CYBER SECURITY AWARENESS OF IT UNDERGRADUATES IN AN EASTERN REGION UNIVERSITY

Received Date: 2025, April 24
Revised Date: 2025, May 26
Accepted Date: 2025, June 20

Woraphon Ruckjhem*
Chiraphorn Chomyim*

ABSTRACT

This research aimed to 1) investigate the level of cyber security threat awareness among undergraduate students in the Faculty of Information Technology at a higher education institution in the Eastern region university, and 2) compare the levels of cyber security threat awareness among these students based on personal demographic factors. This quantitative study employed a survey research design. The sample consisted of 147 undergraduate students selected through simple random sampling from a total population of 218 students. The research instrument was a five-point Likert scale questionnaire. Data were analyzed using frequency, percentage, mean, standard deviation, *t*-test, and one-way analysis of variance (One-way ANOVA).

The findings revealed that the students had a high level of awareness regarding cyber security threats ($\bar{X}$=3.71, *SD*=0.94). When analyzed by personal demographic factors, it was found that gender, age, and year of study did not significantly affect the level of cyber security threat awareness. However, students with different levels of experience in studying Cyber Security courses and participation in Cyber Security training or seminars exhibited statistically significant differences in their awareness of cyber security threats at the .05 level of statistical significance.

Keywords: Awareness, Cyber Threats.

* Faculty of Information Technology, Sripatum University at Chonburi
Corresponding author e-Mail: woraphon.ru@chonburi.spu.ac.th, chiraphorn.ch@chonburi.spu.ac.th

ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของนักศึกษาระดับปริญญาตรี คณะเทคโนโลยีสารสนเทศ สถาบันอุดมศึกษาแห่งหนึ่งในภาคตะวันออก

วันที่ได้รับต้นฉบับบทความ: 24 เมษายน 2568
วันที่แก้ไขปรับปรุงบทความ: 26 พฤษภาคม 2568
วันที่ตอบรับตีพิมพ์บทความ: 20 มิถุนายน 2568

วรพล รักเจียม*
จิราภรณ์ ชมยิ้ม*

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์ 1) เพื่อศึกษาระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของนักศึกษาระดับปริญญาตรี คณะเทคโนโลยีสารสนเทศ สถาบันอุดมศึกษาแห่งหนึ่งในภาคตะวันออก 2) เพื่อเปรียบเทียบระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของนักศึกษาคณะเทคโนโลยีสารสนเทศ สถาบันอุดมศึกษาแห่งหนึ่งในภาคตะวันออก จำแนกตามปัจจัยส่วนบุคคล เป็นการวิจัยเชิงปริมาณ มีรูปแบบการวิจัยเชิงสำรวจ กลุ่มตัวอย่างที่ใช้ในการวิจัย ได้แก่ นักศึกษาระดับปริญญาตรี คณะเทคโนโลยีสารสนเทศ จำนวน 147 คน จากประชากรทั้งหมด 218 คน โดยใช้วิธีการสุ่มตัวอย่างแบบอย่างง่าย เครื่องมือในการวิจัยเป็นแบบสอบถามแบบตราส่วนประมาณค่า 5 ระดับ วิเคราะห์ข้อมูลโดยใช้ค่าความถี่ ร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน การทดสอบค่าที (*t*-test) และการวิเคราะห์ความแปรปรวนทางเดียว (One-Way ANOVA)

ผลการศึกษาพบว่า นักศึกษามีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์อยู่ในระดับมาก ($\bar{X}$=3.71, *SD*=0.94) โดยจำแนกตามปัจจัยส่วนบุคคลพบว่า นักศึกษาระดับปริญญาตรี คณะเทคโนโลยีสารสนเทศแห่งนี้ที่มีเพศ อายุ ชั้นปีที่กำลังศึกษาที่แตกต่างกันมีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่ไม่แตกต่างกัน ในส่วนประสบการณ์การเรียนวิชา Cyber Security ที่ต่างกัน และประสบการณ์การฝึกอบรมหรือสัมมนาด้าน Cyber Security ที่ต่างกัน มีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .05

คำสำคัญ: ความตระหนักรู้ ภัยคุกคามทางไซเบอร์

* คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี
Corresponding author e-Mail: woraphon.ru@chonburi.spu.ac.th, chiraphorn.ch@chonburi.spu.ac.th

บทนำ

ในยุคที่เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในทุกมิติของชีวิตมนุษย์ ตั้งแต่การศึกษา การทำงาน ไปจนถึงกิจกรรมในชีวิตประจำวัน โลกไซเบอร์ (Cyberspace) ได้กลายเป็นพื้นที่สำคัญที่ผู้คนพึ่งพิงเพื่อเข้าถึงข้อมูลสารสนเทศ การสื่อสาร การดำเนินกิจกรรมทางเศรษฐกิจและสังคมอย่างกว้างขวาง อย่างไรก็ตาม การใช้งานระบบสารสนเทศอย่างต่อเนื่องแม้จะช่วยเพิ่มประสิทธิภาพในการดำเนินชีวิต แต่ในขณะเดียวกันก็ก่อให้เกิดความเสี่ยงต่อภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่มีความรุนแรงและซับซ้อนมากขึ้นอย่างต่อเนื่อง รายงานจาก European Union Agency for Cybersecurity (ENISA) (Online, 2023) ระบุว่าแนวโน้มการโจมตีทางไซเบอร์ทั่วโลกยังคงเพิ่มขึ้นอย่างต่อเนื่อง มีการพัฒนาเทคนิคที่หลากหลายและยากต่อการตรวจจับ โดยภัยคุกคามที่พบมาก ได้แก่ มัลแวร์เรียกค่าไถ่ (Ransomware) การโจมตีด้วยอีเมลหลอกลวง (Phishing) วิศวกรรมสังคม (Social Engineering) และการโจมตีผ่านอุปกรณ์ IoT รวมถึงปัญหาจากปัญญาประดิษฐ์ที่ถูกนำไปใช้เพื่อเจาะระบบอัตโนมัติ หรือสร้างเนื้อหาหลอกลวงขั้นสูง เช่น Deepfake และ Voice Spoofing (European Union Agency for Cybersecurity (ENISA) (Online, 2023); National Institute of Standards and Technology (NIST), Online, 2022) ขณะที่รายงานของ Cyber Security Ventures คาดการณ์ว่า ความเสียหายจากอาชญากรรมไซเบอร์ทั่วโลกจะสูงถึง 10.5 ล้านล้านดอลลาร์สหรัฐภายในปี 2025 ซึ่งสะท้อนถึงผลกระทบอันร้ายแรงต่อทั้งองค์กรและบุคคลที่ต้องปรับตัว (Morgan, Online, 2020)

