

การรับมือภัยทางไซเบอร์ของผู้สูงอายุ: ความท้าทายใหม่ของสังคมไทย

Addressing Cyber Threats for the Elderly: A New Challenge for Thai Society

ขวัญตา เบ็ญจะจันทร์ (Khwanta Benchakhan)¹

ไผพจน์ กุลาชัย (Waiphot Kulachai)²

ปฏิพล หอมยามเย็น (Patipol Homyamyen)³

ขันอุทร เพชรราศี (Khanouthone Phetlasy)⁴

¹อาจารย์, วิทยาลัยการเมืองและการปกครอง มหาวิทยาลัยราชภัฏสวนสุนันทา

Lecturer, College of Politics and Government, Suan Sunandha Rajabhat University

²ผู้ช่วยศาสตราจารย์ พันตำรวจโท ดร., วิทยาลัยการเมืองและการปกครอง มหาวิทยาลัยราชภัฏสวนสุนันทา

Asst.Prof. Pol.Lt.Col. Dr., College of Politics and Government Suan Sunandha Rajabhat University

^{3,4}นักศึกษาระดับปริญญาเอก สาขาการเมืองการปกครอง วิทยาลัยการเมืองและการปกครอง

มหาวิทยาลัยราชภัฏสวนสุนันทา

Doctoral student, Politics and Government Program, College of Politics and Government

Suan Sunandha Rajabhat University

E-mail: khwanta.be@ssru.ac.th

Received: 6 November 2024

Revised: 23 December 2024

Accepted: 23 December 2024

บทคัดย่อ

สาระสำคัญของบทความวิชาการนี้มีวัตถุประสงค์เพื่อสรุปประเด็นความท้าทายของผู้สูงอายุเกี่ยวกับการรับมือภัยทางไซเบอร์ในสังคมไทยปัจจุบัน รวมถึงการหาข้อเสนอแนะเชิงนโยบาย โดยทำการทบทวนแนวคิดที่เกี่ยวข้องกับภัยทางไซเบอร์ที่พบบ่อยสำหรับผู้สูงอายุ ผลกระทบของความเสียหายทางไซเบอร์ต่อผู้สูงอายุ และกลยุทธ์การรับมือจากภัยทางไซเบอร์ของผู้สูงอายุ ซึ่งทำให้ได้ข้อสรุปด้านความท้าทายใหม่และข้อเสนอแนะเชิงนโยบายเกี่ยวกับการรับมือภัยทางไซเบอร์ของผู้สูงอายุของสังคมไทยพบว่า ผู้สูงอายุมักจะขาดความรู้ทางเทคโนโลยีและทักษะในการจัดการข้อมูลส่วนตัวบนแพลตฟอร์มดิจิทัลทำให้เกิดความเสี่ยงต่อการถูกหลอกลวงทางการเงินและการโจมตีทางไซเบอร์ นอกจากนี้ การใช้โซเชียลมีเดียและเทคโนโลยีต่าง ๆ ยังเป็นช่องทางให้ผู้สูงอายุต้องเผชิญกับปัญหาการรั่วไหลของข้อมูลส่วนบุคคลและการถูกละเมิดสิทธิส่วนตัว

ในด้านข้อเสนอแนะเชิงนโยบาย พบว่า การปกป้องผู้สูงอายุจากภัยคุกคามทางไซเบอร์ในสังคมไทย จำเป็นต้องพัฒนานโยบายและกลยุทธ์ที่หลากหลาย ซึ่งรวมถึงการสร้างโปรแกรมการศึกษาและอบรมทั้งแบบออนไลน์และออฟไลน์เพื่อเพิ่มความตระหนักรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ การตอบสนองต่อความท้าทายเหล่านี้ต้องมาจากความร่วมมือของทุกภาคส่วนในสังคม รวมถึงการปรับปรุงนโยบายและกฎหมายให้ทันสมัยเพื่อคุ้มครองผู้สูงอายุจากภัยทางไซเบอร์ที่เพิ่มขึ้น

คำสำคัญ: การรับมือ, ภัยทางไซเบอร์ของผู้สูงอายุ, ความท้าทายใหม่, สังคมไทย

Abstract

The central purpose of this academic article is to summarize the challenges faced by the elderly in dealing with cyber threats within contemporary Thai society, including suggestions for policy recommendations. It reviews concepts related to common cyber threats to the elderly, the impact of cyber risks on them, and their strategies for coping with such dangers, leading to new challenge conclusions and policy recommendations on elder cyber threat management in Thai society. It was found that the elderly often lack technological knowledge and skills in managing personal data on digital platforms, leading to risks of financial fraud and cyber-attacks. Furthermore, the use of social media and various technologies opens avenues for personal data leaks and privacy violations for the elderly.

In terms of policy recommendations, it is essential to develop diverse policies and strategies to protect the elderly from cyber threats in Thai society. These include creating both online and offline educational and training programs to enhance cyber security awareness. Responding to these challenges requires cooperation from all sectors of society, including modernizing policies and laws to safeguard the elderly from the increasing cyber threats.

Keywords: Addressing, Cyber Threats for the Elderly, New Challenges, Thai Society

บทนำ

สถานการณ์ความปลอดภัยทางไซเบอร์ทั่วโลกและในประเทศไทยมีความซับซ้อนและต้องเผชิญกับความท้าทายหลายประการ การเพิ่มขึ้นอย่างรวดเร็วของผู้ใช้สมาร์ทโฟนทั่วโลก ซึ่งมีมากถึง 3 พันล้านคนในปี 2020 ตามข้อมูลจาก Jakkrit Chuamuangphan (2020) ได้ทำให้ภาครัฐเป็นเป้าหมายหลักของภัยคุกคามทางไซเบอร์ ในประเทศไทย การเข้าถึงอินเทอร์เน็ตที่เพิ่มขึ้นได้กระตุ้นให้รัฐบาลต้องเสริมสร้างมาตรการป้องกันจากไซเบอร์ จากการศึกษาของ Narong Chaiwut and Worasak Rueangsirarak (2022)

ประเทศไทยได้บังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act: PDPA) เพื่อกำหนดให้องค์กรต่าง ๆ ต้องปฏิบัติตามมาตรการความปลอดภัยทางไซเบอร์ที่เข้มงวด ตามการศึกษา Pavin Chachavalpongpun (2022) กล่าวว่าสถานการณ์เหล่านี้ยืนยันถึงความจำเป็นในการพัฒนากลยุทธ์และวิธีการต่าง ๆ ที่มุ่งเสริมความปลอดภัยทางไซเบอร์ทั้งในระดับโลกและในประเทศไทย

การพัฒนาเทคโนโลยีอย่างรวดเร็วทำให้รูปแบบการโจมตีทางไซเบอร์ก็พัฒนาไปตามการค้นห และนำเสนอวิธีการใหม่ ๆ ของแฮกเกอร์/อาชญากรไซเบอร์ (Hacker) ในการโจมตีผู้ใช้งาน สิ่งนี้ส่งผลให้องค์กรต่าง ๆ จำเป็นต้องปรับเปลี่ยนและพัฒนาวิธีการป้องกันเพื่อตอบสนองต่อภัยคุกคามที่เพิ่มพูนรุนแรงและความซับซ้อนขึ้นอย่างต่อเนื่อง ในประเทศไทยเองก็ต้องเผชิญกับภัยคุกคามทางไซเบอร์ที่หลากหลาย ตลอดช่วงห้าปีที่ผ่านมาประเทศไทยมีเหตุการณ์ความไม่ปลอดภัยด้านข้อมูลส่วนบุคคลหลายครั้งที่สร้างผลกระทบต่อสังคมอย่างมาก SOSECURE (2024) ได้รวบรวมข้อมูลเกี่ยวกับเหตุการณ์โจมตีทางไซเบอร์ซึ่งเคยเกิดขึ้นในประเทศไทย ซึ่งมีรายละเอียดดังนี้ ในปี 2561 ข้อมูลส่วนตัวของลูกค้าบริษัท ค่ายสัญญาณมือถือแห่งหนึ่ง ได้หลุดรั่วออกมาจากระบบ ต่อมาในปี 2563 โรงพยาบาลแห่งหนึ่งในไทยต้องเผชิญกับการโจมตีด้วย Ransomware หรือ Malware เรียกค่าไถ่ ซึ่งทำให้ระบบข้อมูลคนไข้ของโรงพยาบาลถูกล็อก ส่งผลให้ไม่สามารถเข้าถึงข้อมูลเพื่อทำการรักษาได้ ในปี 2564 บริษัทเกี่ยวกับด้านอาหารก็ถูกแฮกข้อมูลลูกค้า ซึ่งหลุดออกไปเป็นชื่อ-นามสกุล ที่อยู่ หมายเลขโทรศัพท์ และอีเมล ปี 2565 ข้อมูลนักเรียนไทยรั่วไหลออกมา มีข้อมูลถึงกว่า 23,000 รายการ และในปีล่าสุด 2566 อาชญากรไซเบอร์ (Hacker) ที่ใช้นามแฝงว่า 9near ได้ประกาศขายข้อมูลส่วนตัวของคนไทยถึง 55 ล้านคน รวมถึงชื่อ-นามสกุล ที่อยู่ วันเกิด เลขบัตรประชาชน และเบอร์โทรศัพท์ที่เป็นหมายเลขใช้งานจริงที่ลงทะเบียนไว้กับหน่วยงานรัฐ

ดังนั้น สถานการณ์ความปลอดภัยทางไซเบอร์ทั่วโลกและในประเทศไทยมีความซับซ้อนและต้องเผชิญกับความท้าทายหลายประการ รวมถึงกลุ่มผู้ใช้ข้อมูลในภาคประชาชนต้องระมัดระวังการให้ข้อมูลเป็นอย่างมาก เนื่องจากมีความเสี่ยงต่อการถูกคุกคามทางไซเบอร์ อีกทั้งสำหรับประเทศไทยต้องมีการป้องกันและรับมือกับการคุกคามทางไซเบอร์อย่างมาก เนื่องจากมีผู้ใช้หรือประชาชนจำนวนมากที่ไม่ระมัดระวังในการเข้าถึงข้อมูล หรือการแลกเปลี่ยนข้อมูลในโลกออนไลน์ เช่น แสดงข้อมูลส่วนบุคคลบนเฟสบุ๊ก (Facebook) โดยไม่มีการตั้งค่าความเป็นส่วนตัว ส่งผลให้เกิดความเสี่ยงในการรั่วไหลของข้อมูลส่วนบุคคล (Laohabut et al., 2021)

