ปัจจัยที่มีผลกระทบต่อระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของผู้ประกอบวิชาชีพบัญชี

Factors Influencing the Level of Cybersecurity Awareness among Accounting Professionals

พรพรรณ วรรณศิริ
นักวิชาการอิสระ
pohnpan.wann@gmail.com

วชิระ บุณยเนตร
รองศาสตราจารย์ประจำ คณะพาณิชยศาสตร์และการบัญชี
จุฬาลงกรณ์มหาวิทยาลัย
wachira@cbs.chula.ac.th

Pohnpan Wannasiri
independent scholar
pohnpan.wann@gmail.com

Wachira Boonyanet, PhD, CPA, FAC
Associate Professor, Chalalongkorn Business School
wachira@cbs.chula.ac.th

ปัจจัยที่มีผลกระทบต่อระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของผู้ประกอบวิชาชีพบัญชี

พรพรรณ วรรณศิริ
นักวิชาการอิสระ
pohnpan.wann@gmail.com

วชิระ บุณยเนตร
รองศาสตราจารย์ประจำ คณะพาณิชยศาสตร์และการบัญชี
จุฬาลงกรณ์มหาวิทยาลัย
wachira@cbs.chula.ac.th

วันที่ได้รับบทความต้นฉบับ: 4 มิถุนายน 2568
วันที่แก้ไขปรับปรุงบทความ: 20 สิงหาคม 2568
วันที่ตอบรับตีพิมพ์บทความ: 21 สิงหาคม 2568

บทคัดย่อ

การศึกษานี้ มีวัตถุประสงค์ในการศึกษาปัจจัยที่มีผลกระทบต่อระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของผู้ประกอบวิชาชีพบัญชี ปัจจัยที่ศึกษาประกอบด้วย (1) ด้านความรู้พื้นฐาน (2) ด้านการฝึกอบรม (3) ด้านทัศนคติ และ (4) ด้านพฤติกรรม เป็นการศึกษาเชิงปริมาณ โดยเก็บข้อมูลจากผู้ประกอบวิชาชีพบัญชีในประเทศไทย จำนวน 305 คน ผ่านแบบสอบถามระหว่างเดือนตุลาคม 2567 ถึง มกราคม 2568 วิเคราะห์ข้อมูลโดยใช้สถิติเชิงพรรณนาและสถิติเชิงอนุมาน กำหนดระดับนัยสำคัญที่ 0.05

ผลการศึกษาพบว่า กลุ่มตัวอย่างมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์โดยรวมอยู่ในระดับมากที่สุด โดยด้านความรู้พื้นฐาน และการฝึกอบรมเป็นปัจจัยที่ได้รับความสำคัญมากที่สุด รองลงมาคือด้านทัศนคติ และด้านพฤติกรรม ตามลำดับ นอกจากนี้ ข้อมูลทั่วไปด้านประชากรศาสตร์ ได้แก่ อายุ ใบอนุญาตประกอบวิชาชีพ ประเภทหน่วยงานที่สังกัด สาขาที่เชี่ยวชาญ และประสบการณ์ในการทำงานมีผลต่อระดับการตระหนักรู้อย่างมีนัยสำคัญทางสถิติ ขณะที่เพศและระดับการศึกษาไม่มีผล การศึกษานี้เสนอให้มีการพัฒนาหลักสูตรและโปรแกรมฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์ที่สอดคล้องกับความต้องการของผู้ประกอบวิชาชีพบัญชี บูรณาการความรู้ด้านไซเบอร์ในหลักสูตรบัญชีระดับปริญญาตรี กำหนดให้ความรู้ด้านไซเบอร์เป็นส่วนหนึ่งของข้อกำหนดใบอนุญาต สร้างวัฒนธรรมองค์กรที่เน้นการป้องกันไซเบอร์ และส่งเสริมความร่วมมือระหว่างสภาวิชาชีพบัญชี สถาบันการศึกษา และหน่วยงานรัฐ เพื่อพัฒนาแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมกับบริบทของวิชาชีพบัญชีไทย

