พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

PREVENTIVE BEHAVIOR OF GENERATION Z ON CYBER THREATS

คณัญญา อิ่มใจ

บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ

2565

พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

คณัญญา อิ่มใจ

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ศิลปศาสตรมหาบัณฑิต สาขาวิชาสารสนเทศศึกษา
คณะมนุษยศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ
ปีการศึกษา 2565

PREVENTIVE BEHAVIOR OF GENERATION Z ON CYBER THREATS

KANANYA IMJAI

A Master's Project Submitted in Partial Fulfillment of the Requirements

for the Degree of MASTER OF ARTS

(Information Studies)

Faculty of Humanities, Srinakharinwirot University

2022

สารนิพนธ์

เรื่อง

พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

ของ

คณัญญา อิ่มใจ

ได้รับอนุมัติจากบัณฑิตวิทยาลัยให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาศิลปศาสตรมหาบัณฑิต สาขาวิชาสารสนเทศศึกษา

ของมหาวิทยาลัยศรีนครินทรวิโรฒ

.....

(รองศาสตราจารย์ นายแพทย์ฉัตรชัย เอกปัญญาสกุล)

คณบดีบัณฑิตวิทยาลัย

.....

คณะกรรมการสอบปากเปล่าสารนิพนธ์

..... ที่ปรึกษาหลัก

(อาจารย์ ดร.วิภากร วัฒนสินธุ์)

..... ประธาน

(ผู้ช่วยศาสตราจารย์ ดร.นิพัทธ์ จงสวัสดิ์)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.ดุษฎี สีวังคำ)

ชื่อเรื่อง	พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด
ผู้วิจัย	คณัญญา อิ่มใจ
ปริญญา	ศิลปศาสตรมหาบัณฑิต
ปีการศึกษา	2565
อาจารย์ที่ปรึกษา	อาจารย์ ดร. วิภากร วัฒนสินธุ์

งานวิจัยนี้มีวัตถุประสงค์เพื่อ (1) เพื่อศึกษาพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่น Z และ (2) ศึกษาอิทธิพลของเพศ ความรู้ และประสบการณ์ ที่มีผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ เครื่องมือที่ใช้คือแบบสอบถามออนไลน์โดยกระจายผ่านทางสื่อสังคมออนไลน์ การหาค่าดัชนีความสอดคล้อง (IOC) จากผู้เชี่ยวชาญ 3 คน มีค่าคะแนนเฉลี่ยระหว่าง 0.67-1.00 คำนวณกลุ่มตัวอย่างโดยใช้โปรแกรม G*Power เก็บข้อมูลจากกลุ่มตัวอย่างในเจเนอเรชั่น Z จำนวน 130 คน ทดลองใช้เครื่องมือวิจัยกับกลุ่มคนเจเนอเรชั่นแซดที่ไม่ใช่กลุ่มตัวอย่าง จำนวน 30 คน เลือกข้อคำถามที่มีค่าความยากง่ายระหว่าง 0.20-0.80 เพื่อวัดความรู้ จากนั้นทดสอบความเชื่อมั่นของแบบสอบถามโดยคำนวณค่าสัมประสิทธิ์ครอนบรัคแอลฟา (Cronbach's alpha coefficient) ได้ค่าสัมประสิทธิ์ครอนบรัคแอลฟาของคำถามด้านประสบการณ์เท่ากับ 0.851 และคำถามด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์เท่ากับ 0.923 สถิติที่ใช้ในการวิเคราะห์ข้อมูล คือ สถิติเชิงพรรณนา ได้แก่ ค่าเฉลี่ย ร้อยละ และส่วนเบี่ยงเบนมาตรฐาน ผลการวิจัยพบว่า ผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง (ร้อยละ 54.60) มีคะแนนเฉลี่ยของความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์อยู่ที่ร้อยละ 46.17 มีประสบการณ์ในภัยคุกคามทางไซเบอร์ในระดับปานกลาง ($\bar{X}$ = 3.14) มีความคิดเห็นในพฤติกรรมป้องกันตนเองจากภัยคุกคามทางไซเบอร์ในระดับมาก ($\bar{X}$ = 3.90) ใช้สถิติเชิงอนุมานเพื่อวิเคราะห์การถดถอยเชิงเส้นหาความสัมพันธ์ของปัจจัยที่มีผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ พบว่า ประสบการณ์สามารถพยากรณ์พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ (b=0.269) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยประสบการณ์มีผลต่อพฤติกรรมในด้านการตั้งค่ารหัสผ่าน การจัดการข้อมูลส่วนบุคคล และการใช้งานอุปกรณ์คอมพิวเตอร์ ในขณะที่เพศและความรู้ไม่มีอิทธิพลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์

คำสำคัญ : พฤติกรรมการป้องกันตนเอง, ภัยคุกคามทางไซเบอร์, ความรู้, ประสบการณ์, เจเนอเรชั่นแซด

Title	PREVENTIVE BEHAVIOR OF GENERATION Z ON CYBER THREATS
Author	KANANYA IMJAI
Degree	MASTER OF ARTS
Academic Year	2022
Thesis Advisor	Vipakorn Vadhanasin , Ph.D.

The purposes of this research are as follows: (1) to study the preventive behavior of Generation Z on cyber threats; and (2) to study impact of gender, knowledge, and experience of preventive behavior on cyber threats. The research tool was an online questionnaire distributed via social media. The instrument was verified by threeexperts with an index of item objective congruence (IOC) scores between 0.67-1.00. The sample was calculated by G*Power program. The data were collected from 130 respondents in Generation Z. The questionnaire was tried out with 30 members of Generation Z, who were not in the sample group. The index of difficulty between 0.2 and 0.8 was used to select questions for knowledge test. A Cronbach's alpha coefficients were used to measure the reliability. The Cronbach's alpha coefficients were 0.851 for experience questions and 0.923 for cyber threat prevention behavior questions. The statistics used in this research were descriptive statistics, comprised of mean, percentage, and standard deviation. The results revealed that most of the respondents were female (54.60%), had the average score of cyber threat knowledge at 46.17%, experienced in cyber threats at medium level ($\bar{X}$ = 3.14), and had opinions on preventive behavior on cyber threats at a high level ($\bar{X}$ = 3.90). The inferential statistics used to analyze a linear regression analysis of factors influencing preventive behavior on cyber threats. The results revealed that cyber threats prevention behavior was predicted by experience (b=0.269) at a statistically significant level of 0.05, who experienced affecting security behavior in areas of password setting, personal information protection, and computer equipment maintenance. However, gender and knowledge did not significantly influence the preventive behavior of cyber threats.

Keyword : Preventive Behavior, Cyber Threat, Knowledge, Experience, Generation Z

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จลุล่วงลงได้ด้วยความกรุณาอย่างสูงจาก อาจารย์ ดร.วิภากร วัฒนสินธุ์ อาจารย์ที่ปรึกษาที่เมตตากรุณาช่วยเหลือให้คำปรึกษา คำแนะนำ ตรวจสอบแก้ไขข้อบกพร่องอันเป็นประโยชน์แก่ผู้วิจัยด้วยความเอาใจใส่อย่างดียิ่ง

ขอขอบพระคุณผู้ช่วยศาสตราจารย์ ดร.นิพัทธ์ จงสวัสดิ์ ประธานกรรมการสอบสารนิพนธ์ และผู้ช่วยศาสตราจารย์ ดร.ดุษฎี สีวังคำ กรรมการสอบสารนิพนธ์ ซึ่งให้ข้อเสนอแนะ ที่เป็นประโยชน์อย่างยิ่งในการจัดทำสารนิพนธ์

ขอขอบพระคุณผู้ช่วยศาสตราจารย์ ดร.นิพัทธ์ จงสวัสดิ์ ผู้ช่วยศาสตราจารย์ ดร.วีรยุทธ เจริญเรืองกิจ และอาจารย์ ดร.ชาญ รัตนะพิสิฐ ผู้เชี่ยวชาญที่กรุณาสละเวลาพิจารณาและให้ข้อเสนอแนะในการปรับปรุงเครื่องที่ใช้ในการวิจัย และขอขอบพระคุณผู้ใช้สื่อสังคมออนไลน์ เพื่อนๆ น้องๆ ทุกท่านที่ให้ความร่วมมือในการให้ข้อมูลที่ประโยชน์ต่อการวิจัยครั้งนี้

ขอขอบพระคุณคณาจารย์และกรรมการบริหารหลักสูตรศิลปศาสตรมหาบัณฑิต สาขาสารสนเทศศึกษา มหาวิทยาลัยศรีนครินทรวิโรฒ ทุกท่านที่ได้กรุณาประสิทธิ์ ประสาทวิชาความรู้ต่างๆ ที่เป็นประโยชน์อย่างยิ่งในการทำวิจัยครั้งนี้

ขอขอบพระคุณพี่ๆ เพื่อนๆ สาขาสารสนเทศศึกษาทุกท่าน รวมถึงบุคคลอีกหลายท่านที่ไม่ได้กล่าวนามไว้ ณ ที่นี้ได้ให้ความช่วยเหลือและคอยเป็นกำลังใจให้กับผู้วิจัยมาโดยตลอด

คุณค่าและประโยชน์อันพึงมีจากสารนิพนธ์ฉบับนี้ ขอมอบแด่ครอบครัว และคณาจารย์ผู้มีพระคุณทุกท่าน

คณัญญา อิ่มใจ

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญรูปภาพ

หน้า

บทที่ 1
บทนำ

ภูมิหลัง

ประเทศไทยเปลี่ยนผ่านสู่การเป็นดิจิทัลเต็มรูปแบบ หรือเรียกว่า Hyber-connented อุปกรณ์อิเล็กทรอนิกส์เป็นสิ่งสำคัญของการใช้ชีวิตในสังคม เพื่อทำกิจกรรมที่เชื่อมต่อสู่โลกออนไลน์ตลอดระยะเวลา 24 ชั่วโมง/วัน และ 7 วัน/สัปดาห์ ในขณะที่โรคโควิด-19 ทำให้วิถีชีวิตดิจิทัลเป็นความปรกติใหม่ที่เกิดขึ้นในสังคมโลก แม้โควิด-19 ได้เปลี่ยนจากการเป็นโรคระบาดมาเป็นโรคประจำถิ่นซึ่งจะคงอยู่ไปตลอด ผู้คนก็ยังคงคุ้นชินกับความสะดวกสบายในการทำกิจกรรมผ่านช่องทางออนไลน์ ซึ่งประกอบไปด้วยการทำงาน เรียน ประชุม ติดต่อสื่อสาร และทำธุรกรรมต่าง ๆ ผ่านระบบดิจิทัล จากการสำรวจสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ในปี พ.ศ. 2565 พบว่า โดยเฉลี่ยแล้วคนส่วนใหญ่มีการใช้งานผ่านระบบอินเทอร์เน็ตวันละ 7 ชั่วโมง 4 นาที ซึ่งกลุ่มคนในเจเนอเรชั่นที่ใช้อินเทอร์เน็ตมากที่สุด คือ เจเนอเรชั่น Z (ช่วงอายุ 18-26 ปี) อยู่ที่ 8 ชั่วโมง 55 นาทีต่อวัน (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2565) ส่วนหนึ่งสะท้อนมาจากการปรับตัวของสังคมจากโรคระบาดที่เคยเกิดขึ้น ในปี พ.ศ. 2562 ซึ่งทุกภาคส่วนมีมาตรการในการปิดสถานศึกษาเพื่อเว้นระยะห่างทางสังคม ทำให้การเรียนการสอนถูกปรับเปลี่ยนรูปแบบมาใช้ระบบออนไลน์เป็นหลัก และการทำงานแบบ work from home เพื่อลดการแพร่เชื้อ ทำให้วิถีชีวิตแบบออนไลน์กลายเป็นความปรกติในชีวิตของผู้คนในสังคม แม้ในปัจจุบันสังคมจะกลับสู่ภาวะปกติ แต่การใช้ชีวิตวิถีใหม่ (New normal) ผู้คนจำนวนมากยังคงทำธุรกรรมบนระบบอินเทอร์เน็ตและใช้เทคโนโลยีดิจิทัล ข้อมูลเกือบทุกอย่างจึงถูกเก็บไว้ในรูปแบบอิเล็กทรอนิกส์บนระบบออนไลน์ ทำให้มีความเสี่ยงในการรั่วไหลของข้อมูลที่อาจจะเกิดขึ้นจากการโจมตีผ่านระบบดิจิทัล ซึ่งการโจมตีโดยอาชญากรบนระบบดิจิทัลที่มีแนวโน้มของอันตรายและความรุนแรงที่เพิ่มมากขึ้นเรื่อย ๆ (Monteith และคนอื่น ๆ, 2021) การก่อกวนทางไซเบอร์ถูกพัฒนาหรือปรับเปลี่ยนรูปแบบตามช่องโหว่จากความก้าวหน้าทางเทคโนโลยี เพื่อมุ่งหมายในการเจาะเข้าถึงข้อมูลที่เป็นของผู้อื่น ทำลายอุปกรณ์คอมพิวเตอร์ รบกวนการใช้งานหรือการทำงานของอุปกรณ์อิเล็กทรอนิกส์ และสินทรัพย์ทางการเงินในรูปแบบออนไลน์ อาทิ Bitcoin ซึ่งเป็นสกุลเงินดิจิทัล หรือเรียกว่า Cryptocurrency ที่พัฒนาบนเทคโนโลยีบล็อกเชน

ภัยคุกคามที่เกิดขึ้นบนระบบไซเบอร์เป็นอาชญากรรมทางดิจิทัลที่เกิดขึ้นจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบ ผ่านการใช้เครือข่ายและอุปกรณ์อิเล็กทรอนิกส์หรือมาทางซอฟต์แวร์ที่ไม่พึงประสงค์ ที่มุ่งหมายทำอันตรายและก่อให้เกิดความเสียหายอันส่งผลกระทบต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลบนอุปกรณ์เคลื่อนที่ทุกชนิด ซึ่งรวมถึงข้อมูลส่วนบุคคลหรือข้อมูลอื่น ๆ ที่เกี่ยวข้อง อาทิ ข้อมูลจากการทำธุรกรรมทางการเงิน (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2562a) ภัยคุกคามบนระบบไซเบอร์เกิดขึ้นจากการใช้เครื่องมือและวิธีการทางดิจิทัลเพื่อก่อกวนหรือเจาะเข้าข้อมูลหรือระบบที่ไม่ได้รับอนุญาต อาจทำให้ระบบหรืออุปกรณ์อิเล็กทรอนิกส์เสียหาย เป็นการสร้างความเสียหายต่อบุคคลหรือองค์กร การโจมตีผ่านระบบดิจิทัลเป็นภัยคุกคามที่เป็นความเสี่ยงต่อความปลอดภัยของข้อมูลส่วนบุคคล เนื่องจากปริมาณและความหลากหลายของการใช้ข้อมูลบนโลกไซเบอร์เพิ่มขึ้นอย่างต่อเนื่องและมีรูปแบบกิจกรรมหลากหลายมิติมากขึ้น เช่น การซื้อของ ความบันเทิง การประชุม การพบแพทย์ และการจัดเก็บข้อมูลต่างๆ บน Cloud service เป็นต้น ด้วยเหตุผลดังกล่าว การตระหนักรู้ต่อการป้องกันตนเองจากการก่อกวนและคุกคามทางไซเบอร์จึงเป็นเรื่องสำคัญในการใช้ระบบดิจิทัล (Zwilling และคนอื่น ๆ, 2020) การกระทำของอาชญากรทางไซเบอร์ที่เข้ามาเจาะระบบหรือขโมยข้อมูลจากช่องโหว่ทางพฤติกรรมที่สุ่มเสี่ยงจากความไม่ระวังในการใช้เครื่องมือหรืออุปกรณ์ผ่านระบบออนไลน์จนกลายเป็นความความเคยชิน ตัวอย่างเช่น การแชร์รหัสผ่านส่วนบุคคล การดาวน์โหลดเนื้อหาที่ผิดกฎหมาย และการละเลยการอัปเดตซอฟต์แวร์ที่แนะนำ เป็นต้น โดยการโจมตีออนไลน์ในรูปแบบต่างๆ ได้แก่ การโจมตีด้วยเว็บไซต์อันตราย (Malicious websites) มัลแวร์ (Malware) แรนซัมแวร์ (Ransomware) สแปมเมล (Spam email) การโจมตีด้วยข้อความบนสื่อสังคมออนไลน์ (Malicious social media messaging) การโจมตีออนไลน์ในรูปแบบฟิชชิ่ง (Phishing) ซึ่งเป็นการหลอกลวงให้หลงเชื่อผ่านทางหน้าเว็บไซต์หรืออีเมล โดยที่มุ่งหวังโจรกรรมข้อมูลความลับส่วนบุคคลเพื่อนำไปใช้ในทางผิดกฎหมาย เช่น เพศ อายุ สัญชาติ ศาสนา รหัสบัตรประชาชน ตำแหน่งที่อยู่อาศัย แม้กระทั่งข้อมูลทางการเงิน เช่น ข้อมูลบัตรเครดิต รหัสบัตร ATM เพื่อสวมรอยทำธุรกรรมในทางมิชอบโดยปราศจากความยินยอมจากเจ้าของข้อมูล ภัยคุกคามดังกล่าวนำไปสู่มาตรการจากภาครัฐ โดยประกาศใช้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อควบคุม ป้องกัน และรับมืออันตรายในภัยคุกคามที่อาจเกิดขึ้น (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2562a) รวมทั้งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อกำหนดหลักเกณฑ์และมาตรการในการรคุ้มครองการล่วงละเมิดสิทธิของข้อมูลส่วนบุคคล (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2562b) ให้สอดคล้องกับแผนยุทธศาสตร์ชาติ

พ.ศ. 2561-2580 ภายใต้ประเด็นยุทธศาสตร์ด้านความมั่นคง การป้องกัน การติดตาม เฝ้าระวัง และแก้ไขปัญหาอาชญากรรมทางดิจิทัล ที่มีผลกระทบต่อความมั่นคงปลอดภัยในระบบเศรษฐกิจ สังคม และอธิปไตยทางไซเบอร์ (สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, 2561)

กลุ่มวัย “เจเนอเรชั่นแซด” คือ กลุ่มคนในช่วงวัยที่เริ่มก้าวเข้าสู่ความเป็นผู้ใหญ่ โดยมีเทคโนโลยีเข้ามาเป็นส่วนหนึ่งของชีวิตประจำวัน มีความสามารถในการเรียนรู้และปรับตัวเข้ากับการแพร่กระจายทางเทคโนโลยีได้อย่างรวดเร็ว ไม่เฉพาะการใช้อุปกรณ์คอมพิวเตอร์หรือมือถือเท่านั้น แต่รวมทั้งความสามารถในการเข้าถึงข้อมูล การค้นคืน การผลิตสื่อดิจิทัล การเข้าสังคมออนไลน์ การสร้างสรรค์เนื้อหา และการแบ่งปันความรู้บนโลกดิจิทัล (Salubi, Ondari-Okemwa, และ Nekhwevha, 2018; Sayavaranont และ Wannapiroon, 2017) อย่างไรก็ตาม จากสถิติผู้เคยตกเป็นเหยื่อทางอาชญากรรมทางไซเบอร์พบว่า วัยรุ่นหนุ่มสาวในช่วงอายุ 18-26 ปี ซึ่งเป็นกลุ่มผู้ใช้ระบบดิจิทัลอย่างคล่องแคล่ว เป็นกลุ่มคนที่มีโอกาสเกิดความเสี่ยงจากภัยคุกคามทางไซเบอร์มากกว่ากลุ่มคนในช่วงวัยอื่น ๆ (McGuire และ Dowling, 2013) เมื่อเปรียบเทียบกลุ่มเจเนอเรชั่นวายและแซดในการใช้สื่อสังคมออนไลน์แล้วพบว่า เจเนอเรชั่นวายมีความระมัดระวังในการทบทวนนโยบายความเป็นส่วนตัว การบำรุงรักษาระบบ หมั่นอัปเดตระบบปฏิบัติการและโปรแกรมเพื่อป้องกันอุปกรณ์จากการโจมตีอย่างสม่ำเสมอ และคอยสังเกตประสิทธิภาพของเครื่องคอมพิวเตอร์ มากกว่ากลุ่มเจเนอเรชั่นแซด ซึ่งเป็นผลมาจากความรู้และประสบการณ์ที่มากกว่าทำให้รับรู้ถึงความเสี่ยงในการใช้ระบบ อีกทั้งการให้ข้อมูลและการทำธุรกรรมทางดิจิทัลซึ่งอาจจะมีการภัยจากคุกคามทางไซเบอร์ (Debb, Schaffer, และ Colson, 2020) ซึ่งหากผู้ใช้ตกเป็นเหยื่อจากภัยคุยคามทางไซเบอร์นั้น อาจส่งผลกระทบต่อตนเองอทั้งด้านร่างกาย ด้านการเงิน และด้านจิตใจ ดังนั้นหากผู้ใช้ผ่านประสบการณ์ที่เคยถูกคุกคามทางไซเบอร์ รวมทั้งเคยผ่านการอบรมเรียนรู้เกี่ยวกับการภัยคุกคามทางไซเบอร์ ย่อยส่งผลในเชิงบวกต่อการตระหนักรู้ถึงอันตรายที่อาจเข้ามาผ่านช่องทางไซเบอร์

นอกจากนี้ ประเด็นเรื่องการป้องกันตนเองจากภัยคุกคามที่มาบนระบบไซเบอร์กำลังเป็นที่สนใจในหมู่นักวิจัย อาทิ สุธารเทพ รุณเรศ (2561) พบว่าลักษณะทางด้านประชากรศาสตร์ ได้แก่ อายุ ระดับการศึกษา และรายได้ มีอิทธิพลต่อความตระหนักต่อภัยคุกคามบนระบบออนไลน์ของผู้ใช้อินเทอร์เน็ต แต่เพศและประสบการณ์ไม่มีผลต่อความตระหนักต่ออันตรายที่อาจได้รับจากภัยคุกคามทางอินเทอร์เน็ต การก่อกวนทางไซเบอร์มีการพัฒนาและปรับเปลี่ยนรูปแบบในการโจมตีเพื่อหาช่องโหว่ที่มีความแตกต่างและเปลี่ยนไปจากรูปแบบเดิม ทำให้ผู้ใช้อินเทอร์เน็ต

ไม่ทันได้ระวังการโจมตีที่มาในวิธีการใหม่ ไม่สามารถเฝ้าระวัง และป้องกันได้เหมือนเดิม จึงทำให้ได้รับอันตรายหรือความเสียหายที่ไม่อาจคาดคิด ความรู้มีผลต่อความตระหนักในภัยคุกคามที่มาจากการก่อกวนบนระบบไซเบอร์ เพื่อการดูแลและป้องกันตนเองจากภัยคุกคามนั้นผู้ที่มีความรู้ย่อมตระหนักและคาดคะเนถึงความเสียหายและอันตรายที่อาจเกิดขึ้น ติดตามข้อมูลข่าวสารการโจมตีรูปแบบใหม่ ตั้งค่าความเป็นส่วนตัวเพื่อปกป้องข้อมูลส่วนบุคคลไม่ให้รั่วไหลสู่สาธารณะ หมั่นดูแลความปลอดภัยบนอุปกรณ์ส่วนตัว และดาวน์โหลดเฉพาะโปรแกรมที่น่าเชื่อถือ นอกจากนี้ อิสริยา ปาริชาติกานนท์ และ อัจศรา ประเสริฐสิน (2560) พบว่า ในกระบวนการดูแลและป้องกันตนเองจากภัยคุกคามทางอินเทอร์ของนักศึกษาได้รับอิทธิพลทางอ้อมจากตัวแปรทุนทางจิตวิทยาผ่านองค์ความรู้เกี่ยวกับความรุนแรงของภัยคุกคามทางออนไลน์ รวมทั้งได้รับอิทธิพลทางอ้อมจากตัวแปรการสนับสนุนทางสังคมที่ก่อให้เกิดมารยาทบนระบบออนไลน์ ซึ่งหมายความว่าหากนักศึกษาเป็นผู้ที่มีคุณลักษณะของทุนทางจิตวิทยาสูง และได้รับการสนับสนุนที่มาจากสังคมย่อมส่งผลให้เป็นผู้ที่มีพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางอินเทอร์เน็ตมากขึ้น อย่างไรก็ตาม งานวิจัยนี้ไม่พบว่าการรับรู้ความรุนแรงของภัยคุกคามทางอินเทอร์เน็ตและมารยาทบนอินเทอร์เน็ตมีอิทธิพลทางตรงต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามที่เข้ามาผ่านช่องทางออนไลน์

ภัยคุกคามบนระบบไซเบอร์อาจเกิดขึ้นได้กับทุกบุคคลโดยเฉพาะกลุ่มเจเนอเรชั่นแซด ซึ่งเป็นวัยที่เติบโตมาพร้อมกับความก้าวหน้าทางเทคโนโลยี คุ้นชินกันการใช้ชีวิตและทำกิจกรรมบนโลกดิจิทัล ทำให้มีของความเสี่ยงทางไซเบอร์สูงกว่ากลุ่มเจเนอเรชั่นอื่น จากตัวอย่างการวิจัยที่ได้กล่าวมาแล้ว จะเห็นได้ว่าภัยคุกคามบนระบบไซเบอร์โดยเฉพาะกับกลุ่มเจเนอเรชั่นแซดเป็นเรื่องที่กำลังได้รับความสนใจเนื่องจากเป็นปัญหาสังคมที่ยังไม่มีทางหมดไป แต่งานวิจัยของกลุ่มเจเนเรชั่นแซดในประเทศมุ่งเน้นเพียงการศึกษาเชิงจิตวิทยาด้านการกลั่นแกล้งทางไซเบอร์ ดังนั้นผู้วิจัยจึงมีความสนใจในกลุ่มเจเนเรชั่นนี้ เพื่อศึกษาว่า เพศ ความรู้ และประสบการณ์ มีผลต่อพฤติกรรมป้องกันตนเองจากภัยที่เกิดจากการคุกคามทางไซเบอร์มากน้อยเพียงใด โดยผลจากการวิจัยครั้งนี้จะทำให้ทราบเกี่ยวกับปัจจัยที่ส่งผลต่อพฤติกรรมดังกล่าว ซึ่งมีประโยชน์ต่อการนำไปใช้เป็นแนวทางในการส่งเสริม สนับสนุนและสร้างความตระหนักรู้ที่มีต่อภัยคุกคามทางไซเบอร์ระดับบุคคลต่อไป

ความมุ่งหมายของงานวิจัย

ในการวิจัยครั้งนี้ผู้วิจัยได้ตั้งความมุ่งหมายไว้ดังนี้

1. เพื่อศึกษาพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

2. เพื่อศึกษาอิทธิพลของเพศ ความรู้ และประสบการณ์ที่มีผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

ความสำคัญของการวิจัย

ภัยคุกคามบนระบบไซเบอร์เป็นภัยร้ายที่มีความเสี่ยงสูงและอยู่ใกล้ตัว โดยมาพร้อมกับกิจกรรมออนไลน์ต่าง ๆ ที่เกิดขึ้นในโลกดิจิทัล ซึ่งเกิดจากความไม่ระมัดระวังตนเองหรือผลจากข้อผิดพลาดของมนุษย์ อาทิ การใช้อุปกรณ์สำนักงานหรือสถาบันการศึกษาที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต ซึ่งสามารถส่งผลกระทบอันรุนแรงต่อข้อมูลสำคัญ รวมถึงการถูกดำเนินคดีทางกฎหมายได้ ดังนั้นจากการศึกษาวิจัยครั้งนี้ทำให้ทราบถึงปัจจัยที่มีอิทธิพลการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ในบริบทของสังคมไทยในยุคของกลุ่มคนเจเนอเรชั่นแซด แล้วนำไปส่งเสริมสนับสนุนและสร้างความตระหนักรู้ ประสบการณ์ ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เช่น จัดอบรมภายในหน่วยงาน สถาบันการศึกษา การจำลองสถานการณ์การเกิดภัยคุกคามทางไซเบอร์ การจัดประชุม (conference) และการรณรงค์ภัยคุกคามทางไซเบอร์อย่างจริงจังต่อไป

ขอบเขตของการวิจัย

ประชากรที่ใช้ในการวิจัย

ชาวไทยที่มีอายุอยู่ในกลุ่มเจเนอเรชั่นแซด ซึ่งมีอายุระหว่าง 18-24 ปี จำนวน 5,885,215 ราย (สำนักงานสถิติแห่งชาติ, 2563) เนื่องจากช่วงเวลาที่ทำการศึกษา มีข้อมูลสถิติประชากรศาสตร์ของประเทศไทยล่าสุดถึงปี พ.ศ. 2563

