัดการตั้งค่าข้อมูลส่วนบุคคลและเกิดเป็นพฤติกรรมเหล่านี้ ซ้ำๆ ได้

ข้อเสนอแนะ

ข้อเสนอแนะเชิงปฏิบัติ

1. จากผลการวิจัยที่สนับสนุนการนำทฤษฎีแรงจูงใจเพื่อการป้องกันมาประยุกต์ใช้กับพฤติกรรมการปกป้องข้อมูลส่วนบุคคล แสดงให้เห็นว่าพฤติกรรมการปกป้องข้อมูลส่วนบุคคลได้รับอิทธิพลทางตรงมาจากความตั้งใจในการปกป้องข้อมูลส่วนบุคคลสูงถึงร้อยละ 93 และปัจจัยเชิงเหตุที่มีอิทธิพลสูงสุดต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลคือ การรับรู้โอกาสเสี่ยงบนธุรกรรมทางอิเล็กทรอนิกส์ ดังนั้นหน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์ที่ทำหน้าที่ส่งเสริม งานประชาสัมพันธ์และการจัดทำสื่อความรู้ เพื่อเผยแพร่ต่อสาธารณะเกี่ยวกับการปกป้องข้อมูลส่วนบุคคลทางอิเล็กทรอนิกส์ ควรมุ่งเน้นให้ความรู้ เผยแพร่ข้อมูล ข่าวสารอาชญากรรมทางอิเล็กทรอนิกส์ มีการใช้สื่อต่างๆ กิจกรรมประชาสัมพันธ์ เพื่อให้กลุ่มผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์รับรู้ข่าวสารและเข้าถึงข้อมูลได้โดยง่าย จะทำให้ผู้ใช้บริการตระหนักถึงภัยคุกคาม การรับรู้ความเสี่ยง อัพเดทข่าวสารทางด้านเทคโนโลยี การใช้งานธุรกรรมทางอิเล็กทรอนิกส์อย่างถูกต้องและปลอดภัย การเป็นแหล่งข้อมูลที่น่าเชื่อถือได้ ซึ่งจะทำให้เกิดความพยายาม ตั้งใจปฏิบัติตามขั้นตอนปกป้องข้อมูลและนำไปสู่การแสดงออก การปฏิบัติตนปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ได้ รวมทั้งหน่วยงานภาครัฐที่เกี่ยวข้องนำไปเป็นแนวปฏิบัติสำหรับดำเนินการของผู้ควบคุมข้อมูล เพื่อป้องกันการละเมิดความเป็นส่วนตัวของข้อมูลส่วนบุคคล

รวมทั้ง ปัจจัยเชิงเหตุที่มีอิทธิพลทางบวกต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล รองลงมาคือ ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูล รวมไปถึงการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล การคล้อยตามกลุ่มอ้างอิง และปัจจัยเชิงเหตุที่มีอิทธิพลทางลบต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคล คือความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคล ถือได้ว่าเป็นตัวแปรที่มีความสำคัญมากที่จะทำให้เกิดพฤติกรรมการปกป้องข้อมูลส่วนบุคคล ดังนั้นหน่วยงานที่เกี่ยวข้องควรมีการพัฒนาทักษะ ฝึกอบรม เพิ่มเติมความรู้ ความเข้าใจและความสามารถทางเทคโนโลยีเชิงป้องกันด้านการจัดการข้อมูลส่วนบุคคลให้กับกลุ่มผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ และความรู้ความสามารถด้านเทคโนโลยีสารสนเทศ ด้านการบริหารจัดการและรับมือกับภัยคุกคามทางธุรกรรมอิเล็กทรอนิกส์

2. จากผลการวิจัยที่สนับสนุนการนำแบบจำลองการยอมรับการใช้เทคโนโลยีมาประยุกต์ใช้กับพฤติกรรมการปกป้องข้อมูลส่วนบุคคล แสดงให้เห็นว่าคุณลักษณะของระบบเพื่อการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางบวกโดยตรงต่อการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล ดังนั้น หน่วยงานผู้พัฒนาระบบสารสนเทศ นักวิจัยพัฒนาซอฟต์แวร์ หากมีการออกแบบหน้าจอเพื่อการจัดการตั้งค่าข้อมูลที่เหมาะสม สะดวกกับผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ เพิ่มความตระหนักในการตั้งค่าข้อมูลส่วนบุคคลที่ง่ายจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จะมีส่วนช่วยให้สนับสนุนให้เกิดการตั้งค่าปกป้องข้อมูลส่วนบุคคล ควรมีการพัฒนาทางด้านเทคโนโลยี เครื่องมือและนวัตกรรมเพื่อตอบสนองความต้องการของผู้บริโภค ให้เข้าถึงและใช้งานที่สะดวกและง่ายขึ้น

ทั้งนี้ หากสร้างการรับรู้ให้กับผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ถึงความง่ายในการตั้งค่าปกป้องข้อมูลส่วนบุคคล โดยแสดงให้เห็นว่าขั้นตอนการเรียนรู้วิธีการปกป้องข้อมูลส่วนบุคคลให้ปลอดภัยบนโปรแกรมหรือแอปพลิเคชัน ไม่ต้องใช้ความพยายามในการเข้าถึง สามารบริหารจัดการได้ด้วยตนเอง ไม่ซับซ้อนและมีขั้นตอนวิธีการตั้งค่าข้อมูลส่วนบุคคลที่ชัดเจน ควบคู่กับการออกแบบระบบที่เข้าถึงง่ายต่อผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ เพราะหากทำให้รู้สึกยุ่งยาก ไม่อำนวยความสะดวกต่อการใช้งาน จะทำให้ผู้ใช้บริการไม่เห็นถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูล เป็นไปได้ว่าอาจส่งผลให้ไม่เกิดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ดังนั้น ผู้พัฒนาระบบสารสนเทศ ผู้พัฒนาแอปพลิเคชัน ควรพยายามออกแบบขั้นตอน วิธีการใช้งานที่ง่ายต่อผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งมีความชัดเจนในขั้นตอนและวิธีการเรียนรู้ เพื่อไม่ให้เกิดความสับสนระหว่างการใช้งานตั้งค่าปกป้องข้อมูลส่วน

บุคคล โดยความง่ายและความชัดเจนในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลนั้นจะช่วยให้ผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์เกิดทัศนคติเชิงบวกและส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลได้

3. บุคคลที่ใกล้ชิด สนิทสนม เป็นปัจจัยหนึ่งที่มีความสำคัญต่อการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลและนำไปสู่การแสดงออกของพฤติกรรมในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ดังนั้น เพื่อนสนิท เพื่อนร่วมงาน หัวหน้างาน รวมไปถึงบุคคลในครอบครัว ควรแสดงให้เห็นถึงข้อดีของการตั้งค่าปกป้องข้อมูลส่วนบุคคลให้ปลอดภัยเมื่อเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ แนะนำวิธีการป้องกันภัยจากธุรกรรมทางอิเล็กทรอนิกส์ ตระหนักถึงภัยในยุคดิจิทัลจากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์นั้นเป็นเรื่องที่ใกล้ตัว และสนับสนุนให้เกิดการตั้งค่าปกป้องข้อมูลส่วนบุคคล

ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

1. ผลการศึกษางานวิจัยนี้ พบว่าตัวแปรความตั้งใจในการปกป้องข้อมูลส่วนบุคคลมีอิทธิพลทางบวกที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์สูง ดังนั้น เพื่อให้สามารถอธิบายคุณลักษณะที่อาจเป็นประโยชน์ต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลในกลุ่มวัยทำงานตอนต้น อาจพัฒนาไปสู่การวิจัยเชิงทดลอง (Intervention) เพื่อจัดทำเป็นโปรแกรมเสริมสร้างพฤติกรรมการปกป้องข้อมูลส่วนบุคคลในการศึกษาระยะถัดไป หรือในการศึกษาครั้งถัดไปอาจจะใช้วิธีการวิจัยเชิงคุณภาพ อย่างเช่น การสัมภาษณ์เชิงลึกกับกลุ่มผู้ให้ข้อมูล การสนทนากลุ่ม เป็นต้น มาเพิ่มประสิทธิภาพและยืนยันในผลการวิจัย ซึ่งอาจทำให้ได้องค์ความรู้ในการนำไปวิจัยที่สามารถสรุปผลและตอบคำถามการวิจัยที่สมบูรณ์ขึ้น

2. จากข้อค้นพบงานวิจัยนี้ ภายใต้การประยุกต์ทฤษฎีแรงจูงใจเพื่อการป้องกันร่วมกับแบบจำลองการยอมรับการใช้เทคโนโลยี ได้ชี้ให้เห็นความตั้งใจมีอิทธิพลทางบวกที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ดังนั้นในการศึกษาครั้งต่อไปภายใต้กรอบแนวคิดและทฤษฎีดังกล่าว ควรทำการศึกษาความตั้งใจของกลุ่มวัยทำงานที่จะปฏิบัติตามนโยบายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act: PDPA) พ.ศ. 2562 ซึ่งมีผลบังคับใช้เมื่อวันที่ 1 มิถุนายน 2565 เกี่ยวกับพฤติกรรมการเป็นเจ้าของข้อมูลส่วนบุคคลในการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ เพื่อสร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย หรือพฤติกรรมการปกป้องสิทธิส่วนบุคคลจากการใช้ข้อมูลส่วนบุคคลเพื่อทำธุรกรรมทางอิเล็กทรอนิกส์ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวม

ไปถึงความตั้งใจของกลุ่มวัยทำงานต่อพฤติกรรมด้านการรักษาความปลอดภัยของระบบสารสนเทศในองค์กร/หน่วยงาน

3. จากผลการศึกษาตัวแปรเหตุของงานวิจัยนี้ ซึ่งพบว่าตัวแปรการรับรู้โอกาสเสี่ยง ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูล การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลและการคล้อยตามกลุ่มอ้างอิงมีอิทธิพลทางบวกที่ส่งผลต่อความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ดังนั้น เพื่อให้อธิบายคุณลักษณะที่เหมาะสมต่อกลุ่มวัยทำงานตอนต้นในการปกป้องข้อมูลส่วนบุคคล อาจทำการวิจัยเชิงคุณภาพเพิ่มเติมในการค้นหากระบวนการที่อาจนำไปสู่คุณลักษณะทางจิตและสังคมต่อความตั้งใจและพฤติกรรมการปกป้องข้อมูลส่วนบุคคล ซึ่งอาจทำให้พบองค์ความรู้ในการนำไปศึกษา เพื่อให้สามารถสรุปผลและตอบคำถามการวิจัยที่สมบูรณ์มากขึ้น รวมไปถึงในการศึกษาครั้งถัดไปเกี่ยวกับปัจจัยเชิงเหตุ อาจนำมาศึกษาถึงความตั้งใจในการปฏิบัติตามนโยบายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือแนวปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ สิทธิของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ในการเปิดเผย ยินยอมและเข้าถึงข้อมูลส่วนบุคคลในภาคธุรกิจด้านมาตรการปกป้องข้อมูลจากการถูกละเมิดสิทธิส่วนตัว

4. ในงานวิจัยนี้ ได้ศึกษากับกลุ่มตัวอย่างซึ่งเป็นวัยทำงานตอนต้นที่มีอายุระหว่าง 20-29 ปี ในเขตกรุงเทพมหานครและปริมณฑล รวมทั้งการเข้าถึงกลุ่มตัวอย่างมาจากหน่วยงานภาครัฐและเอกชนที่ได้รับอนุญาตและให้ความร่วมมือในการเก็บรวบรวมข้อมูล ดังนั้น ในการวิจัยครั้งต่อไปอาจใช้การศึกษาหรือทำการวิจัยเพื่อเปรียบเทียบระหว่างกลุ่มตัวอย่าง อาจใช้การศึกษาแบบจำลองสมการโครงสร้างพหุระดับ (Multi-level Structural Equation Model) ของปัจจัยที่มีอิทธิพลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ระหว่างประเภทของหน่วยงานภาครัฐและภาคเอกชน หรือระหว่างเขตพื้นที่ปฏิบัติงานระหว่างกรุงเทพมหานครและปริมณฑล

5. งานวิจัยนี้ มุ่งเน้นในการศึกษาปัจจัยเชิงเหตุทางจิตวิทยา และปัจจัยทางสังคมเพียงบางส่วนที่ส่งผลต่อความตั้งใจและพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งไม่ได้ครอบคลุมองค์ประกอบอื่นๆ ตามทฤษฎีที่เกี่ยวข้องกระบวนการของอิทธิพลทางสังคม (Social Influence Process) ดังนั้นในการวิจัยครั้งต่อไปควรนำองค์ประกอบอื่นที่อาจเป็นไปได้และมีส่วนเกี่ยวข้องมาศึกษาเพิ่มเติม เพื่อให้สามารถอธิบายถึงสาเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ได้ชัดเจนมากขึ้น

บรรณานุกรม

Aghaei, S., Nematbakhsh, M. A., & Farsani, H. K. (2012). Evolution of the world wide web: From WEB 1.0 TO WEB 4.0. *International Journal of Web & Semantic Technology*, *3*(1), 1-10.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Alnajrani, H. M., & Norman, A. A. (2020). The Effects of Applying Privacy by Design to Preserve Privacy and Personal Data Protection in Mobile Cloud Computing: An Exploratory Study. *Symmetry, 12*(12), 2039.

Ameen, N., Tarhini, A., Shah, M. H., & Madichie, N. O. (2020). Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Computers in Human Behavior, 104*, 106184.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS quarterly*, *34*(3), 613-643.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443.

Arpaci, I. (2016). Understanding and predicting students' intention to use mobile cloud storage services. *Computers in Human Behavior, 58*, 150-157.

Balebako, R., Leon, P., Shay, R., Ur, B., Wang, Y., & Cranor, L. (2012). Measuring the effectiveness of privacy tools for limiting behavioral advertising. *Web 2.0 Security and Privacy Workshop*, May 2012.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*, *84*(2), 191.

Bandura, A. (1986). Social foundations of thought and action. *Englewood Cliffs, NJ*, *1986*.

Bandura, A. (1986). The explanatory and predictive scope of self-efficacy theory. *Journal of social and clinical psychology*, *4*(3), 359-373.

Basak, S. K., Govender, D. W., & Govender, I. (2016, December). Examining the impact of

privacy, Security, and trust on the TAM and TTF models for e-commerce consumers: A pilot study. In *2016 14th Annual Conference on Privacy, Security and Trust (PST) (pp. 19-26)*. IEEE.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: stated preferences vs. actual behavior. *Communications of the ACM*, *48*(4), 101-106.

BLTBangkok. (2018). *Online Transactions and Cashless Society*. Retrieved from: https://www.bltbangkok.com/article/info/8/873

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: towards an intervention strategy for college students. *Behaviour & Information Technology*, *34*(10), 1022-1035.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, 0093650218800915.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157-165.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

Büchi, M., Just, N., & Latzer, M. (2016). Modeling the second-level digital divide: A five-country study of social differences in Internet use. *New Media & Society*, *18*(11), 2703-2722.

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: the importance of Internet skills for online privacy protection. *Information, Communication & Society*, *20*(8), 1261-1278.

Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of social and personal relationships*, *6*(2), 131-158.

Burns, N., & Grove, S. K. (1993). Advanced statistical analyses. *The practice of nursing*

research. Conduct, critique and utilization, 605-629.

Byrne, B. M. (2001). Structural equation modeling with AMOS, EQS, and LISREL: Comparative approaches to testing for the factorial validity of a measuring instrument. *International journal of testing, 1*(1), 55-86.

Cate, F. H. (1997). *Privacy in the information age*. Brookings Institution Press.

Chang, C. W., & Heo, J. (2014). Visiting theories that predict college students' self-disclosure on Facebook. *Computers in Human Behavior*, *30*, 79-86.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, *15*(5/6), 358-368.

Chellappa, R. K. (2008). Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security. *under submission*, *13*.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information technology and management*, *6*(2-3), 181-202.

Chen, H., Beaudoin, C. E., & Hong, T. (2016). Teen online information disclosure: Empirical testing of a protection motivation and social capital model. *Journal of the association for information science and technology*, *67*(12), 2871-2881.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291-302.

Chen, H. T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 13-19.

Chenoweth, T., Minch, R., & Gattiker, T. (2009, January). Application of protection motivation theory to adoption of protective technologies. In *2009 42nd Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.

Chon, B. S., Lee, J. K., Jeong, H., Park, J., & Park, J. (2018). Determinants of the intention to protect personal information among Facebook users. *The Electronics and*

Telecommunications Research Institute Journal, 40(1), 146-155.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS quarterly*, 189-211.

Comrey, A. L., & Lee, H. B. (2013). *A first course in factor analysis*. Psychology press.

Conner, M., & Norman, P. (2005). *Predicting health behaviour*. McGraw-Hill Education (UK).

Crossler, R. E. (2009). *Protection motivation theory: Understanding the determinants of individual security behavior* (Doctoral dissertation, Virginia Polytechnic Institute and State University).

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of social issues*, *59*(2), 323-342.

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (Doctoral dissertation, Massachusetts Institute of Technology).

Davis, F.D. (1989). Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-339.

Davis, F.D., Bagozzi, R.P., & Warshaw, P.R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science, 35*(8), 982-1003.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of computer-mediated communication*, *15*(1), 83-108.

DeCew, J. W. (1997). *In pursuit of privacy: Law, ethics, and the rise of technology*. Cornell University Press.

DeVellis, R. F., & Thorpe, C. T. (2021). *Scale development: Theory and applications*. Sage publications.

Diamond, P., & Vartiainen, H. (Eds.). (2012). *Behavioral economics and its applications*. Princeton University Press.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology*, *45*(3), 285-297.

Digital Ventures. (2017). *Digital Banking Trends*. Retrieved from: http://dv.co.th/blog-th/digital-banking-trend/

DiGiusto, D. M. (2008). *A Protection Motivation Theory Approach to Home Wireless Network Security in New Zealand: Establishing If Groups of Concerned Wireless Network Users Exist and Exploring Characteristics of Behavioral Intention*. (Doctoral dissertation, Open Access Te Herenga Waka-Victoria University of Wellington)

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61-80.

Directive, E. U. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities, 38*(281), 31-50..

Doherty, N. F., Ellis-Chadwick, F., McKechnie, S., Winklhofer, H., & Ennew, C. (2006). Applying the technology acceptance model to the online retailing of financial services. *International Journal of Retail & Distribution Management, 34*(4/5), 388-410.

Doolin, B., Dillon, S., Thompson, F., & Corner, J. L. (2005). Perceived risk, the Internet shopping experience and online purchasing behavior: A New Zealand perspective. *Journal of Global Information Management (JGIM)*, *13*(2), 66-88.

Eastin, M. S., & LaRose, R. (2000). Internet self-efficacy and the psychology of the digital divide. *Journal of computer-mediated communication*, *6*(1), JCMC611.

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment.

Journal of Business Research, 59(8), 877-886.

Ernst, C. P. H. (2015). Privacy protecting behavior in social network sites. In *Factors Driving Social Network Site Usage* (pp. 57-81). Springer Gabler, Wiesbaden.

Featherman, M. S., Miyazaki, A. D., & Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. *Journal of services marketing, 24*(3), 219-229.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International journal of human-computer studies*, *59*(4), 451-474.

Federal Data Protection Act. (2001). *National Data Protection Law*. Retrieved from: https://www.iuscomp.org/gla/statutes/BDSG.htm

Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior*, *33*, 153-162.

Fernandes, L. (2013). Fraud in electronic payment transactions: threats and countermeasures. *Asia Pacific Journal of Marketing & Management Review. ISSN*, *2319*, 2836.

Fishbein, M., & Ajzen, I. (1975). *Intention and Behavior: An Introduction to Theory and Research*. Addition-Wesley, Boston, MA.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology, 30*(2), 407-429.

Foltz, C. B., Newkirk, H. E., & Schwager, P. H. (2016). An empirical investigation of factors that influence individual behavior toward changing social networking security settings. *Journal of theoretical and applied electronic commerce research*, *11*(2), 1-15.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research, 18*(1), 39-50.

Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics, 22*(3), 167-176.

Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T., & Carter, C. (2000). Trust and privacy online: Why Americans want to rewrite the rules. *The Pew Internet & American Life Project*, 1-29.

Frank, R. G. (2004). *Behavioral economics and health economics* (No. w10881). National Bureau of Economic Research.

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International journal of information management*, *35*(2), 137-144.

Giovanis, A. N., Binioris, S., & Polychronopoulos, G. (2012). An extension of TAM model with IDT and security/privacy risk in the adoption of internet banking services in Greece. *EuroMed Journal of Business, 7*(1), 24-53.

Giwah, A. D., Wang, L., Levy, Y., & Hur, I. (2019). Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory. *Journal of Intellectual Capital, 21*(2), 215-233.

Gupta, A. K., Smith, K. G., & Shalley, C. E. (2006). The interplay between exploration and exploitation. *Academy of management journal, 49*(4), 693-706.

Gupta, B., & Chennamaneni, A. (2018). Understanding Online Privacy Protection Behavior of the Older Adults: An Empirical Investigation. *Journal Information Technology Management, 29*(3), 1-13.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis: Global edition*. Pearson Education.

Hair Jr, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1995). *Multivariate Data Analysis with Readings*, 4th Edition, Prentice-Hall International, Inc.

Hajli, N., & Sims, J. (2015). Social commerce: The transfer of power from sellers to buyers. *Technological Forecasting and Social Change, 94*, 350-358.

Hambleton, R. K., & Rovinelli, R. J. (1986). Assessing the dimensionality of a set of test items. *Applied psychological measurement, 10*(3), 287-302.

Head, M., & Yuan, Y. (2001). Privacy protection in electronic commerce–a theoretical framework. *Human Systems Management*, *20*(2), 149-160.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Hichang, C. (2010). Determinants of behavioral responses to online privacy: The effects of concern, risk beliefs, self-efficacy, and communication sources on self-protection strategies. *Journal of Information Privacy and Security*, *6*(1), 3-27.

