# การประเมินความตระหนักรู้และความพร้อมสำหรับการรับมือภัยคุกคามทางไซเบอร์ของกลุ่มผู้สูงอายุในประเทศไทย

# THE EVALUATION REGARDING AWARENESS AND PREPAREDNESS IN COPING WITH CYBERSECURITY THREATS OF THE ELDERLY IN THAILAND

ธันญาพัชญ์ เลื่อยกระโทก[1]
Thanyaphat Lueikrathok

## บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ (1) เปรียบเทียบความแตกต่างของปัจจัยส่วนบุคคลของผู้สูงอายุในประเทศไทยกับระดับความตระหนักรู้ภัยคุกคามทางไซเบอร์ (2) เปรียบเทียบความแตกต่างของประสบการณ์ภัยคุกคามทางไซเบอร์กับพฤติกรรมการรับมือ และ (3)ศึกษาความสัมพันธ์ระหว่างความตระหนักรู้กับพฤติกรรมการรับมือของผู้สูงอายุ กลุ่มตัวอย่างคือผู้สูงอายุอายุ 60 ปีขึ้นไป จำนวน 400 คน ได้จากการสุ่มแบบสโนว์บอล เครื่องมือที่ใช้คือแบบสอบถามออนไลน์ วิเคราะห์ข้อมูลด้วยสถิติเชิงพรรณนา สถิติเชิงอนุมาน Independent Samples t-test One-way ANOVA รวมทั้งการเปรียบเทียบความแตกต่างเป็นรายคู่ (Multiple Comparisons) ในกรณีที่พบความแตกต่างอย่างมีนัยสำคัญ และสัมประสิทธิ์สหสัมพันธ์เพียร์สัน ผลการวิจัยพบว่า ผู้สูงอายุส่วนใหญ่เป็นเพศหญิง อายุ 60–65 ปี ใช้อินเทอร์เน็ตวันละ 1–3 ชั่วโมงเพื่อการติดต่อสื่อสารเป็นหลัก ประมาณหนึ่งในสามเคยเผชิญภัยคุกคามทางไซเบอร์และมีความเสียหายทางการเงินในระดับต่ำ โดยผู้สูงอายุส่วนใหญ่ประเมินตนเองว่ามีความรู้น้อยเกี่ยวกับมาตรการความปลอดภัยไซเบอร์ แต่มีระดับการรับรู้ความเสี่ยง การรับรู้ความรุนแรง ประสิทธิผลของพฤติกรรมตอบสนอง และความเชื่อมั่นในตนเองอยู่ในระดับมาก

ผลการทดสอบสมมติฐานพบว่า เพศและสถานภาพสมรสมีผลต่อความตระหนักรู้ภัยคุกคามทางไซเบอร์ ส่วนอายุ ระดับการศึกษา อาชีพ รายได้ และความถี่การใช้อินเทอร์เน็ตไม่มีผลอย่างมีนัยสำคัญ ผู้สูงอายุที่เคยประสบภัยมีระดับการรับรู้ภัยและการประเมินสถานการณ์สูงกว่าผู้ที่ไม่เคยประสบภัย นอกจากนี้ตัวแปรด้านการรับรู้ภัย การประเมินภัย ความเชื่อมั่นในตนเอง และพฤติกรรมการตอบสนองมีความสัมพันธ์เชิงบวกกันทั้งหมด แสดงให้เห็นว่าการรับรู้ที่เพิ่มขึ้นส่งผลต่อพฤติกรรมการป้องกันที่ดีขึ้นตามไปด้วย

**คำสำคัญ:** ผู้สูงอายุ, การตระหนักรู้ภัยคุกคามทางไซเบอร์, พฤติกรรมการรับมือภัยไซเบอร์, ความเสี่ยงที่รับรู้

[1] นักศึกษาหลักสูตรบริหารธุรกิจมหาบัณฑิต คณะบริหารธุรกิจ มหาวิทยาลัยรามคำแหง
E-mail: 6724101414@rumail.ru.ac.th

**ABSTRACT**

This study aimed to (1) compare differences between personal factors of older adults in Thailand and their levels of cybersecurity threat awareness, (2) compare differences between experiences of cyber threats and coping behaviors, and (3) examine the relationship between cybersecurity awareness and coping behaviors among older adults. The sample consisted of 400 adults aged 60 years and above, selected through snowball sampling. Data were collected using an online questionnaire and analyzed using descriptive statistics and inferential statistics, including Independent Samples t-test, One-way ANOVA with Multiple Comparisons in cases where significant differences were found, and Pearson's correlation coefficient.

The results revealed that most participants were female, aged between 60–65 years, and primarily used the internet for communication for 1–3 hours per day. Approximately one-third of the respondents had experienced cybersecurity threats, with financial losses generally at a low level. Although most older adults perceived their cybersecurity knowledge to be limited, they reported high levels of perceived risk, perceived severity, response efficacy, and self-efficacy.

Hypothesis testing indicated that gender and marital status significantly influenced cybersecurity threat awareness, while age, educational level, occupation, income, and frequency of internet use showed no significant effects. Older adults who had experienced cyber threats demonstrated higher levels of threat perception and threat appraisal than those without such experiences. Furthermore, perceived threat, threat appraisal, self-efficacy, and coping behaviors were all positively correlated, indicating that increased awareness contributes to more effective cybersecurity coping behaviors.

**Keywords:** The Elderly, Cybersecurity Awareness, Cyber-threat Coping, Perceived Risk

**ความเป็นมาและความสำคัญของปัญหา**

ในช่วงทศวรรษที่ผ่านมา ประเทศไทยได้เข้าสู่ สังคมสูงอายุอย่างสมบูรณ์ (Complete Aged Society) โดยมีประชากรอายุ 60 ปีขึ้นไปกว่า 13.34 ล้านคน คิดเป็นร้อยละ 20.23 ของประชากรทั้งหมด (สำนักงานสถิติแห่งชาติ, 2567) การเพิ่มขึ้นของจำนวนผู้สูงอายุเกิดขึ้นพร้อมกับการเปลี่ยนแปลงด้านดิจิทัลที่ขยายตัวอย่างรวดเร็ว ส่งผลให้ผู้สูงอายุไทยเริ่มเข้าถึงเทคโนโลยีมากขึ้น ไม่ว่าจะเป็นการใช้งานสมาร์ตโฟน อินเทอร์เน็ต รวมถึงแพลตฟอร์มโซเชียลมีเดียเพื่อสื่อสาร ทำธุรกรรม และแสวงหาข้อมูลออนไลน์

ข้อมูลจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA, 2566) ระบุว่า ผู้สูงอายุไทยอายุ 60 ปีขึ้นไป ร้อยละ 73.3ใช้โทรศัพท์มือถือ และร้อยละ 67.3 ใช้อินเทอร์เน็ตเป็นประจำ โดยส่วนใหญ่ใช้งานเพื่อสื่อสารผ่าน Line และ Facebook ทำธุรกรรมทางการเงินออนไลน์ และรับข่าวสารจากสื่อสังคมออนไลน์ แม้ผู้สูงอายุจะมีการใช้งานเทคโนโลยีเพิ่มขึ้น แต่การใช้งานดังกล่าวกลับไม่ได้มาพร้อมกับ

ความรู้และทักษะด้านความปลอดภัยทางไซเบอร์ ที่เพียงพอ ทำให้กลุ่มผู้สูงอายุกลายเป็นเป้าหมายที่มิจฉาชีพออนไลน์เข้าถึงได้ง่าย เนื่องจากอาจขาดทักษะในการตรวจสอบข้อมูล การประเมินความเสี่ยง และการรับมือภัยคุกคามทางดิจิทัล

