การประชุมเสนอผลงานวิจัยระดับชาติ มหาวิทยาลัยสุโขทัยธรรมาธิราช ครั้งที่ 14
The 14th STOU National Research Conference

SAM เพื่อเข้าใจปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทางการศึกษา: กรณีศึกษาวิทยาลัยเทคนิคกระบี่

SAM to Understand Factors Affecting Password Creation According to Cyber Security Practices of Academic Personnel: A Case Study of Krabi Technical College

สุจิรา จีนหนู (MissSujira Jeennoo)[1] พิทา จารุพูนผล (Pita Jarupunphol)[2]
วิภาวรรณ บัวทอง (Wipawan Buathong)[3] ณสิทธิ์ เหล่าเสน (Nasith Laosen)[4]

บทคัดย่อ

การศึกษานี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยและความสัมพันธ์ของปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทางการศึกษาในวิทยาลัยเทคนิคกระบี่ ด้วยการใช้โมเดลการยอมรับแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ ที่ประยุกต์มาจากโมเดลการยอมรับเทคโนโลยี โดยทำการเก็บข้อมูลจากกลุ่มตัวอย่างที่เลือกแบบเจาะจง จำนวน 175 คน ใช้แบบสอบถามเป็นเครื่องมือในการเก็บข้อมูล พบว่าผู้ตอบแบบสอบถามส่วนใหญ่อยู่ในช่วงอายุ 26-30 ปี คิดเป็นร้อยละ 13.8 และร้อยละ 16.7 มีอายุมากกว่า 50 ปี แนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ที่มีการใช้งานมากที่สุดคือการใช้รหัสผ่านที่ปลอดภัย คิดเป็นร้อยละ 25.7 รองลงมาคือการใช้การพิสูจน์ตัวตนหลายปัจจัย คิดเป็นร้อยละ 18.3 โดยมีค่าสัมประสิทธิ์ความเชื่อมั่นของชุดคำถามที่ใช้วัดปัจจัยต่าง ๆ ด้วย Cronbach อยู่ที่ 0.907 ในด้านการวิเคราะห์โมเดลสมการโครงสร้างด้วยวิธีการวิเคราะห์เส้นทางชี้ให้เห็นถึงความสัมพันธ์ของตัวแปรสำคัญที่เกี่ยวข้องกับการปฏิบัติด้านความปลอดภัยทางข้อมูล เช่น การรับรู้ถึงประโยชน์ต่อแนวปฏิบัติด้านความมั่นคงของรหัสผ่าน (PUSP) ส่งผลต่อทัศนคติต่อแนวปฏิบัติด้านความมั่นคงของรหัสผ่าน (ATS) ที่ 0.68 โดยเฉพาะอย่างยิ่ง ความตั้งใจที่จะใช้แนวปฏิบัติด้านความมั่นคงของรหัสผ่าน (ITSP) ส่งผลต่อพฤติกรรมการใช้แนวปฏิบัติด้านความมั่นคงของรหัสผ่าน (SPU) ที่ 0.83 ซึ่งผลที่ได้นอกจากยืนยันความถูกต้องของโครงสร้างโมเดลการยอมรับเทคโนโลยีแล้ว ยังชี้ให้เห็นว่าบุคลากรทางการศึกษามีความตั้งใจสูงในการปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ถ้าเห็นถึงประโยชน์ต่อแนวปฏิบัติ และมีการตระหนักถึงความสำคัญของการใช้งานแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์อย่างชัดเจน

คำสำคัญ แนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ การใช้รหัสผ่าน บุคลากรทางการศึกษา ความตั้งใจในการใช้งาน วิทยาลัยเทคนิคกระบี่

[1] สุจิรา จีนหนู นศ.หลักสูตร วิทยาศาสตร์และเทคโนโลยี สาขาวิชาเทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏภูเก็ต
e-mail: s6581423104@pkru.ac.th
[2] รองศาสตราจารย์ ดร. พิทา จารุพูนผล คณะวิทยาศาสตร์และเทคโนโลยี สาขาวิชาเทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏภูเก็ต
e-mail: p.jarupunphol@pkru.ac.th
[3] ผู้ช่วยศาสตราจารย์ ดร. วิภาวรรณ บัวทอง คณะวิทยาศาสตร์และเทคโนโลยี สาขาวิชาเทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏภูเก็ต
e-mail: w.buathong@pkru.ac.th
[4] อ.ดร.ณสิทธิ์ เหล่าเส็น คณะวิทยาศาสตร์และเทคโนโลยี สาขาวิชาเทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏภูเก็ต
e-mail: nasith@pkru.ac.th

Abstract

This study aims to analyze the factors influencing the adoption of security practices among educational personnel at Krabi Technical College by utilizing the Security Acceptance Model (SAM), adapted from the Technology Acceptance Model (TAM). Data was collected from a purposive sampling of 175 participants using a questionnaire as the data collection tool. The results showed that most respondents were between 26 and 30, accounting for 13.8%, and 16.7% were over 50. The most adopted security practice was using secure passwords, accounting for 25.7%, followed by using multi-factor authentication at 18.3%. The reliability coefficient (Cronbach's alpha) for the questionnaire measuring various factors was 0.907. Critical relationships between variables related to security practices were revealed using path analysis in the structural equation modeling (SEM) analysis. For instance, the perceived usefulness of password security practices (PUSP) positively impacted attitudes toward password security practices (ATS), with a coefficient of 0.68. Notably, the intention to use password security practices (ITSP) significantly influenced actual password security practice usage (SPU), with a coefficient of 0.83. These findings confirm the validity of the Technology Acceptance Model structure and highlight that educational personnel demonstrate a solid intention to follow security practices when they perceive the benefits. Furthermore, the staff is aware of the importance of adhering to security practices.

Keywords: Security practices, Password usage, Educational personnel, Intention to use, Krabi Technical College

บทนำ

ในยุคดิจิทัลปัจจุบัน การจัดการกับภัยคุกคามทางไซเบอร์มีความสำคัญมากขึ้นตามที่เทคโนโลยีทันสมัยพัฒนาไป เนื่องจากหน่วยงานภาครัฐมักเป็นเป้าหมายหลักในการโจมตีทางไซเบอร์ Hossain et al. (2024) กล่าวว่าภัยคุกคามเหล่านี้มาจากการโจมตีเพื่อหลอกลวงประชาชนโดยอาศัยความน่าเชื่อถือของหน่วยงานรัฐ หรือเพื่อทำลายความน่าเชื่อถือนั้น ผู้ไม่หวังดีเหล่านี้อาจมีเจตนาหลากหลาย เช่น แสดงพลังต่อต้านนโยบายของรัฐบาล ทำลายชื่อเสียง ก่อกวน หรือแม้กระทั่งทดสอบความสามารถของตนเอง ด้วยการเข้าถึงเครื่องมือการโจมตีทางไซเบอร์ที่ง่ายขึ้นผ่านอินเทอร์เน็ตและเว็บไซต์ต่างๆ ทำให้แฮกเกอร์มือใหม่สามารถเข้าสู่แวดวงนี้ได้ง่ายขึ้น (Bridges et al., 2023) ดังนั้น รัฐบาลจึงจำเป็นต้องให้ความสำคัญกับความมั่นคงปลอดภัยไซเบอร์ โดยมีการประกาศใช้พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งผ่านการทำประชาพิจารณ์เพื่อรับฟังมุมมองที่เป็นประโยชน์และได้รับการยอมรับจากภาคเอกชนและประชาชน ความตระหนักรู้และการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานเป็นสิ่งสำคัญ โดยเฉพาะอย่างยิ่งสำหรับบุคลากรของหน่วยงานภาครัฐ ดังนั้น การติดตามสถานการณ์ความมั่นคงปลอดภัยไซเบอร์เป็นสิ่งจำเป็น เพื่อช่วยให้สามารถเตรียมพร้อมรับมือกับภัยคุกคามใหม่ๆ ได้อย่างทันท่วงที (Hossain et al., 2024).