กลุ่มตัวอย่างที่ใช้ในการวิจัย

กลุ่มตัวอย่าง คำนวณโดยใช้โปรแกรม G*Power กำหนดขนาดตัวอย่างในการวิจัยเชิงปริมาณ สร้างจากสูตรของ (Cohen, 1977) คำนวณอัตราส่วนของกลุ่มตัวอย่างตามจำนวนประชากรและปัดเศษทศนิยมขึ้น (นงลักษณ์ วิรัชชัย, 2555) ได้ขนาดตัวอย่างขั้นต่ำ 129 คน จึงกำหนดกลุ่มตัวอย่างจำนวน 130 คน ใช้วิธีสุ่มตัวอย่างแบบไม่อาศัยความน่าจะเป็น เก็บข้อมูลแบบสะดวก (Convenience Samplings) โดยคัดเลือกเฉพาะผู้ที่อยู่ในกลุ่มเจนเนอเรชั่นแซด หรือเกิดระหว่างปี พ.ศ. 2540 – 2546

ตัวแปรที่ใช้ในการศึกษา

1. ตัวแปรอิสระ แบ่งเป็นดังนี้

1.1 เพศ (Gender)

1.2. ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ (Knowledge)

1.3. ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ (Experience)

2. ตัวแปรตาม ได้แก่ พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ (Behavior)

นิยามคำศัพท์เฉพาะ

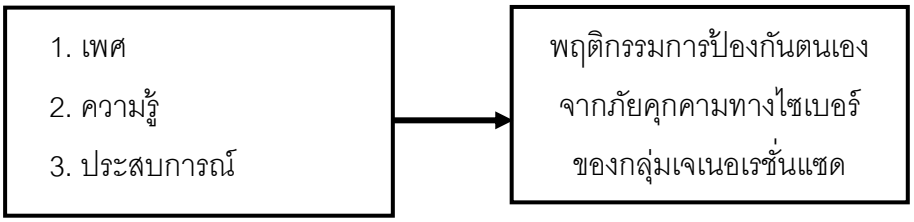
ความรู้ หมายถึง การที่บุคคลในเจนเนอเรชั่นแซดมีความรู้ด้านความปลอดภัยในการป้องกันตนเองภัยคุกคามทางไซเบอร์ ซึ่งครอบคลุมถึงอันตรายจากภัยคุกคามที่เข้ามาบนระบบไซเบอร์ รวมถึงผลที่ตามมาจากการถูกโจมตีและก่อกวนทางไซเบอร์ การตรวจสอบและเข้าถึงเว็บไซต์ที่มีความปลอดภัย วิธีการป้องกันช่องโหว่ทางไซเบอร์โดยการดูแลและสังเกตการทำงานของอุปกรณ์อิเล็กทรอนิกส์ และวิธีการตั้งค่าระดับความปลอดภัยของข้อมูลส่วนบุคคลบนโลกไซเบอร์ทุกประเภท

ภัยคุกคามบนไซเบอร์ หมายถึง ภัยคุกคามความปลอดภัยที่เกิดจากผู้คุกคามทางไซเบอร์ประสงค์ต่อข้อมูลส่วนบุคคล (Data theft) สินทรัพย์ เป็นต้น ซึ่งเป็นภัยคุกคามที่ส่งผลกระทบที่มาจากการกระทำผิดพลาดของเจ้าของข้อมูล การทำลายอุปกรณ์อิเล็กทรอนิกส์ การรบกวนการเข้าถึงข้อมูลหรือการทำงานของอุปกรณ์อิเล็กทรอนิกส์ สินทรัพย์ทางออนไลน์ การปลอมแปลงข้อมูลส่วนบุคคล เป็นต้น

ภัยคุกคามข้อมูลส่วนบุคคล หมายถึง ภัยคุกคามบัญชีผู้ใช้บนโลกไซเบอร์ (Online account) ที่จำเป็นต้องใช้ข้อมูลส่วนบุคคลในการระบุตัวตนไปถึงเจ้าของข้อมูลได้ เช่น ชื่อ-นามสกุล แชร์ตำแหน่งที่ตั้ง เลขประจำตัวประชาชน เบอร์โทรศัพท์ เลขบัญชีธนาคาร สินทรัพย์ออนไลน์ รหัสผ่าน ประวัติการสืบค้น ข้อมูลบนโปรไฟล์สื่อสังคมออนไลน์ ประวัติทางการแพทย์ เป็นต้น ซึ่งทำให้เกิดช่องโหว่จนนำไปสู่การโจรกรรมข้อมูลส่วนบุคคลได้ง่าย เช่น มัลแวร์ แรนซัมแวร์ ฟิชชิง คริปโตแจ็คกิ้ง เป็นต้น

เจเนอเรชั่นแซด (Generation Z) หมายถึง กลุ่มอายุในช่วงที่สังคมความก้าวหน้าทางเครือข่ายอินเทอร์เน็ตและเทคโนโลยีที่ถูกพัฒนาอย่างต่อเนื่อง โดยเทคโนโลยีเข้ามามีบทบาทในชีวิตประจำวัน ส่งผลทำให้เกิดการละเลยการดูแลและป้องกันตนเองจากการคุกคามที่เข้ามาบนระบบไซเบอร์ โดยเป็นกลุ่มที่เกิดระหว่างปี พ.ศ. 2540 – 2546 (Fry และ Parker, 2018)

กรอบแนวคิดในงานวิจัย



ภาพประกอบ 1 กรอบแนวคิดการวิจัย

สมมุติฐานในการวิจัย

1. เพศมีอิทธิพลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

2. ความรู้มีอิทธิพลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

3. ประสบการณ์มีอิทธิพลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

บทที่ 2
ทบทวนวรรณกรรม

ผู้วิจัยได้ศึกษาวรรณกรรมที่เกี่ยวข้อง ดังนี้

1. เจเนอเรชั่น
2. ภัยคุกคามทางไซเบอร์
3. การรักษาความปลอดภัยทางไซเบอร์
4. กฎหมายที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์
5. งานวิจัยที่เกี่ยวข้อง

แนวคิดเกี่ยวกับเจเนอเรชั่น

ยุคปัจจุบันเปลี่ยนแปลงไปอย่างรวดเร็วและต่อเนื่องทั้งในด้านเศรษฐกิจสังคม เทคโนโลยี และการสื่อสาร การเปลี่ยนแปลงเหล่านี้ได้สร้างความแตกต่างทางพฤติกรรมระหว่างรุ่นและช่วงวัยของประชากร ซึ่งอาจเรียกว่า “Generation Gap” หมายถึงความแตกต่างทางวัยระหว่างกลุ่มคนที่เกิดในยุคเดียวกัน ซึ่งมีประสบการณ์และเหตุการณ์ทางประวัติศาสตร์ที่สอดคล้องกัน หนึ่งในปรากฏการณ์ที่เกี่ยวข้องกับ Generation Gap คือความเปลี่ยนแปลงของสภาพแวดล้อมทางเศรษฐกิจที่เกิดจากการดำเนินชีวิตท่ามกลางการเติบโตของอุตสาหกรรม การต่อสู้กับปัญหาสิ่งแวดล้อม การเปลี่ยนแปลงในการใช้เทคโนโลยีโดยเฉพาะอย่างยิ่งคนในรุ่นหลัง ๆ ที่อยู่ในสภาพที่แวดล้อมไปด้วยความเชื่อมโยงกับเทคโนโลยีมากขึ้น จึงส่งผลให้คนแต่ละกลุ่มเจนเนอเรชั่นเกิดแนวคิด ทัศนคติ ค่านิยม พฤติกรรม และความต้องการในการดำรงชีวิตที่แตกต่างกัน (Mannheim, 1952) ซึ่งสอดคล้องกับ Zemke (2001) ที่เสนอว่าเจเนอเรชั่นถูกกำหนดโดยลักษณะทางประชากรศาสตร์และประสบการณ์ที่ผ่านมาร่วมกัน ทำให้แต่ละเจเนอเรชั่นมีความแตกต่างกันในเรื่องของค่านิยม ความต้องการ กระบวนการทางความคิด และมุมมองในการทำงาน และ Glass (2007) กล่าวว่า เจเนอเรชั่น คือผู้ซึ่งผ่านประสบการณ์จากเหตุการณ์ในช่วงยุคสมัยใกล้เคียงกัน ซึ่งก่อให้เกิดลักษณะเฉพาะในทัศนคติและพฤติกรรมร่วมกันในกลุ่มคนรุ่นราวเดียวกัน อย่างไรก็ตามการแบ่งกลุ่มคนตามช่วงวัย (Generation) สามารถแบ่งได้เป็น 4 กลุ่ม ได้แก่ กลุ่มเบบี้บูมเมอร์ (Baby Boomers) ปี พ.ศ. เกิด 2489 - 2507 กลุ่มเจเนอเรชั่น X ปี พ.ศ. เกิด 2508 – 2523 กลุ่มเจเนอเรชั่น Y ปี พ.ศ. เกิด 2524 - 2539 กลุ่มเจเนอเรชั่น Z ปี พ.ศ. เกิด 2540 – 2555 และกลุ่มเจเนอเรชั่นอัลฟาตั้งแต่ ปี พ.ศ. 2556 เป็นต้นไป

เจเนอเนชั่นแซด

กลุ่มเจนเนอเรชันซี (Post millennial or Generation Z) กลุ่มผู้ที่มีปีเกิดระหว่างปี พ.ศ. 2540–2555 มีอายุระหว่าง 9-24 ปี (Fry และ Parker, 2018) ถูกอ้างถึงในชื่อ ไอ เจเนอเรชั่น (I-Generation) เน็ตเจเนอเรชั่น (Net Generation) อินเทอร์เน็ตเจเนอเรชั่น (Internet Generation) หรือ เจเนอเรชั่นเน็กซ์ (Generation Next) (Levickaite, 2010; Turner, 2015) เป็นกลุ่มอายุที่เกิดมาในช่วงที่สังคมเกิดวิวัฒนาการทางด้านเทคโนโลยีดิจิทัลอย่างฉับพลัน ซึ่งแตกต่างอย่างมากจากรุ่นอายุอื่นๆ โดยเติบโตพร้อมกับการวิวัฒนาการของเทคโนโลยี ทำให้มีความชำนาญในการเข้าถึงสารสนเทศต่างๆ ได้อย่างรวดเร็ว การเป็นกลุ่มคนที่เกิดในยุคดิจิทัลหรือที่เรียกว่า “digital native” (Howe และ Strauss, 2008) ทำให้กลุ่มคนเจเนอเรชั่นแซดคุ้นเคยกับเทคโนโลยีต่างๆ (Priporas, Stylos, และ Fotiadis, 2017) เช่น การเข้าถึงเครือข่ายระบบอินเทอร์เน็ต การใช้ไปรษณีย์อิเล็กทรอนิกส์ การติดต่อสื่อสารกับเพื่อนหรือคนในโลกไซเบอร์ได้อย่างไร้พรมแดนและเปิดกว้างผ่านอุปกรณ์ที่ทันสมัย (Smart device) การใช้สื่อสังคมที่มาในรูปแบบออนไลน์จึงไม่สามารถใช้ชีวิตโดยปราศจากเทคโนโลยีได้ (Smith-Trudean, 2016) ดังนั้น คนกลุ่มนี้มีความแตกต่างจากกลุ่มคนในเจเนอเรชั่นอื่น หรือมีลักษณะเฉพาะ (Characteristics) โดยเจเนอเรชั่นแซดมีพฤติกรรมที่ต้องการได้รับข้อมูล ข่าวสารต่างๆ อย่างรวดเร็ว การโพสต์ภาพ ข้อความ การแชร์ข้อมูลที่เป็นของตนเอง เช่น ที่อยู่ สถานที่ต่างๆ บนสื่อออนไลน์ให้กับผู้ติดตามอย่างต่อเนื่อง การใช้เวลาไปกับกิจกรรมออนไลน์เฉลี่ย 6-8 ชั่วโมงต่อวัน ซึ่งการเติบโตขึ้นมาในโลกที่มีเทคโนโลยีดิจิทัลเพียงปลายนิ้วสัมผัส สื่อสังคมออนไลน์ และอุปกรณ์อิเล็กทรอนิกส์ที่ทันสมัย อย่างไรก็ตาม สะท้อนได้ว่าทุกวันนี้คนรุ่นนี้จำนวนมาก มีพฤติกรรม “FOMO” (Fear Of Missing Out) คือ กลัวที่ตนเองจะไม่เท่าทันข่าวสารร้อนมาแรงที่เกิดขึ้นบนโลกใบนี้ อยากจะรู้ อยากจะแชร์ก่อนใคร และด้วยความเคลื่อนไหวของข้อมูลที่เป็นไปอย่างรวดเร็ว จึงทำให้การใช้อินเทอร์เน็ตและโซเชียลมีเดีย-เข้ามามีบทบาทและความจำเป็นสำหรับการเรียน การทำงาน การทำธุรกรรมทางการเงิน การใช้บริการโครงการของรัฐบาลต่างๆ ที่ต้องฝากข้อมูลส่วนตัวของผู้ใช้ หรือข้อมูลทางการเงินไว้บนโลกไซเบอร์ ส่งผลทำให้เกิดพฤติกรรมประมาทจนนำไปสู่ข้อผิดพลาด (Human error) ต่อการโพสต์ข้อความ แชร์ข้อมูลทางออนไลน์ มีการเชื่อมต่อข้อมูลความลับส่วนบุคคลเข้าสู่โลกไซเบอร์ ก่อให้เกิดความเสียหายทางการเงิน พฤติกรรมเสี่ยงของเปิดเผยเรื่องราวของตนเองผ่านสื่อสังคมออนไลน์ เช่น Twitter, Facebook, Instagram, Tiktok หรือ WhatsApp การละเลยความเป็นส่วนตัวทางออนไลน์ การขาดความรู้ความเข้าใจการป้องกันตนเองจากภัยคุกคามที่เข้ามาก่อกวนผ่านระบบออนไลน์ (Altuna, Martinez de Morentin, และ Arkaitz, 2020; Lesjak, Martinez de Morentin, Altuna, และ

Amenabar, 2017) โดยเมื่อเทียบกับกลุ่มเจเนอเรชั่นอื่นๆ พบว่าเจเนอเรชั่นเอ็กซ์และเบบี้บูมเมอร์มีความรู้และวิธีการป้องกันอันตรายทางไซเบอร์ที่ดีกว่าเจเนอเรชั่นแซด (Debb และคนอื่น ๆ, 2020)

แนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์

การแพร่กระจายของเทคโนโลยีส่งผลทางสังคมให้ผู้คนทั่วโลกเชื่อมต่อเครือข่ายอินเทอร์เน็ตผ่านอุปกรณ์เคลื่อนที่อยู่ตลอดเวลา รวมทั้งการเพิ่มขึ้นของกิจกรรมออนไลน์ที่เป็นเครื่องมือสำคัญในการดำเนินชีวิตในช่วงสถานการณ์ของโรคโควิด-19 การขับเคลื่อนของข้อมูลในรูปแบบดิจิทัล จึงเป็นเป้าหมายของการก่อกวนทางไซเบอร์ จากผู้คุกคาม (Threat actors) ในหลากหลายรูปแบบผ่านช่องโหว่ของความปลอดภัยบนระบบอิเล็กทรอกนิกส์ จากการปรับเปลี่ยนของผู้ใช้ในการทำธุรกรรมแทบทุกรูปแบบที่อยู่บนระบบออนไลน์ ทั้งการติดต่อสื่อสาร การทำงานระยะไกล การเรียน การทำธุรกิจ การซื้อขายสินค้า อีกทั้งธุรกรรมทางการเงิน และการรับบริการจากหน่วยงานรัฐซึ่งต้องใช้ข้อมูลส่วนบุคคล เป็นต้น (Hakak, Khan, Imran, Choo, และ Shoaib, 2020; Ma และ Mckinnon, 2021; Nam, 2019) การเกิดอาชญากรรมทางไซเบอร์แตกต่างจากอาชญากรรมทั่วไป โดยคำว่าอาชญากรรมเป็นความรุนแรง หรือ การกระทำความผิดทางกฎหมายอาญา มีเป้าหมายเพื่อทำร้ายทางร่างกาย จิตใจ หรือทรัพย์สิน แต่สำหรับอาชญากรรมทางไซเบอร์เป็นการกระทำที่ไม่ชอบด้วยกฎหมายจากการเข้าถึงหรือการคุกคามอุปกรณ์อิเล็กทรอนิกส์ เครือข่ายอินเทอร์เน็ต เครือข่าย VPN การละเมิดข้อมูลส่วนบุคคล สินทรัพย์โดยไม่ได้รับอนุญาต (Frank และ Odunayo, 2013; Pawlicka, Choras, Pawlicki, และ Kozik, 2021; Timmers, 2019) เนื่องจากปัจจัยความเสี่ยงที่ทำให้เกิดภัยคุกคามทางไซเบอร์ที่มาจากความผิดพลาดหรือความประมาทจากพฤติกรรมการใช้งานบนโลกไซเบอร์อย่างไม่ระมัดระวังโดยไม่ได้คำนึงผลกระทบอย่างร้ายแรงที่จะตามมาในภายหลัง (Gillam และ Foster, 2020; McCormac และคนอื่น ๆ, 2017) ดังนั้น ความเสี่ยงจากภัยคุกคามทางที่เข้ามาทางไซเบอร์จึงจำเป็นต้องได้รับความใส่ใจ (Dawson และ Thomson, 2018) การรับรู้ถึงรูปแบบและขั้นตอนของภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใหม่เป็นสิ่งสำคัญ (Rashid, Noor, และ Altmann, 2021) เพื่อทำให้เจ้าของข้อมูลส่วนบุคคลตระหนักถึงความเสี่ยงที่อาจจะตามมาและใช้ระบบอย่างระมัดระวังสามารถป้องกันข้อมูลของตนเองจากการถูกนำไปใช้ในทางมิชอบโดยอาชญากรทางไซเบอร์ (Ma และ Mckinnon, 2021)

รูปแบบการคุกคามทางไซเบอร์

ภัยคุกคามที่เกิดขึ้นผ่านระบบไซเบอร์มีวิวัฒนาการของรูปแบบการก่อกวนที่ซับซ้อนที่เพิ่มความรุนแรงมากขึ้น อีกทั้งวิถีชีวิตใหม่ของสังคมดิจิทัลเป็นอีกหนึ่งตัวเร่งสำคัญที่ทำให้พฤติกรรมการแสดงตัวตนหรือการเปิดเผยตัวตนสู่สาธารณะเพิ่มมากขึ้น การเปลี่ยนแปลงโครงสร้างพื้นฐานทางกายภาพเดิมให้อยู่ในรูปแบบดิจิทัลเข้ามาปรับเปลี่ยนวิธีการดำเนินชีวิตประจำวันอย่างไม่สามารถหลีกเลี่ยงได้ การเข้าถึงหรือการเชื่อมต่ออุปกรณ์และโครงข่ายต่าง ๆ ที่สามารถอำนวยความสะดวกต่อผู้ใช้งาน ผู้คุกคามใช้โอกาสจากวิถีชีวิตดิจิทัลหลังจากการแพร่ระบาดของเชื้อไวรัสครั้งนี้เป็นเครื่องมือสำหรับการกระทำการก่ออาชญากรรมทางไซเบอร์ในรูปแบบการแฮ็ก โจมตี หรือการหลอกลวง (European union agency for cybersecurity, 2021) ด้วยรูปแบบการคุกคามหลากหลาย ดังนี้

มัลแวร์ (Malware)

มัลแวร์ (Malware) เป็นตัวก่อกวนและทำความเสียหายให้กับระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต โดยมีลักษณะการทำงานและพฤติกรรมที่แตกต่างกันไป ตัวอย่างเช่น

1. ไวรัส (Virus) เป็นมัลแวร์ที่ซ่อนตัวมาพร้อมกับไฟล์โปรแกรมและสามารถขยายตัวไปสู่คอมพิวเตอร์ที่เชื่อมโยงกันเครื่องอื่น ๆ ได้โดยแนบตัวไปกับโปรแกรมหรือไฟล์ที่ส่งต่อกัน ซึ่งไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น

2. เวิร์ม (Worm) คือหน่วยย่อยลงมาจากไวรัสที่สามารถกระจายตัวไปสู่คอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ผ่านทางระบบเครือข่าย เช่น อีเมล หรือระบบแชร์ไฟล์

3. โทรจัน (Trojan) เป็นลักษณะของมัลแวร์ที่เป็นอันตรายและอุปสรรค์ต่อความปลอดภัยของระบบคอมพิวเตอร์โดยล่อลวงผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย แต่จะทำให้เกิดความเสียหายเมื่อผู้ใช้หลงเชื่อนำไปติดตั้งโดยที่ผู้ใช้ไม่รู้ตัวว่ามีโปรแกรมอื่นที่ไม่ปกติแฝงตัวติดมาด้วย

4. Backdoor หรือโปรแกรมหลังบ้าน เป็นช่องทางที่ผู้พัฒนาติดตั้งไว้เพื่อเป็นช่องโหว่ให้ผู้อื่นเข้าถึงอุปกรณ์ของผู้เสียหายโดยไม่รู้ตัว

5. Rootkit เป็นโปรแกรมที่ถูกออกแบบมาเพื่อซ่อนตัวอยู่ในคอมพิวเตอร์ ซึ่งเปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติมเพื่อควบคุมเครื่อง พร้อมได้สิทธิ์ของผู้ดูแลระบบ (Root)

6. สปายแวร์ (Spyware) เป็นโปรแกรมเข้ามาสอดแนมพฤติกรรมของผู้ใช้ โดยจะแอบบันทึกการใช้งานและอาจขโมยข้อมูลที่มีความสำคัญ เช่น เลขบัตรประจำตัว ชื่อผู้ใช้ระบบ รหัสผ่าน วันเดือนปีเกิด หรือเลขบัญชีที่ใช้การเงิน เป็นต้น พร้อมทั้งส่งข้อมูลที่แอบดักจับไปในเครื่องปลายทางที่ตั้งค่าไว้อีกด้วย

7. Ransomware เป็นโปรแกรมที่ทำการเข้ารหัสไฟล์ โดยไม่ให้ผู้ใช้งานเปิดไฟล์นั้นได้ ต่อมาก็จะส่งข้อความมาหาผู้ใช้เพื่อเรียกค่าไถ่แลกกับการถอดรหัส (Decrypt) เพื่อกู้ไฟล์ข้อมูลเหล่านั้นคืน ดังนั้น ผู้ใช้งานคอมพิวเตอร์ทุกคนควรทราบถึงลักษณะและวิธีการทำงานของมัลแวร์ในทุกรูปแบบ เพื่อรักษาความปลอดภัยในข้อมูลดิจิทัลของตนเองไม่ให้ถูกคุกคามทางไซเบอร์ได้

การป้องกันปัญหาที่เกิดขึ้นจากมัลแวร์นั้น ควรอัปเดตระบบปฏิบัติการและโปรแกรมคอมพิวเตอร์อย่างสม่ำเสมอ เพราะมัลแวร์บางประเภทใช้ช่องโหว่ในซอฟต์แวร์เพื่อเข้าสู่ระบบ ติดตั้งและอัปเดตโปรแกรมป้องกันไวรัสที่เชื่อถือได้บนเครื่องดิจิทัลตั้งโต๊ะหรืออุปกรณ์เคลื่อนที่ และควรตรวจสอบไฟล์ที่ดาวน์โหลดหรือได้รับผ่านทางอีเมลก่อนที่จะเปิดใช้งาน รวมทั้งการเลือกใช้รหัสผ่านที่ซับซ้อน ซึ่งแข็งแกร่งและมีความยากต่อการเดา

แรนซัมแวร์ (Ransomware)

สภาพสังคมจากการใช้ชีวิตของผู้คนบนระบบดิจิทัลในวิถีชีวิตใหม่ทำให้การโจมตีด้วยแรนซัมแวร์ (Ransomware) จากปี 2019 มาจนถึงปี 2021 มีปริมาณการโจมตีสูงขึ้นเรื่อย ๆ รวมถึงการที่คนทำงานจะต้องทำงานจากระยะไกล หรือ Work from home ก็ยิ่งทำให้มีความเสี่ยงจากการถูกก่อกวนและโจมตีทางไซเบอร์ด้วยหลากหลายปัจจัย เช่น คนทำงานไม่ได้มีโอกาสอยู่ใกล้กับแผนก IT Security ไปจนถึงการวางมาตรฐานความปลอดภัยที่ไม่ดีพอ และการต้องใช้อินเทอร์เน็ตสำหรับการทำงานตลอดเวลาก็ส่งผลเพิ่มโอกาสการเกิดแรนซัมแวร์ (Ransomware)(วิวัฒน์ รุ่งแสนสุขสกุล, 2564, 8 กันยายน) ซึ่งแรนซัมแวร์เป็นซอฟต์แวร์ที่มีความอันตรายมาก เพราะสามารถเข้าถึงและเข้ารหัสไฟล์ของผู้ใช้คอมพิวเตอร์ได้โดยไม่ได้รับอนุญาต และจะขอค่าไถ่ในการคืนข้อมูลกลับมาให้ผู้ใช้เพื่อหลีกเลี่ยงการสูญเสียข้อมูลทั้งหมด (สำนักบริหารเทคโนโลยีสารสนเทศ, 2563) ช่องทางการแพร่กระจายของแรนซัมแวร์ (Ransomware) ส่วนใหญ่จะแฝงมาในรูปแบบเอกสารแนบทางไปรษณีย์อิเล็กทรอนิกส์ (Email) โดยผู้ส่งก็มักจะเป็นผู้ให้บริการที่เรารู้จักกันดี เช่น สถานบันทางการเงิน สถานการศึกษา หรือหน่วยงานต่าง ๆ ที่น่าเชื่อถือ และจะใช้หัวข้อหรือประโยคขึ้นต้นที่ดูน่าเชื่อถืออย่าง “Dear Valued Customer”, “Undelivered Mail Returned to Sender”, “Invitation to connect on LinkedIn.” เป็นต้น ประเภทของไฟล์แนบที่เห็นก็จะเป็น “.doc” หรือ “.xls” ผู้ใช้อาจจะคิดว่าเป็นไฟล์เอกสารธรรมดา แต่เมื่อตรวจสอบชื่อไฟล์เต็ม ๆ ก็จะเห็นนามสกุล .exe ซ่อนอยู่ ทำให้เข้าใจผิดว่าเป็นไฟล์ปกติที่ไม่น่าอันตราย นอกจากนี้ แรนซัมแวร์ยังอาจแฝงตัวมาในรูปแบบของ Malvertising ซึ่งมารูปแบบของการโฆษณา ไม่ว่าจะเป็นโฆษณาที่แอบแฝงเข้ามากับซอฟต์แวร์หรือหน้าจอหลักเว็บไซต์ต่าง ๆ เชื่อมโยงไปยังเว็บไซต์อันตรายและอาศัยช่องโหว่ของซอฟต์แวร์ โดยผู้ใช้อาจจะกลายเป็นเหยื่อ

ได้โดยไม่ได้ตั้งใจเพียงหลงเข้าหน้าเว็บที่มีผู้ไม่หวังดีควบคุม ตัวอย่างเช่น การเข้าไปดาวน์โหลดโค้ด (Code) ที่เป็นอันตรายผ่านทางโฆษณา แบนเนอร์ใน Flash โดย Ransomware มุ่งผลประโยชน์จากข้อผิดพลาดหรือช่องโหว่ด้านความปลอดภัยอื่น ๆ ในบราวเซอร์โปรแกรมประยุกต์ หรือระบบปฏิบัติการ ซึ่งช่องโหว่ที่พบมากที่สุดของแรนซัมแวร์มาจากโปรแกรม Flash (สำนักบริหารเทคโนโลยีสารสนเทศ, 2563)

ฟิชชิง (Phishing)