ในบริบทของประเทศไทย ภัยคุกคามทางไซเบอร์ได้ทวีความรุนแรงขึ้นอย่างเห็นได้ชัด โดย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ออนไลน์, 2568) รายงานว่า ปี 2567 พบการโจมตีที่มีเป้าหมายต่อภาครัฐ ภาคเอกชน และสถาบันการศึกษาจำนวนมาก โดยเฉพาะการขโมยข้อมูลส่วนบุคคล การโจมตีผ่านแอปปลอม และการแฮ็กระบบด้วยช่องโหว่ของผู้ใช้ปลายทาง (End-user Vulnerabilities) ซึ่งพบมากในกลุ่มนักศึกษาและเยาวชน โดยเฉพาะอย่างยิ่งกลุ่มนักศึกษาในระดับอุดมศึกษาถือเป็นกลุ่มเป้าหมายที่มีความเสี่ยงสูงเนื่องจากเป็นผู้ที่เกิดในยุคดิจิทัล (Digital Natives) ที่ใช้งานเทคโนโลยีในชีวิตประจำวัน แต่กลับพบว่าหลายคนยังขาดความรู้พื้นฐานหรือทักษะด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Literacy) อย่างเพียงพอ งานวิจัยของ Alqahtani (2022, pp. 1-21) ระบุว่า นักศึกษาจำนวนมากมีทัศนคติด้านความมั่นคงปลอดภัยไซเบอร์เป็นตัวกลางในความสัมพันธ์ระหว่างความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ความปลอดภัยของรหัสผ่าน และการรับรู้ทักษะของตนเองกับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ การศึกษานี้ชี้ให้เห็นว่าจำเป็นต้องมีการทุ่มเทมากขึ้นในการให้ข้อมูลแก่นักศึกษาเกี่ยวกับความปลอดภัยทางไซเบอร์ และการใช้อินเทอร์เน็ตอย่างมีจริยธรรม นอกจากนี้ งานวิจัยนี้ยังมีจุดประสงค์หลักเพื่อเน้นย้ำถึงความจำเป็นในการสร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ในกลุ่มนักศึกษา Bottyán (2023, pp. 1-11) จากการศึกษาพบว่า ผู้มีส่วนร่วมในกระบวนการเรียนการสอนและสถาบันการศึกษา มีความเสี่ยงต่อภัยคุกคามทางไซเบอร์เพิ่มมากขึ้น มาตรการป้องกันที่เหมาะสมจึงมีความจำเป็นอย่างยิ่งที่ต้องสร้างความตระหนักรู้ ซึ่งรวมถึงการปกป้องข้อมูลส่วนบุคคลของนักศึกษา ครู และบุคลากรทางการศึกษา และการส่งเสริมการพัฒนาทักษะดิจิทัลที่มีความรับผิดชอบและ

คำนึงถึงความปลอดภัยในกลุ่มนักศึกษา ความตระหนักรู้ด้านความปลอดภัยของข้อมูล แต่ยังพบช่องว่างในการประเมินผลสัมฤทธิ์ของการเรียนรู้ โดยเฉพาะในด้าน “ความตระหนักรู้” (Awareness) ซึ่งเป็นพื้นฐานสำคัญในการส่งเสริมพฤติกรรมความปลอดภัยในระยะยาว งานวิจัยของ Bloom, Engelhart, Furst, Hill & Krathwohl (1956, p. 7) ในทฤษฎีแนวคิดด้าน Affective Domain ชี้ว่า ความตระหนักรู้ถือเป็นระดับต้นของการเรียนรู้ที่นำไปสู่พฤติกรรมเชิงบวก หากไม่มีการกระตุ้นหรือส่งเสริมอย่างเหมาะสม ผู้เรียนจะไม่สามารถพัฒนาไปสู่พฤติกรรมการป้องกันภัยเชิงปฏิบัติได้อย่างยั่งยืน

ดังนั้นในการศึกษาครั้งนี้ผู้วิจัยจึงมีความสนใจในประเด็นเรื่อง ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของนักศึกษาคณะเทคโนโลยีสารสนเทศในระดับปริญญาตรี โดยมุ่งสำรวจระดับความตระหนักรู้ของนักศึกษาในบริบทปัจจุบัน และใช้เป็นแนวทางในการออกแบบกิจกรรมการเรียนรู้หรือแนวทางการส่งเสริมด้านความปลอดภัยไซเบอร์ให้เหมาะสมกับบริบทของผู้เรียนในระดับอุดมศึกษา

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาระดับความตระหนักรู้ถึงภัยคุกคามทางด้านไซเบอร์ของนักศึกษาคณะเทคโนโลยีสารสนเทศ สถาบันอุดมศึกษาแห่งหนึ่งในภาคตะวันออก