Ho, S. M., Ocasio-Velázquez, M., & Booth, C. (2017). Trust or consequences? Causal effects of perceived risk and subjective norms on cloud technology adoption. *Computers & Security, 70*, 581-595.

Ho, S. S., Lwin, M. O., Yee, A. Z., & Lee, E. W. (2017). Understanding factors associated with Singaporean adolescents' intention to adopt privacy protection behavior using an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking*, *20*(9), 572-579.

Hsu, S. F., & Shih, D. H. (2009). The factors influencing individual's behavior on privacy protection. *WSEAS Transactions on Information Science and Applications, 6*(9), 1591-1600.

Iacobucci, D., & Duhachek, A. (2003). Advancing alpha: Measuring reliability with confidence. *Journal of consumer psychology, 13*(4), 478-487.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

Isaac, J. T., & Sherali, Z. (2014). Secure mobile payment systems. *IT Professional*, *16*(3), 36-43.

Jansen, J., & Van Schaik, P. (2018). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior*, *87*, 371-383.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information*

Systems Research, *24*(3), 579-595.

Joinson, A. N. & Paine, C. B. (2007). *Self-disclosure, privacy and the internet*. The oxford handbook of internet psychology. Great Britain: Oxford University Press.

Jöreskog, K. G., Olsson, U. H., & Wallentin, F. Y. (2016). *Multivariate analysis with LISREL*. Springer. DOI 10.1007/978-3-319-33153-9

Jöreskog, K. G., & Sörbom, D. (1996). *LISREL 8: User's reference guide*. Scientific Software International.

Jöreskog, K. G., Sörbom, D., & Du Toit, S. H. C. (2001). *LISREL 8: New statistical features*. Scientific Software International.

Kaspersky Lab. (2019) *Stranger danger: the connection between sharing online and losing the data we love*. Retrieved from: https://www.kaspersky.com/blog/my-precious-data-report-three/16883/

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International journal of human-computer studies*, *71*(12), 1163-1173.

Kim, A., & Kim, T. S. (2016). Factors influencing the intention to adopt identity theft protection services: Severity vs vulnerability. In *Proceeding of the 2016 Pacific-Asia Conference on Information System (PACIS). 68.*

Kim, J., Lee, C., & Elias, T. (2015). Factors affecting information sharing in social networking sites amongst university students: Application of the knowledge-sharing model to social networking sites. *Online Information Review*, *39*(3), 290-309.

Klein, R. H., & Luciano, E. M. (2016). What influences information security behavior? A study with Brazilian users. *JISTEM-Journal of Information Systems and Technology Management*, *13*(3), 479-496.

Kline, R. B. (2010). *Principles and Practice of Structural Equation Modeling*. New York: The Guilford Press.

Lankton, N. K., & Tripp, J. F. (2013, August). A Quantitative and Qualitative Study of Facebook Privacy Using the Antecedent-Privacy Concern-Outcome Macro Model.

Paper presented at the Nineteenth Americas Conference on Information Systems, Chicago, IL.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues*, *33*(3), 22-42.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology, 27*(5), 445-454.

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for information systems*, *12*(1), 50.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187.

LeFebvre, R. (2012, October). The human element in cyber security: a study on student motivation to act. In *Proceedings of the 2012 Information Security Curriculum Development Conference* (pp. 1-8).

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology, 140*, 5–53.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, *42*(2), 289-304.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, *19*(5), 469-479.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), 336-355.

Mangin, J. P. L., BOURGAUL, N., PORRAL, C. C., MESLY, O., TELAHIGUE, I., & TRUDEL, M. (1970). The moderating role of risk, security and trust applied to the TAM model in the offer of banking financial services in Canada. *The Journal of Internet*

Banking and Commerce, 19(2), 1-21.

Martin, S. S., & Camarero, C. (2008). Consumer trust to a web site: Moderating effect of attitudes toward online shopping. *Cyberpsychology & behavior*, *11*(5), 549-554.

McDonald, A., & Cranor, L. F. (2010, August). Beliefs and behaviors: Internet users' understanding of behavioral advertising. In *38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference)*.

McGuinness, D., & Simon, A. (2018). Information disclosure, privacy behaviours, and attitudes regarding employer surveillance of social networking sites. *IFLA journal*, *44*(3), 203-222.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research*, *13*(3), 334-359.

Mehrabian, A., & Russell, J. A. (1974). *An approach to environmental psychology*. the MIT Press.

Mican, D., Sitar-Taut, D. A., & Moisescu, O. I. (2020). Perceived usefulness: A silver bullet to assure user data availability for online recommendation systems. *Decision Support Systems, 139*, 113420.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of interactive marketing*, *18*(3), 15-29.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, *12*(2), 206-215.

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, *43*(3), 449-473.

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs*, *38*(2), 217-232.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106-143.

Moloney, M., & Potì, V. (2013). A behavioral perspective on the privacy calculus model. *SSRN Electronic Journal*.

MoneyandBanking. (2019). *Financial Planning: Road to Wealth*. Retrieved from: https://www.moneyandbanking.co.th/new/magazine/index/15

MoneyGuru. (2018). *Financial Transactions Online*. Retrieved from: https://www.moneyguru.co.th/lifestyle/articles

Moneyhub. (2017). *Financial Transactions in Everyday Life*. Retrieved from: https://moneyhub.in.th/article/

Moscardelli, D. M., & Divine, R. (2007). Adolescents' concern for privacy when using the Internet: An empirical analysis of predictors and relationships with privacy-protecting behaviors. *Family and Consumer Sciences Research Journal*, *35*(3), 232-252.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.

Nikkhah, H. R., & Sabherwal, R. (2017). A Privacy-Security Model of Mobile Cloud Computing Applications. In *International Conference on Information Systems, 11*.

Paine, C., Reips, U. D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies*, *65*(6), 526-536.

Park, C., & Lee, S. W. (2014). A study of the user privacy protection behavior in online environment: Based on protection motivation theory. *Journal of Internet Computing and Services*, *15*(2), 59-71.

Plotnikoff, R. C., Lippke, S., Trinh, L., Courneya, K. S., Birkett, N., & Sigal, R. J. (2010). Protection motivation theory and the prediction of physical activity among adults with type 1 or type 2 diabetes in a large population sample. *British journal of health psychology*, *15*(3), 643-661.

Ratnasingham, P. (1998). The importance of trust in electronic commerce. *Internet research*, *8*(4), 313-321.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & security*, *28*(8), 816-826.

Roca, J. C., García, J. J., & De La Vega, J. J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security, 17*(2), 96-113.

Roe, B., Teisl, M. F., Levy, A., & Russell, M. (2001). US consumers' willingness to pay for green electricity. *Energy policy*, *29*(11), 917-925.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, 153-176.

Rogers, R. W., Prentice-Dunn, S., & Gochman, D. S. (1997). Handbook of health behavior research 1: personal and social determinants. *New York, NY, US: Plenum Press, Xxviii*, *505*, 113-132.

Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health education monographs*, *2*(4), 328-335.

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior. *The Journal of social psychology*, *154*(4), 352-369.

Schiffman, L.G.; & Kanuk, L.L. (2010). *Consumer Behavior*. 10th edition, New York: Prentice Hall.

Schumacker, R. E., & Lomax, R. G. (2004). *A beginner's guide to structural equation modeling*. Psychology press.

Schumacker, R. E., & Lomax, R. G. (2010). *A beginner's guide to structural equation modeling*. 3rd edition, New York: Taylor & Francis Group.

Sedek, M., Ahmad, R., & Othman, N. F. (2018). Motivational Factors in Privacy Protection Behaviour Model for Social Networking. In *MATEC Web of Conferences* (Vol. 150, p. 05014). EDP Sciences.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing*, *19*(1), 62-73.

Shen, C. C., & Chiou, J. S. (2010). The impact of perceived ease of use on Internet service adoption: The moderating effects of temporal distance and perceived risk. *Computers in human behavior, 26*(1), 42-50.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014, April). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2347-2356).

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security, 49*, 177-191.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.

Son, J. Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS quarterly*, 503-529.

Srisawang, S., Thongmak, M., & Ngarmyarn, A. (2015). Factors Affecting Computer Crime Protection Behavior. In *The Pacific Asia Conference on Information Systems (PACIS) Proceeding*. 31.

Stark, D. (2004). TNS-TRUSTe Consumer Privacy Index Q4 2004: Consumer behaviors and attitudes about privacy. *Retrieved December*, *8*, 2005.

Stevens, J. (1996). *Multivariate statistics for the social sciences*. Mahwah, NJ: Lawrence.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology*, *68*(3), 459.

Strauss, A. and Corbin, J. (1990). *Basic of qualitative research*. Thousand Oaks,

CA: SAGE.

Sun, Pan J. (2019). Privacy protection and data security in cloud computing: a survey, challenges, and solutions. *IEEE (Institute of Electrical and Electronics Engineers) Access, 7*, 147420-147452.

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in science education, 48*(6), 1273-1296.

Taufik, N., & Hanafiah, M. H. (2019). Airport passengers' adoption behaviour towards self-check-in Kiosk Services: the roles of perceived ease of use, perceived usefulness and need for human interaction. *Heliyon, 5*(12), e02960.

Teich, A., Frankel, M. S., Kling, R., & Lee, Y. C. (1999). Anonymous communication policies for the Internet: Results and recommendations of the AAAS conference. *The Information Society, 15*(2), 71-77.

Thaler, R. H., & Benartzi, S. (2004). Save more tomorrow™: Using behavioral economics to increase employee saving. *Journal of political Economy*, *112*(S1), S164-S187.

The Standard. (2020). *The Money Case*. Retrieved from: https://thestandard.co/podcast/themoneycase128/

Tingchi Liu, M., Brock, J. L., Cheng Shi, G., Chu, R., & Tseng, T. H. (2013). Perceived benefits, perceived risk, and trust: Influences on consumers' group buying behaviour. *Asia Pacific Journal of Marketing and Logistics*, *25*(2), 225-248.

Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior*, *104*, 106115.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59*, 138-150.

Tsai, Y. C., & Yeh, J. C. (2010). Perceived risk of information security and privacy in online shopping: A study of environmentally sustainable products. *African Journal of Business Management, 4*(18), 4057-4066.

Tu, Z., & Yuan, Y. (2012, January). Understanding user's behaviors in coping with security

threat of mobile devices Loss and theft. In *2012 45th Hawaii International Conference on System Sciences* (pp. 1393-1402). IEEE.

Van Ecke, P. & Truyens, M. (2010). Privacy and social network. *Computer Law & Security Review, 26*(5), 535-546.

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283-297.

Vance, A., & Siponen, M. T. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC)*, *24*(1), 21-41.

Venkatesh, V., & Davis, F. D. (1996). A model of the antecedents of perceived ease of use: Development and test. *Decision sciences*, *27*(3), 451-481.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science*, *46*(2), 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *Management Information System quarterly*, 425-478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *Management Information System quarterly*, 157-178.

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security, 77*, 860-870.

Vroom, V. H. (1964). *Work and motivation*. New York: John Wiley & Sons.

Wilkinson, N., & Klaes, M. (2017). *An introduction to behavioral economics*. Macmillan International Higher Education.

Woon, I. M., & Kankanhalli, A. (2007). Investigation of IS professionals' intention to practise secure development of applications. *International Journal of Human-Computer*

Studies, *65*(1), 29-41.

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. In *the International Conference on Information Systems* (*ICIS) proceedings*, 31.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior*, *24*(6), 2799-2816.

World Health Organization. (2020a). *Coronavirus disease 2019 (covid-19) situation report35*. Retrieved from: https://www.who.int/docs/defaultsource/coronaviruse/situation-reports/20200224-sitrep-35-covid19.pdf

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2019). App users unwittingly in the spotlight: a model of privacy protection in mobile apps. *Journal of Consumer Affairs, 53*(3), 1056-1083.

Wu, S. I. (2003). The relationship between consumer characteristics and attitude toward online shopping. *Marketing intelligence & planning*, *21*(1), 37-44.

Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. *CyberPsychology & Behavior*, *11*(5), 615-617.

Yeh, C. H., Wang, Y. S., Lin, S. J., Tseng, T. H., Lin, H. H., Shih, Y. W., & Lai, Y. H. (2018). What drives internet users' willingness to provide personal information?. *Online Information Review*, *42*(6), 923-939.

Yoon, C. (2011). Theory of planned behavior and ethics theory in digital piracy: An integrated model. *Journal of business ethics*, *100*(3), 405-417.

Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, *23*(4), 407-416.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, *49*(1), 86-110.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer affairs*, *43*(3), 389-418.

กรมควบคุมโรค กระทรวงสาธารณสุข. (2563). *รายงานสถานการณ์โควิด-19*. สืบค้นจาก: https://covid19.dcc.moph.go.th/

กรมอนามัย กระทรวงสาธารณสุข. (2559). *กรอบการจัดแบ่งช่วงวัย*. สืบค้นจาก: http://www.mhso.moph.go.th/mhs/images/PP_age_group%2029-31.pdf

กรมพัฒนาธุรกิจการค้า. (2562). *เอกสารเผยแพร่ด้านพาณิชย์อิเล็กทรอนิกส์*. รายงานข้อมูลการจดทะเบียนของผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์. กรุงเทพฯ : กรมพัฒนาธุรกิจการค้า

กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี. (2561). *การป้องกันข้อมูลส่วนบุคคลจากการซื้อสินค้าออนไลน์บนสมาร์ทโฟน*. สืบค้นจาก: https://tcsd.go.th/

กัลยา วานิชย์บัญชา .(2542). *การวิเคราะห์สถิติ: สถิติเพื่อการตัดสินใจ*. พิมพ์ครั้งที่ 4. กรุงเทพฯ :โรงพิมพ์แห่งจุฬาลงกรณ์วิทยาลัย

ขจรศักดิ์ รุ่งศรีรัตนวงศ์ และคณะ. (2550). *พฤติกรรมการใช้อินเทอร์เน็ตบนโทรศัพท์มือถือของประชากรในเขตกรุงเทพมหานคร ประจำปี 2551*. รายงานการวิจัย คณะวิทยาการจัดการ. กรุงเทพฯ: มหาวิทยาลัยราชภัฏจันทรเกษม.

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ราชกิจจานุเบกษา. (2555). *ประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย*. สืบค้นจาก: http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/E/149/T_0039.PDF

โครงการสุขภาพคนไทย. (2560). *สุขภาพคนไทย 2560*. พิมพ์ครั้งที่ 1. กรุงเทพฯ : อมรินทร์พริ้นติ้ง แอนด์พับลิชชิ่ง จำกัด (มหาชน).

จีราภรณ์ สุธัมมสภา (2555). เทคโนโลยีสารสนเทศและการสื่อสารเพื่อการปฏิรูปธุรกิจอย่างยั่งยืน. *วารสารการจัดการสมัยใหม่, 10*(1), 19.

ฐานเศรษฐกิจ. (2562). *ประชากร Gen Y ใหญ่สุด พฤติกรรมสร้างโอกาส-ความเสี่ยง*. สืบค้นจาก: https://www.thansettakij.com/content/234315

ณัฐศักดิ์ วรวิทยานนท์. (2555). *ทัศนคติของผู้บริโภคที่มีต่อธุรกิจขายสินค้าและบริการผ่านออนไลน์*. การศึกษาค้นคว้าแบบอิสระ หลักสูตรนิเทศศาสตรมหาบัณฑิต สาขาวิชาการโฆษณา, บัณฑิตวิทยาลัย มหาวิทยาลัยศรีปทุม.

ดวงกมล ไตรวิจิตรคุณ. (2550). *วิธีวิทยาการวิจัยทางพฤติกรรมศาสตร์*. กรุงเทพฯ :โรงพิมพ์แห่งจุฬาลงกรณ์วิทยาลัย.

นงลักษณ์ วิรัชชัย. (2542). *โมเดลลิสเรล: สถิติวิเคราะห์สำหรับการวิจัย*. พิมพ์ครั้งที่ 3. กรุงเทพฯ :โรงพิมพ์แห่งจุฬาลงกรณ์วิทยาลัย.

นุศรา ทองรอด. (2555). *บริหารคน Generation Y*. สืบค้นจาก: http://www.stou.ac.th/study/sumrit/

นิภาพร แสงทวีและสมนึก พ่วงพรพิทักษ์. (2558). *การวิเคราะห์ความปลอดภัยและความมั่นคงสำหรับระบบธนาคารผ่านโทรศัพท์มือถือในประเทศไทย*. สืบค้นจาก: http://www.thaiscience.info/Journals/Article/JSMU/10985196.pdf

บริษัทข้อมูลเครดิตแห่งชาติ. (2562*). พฤติกรรมการใช้บัตรเครดิตและสินเชื่อส่วนบุคคล*. รายงานข้อมูลเครดิตบุคคลธรรมดา. กรุงเทพฯ: บริษัทข้อมูลเครดิตแห่งชาติ จำกัด (เครดิตบูโร).

ปวุฒิ บุนนาค (2557). กลยุทธ์การตลาดธุรกิจออนไลน์ที่มีผลต่อพฤติกรรมการใช้งานผ่านระบบเครือข่าย สังคมออนไลน์. กรณีศึกษา Facebook Fanpage ในเขตกรุงเทพมหานคร. *วารสารวิชาการตลาดและการจัดการ, 1*(2), 120-130.

ปิยะพร วงศ์เบี้ยสัจจ์. (2552). *การเปิดเผยข้อมูลส่วนบุคคลโดยธนาคารพาณิชย์กับมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล*. พิมพ์ครั้งที่ 1. กรุงเทพฯ : มหาวิทยาลัยธุรกิจบัณฑิตย์.

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์. (2544). *เพิ่มเติมฉบับที่ 2 (2551)*. สืบค้นจาก: https://www.bot.or.th/Thai/PaymentSystems/PSServices/icas/

พรพรรณ ช้างงาเนียม. (2553). *ลักษณะบุคคล ความพึงพอใจและพฤติกรรมการใช้บริการธุรกรรมทางการเงินผ่านโทรศัพท์มือถือ (Mobile Banking) ของลูกค้าธนาคารในกรุงเทพมหานคร*. สารนิพนธ์ปริญญามหาบัณฑิต: มหาวิทยาลัยศรีนครินทรวิโรฒ.

พลูพงศ์ สุขสว่าง. (2557). หลักการวิเคราะห์โมเดลสมการโครงสร้าง. *วารสารมหาวิทยาลัยนราธิวาสราชนครินทร์, 6*(2), 136-145.

เพจเฟซบุ๊กศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ. (2563). *การถูกขโมยข้อมูลส่วนบุคคล*. สืบค้นจาก: https://www.facebook.com/tacticspolice/

มติชนออนไลน์. (27 พฤษภาคม 2562). *การจัดตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒*. สืบค้นจาก: https://www.matichon.co.th/bullet-news-today/news_1512987

ธาริณี มณีรอด. (2559). *ปัญหากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล*. วิทยานิพนธ์

หลักสูตรนิติศาสตรมหาบัณฑิต สาขาวิชานิติศาสตร์, คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์.

ธนาคารกสิกรไทย. (2560). *ยุทธศาสตร์ทางธุรกิจของธนาคาร*. สืบค้นจาก: https://kasikornbank.com/th/IR/FinanInfoReports/financialReports/Q18_MD_Th.pdf

ธนาคารกรุงศรีอยุธยา. (2562). *โครงการฉลาดคิด ฉลาดใช้ ให้ความรู้ทางการเงิน*. สืบค้นจาก: https://www.krungsri.com/bank/th/krungsri-consumer/chalardkid-chalardchai-2019.html

ธนาคารทหารไทย บริษัทมหาชน จำกัด. (2559). *นโยบายด้านการรักษาความลับ และภัยทุจริตทางอินเทอร์เน็ตประเภท Phishing*. สืบค้นจาก: https://www.tmbbank.com/policy/

ธนาคารไทยพาณิชย์. (2560). *บริการช่องทางอิเล็กทรอนิกส์*. สืบค้นจาก: https://www.scb.co.th/th/corporate-banking/business-cash-management/scb-business-e-channel.html

ธนาคารแห่งประเทศไทย. (2557). *กระบวนการทำธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์สำหรับลูกค้ารายย่อย*. สืบค้นจาก: https://www.bot.or.th/Thai/Statistic/PaymentSystems/StatPaymentTransaction.aspx

ธนาคารแห่งประเทศไทย. (2560). *รายงานภาพรวมระบบการชำระเงิน*. สืบค้นจาก: https://www.bot.or.th/Thai/Statistic/PaymentSystem/Payment_Reports/Q2_2560.pdf

ธนาคารแห่งประเทศไทย. (2561). *รายงานประจำปี 2561 การทำธุรกรรมผ่านบริการธนาคารมือถือ*. สืบค้นจาก: https://www.bot.or.th/Thai/Research/Report/ /AnnualReport2018.pdf

ธนาคารอาคารสงเคราะห์. (2562). *บริการอิเล็กทรอนิกส์*. สืบค้นจาก: https://www.ghbank.co.th/electronic-services/application/ghb-all

ธนัท สุวรรณปริญญา. (2550). *ปัญหาทางกฎหมายเกี่ยวกับ การคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ กรณีศึกษา: การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (privacy policy) ของธนาคาร สถาบันการเงิน และผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทย*. สารนิพนธ์ หลักสูตรนิติศาสตรมหาบัณฑิต, บัณฑิตวิทยาลัย มหาวิทยาลัยกรุงเทพ.

ธนวรรณ สำนวนกลาง (2559). *การยอมรับเทคโนโลยีการทำธุรกรรมทางการเงินรูปแบบ M-Banking*. วิทยานิพนธ์ หลักสูตรวิทยาศาสตรมหาบัณฑิต, วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์.

ราชกิจจานุเบกษา. (2562). *พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒*. สืบค้นจาก:

http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

วสันต์ ลิ่วลมไพศาล และสฤณี อาชวานันทกุล. (2556). *คู่มือพลเมืองเน็ต (Netizen handbook)* (พิมพ์ครั้งที่ 1). กรุงเทพฯ : เครือข่ายพลเมืองเน็ต.

