ความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรสาธารณสุขในประเทศไทย: กรณีศึกษาโรงพยาบาลพุทธโสธร

Knowledge, Awareness, and Behavior on Information Security of Thai Healthcare Providers: A Case Study of Buddhasothorn Hospital

วิไล ฤทธิเดช[1] และสรวง รุ่งประกายพรรณ[2]*

Vilai Rittidej[1] and Suang Rungpragayphan[2]*

[1]กลุ่มงานเภสัชกรรม โรงพยาบาลพุทธโสธร

[1]Deparment of Pharmacy, Buddhasothorn Hospital

[2]สาขาชีวการแพทย์และสารสนเทศศาสตร์ทางสุขภาพ คณะเภสัชศาสตร์ มหาวิทยาลัยศิลปากร

[2]Department of Biomedicine and Health Informatics,

Faculty of Pharmacy, Silpakorn University

*Corresponding author: RUNGPRAGAYPHAN_S@su.ac.th

Received: November 25, 2022

Revised: January 11, 2023

Accepted: January 17, 2023

บทคัดย่อ

การศึกษานี้เป็นการวิจัยเชิงพรรณา มีวัตถุประสงค์เพื่อศึกษาความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรสาธารณสุข โดยมีโรงพยาบาลพุทธโสธรเป็นกรณีศึกษา กลุ่มตัวอย่าง คือ บุคลากรโรงพยาบาลพุทธโสธร จำนวน 353 คน เครื่องมือที่ใช้ คือ เครื่องมือวัดความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศที่พัฒนาขึ้นใหม่ วิเคราะห์ข้อมูลด้วยสถิติเชิงพรรณนาและสถิติสหสัมพันธ์ ผลการศึกษาพบว่า บุคลากรร้อยละ 54.11 มีความรู้เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศในระดับมากถึงมากที่สุด คำถามหมวดความรู้ทั่วไปเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศมีจำนวนผู้ตอบถูกเฉลี่ยร้อยละ 72.4 คำถามหมวดความรู้ด้านกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศมีจำนวนผู้ตอบถูกเฉลี่ยร้อยละ 79.2 คำถามหมวดความรู้ด้านการรักษาความปลอดภัยเกี่ยวกับพาสเวิร์ดมีจำนวนผู้ตอบถูกเฉลี่ยร้อยละ 78.2 ขณะที่คำถามหมวดความรู้ด้านภัยคุกคามทางสารสนเทศและภัยคุกคามทางไซเบอร์ มีจำนวนผู้ตอบถูกเฉลี่ยเพียงร้อยละ 52.32 จากการประเมินความตระหนักและพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศพบว่าบุคลากรร้อยละ 90.60 มีความตระหนักระดับมากถึงมากที่สุด และร้อยละ 93.75 มีพฤติกรรมที่มีความเสี่ยงต่อการรักษาความมั่นคงปลอดภัยสารสนเทศระดับนาน ๆ ครั้งถึงไม่เคยเลย พฤติกรรมเสี่ยงที่ปฏิบัติในระดับบางครั้งได้แก่ การไม่ Log out เมื่อไม่ได้ใช้งานคอมพิวเตอร์ที่อยู่ในระบบสารสนเทศนานเกิน 15 นาที การไม่แจ้งศูนย์คอมพิวเตอร์ทันทีเมื่อพบความผิดปกติของคอมพิวเตอร์ในเครือข่ายสารสนเทศ การไม่ตรวจสอบแหล่งที่มาของอีเมล การไม่ตรวจสอบ URL ของลิงก์ในเมล และการไม่ตรวจสอบเนื้อหาในอีเมล ไม่สแกนไฟล์ที่แนบมากับอีเมล ความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ มีความสัมพันธ์เชิงบวกกับความรู้และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศในระดับปานกลาง ขณะที่ความรู้ไม่มีความสัมพันธ์อย่างมีนัยสำคัญกับพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ผลการศึกษานี้เป็นสารสนเทศสำคัญสำหรับการวางแผนพัฒนาความรู้ สร้างความตระหนัก และส่งเสริมพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคคลากรสาธารณสุข

คำสำคัญ: การรักษาความมั่นคงปลอดภัยสารสนเทศ ความรู้ ความตระหนัก พฤติกรรม บุคลากรสาธารณสุข

Abstract

This study is descriptive research aimed to study knowledge, awareness, and behavior regarding information security among Thai healthcare providers using Buddhasothorn Hospital as a case study. The sample consisted of 353 Buddhasothorn hospital employees. The study instrument was a newly developed assessment tool to measure knowledge, awareness, and behavior in information security. The data were analyzed using descriptive and correlational statistics. Results showed that 54.11% of staff had knowledge of information security at the highest level. Averagely 72.74%, 79.20%, and 78.20% of staffs correctly answered the questions about general knowledge on information security, information security-related laws, and secured password management, respectively, while only 52.32% of staffs correctly answered the questions about information and cyber threats. From the information security awareness and behavior assessment, 90.60% of staff had awareness at the high to highest level, and 93.75% of staff had risky information security behavior at the seldom to never level. Risky behaviors that were at the sometimes level were “do not log out of the information system when not using the computer for longer than 15 minutes”, “do not notify the computer center immediately after finding an abnormality of the computer in the information network”, “do not verify the URL of links in e-mails”, and “do not verify e-mail content and scan files attached with e-mails”. Awareness of information security had moderately positive correlations with information security knowledge and behavior, while knowledge had no significant relationship with information security behavior. The results of this study provide important information for planning knowledge development, raising awareness, and promoting information security behaviors among healthcare staff.

Keyword: information security, cyber security, healthcare, knowledge, awareness, behavior

บทนำ

ตามที่กระทรวงสาธารณสุขมุ่งพัฒนา Health care 4.0 โดยส่งเสริมการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานของหน่วยงานสุขภาพ ทำให้เกิดการเปลี่ยนแปลงด้านสารสนเทศสุขภาพอย่างรวดเร็ว เช่น การพัฒนาการให้บริการรูปแบบดิจิทัล การพัฒนาและประยุกต์แอปพลิเคชันต่าง ๆ ในการบริหารและบริการ และการเชื่อมโยงข้อมูลทั้งในและนอกหน่วยงานผ่านระบบเครือข่าย (Department of Health Service Support, Ministry of Public Health, 2020) ส่งผลให้ปริมาณข้อมูลที่จัดเก็บในระบบเติบโตขึ้นอย่างมาก ซึ่งข้อมูลส่วนใหญ่มีความสำคัญและอ่อนไหว เช่น ประวัติสุขภาพของผู้ป่วยทำให้มีผู้ไม่ประสงค์ดีพุ่งเป้าโจมตีระบบสารสนเทศของหน่วยบริการสุขภาพเป็นลำดับต้น ๆ มีแนวโน้มการโจมตีสูงขึ้นอย่างรวดเร็ว (Morgan, 2013; HIPPA, 2020; Seh et al., 2020) การถูกโจมตีหรือละเมิดระบบความมั่นคงปลอดภัยสารสนเทศอาจส่งผลกระทบรุนแรงต่อการให้บริการ ความปลอดภัยในการรักษาพยาบาล และการรักษาความลับของผู้รับบริการ ดังตัวอย่างการเข้าโจมตีระบบสารสนเทศขององค์กรต่าง ๆ ทั่วโลก (HIPPA,2020; Seh et al., 2020)

สาเหตุสำคัญของความล้มเหลวในการรักษาความมั่นคงปลอดภัยสารสนเทศ มักเกิดจากพฤติกรรมการใช้งานบนระบบสารสนเทศ ซึ่งสืบเนื่องจากการขาดความรู้และความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ (Van Niekerk & Von Solms, 2006; Zakaria, 2006; Albrechtsen, 2007; Ng, Kankanhalli & Xu, 2009) ดังนั้นแนวทางสำคัญในการส่งเสริมการรักษาความมั่นคงปลอดภัยสารสนเทศที่สำคัญคือการพัฒนาให้บุคลากรมีความรู้ ความตระหนัก และทักษะในการรับมือกับภัยคุกคามทางไซเบอร์ และมีความสามารถในการบรรเทาผลกระทบที่เกิดขึ้น (Department of Health & Human Services USA, 2518) อย่างไรก็ตามจากการทบทวนวรรณกรรมยังไม่พบรายงานการศึกษาสถานการณ์ความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรสาธารณสุขในประเทศไทย ผู้วิจัยจึงสนใจศึกษาสถานการณ์ดังกล่าว เพื่อเป็นสารสนเทศสำคัญสำหรับการพัฒนาบุคลากร และการส่งเสริมการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยนำข้อมูลวิจัยไปสู่การวางแผนพัฒนาบุคลากรให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้น