นอกจากนี้ NEWS.CH7 (2567) ได้สรุปข้อมูลจากศูนย์วิจัย Krungthai COMPASS ที่ได้ให้ข้อมูลเกี่ยวกับสถิติการใช้อินเทอร์เน็ตของคนไทย พบว่า ปริมาณผู้ใช้งาน อินเทอร์เน็ต (Internet) และ โซเชียลมีเดีย (Social Media) ปัจจุบันมีผู้ใช้งาน อินเทอร์เน็ต (Internet) 63.2 ล้านคน หรือคิดเป็น 88% ของประชากรทั้งหมด และมีผู้ใช้งาน Social Media 49.1 ล้านคน หรือคิดเป็น 68.3% ของประชากรทั้งหมด เจเนอเรชัน Y (Generation Y) เป็นกลุ่มที่มีการใช้งานอินเทอร์เน็ต (Internet) และ โซเชียลมีเดีย (Social Media) สูงสุด ขณะที่ชาว Baby Boomer (กลุ่มผู้สูงวัย ที่มีอายุระหว่าง 54 - 72 ปี) เป็นกลุ่มที่มีจำนวนผู้ใช้งานเพิ่มขึ้นอย่างมี

นัยสำคัญ สอดคล้องกับสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) ได้ให้ข้อมูล พฤติกรรมการใช้อินเทอร์เน็ตของคนไทยในปี 2566 พบว่า กลุ่มผู้สูงอายุ (อายุ 55 - 74 ปี) สามารถเข้าถึงและ ใช้งานอินเทอร์เน็ตได้มากขึ้นจากเดิม 63.10% เพิ่มขึ้นเกือบ 10% เป็น 71.60% (ไทยรัฐออนไลน์, 2566) อีกทั้งยังสอดคล้องกับการศึกษาของ Kanyarat Sriwisathiyakun and Chawaporn Dhamanitayakul (2022) ได้เน้นย้ำถึงการใช้งานแพลตฟอร์มดิจิทัลของผู้สูงอายุในประเทศไทย พบว่า มีการใช้สมาร์ตโฟนสูงถึง 93.60% โดยแอปพลิเคชันที่ได้รับความนิยมมากที่สุด ได้แก่ ไลน์ (Line) ที่ 4.08% Youtube ที่ 3.71% และ เฟสบุ๊ก (Facebook) ที่ 3.61% ซึ่งสะท้อนถึงการเปลี่ยนแปลงทางเทคโนโลยีในกลุ่มผู้สูงอายุที่มีการใช้ แพลตฟอร์มดิจิทัลเพิ่มขึ้น และในปีที่ผ่านมา ผู้สูงอายุในประเทศไทยยังคงเป็นกลุ่มที่มีความเสี่ยงต่อการตก เป็นเหยื่ออาชญากรรมไซเบอร์อย่างต่อเนื่อง ข้อมูลจากสำนักงานตำรวจแห่งชาติระบุว่า ระหว่างวันที่ 1 มีนาคม 2565 ถึง 30 มิถุนายน 2567 มีการแจ้งความออนไลน์จำนวน 575,507 เรื่อง คิดเป็นมูลค่าความเสียหายรวมกว่า 65,715 ล้านบาท โดยกลุ่มผู้สูงอายุ (อายุ 60 ปีขึ้นไป) คิดเป็นประมาณ 6.42% ของเหยื่อ ทั้งหมด แม้จะไม่ใช่อายุที่มีจำนวนเหยื่อมากที่สุด แต่ความเสียหายที่เกิดขึ้นยังคงมีนัยสำคัญ (สำนักงาน ตำรวจแห่งชาติ, 2567) นอกจากนี้ สายด่วน 1185 AIS Spam Report Center พบว่ามีการแจ้งเบอร์โทรและ ข้อความ SMS ที่คาดว่าจะเป็ฯมิจฉาชีพกว่า 1.6 ล้านครั้งตั้งแต่เริ่มเปิดให้บริการ โดยมีการจับกุมมิจฉาชีพได้ อย่างต่อเนื่องในช่วงปีที่ผ่านมา (ประชาชาติธุรกิจ, 2566) ข้อมูลเหล่านี้สะท้อนถึงความจำเป็นในการ เสริมสร้างทักษะด้านดิจิทัลและสร้างความตระหนักรู้เกี่ยวกับภัยไซเบอร์ให้แก่ผู้สูงอายุ เพื่อให้พวกเขา สามารถใช้งานเทคโนโลยีได้อย่างปลอดภัยและลดความเสี่ยงจากการตกเป็นเหยื่อของอาชญากรรมไซเบอร์

โดยการศึกษาของ Tanpat Kraiwanit and Kris Jangjarat (2023) ได้ชี้ให้เห็นถึงกิจกรรมออนไลน์ ที่ได้รับความนิยมจากผู้สูงอายุในประเทศไทย ซึ่งรวมถึงการได้ตอบทางสังคม ความบันเทิง การชำระเงิน ออนไลน์ การซื้อสินค้าออนไลน์ การค้นหาข้อมูล การติดตามข้อมูล และการสนทนา กิจกรรมเหล่านี้มี บทบาทสำคัญในการช่วยให้ผู้สูงอายุสามารถรักษาความสัมพันธ์กับผู้อื่น ข้อมูลและเป็นอิสระทางการเงินได้ การแบ่งปันความรู้ผ่าน โซเชียลเน็ตเวิร์กออนไลน์ (Kanyarat Sriwisathiyakun and Chawaporn Dhamanitayakul, 2022) กิจกรรมเหล่านี้มีความสำคัญสำหรับผู้สูงอายุในประเทศไทยเนื่องจากมีส่วนช่วย ในการรักษาความสัมพันธ์ ข้อมูลและเป็นอิสระทางการเงิน โซเชียลเน็ตเวิร์กออนไลน์ที่ออกแบบมา โดยเฉพาะสำหรับผู้สูงอายุได้รับการแสดงให้เห็นว่าตอบสนองความต้องการของกลุ่มผู้สูงอายุได้อย่างมี ประสิทธิภาพ

ดังนั้น จากการศึกษาข้างต้นแสดงให้เห็นถึงการใช้งานแพลตฟอร์มดิจิทัลซึ่งเป็นส่วนหนึ่งของ ชีวิตประจำวันของผู้สูงอายุในไทย และมีส่วนสำคัญในการช่วยให้ผู้สูงอายุมีส่วนร่วมในสังคมมากขึ้น อีกทั้ง ยังเพิ่มความสามารถในการเข้าถึงบริการต่าง ๆ และมีอิสระในชีวิตการดำเนินชีวิตของตนเองมากขึ้นอย่างไร ก็ตาม ปัญหาหลักเกี่ยวกับผู้สูงอายุและภัยคุกคามทางไซเบอร์ในประเทศไทย พบว่า ผู้สูงอายุในประเทศไทย มีการใช้เทคโนโลยีดิจิทัลเพิ่มขึ้น ด้วยข้อจำกัดทางด้านความเข้าใจและความชำนาญในการใช้งานเทคโนโลยี

ที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็วอาจส่งผลให้ผู้สูงอายุตกเป็นเหยื่อของภัยทางไซเบอร์ได้ง่ายกว่าประชากรกลุ่มอื่น (Tanpat Kraiwanit and Kris Jangjarat, 2023) การรู้หนังสือทางอินเทอร์เน็ตยังคงเป็นปัญหาสำหรับผู้สูงอายุ โดยหลายคนขาดทักษะในการจดจำอีเมลที่เป็นสแปม ซึ่งอาจทำให้ต้องเผชิญกับความเสี่ยงในการถูกโจมตีทางไซเบอร์หรือการใช้งานที่ไม่ปลอดภัย (Diteeyont and Ku, 2021)

จากความสำคัญดังกล่าว บทความนี้จึงมีวัตถุประสงค์เพื่อสรุปประเด็นความท้าทายของผู้สูงอายุเกี่ยวกับการรับมือภัยทางไซเบอร์ในสังคมไทยปัจจุบัน รวมถึงการหาข้อเสนอแนะและนโยบาย เพื่อให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องร่วมกันพัฒนานโยบายและกลยุทธ์ที่เหมาะสมในการช่วยเหลือและป้องกันผู้สูงอายุจากภัยทางไซเบอร์ เพื่อเป็นแนวทางในการสร้างความตระหนักรู้ การรักษาความปลอดภัยที่เพิ่มขึ้น และการรับมือจากภัยทางไซเบอร์ในสังคมผู้สูงอายุของสังคมไทย

ภัยทางไซเบอร์ที่พบบ่อยสำหรับผู้สูงอายุ

ผู้สูงอายุมักจะเผชิญกับภัยคุกคามทางไซเบอร์ที่เฉพาะเจาะจงเนื่องจากปัจจัยหลายอย่างรวมถึงการเข้าใจเทคโนโลยีที่จำกัด การขาดความรู้เกี่ยวกับแนวทางป้องกันตนเองบนอินเทอร์เน็ต และอาจมีความไว้วางใจในสื่อออนไลน์มากเกินไป ภัยหรือความเสี่ยงทางไซเบอร์ที่พบบ่อยสำหรับผู้สูงอายุ มีดังต่อไปนี้

1. ความเสี่ยงทั่วไปต่อภัยคุกคามทางไซเบอร์ ซึ่งผู้สูงอายุมักจะถูกกลุ่มอาชญากรไซเบอร์ใช้เป็นเป้าหมาย เนื่องจากมีความรู้เกี่ยวกับเทคโนโลยีดิจิทัลและความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่จำกัด (Saariluoma, 2016) เนื่องจากความเข้าใจเกี่ยวกับเทคโนโลยีที่จำกัด ผู้สูงอายุอาจมีความเข้าใจที่จำกัดเกี่ยวกับเทคโนโลยีใหม่ๆ และวิธีการทำงานของอินเทอร์เน็ต ทำให้มีความเสี่ยงต่อการหลงเชื่อในข้อมูลหลอกลวงและเป็นเป้าหมายของการโจมตี (Wiederhold, 2020)

2. การหลอกลวงทางการเงินและการฉ้อโกง ผู้สูงอายุมีความเสี่ยงสูงต่อการหลอกลวงทางการเงินและการฉ้อโกง โดยเฉพาะผ่านการหลอกลวงออนไลน์ เช่น โทรศัพท์หลอกลวงที่แอบอ้างว่าเป็นตัวแทนจากองค์กรนำเชื่อถือ เพื่อให้โอนเงินหรือเปิดเผยข้อมูลส่วนตัว (Sugunaraj Ramchandra, and Ranganathan, 2022) ความรู้ด้านความปลอดภัยไซเบอร์ที่จำกัด เช่น การตั้งค่าความปลอดภัยและการใช้รหัสผ่านที่ปลอดภัย ยังเพิ่มความเสี่ยง (Anderson and Rainie, 2017) กรณีที่พบบ่อยในไทย เช่น “แก๊งคอลเซ็นเตอร์” ซึ่งหลอกลวงผ่านโทรศัพท์หรือ SMS โดยแอบอ้างเป็นเจ้าของหน้าที่จากธนาคารหรือหน่วยงานรัฐ เช่น ตำรวจหรือโรงพยาบาล (Cyber Crime Investigation Bureau, 2020) เหตุการณ์ที่ผู้สูงอายุในจังหวัดเชียงใหม่สูญเสียเงินกว่า 1 ล้านบาท เป็นตัวอย่างที่ชี้ให้เห็นถึงความเร่งด่วนในการแก้ไขปัญหาผ่านมาตรการให้ความรู้ ปรับปรุงกฎหมาย และพัฒนากลไกตอบสนองที่รวดเร็ว (ประชาชาติธุรกิจ, 2566)