2. เพื่อเปรียบเทียบระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของนักศึกษาคณะเทคโนโลยีสารสนเทศ สถาบันอุดมศึกษาแห่งหนึ่งในภาคตะวันออก จำแนกตามปัจจัยส่วนบุคคล

กรอบแนวคิดและวรรณกรรมที่เกี่ยวข้อง

จากการศึกษาแนวคิดและทฤษฎี รวมถึงงานวิจัยที่เกี่ยวข้องของ Protection Motivation Theory (PMT) ของ Rogers (1975, pp. 93-114) ที่อธิบายว่า พฤติกรรมการป้องกันของบุคคลขึ้นอยู่กับการรับรู้ความเสี่ยง (Threat Appraisal) และการประเมินความสามารถในการรับมือ (Coping Appraisal) โดยความตระหนักรู้เป็นส่วนสำคัญของการรับรู้ความเสี่ยงดังกล่าว และการเลือกภัยคุกคามทางไซเบอร์ 5 ด้าน ในการศึกษาครั้งนี้ ได้ใช้หลักการจำแนกตาม NIST Cybersecurity Framework และ ENISA Threat Landscape ซึ่งจัดประเภทภัยคุกคามตามลักษณะการโจมตี และกลุ่มเป้าหมาย ดังนี้

1. วิศวกรรมสังคม (Social Engineering) เนื่องจากเป็นภัยคุกคามที่เน้นการโจมตีผ่านจิตวิทยาและพฤติกรรมของมนุษย์ ซึ่งพบว่า มีแนวโน้มเพิ่มขึ้นในหมู่นักศึกษา และถือเป็น Initial Attack Vector ที่นำไปสู่การโจมตีรูปแบบอื่น

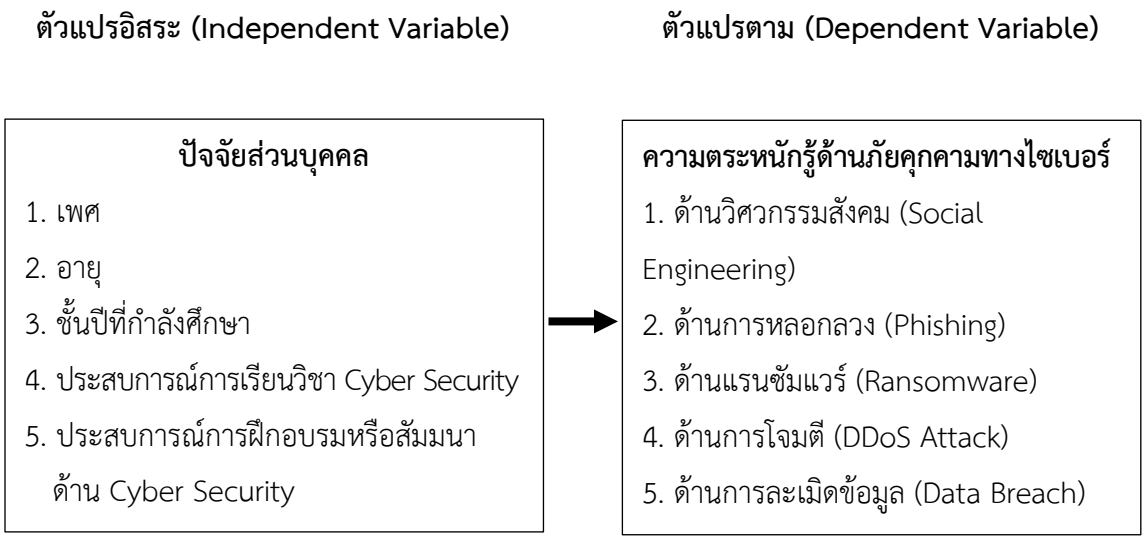
2. การหลอกลวง (Phishing) เป็นภัยคุกคามที่พบบ่อยที่สุดในรายงาน CISA (2023) และ Anti-Phishing Working Group โดยเฉพาะในกลุ่มผู้ใช้อินเทอร์เน็ตวัยรุ่น และนักศึกษา มีลักษณะการโจมตีที่เฉพาะ เจาะจง และใช้เทคนิคทางจิตวิทยา

3. แรนซัมแวร์ (Ransomware) จัดอยู่ในกลุ่ม High-Impact Threats ตามการจำแนกของ NIST SP 800-30 เนื่องจากสร้างความเสียหายทางการเงินและข้อมูลอย่างรุนแรง โดยเฉพาะในสถาบันการศึกษา

4. การโจมตีแบบปฏิเสธการให้บริการ (DDoS Attack) เป็นภัยคุกคามระดับโครงสร้างพื้นฐานที่จำแนกตาม Infrastructure-Level Threats ใน ENISA Threat Taxonomy ซึ่งส่งผลกระทบต่อการให้บริการขององค์กร และเป็นภัยคุกคามที่เพิ่มขึ้นในสถาบันการศึกษา

5. การละเมิดข้อมูล (Data Breach) จัดอยู่ในกลุ่ม Privacy and Data Protection Threats ตาม GDPR และ PDPA ซึ่งมีความสำคัญสูงในยุคข้อมูลส่วนบุคคล และเป็นผลลัพธ์ที่ตามมาจากการโจมตีรูปแบบต่าง ๆ

ซึ่งกรอบแนวคิดนี้สอดคล้องกับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร ที่อธิบายว่า บุคลากรมีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่แตกต่างกันอย่างมีนัยสำคัญทางสถิติ ซึ่งส่งผลต่อพฤติกรรมการป้องกันตนเอง (เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี, 2565, หน้า 1-17) ผู้ศึกษาได้กำหนดกรอบแนวความคิดไว้ดังภาพที่ 1