คำสำคัญ: ความมั่นคงปลอดภัยทางไซเบอร์ การตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ ผู้ประกอบวิชาชีพบัญชี

Factors Influencing the Level of Cybersecurity Awareness among Accounting Professionals

Pohnpan Wannasiri
independent scholar
pohnpan.wann@gmail.com

Wachira Boonyanet, PhD, CPA, FAC
Associate Professor, Chalalongkorn Business School
wachira@cbs.chula.ac.th

Received: June 4, 2025
Revised: August 20, 2025
Accepted: August 21, 2025

ABSTRACT

This study aims to investigate the factors influencing cybersecurity awareness levels among accounting professionals. The study examines four key factors: (1) fundamental knowledge, (2) training, (3) attitudes, and (4) behaviors. Employing a quantitative research methodology, data was collected from 305 accounting professionals in Thailand through questionnaires administered between October 2024 and January 2025. The analysis employed both descriptive and inferential statistics with a significance level set at 0.05.

The findings reveal that respondents demonstrated the highest level of cybersecurity awareness overall. Fundamental knowledge and training were identified as the most significant factors, followed by attitudes and behaviors, respectively. Furthermore, demographic variables including age, professional certification, organizational affiliation, area of expertise, and work experience significantly influenced awareness levels, while gender and educational background showed no significant impact. This study proposes the development of cybersecurity curricula and training programs tailored to accounting professionals' needs, integration of cybersecurity knowledge into undergraduate accounting programs, incorporation of cybersecurity expertise into professional licensing requirements, establishment of organizational cultures emphasizing cybersecurity prevention, and promotion of collaborative networks among professional associations, educational institutions, and government agencies to develop cybersecurity practices appropriate for the Thai accounting profession context.

Key word: Cybersecurity, Cybersecurity Awareness, Accounting Professionals

บทนำ

เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในภาคธุรกิจ การเงิน และการบัญชี ซึ่งการดำเนินงานด้านบัญชีได้พึ่งพาระบบสารสนเทศในการจัดเก็บข้อมูล การทำบัญชี การตรวจสอบ และการรายงานผล อย่างไรก็ตาม ความสะดวกและประสิทธิภาพจากเทคโนโลยีนำมาซึ่งความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ (SEC, 2018) ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) กลายเป็นความท้าทายสำคัญสำหรับวิชาชีพบัญชีที่ต้องรับผิดชอบข้อมูลทางการเงินที่อ่อนไหว รายงาน Global Risks Report ของ World Economic Forum ระบุว่าความเสี่ยงทางไซเบอร์อยู่ในอันดับที่ 5 ของความเสี่ยงระดับโลก โดยผู้เชี่ยวชาญร้อยละ 39 เห็นว่าการโจมตีทางไซเบอร์มีความเป็นไปได้สูงที่จะก่อวิกฤตสากล (World Economic Forum, 2024).

การโจมตีทางไซเบอร์ถือเป็นภัยคุกคามที่สำคัญต่อระบบงานด้านบัญชีและการเงิน เนื่องจากข้อมูลทางบัญชีมีความอ่อนไหวสูงและเป็นเป้าหมายหลักของผู้ไม่หวังดี การถูกโจมตีอาจส่งผลให้เกิดการเข้าถึงโดยไม่ได้รับอนุญาต การบิดเบือน หรือการสูญหายของข้อมูลบัญชี ซึ่งบั่นทอนความถูกต้องของการรายงานทางการเงินและนำไปสู่การหยุดชะงักของการดำเนินงาน เช่น ต้องกลับไปใช้การบันทึกบัญชีด้วยมือ ความล่าช้าในการยื่นรายงาน หรือการไม่ปฏิบัติตามข้อกำหนดทางกฎหมาย กรณีที่พบจริง เช่น เหตุการณ์บริษัทในประเทศสหรัฐอเมริกาที่ต้องยื่นล้มละลายเนื่องจากระบบบัญชีถูกโจมตีด้วย ransomware แสดงให้เห็นถึงความเสี่ยงที่รุนแรง นอกจากนี้ การโจมตีขนาดใหญ่ยังส่งผลกระทบในวงกว้าง ทั้งการลดความเชื่อมั่นของผู้มีส่วนได้เสีย การสูญเสียมูลค่าทางการเงิน การถูกปรับลดอันดับเครดิต ตลอดจนการเพิ่มความเสี่ยงเชิงระบบต่อภาคการเงินโดยรวม