คำว่า “Phishing” เป็นคำที่มีความสัมพันธ์กับคำว่า “Fishing” ที่เป็นการตกปลา ที่มีการใช้เหยื่อล่อ เช่น การติดเหยื่อที่ปลายเบ็ดเพื่อให้ปลามากัดเบ็ด ซึ่ง “Phishing” เป็นกระบวนการทำงานที่คล้ายคลึงกัน ผู้คุกคามจะสร้างเหตุการณ์หรือสร้างข้อความที่ดูเหมือนมีแหล่งที่มาที่เชื่อถือได้เพื่อให้ผู้ใช้งานดิจิทัลตกใจเมื่อได้รับข้อความและต้องการแก้ไขปัญหา เช่น การแจ้งเตือนเกี่ยวกับบัญชีถูกโจรกรรม แล้วผู้คุกคามก็จะร้องขอข้อมูลส่วนตัวหรือข้อมูลบัญชีอื่น ๆ จากผู้ใช้งาน หรืออาจจะส่งลิงค์ที่เสียหายเพื่อให้ผู้เข้างานเข้าไปยังเว็บไซต์ปลอมแล้วกรอกข้อมูลส่วนตัว (มหาวิทยาลัยเชียงใหม่, 2564) โดยเป็นเทคนิคการหลอกลวงโดยใช้ไปรษณีย์อิเล็กทรอนิกส์ (Email) หรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหาย เช่น ปลอมไปรษณีย์อิเล็กทรอนิกส์ (Email) ว่าอีเมลฉบับนั้นถูกส่งออกมาจากธนาคารที่ผู้เสียหายใช้บริการอยู่ ซึ่งเนื้อความในไปรษณีย์อิเล็กทรอนิกส์ (Email) แจ้งว่า ขณะนี้ธนาคารมีการปรับเปลี่ยนระบบรักษาความมั่นคงปลอดภัยของข้อมูลลูกค้า และธนาคารต้องการให้ลูกค้าเข้าไปยืนยันความถูกต้องของข้อมูลส่วนบุคคลผ่านทางลิงค์ที่แนบมาในไปรษณีย์อิเล็กทรอนิกส์ (Email) เป็นต้น เมื่อผู้เสียหายคลิกที่ลิงค์ดังกล่าว พบกับหน้าเว็บไซต์ปลอมของธนาคารซึ่งผู้โจมตีได้เตรียมไว้ เมื่อผู้เสียหายเข้าไปล็อกอินผู้โจมตีก็จะได้ข้อมูลชื่อผู้ใช้และรหัสผ่านของผู้เสียหายไปในทันที ในหลาย ๆ ครั้งการหลอกลวงแบบ Phishing จะอาศัยเหตุการณ์สำคัญที่เกิดในช่วงเวลานั้น ๆ เพื่อเพิ่มโอกาสของการหลอกลวงได้สำเร็จ เช่น อาศัยช่วงเวลาที่มีภัยธรรมชาติหรือโรคระบาด โดยปลอมเป็นไปรษณีย์อิเล็กทรอนิกส์ (Email) หรือเว็บไซต์จากธนาคาร มูลนิธิ ศูนย์บริการโรคติดต่อ เป็นต้น ในปัจจุบันผู้ใช้ต้องระมัดระวังกับการฝังโทรจันในหน้าเว็บไซต์ปลอมที่สามารถขโมยข้อมูลส่วนบุคคลได้ โทรจันที่ทำหน้าที่เป็น Key-logger เป็นตัวอย่างหนึ่งที่สามารถติดตามและบันทึกการกดคีย์บอร์ดที่ผู้เสียหายพิมพ์ได้อย่างลับ ซึ่งข้อมูลที่พิมพ์จะถูกส่งต่อยังผู้คุกคาม ผู้เสียหายอาจหลงกลหรือคลิกลิงค์เข้าสู่หน้าเว็บไซต์ปลอมเพื่อเปิดทางเข้าใช้งาน ในกรณี

นี้โทรจันจะถูกฝังไปพร้อมกับหน้าเว็บไซต์ปลอมโดยอัตโนมัติ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2563)

การปลอมแปลงหน้าเว็บไซต์ (Phishing web)

ผู้ใช้ระบบต้องระมัดระวังกับการปลอมแปลงหน้าเว็บไซต์ที่เรียกว่า “Phishing web” ซึ่งเป็นการลอกเลียนแบบหน้าเว็บไซต์จริงเพื่อหลอกผู้ใช้งานให้กรอกข้อมูลส่วนตัว เช่น ชื่อผู้ใช้และรหัสเข้าโปรแกรม ผู้ใช้งานที่ไม่ระมัดระวังอาจจะตกอยู่ในอันตรายจากการกรอกข้อมูลที่ถูกต้องในหน้าเว็บไซต์ปลอมและส่งข้อมูลดังกว่างให้ผู้ไม่ประสงค์ดีโดยที่ไม่รู้ตัว การป้องกันการเป็นเหยื่อของการปลอมแปลงหน้าเว็บไซต์เพื่อการหลอกลวงเป็นสิ่งสำคัญในปัจจุบัน ผู้ใช้งานควรระมัดระวังและปฏิบัติตามแนวทางด้านความปลอดภัย เช่น อย่าคลิกลิงค์ในอีเมลหรือข้อความที่ไม่น่าเชื่อถือ ตรวจสอบ URL ของเว็บไซต์ที่เข้าชมเพื่อให้แน่ใจว่าเป็นเว็บไซต์ที่ถูกต้องและปลอดภัย อย่ากรอกข้อมูลส่วนตัวบนเว็บไซต์ที่ไม่น่าเชื่อถือ และใช้เครื่องมือและโปรแกรมป้องกันการปลอมแปลงหน้าเว็บไซต์เพื่อเพิ่มระดับความปลอดภัยของการใช้งานอินเทอร์เน็ต

คริปโตแจ็คกิ้ง (Crytojacking)

คริปโตเคอร์เรนซี (cryptocurrency) ได้รับการยอมรับว่าเป็นสินทรัพย์ดิจิทัลประเภทหนึ่งที่ใช้ในระบบการเงิน โดยกำลังได้รับความนิยมสำหรับเป็นสื่อกลางในการแลกเปลี่ยนมูลค่าที่จะมาทดแทนการใช้เงินสดหรือแม้แต่เงินอิเล็กทรอนิกส์ (e-money) (ธนาคารแห่งประเทศไทย, 2563) คำว่า คริปโตเคอร์เรนซี (Cryptocurrency) คือ สินทรัพย์ดิจิทัลประเภทหนึ่งที่ต้องอาศัยการเข้ารหัส โดยคำว่า "Crypto" หมายถึง การเข้ารหัส ส่วนคำว่า "Currency" หมายถึง สกุลเงิน คริปโตเคอร์เรนซีเป็นสกุลเงินดิจิทัลที่ถูกสร้างขึ้นด้วยเทคโนโลยีบล็อกเชน (Blockchain) และมีลักษณะเฉพาะที่ไม่สามารถถูกปลอมแปลงได้ การใช้งานคริปโตเคอร์เรนซีเกี่ยวข้องกับการทำธุรกรรมทางการเงินและการซื้อขายแบบออนไลน์โดยไม่ต้องผ่านบัญชีธนาคารหรือตัวกลางทางการเงินอื่น ๆ ซึ่งทำให้มีความสะดวกรวดเร็วและค่าธรรมเนียมที่ต่ำกว่าการทำธุรกรรมทางการเงินแบบธรรมดา สกุลเงินคริปโตที่รู้จักกันดีที่สุด คือ "Bitcoin" (บิตคอยน์) ซึ่งเป็นเงินดิจิทัลสกุลแรกที่มีบทบาทสำคัญในการเปลี่ยนแปลงลักษณะการดำเนินธุรกรรมต่าง ๆ (ไลฟ์สไตล์, 2564) โดยการพัฒนาทางเทคโนโลยีด้านการแลกเปลี่ยนทางการเงินเป็นช่องทางเจาะลึกในเรื่องของความปลอดภัยทางไซเบอร์ ซึ่งเป็นภัยคุกคามในรูปแบบของ "คริปโตแจ็คกิ้ง" (Cryptojacking)

คริปโตแจ็คกิ้ง (Crytojacking) เป็นภัยคุกคามไซเบอร์รูปแบบใหม่ที่ก่อให้เกิดการฝังโค้ดโปรแกรมไคลเอนต์สคริปต์ เช่น JavaScript ลงในเว็บเบราว์เซอร์ของผู้ใช้ วิธีการฝังโค้ดนั้นสามารถทำ

ได้โดยการเจาะระบบเพื่อเข้าถึงเครื่องเซิร์ฟเวอร์ แล้วนำโค้ดโปรแกรมสกุลเงินคริปโตมาฝังในโค้ดโปรแกรมของเว็บไซต์โดยตรง หรือใช้เขียนโค้ดที่ใช้เรียกใช้โปรแกรมสกุลเงินคริปโตแล้วฝังลงในไลบรารีที่เปิดให้ใช้งานฟรี โดยโค้ดเหล่านี้มักถูกเผยแพร่บนอินเทอร์เน็ตหรือโลกออนไลน์ เช่น Git ซึ่งเป็นเว็บเซิร์ฟเวอร์ที่ให้บริการในการแบ่งปันโค้ดโปรแกรม อย่างไรก็ตามเว็บเซิร์ฟเวอร์หลายแห่งมักมีระบบป้องกันที่มีประสิทธิภาพ จึงทำให้เป็นเรื่องยากต่อมิจฉาชีพที่จะเจาะผ่านระบบได้ ดังนั้นบางครั้งมัลแวร์ที่ติดตั้งบนเว็บไซต์อาจมาจากผู้พัฒนาเว็บหรือโปรแกรมเมอร์ที่มีประสบการณ์ไม่เพียงพอ และมักเขียนโค้ดโปรแกรมเว็บโดยนำโค้ดที่เผยแพร่บนอินเทอร์เน็ตมาใช้โดยไม่ตรวจสอบอย่างละเอียด มัลแวร์ประเภท Cryptojacking เป็นภัยคุกคามที่เจาะเข้าสู่ระบบเครือข่ายคอมพิวเตอร์หรือโทรศัพท์มือถือของผู้ใช้ และใช้ทรัพยากรของอุปกรณ์เหล่านั้นในการขุดเงินคริปโต (Cryptocurrency) ขึ้นมาให้กับผู้โจมตี มัลแวร์นี้มีลักษณะการทำงานที่ทำให้อุปกรณ์ของผู้ใช้งานทำงานช้าลงและเกิดอาการค้าง ผู้โจมตีได้พัฒนาวิธีการใหม่เพื่อลดการตรวจจับ โดยใช้ซีพียูน้อยลงและควบคุมจำนวนเทรดที่มีอยู่ ทำให้ผู้ใช้งานไม่ค่อยรู้สึกถึงการที่อุปกรณ์ของตนถูกทำงานในพื้นหลังโดยไม่ได้ตั้งใจ ผลกระทบที่ผู้ใช้งานต้องเผชิญหน้าคือการทำงานของอุปกรณ์จะช้าลงเนื่องจากถูกดูดกินทรัพยากร บางครั้งอาจเกิดอาการค้างได้ ผู้ใช้งานสามารถสังเกตเห็นได้จากปัจจัยต่าง ๆ เช่น การเข้าสู่เว็บไซต์ที่ติดมัลแวร์แล้วเครื่องเริ่มแสดงอาการหน่วงในการตอบสนอง พัดลมในเครื่องคอมพิวเตอร์หรือโทรศัพท์มือถือเริ่มทำงานอย่างต่อเนื่อง หรือแบตเตอรี่ลดลงอย่างรวดเร็ว วิธีตรวจสอบและป้องกัน Cryptojacking นั้น สามารถใช้ Task Manager เพื่อดูว่าเว็บใดที่มีการเรียกใช้ทรัพยากรของเครื่องสูงผิดปกติ แล้วปิดเว็บไซต์นั้น หรือยกเลิกการใช้ JavaScript บนเว็บเบราเซอร์ นอกจากนี้ ยังสามารถใช้ Plug-in บนเบราเซอร์ เช่น Nocoin เพื่อป้องกันสคริปต์ที่ทำ Cryptojacking ได้อีกด้วย (ชัยพร เขมะภาตะพันธ์, 2564)

แนวคิดเกี่ยวกับการรักษาปลอดภัยทางไซเบอร์

ช่วงยุคสมัยที่เทคโนโลยีเจริญก้าวหน้าอย่างรวดเร็ว การป้องกันอันตรายที่อาจเกิดขึ้นจากการก่อกวนทางไซเบอร์เป็นสิ่งสำคัญที่ไม่ควรมองข้าม เนื่องจากอินเทอร์เน็ตเป็นช่องทางการสื่อสารที่เข้าถึงได้ง่ายและเป็นที่นิยมใช้งานมากที่สุดในปัจจุบัน ผ่านการเชื่อมต่อและการแลกเปลี่ยนข้อมูลในรูปแบบดิจิทัล ทำให้ผู้ใช้ทุกคนต้องระวังและเรียนรู้เทคนิคการป้องกันไวรัส มัลแวร์ และภัยคุกคามอื่น ๆ ที่อาจจะเข้ามาเข้าถึงข้อมูลส่วนตัวได้ เพื่อความปลอดภัยบนโลกไซเบอร์ที่มีประสิทธิภาพ ผู้ให้บริการจำเป็นต้องมีนโยบาย Cyber Security ที่ครอบคลุมความปลอดภัยของเครือข่ายหรือเน็ตเวิร์ค (Network security) กระบวนการปกป้องเครือข่าให้ปลอดภัยจากผู้บุกรุก การดูแลรักษาปลอดภัยของโปรแกรมประยุกต์ (Application security) ซึ่งต้องมีการ

ทดสอบช่องโหว่และอัพเดทอย่างต่อเนื่องเพื่อให้แน่ใจว่าโปรแกรมเหล่านี้ปลอดภัยจากการถูกโจมตีโดยบุคคลที่สาม การรักษาความปลอดภัยข้อมูล (Information security) ที่อยู่ภายในเครือข่าย ซึ่งเป็นข้อมูลของบริษัทและลูกค้าที่ควรมีการจัดการความปลอดภัยที่มากขึ้น เข้าถึงยากขึ้น รวมทั้งความปลอดภัยของระบบคลาวด์ (Cloud security) ซึ่งมีไฟล์ข้อมูลอยู่ปริมาณมหาศาลในสภาพแวดล้อมแบบดิจิทัล จึงถือเป็นความท้าทายในการปกป้องข้อมูลให้คงอยู่และรอดพ้นจากการถูกโจรกรรมไปใช้ในทางมิชอบ ดังนั้น การจัดการความปลอดภัยเพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์จึงเป็นกิจกรรมที่สำคัญในสังคมดิจิทัล (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2562a)

แนวทางการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ในระดับบุคคล

การรักษาความปลอดภัยทางไซเบอร์และการปกป้องข้อมูลส่วนบุคคล รวมทั้งสินทรัพย์ดิจิทัลเป็นสิ่งสำคัญเพื่อไม่ตกเป็นเหยื่อของอาชญากรรมทางไซเบอร์ (Ready Campaign, 2021) โดยมีแนวทางดังนี้

1. อัปเดตซอฟต์แวร์และระบบปฏิบัติการ
2. ใช้ซอฟต์แวร์ป้องกันไวรัส
3. ใช้รหัสผ่านที่คาดเดายาก
4. อย่าเปิดไฟล์แนบอีเมลจากผู้ส่งที่ไม่รู้จัก
5. อย่าคลิกลิงก์ในอีเมลจากผู้ส่งที่ไม่รู้จักหรือเว็บไซต์ที่ไม่คุ้นเคย
6. สำรองข้อมูลอยู่เสมอ
7. หลีกเลี่ยงการใช้เครือข่าย WiFi ที่ไม่ปลอดภัยจะทำให้คุณเสี่ยงต่อการถูกโจมตี

แนวทางปฏิบัติเมื่อถูกคุกคามทางไซเบอร์ (During cyber attack) (Ready Campaign, 2021) ดังนี้

1. ตรวจสอบการทำธุรกรรมทางการเงินที่ไม่สามารถระบุได้ ตรวจสอบรายงานการใช้งานบัตรเครดิตสำหรับบัญชีใหม่หรือสินเชื่อ

2. ระวังการถูกชักชวนหรือล่อลวงให้กรอกข้อมูลสำคัญบนเว็บไซต์ อีเมลและสื่อสังคมออนไลน์

3. หากสังเกตพบกิจกรรมแปลก ๆ ให้เปลี่ยนรหัสผ่านบัญชีทั้งหมดทันที และปิดการใช้อุปกรณ์ทั้งหมด และติดต่อผู้เชี่ยวชาญสแกนหาไวรัสและลบสิ่งที่เป็นอันตรายออก

4. แจ้งให้หน่วยงานที่เกี่ยวกับตนเองทราบถึงการโดนคุกคามทางไซเบอร์

5. การสแกนอุปกรณ์คอมพิวเตอร์ เพื่อตรวจสอบให้แน่ใจว่าระบบและอุปกรณ์ไม่ติดไวรัสหรือมีลักษณะการทำงานของอุปกรณ์ช้าลงหรือไม่มีประสิทธิภาพ

6. ยกเลิกการเชื่อมต่ออุปกรณ์ทั้งหมดจากบัญชีผู้ใช้ เครือข่ายอินเทอร์เน็ตและดำเนินการกู้คืนระบบทั้งหมด

แนวทางรายงานหลังจากการถูกคุกคามทางไซเบอร์ (After cyber attack) (Ready Campaign, 2021) ดังนี้

1. แจ้งให้หน่วยงานของรัฐ และท้องถิ่นทราบว่าตกเป็นเหยื่อของการโจมตีทางอินเทอร์เน็ต

2. ติดต่อธนาคาร บริษัทบัตรเครดิต และสถาบันทางการเงินอื่นๆ ที่มีบัญชีซึ่งอาจต้องระงับบัญชีที่ถูกโจมตี ระงับบัญชีเครดิตหรือค่าใช้จ่ายที่ไม่ได้รับอนุญาต และแจ้งว่าอาจมีมิจฉาชีพนำข้อมูลส่วนบุคคลไปใช้

3. แจ้งความกับตำรวจท้องที่ เพื่อจัดทำบันทึกเหตุการณ์อย่างเป็นทางการ

กฎหมายที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์

ในยุคปัจจุบันที่เทคโนโลยีก้าวล้ำไปอย่างต่อเนื่อง ทำให้เกิดการพัฒนาซอฟต์แวร์และโปรแกรมประยุกต์ในรูปแบบใหม่ ๆ เพื่ออำนวยความสะดวกให้ผู้ใช้งานสามารถเข้าถึงข้อมูลได้อย่างสะดวก รวดเร็ว ประหยัดเวลาและค่าใช้จ่ายทั้งในระดับบุคคลและระดับองค์กร จึงทำให้องค์กรกำกับดูแลที่เกี่ยวข้องในประเทศได้กำหนดนโยบาย กฎหมาย ระเบียบ และ ข้อบังคับเพื่อประโยชน์ต่อชาวไซเบอร์ให้สามารถใช้ชีวิตบนโลกไซเบอร์ได้ปลอดภัยและสามารถดำเนินคดีต่อผู้กระทำผิดได้ (Strzelecki, 2020) หากผู้ผลิตซอฟต์แวร์และโปรแกรมประยุกต์พัฒนาในเชิงสร้างสรรค์ก็จะเป็นประโยชน์ต่อความก้าวหน้าในการยกระดับเศรษฐกิจ แต่หากผู้ประสงค์ร้ายได้พัฒนาเครื่องมือที่สมัยเพื่อต้องการโจมตี สร้างความเสียหายต่อระบบ ขโมย ทำลาย หรือบิดเบือนข้อมูลเพื่อหลอกลวงผู้ใช้ในทางมิชอบ ก็จะสร้างความเสียหายต่อผู้ใช้ได้อย่างรุนแรง (อุดม ประตาทะยัง, 2560) ดังนั้น ทุกภาคส่วนควรร่วมมืออย่างเป็นระบบเพื่อจัดการป้องกันการโจมตีที่มาบนระบบไซเบอร์ซึ่งเกิดจากความประสงค์ร้าย โดยกฎหมายที่เกี่ยวกับภัยคุกคามในประเทศไทยประกอบด้วย (1) พ.ร.บ. ความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 (Cybersecurity Act) มีวัตถุประสงค์เพื่อกำกับดูแลความมั่นคงปลอดภัยของระบบสารสนเทศและการสื่อสารทางอินเทอร์เน็ต และ (2) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection

Act) ที่ได้ถูกกำหนดขึ้นเพื่อคุ้มครองข้อมูลของประชาชน ซึ่งทั้งสองพระราชบัญญัติมีความสำคัญอย่างมากในยุคปัจจุบันที่มีการแพร่กระจายทางดิจิทัลอย่างรวดเร็ว พ.ร.บ. ความมั่นคงปลอดภัยทางไซเบอร์ได้กำหนดหลักเกณฑ์และวิธีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและการสื่อสารผ่านช่องทางออนไลน์ รวมถึงกำหนดหน้าที่ของผู้ประกอบการในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและการสื่อสารทางอินเทอร์เน็ตในองค์กรของตน และการเข้ารหัสข้อมูล เพื่อป้องกันไม่ให้ผู้ไม่หวังดีสามารถเข้าถึงและนำข้อมูลนั้นไปใช้ในทางมิควร ในขณะที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล เป็นกฎหมายที่มีความสำคัญอย่างมากในการปกป้องสิทธิและความเป็นส่วนตัวของบุคคลในการใช้งานเทคโนโลยีและข้อมูลในยุคดิจิทัล โดยมีวัตถุประสงค์เพื่อคุ้มครองสิทธิของเจ้าของข้อมูล และจำกัดสิทธิในการนำข้อมูลของผู้อื่นไปใช้โดยต้องได้รับอนุญาตจากเจ้าของข้อมูล นอกจากนี้ กฎหมายทั้ง 2 ฉบับยังกำหนดการจัดตั้งหน่วยงานสำหรับการควบคุมและดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ไว้ด้วย

แม้ว่าจะมีการบังคับใช้กฎหมาย แต่อันตรายทางไซเบอร์ยังคงเกิดขึ้นอย่างต่อเนื่อง ในฐานะบุคคลผู้เป็นเจ้าของข้อมูล ก่อนจะให้ข้อมูลสำคัญ ควรมีการเก็บบันทึกเป็นหลักฐานไว้หรือขอสำเนาเอกสาร เมื่อใดพบว่าข้อมูลสำคัญส่วนบุคคลได้ถูกนำไปใช้ผิดวัตถุประสงค์ ก็จะได้ใช้เป็นหลักฐานในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ และมีสติรอบคอบในการให้ข้อมูลส่วนตัวแก่เว็บไซต์หรือโปรแกรมประยุกต์ที่มีการข้อความขึ้นเพื่อขอความยินยอมในการใช้หรือเข้าถึงข้อมูล ยกตัวอย่าง ปัจจุบันนี้ หลายโปรแกรมจะเชื่อมต่อระบบสมาชิกกับเฟซบุ๊ก มีการขอชื่ออีเมลและรายชื่อเพื่อนในเฟซบุ๊กของเรา หากเราเห็นว่าไม่จำเป็นที่ต้องให้ข้อมูลรายชื่อเพื่อน ก็สามารถคลิกเพื่อไม่ยินยอม และยินยอมให้เฉพาะอีเมลเพื่อการเข้าระบบของแอปพลิเคชันนั้น ๆ ได้ กล่าวอีกนัยหนึ่ง ตัวเจ้าของข้อมูลต้องทำหน้าที่ “คุ้มครองข้อมูลของตนเอง” ด้วย ไม่ด่วนยินยอมหรือให้ข้อมูลโดยที่ยังไม่ได้ศึกษารายละเอียดของขอบเขตการใช้ข้อมูลส่วนบุคคล

งานวิจัยที่เกี่ยวข้อง

งานวิจัยต่างประเทศ

อามีน, ทาฮินี, และแมดิชี (Ameen, Tarhini, Hussain Shah, และ Madichie, 2020) ศึกษาพฤติกรรมความปลอดภัยในการใช้อุปกรณ์สมาร์ทโฟน เก็บข้อมูลจากผู้ตอบแบบสอบถามที่เป็นพนักงานในบริษัทข้ามชาติ ทำงานอยู่ในประเทศสหรัฐอเมริกาและยูเออี กระจายกลุ่มตัวอย่างให้ครอบคลุมช่วงอายุ 18-35 ปี ตามวิจารณญาณของผู้วิจัย ได้รับข้อมูลตอบกลับจากประเทศยูเออีจำนวน 554 ราย และจากประเทศสหรัฐอเมริกาจำนวน 602 ราย ใช้โปรแกรม SPSS วิเคราะห์ผล โดยกำหนดค่า missing values ขอบบนและขอบล่างของข้อมูล ผลการวิจัยพบว่า เพศของพนักงานมีผล

ต่อพฤติกรรมความปลอดภัยในการใช้สมาร์ทโฟนอย่างมีนัยสำคัญ อย่างไรก็ตามความสามารถส่วนบุคคลของแต่ละเพศไม่ได้แตกต่างกันในประเทศยูเออีซึ่งทำให้พฤติกรรมการใช้งานอุปกรณ์สมาร์ทโฟนอย่างปลอดภัยไม่แตกต่างกัน แต่ความสามารถส่วนบุคคลของพนักงานเพศหญิงในประเทศสหรัฐอเมริกามีผลต่อพฤติกรรมความปลอดภัยในการใช้สมาร์ทโฟน การรับรู้ถึงผลร้ายมีผลต่อพฤติกรรมความปลอดภัยในการใช้สมาร์ทโฟนของพนักงานในประเทศยูเออี แต่ไม่มีผลอย่างมีนัยสำคัญของผู้ใช้ในประเทศสหรัฐเมริกา ต้นทุนไม่เป็นตัวแปรสำคัญในลงทุนความปลอดภัยในกับสมาร์ทโฟน ยกเว้นพนักงานเพศหญิงในประเทศสหรัฐอเมริกาที่กังวลถึงต้นทุนที่มากขึ้นที่จะทำให้สมาร์ทโฟนมีความปลอดภัย

กิลแลมและฟอสเตอร์ (Gillam และ Foster, 2020) ศึกษาเรื่องปัจจัยที่มีผลต่อความเสี่ยงทางพฤติกรรมทางไซเบอร์ของคนทำงานในสหรัฐอเมริกา โดยใช้เก็บข้อมูลจากกลุ่มคนอายุ 18 ปีขึ้นไปที่ทำงานอยู่ในประเทศสหรัฐอเมริกาและใช้อุปกรณ์ไอทีของนายจ้าง คำนวณกลุ่มตัวอย่างโดยกำหนดค่า α เท่ากับ 0.05 และค่า β เท่ากับ 0.20 เก็บข้อมูลจากแบบสอบถามออนไลน์โดยสุ่มตัวอย่างตามความสะดวก ได้ผู้ตอบแบบสอบถามจำนวน 294 คน คัดเลือกเฉพาะผู้ให้ข้อมูลที่ตอบแบบสอบถามได้อย่างสมบูรณ์และใช้อุปกรณ์ไอทีของนายจ้าง ได้กลุ่มตัวอย่างที่นำมาใช้ในการวิเคราะห์ จำนวน 184 คน ผลที่พบจากการวิเคราะห์สมการถดถอย คือ การรับรู้ด้านผลจากความเสียหาย ผลกระทบกับเงินทุน และความสามารถส่วนบุคคล มีผลต่อพฤติกรรมในการหลีกเลี่ยงความเสี่ยงจากภัยคุกคามทางไซเบอร์

โรดริเกส-ปรีเอโก, แวน เบเวิลม และ บริกส์ (Rodríguez-Priego, van Bavel, Vila, และ Briggs, 2020) ศึกษาปรากฏการณ์การวางกรอบ (Framing effects) ของพฤติกรรมความปลอดภัยบนระบบออนไลน์ ใช้การทดลองในห้องปฏิบัติการโดยมีกลุ่มตัวอย่างจำนวน 120 คน แบ่งเป็น 2 รอบ รอบละ 60 คน คัดเลือกผู้ร่วมวิจัยจากผู้ใช้อินเทอร์เน็ตในประเทศสเปนที่มีประสบการณ์ซื้อสินค้าหรือบริการผ่านระบบออนไลน์ช่วง 12 เดือนที่ผ่านมา สังเกตพฤติกรรมผู้ใช้ผ่านระบบออนไลน์ในการตัดสินใจ (1) เลือกการเชื่อมอินเทอร์เน็ตจาก 2 ทางเลือก ทางเลือกที่ปลอดภัยบังคับให้ผู้ใช้รอ 60 วินาทีในการป้อนรหัสผ่าน ผู้ใช้สามารถเปลี่ยนใจไปใช้การเชื่อมต่อที่ไม่ปลอดภัยในขณะที่รอได้ (2) การกำหนดรหัสผ่านที่ยากต่อการคาดเดา เป็นรหัสที่ยาว มีการผสมของตัวอักษร ตัวเลข และอักขระพิเศษ เพื่อวัดระดับความซับซ้อนของรหัสผ่าน (3) การให้ข้อมูลน้อยสุดในขณะที่ลงทะเบียนใช้ระบบ ระบบจะถามข้อมูลส่วนตัวเพื่อใช้ในการลงทะเบียน ข้อมูลที่จำเป็นต้องการจะมีเครื่องหมายดาว ข้อมูลที่ไม่จำเป็นจะใช้ในการส่งโฆษณาสินค้าจากผู้ค้า (4) การเลือกผู้ขายที่น่าเชื่อถือ ระบบจะแสดงรูปของผู้ขายจำนวน 4 ราย เพื่อให้ผู้ใช้เลือกสินค้า ซึ่งมีการเชื่อมต่อไปยังลิงค์ที่ไม่ปลอดภัย ถ้าผู้ใช้เลือกผู้ค้า