ภาพที่ 1 กรอบแนวคิดในการวิจัย

วิธีดำเนินการวิจัย

ประชากรและกลุ่มตัวอย่าง การศึกษาครั้งนี้ผู้วิจัยใช้รูปแบบการวิจัยแบบเชิงสำรวจ (Survey Research) ซึ่งเป็นการวิจัยเชิงปริมาณ (Quantitative Research) โดยที่ผู้วิจัยเก็บข้อมูลเชิงปริมาณโดยใช้แบบสอบถามความคิดเห็น (Questionnaires) เป็นนักศึกษาชั้นปีที่ 1 ถึง ชั้นปีที่ 4 ของคณะเทคโนโลยีสารสนเทศ ซึ่งมีนักศึกษาทั้งหมด 218 คน โดยใช้สูตรการหาขนาดกลุ่มตัวอย่างของยามาเน่ (Yamane, 1973, p. 725) โดยกำหนดระดับความเชื่อมั่นที่ ร้อยละ 95 และความคลาดเคลื่อนที่ ร้อยละ 5 จากสูตรคำนวณได้จำนวนกลุ่มตัวอย่างในการเก็บข้อมูล 141 คน มีผู้ตอบแบบสอบถาม จำนวน 147 คน โดยใช้วิธีการสุ่มตัวอย่างแบบอย่างง่าย เครื่องมือที่ใช้ในการวิจัย เป็นแบบสอบถามที่ผู้วิจัยได้ค้นคว้าจากแนวคิดทฤษฎี และงานวิจัย

ที่เกี่ยวข้องเพื่อนำมาเป็นข้อมูลในการสร้างแบบสอบถามแบบมาตราส่วน Likert 5 ระดับ แบ่งแบบสอบถามที่ใช้ในการวิจัยเป็น 5 ส่วน ได้แก่ ส่วนที่ 1 แบบสอบถามเกี่ยวกับข้อมูลทั่วไปที่เป็นสถานภาพของกลุ่มตัวอย่าง ได้แก่ เพศ อายุ ชั้นปีที่กำลังศึกษา ประสบการณ์การเรียนวิชา Cyber Security และการฝึกอบรมหรือสัมมนาด้าน Cyber Security มีลักษณะคำถามแบบตรวจสอบรายการ (Check List) ส่วนที่ 2 แบบสอบถามเกี่ยวกับความรู้พื้นฐานด้าน Cyber Security ส่วนที่ 3 แบบสอบถามเกี่ยวกับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Cyber Security) ส่วนที่ 4 แบบสอบถามความต้องการในการฝึกอบรม การเรียนรู้เพื่อสร้างความตระหนักรู้ภัยคุกคามทางไซเบอร์ โดยข้อคำถามในส่วนที่ 2 ส่วนที่ 3 และส่วนที่ 4 ใช้มาตราส่วนประมาณค่า 5 ระดับ (Rating Scale) ดังนี้กำหนดให้ระดับ 5 หมายถึง มากที่สุด, ระดับ 4 หมายถึง มาก, ระดับ 3 หมายถึง ปานกลาง, ระดับ 2 หมายถึง น้อย และระดับ 1 หมายถึง น้อยที่สุด และส่วนที่ 5 เป็นแบบสอบถามเพื่อรับฟังข้อเสนอแนะเพิ่มเติม ที่เป็นลักษณะคำถามแบบปลายเปิด แบบสอบถามที่สร้างขึ้นได้ผ่านการตรวจสอบความเที่ยงตรงจากผู้เชี่ยวชาญ 3 ท่าน โดยหาค่าความสอดคล้อง (Item Objective Congruence: IOC) มีค่าความเชื่อมั่นเท่ากับ .89 ถือว่าผ่านเกณฑ์ (IOC>0.50) การวิเคราะห์ข้อมูลใช้โปรแกรมสำเร็จรูปทางสถิติ โดยใช้สถิติเชิงพรรณนา ได้แก่ ความถี่ ร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน และใช้สถิติเชิงอนุมาน ได้แก่ Independent Samples *t*-test และ One-way ANOVA เพื่อเปรียบเทียบระดับความตระหนักรู้จำแนกตามปัจจัยส่วนบุคคล ที่ระดับนัยสำคัญ .05

การเก็บรวมข้อมูล ผู้วิจัยดำเนินการเก็บข้อมูลด้วยแบบสอบถามแบบออนไลน์ ด้วยการส่งลิงก์แบบสอบถาม ให้กลุ่มตัวอย่างตอบแบบสอบถาม และทำการสังเคราะห์และวิเคราะห์ทางสถิติ โดยการเก็บข้อมูลผู้วิจัยได้ชี้แจงวัตถุประสงค์ของการวิจัยและขอความยินยอมจากผู้ตอบแบบสอบถามก่อนการเก็บข้อมูล

การวิเคราะห์ข้อมูล ในการศึกษาครั้งนี้ใช้สถิติในการวิเคราะห์ข้อมูล คือ สถิติเชิงพรรณนา ได้แก่ ค่าความถี่ (Frequency) ค่าร้อยละ (Percentage) ค่าเฉลี่ย (Mean) และค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) โดยใช้เกณฑ์การแปลผลค่าเฉลี่ย (บุญชม ศรีสะอาด, 2553, หน้า 18) ดังนี้

ค่าเฉลี่ย	4.51-5.00	หมายถึง	มากที่สุด
ค่าเฉลี่ย	3.51-4.50	หมายถึง	มาก
ค่าเฉลี่ย	2.51-3.50	หมายถึง	ปานกลาง
ค่าเฉลี่ย	1.51-2.50	หมายถึง	น้อย
ค่าเฉลี่ย	1.00-1.50	หมายถึง	น้อยที่สุด