ในขณะที่รหัสผ่านคือแนวป้องกันด่านแรกในความมั่นคงปลอดภัยไซเบอร์ รหัสผ่านที่รัดกุมไม่ได้เป็นเพียงคำแนะนำแต่กลายเป็นสิ่งจำเป็นเมื่อชีวิตเข้าสู่โลกออนไลน์มากขึ้น โดยเฉพาะอย่างยิ่ง ในสถานการณ์ที่มีการละเมิดข้อมูลและภัยคุกคามทางไซเบอร์แพร่หลาย รหัสผ่านที่รัดกุมถือเป็นลักษณะพื้นฐานของความมั่นคงปลอดภัยไซเบอร์ในยุคปัจจุบันและมีความสำคัญในการปกป้องตัวตนบนโลกออนไลน์ ความเข้มแข็งและความปลอดภัยของรหัสผ่านจึงเป็นสิ่งสำคัญยิ่ง ซึ่งรหัสผ่านที่แข็งแกร่งสามารถป้องกันภัยคุกคามทางไซเบอร์ เนื่องจากหน้าที่หลักของรหัสผ่านที่รัดกุมคือการป้องกันการเข้าถึงข้อมูลส่วนบุคคลและข้อมูลทางอาชีพโดยไม่ได้รับอนุญาต ภัยคุกคามทางไซเบอร์ เช่น การแฮก พิชชิ่ง และการขโมยข้อมูลระบุตัวตนนั้นมีอยู่อย่างแพร่หลาย และรหัสผ่านที่ไม่รัดกุมมักเป็นทางเข้าที่ง่ายที่สุดสำหรับอาชญากรไซเบอร์ รหัสผ่านที่รัดกุมทำหน้าที่เป็นด่านแรกในการป้องกันการโจมตีทางดิจิทัลเหล่านี้ รวมถึงการปกป้องข้อมูลส่วนบุคคลและข้อมูลที่ละเอียดอ่อน เนื่องจากการเพิ่มขึ้นของธนาคารออนไลน์ การชอปปิ้ง และโซเชียลเน็ตเวิร์ก ข้อมูลส่วนบุคคลที่ละเอียดอ่อนจำนวนมากจึงถูกจัดเก็บไว้ทางออนไลน์ รหัสผ่านที่รัดกุมช่วยให้แน่ใจว่าข้อมูลนี้ปลอดภัยจากการละเมิด ปกป้องผู้ใช้จากการสูญเสียทางการเงินที่อาจเกิดขึ้น การบุกรุกความเป็นส่วนตัว และการขโมยข้อมูลส่วนตัว

วิทยาลัยเทคนิคกระบี่ ก่อตั้งขึ้นเมื่อวันที่ 10 มกราคม พ.ศ. 2523 และเปิดการเรียนการสอนครั้งแรกเมื่อวันที่ 17 พฤษภาคม พ.ศ. 2525 โดยเปิดสอน 2 แผนกวิชา คือ ช่างก่อสร้าง และช่างยนต์ ต่อมาวิทยาลัยเทคนิคกระบี่ ได้ขยายแผนกวิชาและระดับการศึกษาให้มากขึ้น โดยในปี พ.ศ. 2558 ได้มีการเปิดสอนระดับปริญญาตรี สายเทคโนโลยีหรือสายปฏิบัติการ (ทล.บ.) หลักสูตรเทคโนโลยีบัณฑิต สาขาวิชาเทคโนโลยียานยนต์ และสาขาวิชาคอมพิวเตอร์ธุรกิจ โดยวิทยาลัยเทคนิคกระบี่มุ่งมั่นผลิตนักเรียน นักศึกษาที่มีความรู้ ความสามารถ มีทักษะวิชาชีพที่ดี มีจิตสาธารณะ สามารถนำความรู้ไปประกอบอาชีพและสร้างประโยชน์ให้กับสังคมได้ ในปัจจุบัน สถาบันการศึกษาตั้งแต่โรงเรียนไปจนถึงมหาวิทยาลัย ต่างตกเป็นเป้าหมายของภัยคุกคามทางไซเบอร์ต่างๆ มากขึ้น สภาพแวดล้อมที่เป็นเอกลักษณ์ของสถาบันเหล่านี้ ซึ่งมักมีลักษณะเป็นเครือข่ายแบบเปิดฐานผู้ใช้ที่กว้างขวาง และข้อมูลที่ละเอียดอ่อนจำนวนมาก ทำให้สถาบันเหล่านี้เสี่ยงต่อการโจมตีทางไซเบอร์เป็นพิเศษ (Khader et al., 2021) ดังนั้น งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษามาตรการป้องกันภัยคุกคามไซเบอร์ในวิทยาลัยเทคนิคกระบี่

โดยมุ่งเน้นไปที่ประเด็นสำคัญของการสร้างรหัสผ่านโดยเฉพาะ ความสำคัญของการศึกษาครั้งนี้อยู่ที่การมุ่งเน้นที่การทำความเข้าใจองค์ประกอบของมนุษย์ในความมั่นคงปลอดภัยไซเบอร์ โดยการตรวจสอบปัจจัยที่มีอิทธิพลต่อการสร้างรหัสผ่านของบุคลากรในวิทยาลัยเทคนิคกระบี่ โดยใช้รูปแบบการยอมรับความปลอดภัย (Security Acceptance Model: SAM) ซึ่งเป็นการประยุกต์รูปแบบจากโมเดลการยอมรับเทคโนโลยี (Technology Acceptance Model: TAM) ที่เป็นที่ยอมรับกันอย่างแพร่หลาย (Davis, 1989; 1993; Johnson, 2005; Jones et al., 2010) โดยการวิจัยมีเป้าหมายเพื่อให้ความกระจ่างในด้านพฤติกรรมและจิตวิทยาที่ขับเคลื่อนแนวทางปฏิบัติความมั่นคงปลอดภัยไซเบอร์ในสภาพแวดล้อมทางวิชาการ ความเข้าใจนี้มีความสำคัญอย่างยิ่งต่อการพัฒนานโยบายและโปรแกรมการฝึกอบรมความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพมากขึ้น (Al-Omari et al., 2012) ซึ่งสามารถนำไปสู่แนวทางปฏิบัติด้านความปลอดภัยไซเบอร์ที่แข็งแกร่งยิ่งขึ้น