วิวัฒณ์ ขันธเขตต์ และสิงหา ฉวีสุข. (2562). การยอมรับระบบการชำระเงินอิเล็กทรอนิกส์ของกลุ่มวัยทำงานในเขตภาคกลาง ประเทศไทย.*วารสารการบริหารและการจัดการ, 9*(1), 153-164.

ศรัณย์ พิมพ์ทอง. (2564). *การพัฒนาเครื่องมือวัดในการวิจัยพฤติกรรมศาสตร์*. กรุงเทพฯ: บุ๊คพลัส พับลิชชิ่ง.

ศิริกุล ภู่พันธ์ และนคร เสรีรักษ์. (2544). *กฎหมายระหว่างประเทศที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล*. สืบค้นจาก: http://www.cola.kku.ac.th/main2/images/POR/RS/DP_guideline_28aug2014.pdf

ศิริชัย กาญจนวาสี, (2556). *ทฤษฎีการทดสอบแบบดั้งเดิม (Classical test theory)*. กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกร์มหาวิทยาลัย.

ศิริรัตน์ ศรีสว่าง. (2558). *ปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์* (วิทยานิพนธ์ปริญญามหาบัณฑิต). ปทุมธานี: มหาวิทยาลัยธรรมศาสตร์

ศูนย์การเรียนรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล. (2563). *การคุ้มครองความเป็นส่วนตัว Big Data และ GDPR ในการพัฒนาเศรษฐกิจดิจิทัล*. สืบค้นจาก: https://egovernment-forum.com/assets/files/Privacy%20Data%20Protection.pdf

ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย. (2562). *รายงานปัญหาธุรกรรมทางอิเล็กทรอนิกส์*. รายงานประจำปี. กรุงเทพฯ: ธนาคารแห่งประเทศไทย.

ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย. (2563). *การกำกับดูแลการให้บริการแก่ลูกค้าอย่างเป็นธรรม*. สืบค้นจาก: https://www.1213.or.th/th/AnnualReport2020_BOX12

ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย. (2563). *ภัยทางการเงิน กลโกงออนไลน์อื่นๆ*. สืบค้นจาก: https://www.1213.or.th/th/finfrauds/OnlineCrime/Pages/OnlineCrime.aspx

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย. (2562). *บทความเชิงเทคนิค*. สืบค้นจาก: https://www.thaicert.or.th/papers/technical/papers-technical.html

ศูนย์วิจัยกฎหมายและการพัฒนา จุฬาลงกรณ์มหาวิทยาลัย. (2561). *Thailand Data Protection Guidelines 2.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล* . พิมพ์ครั้งที่ 1. กรุงเทพฯ : โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

ศูนย์วิจัยเศรษฐกิจ ธุรกิจและเศรษฐกิจฐานราก ธนาคารออมสิน. (2562). *การเปลี่ยนแปลงตามกระแสของเทคโนโลยี*. รายงานภาวะเศรษฐกิจและแนวโน้มรายไตรมาส กรุงเทพฯ: ศูนย์วิจัยธนาคารออมสิน

สถาบันวิจัยเพื่อการพัฒนาประเทศไทย. (2562). *ความเป็นส่วนตัวและข้อมูลส่วนบุคคลสำหรับผู้อ่าน*. สืบค้นจาก: https://tdri.or.th/2019/08/personal-data-protection-act/

สถาบันวิจัยและบริการวิชาการ มหาวิทยาลัยอัสสัมชัญ. (2559). *ผลวิจัยเชิงสำรวจการทำธุรกรรมทางการเงินผ่านโทรศัพท์มือถือของคนกรุงเทพฯ*. รายงานการวิจัย กรุงเทพฯ: มหาวิทยาลัยอัสสัมชัญ.

สถาบันวิทยาการตลาดทุน. (2560). *สังคมไร้เงินสด (Cashless Society)*. สืบค้นจาก: https://www.cma.in.th/cma/uploadFile/downloadFile?filename=SavingThroughSpendingCMA26.pdf

สมชาย วรกิจเกษมสกุล. (2554). *ระเบียบวิธีการวิจัยทางพฤติกรรมศาสตร์และสังคมศาสตร์*. อุดรธานี: อักษรศิลป์การพิมพ์.

สมาคมผู้ดูแลเว็บไทย. (2562). *การตลาดออนไลน์*. สืบค้นจาก: https://www.webmaster.or.th/articles/online-marketing

สมาคมประชาสัมพันธ์ไทย. (2563). *ข้อมูลส่วนบุคคลออนไลน์*. สืบค้นจาก: http://www.prthailand.com/news/news-140701-01.shtml

สมาร์ทเอสเอ็มอี. (2560). *ผู้ประกอบการในยุคดิจิทัล*. รายงานการวิจัย กรุงเทพฯ: ทรูบิสิเนส.

สายกำกับสถาบันการเงิน ธนาคารแห่งประเทศไทย. (2557). *ขอบเขตกระบวนการทำธุรกรรมการเงินผ่านช่องทางอิเล็กทรอนิกส์สำหรับลูกค้ารายย่อย*. สืบค้นจาก: https://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/RiskMgt_Manual/Documents/IT_BestPractices-PhaseII.pdf

สัญชัย อุปะเดีย. (2553). *ปัจจัยด้านการรับรู้เกี่ยวกับระบบพาณิชย์อิเล็กทรอนิกส์ที่ส่งผลต่อการตัดสินใจใช้บริการชำระเงินผ่านระบบอิเล็กทรอนิกส์ของประชาชนในเขตพื้นที่กรุงเทพมหานคร*. การศึกษาเฉพาะบุคคล หลักสูตรบริหารธุรกิจมหาบัณฑิต, บัณฑิตวิทยาลัย มหาวิทยาลัยกรุงเทพ.

สุรัสสา ลิมปพานนท์ (2561) *ปัจจัยที่ส่งผลต่อพฤติกรรมผู้บริโภคเจนเนอเรชันวายในการเปิดใช้งานการชำระสินค้าและบริการผ่านอีวอลเลท ในเขตพื้นที่กรุงเทพมหานคร*. การค้นคว้าอิสระศิลปศาสตรมหาบัณฑิต, คณะนิเทศศาสตร์และนวัตกรรมการจัดการ สถาบันบัณฑิตพัฒนบริหารศาสตร์.

สุภารัตน์ แก้วสุทธิ. (2553). *พฤติกรรมการใช้อินเทอร์เน็ต การรู้เท่าทันสื่อ และพฤติกรรมการป้องกันตัวเอง จากการละเมิดสิทธิส่วนบุคคลทางอินเทอร์เน็ต*. วิทยานิพนธ์ นิเทศศาสตรมหาบัณฑิต, คณะนิเทศศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. (2557). *พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2551*. สืบค้นจาก: https://isoc.msu.ac.th/ICT_Law/22.pdf

สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2562). *กฎหมายและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล*. สืบค้นจาก: http://thainews.prd.go.th/th/news/detail/TCATG190930133235193

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2557). *แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล*. สืบค้นจาก: https://www.etda.or.th/download-publishing/12/

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2557). *รายงานผลสำรวจผู้ใช้อินเทอร์เน็ตในประเทศไทยปี 2557*. สืบค้นจาก: https://www.etda.or.th/publishing-detail/thailand-internet-user-profile-2014.html

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2558). *พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์*. สืบค้นจาก: https://www.etda.or.th/files/1/files/26.pdf

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2559). *รายงานผลสำรวจผู้ใช้อินเทอร์เน็ตในประเทศไทยปี 2559*. สืบค้นจาก: https://www.etda.or.th/publishing-detail/thailand-internet-user-profile-2016.html

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2560). *รู้ทันภัยไซเบอร์ทำธุรกรรมออนไลน์อย่างไรให้หายห่วง*. พิมพ์ครั้งที่ 1. กรุงเทพฯ : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2561). *รายงานผลสำรวจผู้ใช้อินเทอร์เน็ตในประเทศไทยปี 2561*. สืบค้นจาก: https://www.etda.or.th/publishing-detail/thailand-internet-user-profile-2018.html

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2563). *รายงานผลสำรวจผู้ใช้*

อินเทอร์เน็ตในประเทศไทยปี 2563. สืบค้นจาก: https://www.etda.or.th/publishing-detail/thailand-internet-user-profile-2020.html

สำนักงานสถิติแห่งชาติ. (2561). *การสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน*. รายงานการวิจัยไตรมาส 1 กรุงเทพฯ: สำนักงานสถิติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

สำนักยุทธศาสตร์และประเมินผล กรุงเทพมหานคร. (2560). *ศูนย์ข้อมูลกรุงเทพมหานคร แผนพัฒนากรุงเทพมหานคร ระยะ 12 ปี (พ.ศ. 2552-2563)*. สืบค้นจาก: http://203.155.220.230/bmainfo/docs/plans/1plandevelopmentyear(%202552-2563).pdf

อุทัยทิพย์ เจี่ยวิวรรธน์กุล. (2558). *วิธีการสุ่มตัวอย่างการวิจัย โครงการ Research Zone: Phase 6*. สืบค้นจาก: http://rlc.nrct.go.th/seminar/uploadfile/file_20100825035745.doc

อุไรพร ชลสิริรุ่งสกุล. (2554). *Digital Marketing ไอเดียลัดปฏิวัติการตลาด*. พิมพ์ครั้งที่ 1. กรุงเทพฯ : กรุงเทพธุรกิจ.

ภาคผนวก

ภาคผนวก ก

เครื่องมือที่ใช้ในการวิจัย

แบบสอบถามเพื่อการวิจัย

เรื่องปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคล
บนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น

<u>คำชี้แจง</u>

แบบสอบถามฉบับนี้ มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้นในเขตกรุงเทพมหานครและปริมณฑล ผู้วิจัยขอความอนุเคราะห์และความร่วมมือจากท่านให้ความกรุณาตอบแบบสอบถามนี้ โดยปฏิบัติตามคำชี้แจงของแบบสอบถามแต่ละตอน และเนื่องจากแบบสอบถามประกอบด้วยคำถามหลายส่วน จึงขอให้ท่านอ่านคำถามแต่ละข้อให้เข้าใจอย่างชัดเจน และขอให้ตอบตรงตามความเป็นจริงให้มากที่สุดและขอให้ตอบครบทุกข้อคำถาม

การตอบแบบสอบถามเพื่อการวิจัยนี้ ประกอบด้วย 3 ตอน รวมทั้งสิ้นจำนวน 122 ข้อ และใช้เวลาในการตอบแบบสอบถามโดยประมาณ 30-45 นาที ดังนี้

ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม (8 ข้อ)

ตอนที่ 2 พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (29 ข้อ)

ตอนที่ 3 ความคิดเห็นต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (85 ข้อ)

ผู้วิจัยขอรับรองว่าข้อมูลส่วนบุคคลและคำตอบทั้งหมดจะถูกเก็บไว้เป็นความลับเพื่อใช้ประโยชน์ในการวิจัยเท่านั้น ซึ่งเป็นการวิเคราะห์ข้อมูลงานวิจัยในภาพรวมและการตอบแบบสอบถามจะไม่มีผลกระทบใดๆ ต่อท่านทั้งสิ้น ทั้งนี้ ผู้วิจัยขอขอบคุณที่ท่านสละเวลาอันมีค่าในการตอบแบบสอบถามเพื่อการวิจัยนี้ และโครงการวิจัยนี้ผ่านการพิจารณาจริยธรรมสำหรับโครงการวิจัยที่ทำในมนุษย์แล้ว หมายเลขรับรอง SWUEC-G-299/2563X

นายธีรศักดิ์ พลพันธ์ (โทร. 086-788-6687)
นิสิตปริญญาเอก สาขาการวิจัยพฤติกรรมศาสตร์ประยุกต์
สถาบันวิจัยพฤติกรรมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ

นิยามศัพท์ของแบบสอบถามเพื่อการวิจัยนี้

ธุรกรรมทางอิเล็กทรอนิกส์ หมายถึง การเข้าใช้บริการธุรกรรมทางการเงินผ่านช่องทางอิเล็กทรอนิกส์ ที่มีการระบุตัวตนของผู้ใช้งานและสามารถดำเนินการทำธุรกรรมทางการเงินได้ด้วยตนเองในฐานะผู้บริโภค

เครื่องคอมพิวเตอร์ หมายถึง อุปกรณ์อิเล็กทรอนิกส์ในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จำแนกออกเป็น 2 ช่องทาง ได้แก่ 1) เครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งรวมทั้งคอมพิวเตอร์แบบพกพา (Laptop) และคอมพิวเตอร์แบบรับข้อมูลด้วยการเขียนบนจอภาพ (Tablet) และรวมไปถึง 2) สมาร์ทโฟน (Smart Phone)

ข้อมูลส่วนบุคคล หมายถึง ข้อมูลของบุคคลธรรมดาที่สามารถระบุหรือเชื่อมโยงถึงตัวบุคคลในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ไม่ว่าจะทางตรงหรือทางอ้อม และแสดงถึงการเป็นเจ้าของข้อมูล เช่น ชื่อจริง นามสกุลจริง หมายเลขบัตรประจำตัวประชาชน วันเดือนปีเกิด หมายเลขโทรศัพท์ หมายเลขบัญชีธนาคาร อีเมล์ รูปถ่าย ที่อยู่ ประวัติทางการศึกษา หมายเลขบัตรเงินอิเล็กทรอนิกส์ เป็นต้น

ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

คำชี้แจง กรุณาทำเครื่องหมายถูกต้อง ✓ ลงในช่อง ☐ หน้าข้อความหรือเติมข้อความลงในช่องว่างที่ตรงกับความเป็นจริงของท่าน

1. **อายุ** (เศษของ 6 เดือนคิดเป็น 1 ปี) ระบุอายุ.....ปี

(หากตอบ อายุมากกว่า 29 ปี.....ให้สิ้นสุดการตอบแบบสอบถาม)

2. **ในรอบ 6 เดือนติดต่อกันที่ผ่านมา ท่านมีความถี่ในการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์**

☐ โดยเฉลี่ยต่ำกว่าหรือเท่ากับ 5 ครั้ง/เดือน

(หากตอบ โดยเฉลี่ยต่ำกว่าหรือเท่ากับ 5 ครั้ง/เดือน.....ให้สิ้นสุดการตอบแบบสอบถาม)

☐ โดยเฉลี่ย 6-10 ครั้ง/เดือน

☐ โดยเฉลี่ย 11-15 ครั้ง/เดือน

☐ โดยเฉลี่ย มากกว่า 15 ครั้ง/เดือน

3. **เพศ** ☐ ชาย ☐ หญิง ☐ เพศทางเลือก

4. **ระดับการศึกษาสูงสุด**

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ ปริญญาโทหรือสูงกว่า

5. **สถานภาพสมรส**

☐ โสด ☐ สมรส ☐ หย่าร้าง ☐ อยู่ร่วมกันโดยไม่ได้แต่งงาน

6. **เขตพื้นที่ปฏิบัติงาน**

☐ กรุงเทพมหานคร ☐ นนทบุรี ☐ ปทุมธานี

7. **ประเภทของหน่วยงาน**

☐ ราชการ/รัฐวิสาหกิจ ☐ องค์กรธุรกิจเอกชน ☐ อื่นๆ (ระบุ).....

8. **ระดับเงินเดือนปัจจุบัน**

☐ น้อยกว่าหรือเท่ากับ 15,000 บาท ☐ 15,001-20,000 บาท

☐ 20,001-25,000 บาท ☐ 25,001-30,000 บาท

☐ 30,001-35,000 บาท ☐ มากกว่า 35,000 บาท

ตอนที่ 2 พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

คำชี้แจง กรุณาอ่านข้อความแต่ละข้ออย่างละเอียด แล้วโปรดเลือกคำตอบโดยทำเครื่องหมายถูกต้อง ✓ ลงในช่องที่ตรงกับสภาพความเป็นจริงของการเกิดพฤติกรรมของท่านมากที่สุดเพียงข้อเดียวและโปรดตอบคำถามให้ครบทุกข้อ

ข้อคำถาม	การปฏิบัติตนเพื่อปกป้องข้อมูลส่วนบุคคล					
	จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย
	6	5	4	3	2	1
การปฏิบัติตนเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป “ในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์.....”						
1. ฉันตั้งรหัสผ่าน (Password) ที่คาดเดาได้ยาก						
2. ฉันเปลี่ยนรหัสผ่านทุก 30-45 วัน						
3. ฉันนำรหัสผ่านเดิม วนกลับมาใช้ใหม่						
4. ฉันไม่จดบันทึกชื่อผู้ใช้งาน (Username) และรหัสผ่านไว้เป็นลายลักษณ์อักษรหรือในสมาร์ทโฟน						
5. ฉันบอกชื่อผู้ใช้งานและรหัสผ่านกับบุคคลใกล้ชิด						
6. ฉันใช้บริการกับผู้ให้บริการที่แจ้งเงื่อนไขและรายละเอียดนโยบายคุ้มครองความเป็นส่วนตัว						
7. ฉันอ่านนโยบายคุ้มครองความเป็นส่วนตัวก่อนกดยอมรับข้อตกลง						
8. ในแต่ละวันฉันไม่ได้ตั้งค่าจำกัดวงเงิน						
9. ฉันมองบุคคลรอบตัวและใช้มือปกปิดการกรอกข้อมูลระหว่างทำรายการ						
10. ฉันไม่ใช้บริการผ่านคอมพิวเตอร์ที่ใช้งานร่วมกับบุคคลอื่น						
11. ฉันให้ข้อมูลส่วนบุคคลเฉพาะที่จำเป็นในการสมัครเข้าใช้บริการ						
12. ฉันไม่เปิดเผยข้อมูลผ่านสื่อสังคมออนไลน์ที่เชื่อมโยงไปถึงข้อมูลทางการเงินอิเล็กทรอนิกส์						
13. ฉันเลือกเข้าร่วมกิจกรรมส่งเสริมการขายบางอย่างกับผู้ให้บริการ						
14. ฉันไม่เข้าร่วมกิจกรรมประเภทเกมตอบคำถามชิงรางวัลจากการเข้าใช้บริการ						
15. ฉันกดปุ่มออกจากระบบ (Logout) ทุกครั้งหลังเสร็จสิ้นการใช้บริการ						

ข้อคำถาม	การปฏิบัติตนเพื่อปกป้องข้อมูลส่วนบุคคล					
	จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย
	6	5	4	3	2	1
การปฏิบัติตนเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค “ในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์.....”						
1. หากจำเป็นต้องนำเครื่องคอมพิวเตอร์ไปซ่อมแซมยังร้านบริการ ฉันตรวจสอบและลบข้อมูลส่วนบุคคล						
2. ฉันตั้งค่ารหัสผ่านปลดล็อคการแสดงผลหน้าจอ						
3. ฉันดัดแปลงหรือแก้ไขระบบปฏิบัติการ (Jailbreak/Root) เข้ากับเครื่องคอมพิวเตอร์						
4. ฉันปล่อยให้ระบบปฏิบัติการล้าสมัยจนส่งผลต่อการเข้าใช้บริการ						
5. ฉันตรวจสอบที่มาของแอปพลิเคชันก่อนทำการดาวน์โหลดเพื่อเข้าใช้บริการ						
6. ฉันไม่เข้าใช้บริการบนเว็บไซต์ที่ให้ยอมรับเงื่อนไขการใช้งานคุกกี้ (Accept Cookies)						
7. หากเข้าใช้บริการบนเว็บไซต์ ฉันใช้งานผ่านโหมดส่วนตัว (Private Mode) หรือไม่ระบุตัวตน (Incognito Mode)						
8. ฉันลบประวัติ (History) การเข้าใช้บริการทุกครั้ง						
9. ฉันตั้งค่าความเป็นส่วนตัวขั้นสูง (Advanced) เพื่อเข้าใช้บริการ						
10. ฉันตั้งค่าปิดกั้น (Blocked) รับข้อความอีเมล์ไว้ก่อนเสมอ หากเป็นบุคคลหรือองค์กรที่ฉันไม่รู้จัก						
11. ฉันสร้างอีเมล์เพื่อใช้บริการธุรกรรมโดยเฉพาะ						
12. ฉันตั้งค่ายืนยันตัวตนแบบสองชั้น (Two-factor Authentication) ในความเป็นเจ้าของเพื่อเข้าใช้บริการ						
13. ฉันเปิดใช้บริการด้วยวายฟายสาธารณะ (Public/Free Wi-Fi) เช่น ภายในร้านกาแฟ						
14. หากจำเป็นใช้บริการผ่านเครื่องคอมพิวเตอร์สาธารณะหรือบุคคลอื่น ฉันเปลี่ยนรหัสผ่านทุกครั้ง						

ตอนที่ 3 แบบสอบถามความรู้สึก ความความคิดเห็นของฉันที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

คำชี้แจง กรุณาอ่านข้อความแต่ละข้ออย่างละเอียด แล้วโปรดเลือกคำตอบโดยทำเครื่องหมายถูกต้อง ✓ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่านมากที่สุดเพียงข้อเดียวและโปรดตอบคำถามให้ครบทุกข้อ

ข้อคำถาม	ระดับความคิดเห็นของท่าน					
	จริงที่สุด	**จริง**	**ค่อนข้างจริง**	**ค่อนข้างไม่จริง**	**ไม่จริง**	**ไม่จริงเลย**
	6	5	4	3	2	1
ชุดที่ 1 การรับรู้ถึงโอกาสเสี่ยงที่บุคคลอื่นจะเข้าใช้งานแทนตนบนบริการธุรกรรมทางอิเล็กทรอนิกส์ “ในปัจจุบัน ฉันคิดว่าแอปพลิเคชันหรือโปรแกรมที่ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์.....”						
1. มีความเสี่ยงที่ข้อมูลส่วนบุคคลถูกขโมยโดยกลุ่มผู้ไม่หวังดี						
2. ผู้ให้บริการอาจจัดเก็บรักษาข้อมูลของฉันไว้ไม่เหมาะสม						
3. ฉันไม่มั่นใจมาตรการรักษาข้อมูลและนโยบายความเป็นส่วนตัวจากผู้ให้บริการ						
4. หากเป็นผู้ให้บริการที่มีชื่อเสียง ฉันไม่วิตกกังวลว่าข้อมูลจะถูกเปิดเผยและนำไปใช้โดยไม่ได้รับอนุญาต						
5. เป็นไปได้ที่ผู้ให้บริการเก็บข้อมูลส่วนบุคคลเพื่อหาผลประโยชน์ทางการตลาดและเผยแพร่ให้กับบุคคลที่สาม (Third Party)						
6. การเข้าใช้งานร่วมกันหลายแอปพลิเคชัน มีโอกาสที่บุคคลอื่นนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต						
7. เป็นไปได้ที่บุคคลอื่นพยายามเก็บข้อมูลของฉันโดยที่ไม่ได้รับอนุญาต ในขณะที่เข้าใช้บริการ						
8. ฉันมีโอกาสตกเป็นผู้เคราะห์ร้าย ถูกขโมยข้อมูลส่วนบุคคลจากการใช้บริการ						

