

ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต ในมหาวิทยาลัยราชภัฏกาญจนบุรี

นิษฐา ไตรเดชา^{1*} และ เรวัตตะ กิจจานุรักษ์²

รับบทความ 8 พฤศจิกายน 2568 แก้ไขบทความ 28 พฤศจิกายน 2568 ตอรับบทความ 29 มิถุนายน 2569

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยด้านลักษณะทางประชากร ปัจจัยด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ และปัจจัยด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ ที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในมหาวิทยาลัยราชภัฏกาญจนบุรี เก็บรวบรวมข้อมูลโดยใช้แบบสอบถามออนไลน์กับกลุ่มตัวอย่าง จำนวน 365 คน แบ่งเป็นกลุ่มนักศึกษา จำนวน 329 คน และกลุ่มบุคลากรสายวิชาการและสายสนับสนุน จำนวน 36 คน วิเคราะห์ข้อมูลโดยใช้สถิติเชิงพรรณนา ได้แก่ ค่าความถี่ ค่าร้อยละ ค่าเฉลี่ย และค่าส่วนเบี่ยงเบนมาตรฐาน และสถิติเชิงอนุมาน ได้แก่ การวิเคราะห์ความแปรปรวนทางเดียว (One-way ANOVA) และการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ของเพียร์สัน (Pearson's Correlation Coefficient) ผลการวิจัย พบว่า 1) ปัจจัยด้านลักษณะทางประชากร ได้แก่ เพศ อายุ ประสบการณ์การใช้อินเทอร์เน็ต ประเภทบุคลากร ระดับการศึกษา และรายได้ ของกลุ่มตัวอย่างที่แตกต่างกัน มีความตระหนักถึงภัยคุกคามทางไซเบอร์ไม่แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 2) ปัจจัยด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ไม่มีความสัมพันธ์อย่างมีนัยสำคัญทางสถิติที่ระดับ .05 กับความตระหนักถึงภัยคุกคามทางไซเบอร์ 3) ปัจจัยด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ มีความสัมพันธ์เชิงบวกอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 กับความตระหนักถึงภัยคุกคามทางไซเบอร์ ผลการวิจัยชี้ให้เห็นว่า ความรู้เป็นปัจจัยสำคัญที่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในมหาวิทยาลัยราชภัฏกาญจนบุรี ซึ่งสามารถนำไปใช้เป็นแนวทางในการกำหนดนโยบาย พัฒนาการจัดกิจกรรมการอบรมให้ความรู้ เสริมสร้างความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเพิ่มการตระหนักรู้และลดโอกาสการตกเป็นเหยื่อของการโจมตีทางไซเบอร์ อันจะช่วยยกระดับความปลอดภัยในการใช้อินเทอร์เน็ตของบุคลากรและนักศึกษาได้อย่างยั่งยืน

คำสำคัญ: ภัยคุกคามทางไซเบอร์ ความตระหนัก ผู้ใช้อินเทอร์เน็ต

¹นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกาญจนบุรี

²นักวิจัยชำนาญการ สถาบันวิจัยและพัฒนา มหาวิทยาลัยราชภัฏกาญจนบุรี

*ผู้ประสานงานหลัก : nitta.trair@kru.ac.th

Factors Influencing Cyber Threat Awareness Among Internet Users at Kanchanaburi Rajabhat University

Nitta Traidecha^{1*} and Rewatta Kidjanuluk²

Received 8 November 2026.; Revised 28 November 2025; Accepted 29 June 2026

Abstract

This research aimed to study the demographic factors, experience-related factors concerning cyber threats, and knowledge-related factors about cyber threats that influence cyber threat awareness among Internet users at Kanchanaburi Rajabhat University. Data were collected through an online questionnaire from 365 respondents, consisting of 329 students and 36 academic and support staff members. The data were analyzed using descriptive statistics, including frequency, percentage, mean, and standard deviation, and inferential statistics, including One-way Analysis of Variance (ANOVA) and Pearson's Correlation Coefficient. The research findings revealed that: 1. Demographic factors such as gender, age, Internet usage experience, type of personnel, education level, and income showed no statistically significant differences in cyber threat awareness at the .05 level. 2. Experience-related factors concerning cyber threats had no statistically significant relationship with cyber threat awareness at the .05 level. 3. Knowledge-related factors about cyber threats had a positive and statistically significant correlation with cyber threat awareness at the .05 level. The results indicate that knowledge is a key factor influencing cyber threat awareness among Internet users at Kanchanaburi Rajabhat University. The findings can be applied to policy formulation, training program development, and awareness activities to enhance understanding of cybersecurity, increase awareness, and reduce the likelihood of falling victim to cyberattacks. Ultimately, this can help strengthen sustainable Internet safety among university staff and students.

Keywords: Cyber Threats; Awareness; Internet Users

¹Senior Professional Computer Technical Officer, Office of Academic Resources and Information Technology, Kanchanaburi Rajabhat University

²Senior Professional Research Officer, Research and Development Institute, Kanchanaburi Rajabhat University

*Corresponding Author : nitta.trai@kru.ac.th

บทนำ

ในยุคดิจิทัลปัจจุบัน เทคโนโลยีสารสนเทศและอินเทอร์เน็ตมีบทบาทสำคัญต่อการดำเนินชีวิตของผู้คนในทุกภาคส่วน ทั้งในด้านการศึกษา การสื่อสาร การบริหารจัดการ และการให้บริการสาธารณะ การเข้าถึงเทคโนโลยีที่ง่ายและแพร่หลายได้ส่งผลต่อการพัฒนาประเทศในระบบเศรษฐกิจดิจิทัล ควบคู่ไปกับการยกระดับกระบวนการดำเนินงานขององค์กรภาครัฐและเอกชนให้มีประสิทธิภาพสูงขึ้น ซึ่งส่วนใหญ่ถือเป็นเทคโนโลยีที่พัฒนาและถูกเพิ่มพูนการใช้งานมากขึ้นเพื่อให้ได้ประโยชน์อย่างใดอย่างหนึ่งต่อการสร้างสรรค์นวัตกรรมและการพัฒนาสังคมอย่างยั่งยืน แต่ในขณะเดียวกัน การขยายตัวของการพึ่งพาอินเทอร์เน็ตก็ส่งผลให้ภัยคุกคามทางไซเบอร์ (Cyber Threats) มีแนวโน้มเพิ่มความเสี่ยง มีความซับซ้อน และเพิ่มขึ้นอย่างต่อเนื่อง ไม่ว่าจะเป็น มัลแวร์ (Malware) การหลอกลวงฟิชชิ่ง (Phishing) การโจมตีแบบวิศวกรรมสังคม (Social Engineering) หรือการโจมตีแบบเรียกค่าไถ่ (Ransomware) ซึ่งล้วนสร้างความเสียหายต่อฐานข้อมูล โครงสร้างระบบ และทรัพยากรสารสนเทศขององค์กร หากผู้ใช้งานภายในองค์กรยังคงขาดความรู้ ความเข้าใจ หรือขาดความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) ก็จะกลายเป็นจุดที่เปราะบางที่สุดและตกเป็นเหยื่อของภัยไซเบอร์เหล่านี้ได้โดยง่าย

