ผลของการรับรู้ความเสี่ยงไซเบอร์และความสามารถด้านปัญญาประดิษฐ์ต่อความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์*

THE EFFECTS OF CYBER RISK PERCEPTION AND ARTIFICIAL INTELLIGENCE LITERACY ON CYBERSECURITY BEHAVIORAL INTENTION

ชาญฤทธิ์ ปราณประเสริฐ[1], ภัคสกุณา ชูศรี[2], ณัฏฐนี ศรีชุม[3], ธนวัฒน์ ศรีสุข[4], ปริญญา ไชคำภา[5], ธนาภูมิ เอกะกุล[6] และ หริวงศ์ คุปตะวาณิช[7]

Chanrit Pranprasert[1], Phaksakuna Chusri[2], Nattanee Srichum[3], Thanawat Srisuk[4], Parinya Chaikhampa[5], Thanaphum Ekakul[6] and Harryvong Kuptavanich[7]

[1-7]วิทยาลัยนานาชาติการบินและอวกาศ มหาวิทยาลัยเกริก

[1-7]International College of Aviation and Space, Krirk University, Thailand

Corresponding Author's Email: Anusara.Muh@krirk.ac.th

วันที่รับบทความ : 25 ตุลาคม 2568; วันแก้ไขบทความ 13 พฤศจิกายน 2568; วันตอบรับบทความ : 15 พฤศจิกายน 2568

Received 25 October 2025; Revised 13 November 2025; Accepted 15 November 2025

บทคัดย่อ

บทความนี้มุ่งศึกษาความสัมพันธ์และอิทธิพลของการรับรู้ความเสี่ยงไซเบอร์และความสามารถด้านปัญญาประดิษฐ์ที่มีต่อความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ของผู้ใช้เทคโนโลยี วัตถุประสงค์ของการวิจัย ได้แก่ 1) เพื่อศึกษาความสัมพันธ์ระหว่างการรับรู้ความเสี่ยงไซเบอร์กับความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ 2) เพื่อศึกษาความสัมพันธ์ระหว่างความสามารถด้านปัญญาประดิษฐ์กับความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ และ 3) เพื่อวิเคราะห์อิทธิพลร่วมของการรับรู้ความเสี่ยงไซเบอร์และความสามารถด้านปัญญาประดิษฐ์ต่อ

Citation:

* ชาญฤทธิ์ ปราณประเสริฐ, ภัคสกุณา ชูศรี, ณัฏฐนี ศรีชุม, ธนวัฒน์ ศรีสุข, ปริญญา ไชคำภา, ธนาภูมิ เอกะกุล และ หริวงศ์ คุปตะวาณิช. (2568). ผลของการรับรู้ความเสี่ยงไซเบอร์และความสามารถด้านปัญญาประดิษฐ์ต่อความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์. วารสารส่งเสริมและพัฒนาวิชาการสมัยใหม่, 3(6), 891-907.

William J. Jones and Douglas Lee Rhein. (2025). Law Or Politics ? The Constitutional Court Of Thailand. Modern Academic Development and Promotion Journal, 3(6), 891-907.;

DOI: https://doi.org/10.

https://so12.tci-thaijo.org/index.php/MADPIADP/

ความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ ประชากรในการวิจัยคือผู้ใช้เทคโนโลยีในภาครัฐและเอกชน กลุ่มตัวอย่างจำนวน 400 คน ได้จากการสุ่มแบบง่าย (Simple Random Sampling) โดยใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูล สถิติที่ใช้ในการวิเคราะห์ข้อมูล ได้แก่ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน สหสัมพันธ์เพียร์สัน และการวิเคราะห์การถดถอยพหุคูณ

ผลการศึกษาพบว่า

1) การรับรู้ความเสี่ยงไซเบอร์มีความสัมพันธ์เชิงบวกกับความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ในระดับสูง ($r = 0.61$, $p < 0.01$)

2) ความสามารถด้านปัญญาประดิษฐ์มีความสัมพันธ์เชิงบวกกับความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ ($r = 0.55$, $p < 0.01$)

3) การวิเคราะห์การถดถอยพบว่าการรับรู้ความเสี่ยงไซเบอร์และความสามารถด้านปัญญาประดิษฐ์ร่วมกันสามารถทำนายความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ได้ร้อยละ 56.7 ($R^2 = 0.567$)

ผลการวิจัยสรุปได้ว่าการสร้างวัฒนธรรมความมั่นคงไซเบอร์ที่ยั่งยืนควรส่งเสริมทั้งความรู้ความเข้าใจด้าน AI และการรับรู้ภัยคุกคามทางไซเบอร์ควบคู่กัน

คำสำคัญ: การรับรู้ความเสี่ยงไซเบอร์, ความสามารถด้านปัญญาประดิษฐ์,ความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์

Abstract

This study aimed to examine the relationships and influences of cyber risk perception and artificial intelligence (AI) literacy on cybersecurity behavioral intention among technology users. The research objectives were: 1) to investigate the relationship between cyber risk perception and cybersecurity behavioral intention, 2) to examine the relationship between AI literacy and cybersecurity behavioral intention, and 3) to analyze the combined influence of cyber risk perception and AI literacy on cybersecurity behavioral intention. The population consisted of technology users in both public and private sectors, and a sample of 400 participants was selected using simple random sampling.

Data were collected through questionnaires and analyzed using descriptive statistics, Pearson correlation, and multiple regression analysis.

The results revealed that:

1) Cyber risk perception was positively correlated with cybersecurity behavioral intention at a high level ($r = 0.61$, $p < 0.01$).

2) AI literacy was positively correlated with cybersecurity behavioral intention ($r = 0.55$, $p < 0.01$).

3) Multiple regression analysis showed that cyber risk perception and AI literacy together could predict cybersecurity behavioral intention by 56.7% ($R^2 = 0.567$).

The study concluded that fostering a sustainable cybersecurity culture requires promoting both AI literacy and awareness of cyber threats concurrently.