3. ความเสี่ยงทางข้อมูลสุขภาพ ข้อมูลสุขภาพของผู้สูงอายุเป็นเป้าหมายสำคัญของอาชญากรไซเบอร์ เนื่องจากมีมูลค่าสูงในตลาดมืด ข้อมูลเหล่านี้มักถูกนำไปใช้ในหลอกลวงด้านการรักษาพยาบาล การขายเพื่อการโฆษณาเป้าหมาย หรือการโจมตีทางไซเบอร์ เช่น การเรียกค่าไถ่ (Alexandru, Ianculescu, Giura and Pop, 2022) ข้อมูลในระบบสุขภาพอิเล็กทรอนิกส์ (EHRs) ยังมีความเสี่ยงสูงต่อการถูกโจรกรรม

เนื่องจากมีข้อมูลทางการแพทย์และการเงินที่อาจนำไปใช้ในการฉ้อโกง (Kruse et al., 2017) นอกจากนี้ อุปกรณ์ตรวจสุขภาพที่เชื่อมต่ออินเทอร์เน็ต (IoT) อาจมีช่องโหว่ด้านความปลอดภัย ทำให้อาชญากรไซเบอร์สามารถเข้าถึงและขโมยข้อมูลได้ (Jiang and Bai, 2020) ปัญหานี้สะท้อนถึงความจำเป็นในการเสริมสร้างมาตรการป้องกันข้อมูลสุขภาพให้แข็งแกร่งยิ่งขึ้น

4. การโจมตีด้วยฟิชชิงและข้อมูลเท็จ การหลอกลวงผ่านอีเมล (Phishing) มีการส่งอีเมลที่ดูเหมือนจะมาจากแหล่งที่น่าเชื่อถือ เช่น ธนาคาร หรือหน่วยงานรัฐ โดยมีจุดประสงค์เพื่อให้ผู้รับกรอกข้อมูลส่วนบุคคลหรือข้อมูลทางการเงินที่สำคัญ การโจมตีด้วยฟิชชิงเป็นเรื่องที่พบบ่อย โดยใช้ความไว้วางใจ และความเข้าใจ ซึ่งเป็นข้อจำกัดของผู้สูงอายุเกี่ยวกับความถูกต้องของข้อมูลออนไลน์ (Narayanan et al., 2021) สอดคล้องกับผลการศึกษาของ Nigel Martin, and Rice (2013) ได้กล่าวว่า ผู้สูงอายุอาจอ่อนไหวต่อการฉ้อโกงออนไลน์มากขึ้น เนื่องจากปัจจัยต่าง ๆ เช่น ความรู้ความเข้าใจลดลง ลักษณะความไว้วางใจ และความเหงา เนื่องจากผู้สูงอายุพึ่งพาเทคโนโลยีในกิจกรรมประจำวันมากขึ้นจึงมีความเสี่ยงต่อความเสี่ยงทางไซเบอร์มากขึ้น

5. การขาดการศึกษาด้านไซเบอร์ ประเด็นดังกล่าวมีความจำเป็นอย่างยิ่งที่จะต้องมีการศึกษาด้านไซเบอร์ที่มีประสิทธิภาพและออกแบบมาเพื่อผู้สูงอายุ เพื่อปรับปรุงความสามารถในการระบุและหลีกเลี่ยงความเสี่ยงทางไซเบอร์ของผู้สูงอายุมากขึ้น (Blackwood-Brown, Levy and D'Arcy, 2019) การหลอกลวงเกี่ยวกับการลงทุน (Investment Scams) อาชญากรไซเบอร์ (Hacker) มักเสนอโอกาสในการลงทุนที่ “ดีเกินจริง” เพื่อล่อลวงผู้สูงอายุให้ลงทุนด้วยเงินจำนวนมากในสิ่งที่ไม่มียุ่จริง เช่น เหตุการณ์ที่ผู้สูงอายุถูกล่อลวงให้ลงทุนในโครงการที่ไม่มียุ่จริง โดยมีแฮ็กเกอร์แอบอ้างว่าเป็นตัวแทนจากบริษัทการลงทุนที่มีชื่อเสียง (ThaiCERT, 2021)

6. ความเสี่ยงของการใช้โซเชียลมีเดีย การใช้โซเชียลมีเดียของผู้สูงอายุมีความเสี่ยงต่อข้อมูลเท็จ และการหลอกลวง เช่น การปลอมแปลงตัวตนบนโซเชียลมีเดีย (Identity Theft) ซึ่งมักเกี่ยวข้องกับการสร้างโปรไฟล์ปลอมเพื่อหลอกลวงและขโมยข้อมูลส่วนตัว (Mihelić and Žvanut, 2022) ผู้สูงอายุมีแนวโน้มไว้วางใจข้อมูลที่ได้รับจากอินเทอร์เน็ต ซึ่งอาจนำไปสู่การแบ่งปันข้อมูลส่วนตัวโดยไม่ได้ตรวจสอบความถูกต้องของแหล่งที่มา (Holtfreter, Reisig and Pratt, 2018) ความเสี่ยงเหล่านี้เน้นถึงความสำคัญของการพัฒนาแนวทางป้องกันและเสริมสร้างความรู้ด้านความปลอดภัยในโลกโซเชียลมีเดียให้กับผู้สูงอายุ

7. ความเสี่ยงของอุปกรณ์อัจฉริยะ อุปกรณ์อัจฉริยะที่ผู้สูงอายุใช้งานอาจเพิ่มความเสี่ยงต่อภัยคุกคามทางไซเบอร์ โดยเฉพาะในกรณีที่มีการรักษาความปลอดภัยต่ำ (Zulkipli, 2021) ข้อมูลส่วนบุคคลและข้อมูลการใช้งานที่จัดเก็บในอุปกรณ์เหล่านี้สามารถถูกเข้าถึงหรือขโมยได้ หากไม่ได้รับการป้องกันอย่างเหมาะสม ข้อมูลที่ส่งผ่านอุปกรณ์อัจฉริยะอาจถูกดักฟังหรือขโมยระหว่างการถ่ายโอนข้อมูล (Roman, Zhou, & Lopez, 2013; Atzori, Iera, and Morabito, 2017; Sicari et al., 2015) อุปกรณ์ IoT ยังสามารถถูกแปลงเป็นส่วนหนึ่งของเครือข่ายบอทเน็ตเพื่อนำไปใช้ในการโจมตีแบบปฏิเสธการให้บริการ (DDoS) (Kolias et al., 2017) อีกทั้งอุปกรณ์ที่ไม่ได้รับการอัปเดตยังมีช่องโหว่ที่เพิ่มความเสี่ยงต่อการโจมตีจาก

อาชญากรไซเบอร์ (Mosenia and Jha, 2017) ปัญหาเหล่านี้ชี้ให้เห็นถึงความสำคัญของการพัฒนาอุปกรณ์ที่ปลอดภัยและการส่งเสริมความรู้ด้านการใช้งานที่ปลอดภัยในกลุ่มผู้สูงอายุ

จากภัยทางไซเบอร์ที่พบบ่อยสำหรับผู้สูงอายุข้างต้น ผู้สูงอายุมักเผชิญความเสี่ยงทางไซเบอร์ที่เฉพาะเจาะจง เนื่องจากความเข้าใจเกี่ยวกับเทคโนโลยีที่จำกัดและขาดความรู้ในการป้องกันตนเองบนอินเทอร์เน็ต ซึ่งรวมถึงการถูกหลอกลวงทางการเงิน การหลอกลวงเกี่ยวกับการลงทุน การโจมตีด้วยฟิชชิง และข้อมูลเท็จ และการใช้ข้อมูลสุขภาพเป็นเป้าหมาย นอกจากนี้ การใช้โซเชียลมีเดียและอุปกรณ์อัจฉริยะที่มีความปลอดภัยต่ำยังเพิ่มความเสี่ยงต่อการถูกแฮ็กข้อมูลส่วนตัวและการใช้งานที่ไม่ปลอดภัย การศึกษาด้านไซเบอร์ที่เหมาะสมสำหรับผู้สูงอายุจึงมีความสำคัญอย่างยิ่งเพื่อช่วยสร้างความตระหนักและหลีกเลี่ยงภัยคุกคามเหล่านี้ได้ดียิ่งขึ้น

ผลกระทบของความเสี่ยงทางไซเบอร์ต่อผู้สูงอายุ

การวิเคราะห์ผลกระทบของความเสี่ยงทางไซเบอร์ต่อผู้สูงอายุ สามารถแบ่งออกเป็น 4 ด้าน คือ 1) ผลกระทบทางจิตใจ 2) ผลกระทบทางเศรษฐกิจ 3) ผลกระทบทางครอบครัว และ 4) ผลกระทบทางสังคม โดยอธิบายได้ดังนี้

1. ผลกระทบทางจิตใจ

1.1 ความเครียดและความวิตกกังวล ผู้สูงอายุที่ตกเป็นเหยื่อของการหลอกลวงหรือการโจมตีทางไซเบอร์อาจรู้สึกเครียดและวิตกกังวลอย่างมาก เนื่องจากพวกเขาอาจรู้สึกว่าถูกทำให้ต้องรู้สึกไม่มั่นคงและหวาดกลัวในการใช้เทคโนโลยีในอนาคต (Manić and Miljković, 2022; Hiba, Rafih and Cosmin, Munteanu, 2023; Buja et al., 2021)

1.2 ความเชื่อมั่นและความไว้วางใจลดลง หลังจากประสบการณ์การถูกหลอกลวงหรือการโจมตีทางไซเบอร์ ผู้สูงอายุอาจมีความเชื่อมั่นและความไว้วางใจในตนเองลดลง เนื่องจากกลัวที่จะเป็นเหยื่ออีกครั้ง นอกจากนี้ความเชื่อมั่นและความไว้วางใจของผู้สูงอายุต่อการใช้อินเทอร์เน็ตยังเชื่อมโยงกับการรับรู้ลักษณะความไว้วางใจ และลักษณะบุคลิกภาพอื่น ๆ ซึ่งอาจนำไปสู่ความมั่นใจลดลง (Hiba, Rafih and Cosmin, Munteanu, 2023; Ping, Cai. and Tsaifa, (TF), Yen, 2023; Tsai-Fa, Yen, 2022)

