FACTORS AFFECTING PASSWORD CREATION OF PERSONNEL ACCORDING TO CYBER SECURITY PRACTICES: A CASE STUDY OF BANGKOK HOSPITAL PHUKET

Siwatchaya SUKSAI[1], Wipawan BUATHONG[1], Nasith LAOSEN[1] and Pita JARUPUNPHOL[1*]

1 Master of Science Program in Digital Technology, Phuket Rajabhat University, Thailand; p.jarupunphol@pkru.ac.th (Corresponding Author)

ARTICLE HISTORY

Received: 18 October 2024 **Revised:** 1 November 2024 **Published:** 15 November 2024

ABSTRACT

This study explores the factors affecting password creation among personnel at Bangkok Hospital Phuket, focusing on adherence to cyber security practices. The research applies the Technology Acceptance Model (TAM) to examine key variables such as perceived ease of use (PEOU), perceived usefulness (PU), attitudes (ATU), behavioral intentions (ITU), and actual usage (USE) of secure passwords. The methodology includes the use of descriptive statistics and confirmatory factor analysis (CFA) to assess the model fit, using fit indices such as RMSEA (0.000), SRMR (0.011), and CFI (1.000), which indicate a near-perfect model fit. The results reveal that PEOU has a significant negative influence on PU (Estimate = -0.4831, $p < 0.001$), while PU strongly positively impacts ATU (Estimate = 0.8752, $p < 0.001$). Moreover, behavioral intentions significantly predict actual password usage (Estimate = 0.7681, $p < 0.001$), emphasizing the importance of intention in driving secure behavior. Additionally, the role of perceived skills (PS) was examined, with findings showing that PS significantly impacts PU (Estimate = 0.7969, $p < 0.001$) and ITU (Estimate = 0.2742, $p < 0.001$). These findings contribute to developing comprehensive password security guidelines, suggesting that enhancing perceived skills and the usefulness of secure passwords could lead to better cyber security practices. This research provides actionable insights for designing effective training programs aimed at fostering secure password behavior in healthcare environments, a critical area for protecting sensitive patient data.

Keywords: Cyber Security, Password Creation, Technology Acceptance Model (TAM), Behavioral Intention, Healthcare Data Protection

CITATION INFORMATION: Suksai, S., Buathong, W., Laosen, N., & Jarupunphol, P. (2024). Factors Affecting Password Creation of Personnel According to Cyber Security Practices: A Case Study of Bangkok Hospital Phuket. *Procedia of Multidisciplinary Research, 2*(11), 4

ปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในโรงพยาบาล: กรณีศึกษาโรงพยาบาลกรุงเทพภูเก็ต

ศิวัชญา สุขใส[1], วิภาวรรณ บัวทอง[1], ณสิทธิ์ เหล่าเส็น[1] และ พิทา จารุพูนผล[1*]

1 หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีดิจิทัล มหาวิทยาลัยมหาวิทยาลัยราชภัฏภูเก็ต; p.jarupunphol@pkru.ac.th (ผู้ประพันธ์บรรณกิจ)

บทคัดย่อ

งานวิจัยนี้มุ่งศึกษาปัจจัยที่มีอิทธิพลต่อการสร้างรหัสผ่านของบุคลากรในโรงพยาบาลกรุงเทพภูเก็ต โดยเน้นไปที่การปฏิบัติตามแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ การวิจัยนี้ใช้โมเดลการยอมรับเทคโนโลยี (TAM) ในการวิเคราะห์ความสัมพันธ์ของตัวแปรสำคัญ เช่น การรับรู้ถึงความง่ายในการใช้งาน (PEOU) การรับรู้ถึงประโยชน์ (PU) ทัศนคติ (ATU) ความตั้งใจเชิงพฤติกรรม (ITU) และการใช้งานจริง (USE) ในการสร้างรหัสผ่านที่ปลอดภัย โดยใช้สถิติเชิงพรรณนาและการวิเคราะห์องค์ประกอบเชิงยืนยัน (CFA) ในการประเมินความเหมาะสมของโมเดล ผลการวิจัยพบว่า PEOU มีผลเชิงลบต่อ PU อย่างมีนัยสำคัญ (Estimate = -0.4831, $p < 0.001$) ในขณะที่ PU มีผลเชิงบวกอย่างชัดเจนต่อ ATU (Estimate = 0.8752, $p < 0.001$) นอกจากนี้ ITU ยังส่งผลต่อการสร้างรหัสผ่านจริง (USE) อย่างมีนัยสำคัญ (Estimate = 0.7681, $p < 0.001$) ซึ่งเน้นถึงบทบาทของความตั้งใจในการนำไปสู่พฤติกรรมการใช้งานจริง นอกจากนี้ยังพบว่าการรับรู้ถึงทักษะ (PS) มีอิทธิพลต่อ PU (Estimate = 0.7969, $p < 0.001$) และ ITU (Estimate = 0.2742, $p < 0.001$) ผลการวิจัยนี้ชี้ให้เห็นถึงความสำคัญของการเสริมสร้างทักษะและการรับรู้ถึงประโยชน์ของการใช้รหัสผ่านที่ปลอดภัย ซึ่งสามารถนำไปสู่การปรับปรุงแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ และใช้เป็นแนวทางปฏิบัติเพื่อเสริมสร้างพฤติกรรมการใช้งานรหัสผ่านที่ปลอดภัยในสภาพแวดล้อมทางการแพทย์

คำสำคัญ: ความมั่นคงปลอดภัยไซเบอร์, การสร้างรหัสผ่าน, โมเดลการยอมรับเทคโนโลยี (TAM), ความตั้งใจเชิงพฤติกรรม, การปกป้องข้อมูลทางการแพทย์

ข้อมูลการอ้างอิง: ศิวัชญา สุขใส, วิภาวรรณ บัวทอง, ณสิทธิ์ เหล่าเสน และ พิทา จารุพูนผล. (2567). ปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในโรงพยาบาล: กรณีศึกษาโรงพยาบาลกรุงเทพภูเก็ต. *Procedia of Multidisciplinary Research, 2*(11), 4