ข้อคำถาม	ระดับความคิดเห็นของท่าน					
	จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย
	6	5	4	3	2	1
ชุดที่ 2 การรับรู้ถึงความรุนแรงที่บุคคลอื่นจะเข้าใช้งานแทนตนบนบริการธุรกรรมทางอิเล็กทรอนิกส์ “ฉันคิดว่า...การที่บุคคลอื่นเข้าถึงข้อมูลส่วนบุคคลของฉันจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์....”						
1. ถูกนำเงินออกจากบัญชีธนาคาร ทำให้ฉันสูญเสียรายได้						
2. ทราบสถานะทางการเงิน ทรัพย์สินที่มีค่าของฉัน						
3. การลงทุนผ่านบริการธุรกรรม เช่น ออมเงิน กองทุน อาจถูกปรับเปลี่ยนแก้ไขและทำให้เข้าใช้งานไม่ได้						
4. ถูกสวมรอย แอบอ้างชื่อฉันเพื่อหลอกให้บุคคลใกล้ชิดโอนเงินเข้าบัญชีคนร้าย						
5. เป็นเรื่องที่น่ากลัว เพราะบุกรุกความเป็นส่วนตัว						
6. ทราบถึงข้อมูลที่พักหรือสถานที่ทำงานของฉันได้						
7.ฉันอาจถูกทำร้ายร่างกายเพื่อปกป้องทรัพย์สินมีค่า						
8. ฉันอาจประสบอันตรายถึงขั้นทุพพลภาพหรือเสียชีวิตเพื่อปกป้องทรัพย์สินที่มีค่า						
9. อาจทำให้ข้อมูลสุขภาพของฉันถูกเปิดเผยได้						

ข้อคำถาม	ระดับความคิดเห็นของท่าน					
	จริงที่สุด	**จริง**	**ค่อนข้างจริง**	**ค่อนข้างไม่จริง**	**ไม่จริง**	**ไม่จริงเลย**
	6	5	4	3	2	1
ชุดที่ 3 แบบวัดความคาดหวังในผลลัพธ์การปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ “หากฉันปฏิบัติตนตามคู่มือแนะนำการดูแลรักษาข้อมูลส่วนบุคคล….”						
1. หากฉันตั้งรหัสผ่านที่คาดเดาได้ยาก จะทำให้บุคคลอื่นเข้าถึงข้อมูลยากขึ้น						
2. การเปลี่ยนรหัสผ่านทุกๆ 30 วัน เป็นการรักษาความปลอดภัยข้อมูลของฉัน						
3. การหมั่นตรวจสอบรายการธุรกรรมย้อนหลัง ช่วยลดโอกาสที่บุคคลอื่นเข้าถึงข้อมูลของฉันได้						
4. การมีความรู้ดูแลรักษาเครื่องคอมพิวเตอร์ ช่วยลดโอกาสที่บุคคลอื่นเข้าถึงข้อมูลของฉันได้						
5. การปฏิบัติตามคู่มือหรือคลิปแนะนำเป็นขั้นตอน (Step by Step) ในการลบแอปพลิเคชันที่ไม่ใช้งาน เป็นวิธีปกป้องข้อมูลที่เหมาะสม						
6. การไม่เปิดใช้บริการด้วยวายฟายสาธารณะ เป็นวิธีปกป้องข้อมูลของฉันให้ปลอดภัย						
7. ฉันตั้งค่ารหัสผ่านปลดล็อคการแสดงผลหน้าจอไม่ได้ทำให้เกิดความปลอดภัยในข้อมูล						

ข้อคำถาม	ระดับความคิดเห็นของท่าน					
	จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย
	6	5	4	3	2	1
ชุดที่ 4 แบบวัดความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ “ฉันมีความสามารถ/ทักษะ....”						
1. ฉันสามารถใช้เครื่องคอมพิวเตอร์เชื่อมต่อกับบริการธุรกรรมได้						
2. ฉันไม่เปิดโอกาสให้บุคคลอื่นเข้าถึงข้อมูลส่วนบุคคลของฉัน						
3. ฉันไม่สามารถแนะนำผู้อื่น เพื่อปกป้องข้อมูลส่วนบุคคลให้ปลอดภัย						
4. ฉันจัดทำบันทึกแผนฉุกเฉิน เช่น ขั้นตอนเปลี่ยนรหัสผ่าน ขอระงับบริการ ที่เข้าใจได้ง่าย						
5. ฉันใช้บันทึกแผนฉุกเฉินตามขั้นตอน เพื่อปกป้องข้อมูลได้						
6. ฉันสังเกตถึงความผิดปกติในการแสดงผลข้อมูลบนหน้าจอจากการเข้าใช้บริการ						
7. ฉันศึกษาตามแผนปฏิบัติการเข้ายืนยันตัวตนและขอระงับบริการจากผู้ให้บริการได้						
8. ฉันควบคุมตนเองให้ปฏิบัติแผนฉุกเฉินที่ได้ทำการบันทึก						
9. ฉันจัดการกับผู้ต้องการขโมยข้อมูลส่วนบุคคลได้ด้วยตัวเอง						
10. ฉันไม่สามารถใช้สติแก้ไขปัญหา เพื่อปกป้องข้อมูลส่วนบุคคล						
11. หากมีบุคคลอื่นอาจเข้าถึงข้อมูล ฉันวิเคราะห์สาเหตุ และลำดับเหตุการณ์ได้						
12. ฉันปรับเปลี่ยนหรือแก้ไขสิทธิ์ในการเข้าถึงข้อมูลส่วนบุคคลได้รวดเร็ว						
13. ฉันแยกแยะให้ข้อมูลที่ถูกต้องและจำเป็นต่อการเป็นเจ้าของข้อมูลได้						

ข้อคำถาม	ระดับความคิดเห็นของท่าน					
	จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย
	6	5	4	3	2	1
ชุดที่ 5 แบบวัดความคาดหวังในต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ “หากฉันจ่ายเงินเพิ่มให้กับผู้ให้บริการธุรกรรม หรือทุ่มเทศึกษาข้อมูล ฉันคาดว่า/จะทำให้....”						
1. ฉันได้สิทธิพิเศษในการดูแลรักษาข้อมูลและเป็นสมาชิกในระดับที่สูงขึ้น เช่น VIP, Platinum						
2. หากไม่สามารถเข้าใช้บริการได้ ฉันไปศูนย์ให้บริการตรวจสอบสถานะเครื่องคอมพิวเตอร์ทันที						
3. ฉันควบคุมค่าใช้จ่ายที่เพิ่มขึ้นในแต่ละเดือนเพื่อปกป้องข้อมูลส่วนบุคคลได้						
4. การติดตามข่าวสารอาชญากรรมทางธุรกรรมอิเล็กทรอนิกส์ ทำให้ฉันลดโอกาสเสี่ยงที่ข้อมูลถูกนำไปใช้โดยไม่ได้รับอนุญาต						
5. หากฉันตั้งใจศึกษาขั้นตอนปกป้องข้อมูล จะเพิ่มความมั่นใจและความปลอดภัยในการเข้าใช้บริการ						
6. การใช้เวลาศึกษาเรียนรู้ขั้นตอนการปกป้องข้อมูลทำให้ฉันไม่เกิดปัญหาถูกขโมยข้อมูลที่อาจจะตามมา						
7. ฉันไม่สามารถเรียนรู้ขั้นตอนปกป้องข้อมูลได้เนื่องจากมีภาระงานอื่นที่ต้องทำจำนวนมาก						

ข้อคำถาม	ระดับความคิดเห็นของท่าน					
	จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย
	6	5	4	3	2	1
ชุดที่ 6 แบบวัดคุณลักษณะของระบบในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ "ฉันคิดว่า..<u>โดยภาพรวม</u>แอปพลิเคชันธุรกรรมทางอิเล็กทรอนิกส์เพื่อจัดการตั้งค่าปกป้องข้อมูล ในปัจจุบันมีลักษณะ..."						
1. มีข้อมูลเนื้อหาครบถ้วนสมบูรณ์และน่าเชื่อถือ						
2. สามารถปรับแต่งและเข้าถึงความต้องการเฉพาะของฉันได้						
3. ประมวลผลข้อมูลได้รวดเร็ว						
4. ใช้ภาพกราฟิกเชิงสัญลักษณ์และมีปุ่มกดที่สามารถเข้าใจง่าย						
5. ใช้คำอธิบายและคำศัพท์ที่เข้าใจง่าย คุ้นเคย						
6. ค้นหาข้อมูลในการตั้งค่าข้อมูลที่สะดวกและง่าย						
7. นำเสนอภาพแสดงตัวอย่างที่ยังไม่ชัดเจน						

ข้อคำถาม	ระดับความคิดเห็นของท่าน					
	จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย
	6	5	4	3	2	1
ชุดที่ 7 แบบวัดการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ “บุคคลที่ฉันมีความใกล้ชิด เช่น คนในครอบครัว ญาติ เพื่อนสนิท เพื่อนร่วมงาน มักจะ...”						
1. แสดงให้ฉันรู้ว่าการตั้งค่าข้อมูล เป็นสิ่งที่มีคุณค่าและควรปฏิบัติ						
2. การได้เห็นบุคคลที่ใกล้ชิดตั้งค่าข้อมูล ไม่กระตุ้นให้ฉันตั้งค่าปกป้องข้อมูลตามไปด้วย						
3. คอยเตือนฉันให้ตั้งค่าปกป้องข้อมูล เมื่อเห็นว่าฉันละเลยและไม่ปฏิบัติ						
4. ฉันทำในสิ่งที่บุคคลใกล้ชิด คิดว่าฉันควรตั้งค่าในการปกป้องข้อมูลส่วนบุคคล						
5. การติดตามข่าวสารจากไอทีบล็อกเกอร์ (เช่น IT24hrs.com, LDA ลดา) ทำให้ฉันสนใจจัดการตั้งค่าปกป้องข้อมูล						
6. ฉันตั้งค่าปกป้องข้อมูล ตามที่ไอทีบล็อกเกอร์ให้ความคิดเห็นว่าเป็นประโยชน์ทางการเงิน						
7. ไอทีบล็อกเกอร์ไม่ใช่แรงผลักดันให้ฉันตั้งค่าปกป้องข้อมูล						
8. ฉันกระทำตามอย่างไอทีบล็อกเกอร์บอกเล่าข้อมูลในการจัดการตั้งค่าการปกป้องข้อมูล						
9. ฉันมีแนวโน้มตั้งค่าข้อมูลส่วนบุคคล ตามที่ไอทีบล็อกเกอร์แนะนำ						

ข้อคำถาม	ระดับความคิดเห็นของท่าน					
	จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย
	6	5	4	3	2	1
ชุดที่ 8 แบบวัดการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ "การตั้งค่าการปกป้องข้อมูลส่วนบุคคล ช่วยให้ฉัน....."						
1. ป้องกันปัญหาการถูกขโมยข้อมูลส่วนบุคคล						
2. ได้เรียนรู้ รักษาความเป็นส่วนตัวที่ทันกับเหตุการณ์						
3. เพิ่มขีดความสามารถการใช้บริการที่เป็นประโยชน์						
4. ช่วยลดจำนวนการถูกโจรกรรมข้อมูลในปัจจุบันได้						
5. เป็นผู้ใช้บริการที่ดี มีความปลอดภัยด้านข้อมูลสูง						
6. ช่วยรักษาระดับความปลอดภัยในข้อมูลของผู้ใช้บริการได้						

ข้อคำถาม	ระดับความคิดเห็นของท่าน					
	จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย
	6	5	4	3	2	1
ชุดที่ 9 แบบวัดการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ "ฉันคิดว่า วิธีการ/ขั้นตอนตั้งค่าการปกป้องข้อมูลส่วนบุคคลนั้น เป็นเรื่องที่....."						
1. เป็นเรื่องง่ายที่จะเรียนรู้						
2. ฉันสามารถทำความเข้าใจได้ด้วยตนเอง						
3. ฉันสามารถฝึกปฏิบัติตามขั้นตอนได้อย่างสะดวกและรวดเร็ว						
4. ฉันไม่ต้องใช้ความพยายามมากนัก						
5. ฉันสามารถทำตามขั้นตอนการตั้งค่า ตามความต้องการที่มีวัตถุประสงค์เฉพาะ						
6. ฉันรู้สึกกระตือรือร้น เมื่อต้องเรียนรู้การตั้งค่าให้ทันต่อเหตุการณ์ปัจจุบัน						

ข้อคำถาม	ระดับความคิดเห็นของท่าน					
	จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย
	6	5	4	3	2	1
ชุดที่ 10 แบบวัดทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ “ฉันคิดว่า การจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล เป็นเรื่องที่.....”						
1. เป็นสิ่งควรประพฤติ ปฏิบัติตน						
2. เป็นแนวปฏิบัติที่ดีด้านความปลอดภัย						
3. เป็นเรื่องที่ยินดีปฏิบัติตาม						
4. การตั้งค่าข้อมูลสร้างความปลอดภัยกว่าการที่ไม่ตั้งค่าปกป้องใดๆ เลย						
5. ความปลอดภัยในข้อมูลส่วนบุคคลของฉันมีมากขึ้น						
6. เป็นการเตรียมความพร้อมและฝึกการใช้งานเพื่อปกป้องข้อมูลอยู่เสมอ						
7. เป็นประโยชน์และสำคัญในการใช้ชีวิตที่ไม่ประมาททางการเงิน						
8. ช่วยให้ฉันได้ศึกษาความรู้ด้านเทคโนโลยีใหม่ๆ						

ข้อคำถาม	ระดับความคิดเห็นของท่าน					
	จริงที่สุด	จริง	ค่อนข้างจริง	ค่อนข้างไม่จริง	ไม่จริง	ไม่จริงเลย
	6	5	4	3	2	1
ชุดที่ 11 แบบวัดความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ฉันตั้งใจจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล....						
1. ฉันตั้งใจตั้งค่าข้อมูลเมื่อมีโอกาสอย่างแน่นอน						
2. ฉันพยายามหาวิธีปกป้องข้อมูลให้ปลอดภัยอยู่เสมอ						
3. ฉันสนใจศึกษาข้อปฏิบัติดูแลรักษาข้อมูลเป็นประจำ						
4. ฉันพยายามควบคุมเปิดเผยข้อมูลเฉพาะที่จำเป็นกับผู้ให้บริการ						
5. ฉันมีแนวโน้มปฏิบัติตามขั้นตอนจัดการตั้งค่าข้อมูล						

****กรุณาตอบแบบสอบถามให้ครบทุกข้อ ขอขอบคุณทุกท่านที่ให้ความร่วมมือ****

ภาคผนวก ข

รายงานผลประเมินการตรวจสอบความเหมาะสม ความตรงด้านเนื้อหา

รายงานผลประเมินการตรวจสอบความเหมาะสม ความตรงด้านเนื้อหา สำนวนภาษา และความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย
(Index of Item - Objective Congruence: IOC)

(ผลพิจารณาความคิดเห็นของผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญที่มีต่อเครื่องมือวัดงานวิจัย)

เรื่อง ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น

CAUSAL FACTORS OF PRIVACY DATA PROTECTION BEHAVIORS ON ELECTRONICS TRANSACTIONS IN FIRST JOBBERS

(นายธีรศักดิ์ พลพันธ์ นิสิตปริญญาเอก สาขาการวิจัยพฤติกรรมศาสตร์ประยุกต์
มหาวิทยาลัยศรีนครินทรวิโรฒ)

รายงานผลประเมินตรวจสอบความเหมาะสม ความตรงด้านเนื้อหา (Content Validity)

ผลประเมินนี้ เป็นการตรวจประเมินความเหมาะสมของความตรงด้านเนื้อหา สำนวนภาษา ความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ และคุณภาพของเครื่องมือวัดงานวิจัย เรื่องปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น ซึ่งผู้วิจัยได้นำเสนอเครื่องมือวัดงานวิจัยต่ออาจารย์ที่ปรึกษาและผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญ เพื่อทำการตรวจสอบความครบถ้วน ความเหมาะสมของความตรงด้านเนื้อหาของเครื่องมือวัดงานวิจัย โดยมีผู้ทรงคุณวุฒิจำนวน 5 ท่าน ได้พิจารณาเครื่องมือวัดงานวิจัย จากหน่วยงานดังต่อไปนี้

1.สถาบันวิจัยพฤติกรรมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ จำนวน 3 ท่าน ประกอบด้วย ผู้ช่วยศาสตราจารย์ ดร. นริสรา พึ่งโพธิ์สภ, ผู้ช่วยศาสตราจารย์ ดร. พิชญาณี พูนผล และอาจารย์ ดร. ก่อเกียรติ์ มหาวีรชาติกุล

2.คณะสถิติประยุกต์ สถาบันบัณฑิตพัฒนบริหารศาสตร์ จำนวน 1 ท่าน คือ รองศาสตราจารย์ ดร. นิธินันท์ ธรรมากรนนท์

3.คณะวิศวกรรมศาสตร์และเทคโนโลยี สถาบันการจัดการปัญญาภิวัฒน์ จำนวน 1 ท่าน คือ ผู้ช่วยศาสตราจารย์ ดร. อดิศร แขกซอง

วิธีการและขั้นตอนการประเมินความเหมาะสมของความตรงด้านเนื้อหา

วิธีการและขั้นตอนการประเมินความเหมาะสมของความตรงด้านเนื้อหา มีดังนี้

1. ผู้วิจัยได้จัดกระทำโดยการนำนิยามเชิงปฏิบัติการ (Operational Definition) และข้อคำถามที่ได้สร้างขึ้นส่งไปยังผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญ เพื่อพิจารณาตรวจสอบความครบถ้วน ความเหมาะสมของความตรงด้านเนื้อหา สำนวนภาษา และความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ของเครื่องมือวัดงานวิจัย ซึ่งมีเกณฑ์การให้คะแนน/คะแนนการพิจารณา ดังนี้

ให้คะแนน -1 หมายถึง แน่ใจว่าข้อคำถามนั้นไม่เหมาะสม/ไม่สอดคล้องกับวัตถุประสงค์

ให้คะแนน 0 หมายถึง ไม่แน่ใจว่าข้อคำถามนั้นเหมาะสม/สอดคล้องกับวัตถุประสงค์หรือไม่

ให้คะแนน +1 หมายถึง แน่ใจว่าข้อคำถามนั้นมีความเหมาะสม/สอดคล้องกับวัตถุประสงค์

นอกจากนี้ หากข้อคำถามใดที่ไม่แน่ใจหรือไม่ตรงกับนิยามเชิงปฏิบัติการ และ/หรือไม่สอดคล้องกับวัตถุประสงค์ที่ใช้ในการวิจัยนี้ สามารถแสดงความคิดเห็น โดยเขียนข้อเสนอแนะหรือแก้ไขข้อคำถามนั้นๆ ได้

2. ผู้วิจัยใช้เกณฑ์วิธีการคำนวณค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย (Index of Item - Objective Congruence: IOC) โดยทุกข้อคำถามต้องผ่านเกณฑ์ค่าดัชนีความสอดคล้องที่มากกว่าหรือเท่ากับ 0.60 จึงจะถือว่ามีความสอดคล้องความตรงด้านเนื้อหา โดยการนำคะแนนที่ประเมินจากผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญ มาหาค่า IOC รายข้อ

จากสูตร $$IOC = \frac{\sum R}{N}$$

เมื่อ IOC คือ ค่าดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ของเครื่องมือวัด

$\sum R$ คือ ผลรวมของคะแนนจากผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญทั้งหมด

N คือ จำนวนผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญ

ตอนที่ 1 ข้อมูลชีวสังคมของกลุ่มตัวอย่าง

เป็นข้อคำถามสำหรับเก็บข้อมูลพื้นฐานของผู้ตอบแบบสอบถาม ประกอบด้วยข้อคำถามจำนวน 7 ข้อ ได้แก่ เพศ ระดับการศึกษาสูงสุด สถานภาพสมรส เขตพื้นที่ปฏิบัติงาน ประเภทของหน่วยงาน ลักษณะงานที่ปฏิบัติและระดับเงินเดือนปัจจุบัน เพื่อนำข้อมูลพื้นฐานนี้มาวิเคราะห์เชิงบรรยายลักษณะของกลุ่มตัวอย่าง และเงื่อนไขเกี่ยวกับคุณลักษณะเฉพาะของผู้ตอบแบบสอบถามจากการสอบถามคัดเลือก (Screening Question) ซึ่งเป็นคำถามคัดกรองเพื่อให้เป็นไปตามวัตถุประสงค์ของงานวิจัยนี้ ประกอบด้วยข้อคำถามเฉพาะเจาะจง จำนวน 2 ข้อ ได้แก่ ช่วงอายุ 20-29 ปี และความถี่ในการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ โดยเฉลี่ยมากกว่า 5 ครั้ง/เดือน ในรอบ 6 เดือนติดต่อกันที่ผ่านมา

ตารางที่ 1 ค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์และผลประเมินของตอนที่ 1 ข้อมูลชีวสังคมของกลุ่มตัวอย่าง