สถานการณ์อาชญากรรมออนไลน์ในประเทศไทยยังทวีความรุนแรงอย่างต่อเนื่อง ข้อมูลจากกองบัญชาการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท., 2568) ระบุว่า ระหว่างวันที่ 24–30 กรกฎาคม 2568 มีคดีอาชญากรรมออนไลน์สูงถึง 7,349 คดี มูลค่าความเสียหายกว่า 403.60 ล้านบาท ประเภทคดีที่พบมาก ได้แก่ การหลอกลวงซื้อขายสินค้าและบริการ (55.38%), การหลอกให้โอนเงินโดยอ้างการรับรางวัลหรือผลประโยชน์ (13.73%), การหลอกทำงานหารายได้พิเศษ (7.73%), คดีหลอกให้ลงทุนมีเพียง 2.87% แต่ก่อมูลค่าความเสียหายสูงถึง 123.39 ล้านบาท

ผู้สูงอายุถือเป็นกลุ่มที่ได้รับผลกระทบสูง เนื่องจากขาดทักษะในการตรวจสอบความน่าเชื่อถือของข้อมูล มักเชื่อแหล่งข่าวที่ไม่น่าเชื่อถือ และไม่คุ้นเคยกับรูปแบบภัยคุกคามสมัยใหม่ เช่น ฟิชชิ่ง (Phishing) สแกมการเงิน หรือการปลอมแปลงบัญชีบนโซเชียลมีเดีย ส่งผลให้เกิดความสูญเสียทั้งด้านทรัพย์สิน สุขภาพจิต และความเชื่อมั่นในการใช้งานเทคโนโลยี รายงาน Digital 2025 Thailand (We Are Social, 2025) พบว่า คนไทยกว่า 91.2% ของประชากรทั้งหมดเป็นผู้ใช้อินเทอร์เน็ต และมีหมายเลขโทรศัพท์เคลื่อนที่เปิดใช้งานมากถึง 99.5 ล้านเลขหมาย ซึ่งมากกว่าจำนวนประชากร ส่งผลให้สังคมออนไลน์กลายเป็นส่วนหนึ่งของชีวิตประจำวัน และความเสี่ยงทางไซเบอร์ยิ่งทวีความสำคัญมากขึ้นในทุกกลุ่มอายุ โดยเฉพาะกลุ่มผู้สูงอายุที่อาจมีข้อจำกัดด้านทักษะดิจิทัล

ด้วยเหตุนี้ การศึกษาความตระหนักรู้และความพร้อมสำหรับการรับมือภัยคุกคามทางไซเบอร์ในกลุ่มผู้สูงอายุจึงมีความจำเป็นอย่างยิ่ง การวิจัยในประเด็นนี้จะช่วยให้เข้าใจระดับความรู้ ทักษะ ความเสี่ยง รูปแบบการถูกหลอกลวง และช่องโหว่ที่อาจเกิดขึ้น รวมถึงสนับสนุนการออกแบบนโยบายมาตรการป้องกัน และสื่อการเรียนรู้ที่เหมาะสมกับผู้สูงอายุ เพื่อเสริมสร้างความปลอดภัยในการใช้งานดิจิทัลของประชากรกลุ่มนี้อย่างยั่งยืน

**วัตถุประสงค์ของการวิจัย**

1. เพื่อเปรียบเทียบความแตกต่างระหว่างปัจจัยส่วนบุคคลของผู้สูงอายุในประเทศไทยกับการตระหนักรู้ภัยคุกคามทางไซเบอร์
2. เพื่อเปรียบเทียบความแตกต่างระหว่างปัจจัยด้านประสบการณ์เผชิญภัยคุกคามทางไซเบอร์ของผู้สูงอายุในประเทศไทยกับการรับมือภัยคุกคาม
3. เพื่อศึกษาความสัมพันธ์ระหว่างพฤติกรรมการรับมือภัยคุกคามทางไซเบอร์กับความตระหนักรู้ของผู้สูงอายุในประเทศไทย

**สมมติฐานของการวิจัย**

1. ผู้สูงอายุในประเทศไทยที่มีข้อมูลส่วนบุคคลที่แตกต่างกัน มีผลต่อการตระหนักรู้ภัยคุกคามทางไซเบอร์ที่แตกต่างกัน
2. ความถี่การใช้งานอินเทอร์เน็ตที่แตกต่างกันมีผลต่อการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ที่แตกต่างกัน

3. ผู้สูงอายุในประเทศไทยที่มีประสบการณ์เผชิญภัยคุกคามทางไซเบอร์แตกต่างกัน จะมีระดับการรับมือภัยคุกคามทางไซเบอร์แตกต่างกันอย่างมีนัยสำคัญทางสถิติ

4. ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของผู้สูงอายุมีความสัมพันธ์กับพฤติกรรมการรับมือภัยคุกคามทางไซเบอร์ในทิศทางเดียวกัน

**ขอบเขตของการวิจัย**

งานวิจัยนี้มีขอบเขตในการศึกษาพฤติกรรมการใช้งานอินเทอร์เน็ต การรับรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ และการรับมือกับสถานการณ์ภัยไซเบอร์ของผู้สูงอายุในประเทศไทย และมีประสบการณ์ในการใช้งานอินเทอร์เน็ตหรืออุปกรณ์ดิจิทัล โดยใช้แบบสอบถามเป็นเครื่องมือในการเก็บข้อมูล

**ประโยชน์ที่คาดว่าจะได้รับ**

1. เพื่อเป็นแนวทางในการพัฒนานโยบายและมาตรการป้องกันภัยไซเบอร์ที่เหมาะสมกับผู้สูงอายุ

2. เพื่อยกระดับคุณภาพชีวิตและความมั่นใจของผู้สูงอายุในการใช้งานเทคโนโลยี

3. เพื่อเป็นแนวทางให้ผู้สูงอายุสามารถรับมือกับภัยคุกคามทางไซเบอร์

**แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง**

**แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)** นับเป็นประเด็นสำคัญของสังคมดิจิทัลในปัจจุบัน เนื่องจากการดำเนินชีวิตของผู้คนส่วนใหญ่เชื่อมโยงกับระบบออนไลน์อย่างหลีกเลี่ยงไม่ได้ ไม่ว่าจะเป็นการสื่อสาร การเงิน การทำธุรกรรมอิเล็กทรอนิกส์ การใช้บริการภาครัฐ ไปจนถึงโครงสร้างพื้นฐานด้านพลังงาน ขนส่ง และสาธารณสุข ภัยคุกคามทางไซเบอร์จึงสามารถเกิดขึ้นและส่งผลกระทบได้ในหลายระดับ ตั้งแต่ระดับบุคคล องค์กร ไปจนถึงระดับประเทศ ภัยคุกคามทางไซเบอร์ไม่เพียงเป็นการโจมตีระบบหรือขโมยข้อมูลเท่านั้น แต่ยังรวมถึงการเผยแพร่ข้อมูลปลอม การจารกรรมข้อมูลสำคัญ การก่อวินาศกรรมระบบ การทำลายชื่อเสียงของบุคคลหรือองค์กร รวมถึงการปล่อยข่าวเท็จเพื่อสร้างความแตกแยกในสังคม โดยในช่วงปี 2024–2025 ภัยคุกคามมีความซับซ้อนมากขึ้นจากการพัฒนาเทคโนโลยีด้าน AI, Deepfake, และมัลแวร์แบบใหม่ที่สามารถโจมตีได้อัตโนมัติ ทำให้ความเสี่ยงเพิ่มสูงขึ้นอย่างต่อเนื่อง ประเภทของภัยคุกคามทางไซเบอร์ โดยทั่วไป ภัยคุกคามทางไซเบอร์สามารถแบ่งออกได้เป็น 4 กลุ่มหลัก ดังนี้ 1. ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ (Application-Based Threats) ภัยประเภทนี้มักเกิดขึ้นเมื่อผู้ใช้งานดาวน์โหลดโปรแกรม แอปพลิเคชัน หรือไฟล์ต่าง ๆ มาติดตั้งบนคอมพิวเตอร์หรืออุปกรณ์พกพา โดยไม่รู้ว่ามีโปรแกรมอันตราย (มัลแวร์: Malware) แฝงอยู่ภายใน มัลแวร์ถูกออกแบบมาเพื่อสร้างความเสียหาย ได้แก่ 1.ทำลายไฟล์หรือระบบ 2. ขโมยข้อมูล 3. ควบคุมเครื่องเพื่อส่งข้อมูลออก 4.เปิดช่องให้แฮกเกอร์เข้ามาแทรกแซงระบบในภายหลัง 2. ภัยคุกคามจากการใช้งานเว็บไซต์ (Web-Based Threats) ภัยคุกคามประเภทนี้เกิดขึ้นเมื่อผู้ใช้เข้าชมเว็บไซต์ที่ถูกออกแบบมาเพื่อหลอกลวง ได้แก่ 1.เว็บไซต์ฟิชชิ่ง (Phishing Websites) 2. เว็บไซต์ปลอมที่ทำเลียนแบบธนาคาร 3.หน้าเว็บที่มีสคริปต์แอบฝังมัลแวร์ 4.ลิงก์หลอกใน SMS และ LINE เว็บไซต์ฟิชชิ่งจะหลอกให้