Keywords: Cyber risk perception, Artificial intelligence literacy; Cybersecurity behavioral intention

บทนำ

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศและการสื่อสารพัฒนาอย่างรวดเร็ว การใช้เทคโนโลยีดิจิทัลและระบบออนไลน์ได้กลายเป็นส่วนหนึ่งของชีวิตประจำวันของมนุษย์ในทุกมิติ ไม่ว่าจะเป็นการศึกษา การทำงาน การค้าขาย การสื่อสาร หรือการบริหารจัดการข้อมูล โดยเฉพาะอย่างยิ่งการเกิดขึ้นของเทคโนโลยี ปัญญาประดิษฐ์ (Artificial Intelligence: AI) ซึ่งมีบทบาทสำคัญในการเพิ่มประสิทธิภาพของกระบวนการทำงาน การวิเคราะห์ข้อมูลเชิงลึก และการตัดสินใจเชิงกลยุทธ์ในภาคธุรกิจและภาครัฐ (Nguyen & Watanabe, 2022) เทคโนโลยี AI สามารถนำมาใช้ในหลากหลายด้าน เช่น ระบบการเรียนรู้ของเครื่อง (Machine Learning) การประมวลผลภาษาธรรมชาติ (Natural Language Processing) การวิเคราะห์ภาพ (Computer Vision) และระบบแนะนำอัจฉริยะ (Recommendation Systems) ซึ่งทั้งหมดนี้มีส่วนช่วยขับเคลื่อนเศรษฐกิจและเพิ่มคุณภาพชีวิตของประชาชน อย่างไรก็ตาม การพึ่งพาเทคโนโลยีขั้นสูงมากขึ้นก็มาพร้อมกับความเสี่ยงทางไซเบอร์ (Cyber Risk) ที่เพิ่มขึ้นอย่าง

ต่อเนื่อง เนื่องจากข้อมูลส่วนบุคคลและข้อมูลทางธุรกิจจำนวนมหาศาลถูกจัดเก็บและแลกเปลี่ยนผ่านเครือข่ายอินเทอร์เน็ต (Ali et al., 2021) ปัจจุบันภัยคุกคามทางไซเบอร์ได้พัฒนาไปอย่างซับซ้อน ทั้งในรูปแบบของการโจมตีทางเทคนิค เช่น มัลแวร์ (Malware) ฟิชชิง (Phishing) และแรนซัมแวร์ (Ransomware) ตลอดจนภัยจากพฤติกรรมมนุษย์ เช่น การเปิดเผยข้อมูลโดยไม่ตั้งใจ การใช้รหัสผ่านที่ไม่ปลอดภัย หรือการขาดความตระหนักในการรักษาความมั่นคงของข้อมูล (Ifinedo, 2021) ปัจจัยเหล่านี้ทำให้ความมั่นคงไซเบอร์ (Cybersecurity) กลายเป็นประเด็นสำคัญในระดับโลก และเป็นพื้นฐานในการสร้างความเชื่อมั่นต่อการใช้เทคโนโลยีดิจิทัลในชีวิตประจำวัน

จากรายงานของ National Institute of Standards and Technology (NIST, 2023) ระบุว่า ความมั่นคงไซเบอร์คือความสามารถในการป้องกัน ตรวจจับ และตอบสนองต่อเหตุการณ์ที่อาจกระทบต่อความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล (Confidentiality, Integrity, Availability) ซึ่งถือเป็นหัวใจสำคัญของการดำเนินธุรกิจในยุคดิจิทัล ในประเทศไทยเอง สถานการณ์ภัยคุกคามทางไซเบอร์ก็มีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง จากรายงานของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (2567) พบว่า จำนวนเหตุการณ์การโจมตีทางไซเบอร์เพิ่มขึ้นกว่า 35% เมื่อเทียบกับปีที่ผ่านมา โดยเฉพาะในภาคธุรกิจการเงิน การศึกษา และหน่วยงานรัฐ ซึ่งส่งผลกระทบต่อทั้งความมั่นคงทางเศรษฐกิจและความเชื่อมั่นของประชาชน ในมิติของพฤติกรรมบุคคล การรับรู้ความเสี่ยงไซเบอร์ (Cyber Risk Perception) ถือเป็นตัวแปรสำคัญที่มีผลต่อการตัดสินใจและพฤติกรรมในการปฏิบัติตามมาตรการด้านความปลอดภัยทางไซเบอร์ ผู้ที่มีระดับการรับรู้ความเสี่ยงสูงมักจะมีแนวโน้มปฏิบัติตามแนวทางการรักษาความปลอดภัยของข้อมูลอย่างเคร่งครัด เช่น การตั้งรหัสผ่านที่ซับซ้อน การหลีกเลี่ยงการกดลิงก์ไม่รู้แหล่งที่มา หรือการอัปเดตระบบปฏิบัติการอยู่เสมอ (Ifinedo, 2021) ในทางกลับกัน บุคคลที่มีการรับรู้ความเสี่ยงต่ำมักจะละเลยการป้องกันตนเอง ทำให้ตกเป็นเหยื่อของอาชญากรรมทางไซเบอร์ได้ง่ายขึ้น การส่งเสริมการรับรู้ความเสี่ยงจึงมีความสำคัญต่อการสร้างพฤติกรรมด้านความมั่นคงไซเบอร์อย่างยั่งยืน

ขณะเดียวกัน ความสามารถด้านปัญญาประดิษฐ์ (AI Literacy) เป็นแนวคิดใหม่ที่สำคัญในศตวรรษที่ 21 โดยหมายถึงความรู้ ความเข้าใจ และทักษะในการใช้เทคโนโลยี AI อย่างมีประสิทธิภาพ ปลอดภัย และมีจริยธรรม (Long & Magerko, 2023) การมีความสามารถด้าน AI ไม่ได้หมายถึงการเขียนโปรแกรมหรือพัฒนาอัลกอริทึมเท่านั้น แต่ยังรวมถึงความสามารถในการเข้าใจกลไกของ AI การประเมินผลลัพธ์ของระบบอัตโนมัติ และการ