บทนำ

ยุคปัจจุบันขับเคลื่อนด้วยระบบดิจิทัล การรักษาความปลอดภัยทางไซเบอร์ได้กลายเป็นส่วนสำคัญในการปกป้องข้อมูลที่ละเอียดอ่อนและการรักษาความสมบูรณ์ขององค์กร โดยเฉพาะอย่างยิ่งสถาบันด้านการดูแลสุขภาพที่ต้องจัดการกับข้อมูลผู้ป่วยที่เป็นความลับจำนวนมหาศาล ทำให้องค์กรเหล่านี้ตกเป็นเป้าหมายสำคัญของการโจมตีทางไซเบอร์ องค์ประกอบที่สำคัญของการรักษาความปลอดภัยทางไซเบอร์ภายในองค์กรด้านการดูแลสุขภาพ คือ การรักษาความปลอดภัยด้วยรหัสผ่านที่เป็นแนวป้องกันเริ่มต้นด่านแรกไม่ให้มีการเข้าถึงบันทึกสุขภาพอิเล็กทรอนิกส์ ข้อมูลสุขภาพผู้ป่วยและระบบงานสำคัญอื่นโดยผู้ที่ไม่ได้รับอนุญาต (Lee, 2023) ดังนั้นการทำความเข้าใจและเสริมสร้างแนวทางปฏิบัติด้านความปลอดภัยของรหัสผ่านในองค์กรที่ต้องดูแลข้อมูลสุขภาพจึงมีความสำคัญอย่างยิ่ง (ราชกิจจานุเบกษา, 2562ก, 2562ข) ด้วยการปรับเปลี่ยนข้อมูลเป็นดิจิทัล องค์กรส่วนใหญ่เปลี่ยนมาใช้แพลตฟอร์มดิจิทัลสำหรับการจัดเก็บข้อมูล การเข้าถึง และการถ่ายโอน แม้ว่าสิ่งนี้จะนำมาซึ่งความสะดวกสบายและมีประสิทธิภาพ แต่สร้างความกังวลเกี่ยวกับความปลอดภัยของข้อมูลที่ละเอียดอ่อน รหัสผ่านเป็นแนวป้องกันหลักในการรักษาความปลอดภัยข้อมูลดังกล่าว (Shamshad et al., 2022) การดูแลสุขภาพมีข้อมูลตั้งแต่เวชระเบียนของผู้ป่วยไปจนถึงธุรกรรมทางการเงิน การรักษาความปลอดภัยด้วยรหัสผ่านไม่เพียงแต่เป็นเรื่องของความสมบูรณ์ของข้อมูลเท่านั้น แต่ยังรวมถึงความปลอดภัยและความไว้วางใจของผู้ป่วยด้วย (Dickerson, 2022)

ปัจจุบันโรงพยาบาลได้นำระบบบันทึกสุขภาพอิเล็กทรอนิกส์ แพลตฟอร์มการแพทย์ทางไกล และเครื่องมือดิจิทัลอื่นๆ มาใช้มากขึ้น เพื่อปรับปรุงกระบวนการดูแลผู้ป่วยและช่วยในการจัดการข้อมูลสุขภาพขนาดใหญ่ (Lampreia et al., 2024; Ö zdemir Sönmez et al., 2022; Pal et al., 2024; Shreya et al., 2022) แม้ว่าความก้าวหน้าทางเทคโนโลยีให้ประโยชน์มากมาย แต่ก็ยังเกิดช่องโหว่ต่อภัยคุกคามทางไซเบอร์ การเข้าถึงโดยไม่ได้รับอนุญาต การละเมิดข้อมูล และการโจมตีทางไซเบอร์อาจส่งผลร้ายแรงเป็นอันตรายต่อองค์กร และมีผลต่อความไว้วางใจของผู้ป่วยรวมไปถึงผู้มีส่วนได้ส่วนเสีย จังหวัดภูเก็ตในประเทศไทยมีอุตสาหกรรมการท่องเที่ยวเชิงการแพทย์ที่มีชื่อเสียง เป็นที่ตั้งของโรงพยาบาลเอกชนหลายแห่งที่ให้บริการผู้ป่วยทั้งในประเทศและต่างประเทศ โดยเฉพาะอย่างยิ่ง โรงพยาบาลกรุงเทพภูเก็ตที่เกี่ยวข้องกับข้อมูลที่ละเอียดอ่อนเป็นจำนวนมาก ต้องจัดลำดับความสำคัญของมาตรการรักษาความปลอดภัยทางไซเบอร์ที่แข็งแกร่ง ประสิทธิผลของการรักษาความปลอดภัยด้วยรหัสผ่านภายในโรงพยาบาลยังคงเป็นประเด็นที่ต้องให้ความสำคัญ การหละหลวมของการรักษาความปลอดภัยรหัสผ่าน อาจนำไปสู่การละเมิดข้อมูลในหลายรูปแบบ เช่น การละเมิดเข้าถึงข้อมูลส่วนบุคคลของผู้ป่วยโดยไม่ได้รับอนุญาต การสูญเสียทางการเงิน ผลกระทบทางกฎหมาย

การทบทวนวรรณกรรม

ในปัจจุบัน สถานพยาบาลรวมถึงโรงพยาบาลเอกชน ได้นำระบบบันทึกสุขภาพอิเล็กทรอนิกส์ แพลตฟอร์มการแพทย์ทางไกล และเครื่องมือดิจิทัลอื่นๆ มาใช้มากขึ้น เพื่อปรับปรุงการดูแลผู้ป่วยและการจัดการข้อมูล (Lampreia et al., 2024; Ö zdemir Sönmez et al., 2022; Pal et al., 2024; Shamshad et al., 2022; Shreya et al., 2022) ซึ่งอาจเสี่ยงต่อการโจมตีทางไซเบอร์ โดยทั่วไป องค์กรด้านการดูแลสุขภาพอาจกำหนดวิธีการดำเนินการและบังคับใช้การรักษาความปลอดภัยของข้อมูลและการจัดการการดูแลสุขภาพที่ดีที่สุดด้วยรหัสผ่านและไบโอเมทริกซ์ที่มีประสิทธิภาพจะป้องกันการเข้าถึงข้อมูลการรักษาพยาบาลโดยไม่ได้รับอนุญาต (Mathew & Mani, 2023) ซึ่งการรักษาความปลอดภัยด้วยรหัสผ่านไม่เพียงแต่เป็นเรื่องของความสมบูรณ์ของข้อมูลเท่านั้น แต่ยังรวมถึงความปลอดภัยและความไว้วางใจของผู้ป่วยด้วย (Dickerson, 2022) นอกจากนี้ กฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ป่วยที่กำหนดให้ต้องมีการรวบรวม จัดเก็บ ประมวลผล เท่าที่จำเป็น และการกำหนดข้อกำหนดด้านความปลอดภัยเพื่อปกป้องข้อมูลทางการแพทย์ให้สอดคล้องกับพระราชบัญญัติที่เกี่ยวข้อง (ราชกิจจานุเบกษา, 2562ข; พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล, 2562) ธุรกิจด้านการดูแลสุขภาพควรใช้เทคโนโลยีความปลอดภัยทางไซเบอร์ที่ได้รับการพัฒนาเป็นอย่างดี มีการปรับปรุงกระบวนการอย่างต่อเนื่องโดยผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์