จากข้อมูลสถิติภัยคุกคามทางไซเบอร์ของประเทศไทยประจำปี พ.ศ. 2566 โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เผยให้เห็นสถานการณ์ความเปราะบางที่น่ากังวล โดยพบว่าหน่วยงานที่ตกเป็นเป้าหมายและถูกโจมตีทางไซเบอร์มากที่สุดเป็นอันดับ 1 คือ หน่วยงานด้านการศึกษา ซึ่งสถิติการถูกโจมตีสูงถึง 632 ครั้ง รองลงมาคือหน่วยงานภาครัฐอื่น ๆ จำนวน 145 ครั้ง และผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชนสัญชาติไทยจำนวน 148 ครั้ง ทั้งนี้ เมื่อพิจารณาถึงลักษณะรูปแบบของภัยคุกคามที่พบบ่อยที่สุดในรอบปี พบว่าอันดับ 1 เป็นภัยคุกคามในรูปแบบเว็บพแนจออนไลน์ จำนวน 515 ครั้ง อันดับ 2 คือเว็บไซต์ที่ถูกแฮกระบบ จำนวน 336 ครั้ง และอันดับ 3 คือเว็บไซต์ปลอมจำนวน 301 ครั้ง (สปริงนิวส์, 2567) ข้อมูลสถิติเชิงประจักษ์เหล่านี้สะท้อนให้เห็นอย่างเด่นชัดว่า สถาบันการศึกษากลายเป็นพื้นที่เป้าหมายหลักที่มีความเสี่ยงสูงสุดต่อการเผชิญหน้ากับภัยคุกคามทางไซเบอร์ ซึ่งความเสียหายมักมีจุดเริ่มต้นมาจากพฤติกรรมการใช้อินเทอร์เน็ตและความตระหนักรู้ของผู้ใช้งานภายในองค์กรเป็นสำคัญ

มหาวิทยาลัยราชภัฏกาญจนบุรีเป็นสถานศึกษาระดับอุดมศึกษาที่มีบุคลากรและนักศึกษาจำนวนมากใช้เทคโนโลยีสารสนเทศในการเรียนการสอน การทำงาน และการติดต่อสื่อสารอยู่เป็นประจำ ทำให้มีความเสี่ยงต่อการเผชิญภัยคุกคามทางไซเบอร์ได้เช่นเดียวกับองค์กรอื่น ๆ อย่างไรก็ตาม ปัจจุบันยังไม่มีข้อมูลเชิงประจักษ์ที่ชัดเจนเกี่ยวกับระดับความตระหนักรู้ของบุคลากรและนักศึกษาต่อภัยคุกคามทางไซเบอร์ รวมถึงปัจจัยที่อาจส่งผลต่อการรับรู้และพฤติกรรมการใช้งานอินเทอร์เน็ตอย่างปลอดภัย ซึ่งข้อมูลเหล่านี้จำเป็นอย่างยิ่งที่จะนำมาทดสอบความสอดคล้องหรือความแตกต่างเพื่อแก้ไขข้อบกพร่องเชิงพฤติกรรมสารสนเทศภายในพื้นที่สถาบัน

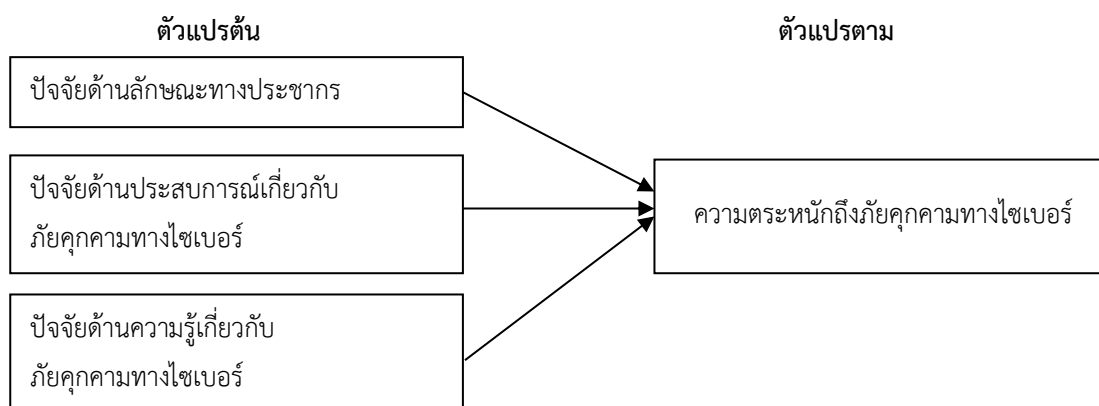
ดังนั้น การศึกษาวิจัยเรื่อง “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในมหาวิทยาลัยราชภัฏกาญจนบุรี” จึงมีความสำคัญอย่างยิ่งในเชิงวิชาการและการบริหารจัดการเทคโนโลยีสารสนเทศ เพื่อวิเคราะห์และระบุปัจจัยที่มีอิทธิพลต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ใช้งานภายในมหาวิทยาลัย ผลการศึกษาที่ได้จะไม่เพียงตอบโจทย์ความสอดคล้องเชิงสถิติเท่านั้น แต่สามารถนำไปใช้ประโยชน์ในเชิงปฏิบัติเพื่อเป็นแนวทางหลักในการวางแผนนโยบายด้านไอที การออกแบบสื่อประชาสัมพันธ์เตือนภัย การจัดหลักสูตรอบรมเสริมสร้างทักษะ หรือการพัฒนากิจกรรมส่งเสริมวัฒนธรรมความปลอดภัยไซเบอร์

(Cybersecurity Culture) อันจะช่วยยกระดับความปลอดภัยในการใช้อินเทอร์เน็ตของบุคลากรและนักศึกษาอย่างมีประสิทธิภาพและยั่งยืน

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาปัจจัยด้านลักษณะทางประชากร ปัจจัยด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ และปัจจัยด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ ของใช้อินเทอร์เน็ตในมหาวิทยาลัยราชภัฏกาญจนบุรี
2. เพื่อเปรียบเทียบความตระหนักถึงภัยคุกคามทางไซเบอร์ของใช้อินเทอร์เน็ตในมหาวิทยาลัยราชภัฏกาญจนบุรี จำแนกตามปัจจัยด้านลักษณะทางประชากร
3. เพื่อศึกษาความสัมพันธ์ระหว่างปัจจัยด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์กับความตระหนักถึงภัยคุกคามทางไซเบอร์ และปัจจัยด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์กับความตระหนักถึงภัยคุกคามทางไซเบอร์ของใช้อินเทอร์เน็ตในมหาวิทยาลัยราชภัฏกาญจนบุรี

กรอบแนวคิด



ภาพที่ 1 กรอบแนวคิดการวิจัย

วิธีดำเนินการวิจัย

1. ประชากรและกลุ่มตัวอย่าง

ประชากรในการวิจัย คือ ผู้ใช้งานอินเทอร์เน็ตภายในมหาวิทยาลัยราชภัฏกาญจนบุรี จำนวน 4,163 คน ประกอบด้วย

1.1 นักศึกษาที่ลงทะเบียนเรียนในภาคการศึกษาที่ 1 ปีการศึกษา 2567 จำนวน 3,749 คน (สำนักส่งเสริม วิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏกาญจนบุรี, 2567)

1.2 บุคลากรสายวิชาการและสายสนับสนุน จำนวน 414 คน (งานบริหารงานบุคคล มหาวิทยาลัยราชภัฏกาญจนบุรี, 2567)

กลุ่มตัวอย่างในการวิจัย ได้จากการกำหนดขนาดตัวอย่าง โดยใช้สูตรคำนวณของ Taro Yamane (1973) ที่ค่าความคลาดเคลื่อนของกลุ่มตัวอย่างร้อยละ 5 ได้จำนวนตัวอย่าง 365 คน สุ่มเลือกตัวอย่างด้วยวิธีการสุ่ม