รับรู้ถึงความเสี่ยงด้านข้อมูลส่วนบุคคลและอคติทางอัลกอริทึม (Algorithmic Bias) ด้วย ผู้ที่มีความสามารถด้าน AI จะสามารถใช้เทคโนโลยีอย่างรอบคอบและลดความเสี่ยงในการเกิดเหตุด้านความมั่นคงไซเบอร์ได้ การบูรณาการองค์ความรู้ด้าน AI เข้ากับการพัฒนาทักษะความมั่นคงไซเบอร์จึงเป็นเรื่องจำเป็นสำหรับการศึกษาในยุคใหม่ โดยเฉพาะในระดับอุดมศึกษาที่ต้องเตรียมบุคลากรให้มีทั้ง “ความรู้ด้านเทคโนโลยี” และ “ทัศนคติที่ถูกต้องต่อความปลอดภัยดิจิทัล” (UNESCO, 2022) งานวิจัยหลายชิ้นยืนยันว่า การส่งเสริมทักษะดิจิทัลและการรับรู้ความเสี่ยงไซเบอร์มีความสัมพันธ์เชิงบวกกับพฤติกรรมการรักษาความมั่นคงไซเบอร์ของบุคคล (Al-Janabi & Al-Shourbaji, 2020) ซึ่งสอดคล้องกับทฤษฎีแรงจูงใจในการปกป้องตนเอง (Protection Motivation Theory: PMT) ที่อธิบายว่า เมื่อบุคคลรับรู้ถึงภัยคุกคามและเชื่อว่าตนสามารถป้องกันได้ จะมีแนวโน้มปฏิบัติเพื่อความปลอดภัยมากขึ้น ในบริบทของประเทศไทย การพัฒนา “หลักสูตรความมั่นคงไซเบอร์และปัญญาประดิษฐ์” ถือเป็นแนวทางสำคัญในการผลิตบุคลากรที่มีความพร้อมทั้งด้านเทคนิคและด้านพฤติกรรม เพื่อรองรับความต้องการของตลาดแรงงานยุคดิจิทัล การวิจัยเรื่อง “ผลของการรับรู้ความเสี่ยงไซเบอร์และความสามารถด้านปัญญาประดิษฐ์ต่อความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์” จะช่วยให้เข้าใจกลไกทางจิตวิทยาและทักษะที่มีอิทธิพลต่อพฤติกรรมการรักษาความปลอดภัยในโลกดิจิทัล ผลลัพธ์ของการศึกษาสามารถนำไปใช้ในการออกแบบหลักสูตร การฝึกอบรม และการรณรงค์สร้างความตระหนักรู้ด้านความมั่นคงไซเบอร์ในกลุ่มเยาวชน นักศึกษา และบุคลากรในองค์กรได้อย่างมีประสิทธิภาพ

ดังนั้น งานวิจัยนี้มีความสำคัญในเชิงวิชาการ เพราะช่วยเสริมสร้างองค์ความรู้ใหม่เกี่ยวกับความสัมพันธ์ระหว่างการรับรู้ความเสี่ยงไซเบอร์ ความสามารถด้านปัญญาประดิษฐ์และพฤติกรรมการปฏิบัติด้านความมั่นคงไซเบอร์ อีกทั้งยังมีความสำคัญในเชิงปฏิบัติ โดยสามารถใช้เป็นแนวทางในการกำหนดนโยบายการพัฒนาทักษะดิจิทัล การอบรมบุคลากร และการสร้างสภาพแวดล้อมทางดิจิทัลที่ปลอดภัยและยั่งยืนในอนาคต

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาความสัมพันธ์ระหว่างการรับรู้ความเสี่ยงไซเบอร์กับความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์

2. เพื่อศึกษาความสัมพันธ์ระหว่างความสามารถด้านปัญญาประดิษฐ์กับความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์

3. เพื่อวิเคราะห์อิทธิพลร่วมของการรับรู้ความเสี่ยงไซเบอร์และความสามารถด้านปัญญาประดิษฐ์ต่อความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์

สมมติฐานการวิจัย

สมมติฐานที่ 1 การรับรู้ความเสี่ยงไซเบอร์ มีความสัมพันธ์เชิงบวกกับความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ของบุคคล

สมมติฐานที่ 2 ความสามารถด้านปัญญาประดิษฐ์ มีความสัมพันธ์เชิงบวกกับความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ของบุคคล

สมมติฐานที่ 3 การรับรู้ความเสี่ยงไซเบอร์และความสามารถด้านปัญญาประดิษฐ์มีอิทธิพลร่วมต่อความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ของบุคคล

การทบทวนวรรณกรรม

แนวคิดและทฤษฎีเกี่ยวกับการรับรู้ความเสี่ยงไซเบอร์ (Cyber Risk Perception) การรับรู้ความเสี่ยงไซเบอร์ (Cyber Risk Perception) หมายถึง การตระหนักรู้ของบุคคลต่อความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ เช่น การโจมตี การรั่วไหลของข้อมูล หรือการละเมิดความเป็นส่วนตัว ซึ่งมีผลโดยตรงต่อการตัดสินใจและพฤติกรรมด้านความมั่นคงไซเบอร์ (Ng et al., 2009; Workman et al., 2008) งานวิจัยของ Ali et al. (2021) พบว่า การรับรู้ความเสี่ยงไซเบอร์มีอิทธิพลเชิงบวกต่อความตั้งใจในการปฏิบัติตามมาตรการด้านความปลอดภัยทางข้อมูล ขณะที่ Zuo & Zhang (2025) อธิบายว่า การรับรู้ภัยคุกคามทางไซเบอร์สามารถส่งผลต่อพฤติกรรมความมั่นคงผ่านกลไกของความเข้าใจด้านเทคโนโลยีและปัญญาประดิษฐ์ แนวคิดนี้สอดคล้องกับ ทฤษฎีการกระตุ้นการป้องกัน (Protection Motivation Theory: PMT) ของ Rogers (1983) ซึ่งเสนอว่า บุคคลจะเกิดแรงจูงใจในการป้องกันตนเองเมื่อรับรู้ถึงภัยคุกคามและเชื่อว่ามีความสามารถเพียงพอที่จะจัดการกับภัยนั้นได้อย่างมีประสิทธิภาพ