รายนั้นจะมีความเสี่ยงต่อการถูกโจมตี (5) การคลิกเพื่อออกจากระบบก่อนปิดหน้าเว็บ ผลการวิจัยพบว่า การใช้ข้อความที่ไม่อยู่ในกรอบ (loss-framed message) เป็นข้อความที่ทำให้ผู้ใช้กลัวต่อผลกระทบที่ร้ายแรง มีผลต่อพฤติกรรมความปลอดภัยของผู้ใช้งาน ความเชื่อส่งผลทางลบต่อพฤติกรรมความปลอดภัย ผู้ใช้ที่เชื่อในระบบของผู้ขายจะมีพฤติกรรมละเลยความปลอดภัย ในขณะที่ความรู้ส่งผลทางบวกต่อพฤติกรรมความปลอดภัยทางไซเบอร์

หลิว, หวัง, และเหลียง (Liu, Wang, และ Liang, 2020) ศึกษาแรงบันดาลใจที่มีต่อการปฏิบัติตามมาตรการการใช้ระบบอย่างปลอดภัยในหน่วยงาน เก็บข้อมูลจากกลุ่มตัวอย่างที่เป็นพนักงานภาครัฐในประเทศจีน จำนวน 235 คน มีตัวแปรควบคุมคือ อายุ เพศ ตำแหน่งงาน ระดับการศึกษา ประสบการณ์ทำงาน การใช้คอมพิวเตอร์ และการตระหนักรู้ ผลการวิจัยพบว่า ความสัมพันธ์ระหว่างหัวหน้าลูกน้องมีผลทางอ้อมต่อการปฏิบัติตามนโยบายความปลอดภัยทางไซเบอร์ขององค์กร ผ่านตัวแปรขั้นกลาง คือ ความมุ่งมั่นที่พนักงานมีต่อองค์กร ซึ่งความมุ่งมั่นที่พนักงานมีต่อองค์กรส่งผลทางบวกต่อการปฏิบัติตามนโยบายด้านความปลอดภัยทางดิจิทัล แม้ว่าต้นทุนของการปฏิบัติตามความปลอดภัยจะสูงก็ตาม

โดนัล และโอไซ-ไบรสัน (Donalds และ Osei-Bryson, 2020) ศึกษาพฤติกรรมด้านความปลอดภัยทางไซเบอร์ และสำรวจรูปแบบการตัดสินในการกระทำเพื่อป้องกันการโจมตีทางไซเบอร์ของแต่ละบุคคล เก็บข้อมูลจากแบบสอบถามออนไลน์ของกลุ่มตัวออย่างในประเทจาไมก้า ส่งข้อมูลในหลายชั้นเรียนในคณะบริหารธุรกิจทั้งระดับปริญญาตรีและบัณฑิตศึกษาลิงค์แบบสอบถามถูกส่งถึง 510 คน แต่ได้รับข้อมูลตอบกลับจำนวน 248 คน ร้อยละ 68 เป็นเพศหญิงร้อยละ 71 มีอายุระหว่าง 18-35 วิเคราะห์ด้วยสมการถดถอยเชิงเส้น ผลการวิจัยพบว่า รูปแบบการตัดสินใจของบุคคลมีผลต่อพฤติกรรมด้านความปลอดภัยทางไซเบอร์ โดยผู้ที่มีการตัดสินใจในสไตล์ที่โดดเด่นจะมีพฤติกรรมที่ตระหนักถึงความปลอดภัยบนระบบไซเบอร์ รวมถึงการตั้งรหัสผ่านที่ปลอดภัย

โควาเซวิค, ปุดนิก, และโทสโกวิค (Kovacevic, Putnik, และ Toskovic, 2020) ศึกษาปัจจัยที่มีความสัมพันธ์กับพฤติกรรมความปลอดภัยทางไซเบอร์ เก็บข้อมูลในชั้นเรียนจากนักศึกษาซึ่งคุ้นเคยกับเทคโนโลยีไอที กลุ่มตัวอย่างเป็นนักศึกษาชั้นปีที่ 1 ของมหาวิทยาลัยเบลเกรด ประเทศเซอร์เบีย จำนวน 147 คน ประกอบด้วยเพศชายร้อยละ 27 เพศหญิงร้อยละ 73 ตัวแปรอิสระแบบสอบถามประกอบด้วย เพศ การศึกษาก่อนหน้า การใช้ไอที ประสบการณ์การละเมิดความปลอดภัยบนระบบไซเบอร์ การรับรู้ด้านความปลอดภัย พฤติกรรมในการตั้งรหัสผ่าน พฤติกรรมการใช้โทรศัพท์มือถือ และความรู้ด้านความปลอดภัยทางไซเบอร์ ผลการวิจัยพบว่า ความรู้และประสบการณ์มีผลต่อการรับรู้ด้านความปลอดภัยทางไซเบอร์ ในขณะที่ปัจจัยด้านข้อมูลส่วนบุคคลมีผลต่อการรับรู้

ไม่มากนัก ความรู้เป็นปัจจัยที่มีอิทธิพลมากที่สุดต่อการตระหนักรู้ในความปลอดภัยทางไซเบอร์ แต่ความรู้ไม่มีความสัมพันธ์อย่างมีนัยสำคัญกับพฤติกรรมการตั้งรหัสผ่าน ผู้ตอบแบบสอบถามไม่มีใครที่สามารถตอบคำถามในวัดความรู้ด้านความปลอดภัยทางไซเบอร์ได้ถูกทุกข้อ สรุปได้ว่า แม้กลุ่มตัวอย่างจะเป็นวัยที่เติบโตมากับเทคโนโลยีดิจิทัล แต่พวกเขาก็รู้สึกไม่เชื่อมั่นในความปลอดภัยในสภาพแวดล้อมที่อยู่บนระบบไซเบอร์ พวกเขายังมีพฤติกรรมที่ไม่ปลอดภัยและมีความรู้ไม่เพียงพอต่อการป้องกับตนเองบนโลกไซเบอร์

เดบและคนอื่น ๆ (Debb และคนอื่น ๆ, 2020) เปรียบเทียบพฤติกรรมในการรักษาความปลอดภัยข้อมูลของเจนเนอเรชั่นวายและแซด เก็บตัวอย่างจากผู้ตอบแบบสอบถามจากคนแอฟริกันอเมริกันและคนผิวขาว ซึ่งคัดเลือกจากนักศึกษาในมหาวิทยาลัยรัฐ 2 แห่ง ในรัฐเวอร์จิเนีย สหรัฐอเมริกา มหาวิทยาลัยแห่งแรกเป็นมหาวิทยาลัยใหญ่ที่มีนักศึกษาจากหลากหลายวัฒนธรรม มหาวิทยาลัยอีกแห่งเป็นมหาวิทยาลัยขนาดเล็กกว่าแห่งแรกซึ่งเป็นที่นิยมของคนผิวสี การเก็บข้อมูลได้รับอนุมัติจากคณะกรรมการของมหาวิทยาลัยทั้ง 2 แห่ง ผู้ตอบแบบสอบถามต้องเป็นผู้ที่เกิดระหว่างปี ค.ศ.1977 ถึง ค.ศ.1999 ให้มั่นใจได้ว่าเป็นผู้อยู่ในเจนเนอเรชั่นวายและแซด ที่มีอายุอย่างน้อย 18 ปี กลุ่มตัวอย่างที่ใช้วิเคราะห์ข้อมูล จำนวน 593 คน มีอายุเฉลี่ย 22.06 ปี เป็นผู้เกิดในปี ค.ศ.1977 ถึง ค.ศ.1994 ซึ่งอยู่ในเจนเนอเรชั่นวาย จำนวน 209 คน อายุเฉลี่ย 27.48 ปี เป็นผู้เกิดปี ค.ศ. 1995 ถึง ค.ศ.1999 ซึ่งอยู่ในเจนเนอเรชั่นแซด จำนวน 384 คน อายุเฉลี่ย 19.52 ปี วิเคราะห์ผลด้วยโปรแกรม SPSS โดยใช้สถิติ T-test พบว่า นักศึกษาเจนเนอเรชั่นวายมีการปฏิบัติตนที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ดีกว่านักศึกษาเจนเนอเรชั่นแซท ได้แก่ การทบทวนนโยบายความเป็นส่วนตัวและความปลอดภัยของบัญชีผู้ใช้สื่อสังคมออนไลน์ อัพเดทโปรแกรมป้องกันไวรัสอยู่สม่ำเสมอ สังเกตอาการตอบสนองที่ผิดปกติของเครื่องคอมพิวเตอร์ และจัดการความปลอดภัยเมื่อเครื่องเตือนเกี่ยวกับมัลแวร์

นัม (Nam, 2019) ศึกษาช่องว่างระหว่างการรับรู้ถึงอันตรายจากการโจมตีผ่านระบบออนไลน์และการดูแลความปลอดภัยทางไซเบอร์ ใช้ชุดข้อมูลทุติยภูมิจากศูนย์วิจัย Pew ซึ่งเก็บข้อมูลในปี 2016 เก็บข้อมูลจากการสัมภาษณ์ผ่านโทรศัพท์ จำนวน 1,000 ราย แบ่งเป็นการสัมภาษณ์จากโทรศัพท์บ้านจำนวน 250 ราย และสัมภาษณ์ผ่านโทรศัพท์มือถือจำนวน 750 ราย ถามข้อคำถามเกี่ยวกับการรับรู้ถึงอันตรายจากการโจมตีทางไซเบอร์เมื่ออยู่ในสภาพแวดล้อมสาธารณะ ซึ่งถามถึงศักยภาพในการรับรู้และการเตรียมการป้องกันจากการก่อกวนที่มาทางไซเบอร์ วิเคราะห์ข้อมูลโดยใช้สมการถดถอยโลจิสติก พบว่า การรับรู้ถึงความเสี่ยงทางไซเบอร์เมื่ออยู่ในที่สาธารณะมีความสัมพันธ์ทางบวกกับการดูแลความปลอดภัย ประสบการณ์ที่ผ่านมามีผลต่อการรับรู้ถึงความเสี่ยงทางไซเบอร์

เมื่ออยู่ในที่สาธารณะ ในขณะที่ความมั่นใจต่อความปลอดภัยทางไซเบอร์ของภาครัฐ ความคิดเสรีนิยม และความไว้วางใจสังคม ส่งผลให้เชื่อมั่นจะดูแลเครือข่ายสาธารณะได้อย่างปลอดภัย กลุ่มที่เชื่อมั่นต่อภาครัฐในมาตรการทางไซเบอร์มีประสบการณ์ด้านลบจากการโจมตีทางไซเบอร์น้อยกว่ากลุ่มอื่น ๆ

ลีและคนอื่น ๆ (Li และคนอื่น ๆ, 2019) สำรวจตัวแปรที่มีผลกระทบกับพฤติกรรมการตระหนักรู้ของพนักงานด้านนโยบายความปลอดภัยทางไซเบอร์ สำรวจข้อมูลจากพนักงานจำนวน 579 คน ที่ทำงานกับบริษัทในประเทศสหรัฐอเมริกา ผู้ให้ข้อมูลทำงานอยู่ในอุตสาหกรรมหลายประเภท เป็นเพศชายร้อยละ 35 และหญิงร้อยละ 65 เมื่อถามถึงนโยบายความปลอดภัยบนระบบไซเบอร์ขององค์กรที่ร่วมงานด้วย ผู้ตอบแบบสอบถามร้อยละ 46.11 ตอบว่า มี ร้อยละ 14.68 ตอบว่า ไม่มี และร้อยละ 39.21 ไม่มีความรู้เกี่ยวกับนโยบายทางไซเบอร์ของบริษัท ผลการวิเคราะห์สมการเชิงโครงสร้างแสดงให้เห็นถึงอิทธิพลของสภาพแวดล้อมขององค์กร ได้แก่ พฤติกรรมจากเพื่อนร่วมงาน กิจกรรมที่กระตุ้น ประสบการณ์ด้านความปลอดภัยของข้อมูล ที่มีต่อแรงจูงใจของพนักงานในการป้องกันตนเองจากการรับรู้ต่อปัญหาและระดับความรุนแรงที่อาจเกิดขึ้น ซึ่งส่งผลต่อพฤติกรรมการใช้ระบบและป้องกันตนเองจากภัยคุกคามที่อาจเกิดขึ้นบนไซเบอร์

ยู, ลี, ฮี,วัง, และเจียว (Yu, Li, He, Wang, และ Jiao, 2020) สำรวจการตระหนักรู้เรื่องความเป็นส่วนตัวของข้อมูลที่มีอิทธิพลต่อการเปิดเผยข้อมูลของผู้ใช้อินเทอร์เน็ต รวบรวมข้อมูลจากงานวิจัยในฐานข้อมูลวารสารวิชาการ ตั้งแต่เดือนตุลาคม 2017 ถึงธันวาคม 2017 และตั้งแต่เดือนกุมภาพันธ์ 2019 ถึงมีนาคม 2019 โดยใช้คำสำคัญในการค้นหา ได้แก่ privacy concern, perceive privacy risks, privacy beliefs, self-disclosure, privacy paradox และคำที่เกี่ยวข้องอื่นๆ ได้ข้อมูลจากวารสาร 101 ฉบับ ที่มีจำนวนกลุ่มตัวอย่างรวม 42,256 ราย ผลการวิจัยพบว่าการรับรู้ด้านความเสี่ยงและความกังวลในข้อมูลส่วนตัวมีผลทางลบกับความตั้งใจในการเปิดเผยข้อมูล และมีผลทางลบกับพฤติกรรมในการเปิดเผยข้อมูล ในขณะที่ความตั้งใจในการเปิดเผยข้อมูลมีผลทางบวกต่อพฤติกรรมการเปิดเผยข้อมูลส่วนตัว

แอนวอร์และคนอื่น ๆ (Anwar และคนอื่น ๆ, 2017) ศึกษาความแตกต่างทางเพศที่มีผลต่อพฤติกรรมด้านความปลอดภัยบนไซเบอร์ของพนักงาน เก็บข้อมูลจากพนักงานหลายบริษัทเกี่ยวกับประสบการณ์และความเชื่อด้านคอมพิวเตอร์และความปลอดภัยของอินเทอร์เน็ต ได้รับข้อมูลตอบกลับจำนวน 579 คน จากภาคธุรกิจและมหาวิทยาลัย กลุ่มตัวอย่างจากมหาวิทยาลัยที่ไม่เคยมีประสบการณ์การทำงานภายนอกถูกเอาออกจากการวิเคราะห์ เหลือข้อมูลที่ใช้วิเคราะห์จำนวน 481 คน เพศหญิงร้อยละ 66 และเพศชายร้อยละ 34 เมื่อถูกถามถึงนโยบายด้านความปลอดภัยทางไซเบอร์ที่องค์กรบังคับให้พนักงานปฏิบัติ ร้อยละ 49 ตอบว่า มี ร้อยละ15 ตอบว่า ไม่มี และร้อยละ 36 ไม่มี

ความรู้เกี่ยวกับนโยบายทางไซเบอร์ขององค์กรที่ปฏิบัติงานด้วย ผลการวิจัยนำเสนอความแตกต่างของค่าเฉลี่ยของความสามารถส่วนบุคคลที่เกี่ยวกับการดูแลความปลอดภัยทางไซเบอร์ พบว่า เพศหญิงมีค่าเฉลี่ยต่ำกว่าเพศชาย อย่างไรก็ตาม เพศต่างกันมีประสบการณ์ด้านความปลอดภัยทางไซเบอร์และทักษะคอมพิวเตอร์แตกต่างกันด้วย

งานวิจัยในประเทศ

สุธารเทพ รุณเรศ (2561) ได้ศึกษาปัจจัยที่ส่งผลต่อการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต พบว่า ลักษณะทางประชากรศาสตร์ ได้แก่ อายุ ระดับการศึกษา และรายได้ส่วนบุคคล มีผลต่อความตระหนักภัยที่เกิดจากการคุกคามทางไซเบอร์ อย่างไรก็ตามเพศและประสบการณ์ในการเผชิญกับภัยคุกคามทางไซเบอร์ไม่มีผลต่อความตระหนักถึงภัยที่อาจเกิดขึ้น การโจมตีทางไซเบอร์มีการปรับเปลี่ยนรูปแบบการโจมตีเพื่อค้นหาช่องโหว่ที่แตกต่างจากเดิม นั่นหมายความว่าผู้เสียหาอาจไม่สามารถระวังการโจมตีรูปแบบใหม่ได้ทันเวลา และมีความยากที่จะเฝ้าระวังและป้องกันอย่างมีประสิทธิภาพเหมือนภัยในรูปแบบเดิม จึงทำให้ได้รับความเสียหายที่ไม่อาจคาดคิด ความรู้มีผลต่อการตระหนักต่อภัยคุกคามที่เกิดขึ้นบนไซเบอร์ ผู้ที่มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์สามารถคาดคะเนถึงอันตรายและความเสียหายที่อาจเกิดขึ้น ติดตามข้อมูลข่าวสารการโจมตีรูปแบบใหม่ ระมัดระวังการเปิดเผยข้อมูลผ่านพื้นที่สาธารณะ หมั่นดูแลความปลอดภัยบนอุปกรณ์ส่วนตัว และดาวน์โหลดเฉพาะโปรแกรมที่น่าเชื่อถือ

วารินทร์ เคียร่า, สุธี จันทรพันธุ์, และ Fung (2560a) ได้ศึกษาพฤติกรรมการระวังป้องกันภัยคุกคามบนสมาร์ทโฟน พบว่า สมาร์ทโฟนกลายเป็นสิ่งจำเป็นที่อำนวยความสะดวกให้กับชีวิตประจำวันอย่างที่ไม่เคยมีมาก่อน ทำให้ผู้คนสามารถเชื่อมต่อกับโลกภายนอกผ่านเครือข่ายอินเทอร์เน็ตได้เป็นการเสริมสร้างศักยภาพการทำงานและความบันเทิง อย่างไรก็ตาม ความก้าวหน้าทางด้านไซเบอร์จะมาควบคู่กับการก่อกวนเพื่อโจมตีทางอินเทอร์เน็ต ซึ่งรูปแบบการโจมตีในปัจจุบันไม่ได้เกิดขึ้นเฉพาะคอมพิวเตอร์ แต่ยังเกิดขึ้นกับสมาร์ทโฟนเช่นกัน การโจมตีอาจเป็นการปล่อยมัลแวร์ การโจรกรรมเพื่อเข้าถึงข้อมูล หรือการเรียกค่าไถ่จากข้อมูล ซึ่งจัดเป็นภัยคุกคามที่ร้ายแรงที่สร้างความเสียหายให้แก่ผู้ใช้อุปกรณ์สมาร์ทโฟนได้อย่างมาก การศึกษานี้ได้นำทฤษฎีแรงบันดาลใจในการป้องกันตนเอง (Protection motivation theory: PMT) ของ Roger R.W. ทฤษฎีศึกษาความหวาดกลัวของคนไข้ (Fear appeal) ที่เป็นการกระตุ้นให้เกิดพฤติกรรมในการระวังป้องกันตนเอง (Protection behavior) ประยุกต์ใช้ในการศึกษาพฤติกรรมการระวังป้องกันภัยคุกคามทางไซเบอร์ของ

ผู้ใช้สมาร์ทโฟน ผลที่ได้การวิจัยจะเป็นประโยชน์สำหรับการนำไปใช้ในการศึกษาความสัมพันธ์เชิงสาเหตุของแต่ละปัจจัยในตัวแบบด้วยวิธีการวิเคราะห์สถิติโดยใช้สมการเชิงโครงสร้าง

วารินทร์ เคียร่า, สุธี จันทรพันธุ์, และ Fung (2560b) ได้ศึกษาพฤติกรรมของคนไทยในการป้องกันสมาร์ทโฟนจากภัยคุกคามทางไซเบอร์ พบว่า (1) ระดับพฤติกรรมในการป้องกันภัยคุกคามทางโทรศัพท์มือถือของคนไทยอยู่ในระดับดี อย่างไรก็ตาม คนไทยได้รับอิทธิพลด้านข่าวสารจากสื่อหรือจากเพื่อนที่เกี่ยวกับภัยคุกคามทางโทรศัพท์ในระดับที่น้อย รวมถึงมีความสามารถในการประเมินภัยคุกคามในระดับที่น้อยเมื่อเทียบกับตัวแปรอื่นๆ (2) เพศหญิงมีระดับพฤติกรรมในการป้องกันทางโทรศัพท์มือถือน้อยกว่าผู้ชาย (3) ผู้ที่มีอายุระหว่าง 51-60 ปี เป็นกลุ่มที่มีระดับพฤติกรรมในการป้องกันภัยคุกคามทางโทรศัพท์น้อยกว่ากลุ่มอายุอื่น (4) ผู้ที่เคยติดไวรัสมีระดับพฤติกรรมในการป้องกันภัยคุกคามทางโทรศัพท์มือถือมากกว่าผู้ที่ไม่เคยติด (5) ผู้ที่นิยมใช้เครือข่ายไร้สายสาธารณะมีระดับพฤติกรรมในการป้องกันภัยคุกคามทางโทรศัพท์มือถือมากกว่าผู้ที่ไม่ใช้ และ (6) ผู้ใช้บริการโอนเงินผ่านโทรศัพท์มีระดับพฤติกรรมในการป้องกันภัยคุกคามทางโทรศัพท์มือถือมากกว่าผู้ที่เคยไม่ใช้

ศิริรตน์ ศรีสว่าง (2558) พบว่า พฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ได้รับอิทธิพลจากปัจจัยส่วนบุคคล ได้แก่ บุคลิกภาพแบบมีจิตสำนึก การรับคุณค่าของข้อมูล และประสบการณ์ในอดีต รวมทั้งปัจจัยด้านสภาพแวดล้อม ได้แก่ การคล้อยตามกลุ่มอ้างอิง ความรู้ด้านความปลอดภัยและค่าใช้จ่ายในการป้องกัน โดยส่งผ่านการรับรู้ต่อสภาวะคุกคาม การรับรู้ความสามารถในการจัดการกับภัยคุกคาม และแรงจูงในการป้องกัน ซึ่งพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้ที่มีทักษะด้านเทคโนโลยีมีค่าเท่ากับกลุ่มที่ไม่มีทักษะด้านเทคโนโลยี โดยพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้ทั้งสองกลุ่มเป็นผลมาจากการรับรู้ความสามารถในการจัดการภัยคุกคามมากที่สุด

สรุปงานวิจัยที่เกี่ยวข้อง

จากการสังเคราะห์วรรณกรรมที่เกี่ยวข้อง สรุปตัวแปรต้นที่เกี่ยวข้องกับพฤติกรรมการป้องกันตนเองให้พ้นจากภัยคุกคามที่เข้ามาทางไซเบอร์แสดงใน ตาราง 1 สรุปงานวิจัยที่เกี่ยวข้อง ซึ่งประกอบด้วยเพศ ความรู้ และประสบการณ์

ตาราง 1 สรุปงานวิจัยที่เกี่ยวข้องกับพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์

ผู้วิจัย	ตัวแปร		
	เพศ	ความรู้	ประสบการณ์/การรับรู้
Anwar และคนอื่น ๆ (2017)	✓		
Nam (2019)			✓
Li และคนอื่น ๆ (2019)			✓
Ameen และคนอื่น ๆ (2020)			✓
Ameen และคนอื่น ๆ (2020)	✓		✓
Gillam และ Foster (2020)			✓
Rodríguez-Priego และคนอื่น ๆ (2020)		✓	
Kovacevic และคนอื่น ๆ (2020)	✓	✓	
สุธารเทพ รุณเรศ (2561)		✓	

บทที่ 3
วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณ มีขั้นตอนการดำเนินการวิจัยดังนี้

1. การกำหนดประชากรและการสุ่มตัวอย่าง
2. การสร้างเครื่องมือที่ใช้ในการวิจัย
3. การเก็บรวบรวมข้อมูล
4. การจัดกระทำและการวิเคราะห์ข้อมูล
5. สรุปขั้นตอนการวิจัย

การกำหนดประชากรและการสุ่มตัวอย่าง

ประชากร

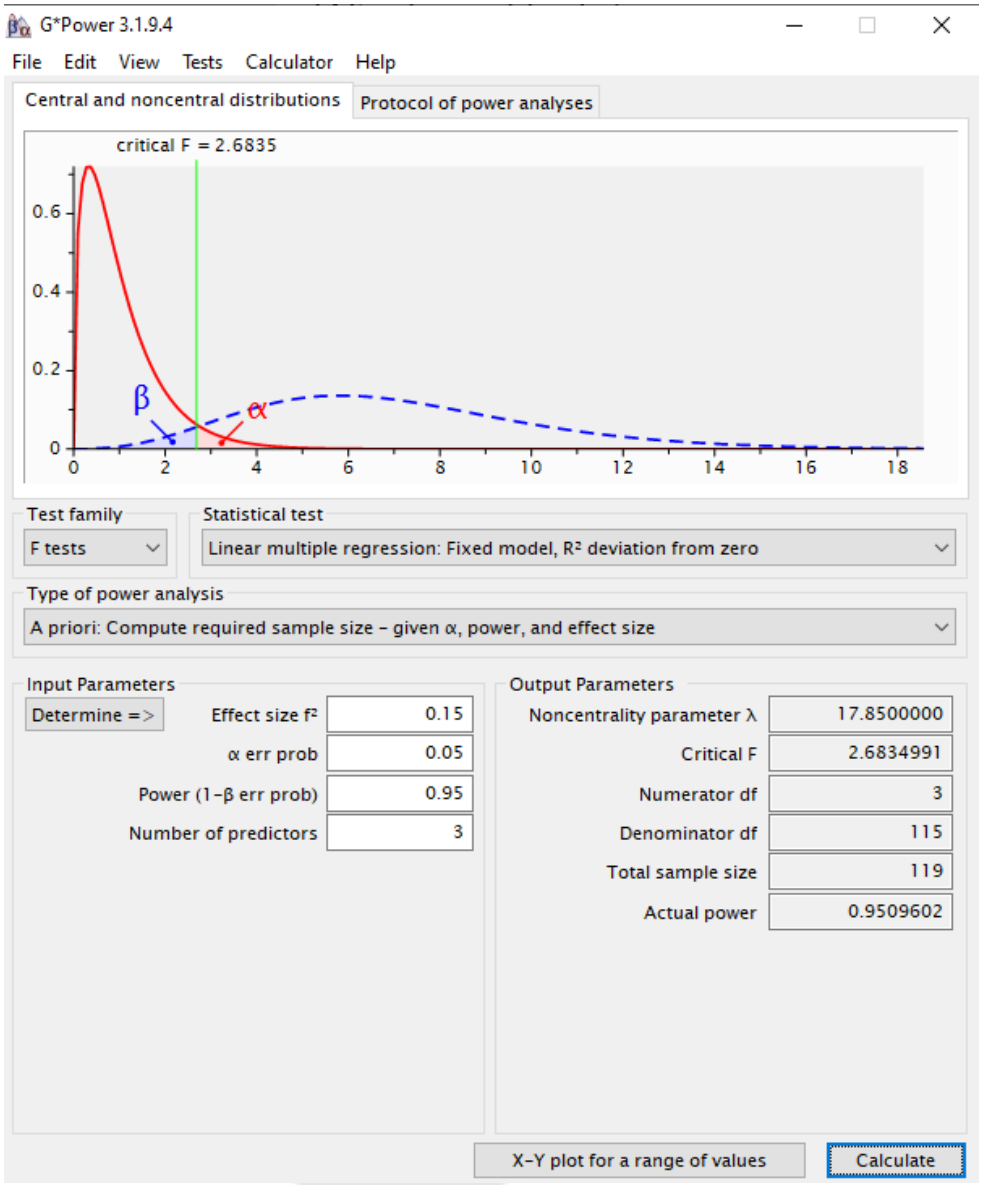
ประชากรที่มีอายุอยู่ในกลุ่มเจเนอเรชั่นแซด ซึ่งเกิดในปี พ.ศ. 2540-2546 (อายุระหว่าง 20-26 ปี) จำนวนทั้งหมด 5,885,215 คน (สำนักงานสถิติแห่งชาติ, 2563)