วัตถุประสงค์การวิจัย

1. เพื่อวัดความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรสาธารณสุข

2. เพื่อหาความสัมพันธ์ระหว่าง ความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรสาธารณสุข

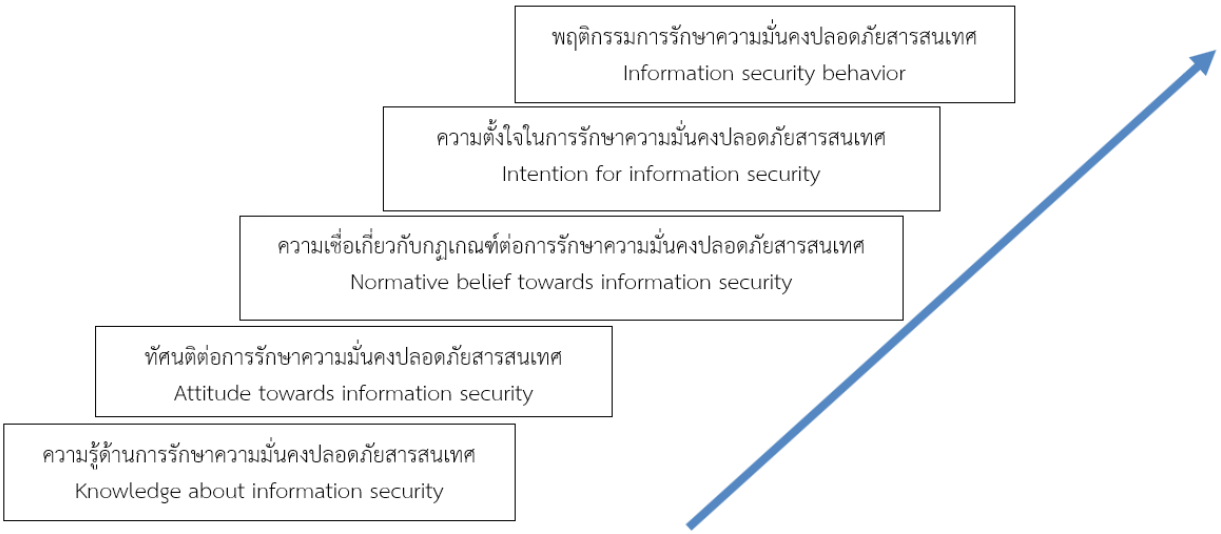
แนวคิดทฤษฎีที่เกี่ยวข้อง

สถานการณ์ความมั่นคงปลอดภัยสารสนเทศต่อระบบสาธารณสุข

ระบบสารสนเทศของหน่วยงานสาธารณสุขมีแนวโน้มถูกโจมตีมากขึ้น มีตัวอย่างการโจมตีและความเสียหายหลายกรณี (HIPPA,2020; Seh et al., 2020) ในปี พ.ศ. 2560 เกิดการโจมตีโดยแรนซัมแวร์ (Ransomware) ชื่อ Wannacry ที่ทำให้เกิดการล็อคข้อมูล และองค์กรไม่สามารถเข้าถึงและใช้งานข้อมูลในระบบ ผู้โจมตีได้เรียกค่าไถ่เพื่อแลกกับรหัสปลดล็อคข้อมูล ส่งผลให้หน่วยงานสาธารณสุขหลายแห่งต้องหยุดให้บริการ และเลื่อนการให้บริการคนไข้ออกไป (Ehrenfeld, 2017) ในปี พ.ศ. 2561 เกิดกรณีจารกรรมข้อมูลส่วนบุคคลและข้อมูลการจ่ายยา 1.5 ล้านคนจากฐานข้อมูลสุขภาพแห่งประเทศสิงค์โปร์ SingHealth (American Accreditation Commission International (AACI), 2018) ในปี พ.ศ. 2563 โรงพยาบาลสระบุรีถูกโจมตีจากแรนซัมแวร์ ทำให้ไม่สามารถเข้าใช้ข้อมูลในระบบสารสนเทศ (Tech & Sci, 2020) และในปี พ.ศ. 2564 โรงพยาบาลเพชรบูรณ์ และสถาบันโรคไตภูมิราชนครินทร์ถูกแฮกเกอร์ลักลอบเจาะข้อมูลและนำข้อมูลผู้ป่วยมาขายในโลกไซเบอร์อาชญากรรมไซเบอร์ (Kongwarakom, 2021; Wipatayotin, 2021) ภัยคุกคามมาในรูปแบบมัลแวร์ แรนซัมแวร์ และการหลอกลวงแบบฟิชชิ่ง (Nifakos et al., 2021) มีรายงานการศึกษาว่า ความรู้เรื่องความมั่นคงปลอดภัยสารสนเทศมีผลต่อความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ (Box & Pottas, 2014; Saracli & Erdoğmuş, 2019; Zwilling et al., 2020)

ทฤษฎีเกี่ยวกับความรู้ ทัศนคติ และพฤติกรรม ต่อการรักษาความมั่นคงปลอดภัยสารสนเทศ

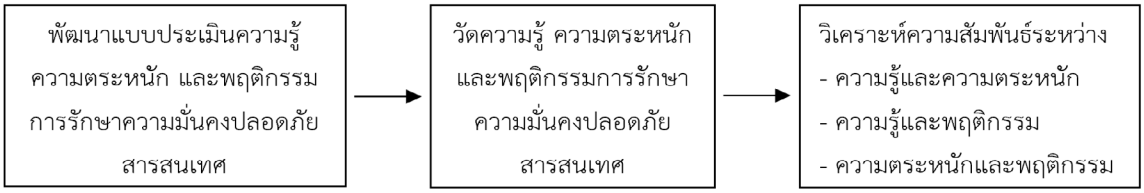
การไม่สามารถรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานได้ มักเป็นผลจากพฤติกรรมการใช้งานระบบสารสนเทศที่ทำให้เกิดช่องโหว่ในการเข้าโจมตีโดยผู้ไม่ประสงค์ดี (Samy, Ahmad & Ismail, 2010; Kruse, Frederick, Jacobson & Monticone, 2017; Erceg, 2019) โดยความรู้ทั่วไปเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ และความเข้าใจเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร มีผลต่อความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคคลากร (Bulgurcu, Cavusoglu & Benbasat, 2009) นอกจากนั้น ความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศจะส่งผลต่อพฤติกรรมในการรักษาความมั่นคงปลอดภัยสารสนเทศ ทั้งทางตรงและทางอ้อม ดังนำเสนอด้วยโมเดลความรู้ ทัศนคติ และพฤติกรรม (model of knowledge-attitude-behavior) ในรูปแบบบันไดขั้นตอน 5 ขั้นของ Khan ดังภาพ 1



ภาพ 1 องค์ประกอบของรูปแบบบันไดขั้นตอน 5 ขั้นตอน

Note. From Effectiveness of information security awareness methods based on psychological theories, by K. Bilal, S. A. Khaled, I. N. Syed and K. K. Muhammad, 2011, *African Journal of Business Management, 5*(26), pp. 10862-10868. Copyright 2011 by Academic Journals

กรอบแนวคิดการวิจัย



ภาพ 2 กรอบแนวคิดการวิจัย

สมมติฐานการวิจัย

1. บุคลากรสาธารณสุขโรงพยาบาลพุทธโสธรไม่น้อยกว่าร้อยละ 50 มีความรู้เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ ระดับความรู้มากถึงมากที่สุด

2. บุคลากรสาธารณสุขโรงพยาบาลพุทธโสธรไม่น้อยกว่าร้อยละ 50 มีความตระหนักระดับมาก ถึงมากที่สุด

3. บุคลากรสาธารณสุขโรงพยาบาลพุทธโสธรไม่น้อยกว่าร้อยละ 50 มีพฤติกรรมที่มีความเสี่ยงต่อการรักษาความมั่นคงปลอดภัยสารสนเทศระดับนาน ๆ ครั้ง ถึงไม่เคย

4.ความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรสาธารณสุขมีความสัมพันธ์เชิงบวก