สำหรับประเทศไทย สถิติจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พบว่าในไตรมาสที่ 1 ปี 2568 ภาคการเงินการธนาคารถูกโจมตีร้อยละ 18 ของทั้งหมด โดยมีเหตุการณ์ภัยคุกคาม 105 ครั้ง ซึ่งเป็นเกือบครึ่งหนึ่งของทั้งปี 2567 (NCSA, 2025) สะท้อนสถานการณ์ความเสี่ยงที่ทวีความรุนแรง แม้ผู้ประกอบวิชาชีพบัญชีมีบทบาทสำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลทางการเงิน แต่งานวิจัยเกี่ยวกับปัจจัยที่มีผลต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในกลุ่มนี้ยังมีจำกัด การศึกษาส่วนใหญ่เน้นกลุ่มเป้าหมายทั่วไป เช่น นักศึกษา พนักงานไอที หรือบุคลากรภาครัฐ โดยเฉพาะในบริบทประเทศไทย ยังขาดความเข้าใจเชิงลึกเกี่ยวกับอิทธิพลของปัจจัยด้านประชากรศาสตร์ต่อระดับการตระหนักรู้

ผู้ศึกษาจึงมีความสนใจศึกษาปัจจัยที่มีผลกระทบต่อระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของผู้ประกอบวิชาชีพบัญชี เพื่อเติมเต็มช่องว่างในองค์ความรู้เกี่ยวกับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในบริบทของวิชาชีพบัญชีไทย ที่เกี่ยวข้องกับการจัดการข้อมูลทางการเงินอ่อนไหว การสร้างความตระหนักรู้ด้านความปลอดภัยทาง ไซเบอร์จึงเป็นสิ่งจำเป็น โดยพบว่าเหตุการณ์ความปลอดภัยส่วนใหญ่มีต้นเหตุจากความผิดพลาดของมนุษย์ เช่น การเปิดเผยรหัสผ่าน การคลิกลิงก์อันตราย หรือการสื่อสารข้อมูลอย่างไม่ระมัดระวัง การฝึกอบรมอย่างต่อเนื่องที่มีองค์ประกอบแบบจำลองสถานการณ์ เกมจำลอง หรือการทดสอบ phishing ที่ออกแบบดี สามารถลดความเสี่ยงเหล่านี้ได้อย่างมีนัยสำคัญ ยิ่งไปกว่านั้น พนักงานบัญชียังทำหน้าที่เป็น “แนวป้องกันคน” ที่มีความสำคัญไม่แพ้ระบบเทคนิค การส่งเสริมให้บุคลากร มีความรู้ด้านไซเบอร์จึงช่วยเสริมความมั่นใจในระบบบัญชี เพิ่มความน่าเชื่อถือ และลดความเสี่ยงในการจัดทำรายงานทางการเงิน โดยมีวัตถุประสงค์ เพื่อศึกษาปัจจัยที่มีผลกระทบต่อระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของ ผู้ประกอบวิชาชีพบัญชี และเพื่อวิเคราะห์ปัจจัยที่ส่งผลให้เกิดความความแตกต่างของระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของผู้ประกอบวิชาชีพบัญชี