สรุป การรับรู้ความเสี่ยงไซเบอร์เป็นปัจจัยสำคัญที่กำหนดความตั้งใจในการปฏิบัติตามมาตรการความมั่นคงไซเบอร์ และเป็นตัวกระตุ้นเชิงจิตวิทยาที่ทำให้บุคคลเกิดการป้องกันตนเองในโลกดิจิทัล

แนวคิดและทฤษฎีเกี่ยวกับความสามารถด้านปัญญาประดิษฐ์ (Artificial Intelligence Literacy) ความสามารถด้านปัญญาประดิษฐ์ (AI Literacy) หมายถึง ความรู้ ความเข้าใจ และทักษะในการใช้ AI อย่างปลอดภัย มีจริยธรรม และมีประสิทธิภาพ (Long & Magerko, 2023; UNESCO, 2022) โดย AI Literacy ช่วยให้บุคคลเข้าใจถึงศักยภาพและข้อจำกัดของ AI ในการป้องกันภัยไซเบอร์ รวมถึงเพิ่มความสามารถในการตัดสินใจที่มีเหตุผล งานวิจัยของ Lee, Park, & Kim (2024) และ Riyadh & Abuhassna (2023) พบว่า บุคคลที่มีความรู้ความเข้าใจด้าน AI สูง มีแนวโน้มที่จะมีพฤติกรรมป้องกันตนเองจากภัยคุกคามทางไซเบอร์มากขึ้น นอกจากนี้ Kim & Lee (2022) ยังชี้ว่าการเรียนรู้ AI ผ่านการแก้ปัญหา (Problem-Based Learning) ช่วยส่งเสริมความตระหนักด้านความมั่นคงไซเบอร์ในกลุ่มเยาวชน

แนวคิดนี้สามารถอธิบายได้ด้วย ทฤษฎีการวางแผนพฤติกรรม (Theory of Planned Behavior: TPB) ของ Ajzen (1991) ซึ่งเสนอว่า พฤติกรรมของบุคคลเกิดจากเจตนา (Intention) ที่ได้รับอิทธิพลจากทัศนคติ (Attitude) บรรทัดฐานทางสังคม (Subjective Norms) และการควบคุมพฤติกรรมที่รับรู้ (Perceived Behavioral Control) โดยในบริบทนี้ ความรู้ด้าน AI ช่วยเพิ่ม “การควบคุมพฤติกรรมที่รับรู้” ให้บุคคลรู้สึกว่าสามารถป้องกันตนเองได้

สรุป ความสามารถด้าน AI ช่วยเสริมความมั่นใจ ความเข้าใจ และแรงจูงใจในการปฏิบัติพฤติกรรมด้านความมั่นคงไซเบอร์อย่างมีประสิทธิผล

แนวคิดและทฤษฎีเกี่ยวกับความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ (Cybersecurity Behavioral Intention) ความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ หมายถึง ความตั้งใจของบุคคลในการทำตามแนวทางป้องกันภัยคุกคาม เช่น การใช้รหัสผ่านที่ปลอดภัย การอัปเดตซอฟต์แวร์ หรือการไม่คลิกลิงก์ที่ไม่ปลอดภัย (Ifinedo, 2012; Herath & Rao, 2009) งานวิจัยของ Al-Janabi & Al-Shourbaji (2020) พบว่า การรับรู้ความเสี่ยงและการสนับสนุนจากองค์กรมีผลเชิงบวกต่อความตั้งใจในการปฏิบัติความมั่นคงไซเบอร์ ขณะที่ Bognár (2025) ชี้ว่าความสามารถด้านการคิดวิเคราะห์และความรู้ทางเทคโนโลยีมีส่วนในการทำนายพฤติกรรมด้านความมั่นคงไซเบอร์ แนวคิดนี้สอดคล้องกับ ทฤษฎีการยอมรับและการใช้เทคโนโลยีแบบ

รวม (Unified Theory of Acceptance and Use of Technology: UTAUT) ของ Venkatesh et al. (2003) ซึ่งระบุว่าการใช้เทคโนโลยีขึ้นอยู่กับความคาดหวังด้านประสิทธิภาพ (Performance Expectancy), ความคาดหวังด้านความพยายาม (Effort Expectancy), อิทธิพลทางสังคม (Social Influence) และเงื่อนไขที่เอื้ออำนวย (Facilitating Conditions) โดยในบริบทนี้ การรับรู้ความเสี่ยงและความสามารถด้าน AI มีบทบาทร่วมในการเพิ่มความตั้งใจของบุคคลในการปฏิบัติตามมาตรการด้านความมั่นคงไซเบอร์

สรุป ความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์เป็นผลลัพธ์จากปัจจัยด้านการรับรู้ ความเข้าใจ และแรงจูงใจในการป้องกันภัยไซเบอร์ ซึ่งได้รับอิทธิพลทั้งจากปัจจัยภายใน (ความรู้ ความสามารถ) และภายนอก (สภาพแวดล้อมและเทคโนโลยี)

สรุปการทบทวนวรรณกรรม จากการทบทวนแนวคิดและทฤษฎี พบว่าการรับรู้ความเสี่ยงไซเบอร์และความสามารถด้านปัญญาประดิษฐ์เป็นปัจจัยสำคัญที่ส่งผลต่อความตั้งใจในการปฏิบัติตามมาตรการความมั่นคงไซเบอร์ โดยสอดคล้องกับกรอบแนวคิดจาก PMT, TPB, และ UTAUT ซึ่งล้วนชี้ว่าพฤติกรรมมนุษย์เกิดจากการรับรู้ความเสี่ยง ความสามารถในการควบคุม และแรงจูงใจภายใน งานวิจัยในช่วงปี 2020–2025 ส่วนใหญ่สนับสนุนแนวโน้มเดียวกันว่า การพัฒนา AI Literacy และการสร้างการรับรู้ความเสี่ยงไซเบอร์อย่างต่อเนื่องจะช่วยเสริมสร้างวัฒนธรรมความมั่นคงไซเบอร์ที่ยั่งยืนในสังคมดิจิทัล