วิธีดำเนินการวิจัย

การศึกษาครั้งนี้เป็นการวิจัยเชิงพรรณนา โดยศึกษา ณ เวลาใดเวลาหนึ่ง (cross-sectional descriptive study design) ผู้วิจัยกำหนดวิธีดำเนินการวิจัยเป็น 2 ระยะ ได้แก่

ระยะที่ 1 พัฒนาเครื่องมือ สำหรับวัดความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ แบ่งเป็น แบบทดสอบความรู้เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ แบบประเมินความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ และแบบประเมินพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ดำเนินการดังนี้

- ทบทวน สังเคราะห์ และวิเคราะห์วรรณกรรมในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ ภัยคุกคามระบบสารสนเทศ ภัยคุกคามทางไซเบอร์ กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงทางไซเบอร์

- กำหนดความครอบคลุมของเครื่องมือวัดฯ แบ่งหมวดการวัดออกเป็น 4 ด้าน ได้แก่ ด้านทั่วไปเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ด้านการจัดการความปลอดภัยเกี่ยวกับพาสเวิร์ด ด้านภัยคุกคามทางสารสนเทศและภัยคุกคามทางไซเบอร์ ด้านกฎหมาย (การกระทำในลักษณะใดเป็นความผิดตามกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ)

- สร้างเครื่องมือโดยพัฒนาจากคู่มือ “Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients” โดย Healthcare & Public Health Sector Coordinating Councils ของประเทศสหรัฐอเมริกา (Department of Health & Human Services USA, 2518) การศึกษาของ Kathryn Parsons และคณะ เรื่อง“The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies”(Parsons et al., 2017) การศึกษาของ Sen M. Decarlo เรื่อง “Measuring the Application of Knowledge Gained from the Gamification of Cybersecurity Training in Healthcare”(Sean M. DeCarlo, 2020) และการศึกษาของ Aleksandar ERCEG เรื่อง “Information Security: Threat From Employee”(Erceg, 2019)

- ตรวจสอบความตรงตามเนื้อหา (content validity test) โดยผู้ทรงคุณวุฒิ 5 ท่าน กำหนดค่าดัชนีความสอดคล้อง (IOC-Index of Item Objective Congruence) สำหรับการยอมรับ เมื่อมีค่า > 0.5 นำเครื่องมือมาปรับปรุงตามคำแนะนำของผู้ทรงคุณวุฒิ จากนั้นนำไปทดสอบกับบุคลากรสาธารณสุขหน่วยงานอื่น จำนวน 30 ราย

- ทดสอบความเที่ยง (reliability test) ตามเกณฑ์ดังนี้ แบบวัดความรู้ ใช้ค่า KR-20 กำหนดเกณฑ์ KR-20 มากกว่า 0.5 สำหรับแบบประเมินความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ และแบบประเมินพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ใช้ค่าสัมประสิทธิ์แอลฟาครอนบาช กำหนดเกณฑ์มากกว่า 0.70

ระยะที่ 2 รวบรวมข้อมูล ความรู้ ความตระหนักและพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรสาธารณสุขโรงพยาบาลพุทธโสธร โดยให้ผู้เข้าร่วมวิจัยเป็นผู้ตอบแบบวัดด้วยตนเอง ผ่าน Google form เมื่อได้ข้อมูลครบตามที่กำหนด นำข้อมูลที่ได้มาวิเคราะห์ด้วยสถิติเชิงพรรณาและสถิติสหสัมพันธ์

ประชากรและกลุ่มตัวอย่าง

ประชากรในการศึกษาครั้งนี้ คือ บุคลากรสาธารณสุขโรงพยาบาลพุทธโสธร จังหวัดฉะเชิงเทรา (จำนวน 1,530 คน) จำนวนตัวอย่างคำนวณโดยใช้สูตรของ Taro Yamane กำหนดความคลาดเคลื่อนที่ยอมรับ ได้ร้อยละ 5.0 ได้จำนวนตัวอย่าง 320 คน เลือกกลุ่มตัวอย่างโดยประชาสัมพันธ์ขอความร่วมมือผ่านกลุ่มไลน์บุคคลากรโรงพยาบาล ให้ผู้ที่ทำงานบนระบบสารสนเทศฯ และประสงค์ให้ข้อมูลเป็นผู้ตอบตามความสมัครใจ กำหนดผู้ที่ตอบแบบสอบถามออนไลน์ที่ตอบแบบสอบถามที่สมบูรณ์กลับคืนในช่วงเวลาที่กำหนด (มีผู้ตอบกลับ 353 คน มีลักษณะดังแสดงในตาราง 1)

ตาราง 1

ลักษณะของตัวอย่าง

ลักษณะประชากร	จำนวน (คน)	ร้อยละ
เพศ		
ชาย	48	13.6
หญิง	305	86.4
อายุ (ปี)		
ต่ำกว่า 20 – 30	89	19.6
31 – 40	87	24.6
41 -50	121	34.3
51 – 60	76	21.5
ระดับการศึกษาสูงสุด		
ต่ำกว่าปริญญาตรี	49	13.9
ปริญญาตรี	247	70.0
ปริญญาโท	42	11.9
สูงกว่าปริญญาโท	15	4.2
ประเภทตำแหน่ง		
ข้าราชการ	285	80.7
พนักงานราชการ	8	2.3
พนักงานกระทรวงสาธารณสุข	43	12.2
ลูกจ้างกระทรวงสาธารณสุข	7	2.0
อื่นๆ	10	2.8
ตำแหน่งงาน		
พยาบาล	167	47.3
เภสัชกร	35	9.9
แพทย์/ทันตแพทย์	28	7.9
เจ้าพนักงานเภสัชกรรม/เจ้าหน้าที่ห้องยา	30	8.5
เจ้าพนักงานธุรการ/เจ้าพนักงานพัสดุ/เจ้าพนักงานการเงินและบัญชี	20	5.7
นักเทคนิคการแพทย์/เจ้าพนักงานวิทยาศาสตร์การแพทย์/เจ้าหน้าที่ห้องปฏิบัติการ	18	5.1
ผู้ช่วยพยาบาล/พนักงานช่วยเหลือคนไข้	13	3.7
นักวิชาการสาธารณสุข	11	3.1
อื่นๆ	31	8.8

การพิทักษ์สิทธิ์ของกลุ่มตัวอย่าง การศึกษานี้ผ่านการพิจารณาและรับรองจากคณะกรรมการจริยธรรมการวิจัยในมนุษย์มหาวิทยาลัยศิลปากร เลขที่ REC 64.1122-183-7788 ลงวันที่ 22 พฤศจิกายน 2564 และคณะกรรมการจริยธรรมการวิจัยในมนุษย์โรงพยาบาลพุทธโสธร เลขที่ BSH-IRB 001/2565 ลงวันที่ 30 ธันวาคม 2564 อาสาสมัครได้รับคำอธิบายถึงวัตถุประสงค์ รายละเอียดเกี่ยวกับงานวิจัย เข้าร่วมอย่างเป็นอิสระโดยเป็นผู้ตอบแบบสอบถาม และลงความยินยอมด้วยตนเองในแบบสอบถาม ข้อมูลที่ได้จะถูกเก็บเป็นความลับและนำเสนอผลการวิจัยเป็นภาพรวมเท่านั้น

เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัย เป็นแบบสอบถามออนไลน์ แบ่งเป็น 4 ตอน ได้แก่ ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ตอนที่ 2 แบบวัดความรู้เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ ตอนที่ 3 แบบประเมินความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ ตอนที่ 4 แบบประเมินพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ

แบบวัดความรู้เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศจำนวน 30 ข้อ แบ่งคำถามแยกหมวดความรู้เป็น 4 ด้าน ได้แก่ ด้านความรู้ทั่วไปเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ (5 ข้อ) ด้านการจัดการความปลอดภัยเกี่ยวกับพาสเวิร์ด (3 ข้อ) ด้านภัยคุกคามทางสารสนเทศและภัยคุกคามทางไซเบอร์ (18 ข้อ) ด้านกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ (4 ข้อ) เมื่อตอบถูกจะได้ข้อละ 1 คะแนน คิดเป็น 30 คะแนน แบ่งระดับความรู้เป็น 5 ระดับดังนี้ น้อยที่สุด 1-6 คะแนน น้อย 7-12 คะแนน ปานกลาง 13-18 คะแนน มาก 19-24 คะแนน และ มากที่สุด 25-30 คะแนน คำนวณร้อยละของผู้ที่ตอบถูกแต่ละข้อ จากนั้นหาค่าเฉลี่ยร้อยละผู้ตอบถูกของความรู้แต่ละด้าน (เช่นด้านความรู้ทั่วไปมีข้อสอบ 5 ข้อ นำร้อยละของผู้ตอบถูกทั้ง 5 ข้อมาหาค่าเฉลี่ย ได้ค่าเฉลี่ยร้อยละผู้ตอบถูกด้านความรู้ทั่วไป)

แบบประเมินความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นคำถามแบบประเมินค่า (rating scale) 5 ระดับ โดยความตะหนักแบ่งเป็นความตระหนักเชิงบวกและเชิงลบ ให้ค่าประเมินดังตาราง 2

นำคะแนนความตระหนักมาคำนวณค่าเฉลี่ยและจัดระดับความตระหนักตามระดับ ดังนี้ คะแนนเฉลี่ย 1.00–1.80 =ตระหนักน้อยที่สุด คะแนนเฉลี่ย 1.81–2.60=ตระหนักน้อย คะแนนเฉลี่ย 2.61–3.40=ตระหนักปานกลาง คะแนนเฉลี่ย 3.41–4.20=ตระหนักมาก คะแนนเฉลี่ย 4.21–5.00=ตระหนักมากที่สุด

ส่วนแบบประเมินพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นคำถามแบบประเมินค่า 5 ระดับ พฤติกรรมที่ควรปฏิบัติให้ค่าประเมินดังตาราง 3

นำคะแนนพฤติกรรมมาคำนวณค่าเฉลี่ย และนำมาจัดระดับการปฏิบัติพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศที่ไม่ควรปฏิบัติ 5 ระดับ ดังนี้ คะแนนเฉลี่ย 1.00–1.80=เสมอ คะแนนเฉลี่ย 1.81–2.60=บ่อย คะแนนเฉลี่ย 2.61–3.40=บางครั้ง คะแนนเฉลี่ย 3.41–4.20=นาน ๆ ครั้ง คะแนนเฉลี่ย 4.21–5.00=ไม่เคยเลย

เครื่องมือวัดความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่พัฒนาขึ้นได้ผ่านการทดสอบความตรงตามเนื้อหาโดยผู้ทรงคุณวุฒิ 5 ท่าน (IOC มากกว่า 0.5) มีจำนวนข้อดังนี้ แบบวัดความรู้ 30 ข้อ แบบประเมินความตระหนัก 12 ข้อ แบบประเมินพฤติกรรม 12 ข้อ เครื่องมือที่ปรับปรุงตามคำแนะนำของผู้ทรงคุณวุฒิไปทดสอบความเที่ยงกับกลุ่มบุคลากรสาธารณสุข จำนวน 30 คน ซึ่งแบบวัดความรู้ มีค่า KR-20 เท่ากับ 0.65 แบบประเมินความตระหนัก ฯ มีค่าสัมประสิทธิ์แอลฟาของครอนบาช 0.78 และแบบประเมินพฤติกรรม ฯ มีค่าสัมประสิทธิ์แอลฟาของครอนบาช 0.70 เครื่องมือที่พัฒนาขึ้นมีคุณสมบัติและคุณภาพอยู่ในเกณฑ์ที่ดี สามารถนำไปใช้ในการวัดความรู้ ความตระหนัก และพฤติกรรมของบุคลากรสาธารณสุข และการศึกษาวิจัยที่เกี่ยวข้องได้ สามารถดูรายละเอียดเครื่องมือได้ที่ https://shorturl.asia/DKIm8

ตาราง 2

ระดับและคะแนนความตระหนัก

ระดับ	ความตระหนักเชิงบวก	ความตระหนักเชิงลบ
ไม่เห็นด้วยอย่างยิ่ง	1	5
ไม่เห็นด้วย	2	4
ไม่แน่ใจ	3	3
เห็นด้วย	4	2
เห็นด้วยอย่างยิ่ง	5	1

ตาราง 3

ระดับและคะแนนพฤติกรรม

ความถี่ในการปฏิบัติ	พฤติกรรมที่ควรปฏิบัติ	พฤติกรรมที่ไม่ควรปฏิบัติ
ไม่เคยเลย	1	5
นาน ๆ ครั้ง (น้อยกว่าปีละครั้ง)	2	4
บางครั้ง (1-4 ครั้งต่อปี)	3	3
บ่อย (1-4 ครั้งต่อเดือน)	4	2
เสมอ (ทุกครั้งที่มีกิจกรรมนั้น ๆ)	5	1

การเก็บรวบรวมข้อมูล

หลังจากผ่านการรับรองจริยธรรมการวิจัยในมนุษย์จากมหาวิทยาลัยศิลปากรและโรงพยาบาลพุทธโสธรแล้ว ผู้วิจัยขอความร่วมมือเจ้าหน้าที่โรงพยาบาลพุทธโสธรช่วยตอบแบบวัดความรู้ฯ โดยประชาสัมพันธ์ลิงก์แบบสอบถามงานวิจัยผ่านกลุ่มไลน์เจ้าหน้าที่โรงพยาบาลพุทธโสธรดังที่ระบุในประชากรและกลุ่มตัวอย่าง ทำการเก็บข้อมูลช่วงเดือนมกราคม-กุมภาพันธ์ 2565 โดยผู้เข้าร่วมงานวิจัยเป็นผู้ตอบด้วยตนเอง (self-assessment) ผ่านทาง google form

สถิติที่ใช้ในการวิเคราะห์ข้อมูล

วิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ข้อมูลความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศใช้สถิติเชิงพรรณา (descriptive statistics) ได้แก่ การแจกแความถี่ (frequency) ร้อยละ (percentage) ค่าเฉลี่ย (mean) และส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation--SD) การวิเคราะห์ความสัมพันธ์ระหว่างความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศใช้สถิติสหสัมพันธ์เพียร์สัน (Pearson correlation Coefficient)

