ปัจจัยที่ส่งต่อการตระหนักรู้ถึงความปลอดภัยทางไซเบอร์ของนักศึกษามหาวิทยาลัย

Factors Affecting University Students' Cybersecurity Awareness

กิติยา วิสิฐพงศ์พันธ์[1], ชูเกียรติ บุญก่อเกื้อ[2], กิตติพงศ์ อยู่นิรันดร[3*], นลินภัสร์ บำเพ็ญเพียร[4]

Kitiya Wisitpongpun[1], Chukiat Boonkorkoer[2], Kittipong Yoonirundorn[3*], Nalinpat Bhumpenpein[4]

[1, 2, 3, 4] ภาควิชาเทคโนโลยีสารสนเทศ คณะวิชาเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

[1, 2, 3, 4] Department of Information Technology, Faculty of Information Technology and Digital Technology,
King Mongkut's University of Technology North Bangkok

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่มีผลต่อการตระหนักรู้ถึงภัยคุกคามทางด้านไซเบอร์ของนักศึกษามหาวิทยาลัยในประเทศไทย โดยได้ทำการเก็บรวบรวมข้อมูลด้วยแบบสอบถามออนไลน์แบบลิเคิร์ท 5 ระดับ ระหว่างเดือนเมษายนถึงเดือนพฤษภาคม 2565 จากนักศึกษามหาวิทยาลัยในประเทศไทย ระดับอนุปริญญาและระดับปริญญา จำนวนทั้งหมด 422 คน และวิเคราะห์ข้อมูลด้วยค่าร้อยละ ค่าความถี่สะสม ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และสมการถดถอยเชิงเส้นพหุคูณแบบ Stepwise ด้วยโปรแกรม SPSS ผลการวิจัยพบว่า มี 3 จาก 5 ปัจจัยหลักที่ส่งต่อการตระหนักรู้ถึงภัยคุกคามทางด้านไซเบอร์ของนักศึกษามหาวิทยาลัย ได้แก่ ความรู้ความเข้าใจในเรื่องภัยคุกคามทางไซเบอร์ ความปลอดภัยของอุปกรณ์และการเชื่อมต่อและพฤติกรรมของผู้ใช้งาน ณ ระดับนัยสำคัญทางสถิติที่ระดับ 0.05

คำสำคัญ: การตระหนักรู้ความปลอดภัยทางไซเบอร์ ภัยคุกคามทางด้านไซเบอร์ ปัจจัยที่ส่งผล

Abstract

The purpose of this research was to study the factors affecting university students' cybersecurity awareness in Thailand. Data were collected using online 5-point Likert scale questionnaires during April-May 2022 from 422 university students in Thailand including diplomas, bachelor's degrees, master's degrees, doctorate degrees. Data also were analyzed using percentage, cumulative frequency, mean, standard deviation, and stepwise multiple linear regression by SPSS program. The results showed that there were 3 out of 5 factors influencing university students' cybersecurity awareness, i.e., knowledge and understandings of cyber threats, device security and connectivity, and user behavior at a statistical significance level of 0.05.