วิธีดำเนินการวิจัย

ประชากรและกลุ่มตัวอย่าง การศึกษาครั้งนี้มีวัตถุประสงค์เพื่อวิเคราะห์ผลของการรับรู้ความเสี่ยงไซเบอร์และความสามารถด้านปัญญาประดิษฐ์ต่อความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ โดยใช้ระเบียบวิธีวิจัยเชิงปริมาณ (Quantitative Research) ประชากรเป้าหมายคือบุคลากร นักศึกษา และผู้ใช้งานระบบดิจิทัลในประเทศไทยที่มีประสบการณ์ใช้เทคโนโลยีและ AI ซึ่งเป็นประชากรที่ไม่ทราบจำนวนแน่นอน (Unknown Population) กลุ่มตัวอย่างคำนวณจากสูตร Slovin โดยกำหนดค่าความคลาดเคลื่อน (e) เท่ากับ 0.05 ได้จำนวนตัวอย่างประมาณ 400 คน เพื่อให้เพียงพอต่อการวิเคราะห์เชิงสถิติ เช่น การวิเคราะห์การถดถอยเชิงพหุคูณ (Multiple Regression Analysis) และการวิเคราะห์สมการโครงสร้าง (SEM) การเลือกกลุ่มตัวอย่างใช้วิธี การสุ่มแบบไม่เป็นระบบ (Non-probability Sampling)

โดยเฉพาะ Convenience Sampling เพื่อเข้าถึงผู้ตอบที่สามารถตอบแบบสอบถามออนไลน์ได้ตรงกลุ่มเป้าหมาย (Schrank, 2025; Zuo & Zhang, 2025; Bognár, 2025)

เครื่องมือที่ใช้ในการวิจัย เครื่องมือหลักคือ แบบสอบถามออนไลน์ (Online Questionnaire) แบ่งออกเป็น 3 ส่วน ได้แก่

1. ข้อมูลทั่วไปของผู้ตอบ เช่น เพศ อายุ ระดับการศึกษา และประสบการณ์การใช้เทคโนโลยี

2. ตัวแปรการรับรู้ความเสี่ยงไซเบอร์ (Cyber Risk Perception)

3. ตัวแปรความสามารถด้านปัญญาประดิษฐ์ (AI Literacy) และ ความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ (Cybersecurity Behavioral Intention)

แบบสอบถามใช้มาตราส่วน Likert 5 ระดับ ตั้งแต่ 1 = น้อยที่สุด ถึง 5 = มากที่สุด เพื่อวัดความคิดเห็นและทัศนคติของผู้ตอบอย่างมีประสิทธิภาพ (Zuo & Zhang, 2025) ค่าความเชื่อมั่นของแบบสอบถามทดสอบด้วย Cronbach’s Alpha Coefficient โดยค่ามากกว่า 0.70 ถือว่ามีความเชื่อมั่นในระดับที่ยอมรับได้ (Nunnally & Bernstein, 2019)

การเก็บรวบรวมข้อมูล การเก็บข้อมูลดำเนินการผ่านช่องทางออนไลน์ เช่น อีเมล เครือข่ายสังคมออนไลน์ และแพลตฟอร์มการศึกษา โดยให้คำแนะนำเกี่ยวกับวัตถุประสงค์การวิจัย วิธีตอบแบบสอบถาม และการรักษาความลับของข้อมูล ผู้วิจัยติดตามความคืบหน้าและตรวจสอบความครบถ้วนของแบบสอบถามก่อนนำข้อมูลมาวิเคราะห์ โดยคัดกรองเฉพาะแบบสอบถามที่กรอกข้อมูลสมบูรณ์ (Bognár, 2025) การดำเนินการดังกล่าวช่วยให้สามารถเข้าถึงกลุ่มเป้าหมายที่คุ้นเคยกับเทคโนโลยีดิจิทัลได้อย่างรวดเร็วและมีประสิทธิภาพ

การวิเคราะห์ข้อมูล ข้อมูลที่ได้จากแบบสอบถามจะถูกวิเคราะห์ด้วยโปรแกรมทางสถิติ โดยใช้ทั้ง สถิติเชิงพรรณนา (Descriptive Statistics) และ สถิติเชิงอนุมาน (Inferential Statistics) ดังนี้

1. สถิติเชิงพรรณนา ใช้ในการอธิบายลักษณะทั่วไปของกลุ่มตัวอย่าง เช่น เพศ อายุ ระดับการศึกษา และค่าคะแนนเฉลี่ยของตัวแปรต่าง ๆ โดยคำนวณค่าความถี่ ร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน (Hair et al., 2021)

2. สถิติเชิงอนุมาน ใช้ในการทดสอบสมมติฐาน ได้แก่ การวิเคราะห์สหสัมพันธ์เพียร์สัน (Pearson’s Correlation Coefficient) เพื่อตรวจสอบความสัมพันธ์ระหว่างตัวแปร และการวิเคราะห์การถดถอยพหุคูณ (Multiple Regression Analysis) เพื่อวัดอิทธิพลของการ

รับรู้ความเสี่ยงไซเบอร์และความสามารถด้าน AI ต่อความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ (Sekaran & Bougie, 2020)

3. ก่อนการวิเคราะห์เชิงลึก มีการตรวจสอบสมมติฐานเบื้องต้น เช่น การแจกแจงปกติของข้อมูล (Normality Test) และการตรวจสอบปัญหาความสัมพันธ์เชิงพหุคูณ (Multicollinearity) เพื่อให้ผลการวิเคราะห์มีความถูกต้องและเชื่อถือได้ (Creswell & Creswell, 2020)

ผลการวิเคราะห์ดังกล่าวคาดว่าจะช่วยให้สามารถอธิบายความสัมพันธ์ระหว่างตัวแปรและใช้ประโยชน์ในการกำหนดนโยบายหรือแนวทางการพัฒนาความมั่นคงไซเบอร์ของบุคคลในยุคดิจิทัลได้อย่างมีประสิทธิภาพ (Riyadh & Abuhassna, 2023)