ผู้ใช้กรอกข้อมูล เช่น ยูสเซอร์เนม รหัสผ่าน หรือรหัส OTP ซึ่งทำให้บัญชีอีเมล โซเชียลมีเดีย หรือบัญชีธนาคารเสี่ยงถูกยึดครอง 3. ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย (Wireless Network Threats) เครือข่ายไร้สาย เช่น Wi-Fi, Bluetooth, NFC เป็นช่องทางที่เสี่ยงต่อการถูกดักข้อมูล เนื่องจากการส่งสัญญาณผ่านอากาศสามารถถูกดักจับหรือถูกปลอมแปลงได้ ได้แก่ 1.การตั้ง Wi-Fi ฟรีปลอม (Evil Twin Wi-Fi) 2.การดักข้อมูลผ่านการเชื่อมต่อสาธารณะ 3.การโจมตีอุปกรณ์ IoT เช่น กล้องวงจรปิด Smart TV 4. การแทรกแซงผ่าน Bluetooth หรืออุปกรณ์สมาร์ตโฮม อุปกรณ์จำนวนมากในปัจจุบันเชื่อมต่อด้วยระบบไร้สาย แต่ส่วนใหญ่ขาดระบบป้องกันที่ดี ทำให้เป็นช่องทางที่แฮกเกอร์ใช้โจมตีได้ง่ายและมีประสิทธิภาพ 4. ภัยคุกคามจากการโจมตีแบบเจาะจงเป้าหมาย (Targeted Attacks / APT) ภัยประเภทนี้เป็นการโจมตีที่ใช้เทคนิคขั้นสูง มีเป้าหมายชัดเจน และมักมุ่งโจมตีองค์กรขนาดใหญ่ สถาบันการเงิน หน่วยงานรัฐ หรือโครงสร้างพื้นฐานของประเทศ ได้แก่ 1.ระบบธนาคาร 2.ระบบสาธารณสุข 3.สายการบิน 4.สาธารณูปโภค ผู้โจมตีอาจเป็นทั้งแฮกเกอร์ทั่วไป กลุ่มอาชญากรไซเบอร์ ไปจนถึงกลุ่มที่ได้รับการสนับสนุนจากรัฐ (State-Sponsored Attack) การโจมตีลักษณะนี้สามารถลอบแทรกซึมในระบบเป็นเวลาหลายเดือนโดยไม่ถูกตรวจจับ และสร้างความเสียหายรุนแรง เช่น การขโมยข้อมูลประชาชน การทำลายระบบ หรือการเรียกค่าไถ่

**แนวคิดของการรับมือภัยคุกคามทางไซเบอร์** สามารถแบ่งออกได้เป็น 2 ลักษณะหลัก ได้แก่

1.การรับมือเชิงปัญหา (Problem-focused coping) หมายถึง การดำเนินการโดยตรงเพื่อจัดการกับภัยคุกคาม เช่น การเปลี่ยนรหัสผ่าน การอัปเดตโปรแกรมรักษาความปลอดภัย การหลีกเลี่ยงเว็บไซต์ที่ไม่ปลอดภัย หรือการแจ้งหน่วยงานที่เกี่ยวข้องเมื่อพบพฤติกรรมที่น่าสงสัย (Folkman & Moskowitz, 2004)

2.การรับมือเชิงอารมณ์ (Emotion-focused coping) หมายถึง การจัดการกับความรู้สึกวิตกกังวลหรือกลัวที่เกิดขึ้นจากภัยไซเบอร์ เช่น การปรึกษาครอบครัว การขอคำแนะนำจากเพื่อน หรือการใช้วิธีผ่อนคลายความเครียดเพื่อลดผลกระทบทางอารมณ์ (Folkman, 2011) ในกลุ่มผู้สูงอายุ การรับมือภัยคุกคามทางไซเบอร์ยังขึ้นอยู่กับระดับความรู้ด้านเทคโนโลยี การรับรู้ความเสี่ยง และประสบการณ์การใช้งานอินเทอร์เน็ตของแต่ละบุคคล ผู้สูงอายุที่มีความรู้และความตระหนักรู้ด้านความปลอดภัยไซเบอร์สูงมักจะสามารถเลือกใช้วิธีรับมือที่มีประสิทธิภาพมากกว่า เช่น การตรวจสอบแหล่งที่มาของข้อมูลก่อนตัดสินใจ หรือการใช้ระบบยืนยันตัวตนหลายชั้นในการเข้าถึงบัญชีส่วนตัว (Chou & Chou, 2021)

**แนวคิดการปฏิบัติหน้าที่ พ.ร.ก. อาชญากรรมทางเทคโนโลยี 2566** มีจุดประสงค์เพื่อรับมือกับอาชญากรรมออนไลน์ โดยกำหนดการปฏิบัติหน้าที่ของสถาบันการเงินและผู้ประกอบธุรกิจเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ผ่านการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องตามมาตรา 4 และ 5 หากพบว่ามีการกระทำความผิด ให้สถาบันการเงินระงับการทำธุรกรรมและแจ้งพนักงานสอบสวนตามมาตรา 7 กฎหมายนี้ยังได้กำหนดการลงโทษผู้ที่เปิดเผยหรือยินยอมให้ผู้อื่นใช้บัญชีเงินฝากหรือเบอร์โทรศัพท์เพื่อกระทำความผิด (มาตรา 9-11) และเปิดช่องทางให้ผู้เสียหายสามารถแจ้งเหตุทางอิเล็กทรอนิกส์ได้ (มาตรา 8) ผลกระทบต่อความตระหนักของผู้ใช้อินเทอร์เน็ต มิติการป้องกัน: มาตรา 7 ที่กำหนดให้ระงับการทำธุรกรรม ทำให้ผู้ใช้มีความมั่นใจในการทำธุรกรรมออนไลน์ แต่ก็อาจลดความระมัดระวัง (moral hazard) มิติการลงโทษ มาตรา 9-11 ทำให้ผู้ใช้ตระหนักถึง

ความรับผิดชอบในการแชร์ข้อมูลส่วนตัวมากขึ้น มิติการรายงาน: การแจ้งความผ่านระบบอิเล็กทรอนิกส์ (มาตรา 8) ทำให้ผู้เสียหายสามารถรายงานได้ง่ายขึ้น ส่งผลให้สังคมตระหนักถึงปัญหามากขึ้น