Keywords: Cybersecurity Awareness, Cyber Threat, Influential Factor

** Corresponding author : s6407011857031@email.kmutnb.ac.th*

1. บทนำ

จากความก้าวหน้าทางเทคโนโลยีสารสนเทศที่ถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือการติดต่อสื่อสารจึงก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็วและทวีความรุนแรงมากขึ้นสร้างความเสียหายทั้งในระดับบุคคล ระดับองค์กรไปจนถึงระดับประเทศ การโจมตีทางไซเบอร์มีปริมาณเพิ่มมากขึ้นเรื่อย ๆ โดยคาดว่าน่าจะเพิ่มขึ้นถึง ร้อยละ 400 ตามรายงานในปี ค.ศ. 2022 และพบว่ามีการโจมตีแบบ Phishing และ Social Engineering ถึง 30,000 ครั้งต่อวัน ตามรายงานของบริษัท Microsoft และยังพบว่ามีการเพิ่มของ Ransomware Attacks ถึงร้อยละ 800 (Prospace, 2022) จากข้อมูลระหว่างเดือน มกราคม 2564 - กุมภาพันธ์ 2565 หน่วยงานในประเทศไทยถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ถึง 15 ครั้งด้วยกัน สูงเป็นอันดับ 6 ของเอเชียแปซิฟิกและญี่ปุ่น อุตสาหกรรมที่ถูกโจมตีสูงสุด ได้แก่อุตสาหกรรมด้านบริการเชิงพาณิชย์ และรองลงมาเป็นอุตสาหกรรมซอฟต์แวร์และบริการ ซึ่งถูกโจมตีด้วยมัลแวร์ Locbit 2.0 Ransomware สูงที่สุดถึง 9 ครั้ง โดย Ransomware นี้แฮ็กเกอร์สามารถปรับแต่งรูปแบบการโจมตีได้ตามความต้องการ (ThaiPublica, 2022) เห็นได้ชัดว่าการโจมตีทางไซเบอร์มีความรุนแรงมากขึ้น ซึ่งสิ่งที่ต้องระมัดระวังอย่างมาก คือ การโจรกรรมข้อมูลซึ่งข้อมูลที่รั่วไหลออกไปสามารถนำไปสู่การหลอกลวงออนไลน์รวมไปถึงการรั่วไหลของข้อมูลที่อ่อนไหว เช่นข้อมูลส่วนบุคคล และข้อมูลสุขภาพ เป็นต้น จากเหตุผลดังกล่าวทางผู้วิจัยจึงได้ศึกษาปัจจัยที่ส่งผลต่อการตระหนักรู้ถึงความปลอดภัยทางไซเบอร์ของนักศึกษามหาวิทยาลัย ซึ่งผลของการศึกษานี้สามารถนำไปต่อยอดในการส่งเสริมการรู้เท่าทันภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ เพื่อป้องกันภัยที่อาจเกิดขึ้นได้ในอนาคต

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

จากการทบทวนวรรณกรรม พบว่า มี 5 ปัจจัยที่ส่งผลต่อการตระหนักรู้ถึงความปลอดภัยทางไซเบอร์ ดังนี้

การตั้งรหัสผ่าน (X1) รหัสผ่านเป็นปราการด่านแรกในการป้องกันบัญชีการใช้งานของผู้ใช้ โดยเฉพาะอย่างยิ่ง รหัสผ่านที่มีความซับซ้อนมาก ๆ เพราะถึงแม้จะมีการอนุญาตการเข้าใช้งานรูปแบบอื่น ๆ แต่การเข้าใช้งานด้วยชื่อบัญชีผู้ใช้ร่วมกับรหัสผ่านก็ยังได้รับความนิยมอยู่ (Alqahtani, 2022; Butavicius et al., 2020; Garba et al., 2020; Gratian et al., 2018; Kovačević et al., 2020; Lesjak et al., 2019; Tirumala et al., 2019; Zwilling et al., 2022)

ความรู้ความเข้าใจในเรื่องภัยคุกคามทางไซเบอร์ (X2) การอบรมหรือการศึกษาด้วยตนเองด้านความมั่นคงปลอดภัยในการใช้ทรัพยากรสารสนเทศนั้น เป็นการรับความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ที่อาจเกิดขึ้น เพื่อให้สามารถลดผลกระทบจากภัยคุกคามได้ รวมทั้งยังส่งเสริมวัฒนธรรมการรักษาความปลอดภัย(Alqahtani, 2022; Garba et al., 2020; Gratian et al., 2018; Holdsworth & Apeh, 2017; Kovačević et al., 2020; Lesjak et al., 2019; Tirumala et al., 2019; Zwilling et al., 2022)

ความปลอดภัยของอุปกรณ์และการเชื่อมต่อ (X3) การสำรองข้อมูลบ่อย ๆ หรือการจัดเก็บข้อมูลบนคลาวด์จะทำให้สามารถกู้คืนข้อมูลและทำให้อุปกรณ์กลับมาใช้งานได้อย่างรวดเร็วหลังจากการถูกคุกคามทางไซเบอร์ และการระมัดระวังไม่เชื่อมต่อกับเครือข่ายที่ไม่ปลอดภัยก็จะช่วยลดปัญหาการถูกโจมตีทางไซเบอร์ได้เช่นกัน(Alotaibi, 2019; Ani et al., 2019; Butavicius et al., 2020; Holdsworth & Apeh, 2017; Kovačević et al., 2020)