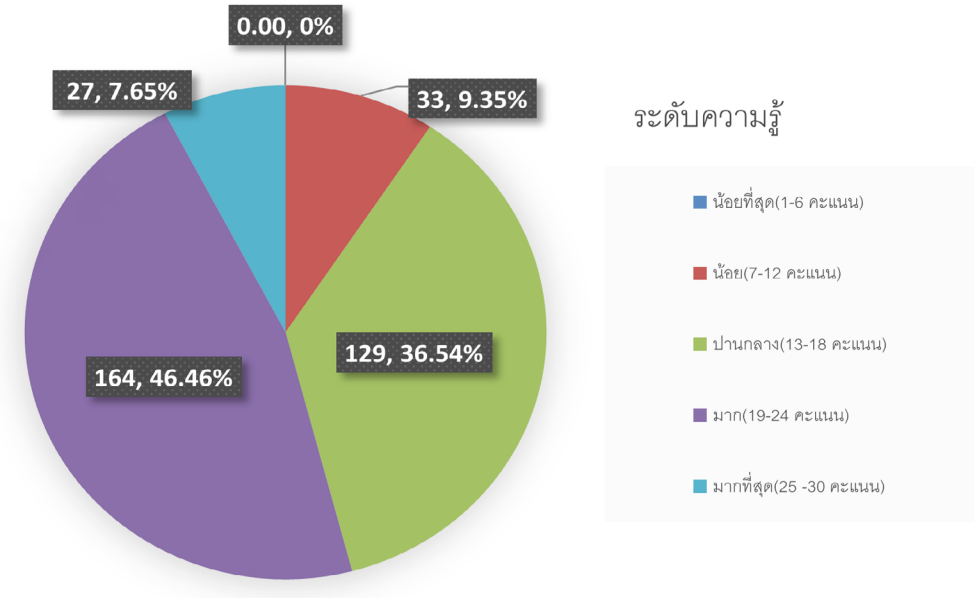
ผลการวิจัย

ความรู้เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ

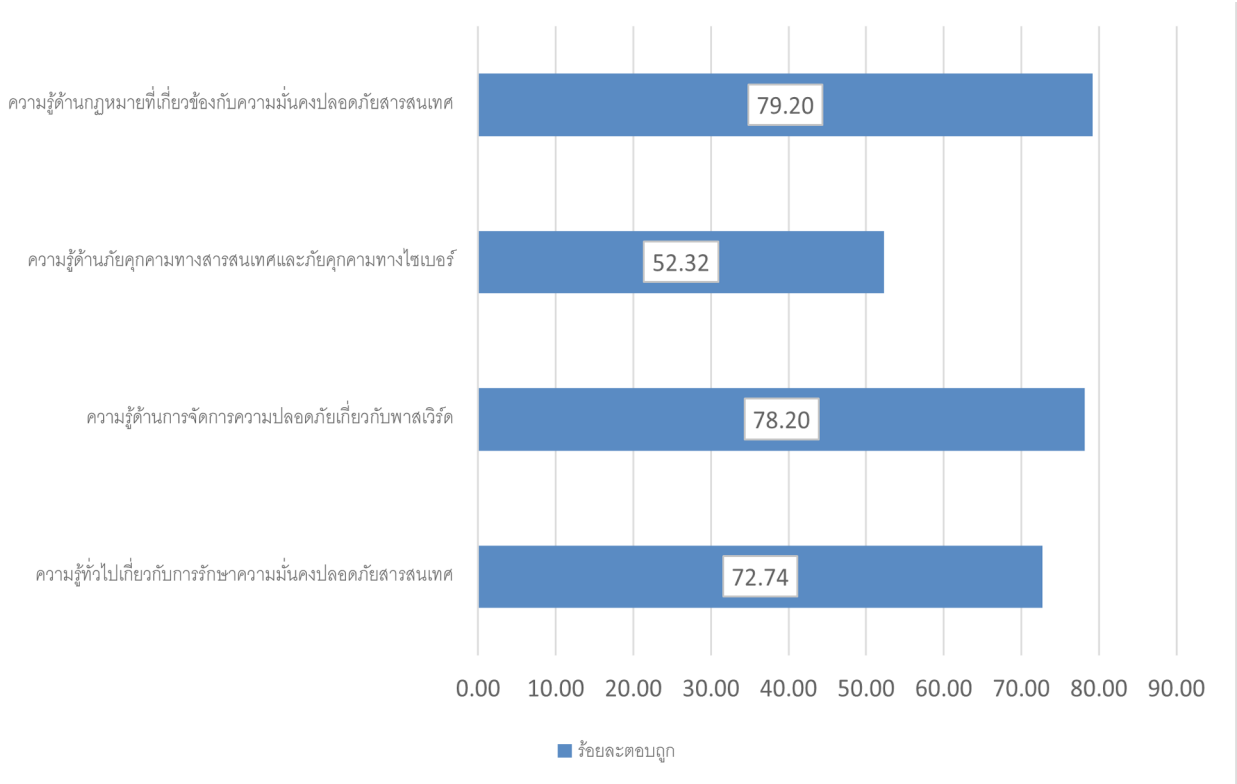
ผลการศึกษาความรู้เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ พบว่า บุคลากรที่มีความรู้ตั้งแต่ระดับมาก ถึงระดับมากที่สุดมีจำนวน 191 คน (ร้อยละ 54.11) ดังแสดงในภาพ 3 จากความรู้ที่กำหนดไว้ 4 หมวด ได้แก่ (1) ความรู้ทั่วไปเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ (2) ด้านการจัดการพาสเวิร์ด (3) ด้านภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ ภัยคุกคามทางไซเบอร์ และ (4) ความรู้ด้านกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ พบว่า กลุ่มตัวอย่างตอบคำถามถูกต้องในแต่ละหมวด คิดเป็นร้อยละเฉลี่ยดังแสดงในภาพ 4 ซึ่งจะเห็นว่าหมวดที่ 1 2 และ 4 มีผู้ตอบถูกเฉลี่ยสูงกว่าร้อยละ 70 ขณะที่หมวดที่ 3 ซึ่งเป็นเรื่องภัยคุกคามความมั่นคงปลอดภัยสารสนเทศและภัยคุกคามทางไซเบอร์นั้นมีร้อยละเฉลี่ยผู้ตอบถูกเพียง 52.32

ความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ

ผลการศึกษาความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรโรงพยาบาลพุทธโสธร พบว่า กลุ่มตัวอย่างมีความตระหนักอยู่ในระดับตระหนักมากถึงมากที่สุดจำนวน 341 ราย (ร้อยละ 90.60) ดังแสดงในภาพ 5 โดยกลุ่มตัวอย่างมีความตระหนักมากที่สุดในเรื่อง การไม่บอกพาสเวิร์ดแก่ผู้อื่น (คะแนนเฉลี่ย 4.64) รองลงมาได้แก่ ทุกคนมีส่วนร่วมในการรักษาความมั่นคงปลอดภัยสารสนเทศ (คะแนนเฉลี่ย 4.61) การตั้งพาสเวิร์ดที่คาดเดาได้อยาก (คะแนนเฉลี่ย 4.58) การสำรองข้อมูลอย่างสม่ำเสมอ (คะแนนเฉลี่ย 4.54) ตามลำดับ ดังแสดงในตาราง 4



ภาพ 3 จำนวนและร้อยละของบุคลากรสาธารณสุขที่มีความรู้ในแต่ละระดับความรู้เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ



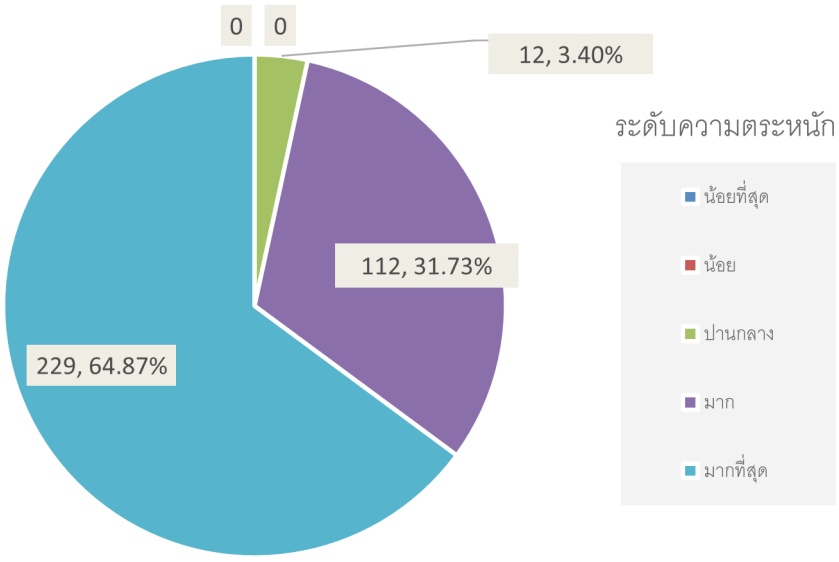
ภาพ 4 ร้อยละเฉลี่ยของผู้ตอบคำถามถูกในแต่ละหมวดความรู้เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ

พฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ

ผลการศึกษาพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศพบว่า บุคลากรส่วนใหญ่มีระดับการปฏิบัติพฤติกรรมที่มีความเสี่ยง ระดับนาน ๆ ครั้ง ถึงไม่เคยเลย จำนวน 330 ราย คิดเป็นร้อยละ 93.75 ดังแสดงในภาพ 6 เมื่อพิจารณาแยกตามพฤติกรรมที่มีความเสี่ยงต่อระบบสารสนเทศ พบว่า การปฏิบัติพฤติกรรมที่มีความเสี่ยงระดับบางครั้ง (1-4 ครั้งต่อปี) ได้แก่ การไม่ Log out เมื่อไม่ได้ใช้งานคอมพิวเตอร์ที่อยู่ในระบบสารสนเทศนานเกิน 15 นาที การไม่แจ้งศูนย์คอมพิวเตอร์ทันทีเมื่อพบความผิดปกติของคอมพิวเตอร์ในเครือข่ายสารสนเทศ การไม่ตรวจสอบแหล่งที่มาของอีเมล การไม่ตรวจสอบ URL ของลิงก์ในเมล และการไม่ตรวจสอบเนื้อหาในอีเมล ไม่สแกนไฟล์ที่แนบมากับอีเมล ดังแสดงในตาราง 5