ผลการวิจัย

ผลการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถามพบว่า กลุ่มตัวอย่างเป็นเพศชาย จำนวน 108 คน คิดเป็น ร้อยละ 73.50 และเป็นเพศหญิง จำนวน 39 คน คิดเป็น ร้อยละ 26.50 กลุ่มตัวอย่างส่วนใหญ่มีอายุ 21-23 ปี จำนวน 74 คน คิดเป็น ร้อยละ 50.30 อายุ 24 ปีขึ้นไป จำนวน 40 คน คิดเป็น ร้อยละ 27.20

อายุ 18-20 ปี จำนวน 32 คน คิดเป็น ร้อยละ 21.80 และอายุน้อยกว่า 18 ปี จำนวน 1 คน คิดเป็น ร้อยละ 0.70 ตามลำดับ พบว่า กลุ่มตัวอย่างส่วนใหญ่กำลังศึกษาอยู่ชั้นปีที่ 3 จำนวน 54 คน คิดเป็น ร้อยละ 36.73 รองลงมาได้แก่ ชั้นปีที่ 4 จำนวน 46 คน คิดเป็น ร้อยละ 31.29 ชั้นปีที่ 2 จำนวน 29 คน คิดเป็น ร้อยละ 19.73 ชั้นปีที่ 1 จำนวน 18 คน คิดเป็น ร้อยละ 12.25 ตามลำดับ ด้านประสบการณ์การเรียนวิชา Cyber Security พบว่า กลุ่มตัวอย่างส่วนใหญ่เคยเรียนวิชา Cyber Security จำนวน 134 คน คิดเป็น ร้อยละ 91.20 ไม่เคยเรียนวิชา Cyber Security จำนวน 13 คน คิดเป็น ร้อยละ 8.80 ตามลำดับ สำหรับการฝึกอบรมหรือสัมมนาด้าน Cyber Security พบว่า กลุ่มตัวอย่างส่วนใหญ่เคยเข้าร่วมฝึกอบรม หรือสัมมนาด้าน Cyber Security จำนวน 112 คน คิดเป็นร้อยละ 76.19 ไม่เคยเข้าร่วมฝึกอบรมหรือสัมมนาด้าน Cyber Security จำนวน 35 คน คิดเป็น ร้อยละ 23.81 ตามลำดับ

ตารางที่ 1 ข้อมูลพื้นฐานของกลุ่มตัวอย่าง

ข้อมูลส่วนบุคคล		**จำนวน**	**ร้อยละ**
เพศ	ชาย	108	73.50
	หญิง	39	26.50
	รวม	147	100.00
อายุ	อายุน้อยกว่า 18 ปี	1	0.70
	18-20 ปี	32	21.80
	21-23 ปี	74	50.30
	24 ปี ขึ้นไป	40	27.20
	รวม	147	100.00
ชั้นปี	ชั้นปีที่ 1	18	12.25
	ชั้นปีที่ 2	29	19.73
	ชั้นปีที่ 3	54	36.73
	ชั้นปีที่ 4	46	31.29
	รวม	147	100.00
เรียนวิชา Cyber Security	เคยเรียน	134	91.20
	ไม่เคยเรียน	13	8.80
	รวม	147	100.00
ฝึกอบรมหรือสัมมนา	เคยฝึกอบรม	112	76.19
ด้าน Cyber Security	ไม่เคยฝึกอบรม	35	23.81
	รวม	147	100.00

จากตารางที่ 1 พบว่า กลุ่มตัวอย่างส่วนใหญ่เป็นเพศชาย ร้อยละ 73.50 และมีช่วงอายุระหว่าง 21-23 ปี มากที่สุด ร้อยละ 50.30 ส่วนใหญ่อยู่ในชั้นปีที่ 3 ร้อยละ 36.73 และเคยเรียนวิชา Cyber Security ร้อยละ 91.20 รวมทั้งเคยเข้าร่วมการฝึกอบรมหรือสัมมนาด้าน Cyber Security ร้อยละ 76.19 แสดงให้เห็นว่า กลุ่มตัวอย่างมีพื้นฐานด้านความรู้หรือประสบการณ์ที่เกี่ยวข้องกับ Cyber Security ในระดับหนึ่ง ซึ่งอาจส่งผลต่อระดับความตระหนักรู้ต่อภัยไซเบอร์ได้อย่างมีนัยสำคัญ

ตารางที่ 2 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของระดับความตระหนักรู้ถึงภัยคุกคามทางด้านไซเบอร์ จำแนกตามรายด้าน

ด้านความตระหนักรู้	$\bar{x}$	*SD*	ระดับความตระหนักรู้
1. ความตระหนักรู้เกี่ยวกับวิศวกรรมสังคม (Social Engineering Awareness)	3.78	0.88	มาก
2. ความตระหนักรู้เกี่ยวกับการหลอกลวง (Phishing Awareness)	3.66	0.90	มาก
3. ความตระหนักรู้เกี่ยวกับแรนซัมแวร์ (Ransomware Awareness)	3.50	0.95	มาก
4. ความตระหนักรู้เกี่ยวกับการโจมตีแบบปฏิเสธการให้บริการแบบกระจาย (DDoS Attack Awareness)	3.37	0.98	ปานกลาง
5. ความตระหนักรู้เกี่ยวกับการละเมิดข้อมูล (Data Breach Awareness)	3.08	0.99	ปานกลาง
รวม	**3.71**	**0.94**	**มาก**