การใช้และดูแลแอปพลิเคชัน (X4) การอัพเดตระบบปฏิบัติการ แอปพลิเคชัน และ anti-virus เพื่อแก้ไขช่องโหว่ความปลอดภัย แก้ไขข้อบกพร่องของตัวโปรแกรม และเพิ่มคุณสมบัติความสามารถใหม่ ๆ ในทุกครั้งที่มีการแจ้งเตือน หรือการตั้งอัพเดตแบบอัตโนมัติช่วยให้มีความปลอดภัยจากภัยคุกคามทางด้านไซเบอร์(Alqahtani, 2022; Alzubaidi, 2021; Ani et al., 2019; Butavicius et al., 2020; Garba et al., 2020; Holdsworth & Apeh, 2017)

พฤติกรรมของผู้ใช้งาน (X5) การตรวจสอบที่มาของเว็บไซต์ (เช่น ตรวจสอบ URL) ก่อนเข้าใช้งาน การระมัดระวังในการเปิดไฟล์แนบในอีเมล รวมทั้งการไม่ตั้งค่าการโพสต์ข้อมูลส่วนตัวแบบสาธารณะ จะช่วยเพิ่มความปลอดภัยจาก ภัยคุกคามทางไซเบอร์

(Alqahtani, 2022; Ani et al., 2019; Garba et al., 2020; Holdsworth & Apeh, 2017; Kovačević et al., 2020; Tirumala et al., 2019; Zwilling et al., 2022)

3. วิธีดำเนินการวิจัย

3.1 ประชากรและกลุ่มตัวอย่าง

ประชากร คือ นักศึกษามหาวิทยาลัยตั้งแต่ระดับ อนุปริญญา (ปวช. และ ปวส.) รวมไปถึงระดับปริญญาตรี ปริญญาโท และปริญญาเอก ในประเทศไทย จากข้อมูลในปี 2563 มีทั้งสิ้น 1,917,756 คน(สถิติการศึกษา, n.d.) กลุ่มตัวอย่าง คือ นักศึกษามหาวิทยาลัย จากสูตรของเครจซี่และมอร์แกน กำหนดความคลาดเคลื่อนที่ร้อยละ 5 ที่ระดับความเชื่อมั่นร้อยละ 95 และสัดส่วนประชากรเท่ากับ 0.5 คำนวณขนาดตัวอย่างได้จำนวน 385 คน ทั้งนี้ใช้การสุ่มตัวอย่างแบบสโนว์บอล ระหว่างเดือนเมษายนถึงเดือนพฤษภาคม 2565 โดยมีจำนวนผู้ตอบแบบสอบถามรวมทั้งสิ้น 422 คน

3.2 ตัวแปรที่ใช้ในการวิจัย

ตัวแปรต้น คือ 5 ปัจจัยที่ส่งผลต่อการตระหนักรู้ถึงความปลอดภัยทางไซเบอร์ (X1 – X5) และตัวแปรตาม คือ การตระหนักรู้ถึงความปลอดภัยทางไซเบอร์ของนักศึกษามหาวิทยาลัยในประเทศไทย

3.3 เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการศึกษาวิจัยครั้งนี้ คือ แบบสอบถามออนไลน์แบบลิเคิร์ท 5 ระดับที่ผ่านการประเมินความเที่ยงตรงด้วยค่าความสอดคล้อง IOC โดยผู้เชี่ยวชาญจำนวน 3 ท่าน พบว่า ทุกข้อคำถามมีความสอดคล้องกับวัตถุประสงค์ของงานวิจัย และผลการตรวจสอบความเชื่อมั่นของครอนบัค (Cronbach Alpha) ทั้งฉบับมีค่าเท่ากับ 0.75

แบบสอบถามแบ่งเป็น 3 ตอน ได้แก่ ตอนที่ 1 ข้อมูลปัจจัยประชากรศาสตร์ของผู้ตอบแบบสอบถาม ตอนที่ 2 พฤติกรรมการใช้คอมพิวเตอร์ อินเทอร์เน็ตและความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ และตอนที่ 3 ความคิดเห็นต่อปัจจัยที่ส่งผลต่อการตระหนักรู้ถึงความปลอดภัยทางไซเบอร์ของนักศึกษามหาวิทยาลัยในประเทศไทย