แนวคิด ทฤษฎี หรือวรรณกรรมทางการบัญชีที่เกี่ยวข้อง

ความหมายของผู้ประกอบวิชาชีพบัญชี

พระราชบัญญัติวิชาชีพบัญชี พ.ศ. 2547 ของประเทศไทย (Royal Gazette, 2004) ได้ให้คำจำกัดความผู้ประกอบวิชาชีพบัญชี หมายถึง ผู้ประกอบวิชาชีพในด้านการทำบัญชี การสอบบัญชี การบัญชีบริหาร การวางระบบบัญชี การบัญชีภาษีอากร การศึกษาและเทคโนโลยีการบัญชี และบริการเกี่ยวกับการบัญชีด้านอื่นตามที่กำหนดโดยกฎกระทรวง สหพันธ์นักบัญชีระหว่างประเทศ (International Federation of Accountants, IFAC) ได้ให้คำนิยามว่า ผู้ประกอบวิชาชีพบัญชี คือ บุคคลที่มีความสามารถในการทำงานในวิชาชีพบัญชี ซึ่งได้แสดงออกและพัฒนาความสามารถทางวิชาชีพอย่างต่อเนื่อง และต้องปฏิบัติตามจรรยาบรรณตามที่กำหนดโดยองค์กรวิชาชีพบัญชีหรือหน่วยงานที่ออกใบอนุญาต

ความหมายของการตระหนักรู้

การตระหนักรู้ (Awareness) หมายถึง กระบวนการทางจิตวิทยาในการรับรู้ ทำความเข้าใจ และให้ความสำคัญต่อข้อมูลที่เกี่ยวข้องกับสิ่งแวดล้อมหรือสถานการณ์ที่บุคคลกำลังเผชิญ (Endsley, 1995) ตามทฤษฎีพฤติกรรมที่วางแผนไว้โดย Ajzen (1991) การรับรู้ของบุคคลเป็นจุดเริ่มต้นสำคัญของกระบวนการเปลี่ยนแปลงพฤติกรรม ในบริบทของความมั่นคงปลอดภัยทางไซเบอร์ การตระหนักรู้หมายถึงระดับความเข้าใจของผู้ใช้งานเกี่ยวกับความสำคัญของการรักษาความปลอดภัยของข้อมูล ความเสี่ยงที่อาจเกิดขึ้น และความรับผิดชอบในการปฏิบัติตามแนวทางเพื่อปกป้องข้อมูลและระบบเครือข่าย (Shaw et al., 2009)

ทฤษฎีที่เกี่ยวข้องกับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

ทฤษฎีการรับรู้ภัยคุกคามโดย Rogers (1975) อธิบายว่าบุคคลจะปกป้องตนเองเมื่อรับรู้ความรุนแรงของภัยคุกคาม ความเสี่ยง ประสิทธิภาพของพฤติกรรมป้องกัน และความสามารถของตนเอง ทฤษฎีพฤติกรรมตามแผนโดย Ajzen (1991) ชี้ให้เห็นว่าเจตนารมณ์ในการกระทำขึ้นอยู่กับทัศนคติ อิทธิพลทางสังคม และการรับรู้การควบคุมพฤติกรรม Dunning-Kruger Effect อธิบายลักษณะของบุคคลที่มีความสามารถต่ำแต่ประเมินตนเองสูงเกินจริง ขณะที่บุคคลที่มีความสามารถสูงมักประเมินตนเองต่ำกว่าความเป็นจริง (Kruger & Dunning, 1999) ทฤษฎีหน้าที่ของทัศนคติ (Functional Theories of Attitudes) โดย Katz (1960) ช่วยทำความเข้าใจแรงจูงใจที่แตกต่างกันเบื้องหลังทัศนคติและพฤติกรรม

กฎหมายและข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์สำหรับวิชาชีพบัญชี

ในประเทศไทย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (Royal Gazette, 2017) และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Royal Gazette, 2019) เป็นกฎหมายหลักที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ สภาวิชาชีพบัญชีมีแนวปฏิบัติเกี่ยวกับการใช้เทคโนโลยีสารสนเทศและการบริหารความเสี่ยงด้านไซเบอร์ ในระดับสากล มาตรฐาน ISO/IEC 27001 (ISO/IEC, 2013) และ GDPR (European Parliament, 2016) มีผลกระทบต่อการดำเนินงานของผู้ประกอบวิชาชีพบัญชี กฎหมายเหล่านี้เป็นกลไกสำคัญที่ส่งเสริมให้วิชาชีพบัญชีดำเนินงานภายใต้หลักความมั่นคงปลอดภัยทางไซเบอร์อย่างมีประสิทธิภาพ