ความสัมพันธ์ระหว่างความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ

จากการศึกษาความสัมพันธ์ระหว่างความรู้กับความตระหนัก ความรู้กับพฤติกรรม และความตระหนักกับพฤติกรรม เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยหาความสัมพันธ์ด้วยค่าสัมประสิทธิ์สหสัมพันธ์บางส่วน (partial correlation) พบว่าความตระหนักมีความสัมพันธ์เชิงบวกกับความรู้และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศในระดับปานกลาง ที่ระดับนัยสำคัญ 0.05 (ค่า r=0.36 และ 0.43 ตามลำดับ) ขณะที่ความรู้กับพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศไม่มีความสัมพันธ์กันอย่างมีนัยสำคัญ ดังแสดงในตาราง 6 กล่าวคือ ความตระหนักต่อการรักษาความมั่นคงปลอดภัยสารสนเทศที่เพิ่มขึ้น มีความสัมพันธ์กับความรู้และพฤติกรรมการรักษาความมั่นคงปลอดภัยที่เพิ่มขึ้น

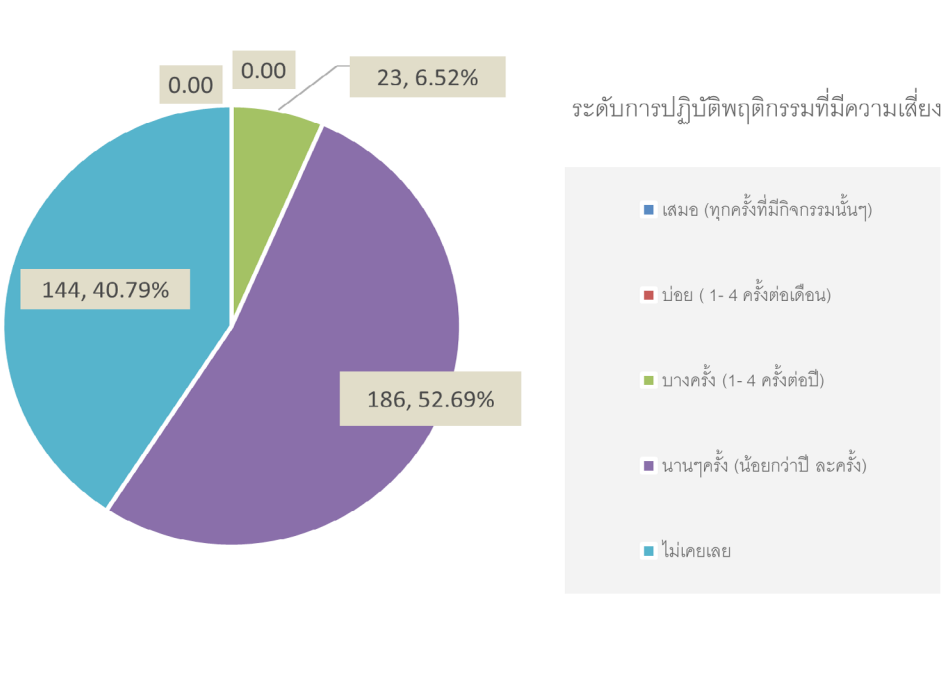


ภาพ 5 จำนวนและร้อยละของบุคลากรแบ่งตามระดับความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ

ตาราง 4

ความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรโรงพยาบาลพุทธโสธร

ข้อความ	Mean	SD	ระดับความตระหนัก
1. ทุกคนในองค์กรมีส่วนต่อการรักษาความมั่นคงปลอดภัยสารสนเทศ	4.61	0.79	มากที่สุด
2. เหตุการณ์ที่ รพ.สระบุรี ถูกโจมตีทางไซเบอร์ ในเดือนกันยายน 2563 ส่งผลกระทบต่อการให้บริการที่ล่าช้า เนื่องจากการเข้าถึงประวัติเก่าทำไม่ได้ เหตุการณ์ในลักษณะนี้ “มีโอกาสเกิด” กับโรงพยาบาลที่เราทำงานอยู่	4.34	0.83	มาก
3. การใช้ Antivirus ที่ถูกต้องตามลิขสิทธิ์เป็นการสิ้นเปลือง มีราคาแพง ไม่คุ้มค่า	4.16	1.00	มาก
4. ทุกครั้งที่ไม่ได้ใช้งานในระบบคอมพิวเตอร์นานกว่า 15 นาที ต้อง log out เสมอ	4.04	1.02	มาก
5. การอัปเดตระบบปฏิบัติการคอมพิวเตอร์อย่างสม่ำเสมอ เป็นเรื่องยุ่งยาก และเสียเวลา เมื่อเทียบกับประโยชน์ที่ได้รับ	4.26	0.76	มาก
6. เมื่อนำอุปกรณ์จัดเก็บข้อมูล เช่น USB Drive External Hard Disk มาใช้กับคอมพิวเตอร์ที่อยู่บนระบบสารสนเทศ มีโอกาสเสี่ยงต่อการติดไวรัสทั้งเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อกันอยู่	4.30	0.83	มาก
7. มีการประกาศขายข้อมูลของโรงพยาบาลเพชรบูรณ์ในโลกไซเบอร์ เมื่อทำการตรวจสอบพบว่า เป็นเพียงข้อมูลเกี่ยวกับ รายชื่อผู้รับบริการ สิทธิการรักษา ชื่อแพทย์ที่ดูแล ไม่ใช่ข้อมูลด้านการรักษา “จึงไม่ส่งผลกระทบต่อคนไข้ และโรงพยาบาล”	4.23	0.92	มาก
8. การบอก Username และพาสเวิร์ด ให้ผู้อื่น ไม่น่าจะเป็นอะไร	4.64	0.71	มากที่สุด
9. ควรสำรองข้อมูลอย่างสม่ำเสมอ	4.54	0.67	มากที่สุด
10. ควรตั้งพาสเวิร์ดที่คาดเดาได้ยาก	4.58	0.66	มากที่สุด
11. การใช้งานบนเครือข่ายอินเตอร์เน็ตผ่านระบบคอมพิวเตอร์ของหน่วยงาน จะไม่มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ (Cyber Attack)	3.90	1.15	มาก
12. การใช้งานอีเมลต้องทำด้วยความระมัดระวัง	4.47	0.63	มาก



ภาพ 6 จำนวนและร้อยละของบุคลากรแบ่งตามระดับการปฏิบัติพฤติกรรมที่มีความเสี่ยง

ตาราง 5

ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของพฤติกรรมการรักษาความมั่นคงปลอดภัย

ข้อความ	Mean	SD	ระดับการปฏิบัติพฤติกรรมที่มีความเสี่ยง
1. ไม่ Log out เมื่อไม่ได้ใช้งานคอมพิวเตอร์ที่อยู่ในระบบสารสนเทศ นานเกิน 15 นาที	3.38	1.30	บางครั้ง
2. เข้าเว็บไซต์ที่มีความเสี่ยง เช่น เว็บไซต์อนาจาร เว็บไซต์ที่มีการเผยแพร่ซอฟท์แวร์ละเมิดลิขสิทธิ์จากคอมพิวเตอร์ที่เชื่อมต่อในระบบสารสนเทศของโรงพยาบาล	4.83	0.51	ไม่เคย
3. ขณะดูหนัง ผ่านเว็บไซต์เมื่อมี pop-up โฆษณา มักจะกด pop-up ดู	4.80	0.52	ไม่เคย
4. นำโปรแกรมละเมิดลิขสิทธิ์ มาใช้กับคอมพิวเตอร์ที่อยู่ในระบบสารสนเทศ	4.77	0.75	ไม่เคย
5. ดาวน์โหลดโปรแกรมจากเว็บไซต์ มาติดตั้งในคอมพิวเตอร์ที่อยู่ในระบบสารสนเทศของโรงพยาบาล	4.76	0.63	ไม่เคย
6. ไม่สแกนไวรัสก่อนเปิดไฟล์ เมื่อต้องการใช้ข้อมูลผ่านอุปกรณ์พกพา เช่น USB Drive External Hard Drive กับเครื่องคอมพิวเตอร์ที่อยู่บนระบบสารสนเทศของโรงพยาบาล	3.87	1.15	นานๆ ครั้ง

ตาราง 5 (ต่อ)