วัตถุประสงค์

ปัญหาหลักที่งานวิจัยนี้ระบุคือการทำความเข้าใจปัจจัยเฉพาะที่มีอิทธิพลต่อพฤติกรรมการสร้างรหัสผ่านในสภาพแวดล้อมทางวิชาการ โดยทำความเข้าใจว่าปัจจัยเหล่านี้เกี่ยวข้องกับกรอบการทำงาน SAM อย่างไร และสำรวจประสิทธิผลของ SAM ในการทำนาย และปรับปรุงแนวทางปฏิบัติด้านความปลอดภัยของรหัสผ่านในวิทยาลัยเทคนิคกระบี่ ดังนั้น วัตถุประสงค์ของงานวิจัย มีดังนี้

1. เพื่อศึกษาปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทางการศึกษาในวิทยาลัยเทคนิคกระบี่
2. เพื่อศึกษาความสัมพันธ์ของปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทางการศึกษาในวิทยาลัยเทคนิคกระบี่

ระเบียบวิธีวิจัย

เนื่องจากงานวิจัยนี้มุ่งเน้นการศึกษาปัจจัยและความสัมพันธ์ของปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทางการศึกษาในวิทยาลัยเทคนิคกระบี่ ขั้นตอนต่อไปนี้คือวิธีการวิจัยที่นำมาใช้ในการศึกษา

การกำหนดกลุ่มตัวอย่าง

งานวิจัยนี้ใช้วิธีวิจัยเชิงปริมาณ (Quantitative Research) เพื่อทำความเข้าใจปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทางการศึกษาในวิทยาลัยเทคนิคกระบี่ โดยใช้โมเดล SAM (Security Awareness Model) เพื่อเป็นกรอบแนวคิดในการวิเคราะห์ โดยการเก็บข้อมูล ซึ่งประชากรคือบุคลากรทางการศึกษาในวิทยาลัยเทคนิคกระบี่ จำนวน 210 คน โดยกลุ่มตัวอย่างที่เลือกใช้มีการกำหนดเกณฑ์การคัดเลือกเพื่อให้ครอบคลุมถึงกลุ่มบุคลากรในตำแหน่งและบทบาทต่าง ๆ เช่น อาจารย์ ฝ่ายบริหาร เป็นต้น ทั้งนี้ การกำหนดขนาดตัวอย่างคำนวณโดยใช้การสุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) จำนวน 175 คน ตามสูตรของ Krejcie and Morgan (1970) โดยมีค่าความ

คลาดเคลื่อน 5% ซึ่งแนะนำให้ใช้ขนาดตัวอย่าง 132 คนจากประชากรทั้งหมด 200 คน ขนาดตัวอย่าง 175 จึงถือว่าเกินกว่าคำแนะนำนี้และส่งผลให้ได้ชุดข้อมูลที่มีความแข็งแกร่งและเชื่อถือได้

การออกแบบเครื่องมือเก็บข้อมูล

งานวิจัยนี้ใช้วิธีการวิจัยเชิงปริมาณ โดยเน้นการวิเคราะห์เชิงลึกและเชิงบริบทเกี่ยวกับแนวทางปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทางการศึกษาในวิทยาลัยเทคนิคกระบี่ เป็นการศึกษาที่มุ่งเน้นการรวบรวมและวิเคราะห์ข้อมูลเชิงปริมาณ โดยอาศัยวิธีการทางสถิติเพื่อหาความสัมพันธ์ระหว่างตัวแปรต่างๆ งานวิจัยนี้ใช้หลักการของ SAM ที่ประยุกต์จาก TAM เพื่อให้เข้ากับบริบททางความมั่นคงปลอดภัยไซเบอร์ สำหรับค้นหาปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวทางปฏิบัติความมั่นคงปลอดภัยไซเบอร์ ข้อมูลที่ใช้ในการศึกษาได้มาจากแบบสอบถามออนไลน์ที่ส่งไปยังผู้เข้าร่วม ซึ่งการเก็บข้อมูลครอบคลุมข้อมูลส่วนบุคคล เช่น อายุ เพศ ระดับการศึกษา และปัจจัยที่เกี่ยวข้องกับการสร้างรหัสผ่าน การวิเคราะห์ปัจจัยที่มีผลต่อการสร้างรหัสผ่านแนวทางปฏิบัติความมั่นคงปลอดภัยไซเบอร์นั้น เพื่อช่วยให้สามารถวิเคราะห์รูปแบบข้อมูลที่ซับซ้อนและสรุปผลได้ชัดเจน การวิเคราะห์ข้อมูลในงานวิจัยนี้ประกอบด้วยการใช้สถิติพื้นฐานและการใช้โมเดลสมการโครงสร้าง (Structural Equation Modelling: SEM) ตามทฤษฎีการยอมรับเทคโนโลยี TAM เพื่อให้ได้มุมมองเชิงลึกและคำตอบที่เชื่อถือได้ในการศึกษาเรื่องความมั่นคงปลอดภัยไซเบอร์ (Davis, 1989; 1993)

การรวบรวมข้อมูล

วิธีการรวบรวมข้อมูลที่เหมาะสมสำหรับการศึกษานี้คือการใช้แบบสอบถามออนไลน์ เนื่องจากสามารถเข้าถึงกลุ่มตัวอย่างได้จำนวนมากและรวบรวมข้อมูลได้หลากหลายด้านที่เกี่ยวข้องกับการสร้างรหัสผ่านที่ปลอดภัย การรวบรวมข้อมูลจะดำเนินการผ่านแบบสอบถามออนไลน์ ซึ่งมีการพัฒนาคำถามและรายการสำรวจอย่างรอบคอบ เพื่อให้สอดคล้องกับวัตถุประสงค์ของการวิจัย เริ่มต้นด้วยการอธิบายวัตถุประสงค์ของโครงการวิจัย ข้อมูลเกี่ยวกับแบบสอบถาม และการขอความยินยอมจากผู้เข้าร่วม หลังจากนั้นจึงเริ่มกระบวนการเก็บข้อมูล โดยตัวอย่างคำถามในแบบสอบถามออนไลน์จะใช้เพื่อรวบรวมข้อมูลเกี่ยวกับปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ในวิทยาลัยเทคนิคกระบี่ โดยไม่มีการเก็บข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ ผู้เข้าร่วมจะถูกถามเกี่ยวกับเงื่อนไขทางจิตวิทยาและพฤติกรรมที่เกี่ยวข้องกับการสร้างรหัสผ่าน โดยใช้มาตรวัด 7 ระดับจากการกำหนดวัตถุประสงค์ที่ชัดเจน เช่น การตรวจสอบปัจจัยที่มีอิทธิพลต่อการยอมรับการสร้างรหัสผ่านที่ปลอดภัยในบุคลากรของวิทยาลัย โดยใช้แบบจำลอง SAM ที่ปรับจาก TAM (Davis, 1989; 1993) หลังจากนั้นจะกำหนดสมมติฐานเพื่อทดสอบ โดยใช้คำถามที่เกี่ยวข้องกับปัจจัยต่างๆ เช่น การรับรู้ถึงความง่ายของแนวปฏิบัติด้านความมั่นคง (Perceived Ease of Security Practice: PESP) การรับรู้ถึงประโยชน์ของแนวปฏิบัติ (Perceived Usefulness of Security Practice: PUSP) ทัศนคติต่อแนวปฏิบัติ (Attitudes towards Security Practice: ATSP) ความตั้งใจที่จะใช้แนวปฏิบัติ (Intention to Use Security Practice: ITSP) และพฤติกรรมการใช้แนวปฏิบัติด้านความมั่นคง (Security Practice Usage: SPU) เพื่อศึกษาความสัมพันธ์ระหว่างปัจจัยเหล่านี้

การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลในงานวิจัยนี้เริ่มต้นด้วยการใช้สถิติพื้นฐานเพื่อตรวจสอบความน่าเชื่อถือและความถูกต้องของข้อมูลที่ได้จากการเก็บรวบรวม โดยมีการคำนวณค่าเฉลี่ย (Mean) เพื่อสะท้อนถึงแนวโน้มส่วนกลางของข้อมูล และการคำนวณส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) เพื่อตรวจสอบการกระจายตัวของข้อมูล จากนั้นจึงทำการวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรที่ศึกษา เพื่อให้เข้าใจถึงความสัมพันธ์เชิงเส้นระหว่างตัวแปรต่างๆ โดยการใช้การวิเคราะห์การถดถอยเชิงเส้น (Regression Analysis) หรือการวิเคราะห์เส้นทาง (Path Analysis) วัตถุประสงค์หลักของการวิเคราะห์นี้คือการตรวจสอบว่าตัวแปรสำคัญ เช่น การรับรู้ถึงความง่ายของแนวปฏิบัติด้านความมั่นคง (PESP) การรับรู้ถึงประโยชน์ของแนวปฏิบัติ (PUSP) ทัศนคติต่อแนวปฏิบัติ (ATSP) ความตั้งใจที่จะใช้แนวปฏิบัติ (ITSP) และพฤติกรรมการใช้แนวปฏิบัติด้านความมั่นคง (SPU) มีความสัมพันธ์กันอย่างไร ตัวอย่างเช่น การวิเคราะห์การถดถอยสามารถใช้เพื่อทำนายว่าการรับรู้ถึงความง่ายของแนวปฏิบัติมีผลต่อทัศนคติและความตั้งใจที่จะใช้แนวปฏิบัติหรือไม่ และในทางกลับกัน การวิเคราะห์เส้นทางช่วยให้สามารถศึกษาเส้นทางที่ตัวแปรเหล่านี้มีผลกระทบต่อกันในเชิงสาเหตุ หลังจากทำการวิเคราะห์แล้ว ผลลัพธ์จะถูกตีความเพื่อตอบคำถามวิจัย โดยผลที่ได้จากการวิเคราะห์จะช่วยให้เห็นถึงความเชื่อมโยงระหว่างตัวแปรและทิศทางของความสัมพันธ์ระหว่างปัจจัยต่างๆ เช่น หากพบว่าการรับรู้ถึงความง่ายของแนวปฏิบัติมีอิทธิพลอย่างมากต่อทัศนคติและพฤติกรรมการใช้แนวปฏิบัติ จะสามารถสรุปได้ว่าแนวทางความมั่นคงที่ถูกออกแบบให้ใช้งานง่ายจะเพิ่มความน่าจะเป็นในการยอมรับและนำไปปฏิบัติจริงในชีวิตประจำวัน

ข้อพิจารณาทางจริยธรรม

กระบวนการอนุมัติด้านจริยธรรมในการวิจัยเป็นขั้นตอนที่สำคัญอย่างยิ่งในการรับรองว่าการศึกษาจะดำเนินการอย่างมีความรับผิดชอบและให้ความเคารพต่อสิทธิของผู้เข้าร่วม โดยเฉพาะอย่างยิ่งในการศึกษาที่เกี่ยวข้องกับการประเมินความเสี่ยงและผลประโยชน์ที่อาจเกิดขึ้น รวมถึงการพิจารณาถึงอันตรายหรือความไม่สบายใจที่ผู้เข้าร่วมอาจประสบ และการวางแผนวิธีการบรรเทาปัญหาเหล่านั้น ในกรณีของการศึกษาปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวทางปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในวิทยาลัยเทคนิคกระบี่ การได้รับการอนุมัติด้านจริยธรรมจึงเป็นสิ่งสำคัญ เพื่อให้แน่ใจว่าการวิจัยจะส่งผลประโยชน์และไม่ก่อให้เกิดอันตรายแก่ผู้เข้าร่วม โดยการขออนุมัติด้านจริยธรรมในงานวิจัยนี้ช่วยรับประกันว่าการศึกษาจะดำเนินการอย่างมีความรับผิดชอบ ปกป้องสิทธิและความรู้สึกของผู้เข้าร่วม ตลอดจนรักษาความน่าเชื่อถือของผลการวิจัยได้อย่างมีประสิทธิภาพ งานวิจัยเรื่อง “SAM เพื่อเข้าใจปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทางการศึกษา: กรณีศึกษาวิทยาลัยเทคนิคกระบี่” ได้รับการอนุมัติจากคณะกรรมการพิจารณาจริยธรรมการวิจัยในมนุษย์ มหาวิทยาลัยราชภัฏภูเก็ต เมื่อวันที่ 29 เมษายน 2567 หมายเลขใบรับรอง PKRU2567/07 โดยการอนุมัติครอบคลุมตั้งแต่วันที่ 29 เมษายน 2567 ถึงวันที่ 28 เมษายน 2568

ผลการวิจัย

ในงานวิจัยนี้ได้นำเสนอผลลัพธ์ที่ได้จากการวิเคราะห์ข้อมูลเกี่ยวกับปัจจัยและความสัมพันธ์ของปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทางการศึกษาในวิทยาลัยเทคนิคกระบี่ ซึ่งผลการวิจัยที่สำคัญสรุปได้ดังนี้:

ภาพรวมประชากรของผู้เข้าร่วม

ผู้ตอบแบบสอบถามทั้งหมดเป็นกลุ่มตัวอย่างจำนวน 175 คน จากประชากรบุคลากรจากวิทยาลัยเทคนิคกระบี่ จำนวน 210 โดยในส่วนของช่วงอายุ พบว่ากลุ่มอายุระหว่าง 26-30 ปีมีสัดส่วน 13.8% และกลุ่มอายุ 50 ปีขึ้นไปมีสัดส่วน 16.7% ในด้านระดับการศึกษา บุคลากรสายวิชาการส่วนใหญ่จบการศึกษาระดับปริญญาตรี (52.9%) ขณะที่บุคลากรสายสนับสนุนส่วนใหญ่จบการศึกษาระดับอนุปริญญาหรือ ปวส. (16.7%) ตารางที่ 1 แสดงจำนวนประชากรของสายปฏิบัติงานที่สำเร็จการศึกษา

ตารางที่ 1 แสดงจำนวนประชากรของสายปฏิบัติงานที่สำเร็จการศึกษา

สายปฏิบัติงาน	การศึกษา	Counts	% of Total	Cumulative %
สายวิชาการ	อนุปริญญา/ปวส	4	2.3 %	2.3 %
	ปริญญาตรี	89	50.9 %	53.1 %
	ปริญญาโท	26	14.9 %	68.0 %
	ปริญญาเอก	1	0.6 %	68.6 %
สายสนับสนุน	อนุปริญญา/ปวส	29	16.6 %	85.1 %
	ปริญญาตรี	22	12.6 %	97.7 %
	ปริญญาโท	4	2.3 %	100.0 %
	ปริญญาเอก	0	0.0 %	100.0 %

ผลลัพธ์เกี่ยวกับการสร้างรหัสผ่าน

จากกลุ่มตัวอย่างจำนวน 175 คนที่ตอบแบบสอบถามเกี่ยวกับการใช้งานรหัสผ่าน พบว่า 25.7% (n=54) ของผู้ตอบใช้รหัสผ่านที่มีความยาวน้อยกว่า 8 ตัวอักษร, 59.0% (n=124) ใช้รหัสผ่านที่มีความยาวระหว่าง 8-10 ตัวอักษร, 7.1% (n=15) ใช้รหัสผ่านที่มีความยาว 10-12 ตัวอักษร และ 8.1% (n=17) ใช้รหัสผ่านที่มีความยาวมากกว่า 12 ตัวอักษร นอกจากนี้ 97.6% (n=205) ของผู้ตอบมีการใช้งานตัวเลขในรหัสผ่าน 93.3% (n=196) ใช้อักษรตัวใหญ่, และ 73.3% (n=154) ใช้อักขระพิเศษ เช่น @, $, %, #, * สำหรับความเสี่ยงในการโจมตีรหัสผ่าน พบว่า 7.6% (n=16) ของผู้ตอบแบบสอบถามยอมรับว่ารหัสผ่านของพวกเขาอาจถูกโจมตีด้วยหลักการพจนานุกรม และ 33.3% (n=70) มีความเสี่ยงที่จะถูกโจมตีด้วยการสุ่มตัวเลข (Brute force) นอกจากนี้ 33.8% (n=71) ใช้รหัสผ่านเดียวกันในหลายบัญชี ขณะที่ 90% (n=189) มีรหัสผ่านมากกว่า 1 รหัส แต่ 93.3% (n=196) เคยลืมรหัสผ่านมาก่อน และ 51.0% (n=107) ของผู้ตอบแบบสอบถามไม่รู้วิธีในการกู้คืนรหัสผ่าน ตารางที่ 2 แสดงค่าความยาวของรหัสผ่านที่ใช้โดยบุคลากรในวิทยาลัยเทคนิคกระบี่

ตารางที่ 2 ความยาวของรหัสผ่านที่ใช้โดยบุคลากรในวิทยาลัยเทคนิคกระบี่

ความยาวของรหัสผ่านของคุณ	Counts	% of Total	Cumulative %
น้อยกว่า 8 ตัวอักษร	45	25.7 %	25.7 %
8-10 ตัวอักษร	100	57.1 %	82.9 %
10-12 ตัวอักษร	14	8.0 %	90.9 %
มากกว่า 12 ตัวอักษร	16	9.1 %	100.0 %

ความน่าเชื่อถือของเครื่องมือวัด

การวิเคราะห์ความน่าเชื่อถือของเครื่องมือวัดความปลอดภัยในข้อมูลทางสถิติโดยใช้ Cronbach's α แสดงให้เห็นว่าแต่ละตัวแปรมีค่าความน่าเชื่อถือที่สูง โดยตัวแปรในกลุ่ม Perceived Ease of Security Practice (PESP) มีค่า Cronbach's α อยู่ระหว่าง 0.900 ถึง 0.904 ซึ่งบ่งบอกถึงความสอดคล้องกันภายในที่ดีมาก สำหรับ Perceived Usefulness of Security Practice (PUSP) ค่า Cronbach's α อยู่ระหว่าง 0.887 ถึง 0.891 ส่วนตัวแปร Attitudes towards Security Practice (ATSP) และ Intention to Use Security Practice (ITSP) มีค่า Cronbach's α ที่ใกล้เคียงกัน คืออยู่ระหว่าง 0.888 ถึง 0.891 ในขณะที่ตัวแปร Security Practice Usage (SPU) มีค่า Cronbach's α ระหว่าง 0.889 ถึง 0.891 ซึ่งทั้งหมดนี้บ่งบอกถึงความน่าเชื่อถือของตัวแปรในระดับสูง ซึ่งสอดคล้องกับการวิเคราะห์ความน่าเชื่อถือของเครื่องมือวัดความปลอดภัยในข้อมูลทางสถิติโดยใช้ McDonald's ω ที่ให้ค่าความเชื่อมั่นสูงกว่า ตารางที่ 2 แสดงค่าความน่าเชื่อถือของเครื่องมือวัดชุดคำถามในข้อมูลทางสถิติโดยใช้ Cronbach's α และ McDonald's ω

ตารางที่ 3 ค่าความน่าเชื่อถือของเครื่องมือวัดชุดคำถามในข้อมูลทางสถิติโดยใช้ Cronbach's α และ McDonald's ω

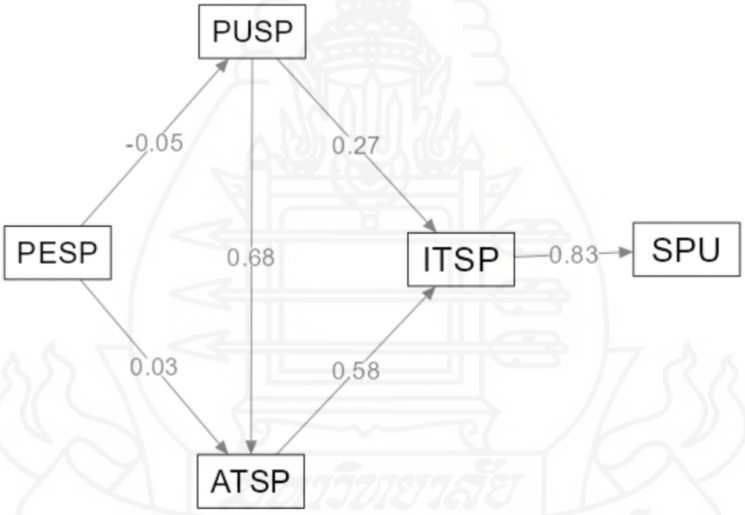
	Cronbach's α	McDonald's ω
scale	0.907	0.934