เนื่องจากรหัสผ่านคือแนวป้องกันแรกของการป้องกันการเข้าถึงข้อมูล (Tanni et al., 2022) การเสริมสร้างความปลอดภัยของรหัสผ่านจำเป็นต้องปฏิบัติตามแนวปฏิบัติด้านความมั่นคงปลอดภัยของรหัสผ่าน เช่น การใช้รหัสผ่านที่ไม่ซ้ำกันและซับซ้อนสำหรับแต่ละบัญชี การใช้ตัวอักษรตัวใหญ่และตัวเล็ก ตัวเลข และสัญลักษณ์ผสมกัน ควรเปลี่ยนรหัสผ่านเป็นประจำ และหลีกเลี่ยงการใช้คำที่คาดเดาได้ง่าย (Yildirim & Mackie, 2019)

งานวิจัยนี้จึงทำการศึกษาปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในโรงพยาบาลกรุงเทพภูเก็ต ด้วยการใช้โมเดลการยอมรับเทคโนโลยี (Technology Acceptance Model: TAM) (Davis, 1989) ซึ่งสามารถใช้ทำนายและอธิบายปัจจัยที่ส่งผลต่อการยอมรับแนวปฏิบัติความมั่นคงปลอดภัย โดย TAM ถูกพัฒนาต่อยอดจากทฤษฎีการกระทำด้วยเหตุผล (Theory of Reasoned Action: TRA) (Trafimow, 2009) และทฤษฎีพฤติกรรมตามแผน (Theory of Planned Behavior: TPB) (Rich et al., 2015) ซึ่งเป็นทฤษฎีทางจิตวิทยาสังคมที่อธิบายว่า พฤติกรรมของมนุษย์ถูกกำหนดโดยความตั้งใจที่จะกระทำ ซึ่ง TAM ถูกออกแบบมาเพื่อวิเคราะห์พฤติกรรมและความตั้งใจในการใช้นวัตกรรมที่ประกอบด้วย ปัจจัยที่ส่งผลต่อการตัดสินใจ เช่น การรับรู้ถึงประโยชน์ (Perceived Usefulness: PU) การรับรู้ถึงความง่ายในการใช้งาน (Perceived Ease of Use: PEOU) โดย PU หมายถึง ระดับที่บุคคลเชื่อว่าการใช้นวัตกรรมจะเพิ่มประสิทธิภาพในการทำงาน ส่วน PEOU หมายถึง ระดับที่บุคคลเชื่อว่าการใช้ระบบนั้นจะไม่ซับซ้อน ยิ่งใช้งานง่ายส่งผลให้มีโอกาสที่จะถูกยอมรับมากขึ้น ซึ่งทั้งสององค์ประกอบนี้จะมีผลต่อทัศนคติต่อการใช้เทคโนโลยี (Attitude towards Using: ATU) ที่ส่งผลต่อความตั้งใจเชิงพฤติกรรมที่จะใช้ระบบ (Behavioral Intention to Use: BI) ซึ่งในที่สุดจะส่งผลต่อการใช้งานระบบจริง (Actual System Use: USE)

มีงานวิจัยมากมายได้สำรวจการประยุกต์ใช้ TAM ในสถานพยาบาล ซึ่งแสดงให้เห็นถึงความคล่องตัวในการทำความเข้าใจและคาดการณ์การนำเทคโนโลยีมาใช้ในบริบทต่าง ๆ เช่น Kim (2024) ได้ประยุกต์ใช้ TAM ในสถานพยาบาลผู้สูงอายุ โดยใช้ประโยชน์จากข้อมูลเชิงลึกจาก ChatGPT เพื่อศึกษาปัจจัยที่มีอิทธิพลต่อการยอมรับเทคโนโลยีด้านสุขภาพของผู้สูงอายุ ในทำนองเดียวกัน AlQudah et al. (2021) ได้ประยุกต์ใช้ TAM ในสถานพยาบาล โดยระบุข้อกำหนดหลักในการนำเทคโนโลยีทางการแพทย์ที่หลากหลายมาใช้ นอกจากนี้ Al-Sulami (2023) ใช้ TAM กับเทคโนโลยีบล็อคเชนในสถานพยาบาลเพื่อศึกษาความท้าทายและทิศทางการวิจัยในอนาคต ดังนั้น ผู้วิจัยจึงเห็นว่า TAM สามารถใช้เพื่อศึกษาปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในโรงพยาบาลกรุงเทพภูเก็ต

สมมติฐานการวิจัย

1) เพื่อศึกษาปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในโรงพยาบาลกรุงเทพภูเก็ต

2) เพื่อศึกษาความสัมพันธ์ของปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในโรงพยาบาลกรุงเทพภูเก็ต

กรอบแนวคิดการวิจัย

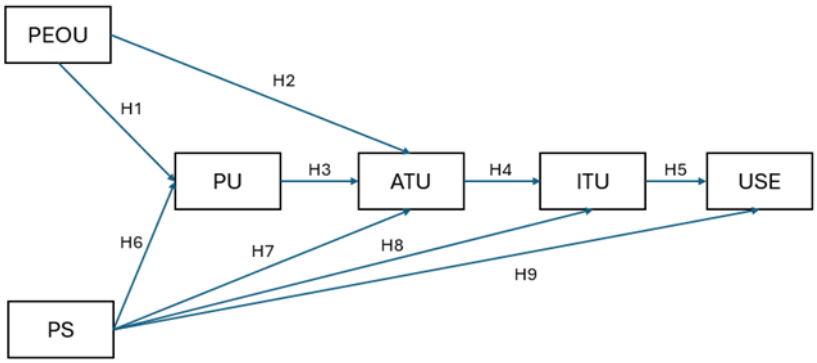
การศึกษาความสัมพันธ์ของปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในโรงพยาบาลกรุงเทพภูเก็ต ประกอบด้วยสมมติฐานย่อยตามหลักการ TAM ที่นำมาสร้างกรอบแนวคิดการวิจัยตามภาพที่ 1 ดังนี้

H1: การรับรู้ถึงความง่ายในการสร้างรหัสผ่านตามแนวปฏิบัติ (PEOU) ส่งผลต่อการรับรู้ถึงประโยชน์ในการสร้างรหัสผ่านตามแนวปฏิบัติ (PU)

H2: การรับรู้ถึงความง่ายในการสร้างรหัสผ่านตามแนวปฏิบัติ (PEOU) ส่งผลต่อทัศนคติต่อการสร้างรหัสผ่านตามแนวปฏิบัติ (ATU)

H3: การรับรู้ถึงประโยชน์ในการสร้างรหัสผ่านตามแนวปฏิบัติ (PU) ส่งผลต่อทัศนคติต่อการสร้างรหัสผ่านตามแนวปฏิบัติ (ATU)