**แนวคิดการสร้างความตระหนักรู้และการรับมือกับภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ** ในยุคดิจิทัล ภัยคุกคามทางไซเบอร์มีความซับซ้อนและเพิ่มขึ้นอย่างต่อเนื่อง ส่งผลให้ผู้ใช้อินเทอร์เน็ตจำนวนมาก โดยเฉพาะผู้สูงอายุซึ่งมีทักษะด้านเทคโนโลยีจำกัด ตกเป็นเหยื่อของอาชญากรรมออนไลน์ได้ง่าย การสร้างความตระหนักรู้และพัฒนาทักษะด้านความปลอดภัยไซเบอร์จึงมีความสำคัญ เพื่อช่วยลดความเสี่ยงและเสริมสร้างความสามารถในการป้องกันตนเอง แนวคิดดังกล่าวครอบคลุมทั้งด้านความรู้เกี่ยวกับภัยไซเบอร์ การรับรู้พฤติกรรมเสี่ยง การตรวจจับภัย และการตอบสนองต่อเหตุการณ์ผิดปกติ โดยควรออกแบบให้เหมาะสมกับระดับความเข้าใจของผู้สูงอายุ ประการแรก การสร้างความตระหนักรู้ควรเริ่มจากการให้ความรู้พื้นฐานเกี่ยวกับรูปแบบและลักษณะของภัยคุกคามทางไซเบอร์ เช่น ฟิชชิ่ง การหลอกโอนเงิน การปลอมแปลงเว็บไซต์ และการดักข้อมูลส่วนบุคคล แนวคิดของ Good และ Bloom ชี้ให้เห็นว่าความตระหนักรู้เกิดจากการเรียนรู้ซ้ำและประสบการณ์จริง การใช้ตัวอย่างสถานการณ์ใกล้ตัวและภาษาที่เข้าใจง่ายจึงช่วยให้ผู้สูงอายุสามารถจดจำและนำไปใช้ได้จริง ประการที่สอง การรับมือภัยควรอาศัยการจำแนกประเภทภัยอย่างเป็นระบบ พร้อมแนวทางป้องกันที่เหมาะสม เช่น การหลีกเลี่ยงลิงก์ที่ไม่รู้จัก การไม่เปิดเผยข้อมูลส่วนตัวหรือรหัส OTP การตั้งค่าความเป็นส่วนตัว และการเก็บหลักฐานเมื่อพบเหตุผิดปกติ ซึ่งจะช่วยลดความเสียหายและเพิ่มประสิทธิภาพในการรายงานเหตุ ประการที่สาม การสนับสนุนให้สามารถแจ้งเหตุได้สะดวกและรวดเร็วเป็นกลไกสำคัญในการลดผลกระทบจากอาชญากรรมไซเบอร์ การเปิดช่องทางการแจ้งผ่านระบบออนไลน์หรือแพลตฟอร์มของหน่วยงานที่เกี่ยวข้อง ช่วยให้ผู้เสียหายเข้าถึงกระบวนการยุติธรรมได้ง่ายขึ้น และเพิ่มประสิทธิภาพในการจัดการปัญหาในระดับสังคม ประการที่สี่ การใช้กฎหมายเป็นเครื่องมือสนับสนุนความปลอดภัย เช่น พระราชกำหนดการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มีบทบาทสำคัญในการสกัดกั้นอาชญากรรมไซเบอร์ ทั้งในด้านการอายัดธุรกรรม การแจ้งเหตุทางอิเล็กทรอนิกส์ และการกำหนดบทลงโทษผู้ที่เกี่ยวข้องกับบัญชีม้าและเบอร์โทรศัพท์ผิดกฎหมาย ซึ่งช่วยเสริมสร้างวินัยและความรับผิดชอบในการใช้เทคโนโลยี

**ทฤษฎีแรงจูงใจเพื่อการป้องกัน (Protection Motivation Theory: PMT)** ได้รับการพัฒนาขึ้นโดย Ronald W. Rogers (1975) โดยมีพื้นฐานมาจากการผสมผสานแนวคิดของ แบบแผนความเชื่อด้านสุขภาพ (Health Belief Model) และ ทฤษฎีความคาดหวังในความสามารถของตนเอง (Self-Efficacy Theory) ทฤษฎีนี้ได้รับการพัฒนาขึ้นเพื่ออธิบายการตอบสนองของบุคคลต่อการสื่อสารเกี่ยวกับภัยคุกคามที่ก่อให้เกิดความกลัว (Fear Appeals) และเพื่อทำความเข้าใจถึงแรงจูงใจของบุคคลในการป้องกันตนเองจากภัยคุกคามดังกล่าว (Rogers, 1975) ในระยะแรก ทฤษฎีนี้ได้เสนอว่าความกลัวเกิดขึ้นจากการรับรู้ตัวแปรหลัก 3 ประการ ได้แก่ 1.การรับรู้ความรุนแรงของภัย (Perceived Severity) หมายถึง การรับรู้ถึงความร้ายแรงของผลลัพธ์ที่อาจเกิดขึ้นจากภัยคุกคาม 2.การรับรู้โอกาสเสี่ยงต่อการถูกคุกคาม (Perceived Vulnerability) หมายถึง การรับรู้ถึงความเป็นไปได้ที่ภัยคุกคามนั้นจะเกิดขึ้นกับตนเอง 3. ความคาดหวังในประสิทธิภาพของการตอบสนอง (Response Efficacy) หมายถึง ความเชื่อว่าการกระทำหรือมาตรการป้องกันจะสามารถลดหรือหลีกเลี่ยงภัยคุกคามได้ ต่อมา Rogers (1983) ได้เพิ่มเติมตัวแปรที่สำคัญคือ ความคาดหวังในความสามารถของตนเอง (Self-Efficacy) ซึ่งหมายถึง ความเชื่อมั่นว่าตนเอง

มีความสามารถเพียงพอที่จะดำเนินการตอบสนองเพื่อป้องกันภัยได้อย่างมีประสิทธิภาพ Rogers (1983) อธิบายกระบวนการทางความคิดในทฤษฎี PMT ว่าแบ่งออกเป็น 2 กระบวนการหลัก ได้แก่ 1. กระบวนการประเมินภัยคุกคาม (Threat Appraisal) ซึ่งเป็นการประเมินระดับความรุนแรงและโอกาสที่ภัยจะเกิดขึ้นกับตนเอง 2.กระบวนการประเมินการเผชิญภัย (Coping Appraisal) ซึ่งเป็นการประเมินถึงประสิทธิภาพของการตอบสนองและความสามารถของตนเองในการจัดการกับภัยนั้น ผลของกระบวนการประเมินทั้งสองจะนำไปสู่ แรงจูงใจในการป้องกัน (Protection Motivation) ซึ่งมีอิทธิพลโดยตรงต่อความตั้งใจและพฤติกรรมในการป้องกันภัยในที่สุด

**ทฤษฎีการจัดการกับความเครียดเชิงปฏิสัมพันธ์ (Transactional Theory of Stress and Coping)** ได้รับการพัฒนาขึ้นโดย Lazarus และ Folkman (1984) เพื่ออธิบายกระบวนการที่บุคคลใช้ในการรับรู้และจัดการกับสถานการณ์ที่ก่อให้เกิดความเครียด โดยทฤษฎีนี้มองว่าความเครียด (Stress) เป็นผลมาจาก ปฏิสัมพันธ์ระหว่างบุคคลกับสิ่งแวดล้อม (Person–Environment Transaction) ซึ่งบุคคลจะประเมินสถานการณ์และทรัพยากรของตนเองในการเผชิญกับสถานการณ์นั้น โดยกระบวนการตามทฤษฎีนี้ประกอบด้วย การประเมินปฐมภูมิ (Primary Appraisal) และ การประเมินทุติยภูมิ (Secondary Appraisal) โดยในการประเมินปฐมภูมิ บุคคลจะพิจารณาว่าสถานการณ์ที่เกิดขึ้นมีความสำคัญต่อความเป็นอยู่ของตนหรือไม่ เช่น มองว่าเป็นภัยคุกคาม เป็นความท้าทาย หรือไม่สำคัญ ส่วนในการประเมินทุติยภูมิ บุคคลจะประเมินว่าตนมีทรัพยากรหรือความสามารถเพียงพอในการรับมือกับสถานการณ์นั้นหรือไม่ เช่น การประเมินทักษะ การสนับสนุนทางสังคม หรือกลยุทธ์ในการจัดการ (coping strategies)