แบบแบ่งชั้นภูมิ โดยแบ่งประชากรออกเป็น 2 กลุ่มได้แก่ กลุ่มนักศึกษา และกลุ่มบุคลากรสายวิชาการและสายสนับสนุน จากนั้นจึงสุ่มตัวอย่างตามสัดส่วนของประชากรจากแต่ละกลุ่มอย่างง่าย ได้จำนวนตัวอย่าง ดังนี้

- 1) กลุ่มนักศึกษา จำนวน 329 คน
- 2) กลุ่มบุคลากรสายวิชาการและสายสนับสนุน จำนวน 36 คน

2. เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัย คือ แบบสอบถาม ประกอบด้วย

ตอนที่ 1 ปัจจัยด้านลักษณะทางประชากร

ตอนที่ 2 ปัจจัยด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

ตอนที่ 3 ปัจจัยด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

แบบสอบถามทั้งฉบับผ่านการตรวจสอบความตรงเชิงเนื้อหาโดยผู้เชี่ยวชาญจำนวน 3 ท่าน ได้ค่าดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ของการวิจัย (Index of Item-Objective Congruence: IOC) โดยดำเนินการปรับปรุงคำถามตามข้อเสนอแนะของผู้เชี่ยวชาญ และเมื่อทำการคำนวณค่า IOC พบว่า มีค่าเฉลี่ยของคำถามรายข้อระหว่าง 0.67-1.00 แสดงให้เห็นว่าแบบสอบถามมีความเหมาะสมและมีความเที่ยงตรงในระดับดีมาก

3. การเก็บรวบรวมข้อมูล

การเก็บรวบรวมข้อมูลดำเนินการโดยเผยแพร่แบบสอบถามไปยังกลุ่มตัวอย่างผ่านช่องทางออนไลน์ของมหาวิทยาลัยราชภัฏกาญจนบุรี โดยใช้ Google Form เป็นเครื่องมือหลักในการตอบแบบสอบถาม ทั้งนี้ คณะผู้วิจัยได้ดำเนินการเก็บรวบรวมข้อมูลในช่วงระหว่างเดือนกันยายน - ธันวาคม พ.ศ. 2567 โดยได้ส่งลิงก์แบบสอบถามผ่านแอปพลิเคชัน Line ของหน่วยงานและกลุ่มนักศึกษา รวมถึงแจก QR Code เพื่อให้ผู้ตอบสามารถสแกนและเข้าถึงแบบสอบถามได้สะดวก เพื่อให้ได้ข้อมูลครบถ้วนตามจำนวนกลุ่มตัวอย่างที่กำหนด

4. การวิเคราะห์และสถิติที่ใช้ในการวิเคราะห์ข้อมูล

วิเคราะห์ข้อมูลตามระเบียบวิธีทางสถิติ โดยใช้โปรแกรมสำเร็จรูปทางสถิติ แบ่งการวิเคราะห์ออกเป็น 2 ประเภทดังนี้

4.1 สถิติเชิงพรรณนา ใช้อธิบายค่าของข้อมูลปัจจัยด้านลักษณะทางประชากร ด้านประสบการณ์ด้านความรู้ และด้านความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ ของผู้ใช้อินเทอร์เน็ตในมหาวิทยาลัยราชภัฏกาญจนบุรี ด้วยค่าแจกแจงความถี่ ค่าร้อยละ ค่าเฉลี่ย และค่าส่วนเบี่ยงเบนมาตรฐาน

4.2 สถิติเชิงอนุมาน ใช้สำหรับวิเคราะห์ข้อมูลเพื่อทดสอบสมมติฐานการวิจัย ได้แก่

1) การทดสอบความแตกต่างของลักษณะทางประชากรกับความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในมหาวิทยาลัยราชภัฏกาญจนบุรี โดยใช้การวิเคราะห์ความแปรปรวนทางเดียว (One-way ANOVA) ทั้งนี้หากพบความแตกต่างอย่างมีนัยสำคัญทางสถิติ จะทำการเปรียบเทียบค่าเฉลี่ยความแตกต่างเป็นรายคู่ ด้วยวิธีของ Scheffé

2) การทดสอบความสัมพันธ์ระหว่างตัวแปร ได้แก่ ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์กับความตระหนักถึงภัยคุกคามทางไซเบอร์ และ ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์กับความตระหนักถึงภัยคุกคามทางไซเบอร์ ของผู้ใช้อินเทอร์เน็ตในมหาวิทยาลัยราชภัฏกาญจนบุรี ด้วยการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ของเพียร์สัน (Pearson's Correlation Coefficient)

ผลการวิจัย

1. ปัจจัยด้านลักษณะทางประชากร

ผลการวิเคราะห์ข้อมูลด้านลักษณะทางประชากรของกลุ่มตัวอย่าง จำนวน 365 คน พบว่า ส่วนใหญ่เป็นเพศชาย จำนวน 202 คน คิดเป็นร้อยละ 55.34 รองลงมาคือเพศหญิง จำนวน 156 คน คิดเป็นร้อยละ 42.74 และผู้ไม่ประสงค์ระบุเพศ จำนวน 7 คน คิดเป็นร้อยละ 1.92 ตามลำดับ ในด้านอายุ พบว่า ส่วนใหญ่มีอายุต่ำกว่า 27 ปี (Generation Z) จำนวน 328 คน คิดเป็นร้อยละ 89.86 ขณะที่กลุ่มอายุ 28–43 ปี (Generation Y) มีจำนวน 21 คน คิดเป็นร้อยละ 5.75 และกลุ่มอายุ 44–59 ปี (Generation X) มีจำนวน 13 คน คิดเป็นร้อยละ 3.56 ส่วนผู้ที่ไม่ประสงค์ระบุอายุ มีจำนวน 3 คน คิดเป็นร้อยละ 0.82

เมื่อจำแนกตามประเภทบุคลากร พบว่า ส่วนใหญ่เป็นกลุ่มนักศึกษา จำนวน 329 คน คิดเป็นร้อยละ 90.14 ขณะที่บุคลากรสายวิชาการและบุคลากรสายสนับสนุนมีจำนวนเท่ากัน คือ 18 คนต่อกลุ่ม คิดเป็นร้อยละ 4.93 สำหรับด้านระดับการศึกษา พบว่า เป็นกลุ่มที่กำลังศึกษาในระดับปริญญาตรีมีจำนวนมากที่สุด จำนวน 289 คน คิดเป็นร้อยละ 79.18 รองลงมาคือ ผู้สำเร็จการศึกษาในระดับปริญญาตรี จำนวน 58 คน คิดเป็นร้อยละ 15.89 ระดับปริญญาโท จำนวน 14 คน คิดเป็นร้อยละ 3.84 และระดับสูงกว่าปริญญาโท จำนวน 4 คน คิดเป็นร้อยละ 1.10 และในด้านรายได้เฉลี่ยต่อเดือน พบว่า ส่วนใหญ่มีรายได้ไม่เกิน 15,000 บาท จำนวน 170 คน คิดเป็นร้อยละ 46.58 รองลงมาคือ กลุ่มที่ไม่มีรายได้ จำนวน 153 คน คิดเป็นร้อยละ 41.92 ขณะที่กลุ่มที่มีรายได้ระหว่าง 15,001–30,000 บาท มีจำนวน 22 คน คิดเป็นร้อยละ 6.03 กลุ่มที่มีรายได้ระหว่าง 30,001–45,000 บาท จำนวน 14 คน คิดเป็นร้อยละ 3.84 รายได้ระหว่าง 45,001–60,000 บาท จำนวน 5 คน คิดเป็นร้อยละ 1.37 และรายได้ตั้งแต่ 60,001 บาทขึ้นไป มีเพียง 1 คน คิดเป็นร้อยละ 0.27