H4: ทัศนคติต่อการสร้างรหัสผ่านตามแนวปฏิบัติ (ATU) ส่งผลต่อความตั้งใจเชิงพฤติกรรมที่จะสร้างรหัสผ่านตามแนวปฏิบัติ (ITU)
H5: ความตั้งใจเชิงพฤติกรรมที่จะสร้างรหัสผ่านตามแนวปฏิบัติ (ITU) ส่งผลต่อพฤติกรรมการสร้างรหัสผ่านตามแนวปฏิบัติ (USE)
H6: การรับรู้ถึงทักษะในการสร้างรหัสผ่านตามแนวปฏิบัติ (PS) ส่งผลต่อการรับรู้ถึงประโยชน์ในการสร้างรหัสผ่านตามแนวปฏิบัติ (PU)
H7: การรับรู้ถึงทักษะในการสร้างรหัสผ่านตามแนวปฏิบัติ (PS) ส่งผลต่อทัศนคติต่อการสร้างรหัสผ่านตามแนวปฏิบัติ (ATU)
H8: การรับรู้ถึงทักษะในการสร้างรหัสผ่านตามแนวปฏิบัติ (PS) ส่งผลต่อความตั้งใจเชิงพฤติกรรมที่จะสร้างรหัสผ่านตามแนวปฏิบัติ (ITU)
H9: การรับรู้ถึงทักษะในการสร้างรหัสผ่านตามแนวปฏิบัติ (PS) ส่งผลต่อพฤติกรรมการสร้างรหัสผ่านตามแนวปฏิบัติ (USE)



ภาพที่ 1 กรอบแนวคิดการวิจัยเพื่อศึกษาปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในโรงพยาบาลกรุงเทพภูเก็ต

วิธีดำเนินการวิจัย

ขั้นตอนต่อไปนี้คือวิธีการวิจัยที่นำมาใช้ในการศึกษาปัจจัยและความสัมพันธ์ของปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในโรงพยาบาลกรุงเทพภูเก็ต

การกำหนดกลุ่มตัวอย่าง

วิจัยฉบับนี้เป็นการศึกษาที่มุ่งเน้นไปที่การรวบรวมและวิเคราะห์ข้อมูลเชิงปริมาณ โดยอาศัยวิธีการทางสถิติเพื่อหาความสัมพันธ์ระหว่างตัวแปรต่างๆ การศึกษานี้ใช้วิธีการวิจัยเชิงปริมาณเพื่อหาปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ โดยใช้หลักการของ TAM ซึ่งข้อมูลที่ใช้ในการศึกษานี้รวบรวมจากแบบสอบถามออนไลน์ที่ส่งถึงผู้เข้าร่วมการศึกษา ประชากรที่ใช้ในการศึกษา คือ พนักงานโรงพยาบาลกรุงเทพภูเก็ต โดยกลุ่มตัวอย่าง ได้แก่ เจ้าหน้าที่ที่ทำงานในโรงพยาบาล ทั้งส่วนงานบริการ (Clinical) ส่วนงานสนับสนุน (Semi-Clinical) และพนักงาน Office (Back Office) อายุ 20 ปีขึ้นไป ที่ตอบแบบสอบถาม จำนวน 416 คน โดยกำหนดระดับความคลาดเคลื่อนไว้ที่ 0.05 ซึ่งมากกว่าจำนวนตัวแทนของประชากรรวมในตำแหน่งที่กล่าวมาเท่ากับ 1,000 คน เพื่อให้ได้ข้อมูลที่สะท้อนถึงลักษณะของประชากรทั้งหมด สำหรับวิธีการชักตัวอย่าง หรือวิธีการเลือกหน่วยตัวอย่างจากประชากรศึกษาจะใช้วิธีการสุ่มตัวอย่างแบบง่าย (Simple random sampling) คือ วิธีการเลือกหน่วยตัวอย่างโดยสุ่มจากประชากรทั้งหมด การเก็บข้อมูลครอบคลุมตั้งแต่ข้อมูลส่วนบุคคล เช่น อายุ เพศ การศึกษา อาชีพ และปัจจัยที่เกี่ยวข้องกับการสร้างรหัสผ่าน

การออกแบบเครื่องมือเก็บข้อมูล

การวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณ (Quantitative Research) โดยใช้การสำรวจ (Survey) จากแบบสอบถามออนไลน์ที่ส่งถึงผู้เข้าร่วมการศึกษา ใช้วิธีการสุ่มตัวอย่างแบบไม่อาศัยความน่าจะเป็นแบบเจาะจง (Purposive Sampling) เฉพาะพนักงานประจำ (Full time) ใช้สถิติพื้นฐานในการตรวจสอบความน่าเชื่อถือของข้อมูล เช่น ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน วิเคราะห์ความสัมพันธ์ระหว่างตัวแปรโดยใช้การวิเคราะห์การถดถอย (Regression Analysis) การวิเคราะห์เส้นทาง (Path Analysis) ด้วยการใช้โมเดลสมการโครงสร้าง (Structural Equation Modelling: SEM) ตามทฤษฎีของ TAM เพื่อช่วยในการวิเคราะห์รูปแบบข้อมูลซับซ้อนและสรุปผลที่ชัดเจน และได้มุมมองและคำตอบน่าเชื่อถือในการศึกษาเรื่องความมั่นคงปลอดภัยไซเบอร์ (Davis, 1989)

การรวบรวมข้อมูล

วิธีการรวบรวมข้อมูลที่เหมาะสมสำหรับการศึกษานี้ คือ การใช้แบบสอบถามออนไลน์ เนื่องจากสามารถเข้าถึงกลุ่มตัวอย่างได้เป็นจำนวนมาก และรวบรวมข้อมูลที่หลากหลายเกี่ยวกับการสร้างรหัสผ่านตามแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในโรงพยาบาลกรุงเทพภูเก็ต แบบสอบถามออนไลน์ได้รับการพัฒนาขึ้นอย่างรอบคอบ โดยเริ่มต้นด้วยการอธิบายวัตถุประสงค์ของการวิจัย รายละเอียดของแบบสอบถาม และการขอความยินยอมจากผู้เข้าร่วม ก่อนเข้าสู่กระบวนการเก็บข้อมูล ข้อคำถามจะครอบคลุมปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านที่ปลอดภัย โดยไม่เก็บข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ ซึ่งคำถามในแบบสอบถามมุ่งเน้นการประเมินเงื่อนไขทางจิตวิทยาและพฤติกรรมในการสร้างรหัสผ่าน โดยใช้มาตรวัด 7 ระดับ ตามวัตถุประสงค์ที่ชัดเจน เช่น การตรวจสอบปัจจัยที่ส่งผลต่อการยอมรับการสร้างรหัสผ่านที่ปลอดภัยของบุคลากรโรงพยาบาล ภายใต้กรอบแบบจำลอง TAM (Davis, 1989) สมมติฐานจะถูกกำหนดขึ้นเพื่อทดสอบความสัมพันธ์ระหว่างปัจจัยต่างๆ

การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลในงานวิจัยนี้เริ่มต้นด้วยการใช้สถิติพื้นฐานเพื่อประเมินความน่าเชื่อถือและความถูกต้องของข้อมูลที่เก็บรวบรวม โดยคำนวณค่าเฉลี่ย (Mean) เพื่อสะท้อนแนวโน้มของข้อมูลส่วนใหญ่ และคำนวณส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) เพื่อตรวจสอบการกระจายตัวของข้อมูล จากนั้นทำการวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรต่างๆ โดยใช้การวิเคราะห์การถดถอยเชิงเส้น (Regression Analysis) หรือการวิเคราะห์เส้นทาง (Path Analysis) เพื่อเข้าใจความสัมพันธ์เชิงเส้นระหว่างตัวแปรสำคัญ เช่น การรับรู้ความง่ายในการใช้งาน (PEOU) และการรับรู้ประโยชน์ (PU) กับทัศนคติ (ATU) และความตั้งใจในการใช้งาน (ITU) และตรวจสอบว่าความตั้งใจ (ITU) ส่งผลต่อพฤติกรรมการใช้งาน (USE) อย่างไร นอกจากนี้ยังวิเคราะห์ว่าทักษะที่รับรู้ (PS) ส่งผลต่อ PEOU, PU และ ITU อย่างไร ทั้งนี้ เพื่อประเมินความเที่ยงตรงและความน่าเชื่อถือของโมเดล งานวิจัยทำการวิเคราะดัชนีความเหมาะสม (Fit Indices) โดยใช้ข้อมูลจากตัวชี้วัดเพื่อประเมินการ Fit ของโมเดล (Shi et al., 2019)

ข้อพิจารณาทางจริยธรรม

การขออนุมัติด้านจริยธรรมในการวิจัยเป็นกระบวนการที่มีความสำคัญอย่างยิ่ง เนื่องจากเป็นการรับรองว่าการศึกษาใดๆ จะดำเนินการด้วยความรับผิดชอบและให้ความเคารพต่อสิทธิของผู้เข้าร่วม โดยเฉพาะในการศึกษาที่ต้องประเมินความเสี่ยงและผลประโยชน์ที่อาจเกิดขึ้น รวมถึงพิจารณาถึงอันตรายหรือความไม่สบายใจที่อาจเกิดกับผู้เข้าร่วม และการวางแผนเพื่อบรรเทาปัญหาเหล่านั้น งานวิจัยเรื่อง “ปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในโรงพยาบาล: กรณีศึกษาโรงพยาบาลกรุงเทพภูเก็ต” เป็นหนึ่งในงานวิจัยที่ได้รับการอนุมัติด้านจริยธรรมจากคณะกรรมการพิจารณาจริยธรรมการวิจัยในมนุษย์ มหาวิทยาลัยราชภัฏภูเก็ต เมื่อวันที่ 29 เมษายน 2567 หมายเลขใบรับรอง PKRU2567/08 การอนุมัตินี้มีผลครอบคลุมตั้งแต่วันที่ 29 เมษายน 2567 ถึง 28 เมษายน 2568 เพื่อให้มั่นใจว่างานวิจัยจะเกิดประโยชน์ต่อผู้เข้าร่วมและไม่ก่อให้เกิดอันตรายใดๆ โดยการขออนุมัตินี้เป็นการรับประกันว่าการศึกษาจะดำเนินการอย่างถูกต้อง ปกป้องสิทธิของผู้เข้าร่วม และรักษาความน่าเชื่อถือของผลการวิจัย

ผลการวิจัย

ผลการวิจัยพบว่า พนักงานส่วนใหญ่ที่โรงพยาบาลกรุงเทพภูเก็ต มีการใช้รหัสผ่านที่ประกอบด้วยการผสมตัวอักษรพิมพ์ใหญ่ ตัวเลข และตัวอักขระพิเศษ เช่น @, $, %, #, * และอื่นๆ โดยมีผู้ใช้ที่ตอบว่า ใช้วิธีนี้อยู่ทั้งหมด 410 คน ซึ่งคิดเป็นสัดส่วนที่สูงมาก เพียงแต่มี 6 คนเท่านั้นที่ไม่ได้ใช้รหัสผ่านแบบนี้ การใช้รหัสผ่านที่มีความซับซ้อนด้วยการผสมองค์ประกอบต่างๆ นี้ช่วยเพิ่มความปลอดภัยในการเข้าถึงข้อมูลส่วนบุคคลและข้อมูลสำคัญอื่นๆ ในระบบ นอกจากนี้ การศึกษานี้ได้จัดทำคำถามแบบมาตรวัด 7 ระดับ ซึ่งเกี่ยวข้องกับปัจจัยต่างๆ ได้แก่ ความง่ายในการใช้งานที่รับรู้ (PEOU) การรับรู้ถึงประโยชน์ (PU) ทัศนคติต่อการใช้ (ATU) ความตั้งใจเชิงพฤติกรรมที่จะใช้ (ITU) การใช้งานจริง (USE) และการรับรู้ถึงทักษะ (Perceived Skills: PS) ซึ่งผลการวิเคราะห์ค่าความเชื่อมั่นของชุดคำถามที่เกี่ยวข้องกับปัจจัยที่มีผลกับการสร้างรหัสผ่านตามแนวปฏิบัติแบบ Cronbach's α และ McDonald's ω พบว่า มีค่าความเชื่อมั่นสูง โดยค่า Cronbach's α ของระดับรวมมีค่า 0.874 และค่า McDonald's ω อยู่ที่ 0.924 นอกจากนี้ ผลการวิเคราะห์ค่า Fit Indices ของโมเดลนี้แสดงถึงความเหมาะสมอย่างมากในหลายตัวชี้วัด ค่าดัชนีสำคัญ เช่น RMSEA มีค่า 0.000 ซึ่งบ่งชี้ว่า โมเดลนี้ Fit กับข้อมูลได้อย่างสมบูรณ์ และช่วงความเชื่อมั่น (Confidence Interval) อยู่ในช่วงแคบมาก ค่า CFI ที่ 1.000 และ TLI ที่มากกว่า 1 แสดงถึง การ Fit ที่สมบูรณ์เช่นกัน นอกจากนี้ ค่า SRMR ที่ต่ำกว่า 0.05 แสดงว่าความคลาดเคลื่อนระหว่างโมเดลและข้อมูลจริงมีน้อยมาก ซึ่งเป็นสัญญาณว่าข้อมูลและโมเดลสอดคล้องกันสูงมาก