**ทฤษฎีการตระหนักรู้ในตนเอง (Self-Awareness Theory)** ได้รับการพัฒนาขึ้นโดย Duval และ Wicklund (1972) เพื่ออธิบายกระบวนการที่บุคคลหันกลับมาสนใจตนเอง (self-focused attention) และตระหนักรู้ถึงมาตรฐานหรือคุณค่าภายในของตนเอง ทฤษฎีนี้เสนอว่า การที่บุคคลมี “การตระหนักรู้ในตนเอง” (self-awareness) จะทำให้เกิดการเปรียบเทียบตนเองกับบรรทัดฐานหรือมาตรฐานภายใน (internal standards) เช่น ค่านิยม ศีลธรรม หรือเป้าหมายส่วนบุคคล เพื่อประเมินว่าพฤติกรรมของตนสอดคล้องกับสิ่งเหล่านั้นหรือไม่ หากบุคคลรับรู้ว่าพฤติกรรมของตนสอดคล้องกับมาตรฐานภายใน จะเกิดความพึงพอใจและคงสภาวะดังกล่าวไว้ แต่หากพบว่ามีความไม่สอดคล้อง (discrepancy) ระหว่างตนเองกับมาตรฐาน จะเกิดแรงจูงใจภายในเพื่อปรับเปลี่ยนพฤติกรรมให้สอดคล้องกับค่านิยมที่ตนยึดถือ (Duval & Wicklund, 1972) ซึ่งกระบวนการนี้เป็นพื้นฐานสำคัญของการควบคุมตนเอง (self-regulation)

**งานวิจัยที่เกี่ยวข้อง**

Li et al. (2565) ศึกษาพฤติกรรมการป้องกันภัยไซเบอร์ของพนักงานในองค์กรโดยใช้ Extended Protection Motivation Theory (PMT) เพื่อทดสอบความสัมพันธ์ระหว่าง ความพยายามขององค์กร (organization effort), ประสบการณ์ของพนักงาน, การประเมินภัย (threat appraisal), การประเมินการรับมือ (coping appraisal) และ การปฏิบัติด้านความปลอดภัยไซเบอร์ งานวิจัยนี้ พบว่า coping appraisal เป็นปัจจัยสำคัญที่ส่งผลต่อพฤติกรรมการป้องกันภัยไซเบอร์ของพนักงาน มากกว่า threat appraisal และพบความแตกต่างของพฤติกรรมตาม เพศ, อายุ (generation), และประเภทองค์กร เช่น ผู้หญิงมีความตระหนักด้านภัยไซเบอร์สูงกว่า และ Gen Edge มีการป้องกันภัยต่ำกว่า Millennials และ

Gen X นอกจากนี้ การฝึกอบรมและการส่งเสริมความตระหนักด้านความปลอดภัยขององค์กรมีผลสำคัญต่อการปรับพฤติกรรมของพนักงาน

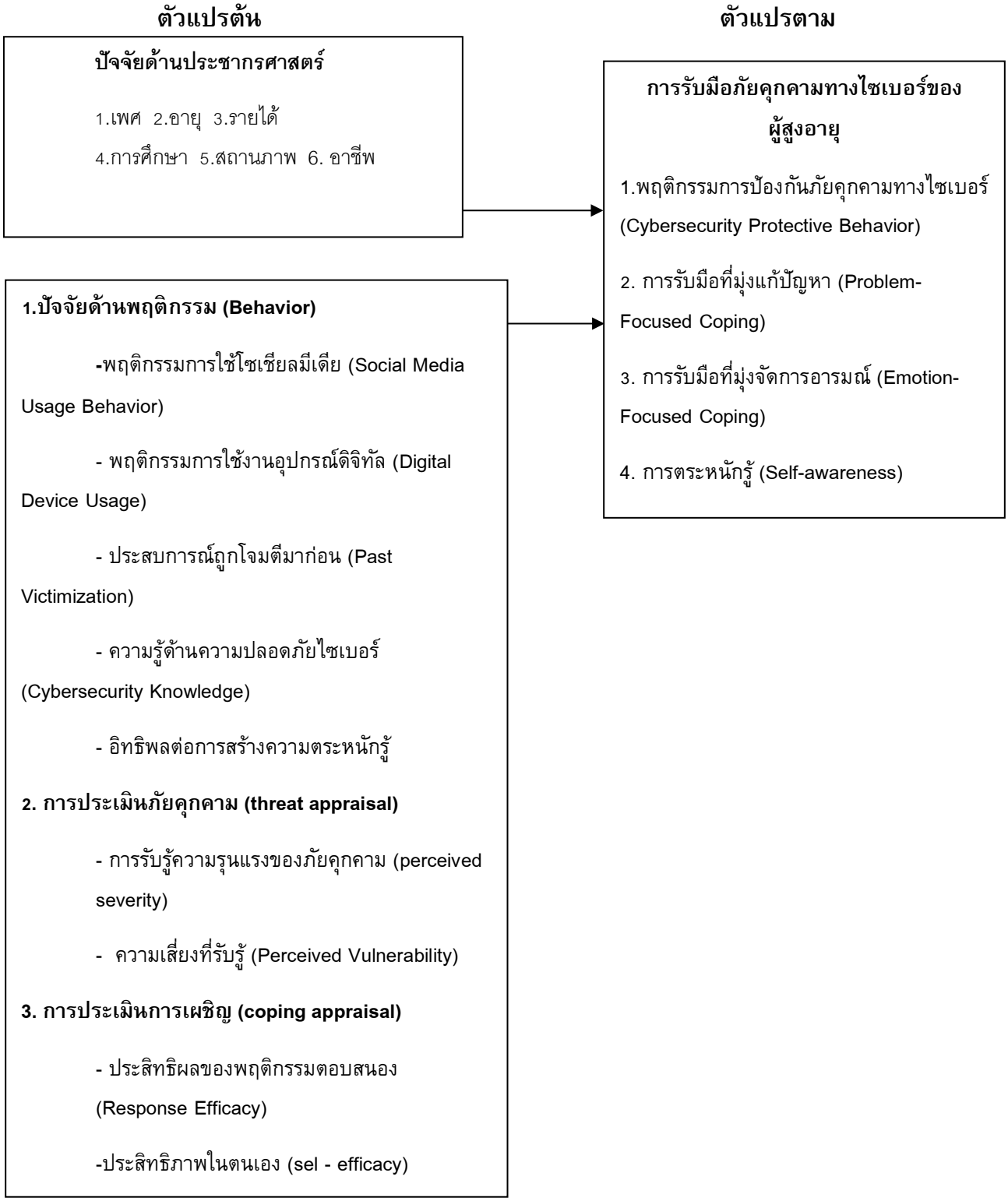
Haslinda et al. (2568) ศึกษาระดับความตระหนักรู้ด้านความปลอดภัยไซเบอร์ของผู้สูงอายุในประเทศมาเลเซีย โดยเก็บข้อมูลจากผู้สูงอายุ 331 คน พบว่ากว่า 30% ใช้อินเทอร์เน็ต 4–8 ชั่วโมงต่อวัน และมากกว่าครึ่ง ไม่รู้ถึงภัยไซเบอร์ที่สำคัญ เช่น มัลแวร์และแรนซัมแวร์ แม้จะมีความรู้เกี่ยวกับการเข้าถึงโดยไม่ได้รับอนุญาตและการฉ้อโกงคอมพิวเตอร์บ้าง แต่ยังมีช่องว่างด้านความรู้ (knowledge gaps) อย่างมาก งานวิจัยชี้ว่าผู้สูงอายุมักเรียนรู้ด้วยตนเองหรือจากชุมชน ต้องการโปรแกรมฝึกอบรมเฉพาะทางเพื่อเพิ่มทักษะ รวมทั้งแนะนำให้ออกแบบเทคโนโลยีให้เป็นมิตรกับผู้สูงอายุเพื่อสร้างสังคมดิจิทัลที่ปลอดภัยและครอบคลุมมากขึ้น

เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี (2565) ศึกษาวิจัยเรื่อง “ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร”มีวัตถุประสงค์ (1) เพื่อศึกษาระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร และ (2) เพื่อเปรียบเทียบระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร จำแนกตามปัจจัยส่วนบุคคล โดยเป็นการวิจัยเชิงปริมาณ มีรูปแบบการวิจัยในเชิงสำรวจ ใช้แบบสอบถามเป็นเครื่องมือในการวิจัย ประชากรคือ บุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร กำหนดกลุ่มตัวอย่างจำนวน 170 คน