1.3 ผลกระทบต่อสุขภาพจิต ปัญหาเหล่านี้สามารถนำไปสู่ภาวะซึมเศร้าและความโดดเดี่ยว เนื่องจากผู้สูงอายุอาจรู้สึกว่าตัวเองถูกแยกออกจากสังคมหรือไม่มีใครคอยสนับสนุน (Hamilton, Ugur Orak and Wallace, 2022; Varela, Hernández, Miranda, Barlett and Rodríguez-Rivas, 2022)

2. ผลกระทบทางเศรษฐกิจ

2.1 การสูญเสียทรัพย์สิน ผู้สูงอายุที่ตกเป็นเหยื่อการฉ้อโกงทางการเงินอาจสูญเสียเงินออมที่เก็บไว้เพื่อการเกษียณหรือค่าใช้จ่ายสำคัญอื่น ๆ ซึ่งส่งผลกระทบต่อความสามารถในการดูแลตนเองและคุณภาพชีวิต โดยการโจรกรรมข้อมูลหรือทรัพย์สินจะอยู่ในกลุ่มผู้สูงอายุหกสิบห้าปีขึ้นไป (Manić and Miljković, 2022)

2.2 ค่าใช้จ่ายในการแก้ไขปัญหา ค่าใช้จ่ายเพื่อกู้คืนข้อมูลหรือทรัพย์สินที่สูญหายอาจสูงมาก ทำให้ครอบครัวต้องรับภาระค่าใช้จ่ายเพิ่มเติมในการช่วยเหลือ ดังนั้น การขาดความตระหนักและความรู้ในกลุ่มผู้สูงอายุทำให้กลายเป็นความง่ายสำหรับอาชญากรไซเบอร์นำไปสู่การสูญเสียทางการเงินและการละเมิดข้อมูล ผลกระทบทางเศรษฐกิจของความเสี่ยงทางไซเบอร์ต่อผู้สูงอายุรวมถึงค่าใช้จ่ายที่เกี่ยวข้องกับการกู้คืนข้อมูลหรือทรัพย์สินที่สูญหายซึ่งอาจมีนัยสำคัญ เนื่องจากความไวต่อการโจมตีทางไซเบอร์ (Azam, Buja, Darus and Sahri, 2022)

2.3 ผลกระทบต่อเศรษฐกิจระดับกว้าง เมื่อผู้สูงอายุถูกหลอกลวงและสูญเสียเงิน มีผลกระทบต่อเศรษฐกิจครัวเรือนและตลาด เนื่องจากอาจไม่สามารถใช้จ่ายหรือลงทุนในสิ่งที่ส่งเสริมการเติบโตเศรษฐกิจได้ (Manić and Miljković, 2022) โดยรวมแล้ว การจัดการกับความเสี่ยงทางไซเบอร์เป็นสิ่งสำคัญสำหรับการปกป้องผู้สูงอายุ เศรษฐกิจครัวเรือน และความมั่นคงของตลาดเมื่อเผชิญกับภัยคุกคามทางดิจิทัลที่กำลังพัฒนาขึ้น (Kopp, Kaffenberger and Wilson, 2017)

3. ผลกระทบทางครอบครัว

3.1 ความเครียดทางอารมณ์และจิตใจ ได้แก่ 1) ความไม่มั่นคงทางอารมณ์ ผู้สูงอายุที่ถูกหลอกลวงอาจมีความรู้สึกไม่มั่นคงและวิตกกังวล ซึ่งสามารถแผ่กระจายไปยังสมาชิกในครอบครัวที่ต้องดูแลและให้การสนับสนุนทางอารมณ์ 2) ความเครียดทางการเงิน ครอบครัวอาจต้องแบกรับความเครียดทางการเงินหากมีการสูญเสียทรัพย์สินหรือเงินทุนจากการหลอกลวง เนื่องจากผู้สูงอายุมักมีรายได้น้อย

3.2 ความตึงเครียดในครอบครัว ได้แก่ 1) ความไม่เข้าใจและความสับสน กล่าวคือ ผู้สูงอายุอาจไม่เข้าใจว่าทำไมถึงกลายเป็นเหยื่อ ความไม่เข้าใจนี้อาจทำให้เกิดความขัดแย้งกับสมาชิกในครอบครัวที่พยายามช่วยเหลือ 2) การตอบสนองที่แตกต่างกัน สมาชิกครอบครัวบางคนอาจมีการตอบสนองต่อเหตุการณ์ด้วยความไม่เข้าใจหรือหงุดหงิด ทำให้เกิดความตึงเครียดภายในครอบครัว (Arfi and Agarwa, 2013)

4. ผลกระทบทางสังคม

4.1 ความไว้วางใจในเทคโนโลยี ได้แก่ 1) ผลกระทบทางไซเบอร์สามารถทำให้ผู้สูงอายุและชุมชนรอบข้างมีความไว้วางใจในเทคโนโลยีลดลง ส่งผลกระทบต่อการยอมรับและการใช้งานเทคโนโลยีในอนาคต 2) การแพร่กระจายของข้อมูลเท็จ กล่าวคือ ข้อมูลเท็จและการโฆษณาที่หลอกลวงสามารถแพร่กระจายในสังคมผ่านผู้สูงอายุที่อาจมีความไว้วางใจสูงและแบ่งปันข้อมูลที่ได้รับโดยไม่มีการตรวจสอบว่ามีความถูกต้องหรือไม่ (Manić and Miljković, 2022)

4.2 การใช้ทรัพยากรสังคมและสุขภาพ ได้แก่ 1) ความต้องการทรัพยากรเพิ่มเติม กล่าวคือ การฟื้นฟูผู้สูงอายุจากผลกระทบทางไซเบอร์อาจต้องการทรัพยากรสุขภาพจิตและการสนับสนุนทางสังคมที่มากขึ้น เช่น การให้คำปรึกษาและการสนับสนุนทางการเงิน 2) ภาครัฐมีส่วนร่วมในการแก้ไขปัญหา

การรับมือกับความเสียหายทางไซเบอร์ต่อผู้สูงอายุอาจต้องการนโยบายจากรัฐบาลให้มีความสำคัญกับการป้องกันและการศึกษาเพื่อลดผลกระทบเหล่านี้ (Brashier and Schacter, 2020)

จากข้างต้น ผู้สูงอายุที่ตกเป็นเหยื่อของการหลอกลวงหรือการโจมตีทางไซเบอร์มักประสบกับผลกระทบทั้งทางจิตใจและเศรษฐกิจที่รุนแรง ซึ่งส่งผลกระทบต่อครอบครัวและสังคมอย่างกว้างขวางทางจิตใจ รู้สึกเครียดและวิตกกังวล สูญเสียความเชื่อมั่นและความไว้วางใจในตนเอง และอาจนำไปสู่ภาวะซึมเศร้าและความโดดเดี่ยว ในด้านเศรษฐกิจ การสูญเสียทรัพย์สินและค่าใช้จ่ายในการแก้ไขปัญหาทำให้เกิดความเครียดทางการเงินในครอบครัวและส่งผลกระทบต่อเศรษฐกิจระดับกว้าง ความเครียดในครอบครัวและการไม่เข้าใจทำให้เกิดความตึงเครียดและความขัดแย้ง ในขณะที่ในระดับสังคม ความไว้วางใจในเทคโนโลยีลดลงและความต้องการทรัพยากรสังคมและการสนับสนุนเพิ่มขึ้น ดังนั้นจึงจำเป็นต้องมีนโยบายและการสนับสนุนจากรัฐเพิ่มขึ้นเพื่อปกป้องและฟื้นฟูผู้สูงอายุจากผลกระทบทางไซเบอร์

กลยุทธ์การรับมือจากภัยทางไซเบอร์ของผู้สูงอายุ

กลยุทธ์การป้องกันและรับมือของผู้สูงอายุในการเผชิญกับภัยคุกคามทางไซเบอร์สามารถแบ่งได้เป็นหลายด้าน ซึ่งจะช่วยให้ผู้สูงอายุสามารถใช้เทคโนโลยีอย่างปลอดภัยและมีประสิทธิภาพ มีดังนี้

1. การศึกษาและการรับรู้ ได้แก่ 1) การเข้าร่วมการอบรม ผู้สูงอายุควรเข้าร่วมการอบรมหรือการประชุมเชิงปฏิบัติการ(Workshop) เกี่ยวกับการใช้งานอินเทอร์เน็ตอย่างปลอดภัย เพื่อเรียนรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ต่าง ๆ และวิธีการป้องกันตนเอง เช่น การสอนเกี่ยวกับวิธีตรวจสอบว่าอีเมลหรือเว็บไซต์นั้นปลอดภัยหรือไม่ และ 2) ติดตามข่าวสาร โดยมีการอัปเดต (Update) ข้อมูลเกี่ยวกับภัยคุกคามใหม่ ๆ ทางไซเบอร์อยู่เสมอ การติดตามข่าวสาร เช่น การสมัครรับจดหมายข่าวจากแหล่งข้อมูลที่น่าเชื่อถือ โดยมีการแจ้งเตือนจากธนาคารหรือกระทรวงเทคโนโลยี ซึ่งจะมีข้อมูลเกี่ยวกับภัยคุกคามใหม่ ๆ (Manić and Miljković, 2022; Katsantonis, Manikas, Mavridis and Gritzalis, 2023; Buja, Wahid, Abdul Rahman, Deraman, Afni, Hasrol Jono, 2021)

1.1 การใช้เทคโนโลยีอย่างมีสติ ได้แก่ 1) การตั้งรหัสผ่านที่แข็งแกร่งและปลอดภัย ควรใช้รหัสผ่านที่ประกอบด้วยตัวอักษรใหญ่เล็ก ตัวเลข และสัญลักษณ์ และหลีกเลี่ยงการใช้รหัสผ่านเดียวกันกับหลายบัญชี เช่น การใช้รหัสผ่านที่มีความยาวอย่างน้อย 12 ตัวอักษรและประกอบด้วยอักขระหลายประเภท 2) การใช้การตรวจสอบสิทธิ์แบบสองขั้นตอน (2FA) เพิ่มการป้องกันเพิ่มเติมด้วยการตรวจสอบความถูกต้องสองชั้น จะช่วยลดความเสี่ยงจากการถูกแฮ็กได้ เช่น การเพิ่มการยืนยันตัวตนผ่านข้อความ SMS และ 3) การอัปเดต (Update) ซอฟต์แวร์ โดยการให้ซอฟต์แวร์และระบบปฏิบัติการต้องอัปเดตอยู่เสมอ เพื่อช่วยป้องกันไม่ให้ใช้ช่องโหว่เก่า ๆ มาก่อวินาศภัย (Padikkapparambil, Ncube, Singh and Singh, 2020; Hill, Betts and Gardner, 2015; Vailati, Sadowski, Comazzi and Pagnini, 2022)