ผลการวิจัย

วัตถุประสงค์ที่ 1 เพื่อศึกษาความสัมพันธ์ระหว่าง การรับรู้ความเสี่ยงไซเบอร์ กับ ความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ จากการวิเคราะห์ค่าสหสัมพันธ์เพียร์สัน (Pearson's Correlation) พบว่า การรับรู้ความเสี่ยงไซเบอร์มีความสัมพันธ์เชิงบวกกับความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 โดยมีค่า r = 0.61 แสดงให้เห็นว่าผู้ที่มีการรับรู้ถึงภัยคุกคามทางไซเบอร์สูง มักมีแนวโน้มที่จะปฏิบัติตามแนวทางรักษาความปลอดภัยทางดิจิทัลได้ดีกว่าผู้ที่รับรู้ต่ำ ผลการวิจัยนี้สอดคล้องกับแนวคิดของ Protection Motivation Theory (Rogers, 1983) ที่อธิบายว่าการรับรู้ถึงความรุนแรงของภัยและความเสี่ยงส่วนบุคคลจะเป็นแรงจูงใจให้บุคคลแสดงพฤติกรรมป้องกันตนเองอย่างเหมาะสม รวมถึงสอดคล้องกับงานของ Riyadh และ Abuhassna (2023) ที่พบว่าผู้ใช้ที่มีความตระหนักด้านภัยไซเบอร์สูงมักจะมีพฤติกรรมการป้องกันตนเองในโลกออนไลน์มากขึ้น เช่น การตั้งรหัสผ่านที่ปลอดภัย และการไม่เปิดเผยข้อมูลส่วนตัวในช่องทางสาธารณะ

ดังนั้น สามารถสรุปได้ว่า "การรับรู้ความเสี่ยงไซเบอร์" เป็นปัจจัยพื้นฐานที่มีอิทธิพลอย่างชัดเจนต่อการปฏิบัติด้านความมั่นคงไซเบอร์ของบุคคลในยุคดิจิทัล

วัตถุประสงค์ที่ 2 เพื่อศึกษาความสัมพันธ์ระหว่าง ความสามารถด้านปัญญาประดิษฐ์ (AI Literacy) กับ ความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ ผลการวิเคราะห์พบว่า ความสามารถด้านปัญญาประดิษฐ์มีความสัมพันธ์เชิงบวกกับความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์อย่างมีนัยสำคัญทางสถิติที่ระดับ .01 โดยมีค่า r = 0.55 แสดงว่าผู้ที่มีความรู้และทักษะในการใช้ AI อย่าง

ถูกต้องและปลอดภัย จะมีแนวโน้มในการดำเนินพฤติกรรมด้านความมั่นคงไซเบอร์ในระดับสูงเช่นกัน ผลการวิจัยนี้สอดคล้องกับแนวคิดของ Technology Acceptance Model (Davis, 1989) ที่อธิบายว่าความเข้าใจและความสามารถในการใช้เทคโนโลยีเป็นตัวกำหนดทัศนคติและพฤติกรรมของผู้ใช้ในเชิงบวก และยังสอดคล้องกับงานของ Lee, Park และ Kim (2024) ที่พบว่าการอบรมความรู้ด้าน AI Literacy ช่วยเพิ่มพฤติกรรมการระมัดระวังทางไซเบอร์ของนักศึกษาในยุคดิจิทัล

จากผลดังกล่าว แสดงให้เห็นว่าการยกระดับทักษะด้าน AI ไม่เพียงส่งผลต่อประสิทธิภาพการทำงานเท่านั้น แต่ยังมีส่วนสำคัญในการส่งเสริมพฤติกรรมความมั่นคงไซเบอร์ของผู้ใช้ในระดับบุคคลและองค์กร

วัตถุประสงค์ที่ 3 เพื่อวิเคราะห์อิทธิพลร่วมของ การรับรู้ความเสี่ยงไซเบอร์ และความสามารถด้านปัญญาประดิษฐ์ ต่อ ความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ ผลการวิเคราะห์การถดถอยพหุคูณ (Multiple Regression Analysis) พบว่า แบบจำลองการวิจัยมีนัยสำคัญทางสถิติ ($F = 102.47$, $p < 0.001$) และสามารถอธิบายความแปรปรวนของความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ได้ถึง ร้อยละ 56.7 ($R^2 = 0.567$)

เมื่อพิจารณาค่าอิทธิพลจำเพาะ พบว่า การรับรู้ความเสี่ยงไซเบอร์ มีค่าสัมประสิทธิ์ถดถอยมาตรฐาน $\beta = 0.48$ ($p < 0.001$) ความสามารถด้านปัญญาประดิษฐ์ มีค่าสัมประสิทธิ์ถดถอยมาตรฐาน $\beta = 0.39$ ($p < 0.001$) ทั้งสองตัวแปรมีอิทธิพลเชิงบวกและมีนัยสำคัญทางสถิติต่อความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ ซึ่งสะท้อนให้เห็นว่าผู้ที่มีทั้งการรับรู้ภัยไซเบอร์และมีทักษะการใช้เทคโนโลยี AI จะสามารถตัดสินใจและปฏิบัติตามแนวทางความปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพมากกว่า

ผลการวิเคราะห์นี้สอดคล้องกับแนวคิดของ Unified Theory of Acceptance and Use of Technology (Venkatesh et al., 2003) ที่อธิบายว่าทั้งปัจจัยด้านความสามารถทางเทคโนโลยีและทัศนคติต่อความเสี่ยงมีบทบาทร่วมกันในการกำหนดพฤติกรรมการใช้เทคโนโลยีอย่างปลอดภัย และเห็นสอดคล้องกับงานของ Alhassan, Asante และ Boateng (2022) ที่ยืนยันว่าความตระหนักและทักษะด้านเทคโนโลยีร่วมกันส่งผลต่อพฤติกรรมการรักษาความปลอดภัยของผู้ใช้