จากตารางที่ 2 ผลการวิเคราะห์ระดับความตระหนักรู้ถึงภัยคุกคามทางด้านไซเบอร์ของนักศึกษาคณะเทคโนโลยีสารสนเทศ สถาบันอุดมศึกษาแห่งหนึ่งในภาคตะวันออกพบว่า ในภาพรวมกลุ่มตัวอย่างมีระดับความตระหนักรู้ด้านภัยคุกคามทางด้านไซเบอร์อยู่ในระดับมาก มีค่าเฉลี่ยเท่ากับ 3.71 และมีค่าส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.94 เมื่อพิจารณาเป็นรายด้านพบว่า ด้านความตระหนักรู้เกี่ยวกับวิศกรรมสังคม (Social Engineering Awareness) เป็นด้านที่มีค่าเฉลี่ยสูงสุดอยู่ในระดับ 3.78 มีค่าส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.88 รองลงมา คือ ด้านความตระหนักรู้เกี่ยวกับการหลอกลวง (Phishing Awareness) มีค่าเฉลี่ยเท่ากับ 3.66 มีค่าส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.90 ด้านความตระหนักรู้เกี่ยวกับแรนซัมแวร์ (Ransomware Awareness) มีค่าเฉลี่ย เท่ากับ 3.50 มีค่าส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.95 ด้านความตระหนักรู้เกี่ยวกับการโจมตีแบบปฏิเสธการให้บริการแบบกระจาย (DDoS Attack Awareness) มีค่าเฉลี่ยอยู่ในระดับปานกลาง เท่ากับ 3.37 มีค่าส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.98 และด้านความตระหนักรู้เกี่ยวกับการละเมิดข้อมูล (Data Breach Awareness) มีค่าเฉลี่ยอยู่ในระดับปานกลางเท่ากับ 3.08 มีค่าส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.99 ตามลำดับ

ตารางที่ 3 การเปรียบเทียบระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์จำแนกตามปัจจัยส่วนบุคคล

ข้อมูลส่วนบุคคล	ความตระหนักรู้			ผลการทดสอบ
	t	*F*	*P*	
เพศ		0.27	.08	ไม่มีผล
อายุ		0.189	.08	ไม่มีผล
ชั้นปี		0.43	.08	ไม่มีผล
เรียนวิชา Cyber Security		0.02	.00	มีผล
ฝึกอบรม หรือสัมมนา ด้าน Cyber Security		0.03	.00	มีผล

*$p<.05$

จากตารางที่ 3 พบว่า ปัจจัยส่วนบุคคลที่มีผลต่อระดับความตระหนักรู้ ได้แก่ การเคยเรียนวิชา Cyber Security และการเคยผ่านการอบรมหรือสัมมนา มีความแตกต่างอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 ส่วนปัจจัยเพศ อายุ และชั้นปีการศึกษาไม่มีความแตกต่างอย่างมีนัยสำคัญ

อภิปรายผล

จากผลการวิจัยในประเด็นของระดับความตระหนักรู้ถึงภัยคุกคามทางด้านไซเบอร์ของนักศึกษาคณะเทคโนโลยีสารสนเทศ สถาบันอุดมศึกษาแห่งหนึ่งในภาคตะวันออกพบว่า กลุ่มตัวอย่างมีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในภาพรวมอยู่ในระดับมาก มีค่าเฉลี่ย ($\bar{X}$) เท่ากับ 3.71 และค่าเบี่ยงเบนมาตรฐาน (*SD*) เท่ากับ 0.94 ซึ่งสะท้อนถึงความตื่นตัวของนักศึกษาในการรับรู้และระวังภัยไซเบอร์ที่อาจเกิดขึ้นในการใช้งานเทคโนโลยีสารสนเทศ โดยเฉพาะในด้านวิศวกรรมสังคม (Social Engineering) และการหลอกลวงผ่านอีเมล (Phishing) ซึ่งเป็นภัยที่เกี่ยวข้องกับพฤติกรรมของผู้ใช้โดยตรง และมักถูกใช้เป็นช่องทางเริ่มต้นในการโจมตี (Initial Attack Vector) ระดับความตระหนักรู้สูงในด้านดังกล่าวมีความสอดคล้องกับผลการศึกษาของ Aljohni, Elfadil, Jarajreh & Gasmelsied (2021, pp. 276-281) ซึ่งพบว่าผู้ที่เคยผ่านการฝึกอบรมหรือการเรียนรู้ด้านความปลอดภัยทางไซเบอร์มีแนวโน้มที่จะสามารถระบุพฤติกรรมเสี่ยงและป้องกันตนเองได้ดีกว่าผู้ที่ไม่เคยผ่านการฝึกอบรมหรือไม่ได้เรียนรู้ด้านความปลอดภัยทางไซเบอร์ นอกจากนี้งานวิจัยของ เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี (2565, หน้า 1-17) พบว่าผู้ที่เคยผ่านการเรียนรู้หรือการฝึกอบรมด้าน Cyber Security มักมีระดับความตระหนักรู้ต่อภัยใกล้ตัวสูงและสามารถระบุพฤติกรรมเสี่ยงได้ดี

เมื่อพิจารณาเป็นรายด้านพบว่า ด้านความตระหนักรู้เกี่ยวกับวิศวกรรมสังคม (Social Engineering Awareness) มีค่าเฉลี่ยสูงสุด ($\bar{X}$=3.78, *SD*=0.88) ซึ่งอาจเป็นผลจากกลุ่มตัวอย่างส่วนใหญ่ ร้อยละ 91.20