สำหรับประสบการณ์ในการใช้งานอินเทอร์เน็ต พบว่า ส่วนใหญ่มีประสบการณ์ใช้งานมากกว่า 6 ปี จำนวน 158 คน คิดเป็นร้อยละ 43.29 รองลงมาคือ กลุ่มที่มีประสบการณ์ใช้งานระหว่าง 1–3 ปี จำนวน 146 คน คิดเป็นร้อยละ 40.00 กลุ่มที่มีประสบการณ์ใช้งานระหว่าง 4–6 ปี จำนวน 47 คน คิดเป็นร้อยละ 12.88 และกลุ่มที่มีประสบการณ์ใช้งานน้อยกว่า 1 ปี จำนวน 14 คน คิดเป็นร้อยละ 3.84 และในส่วนของอุปกรณ์ที่ใช้เข้าถึงอินเทอร์เน็ต พบว่า ใช้โทรศัพท์มือถือเป็นอุปกรณ์ที่ได้รับความนิยมมากที่สุด จำนวน 361 คน คิดเป็นร้อยละ 47.88 รองลงมาคือ แท็บเล็ต จำนวน 199 คน คิดเป็นร้อยละ 26.39 และคอมพิวเตอร์ จำนวน 194 คน คิดเป็นร้อยละ 25.73

2. ปัจจัยด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

ผลการวิเคราะห์ข้อมูลด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ พบว่า กลุ่มตัวอย่าง 365 คน มีผู้ที่ไม่เคยมีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์จำนวน 133 คน คิดเป็นร้อยละ 36.44 ขณะที่ผู้ที่เคยมีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์มีจำนวน 232 คน คิดเป็นร้อยละ 63.56 ซึ่งพบภัยคุกคามในหลากหลายรูปแบบโดยลำดับเหตุการณ์ที่พบบ่อยที่สุดคือ การได้รับผลกระทบจากไวรัสที่ทำให้ไฟล์หรือโปรแกรมเสียหาย จำนวน 139 ครั้ง คิดเป็นร้อยละ 15.14 รองลงมา คือ การได้รับโฆษณาหรือป๊อปอัพไม่พึงประสงค์ จำนวน 128 ครั้ง คิดเป็นร้อยละ 13.94 และการได้รับอีเมลหลอกลวงที่พยายามให้คลิกลิงก์หรือเปิดไฟล์แนบ จำนวน 119 ครั้ง คิดเป็นร้อยละ 12.96

เมื่อจำแนกกลุ่มตัวอย่างตามระดับประสบการณ์ พบว่า ส่วนใหญ่มีระดับประสบการณ์อยู่ในระดับน้อย คิดเป็นร้อยละ 76.16 รองลงมาคือ ระดับปานกลาง คิดเป็นร้อยละ 19.73 และระดับมาก คิดเป็นร้อยละ 4.11

ในการอบรมหรือการรับรู้ข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ พบว่า กลุ่มตัวอย่างส่วนใหญ่เคยได้รับการอบรมหรือรับข้อมูลข่าวสาร จำนวน 226 คน คิดเป็นร้อยละ 61.92 ขณะที่ผู้ที่ไม่เคยได้รับการอบรมมีจำนวน 139 คน คิดเป็นร้อยละ 38.08 โดยช่องทางที่ได้รับข้อมูลมากที่สุดคือ โซเชียลมีเดีย เช่น Facebook, Line และ YouTube จำนวน 175 คน คิดเป็นร้อยละ 38.04 รองลงมาคือโทรศัพท์และสื่อสาธารณะ จำนวน 112 คน คิดเป็นร้อยละ 24.35 เว็บไซต์ของมหาวิทยาลัยหรือองค์กร จำนวน 88 คน คิดเป็นร้อยละ 19.13 อีเมลจากหน่วยงาน จำนวน 60 คน คิดเป็นร้อยละ 13.04 และการเข้าร่วมอบรมเชิงปฏิบัติการ (Workshop/Seminar) จำนวน 25 คน คิดเป็นร้อยละ 5.43

3. ปัจจัยด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

ผลการวิเคราะห์ข้อมูลด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ พบว่า กลุ่มตัวอย่างส่วนใหญ่มีความรู้ความเข้าใจที่ถูกต้องเกี่ยวกับภัยคุกคามทางไซเบอร์ โดยประเด็นความรู้ที่กลุ่มตัวอย่างมีความรู้ความเข้าใจที่ถูกต้องสูงสุดคือ การสำรองข้อมูลและตั้งรหัสเข้าใช้ทำให้ความปลอดภัยมากขึ้น โดยมีผู้ตอบถูกจำนวน 307 คน คิดเป็นร้อยละ 84.11 รองลงมาคือ การตั้งรหัสผ่านที่รัดกุมจะเป็นการผสมตัวอักษรพิมพ์เล็ก-ใหญ่ ตัวเลข และสัญลักษณ์พิเศษ ความยาวไม่น้อยกว่า 8 ตัวอักษร มีผู้ตอบถูก 304 คน คิดเป็นร้อยละ 83.29 ในขณะที่ประเด็นความรู้การเข้าเว็บไซต์ที่ขึ้นต้นด้วย https มีความปลอดภัยมากกว่า http และการติดตามข่าวสารเกี่ยวกับรูปแบบการโจมตีทางไซเบอร์ช่วยลดความเสี่ยง มีจำนวนผู้ตอบถูกเท่ากัน คือ 297 คน คิดเป็นร้อยละ 81.37 นอกจากนี้ ยังพบว่า ประเด็นความรู้ การเปิดเผยข้อมูลส่วนตัว เช่น ชื่อ-นามสกุล เบอร์โทรศัพท์ หรือรูปภาพบนโซเชียลมีเดียไม่มีความเสี่ยง และการเปิดเผยตำแหน่งปัจจุบันของตนเองผ่านการเช็คอินหรือแชร์โลเคชันบนโซเชียลมีเดีย ก็มีความรู้ความเข้าใจถูกต้องอยู่ในระดับสูงเช่นกัน โดยมีจำนวนผู้ตอบถูก 292 คน คิดเป็นร้อยละ 80.00 และ 290 คน คิดเป็นร้อยละ 79.45 ตามลำดับ ขณะที่ประเด็นเรื่องการดาวน์โหลดแอปพลิเคชันที่มีชื่อคล้ายกับแอปพลิเคชันยอดนิยมมักปลอดภัยเสมอ มีผู้ตอบถูก 269 คน คิดเป็นร้อยละ 73.70 และการเข้าใช้เครือข่ายไร้สายสาธารณะมีความเสี่ยงต่อการทำธุรกรรมออนไลน์มีผู้ตอบถูก 255 คน คิดเป็นร้อยละ 69.86 ส่วนประเด็นความรู้ที่กลุ่มตัวอย่างมีความรู้ความเข้าใจอยู่ในระดับต่ำได้แก่ การใช้รหัสผ่านเดียวกันสำหรับทุกเว็บไซต์หรือแอปพลิเคชันเป็นเรื่องที่ปลอดภัย ซึ่งมีผู้ตอบถูกเพียง 224 คน คิดเป็นร้อยละ 61.37 และการใช้ซอฟต์แวร์ลูกลิขสิทธิ์มีความเสี่ยงเท่ากับซอฟต์แวร์ละเมิดลิขสิทธิ์ โดยมีผู้ตอบถูกเพียง 181 คน คิดเป็นร้อยละ 49.59