กลุ่มตัวอย่าง

กลุ่มตัวอย่าง คือ กลุ่มเจเนอเรชั่นแซด ซึ่งเป็นผู้ที่เกิดในปี พ.ศ.2540-2546 (อายุระหว่าง 20-26 ปี) ซึ่งใช้วิธีสุ่มตัวอย่างแบบไม่อาศัยความน่าจะเป็น เก็บข้อมูลแบบสะดวกด้วยการคัดเลือกผู้ที่อยู่ในเจนเนอเรชั่นแซด โดยมีขั้นตอนในการเลือกกลุ่มตัวอย่างด้วยการคำนวณโดยใช้โปรแกรม G* Power ดังนี้

1. คำนวณกลุ่มตัวอย่างโดยใช้โปรแกรม G*Power ซึ่งเป็นโปรแกรมที่ช่วยในการกำหนดขนาดตัวอย่าง สร้างจากสูตรของ (Cohen, 1977) ใช้ในการวิจัยเชิงปริมาณ โดยอาศัยค่าขนาดอิทธิพล (Effect) ค่าความคาดเคลื่อนประเภท 1 (Type 1 error) และค่าความคาดเคลื่อนประเภท 2 (Type 2 error) ช่วยในการคำนวณขนาดกลุ่มตัวอย่างได้อย่างถูกต้องและสะดวกรวดเร็ว (นงลักษณ์ วิรัชชัย, 2555)

2. กำหนดค่าในการสุ่มตัวอย่างในโปรแกรม ดังนี้ (1) สถิติที่ใช้ F-test, Linear multiple regression: R2 deviation from zero (2) ค่าอิทธิพลขนาดกลาง (Effect size) = 0.15 (3) ค่าความคาดเคลื่อน (Alpha) = 0.05 (4) ค่า Power = 0.95 และ (5) ตัวแปรอิสระ (Number of predictors) = 3 ตัวแปร ได้ขนาดตัวอย่างขั้นต่ำ 119 ราย ตามภาพประกอบ 2



ภาพประกอบ 2 การคำนวณกลุ่มตัวอย่างโดยใช้โปรแกรม G*Power

3. ผู้วิจัยกำหนดจำนวนตัวอย่างขั้นต่ำในการเก็บข้อมูลไว้ที่ไม่ต่ำกว่า 120 ราย โดยปรับปรุงขนาดตัวอย่างให้เหมาะสมกับงานวิจัยครั้งนี้ ได้รับข้อมูลจากผู้ตอบแบบสอบถามจำนวนทั้งสิ้น 130 ราย

การสร้างเครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัยครั้งนี้ คือ แบบสอบถาม ประกอบด้วยชุดคำถามที่มีเนื้อหาครอบคลุมข้อมูลที่ต้องการ โดยเริ่มต้นเป็นข้อคำถามที่ใช้ในการคัดกรองผู้ตอบแบบสอบถามเฉพาะเจเนอเรชั่นแซด เมื่อผ่านการคัดกรองจึงเข้าสู่แบบสอบถาม ประกอบด้วยข้อคำถาม 5 ตอน ดังนี้

ตอนที่ 1 ข้อมูลคุณลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม ซึ่งมีลักษณะคำถามแบบปลายปิด ให้เลือกตอบเพียงคำตอบเดียว ประกอบด้วย ปีเกิด เพศ และ อาชีพ

ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ ซึ่งมีลักษณะคำถามแบบปลายปิด (Close Ended Question) ให้เลือกตอบเพียงคำตอบเดียว ประกอบด้วย 4 ตัวเลือก

ตอนที่ 3 ประสบการณ์ที่มีต่อภัยคุกคามทางไซเบอร์ เป็นแบบตรวจรายการ โดยให้เลือกคำตอบเพียงคำตอบเดียว จากระดับวัดข้อมูลประเภทอันตรภาคชั้น มี 5 ระดับ ได้แก่ 5=มากที่สุด 4=มาก 3=ปานกลาง 2=น้อย และ 1=น้อยที่สุด

ตอนที่ 4 พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น 4 ด้าน ได้แก่ ด้านการตั้งค่ารหัสผ่าน ด้านการจัดการข้อมูลส่วนบุคคล ด้านการใช้งานอุปกรณ์คอมพิวเตอร์ ด้านการใช้อุปกรณ์เคลื่อนที่ และด้านการใช้สื่อสังคมออนไลน์ ซึ่งเป็นแบบตรวจรายการ โดยให้เลือกคำตอบเพียงคำตอบเดียว จากระดับวัดข้อมูลประเภทอันตรภาคชั้น มี 5 ระดับ ได้แก่ 5=มากที่สุด 4=มาก 3=ปานกลาง 2=น้อย และ 1=น้อยที่สุด

ตอนที่ 5 ข้อเสนอแนะเพิ่มเติมเกี่ยวกับพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ ซึ่งมีลักษณะคำถามแบบปลายเปิด

ขั้นตอนการสร้างเครื่องมือในการวิจัย

ผู้วิจัยได้ดำเนินการสร้างแบบสอบถามตามลำดับขั้นตอน ดังนี้

1. ศึกษาข้อมูลจากวารสาร ตำรา แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้องกับพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์

2. ทบทวนวรรณกรรมที่เกี่ยวข้องกับปัจจัยที่มีอิทธิผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ เพื่อพิจารณาคัดเลือกตัวแปรอิสระที่เป็นปัจจัยสำคัญต่อพฤติกรรมของกลุ่มเจเนอเรชั่นแซด ได้แก่ เพศ ความรู้ และประสบการณ์

3. ดำเนินการพัฒนาเครื่องมือในการวิจัยทั้ง 2 วิธี คือ แบบสอบถาม จากระดับวัดข้อมูลประเภทอันตรภาคชั้น (Interval Scale) ทั้งหมด 5 ระดับ และแบบทดสอบ จำนวน 12 ข้อ ประกอบด้วย 4 ตัวเลือกให้สอดคล้องและเหมาะสมกับตัวแปรที่จะศึกษาครั้งนี้

4. ผู้วิจัยนำเครื่องมือที่สร้างขึ้นส่งให้ผู้เชี่ยวชาญ 3 คนตรวจสอบโดยการประเมินความตรงตามเนื้อหา ด้วยการหาค่าดัชนีความสอดคล้อง (IOC) โดยหาค่าเฉลี่ยนของคะแนนประเมินในข้อคำถามแต่ละข้อ พิจารณาเลือกข้อคำถามที่มีค่าคะแนน IOC อยู่ระหว่าง 0.67-1.00 และปรับปรุงเครื่องมือตามคำแนะนำของผู้เชี่ยวชาญ

5. ตรวจสอบความสมบูรณ์ก่อนนำไปทดลองใช้ (Try out) กับกลุ่มคนเจเนอเรชั่นแซดที่ไม่ใช่กลุ่มตัวอย่าง จำนวน 30 คน ส่วนของความรู้เลือกข้อคำถามที่มีค่าความยากง่ายระหว่าง 0.20-0.80 จากนั้นทดสอบความเชื่อมั่นของแบบสอบถามโดยคำนวณค่าสัมประสิทธิ์ครอนบรัคแอลฟา (Cronbach's alpha coefficient) ตัวแปรชุดประสบการณ์ในภัยคุกคามทางไซเบอร์ได้ค่าสัมประสิทธิ์ครอนบรัคเท่ากับ 0.851 ตัวแปรชุดพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ได้ค่าสัมประสิทธิ์ครอนบรัคเท่ากับ 0.923 ซึ่งตามเกณฑ์ค่าสัมประสิทธิ์ครอนบรัคแอลฟาควรมีค่าตั้งแต่ 0.7 ขึ้นไป จึงถือว่าเครื่องมือวิจัยนี้มีค่าความเชื่อมั่นเพียงพอที่จะใช้ศึกษา (Cortina, 1993; ชไมพร กาญจนกิจสกุล, 2555)

6. ปรับปรุงแบบสอบถามฉบับสมบูรณ์ เพื่อเตรียมนำมาใช้จริง

7. ผู้วิจัยนำเสนอโครงการวิจัยเพื่อรับการพิจารณาจากคณะกรรมการจริยธรรมสำหรับโครงการวิจัยที่ทำในมนุษย์ รหัสโครงการวิจัย SWUEC/E/G-081/2565 โดยได้รับการรับรอง อายุการรับรองโครงการตั้งแต่วันที่ 22 กุมภาพันธ์ 2565 ถึง 22 กุมภาพันธ์ 2566 จากนั้นผู้วิจัยจึงดำเนินการเก็บข้อมูล

การเก็บรวบรวมข้อมูล

1. ผู้วิจัยได้ดำเนินการขอหนังสือรับรองการพิจารณาจากคณะกรรมการจริยธรรมสำหรับโครงการวิจัยที่ทำในมนุษย์ รหัสโครงการวิจัย SWUEC/E/G-081/2565E เมื่อวันที่ 22 กุมภาพันธ์ 2565

2. ผู้วิจัยได้คัดเลือกผู้ตอบแบบสอบถามเฉพาะที่อยู่ในกลุ่มเจเนเรชั่นแซดที่เกิดในปี พ.ศ. 2540-2546 โดยสุ่มตัวอย่างแบบเฉพาะเจาะจงเพื่อคัดเลือกกลุ่มตัวอย่างตามความสะดวก

3. ผู้วิจัยได้ดำเนินการเก็บรวบรวมข้อมูลด้วยตนเองระหว่างเดือนมิถุนายน ถึง เดือนสิงหาคม 2565 ผ่านแบบสอบถามออนไลน์ที่สร้างด้วยเครื่องมือ Google form โดยกระจายผ่าน

สื่อสังคมออนไลน์ ได้แก่ Facebook Twitter Line และ Instragram ผู้ตอบแบบสอบถามช่วยส่งต่อแบบสอบถามผ่านสื่อสังคมออนไลน์ดังกล่าวตามกลุ่มตัวอย่างและจำนวนที่กำหนด

4. ผู้วิจัยดำเนินเก็บรวบรวมข้อมูลเพิ่มเต็มให้ครบตามจำนวนกลุ่มตัวอย่างขั้นต่ำที่กำหนด โดยพิจารณาการคัดเลือกผู้ตอบแบบสอบถามเพิ่มเติมให้ข้อมูลกระจายตามตัวแปรกลุ่มที่ศึกษา

5. ตรวจสอบข้อมูลและนำข้อมูลที่ได้รับไปวิเคราะห์ทางสถิติต่อไป

การจัดกระทำและการวิเคราะห์ข้อมูล

ผู้วิจัยตรวจสอบความครบถ้วนและความสมบูรณ์ของข้อมูลที่ได้รับจากแบบสอบถามออนไลน์ ในการศึกษาครั้งนี้ ผู้ศึกษาดำเนินการนำข้อมูลจากแบบสอบถามที่ได้รับคำตอบแล้วที่อยู่ในรูปแบบ Spreadsheet มาจัดรูปแบบข้อมูลเพื่อวิเคราะห์โดยใช้โปรแกรมสำเร็จรูป ดังนี้

1. สถิติเชิงพรรณนาเพื่อบรรยายข้อมูลพื้นฐานทั่วไปของผู้ตอบแบบสอบถาม

2. การหาค่าความถี่ ค่าร้อยละ ของการทดสอบความรู้ โดยข้อที่ตอบถูกให้ 1 คะแนน และข้อที่ตอบผิดให้ 0 คะแนน และนำมาหาค่าเฉลี่ยของความรู้

3. สถิติพื้นฐาน โดยใช้ค่าเฉลี่ย ($\bar{x}$) ส่วนเบี่ยงเบนมาตรฐาน (SD) และแปลผลตามระดับคะแนนเพื่อวิเคราะห์ระดับของประสบการณ์และพฤติกรรมการป้องกันตนเองจากภัยคุกคามโดยรวมและรายด้าน ใช้เกณฑ์ในการแปลผลคะแนนดังนี้ (บุญชม ศรีสะอาด, 2545)

ระดับคะแนนเฉลี่ย	การแปลความหมาย
4.51 – 5.00	มีความคิดเห็นอยู่ในระดับมากที่สุด
3.51 – 4.50	มีความคิดเห็นอยู่ในระดับมาก
2.51 - 3.50	มีความคิดเห็นอยู่ในระดับปานกลาง
1.51 – 2.00	มีความคิดเห็นอยู่ในระดับน้อย
1.00 – 1.50	มีความคิดเห็นอยู่ในระดับน้อยที่สุด

4. ทดสอบสมมติฐานด้วยการวิเคราะห์สถิติเชิงอนุมาน เพื่อวิเคราะห์สมการถดถอย (linear regression analysis) ของตัวแปรที่มีอิทธิพลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามบนไซเบอร์ของเจเนอเรชั่นแซด หาค่าสัมประสิทธิ์สหสัมพันธ์ ประกอบด้วยเพศซึ่งเป็นตัวแปรหุ่น (dummy variable) ความรู้และประสบการณ์ซึ่งเป็นตัวแปรต่อเนื่อง วิเคราะห์สถิติที่ระดับนัยสำคัญ 0.05

5. นำข้อมูลจากแบบสอบถามตอนที่ 5 ข้อเสนอแนะเพิ่มเติมซึ่งเป็นคำถามปลายเปิดมาสรุปประเด็นจากข้อคิดเห็น

สรุปขั้นตอนการวิจัย

ตาราง 2 แสดงขั้นตอนที่ใช้ในการวิจัย พร้อมทั้งกระบวนการและผลลัพธ์จากการวิจัยในแต่ละขั้นตอน

ตาราง 2 สรุปขั้นตอนการวิจัย

ขั้นตอน	กระบวนการ	ผลลัพธ์
ขั้นตอนที่ 1 การพัฒนา	การนำกรอบแนวคิดที่ได้จากการทบทวนวรรณกรรมมาพัฒนาเป็นแบบสอบถาม	แบบสอบถาม
ขั้นตอนที่ 2 การตรวจสอบคุณภาพของเครื่องมือวิจัย	การพิจารณาตรวจสอบความตรงของเนื้อหาโดยผู้ทรงคุณวุฒิ จำนวน 3 ท่าน และนำผลที่ได้มาหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ (Item-Objective Congruence Index: IOC)	ความตรงของเนื้อหา (Validity)
ขั้นตอนที่ 3 ทดลองใช้แบบสอบถาม	การนำแบบสอบถามไปทดลองใช้ จำนวน 30 ชุด เพื่อนำมาวิเคราะห์คุณภาพของเครื่องมือ โดยวิธีการหาค่าความเชื่อมั่น (Reliability) โดยใช้วิธีการหาค่าสัมประสิทธิ์ครอนบรัคอัลฟ่า	ความเชื่อมั่นของเนื้อหา (Reliability)
ขั้นตอนที่ 4 การเก็บรวบรวมข้อมูล	เก็บรวบรวมข้อมูลโดยการกระจายแบบสอบถามออนไลน์	ข้อมูลที่ใช้ในการวิเคราะห์ผลการวิจัย
ขั้นตอนที่ 5 วิเคราะห์ผลการวิจัย	วิเคราะห์ผลจากการวิจัย โดยใช้โปรแกรมสำเร็จรูปทางสถิติ	ผลการวิจัย

บทที่ 4
ผลการวิเคราะห์ข้อมูล

การวิจัยเรื่อง พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด สามารถเก็บแบบสอบถามที่สมบูรณ์ได้ 130 ชุด คิดเป็นร้อยละ 100 แล้วนำมาวิเคราะห์ข้อมูลด้วยโปรแกรมคำนวณสำเร็จรูป สามารถสรุปผลการวิเคราะห์ข้อมูลดังนี้ (คณัญญา อิ่มใจ และ วิภากร วัฒนสินธุ์, 2566)

สัญลักษณ์ที่ใช้ในการวิเคราะห์ข้อมูล

ในการวิจัย ผู้วิจัยได้กำหนดสัญลักษณ์ที่ใช้ในการวิเคราะห์ข้อมูลและแปลความหมายของผลการวิเคราะห์ข้อมูลตามตาราง 3 ดังนี้

ตาราง 3 อธิบายสัญลักษณ์

สัญลักษณ์	ความหมาย
n	จำนวนกลุ่มเจเนอเรชั่นแซดที่เป็นกลุ่มตัวอย่าง
$\bar{X}$	ค่าเฉลี่ย
SD	ค่าส่วนเบี่ยงแบนมาตรฐาน
R	ค่าสัมประสิทธิ์สหสัมพันธ์พหุคูณ (Multiple Correlation)
R Square	ค่าสัมประสิทธิ์การตัดสินใจพหุคูณ (Coefficient of Multiple Determination)
Adjusted R Square	ค่า R Square ปรับปรุงเรียบร้อย
SE	ค่าที่แสดงระดับความคลาดเคลื่อนที่เกิดจากการใช้ตัวแปรอิสรทั้งหมดมาพยากรณ์ตัวแปรตาม
SS	ค่าผลรวมของส่วนเบี่ยงเบนกำลังสอง
df.	ขั้นของความเป็นอิสระ (Degree of freedoms)
MS	ค่าความแปรปรวน หรือส่วนเบี่ยงเบนกำลังสองเฉลี่ย
f	ค่าสถิติที่ใช้ในการกระจายของ F (F-distribution)
p-value	ค่าความน่าจะเป็นสำหรับบอกนัยสำคัญทางสถิติ
B	ค่าสัมประสิทธิ์การถดถอยของตัวแปรอิสระแต่ละตัวที่นำมาสร้างสมการพยากรณ์ (Unstandardized Coefficient)

ตาราง 3 (ต่อ)

สัญลักษณ์	ความหมาย
Beta	ค่าสัมประสิทธิ์การถดถอยของตัวแปรอิสระแต่ละตัวนำมาสร้างสมการพยากรณ์ (Standardized Coefficient)
t	ค่าสถิติทดสอบตัวแปรอิสระที่สามารถใช้พยากรณ์ตัวแปรตามได้
*	มีนัยสำคัญทางสถิติที่ระดับ .05

การเสนอผลการวิเคราะห์ข้อมูล

ผู้วิจัยได้เสนอผลการวิเคราะห์ข้อมูลและแปลความหมายตามลำดับ ดังนี้

1. ข้อมูลคุณลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม

2. พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

3. อิทธิพลของเพศ ความรู้ และประสบการณ์ที่มีผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

4. การวิเคราะห์สหสัมพันธ์ของปัจจัยที่มีอิทธิผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

5. ข้อเสนอแนะเพิ่มเติม

ผลการวิเคราะห์ข้อมูล

ผลการวิเคราะห์ข้อมูลที่ได้จากการวิจัย มีดังนี้

1. ข้อมูลคุณลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม ได้แก่ ปีเกิด เพศ และอาชีพ

ตาราง 4 ข้อมูลคุณลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม

สถานภาพ	จำนวน (n)	ร้อยละ
ปีเกิด		
2540	64	49.20
2541	22	17.00
2542	15	11.50
2543	14	10.80
2544	9	6.90

ตาราง 4 (ต่อ)

สถานภาพ	จำนวน (n)	ร้อยละ
2545	4	3.10
2546	2	1.50
รวม	130	100.00
เพศ		
ชาย	59	45.40
หญิง	71	54.60
รวม	130	100.00
อาชีพ		
นิสิตนักศึกษา	56	43.08
ข้าราชการรัฐวิสาหกิจพนักราชการ	17	13.08
เอกชนธุรกิจส่วนตัว	53	40.76
ว่างงาน	4	3.08
รวม	130	100.00

จากตาราง 4 พบว่า กลุ่มตัวอย่างที่เป็นกลุ่มเจเนอเรชั่นแซด จำนวน 130 คน ส่วนใหญ่เป็นเพศหญิง จำนวน 71 คน (ร้อยละ 54.60) เกิดปีพ.ศ. 2540 จำนวน 64 คน (ร้อยละ 49.20) และประกอบอาชีพเป็นนิสิต/นักศึกษา จำนวน 56 คน (ร้อยละ 43.10)

2. ปัจจัยที่มีผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด ได้แก่ ความรู้ ประสบการณ์ ดังนี้

2.1. ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

ตาราง 5 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

รายข้อแบบทดสอบ	ถูก		ผิด	
	จำนวน(n)	ร้อยละ	จำนวน(n)	ร้อยละ
1. การหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมที่มีข้อความซึ่งทำให้	51	39.2	79	60.8

ตาราง 5 (ต่อ)

รายข้อแบบทดสอบ	ถูก		ผิด	
	จำนวน (n)	ร้อยละ	จำนวน (n)	ร้อยละ
ผู้เสียหายอ่านแล้วหลงเชื่อเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่นๆ เป็นประเภทของการโจมตีทางไซเบอร์ในข้อใด				
2. เว็บไซต์ใดไม่มีความน่าเชื่อถือในเรื่องความปลอดภัย หากบังคับให้ผู้ใช้มีการกรอก Password	58	44.6	72	55.4
3. ข้อใดเป็นการเพิ่มความปลอดภัยในการยืนยันตัวตน	94	72.3	36	27.7
4. ข้อใดคือวิธีการตั้งรหัสผ่านที่ดี	91	70	39	30
5. ท่านชื่อ Biden ท่านจะตั้งรหัสผ่านตามข้อใด เพื่อให้รหัสมีความปลอดภัยมากที่สุด	45	34.6	85	65.4
6. การตั้งค่า Wi-Fi router แบบใดมีความปลอดภัยสูงสุด	56	43.1	74	56.9
7. ข้อใดเป็นการละเมิดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	51	39.2	79	60.8
8. เมื่อท่านได้รับอีเมลให้ดำเนินการส่งชื่อบัญชีผู้ใช้และรหัสผ่าน เพื่อปรับปรุงระบบการทำงานอีเมลมหาวิทยาลัย จากสำนักคอมพิวเตอร์ มหาวิทยาลัย ท่านจะดำเนินการอย่างไร	44	33.8	86	66.2
9. ข้อใดเป็นการรักษาความปลอดภัยของเราเตอร์ (Router)	92	70.8	38	29.2

ตาราง 5 (ต่อ)

รายข้อแบบทดสอบ	ถูก		ผิด	
	จำนวน (n)	ร้อยละ	จำนวน (n)	ร้อยละ
10. ข้อใดคือการดำเนินการเพื่อจำกัดการเข้าถึงไฟล์และอุปกรณ์	75	57.7	55	42.3
11. ข้อใดคือพฤติกรรมป้องกันตนเองจากภัยคุกคามจากอาชญากรทางไซเบอร์	86	66.2	44	33.8
12. ข้อใดคือพฤติกรรมเสี่ยงต่อการโจมตีทางไซเบอร์	68	52.3	62	47.7

จากตาราง 5 พบว่า ข้อแบบทดสอบที่มีการตอบถูกมากที่สุด 3 อันดับ ได้แก่ ข้อที่ 3 เว็บไซต์ใดไม่มีความน่าเชื่อถือในเรื่องความปลอดภัย หากบังคับให้ผู้ใช้มีการกรอก Password จำนวน 94 คน (ร้อยละ72.3) รองลงมา คือ ข้อที่ 9 ข้อใดเป็นการรักษาความปลอดภัยของเราเตอร์ (Router) จำนวน 92 คน (ร้อยละ 70.8) และ ข้อที่ 4 ข้อใดคือวิธีการตั้งรหัสผ่านที่ดี จำนวน 91 คน (ร้อยละ 70) ตามลำดับ โดยมีค่าคะแนนเฉลี่ยของความรู้อยู่ที่ 5.54 คะแนน (ร้อยละ 46.17)

2.2 ประสบการณ์ในภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

ตาราง 6 ประสบการณ์ในภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

ประสบการณ์ในภัยคุกคามทางไซเบอร์	ระดับความคิดเห็น		
	$\bar{X}$	SD	แปลความ
1. ท่านเคยได้รับการอบรมเกี่ยวกับภัยคุกคามทางไซเบอร์	2.96	1.18	ปานกลาง
2. ท่านรับรู้ความเสี่ยงที่เกิดขึ้น หากถูกละเมิดในข้อมูลส่วนบุคคล (เช่น การขายต่อข้อมูลส่วนบุคคล การสวมรอยบัตรประชาชน การขโมยข้อมูลบัตรเครดิต)	3.86	0.82	มาก
3. ท่านหรือบุคคลที่ท่านรู้จักเคยมีประสบการณ์ถูก hack บัญชีอีเมลหรือสื่อสังคมออนไลน์	3.58	1.20	มาก

ตาราง 6 (ต่อ)

ประสบการณ์ในภัยคุกคามทางไซเบอร์	ระดับความคิดเห็น		
	$\overline{X}$	SD	แปลความ
4. ท่านเคยได้รับอีเมลหลอกลวง (Phishing, Scams email)	3.76	1.06	มาก
5. ท่านเคยคลิกเข้าไปในเว็บไซต์หลอกลวงหรือแอบอ้างว่าเป็นเว็บไซต์จริง	2.87	1.27	ปานกลาง
6. ท่านรู้จักและเคยใช้ VPN	3.82	1.05	มาก
7. ท่านเคยโดน malware เข้ามาก่อกวนการทำงานระบบคอมพิวเตอร์	2.97	1.19	ปานกลาง
8. ท่านหรือบุคคลรอบข้างเคยถูกมิจฉาชีพหลอกให้โอนเงินด้วยวิธีการต่างๆ เช่น การซื้อสินค้าออนไลน์ เงินบริจาค เป็นต้น	3.08	1.31	ปานกลาง
9. ท่านเคยปิดการใช้งานโปรแกรมป้องกันไวรัสในคอมพิวเตอร์ เพื่อสามารถดาวน์โหลดข้อมูลจากเว็บไซต์	3.25	1.31	ปานกลาง
10. ท่านเคยร่วมลงทุนกับผู้อื่นในการแลกเปลี่ยนสกุลเงินดิจิทัล	2.39	1.41	น้อย
11. ท่านเคยใช้งานแอปพลิเคชั่นหาคู่	2.57	1.41	น้อย
ค่าเฉลี่ยรวม	3.14	1.25	ปานกลาง

จากตาราง 6 พบว่า กลุ่มเจเนอเรชันแซดโดยรวมมีความคิดเห็นต่อประสบการณ์ในภัยคุกคามทางไซเบอร์ระดับปานกลาง ($\overline{X}$= 3.14)) เมื่อทำการวิเคราะห์เป็นรายข้อ พบว่าข้อที่มีค่าเฉลี่ยมากที่สุด คือ ข้อที่ 2 ท่านรับรู้ความเสี่ยงที่เกิดขึ้น หากถูกละเมิดในข้อมูลส่วนบุคคล ($\overline{X}$= 3.86) รองลงมา คือ ข้อที่ 6 ท่านรู้จักและเคยใช้ VPN ($\overline{X}$= 3.82) และข้อที่ 4 ท่านเคยได้รับอีเมลหลอกลวง (Phishing, Scams email) ($\overline{X}$= 3.76) ตามลำดับ ส่วนข้อที่มีค่าเฉลี่ยน้อยที่สุด คือ ข้อที่ 10 ท่านเคยร่วมลงทุนกับผู้อื่น ในการแลกเปลี่ยนสกุลเงินดิจิทัล ($\overline{X}$= 2.39)

3. พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด ได้แก่ ด้านการตั้งค่ารหัสผ่าน ด้านการจัดการข้อมูลส่วนบุคคล ด้านการใช้งานอุปกรณ์คอมพิวเตอร์