4. ผลการดำเนินงานวิจัย

4.1 ผลการวิเคราะห์ข้อมูลส่วนบุคคล

จากผู้ที่ตอบแบบสอบถามทั้งหมดจำนวน 422 คน มีผู้ตอบแบบสอบถามเป็นเพศชาย 240 คนคิดเป็นร้อยละ 57.8 มากกว่าเพศหญิงที่ 178 คนคิดเป็นร้อยละ 42.2 อยู่เล็กน้อย ส่วนใหญ่อยู่ในช่วงวัย 21-30 ปีถึงร้อยละ 56.9 และรองลงมาเป็นช่วงวัยต่ำกว่า 20 ปี ร้อยละ 35.3 สำหรับการจำแนกตามระดับการศึกษา เป็นระดับปริญญาตรีสูงถึง ร้อยละ 63.5 ตามมาด้วยระดับ ปวส. ที่ร้อยละ 19.7 และในระดับอื่น ๆ ไม่เกินระดับละร้อยละ 10

4.2 ผลการวิเคราะห์ข้อมูลการใช้งานอินเทอร์เน็ต

ผู้วิจัยได้ออกแบบคำถามจำนวน 19 ข้อ โดยแบ่งเป็น 5 ปัจจัยคือ ความรู้เรื่องภัยคุกคามทางไซเบอร์ 3 ข้อ พฤติกรรมการใช้งานอินเทอร์เน็ต 2 ข้อ การใช้รหัสผ่าน 4 ข้อ ความปลอดภัยของอุปกรณ์และการเชื่อมต่อ 8 ข้อ และการใช้และดูแลแอปพลิเคชัน 2 ข้อ ต่อข้อถามเกี่ยวกับปัจจัยความรู้เรื่องภัยคุกคามทางไซเบอร์ ผู้ตอบแบบสอบถามส่วนใหญ่รู้จักคอมพิวเตอร์ไวรัสสูงที่สุดร้อยละ 82.2 ตามด้วย มัลแวร์ สปายแวร์ ร้อยละ 61.4 และ 51.9 ตามลำดับ โดยเฉลี่ยแล้วผู้ตอบแบบสอบถามรู้จักภัยคุกคามเฉลี่ย 3.42 ชนิดต่อคน มีผู้ที่เคยได้รับการอบรมหรือศึกษาด้วยตนเองทางด้านความปลอดภัยทางไซเบอร์ร้อยละ 41.9 โดยมีสัดส่วนเพศชายสูงกว่าเพศหญิง ผู้อยู่ในช่วงวัยที่สูงกว่า 30 ปีมีสัดส่วนสูงกว่าผู้ที่มีอายุต่ำกว่าและผู้ที่มีการศึกษาสูงมีสัดส่วนการมีความรู้ด้านนี้สูงกว่าผู้ที่มีระดับการศึกษาที่ต่ำกว่าเป็นลำดับขั้นไป พบว่ามีผู้ตอบแบบสอบถามถึงร้อยละ 51.4 ที่ไม่ทราบเกี่ยวกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์

สำหรับปัจจัยพฤติกรรมการใช้งานอินเทอร์เน็ต มีผู้ตั้งค่าการโพสต์บนโซเชียลมีเดียเป็นสาธารณะร้อยละ 24.6 และมีผู้ที่มักเปิดไฟล์แนบในอีเมล์ที่ได้รับจากบุคคลที่ไม่รู้จัก ร้อยละ 19.4 สำหรับคำถามปัจจัยการใช้รหัสผ่านมีผู้ตั้งรหัสผ่านให้สอดคล้องกับข้อมูลส่วนบุคคลร้อยละ 63.27 ผู้ที่ตั้งรหัสผ่านให้มีความยาวไม่ต่ำกว่า 8 ตัวอักษร ประกอบด้วยตัวอักษร ตัวเลขและอักขระพิเศษสูงถึงร้อยละ 81.8 ผู้ที่ใช้ 2-factor authentication ในการยืนยันตัวตนร้อยละ 82.46 และร้อยละ 70.6 ของผู้ตอบแบบสอบถามมีการตั้งรหัสผ่านสำหรับแต่ละแอปพลิเคชันเหมือน ๆ กัน ต่อข้อถามเกี่ยวกับปัจจัยความปลอดภัยของอุปกรณ์และการเชื่อมต่อ พบว่ามีกลุ่มที่มีความเสี่ยงสูงจากการใช้สมาร์ทโฟนเป็นอุปกรณ์หลักในการใช้งานอีเมล์ถึงร้อยละ 32.9 มีผู้ที่เคยใช้คอมพิวเตอร์สาธารณะสูงถึงร้อยละ 75.4 แต่พบว่าส่วนใหญ่มีการปฏิบัติที่ถูกต้องหลังเลิกใช้งาน เช่นการล็อคเอาท์ การลบประวัติการใช้งาน เป็นต้น ผู้ตอบคำถามร้อยละ 34.1 อนุญาตให้แอปพลิเคชัน ใช้งานกล้อง หรือการระบุตำแหน่งตลอดเวลา และผู้ตอบแบบสอบถามส่วนใหญ่ร้อยละ 73 ตระหนักถึงความไม่ปลอดภัยของการใช้ Wi-Fi สาธารณะ