เมื่อจำแนกกลุ่มตัวอย่างตามระดับความรู้ พบว่า กลุ่มตัวอย่างส่วนใหญ่มีความรู้อยู่ในระดับมาก จำนวน 255 คน คิดเป็นร้อยละ 69.86 รองลงมาคือ มีความรู้ในระดับปานกลาง จำนวน 82 คน คิดเป็นร้อยละ 22.47 และมีความรู้ในระดับน้อย จำนวน 28 คน คิดเป็นร้อยละ 7.67

4. ปัจจัยด้านความตระหนักถึงภัยคุกคามทางไซเบอร์

ผลการวิเคราะห์ข้อมูลด้านความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ ใน 6 ประเด็น ได้แก่ ด้านความปลอดภัย (Security) ด้านการฉ้อโกง (Flaming) ด้านการข่มขู่ใส่ร้าย (Harassment) ด้านการแอบอ้าง (Masquerading) ด้านการเผยแพร่อกนอกกลุ่ม (Outing) และด้านการกีดกัน (Exclusion) พบว่า โดยภาพรวมกลุ่มตัวอย่างมีความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ อยู่ในระดับมากที่สุด มีค่าเฉลี่ย 4.54 (S.D.=0.33) โดยด้านที่มีความตระหนักสูงที่สุด คือ ด้านความปลอดภัย มีค่าเฉลี่ย 4.62 (S.D.=0.39) โดยให้ความสำคัญในการป้องกันการถูกโปรแกรมคอมพิวเตอร์ที่ไม่พึงประสงค์ทำความเสียหายต่อข้อมูลในระบบ การป้องกันการเจาะระบบเพื่อขโมยหรือทำลายข้อมูล และการป้องกันการถูกหลอกให้กรอกข้อมูลส่วนตัวทางเว็บไซต์ปลอม

รองลงมาได้แก่ ด้านการแอบอ้าง ซึ่งมีค่าเฉลี่ย 4.56 (S.D.=0.41) แสดงถึงการตระหนักถึงอันตรายจากการแอบอ้างชื่อรูปภาพ หรือบัญชีผู้ใช้งานของผู้อื่นในโลกออนไลน์ ในขณะที่ด้านการข่มขู่ใส่ร้าย และด้านการเผยแพร่ข้อมูลนอกกลุ่ม มีค่าเฉลี่ยเท่ากัน คือ 4.54 (S.D.=0.41 และ 0.43 ตามลำดับ) สะท้อนถึงการให้ความสำคัญกับการไม่ใส่ร้าย ไม่เผยแพร่ภาพหรือข่าวลือที่ก่อให้เกิดความเสียหายแก่ผู้อื่น และด้านการยั่วยุโมโห มีค่าเฉลี่ย 4.53 (S.D.=0.47) แสดงถึงการตระหนักถึงการไม่ใช้ถ้อยคำหยาบคายหรือโพสต์ข้อความที่ทำให้ผู้อื่นเสียชื่อเสียง ส่วนด้านการกีดกัน มีค่าเฉลี่ยต่ำสุดเมื่อเทียบกับด้านอื่น ๆ โดยมีค่าเฉลี่ย 4.45 (S.D.=0.51) แสดงให้เห็นถึงการตระหนักในผลกระทบจากพฤติกรรม การบล็อก การลบ หรือการกีดกันให้ผู้อื่นออกจากกลุ่มสนทนา

5. เปรียบเทียบความตระหนักถึงภัยคุกคามทางไซเบอร์ จำแนกตามปัจจัยด้านลักษณะทางประชากร

ตารางที่ 1 การวิเคราะห์ความแปรปรวนทางเดียว (One-Way ANOVA) ของความตระหนักถึงภัยคุกคามทางไซเบอร์ จำแนกตามปัจจัยด้านลักษณะทางประชากร

ปัจจัยด้านลักษณะทางประชากร	แหล่งความแปรปรวน	SS	df	MS	F	p-value
1. เพศ	ระหว่างกลุ่ม	.045	2	.023	.208	.812
	ภายในกลุ่ม	39.408	362	.109		
	รวม	39.453	364			
2. อายุ	ระหว่างกลุ่ม	.725	3	.242	2.251	.082
	ภายในกลุ่ม	38.729	361	.107		
	รวม	39.453	364			
3. ประสบการณ์การใช้อินเทอร์เน็ต	ระหว่างกลุ่ม	.330	3	.110	1.014	.387
	ภายในกลุ่ม	39.124	361	.108		
	รวม	39.453	364			
4. ประเภทบุคลากร	ระหว่างกลุ่ม	.752	2	.376	3.518	.031*
	ภายในกลุ่ม	38.701	362	.107		
	รวม	39.453	364			
5. ระดับการศึกษา	ระหว่างกลุ่ม	.446	3	.149	1.377	.250
	ภายในกลุ่ม	39.007	361	.108		
	รวม	39.453	364			
6. รายได้	ระหว่างกลุ่ม	.994	5	.199	1.856	.101
	ภายในกลุ่ม	38.459	359	.107		
	รวม	39.453	364			

* มีนัยสำคัญทางสถิติที่ระดับ .05

ตารางที่ 2 ผลการเปรียบเทียบค่าเฉลี่ยรายคู่ (Post Hoc) ความตระหนักถึงภัยคุกคามทางไซเบอร์ จำแนกตามประเภทบุคลากร ด้วยวิธี Scheffé

ประเภทบุคลากร	n	$\bar{X}$	S.D.	กลุ่มตัวอักษรกำกับ
นักศึกษา	329	4.52	0.33	a
บุคลากรสายวิชาการ	18	4.67	0.31	b
บุคลากรสายสนับสนุน	18	4.68	0.29	b

หมายเหตุ: ค่าเฉลี่ยที่กำกับด้วยตัวอักษรที่แตกต่างกัน (a, b) มีความแตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .05

จากตารางที่ 1 และ 2 ผลการวิเคราะห์เปรียบเทียบความตระหนักถึงภัยคุกคามทางไซเบอร์ จำแนกตามลักษณะทางประชากร พบว่า เพศ อายุ ประสบการณ์การใช้อินเทอร์เน็ต ระดับการศึกษา และรายได้ ที่แตกต่างกัน มีความตระหนักต่อภัยคุกคามทางไซเบอร์ไม่แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 อย่างไรก็ตาม พบความแตกต่างอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 ในปัจจัยด้านประเภทบุคลากร ($F = 3.518, p = .031$) เมื่อทดสอบรายคู่ด้วยวิธี Scheffé พบว่า กลุ่มบุคลากรสายสนับสนุน ($\bar{X} = 4.68$) และกลุ่มบุคลากรสายวิชาการ ($\bar{X} = 4.67$) มีระดับความตระหนักไม่แตกต่างกัน (อยู่ในกลุ่มตัวอักษร b เหมือนกัน) แต่ทั้งสองกลุ่มมีระดับความตระหนักสูงกว่ากลุ่มนักศึกษา ($\bar{X} = 4.52$) อย่างมีนัยสำคัญทางสถิติที่ระดับ .05 (แยกออกมาอยู่ในกลุ่มตัวอักษร a)