ปัจจัยที่มีผลต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

การโจมตีทางไซเบอร์มีหลายประเภทและรูปแบบที่พัฒนาอย่างต่อเนื่อง โดยการโจมตีที่พบบ่อย ได้แก่ มัลแวร์ (Malware) เช่น ไวรัส โทรจัน และแรนซัมแวร์ ที่มุ่งทำลายหรือเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่, ฟิชชิง (Phishing) ที่ใช้การส่งอีเมลหรือข้อความลวงเพื่อหลอกขโมยข้อมูลส่วนบุคคลหรือข้อมูลบัญชี, การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service: DoS/DDoS) ที่ทำให้ระบบล่มและไม่สามารถใช้งานได้, รวมถึง การเจาะระบบ (Hacking/Brute Force Attack) เพื่อเข้าถึงฐานข้อมูลโดยไม่ได้รับอนุญาต การถูกโจมตีลักษณะเหล่านี้ส่งผลกระทบทั้งในเชิงการสูญหายหรือบิดเบือนของข้อมูลทางบัญชี การหยุดชะงักของระบบงานบัญชีและการเงิน การสูญเสียทางเศรษฐกิจและชื่อเสียงองค์กร ตลอดจนความเสี่ยงต่อความเชื่อมั่นของผู้ใช้งบการเงิน เพื่อป้องกันเหตุการณ์ดังกล่าว องค์กรควรดำเนินมาตรการเชิงรุก เช่น การติดตั้งและอัปเดตซอฟต์แวร์ด้านความปลอดภัยอย่างสม่ำเสมอ การเข้ารหัสและสำรองข้อมูลทางบัญชี การใช้ระบบยืนยันตัวตนหลายชั้น (Multi-factor Authentication) การเฝ้าระวังและตรวจสอบความผิดปกติของระบบ และการสร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ให้แก่บุคลากรบัญชี ซึ่งมาตรการเหล่านี้ช่วยลดความเสี่ยงและเพิ่มความเชื่อมั่นในคุณภาพของข้อมูลทางการบัญชีได้อย่างมีประสิทธิภาพ

การศึกษาของ Fattah et al. (2023) พบว่าความรู้ ทัศนคติ พฤติกรรม และการฝึกอบรมมีผลกระทบเชิงบวกต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของนักศึกษามหาวิทยาลัย Trim and Lee (2019) พบความสัมพันธ์อย่างมีนัยสำคัญระหว่างการตระหนักรู้กับพฤติกรรมการป้องกันภัยคุกคามทางไซเบอร์ของบุคลากรในองค์กร นอกจากนี้ Thammasiri and Wongthongdee (2022) พบว่าบุคลากรเอกชนมีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในระดับสูง และการละเมิดข้อมูลทางไซเบอร์มีต้นตอมาจากความผิดพลาดของบุคคล เช่น การตั้งรหัสผ่านที่ไม่ปลอดภัยหรือการตกเป็นเหยื่อของอีเมลฟิชชิง ซึ่งย้ำถึงบทบาทของมนุษย์ในฐานะจุดอ่อน แต่ในขณะเดียวกันก็เป็นกุญแจสำคัญในการเสริมสร้างความมั่นคงทางไซเบอร์หากมีการพัฒนาความรู้และความตระหนักรู้ที่เพียงพอ การศึกษานี้นำกรอบแนวคิดดังกล่าวมาประยุกต์ใช้กับผู้ประกอบวิชาชีพบัญชีเพื่อศึกษาปัจจัยที่มีผลกระทบต่อระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของกลุ่มวิชาชีพนี้ ซึ่งประกอบด้วย 4 ด้านหลัก ดังนี้