ตาราง 7 พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์	ระดับความคิดเห็น		
	$\overline{X}$	SD	แปลความ
ด้านการตั้งค่ารหัสผ่าน			
1.ท่านตั้งรหัสผ่านของแต่ละระบบแตกต่างกัน	3.44	1.18	ปานกลาง
2.แม้ยังจำรหัสผ่านเดิมได้ ท่านเปลี่ยนรหัสผ่านเข้าระบบอยู่บ่อยครั้ง	3.09	1.24	ปานกลาง
ค่าเฉลี่ยด้านการตั้งค่ารหัสผ่าน	**3.27**	**1.09**	**ปานกลาง**
ด้านการจัดการข้อมูลส่วนบุคคล			
3.ท่านอ่านนโยบายความเป็นส่วนตัว (Privacy Policy) ก่อนคลิกตกลงทุกครั้ง	3.38	1.14	ปานกลาง
4.ท่านไม่แบ่งปันข้อมูลส่วนบุคคลให้แก่บุคคลที่รู้จักหรือคุ้นเคย โดยไม่ทราบวัตถุประสงค์	4.13	0.90	มาก
5.ท่านตั้งค่าความเป็นส่วนตัวบนบัญชีออนไลน์ทั้งหมด (เช่น การยืนยันตัวตนแบบสองปัจจัย ป้องกันการรีเซ็ตรหัสผ่าน รับแจ้งเตือนเมื่อมีการเข้าสู่ระบบที่ไม่รู้จัก)	4.09	0.86	มาก
6.ท่านกำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคลบนอุปกรณ์ (เช่น รูปภาพ ไมโครโฟน กล้อง)	3.92	0.99	มาก
7.ท่านบล็อคหรือปิดการเข้าถึงข้อมูลคุกกี้จากบุคคลที่สาม	3.82	1.05	มาก
ค่าเฉลี่ยด้านการจัดการข้อมูลส่วนบุคคล	**3.88**	**0.74**	**มาก**
ด้านการใช้งานอุปกรณ์คอมพิวเตอร์			
8.ท่าน update โปรแกรม anti-virus และระบบปฏิบัติการอย่างสม่ำเสมอ	3.72	1.12	มาก

ตาราง 7 (ต่อ)

พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์	ระดับความคิดเห็น		
	$\bar{X}$	SD	แปลความ
9.ท่านหมั่นสังเกตอาการผิดปกติของอุปกรณ์คอมพิวเตอร์ (เช่น เครื่องช้า เครื่องนิ่ง หรือมีการเตือนข้อความจากอุปกรณ์)	4.05	0.85	มาก
10. ท่านไม่เปิดไฟล์เอกสารแนบในอีเมลที่มาจากบุคคลที่ท่านไม่ทราบแหล่งที่มา	4.04	0.85	มาก
11. ท่านจัดการความปลอดภัยกับเครื่องคอมพิวเตอร์ทันทีเมื่อมีการแจ้งเตือนมัลแวร์	3.96	0.93	มาก
12. ท่านสำรองข้อมูลบนเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ (backup)	3.66	1.02	มาก
13. ท่านล็อคหน้าจอคอมพิวเตอร์ทุกครั้งที่ท่านเดินออกจากโต๊ะทำงาน	3.86	1.05	มาก
14. ท่านดาวน์โหลดข้อมูลและสื่อดิจิทัลจากแหล่งที่ได้รับอนุญาต น่าเชื่อถือ และตรวจสอบความถูกต้อง	4.04	0.86	มาก
ค่าเฉลี่ยด้านการใช้งานอุปกรณ์คอมพิวเตอร์	**3.91**	**0.71**	**มาก**
ด้านการใช้งานอุปกรณ์เคลื่อนที่			
15. ท่านตั้งค่ารหัสผ่านสำหรับล็อคหน้าจอของ Laptop, Tablet และโทรศัพท์มือถือ	4.32	0.79	มาก
16. ท่านเลือกใช้เครือข่ายสาธารณะเฉพาะผู้ให้บริการเครือข่ายที่น่าเชื่อถือ (เช่น AIS DTAC TRUE)	4.24	0.83	มาก
ค่าเฉลี่ยด้านการใช้งานอุปกรณ์เคลื่อนที่	**4.28**	**0.70**	**มาก**
ด้านการใช้งานสื่อสังคมออนไลน์			
17. ท่านไม่กดเข้าลิงค์ที่แชร์มาจากสื่อสังคมออนไลน์	3.92	0.97	มาก
18. ท่านไม่ส่งข้อมูลส่วนบุคคลให้กับผู้อื่น (เช่น ชื่อผู้ใช้ รหัสผ่าน รหัส OTP เลขบัตรประชาชน วันเกิด เบอร์โทร)	4.20	0.88	มาก

ตาราง 7 (ต่อ)

พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์	ระดับความคิดเห็น		
	$\overline{X}$	SD	แปลความ
19. ท่านไม่แชร์ตำแหน่งที่อยู่อาศัยของตนเองที่สามารถระบุถึงตัวตนได้บนสื่อสังคมออนไลน์	4.06	0.97	มาก
20. ท่านไม่ยอมรับการเป็นเพื่อนบนสื่อสังคมออนไลน์ที่ไม่รู้จัก	4.03	0.91	มาก
21. ท่านตรวจสอบประวัติการใช้งานบนสื่อสังคมออนไลน์เสมอ	3.89	0.98	มาก
ค่าเฉลี่ยด้านการใช้งานสื่อสังคมออนไลน์	**4.02**	**0.73**	**มาก**
ค่าเฉลี่ยรวม	**3.90**	**0.97**	**มาก**

จากตาราง 7 พบว่า กลุ่มเจเนอเรชันแซดมีพฤติกรรมป้องกันตนเองจากภัยคุกคามทางไซเบอร์โดยเฉลี่ยในระดับมาก ($\overline{X}$= 3.90) เมื่อทำการวิเคราะห์เป็นรายข้อ พบว่า ด้านที่มีค่าเฉลี่ยมากที่สุด คือ ด้านการใช้งานอุปกรณ์เคลื่อนที่ ($\overline{X}$ = 4.28) รองลงมา คือ ด้านการใช้งานสื่อสังคมออนไลน์ ($\overline{X}$= 4.02) และด้านการใช้งานอุปกรณ์คอมพิวเตอร์ ($\overline{X}$= 3.91) ตามลำดับ ส่วนข้อที่มีค่าเฉลี่ยน้อยที่สุด คือ ด้านการตั้งค่ารหัสผ่าน ($\overline{X}$= 3.27)

4. การวิเคราะห์สหสัมพันธ์ของปัจจัยที่มีอิทธิผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด ดังนี้

4.1 การวิเคราะห์ความสัมพันธ์ระหว่างพฤติกรรมป้องกันตนเองจากภัยคุกคามทางไซเบอร์กับตัวแปรอิสระทุกตัว ได้แก่ เพศ ความรู้ และประสบการณ์

ตาราง 8 พฤติกรรมป้องกันตนเองจากการคุกคามทางไซเบอร์กับตัวแปรอิสระทุกตัว

แหล่งความแปรปรวน	SS	df	MS	F	p-value
ระหว่างกลุ่ม	7.217	3	2.4.6	7.259	0.001*
ภายในกลุ่ม	41.757	126	0.331		
รวม	48.974	129			

*p-value < 0.05

จากตาราง 8 พบว่า พฤติกรรมขึ้นกับเพศ ความรู้ และประสบการณ์ อย่างน้อย 1 ปัจจัย จึงตรวจสอบความสัมพันธ์ระหว่างตัวแปรตามกับตัวแปรอิสระครั้งละ 1 ตัว ดังแสดงในตาราง 8 พบว่า มีเพียงปัจจัยเดียวที่ส่งผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์อย่างมีนัยสำคัญทางสถิติ คือ ประสบการณ์ ในขณะที่เพศและความรู้ไม่มีผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ จึงใช้การวิเคราะห์สมการถดถอยเชิงเดี่ยว เพื่อศึกษาความสัมพันธ์ระหว่างประสบการณ์กับพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์

ตาราง 9 พฤติกรรมป้องกันตนเองจากการคุกคามทางไซเบอร์ กับเพศ ความรู้ และประสบการณ์ ครั้งละ 1 ตัว

ตัวแปรอิสระ	Unstandardized Coefficients		Standardized Coefficients	t	p-value
	B	Std. Error	Beta		
ค่าคงที่ (Constant)	2.673	0.304		8.805	0.001*
เพศ (Gender)	-0.187	0.106	-0.151	-1.757	0.081
ความรู้ (Knowledge)	0.041	0.022	0.168	1.857	0.066
ประสบการณ์ (Experience)	0.330	0.072	0.412	4.601	0.001*
R = 0.384, R Square = 0.147, Adjusted R Square = 0.127, SE = 0.576, Durbin-Watson = 1.821					

*p-value < 0.05

จากตาราง 9 พบว่า พฤติกรรมป้องกันตนเองจากภัยคุกคามทางไซเบอร์สามารถทำนายด้วยตัวแปรอิสระเพียงตัวเดียว คือ ประสบการณ์ จึงทดสอบค่า F เพื่อวิเคราะห์ความสัมพันธ์ระหว่างพฤติกรรมป้องกันตนเองจากภายคุกคามทางไซเบอร์และประสบการณ์

4.2 การวิเคราะห์ความสัมพันธ์ระหว่างพฤติกรรมป้องกันตนเองจากภัยคุกคามทางไซเบอร์กับประสบการณ์ ได้แก่ ด้านการตั้งค่ารหัสผ่าน ด้านการจัดการข้อมูลส่วนบุคคล ด้านการใช้งานอุปกรณ์คอมพิวเตอร์ ด้านการใช้งานอุปกรณ์เคลื่อนที่ และด้านการใช้งานสื่อสังคมออนไลน์ ดังนี้

ตาราง 10 ความสัมพันธ์ระหว่างพฤติกรรมป้องกันตนเองจากภัยคุกคามทางไซเบอร์กับประสบการณ์

แหล่งความแปรปรวน	SS	df	MS	F	p-value
ระหว่างกลุ่ม	5.505	1	5.505	16.210	0.001*
ภายในกลุ่ม	43.469	128	0.340		
รวม	48.974	129			

*p-value < 0.05

ตาราง 11 พฤติกรรมป้องกันตนเองจากภัยคุกคามทางไซเบอร์กับประสบการณ์โดยใช้สมการถดถอยเชิงเดี่ยว

ตัวแปรอิสระ	Unstandardized Coefficients		Standardized Coefficients	t	p-value
	B	Std. Error	Beta		
ค่าคงที่ (Constant)	3.042	0.219		13.885	0.001*
ประสบการณ์ (Experience)	0.269	0.067	0.335	4.026	0.001*
R = 0.335, R Square = 0.112, Adjusted R Square = 0.105, SE = 0.583, Durbin-Watson = 1.836					

*p-value < 0.05

ผลการวิเคราะห์ความสัมพันธ์ของตัวแปรในตาราง 10 และวิเคราะห์สมการถดถอยเชิงเดี่ยวในตาราง 11 พบว่า ค่า t มีค่า p-value น้อยกว่า 0.05 นั่นคือ ประสบการณ์เกี่ยวภัยคุกคามทางไซเบอร์ (X) สามารถพยากรณ์พฤติกรรมการป้องกันตนเองจากภัยคุกคาม ($\hat{Y}$) ได้ที่ค่าร้อยละ 11.2 (R Square = 0.112) สามารถเขียนสมการได้ดังนี้ $\hat{Y}$=3.042+0.269 (Experience) กล่าวคือ หากประสบการณ์ในภัยคุกคามทางไซเบอร์เพิ่มขึ้น 1 หน่วยจะส่งผลให้พฤติกรรมในการป้องกันตนเองจากภัยคุกคามเพิ่มขึ้น 0.269 หน่วย

4.2.1 ความสัมพันธ์ระหว่างพฤติกรรมด้านการตั้งรหัสผ่านกับประสบการณ์

ตาราง 12 พฤติกรรมด้านการตั้งรหัสผ่านกับประสบการณ์

แหล่งความแปรปรวน	SS	df	MS	F	p-value
ระหว่างกลุ่ม	99.700	1	99.700	24.892	0.000*
ภายในกลุ่ม	512.677	128	4.005		
รวม	612.377	129			

*p-value < 0.05

ตาราง 13 พฤติกรรมด้านการตั้งรหัสผ่านกับประสบการณ์โดยใช้สมการถดถอยเชิงเดี่ยว

ตัวแปรอิสระ	Unstandardized Coefficients		Standardized Coefficients	t	p-value
	B	Std. Error	Beta		
ค่าคงที่ (Constant)	2.880	0.752		3.828	0.000*
ประสบการณ์ (Experience)	1.144	0.229	0.403	4.989	0.000*
R = 0.403, R Square = 0.163, Adjusted R Square = 0.156, SE = 2.000, Durbin-Watson = 1.665					

*p-value < 0.05

ผลการวิเคราะห์ความสัมพันธ์ระหว่างพฤติกรรมด้านการตั้งรหัสผ่านกับประสบการณ์ในตาราง 12 และการวิเคราะห์ความถดถอยเชิงเดี่ยวในตาราง 13 พบว่า ค่า t มีค่า p-value น้อยกว่า 0.05 นั่นคือ ประสบการณ์เกี่ยวภัยคุกคามทางไซเบอร์ (X) สามารถพยากรณ์พฤติกรรมด้านการตั้งรหัสผ่าน($\hat{Y}$)ได้ที่ค่าร้อยละ 16.3 (RSquare = 0.163) สามารถเขียนสมการได้ดังนี้ $\hat{Y}$ = 2.880 + 1.144 (Experience)กล่าวคือหากประสบการณ์ในภัยคุกคามทางไซเบอร์เพิ่มขึ้น 1 หน่วยจะส่งผลให้พฤติกรรมด้านการตั้งรหัสผ่านในการป้องกันตนเองจากภัยคุกคามเพิ่มขึ้น 1.144 หน่วย

4.2.2 การวิเคราะห์ความสัมพันธ์ระหว่างพฤติกรรมด้านการจัดการข้อมูลส่วนบุคคลกับประสบการณ์

ตาราง 14 พฤติกรรมด้านการจัดการข้อมูลส่วนบุคคลกับประสบการณ์

แหล่งความแปรปรวน	SS	df	MS	F	p-value
ระหว่างกลุ่ม	6.649.	1	6.649	13.329	0.000*
ภายในกลุ่ม	63.852	128	0.499		
รวม	70.501	129			

*p-value < 0.05

ตาราง 15 พฤติกรรมด้านการจัดการข้อมูลส่วนบุคคลกับประสบการณ์โดยใช้สมการถดถอยเชิงเดี่ยว

ตัวแปรอิสระ	Unstandardized Coefficients		Standardized Coefficients	t	p-value
	B	Std. Error	Beta		
ค่าคงที่ (Constant)	2.933	0.266		11.044	0.001*
ประสบการณ์ (Experience)	0.295	0.081	0.307	3.651	0.001*
R = 0.307, R Square = 0.094, Adjusted R Square = 0.087, SE = 0.706, Durbin-Watson = 1.825					

*p-value < 0.05

ผลการวิเคราะห์ความสัมพันธ์ระหว่างพฤติกรรมด้านการจัดการข้อมูลส่วนบุคคลกับประสบการณ์ความถดถอยเชิงเดี่ยวในตาราง 14และการวิเคราะห์สมการถดถอยเชิงเดี่ยวในตาราง 15 พบว่า ค่า t มีค่า p-value น้อยกว่า 0.05 นั่นคือ ประสบการณ์เกี่ยวภัยคุกคามทางไซเบอร์ (X) สามารถพยากรณ์พฤติกรรมด้านการจัดการข้อมูลส่วนบุคคล($\hat{Y}$)ได้ที่ค่าร้อยละ9.4 (R Square = 0.094) สามารถเขียนสมการได้ดังนี้ $\hat{Y}$ = 2.933+0.295 (Experience) กล่าวคือหากประสบการณ์ในภัยคุกคามทางไซเบอร์เพิ่มขึ้น1 หน่วย จะส่งผลให้พฤติกรรมด้านการจัดการข้อมูลส่วนบุคคลในการป้องกันตนเองจากภัยคุกคามเพิ่มขึ้น 0.295 หน่วย

4.2.3 การวิเคราะห์ความสัมพันธ์ระหว่างพฤติกรรมด้านการใช้งานอุปกรณ์คอมพิวเตอร์กับประสบการณ์

ตาราง 16 พฤติกรรมด้านการจัดการข้อมูลส่วนบุคคลกับประสบการณ์

แหล่งความแปรปรวน	SS	df	MS	F	p-value
ระหว่างกลุ่ม	8.437	1	8.437	19.329	0.001*
ภายในกลุ่ม	55.871	128	0.436		
รวม	64.308	129			

*p-value < 0.05

ตาราง 17 พฤติกรรมด้านการจัดการข้อมูลส่วนบุคคลกับประสบการณ์โดยใช้สมการถดถอยเชิงเดี่ยว

ตัวแปรอิสระ	Unstandardized Coefficients		Standardized Coefficients	t	p-value
	B	Std. Error	Beta		
ค่าคงที่ (Constant)	2.844	0.248		11.448	0.001*
ประสบการณ์ (Experience)	0.333	0.076	0.362	4.397	0.001*
R = 0.362, R Square = 0.131, Adjusted R Square = 0.124, SE = 0.660					

*p-value < 0.05

ผลการวิเคราะห์ความสัมพันธ์ระหว่างพฤติกรรมด้านการจัดการข้อมูลส่วนบุคคลกับประสบการณ์ในตาราง 16และการวิเคราะห์ความถดถอยเชิงเดี่ยวในตาราง 17 พบว่า ค่า t มีค่า p-value น้อยกว่า 0.05 นั่นคือ ประสบการณ์เกี่ยวภัยคุกคามทางไซเบอร์ (X) สามารถพยากรณ์พฤติกรรมด้านการจัดการข้อมูลส่วนบุคคล ($\hat{Y}$) ได้ที่ค่าร้อยละ 13.1 (R Square = 0.131)สามารถเขียนสมการได้ดังนี้ $\hat{Y}$ = 2.844 + 0.333 (Experience) กล่าวคือ หากประสบการณ์ในภัยคุกคามทางไซเบอร์เพิ่มขึ้น 1 หน่วย จะส่งผลให้พฤติกรรมด้านการจัดการข้อมูลส่วนบุคคลในการป้องกันตนเองจากภัยคุกคามเพิ่มขึ้น 0.333 หน่วย

4.2.4 การวิเคราะห์ความสัมพันธ์ระหว่างพฤติกรรมด้านการใช้งานอุปกรณ์เคลื่อนที่กับประสบการณ์

ตาราง 18 พฤติกรรมด้านการใช้งานอุปกรณ์เคลื่อนที่กับประสบการณ์

แหล่งความแปรปรวน	SS	df	MS	F	p-value
ระหว่างกลุ่ม	0.449	1	0.449	0.911	0.342
ภายในกลุ่ม	63.082	128	0.493		
รวม	63.531	129			

*p-value < 0.05

ตาราง 19 พฤติกรรมด้านการใช้งานอุปกรณ์เคลื่อนที่กับประสบการณ์โดยใช้สมการณ์ถดถอยเชิงเดี่ยว

ตัวแปรอิสระ	Unstandardized Coefficients		Standardized Coefficients	t	p-value
	B	Std. Error	Beta		
ค่าคงที่ (Constant)	4.032	0.264		15.278	0.000*
ประสบการณ์ (Experience)	0.077	0.080	0.84	0.954	0.342
R = 0.084, R Square = 0.007, Adjusted R Square = - 0.001, SE = 0.702					

*p-value > 0.05

ผลการวิเคราะห์ความสัมพันธ์ในตาราง 18และวิเคราะห์สมการถดถอยเชิงเดี่ยวในตาราง 19 พบว่า ค่า t มีค่า p-value มากกว่า 0.05 นั่นคือ ประสบการณ์เกี่ยวภัยคุกคามทางไซเบอร์(X) ไม่สามารถพยากรณ์พฤติกรรมด้านการใช้งานอุปกรณ์เคลื่อนที่($\hat{Y}$) ได้อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

4.2.5 การวิเคราะห์ความสัมพันธ์ระหว่างพฤติกรรมด้านการใช้สื่อสังคมออนไลน์กับประสบการณ์

ตาราง 20 พฤติกรรมด้านการใช้สื่อสังคมออนไลน์กับประสบการณ์

แหล่งความแปรปรวน	SS	df	MS	F	p-value
ระหว่างกลุ่ม	0.892	1	0.892	1.703	0.194
ภายในกลุ่ม	67.016	128	0.524		
รวม	67.908	129			

*p-value < 0.05

ตาราง 21 พฤติกรรมด้านการใช้สื่อสังคมออนไลน์กับประสบการณ์โดยใช้สมการณ์ถดถอยเชิงเดี่ยว

ตัวแปรอิสระ	Unstandardized Coefficients		Standardized Coefficients	t	p-value
	B	Std. Error	Beta		
ค่าคงที่ (Constant)	3.675	0.272		13.508	0.000*
ประสบการณ์ (Experience)	0.108	0.083	0.115	1.305	0.194
R = 0.403, R Square = 0.163, Adjusted R Square = 0.156, SE = 2.000, Durbin-Watson = 1.665					

*p-value < 0.05

ผลการวิเคราะห์ในตาราง 21 พบว่า ค่า t มีค่า p-value มากกว่า 0.05 นั่นคือ ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ (X) ไม่สามารถพยากรณ์พฤติกรรมด้านการใช้สื่อสังคมออนไลน์ ($\hat{Y}$) ได้อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5. ข้อเสนอแนะเพิ่มเติม

ผู้ตอบแบบสอบถามมีข้อเสนอแนะเพิ่มเติมเกี่ยวกับพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ ดังนี้

5.1 ผู้คนส่วนใหญ่ไม่ได้มีความรู้ ข้อมูล หรือนิยามคำศัพท์เกี่ยวกับภัยคุกคามทางไซเบอร์ จึงคิดว่าเรื่องนี้ยังเป็นเรื่องที่ใหม่สำหรับหลายคนซึ่งอาจมีคนไม่ทราบหรือไม่เคยได้ยินคำศัพท์เหล่านี้เลยด้วยซ้ำ

5.2 ผู้ตอบเป็นผู้ใช้งานอุปกรณ์คอมพิวเตอร์ที่เป็นผลิตภัณฑ์ของบริษัท Apple ด้วยระบบปฏิบัติการ macOS มีการออกแบบระบบที่มั่นคงปลอดภัยต่อการโจมตีทางไซเบอร์ จึงทำให้ลดความเสี่ยงต่อภัยคุกคามทาไซเบอร์ได้

สรุปผลการวิเคราะห์ข้อมูล

ตาราง 22 พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ในแต่ละด้านกับประสบการณ์

พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์รายด้าน	ประสบการณ์		t	R Square	p-value
	B	Std. Error			
การตั้งค่ารหัสผ่าน	1.144	0.229	4.989	0.163	0.000*
การจัดการข้อมูลส่วนบุคคล	0.295	0.081	3.651	0.094	0.000*
การใช้งานอุปกรณ์คอมพิวเตอร์	0.333	0.076	4.379	0.131	0.000*
การใช้งานอุปกรณ์เคลื่อนที่	0.077	0.080	0.954	0.007	0.342
การใช้งานสื่อสังคมออนไลน์	0.108	0.083	1.305	0.163	0.194
ค่าเฉลี่ย	0.269	0.067	4.026	0.112	0.000*

*p-value < 0.05

จากตาราง 22 สรุปได้ว่าประสบการณ์มีผลต่อพฤติกรรมในด้านการตั้งค่ารหัสผ่าน การจัดการข้อมูลส่วนบุคคล และการใช้งานอุปกรณ์คอมพิวเตอร์ โดยเมื่อพิจารณาความสัมพันธ์ระหว่างพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ในภาพรวม พบว่า ประสบการณ์มีผลต่อความสัมพันธ์ระหว่างพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

บทที่ 5
สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

ในการวิจัยเรื่องพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด สามารถสรุปผลการดำเนินงาน โดยแบ่งหัวข้อในการสรุปผลได้ดังต่อไปนี้

1. ความมุ่งหมายของการวิจัย
2. สมมติฐานการวิจัย
3. วิธีดำเนินการวิจัย
4. สรุปผลการวิจัย
5. อภิปรายผลการวิจัย
6. ข้อเสนอแนะ

ความมุ่งหมายของงานวิจัย

ในการวิจัยครั้งนี้ผู้วิจัยได้ตั้งความมุ่งหมายไว้ดังนี้

1. เพื่อศึกษาพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

2. เพื่อศึกษาอิทธิพลของเพศ ความรู้ และประสบการณ์ที่มีผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

สมมุติฐานในการวิจัย

1. เพศมีอิทธิพลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

2. ความรู้มีอิทธิพลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

3. ประสบการณ์มีอิทธิพลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

วิธีดำเนินการวิจัย

1. ประชากรชาวไทยที่มีอายุอยู่ในกลุ่มเจเนอเรชันแซด ซึ่งมีอายุระหว่าง 18-24 ปี จำนวน 5,885,215 คน (สำนักงานสถิติแห่งชาติ,2563) และกลุ่มตัวอย่างในการวิจัยครั้งนี้ คำนวณโดยใช้โปรแกรมสำเร็จรูป (Cohen, 1977) โดยปรับปรุงขนาดตัวอย่างให้เหมาะสมกับงานวิจัยครั้งนี้จึงได้จำนวนทั้งหมด 130 ราย

2. เครื่องมือที่ใช้ในการวิจัยครั้งนี้ คือ แบบสอบถามเกี่ยวกับพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่น ซึ่งแบ่งออกเป็น 5 ตอน ดังนี้

ตอนที่ 1 ข้อมูลคุณลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม

ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

ตอนที่ 3 ประสบการณ์ในภัยคุกคามทางไซเบอร์

ตอนที่ 4 พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์

ตอนที่ 5 ข้อเสนอแนะเพิ่มเติมเกี่ยวกับพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์

3. การตรวจสอบคุณภาพเครื่องมือที่ใช้ในการวิจัย โดยการประเมินความตรงตามเนื้อหา (Content Validity) ด้วยการหาค่าดัชนีความสอดคล้อง (IOC) จากผู้เชี่ยวชาญทั้งหมด 3 คน โดยหาค่าเฉลี่ยนของคะแนนประเมินในข้อคำถามแต่ละข้อ พิจารณาเลือกข้อคำถามที่มีค่าคะแนน IOC อยู่ระหว่าง 0.67-1.00 จากนั้นนำแบบสอบถามทดลองใช้ (Try out) กับกลุ่มคนเจเนอเรชั่นแซดที่ไม่ใช่กลุ่มตัวอย่าง จำนวน 30 คน ส่วนของความรู้เลือกข้อคำถามที่มีค่าความยากง่ายระหว่าง 0.20-0.80 จากนั้นทดสอบความเชื่อมั่นของแบบสอบถามโดยคำนวณค่าสัมประสิทธิ์ครอนบรัคแอลฟา (Cronbach's alpha coefficient) ตัวแปรชุดประสบการณ์ในภัยคุกคามทางไซเบอร์ได้ค่าสัมประสิทธิ์ครอนบรัคเท่ากับ 0.851 ตัวแปรชุดพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ได้ค่าสัมประสิทธิ์ครอนบรัคเท่ากับ 0.923 ซึ่งเป็นไปตามเกณฑ์ค่าสัมประสิทธิ์ครอนบรัคแอลฟา จึงถือว่ามีความเชื่อมั่นของเครื่องมือวิจัยนี้พอเพียงที่สามารถนำไปเก็บรวบรวมข้อมูลต่อไป (Cortina, 1993; ชไมพร กาญจนกิจสกุล, 2555)

4. การเก็บรวบรวมข้อมูล ผู้วิจัยได้ดำเนินการขอหนังสือรับรองการพิจารณาจากคณะกรรมการจริยธรรมสำหรับโครงการวิจัยที่ทำในมนุษย์ มหาวิทยาลัยศรีนครินทรวิโรฒ หลังจากนั้นผู้วิจัยได้เก็บรวบรวมข้อมูลด้วยตนเอง โดยกระจายแบบสอบถามบน Google Form ผ่านสื่อสังคมออนไลน์ ตามกลุ่มตัวอย่างและจำนวนที่กำหนด

5. การจัดกระทำและการวิเคราะห์ข้อมูล ผู้วิจัยศึกษาดำเนินการนำแบบสอบถามที่ได้รับคำตอบแล้วมาวิเคราะห์ข้อมูลโดยใช้โปรแกรมสำเร็จรูปทางสถิติ วิเคราะห์ค่าสถิติเชิงพรรณนาของข้อมูลเบื้องต้นของกลุ่มตัวอย่าง หาค่าเฉลี่ย ค่าร้อยละ และส่วนเบี่ยงเบนมาตรฐาน ทดสอบสมมติฐานด้วยการวิเคราะห์สถิติเชิงอนุมาน เพื่อวิเคราะห์สมการถดถอยของตัวแปรที่มีอิทธิพลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามบนไซเบอร์ของเจเนอเรชั่นแซด หาค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างตัวแปรตามและตัวแปรพยากรณ์ ประกอบด้วยเพศซึ่งเป็นตัวแปรหุ่น (dummy variable) ความรู้และประสบการณ์ซึ่งเป็นตัวแปรต่อเนื่อง วิเคราะห์สถิติที่ระดับนัยสำคัญ 0.05