ข้อ	ข้อคำถามที่ใช้ในเครื่องมือวัด	คะแนนของผู้ทรงคุณวุฒิ (คนที่)					IOC	การแปลผลและข้อเสนอแนะ
		1	2	3	4	5		
ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม								
1	เพศ	+1	+1	+1	+1	+1	1.00	ใช้ได้ *(ควรเพิ่มกลุ่มเพศทางเลือก)*
2	อายุ	+1	+1	+1	0	+1	0.80	ใช้ได้ *(ควรปรับเป็น Ratio Scale)*
3	ความถี่ในการเข้าใช้บริการธุรกรรม	+1	+1	0	+1	+1	0.80	ใช้ได้
4	ระดับการศึกษาสูงสุด	+1	+1	0	+1	+1	0.80	ใช้ได้
5	สถานภาพสมรส	+1	+1	+1	0	+1	0.80	ใช้ได้*(เพิ่มกลุ่มอยู่ร่วมกันโดยไม่ได้แต่งงาน)*
6	เขตพื้นที่ปฏิบัติงาน	+1	+1	0	0	+1	0.60	ใช้ได้ *(ควรแยกเป็นชื่อจังหวัด)*
7	ประเภทของหน่วยงาน	+1	+1	+1	0	+1	0.80	ใช้ได้
8	ลักษณะงานที่ปฏิบัติ	0	+1	0	+1	0	0.40	*แบ่งกลุ่มงานยังไม่ชัดเจน+ควรลดข้อคำถาม*
9	ระดับเงินเดือนปัจจุบัน	+1	+1	0	+1	+1	0.80	ใช้ได้

โดยสรุป ตอนที่ 1 ข้อมูลชีวสังคมของกลุ่มตัวอย่าง นำมาจัดทำเป็นแบบสอบถามเพื่อการวิจัยจำนวน 8 ข้อและปรับตามข้อเสนอแนะของผู้ทรงคุณวุฒิ

ตอนที่ 2 พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์

ตารางที่ 2 ค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์และผลประเมินของตอนที่ 2 พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ในองค์ประกอบที่ 1 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป

ข้อ	ข้อคำถามที่ใช้ในเครื่องมือวัด	คะแนนของผู้ทรงคุณวุฒิ (คนที่)					IOC	การแปลผล และข้อเสนอแนะ
		1	2	3	4	5		
ตอนที่ 2 พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ องค์ประกอบที่ 1 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป								
1	ฉันได้ตั้งรหัสผ่าน เมื่อเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่ยากต่อการคาดเดา*(+)*	0	+1	+1	+1	+1	0.80	ใช้ได้ ***(ควรตั้งเป็นหัวข้อคำถาม**.., ปรับข้อความให้กระชับ,คำขยายผิดที่) "**ในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์**..." ฉันตั้งรหัสผ่านที่คาดเดาได้ยาก*
2	ฉันเลือกใช้รหัสผ่านที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น วัน/เดือน/ปีเกิด หมายเลขโทรศัพท์ หรือหมายเลขบัตรอื่นๆ ที่สำคัญของฉัน *(-)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *(ปรับข้อความให้กระชับ) ฉันเลือกใช้รหัสผ่านที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น วันเกิด เบอร์โทรศัพท์"*
3	เมื่อเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ผ่านทางแอปพลิเคชัน ฉันได้ใช้รหัสผ่านหมายเลขที่เรียงติดกัน *(-)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันใช้รหัสผ่านที่เป็นตัวเลขเรียงติดกัน เช่น 1234*
4	หากมีการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ในจำนวนหลายแอปพลิเคชัน ฉันไม่ใช้รหัสผ่านที่ซ้ำซ้อนกัน *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *(ประโยคซับซ้อน+ปรับข้อความให้กระชับ) ฉันใช้รหัสผ่านที่แตกต่างกันในแต่ละแอปพลิเคชัน*
5	ฉันทำการเปลี่ยนรหัสผ่านทุกๆ 30-45 วัน ตามข้อแนะนำของการรักษาความปลอดภัยข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันเปลี่ยนรหัสผ่านทุก 30-45 วัน*
6	ฉันนำรหัสผ่านเดิม วนกลับมาใช้ในบริการธุรกรรมทางอิเล็กทรอนิกส์ *(-)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันนำรหัสผ่านเดิม วนกลับมาใช้ใหม่*
7	ฉันไม่จดบันทึก ชื่อผู้ใช้งานและรหัสผ่าน	+1	+1	+1	+1	+1	1.00	ใช้ได้

ข้อ	ข้อคำถามที่ใช้ในเครื่องมือวัด	คะแนนของผู้ทรงคุณวุฒิ (คนที่)					IOC	การแปลผล และข้อเสนอแนะ
		1	2	3	4	5		
	ธุรกรรมทางอิเล็กทรอนิกส์ไว้เป็นลายลักษณ์อักษร *(+)*							*ฉันไม่จดบันทึกชื่อผู้ใช้งาน (Username) และรหัสผ่านไว้เป็นลายลักษณ์อักษรหรือในสมาร์ทโฟน*
8	ฉันเก็บรักษาบัตรธนาคารอิเล็กทรอนิกส์โดยแยกออกจากการจดบันทึกรหัสผ่านจำนวน 6 หลัก *(+)*	+1	0	0	+1	-1	0.20	*เป็นคำแนะนำของการรักษาความปลอดภัย*
9	ฉันได้บอกชื่อผู้ใช้งานและรหัสผ่านธุรกรรมทางอิเล็กทรอนิกส์กับบุคคลที่ฉันมีความใกล้ชิด สนิทสนม *(-)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันบอกชื่อผู้ใช้งานและรหัสผ่านกับบุคคลใกล้ชิด*
10	ฉันเลือกใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ กับผู้ให้บริการที่มีการแจ้งเงื่อนไขและรายละเอียดนโยบายคุ้มครองความเป็นส่วนตัว *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันใช้บริการกับผู้ให้บริการที่แจ้งเงื่อนไขและรายละเอียดนโยบายคุ้มครองความเป็นส่วนตัว*
11	ฉันได้อ่าน ศึกษาเงื่อนไขและรายละเอียดนโยบายคุ้มครองความเป็นส่วนตัว การจัดเก็บข้อมูลและการเปิดเผยข้อมูลแก่บุคคลที่สามจนครบเนื้อหา ก่อนยอมรับข้อตกลงกับผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันอ่านนโยบายคุ้มครองความเป็นส่วนตัวก่อนกดยอมรับข้อตกลง*
12	ฉันได้อ่าน ศึกษาเงื่อนไขและรายละเอียดนโยบายคุ้มครองความเป็นส่วนตัวทุกครั้งเมื่อมีการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(+)*	0	+1	0	+1	-1	0.20	*คำถามมีลักษณะใกล้เคียงกันกับข้อที่แล้ว ไม่แตกต่าง*
13	หากฉันอ่านแล้วไม่เข้าใจในเงื่อนไขและรายละเอียดนโยบายคุ้มครองความเป็นส่วนตัวฉบับภาษาไทย ฉันพยายามศึกษาฉบับภาษาอังกฤษแทน *(+)*	0	+1	0	+1	0	0.40	*เป็นคำแนะนำของการรักษาความปลอดภัย*
14	ในแต่ละวัน ฉันไม่ได้ตั้งค่าจำกัดวงเงินในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(-)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันไม่ได้ตั้งค่าจำกัดวงเงินการใช้บริการในแต่ละวัน*
15	ฉันหมั่นตรวจสอบการทำรายการธุรกรรม	+1	+1	+1	+1	+1	1.00	ใช้ได้

ข้อ	ข้อคำถามที่ใช้ในเครื่องมือวัด	คะแนนของผู้ทรงคุณวุฒิ (คนที่)					IOC	การแปลผล และข้อเสนอแนะ
		1	2	3	4	5		
	ทางอิเล็กทรอนิกส์ย้อนหลัง อย่างสม่ำเสมอ *(+)*							*ฉันตรวจสอบการทำรายการธุรกรรมย้อนหลังอย่างสม่ำเสมอ*
16	ฉันได้บันทึกข้อมูลส่วนบุคคลหรือรูปภาพที่อาจเกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์ไว้ในเครื่องคอมพิวเตอร์ เช่น สมาร์ทโฟน คอมพิวเตอร์แบบพกพา คอมพิวเตอร์ส่วนบุคคล เป็นต้น *(-)*	+1	0	+1	0	-1	0.20	*ระบบบันทึกเองแบบอัตโนมัติ*
17	ฉันไม่บันทึกข้อมูลหรือรูปภาพ การทำรายการธุรกรรมทางอิเล็กทรอนิกส์ไว้ในเครื่องคอมพิวเตอร์ชนิดต่างๆ เช่น สมาร์ทโฟน คอมพิวเตอร์แบบพกพา คอมพิวเตอร์ส่วนบุคคล เป็นต้น *(+)*	+1	0	+1	0	-1	0.20	*ระบบบันทึกเองแบบอัตโนมัติ+วิธีการตั้งค่า*
18	ฉันได้ตรวจสอบบุคคลรอบตัวและพยายามใช้มือปกปิดข้อมูลส่วนบุคคลในระหว่างเข้าทำรายการธุรกรรมทางอิเล็กทรอนิกส์ *(+)*	+1	0	+1	+1	+1	0.80	ใช้ได้ *ฉันมองบุคคลรอบตัวและใช้มือปกปิดการกรอกข้อมูลระหว่างทำรายการ*
19	ฉันไม่เข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ผ่านเครื่องคอมพิวเตอร์ที่ใช้งานร่วมกับบุคคลที่ฉันมีความใกล้ชิด สนิมสนมหรือบุคคลอื่น *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันไม่ใช้บริการผ่านคอมพิวเตอร์ที่ใช้งานร่วมกับบุคคลอื่น*
20	ฉันเลือกให้ข้อมูลส่วนบุคคลเฉพาะที่จำเป็นต่อผลการสมัครเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันให้ข้อมูลส่วนบุคคลเฉพาะที่จำเป็นในการสมัครเข้าใช้บริการ*
21	ฉันได้ให้ข้อมูลส่วนบุคคลเกินว่าข้อมูลที่เป็นข้อบังคับ ต่อการสมัครเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(-)*	+1	+1	0	0	0	0.40	*"ข้อบังคับ" ยังไม่ชัดเจนในรายละเอียด*
22	ฉันหลีกเลี่ยงให้ข้อมูลส่วนบุคคลเพิ่มเติมหากวัตถุประสงค์การขอข้อมูลส่วนบุคคลจากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์มีความคลุมเครือและไม่ชัดเจน *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันหลีกเลี่ยงให้ข้อมูลส่วนบุคคลเพิ่มเติมหากวัตถุประสงค์การขอข้อมูลมีความคลุมเครือ*
23	ฉันพยายามหลีกเลี่ยงให้ข้อมูลส่วนบุคคล	+1	0	+1	0	0	0.40	*"การปรับปรุงข้อมูล" อาจเป็นประโยชน์แก่ผู้ใช้งาน ทำให้ไม่แน่ใจข้อความ +/-*

ข้อ	ข้อคำถามที่ใช้ในเครื่องมือวัด	คะแนนของผู้ทรงคุณวุฒิ (คนที่)					IOC	การแปลผล และข้อเสนอแนะ
		1	2	3	4	5		
	เมื่อผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์เรียกร้องหรือแจ้งให้มีการแก้ไขหรือปรับเปลี่ยนข้อมูลส่วนบุคคลของฉันให้เป็นปัจจุบัน *(+)*							
24	ฉันทำการกำหนดสิทธิ์ในการเข้าถึงข้อมูลส่วนบุคคลเฉพาะที่จำเป็น แก่ผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันกำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคลเท่าที่จำเป็นแก่ผู้ให้บริการ*
25	ฉันไม่เปิดเผยข้อมูลส่วนบุคคลผ่านสื่อสังคมออนไลน์ต่างๆ ที่คาดว่าสามารถเชื่อมโยงไปถึงข้อมูลทางการเงินอิเล็กทรอนิกส์ของฉัน *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันไม่เปิดเผยข้อมูลผ่านสื่อสังคมออนไลน์ที่เชื่อมโยงไปถึงข้อมูลทางการเงินอิเล็กทรอนิกส์*
26	ฉันยินยอมหรืออนุญาตให้ผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์สามารถทำการเชื่อมต่อข้อมูลส่วนบุคคลของฉันไปยังสื่อสังคมออนไลน์ต่างๆ *(-)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันอนุญาตผู้ให้บริการเชื่อมต่อข้อมูลของฉันไปยังสื่อสังคมออนไลน์*
27	ฉันเลือกเข้าร่วมบางกิจกรรมส่งเสริมการขายและการตลาด กับผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(+)*	+1	0	+1	+1	+1	0.80	ใช้ได้ *ฉันเลือกเข้าร่วมกิจกรรมส่งเสริมการขายบางอย่างกับผู้ให้บริการ*
28	ฉันไม่เข้าร่วมกิจกรรมประเภทเกมตอบคำถามชิงรางวัล จากการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันไม่เข้าร่วมกิจกรรมประเภทเกมตอบคำถามชิงรางวัลจากการเข้าใช้บริการ*
29	ฉันเข้าร่วมกิจกรรมประเภทการทดสอบเกมเกมทายใจ ที่จำเป็นต้องมีการให้ข้อมูลส่วนบุคคล กับผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(-)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันเข้าร่วมกิจกรรมการทดสอบเกมทายใจ ที่ต้องให้ข้อมูลส่วนบุคคลกับผู้ให้บริการ*
30	เมื่อเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ฉันได้ทำการกดปุ่มออกจากระบบการใช้บริการ (Logout) ทุกครั้งภายหลังเสร็จสิ้นการใช้บริการ *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันกดปุ่มออกจากระบบ (Logout) ทุกครั้งหลังเสร็จสิ้นการใช้บริการ*

โดยสรุป ตอนที่ 2 พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ในองค์ประกอบที่ 1 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป นำมาจัดทำเป็นแบบสอบถามเพื่อการวิจัยรวมทั้งสิ้น จำนวน 23 ข้อและปรับตามข้อเสนอแนะของผู้ทรงคุณวุฒิ

ตารางที่ 3 ค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์และผลประเมินของตอนที่ 2 พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ในองค์ประกอบที่ 2 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค

ข้อ	ข้อคำถามที่ใช้ในเครื่องมือวัด	คะแนนของผู้ทรงคุณวุฒิ (คนที่)					IOC	การแปลผล และข้อเสนอแนะ
		1	2	3	4	5		
ตอนที่ 2 พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ องค์ประกอบที่ 2 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค								
1	ฉันไม่ทำการติดตั้งอุปกรณ์เสริมหรือเพิ่มเติมชิ้นส่วนอะไหล่ เช่น ความจุข้อมูล (Harddisk) หน่วยความจำหลัก (RAM) อุปกรณ์เก็บบันทึกข้อมูล (USB Flash Drive) กล้องหลัง (Rear Camera) เป็นต้น ที่ไม่ได้มาตรฐานและอาจเสี่ยงต่อภัยคุกคามด้านความปลอดภัยของข้อมูลภายในสมาร์ทโฟน คอมพิวเตอร์แบบพกพา หรือคอมพิวเตอร์ส่วนบุคคลของฉัน *(+)*	+1	+1	+1	0	+1	0.80	ใช้ได้ *(**ควรตั้งเป็นหัวข้อคำถาม**.., ปรับข้อความให้กระชับ, ตรวจสอบคำขยาย, คำปฏิเสธซ้อน) "**ในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์**..." ฉันติดตั้งอุปกรณ์เสริม เช่น หน่วยความจำหลัก (RAM) ที่ไม่ได้มาตรฐานภายในเครื่องคอมพิวเตอร์*
2	ฉันทำการดัดแปลงหรือแก้ไขชิ้นส่วนอะไหล่ภายในสมาร์ทโฟน คอมพิวเตอร์แบบพกพา หรือคอมพิวเตอร์ส่วนบุคคลของฉัน เพื่ออำนวยความสะดวกต่อการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(-)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *(ปรับข้อความให้กระชับ) ฉันดัดแปลงหรือแก้ไขอุปกรณ์ภายในเครื่องคอมพิวเตอร์ เพื่อความสะดวกต่อการใช้บริการ*
3	สมาร์ทโฟน คอมพิวเตอร์แบบพกพา หรือคอมพิวเตอร์ส่วนบุคคลของฉันไม่ล้าสมัยต่อการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(+)*	-1	0	+1	0	0	0.00	*"ล้าสมัย" ไม่สะท้อนทักษะตามนิยามเชิงปฏิบัติการ*
4	ฉันได้ใช้สมาร์ทโฟน คอมพิวเตอร์แบบพกพา หรือคอมพิวเตอร์ส่วนบุคคล รุ่นเก่าซึ่งมีมาตรฐานความปลอดภัยของข้อมูลค่อนข้างต่ำและมีระบบปฏิบัติการล้าสมัยในการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(-)*	-1	+1	+1	0	+1	0.40	*ไม่ตรงกับนิยามเชิงปฏิบัติการ*

ข้อ	ข้อคำถามที่ใช้ในเครื่องมือวัด	คะแนนของผู้ทรงคุณวุฒิ (คนที่)					IOC	การแปลผล และข้อเสนอแนะ
		1	2	3	4	5		
5	ฉันดูแลรักษา และมีเทคนิคสำหรับใช้งานสมาร์ทโฟน คอมพิวเตอร์แบบพกพา หรือคอมพิวเตอร์ส่วนบุคคลอย่างทะนุถนอม *(+)*	-1	0	0	0	+1	0.00	*ไม่ตรงกับนิยามเชิงปฏิบัติการ+คำถามมี 2 ประเด็น*
6	ฉันทำการเปลี่ยนหรือซื้อสมาร์ทโฟน คอมพิวเตอร์แบบพกพา หรือคอมพิวเตอร์ส่วนบุคคลใหม่ จนกว่าจะส่งผลต่อการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(-)*	-1	-1	0	0	0	-0.40	*อ่านแล้วไม่เข้าใจคำถาม*
7	ฉันได้ทำการตรวจสอบ หรือลบข้อมูลส่วนบุคคลที่จำเป็นก่อนเสมอ หากมีความจำเป็นต้องนำสมาร์ทโฟน คอมพิวเตอร์แบบพกพา หรือคอมพิวเตอร์ส่วนบุคคล ไปปรับปรุง ซ่อมแซมยังร้านบริการซ่อมคอมพิวเตอร์ เพื่อให้สามารถนำมาใช้งานได้ตามปกติ *(+)*	+1	0	+1	+1	+1	0.80	ใช้ได้ *หากจำเป็นต้องนำเครื่องคอมพิวเตอร์ไปซ่อมแซมยังร้านบริการ ฉันตรวจสอบและลบข้อมูลส่วนบุคคล*
8	ฉันทำการตั้งค่าปลดล็อคการแสดงผลหน้าจอบนสมาร์ทโฟน คอมพิวเตอร์แบบพกพา หรือคอมพิวเตอร์ส่วนบุคคลโดยใช้รหัสผ่าน *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันตั้งค่ารหัสผ่านปลดล็อคการแสดงผลหน้าจอ*
9	ฉันพยายามหลีกเลี่ยงไม่ให้บุคคลที่ฉันใกล้ชิด สนิทสนม หยิบยืมเพื่อใช้งานสมาร์ทโฟน คอมพิวเตอร์แบบพกพา หรือคอมพิวเตอร์ส่วนบุคคลของฉัน *(+)*	+1	0	0	0	+1	0.40	*ทับซ้อนกับองค์ประกอบที่ 1*
10	ฉันใช้คอมพิวเตอร์แบบพกพาหรือคอมพิวเตอร์ส่วนบุคคลที่ต้องใช้งานหรือทำงานร่วมกับบุคคลอื่น ในการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(-)*	+1	0	0	0	+1	0.40	*ทับซ้อนกับองค์ประกอบที่ 1*
11	ฉันทำการดัดแปลง เพิ่มเติม หรือแก้ไข	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันดัดแปลงหรือแก้ไขระบบปฏิบัติการ*

ข้อ	ข้อคำถามที่ใช้ในเครื่องมือวัด	คะแนนของผู้ทรงคุณวุฒิ (คนที่)					IOC	การแปลผล และข้อเสนอแนะ
		1	2	3	4	5		
	เกี่ยวกับระบบปฏิบัติการ (Jailbreak/Root) ในสมาร์ทโฟน คอมพิวเตอร์แบบพกพา หรือคอมพิวเตอร์ส่วนบุคคลของฉัน *(-)*							*(Jailbreak/Root) เข้ากับเครื่องคอมพิวเตอร์*
12	ฉันไม่ทำการปรับปรุงรุ่นของระบบปฏิบัติการให้เป็นปัจจุบัน จนกว่าจะส่งผลต่อประสิทธิภาพการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(-)*	0	0	+1	+1	+1	0.60	ใช้ได้ *ฉันปล่อยให้ระบบปฏิบัติการล้าสมัยจนส่งผลต่อการเข้าใช้บริการ*
13	ฉันได้ตรวจสอบแหล่งที่มาของโปรแกรมหรือแอปพลิเคชันที่ได้ถูกพัฒนาขึ้นก่อนทำการดาวน์โหลดเพื่อเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(+)*	0	+1	+1	+1	+1	0.80	ใช้ได้ *ฉันตรวจสอบที่มาของแอปพลิเคชันก่อนทำการดาวน์โหลดเพื่อเข้าใช้บริการ*
14	ฉันติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่มีลิขสิทธิ์ เพื่อปกป้องข้อมูลส่วนบุคคลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่มีลิขสิทธิ์*
15	ฉันทำการปรับปรุงรุ่นของโปรแกรมป้องกันไวรัสคอมพิวเตอร์ให้เป็นปัจจุบันอยู่เสมอเพื่อปกป้องข้อมูลส่วนบุคคลจากการใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(+)*	+1	+1	0	0	0	0.40	*ข้อคำถามใกล้เคียงกับประเด็นก่อนนี้*
16	ฉันทำการปรับปรุงรุ่นของโปรแกรมหรือแอปพลิเคชันเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ให้เป็นปัจจุบัน จนกว่าจะส่งผลต่อประสิทธิภาพการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่ลดลง *(-)*	0	0	0	0	+1	0.20	*อ่านแล้วไม่เข้าใจคำถาม*
17	เมื่อเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ หากมีการแจ้งหรือแสดงข้อมูลเพื่อการ	+1	0	+1	+1	+1	0.80	ใช้ได้ *หากมีการแสดงข้อมูลเพื่อการโฆษณาผลิตภัณฑ์จากผู้ให้บริการ ฉันพยายามปิด*