ด้านความรู้พื้นฐานต่อความมั่นคงปลอดภัยทางไซเบอร์ Zwilling et al. (2022) พบว่าระดับความรู้มีความสัมพันธ์เชิงบวกกับการตระหนักรู้ โดยความรู้เป็นตัวขับเคลื่อนสำคัญที่มีอิทธิพลต่อพฤติกรรมด้านความปลอดภัยสำหรับผู้ประกอบวิชาชีพบัญชี ความรู้พื้นฐานมีความจำเป็นอย่างยิ่งเนื่องจากต้องรับผิดชอบข้อมูลทางการเงินที่อ่อนไหว **ด้านการฝึกอบรมต่อความมั่นคงปลอดภัยทางไซเบอร์** การฝึกอบรมที่ต่อเนื่องและหลากหลายรูปแบบส่งเสริมให้บุคลากรเข้าใจความสำคัญของการปฏิบัติตามนโยบายและเพิ่มทักษะการประเมินสถานการณ์ (Fattah et al. 2023) Swain (2014) เสนอให้บูรณาการ หัวข้อความมั่นคงปลอดภัยไซเบอร์เข้ากับหลักสูตรหรือพัฒนาเป็นรายวิชาเฉพาะ **ด้านทัศนคติต่อความมั่นคงปลอดภัยทางไซเบอร์** ทัศนคติหมายถึงชุดความเชื่อ ความรู้สึก และแนวโน้มในการกระทำที่บุคคลมีต่อสิ่งใดสิ่งหนึ่ง (Ajzen, 1991) ทัศนคติเชิงบวกต่อความมั่นคงปลอดภัยทางไซเบอร์ส่งเสริมให้บุคคลปฏิบัติตามมาตรการป้องกันอย่างเคร่งครัด (Ifinedo, 2014) สำหรับผู้ประกอบวิชาชีพบัญชี ทัศนคติที่ดีช่วยรักษามาตรฐานทางจริยธรรมและความปลอดภัยของข้อมูลทางการเงิน **ด้านพฤติกรรมต่อความมั่นคงปลอดภัยทางไซเบอร์** Felt et al. (2017) ศึกษาการใช้โปรโตคอล (Hypertext Transfer Protocol Secure, HTTPS) ซึ่งป้องกันภัยคุกคามในสามด้าน คือ ความลับของข้อมูล ความถูกต้องของข้อมูล และการยืนยันตัวตนของเซิร์ฟเวอร์ ความสำเร็จของการป้องกันต้องอาศัยพฤติกรรมที่เหมาะสมของผู้ใช้งาน

นอกจากนี้ ด้านประชากรศาสตร์ที่มีผลกระทบต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ Branley-Bell et al. (2022) ศึกษาความแตกต่างด้านอายุ และเพศในการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ ในบริบทของการใช้เทคโนโลยีสารสนเทศและการสื่อสาร พบว่าการรักษาความปลอดภัยของอุปกรณ์ ผู้ใช้อายุน้อยมีแนวโน้มที่จะรักษาความปลอดภัยของอุปกรณ์ เช่น การล็อกหน้าจอ มากกว่าผู้ใช้อายุมาก ในทางตรงกันข้าม ผู้ใช้อายุมากกลับมีแนวโน้มที่จะสร้างรหัสผ่านที่ปลอดภัย และติดตั้งการอัปเดตอย่างสม่ำเสมอมากกว่าผู้ใช้อายุน้อย และการศึกษาไม่พบความแตกต่างทางเพศที่มีนัยสำคัญในการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ อีกทั้ง Hasan et al. (2024) พบว่าการบูรณาการความมั่นคงปลอดภัยทางไซเบอร์เข้ากับการปฏิบัติงานบัญชีส่งผลกระทบอย่างมีนัยสำคัญต่อบทบาทและความสามารถที่จำเป็นสำหรับ ผู้ประกอบวิชาชีพบัญชี นอกจากนี้ Mamade and Dabala (2021) พบว่าสาขาวิชาที่ศึกษามีความสัมพันธ์ที่มีนัยสำคัญระหว่างสาขาวิชาที่ศึกษากับระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ และเน้นย้ำความสำคัญของการพัฒนาโปรแกรมฝึกอบรมและการสร้างความตระหนักรู้ที่เหมาะสมกับแต่ละสาขาความเชี่ยวชาญ โดยคำนึงถึงลักษณะเฉพาะและความต้องการของแต่ละกลุ่ม