เคยเรียนวิชา Cyber Security และ ร้อยละ 76.19 เคยเข้าร่วมฝึกอบรมหรือสัมมนาด้าน Cyber Security มาก่อน ทั้งนี้สอดคล้องกับผลการวิจัยของ Goliath, Tsibolane & Snyman (Online, 2024) พบว่า ความตระหนักรู้ด้านไซเบอร์เพิ่มขึ้นตามอายุของผู้เรียน บทความเสนอให้สถาบันอุดมศึกษาพัฒนาโปรแกรมการศึกษาความมั่นคงปลอดภัยแบบครอบคลุมโดยเน้นการแทรกแซงในช่วงต้นของการศึกษาระดับปริญญาตรี และส่งเสริมการเรียนรู้เชิงปฏิบัติ รวมถึงการขยายการอบรมไปยังบุคลากร เพื่อเสริมสร้างวัฒนธรรมความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ในระดับสถาบันอย่างยั่งยืน ประสบการณ์การเรียนรู้และการใช้งานส่งผลอย่างชัดเจนต่อระดับความตระหนักรู้ของผู้เรียน ในทางตรงกันข้ามด้านที่นักศึกษามีระดับความตระหนักรู้น้อยที่สุด ได้แก่ ความตระหนักรู้เกี่ยวกับการละเมิดข้อมูล (Data Breach) ผลดังกล่าวสะท้อนถึงความเข้าใจเชิงลึกที่เกี่ยวข้องกับผลกระทบของการรั่วไหลของข้อมูลส่วนบุคคล การจัดการสิทธิ์การเข้าถึงข้อมูลส่วนบุคคล และการปฏิบัติตามข้อกฎหมาย เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ผลการศึกษานี้สอดคล้องกับงานวิจัยของ Albediwi & Sadaf (2023, pp. 35-53) ซึ่งพบว่า ความก้าวหน้าทางเทคโนโลยีอย่างรวดเร็วได้พัฒนาคุณภาพชีวิตของผู้คน แต่ก็เพิ่มความเสี่ยงที่มาพร้อมกับการใช้อินเทอร์เน็ต รวมถึงอาชญากรรมไซเบอร์ด้วย ซาอุดีอาระเบียเป็นประเทศที่มีเศรษฐกิจเฟื่องฟู และได้กลายเป็นหนึ่งในเป้าหมายหลักของการโจมตีทางไซเบอร์ ผลการโจมตีทางไซเบอร์จำนวนมหาศาลที่พุ่งเป้าไปที่ซาอุดีอาระเบียนั้น เป็นผลมาจากการขาดความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในซาอุดีอาระเบีย วัตถุประสงค์ของการศึกษานี้คือ การนำเสนอวิธีการเพิ่มความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ให้ชาวซาอุดีอาระเบีย ด้วยการสำรวจและประเมินความมั่นคงปลอดภัยทางไซเบอร์เพื่อประเมินความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ ผลการสำรวจชี้ให้เห็นถึงพฤติกรรมที่ประมาทเลินเล่อและการขาดความตระหนักรู้ เพื่อแก้ไขปัญหานี้ จึงเสนอกรอบการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งมุ่งเป้าไปที่ประชากรทุกระดับชั้นของซาอุดีอาระเบีย กรอบที่นำเสนอไม่ได้เน้นย้ำแต่โครงการฝึกอบรมในโรงเรียน มหาวิทยาลัย และองค์กรต่าง ๆ เท่านั้น แต่ยังครอบคลุมถึงปัญหาความตระหนักรู้ให้ประชาชนทั่วไปด้วย ทั้งนี้ภัยคุกคามประเภทดังกล่าวมีลักษณะเชิงโครงสร้างและมีความซับซ้อนทางเทคนิคสูง จึงควรมีการส่งเสริมให้มีการฝึกอบรมหรือการเรียนรู้ด้านความปลอดภัยทางไซเบอร์เพิ่มขึ้นงานวิจัยของ Bottyán (2023, pp. 1-11) พบว่า นักศึกษาส่วนใหญ่ตระหนักถึงความจำเป็นของการจัดการเรียนรู้ด้านความมั่นคงปลอดภัยสารสนเทศในระดับวิทยาลัย โดยเฉพาะในรูปแบบที่สามารถตอบสนองต่อบริบทและความต้องการเฉพาะของผู้เรียนในแต่ละสาขาวิชา อีกทั้งยังควรส่งเสริมความรู้เกี่ยวกับกฎหมายและข้อบังคับด้านไซเบอร์ให้กับนักศึกษาทุกคนอย่างครอบคลุม เพื่อเสริมสร้างพฤติกรรมการใช้งานเทคโนโลยีที่ปลอดภัยและยั่งยืนในอนาคต เมื่อเปรียบเทียบระดับความตระหนักรู้ตามปัจจัยส่วนบุคคลพบว่า นักศึกษาที่เคยเรียนวิชา Cybersecurity และเข้าร่วมอบรม มีระดับความตระหนักรู้สูงกว่ากลุ่มที่ไม่ได้เรียนวิชา Cybersecurity และไม่ได้เข้าร่วมการอบรม สอดคล้องกับข้อเสนอของ Aljohni, Elfadil, Jarajreh & Gasmelsied (2021, pp. 276-281) ที่เน้นความสำคัญของการฝึกอบรมแบบต่อเนื่องและการเรียนรู้ผ่านประสบการณ์จริง ในขณะที่ปัจจัยด้านเพศ อายุ และชั้นปี ไม่แสดงผลแตกต่างอย่างมีนัยสำคัญ ซึ่งสอดคล้องกับข้อเสนอของ Bottyán (2023, pp. 1-11) ที่ระบุว่า ระดับความตระหนักรู้ไม่ได้

ขึ้นอยู่กับคุณลักษณะประชากร แต่ขึ้นกับโอกาสในการเข้าถึงความรู้และรูปแบบการเรียนรู้ที่มีประสิทธิภาพ จากข้อมูลทั้งหมดข้างต้น ผลการวิจัยจึงเน้นย้ำถึงความจำเป็นในการออกแบบกิจกรรมการเรียนรู้ที่มีลักษณะเชิงปฏิบัติการ (Experiential Learning) และสามารถเข้าถึงผู้เรียนทุกกลุ่ม โดยไม่จำกัดตามคุณลักษณะเฉพาะบุคคล เช่น การใช้การเรียนรู้ผ่านสถานการณ์จำลอง (Simulation) การวิเคราะห์กรณีศึกษา (Case-based Learning) และการฝึกในรูปแบบ Red Team vs Blue Team ซึ่งมีประสิทธิภาพในการสร้างทั้งความเข้าใจเชิงลึก และทักษะการป้องกันเชิงพฤติกรรม