ผลการศึกษาพบว่า บุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร มีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์อยู่ในระดับมาก โดยเมื่อจำแนกตามปัจจัยส่วนบุคคลพบว่าบุคลากรในบริษัทเอกชนแห่งนี้ที่มี เพศ อายุ และประสบการณ์การทำงาน (อายุงาน) ที่ต่างกันมีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่ไม่แตกต่างกัน และในส่วนบุคลากรที่มีระดับการศึกษาสูงสุด แผนกที่สังกัด และประสบการณ์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ที่ต่างกัน มีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่แตกต่างกันอย่างมีนัยสำคัญทางสถิติ

รุ่งเรืองกิจ วงษ์ที (2565) ศึกษาเรื่อง ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโป่ง อำเภอหนองโดน จังหวัดสระบุรีการศึกษาวิจัยนี้ มีวัตถุประสงค์เพื่อศึกษาปัญหาของภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโป่ง อำเภอหนองโดน จังหวัดสระบุรี โดยผู้วิจัยรวบรวมความเห็นจากกลุ่มตัวอย่างจำนวน 180 คน และนำกลับมาวิเคราะห์ผลด้วยสถิติวิเคราะห์ค่าความถี่ ร้อยละ ผลวิจัยพบว่า การศึกษาปัญหาของภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโป่ง อำเภอหนองโดน จังหวัดสระบุรี ค่าเฉลี่ยอยู่ในระดับมากทุกองค์ประกอบ ทั้งในด้านความปลอดภัยการเข้าใช้งานอินเตอร์เน็ต ด้านการป้องกันข้อมูล

**กรอบแนวคิดในการวิจัย**




ภาพประกอบที่ 1.1 กรอบแนวความคิดในการวิจัย (ผู้วิจัย, 2568)

**ระเบียบวิธีวิจัย**

**ประชากรและกลุ่มตัวอย่าง**

โประชากรที่ใช้ในการศึกษาครั้งนี้ ได้แก่ ผู้สูงอายุที่มีอายุ 60 ปีขึ้นไป และมีการใช้งานโทรศัพท์มือถือที่เชื่อมต่ออินเทอร์เน็ตในประเทศไทย กลุ่มตัวอย่าง เนื่องจากผู้วิจัยไม่สามารถเข้าถึงข้อมูลรายชื่อผู้สูงอายุทั้งหมด จึงใช้การคำนวณขนาดกลุ่มตัวอย่างตามสูตรของ W.G. Cochran (1953) โดยกำหนดระดับค่าความเชื่อมันร้อยละ 95 และระดับค่าความคลาดเคลื่อน ร้อยละ 5 ทำให้ได้กลุ่มตัวอย่างรวมทั้งสิ้น 400 คน และใช้วิธีการสุ่มตัวอย่างแบบไม่ใช้หลักความน่าจะเป็น (Non-Probability Sampling) และวิธีการสุ่มแบบสโนว์บอล (Snowball Sampling)

**เครื่องมือที่ใช้ในการวิจัย**

ตอนที่ 1 แบบสอบถามเกี่ยวกับลักษณะทางประชากร เกี่ยวกับปัจจัยส่วนบุคคล ได้แก่ เพศ อายุ สถานภาพ รายได้เฉลี่ยต่อเดือน และระดับการศึกษา แบบสอบถามเป็นแบบตรวจสอบรายการ (Chech-List) จำนวน 5 ข้อ

ตอนที่ 2 แบบสอบถามเกี่ยวกับประสบการณ์เกี่ยวกับแบบสอบถามเชิงพฤติกรรมด้านการใช้งานและประสบการณ์ ซึ่งสามารถตอบได้มากกว่าหนึ่งคำตอบ แบบสอบถามเป็นแบบตรวจสอบรายการ (Chech-List) จำนวน 7 ข้อ

ตอนที่ 3 แบบสอบถามเกี่ยวกับการรับรู้ด้านประสิทธิภาพตนเองและต้นทุนการปฏิบัติตามมาตรการความปลอดภัย ประกอบด้วยข้อคำถามแบบมาตราส่วนประมาณค่า (Rating Scale) ซึ่งมีเกณฑ์ในการกำหนดค่าน้ำหนักของการประเมิน 5 ระดับ ตามวิธีของลิเคิร์ท (Likert) (ธานินทร์ ศิลป์จารุ, 2557: 77) จำนวน 5 ด้าน รวมทั้งสิ้น 20 ข้อ

ตอนที่ 4 การรับมือภัยคุกคามทางไซเบอร์ของผู้สูงอายุ ประกอบด้วยข้อคำถามแบบมาตราส่วนประมาณค่า (Rating Scale) ซึ่งมีเกณฑ์ในการกำหนดค่าน้ำหนักของการประเมิน 5 ระดับ ตามวิธีของลิเคิร์ท (Likert) (ธานินทร์ ศิลป์จารุ, 2557: 77) จำนวน 4 ด้าน รวมทั้งสิ้น 18 ข้อ

ตอนที่ 5 คำถามปลายเปิด ที่ถามความคิดเห็นของผู้ตอบแบบสอบถามเกี่ยวกับการรับมือและการตระหนักภัยทางไซเบอร์ ทั้งหมด 3 ข้อ

ตอนที่ 6 เป็นแบบสอบถามเพื่อรับฟังข้อเสนอแนะเพิ่มเติม

**การตรวจสอบคุณภาพของเครื่องมือ**

1. ตรวจสอบความตรงเชิงเนื้อหา (Content Validity) โดยการวิเคราะห์แบบสอบถาม ด้วยวิธี IOC: Index of item Objective Congruence จากผู้เชี่ยวชาญ จำนวน 3 ท่าน เพื่อหาค่าความเที่ยงตรงของแบบสอบถาม หรือค่าสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ ดำเนินการวิเคราะห์ผลจากแบบสอบถามด้วยโปรแกรมวิเคราะห์ข้อมูลทางสถิติ เกณฑ์การพิจารณาคือ ค่า IOC

2. ผลการทดสอบของแบบสอบถามโดยใช้โปรแกรมการวิเคราะห์ค่าทางสถิติ มีค่าสัมประสิทธิ์อัลฟาของความเชื่อถือได้ เท่ากับ 1 แสดงว่า ชุดข้อมูลแบบสอบถามมีความเชื่อถือได้

3. ทดสอบความเชื่อมั่น (Reliability) กับกลุ่มตัวอย่างนำร่อง 40 คน โดยใช้ค่าสัมประสิทธิ์แอลฟาของครอนบาค (Cronbach's Alpha)ได้ค่าเท่ากับ 0.956 แสดงถึงความเชื่อมั่นในระดับสูง

**การเก็บรวบรวมข้อมูล**

การวิจัยนี้เก็บรวบรวมข้อมูลโดยใช้แบบสอบถามออนไลน์ผ่าน Google Form จำนวน 400 ชุด จากกลุ่มตัวอย่างผู้สูงอายุ โดยเผยแพร่ผ่านช่องทางออนไลน์ และใช้วิธีการสุ่มตัวอย่างแบบ Snowball Sampling ให้ผู้ตอบแบบสอบถามส่งต่อไปยังผู้สูงอายุรายอื่นจนได้จำนวนครบตามที่กำหนด

**สถิติที่ใช้ในการวิเคราะห์ข้อมูล**

การวิเคราะห์ข้อมูลใช้โปรแกรมสำเร็จรูปทางสถิติ โดยใช้สถิติเชิงพรรณนาและสถิติเชิงอนุมาน ดังนี้

1. สถิติเชิงพรรณนา ได้แก่ ความถี่ ร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน เพื่ออธิบายข้อมูลส่วนบุคคล พฤติกรรมการใช้งานอินเทอร์เน็ต ประสบการณ์จากภัยคุกคามทางไซเบอร์ และระดับตัวแปรที่ศึกษา

2. สถิติเชิงอนุมาน ได้แก่ Independent Samples t-test และการวิเคราะห์ความแปรปรวนทางเดียว (One-way ANOVA: F-test) เพื่อเปรียบเทียบความแตกต่างของระดับการตระหนักรู้ภัยคุกคามทางไซเบอร์จำแนกตามปัจจัยส่วนบุคคลและประสบการณ์จากภัยคุกคามทางไซเบอร์