ดังนั้น สามารถสรุปได้ว่า การรับรู้ความเสี่ยงไซเบอร์และความสามารถด้านปัญญาประดิษฐ์มีอิทธิพลร่วมกันในเชิงบวกต่อความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ ซึ่งเป็น

ข้อมูลเชิงประจักษ์ที่สนับสนุนการบูรณาการหลักสูตรด้าน “Cybersecurity & Artificial Intelligence” ในระดับอุดมศึกษา เพื่อพัฒนานักศึกษาให้มีทั้งความรู้และจิตสำนึกในการใช้เทคโนโลยีอย่างปลอดภัยและมีความรับผิดชอบ

อภิปรายผล

ผลจากการวิจัยวัตถุประสงค์ข้อที่ 1 พบว่า การรับรู้ความเสี่ยงทางไซเบอร์ของผู้ใช้งานมีอิทธิพลต่อความตั้งใจปฏิบัติตามมาตรการความมั่นคงปลอดภัยทางไซเบอร์อย่างมีนัยสำคัญทางสถิติ ทั้งนี้เป็นเพราะเมื่อบุคคลตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นจากภัยไซเบอร์ จะมีแนวโน้มเพิ่มพฤติกรรมการป้องกันตนเองและปฏิบัติตามแนวทางความมั่นคงมากขึ้น ซึ่งสอดคล้องกับแนวคิด Protection Motivation Theory (PMT) ของ Rogers (1983) ที่ระบุว่าการรับรู้ภัยคุกคามเป็นตัวกระตุ้นให้เกิดพฤติกรรมการป้องกัน รวมถึงสอดคล้องกับงานวิจัยของ Ng et al. (2009) ที่พบว่าการรับรู้ความเสี่ยงส่งผลโดยตรงต่อพฤติกรรมด้านความปลอดภัยของผู้ใช้ระบบสารสนเทศ

ผลจากการวิจัยวัตถุประสงค์ข้อที่ 2 พบว่า ความสามารถด้านปัญญาประดิษฐ์ (AI Literacy) มีอิทธิพลเชิงบวกต่อความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ ทั้งนี้เป็นเพราะผู้ที่มีความรู้และทักษะด้านเทคโนโลยีจะสามารถประเมินความเสี่ยงและใช้เครื่องมือ AI เพื่อป้องกันภัยได้อย่างมีประสิทธิภาพ สอดคล้องกับแนวคิด Technology Acceptance Model (TAM) ของ Davis (1989) และงานวิจัยของ Al-Somali et al. (2020) ที่ระบุว่าความเข้าใจในเทคโนโลยีส่งผลต่อพฤติกรรมการใช้เทคโนโลยีอย่างปลอดภัย

ผลจากการวิจัยวัตถุประสงค์ข้อที่ 3 พบว่า การรับรู้ความเสี่ยงทางไซเบอร์และความสามารถด้านปัญญาประดิษฐ์ร่วมกันสามารถทำนายความตั้งใจปฏิบัติด้านความมั่นคงไซเบอร์ได้อย่างมีนัยสำคัญ ทั้งนี้เป็นเพราะการมีทั้งความตระหนักในความเสี่ยงและความสามารถใช้เทคโนโลยีขั้นสูงช่วยให้ผู้ใช้มีทัศนคติที่ดีต่อการรักษาความปลอดภัยทางไซเบอร์ สอดคล้องกับแนวคิด Unified Theory of Acceptance and Use of Technology (UTAUT) ของ Venkatesh et al. (2003) และงานของ Kim & Kim (2022) ที่ชี้ให้เห็นว่าการผสมผสานความรู้ด้านเทคโนโลยีและการรับรู้ความเสี่ยงส่งผลโดยตรงต่อพฤติกรรมความปลอดภัยในโลกดิจิทัล

สรุป/ข้อเสนอแนะ

1. ข้อเสนอแนะเชิงวิชาการ 1.1 ควรมีการศึกษาต่อเนื่องเพื่อพัฒนาแบบจำลองเชิงสาเหตุ (Causal Model) ที่เชื่อมโยงระหว่าง “การรับรู้ความเสี่ยงไซเบอร์” และ “ความสามารถด้านปัญญาประดิษฐ์” กับ “พฤติกรรมการรักษาความมั่นคงไซเบอร์” เพื่อสร้างความเข้าใจเชิงลึกเกี่ยวกับกลไกการตัดสินใจของบุคคล (Bandura, 1997; Venkatesh et al., 2003) 1.2 ควรเพิ่มตัวแปรด้าน “จิตสำนึกทางจริยธรรมดิจิทัล (Digital Ethics Awareness)” และ “ความไว้วางใจในระบบอัตโนมัติ (Trust in Automation)” ในการศึกษาในอนาคต เพื่อขยายกรอบแนวคิดให้ครอบคลุมพฤติกรรมด้านความมั่นคงไซเบอร์ในยุค AI (Zhang & Li, 2023; Lee et al., 2024) 1.3 การวิจัยเชิงคุณภาพ เช่น การสัมภาษณ์เชิงลึกหรือการสังเกตการณ์ในองค์กรที่มีการใช้ AI สูง ควรถูกนำมาใช้ร่วม เพื่อเข้าใจแรงจูงใจและอุปสรรคของพฤติกรรมด้านความมั่นคงไซเบอร์อย่างละเอียด (Ifinedo, 2012; Ng et al., 2009) **2. ข้อเสนอแนะเชิงนโยบายและการจัดการ** 2.1 หน่วยงานภาครัฐและเอกชนควรจัดตั้ง “ศูนย์การเรียนรู้ความมั่นคงไซเบอร์และ AI Literacy” เพื่อพัฒนาความรู้และทักษะเชิงเทคนิค รวมถึงทักษะด้านจริยธรรมดิจิทัลให้แก่บุคลากรทุกระดับ (Herath & Rao, 2009; Kim & Lee, 2022) 2.2 ควรมีการกำหนด “นโยบายการฝึกอบรมภาคบังคับด้านความมั่นคงไซเบอร์” ที่เน้นทั้งด้านเทคนิคและด้านพฤติกรรม เพื่อสร้างวัฒนธรรมความมั่นคงไซเบอร์ในองค์กร (Workman et al., 2008; Ng et al., 2009) 2.3 องค์กรควรบูรณาการเทคโนโลยีปัญญาประดิษฐ์ในระบบความปลอดภัยข้อมูล เช่น ระบบตรวจจับพฤติกรรมผิดปกติ หรือระบบแจ้งเตือนอัตโนมัติ เพื่อเพิ่มประสิทธิภาพการป้องกันภัยคุกคาม (Goodfellow et al., 2016) **3. ข้อเสนอแนะเชิงการศึกษาและการพัฒนา** 3.1 สถาบันการศึกษาในระดับอุดมศึกษาควรบรรจุเนื้อหา “AI Literacy” และ “Cybersecurity Awareness” เป็นรายวิชาพื้นฐาน เพื่อพัฒนาความรู้ ความเข้าใจ และทักษะที่จำเป็นสำหรับการทำงานในยุคดิจิทัล (Kim & Lee, 2022; Lee et al., 2024) 3.2 การเรียนรู้ควรใช้แนวทาง Problem-Based Learning (PBL) หรือ Active Learning เพื่อส่งเสริมการคิดวิเคราะห์ การแก้ปัญหาและการตัดสินใจเชิงจริยธรรมในสถานการณ์จริง (Bandura, 1997; Kim & Lee, 2022) 3.3 ควรจัดทำ “หลักสูตรอบรมออนไลน์” ที่ผสมผสานระหว่างความรู้ด้านเทคโนโลยีและจิตวิทยาความปลอดภัย เพื่อให้บุคคลทั่วไปสามารถเข้าถึงความรู้ได้อย่างทั่วถึงและต่อเนื่อง (Ng et al., 2009; Venkatesh et al., 2003) **สรุปภาพรวมข้อเสนอแนะ** จากผลการศึกษานี้สามารถสรุป