สรุปผลการวิจัย

1. ข้อมูลคุณลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม พบว่า กลุ่มตัวอย่างที่เป็นกลุ่มเจเนอเรชั่นแซด จำนวน 130 คน ส่วนใหญ่เป็นเพศหญิง จำนวน 71 คน (ร้อยละ 54.60) เกิดปี พ.ศ. 2540 จำนวน 64 คน (ร้อยละ 49.20) และประกอบอาชีพเป็นนิสิต/นักศึกษา จำนวน 56 คน (ร้อยละ 43.10)

2. การวิเคราะห์ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด พบว่า ข้อแบบทดสอบที่มีการตอบถูกมากที่สุด 3 อันดับ ได้แก่ ข้อที่ 3 เว็บไซต์ใดไม่มีความน่าเชื่อถือในเรื่องความปลอดภัย หากบังคับให้ผู้ใช้มีการกรอก Password จำนวน 94 คน (ร้อยละ72.3) รองลงมา คือ ข้อที่ 9 ข้อใดเป็นการรักษาความปลอดภัยของเราเตอร์ (Router) จำนวน 92 คน (ร้อยละ 70.8) และ ข้อที่ 4 ข้อใดคือวิธีการตั้งรหัสผ่านที่ดี จำนวน 91 คน (ร้อยละ 70) ตามลำดับ โดยมีค่าคะแนนเฉลี่ยของความรู้อยู่ที่ 5.54 คะแนน (ร้อยละ 46.17)

3. การวิเคราะห์ประสบการณ์ในภัยคุกคามทางไซเบอร์ของกลุ่มเจนเนอเรชั่นแซด พบว่า กลุ่มเจเนอเรชันแซดโดยรวมมีความคิดเห็นต่อประสบการณ์ในภัยคุกคามทางไซเบอร์ระดับปานกลาง ($\overline{X}$= 3.14) เมื่อทำการวิเคราะห์เป็นรายข้อ พบว่า ข้อที่มีค่าเฉลี่ยมากที่สุด คือ ข้อที่ 2 ท่านรับรู้ความเสี่ยงที่เกิดขึ้น หากถูกละเมิดในข้อมูลส่วนบุคคล ($\overline{X}$= 3.86) รองลงมา คือ ข้อ 6 ท่านรู้จักและเคยใช้ VPN ($\overline{X}$= 3.82) และข้อ 4 ท่านเคยได้รับอีเมลหลอกลวง (Phishing, Scams email) ($\overline{X}$= 3.76) ตามลำดับ ส่วนข้อที่มีค่าเฉลี่ยน้อยที่สุด คือ 10 ท่านเคยร่วมลงทุนกับผู้อื่นในการแลกเปลี่ยนสกุลเงินดิจิทัล ($\overline{X}$= 2.39)

4. การวิเคราะห์พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด พบว่า คนกลุ่มนี้มีพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์โดยเฉลี่ยในระดับมาก ($\overline{X}$= 3.90) เมื่อทำการวิเคราะห์เป็นรายข้อ พบว่า ด้านที่มีค่าเฉลี่ยมากที่สุด คือ ด้านการใช้งานอุปกรณ์เคลื่อนที่ ($\overline{X}$ = 4.28) รองลงมา คือ ด้านการใช้งานสื่อสังคมออนไลน์ ($\overline{X}$= 4.02) และด้านการใช้งานอุปกรณ์คอมพิวเตอร์ ($\overline{X}$= 3.91) ตามลำดับ ส่วนข้อที่มีค่าเฉลี่ยน้อยที่สุด คือ ด้านการตั้งค่ารหัสผ่าน ($\overline{X}$= 3.27)

5. การวิเคราะห์ปัจจัยที่มีอิทธิผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด พบว่า มีเพียงปัจจัยเดียวที่ส่งผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์อย่างมีนัยสำคัญทางสถิติ คือ ประสบการณ์ ในขณะที่เพศและความรู้ไม่มีผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ จึงใช้การวิเคราะห์สถิติโดยใช้ความถดถอยเชิงเดี่ยว เพื่อศึกษาความสัมพันธ์ระหว่างประสบการณ์กับพฤติกรรมในการดูแลและป้องกันตนเองจากภัยคุกคามทางไซเบอร์

6. การวิเคราะห์ความสัมพันธ์ระหว่างพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ในแต่ละด้านกับประสบการณ์ โดยประสบการณ์มีผลต่อพฤติกรรมในด้านการตั้งค่ารหัสผ่าน การจัดการข้อมูลส่วนบุคคล และการใช้งานอุปกรณ์คอมพิวเตอร์ โดยเมื่อพิจารณาความสัมพันธ์ระหว่างพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ในภาพรวม พบว่าประสบการณ์มีผลต่อความสัมพันธ์ระหว่างพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

อภิปรายผลการวิจัย

จากผลการศึกษา เรื่อง พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด สามารถอภิปรายผลการวิจัยได้ดังนี้

1. พฤติกรรมการป้องตนเองจากภัยคุกคามทางไซเบอร์ของเจเนอเรชั่นแซด โดยรวมอยู่ในระดับมาก อาจเป็นเพราะกลุ่มเจเนอเรชั่นแซดเป็นวัยที่อยู่ในช่วงกำลังศึกษาจนถึงช่วงเริ่มต้นการทำงานมีประมาณช่วงเวลาในการใช้งานบนโลกออนไลน์ตลอด 24 ชั่วโมงจากกิจกรรมต่าง ๆ ในการใช้ชีวิตประจำวันในยุคที่มีนวัตกรรมทางเทคโนโลยีที่ทันสมัย ทำให้มีโอกาสถูกก่อกวนและโจมตีที่มาทางไซเบอร์ที่หลากหลายรูปแบบ จึงส่งผลทำให้เกิดพฤติกรรมตระหนักในการป้องกันตนเองจากถูกละเมิดข้อมูลส่วนบุคคลและข้อมูลสำคัญต่าง ๆ โดยประสบการณ์ อาจเกิดจากการได้พบเจอภัยคุกคามทางไซเบอร์รูปแบบใหม่ๆ ในปัจจุบัน สอดคล้องกับสุธารเทพ รุณเรศ (2561) พบว่า ผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานครมีความตระหนักในภัยคุกคามทางไซเบอร์อยู่ในระดับมาก และเมธาพร ธรรมศิริ และ

ศิรภัสสรศ์ วงศ์ทองดี (2565) พบว่า การตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรของบริษัทเอกชนแห่งหนึ่งที่อยู่ในกรุงเทพมหานครอยู่ในระดับมากเช่นเดียวกัน ส่วนด้านที่มีค่าเฉลี่ยน้อยที่สุด คือ ด้านการตั้งค่ารหัสผ่าน อาจเป็นเพราะการใช้ชีวิตบนระบบดิจิทัลทำให้เจเนอเรชั่นแซดต้องเข้าใช้แอปพลิเคชั่นหลายระบบ ซึ่งแต่ละระบบมีข้อบังคับการใช้รหัสผ่านที่แตกต่างกัน จึงเป็นเรื่องยากที่จะต้องจดจำรหัสผ่านทั้งหมดหากต้องเลือกใช้รหัสที่มีความซับซ้อนยากต่อการคาดเดา สอดคล้องกับ Titiakarawongse และ Boonkrong (2023) พบว่า ในทางปฏิบัติคนส่วนใหญ่ยังคงเลือกใช้รหัสผ่านที่สะดวกต่อการจดจำ

2. จากการศึกษาอิทธิพลของเพศ ความรู้ และประสบการณ์ที่มีผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด สามารถอภิปรายผลการวิจัยตามสมมติฐานที่ตั้งไว้ ดังนี้

2.1 ประสบการณ์มีอิทธิพลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซดอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งเป็นไปตามสมมติฐาน แสดงว่าหากกลุ่มเจเนอเรชั่นแซดผ่านประสบการณ์ตกเป็นเหยื่อจากภัยคุกคามทางไซเบอร์จะมีพฤติกรรมที่ไม่เสี่ยงต่ออันตรายซึ่งอาจจะเกิดขึ้น รู้เท่าทันเหตุการณ์ผิดปกติที่เกิดจากอาชญากรทางไซเบอร์ ไม่หลงคลิกอีเมลหลอกลวง (Phishing email, Scams email) ระมัดระวังในการให้ข้อมูลส่วนตัว เช่น เลขบัตรประชาชนหรือเลขบัตรเครดิต เป็นต้น กลุ่มคนที่มีพฤติกรรมระมัดระวังอันตรายต่อภัยคุกคามทางไซเบอร์อาจมาจากประสบการณ์การถูกโจมตีบัญชีอีเมลหรือสื่อสังคมออนไลน์ เคยหลงคลิกเข้าไปในเว็บไซต์หลอกลวง เคยโดนมัลแวร์เข้ามาก่อกวนการทำงานระบบคอมพิวเตอร์ เป็นต้น ซึ่งสอดคล้องกับงานวิจัย Ameen และคนอื่น ๆ (2020) กล่าวว่าผู้ที่มีประสบการณ์จากภัยคุกคามสามารถรับรู้ถึงความเสี่ยงและผลเสียจากอันตรายทางไซเบอร์ ทำให้ตระหนักถึงการใช้อุปกรณ์เคลื่อนที่ไม่ให้ข้อมูลส่วนบุคคลรั่วไหลไปสู่สาธารณะ

2.2 เพศไม่มีอิทธิพลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด ซึ่งไม่เป็นไปตามสมมติฐานของการวิจัยครั้งนี้ แสดงว่าการมีเพศที่แตกต่างกันไม่ได้ส่งผลพฤติกรรมความความปลอดภัยจากภัยคุกคามทางไซเบอร์ที่แตกต่างกัน โดยสอดคล้องกับงานวิจัยของ Bona และ Paci (2020); Buckley, Lottridge, Murphy, และ P.M. (2023); Lévesque, Chiasson, Somayaji, และ Fernandez (2018) กล่าวว่า อายุและเพศไม่มีความสัมพันธ์กับความเสี่ยงในการคลิกลิงก์จากอีเมลฟิชชิ่งและการคลิกดาวน์โหลดเอกสารที่อาจมีมัลแวร์เข้ามาโจรกรรมข้อมูลส่วนตัว ข้อมูลธุรกรรมทางการเงิน หรือข้อมูลขององค์กร อย่างไรก็ตาม ผลการวิจัยนี้ขัดแย้งกับงานวิจัย Anwar และคนอื่น ๆ (2017) กล่าวว่า เพศส่งผลต่อพฤติกรรมด้านความปลอดภัยทางไซเบอร์

โดยเพศหญิงมีค่าเฉลี่ยในทักษะทางคอมพิวเตอร์และพฤติกรรมการดูแลความปลอดภัยบนโลกออนไลน์ต่ำกว่าค่าเฉลี่ยของเพศชาย

2.3 ความรู้ไม่มีอิทธิพลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด ซึ่งไม่เป็นไปตามสมมติฐาน แสดงว่ากลุ่มเจเนอเรชั่นแซดเป็นกลุ่มวัยที่มีเทคโนโลยีเป็นส่วนหนึ่งของชีวิต มีความสามารถในการเรียนรู้และปรับตัวเข้ากับการแพร่กระจายทางเทคโนโลยีได้อย่างรวดเร็ว (Salubi และคนอื่น ๆ, 2018; Sayavaranont และ Wannapiroon, 2017) ทั้งการสืบค้นข้อมูลข่าวสาร การทำกิจกรรมบนระบบดิจิทัล ทำให้มีความรู้เกี่ยวกับการใช้เทคโนโลยีด้านต่างๆ ทำกิจกรรมบนเว็บไซต์และสื่อสังคมออนไลน์จนเกิดเป็นพฤติกรรมคุ้นชินบนโลกไซเบอร์ จึงมีพฤติกรรมที่ละเลยต่อการใช้ระบบออนไลน์อย่างปลอดภัย ไม่ระวังต่อการป้องกันข้อมูลส่วนตัวของตนเองจากความเสี่ยงทางไซเบอร์ ซึ่งกลายเป็นความผิดพลาดของมนุษย์ (Human error) จากการกระทำที่อาจไม่ได้ตั้งใจหรือขาดความยั้งคิดจนทำให้เกิดความเสียหายขึ้น ปล่อยให้ตนเองถูกละเมิดความปลอดภัยทั้งด้านข้อมูลและอุปกรณ์ ตั้งแต่การดาวน์โหลดไฟล์แนบที่มีมัลแวร์ติดมาด้วย การตั้งรหัสผ่านที่คาดเดาได้ง่าย ไปจนถึงการคลิกอนุญาตสิทธิ์ให้เปิดเผยข้อมูลอย่างไม่ระมัดระวัง หรือมีความรู้ว่าการตั้งรหัสผ่านที่ดีควรใช้รหัสที่มีความซับซ้อน แต่เมื่อสร้างบัญชีผู้ใช้บนระบบออนไลน์กลับเลือกใช้รหัสผ่านที่ง่ายต่อการจดจำและคาดเดา ผลการวิจัยนี้ขัดแย้งกับงานวิจัย Kovacevic และคนอื่น ๆ (2020) และกิติยา วิสิฐพงศ์พันธ์, ชูเกียรติ บุญก่อเกื้อ, กิตติพงศ์ อยู่นิรันดร์, และ นลินภัสร์ บำเพ็ญ (2565) พบว่า ความรู้เป็นปัจจัยที่สำคัญต่อการตระหนักถึงความปลอดภัยทางไซเบอร์ของนักศึกษา อย่างไรก็ตาม ความรู้ไม่มีความสัมพันธ์กับพฤติกรรมการตั้งค่ารหัสผ่าน สอดคล้องกับ Titiakarawongse และ Boonkrong (2023) พบว่า แม้คนส่วนใหญ่จะมีความรู้พื้นฐานในการตั้งรหัสผ่านที่ซับซ้อนเพื่อความปลอดภัย แต่ในทางปฏิบัติก็ยังคงเลือกใช้รหัสผ่านที่ง่ายต่อการจดจำ

ข้อเสนอแนะ

งานวิจัยเรื่องพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด มีข้อเสนอแนะดังนี้

1. ความสะดวกของการทำธุรกรรมบนระบบออนไลน์ทำให้เป็นช่องทางของมิจฉาชีพในการฉ้อโกง พฤติกรรมการดูแลตนเองจากภัยคุกคามทางไซเบอร์จึงจำเป็นไม่เฉพาะกับเจเนอเรชั่นแซดเท่านั้น แต่จำเป็นต่อประชาชนในทุกช่วงวัยไม่ให้ตกเป็นเหยื่อของมิจฉาชีพทางไซเบอร์

2. ผลการวิจัยพบความสัมพันธ์ของประสบการณ์กับพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ จึงควรสร้างความตระหนักให้ประชาชนคำนึงถึงอันตรายทางไซเบอร์

ที่อาจเกิดขึ้นได้จากการทำธุรกรรมในทุกระบบงาน แม้ว่าระบบนั้นจะมีการออกแบบความปลอดภัยได้มาตรฐานอยู่แล้ว อาทิระบบธุรกรรมทางธนาคาร ผู้ได้รับผลกระทบจากภัยคุกคามจึงควรถ่ายทอดประสบการณ์เพื่อเป็นกรณีศึกษาให้ผู้อื่นตระหนักถึงวิธีการหลอกลวง และผลกระทบที่เกิดขึ้นจริงไม่ว่าจะเป็นผลกระทบต่อบุคคลหรือสังคม

3. ผลการวิจัยไม่พบการมีนัยสำคัญของความรู้ที่มีผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ แสดงให้เห็นถึงการให้ความรู้เพียงอย่างเดียวอาจจะไม่เพียงพอต่อการสร้างพฤติกรรมในการดูแลตนเองจากภัยคุกคาม สถานศึกษาให้ควรจัดการเรียนการสอนแบบกรณีศึกษาโดยถ่ายทอดประสบการณ์จากภัยทางไซเบอร์ที่เกิดขึ้นจริงในสังคม ให้ผู้เรียนตระหนักในผลเสียที่จะตามมาหากมีพฤติกรรมที่เสี่ยงต่อความปลอดภัยทางไซเบอร์

4. ผลจากการวิจัยนี้เป็นการศึกษาจากกลุ่มตัวอย่างของเจเนอเรชั่นแซด คือ ผู้ที่เกิดระหว่างปี พ.ศ. 2540 ถึง พ.ศ. 2546 เท่านั้น ควรศึกษากลุ่มเจเนอเรชั่นอื่นๆ เพิ่มขึ้นเพื่อสามารถเปรียบเทียบหรือได้มองเห็นมุมมองใหม่ๆ เกี่ยวกับด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์

ข้อเสนอแนะสำหรับการทำวิจัยครั้งต่อไป

1. ควรขยายกลุ่มเจเนอเรชั่นที่ทำการศึกษา เพื่อให้เห็นความหลากหลายของพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ในทุกช่วงอายุ

2. ควรมีการศึกษาปัจจัยที่มีอิทธิพลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ในมิติอื่นๆ ได้แก่ ปัจจัยการรับรู้เทคโนโลยี อาชีพ ช่วงอายุ และทัศนคติ

3. การวิจัยครั้งถัดไปควรใช้วิธีการวิจัยแบบผสมผสานวิธี ทั้งในเชิงปริมาณ และเชิงคุณภาพ เพื่อให้ได้คำตอบสาเหตุของความสัมพันธ์ของตัวแปรได้ลึกซึ้งและชัดเจนมากยิ่งขึ้น

4. ในการวิจัยครั้งถัดไปเกี่ยวกับภัยคุกคามทางไซเบอร์ ควรใช้วิธีการศึกษาเชิงลึกกับกลุ่มผู้ที่เคยมีประสบการณ์กับภัยคุกคามทางไซเบอร์โดยใช้วิธีการสัมภาษณ์ ซึ่งเป็นวิธีการเชิงคุณภาพที่ช่วยให้ได้ข้อมูลลึกซึ้งเกี่ยวกับประสบการณ์และความรู้ของกลุ่มเป้าหมาย โดยการสัมภาษณ์ผู้เชี่ยวชาญหรือบุคคลภายในกลุ่มที่มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ จะช่วยให้เข้าใจเพิ่มเติมเกี่ยวกับประสบการณ์ที่เคยเกิดขึ้น และสามารถระบุแนวทางแก้ไขหรือป้องกันที่เหมาะสมได้ อีกทั้งได้มุมมองจากการถูกคุกคามทางไซเบอร์หลากหลายมิติ

บรรณานุกรม

Altuna, J., Martinez de Morentin, J. I., และ Arkaitz, L. (2020). The impact of becoming a parent about the perception of internet risk behaviors. *Children and youth services review,* 110(2020).

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

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

Bona, M. D., และ Paci, F. (2020). *A real world study on employee' susceptibility to phishing attacks*. Paper presented at the Proceedings of the 15th International Conference on Availability, Reliability and Securitys.

Buckley, j., Lottridge, D., Murphy, J. G., และ P.M., C. (2023). Indicators of employee phishing email behaviours: Intuition, elaboration, attention, and email typology. *International journal of human - Computer studies,* 172, 102996.

Cohen, J. (1977). *Statistical power for the behavioral sciences* (2nd ed.). New York: Academic Press.

Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of applied psychology,* 78(1), 98.

Dawson, J., และ Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skill for successful cyber performance. *Frontier in psychology,* 9, 744.

Debb, S. M., Schaffer, D. R., และ Colson, D. G. (2020). A reverse digital divide: comparing information security behaviors of generation Y and generation Z adults. *International Journal of Cybersecurity Intelligence & Cybercrime,* 3(1), 42-55.

Donalds, C., และ Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management,* 51, 102056.

European union agency for cybersecurity. (2021). *Enisa threat landscape* 2021.

Frank, I., และ Odunayo, E. (2013). Approach to cyber security issues in nigeria: challenges and solution. *(IJCRSEE),* 1(1).

Fry, R., และ Parker, K. (2018). *Early benchmarks show "Post-Millennials" on track to be most diverse, best-educated generation yet*.

Gillam, A. R., และ Foster, W. T. (2020). Factor affecting risking cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in human behavior,* 108(2020).

Glass, A. (2007). Understanding genertional differences for competitive success. *Industrial and commercial training* 39(2), 98-103.

Hakak, S., Khan, W. Z., Imran, M., Choo, K.-K. R., และ Shoaib, M. (2020). Have you been a victim of COVID-19-related cyber incidents? survery, taxonomy and mitigation strategies. *IEEE Acess,* 8(2020).

Howe, N., และ Strauss, W. (2008). *Millennials & K-12 school*: LifeCourse Associates.

Kovacevic, A., Putnik, N., และ Toskovic, O. (2020). Factors Related to Cyber Security Behavior. *IEEE access,* 8, 125140-125148.

Lesjak, A., Martinez de Morentin, J. I., Altuna, J., และ Amenabar, N. (2017). Teenagers' perception of risk behaviors regrading digital technologies. *Computers in human behavior,* 68(2017), 395-402.

Lévesque, F. L., Chiasson, S., Somayaji, A., และ Fernandez, J. M. (2018). Technological and human factors of malware attack: A compter security clinical trial approach. *ACM Transactions on Privacy and Security,* 21(4), 1-30.

Levickaite, R. (2010). Generation X,Y,Z: How social networks form the concept of the world without borders (the case of Lithuania). *Creativity Studies,* 3(11), 170-183.

Li, L., He, W., Xu, L., Ash, I., Awar, M., และ Yuan, X. (2019). Investigatng the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *Internationl journal of information management,* 45(2019), 13-24.

Liu, C., Wang, N., และ Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management,* 54, 102152.

Ma, K. W. F., และ Mckinnon, T. (2021). COVID-19 and cyber fraud: emerging threats

during the pandemic. *Journal of financial crime*.

Mannheim, K. (1952). *Essays on the sociology of knowledge*. London: Routledge and Kegan Paul.

McClain, C., Vogels, E. A., Perrin, A., Sechopoulos, S., และ Rainie, L. (2021). *The internet and the pandemic*.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., และ Pattinson, M. (2017). Individual differences and information security awarreness. *Computers in human behavior,* 69(2019), 151-156.

McGuire, M., และ Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report,* 75.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., และ Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports,* 23(4), 1-9.

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in society,* 58(2019).

National academies of sciences engineering and medicine. (2020). *Are generational categories meaningfl distinctions for workforce management?* Washington, DC: The national academies press.

Pawlicka, A., Choras, M., Pawlicki, M., และ Kozik, R. (2021). A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic. *Business Horizons,* 64(2021), 729-734.

Priporas, C.-V., Stylos, N., และ Fotiadis, A. K. (2017). Generation Z consumer' expectations of interactions in smart retailing: A future agenda. *Computers in human behavior,* 77(2017), 347-381.

Rashid, Z., Noor, U., และ Altmann, J. (2021). Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. *Future generation computer system,* 124(2021), 436-466.

Ready Campaign. (2021). Cybersecurity. https://www.ready.gov/cybersecurity

Rodríguez-Priego, N., van Bavel, R., Vila, J., และ Briggs, P. (2020). Framing Effects on Online Security Behavior. *Frontiers in Psychology,* 11(2833).

Salubi, O. G., Ondari-Okemwa, E., และ Nekhwevha, F. (2018). Utilisation of library information resources among Generation Z students: Facts and fiction. *Publications,* 6(2), 16.

Sayavaranont, P., และ Wannapiroon, P. (2017). Why Generation Z' Digital Literacy can be Improved through Digital Storytelling? *Journal of Mass Communication Technology, RMUTP,* 1(2), 64-73.

Smith-Trudean, P. (2016). Generation Z nurses have arrived. Are you ready? *New hampshire nursing news,* 40, p. 30.

Timmers, P. (2019). Ethics of AI and cybersecurity when sovereight is at Stake. *Minds and machines,* 29(2019), 635-645.

Titiakarawongse, C., และ Boonkrong, S. (2023). A Study of Password Management Behaviors of Young People. *Applied science and engineering progress,* 16(4), 1-16.

Turner, A. (2015). Generatin Z: Technology and social interest. *Journal of individual psychology,* 71(2), 103-113.

Yu, L., Li, H., He, W., Wang, F.-K., และ Jiao, S. (2020). A meta-analysis to explore privacy cognition and information disclosure of internet users. *International journal of Information management,* 51.

Zemke, R. (2001). Here come the millennials. *Training,* 38(7), 44-49.

Zwilling, M., Klien, G., Lesjak, G., Wiechetek, L., Cetin, F., และ Basim, H. N. (2020). Cyber security awareness, knowledge and behavior : a comparative study *Journal of computer infomation system*.

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2562a, 27 พฤษภาคม). พระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 (เล่ม 136 ตอนที่ 69 ก, น. 20-51). http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2562b, 27 พฤษภาคม). พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (เล่ม 136 ตอนที่ 69 ก, น. 52-95).

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

กิติยา วิสิฐพงศ์พันธ์, ชูเกียรติ บุญก่อเกื้อ, กิตติพงศ์ อยู่นิรันดร์, และ นลินภัสร์ บำเพ็ญ. (2565). ปัจจัยที่ส่งต่อการตระหนักรู้ถึงความปลอดภัยทางไซเบอร์ของนักศึกษามหาวิทยาลัย. วารสารวิชาการวิทยาศาสตร์ มหาวิทยาลัยราชภัฏจันทรเกษม, 32(1), 33-38.

คณัญญา อิ่มใจ, และ วิภากร วัฒนสินธุ์. (2566). พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่น *Z*. Paper presented at the การประชุมวิชาการ และเผยแพร่ผลงานวิจัยคัดสรรระดับชาติครั้งที่ 7 และระดับนานาชาติครั้งที่ 3 "ความร่วมมือเพื่อการเปลี่ยนแปลงทางการศึกษาในอนาคต" (APHEIT-EDU 2023), พัทยา จังหวัดชลบุรี.

ชไมพร กาญจนกิจสกุล. (2555). ระเบียบวิธีวิจัยทางสังคมศาสตร์ (1). ตาก: โพรเจ็คท์ ไฟฟ์-โฟว์ จำกัด.

ชัยพร เขมะภาตะพันธ์. (2564). เตือนภัย!! เว็บดังติดมัลแวร์ขุดเงินคริปโต หลังแฮกเกอร์หัวใสฝังคริปโตแจ๊คกิ้งให้ผู้ใช้งานขุดเงินแทน. สยามรัฐออนไลน์. https://siamrath.co.th/n/220125

ธนาคารแห่งประเทศไทย. (2563). ทำความรู้จักกับ CBDC และคามคืบหน้าในประเทศไทย. *BOT* พระสยาม *Magazine*, 4, 36-37.

นงลักษณ์ วิรัชชัย. (2555). การกำหนดขนาดตัวอย่างในการทดสอบสมมติฐานวิจัย. Paper presented at the วิธีการที่ถูกต้องและทันสมัยในการกำหนดขนาดตัวอย่างในโครงการ Research zone, กรุงเทพ: สำนักงานคณะกรรมการวิจัยแห่งชาติ (วช.). https://lllskill.com/web/files/GPower.pdf

บุญชม ศรีสะอาด. (2545). การวิจัยเบื้องต้น (ฉบับปรับปรุง) (7). กรุงเทพฯ: สุวีริยาสาส์น.

มหาวิทยาลัยเชียงใหม่. (2564). Phishing. สืบค้นจาก https://network.cmu.ac.th/wiki/index.php/Phishing

เมธาพร ธรรมศิริ, และ ศิรภัสสรศ์ วงศ์ทองดี. (2565). ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร. วารสารวิชาการไทยวิจัยและการจัดการ, 2(3).

ไลฟ์สไตล์. (2564). Cryptocurrency คืออะไร? ทำความเข้าใจง่ายๆ ฉบับนักลงทุนมือใหม่. ไทยรัฐออนไลน์. https://www.thairath.co.th/lifestyle/money/2121706

วารินทร์ เคียร่า, สุธี จันทรพันธุ์, และ Fung, C. C. (2560a). การศึกษาพฤติกรรมการระวังป้องกันภัยคุกคามบนสมาร์ทโฟน. วารสารมนุษยศาสตร์และสังคมศาสตร์ นายเรืออากาศ, 5(5), 50-59.