3. การเปรียบเทียบความแตกต่างเป็นรายคู่ (Multiple Comparisons) เพื่อวิเคราะห์ความแตกต่างของปัจจัยส่วนบุคคลด้านสถานภาพสมรส

4. การวิเคราะห์สหสัมพันธ์แบบเพียร์สัน (Pearson's Correlation) เพื่อศึกษาความสัมพันธ์ระหว่างความตระหนักรู้และพฤติกรรมการรับมือภัยคุกคามทางไซเบอร์

**ผลการวิจัย**

1. ข้อมูลทั่วไปของกลุ่มตัวอย่าง กลุ่มตัวอย่างผู้สูงอายุในประเทศไทยส่วนใหญ่เป็นเพศหญิง มีอายุระหว่าง 60–65 ปี มีสถานภาพสมรส ระดับการศึกษาต่ำกว่าปริญญาตรี และมีรายได้เฉลี่ยต่อเดือนต่ำกว่า 10,000 บาท สะท้อนให้เห็นว่าผู้สูงอายุส่วนใหญ่อยู่ในกลุ่มที่มีข้อจำกัดด้านรายได้

2. พฤติกรรมการใช้งานอินเทอร์เน็ตและประสบการณ์ภัยคุกคามทางไซเบอร์ ผู้สูงอายุส่วนใหญ่ใช้งานอินเทอร์เน็ตวันละ 1–3 ชั่วโมง โดยมีวัตถุประสงค์หลักเพื่อการติดต่อสื่อสารและความบันเทิง กลุ่มตัวอย่างส่วนใหญ่ไม่เคยประสบภัยคุกคามทางไซเบอร์ อย่างไรก็ตาม ผู้ที่เคยประสบภัยมักได้รับความเสียหายในระดับไม่สูง และประเมินว่าตนเองมีความรู้ด้านความปลอดภัยไซเบอร์อยู่ในระดับน้อยถึงปานกลาง

3. ระดับการรับรู้และความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ ผู้สูงอายุมีระดับการรับรู้ความเสี่ยง การรับรู้ความรุนแรงของภัย ประสิทธิภาพในตนเอง ประสิทธิผลของพฤติกรรมตอบสนอง ต้นทุนของการตอบสนอง พฤติกรรมการป้องกัน และการตระหนักรู้ โดยรวมอยู่ในระดับมาก แสดงให้เห็นว่าผู้สูงอายุรับรู้ถึงความสำคัญของภัยคุกคามทางไซเบอร์ แม้จะยังมีข้อจำกัดด้านทักษะเชิงปฏิบัติบางประการ

5. ผลการทดสอบสมมติฐาน ผลการวิเคราะห์พบว่า ปัจจัยส่วนบุคคลด้านเพศและสถานภาพสมรสส่งผลต่อระดับการตระหนักรู้ภัยคุกคามทางไซเบอร์ของผู้สูงอายุอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ขณะที่อายุ ระดับการศึกษา อาชีพ รายได้เฉลี่ยต่อเดือน และความถี่ในการใช้งานอินเทอร์เน็ตไม่

ส่งผลต่อระดับการตระหนักรู้ดังกล่าว นอกจากนี้ ผู้สูงอายุที่เคยประสบภัยคุกคามทางไซเบอร์มีระดับการรับรู้และการประเมินภัยสูงกว่าผู้ที่ไม่เคยประสบภัยอย่างชัดเจน

6. ความสัมพันธ์ระหว่างตัวแปร ผลการวิเคราะห์ความสัมพันธ์พบว่า การรับรู้ภัยคุกคาม ความเสี่ยงที่รับรู้ การรับรู้ความรุนแรงของภัย การตอบสนองต่อภัย ประสิทธิภาพในตนเอง และการประเมินภัยคุกคาม มีความสัมพันธ์กันในทิศทางเดียวกันทั้งหมด แสดงให้เห็นว่าองค์ประกอบด้านการรับรู้และการรับมือภัยคุกคามทางไซเบอร์ของผู้สูงอายุมีความเชื่อมโยงและส่งเสริมกันในเชิงบวก

**สรุปและอภิปรายผล**

1. ด้านปัจจัยส่วนบุคคลของผู้สูงอายุ ผลการวิจัยพบว่า กลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิง อายุระหว่าง 60–65 ปี มีสถานภาพสมรส ระดับการศึกษาต่ำกว่าปริญญาตรี และมีรายได้เฉลี่ยต่อเดือนค่อนข้างต่ำ ลักษณะดังกล่าวสะท้อนโครงสร้างประชากรผู้สูงอายุในประเทศไทยที่ผู้หญิงมีสัดส่วนมากกว่าผู้ชาย และอาจมีข้อจำกัดด้านทรัพยากรและทักษะดิจิทัล ซึ่งส่งผลต่อความเปราะบางต่อภัยคุกคามทางไซเบอร์ ผลการศึกษานี้สอดคล้องกับงานวิจัยที่ระบุว่าผู้สูงอายุเป็นกลุ่มเสี่ยงต่อภัยไซเบอร์เนื่องจากมีข้อจำกัดด้านทักษะการใช้เทคโนโลยีและการประเมินความเสี่ยง แม้จะมีการใช้งานอินเทอร์เน็ตเพิ่มขึ้นอย่างต่อเนื่อง

2. ด้านพฤติกรรมการใช้งานอินเทอร์เน็ตและประสบการณ์ภัยคุกคามทางไซเบอร์ ผลการวิจัยพบว่า ผู้สูงอายุส่วนใหญ่ใช้งานอินเทอร์เน็ตวันละ 1–3 ชั่วโมง โดยมีวัตถุประสงค์หลักเพื่อการติดต่อสื่อสารและความบันเทิง และมีเพียงบางส่วนที่ใช้เพื่อกิจกรรมที่มีความเสี่ยงสูง เช่น การซื้อขายสินค้าออนไลน์ แม้ว่าผู้สูงอายุส่วนใหญ่จะระบุว่าไม่เคยถูกหลอกจากภัยคุกคามทางไซเบอร์ แต่ยังพบว่ามีผู้สูงอายุจำนวนหนึ่งเคยได้รับผลกระทบ โดยเฉพาะด้านการเงิน ซึ่งเมื่อพิจารณาร่วมกับระดับรายได้ที่ไม่สูง ความเสียหายดังกล่าวย่อมส่งผลต่อคุณภาพชีวิต ผลการศึกษานี้สอดคล้องกับงานวิจัยก่อนหน้าที่ชี้ว่าประสบการณ์การเผชิญภัยไซเบอร์ส่งผลต่อความรู้สึกหวาดระแวงและพฤติกรรมการใช้งานเทคโนโลยีของผู้สูงอายุในระยะยาว

3. ด้านระดับการรับรู้และความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ ผลการวิจัยพบว่าผู้สูงอายุมีระดับการรับรู้ความเสี่ยง การรับรู้ความรุนแรงของภัย ประสิทธิภาพในตนเอง และพฤติกรรมการรับมือภัยคุกคามทางไซเบอร์โดยรวมอยู่ในระดับมาก แสดงให้เห็นว่าผู้สูงอายุตระหนักถึงความสำคัญของภัยคุกคามทางไซเบอร์ อย่างไรก็ตาม เมื่อพิจารณาเชิงลึก พบว่าผู้สูงอายุยังมีข้อจำกัดด้านทักษะเชิงเทคนิค เช่น การตั้งค่าความปลอดภัยของอุปกรณ์ การตั้งรหัสผ่านที่ซับซ้อน และการใช้ระบบยืนยันตัวตนหลายขั้นตอน ซึ่งสอดคล้องกับแนวคิดทฤษฎีแรงจูงใจในการป้องกัน (Protection Motivation Theory: PMT) ที่ชี้ว่าการรับรู้ภัยเพียงอย่างเดียวอาจยังไม่เพียงพอ หากขาดการสนับสนุนด้านทักษะและความสะดวกในการปฏิบัติ