1.2 การเตรียมความพร้อมในการรับมือกับภัยคุกคาม มีดังนี้ 1) มีการสำรองข้อมูลที่สำคัญ โดยการมีสำเนาข้อมูลสำคัญ เช่น รูปภาพ ข้อมูลการเงิน และเอกสารสำคัญ ในอุปกรณ์สำรองหรือบริการคลาวด์ ยกตัวอย่างเช่น การใช้บริการคลาวด์ใน Google Drive หรือ Dropbox เพื่อเก็บสำเนาข้อมูลสำคัญไว้ นอกจากในอุปกรณ์ และ 2) การเรียนรู้วิธีการรายงานปัญหา ผู้สูงอายุควรทราบวิธีการติดต่อเจ้าหน้าที่หรือองค์กรที่เกี่ยวข้องเมื่อต้องเผชิญหน้ากับปัญหาทางไซเบอร์ ตัวอย่างเช่น ผู้สูงอายุควรทราบว่าสามารถรายงานเหตุการณ์ทางไซเบอร์ได้ที่หน่วยงานตำรวจหรือเว็บไซต์ (Manić and Miljković, 2022; Vailati, Sadowski, Comazzi and Pagnini, 2022)

1.3 การใช้เครือข่ายอินเทอร์เน็ตหรือโซเชียลมีเดียอย่างระมัดระวัง ได้แก่ 1) ระมัดระวังในการแชร์ข้อมูลส่วนตัว ควรหลีกเลี่ยงการแชร์ข้อมูลส่วนตัว เช่น ที่อยู่ วันเกิด หรือข้อมูลการเงินในโซเชียลมีเดีย ตัวอย่างเช่น ไม่โพสต์ที่อยู่หรือวันเกิดของตนเองบน Facebook หรือ Twitter และ 2) การระวังข้อความหลอกลวง โดยการสอนผู้สูงอายุให้ระมัดระวังต่ออีเมลหรือข้อความที่ดูเหมือนผิดปกติ ซึ่งอาจเป็นการพยายามหลอโก้ง เช่น สอนผู้สูงอายุให้ตรวจสอบความถูกต้องของอีเมลที่อ้างว่ามาจากธนาคารหรือบริการอื่น ๆ ที่ต้องการข้อมูลการเข้าสู่ระบบ (Rice, Haynes, Royce and Thompson, 2016; Nef, Ganea, Müri and Mosimann, 2013)

จากข้างต้น กลยุทธ์การป้องกันและรับมือภัยคุกคามทางไซเบอร์สำหรับผู้สูงอายุประกอบด้วยหลายมิติ ได้แก่ การศึกษาและการรับรู้ผ่านการเข้าร่วมการอบรมและการติดตามข่าวสารเกี่ยวกับภัยคุกคามใหม่ ๆ การใช้เทคโนโลยีอย่างมีสติ เช่น การตั้งรหัสผ่านที่ปลอดภัยและการใช้การตรวจสอบสิทธิ์แบบสองขั้นตอน การเตรียมความพร้อมในการรับมือภัยคุกคาม โดยมีการสำรองข้อมูลสำคัญและการรายงานปัญหาที่เกิดขึ้น รวมถึงการใช้เครือข่ายอินเทอร์เน็ตหรือโซเชียลมีเดียอย่างระมัดระวัง เช่น หลีกเลี่ยงการแชร์ข้อมูลส่วนตัว กลยุทธ์เหล่านี้จะช่วยให้ผู้สูงอายุสามารถใช้เทคโนโลยีได้อย่างปลอดภัยและมีประสิทธิภาพในยุคดิจิทัล

สรุป

ความท้าทายใหม่ของสังคมไทยในการรับมือภัยทางไซเบอร์สำหรับผู้สูงอายุ

ความท้าทายใหม่ของสังคมไทยในการรับมือภัยทางไซเบอร์สำหรับผู้สูงอายุนั้นมีหลายด้านและต้องมีการตอบสนองที่ครอบคลุม รวมถึงการปรับปรุงและพัฒนาทั้งในด้านเทคโนโลยีและนโยบายเพื่อป้องกันและลดผลกระทบจากภัยคุกคามที่เพิ่มขึ้น

การสร้างการปกป้องและช่วยเหลือผู้สูงอายุจากภัยคุกคามทางไซเบอร์ จำเป็นต้องพัฒนานโยบายและกลยุทธ์ที่หลากหลายเพื่อให้ผู้สูงอายุสามารถใช้เทคโนโลยีได้อย่างปลอดภัย และมีการป้องกันจากการถูกโจมตีทางไซเบอร์ นโยบายเหล่านี้ควรรวมถึงการจัดตั้งโปรแกรมการศึกษาและอบรมทั้งในรูปแบบออนไลน์และออฟไลน์เพื่อเพิ่มความตระหนักรู้เกี่ยวกับการใช้เทคโนโลยีและความปลอดภัยทางไซเบอร์

การปรับปรุงกฎหมายเพื่อป้องกันการใช้งานอินเทอร์เน็ต และการสร้างความร่วมมือกับภาคเอกชนในการพัฒนาเครื่องมือและแพลตฟอร์มที่เหมาะสมกับผู้สูงอายุ นอกจากนี้ การสนับสนุนจากศูนย์บริการเฉพาะทาง และการส่งเสริมการเข้าถึงเทคโนโลยีคุณภาพสูงยังเป็นส่วนสำคัญในการสร้างสังคมไซเบอร์ที่ปลอดภัยและเข้าถึงได้สำหรับผู้สูงอายุ นอกจากนี้ การสร้างความร่วมมือระดับชาติและระหว่างประเทศ การตรวจสอบและประเมินผลโปรแกรมที่มีอยู่ และการจัดการอบรมที่เข้าถึงง่ายและเหมาะสมกับผู้สูงอายุ เป็นส่วนสำคัญในการสร้างสังคมไซเบอร์ที่ปลอดภัยและเข้าถึงได้สำหรับผู้สูงอายุ

จากการศึกษาข้างต้น ผู้เขียนสามารถสรุปประเด็นการรับมือและความท้าทายกับภัยทางไซเบอร์สำหรับผู้สูงอายุในสังคมไทยในปัจจุบันได้ดังนี้

1. การขาดความรู้เกี่ยวกับเทคโนโลยีและความปลอดภัยทางไซเบอร์

การขาดความรู้เกี่ยวกับเทคโนโลยีและความปลอดภัยทางไซเบอร์ในกลุ่มผู้สูงอายุในไทยนับเป็นปัญหาสำคัญที่ต้องได้รับการจัดการอย่างจริงจัง เนื่องจากผู้สูงอายุหลายคนเริ่มต้นใช้เทคโนโลยีในช่วงชีวิตที่อายุมากขึ้นโดยไม่มีพื้นฐานความรู้เบื้องต้นที่เพียงพอ การที่ผู้สูงอายุในไทยเริ่มใช้งานเทคโนโลยีในช่วงวัยที่ไม่มีพื้นฐานความรู้มาก่อน ส่งผลให้พวกเขาตกเป็นเป้าหมายของภัยทางไซเบอร์ เช่น การหลอกลวงออนไลน์และการโจมตีแบบฟิชชิ่ง หรือการติด Malware การขาดแหล่งข้อมูลที่เหมาะสมทำให้การเรียนรู้เป็นไปได้ยาก ดังนั้น จึงควรพัฒนาแพลตฟอร์มและเครื่องมือที่ออกแบบเฉพาะสำหรับผู้สูงอายุ พร้อมทั้งจัดหาแหล่งข้อมูลและการศึกษาที่ตอบโจทย์ความต้องการ เพื่อเสริมสร้างความปลอดภัยและการใช้งานที่มีประสิทธิภาพ

2. การใช้งานโซเชียลมีเดีย (Social Media)

การใช้งานโซเชียลมีเดีย (Social Media) ของผู้สูงอายุในไทยมีทั้งประโยชน์และความเสี่ยงที่ต้องรับมืออย่างรอบคอบ แม้โซเชียลมีเดียจะช่วยลดความโดดเดี่ยวและส่งเสริมการมีส่วนร่วมในสังคม แต่การใช้งานอย่างไม่ระมัดระวังอาจนำไปสู่การละเมิดข้อมูลส่วนบุคคลหรือการหลอกลวง เช่น การสร้างบัญชีปลอมเพื่อขอเงินหรือข้อมูลสำคัญ ดังนั้น การอบรมผู้สูงอายุเกี่ยวกับการตั้งค่าความเป็นส่วนตัวและการระบุข้อมูลหลอกลวงจึงเป็นสิ่งจำเป็น นอกจากนี้ การใช้ซอฟต์แวร์ป้องกันไวรัสสามารถช่วยลดความเสี่ยงได้อย่างมาก

3. การหลอกลวงทางการเงิน

ผู้สูงอายุในสังคมไทยเผชิญความเสี่ยงสูงจากการหลอกลวงทางการเงินออนไลน์ เนื่องจากขาดความรู้ในการระบุภัยคุกคามไซเบอร์ วิธีการที่พบบ่อย ได้แก่ อีเมลฟิชชิ่งที่ปลอมเป็นแหล่งนำเชื่อถือเพื่อขอข้อมูลส่วนตัว ข้อความจากบัญชีโซเชียลมีเดียปลอมที่ขอเงินด่วน หรือการโทรศัพท์หลอกลวงโดยแอบอ้างเป็นหน่วยงานราชการหรือบริษัทประกันภัยเพื่อให้โอนเงินหรือเปิดเผยข้อมูลส่วนตัว การป้องกันปัญหานี้จำเป็นต้องเสริมสร้างความรู้ด้านไซเบอร์ให้กับผู้สูงอายุ เพื่อให้สามารถระบุสัญญาณเตือนและป้องกันตนเองได้อย่างมีประสิทธิภาพ นอกจากนี้ การพัฒนากฎหมายและนโยบายที่ทันสมัยเพื่อรับมือกับรูปแบบการหลอกลวงที่ซับซ้อน จะเป็นกุญแจสำคัญในการลดผลกระทบต่อนักผู้สูงอายุในสังคมไทย

4. ความต้องการการเข้าถึงเทคโนโลยีที่เหมาะสม

การพัฒนาเทคโนโลยีสำหรับผู้สูงอายุในไทยยังคงเป็นความท้าทาย เนื่องจากเทคโนโลยีในตลาดมักออกแบบมาเพื่อผู้ใช้ที่มีความคุ้นเคยกับเทคโนโลยี โดยไม่คำนึงถึงข้อจำกัดเฉพาะของผู้สูงอายุ เช่น การมองเห็น การได้ยิน การเคลื่อนไหว หรือความจำที่ลดลง การออกแบบที่ไม่เหมาะสมส่งผลให้ผู้สูงอายุใช้งานได้ยาก และเพิ่มความเสี่ยงต่อความผิดพลาด เช่น การจัดการข้อมูลส่วนตัวที่ไม่ปลอดภัยหรือการติดต่อกับฉ้อโกง การแก้ปัญหานี้จำเป็นต้องพัฒนาเทคโนโลยีที่สามารถปรับแต่งได้ เช่น ฟิเจอร์คำอธิบายเสียงและขนาดตัวอักษรที่ปรับเปลี่ยนได้ รวมถึงสนับสนุนการฝึกอบรมที่เข้าถึงง่าย เพื่อช่วยให้ผู้สูงอายุสามารถใช้เทคโนโลยีอย่างปลอดภัย มีประสิทธิภาพ และเชื่อมโยงกับครอบครัวและสังคมได้ดียิ่งขึ้น