ข้อ	ข้อคำถามที่ใช้ในเครื่องมือวัด	คะแนนของผู้ทรงคุณวุฒิ (คนที่)					IOC	การแปลผล และข้อเสนอแนะ
		1	2	3	4	5		
	โฆษณาผลิตภัณฑ์จากผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ ฉันได้พยายามปิดหน้าต่างป๊อบอัพ (Pop-up Window Blocked) *(+)*							*หน้าต่างป๊อบอัพ (Pop-up Window Blocked)*
18	ฉันเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์บนเว็บไซต์ ก็ต่อเมื่อผู้ให้บริการเว็บไซต์นั้นให้ฉันทำการยอมรับเงื่อนไขการใช้งานคุกกี้ (Accept Cookies) ซึ่งเป็นการเก็บประวัติข้อมูลส่วนบุคคลของผู้ใช้บริการ *(-)*	+1	0	0	+1	+1	0.60	ใช้ได้ *ฉันไม่เข้าใช้บริการบนเว็บไซต์ที่ให้ยอมรับเงื่อนไขการใช้งานคุกกี้ (Accept Cookies)*
19	หากฉันใช้บริการธุรกรรมทางอิเล็กทรอนิกส์บนเว็บไซต์ ฉันใช้งานผ่านโหมดท่องเว็บไซต์แบบส่วนตัว (Private Mode) หรือโหมดไม่ระบุตัวตน (Incognito Mode) *(+)*	+1	0	+1	+1	+1	0.80	ใช้ได้ *หากเข้าใช้บริการบนเว็บไซต์ ฉันใช้งานผ่านโหมดส่วนตัว (Private Mode) หรือไม่ระบุตัวตน (Incognito Mode)*
20	หากใช้บริการธุรกรรมทางอิเล็กทรอนิกส์บนเว็บไซต์ ฉันปิดการใช้งานแบบ Do not track เพื่อปกป้องการติดตามและการเก็บข้อมูลส่วนบุคคลจากผู้ให้บริการเครือข่ายอินเทอร์เน็ต *(-)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *หากเข้าใช้บริการบนเว็บไซต์ ฉันเปิดใช้งานแบบ Do not track เพื่อป้องกันการติดตามและเก็บข้อมูล*
21	เมื่อฉันใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ผ่านทางเว็บไซต์หรือแอปพลิเคชันที่ได้พัฒนาขึ้น ฉันทำการลบประวัติการใช้งานทุกครั้ง *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันลบประวัติ (History) การเข้าใช้บริการทุกครั้ง*
22	เมื่อฉันใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ผ่านทางเว็บไซต์หรือแอปพลิเคชันที่ได้พัฒนาขึ้น ฉันทำการตั้งค่าความเป็นส่วนตัวแบบขั้นสูง (Advanced) เพื่อปกป้องการบันทึกข้อมูลส่วนบุคคลลงในแบบฟอร์มต่างๆ โดยอัตโนมัติ *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันตั้งค่าความเป็นส่วนตัวขั้นสูง (Advanced) เพื่อเข้าใช้บริการ*
23	ฉันหมั่นตรวจสอบและลบโปรแกรมหรือแอปพลิเคชันเกี่ยวกับธุรกรรมทาง	+1	+1	0	+1	+1	0.80	ใช้ได้ *ฉันหมั่นตรวจสอบและลบแอปพลิเคชันที่ไม่มีการใช้บริการ*

ข้อ	ข้อคำถามที่ใช้ในเครื่องมือวัด	คะแนนของผู้ทรงคุณวุฒิ (คนที่)					IOC	การแปลผล และข้อเสนอแนะ
		1	2	3	4	5		
	อิเล็กทรอนิกส์ที่ไม่มีการใช้งานเกิดขึ้นแล้วเป็นประจำ *(+)*							
24	ฉันทำการตั้งค่าการปิดกั้น (Blocked) การรับข้อความทางอีเมล์ไว้ก่อนเสมอ หากเป็นบุคคลที่ฉันไม่รู้จักมาก่อน *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันตั้งค่าปิดกั้น (Blocked) รับข้อความอีเมล์ไว้ก่อนเสมอ หากเป็นบุคคลหรือองค์กรที่ฉันไม่รู้จัก*
25	ฉันทำการตั้งค่าการปิดกั้น การรับข้อความทางอีเมล์ไว้ก่อนเสมอ หากเป็นหน่วยงานหรือองค์การที่ฉันไม่รู้จักมาก่อน *(+)*	+1	0	0	0	+1	0.40	*ควรรวมข้อคำถามกับข้อที่แล้ว*
26	ฉันสร้างอีเมล์เพื่อใช้บริการธุรกรรมทางอิเล็กทรอนิกส์โดยเฉพาะ *(+)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันสร้างอีเมล์เพื่อใช้บริการธุรกรรมโดยเฉพาะ*
27	ฉันทำการตั้งค่าการยืนยันตัวตนแบบสองชั้น (Two-factor Authentication) เพื่อยืนยันความเป็นเจ้าของอีเมล์ในการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ *(+)*	+1	+1	+1	0	+1	0.80	ใช้ได้ *ฉันตั้งค่ายืนยันตัวตนแบบสองชั้น (Two-factor Authentication) ในความเป็นเจ้าของเพื่อเข้าใช้บริการ*
28	ฉันใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ด้วยบริการวายฟายสาธารณะ (Public/Free Wi-Fi) เช่น ภายในห้างสรรพสินค้า ร้านกาแฟ ร้านอาหาร เป็นต้น *(-)*	+1	+1	+1	+1	+1	1.00	ใช้ได้ *ฉันเปิดใช้บริการด้วยวายฟายสาธารณะ (Public/Free Wi-Fi) เช่น ภายในร้านกาแฟ*
29	ฉันเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์โดยใช้อินเตอร์เน็ตบ้านของฉันหรือผ่านเครือข่ายโทรศัพท์มือถือบนสมาร์ทโฟนของฉัน *(+)*	+1	+1	0	0	0	0.40	*ไม่แน่ใจข้อคำถาม +/-*
30	หากมีความจำเป็นใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ผ่านเครื่องคอมพิวเตอร์สาธารณะหรือคอมพิวเตอร์ร่วมกับบุคคลื่น ฉันทำการเปลี่ยนรหัสผ่านทุกครั้ง ภายหลังจากเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์เสร็จสิ้นแล้ว *(+)*	+1	0	+1	0	+1	0.60	ใช้ได้ *หากจำเป็นใช้บริการผ่านเครื่องคอมพิวเตอร์สาธารณะหรือบุคคลอื่น ฉันเปลี่ยนรหัสผ่านทุกครั้ง*

โดยสรุป ตอนที่ 2 พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ ในองค์ประกอบที่ 2 การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค นำมาจัดทำเป็นแบบสอบถามเพื่อการวิจัยรวมทั้งสิ้น จำนวน 20 ข้อและปรับตามข้อเสนอแนะของผู้ทรงคุณวุฒิ

ตอนที่ 3 แบบสอบถามความรู้สึก ความคิดเห็นที่มีต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของกลุ่มวัยทำงานตอนต้น เป็นมาตรวัดตัวแปรอิสระที่เกี่ยวข้องกับพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ มีจำนวนทั้งสิ้น 11 ชุด ดังนี้

ชุดที่ 1 แบบวัดการรับรู้ถึงโอกาสเสี่ยงบนธุรกรรมทางอิเล็กทรอนิกส์
ชุดที่ 2 แบบวัดการรับรู้ถึงความรุนแรงบนธุรกรรมทางอิเล็กทรอนิกส์
ชุดที่ 3 แบบวัดความคาดหวังในผลลัพธ์ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล
ชุดที่ 4 แบบวัดความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล
ชุดที่ 5 แบบวัด ความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่ายเพื่อปกป้องข้อมูลส่วนบุคคล
ชุดที่ 6 แบบวัดคุณลักษณะของระบบเพื่อปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์
ชุดที่ 7 แบบวัดการคล้อยตามกลุ่มอ้างอิงในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์
ชุดที่ 8 แบบวัดการรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล
ชุดที่ 9 แบบวัดการรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล
ชุดที่ 10 แบบวัดทัศนคติที่มีต่อการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์
ชุดที่ 11 แบบวัดความตั้งใจในการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ผู้วิจัยขอนำเสนอ เป็นตารางสรุปผลประเมินของแต่ละแบบวัด ดังต่อไปนี้

ตารางสรุปผลประเมินของแต่ละแบบวัด

จากการคำนวณค่าดัชนีความสอดคล้องระหว่างข้อคำถามตามวัตถุประสงค์ของงานวิจัย (Index of Item - Objective Congruence: IOC) โดยทุกข้อคำถามต้องผ่านเกณฑ์ค่าดัชนีความสอดคล้องที่มากกว่าหรือเท่ากับ 0.60 จึงจะถือว่ามีความสอดคล้องความตรงด้านเนื้อหา โดยการนำคะแนนที่ประเมินจากผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญ มาหาค่า IOC รายข้อ สามารถสรุปเป็นตารางที่ 4 ผลการตรวจประเมินความเหมาะสมของความตรงด้านเนื้อหาของเครื่องมือวัดงานวิจัย ดังนี้

ตารางที่ 4 ผลการตรวจประเมินความเหมาะสมของความตรงด้านเนื้อหาของเครื่องมือวัดงานวิจัย

ตอนที่	แบบวัดชุดที่และองค์ประกอบ	ข้อคำถามเดิม (ข้อ)	ผ่านเกณฑ์ IOC ≥ 0.60 (ข้อ)	ข้อคำถามทางบวกและทางลบ (ข้อ)
1	ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม	9	8	-
2	พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมฯ			
	องค์ประกอบที่ 1 การปฏิบัติตนในข้อควรระวังฯ ทั่วไป	30	23	16 ข้อ และ7 ข้อ
	องค์ประกอบที่ 2 การปฏิบัติตนในข้อควรระวังฯ เชิงเทคนิค	30	20	14 ข้อ และ 6 ข้อ
3	แบบสอบถามความรู้สึก ความคิดเห็นที่มีต่อพฤติกรรมฯ			
	ชุดที่ 1 การรับรู้ถึงโอกาสเสี่ยงฯ			
	-จากผู้ให้บริการ	10	7	5 ข้อ และ2 ข้อ
	-จากการเข้าใช้บริการ	10	6	5 ข้อ และ1 ข้อ
	ชุดที่ 2 การรับรู้ถึงความรุนแรงฯ			
	-ด้านทรัพย์สิน	10	6	4 ข้อ และ2 ข้อ
	-ตัวบุคคล	10	7	6 ข้อ และ1 ข้อ
	ชุดที่ 3 ความคาดหวังในผลลัพธ์ฯ			
	-ปฏิบัติโดยทั่วไป	10	6	4 ข้อ และ2 ข้อ
	-ปฏิบัติแบบขั้นสูง	10	6	5 ข้อ และ1 ข้อ
	ชุดที่ 4 ความคาดหวังความสามารถตนเอง			
	-การใช้งานเครือข่ายคอมพิวเตอร์	10	6	5 ข้อ และ1 ข้อ
	-ความพร้อมในการรับมือกับปัญหา	10	7	6 ข้อ และ1 ข้อ
	-ความสามารถในการควบคุมสถานการณ์	10	6	5 ข้อ และ1 ข้อ
	ชุดที่ 5 ความคุ้มค่าต้นทุนและค่าใช้จ่าย			
	-ในรูปตัวเงิน	10	6	6 ข้อ
	-ไม่ได้อยู่ในรูปตัวเงิน	10	6	5 ข้อ และ1 ข้อ
	ชุดที่ 6 คุณลักษณะของระบบ			
	-คุณลักษณะเด่น	10	6	5 ข้อ และ1 ข้อ
	-ส่วนติดต่อกับผู้ใช้งาน	10	6	5 ข้อ และ1 ข้อ
	ชุดที่ 7 การคล้อยตามกลุ่มอ้างอิง			
	-บุคคลรอบข้างที่ใกล้ชิด	10	6	5 ข้อ และ1 ข้อ
	-ผู้ทรงอิทธิพลทางเทคโนโลยี	10	7	5 ข้อ และ2 ข้อ
	ชุดที่ 8 การรับรู้ถึงประโยชน์การตั้งค่าฯ			
	-ก่อให้เกิดประโยชน์ต่อตนเอง	10	6	5 ข้อ และ1 ข้อ
	-การเพิ่มประสิทธิผลในความปลอดภัย	10	6	5 ข้อ และ1 ข้อ
	ชุดที่ 9 การรับรู้ถึงความง่ายในการตั้งค่าฯ			

ตอนที่	แบบวัดชุดที่และองค์ประกอบ	ข้อคำถามเดิม (ข้อ)	ผ่านเกณฑ์ IOC ≥ 0.60 (ข้อ)	ข้อคำถามทางบวกและทางลบ (ข้อ)
	-ง่ายต่อการเรียนรู้	10	6	4 ข้อ และ2 ข้อ
	-ความไม่ซับซ้อนของระบบ	10	6	5 ข้อ และ1 ข้อ
	ชุดที่ 10 ทัศนคติต่อการปกป้องข้อมูลฯ			
	-ความเชื่อในผลของการกระทำ	10	7	6 ข้อ และ1 ข้อ
	-การประเมินคุณค่าการกระทำ	10	6	6 ข้อ
	ชุดที่ 11 ความตั้งใจในการปกป้องข้อมูลฯ			
	-ความตั้งใจปกป้องข้อมูลส่วนบุคคล	10	8	7 ข้อ และ1 ข้อ
รวมทั้งสิ้น (ข้อ)		289	190	-

จากตางรางที่ 4 จะเห็นว่าผลพิจารณาความคิดเห็นของผู้ทรงคุณวุฒิ/ผู้เชี่ยวชาญที่มีต่อเครื่องมือวัดงานวิจัยนี้ ถึงความเหมาะสมของความตรงด้านเนื้อหา พบว่าข้อคำถามที่ผู้วิจัยได้สร้างขึ้นตรงกับนิยามศัพท์เฉพาะและสอดคล้องกับวัตถุประสงค์ที่ใช้ในการวิจัยนี้ รวมทั้งสิ้น 190 ข้อ สามารถใช้การจัดแบ่งองค์ประกอบตามที่นำเสนอแบบประเมินตรวจสอบความตรงด้านเนื้อหา ทั้งนี้มีผู้ทรงคุณวุฒิให้ข้อเสนอแนะของการแบ่งองค์ประกอบในเรื่องการมีนิยามเชิงปฏิบัติการที่ใกล้เคียงและอาจทับซ้อนกัน โดยให้พิจารณาการปรับรวมองค์ประกอบเป็นด้านเดียว เพื่อความชัดเจนและลดความซ้ำซ้อนของข้อคำถาม ได้แก่ แบบวัดชุดที่ 8 การรับรู้ถึงประโยชน์ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล และแบบวัดชุดที่ 9 การรับรู้ถึงความง่ายในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ภาคผนวก ค

หนังสือรับรองจริยธรรมในงานวิจัย

MF-04-version-2.0
วันที่ 18 ต.ค. 61

หนังสือยืนยันการยกเว้นการรับรอง
คณะกรรมการจริยธรรมสำหรับพิจารณาโครงการวิจัยที่ทำในมนุษย์
มหาวิทยาลัยศรีนครินทรวิโรฒ

(เอกสารนี้เพื่อแสดงว่าคณะกรรมการจริยธรรมสำหรับพิจารณาโครงการวิจัยที่ทำในมนุษย์ ได้พิจารณาโครงการวิจัยนี้)

ชื่อโครงการวิจัย : ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น

ชื่อหัวหน้าโครงการวิจัย : นาย ธีรศักดิ์ พลพันธ์

หน่วยงานต้นสังกัด : สถาบันวิจัยพฤติกรรมศาสตร์

รหัสโครงการวิจัย : SWUEC-G-299/2563X

โครงการวิจัยนี้เป็นโครงการวิจัยที่เข้าข่ายยกเว้น (Research with Exemption from SWUEC)

วันที่ยืนยัน : 11 สิงหาคม 2563

ยืนยันโดย : คณะกรรมการจริยธรรมสำหรับพิจารณาโครงการวิจัยที่ทำในมนุษย์
มหาวิทยาลัยศรีนครินทรวิโรฒ

คณะกรรมการจริยธรรมสำหรับพิจารณาโครงการวิจัยที่ทำในมนุษย์ มหาวิทยาลัยศรีนครินทรวิโรฒ ดำเนินการรับรองโครงการวิจัยตามแนวทางหลักจริยธรรมการวิจัยในคนที่เป็นสากล ได้แก่ Declaration of Helsinki, the Belmont Report, CIOMS Guidelines และ the International Conference on Harmonization in Good Clinical Practice (ICH-GCP)

ออกให้ ณ วันที่ 25 กันยายน 2563

(ลงชื่อ).....
(ผู้ช่วยศาสตราจารย์ ดร.ทันตแพทย์หญิงณปภา เอี่ยมจิรกุล)
กรรมการและเลขานุการคณะกรรมการจริยธรรม
สำหรับพิจารณาโครงการวิจัยที่ทำในมนุษย์

(ลงชื่อ).....
(แพทย์หญิงสุรีพร ภัทรสุวรรณ)
ประธานคณะกรรมการจริยธรรม
สำหรับพิจารณาโครงการวิจัยที่ทำในมนุษย์

หมายเลขรับรอง : SWUEC/X/G-299/2563

ภาคผนวก ง

หนังสือขอความอนุเคราะห์เก็บข้อมูลเพื่อการวิจัย

ที่ อว 8718/1769

บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ
114 สุขุมวิท 23 แขวงคลองเตยเหนือ
เขตวัฒนา กรุงเทพฯ 10110

9 สิงหาคม 2564

เรื่อง ขอความอนุเคราะห์เก็บข้อมูลเพื่อการวิจัย

เรียน อธิการบดีสถาบันการจัดการปัญญาภิวัฒน์

เนื่องด้วย นายธีรศักดิ์ พลพันธ์ นิสิตระดับปริญญาเอก สาขาวิชาการวิจัยพฤติกรรมศาสตร์ประยุกต์ มหาวิทยาลัยศรีนครินทรวิโรฒ ได้รับอนุมัติให้ทำปริญญานิพนธ์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” โดยมี ผู้ช่วยศาสตราจารย์ ดร.ศรัณย์ พิมพ์ทอง และผู้ช่วยศาสตราจารย์ ดร.กาญจนา ภัทราวิวัฒน์ เป็นอาจารย์ที่ปรึกษาปริญญานิพนธ์

ในการนี้ นิสิตขอความอนุเคราะห์เก็บข้อมูล โดยใช้แบบสอบถามออนไลน์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” กับพนักงานในวัยทำงานตอนต้น โดยสแกนผ่าน QR Code หรือ https://shorturl.at/abgBI เพื่อเป็นข้อมูลในการวิจัย ระหว่างเดือนสิงหาคม 2564 ถึงเดือนตุลาคม 2564 ทั้งนี้ นิสิตจะเป็นผู้ประสานงานในรายละเอียดดังกล่าวต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาขอความอนุเคราะห์ และขอขอบพระคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

(รองศาสตราจารย์ นายแพทย์ฉัตรชัย เอกปัญญาสกุล)
รักษาการแทนคณบดีบัณฑิตวิทยาลัย ปฏิบัติการแทน
อธิการบดีมหาวิทยาลัยศรีนครินทรวิโรฒ

แบบสอบถาม

สำนักงานคณบดีบัณฑิตวิทยาลัย
โทร. 0 2649 5064
หมายเหตุ : สอบถามข้อมูลเพิ่มเติมกรุณาติดต่อนิสิต โทรศัพท์ 086 788 6687

ที่ อว 8718/1769

บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ
114 สุขุมวิท 23 แขวงคลองเตยเหนือ
เขตวัฒนา กรุงเทพฯ 10110

9 สิงหาคม 2564

เรื่อง ขอความอนุเคราะห์เก็บข้อมูลเพื่อการวิจัย

เรียน ผู้จัดการฝ่ายทรัพยากรบุคคล บริษัท ทเวนตี้โฟร์ ช้อปปิ้ง จำกัด

เนื่องด้วย นายธีรศักดิ์ พลพันธ์ นิสิตระดับปริญญาเอก สาขาวิชาการวิจัยพฤติกรรมศาสตร์ประยุกต์ มหาวิทยาลัยศรีนครินทรวิโรฒ ได้รับอนุมัติให้ทำปริญญานิพนธ์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” โดยมี ผู้ช่วยศาสตราจารย์ ดร.ศรัณย์ พิมพ์ทอง และผู้ช่วยศาสตราจารย์ ดร.กาญจนา ภัทราวิวัฒน์ เป็นอาจารย์ที่ปรึกษาปริญญานิพนธ์

ในการนี้ นิสิตขอความอนุเคราะห์เก็บข้อมูล โดยใช้แบบสอบถามออนไลน์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” กับพนักงานในวัยทำงานตอนต้น โดยสแกนผ่าน QR Code หรือ https://shorturl.at/abgBI เพื่อเป็นข้อมูลในการวิจัย ระหว่างเดือนสิงหาคม 2564 ถึงเดือนตุลาคม 2564 ทั้งนี้ นิสิตจะเป็นผู้ประสานงานในรายละเอียดดังกล่าวต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาขอความอนุเคราะห์ และขอขอบพระคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