**ข้อเสนอแนะ**

**ข้อเสนอแนะในการนำไปใช้**

จากผลการวิจัยเกี่ยวกับความตระหนักรู้และการตอบสนองต่อภัยคุกคามทางไซเบอร์ของผู้สูงอายุ สามารถเสนอแนวทางเพื่อพัฒนาการป้องกันและเพิ่มความปลอดภัยด้านไซเบอร์ในสังคมไทยได้ดังนี้

1. ข้อเสนอแนะเชิงนโยบายต่อหน่วยงานรัฐ หน่วยงานภาครัฐควรพัฒนาและดำเนินโครงการอบรมด้านความปลอดภัยไซเบอร์สำหรับผู้สูงอายุอย่างต่อเนื่อง โดยอาศัยเครือข่ายในชุมชน เช่น อสม. ศูนย์ผู้สูงอายุ หรือองค์กรปกครองส่วนท้องถิ่น นอกจากนี้ควรผลิตสื่อรณรงค์ที่เข้าใจง่าย เช่น วิดีโอสั้นและอินโฟกราฟิก เพื่อให้ผู้สูงอายุสามารถเข้าถึงข้อมูลได้สะดวก รวมทั้งควรส่งเสริมความร่วมมือระหว่างภาครัฐ เอกชน และชุมชน เพื่อร่วมกันป้องกันภัยไซเบอร์และให้ข้อมูลเตือนภัยรูปแบบใหม่อย่างทันเหตุการณ์

2. ข้อเสนอแนะสำหรับหน่วยงานหรือองค์กรที่เกี่ยวข้องกับผู้สูงอายุควรออกแบบบริการดิจิทัลที่เหมาะสมกับลักษณะการใช้งานของผู้สูงอายุ เช่น ปุ่มขนาดใหญ่ ตัวอักษรชัดเจน ขั้นตอนน้อย และระบบยืนยันตัวตนที่ไม่ซับซ้อน ควรมีระบบแจ้งเตือนภัยไซเบอร์แบบเรียลไทม์ เพื่อช่วยให้ผู้สูงอายุสามารถรับรู้ถึงเหตุการณ์หรือรูปแบบการหลอกลวงใหม่ได้ทันที

3. ข้อเสนอแนะสำหรับผู้ดูแล ครอบครัว และชุมชน ครอบครัวและผู้ดูแลควรมีบทบาทสำคัญในการให้คำแนะนำ เช่น การตั้งรหัสผ่านที่ปลอดภัย การตรวจสอบลิงก์ปลอม และการปกป้องข้อมูลส่วนตัว ควรสร้างสภาพแวดล้อมที่เอื้อต่อการเรียนรู้ ให้ผู้สูงอายุรู้สึกว่าขอความช่วยเหลือได้ตลอดเวลา เพื่อเพิ่มความมั่นใจในการใช้งานเทคโนโลยี

**ข้อเสนอแนะเชิงวิชาการสำหรับการวิจัยครั้งต่อไป**

1. ควรขยายกลุ่มตัวอย่างให้ครอบคลุมหลายภูมิภาคทั่วประเทศ เพื่อให้ผลการวิจัยสะท้อนสภาพจริงได้แม่นยำยิ่งขึ้น รวมทั้งควรใช้วิธีวิจัยเชิงคุณภาพ เช่น การสัมภาษณ์เชิงลึก เพื่อให้เข้าใจประสบการณ์และมุมมองของผู้สูงอายุเกี่ยวกับภัยไซเบอร์ได้ละเอียดและลึกซึ้งมากขึ้น

2. ควรศึกษาเพิ่มเติมเกี่ยวกับตัวแปรอื่นที่อาจมีผลต่อความตระหนักรู้ด้านภัยไซเบอร์ เช่น ระดับทักษะดิจิทัล ความวิตกกังวลต่อเทคโนโลยี หรือบทบาทของครอบครัวและชุมชนในการสร้างความรู้เท่าทัน รวมถึงศึกษาปัจจัยที่เอื้อต่อการนำความรู้ไปใช้จริงในชีวิตประจำวัน

**เอกสารอ้างอิง**


กฤชนัท เหล่ากอ และสมบูรณ์ สุขสำราญ. (2567). การตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในจังหวัดปทุมธานี. *วารสารสันติศึกษาปริทรรศน์ มจร., 9*(2), 177-189.

กองบัญชาการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี. (2568). *รายงานสถิติอาชญากรรมออนไลน์ประจำเดือนกรกฎาคม 2568*. สำนักงานตำรวจแห่งชาติ. ค้นเมื่อ 14 ตุลาคม 2568, จาก https://www.pct.go.th

ธนาคารแห่งประเทศไทย. (2568). *ภัยทุจริตทางการเงินและการป้องกันภัยออนไลน์*. ค้นเมื่อ 14 ตุลาคม 2568, จาก https://www.bot.or.th

ธนินทร์ ศิลปจารุ. (2557). *การวิจัยและการวิเคราะห์ข้อมูลทางสถิติด้วย SPSS และ AMOS* (พิมพ์ครั้งที่ 15). กรุงเทพฯ: วี.อินเตอร์ พริ้นท์.

*พระราชกำหนดการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566*. (2566). ราชกิจจานุเบกษา, เล่ม 140 ตอนที่ 18 ก, หน้า 1–41.

เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี. (2565). ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร. *วารสารวิชาการไทยวิจัยและการจัดการ, 3*(2), 4-16.

รุ่งเรืองกิจ วงษ์ธี. (2565). ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของชุมชนตำบลบ้านโปร่ง อำเภอหนองโดน จังหวัดสระบุรี. *วารสารไตรศาสตร์, 8*(1), 51-61.

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2567). *ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล*. ค้นเมื่อ 15 ตุลาคม 2568, จาก https://www.pdpc.or.th

สำนักงานตำรวจแห่งชาติ. (2566). *ระบบแจ้งความออนไลน์ (Thai Police Online)*. ค้นเมื่อ 30 กรกฎาคม 2568, จาก https://www.thaipoliceonline.go.th

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2566). *พฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย*. ค้นเมื่อ 17 ตุลาคม 2568, จาก https://www.etda.or.th

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2566). *แนวทางการใช้งานอินเทอร์เน็ตอย่างปลอดภัยสำหรับประชาชน*. ค้นเมื่อ 17 ตุลาคม 2568, จาก https://www.etda.or.th

สำนักงานสถิติแห่งชาติ. (2567). *สรุปผลสำคัญการทำงานของผู้สูงอายุในประเทศไทย พ.ศ. 2567*. ค้นเมื่อ 20 พฤศจิกายน 2568, จาก https://www.nso.go.th

Chou, Y. K., & Chou, C. (2021). Digital safety behavior and self-efficacy among older adults. *Journal of Cybersecurity Studies, 6*(2), 89–104.

Cochran, W. G. (1953). *Sampling techniques*. New York: John Wiley & Sons.

Duval, T. S., & Wicklund, R. A. (1972). *A theory of objective self-awareness*. New York: Academic Press.

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. Retrieved October 14, 2025, from https://www.enisa.europa.eu

Folkman, S. (Ed.). (2011). *The Oxford handbook of stress, health, and coping*. New York: Oxford University Press.

Folkman, S., & Moskowitz, J. T. (2004). Coping: Pitfalls and promise. *Annual Review of Psychology, 55*(1), 745-774. https://doi.org/10.1146/annurev.psych.55.090902.141456

Haslinda, N., Abdullah, N. H., Zainal, A., & Rahman, R. A. (2025). Cybersecurity awareness among older adults in Malaysia. *Malaysian Journal of Gerontology, 12*(2), 44-59.

Lazarus, R. S., & Folkman, S. (1984). *Stress appraisal and coping*. New York: Springer Publishing.

Li, Y., Xue, Y., Liang, H., & Yan, H. (2022). Understanding cybersecurity protection behavior in organizations: An extended protection motivation theory perspective. *Information & Computer Security, 30*(2), 1-18.

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

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

WeAreSocial. (2025). *Digital 2025: Thailand*. Retrieved October 14, 2025, from https://wearesocial.com