การวิเคราะห์โมเดลสมการโครงสร้าง

การวิเคราะห์โมเดลสมการโครงสร้างด้วยวิธีการวิเคราะห์เส้นทาง (Path Analysis) ชี้ให้เห็นถึงความสัมพันธ์เชิงสาเหตุระหว่างหลายตัวแปรสำคัญที่เกี่ยวข้องกับการปฏิบัติความมั่นคงปลอดภัยทางข้อมูล โดยเริ่มจาก Intention to Use Security Practice (ITSP) ซึ่งแสดงอิทธิพลอย่างมีนัยสำคัญต่อ Security Practice Usage (SPU) ด้วยค่าประมาณการ (β = 0.8337) และค่า z เท่ากับ 19.339 ซึ่งสะท้อนถึงความสัมพันธ์ที่แข็งแกร่ง การตั้งใจใช้งานแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์จึงมีความสัมพันธ์ในทางบวกกับการใช้งานจริง ผู้ที่มีความตั้งใจสูงมักจะนำแนวปฏิบัติมาใช้มากขึ้น ปัจจัยถัดมาคือ Attitudes towards Security Practice (ATSP) มีอิทธิพลอย่างชัดเจนต่อ ITSP โดยมีค่าประมาณการ 0.5840 (β) และ z =

11.733 ซึ่งชี้ให้เห็นว่า ทัศนคติที่ดีต่อแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ช่วยกระตุ้นให้ผู้ใช้มีความตั้งใจในการนำไปใช้มากขึ้น นอกจากนี้ Perceived Usefulness of Security Practice (PUSP) มีอิทธิพลต่อ ITSP ด้วยค่าประมาณการ 0.2684 ($z = 5.684$, $p < .001$) แสดงให้เห็นว่าการรับรู้ประโยชน์ของการปฏิบัติด้านความปลอดภัยส่งผลให้ผู้ใช้มีความตั้งใจที่จะนำมาใช้งานมากขึ้น

ในทางกลับกัน ATSP ยังมีความสัมพันธ์กับ PUSP โดยค่าประมาณการ 0.6832 (β) และ $z = 14.902$ ($p < .001$) ซึ่งแสดงให้เห็นว่าเมื่อบุคคลรับรู้ว่าการปฏิบัติด้านความปลอดภัยมีประโยชน์ พวกเขามักจะมีทัศนคติที่ดีต่อการนำไปใช้งาน อย่างไรก็ตาม ในส่วนของ Perceived Ease of Security Practice (PESP) พบว่าไม่มีอิทธิพลที่มีนัยสำคัญต่อทั้ง ATSP ($p = 0.325$) และ PUSP ($p = 0.236$) ซึ่งหมายความว่าความง่ายในการใช้งานแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ไม่ได้ส่งผลต่อการสร้างทัศนคติหรือการรับรู้ถึงประโยชน์อย่างมีนัยสำคัญ ภาพที่ 1 แสดงผลลัพธ์จากการวิเคราะห์ด้วยวิธีการวิเคราะห์เส้นทางที่แสดงให้เห็นว่าความตั้งใจต่อการใช้แนวปฏิบัติด้านความมั่นคงของรหัสผ่านส่งผลอย่างมีนัยยะสำคัญต่อการใช้แนวปฏิบัติด้านความมั่นคงของรหัสผ่านที่วิทยาลัยเทคนิคกระบี่



ภาพที่ 1 การวิเคราะห์เส้นทางของปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในวิทยาลัยเทคนิคกระบี่

อภิปรายผลการวิจัย

จากงานวิจัยนี้ ผลการวิจัยได้แสดงให้เห็นถึงพฤติกรรมการสร้างปัจจัยและความสัมพันธ์ของปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทางการศึกษาในวิทยาลัยเทคนิคกระบี่ ซึ่งสามารถประเมินและวิเคราะห์ได้ตามหลักการและทฤษฎีที่เกี่ยวข้อง เช่น พฤติกรรมการสร้างรหัสผ่านที่ผู้ตอบแบบสอบถามมีความยาวของรหัสผ่านน้อยกว่า 8 ตัวอักษรในกลุ่มใหญ่ (25.7%) อาจชี้ให้เห็นถึงการขาดความตระหนักความมั่นคงปลอดภัยไซเบอร์ (Security Awareness) หลักการความมั่นคงปลอดภัยไซเบอร์พื้นฐานของการสร้างรหัสผ่านที่ดีควรประกอบไปด้วยความยาว

เพียงพอและการใช้ตัวอักษรที่หลากหลาย ซึ่งได้รับการสนับสนุนโดยทฤษฎี “Password Security Best Practices” ที่แนะนำว่ารหัสผ่านควรมีความยาวไม่น้อยกว่า 8-12 ตัวอักษร และควรประกอบด้วยตัวเลข ตัวอักษรพิเศษ และตัวอักษรตัวใหญ่ เพื่อป้องกันการโจมตีด้วยการเดารหัสผ่าน (Brute Force หรือ Dictionary Attacks) ในแง่นี้ ผลการวิจัยพบว่า ผู้ตอบแบบสอบถามจำนวนมาก (59%) มีความยาวของรหัสผ่านที่อยู่ในช่วง 8-10 ตัวอักษร ซึ่งเป็นไปตามแนวทางที่ดี อย่างไรก็ตาม จำนวนผู้ตอบแบบสอบถามที่ใช้รหัสผ่านที่มีความยาวน้อยกว่า 8 ตัวอักษร (25.7%) ยังคงมีอยู่ ซึ่งเป็นข้อบ่งชี้ว่าการสร้างความตระหนักความมั่นคงปลอดภัยไซเบอร์ในองค์กรยังเป็นปัญหาที่ควรได้รับการพัฒนา