5. ความเปราะบางทางข้อมูลส่วนบุคคล

การปกป้องข้อมูลส่วนบุคคลของผู้สูงอายุในยุคดิจิทัลเป็นเรื่องสำคัญ เนื่องจากขาดความรู้และความเข้าใจในการป้องกันข้อมูล อาจทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงและโจมตีทางไซเบอร์ได้ง่าย การเสริมสร้างความรู้ เช่น การตั้งค่าความเป็นส่วนตัว การสร้างรหัสผ่านที่ปลอดภัย การใช้การตรวจสอบสองขั้นตอน และการตรวจสอบลิงก์หรือไฟล์ก่อนคลิก รวมถึงการติดตั้งซอฟต์แวร์ป้องกันไวรัสล้วนเป็นมาตรการสำคัญในการลดความเสี่ยง นอกจากนี้ การรับรู้เกี่ยวกับวิธีการหลอกลวงทางไซเบอร์ช่วยเสริมความมั่นใจในการป้องกันข้อมูลส่วนตัว มาตรการเหล่านี้จะช่วยให้ผู้สูงอายุสามารถใช้เทคโนโลยีได้อย่างปลอดภัย ลดความเสี่ยงต่อการละเมิดข้อมูล และเพิ่มความมั่นใจในการใช้งานในยุคดิจิทัล

6. การปรับปรุงและพัฒนาของกฎหมายและนโยบาย

การปรับปรุงกฎหมายและนโยบายในไทยเพื่อรับมือกับการเปลี่ยนแปลงทางเทคโนโลยีและภัยคุกคามใหม่เป็นสิ่งจำเป็นอย่างยิ่ง สังคมไทยควรพัฒนากฎหมายให้สอดคล้องกับมาตรฐานสากล โดยเฉพาะด้านการป้องกันข้อมูลส่วนบุคคล การต่อต้านการหลอกลวงทางไซเบอร์ และการรับมือกับ Malware และไวรัส รวมถึงกำหนดมาตรฐานความปลอดภัยสำหรับอุปกรณ์ IoT (Internet of Things) การสร้างกรอบความร่วมมือระหว่างหน่วยงานรัฐและภาคเอกชนจะช่วยเพิ่มประสิทธิภาพในการจัดการภัยคุกคามเหล่านี้ นอกจากนี้ การส่งเสริมการศึกษาและสร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์ให้กับประชาชน โดยเฉพาะผู้สูงอายุ เป็นอีกปัจจัยสำคัญในการช่วยลดความเสี่ยงและเพิ่มความสามารถในการรับมือกับความท้าทายจากเทคโนโลยีใหม่ได้อย่างมีประสิทธิภาพ

อย่างไรก็ตาม การรับมือกับภัยทางไซเบอร์สำหรับผู้สูงอายุในสังคมไทยต้องเผชิญกับความท้าทายหลายด้าน ทั้งในเรื่องของการขาดความรู้ทางเทคโนโลยี การใช้งานโซเชียลมีเดีย การหลอกลวงทางการเงินการเข้าถึงเทคโนโลยีที่เหมาะสม การปกป้องข้อมูลส่วนบุคคล และการปรับปรุงและพัฒนาของกฎหมายและนโยบาย ปัญหาเหล่านี้ไม่เพียงแต่ส่งผลกระทบต่อความปลอดภัยของผู้สูงอายุเท่านั้น แต่ยังส่งผลกระทบต่อคุณภาพชีวิตและความสามารถในการใช้ประโยชน์จากเทคโนโลยีในยุคดิจิทัลของผู้สูงอายุอีกด้วย

ข้อเสนอแนะเชิงนโยบาย

การสร้างการปกป้องและช่วยเหลือผู้สูงอายุจากภัยคุกคามทางไซเบอร์ ควรรวมถึงการพัฒนา นโยบายและกลยุทธ์ในหลายด้าน เพื่อให้ผู้สูงอายุสามารถใช้เทคโนโลยีอย่างปลอดภัยและเพื่อเสริมสร้าง การป้องกันจากการถูกโจมตีทางไซเบอร์ ผู้เขียนสามารถสรุปแนวทางข้อเสนอแนะเชิงนโยบายได้ดังต่อไปนี้

1. การศึกษาและการเพิ่มความตระหนักรู้ โดยการจัดตั้งโปรแกรมหรือแผนการศึกษาและการ อบรมต่อเนื่องเกี่ยวกับการใช้เทคโนโลยีและความปลอดภัยทางไซเบอร์สำหรับผู้สูงอายุ ทั้งในรูปแบบ ออนไลน์และออฟไลน์ เช่น การอบรมเชิงปฏิบัติการสำหรับผู้สูงอายุในชุมชน โดยหน่วยงานภาครัฐควรร่วมมือกับองค์กรเอกชนและองค์กรไม่แสวงผลกำไร จัดกิจกรรมให้ความรู้เกี่ยวกับการใช้อินเทอร์เน็ตอย่าง ปลอดภัย พร้อมสร้างแคมเปญผ่านแพลตฟอร์มที่ผู้สูงอายุใช้เป็นประจำ เช่น เฟสบุ๊ก (Facebook) และ ไลน์ (Line) โดยนำกรณีตัวอย่างจริงมาเสริมสร้างความเข้าใจ

2. นโยบายและกฎหมาย ภาครัฐควรมีการปรับปรุงพัฒนากฎหมายเพื่อปกป้องผู้ใช้งาน อินเทอร์เน็ตจากการถูกโจมตีทางไซเบอร์ โดยเฉพาะกลุ่มที่เปราะบางกรณีผู้สูงอายุ และสนับสนุนการสร้าง นโยบายหรือโครงการที่มุ่งเน้นไปที่การป้องกันและการแจ้งเตือนการฉ้อโกง หรือภัยทางไซเบอร์ เช่น มีระบบแจ้งเตือนภัยไซเบอร์แบบเรียลไทม์ในรูปแบบง่าย เช่น SMS หรือข้อความเสียง เพื่อแจ้งเตือนภัย ใหม่ ๆ รวมถึงสนับสนุนนโยบายเกี่ยวกับความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคลของผู้สูงอายุ

3. การสร้างความร่วมมือกับภาคเอกชน ได้แก่ การสร้างความร่วมมือกับภาคเอกชนหรือบริษัท ที่เกี่ยวกับด้านเทคโนโลยี โดยภาครัฐและภาคเอกชนจับมือร่วมกันเพื่อพัฒนาเครื่องมือและแพลตฟอร์ม ที่เข้าใจง่าย สามารถใช้งานง่ายสำหรับผู้สูงอายุ ซึ่งอาจรวมถึงการเพิ่มความปลอดภัยในอุปกรณ์และบริการ ที่ใช้เป็นประจำ เช่น สมาร์ทโฟน/มือถือ แท็บเล็ต (Tablet) คอมพิวเตอร์ รวมถึงการสนับสนุนการวิจัยและ พัฒนาเทคโนโลยีที่เน้นความปลอดภัยและความเข้าถึงสำหรับผู้สูงอายุ

4. การสนับสนุนและจัดหาแหล่งข้อมูล ได้แก่ การจัดตั้งศูนย์บริการช่วยเหลือเฉพาะทางสำหรับ ผู้สูงอายุที่ต้องการคำปรึกษาหรือช่วยเหลือเกี่ยวกับปัญหาทางไซเบอร์ และสร้างเครือข่ายการสนับสนุน ที่รวมหน่วยงานของรัฐ ภาคเอกชน องค์กรปกครองส่วนท้องถิ่น และอาสาสมัครที่พร้อมให้ความช่วยเหลือ ในการใช้เทคโนโลยีอย่างปลอดภัย

5. การส่งเสริมการเข้าถึงเทคโนโลยีอย่างมีคุณภาพ ภาครัฐและหน่วยงานที่เกี่ยวข้องควร สนับสนุนการเข้าถึงเทคโนโลยีอย่างมีคุณภาพสำหรับผู้สูงอายุ ซึ่งรวมถึงการให้บริการอินเทอร์เน็ตที่เสถียร และเครื่องมือเทคโนโลยีที่ออกแบบมาเพื่อความสะดวกต่อการใช้งาน และการจัดหาอุปกรณ์และซอฟต์แวร์ที่มี ความปลอดภัยภายในตัว เช่น ระบบปฏิบัติการที่มีฟังก์ชันการป้องกันภัยคุกคามอัตโนมัติ เป็นต้น

6. การสร้างความร่วมมือระดับชาติและระหว่างประเทศ ได้แก่ ส่งเสริมการร่วมมือระหว่าง ประเทศในการพัฒนามาตรการความปลอดภัยทางไซเบอร์สำหรับผู้สูงอายุ การแบ่งปันข้อมูลและทรัพยากร ระหว่างประเทศ เช่น อาเซียน ยุโรป เอเชียตะวันออกเฉียงใต้ เป็นต้น สามารถช่วยให้มีมาตรฐานที่ดีขึ้นและ

เทคโนโลยีที่มีประสิทธิภาพสูงในการปกป้องกลุ่มผู้สูงอายุ รวมถึงการจัดการประชุมหรือเวทีวิชาการระหว่างประเทศเพื่อแลกเปลี่ยนความรู้และประสบการณ์เกี่ยวกับนโยบายและแนวทางการป้องกันที่เหมาะสม

7. การตรวจสอบและการประเมินผล ได้แก่ การพัฒนาระบบตรวจสอบและประเมินผลการปฏิบัติของนโยบายและโครงการที่จัดขึ้นเพื่อปกป้องผู้สูงอายุจากภัยคุกคามทางไซเบอร์ เพื่อให้แน่ใจว่ามีประสิทธิภาพและตอบสนองต่อความต้องการของผู้สูงอายุได้อย่างเหมาะสม และการสร้างกลไกในการรับฟังข้อเสนอแนะและประสบการณ์จากผู้สูงอายุโดยตรง เพื่อปรับปรุงและพัฒนาโครงการและนโยบายต่อไป