6. การวิเคราะห์ความสัมพันธ์ (Pearson Correlation)

ตารางที่ 3 ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างประสบการณ์และความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์กับความตระหนักถึงภัยคุกคามทางไซเบอร์

ตัวแปร	ความตระหนักถึงภัยคุกคามทางไซเบอร์		
	r	p-value	ผลการทดสอบ
1. ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์	-0.090	.086	ไม่มีนัยสำคัญ
2. ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์	0.212	.000*	มีนัยสำคัญเชิงบวก

* มีนัยสำคัญทางสถิติที่ระดับ .05

จากตารางที่ 3 ผลการวิเคราะห์ความสัมพันธ์พบว่า ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ ไม่มีความสัมพันธ์กับความตระหนักถึงภัยคุกคามทางไซเบอร์อย่างมีนัยสำคัญทางสถิติ $r = -0.090$ โดยมีค่า $p = .086$ ในขณะที่ ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ มีความสัมพันธ์เชิงบวกในระดับต่ำกับความตระหนักถึงภัยคุกคามทางไซเบอร์อย่างมีนัยสำคัญทางสถิติที่ระดับ .05 ($r = 0.212, p = .000$) ซึ่งแสดงให้เห็นว่า หากผู้ใช้อินเทอร์เน็ต มีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ที่ถูกต้องเพิ่มขึ้น จะส่งผลให้มีแนวโน้มความตระหนักถึงภัยคุกคามทางไซเบอร์สูงขึ้นตามไปด้วย

อภิปรายผลการวิจัย

การวิจัยเรื่อง ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในมหาวิทยาลัย ราชภัฏกาญจนบุรี สามารถอภิปรายผลการวิจัยได้ดังนี้

1. ปัจจัยด้านลักษณะทางประชากร ผลการศึกษาจากกลุ่มตัวอย่างจำนวน 365 คน เมื่อจำแนกตามลักษณะทางประชากร ได้แก่ เพศ อายุ ประสบการณ์การใช้งานอินเทอร์เน็ต ประเภทบุคลากร ระดับการศึกษา และรายได้ พบว่าส่วนใหญ่เป็นนักศึกษาเพศชายในช่วงวัย Generation Z ที่มีอายุน้อยกว่า 27 ปี กำลังศึกษาในระดับปริญญาตรี มีประสบการณ์ใช้งานอินเทอร์เน็ตสูง และนิยมใช้อุปกรณ์โทรศัพท์มือถือเป็นหลัก มีรายได้ไม่เกิน 15,000 บาทต่อเดือน หรือไม่มีรายได้ ซึ่งสะท้อนถึงลักษณะของนักศึกษาเป็นหลัก ข้อมูลนี้แสดงให้เห็นว่ากลุ่มตัวอย่างเป็นคนรุ่นใหม่ที่มีความคุ้นเคยกับการใช้งานเทคโนโลยีและอินเทอร์เน็ตในชีวิตประจำวัน เมื่อทำการเปรียบเทียบความตระหนักถึงภัยคุกคามทางไซเบอร์ จำแนกตามปัจจัยด้านลักษณะทางประชากร ได้แก่ เพศ อายุ ประสบการณ์การใช้งานอินเทอร์เน็ต ประเภทบุคลากร ระดับการศึกษา และรายได้ ของกลุ่มตัวอย่างที่แตกต่างกัน พบว่า มีความตระหนักถึงภัยคุกคามทางไซเบอร์ไม่แตกต่างกัน อย่างมีนัยสำคัญทางสถิติ ที่ระดับ .05 ซึ่งสอดคล้องกับงานวิจัยของ สุธาเทพ รุณเรศ (2561) ที่ศึกษาเกี่ยวกับปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร ที่พบว่า เพศที่แตกต่างกัน มีระดับความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตไม่แตกต่างกัน อีกทั้งยังสอดคล้องกับงานวิจัยของ เมธพร ธรรมศิริ และศิริภัสสรค์ วงศ์ทองดี (2565) ที่ศึกษาความตระหนักด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร โดยพบว่า กลุ่มบุคลากรที่มีเพศและอายุที่แตกต่างกันมีระดับความตระหนักด้านภัยคุกคามทางไซเบอร์ที่ไม่แตกต่างกัน

2. ปัจจัยด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ ผลการศึกษา พบว่า กลุ่มตัวอย่างส่วนใหญ่มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ในหลากหลายรูปแบบ โดยประสบการณ์ที่พบบ่อยที่สุดคือ การได้รับผลกระทบจากไวรัสที่ทำให้ไฟล์หรือโปรแกรมเสียหาย การได้รับโฆษณาหรือป๊อปอัพไม่พึงประสงค์ และการได้รับอีเมลหลอกลวงที่พยายามให้คลิกลิงก์หรือเปิดไฟล์แนบ เป็นต้น ซึ่งเป็นภัยที่เกิดขึ้นได้บ่อยในชีวิตประจำวันของผู้ใช้อินเทอร์เน็ต ขณะเดียวกันยังพบว่า มีกลุ่มตัวอย่างจำนวนหนึ่งที่ไม่เคยประสบภัยคุกคามทางไซเบอร์ ในสัดส่วนที่ค่อนข้างสูง อันมีผลจากเคยได้รับการอบรมหรือการได้รับข้อมูลข่าวสารจากช่องทางต่างๆ ทำให้มีความรู้ความเข้าใจ และสามารถป้องกันตนเองจากภัยคุกคามทางไซเบอร์ได้ ผลการวิเคราะห์ความสัมพันธ์ระหว่างปัจจัยด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์กับความตระหนักถึงภัยคุกคามทางไซเบอร์ ของกลุ่มตัวอย่าง พบว่า ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ไม่มีความสัมพันธ์อย่างมีนัยสำคัญทางสถิติที่ระดับ .05 กับความตระหนักถึงภัยคุกคามทางไซเบอร์ สะท้อนให้เห็นว่า การเผชิญเหตุการณ์เพียงอย่างเดียวมิได้ทำให้เกิดความตระหนัก หากไม่ได้รับการถ่ายทอดหรือเสริมสร้างความเข้าใจเพิ่มเติม ผลการศึกษาครั้งนี้สอดคล้องกับงานของ สุธาเทพ รุณเรศ (2561) ที่ศึกษาเกี่ยวกับปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร ซึ่งพบว่า ประสบการณ์ไม่มีผลต่อระดับความตระหนักถึงภัยคุกคามทางไซเบอร์เช่นกัน อย่างไรก็ตาม ผลการศึกษานี้แตกต่างจากงานของ คณัญญา อิมใจ (2565) ที่ศึกษาพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจนเอเรชั่น Z ซึ่งพบว่า ประสบการณ์มีผลต่อพฤติกรรมการป้องกันภัยไซเบอร์ของกลุ่มตัวอย่าง แสดงให้เห็นว่าผลของประสบการณ์อาจแตกต่างกันไปตามลักษณะของกลุ่มเป้าหมายและบริบทแวดล้อมที่พบ

3. ปัจจัยด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ ผลการศึกษาเมื่อจำแนกกลุ่มตัวอย่างตามระดับความรู้ พบว่า กลุ่มตัวอย่างส่วนใหญ่มีความรู้ในระดับมาก โดยมีความรู้ความเข้าใจที่ถูกต้องในประเด็นพื้นฐานด้านความปลอดภัยทางไซเบอร์ เช่น การสำรองข้อมูล การตั้งรหัสผ่านที่รัดกุม การใช้เว็บไซต์ที่มีความปลอดภัย (https) และไม่เปิดเผยข้อมูลส่วนบุคคลและตำแหน่งปัจจุบันของตนเองบนสื่อสังคมออนไลน์ อย่างไรก็ตาม ยังพบว่า