ตารางที่ 1 แสดงผลการวิเคราะห์ที่กี่ยวข้องกับความสัมพันธ์ระหว่างตัวแปร โดย PEOU ส่งผลต่อ PU มีค่า Estimate เท่ากับ -0.4831 ค่าความคลาดเคลื่อนมาตรฐาน (SE) อยู่ที่ 0.0311 และค่าพิสัยความเชื่อมั่น 95% (95% CI) อยู่ในช่วง -0.5440 ถึง -0.4222 ค่า z-value คือ -15.54 และค่า p-value น้อยกว่า 0.001 ซึ่งแสดงว่า ผลลัพธ์นี้มีนัยสำคัญทางสถิติ นอกจากนี้ PEOU ยังส่งผลต่อ ATU มีค่า Estimate อยู่ที่ -0.0635 ค่า SE คือ 0.0198 โดยมีค่าพิสัยความเชื่อมั่น 95% อยู่ที่ -0.1023 ถึง -0.0247 ค่า z-value คือ -3.21 และค่า p-value เท่ากับ 0.001 ซึ่งบ่งชี้ว่า ผลลัพธ์นี้มีนัยสำคัญทางสถิติ ทั้งนี้ PU ส่งผลต่อ ATU มีค่า Estimate สูงถึง 0.8752 ค่า SE อยู่ที่ 0.0248 และค่าพิสัยความเชื่อมั่น 95% อยู่ในช่วง 0.8265 ถึง 0.9239 ค่า z-value คือ 35.23 และค่า p-value น้อยกว่า 0.001 ซึ่งแสดงให้เห็นถึงความมีนัยสำคัญทางสถิติอย่างมาก ในขณะที่ ATU ส่งผลต่อ ITU มีค่า Estimate ของสมมติฐานนี้อยู่ที่ 0.1399 ซึ่งแม้จะเป็นผลบวก แต่มีค่าไม่สูงนัก และไม่มีนัยสำคัญทางสถิติ เนื่องจากค่า p-value เท่ากับ 0.264 ค่า SE คือ 0.1252 และค่าพิสัยความเชื่อมั่น 95% อยู่ในช่วง -0.1055 ถึง 0.3853 และที่สำคัญคือ ITU ส่งผลต่อ USE แสดงผลกระทบเชิงบวกที่ชัดเจน โดยค่า Estimate อยู่ที่ 0.7681 ค่า SE คือ 0.0466 และค่าพิสัยความเชื่อมั่น 95% อยู่ในช่วง 0.6768 ถึง 0.8594 ค่า z-value คือ 16.49 และค่า p-value น้อยกว่า 0.001 ซึ่งแสดงให้เห็นถึงความมีนัยสำคัญทางสถิติ

สำหรับการทดสอบตัวแปรด้านทักษะที่รับรู้ แสดงให้เห็นว่า PS ส่งผลต่อ PU แสดงค่า Estimate ที่ 0.7969 ซึ่งบ่งชี้ถึงผลเชิงบวกที่ชัดเจน ค่า SE คือ 0.0538 และค่าพิสัยความเชื่อมั่น 95% อยู่ที่ 0.6915 ถึง 0.9023 ค่า z-value คือ 14.82 และค่า p-value น้อยกว่า 0.001 แสดงถึงความมีนัยสำคัญทางสถิติ นอกจากนี้ PS ส่งผลต่อ ATU มีค่า Estimate ที่ 0.1173 ซึ่งแสดงผลเชิงบวกเล็กน้อย ค่า SE คือ 0.0337 และค่าพิสัยความเชื่อมั่น 95% อยู่ที่ 0.0513 ถึง 0.1833 ค่า z-value คือ 3.48 และค่า p-value น้อยกว่า 0.001 ซึ่งแสดงถึงความมีนัยสำคัญทางสถิติ ในขณะที่ PS ส่งผลต่อ ITU มีค่า Estimate ที่ 0.2742 แสดงถึงผลเชิงบวก ค่า SE คือ 0.0549 และค่าพิสัยความเชื่อมั่น 95% อยู่ในช่วง 0.1666 ถึง 0.3817 ค่า z-value คือ 5.00 และค่า p-value น้อยกว่า 0.001 ซึ่งแสดงถึงความมีนัยสำคัญทางสถิติ และ PS ส่งผลต่อ USE มีค่า Estimate อยู่ที่ 0.2177 ค่า SE คือ 0.0647 และค่าพิสัยความเชื่อมั่น 95% อยู่ที่ 0.0909 ถึง 0.3445 ค่า z-value คือ 3.36 และค่า p-value น้อยกว่า 0.001

ตารางที่ 1 ผลการวิเคราะห์ที่เกี่ยวข้องกับความสัมพันธ์ระหว่างตัวแปร

				95% Confidence Intervals				
Dep	Pred	Estimate	SE	Lower	Upper	β	z	p
USE	ITU	0.7681	0.0466	0.6768	0.8594	0.627	16.49	< .001
USE	PS	0.2177	0.0647	0.0909	0.3445	0.128	3.36	< .001
ITU	ATU	0.1399	0.1252	-0.1055	0.3853	0.109	1.12	0.264
ITU	PU	0.5769	0.1264	0.3291	0.8247	0.445	4.56	< .001
ITU	PS	0.2742	0.0549	0.1666	0.3817	0.197	5.00	< .001
ATU	PU	0.8752	0.0248	0.8265	0.9239	0.865	35.23	< .001
ATU	PEOU	-0.0635	0.0198	-0.1023	-0.0247	-0.101	-3.21	0.001
ATU	PS	0.1173	0.0337	0.0513	0.1833	0.108	3.48	< .001
PU	PEOU	-0.4831	0.0311	-0.5440	-0.4222	-0.780	-15.54	< .001
PU	PS	0.7969	0.0538	0.6915	0.9023	0.744	14.82	< .001

สรุปและอภิปรายผลการวิจัย

งานวิจัยนี้มุ่งเน้นการศึกษาปัจจัยที่ส่งผลต่อการสร้างรหัสผ่านตามแนวปฏิบัติความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในโรงพยาบาลกรุงเทพภูเก็ต โดยใช้ TAM เพื่อประเมินความสัมพันธ์ของตัวแปรต่างๆ ที่เกี่ยวข้อง เช่น การรับรู้ถึงความง่ายในการใช้งาน การรับรู้ถึงประโยชน์ ทัศนคติ ความตั้งใจเชิงพฤติกรรม และการใช้งานจริง ผลการวิจัยนี้ได้ยืนยันสมมติฐานที่ตั้งไว้บางส่วนและปฏิเสธบางส่วน ดังนี้