ปัจจัยการใช้และดูแลแอปพลิเคชัน มีเพียงร้อยละ 57.1 ที่มีการตั้งค่าการปรับปรุงแอปพลิเคชันแบบอัตโนมัติและมีเพียงร้อยละ 67 ที่ได้ทำการสำรองข้อมูลไว้เป็นประจำบนอุปกรณ์ภายนอกอื่นหรือบนคลาวด์

4.3 ผลการวิเคราะห์ปัจจัยที่มีอิทธิพลต่อการตระหนักรู้ความปลอดภัยทางไซเบอร์

จากการวิเคราะห์เบื้องต้นด้วยสถิติเชิงพรรณนา พบว่าปัจจัยแต่ละตัวมีคะแนนเฉลี่ยในช่วง 3.51-4.50 ในทุก ๆ ด้าน สรุปได้ว่าผู้ตอบแบบสอบถาม “เห็นด้วย” กับปัจจัยต่าง ๆ และการตระหนักรู้ภัยคุกคามทางไซเบอร์

จากการวิเคราะห์ข้อมูลด้วยสมการถดถอยเชิงเส้นพหุคูณวิธี Stepwise พบว่ามีเฉพาะปัจจัยด้าน ความรู้ความเข้าใจในเรื่องภัยคุกคามทางไซเบอร์ (X2) ความปลอดภัยของอุปกรณ์และการเชื่อมต่อ (X3) และพฤติกรรมของผู้ใช้งาน (X5) เท่านั้นที่มีอิทธิพลต่อการตระหนักรู้ความปลอดภัยทางไซเบอร์ ที่ระดับนัยยะสำคัญทางสถิติ 0.05 ซึ่งปัจจัยที่ไม่มีอิทธิพลคือ การตั้งรหัสผ่าน (X1) และการใช้และดูแลแอปพลิเคชัน (X4) ได้ถูกตัดทิ้งไปและได้ผลวิเคราะห์ดังตารางที่ 1

ตารางที่ 1 ผลการวิเคราะห์การถดถอยพหุคูณวิธี stepwise

	Unstandardized Coefficients		Standardized Coefficients	t	P-Value
	B	Std. Error	Beta		
(Constant)	1.60	.19	.00	8.57	.000
X2	.24	.04	.28	6.38	.000
X3	.09	.04	.11	2.41	.016
X5	.34	.04	.36	8.19	.000

5. สรุปผลและอภิปรายผล

ปัจจัยที่มีอิทธิพลต่อการตระหนักรู้ความปลอดภัยทางไซเบอร์จากการเก็บข้อมูลตัวอย่างจากนักศึกษาตั้งแต่ระดับ ปวช. ปวส. ปริญญาตรี ปริญญาโท และ ปริญญาเอก ในมหาวิทยาลัย จากปัจจัยที่ตั้งสมมติฐานไว้ 5 ปัจจัย พบว่ามี 3 ปัจจัยที่ส่งผลทางบวก ได้แก่ ปัจจัยความรู้ความเข้าใจในเรื่องภัยคุกคามทางไซเบอร์ ปัจจัยความปลอดภัยของอุปกรณ์และการเชื่อมต่อและปัจจัยพฤติกรรมของผู้ใช้งาน และมี 2 ปัจจัยที่ไม่ส่งผล ได้แก่ปัจจัยการตั้งรหัสผ่าน และปัจจัยการใช้และดูแลแอปพลิเคชัน ซึ่งการทราบถึงปัจจัยที่มีอิทธิพลรวมทั้งโมเดลที่ได้ สามารถนำไปใช้ในการ พยากรณ์โอกาสในการถูกโจมตีทางไซเบอร์ได้ และทำให้ทราบว่าการป้องกันการถูกโจมตีทางไซเบอร์ที่ดีที่สุดก็คือการให้ความรู้ความเข้าใจในการใช้งานอินเตอร์เน็ต เพื่อให้ผู้ใช้รู้เท่าทันภัยคุกคามรูปแบบต่างๆ การสำรองข้อมูลรวมทั้งการหลีกเลี่ยงพฤติกรรมที่ไม่พึงประสงค์ จะทำให้ผู้ใช้ลดโอกาสจากการถูกโจมตีทางไซเบอร์ได้ ทั้งนี้สอดคล้องกับ(Alqahtani, 2022) ที่กล่าวว่าสถาบันการศึกษาควรให้นักศึกษาได้รับการอบรมที่มีประสิทธิภาพเพื่อให้มีพฤติกรรมการใช้งานอินเตอร์เน็ตที่พึง