8. การสร้างความตระหนักรู้และการอบรมเชิงปฏิบัติการ การวางแผนและพัฒนาหลักสูตรอบรมสำหรับผู้สูงอายุควรเน้นที่ความเข้าใจง่ายและเหมาะสมกับความสามารถและความต้องการเฉพาะกลุ่ม โดยหลักสูตรควรรวมเนื้อหาพื้นฐานเกี่ยวกับการใช้งานอินเทอร์เน็ต การจัดการอีเมล การใช้งานโซเชียลมีเดีย และการป้องกันตนเองจากการหลอกลวง การอบรมควรจัดในสถานที่ที่เข้าถึงง่าย เช่น ชุมชนหรือศูนย์การเรียนรู้สำหรับผู้สูงอายุ โดยใช้วิธีการสอนที่เน้นการมีส่วนร่วมและการปฏิบัติจริง เช่น การใช้สมาร์ตโฟนหรือแท็บเล็ต เพื่อให้ผู้สูงอายุได้ฝึกใช้งานจริง สื่อการเรียนการสอนควรหลากหลาย เช่น วิดีโอสอน การสอนออนไลน์ และแอปพลิเคชันเพื่อการศึกษา เพื่อเพิ่มประสิทธิภาพในการเรียนรู้ นอกจากนี้ ควรจัดทำแบบประเมินผลหลังการอบรมเพื่อติดตามความก้าวหน้า และปรับปรุงโปรแกรมให้เหมาะสมยิ่งขึ้นกับความต้องการของผู้สูงอายุ ทั้งนี้ การจัดอบรมในรูปแบบดังกล่าวจะช่วยเสริมสร้างทักษะด้านเทคโนโลยีให้กับผู้สูงอายุได้อย่างมีประสิทธิภาพและตรงจุด

9. การทำงานร่วมกับหน่วยงานท้องถิ่น องค์กรไม่แสวงผลกำไร และภาคเอกชน เพื่อร่วมกันจัดการอบรม และส่งเสริมการมีส่วนร่วมของครอบครัวและผู้ดูแลผู้สูงอายุ ซึ่งเป็นกลยุทธ์ที่สำคัญในการสร้างเครือข่ายความปลอดภัยที่ครอบคลุมและมีประสิทธิภาพ การมีความร่วมมือนี้จะช่วยให้แต่ละฝ่ายสามารถแบ่งปันทรัพยากร ความเชี่ยวชาญ และข้อมูลที่มีอยู่ นอกจากนี้ การมีส่วนร่วมของครอบครัวและผู้ดูแลให้การสนับสนุนทางอารมณ์และการเรียนรู้ที่สำคัญสำหรับผู้สูงอายุ เพิ่มความมั่นใจและความเข้าใจในการใช้เทคโนโลยีอย่างปลอดภัย

ดังนั้น การตอบสนองต่อความท้าทายเหล่านี้ต้องเกิดจากการสร้างความร่วมมือจากทุกภาคส่วนในสังคม ทั้งภาครัฐบาล ภาคเอกชน และชุมชน รวมถึงการปรับปรุงนโยบายและกฎหมายให้ทันสมัย ปิดช่องว่างทางกฎหมาย เพื่อคุ้มครองผู้สูงอายุจากภัยทางไซเบอร์ที่เพิ่มขึ้น การส่งเสริมการศึกษาและการให้ความรู้เกี่ยวกับการใช้งานเทคโนโลยีอย่างปลอดภัยก็มีความสำคัญในการช่วยให้ผู้สูงอายุสามารถป้องกันตัวเองจากภัยทางไซเบอร์และใช้ประโยชน์จากเทคโนโลยีใหม่ ๆ ได้อย่างมีประสิทธิภาพ

อีกทั้งในด้านการปรับปรุงและการพัฒนาแนวทางรับมือต้องมีการพัฒนาแนวทางและกลยุทธ์ที่เข้าถึงได้ง่ายและปลอดภัยสำหรับผู้สูงอายุ โดยเน้นไปที่การออกแบบเทคโนโลยีที่เหมาะสมกับความ

ต้องการของผู้สูงอายุ รวมถึงการสนับสนุนในด้านการเข้าถึงแหล่งข้อมูลและการฝึกอบรมที่เพียงพอ การรับรู้ถึงความเสี่ยงและการป้องกันตนเองจากภัยทางไซเบอร์เป็นสิ่งที่ช่วยให้ผู้สูงอายุสามารถใช้ชีวิตในยุคดิจิทัลได้อย่างมั่นใจและปลอดภัย

จากข้างต้นผู้เขียนเห็นว่า การประยุกต์ใช้ข้อเสนอแนะในประเทศไทย สามารถเริ่มต้นด้วยการจัดโครงการอบรมผู้สูงอายุในชุมชน เช่น ศูนย์ผู้สูงอายุ โดยใช้เครื่องมือที่เข้าถึงง่าย เช่น แอปพลิเคชันบนสมาร์ทโฟนที่มีอินเทอร์เฟซเรียบง่ายและเป็นภาษาไทย นอกจากนี้ การสร้างสื่อการสอนที่เข้าใจง่าย เช่น วิดีโอเกี่ยวกับการป้องกันฟิชชิ่งและภัยไซเบอร์ ก็เป็นอีกวิธีที่สามารถช่วยสร้างความรู้ให้แก่ผู้สูงอายุได้อย่างมีประสิทธิภาพ ในด้านการพัฒนากฎหมาย ควรเพิ่มบทลงโทษสำหรับผู้กระทำการหลอกลวงผู้สูงอายุในโลกออนไลน์ และสนับสนุนการพัฒนากฎหมายใหม่ที่มุ่งเน้นการปกป้องข้อมูลส่วนบุคคลและการต่อต้านภัยไซเบอร์อย่างครอบคลุม ความร่วมมือกับภาคเอกชนยังเป็นปัจจัยสำคัญในการพัฒนาระบบเทคโนโลยีที่ปลอดภัยสำหรับผู้สูงอายุ เช่น การออกแบบสมาร์ทโฟนที่มีฟีเจอร์แจ้งเตือนภัยไซเบอร์อัตโนมัติ รวมถึงการพัฒนาแพลตฟอร์มที่ผู้สูงอายุสามารถติดต่อหน่วยงานรัฐได้ง่ายเมื่อเกิดปัญหา นอกจากนี้ การจัดตั้งเครือข่ายสนับสนุนในชุมชน เช่น อาสาสมัครที่ช่วยให้คำปรึกษาด้านเทคโนโลยีแก่ผู้สูงอายุ จะช่วยลดความเปราะบางของกลุ่มเป้าหมายได้อีกทางหนึ่ง อีกทั้งการสร้างแคมเปญรณรงค์ในสื่อต่าง ๆ เช่น โทรทัศน์ วิทยุ และโซเชียลมีเดีย ยังช่วยเพิ่มการตระหนักรู้ของผู้สูงอายุและครอบครัวเกี่ยวกับภัยทางไซเบอร์อย่างมีประสิทธิภาพ ดังนั้น การนำข้อเสนอแนะดังกล่าวมาปรับใช้ในประเทศไทยควรพิจารณาให้เหมาะสมกับบริบททางสังคมและวัฒนธรรมของประเทศ รวมถึงการสร้างความร่วมมือระหว่างภาครัฐ เอกชน และชุมชน เพื่อให้การป้องกันภัยไซเบอร์สำหรับผู้สูงอายุมีความยั่งยืนและครอบคลุมทุกมิติ ซึ่งจะช่วยเสริมสร้างความมั่นใจและความปลอดภัยในการใช้เทคโนโลยีสำหรับผู้สูงอายุในยุคดิจิทัลได้อย่างมีประสิทธิภาพ

องค์ความรู้ใหม่ที่ได้รับ

1. ทำให้ได้รับองค์ความรู้เกี่ยวกับความเปราะบางของผู้สูงอายุ โดยผู้สูงอายุมักมีความรู้และทักษะด้านเทคโนโลยีจำกัด ส่งผลให้ตกเป็นเป้าหมายของภัยไซเบอร์ที่หลากหลาย เช่น การหลอกลวงทางการเงิน การโจมตีข้อมูลสุขภาพ และการละเมิดข้อมูลส่วนตัวผ่านโซเชียลมีเดียหรืออุปกรณ์ IoT ซึ่งช่องโหว่เหล่านี้เพิ่มความเสี่ยงต่อการสูญเสียทรัพย์สินและความเป็นส่วนตัวอย่างมาก

2. ทำให้ได้รับองค์ความรู้เกี่ยวกับผลกระทบของภัยไซเบอร์หลายมิติ ได้แก่ ด้านจิตใจ เช่น ความเครียดและการสูญเสียความมั่นใจ ด้านเศรษฐกิจ เช่น การสูญเสียทรัพย์สินและการค่าใช้จ่ายเพิ่มเติม และด้านสังคม เช่น การลดความไว้วางใจในเทคโนโลยี รวมถึงความต้องการทรัพยากรเพื่อช่วยฟื้นฟูปัญหาจากภัยไซเบอร์ที่เพิ่มขึ้น

3. ทำให้ได้รับองค์ความรู้เกี่ยวกับแนวทางป้องกันและรับมือภัยไซเบอร์สำหรับผู้สูงอายุที่ควรมุ่งเน้นการให้ความรู้ เช่น การจัดอบรมเพื่อสร้างความตระหนักรู้ การใช้เทคโนโลยีอย่างระมัดระวัง เช่น การตั้งรหัสผ่านที่ปลอดภัย และการเตรียมพร้อมรับมือเหตุการณ์ เช่น การสำรองข้อมูลสำคัญ รวมถึงการเรียนรู้วิธีรายงานปัญหาเพื่อแก้ไขได้อย่างมีประสิทธิภาพ

4. สามารถนำองค์ความรู้เพื่อไปประยุกต์ใช้เกี่ยวกับข้อเสนอเชิงนโยบาย เพื่อปกป้องผู้สูงอายุจากภัยไซเบอร์ ซึ่งควรมีการจัดตั้งโปรแกรมอบรมและกิจกรรมเสริมความรู้ การพัฒนากฎหมายที่ทันสมัย เช่น การป้องกันข้อมูลส่วนบุคคลและการต่อต้านการหลอกลวง รวมถึงการพัฒนาเทคโนโลยีที่เหมาะสมและปลอดภัย เช่น สมาร์ทโฟนที่ใช้งานง่าย และการสร้างความร่วมมือระหว่างหน่วยงานต่าง ๆ เพื่อเสริมสร้างมาตรการป้องกันภัยไซเบอร์ให้ยั่งยืนและครอบคลุมทุกมิติ

5. องค์ความรู้ดังกล่าวจะเป็นการสร้างความตระหนักรู้ในสังคม พัฒนามาตรการป้องกันภัยไซเบอร์ และออกแบบเทคโนโลยีที่ปลอดภัยและใช้งานง่าย อีกทั้งเป็นแนวทางสร้างความร่วมมือระหว่างภาครัฐ เอกชน และองค์กรท้องถิ่น เพื่อสร้างมาตรการป้องกันที่ยั่งยืน การปรับใช้นโยบายและกฎหมายที่ทันสมัย รวมถึงการอบรมความรู้ด้านไซเบอร์ จะช่วยลดความเสี่ยงและยกระดับคุณภาพชีวิตผู้สูงอายุในยุคดิจิทัลอย่างมั่นใจและปลอดภัย