H1: PEOU ส่งผลต่อ PU ที่แสดงว่าการรับรู้ถึงความง่ายในการสร้างรหัสผ่านส่งผลกระทบเชิงลบอย่างมีนัยสำคัญต่อการรับรู้ถึงประโยชน์ในการสร้างรหัสผ่าน ซึ่งสอดคล้องกับการศึกษาในอดีตที่ระบุว่า การทำให้กระบวนการง่ายเกินไปอาจทำให้บุคลากรรู้สึกว่าระบบไม่มีประสิทธิภาพเพียงพอในการป้องกันข้อมูล (Yildirim & Mackie, 2019) การรับรู้ว่ารหัสผ่านนั้นง่ายต่อการสร้างอาจส่งผลให้บุคลากรไม่เห็นความสำคัญในการสร้างรหัสผ่านที่ปลอดภัยและซับซ้อน

H2: PEOU ส่งผลต่อ ATU ซึ่งผลการวิจัยแสดงให้เห็นว่าการรับรู้ถึงความง่ายในการสร้างรหัสผ่านส่งผลเชิงลบเล็กน้อยต่อทัศนคติของบุคลากรต่อการสร้างรหัสผ่าน ถึงแม้จะเป็นผลกระทบที่น้อย แต่ก็มีนัยสำคัญทางสถิติ ซึ่งสอดคล้องกับการวิจัยของ Davis (1989) ที่กล่าวถึงว่า ความง่ายในการใช้งานของระบบไม่สามารถสร้างทัศนคติที่ดีได้เสมอไป การสร้างรหัสผ่านที่ง่ายเกินไปอาจทำให้บุคลากรไม่เห็นความจำเป็นในการปฏิบัติตามแนวทางที่เข้มงวด

H3: PU ส่งผลต่อ ATU ที่แสดงว่าการรับรู้ถึงประโยชน์มีผลเชิงบวกอย่างชัดเจนต่อทัศนคติของบุคลากร ซึ่งชี้ให้เห็นว่าเมื่อบุคลากรเข้าใจว่าการสร้างรหัสผ่านที่ปลอดภัยมีประโยชน์ต่อการป้องกันข้อมูล บุคลากรจะมีทัศนคติที่ดีต่อการปฏิบัติตามแนวทางนี้ ผลการวิจัยนี้สอดคล้องกับ Davis (1989) ที่ระบุว่า การรับรู้ถึงประโยชน์เป็นปัจจัยหลักที่มีอิทธิพลต่อทัศนคติของผู้ใช้

H4: ATU ส่งผลต่อ ITU ซึ่งผลการวิจัยนี้ชี้ว่าทัศนคติที่ดีต่อการสร้างรหัสผ่านไม่ได้ส่งผลต่อความตั้งใจในการสร้างรหัสผ่านอย่างมีนัยสำคัญทางสถิติ ซึ่งอาจเนื่องมาจากปัจจัยอื่นๆ เช่น ข้อจำกัดด้านเวลาและความสะดวกในการสร้างรหัสผ่าน ทำให้ทัศนคติที่ดีไม่ได้แปรผันตรงกับความตั้งใจที่จะสร้างรหัสผ่านที่ซับซ้อนอย่างที่ควรจะเป็น (Shamshad et al., 2022)

H5: ITU ส่งผลต่อ USE แสดงให้เห็นว่าความตั้งใจเชิงพฤติกรรมมีผลเชิงบวกและมีนัยสำคัญอย่างมากต่อพฤติกรรมการสร้างรหัสผ่านจริง ซึ่งชี้ให้เห็นว่าบุคลากรที่มีความตั้งใจสูงในการสร้างรหัสผ่านจะมีแนวโน้มในการปฏิบัติตามมากขึ้น สอดคล้องกับการศึกษาของ Rich et al. (2015) ที่กล่าวถึงความตั้งใจเชิงพฤติกรรมส่งผลต่อการกระทำจริงในทางปฏิบัติ

H6: PS ส่งผลต่อ PU ที่ชี้ให้เห็นว่าการรับรู้ถึงทักษะมีผลกระทบเชิงบวกอย่างชัดเจนต่อการรับรู้ถึงประโยชน์ในการสร้างรหัสผ่าน บุคลากรที่รู้สึกว่าตนเองมีทักษะในการสร้างรหัสผ่านจะมองว่าการสร้างรหัสผ่านที่ปลอดภัยมีประโยชน์มากขึ้น ซึ่งสอดคล้องกับการศึกษาของ Venkatesh et al. (2016) ที่แสดงถึงความสำคัญของทักษะที่รับรู้ในการกำหนดการรับรู้ถึงประโยชน์ของเทคโนโลยี

H7: PS ส่งผลต่อ ATU ที่แสดงให้เห็นว่าการรับรู้ถึงทักษะมีผลกระทบเชิงบวกเล็กน้อยต่อทัศนคติของบุคลากร แม้จะเป็นผลเชิงบวก แต่การรับรู้ถึงทักษะเพียงอย่างเดียวอาจไม่เพียงพอที่จะสร้างทัศนคติที่ดีอย่างชัดเจน การฝึกอบรมเพิ่มเติมอาจจำเป็นเพื่อเสริมสร้างทัศนคติของบุคลากร

H8: PS ส่งผลต่อ ITU ซึ่งพบว่าการรับรู้ทักษะส่งผลเชิงบวกอย่างชัดเจนต่อความตั้งใจเชิงพฤติกรรมในการสร้างรหัสผ่าน (Estimate = 0.2742, $p < 0.001$) บุคลากรที่รับรู้ว่าตนเองมีทักษะจะมีความตั้งใจในการสร้างรหัสผ่านที่แข็งแรงมากขึ้น ซึ่งสอดคล้องกับ Trafimow (2009) ที่ชี้ให้เห็นว่าการรับรู้ทักษะสามารถส่งเสริมความตั้งใจในการปฏิบัติตามแนวทางที่ดี

H9: PS ส่งผลต่อ USE แสดงให้เห็นว่าการรับรู้ถึงทักษะมีผลกระทบเชิงบวกในระดับปานกลางต่อพฤติกรรมการสร้างรหัสผ่าน บุคลากรที่รู้สึกว่าตนเองมีทักษะในการสร้างรหัสผ่านจะมีแนวโน้มในการปฏิบัติตามแนวทางที่ดีมากขึ้น แต่ยังไม่เพียงพอที่จะเป็นปัจจัยหลักที่กำหนดพฤติกรรม การสนับสนุนเพิ่มเติมเช่นการอบรมและการจัดการรหัสผ่านอย่างมีประสิทธิภาพอาจจำเป็น (Mathew & Mani, 2023)