ประสงค์ ทั้งนี้ในการศึกษายังพบด้วยว่าเพศหญิงและเพศชายมีการตระหนักรู้ภัยคุกคามทางไซเบอร์ไม่แตกต่างกัน แต่ผู้ที่มีอายุต่างกันและผู้ที่อยู่ในระดับการศึกษาที่ต่างกันมีการตระหนักรู้ต่างกันอย่างน้อย 1 ด้าน

6. ข้อเสนอแนะ

ผลการวิจัยครั้งนี้พบว่าค่าสัมประสิทธิ์แสดงการตัดสินใจเชิงซ้อน (Coefficient of Multiple Determination) หรือ R^2 = 0.35 ซึ่งมีค่าค่อนข้างต่ำ ในการวิจัยในอนาคตควรเพิ่มจำนวนตัวแปรต้น และจำนวนคำถามในแต่ละตัวแปรต้นให้มากขึ้น

7. เอกสารอ้างอิง

สำนักงานสถิติแห่งชาติ. (ม.ป.ป.) *สถิติการศึกษา*. สืบค้น 12 กรกฎาคม 2565, จาก http://statbbi.nso.go.th/staticreport/page/sector/th/03.aspx

Alotaibi, F. F. G. (2019). *Evaluation and Enhancement of Public Cyber Security Awareness* (Thesis). University of Plymouth. Retrieved from https://pearl.plymouth.ac.uk/handle/10026.1/14209

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*, *12*(5), 2589. https://doi.org/10.3390/app12052589

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., & Calic, D. (2020). When believing in technology leads to poor cyber security: Development of a trust in technical controls scale. *Computers & Security*, *98*, 102020. https://doi.org/10.1016/j.cose.2020.102020

Garba, A., Siraj, M., Alhaji Musa, M., & Othman, S. (2020). *A Study on Cybersecurity Awareness Among Students in Yobe: A Quantitative Approach*. 41–49.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). *Correlating human traits and cyber security behavior intentions. Computers & Security, 73,* 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Holdsworth, J., & Apeh, E. (2017). An Effective Immersive Cyber Security Awareness Learning Platform for Businesses in the Hospitality Sector. *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)*, 111–117. https://doi.org/10.1109/REW.2017.47

Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access, 8, 125140–125148.* https://doi.org/10.1109/ACCESS.2020.3007867

Lesjak, D., Zwilling, M., & Klein, G. (2019). *CYBER CRIME AND CYBER SECURITY AWARENESS AMONG STUDENTS: A COMPARATIVE STUDY IN ISRAEL AND SLOVENIA*.

ProSpace. Cyber threat 5 ภัยคุกคามทางไซเบอร์ ที่ธุรกิจต้องเผชิญหลังโรคระบาด. (2022). สืบค้น 13 กุมภาพันธ์ 2565, จาก https://prospace.services/cybersecurity-threats-business-2021/

ThaiPublica. รายงานเผยทั่วโลกทุบสถิติจ่ายค่าไถ่ให้มัลแวร์ ปี'64 ไทยโดนโจมตีติดอับดับ 6 เอเชียแปซิฟิค (2022). สืบค้น 20 เมษายน 2565, จาก https://thaipublica.org/2022/04/paloalto-unit-42-ransomware-threat-2022-report/

Tirumala, S. S., Valluri, M. R., & Babu, G. (2019). A survey on cybersecurity awareness concerns, practices and conceptual measures. *2019 International Conference on Computer Communication and Informatics (ICCCI)*, 1–6. https://doi.org/10.1109/ICCCI.2019.8821951

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Çetin, F., & Basım, N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*, 82–97. https://doi.org/10.1080/08874417.2020.1712269