รายการอ้างอิง

ภาษาไทย

- Cyber Crime Investigation Bureau. (2020). *Annual report on cybercrime in Thailand*. กรุงเทพฯ: กรมสืบสวนคดีอาชญากรรมไซเบอร์.
- ThaiCERT. (2021). *Threat Report: Cyber threats in Thailand*. กรุงเทพฯ: ศูนย์ประสานงานความมั่นคงเครือข่ายคอมพิวเตอร์ไทย.
- ไทยรัฐออนไลน์. (2566). 10 อันดับกิจกรรม และพฤติกรรมการใช้อินเทอร์เน็ตของคนไทย 2566. วันที่ค้นข้อมูล 15 ตุลาคม 2567, เข้าถึงได้จาก <https://www.thairath.co.th/lifestyle/life/2722450>
- NEWS.CH7. (2024). เปิดสถิติคนไทยใช้อินเทอร์เน็ต ปี 2024 กลุ่มผู้สูงอายุ มาแรง! กลายเป็นกลุ่มลูกค้าสำคัญในโลกออนไลน์. วันที่ค้นข้อมูล 15 ตุลาคม 2567, <https://news.ch7.com/detail/725604>
- ประชาชาติธุรกิจ. (2566). 5 ที่สุดภัยไซเบอร์ที่คนไทยตกเป็นเหยื่อปี'66 สูงวัย60+ เสี่ยง. วันที่ค้นข้อมูล 15 ตุลาคม 2567, เข้าถึงได้จาก <https://www.prachachat.net/ict/news-1469728>
- SOSECURE. (2024). สรุป 9 เหตุการณ์การโจมตีทางไซเบอร์ครั้งใหญ่ในไทย. วันที่ค้นข้อมูล 15 ตุลาคม 2567, เข้าถึงได้จาก <https://www.sosecure.co.th/>
- สำนักงานตำรวจแห่งชาติ. (2567). เปิดสถิติอายุ 'เหยื่ออาชญากรรมไซเบอร์' ไม่ใช่กลุ่มคนชรา แต่เป็นวัยทำงาน. วันที่ค้นข้อมูล 15 ตุลาคม 2567, เข้าถึงได้จาก <https://thethaiger.com/th/news/1198860/>

ภาษาอังกฤษ

- Alexandru, A., Ianculescu, M., Giura, I., & Pop, F. (2022). Managing Cybersecurity Threats for Seniors' Digital Needs Using Age-Friendly Remote Healthcare Monitoring Model. *E-Health and Bioengineering Conference (EHB)*, 1-4.
- Anderson, J., & Rainie, L. (2017). *The future of truth and misinformation online*. Pew Research Center. Retrieved November 2, 2024, from <https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/>
- Arfi, N., Agarwal, S. (2013). Knowledge of Cybercrime among Elderly. *International Journal of Scientific & Engineering Research*, 4(7), 1463-1468.
- Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: definition, potentials, and societal role of a fast Evolving Paradigm. *Ad Hoc Networks*, 56, 122-140.
- Azam, N. A., Buja, A. G., Darus, M. Y., & Sahri., N. M. (2022). "SCSAM-Elderly: A New Synergistic Cyber Security Model for the Elderly for IR4.0. Readiness in Malaysia," 2022 IEEE 12th Symposium on Computer Applications & Industrial Electronics (ISCAIE), (pp. 117-122). Penang, Malaysia, 2022.
- Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2019). Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective. *Journal of Computer Information Systems*, 61, 195-206.
- Buja, A. G., Daleela, S., Wahid, M., Faradilla, T., Rahman, A., Deraman, N. A., Hajar Hasrol Jono, M. N., & Aziz, A. D. (2021). Development of organization, social and individual cyber security awareness model (OSICSAM) for the elderly. *International Journal of Advanced Technology and Engineering Exploration; Bhopal*, 8(76), 511-519.
- Buja, A. G., Wahid, S. D. M., Rahman, T. F. A., Deraman, N. A., Jono, M. N. H. H., & Aziz, A. A. (2021). Development of organization, social and individual cyber security awareness model (OSICSAM) for the elderly. *International Journal of Advanced Technology and Engineering Exploration*, 8(76), 511.
- Chachavalpongpun, P. (2022). Nationhood in the Cloud: Cyber Sovereignty in Thailand. *Asian Studies Review*, 47(2), 392-411.
- Chaiwut, N., & Rueangsirarak, W. (2022). *An Online Gap Analysis on Cyber Security Principles for Thailand Organizations Based on ISO/IEC 27001:2013 Standard*. In 2022 6th International Conference on Information Technology (InCIT), (pp.479-484). Nonthaburi, Thailand, 2022.

- Charness, N., & Boot, W. R. (2009). Aging and information technology use: Potential and barriers. *Current directions in psychological science*, 18(5), 253-258.
- Chuamuangphan, J. (2020). The Conception of Cybersecurity in Thailand. *Journal of Technology and Innovation in Tertiary Education Siam Technology College*, 1(2), 37-45.
- Diteeyont, W., & Ku, H. (2021). Internet literacy among the elderly in Thailand. *Educational Media International*, 58, 248-260.
- Hamilton, B. M., Orak, U., Wallace, J. B. (2022). Internet Use as a Moderator of the Relationship between Age and Depression: Implications for Older Adults. *Journal of Applied Gerontology*, 42(5), 942-950.
- Hill, R., Betts, L. R., & Gardner, S. E. (2015). Older adults' experiences and perceptions of digital technology:(Dis) empowerment, wellbeing, and inclusion. *Computers in Human Behavior*, 48, 415-423.
- Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2018). Risky remote purchasing and identity theft victimization among older Internet users. *Psychology, Crime & Law*, 24(3), 243-256.
- Jiang, L., & Bai, G. (2020). Security analysis and improvements of authentication and access control in the Internet of Things. *Sensors*, 20(17), 4794.
- Jorge, J., Varela, Cristóbal, Hernández, Rafaela, Ramos, Miranda, Christopher, P., Barlett, Matías, E., Rodríguez-Rivas. (2022). Victims of Cyberbullying: Feeling Loneliness and Depression among Youth and Adult Chileans during the Pandemic. *International Journal of Environmental Research and Public Health*, 19(10), 5886-5886.
- Katsantonis, M., Manikas, A., Mavridis, I., & Gritzalis, D. (2023). Cyber range design framework for cyber security education and training. *International Journal of Information Security*, 22, 1005-1027.
- Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, 50(7), 80-84.
- Kopp, E., Kaffenberger, L., Wilson, C. (2017). *Cyber Risk, Market Failures, and Financial Stability*, 17(185).
- Kraiwanit, T., Jangjarat, K. (2023). Factors Determining Online Activities and Technology Use Among Older Adults in Thailand. *Pertanika Journal of Social Science and Humanities*, 31(2).
- Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1), 1-10.

- Laohabutr, P., Subchartanan, J., Suteerotrakool, O., Tempark, T., & Bongsebandhu-phubhakdi, C. (2021). Thai teens' privacy-related practices on Facebook. *Journal of Children and Media*, 16, 406-414.
- Manić, L., Miljković, J. (2022). Cyber security of the elderly. *Bezbednost*, 643, 120-139.
- Martin, N., & Rice, J. P. (2013). Spearing High Net Wealth Individuals: The Case of Online Fraud and Mature Age Internet Users. *International Journal of Information Security and Privacy*, 7(1), 15.
- Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing*, 5(4), 586-602.
- Nadia, M., Brashier, Daniel, L., Schacter. (2020). Aging in an Era of Fake News. *Current Directions in Psychological Science*, 29(3), 316-323.
- Narayanan, V., Robertson, B., Hickerson, A., Srivastava, B., & Smith, B. (2021). Securing social media for seniors from information attacks: Modeling, detecting, intervening, and communicating risks. *Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 297-302.
- Nef, T., Ganea, R. L., Müri, R. M., & Mosimann, U. P. (2013). Social networking sites and older users—a systematic review. *International psychogeriatrics*, 25(7), 1041-1053.
- Padikkapparambil, J., Ncube, C., Singh, K. K., & Singh, A. (2020). Internet of Things technologies for elderly health-care applications. In *Emergence of pharmaceutical industry growth with industrial IoT approach*, (pp. 217-243). Academic Press.
- Ping, C., Tsaifa, (TF), Yen. (2023). How does Digital Trust Make Up for the Digital Divide in Elderly Care Services. *Asian Journal of Advanced Research and Reports*, 17(9).
- Rafih, H., & Munteanu, C. (2023). Understanding Older Adults' Safety Perceptions and Risk Mitigation Strategies when Accessing Online Services. *Lecture Notes in Computer Science*, 467-491.
- Rice, E. S., Haynes, E., Royce, P., & Thompson, S. C. (2016). Social media and digital technology use among Indigenous young people in Australia: a literature review. *International journal for equity in health*, 15, 1-16.
- Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2266-2279.
- Saariluoma, P. (2016). Cybersecurity for old people. *Gerontechnology*, 14(63).
- Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146-164.

- Sriwisathiyakun, K., & Dhamanitayakul, C. (2022). Enhancing digital literacy with an intelligent conversational agent for senior citizens in Thailand. *Education and Information Technologies*, 27, 6251-6271.
- Sugunaraj, N., Ramchandra, A., & Ranganathan, P. (2022). *Cyber Fraud Economics, Scam Types, and Potential Measures to Protect U.S. Seniors: A Short Review*. In 2022 IEEE International Conference on Electro Information Technology (eIT), (pp. 623-627).
- Tsai-Fa, Yen. (2022). Digital Risk, Digital Privacy and their Impacts on the Usage Intentions of Smart Senior Health Care Service. *International journal of social sciences perspectives*, 11(2), 105-113.
- Vailati Riboni, F., Sadowski, I., Comazzi, B., & Pagnini, F. (2022). Mindful age and technology: A qualitative analysis of a tablet/smartphone app intervention designed for older adults. *Integrative Psychological and Behavioral Science*, 56(3), 739-754.
- Wiederhold, B. K. (2020). Connecting through technology during the coronavirus disease 2019 pandemic: Avoiding "Zoom Fatigue". *Cyberpsychology, Behavior, and Social Networking*, 23(7), 437-438.
- Zulkipli, N. (2021). Synthesizing Cybersecurity Issues and Challenges For The Elderly. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(5), 1775-1781.
- Žvanut, B., & Mihelič, A. (2022). Qualitative study on domestic social robot adoption and associated security concerns among older adults in Slovenia. *Front. Psychol.* 15.