ข้อความ	Mean	SD	ระดับการปฏิบัติพฤติกรรมที่มีความเสี่ยง
7. เมื่อพบความผิดปกติของคอมพิวเตอร์ที่ใช้งานในเครือข่ายสารสนเทศ เช่น มี pop-up ขึ้นมาตลอดเวลา รบกวนการทำงาน เครื่องทำงานช้าผิดปกติมาก ๆ จากที่เคยเป็น ท่านไม่แจ้งศูนย์คอมพิวเตอร์ทันที	3.48	1.42	บางครั้ง
8. บอกบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของท่านให้ผู้อื่นลงข้อมูลแทน	4.51	0.76	ไม่เคย
9. จดบัญชีผู้ใช้งาน และรหัสผ่าน ไว้ตามจุดที่ผู้อื่นอาจเห็นได้ เช่น บนโต๊ะทำงาน หน้าจอคอมพิวเตอร์ บนปฏิทิน เป็นต้น	4.79	0.59	ไม่เคย
10. รหัสผ่านที่ท่านตั้งเป็นรหัสที่ง่ายต่อการคาดเดา เช่น 1234 123456789 password วันเกิดของท่าน เบอร์โทรศัพท์ ข้อมูลส่วนตัว คำที่มีความหมายในพจนานุกรม เป็นต้น	3.74	1.30	นานๆ ครั้ง
11. ไม่ตรวจสอบแหล่งที่มาของอีเมล ตรวจสอบ URL ของลิงก์ในอีเมล และตรวจสอบเนื้อหาที่อยู่ในอีเมล	2.94	1.42	บางครั้ง
12. ไม่สแกนไฟล์ที่แนบมากับอีเมล ด้วยซอฟต์แวร์ Antivirus ก่อนเปิดใช้งาน	2.95	1.48	บางครั้ง

ตาราง 6

ค่าสัมประสิทธิ์สหสัมพันธ์เพียร์สัน ระหว่างตัวแปรในการรักษาความมั่นคงปลอดภัยสารสนเทศ

ตัวแปร	ความรู้เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ	ความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ	พฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ
ความรู้เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ	1		
ความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ	0.36**	1	
พฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ	0.08	0.43**	1

หมายเหตุ ** มีนัยสำคัญทางสถิติที่ระดับ .05

การอภิปรายผล

จากการศึกษาพบว่า บุคลากรโรงพยาบาลพุทธโสธรมีความรู้เรื่องการรักษาความมั่นคงปลอดภัย อยู่ในเกณฑ์พอใช้ มีบุคลากรเพียงร้อยละ 54.11 ที่มีความรู้ระดับมากถึงมากที่สุด โดยความรู้ด้านที่บุคคลากรตอบถูกเกินร้อยละ 70 ได้แก่ การจัดการพาสเวิร์ด กฎหมายที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ และความรู้ทั่วไปเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งเป็นความรู้ที่ตรงกับประกาศข้อปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาล ที่ถูกติดตั้งให้แสดงที่หน้าจอคอมพิวเตอร์ก่อนการเข้าใช้งาน สอดคล้องกับการศึกษาวิจัยของ Safa และคณะที่พบว่าบุคคลากรในองค์กรจะมีความรู้ตามนโยบายองค์กร (Safa, Von Solms & Furnell, 2016; Chantanawaranont & Vibultangman, 2017) อย่างไรก็ตามมีบุคลากรเฉลี่ยเพียงร้อยละ 52.32 ที่ตอบคำถามด้านภัยคุกคามสารสนเทศและภัยคุกคามทางไซเบอร์ได้ถูกต้อง ซึ่งสอดคล้องกับผลการศึกษาในต่างประเทศที่พบว่าบุคลากรทางสาธารณสุขมีความรู้น้อยในเรื่องภัยคุกคามทางไซเบอร์ และนำไปสู่การไม่สามารถรักษาความมั่นคงปลอดภัยสารสนเทศได้ (Nifakos et al., 2021; Singh, 2022) การขาดความรู้ด้านภัยคุกคามสารสนเทศ ภัยคุกคามทางไซเบอร์นั้น อาจเกิดจากนโยบายการส่งเสริมให้หน่วยงานสาธารณสุขเข้าสู่การให้บริการรูปแบบดิจิทัล ซึ่งในช่วงแรกเน้นให้บุคลากรมีความสามารถในการใช้งานระบบต่าง ๆ เป็นสำคัญ โดยขาดการสร้างเสริมความความรู้ ทักษะ และความตระหนักในการรับมือกับภัยคุกคามทางไซเบอร์แก่บุคลากรสาธารณสุข (Office of the Permanent Secretary Ministry of Public Health, 2022) จึงมีความจำเป็นเร่งด่วนในการให้ความรู้และสร้างทักษะ เพื่อให้เกิดความตระหนักอันเป็นปัจจัยสำคัญ ที่มีอิทธิพลต่อพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ แก่บุคคลากรสาธารณสุขให้เท่าทันความก้าวหน้าของเทคโนโลยีและภัยคุกคามทางไซเบอร์

เมื่อพิจารณาความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ ในภาพรวมบุคลากรโรงพยาบาลพุทธโสธรมีความตระหนักที่ดี คือ มีความตระหนักระดับมากถึงมากที่สุด เกินกว่าร้อยละ 90 และบุคลากรส่วนใหญ่มีพฤติกรรมการรักษาความมั่นคงปลอดภัยที่เหมาะสม คือ ปฏิบัติพฤติกรรมที่มีความเสี่ยงระดับนาน ๆ ครั้ง ถึงไม่เคยเลย เกินกว่าร้อยละ 90 อย่างไรก็ตามยังพบพฤติกรรมที่มีความเสี่ยงระดับบางครั้ง ได้แก่ การไม่ตรวจสอบที่มาของอีเมล ไม่สแกนไฟล์ที่แนบมากับอีเมล หรือไฟล์จากอุปกรณ์พกพาด้วยซอฟแวร์แอนตี้ไวรัส ซึ่งพฤติกรรมเหล่านี้มีความสัมพันธ์กับการขาดความรู้ด้านภัยคุกคามทางไซเบอร์ ในการศึกษานี้พบว่า ความตระหนักมีความสัมพันธ์กับความรู้และพฤติกรรมในการรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งสอดคล้องกับหลายการศึกษา (Box & Pottas, 2013; Parsons, McCormac, Butavicius, Pattinson & Jerram, 2014; Safa et al., 2015; Saracli & Erdoğmuş, 2019; Zwilling et al., 2022) แต่กลับพบว่า ความรู้กับพฤติกรรมไม่มีความสัมพันธ์กันในทางสถิติ สอดคล้องกับการศึกษาของ Sarkar ที่พบว่า บุคลากรสาธารณสุขให้ความสำคัญกับความเร่งรีบต่อการรักษาผู้ป่วย ทำให้ขาดความตระหนักในความร่วมมือในการรักษาความมั่นคงปลอดภัยสารสนเทศ (Sarkar, 2020) ดังนั้นการส่งเสริมเรื่องความรู้เพียงด้านเดียวอาจไม่เพียงพอ ควรทำควบคู่กับการสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ โรงพยาบาลควรรณรงค์และสร้างเสริมความรู้ ความตระหนักเพื่อนำไปสู่พฤติกรรมที่ควรปฏิบัติเหล่านี้แก่บุคคลากรอย่างเร่งด่วน เพื่อประสิทธิภาพการรักษาความมั่นคงปลอดภัยสารสนเทศ

ผลการศึกษานี้สะท้อนให้เห็นสถานการณ์ความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรสาธารณสุขไทย โดยมีโรงพยาบาลพุทธโสธรที่มีโครงสร้างของบุคลากรในหน่วยงานหลากหลายวิชาชีพ มีระบบงานที่เป็นไปตามมาตรฐานที่กำหนดจากการแผนการพัฒนาของกระทรวงที่มุ่งพัฒนาเข้าสู่การให้บริการรูปแบบดิจิทัล อันมีลักษณะคล้ายคลึงกันในหน่วยงานสาธารณสุขไทย จึงอาจกล่าวได้ว่าบุคลากรสาธารณสุขไทย ยังขาดความรู้เรื่องภัยคุกคามสารสนเทศ ภัยคุกคามทางไซเบอร์ สอดคล้องกับพฤติกรรมที่ละเลยการป้องกันภัยคุกคามทางไซเบอร์ อันเป็นช่องโหว่ให้ผู้ไม่ประสงค์ดีเข้าโจมตีระบบ เป็นผลให้ไม่สามารถรักษาความมั่นคงปลอดภัยสารสนเทศ ส่งผลการกระทบต่อการให้บริการและความปลอดภัยของผู้รับบริการ