วารินทร์ เคียร่า, สุธี จันทรพันธุ์, และ Fung, C. C. (2560b). พฤติกรรมของคนไทยในการป้องกันสมาร์ทโฟนจากภัยคุกคามทางไซเบอร์. วารสารสถาบันวิชาการป้องกันประเทศ, 8(2), 86-100.

วิวัฒน์ รุ่งแสนสุขสกุล. (2564, 8 กันยายน). ทำไม Ransomeware ระบาดหนัก เชื่อใจแฮกเกอร์ได้ไหม ถ้ายอมจ่ายค่าไถขอคืนข้อมูล. ไทยรัฐออนไลน์.

ศิริรตน์ ศรีสว่าง. (2558). ปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์. (วิทยาศาสตร์มหาบัณฑิต). มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, ส. (2561, 13 ตุลาคม). ยุทธศาสตร์ชาติ พ.ศ. 2561-2580 (เล่ม 135 ตอนที่ 82 ก, น. 1-71). http://www.ratchakitcha.soc.go.th/DATA/PDF/2561/A/082/T_0001.PDF

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2563). รู้จัก Phishing และการป้องกัน. สืบค้นจาก https://www.etda.or.th/th/Our-Service/ThaiCERT/Incident-Coordination/Information/Published-documents/General/papers-general/รจก-Phishing-และการปองกน.aspx

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2565). รายงานผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2565. In. https://www.etda.or.th/th/Useful-Resource/publications/iub2022.aspx

สำนักงานสถิติแห่งชาติ. (2563). จำนประชากรจากทะเบียน จำนวนตามอายุ เพศ และจังหวัด พ.ศ. 2563. http://statbbi.nso.go.th/staticreport/page/sector/th/01.aspx

สำนักบริหารเทคโนโลยีสารสนเทศ. (2563). Ransomware คืออะไร? สืบค้นจาก https://www.it.chula.ac.th/ransomware-คืออะไร/

สุธารเทพ รุณเรศ. (2561). ปัจจัยที่มีผลต่อการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร. (สารนิพนธ์มหาบัณฑิต). มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

อิสริยา ปาริชาติกานนท์, และ อัจศรา ประเสริฐสิน. (2560). ปัจจัยเชิงสาเหตุที่มีอิทธิพลต่อพฤติกรรมป้องกันตนเองจากภัยคุกคามทางอินเทอร์เน็ตของนิสิตระดับปริญญาตรี มหาวิทยาลัยศรีนครินทรวิโรฒ. วารสารบรรณศาสตร์ มศว, 10(1), 77-91.

อุดม ประตาทะยัง. (2560). แนวทางที่เหมาะสมในการะพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์. (วปอ.รุ่นที่ 60). วิทยาลัยป้องกันราชอาณาจักร, กรุงเทพฯ.

ภาคผนวก

ภาคผนวก ก
ใบรับรองจริยธรรมในการวิจัย

หนังสือรับรองจริยธรรมการวิจัยของข้อเสนอการวิจัย
เอกสารข้อมูลคำอธิบายสำหรับผู้เข้าร่วมการวิจัยและใบยินยอม
หมายเลขข้อเสนอการวิจัย SWUEC-G- 081/2565E

ข้อเสนอการวิจัยนี้และเอกสารประกอบของข้อเสนอการวิจัยตามรายการแสดงด้านล่าง ได้รับการพิจารณาจากคณะกรรมการจริยธรรมสำหรับพิจารณาโครงการวิจัยที่ทำในมนุษย์ มหาวิทยาลัยศรีนครินทรวิโรฒแล้ว คณะกรรมการฯ มีความเห็นว่าข้อเสนอการวิจัยที่จะดำเนินการมีความสอดคล้องกับหลักจริยธรรมสากล ตลอดจนกฎหมาย ข้อบังคับและข้อกำหนดภายในประเทศ จึงเห็นสมควรให้ดำเนินการวิจัยตามข้อเสนอการวิจัยนี้ได้

ชื่อโครงการวิจัยเรื่อง: พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด
ชื่อผู้วิจัยหลัก: นางสาว คณัญญา อิ่มใจ
สังกัด: คณะมนุษยศาสตร์
เอกสารที่รับรอง:
1. แบบเสนอโครงการวิจัย
2. โครงการวิจัย
3. เอกสารชี้แจงผู้เข้าร่วมการวิจัย
4. หนังสือให้ความยินยอมเข้าร่วมโครงการวิจัย

เอกสารที่พิจารณาทบทวน

1. แบบเสนอโครงการวิจัย	ฉบับที่ 2 วัน/เดือน/ปี 22 กุมภาพันธ์ 2565
2. โครงร่างการวิจัย	ฉบับที่ 2 วัน/เดือน/ปี 22 กุมภาพันธ์ 2565
3. เอกสารชี้แจงผู้เข้าร่วมการวิจัย	ฉบับที่ 2 วัน/เดือน/ปี 22 กุมภาพันธ์ 2565
4. หนังสือให้ความยินยอมเข้าร่วมโครงการวิจัย	ฉบับที่ 2 วัน/เดือน/ปี 22 กุมภาพันธ์ 2565

(ลงชื่อ).....
(ผู้ช่วยศาสตราจารย์ ดร.ทันตแพทย์หญิงณปภา เอี่ยมจิรกุล)
กรรมการและเลขานุการคณะกรรมการจริยธรรมสำหรับพิจารณาโครงการวิจัยที่ทำในมนุษย์

(ลงชื่อ).....
(แพทย์หญิงสุรีพร ภัทรสุวรรณ)
ประธานคณะกรรมการจริยธรรมสำหรับพิจารณาโครงการวิจัยที่ทำในมนุษย์

หมายเลขรับรอง : SWUEC/E/G-081/2565
วันที่ให้การรับรอง : 22/02/2565
วันหมดอายุใบรับรอง : 22/02/2566

ที่ อว 8718/

มหาวิทยาลัยศรีนครินทรวิโรฒ
สุขุมวิท 23 กรุงเทพฯ 10110

22 กุมภาพันธ์ 2565

เรื่อง ขอแจ้งผลการพิจารณาโครงการวิจัยเลขที่ SWUEC-G- 081/2565E

เรียน นางสาว คณัญญา อิ่มใจ

สิ่งที่ส่งมาด้วย ใบรับรองโครงการวิจัย SWUEC/E/G-081/2565

ตามที่ท่านได้ส่งโครงร่างการวิจัยเรื่อง พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด โครงการวิจัยเลขที่ SWUEC-G 081/2565E เพื่อรับการพิจารณาจากคณะกรรมการจริยธรรมสำหรับพิจารณาโครงการวิจัยที่ทำในมนุษย์ นั้น

คณะกรรมการจริยธรรมสำหรับพิจารณาโครงการวิจัยที่ทำในมนุษย์ ได้พิจารณาโครงการวิจัยดังกล่าว บัดนี้ คณะกรรมการฯ ให้การรับรองโครงการวิจัยดังกล่าวแล้วเมื่อวันที่ 22 กุมภาพันธ์ 2565 รายละเอียดดังนี้

Certificate Number	SWUEC/E/G-081/2565
Date of Approval	22 กุมภาพันธ์ 2565 (อายุใบรับรองโครงการวิจัย 12 เดือน)
Date of Expiration	22 กุมภาพันธ์ 2566
Continuing Review	ทุก 12 เดือน (ครบกำหนดส่งรายงานครั้งแรก วันที่ 22 กุมภาพันธ์ 2566)

ในการนี้ คณะกรรมการจริยธรรมสำหรับพิจารณาโครงการวิจัยที่ทำในมนุษย์ ใคร่ขอความกรุณาให้ผู้วิจัยส่งรายงานความก้าวหน้าของการวิจัยและต่ออายุการรับรองก่อนกำหนดวันหมดอายุ 30 วัน เพื่อให้เป็นไปตามวิธีดำเนินการมาตรฐาน (SOPs version 2.0) ของคณะกรรมการฯ ทั้งนี้รายละเอียดของเอกสารที่ให้การรับรองตามที่ปรากฏใน Certificate of Approval (Certificate Number SWUEC/E/G-081/2565) ที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบและดำเนินการต่อไป

ขอแสดงความนับถือ

(แพทย์หญิงสุรีพร ภัทรสุวรรณ)
ประธานคณะกรรมการจริยธรรมสำหรับพิจารณาโครงการวิจัยที่ทำในมนุษย์

บัณฑิตวิทยาลัย
มหาวิทยาลัยศรีนครินทรวิโรฒ
โทรศัพท์ 0-2649-5000 ต่อ 12430
โทรสาร 0-2259-1822

ภาคผนวก ข
เครื่องมือที่ใช้ในการวิจัย

แบบสอบถาม

งานวิจัยเรื่อง พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

ผู้วิจัย นางสาวคณัญญา อิ่มใจ
นิสิตระดับปริญญาโท หลักสูตร ศศ (สารสนเทศศึกษา) .ม.
มหาวิทยาศรีนครินทรวิโรฒ

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด
2. เพื่อศึกษาอิทธิพลของเพศ ความรู้ และประสบการณ์ที่มีผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

นิยามศัพท์เฉพาะ

ความรู้ หมายถึง การที่บุคคลในเจนเนอเรชั่นแซดมีความรู้ด้านความปลอดภัยในการป้องกันตนเองภัยคุกคามทางไซเบอร์ ซึ่งครอบคลุมถึงอันตรายจากภัยคุกคามที่เข้ามาบนระบบไซเบอร์ รวมถึงผลกระทบจากการถูกโจมตีและก่อกวนทางไซเบอร์ การตรวจสอบและเข้าถึงเว็บไซต์ที่มีความปลอดภัย วิธีการป้องกันช่องโหว่ทางไซเบอร์โดยการดูแลและสังเกตการทำงานของอุปกรณ์อิเล็กทรอนิกส์ และวิธีการตั้งค่าระดับความปลอดภัยของข้อมูลส่วนบุคคลบนโลกไซเบอร์ทุกประเภท

ภัยคุกคามบนไซเบอร์ หมายถึง ภัยคุกคามความปลอดภัยที่เกิดจากผู้คุกคามทางไซเบอร์ประสงค์ต่อข้อมูลส่วนบุคคล (Data theft) สินทรัพย์ เป็นต้น ซึ่งเป็นภัยคุกคามที่ส่งผลกระทบที่มาจากการกระทำผิดพลาดของเจ้าของข้อมูล(Human error) การทำลายอุปกรณ์อิเล็กทรอนิกส์ การรบกวนการเข้าถึงข้อมูลหรือการทำงานของอุปกรณ์อิเล็กทรอนิกส์ สินทรัพย์ทางออนไลน์ การปลอมแปลงข้อมูลส่วนบุคคล เป็นต้น

ภัยคุกคามข้อมูลส่วนบุคคล หมายถึง ภัยคุกคามบัญชีผู้ใช้บนโลกไซเบอร์ (Online account) ที่จำเป็นต้องใช้ข้อมูลส่วนบุคคลในการระบุตัวตนไปถึงเจ้าของข้อมูลได้ เช่น ชื่อ-นามสกุล แชร์ตำแหน่งที่ตั้ง เลขประจำตัวประชาชน เบอร์โทรศัพท์ เลขบัญชีธนาคาร สินทรัพย์ออนไลน์ รหัสผ่าน ประวัติการสืบค้น ข้อมูลบนโปรไฟล์สื่อสังคมออนไลน์ ประวัติทางการแพทย์

เป็นต้น ซึ่งทำให้เกิดช่องโหว่จนนำไปสู่การโจรกรรมข้อมูลส่วนบุคคลได้ง่าย เช่น มัลแวร์ แรนซัมแวร์ ฟิชชิง คริปโตแจ็คกิ้ง เป็นต้น

เจเนอเรชั่นแซด (Generation Z) หมายถึง กลุ่มอายุในช่วงที่สังคมเกิดความก้าวหน้าทางเครือข่ายอินเทอร์เน็ตและเทคโนโลยีที่ถูกพัฒนาอย่างต่อเนื่องที่เข้ามามีบทบาทในชีวิตประจำวัน ส่งผลทำให้เกิดการละเลยการดูแลและป้องกันตนเองจากการคุกคามที่เข้ามาบนระบบไซเบอร์ โดยเป็นกลุ่มที่เกิดระหว่างปี พ.ศ. 2540 – 2546 (Fry และ Parker, 2018)

คำชี้แจงสำหรับผู้ตอบแบบสอบถาม แบบสอบถามแบ่งเป็น 4 ตอน ดังนี้

ตอนที่ 1 ข้อมูลคุณลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม

ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

ตอนที่ 3 ประสบการณ์ในภัยคุกคามทางไซเบอร์

ตอนที่ 4 พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์

ตอนที่ 5 ข้อเสนอแนะเพิ่มเติมเกี่ยวกับพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์

ตอนที่ 1 ข้อมูลคุณลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม

คำชี้แจง ให้ทำเครื่องหมาย ✓ หน้าหมายเลขคำตอบหรือเขียนคำตอบในช่องว่างที่ตรงกับความเป็นจริงของท่าน

1.1 เพศ [1] ชาย [2] หญิง

1.2 ปีเกิด [1] 2540 [2] 2541 [3] 2542
[4] 2543 [5] 2545 [6] 2546

1.3 อาชีพ [1] นิสิต/นักศึกษา [2] ข้าราชการ/รัฐวิสาหกิจ/พนักงานราชการ
[3] ลูกจ้าง/เอกชน/ธุรกิจส่วนตัว [4] อื่นๆ ระบุ…….

ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

คำชี้แจง ให้ทำเครื่องหมาย✓ หน้าหมายเลขคำตอบหรือเขียนคำตอบในช่องว่างที่ตรงกับความเป็นจริงของท่าน

2.1 การหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมที่มีข้อความซึ่งทำให้ผู้เสียหายอ่านแล้วหลงเชื่อเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่นๆ เป็นประเภทของการโจมตีทางไซเบอร์ในข้อใด

[1] โทรจัน (Trojan)

[2] มัลแวร์ (Malwave)

[3] ฟิชชิ่ง (Phishing)

[4] คริปโตแจ็คกิ้ง (cryptojacking)

2.2 เว็บไซต์ใดไม่มีความน่าเชื่อถือในเรื่องความปลอดภัย หากบังคับให้ผู้ใช้มีการกรอก Password

[1] https://www.netflix.com/th-en/

[2] https://www.moph.go.th/

[3] http://phitsanulok.go.th/

[4] https://www.คนละครึ่ง.com/

2.3 ข้อใดเป็นการเพิ่มความปลอดภัยในการยืนยันตัวตน

[1] การใช้ one-time password ที่มีอายุการใช้งานแค่ครั้งเดียวในช่วงสั้น ๆ

[2] ได้รับแจ้งเตือนผ่านทาง SMS, Email หรือ Application หากมีการนำ User ไปใช้ log-in ในเครื่องอื่น ๆ

[3] การอ่าน QR Code เพื่อพิสูจน์ตัวตนก่อนเข้าระบบ

[4] ถูกทุกข้อ

2.4 ข้อใดคือวิธีการตั้งรหัสผ่านที่ดี

[1] ควรมีความยาวไม่เกิน 10 ตัวอักษร

[2] รหัสง่ายต่อการจดจำ

[3] มีการผสมอักขระที่หลากหลาย เช่น ตัวเลข ตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก อักขระพิเศษ

[4] ถูกทุกข้อ

2.5 ท่านชื่อ Biden ท่านจะตั้งรหัสผ่านตามข้อใด เพื่อให้รหัสมีความปลอดภัยมากที่สุด

[1] @biden1*

[2] RedNot1ce!

[3] ned1^B-

[4] Wh1teH0use

2.6 การตั้งค่า Wi-Fi router แบบใดมีความปลอดภัยสูงสุด

[1] WPA2 Personal (AES)

[2] WPA/WPA2 Mixed Mode

[3] WPA Personal

[4] WEP with 802.1X

2.7 ข้อใดเป็นการละเมิดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

[1] ธนาคารส่งข้อมูลการชำระหนี้ของลูกหนี้ให้เครดิตบูโร

[2] ฟิตเนสนำประวัติการออกกำลังกายของสมาชิก ไปวิเคราะห์ข้อมูลสินค้าออกกำลังกาย

[3] โรงพยาบาลส่งข้อมูลประวัติการรักษาของคนไข้ให้แพทย์เจ้าของไข้

[4] ฝ่ายอาคารเก็บข้อมูลใบหน้าของผู้พักอาศัย เพื่อใช้ในการยืนยันตัวตนก่อนเข้าอาคาร

2.8 เมื่อท่านได้รับอีเมลให้ดำเนินการส่งชื่อบัญชีผู้ใช้และรหัสผ่าน เพื่อปรับปรุงระบบการทำงานอีเมลมหาวิทยาลัย จากสำนักคอมพิวเตอร์ มหาวิทยาลัย ท่านจะดำเนินการอย่างไร

[1] ดำเนินการส่งบัญชีผู้ใช้และรหัสผ่านทันที เพื่อดำเนินการแก้ไขโดยเร็วที่สุด

[2] ดำเนินการลบอีเมลดังกล่าวทันทีและแจ้งสำนักคอมพิวเตอร์ มหาวิทยาลัย

[3] โทรศัพท์แจ้งการส่งอีเมลตอบกลับให้กับสำนักคอมพิวเตอร์ มหาวิทยาลัยได้ดำเนินการเรียบร้อย

[4] ดำเนินการเปิดไฟล์เอกสารที่แนบมา เพื่อตรวจสอบให้แน่ใจว่าเป็นอีเมลจากสำนักคอมพิวเตอร์ มหาวิทยาลัย

2.9 ข้อใดเป็นการรักษาความปลอดภัยของเราเตอร์ (Router)

[1] เปลี่ยนชื่อและรหัสผ่านเริ่มต้นของเราเตอร์ (Router)

[2] ปิดการกระจายสัญญาณระยะไกลของเราเตอร์ (Router)

[3] ออกจากระบบในฐานะผู้ดูแลระบบ เมื่อทำการตั้งค่าเราเตอร์ (Router) เสร็จเรียบร้อย

[4] ถูกต้องทุกข้อ

2.10 ข้อใดคือการดำเนินการเพื่อจำกัดการเข้าถึงไฟล์และอุปกรณ์

[1] อัปเดตซอร์ฟแวร์ทุกปีและติดตั้งโปรแกรมสแกนไวรัสและสแปม

[2] แบ่งปันรหัสผ่านกับเพื่อนหรือครอบครัวที่ไว้วางใจเท่านั้น

[3] อนุญาติให้เฉพาะเจ้าหน้าที่ดูแลระบบสามารถเข้าถึงข้อมูลผ่านเครือข่าย WI-FI

[4] ตั้งค่าการยืนยันตัวตนแบบหลายปัจจัย (Multi-factor authentication)

2.11 ข้อใดคือพฤติกรรมป้องกันตนเองจากภัยคุกคามจากอาชญากรทางไซเบอร์

[1] นิดหน่อยได้รับอีเมลจากคนที่รู้จักเป็น Link ก็ไม่ลังเลที่จะกดเข้าดูทันทีเนื่องจากคอมพิวเตอร์ของตนติดตั้งโปรแกรมป้องกันไวรัสและสแปม

[2] เล็กน้อยกดยอมรับทุกเงื่อนไขนโยบายคุ้กกี้ (Cookies Policy) บนเว็บไซต์ เพื่อสามารถเข้าใช้งานเนื้อหาบนเว็บไซต์ได้ตามที่ต้องการ

[3] บิ๊กให้เพื่อนร่วมชั้นเรียนช่วยลงทะเบียนเรียนแทนตนเอง โดยบอกชื่อผู้ใช้และรหัสเข้าลงทะเบียนเรียนให้เพื่อนโดยไม่ลังเล

[4] ไจแอนระงับการใช้งานบัญชีออนไลน์ บนอุปกรณ์อิเล็กทรอนิกส์อื่นที่ไม่ได้ใช้งาน

2.12 ข้อใดคือพฤติกรรมเสี่ยงต่อการโจมตีทางไซเบอร์

[1] การตั้งค่าการยืนยันตัวตนแบบหลายปัจจัย (Multi-factor authentication) เพื่อเข้าถึงข้อมูลและเครือข่ายสำคัญ

[2] การตั้งรหัสผ่านที่แตกต่างกันและยากต่อการคาดเดาของบัญชีออนไลน์ การเข้าทำธุรกรรม หรืออุปกรณ์ส่วนบุคคล

[3] ยกเลิกระบบการทำงานของอุปกรณ์ในการสแกนหาไวรัส หรือ Firewall บางครั้ง เพื่อต้องการดาวน์โหลดไฟล์ที่ต้องการ

[4] เลือกใช้เครือข่าย WIFI สาธารณะจากผู้ให้บริการที่น่าเชื่อถือทุกครั้งก่อนการใช้งาน

ตอนที่ 3 ประสบการณ์ในภัยคุกคามทางไซเบอร์

คำชี้แจงกรุณาทำเครื่องหมาย ✓ ในช่องที่ตรงกับความเป็นจริง

5= มากที่สุด 4 = มาก 3 = ปานกลาง 2 = น้อย 1 = น้อยที่สุด

3. ประสบการณ์ในภัยคุกคามทางไซเบอร์		ระดับความคิดเห็น				
		มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด
3.1	ท่านเคยได้รับการอบรมเกี่ยวกับภัยคุกคามทางไซเบอร์					
3.2	ท่านรับรู้ความเสี่ยงที่เกิดขึ้น หากถูกละเมิดในข้อมูลส่วนบุคคล เช่น การขายต่อข้อมูลส่วนบุคคล การสวมรอยบัตรประชาชน การขโมยข้อมูลบัตรเครดิต					
3.3	ท่านหรือบุคคลที่ท่านรู้จักเคยมีประสบการณ์ถูก hack บัญชีอีเมลหรือสื่อสังคมออนไลน์					
3.4	ท่านเคยได้รับอีเมลหลอกลวง (Phishing email, Scams email)					
3.5	ท่านเคยคลิกเข้าไปในเว็บไซต์หลอกลวงหรือแอบอ้างว่าเป็นเว็บไซต์จริง					
3.6	ท่านรู้จักและเคยใช้ VPN					
3.7	ท่านเคยโดน malware เข้ามาก่อกวนการทำงานระบบคอมพิวเตอร์					
3.8	ท่าน หรือบุคคลรอบข้างเคยถูกมิจฉาชีพหลอกให้โอนเงินด้วยวิธีการต่างๆ เช่น การซื้อสินค้าออนไลน์ เงินบริจาค เป็นต้น					
3.9	ท่านเคยปิดการใช้งานโปรแกรมป้องกันไวรัสในคอมพิวเตอร์ เพื่อสามารถดาวน์โหลดข้อมูลจากเว็บไซต์					
3.10	ท่านเคยร่วมลงทุนกับผู้อื่นในการแลกเปลี่ยนสกุลเงินดิจิทัล					

3. ประสบการณ์ในภัยคุกคามทางไซเบอร์		ระดับความคิดเห็น				
		มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด
3.11	ท่านเคยใช้งานแอปพลิเคชันหาคู่					
3.12	อื่น ๆ (โปรดระบุ).....					

ตอนที่ 4พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์

คำชี้แจงกรุณาทำเครื่องหมาย ✓ ในช่องที่ตรงกับความเป็นจริง

5= มากที่สุด 4 = มาก 3 = ปานกลาง 2 = น้อย 1 = น้อยที่สุด

4. พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์		ระดับความคิดเห็น				
		มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด
การตั้งค่ารหัสผ่าน						
4.1	ท่านตั้งรหัสผ่านของแต่ละระบบแตกต่างกัน (ตัวอย่าง เช่น รหัสผ่านของ Email, Facebook, YouTube, Twitter)					
4.2	แม้ยังจำรหัสผ่านเดิมได้ ท่านเปลี่ยนรหัสผ่านเข้าระบบอยู่บ่อยครั้ง					
การจัดการข้อมูลส่วนบุคคล						
4.3	ท่านอ่านนโยบายความเป็นส่วนตัว (Privacy Policy) ก่อนคลิกตกลงทุกครั้ง					
4.4	ท่านไม่แบ่งปันข้อมูลส่วนบุคคลให้แก่บุคคลที่รู้จักหรือคุ้นเคย โดยไม่ทราบวัตถุประสงค์					
4.5	ท่านตั้งค่าความเป็นส่วนตัวบนบัญชีออนไลน์ทั้งหมด เช่น การยืนยันตัวตนแบบสองปัจจัย ป้องกันการรีเซ็ตรหัสผ่าน รับแจ้งเตือนเมื่อมีการเข้าสู่ระบบที่ไม่รู้จัก เป็นต้น					
4.6	ท่านกำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคลบน					

4. พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์		ระดับความคิดเห็น				
		มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด
	อุปกรณ์ เช่น รูปภาพ ไมโครโฟน กล้อง เป็นต้น					
4.7	ท่านบล็อคหรือปิดการเข้าถึงข้อมูลคุกกี้จากบุคคลที่สาม					
การใช้งานอุปกรณ์คอมพิวเตอร์						
4.8	ท่าน update โปรแกรม anti-virus และระบบปฏิบัติการอย่างสม่ำเสมอ					
4.9	ท่านหมั่นสังเกตอาการผิดปกติของอุปกรณ์คอมพิวเตอร์ (เช่น เครื่องช้า เครื่องนิ่ง หรือมีการเตือนข้อความจากอุปกรณ์)					
4.10	ท่านไม่เปิดไฟล์เอกสารแนบในอีเมลที่มาจากบุคคลที่ท่านไม่ทราบแหล่งที่มา					
4.11	ท่านจัดการความปลอดภัยกับเครื่องคอมพิวเตอร์ทันทีเมื่อมีการแจ้งเตือนมัลแวร์					
4.12	ท่านสำรองข้อมูลบนเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ (backup)					
4.13	ท่านล็อคหน้าจอคอมพิวเตอร์ทุกครั้งที่ท่านเดินออกจากโต๊ะทำงาน					
4.14	ท่านดาวน์โหลดข้อมูลและสื่อดิจิทัลจากแหล่งที่ได้รับอนุญาต น่าเชื่อถือ และตรวจสอบความถูกต้อง					
การใช้งานอุปกรณ์เคลื่อนที่						
4.15	ท่านตั้งค่ารหัสผ่านสำหรับล็อคหน้าจอของ Laptop, Tablet และโทรศัพท์มือถือ					
4.16	ท่านเลือกใช้เครือข่ายสาธารณะ**<u>เฉพาะ</u>**ผู้ให้บริการเครือข่ายที่น่าเชื่อถือ (เช่น AIS DTAC TRUE)					
การใช้งานสื่อสังคมออนไลน์						
4.17	ท่านไม่กดเข้าลิงค์ที่แชร์มาจากสื่อสังคมออนไลน์					

4. พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์		ระดับความคิดเห็น				
		มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด
4.18	ท่านไม่ส่งข้อมูลส่วนบุคคลให้กับผู้อื่น (เช่น ชื่อผู้ใช้ รหัสผ่าน รหัส OTP เลขบัตรประชาชน วันเกิด เบอร์โทร)					
4.19	ท่านไม่แชร์ตำแหน่งที่อยู่อาศัยของตนเองที่สามารถระบุถึงตัวตนได้บนสื่อสังคมออนไลน์					
4.20	ท่านไม่ยอมรับการเป็นเพื่อนบนสื่อสังคมออนไลน์ที่ไม่รู้จัก					
4.21	ท่านตรวจสอบประวัติการใช้งานบนสื่อสังคมออนไลน์เสมอ					

ตอนที่ 5 ข้อเสนอแนะเพิ่มเติมเกี่ยวกับพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์

……

……

……

……

……

เฉลยแบบทดสอบ ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

ข้อที่ 2.1 ตอบ 3

ข้อที่ 2.2 ตอบ 3

ข้อที่ 2.3 ตอบ 4

ข้อที่ 2.4 ตอบ 3

ข้อที่ 2.5 ตอบ 2

ข้อที่ 2.6 ตอบ 1

ข้อที่ 2.7 ตอบ 2

ข้อที่ 2.8 ตอบ 2

ข้อที่ 2.9 ตอบ 4

ข้อที่ 2.10 ตอบ 4

ข้อที่ 2.11 ตอบ 4

ข้อที่ 2.12 ตอบ 3

ประวัติผู้เขียน