ข้อเสนอแนะ

ข้อเสนอแนะในการนำผลวิจัยไปใช้

1. สถาบันการศึกษาควรจัดกิจกรรมอบรมความรู้ด้าน Cyber Security อย่างต่อเนื่อง โดยเฉพาะอย่างยิ่งในหัวข้อที่นักศึกษามีความตระหนักรู้อยู่ในระดับปานกลาง ได้แก่ การละเมิดข้อมูล (Data Breach) และการโจมตีแบบปฏิเสธการให้บริการแบบกระจาย (DDoS Attack)

2. ควรใช้สื่อการเรียนรู้ที่หลากหลาย เช่น วิดีโอ อินโฟกราฟิก และกิจกรรมเวิร์กชอปเชิงปฏิบัติการ เป็นช่องทางในการส่งเสริมการเรียนรู้เพื่อให้นักศึกษาได้เข้าใจกระบวนการและแนวทางการป้องกันภัยคุกคามทางไซเบอร์อย่างเป็นรูปธรรม

3. ควรบูรณาการเนื้อหาด้านความปลอดภัยทางไซเบอร์เข้ากับรายวิชาอื่น ๆ ในหลักสูตร เพื่อให้นักศึกษาได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยทางไซเบอร์ในทุกมิติของการทำงานด้านเทคโนโลยีสารสนเทศ

ข้อเสนอแนะในการวิจัยครั้งต่อไป

1. การวิจัยครั้งนี้เป็นการศึกษาวิจัยเชิงปริมาณ ข้อมูลที่ได้จากการตอบแบบสอบถามจึงเป็นข้อมูลเบื้องต้น ดังนั้นเพื่อให้ได้ข้อมูลเชิงลึกเพื่อใช้ในการวิเคราะห์ปัจจัยต่าง ๆ อาจเพิ่มเติมด้วยวิธีวิจัยเชิงคุณภาพ (Qualitative Research) การสัมภาษณ์กลุ่ม (Focus Group Interview) หรือการสัมภาษณ์เจาะลึก (In-Depth Interview) เพื่อให้ทราบแนวคิดและระดับความรู้ของนักศึกษาในประเด็นความตระหนักรู้ถึงภัยคุกคามทางด้านไซเบอร์ให้ชัดเจนยิ่งขึ้น

2. ควรมีการศึกษาความสัมพันธ์ระหว่างความตระหนักรู้ถึงภัยคุกคามทางด้านไซเบอร์กับพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของนักศึกษา เพื่อให้เข้าใจว่าการมีความตระหนักรู้ในระดับสูงจะนำไปสู่การปฏิบัติตนอย่างปลอดภัยในโลกไซเบอร์ หรือไม่

บรรณานุกรม

บุญชม ศรีสะอาด. (2553). ***การวิจัยเบื้องต้น***. กรุงเทพฯ: สุวีริยาสาส์น.

เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี. (2565). ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร. ***วารสารวิชาการไทยวิจัยและการจัดการ***, ***3***(2), หน้า 1-17.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2568). ***ETDA โชว์สถิติร้องเรียนปัญหาออนไลน์ ปี 67 กว่า 3.5 หมื่นเคส ชี้ “หลอกซื้อขายออนไลน์ – เว็บผิดกฎหมาย” ยังครองแชมป์ เร่งกลไก ‘กฎหมาย DPS-สร้างเกราะคุ้มกัน” ดันคนไทย ทันภัยออนไลน์*** (ออนไลน์). เข้าถึงได้จาก: https://www.etda.or.th/th/pr-news/etda_stat_online_fraund.aspx [2568, 20 กุมภาพันธ์].

Albediwi, M. R., & Sadaf, K. (2023). A framework for cybersecurity awareness in saudi arabia. ***Journal of Engineering and Applied Sciences***, ***10***(1), pp. 35-53. https://doi.org/10.5455/jeas.2023050103

Aljohni, W., Elfadil, N., Jarajreh, M., & Gasmelsied, M. (2021). Cybersecurity awareness level: The case of Saudi Arabia University students. ***International Journal of Advanced Computer Science and Applications***, ***12***(3), pp. 276-281.

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. ***Applied Sciences***, ***12***(5), 2589 (pp. 1-22). https://doi.org/10.3390/app12052589

Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H. & Krathwohl, D. R. (1956). Taxonomy of educational objectives: The classification of educational goals. ***Handbook I: The cognitive domain***. New York, NY: David McKay Company.

Bottyán, L. (2023). Cybersecurity awareness among university students. ***Journal of Applied Technical and Educational Sciences***, ***13***(3), 363 (pp. 1-11). https://doi.org/10.24368/jates363

European Union Agency for Cybersecurity (ENISA). (2023). ***ENISA Threat Landscape 2023*** (Online). Available: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf [2025, May 20].

Goliath, S., Tsibolane, P., & Snyman, D. (2024). ***Exploring the cybersecurity-resilience gap: An analysis of student attitudes and behaviors in Higher Education*** (Online). Available: https://arxiv.org/pdf/2411.03219 [2025, May 20].

Morgan, S. (2020). ***Cybercrime to cost the world $10.5 trillion annually by 2025*** (Online). Available: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ [2025, May 20].

National Institute of Standards and Technology (NIST). (2022). ***AI Risk Management Framework: Second Draft*** (Online). Available: https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf [2025, May 20].

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

Yamane, T. (1973). ***Statistics: An introductory analysis*** (3rd ed.). New York, NY: Harper & Row.