ข้อเสนอแนะ

จากการศึกษาในครั้งนี้พบว่า บุคลากรสาธารณสุขยังขาดความรู้ด้านภัยคุกคามสารสนเทศ และภัยคุกคามทางไซเบอร์ จึงควรมีกิจกรรมให้ความรู้ เสริมทักษะ สร้างความตระหนัก และฝึกปฏิบัติเมื่อต้องเผชิญหน้ากับภัยคุกคามทางไซเบอร์ การวิจัยมีข้อจำกัดบางประการได้แก่ การประเมินเป็นลักษณะการประเมินตนเอง ซึ่งผลการประเมินอาจไม่เป็นจริงทั้งหมด การตอบกลับของบุคคลากรบางสายวิชาชีพมีจำนวนน้อย อาจเนื่องมาจากบุคคลากรเหล่านั้นต้องปฏิบัติหน้าที่สำคัญเร่งด่วนในการดูแลผู้ป่วย แนวทางในการศึกษาในอนาคต ควรทำการศึกษาถึงปัจจัยอื่น (นอกเหนือจาก ความรู้และพฤติกรรม) ที่มีผลส่งเสริมความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรสาธารณสุข

โดยสรุปพบว่า บุคลากรส่วนใหญ่มีความรู้เรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศอยู่ในเกณฑ์พอใช้ มีความตระหนักที่ดี และมีพฤติกรรมที่เหมาะสม แต่บุคลากรส่วนใหญ่ยังขาดความรู้ด้านภัยคุกคามสารสนเทศ และภัยคุกคามทางไซเบอร์ ซึ่งเป็นเรื่องสำคัญ จึงจำเป็นต้องเสริมความรู้และทักษะในการรับมือกับภัยคุกคามที่เพิ่มขึ้นอย่างรวดเร็ว และทุกองค์กรควรให้การสนับสนุนอย่างจริงจัง เนื่องจากภัยคุกคามทางไซเบอร์ มีโอกาสเกิดขึ้นได้กับทุกองค์กร

กิตติกรรมประกาศ

การศึกษานี้ได้รับทุนอุดหนุนการวิจัยประเภทนักศึกษาระดับบัณฑิตศึกษา จากกองทุนวิจัยและสร้างสรรค์ คณะเภสัชศาสตร์ มหาวิทยาลัยศิลปากร (Research and Creative Fund, Faculty of Pharmacy, Silpakorn University) ขอขอบพระคุณ ดร.นายแพทย์นวนรรณ ธีระอัมพรพันธุ์ ที่ให้คำปรึกษาในการสร้างเครื่องมือฯในงานวิจัยครั้งนี้

References

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289. https://doi.org/10.1016/j.cose.2006.11.004

American Accreditation Commission International (AACI). (2018). *Personal info of 1.5m Sing health patients, including PM Lee, stolen in Singapore's worst cyber attack.* Retrieved from https://aacihealthcare.com/news/personal-info-of-1-5m-singhealth-patients-stolen-in-singapores-worst-cyber-attack/

Bilal, K., Khaled, S. A., Syed, I. N., & Muhammad, K. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management, 5*(26), 10862-10868. doi: 10.5897/AJBM11.067

Box, D., & Pottas, D. (2013). Improving information security behaviour in the healthcare context. *Procedia Technology, 9*, 1093-1103. https://doi.org/10.1016/j.protcy.2013.12.122

Box, D., & Pottas, D. (2014). A model for information security compliant behaviour in the healthcare context. *Procedia Technology, 16*, 1462-1470. https://doi.org/10.1016/j.protcy.2014.10.166

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors. *Conference: Proceedings IEEE CSE'09, 12th IEEE International Conference on Computational Science and Engineering, August 29-31, 2009, Vancouver, BC, Canada* (pp. 476-481). BC, Canada: IEEE

Chantanawaranont, P., & Vibultangman, A. (2017). Compliance with information technology security policies of employees in the system of a large real estate development company. *EAU Heritage Journal Science and Technology, 11*(2), 122-135. (in Thai)

Department of Health & Human Services USA. (2518). *Health industry cybersecurity practices: Managing threats and protecting patients*. USA: Healthcare & Public Health Sector Coordinating Councils.

Department of Health Service Support, Ministry of Public Health. (2020). *Digital development strategic plan for the health service system and the public health system, a 5-year period of the Department of Health Service Support, 2021 - 2025*. Retrieved from https://hss.moph.go.th/image/plan1.pdf (in Thai)

Ehrenfeld J. M. (2017). WannaCry, cybersecurity and health information technology: A time to act. *Journal of Medical Systems, 41*(7), 104. https://doi.org/10.1007/s10916-017-0752-1

Erceg, A. (2019). Information security: Threat from employees. *Tehnički Glasnik, 13*(2), 123-128. doi:10.31803/tg-20180717222848

HIPPA. (2020). *Healthcare data breach report 2019*. Retrieved from https://www.hipaajournal.com/january-2019-healthcare-data-breach-report/

Kongwarakom, S. (2021, Sep 7). *Hacked hospital patients' data 'not important'*. Bangkok Post. Retrieved from https://www.bangkokpost.com/thailand/general/2177887/hacked-hospital-patients-data-not-important. (in Thai)

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and health care: Official journal of the European Society for Engineering and Medicine, 25*(1), 1–10. https://doi.org/10.3233/THC-161263

Morgan, S. (2013). *Healthcare industry to spend $125 billion on cybersecurity from 2020 to 2025, Cyber Security Ventures*. Retrieved from https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825. https://doi.org/10.1016/j.dss.2008.11.010

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors, 21*(15), 5119. https://doi.org/10.3390/s21155119

Office of the Permanent Secretary Ministry of Public Health.(2022). *Government inspection issues that focus on issue 4 digital health (health information system and medical technology)*. Retrieved from https://drive.google.com/drive/folders/1RuQlUOqqHTyddseJFd3DnC2ObusqdyoE. (in Thai)

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66, 40-51. https://doi.org/10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176. https://doi.org/10.1016/j.cose.2013.12.003

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78. https://doi.org/10.1016/j.cose.2015.05.012

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

Sarkar, S., Vance, A., Ramesh, B., Demestihas, M., & Wu, D. T. (2020). The influence of professional subculture on information security policy violations: A field study in a healthcare context. *Information Systems Research, 31*(4), 1240-1259. https://doi.org/10.1287/isre.2020.0941

Samy, G. N., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health Informatics Journal, 16*(3), 201–209. https://doi.org/10.1177/1460458210377468

Saracli, S., & Erdoğmuş, A. (2019). Determining the effects of information security knowledge on information security awareness via structural equation modelings. *Hacettepe Journal of Mathematics and Statistics, 48*(4), 1201-1212. https://dergipark.org.tr/tr/pub/hujms/issue/47862/604508

Sean M. DeCarlo. (2020). *Measuring the application of knowledge gained from the gamification of cybersecurity training in healthcare* (Master's thesis). Robert Morris University. USA

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare (Basel, Switzerland), 8*(2), 133. https://doi.org/10.3390/healthcare8020133

Singh, I., & SINGH, Y. (2022). Cyber-security knowledge and practice of nurses in private hospitals in Northern Durban, Kwazulu-Natal. *Journal of Theoretical and Applied Information Technology, 100*(1), 246- 267. http://www.jatit.org/volumes/Vol100No1/21Vol100No1.pdf

Tech & Sci. (2020, Sep 9). Ransomware attack on Saraburi hospital. Thai News Agency. Retriveved from https://tna.mcot.net/techsci-533371

Van Niekerk, J., & Von Solms, R. (2006). Understanding information security culture: A conceptual framework. *Conference: Proceedings of the ISSA 2006 from Insight to Foresight Conference, 5-7 July 2006, Balalaika Hotel, Sandton, South Africa* (pp. 1-10). South Africa: Information Security South Africa (ISSA). https://digifors.cs.up.ac.za/issa/2006/Proceedings/Full/21_Paper.pdf

Wipatayotin, A. (2021, Sep 8). Hacker steals 40,000 patients' data from kidney hospital. *Bangkok Post*. Retrieved from https://www.bangkokpost.com/thailand/general/2178503/hacker-steals-40-000-patients-data-from-kidney-hospital. (in Thai)

Zakaria, O. (2006). Internalisation of information security culture amongst employees through basic security knowledge. In: S. Fischer-Hübner, K. Rannenberg, L. Yngström, & S. Lindskog, (Eds) *Security and Privacy in Dynamic Environments. SEC 2006. IFIP International Federation for Information Processing, vol 201*. Boston: Springer. https://doi.org/10.1007/0-387-33406-8_38

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269