ผลการวิเคราะห์แสดงให้เห็นถึงบทบาทที่สำคัญของ ITSP และ ATSP ในการส่งเสริมการนำแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์มาใช้งานจริง (SPU) ในส่วนของ ITSP พบว่ามีความสัมพันธ์ที่แข็งแกร่งกับการใช้งานจริง (SPU; β = 0.8337, $p < .001$) ซึ่งสะท้อนว่าการตั้งใจที่จะใช้แนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์นั้นเป็นปัจจัยสำคัญในการกระตุ้นการนำแนวปฏิบัติมาใช้จริง แสดงว่าผู้ที่มีความตั้งใจมากขึ้นมีแนวโน้มที่จะนำแนวปฏิบัติดังกล่าวไปปรับใช้ในชีวิตจริงมากกว่า นอกจากนี้ ATSP ยังมีอิทธิพลเชิงบวกอย่างชัดเจนต่อ ITSP (β = 0.5840, $p < .001$) ซึ่งแสดงว่าทัศนคติที่ดีเกี่ยวกับแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์สามารถส่งเสริมให้ผู้ใช้งานมีความตั้งใจมากขึ้นที่จะนำมาใช้ นอกจากนี้ PUSP ยังส่งผลต่อ ITSP อย่างมีนัยสำคัญ (β = 0.2684, $p < .001$) ซึ่งบ่งบอกว่าเมื่อผู้ใช้รับรู้ถึงประโยชน์ของการใช้งานแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ พวกเขาจะมีความตั้งใจที่จะนำไปใช้งานเพิ่มมากขึ้น และ PUSP ยังส่งผลบวกต่อ ATSP (β = 0.6832, $p < .001$) ชี้ให้เห็นว่าเมื่อผู้ใช้เห็นว่าแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์มีประโยชน์ จะมีการพัฒนาทัศนคติในเชิงบวกต่อแนวปฏิบัติดังกล่าวมากขึ้น

อย่างไรก็ตาม ผลการวิเคราะห์ระบุว่า PESP ไม่มีความสัมพันธ์ที่มีนัยสำคัญกับทั้ง ATSP และ PUSP ($p > .05$) ซึ่งหมายความว่าความง่ายในการใช้งานแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ไม่ได้มีผลต่อการสร้างทัศนคติที่ดีหรือการรับรู้ถึงประโยชน์อย่างมีนัยสำคัญ การค้นพบนี้น่าสนใจเนื่องจากแสดงให้เห็นว่าความง่ายในการใช้งานอาจไม่ใช่ปัจจัยหลักที่ส่งผลต่อการนำแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์มาใช้ แต่ปัจจัยที่สำคัญยิ่งกว่าคือการรับรู้ถึงประโยชน์และทัศนคติที่ดีต่อแนวปฏิบัติดังกล่าว ซึ่งการค้นพบเหล่านี้สามารถนำไปใช้เพื่อพัฒนากลยุทธ์ที่มุ่งเน้นการส่งเสริมให้ผู้ใช้งานมีทัศนคติที่ดีต่อการปฏิบัติความมั่นคงปลอดภัยไซเบอร์และช่วยให้พวกเขาเห็นถึงความสำคัญและประโยชน์ในการนำไปใช้ในชีวิตจริง การวิเคราะห์นี้ชี้ให้เห็นว่า หากบุคลากรมีการรับรู้ว่าการใช้รหัสผ่านที่ปลอดภัยไม่ซับซ้อนและมีประโยชน์ในการป้องกันข้อมูล บุคลากรก็จะยอมรับและนำไปปฏิบัติตาม นอกจากนี้ การสนับสนุนจากองค์กร เช่น การให้คำแนะนำในการจัดการรหัสผ่านและการฟื้นฟูรหัสผ่าน มีผลต่อการสร้างพฤติกรรมที่ปลอดภัยมากยิ่งขึ้น ซึ่งเป็นสิ่งสำคัญที่แสดงให้เห็นในงานวิจัยนี้

ผลการวิจัยพบว่า 33.8% ของผู้ตอบแบบสอบถามใช้รหัสผ่านเดียวกันสำหรับหลายบัญชี ซึ่งเป็นพฤติกรรมที่เสี่ยงต่อการถูกโจมตี การใช้รหัสผ่านซ้ำถือเป็นหนึ่งในปัจจัยที่ทำให้การป้องกันระบบไม่แข็งแรง และสอดคล้องกับทฤษฎีความเสี่ยง (Risk Theory) ที่ระบุว่าการลดการรับรู้ถึงความเสี่ยงจะทำให้ผู้ใช้ไม่ค่อยระวังภัยคุกคามจากการโจมตีทางไซเบอร์ ซึ่งหมายความว่าหากผู้ใช้ไม่ตระหนักถึงผลกระทบจากการใช้รหัสผ่านซ้ำกัน โอกาสที่จะเกิดความเสียหายจากการโจมตีทางไซเบอร์จะสูงขึ้น การวิจัยก่อนหน้านี้ เช่น Patterson et al. (2024) ชี้ให้เห็นว่าผู้ใช้งานส่วนใหญ่มีแนวโน้มที่จะใช้รหัสผ่านซ้ำเพราะสะดวกสบาย แม้ว่าจะทราบถึงความเสี่ยง ดังนั้น การฝึกอบรมและสร้างความตระหนักถึงผลเสียจากการใช้รหัสผ่านซ้ำจึงเป็นสิ่งจำเป็นในการลดความเสี่ยงนี้ (Nautiyal & Rashid, 2024)

จากผลของงานวิจัยนี้ที่พบว่า 93.3% ของผู้ตอบเคยลืมรหัสผ่าน แสดงถึงปัญหาเกี่ยวกับ Password Fatigue หรือการอ่อนล้าจากการต้องจดจำรหัสผ่านที่หลากหลาย แสดงให้เห็นว่า ผู้ใช้งานที่มีหลายบัญชีออนไลน์มักเผชิญปัญหาการลืมรหัสผ่านซึ่งส่งผลให้เกิดพฤติกรรมเช่น การจดบันทึกรหัสผ่านหรือใช้รหัสผ่านง่ายๆ การปรับปรุงระบบช่วยจำรหัสผ่านหรือการใช้เทคโนโลยีเช่นการรับรองตัวตนสองขั้นตอน (Two-Factor Authentication) จึงเป็นอีกหนึ่งทางออกที่ควรพิจารณา ข้อค้นพบนี้สอดคล้องกับงานวิจัยก่อนหน้า เช่น งานวิจัยของ Bhardwaj & Goundar (2017) ที่ชี้ให้เห็นว่า ปัจจัยความง่ายในการใช้งาน (PESP) และการสนับสนุนจากองค์กรเป็นตัวแปรที่สำคัญในการส่งเสริมพฤติกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กร ขณะเดียวกันข้อค้นพบเรื่องการลืมรหัสผ่านและการใช้รหัสผ่านซ้ำก็สอดคล้องการบริหารจัดการรหัสผ่านในองค์กรทางการศึกษา ซึ่งมักพบปัญหาเกี่ยวกับความซับซ้อนในการจำรหัสผ่านเช่นกัน (Kumar, 2023)

ข้อเสนอแนะ

จากผลของงานวิจัยนี้เรื่อง SAM เพื่อเข้าใจปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรทางการศึกษา: กรณีศึกษาวิทยาลัยเทคนิคกระบี่ มีข้อเสนอแนะในการนำผลการวิจัยไปประยุกต์ใช้เพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์และเพิ่มประสิทธิภาพในการจัดการด้านไซเบอร์ซิเคียวริตี้ ดังนี้:

1. วิทยาลัยเทคนิคกระบี่ ควรพัฒนานโยบายที่ชัดเจนเกี่ยวกับการสร้างรหัสผ่าน เช่น การกำหนดมาตรฐานความยาวและความซับซ้อนของรหัสผ่านที่บุคลากรต้องปฏิบัติตาม นโยบายนี้ควรระบุถึงความถี่ในการเปลี่ยนรหัสผ่านและห้ามการใช้รหัสผ่านซ้ำในหลายระบบ การดำเนินการนี้จะช่วยเพิ่มความปลอดภัยของระบบและลดความเสี่ยงในการถูกโจมตี ตามที่แนะนำโดย (Al-Omari et al., 2012)

2. ควรจัดให้มีการฝึกอบรมอย่างต่อเนื่องสำหรับบุคลากรเพื่อเพิ่มความตระหนักในด้านความมั่นคงปลอดภัยไซเบอร์ การฝึกอบรมควรครอบคลุมถึงวิธีการสร้างรหัสผ่านที่ปลอดภัย ความเสี่ยงจากการใช้รหัสผ่านซ้ำ การจัดการรหัสผ่านอย่างมีประสิทธิภาพ และการใช้เครื่องมือช่วย เช่น การยืนยันตัวตนสองขั้นตอน (Two-Factor Authentication) เพื่อเพิ่มความปลอดภัย (Heiding et al., 2023; Ho-Sam-Sooi et al., 2021)

3. องค์กรควรส่งเสริมให้บุคลากรใช้เทคโนโลยี เช่น การใช้โปรแกรม Password Manager เพื่อลดภาระในการจดจำรหัสผ่านหลายชุด และลดความเสี่ยงในการใช้รหัสผ่านซ้ำ เทคโนโลยีนี้ยังสามารถช่วยให้บุคลากรสร้างรหัสผ่านที่มีความซับซ้อนและยากต่อการคาดเดา (Tanni et al., 2022)

4. การนำระบบยืนยันตัวตนแบบหลายขั้นตอนมาใช้ในวิทยาลัยฯ จะช่วยเพิ่มระดับความปลอดภัยของระบบมากยิ่งขึ้น นอกจากการใช้รหัสผ่านแล้ว ควรมีการยืนยันตัวตนด้วยขั้นตอนเพิ่มเติม เช่น การใช้รหัส OTP ที่ส่งไปยังโทรศัพท์มือถือของผู้ใช้งาน หรือการใช้ลายนิ้วมือ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เพื่อป้องกันการโจมตีด้วยปัญญาประดิษฐ์ (Artificial Intelligence: AI) (Jada & Mayayise, 2024)

5. ควรมีการทบทวนและปรับปรุงระบบความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ โดยเฉพาะอย่างยิ่งการตรวจสอบรหัสผ่านของผู้ใช้งานในระบบ เพื่อให้แน่ใจว่ารหัสผ่านที่ใช้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ และไม่มีการใช้รหัสผ่านซ้ำ การทบทวนนี้ควรทำเป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลงนโยบายความมั่นคงปลอดภัยไซเบอร์ (Ezugwu et al., 2023)

6. ควรมีการจัดทำแคมเปญหรือกิจกรรมภายในวิทยาลัยฯ ที่เน้นให้บุคลากรตระหนักถึงความเสี่ยงจากการโจมตีทางไซเบอร์ เช่น การเผยแพร่ข้อมูลเกี่ยวกับภัยคุกคามที่อาจเกิดขึ้น การจำลองสถานการณ์การโจมตี (Cyber Attack Simulation) เพื่อสร้างประสบการณ์จริงในการป้องกันข้อมูล การตระหนักถึงความเสี่ยงจะช่วยลดโอกาสในการเกิดการโจมตีที่อาจส่งผลเสียต่อองค์กร (Khader et al., 2021)

เอกสารอ้างอิง

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security policy compliance: User acceptance perspective. In 2012 45th Hawaii International Conference on System Sciences (pp. 3317–3326). IEEE. https://doi.org/10.1109/HICSS.2012.516

Bhardwaj, A., & Goundar, S. (2017). Security challenges for cloud-based email infrastructure. *Network Security, 2017*(11), 8-15. https://doi.org/10.1016/S1353-4858(17)30094-6

Bridges, R. A., Rice, A. E., Oesch, S., Nichols, J. A., Watson, C., Spakes, K., Norem, S., Huettel, M., Jewell, B., Weber, B., Gannon, C., Bizovi, O., Hollifield, S. C., & Erwin, S. (2023). Testing SOAR tools in use. *Computers & Security, 129*, 103201. https://doi.org/10.1016/j.cose.2023.103201

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

Davis, F. D. (1993). User acceptance of information technology: Ssystem characteristics, user perceptions and behavioral impacts. International Journal of Man-Machine Studies, 38(3), 475–487. https://doi.org/10.1006/imms.1993.1022

Ezugwu, A., Ukwandu, E., Ugwu, C., Ezema, M., Olebara, C., Ndunagu, J., Ofusori, L., & Ome, U. (2023). Password-based authentication and the experiences of end users. Scientific African, 21, e01743. https://doi.org/10.1016/j.sciaf.2023.e01743

Heiding, F., Katsikeas, S., & Lagerström, R. (2023). Research communities in cyber security vulnerability assessments: A comprehensive literature review. *Computer Science Review, 48*, 100551. https://doi.org/10.1016/j.cosrev.2023.100551

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Understanding local government cybersecurity policy: a concept map and framework. *Information, 15*(6), 342. https://doi.org/10.3390/info15060342

Ho-Sam-Sooi, N., Pieters, W., & Kroesen, M. (2021). Investigating the effect of security and privacy on IoT device purchase behaviour. *Computers & Security, 102*, 102132. https://doi.org/10.1016/j.cose.2020.102132

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management, 8*(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

Johnson, A. (2005). The technology acceptance model and the decision to invest in information security. SAIS 2005 Proceedings. https://aisel.aisnet.org/sais2005/21

Jones, C., McCarthy, R., Halawi, L., & Mujtaba, B. (2010). Utilizing the technology acceptance model to assess the employee adoption of information systems security measures. Issues in Information Systems, 11(1), 9–16

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information, 12*(10), 417. https://doi.org/10.3390/info12100417

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, 30, 607-610.

Kumar, P. (2023). Exploring how u.s. k-12 education addresses privacy literacy. Aoir Selected Papers of Internet Research. https://doi.org/10.5210/spir.v2023i0.13439

Nautiyal, L., & Rashid, A. (2024). A framework for mapping organisational workforce knowledge profile in cyber security. *Computers & Security, 145*, 103925. https://doi.org/10.1016/j.cose.2024.103925

Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2024). "I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents. *Computers & Security, 139*, 103699. https://doi.org/10.1016/j.cose.2023.103699

Tanni, T., Taharat, T., Parvez, M., Rumee, S., & Zaber, M. (2022). Is my password strong enough? A study on user perception in the developing world. EAI Endorsed Transactions on Creative Technologies, 9(30). https://doi.org/10.4108/eai.11-2-2022.173452