(รองศาสตราจารย์ นายแพทย์ฉัตรชัย เอกปัญญาสกุล)
รักษาการแทนคณบดีบัณฑิตวิทยาลัย

แบบสอบถาม

สำนักงานคณบดีบัณฑิตวิทยาลัย
โทร. 0 2649 5064
หมายเหตุ : สอบถามข้อมูลเพิ่มเติมกรุณาติดต่อนิสิต โทรศัพท์ 086 788 6687

ที่ อว 8718/1769

บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ
114 สุขุมวิท 23 แขวงคลองเตยเหนือ
เขตวัฒนา กรุงเทพฯ 10110

9 สิงหาคม 2564

เรื่อง ขอความอนุเคราะห์เก็บข้อมูลเพื่อการวิจัย

เรียน Human Resources Management (AIS) บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)

เนื่องด้วย นายธีรศักดิ์ พลพันธ์ นิสิตระดับปริญญาเอก สาขาวิชาการวิจัยพฤติกรรมศาสตร์ประยุกต์ มหาวิทยาลัยศรีนครินทรวิโรฒ ได้รับอนุมัติให้ทำปริญญานิพนธ์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” โดยมี ผู้ช่วยศาสตราจารย์ ดร.ศรัณย์ พิมพ์ทอง และผู้ช่วยศาสตราจารย์ ดร.กาญจนา ภัทราวิวัฒน์ เป็นอาจารย์ที่ปรึกษาปริญญานิพนธ์

ในการนี้ นิสิตขอความอนุเคราะห์เก็บข้อมูล โดยใช้แบบสอบถามออนไลน์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” กับพนักงานในวัยทำงานตอนต้น โดยสแกนผ่าน QR Code หรือ https://shorturl.at/abgBI เพื่อเป็นข้อมูลในการวิจัย ระหว่างเดือนสิงหาคม 2564 ถึงเดือนตุลาคม 2564 ทั้งนี้ นิสิตจะเป็นผู้ประสานงานในรายละเอียดดังกล่าวต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาขอความอนุเคราะห์ และขอขอบพระคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

(รองศาสตราจารย์ นายแพทย์ฉัตรชัย เอกปัญญาสกุล)
รักษาการแทนคณบดีบัณฑิตวิทยาลัย

แบบสอบถาม

สำนักงานคณบดีบัณฑิตวิทยาลัย
โทร. 0 2649 5064
หมายเหตุ : สอบถามข้อมูลเพิ่มเติมกรุณาติดต่อนิสิต โทรศัพท์ 086 788 6687

ที่ อว 8718/1769

บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ
114 สุขุมวิท 23 แขวงคลองเตยเหนือ
เขตวัฒนา กรุงเทพฯ 10110

9 สิงหาคม 2564

เรื่อง ขอความอนุเคราะห์เก็บข้อมูลเพื่อการวิจัย

เรียน Director of Project Management and Development (MontAzure) บริษัท กมลา บีช รีสอร์ท แอนด์ โฮเทลแมเนจเม้นท์ จำกัด

เนื่องด้วย นายธีรศักดิ์ พลพันธ์ นิสิตระดับปริญญาเอก สาขาวิชาการวิจัยพฤติกรรมศาสตร์ประยุกต์ มหาวิทยาลัยศรีนครินทรวิโรฒ ได้รับอนุมัติให้ทำปริญญานิพนธ์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” โดยมี ผู้ช่วยศาสตราจารย์ ดร.ศรัณย์ พิมพ์ทอง และผู้ช่วยศาสตราจารย์ ดร.กาญจนา ภัทราวิวัฒน์ เป็นอาจารย์ที่ปรึกษาปริญญานิพนธ์

ในการนี้ นิสิตขอความอนุเคราะห์เก็บข้อมูล โดยใช้แบบสอบถามออนไลน์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” กับพนักงานในวัยทำงานตอนต้น โดยสแกนผ่าน QR Code หรือ https://shorturl.at/abgBI เพื่อเป็นข้อมูลในการวิจัย ระหว่างเดือนสิงหาคม 2564 ถึงเดือนตุลาคม 2564 ทั้งนี้ นิสิตจะเป็นผู้ประสานงานในรายละเอียดดังกล่าวต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาขอความอนุเคราะห์ และขอขอบพระคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

(รองศาสตราจารย์ นายแพทย์ฉัตรชัย เอกปัญญาสกุล)
รักษาการแทนคณบดีบัณฑิตวิทยาลัย

แบบสอบถาม

สำนักงานคณบดีบัณฑิตวิทยาลัย
โทร. 0 2649 5064
หมายเหตุ : สอบถามข้อมูลเพิ่มเติมกรุณาติดต่อนิสิต โทรศัพท์ 086 788 6687

ที่ อว 8718/1775

บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ
114 สุขุมวิท 23 แขวงคลองเตยเหนือ
เขตวัฒนา กรุงเทพฯ 10110

10 สิงหาคม 2564

เรื่อง ขอความอนุเคราะห์เก็บข้อมูลเพื่อการวิจัย

เรียน ผู้กำกับการสถานีตำรวจภูธรคลองหลวง ปทุมธานี

เนื่องด้วย นายธีรศักดิ์ พลพันธ์ นิสิตระดับปริญญาเอก สาขาวิชาการวิจัยพฤติกรรมศาสตร์ประยุกต์ มหาวิทยาลัยศรีนครินทรวิโรฒ ได้รับอนุมัติให้ทำปริญญานิพนธ์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” โดยมี ผู้ช่วยศาสตราจารย์ ดร.ศรัณย์ พิมพ์ทอง และผู้ช่วยศาสตราจารย์ ดร.กาญจนา ภัทราวิวัฒน์ เป็นอาจารย์ที่ปรึกษาปริญญานิพนธ์

ในการนี้ นิสิตขอความอนุเคราะห์เก็บข้อมูล โดยใช้แบบสอบถามออนไลน์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” กับพนักงานในวัยทำงานตอนต้น โดยสแกนผ่าน QR Code หรือ https://shorturl.at/abgBI เพื่อเป็นข้อมูลในการวิจัย ระหว่างเดือนสิงหาคม 2564 ถึงเดือนตุลาคม 2564 ทั้งนี้ นิสิตจะเป็นผู้ประสานงานในรายละเอียดดังกล่าวต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาขอความอนุเคราะห์ และขอขอบพระคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

(รองศาสตราจารย์ นายแพทย์ฉัตรชัย เอกปัญญาสกุล)
รักษาการแทนคณบดีบัณฑิตวิทยาลัย

แบบสอบถาม

สำนักงานคณบดีบัณฑิตวิทยาลัย
โทร. 0 2649 5064
หมายเหตุ : สอบถามข้อมูลเพิ่มเติมกรุณาติดต่อนิสิต โทรศัพท์ 086 788 6687

ที่ อว 8718/1775

บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ
114 สุขุมวิท 23 แขวงคลองเตยเหนือ
เขตวัฒนา กรุงเทพฯ 10110

10 สิงหาคม 2564

เรื่อง ขอความอนุเคราะห์เก็บข้อมูลเพื่อการวิจัย

เรียน ผู้จัดการฝ่ายทรัพยากรบุคคล บริษัท จีเอเบิล จำกัด (สำนักงานใหญ่)

เนื่องด้วย นายธีรศักดิ์ พลพันธ์ นิสิตระดับปริญญาเอก สาขาวิชาการวิจัยพฤติกรรมศาสตร์ประยุกต์ มหาวิทยาลัยศรีนครินทรวิโรฒ ได้รับอนุมัติให้ทำปริญญานิพนธ์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” โดยมี ผู้ช่วยศาสตราจารย์ ดร.ศรัณย์ พิมพ์ทอง และผู้ช่วยศาสตราจารย์ ดร.กาญจนา ภัทราวิวัฒน์ เป็นอาจารย์ที่ปรึกษาปริญญานิพนธ์

ในการนี้ นิสิตขอความอนุเคราะห์เก็บข้อมูล โดยใช้แบบสอบถามออนไลน์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” กับพนักงานในวัยทำงานตอนต้น โดยสแกนผ่าน QR Code หรือ https://shorturl.at/abgBI เพื่อเป็นข้อมูลในการวิจัย ระหว่างเดือนสิงหาคม 2564 ถึงเดือนตุลาคม 2564 ทั้งนี้ นิสิตจะเป็นผู้ประสานงานในรายละเอียดดังกล่าวต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาขอความอนุเคราะห์ และขอขอบพระคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

(รองศาสตราจารย์ นายแพทย์ฉัตรชัย เอกปัญญาสกุล)
รักษาการแทนคณบดีบัณฑิตวิทยาลัย

แบบสอบถาม

สำนักงานคณบดีบัณฑิตวิทยาลัย
โทร. 0 2649 5064
หมายเหตุ : สอบถามข้อมูลเพิ่มเติมกรุณาติดต่อนิสิต โทรศัพท์ 086 788 6687

ที่ อว 8718/1769

บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ
114 สุขุมวิท 23 แขวงคลองเตยเหนือ
เขตวัฒนา กรุงเทพฯ 10110

9 สิงหาคม 2564

เรื่อง ขอความอนุเคราะห์เก็บข้อมูลเพื่อการวิจัย

เรียน ผู้อำนวยการศูนย์อนุรักษ์พลังงานแห่งประเทศไทย สภาอุตสาหกรรมแห่งประเทศไทย

เนื่องด้วย นายธีรศักดิ์ พลพันธ์ นิสิตระดับปริญญาเอก สาขาวิชาการวิจัยพฤติกรรมศาสตร์ประยุกต์ มหาวิทยาลัยศรีนครินทรวิโรฒ ได้รับอนุมัติให้ทำปริญญานิพนธ์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” โดยมี ผู้ช่วยศาสตราจารย์ ดร.ศรัณย์ พิมพ์ทอง และผู้ช่วยศาสตราจารย์ ดร.กาญจนา ภัทราวิวัฒน์ เป็นอาจารย์ที่ปรึกษาปริญญานิพนธ์

ในการนี้ นิสิตขอความอนุเคราะห์เก็บข้อมูล โดยใช้แบบสอบถามออนไลน์ เรื่อง “ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น” กับพนักงานในวัยทำงานตอนต้น โดยสแกนผ่าน QR Code หรือ https://shorturl.at/abgBI เพื่อเป็นข้อมูลในการวิจัย ระหว่างเดือนสิงหาคม 2564 ถึงเดือนตุลาคม 2564 ทั้งนี้ นิสิตจะเป็นผู้ประสานงานในรายละเอียดดังกล่าวต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาขอความอนุเคราะห์ และขอขอบพระคุณมา ณ โอกาสนี้

ขอแสดงความนับถือ

(รองศาสตราจารย์ นายแพทย์ฉัตรชัย เอกปัญญาสกุล)
รักษาการแทนคณบดีบัณฑิตวิทยาลัย

แบบสอบถาม

สำนักงานคณบดีบัณฑิตวิทยาลัย
โทร. 0 2649 5064
หมายเหตุ : สอบถามข้อมูลเพิ่มเติมกรุณาติดต่อนิสิต โทรศัพท์ 086 788 6687

ภาคผนวก จ

รายงานผลการตรวจสอบค่าความเชื่อมั่น (Reliability) **ของเครื่องมือวัดงานวิจัย**

รายงานผลการตรวจสอบค่าความเชื่อมั่น (Reliability) ของเครื่องมือวัดงานวิจัย

เรื่อง ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น

CAUSAL FACTORS OF PRIVACY DATA PROTECTION BEHAVIORS ON ELECTRONICS TRANSACTIONS IN FIRST JOBBERS

รายงานผลการตรวจสอบค่าความเชื่อมั่น (Reliability) ของเครื่องมือวัดงานวิจัย

ผลการตรวจสอบนี้ เป็นการตรวจประเมินคุณภาพความเที่ยง ความคงเส้นคงวา (Consistency) และความน่าเชื่อถือของเครื่องมือวัดของผลที่ได้ ถึงแม้จะมีการวัดซ้ำหรือวัดจำนวนหลายๆ ครั้งซึ่งผลที่ได้มีความคงที่ไม่เปลี่ยนแปลงไปจากเดิม ของงานวิจัยเรื่องปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเล็กทรอนิกส์ในกลุ่มวัยทำงานตอนต้น รวมไปถึงเพื่อให้แน่ใจว่ากลุ่มตัวอย่างเมื่อได้อ่านในเนื้อหาจะมีความเข้าใจที่ตรงกันและสามารถตอบคำถามได้ตามความเป็นจริงทุกข้อ จากการนำเครื่องมือวัด/แบบสอบถามงานวิจัยไปทดลองใช้ (Try out) กับกลุ่มตัวอย่างที่มีลักษณะใกล้เคียงกับกลุ่มตัวอย่างในงานวิจัยนี้ จำนวน 100 ชุด ด้วยวิธีการประมาณค่าความเชื่อมั่นแบบสอดคล้องภายใน (Internal Consistency Reliability) จากการหาค่าสัมประสิทธิ์แอลฟ่าของครอนบาค (Cronbach's Alpha Coefficient) เพื่อตรวจสอบความสอดคล้องของข้อคำถามในเครื่องมือวัด/แบบสอบถาม

วิธีการและขั้นตอนการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัดงานวิจัย

วิธีการและขั้นตอนการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัดงานวิจัย มีดังนี้

1. การเก็บรวบรวมข้อมูลและการเตรียมข้อมูลกลุ่มทดลองใช้

1) นำเครื่องมือวัด/แบบสอบถามงานวิจัยที่ได้ดำเนินการปรับปรุงแก้ไขเป็นที่เรียบร้อยแล้วจากการประเมินความเหมาะสมของความตรงด้านเนื้อหา ไปหาค่าความเชื่อมั่นของเครื่องมือวัดโดยจัดทำเป็นแบบสอบถามออนไลน์ เพื่อเป็นการรวบรวมข้อมูลทดลองใช้ ในงานวิจัยตั้งแต่วันที่

3-25 กรกฎาคม 2564 ทั้งนี้ ในแบบสอบถามออนไลน์ เป็นลักษณะการบังคับตอบ/จำเป็น (Required) ที่ให้ผู้ตอบแบบสอบถามจำเป็นต้องตอบคำถามนั้นๆ ให้ครบทุกข้อคำถามถึงจะส่งแบบสอบถาม/คำตอบได้ เพื่อป้องกันปัญหาข้อมูลขาดหาย (Missing Data)

แบบสอบถามมีจำนวนข้อคำถามทั้งหมด 190 ข้อคำถามแบ่งออกเป็น ตอนที่ 1 ข้อมูลทั่วไป (จำนวน 8 ข้อคำถาม เริ่มต้นข้อ 1-8) ได้แก่ อายุ ความถี่ในการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ เพศ ระดับการศึกษาสูงสุด สถานภาพสมรส เขตพื้นที่ปฏิบัติงาน ประเภทหน่วยงาน และระดับเงินเดือนปัจจุบัน ตอนที่ 2 พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (จำนวน 43 ข้อคำถาม เริ่มต้นข้อ 9-51) และตอนที่ 3 ความความคิดเห็นต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (จำนวน 139 ข้อคำถาม เริ่มต้นข้อ 52-190)

2) การเก็บรวมรวบรวมข้อมูลจากกลุ่มทดลองใช้ ซึ่งมีลักษณะใกล้เคียงกับกลุ่มตัวอย่างในงานวิจัยนี้คือ กลุ่มวัยทำงานตอนต้น อายุระหว่าง 20-29 ปี และมีความถี่ในการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์โดยเฉลี่ยมากกว่า 5 ครั้ง/เดือน ในรอบ 6 เดือนติดต่อกันที่ผ่านมา ยกเว้นเขตพื้นที่ปฏิบัติงานของงานวิจัยนี้ (กรุงเทพมหานคร นนทบุรีและปทุมธานี) ที่มาจากการสุ่มกลุ่มตัวอย่างแบบกลุ่ม 2 ขั้นตอน (Two-stage cluster sampling) โดยเก็บรวมรวบข้อมูลจากกลุ่มทดลองใช้และสามารถให้ข้อมูลทดลองในงานวิจัยนี้ได้ในจังหวัดสมุทรปราการ สมุทรสาคร นครปฐม ฉะเชิงเทราและชลบุรี ซึ่งจะเห็นว่ามีเขตพื้นที่ปฏิบัติงานใกล้เคียงกับกลุ่มตัวอย่างในงานวิจัยนี้

ผลจากการเก็บรวมรวบรวมข้อมูลจากกลุ่มทดลองใช้ ตั้งแต่วันที่ 3-25 กรกฎาคม 2564 พบว่ากลุ่มทดลองใช้ให้ข้อมูลมาทั้งสิ้น 126 ชุด ทั้งนี้ผู้วิจัยได้คัดเลือกข้อมูลการตอบแบบสอบถามที่มีความสมบูรณ์ คัดเลือกค่าสุดโต่ง (Outlier) หรือการทิ้งดิ่งของการให้คะแนนออกไป และใช้เป็นข้อมูลทดลองใช้ (Try out) ของการตรวจสอบค่าความเชื่อมั่นของเครื่องมือวัดงานวิจัยนี้ จำนวนทั้งสิ้น 100 ชุด

2. การเตรียมการวิเคราะห์ข้อมูลเพื่อหาค่าความเชื่อมั่น

การวิเคราะห์หาค่าความเชื่อมั่นของเครื่องมือวัด หรือวิธีการประมาณค่าความเชื่อมั่นแบบสอดคล้องภายในเพื่อตรวจสอบความสอดคล้องของข้อคำถามในเครื่องมือวัด งานวิจัยนี้ใช้วิธีการ

หาค่าสัมประสิทธิ์แอลฟ่าของครอนบาคซึ่งเป็นเครื่องมือวัด และใช้โปรแกรมสำเร็จรูปทางสถิติหาค่าความเชื่อมั่นของเครื่องมือวัด/แบบสอบถาม

แบบสอบถาม ตอนที่ 1 ข้อมูลทั่วไป (จำนวน 8 ข้อคำถาม เริ่มต้นข้อ 1-8) ซึ่งเป็นข้อมูลเชิงคุณภาพ ได้กำหนดระดับของข้อมูล (Measure) เป็นแบบ Nominal Scale (นามบัญญัติ) เพื่อแบ่งกลุ่ม/จำแนกข้อมูล ได้แก่ ความถี่ในการเข้าใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ เพศ ระดับการศึกษาสูงสุด สถานภาพสมรส เขตพื้นที่ปฏิบัติงาน ประเภทหน่วยงานและระดับเงินเดือนปัจจุบัน ยกเว้นอายุ ซึ่งเป็นข้อมูลเชิงปริมาณ จะกำหนดข้อมูลเป็นแบบ Ratio Scale/Scale โดยจะใช้เป็นสถิติเชิงบรรยาย (Descriptive statistics) ของกลุ่มทดลองใช้

สำหรับแบบสอบถามในตอนที่ 2 พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (จำนวน 43 ข้อคำถาม เริ่มต้นข้อ 9-51) และตอนที่ 3 ความความคิดเห็นต่อพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ (จำนวน 139 ข้อคำถาม เริ่มต้นข้อ 52-190) รวมทั้ง 2 ตอนจำนวน 182 ข้อ กำหนดข้อมูลเป็นแบบ Scale เนื่องจากเป็นแบบมาตราส่วนประมาณค่า (Rating Scale) โดยใช้ 6 ระดับการวัด (ตั้งแต่ระดับ “จริงที่สุด” ถึง “ไม่จริงเลย” โดยการตรวจให้คะแนนมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน) ตามลำดับตามวิธีการวัดแบบประเมินเกี่ยวกับพฤติกรรมและความคิดเห็น โดยจะใช้ในการหาค่าความเชื่อมั่นของเครื่องมือวัด/แบบสอบถาม

การกำหนดช่องค่า Values หรือการกำหนดคำอธิบายให้กับค่าตัวแปร หากข้อคำถามเชิงบวก จะให้คะแนนมาจากผู้ที่ตอบ จริงที่สุดได้ 6 คะแนน จริงได้ 5 คะแนน ค่อนข้างจริงได้ 4 คะแนน ค่อนข้างไม่จริงได้ 3 คะแนน ไม่จริงได้ 2 คะแนน และไม่จริงเลยได้ 1 คะแนน ส่วนข้อคำถามเชิงลบ/นิเสธ จะให้คะแนนตรงกันข้าม จริงที่สุดได้ 1 คะแนน จริงได้ 2 คะแนน ค่อนข้างจริงได้ 3 คะแนน ค่อนข้างไม่จริงได้ 4 คะแนน ไม่จริงได้ 5 คะแนน และไม่จริงเลยได้ 6 คะแนน โดยการพิจารณาข้อคำถามของแต่ละแบบวัด

ข้อคำถามของแบบวัดพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ สำหรับการกำหนดช่องค่า Values มีรายละเอียด ดังนี้