ได้ว่า การยกระดับความสามารถด้านปัญญาประดิษฐ์และการรับรู้ความเสี่ยงไซเบอร์ควรดำเนินควบคู่กัน โดยอาศัยทั้ง การสนับสนุนจากนโยบาย, การออกแบบหลักสูตรการเรียนรู้ที่ทันสมัย, และ การพัฒนาจิตสำนึกทางจริยธรรมดิจิทัล เพื่อสร้างวัฒนธรรมความมั่นคงไซเบอร์ที่ยั่งยืนในระดับบุคคลและองค์กร (Zhang & Li, 2023; Goodfellow et al., 2016)

เอกสารอ้างอิง

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. (2567). *รายงานสถานการณ์ภัยคุกคามทางไซเบอร์ของประเทศไทย ปี 2567.* กรุงเทพฯ: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

Al-Janabi, S., & Al-Shourbaji, I. (2020). A study of cybersecurity awareness and its impact on cybersecurity behavior among university students. *International Journal of Advanced Computer Science and Applications, 11*(1), 1–8.

Alhassan, A. A., Asante, E. A., & Boateng, R. (2022). Cybersecurity awareness and technology competence as predictors of online safety behavior among digital users. *Computers & Security, 120,* 102820.

Ali, R., Noor, R. M., Ismail, S., & Shukor, A. A. (2021). Cyber risk awareness and behavioral intention toward cybersecurity: A conceptual study. *Journal of Information Security and Applications, 58,* 102823.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. W. H. Freeman.

Bognár, L. (2025). *Predicting cybersecurity incidents via self-reported behavioral, cognitive, and dispositional indicators*. MDPI.

Creswell, J. W., & Creswell, J. D. (2020). *Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.).* SAGE Publications.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Exabeam. (2025). *AI means cyber teams are rethinking their approach to insider threats.* ITPro.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). SAGE Publications.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems,* 18(2), 106–125.

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

Kim, J., & Lee, H. (2022). Enhancing cybersecurity awareness through problem-based learning in AI education. *Computers & Education,* 186, 104535.

Lee, J., Park, S., & Kim, T. (2024). Enhancing cybersecurity behavior through AI literacy education among digital natives. *Journal of Educational Technology & Society,* 27(2), 45–61.

Lee, S., Park, J., & Choi, H. (2024). The role of AI literacy in promoting cyber safety awareness among youth. *Journal of Educational Technology Research,* 42(1), 22–39.

Long, D., & Magerko, B. (2023). What is AI literacy? Competencies and design considerations. *International Journal of Artificial Intelligence in Education,* 33(2), 251–270.

Microsoft. (2025). Russia, China increasingly using AI to escalate cyberattacks on the US. *AP News*.

National Institute of Standards and Technology. (2023). *Cybersecurity framework: Version 2.0 (Draft).* U.S. Department of Commerce.

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

Nguyen, T. M., & Watanabe, T. (2022). The impact of artificial intelligence on business performance: A review of current research and future perspectives. *Journal of Business Research,* 142, 11–24.

Nunnally, J. C., & Bernstein, I. H. (2019). *Psychometric theory* (3rd ed.). McGraw-Hill.

Riyadh, K., & Abuhassna, H. (2023). The role of AI literacy and cybersecurity awareness in promoting safe digital behavior among university students. *Computers & Education: Artificial Intelligence,* 5(2), 45–58.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In *Social psychophysiology* (pp. 153–176). Guilford Press.

Schrank, J. (2025). *The impact of artificial intelligence on behavioral intentions to use mobile banking in the post-COVID-19 era*. Frontiers in Artificial Intelligence.

Sekaran, U., & Bougie, R. (2020). *Research methods for business: A skill-building approach* (8th ed.). Wiley.

UNESCO. (2022). *AI and education: Guidance for policymakers*. United Nations Educational, Scientific and Cultural Organization.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly,* 27(3), 425–478.

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

Zhang, L., & Li, X. (2023). Artificial intelligence literacy and cybersecurity: Exploring the intersection of knowledge, skills, and ethics. *Computers & Security,* 127, 103099.

Zuo, Z., & Zhang, Y. (2025). *From perception to practice: Artificial intelligence as a cybersecurity behavioral intention mediator.* MDPI.