มีกลุ่มตัวอย่างจำนวนหนึ่งที่มีความรู้ความเข้าใจที่คลาดเคลื่อนในประเด็นที่สำคัญ โดยเฉพาะเรื่องการใช้ซอฟต์แวร์
ถูกลิขสิทธิ์และการใช้รหัสผ่านเดียวกันทุกเว็บไซต์ ซึ่งควรได้รับการให้ความรู้เพิ่มเติมเพื่อป้องกันความเสี่ยง
จากภัยคุกคามที่อาจเกิดขึ้นในอนาคต ผลการวิเคราะห์ความสัมพันธ์ระหว่างปัจจัยด้านความรู้เกี่ยวกับภัยคุกคาม
ทางไซเบอร์กับความตระหนักถึงภัยคุกคามทางไซเบอร์ ของกลุ่มตัวอย่าง พบว่า ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์
มีความสัมพันธ์เชิงบวกอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 กับความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้
อินเทอร์เน็ตในมหาวิทยาลัยราชภัฏกาญจนบุรี ซึ่งผลการศึกษาครั้งนี้สอดคล้องกับงานวิจัยของ สุธาเทพ รุณเรศ (2561)
ที่ศึกษาปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร ซึ่งให้เห็นว่า
ความรู้มีผลต่อระดับความตระหนักถึงภัยคุกคามทางไซเบอร์ อีกทั้งยังสอดคล้องกับงานวิจัยของ วิไล ฤทธิเดช และ
สรวง รุ่งประกายพรรณ (2566) ที่ศึกษาในประเด็นความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคง
ปลอดภัยสารสนเทศของบุคลากรสาธารณสุขในประเทศไทย: กรณีศึกษาโรงพยาบาลพุทธโสธร ซึ่งพบว่า ความรู้มีผลต่อ
ความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตเช่นเดียวกัน อย่างไรก็ตาม ผลการศึกษานี้แตกต่างจาก
งานวิจัยของ คณัญญา อิมใจ (2565) ที่ศึกษาเรื่อง พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่ม
เจนเอเรชั่นแซต ซึ่งพบว่า ความรู้ไม่มีอิทธิพลต่อพฤติกรรมการป้องกันภัยไซเบอร์ สะท้อนว่าการมีความรู้เพียงอย่าง
เดียวอาจไม่เพียงพอหากไม่ได้ถูกนำไปปรับใช้จริงในชีวิตประจำวัน

4. ปัจจัยด้านความตระหนักถึงภัยคุกคามทางไซเบอร์ ผลการศึกษา พบว่า กลุ่มตัวอย่างมีความตระหนักถึง
ภัยคุกคามทางไซเบอร์ โดยภาพรวมอยู่ในระดับมากที่สุด (ค่าเฉลี่ย 4.54, S.D.=0.33) เมื่อพิจารณาแยกเป็นรายด้าน
พบว่า มีความตระหนักถึงภัยคุกคามทางไซเบอร์อยู่ในระดับมากที่สุดถึงมากที่สุด (ค่าเฉลี่ยระหว่าง 4.62 – 4.45) โดย
ด้านที่มีระดับความตระหนักถึงภัยคุกคามทางไซเบอร์สูงที่สุดคือ ด้านความปลอดภัย รองลงมาได้แก่ ด้านการแอบอ้าง
ด้านการข่มขู่ใส่ร้าย ด้านการเผยแพร่ข้อมูลนอกกลุ่ม และด้านการยั่วยุโมโห ตามลำดับ ส่วนด้านการกีดกัน เป็นด้านที่มี
ระดับความตระหนักภัยคุกคามทางไซเบอร์ต่ำที่สุดเมื่อเทียบกับด้านอื่น ๆ แม้ความสำคัญในประเด็นนี้ อาจไม่เท่ากับ
ด้านความปลอดภัยและด้านการแอบอ้าง แต่ก็สะท้อนถึงความตระหนักในเชิงสังคมออนไลน์ของกลุ่มตัวอย่าง จาก
การศึกษาปัจจัยด้านความตระหนักถึงภัยคุกคามทางไซเบอร์ เมื่อทำการเปรียบเทียบโดยจำแนกตามปัจจัยด้านลักษณะ
ทางประชากร รวมถึงการวิเคราะห์ความสัมพันธ์กับด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ พบว่า
ไม่มีนัยสำคัญทางสถิติ ทั้งนี้ผลการวิเคราะห์ความสัมพันธ์กับด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์นั้น พบว่า
มีความสัมพันธ์เชิงบวกกับระดับความตระหนักถึงภัยคุกคามทางไซเบอร์อย่างมีนัยสำคัญทางสถิติ สอดคล้องกับ
งานวิจัยของ สุธาเทพ รุณเรศ (2561) และวิไล ฤทธิเดช และสรวง รุ่งประกายพรรณ (2566) พบว่า ความรู้มีบทบาท
สำคัญต่อการเสริมสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ ผลการวิจัยนี้จึงชี้ให้เห็นว่าการเสริมสร้างองค์ความรู้
ด้านภัยคุกคามทางไซเบอร์ เป็นแนวทางที่มีประสิทธิภาพในการยกระดับความตระหนักของผู้ใช้อินเทอร์เน็ตใน
มหาวิทยาลัยราชภัฏกาญจนบุรี อีกทั้งเป็นแนวทางสำคัญในการกำหนดมาตรการเชิงนโยบาย การพัฒนากิจกรรม และ
การจัดอบรม เพื่อเสริมสร้างการตระหนักรู้ด้านความปลอดภัยไซเบอร์ให้เกิดประสิทธิภาพมากยิ่งขึ้น

สรุปผลการวิจัยและข้อเสนอแนะ

สรุปผลการวิจัย

การวิจัยเรื่อง ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในมหาวิทยาลัยราชภัฏกาญจนบุรี สรุปผลการวิเคราะห์ข้อมูลได้ดังนี้

1. ปัจจัยด้านลักษณะทางประชากร

ปัจจัยด้านลักษณะทางประชากร ประกอบด้วย เพศ อายุ ประสบการณ์การใช้อินเทอร์เน็ต ประเภทบุคลากร ระดับการศึกษา และรายได้ จากผลการเปรียบเทียบความแตกต่างของลักษณะทางประชากร ด้วยการวิเคราะห์ความแปรปรวนทางเดียว (One-way ANOVA) พบว่า ลักษณะทางประชากรของกลุ่มตัวอย่างที่แตกต่างกันมีความตระหนักถึงภัยคุกคามทางไซเบอร์ไม่แตกต่างกันอย่างมีนัยสำคัญทางสถิติ ที่ระดับ .05

2. ปัจจัยด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

ผลการวิเคราะห์ความสัมพันธ์ระหว่างประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์กับระดับความตระหนักถึงภัยคุกคามทางไซเบอร์ พบว่า ไม่มีความสัมพันธ์อย่างมีนัยสำคัญทางสถิติที่ระดับ .05

3. ปัจจัยด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

ผลการวิเคราะห์ความสัมพันธ์ระหว่างความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์กับระดับความตระหนักถึงภัยคุกคามทางไซเบอร์ พบว่า มีความสัมพันธ์เชิงบวกอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 โดยมีค่าสัมประสิทธิ์สหสัมพันธ์ $r = 0.212$ และค่า $p = .000$