องค์ประกอบ/แต่ละแบบวัด	ข้อคำถาม		จำนวนข้อ
	ทางบวก	ทางลบ	
การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป **(ข้อที่** 9-31)	16 ข้อ	7 ข้อ (2, 3, 6, 8, 11, 19, 22) *ข้อที่ 10, 11, 14, 16, 19, 27, 30*	23 ข้อ
การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค **(ข้อที่** 32-51)	15 ข้อ	5 ข้อ (1, 2, 5, 6, 19) *ข้อที่ 32, 33, 36, 37, 50*	20 ข้อ
ชุดที่ 1 แบบวัดการรับรู้ถึงโอกาสเสี่ยง (Perceived Vulnerability) ที่บุคคลอื่นจะเข้าใช้งานแทนตน **(ข้อที่** 52-64)	10 ข้อ	3 ข้อ (4, 5, 12)	13 ข้อ
-จากผู้ให้บริการ (7 ข้อ)	*+,-(5 ข้อ และ2 ข้อ)*	*ข้อที่ 55, 56*	
-จากการเข้าใช้บริการ (6 ข้อ)	*+,- (5 ข้อ และ1 ข้อ)*	*ข้อที่ 63*	
ชุดที่ 2 แบบวัดการรับรู้ถึงความรุนแรง (Perceived Severity) ที่บุคคลอื่นจะเข้าใช้งานแทนตน **(ข้อที่** 65-77)	10 ข้อ	3 ข้อ (1, 4, 7)	13 ข้อ
-ด้านทรัพย์สิน (6 ข้อ)	*+,- (4 ข้อ และ2 ข้อ)*	*ข้อที่ 65, 68*	
-ตัวบุคคล (7 ข้อ)	*+,- (6 ข้อ และ1 ข้อ)*	*ข้อที่ 71*	
ชุดที่ 3 แบบวัดความคาดหวังในผลลัพธ์ (Response Efficacy) ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล **(ข้อที่** 78-89)	9 ข้อ	3 ข้อ (4, 5, 11)	12 ข้อ
-ปฏิบัติโดยทั่วไป (6 ข้อ)	*+,- (4 ข้อ และ2 ข้อ)*	*ข้อที่ 81, 82*	
-ปฏิบัติแบบขั้นสูง (6 ข้อ)	*+,- (5 ข้อ และ1 ข้อ)*	*ข้อที่ 88*	
ชุดที่ 4 แบบวัดความคาดหวังความสามารถของตนเอง (Self-efficacy) ในการปกป้องข้อมูลส่วนบุคคล **(ข้อที่** 90-108)	16 ข้อ	3 ข้อ (6, 11, 15)	19 ข้อ
-การใช้งานเครือข่ายคอมฯ (6 ข้อ)	*+,- (5 ข้อ และ1 ข้อ)*	*ข้อที่ 95*	
-ความพร้อมรับมือกับปัญหา (7 ข้อ)	*+,- (6 ข้อ และ1 ข้อ)*	*ข้อที่ 100*	
-สามารถควบคุมสถานการณ์ (6 ข้อ)	*+,- (5 ข้อ และ1 ข้อ)*	*ข้อที่ 104*	

องค์ประกอบ/แต่ละแบบวัด	ข้อคำถาม		จำนวนข้อ
	ทางบวก	ทางลบ	
ชุดที่ 5 แบบวัดความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่าย (Response Cost) เพื่อปกป้องข้อมูลส่วนบุคคล **(ข้อที่** 109-120)	11 ข้อ	1 ข้อ (12)	12 ข้อ
-ในรูปตัวเงิน (6 ข้อ)	*+(6 ข้อ)*	*ไม่มี*	
-ไม่ได้อยู่ในรูปตัวเงิน (6 ข้อ)	*+,- (5 ข้อ และ1 ข้อ)*	*ข้อที่ 120*	
ชุดที่ 6 แบบวัดคุณลักษณะของระบบ (System Characteristics) เพื่อปกป้องข้อมูลส่วนบุคคล **(ข้อที่** 121-132)	10 ข้อ	2 ข้อ (6, 12)	12 ข้อ
-คุณลักษณะเด่น (6 ข้อ)	*+,- (5 ข้อ และ1 ข้อ)*	*ข้อที่ 126*	
-ส่วนติดต่อกับผู้ใช้งาน (6 ข้อ)	*+,- (5 ข้อ และ1 ข้อ)*	*ข้อที่ 132*	
ชุดที่ 7 แบบวัดการคล้อยตามกลุ่มอ้างอิง (Subjective Norms) ในการปกป้องข้อมูลส่วนบุคคล **(ข้อที่** 133-145)	10 ข้อ	3 ข้อ (4, 9, 11)	13 ข้อ
-บุคคลรอบข้างที่ใกล้ชิด (6 ข้อ)	*+,- (5 ข้อ และ1 ข้อ)*	*ข้อที่ 136*	
-ผู้ทรงอิทธิพลเทคโนโลยี (7 ข้อ)	*+,- (5 ข้อ และ2 ข้อ)*	*ข้อที่ 141, 143*	
ชุดที่ 8 แบบวัดการรับรู้ถึงประโยชน์ (Usefulness) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล **(ข้อที่** 146-157)	10 ข้อ	2 ข้อ (5, 10)	12 ข้อ
-เกิดประโยชน์ต่อตนเอง (6 ข้อ)	*+,- (5 ข้อ และ1 ข้อ)*	*ข้อที่ 150*	
-เพิ่มประสิทธิผลปลอดภัย (6 ข้อ)	*+,- (5 ข้อ และ1 ข้อ)*	*ข้อที่ 155*	
ชุดที่ 9 แบบวัดการรับรู้ถึงความง่าย (Ease of Use) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล **(ข้อที่** 158-169)	9 ข้อ	3 ข้อ (4, 6, 11)	12 ข้อ
-ง่ายต่อการเรียนรู้ (6 ข้อ)	*+,- (4 ข้อ และ2 ข้อ)*	*ข้อที่ 161, 163*	
-ความไม่ซับซ้อนของระบบ(6 ข้อ)	*+,- (5 ข้อ และ1 ข้อ)*	*ข้อที่ 168*	
ชุดที่ 10 แบบวัดทัศนคติ (Attitude) มีต่อการปกป้องข้อมูลส่วนบุคคล **(ข้อที่** 170-182)	12 ข้อ	1 ข้อ (4)	13 ข้อ

องค์ประกอบ/แต่ละแบบวัด	ข้อคำถาม		จำนวนข้อ
	ทางบวก	ทางลบ	
-ความเชื่อผลการกระทำ (7 ข้อ) -ประเมินคุณค่าการกระทำ(6 ข้อ)	*+,- (6 ข้อ และ1 ข้อ)* *+(6 ข้อ)*	*ข้อที่ 173* *ไม่มี*	
ชุดที่ 11 แบบวัดความตั้งใจ (Intention) ในการปกป้องข้อมูลส่วนบุคคล **(ข้อที่** 183-190) -ความตั้งใจปกป้องข้อมูล (8 ข้อ)	7 ข้อ *+,- (7 ข้อ และ1 ข้อ)*	1 ข้อ (6) *ข้อที่ 188*	8 ข้อ
รวมข้อคำถาม		***คำถามเชิงลบ/นิเสธ= 37***	182

ดังนั้น รวมการกำหนดช่องค่า Values หรือการกำหนดคำอธิบายให้กับค่าตัวแปร หากข้อคำถามเชิงลบ/นิเสธ ทั้งหมดจำนวน 37 ข้อคำถาม (จริงที่สุดได้ 1 คะแนน จริงได้ 2 คะแนน ค่อนข้างจริงได้ 3 คะแนน ค่อนข้างไม่จริงได้ 4 คะแนน ไม่จริงได้ 5 คะแนน และไม่จริงเลยได้ 6 คะแนน)

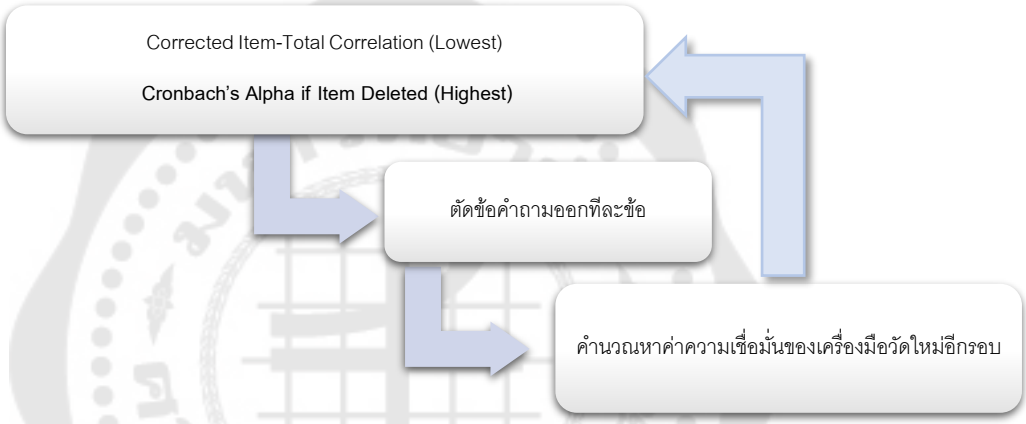
3. **เกณฑ์ที่ใช้พิจารณา** ช่วงสัมประสิทธิ์ความเชื่อมั่น (Reliabilty Coefficent) คือ 0-1 หากเข้าใกล้ 1 แสดงว่าเครื่องมือวัด/แบบสอบถามมีความน่าเชื่อถือสูง (Iacobucci & Duhachek, 2003; Taber, 2018) และหากเป็นค่าความเชื่อมั่นแบบสัมประสิทธิ์แอลฟ่าของครอนบาค (Cronbach's Alpha Coefficient) ควรมีค่าตั้งแต่ 0.70 ขึ้นไปสำหรับแบบวัดจากแนวคิดที่พัฒนาขึ้นมาใหม่ จึงจะถือว่าแบบวัดนั้นๆ มีความน่าเชื่อถือได้สูง ข้อคำถามมีความสอดคล้องกันภายใน ความเชื่อมั่นแบบสอดคล้องภายในสูง (DeVellis & Thorpe, 2021) นอกจากนี้เกณฑ์การประเมินความเที่ยงสัมประสิทธิ์แอลฟ่าของครอนบาคของ ศิริชัย กาญจนวาสี (2556) โดยพิจารณาค่าสัมประสิทธิ์แอลฟา (α) มีการแปลความหมายระดับความเที่ยงดังนี้ มากกว่า 0.9 = ดีมาก, มากกว่า 0.8 = ดี, มากกว่า 0.7 = พอใช้, มากกว่า 0.6 = ค่อนข้างพอใช้, มากกว่า 0.5 = ต่ำ และน้อยกว่าหรือเท่ากับ 0.5 = ไม่สามารถรับได้

วิธีการ/ขั้นตอนที่ใช้ให้เครื่องมือวัด/แบบสอบถามมีค่าความเชื่อมั่นเพิ่มขึ้น

(1) พิจารณาจากข้อคำถามที่มีค่า Corrected Item-Total Correlation ต่ำที่สุด ควบคู่กับ Cronbach's Alpha if Item Deleted ที่มีค่าสูงสุด (เป็นค่าหลักในการพิจารณาตัดข้อคำถาม)

(2) โดยตัดข้อคำถามออกทีละข้อ จะมีผลทำให้ค่าความเชื่อมั่นของเครื่องมือวัด/แบบสอบถามเพิ่มขึ้น

(3) จากนั้นทำการคำนวณหาค่าความเชื่อมั่นของเครื่องมือวัด/แบบสอบถามอีกรอบ



4. ผลการวิเคราะห์ข้อมูลเพื่อหาค่าความเชื่อมั่น (แต่ละแบบวัด)

ผู้วิจัยขอจัดทำเป็นตารางสรุปการวิเคราะห์ข้อมูลเพื่อหาค่าความเชื่อมั่นของแต่ละแบบวัด ดังนี้

ตารางสรุปการตรวจสอบค่าความเชื่อมั่น (Reliability) ของเครื่องมือวัดงานวิจัย

องค์ประกอบ/แต่ละแบบวัด	**ข้อคำถาม**				**จำนวนข้อที่นำไปใช้เป็นเครื่องมือ**
	เดิม		**ภายหลังตัดข้อคำถาม**		
	จำนวนข้อ (+,-)	**α**	**จำนวนข้อ (+,-)**	**α>0.70**	
การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป	23 ข้อ (16, 7)	0.508	15 ข้อ (12, 3)	**0.730**	**15 ข้อ**
การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค	20 ข้อ (15, 5)	0.519	14 ข้อ (11, 3)	**0.719**	**14 ข้อ**
ชุดที่ 1 แบบวัดการรับรู้ถึงโอกาสเสี่ยง (Perceived Vulnerability) ที่บุคคลอื่นจะเข้าใช้งานแทนตน	13 ข้อ (10, 3)	0.541	8 ข้อ (7, 1)	**0.724**	**8 ข้อ**
-จากผู้ให้บริการ (7 ข้อ)	7 ข้อ (5, 2)		5 ข้อ (4, 1)		
-จากการเข้าใช้บริการ (6 ข้อ)	6 ข้อ (5, 1)		3 ข้อ (3, 0)		
ชุดที่ 2 แบบวัดการรับรู้ถึงความรุนแรง (Perceived Severity) ที่บุคคลอื่นจะเข้าใช้งานแทนตน	13 ข้อ (10, 3)	0.641	9 ข้อ (9, 0)	**0.737**	**9 ข้อ**
-ด้านทรัพย์สิน (6 ข้อ)	6 ข้อ (4, 2)		4 ข้อ (4, 0)		
-ตัวบุคคล (7 ข้อ)	7 ข้อ (6, 1)		5 ข้อ (5, 0)		
ชุดที่ 3 แบบวัดความคาดหวังในผลลัพธ์ (Response Efficacy) ของการปฏิบัติตามวิธีการปกป้องข้อมูลส่วนบุคคล	12 ข้อ (9, 3)	0.584	7 ข้อ (6, 1)	**0.730**	**7 ข้อ**
-ปฏิบัติโดยทั่วไป (6 ข้อ)	6 ข้อ (4, 2)		3 ข้อ (3, 0)		
-ปฏิบัติแบบขั้นสูง (6 ข้อ)	6 ข้อ (5, 1)		4 ข้อ (3, 1)		
ชุดที่ 4 แบบวัดความคาดหวังความสามารถของตนเอง (Self-efficacy) ในการปกป้องข้อมูลส่วนบุคคล	19 ข้อ (16, 3)	0.467	13 ข้อ (11, 2)	**0.754**	**13 ข้อ**
-การใช้งานเครือข่ายคอมฯ (6 ข้อ)	6 ข้อ (5, 1)		3 ข้อ (2, 1)		

องค์ประกอบ/แต่ละแบบวัด	ข้อคำถาม				จำนวนข้อที่นำไปใช้เป็นเครื่องมือ
	เดิม		ภายหลังตัดข้อคำถาม		
-ความพร้อมรับมือกับปัญหา (7 ข้อ)	7 ข้อ (6, 1)		5 ข้อ (5, 0)		
-สามารถควบคุมสถานการณ์ (6 ข้อ)	6 ข้อ (5, 1)		5 ข้อ (4, 1)		
ชุดที่ 5 แบบวัดความคาดหวังในความคุ้มค่าของต้นทุนและค่าใช้จ่าย (Response Cost) เพื่อปกป้องข้อมูลส่วนบุคคล	12 ข้อ (11, 1)	0.528	7 ข้อ (6, 1)	0.734	**7 ข้อ**
-ในรูปตัวเงิน (6 ข้อ)	6 ข้อ (6, 0)		3 ข้อ (3, 0)		
-ไม่ได้อยู่ในรูปตัวเงิน (6 ข้อ)	6 ข้อ (5, 1)		4 ข้อ (3, 1)		
ชุดที่ 6 แบบวัดคุณลักษณะของระบบ (System Characteristics) เพื่อปกป้องข้อมูลส่วนบุคคล	12 ข้อ (10, 2)	0.559	7 ข้อ (6, 1)	0.725	**7 ข้อ**
-คุณลักษณะเด่น (6 ข้อ)	6 ข้อ (5, 1)		3 ข้อ (3, 0)		
-ส่วนติดต่อกับผู้ใช้งาน (6 ข้อ)	6 ข้อ (5, 1)		4 ข้อ (3, 1)		
ชุดที่ 7 แบบวัดการคล้อยตามกลุ่มอ้างอิง (Subjective Norms) ในการปกป้องข้อมูลส่วนบุคคล	13 ข้อ (10, 3)	0.564	9 ข้อ (7, 2)	0.721	**9 ข้อ**
-บุคคลรอบข้างที่ใกล้ชิด (6 ข้อ)	6 ข้อ (5, 1)		4 ข้อ (3, 1)		
-ผู้ทรงอิทธิพลเทคโนโลยี (7 ข้อ)	7 ข้อ (5, 2)		5 ข้อ (4, 1)		
ชุดที่ 8 แบบวัดการรับรู้ถึงประโยชน์ (Usefulness) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล	12 ข้อ (10, 2)	0.542	6 ข้อ (6, 0)	0.722	**6 ข้อ**
-เกิดประโยชน์ต่อตนเอง (6 ข้อ)	6 ข้อ (5, 1)		3 ข้อ (3, 0)		
-เพิ่มประสิทธิผลปลอดภัย(6 ข้อ)	6 ข้อ (5, 1)		3 ข้อ (3, 0)		
ชุดที่ 9 แบบวัดการรับรู้ถึงความง่าย (Ease of Use) ในการจัดการตั้งค่าปกป้องข้อมูลส่วนบุคคล	12 ข้อ (9, 3)	0.520	6 ข้อ (6, 0)	0.837	**6 ข้อ**
-ง่ายต่อการเรียนรู้ (6 ข้อ)	6 ข้อ (4, 2)		3 ข้อ (3, 0)		
-ความไม่ซับซ้อนระบบ(6 ข้อ)	6 ข้อ (5, 1)		3 ข้อ (3, 0)		

องค์ประกอบ/แต่ละแบบวัด	ข้อคำถาม				จำนวนข้อที่นำไปใช้เป็นเครื่องมือ
	เดิม		ภายหลังตัดข้อคำถาม		
ชุดที่ 10 แบบวัดทัศนคติ (Attitude) มีต่อการปกป้องข้อมูลส่วนบุคคล	13 ข้อ (12, 1)	0.563	8 ข้อ (8, 0)	0.753	**8 ข้อ**
-ความเชื่อผลการกระทำ (7 ข้อ)	7 ข้อ (6, 1)		4 ข้อ (4, 0)		
-ประเมินคุณค่าการกระทำ(6 ข้อ)	6 ข้อ (6, 0)		4 ข้อ (4, 0)		
ชุดที่ 11 แบบวัดความตั้งใจ (Intention) ในการปกป้องข้อมูลส่วนบุคคล	8 ข้อ (7, 1)	0.540	5 ข้อ (5, 0)	0.847	**5 ข้อ**
-ความตั้งใจปกป้องข้อมูล (8 ข้อ)	8 ข้อ (7, 1)		5 ข้อ (5, 0)		
ค่าความเชื่อมั่น (α) ภาพรวมทั้งฉบับ	**α** = 0.916 **182 ข้อ**		**α** = 0.941 **114 ข้อ**		114

โดยสรุปรายงานผลการตรวจค่าความเชื่อมั่น (Reliability) ของเครื่องมือวัดงานวิจัยนี้

องค์ประกอบ/แต่ละแบบวัด	ข้อคำถาม				จำนวนข้อที่ลดลง	Corrected Item-Total Correlation (r)
	เดิม		ภายหลังตัดข้อคำถาม			
	จำนวนข้อ (+,-)	α	จำนวนข้อ (+,-)	α>0.70		
การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลทั่วไป	23 ข้อ	0.508	**15 ข้อ**	**0.730**	(8 ข้อ)	0.243-0.670
การปฏิบัติตนในข้อควรระวังเพื่อการปกป้องข้อมูลส่วนบุคคลเชิงเทคนิค	20 ข้อ	0.519	**14 ข้อ**	**0.719**	(6 ข้อ)	0.231-0.609
ชุดที่ 1 แบบวัดการรับรู้ถึงโอกาสเสี่ยง (Perceived Vulnerability)	13 ข้อ	0.541	**8 ข้อ**	**0.724**	(5 ข้อ)	0.238-0.696
ชุดที่ 2 แบบวัดการรับรู้ถึงความรุนแรง (Perceived Severity)	13 ข้อ	0.641	**9 ข้อ**	**0.737**	(4 ข้อ)	0.209-0.706
ชุดที่ 3 แบบวัดความคาดหวังในผลลัพธ์ (Response Efficacy)	12 ข้อ	0.584	**7 ข้อ**	**0.730**	(5 ข้อ)	0.210-0.704
ชุดที่ 4 แบบวัดความคาดหวังความสามารถของตนเอง (Self-efficacy)	19 ข้อ	0.467	**13 ข้อ**	**0.754**	(6 ข้อ)	0.215-0.727
ชุดที่ 5 แบบวัดความคาดหวังในความคุ้มค่าของค่าใช้จ่าย (Response Cost)	12 ข้อ	0.528	**7 ข้อ**	**0.734**	(5 ข้อ)	0.243-0.699
ชุดที่ 6 แบบวัดคุณลักษณะของระบบ (System Characteristics)	12 ข้อ	0.559	**7 ข้อ**	**0.725**	(5 ข้อ)	0.224-0.645
ชุดที่ 7 แบบวัดการคล้อยตามกลุ่มอ้างอิง (Subjective Norms)	13 ข้อ	0.564	**9 ข้อ**	**0.721**	(4 ข้อ)	0.228-0.688
ชุดที่ 8 แบบวัดการรับรู้ถึงประโยชน์ (Usefulness)	12 ข้อ	0.542	**6 ข้อ**	**0.722**	(6 ข้อ)	0.242-0.649
ชุดที่ 9 แบบวัดการรับรู้ถึงความง่าย (Ease of Use)	12 ข้อ	0.520	**6 ข้อ**	**0.837**	(6 ข้อ)	0.329-0.740
ชุดที่ 10 แบบวัดทัศนคติ (Attitude)	13 ข้อ	0.563	**8 ข้อ**	**0.753**	(5 ข้อ)	0.212-0.674
ชุดที่ 11 แบบวัดความตั้งใจ (Intention) ในการปกป้องข้อมูลส่วนบุคคล	8 ข้อ	0.540	**5 ข้อ**	**0.847**	(3 ข้อ)	0.350-0.756
ค่าความเชื่อมั่น (α) ภาพรวมทั้งฉบับ	**α = 0.916 182 ข้อ**		**α = 0.941 114 ข้อ**		(68 ข้อ)	-

ประวัติผู้เขียน

ชื่อ-สกุล	ธีรศักดิ์ พลพันธ์
สถานที่เกิด	เลย
วุฒิการศึกษา	พ.ศ. 2545 วิทยาการสารสนเทศบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ หลักสูตรระบบสารสนเทศเพื่อการจัดการ จาก มหาวิทยาลัยเทคโนโลยีสุรนารี พ.ศ. 2550 วิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการระบบสารสนเทศ จาก สถาบันบัณฑิตพัฒนบริหารศาสตร์ พ.ศ. 2565 ปรัชญาดุษฎีบัณฑิต สาขาวิชาการวิจัยพฤติกรรมศาสตร์ประยุกต์ จาก มหาวิทยาลัยศรีนครินทรวิโรฒ