ข้อเสนอแนะที่ได้รับจากการวิจัย

โรงพยาบาลควรมีการจัดฝึกอบรมเพิ่มเติมเกี่ยวกับการสร้างรหัสผ่านที่ปลอดภัยสำหรับบุคลากรในโรงพยาบาล โดยเน้นถึงความสำคัญของการเสริมสร้างทักษะในการใช้งานเทคโนโลยีเพื่อเพิ่มความมั่นใจในการปฏิบัติจริง นอกจากนี้โรงพยาบาลควรพิจารณาการนำเครื่องมือช่วยจัดการรหัสผ่านมาใช้ เพื่ออำนวยความสะดวกในการสร้างและจัดการรหัสผ่านที่มีความปลอดภัย อ้างอิงจากการศึกษาของ Tanni et al. (2022) ที่กล่าวถึงการเสริมสร้างความมั่นคงของรหัสผ่านผ่านเครื่องมือช่วยจัดการรหัสผ่านและการเข้ารหัสข้อมูลอย่างเป็นระบบ รวมถึงการประเมินความง่ายในการใช้งานและความปลอดภัยที่โรงพยาบาลควรปรับปรุงระบบการสร้างรหัสผ่านให้มีความสมดุลระหว่างความง่ายในการใช้งานและความปลอดภัย (Shamshad et al., 2022) งานวิจัยนี้มีส่วนช่วยให้โรงพยาบาลกรุงเทพภูเก็ตปรับปรุงการรักษาความมั่นคงปลอดภัยข้อมูลผู้ป่วยและระบบต่างๆ โดยใช้แนวทางการสร้างรหัสผ่านที่มีประสิทธิภาพมากขึ้น ซึ่งมีความสำคัญอย่างยิ่งในการป้องกันการโจมตีทางไซเบอร์ (Lee, 2023) ซึ่งเป็นการช่วยยกระดับความมั่นคงปลอดภัยไซเบอร์ในโรงพยาบาล นอกจากนี้ งานวิจัยได้เน้นให้เห็นถึงความสำคัญของการสร้างรหัสผ่านที่แข็งแรง ซึ่งช่วยให้การจัดการข้อมูลสุขภาพของผู้ป่วยมีความปลอดภัยมากยิ่งขึ้น ส่งผลให้การดำเนินงานของโรงพยาบาลมีความมั่นคงและมีประสิทธิภาพ และใช้เป็นแนวทางในการปรับปรุงนโยบายและมาตรการความปลอดภัยที่เน้นความสำคัญของการปรับปรุงมาตรการป้องกันการเข้าถึงข้อมูลที่ละเอียดอ่อนในองค์กร (Mathew & Mani, 2023)

ข้อเสนอแนะในการวิจัยครั้งต่อไป

ควรศึกษาปัจจัยด้านลักษณะงาน การใช้และการเข้าถึงข้อมูลผู้ป่วยในแต่ละตำแหน่งงานที่มีผลต่อการเข้าใจ ยอมรับ ศึกษาเชิงเปรียบเทียบกับโรงพยาบาลอื่นๆ ภาครัฐ เพื่อนำมาวิเคราะห์ข้อดี ข้อเสียและนำมาเป็นแนวทางการในการพัฒนาต่อไป และควรทำการศึกษาด้วยวิธีเชิงคุณภาพ โดยเฉพาะการสัมภาษณ์เชิงลึกถึงสิ่งที่พนักงานต้องการ เพื่อให้ได้ข้อมูลเชิงลึกที่ชัดเจนยิ่งขึ้น และเป็นประโยชน์ในการพัฒนาระบบให้สามารถตอบสนองความต้องการของพนักงานบนพื้นฐานความมั่นคงปลอดภัยไซเบอร์ได้สูงสุด รวมถึงการนำผลการวิจัยนี้ไปใช้เป็นแนวทางในการศึกษาต่อยอดการวิจัยครั้งต่อไปในประเด็นเกี่ยวกับแผนการให้บริการกรณีที่อาจเกิดหยุดชะงักของการให้บริการ เนื่องจากอาชญากรไซเบอร์อาจเข้ายึดระบบปฏิบัติการของหน่วยงาน ทำให้ระบบไม่สามารถทำงานได้ ส่งผลให้ผู้ป่วยไม่สามารถเข้าถึงบริการด้านการดูแลสุขภาพได้

เอกสารอ้างอิง

AlQudah, A., Al-Emran, M., & Shaalan, K. (2021). Technology acceptance in healthcare: a systematic review. *Applied Sciences, 11*(22), 10537.

Al-Sulami, Z. (2023). Blockchain adoption in healthcare: models, challenges, and future work. *Basrah Researches Sciences, 49.2*(2), 79-93.

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

Dickerson, J. E. (2022). Privacy, confidentiality, and security of healthcare information. *Anaesthesia & Intensive Care Medicine, 23*(11), 740-743.

Kim, S. (2024). Application and challenges of the technology acceptance model in elderly healthcare: insights from ChatGPT. *Technologies, 12*(5), 68.

Lee. (2023). Analyzing web descriptions of cybersecurity breaches in the healthcare provider sector: A content analytics research method. *Computers & Security, 129*, 103185.

Lampreia, F., Madeira, C., & Dores, H. (2024). Digital health technologies and artificial intelligence in cardiovascular clinical trials: A landscape of the European space. *Digital Health*, 10.

Mathew, A. T., & Mani, P. (2023). Strength of deep learning-based solutions to secure healthcare IoT: A critical review. *The Open Biomedical Engineering Journal, 17*, e230505.

Ö zdemir Sönmez, F., Hankin, C., & Malacaria, P. (2022). Decision support for healthcare cyber security. *Computers & Security, 122*, 102865.

Pal, P., Sahana, B. C., & Poray, J. (2024). Secure electronic medical infrastructure for Healthcare 4.0: A voice identity management-based approach. *Procedia Computer Science, 235*, 468-477.

Rich, A., Brandes, K., Mullan, B., & Hagger, M. (2015). Theory of planned behavior and adherence in chronic illness: a meta-analysis. *Journal of Behavioral Medicine, 38*(4), 673-688.

Shamshad, S., Ayub, M. F., Mahmood, K., Kumari, S., Chaudhry, S. A., & Chen, C.-M. (2022). An enhanced scheme for mutual authentication for healthcare services. *Digital Communications and Networks, 8*(2), 150-161.

Shi, D., Lee, T., & Maydeu-Olivares, A. (2019). Understanding the model size effect on SEM fit indices. *Educational and Psychological Measurement, 79*(2), 310-334.

Shreya, S., Chatterjee, K., & Singh, A. (2022). A smart secure healthcare monitoring system with Internet of Medical Things. *Computers and Electrical Engineering, 101*, 107969.

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), 173452.

Trafimow, D. (2009). The theory of reasoned action. *Theory & Psychology, 19*(4), 501-518.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems, 17*(5), 328-376.

Yildirim, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security, 18*(6), 741-759.

ราชกิจจานุเบกษา. (2562ก). *พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562*. สืบค้นจาก https://ratchakitcha.soc.go.th.

ราชกิจจานุเบกษา. (2562ข). *พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562*. สืบค้นจาก https://ratchakitcha.soc.go.th.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Conflicts of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.