ข้อเสนอแนะจากคณะผู้วิจัย

1. ข้อเสนอแนะเชิงนโยบาย

1.1 มหาวิทยาลัยราชภัฏกาญจนบุรีควรกำหนดนโยบายและแผนยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Policy) ให้เป็นลายลักษณ์อักษรและประกาศใช้อย่างเป็นทางการ โดยกำหนดให้การตระหนักรู้ด้านภัยไซเบอร์เป็นสมรรถนะพื้นฐานทางดิจิทัลที่นักศึกษาทุกคนต้องผ่านเกณฑ์ และบุคลากรทุกคนต้องได้รับการทดสอบประจำปีเพื่อสร้างความปลอดภัยอย่างยั่งยืนในระบบสารสนเทศของสถาบัน

1.2 ควรมุ่งเน้นนโยบายเชิงรุกในการจัดสรรงบประมาณสำหรับทุนอุดหนุนเพื่อขับเคลื่อนระบบตรวจสอบสิทธิ์และโครงสร้างพื้นฐานเครือข่ายความปลอดภัย โดยเฉพาะแนวทางการใช้งานระบบเครือข่ายไร้สายสาธารณะและการกำหนดมาตรฐานรหัสผ่านที่รัดกุมภายในองค์กร

2. ข้อเสนอแนะเชิงวิชาการ

2.1 มหาวิทยาลัยราชภัฏกาญจนบุรีควรจัดทำหลักสูตรระยะสั้นเกี่ยวกับการให้ความรู้เบื้องต้นด้านภัยคุกคามทางไซเบอร์ พร้อมแนวทางการรับมือ การป้องกัน และการแก้ไขปัญหา โดยนำผลวิจัยในประเด็นที่กลุ่มตัวอย่างยังมีความเข้าใจคลาดเคลื่อนสูง เช่น ความเสี่ยงจากการใช้ซอฟต์แวร์ละเมิดลิขสิทธิ์ และอันตรายจากการใช้รหัสผ่านเดียวกันในทุกระบบ มาออกแบบกระบวนการเรียนรู้เพื่อปรับพฤติกรรมการใช้งานระบบสารสนเทศของนักศึกษาและบุคลากร

2.2 มหาวิทยาลัยราชภัฏกาญจนบุรีควรจัดทำสื่อความรู้ด้านการป้องกันภัยคุกคามทางไซเบอร์ในรูปแบบสื่อสร้างสรรค์ดิจิทัลที่เข้าใจง่าย เช่น อินโฟกราฟิก หรือคลิปวิดีโอ เผยแพร่ผ่านช่องทาง Facebook,

YouTube และ TikTok เป็นต้น เพื่อเน้นย้ำเรื่องความปลอดภัยรายด้าน โดยเฉพาะ "ด้านความปลอดภัย" และ "ด้านการแอบอ้าง" ซึ่งเป็นมิติที่กลุ่มตัวอย่างระบุว่ามีสำคัญและพบการเผชิญเหตุบ่อยครั้ง

3. ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

3.1 ควรขยายขอบเขตการวิจัยไปยังกลุ่มตัวอย่างที่หลากหลายมากขึ้น เช่น นักเรียนระดับมัธยมศึกษา บุคลากรภาครัฐ ภาคเอกชน หรือประชาชนทั่วไป เพื่อให้ได้ข้อมูลเชิงเปรียบเทียบที่ครอบคลุมมากยิ่งขึ้น

3.2 ควรใช้ระเบียบวิธีวิจัยแบบผสมผสาน (Mixed Methods) โดยเก็บข้อมูลทั้งเชิงปริมาณและเชิงคุณภาพ เพื่อให้เข้าใจลึกซึ้งถึงพฤติกรรม แรงจูงใจ และปัจจัยที่มีผลต่อการตระหนักรู้ด้านความปลอดภัยไซเบอร์

กิตติกรรมประกาศ

งานวิจัยนี้ได้รับทุนอุดหนุนการวิจัยสำหรับบุคลากรสายสนับสนุนจากมหาวิทยาลัยราชภัฏกาญจนบุรี ประจำปีงบประมาณ พ.ศ. 2567 คณะผู้วิจัยขอขอบคุณคณะผู้บริหารสำนักวิทยบริการและเทคโนโลยีสารสนเทศ และสถาบันวิจัยและพัฒนา มหาวิทยาลัยราชภัฏกาญจนบุรี ที่ให้การสนับสนุนมาอย่างต่อเนื่อง ขอขอบคุณนักศึกษาและบุคลากรของมหาวิทยาลัยราชภัฏกาญจนบุรี ที่ให้ความร่วมมือตอบแบบสอบถาม ตลอดจนแหล่งข้อมูลทางวิชาการอื่น ๆ ที่เอื้ออำนวยให้คณะผู้วิจัยสามารถเข้าถึงข้อมูลที่เกี่ยวข้องได้อย่างครบถ้วน

เอกสารอ้างอิง

- คณัญญา อิมใจ. (2565). พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจนเอเรชั่นแซด. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ. มหาวิทยาลัยศรีนครินทรวิโรฒ. กรุงเทพฯ.
- งานบริหารงานบุคคล มหาวิทยาลัยราชภัฏกาญจนบุรี. (2567). ข้อมูลบุคลากรมหาวิทยาลัยราชภัฏกาญจนบุรี ณ วันที่ 1 มิถุนายน 2567. เอกสารภายในสถาบัน.
- เมธพร ธรรมศิริ และ ศิริภัสสร วงศ์ทองดี. (2565). ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร. วารสารวิชาการไทยวิจัยและการจัดการ มหาวิทยาลัยสยาม. 3(2), 1-17. ค้นจาก <https://so05.tci-thaijo.org/index.php/TRDMJOPOLSU/article/view/259170>
- วิไล ฤทธิเดช และ สรวง รุ่งประกายพรรณ. (2566). ความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรสาธารณสุขในประเทศไทย: กรณีศึกษาโรงพยาบาลพุทธโสธร. วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเซีย ฉบับวิทยาศาสตร์และเทคโนโลยี. 17(1), 183-200. ค้นจาก <https://he01.tci-thaijo.org/index.php/EAUHJSci/article/view/260148>
- สปริงนิวส์. (2567). เปิดสถิติภัยคุกคามทางไซเบอร์ ประจำปี 2566 หน่วยงานด้านการศึกษาว่มนสุด. สืบค้นจาก <https://www.springnews.co.th/digital-tech/847630>
- สุธาเทพ รุนเรศ. (2561). ปัจจัยที่มีผลต่อการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร. การค้นคว้าอิสระปริญญาโทบริหารธุรกิจ. วิทยาลัยนวัตกรรมการศึกษา มหาวิทยาลัยธรรมศาสตร์. กรุงเทพฯ.
- สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2566). สถิติภัยคุกคามทางไซเบอร์ ประจำปี 2566. ค้นจาก <https://www.sec.or.th/TH/Pages/CYBERRESILIENCE-STATISTICS-2566.aspx>

สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏกาญจนบุรี. (2567). *ข้อมูลนักศึกษาที่ลงทะเบียนเรียน
ภาคการศึกษา 1/2567*. เอกสารภายในสถาบัน.

Yamane, T. (1973). *Statistics: An Introductory Analysis*. (3rd ed.). New York: Harper and Row.