วิธีการศึกษา

ประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้ในการศึกษาครั้งนี้ ได้แก่ ผู้ประกอบวิชาชีพบัญชีที่ทำงานอยู่ในประเทศไทย ที่มีความรู้และประสบการณ์ในสาขาที่เกี่ยวข้อง ซึ่งกลุ่มเป้าหมายต้องมีความเป็นอิสระในการตอบคำถามเพื่อเป็นตัวแทนของผู้ประกอบวิชาชีพที่มีความน่าเชื่อถือ เนื่องจากประชากรมีขนาดใหญ่และไม่ทราบจำนวนประชากรที่แน่นอน ดังนั้นผู้ศึกษาได้กำหนดกลุ่มตัวอย่างตามหลักของ Cochran (1977) ที่ระดับความเชื่อมั่นร้อยละ 95 โดยเมื่อคำนวณตามสูตรแล้วจะได้จำนวนกลุ่มตัวอย่างทั้งสิ้น 385 ตัวอย่าง

การสร้างเครื่องมือในการศึกษาครั้งนี้ดำเนินการผ่านขั้นตอนที่เป็นระบบ โดยเริ่มจากการศึกษาบทความทางวิชาการ งานวิจัย และวิทยานิพนธ์ที่เกี่ยวข้องเพื่อพัฒนาแบบสอบถาม จากนั้นจึงนำแบบสอบถามเสนอต่ออาจารย์ที่ปรึกษาเพื่อตรวจสอบความถูกต้องและปรับปรุงให้สอดคล้องกับวัตถุประสงค์การศึกษา การทดสอบความเชื่อมั่นของเครื่องมือดำเนินการโดยทดลองแบบสอบถามกับกลุ่มตัวอย่างจำนวน 30 คน ผ่านช่องทาง Social Media เพื่อให้การกระจายข้อมูลมีประสิทธิภาพ ผลการทดสอบความเชื่อมั่นแสดงค่าสัมประสิทธิ์ครอนบัคอัลฟาเท่ากับ 0.821 ซึ่งสูงกว่าเกณฑ์ที่ยอมรับได้ที่ 0.70 ตามงานศึกษาของ Cronbach (1990) ขั้นตอนสุดท้ายเป็นการปรับปรุงแบบสอบถามตามคำแนะนำของกลุ่มตัวอย่าง จากนั้นจึงสร้างแบบสอบถามด้วย Google Forms และกระจายผ่านช่องทางต่างๆ เช่น กลุ่ม Line กลุ่ม Facebook และ Instagram

เครื่องมือที่ใช้ในการเก็บและรวบรวมข้อมูล

การศึกษานี้เป็นการเก็บข้อมูลปฐมภูมิ ซึ่งรวบรวมข้อมูลโดยใช้แบบสอบถาม ระหว่างวันที่ 15 ตุลาคม 2567 ถึง 31 มกราคม 2568 โดยให้กลุ่มตัวอย่างเป็นผู้ตอบแบบสอบถามด้วยตนเอง มีทั้งหมด 3 ส่วน ได้แก่ คำถามปลายปิด 2 ส่วน และปลายเปิด 1 ส่วน โดยส่วนที่ 1 คำถามข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ส่วนที่ 2 คำถามเกี่ยวกับการตระหนักรู้ทั่วไปในเรื่องความมั่นคงปลอดภัยทางไซเบอร์ ปรับจากแบบสอบถามของ Charoenpichet (2023) โดยใช้มาตรวัด 5 ระดับ ได้แก่ ระดับที่ 1 = เห็นด้วยต่ำที่สุด ระดับที่ 2 = เห็นด้วยต่ำ ระดับที่ 3 = เห็นด้วยปานกลาง ระดับที่ 4 = เห็นด้วยมาก และระดับที่ 5 = เห็นด้วยมากที่สุด จากนั้นนำคะแนนที่ได้ตามเกณฑ์การให้คะแนนข้างต้นมาเฉลี่ยเป็นคะแนนระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์พร้อมความหมาย ดังตารางที่ 1

ตารางที่ 1 เกณฑ์การให้คะแนนและความหมายของระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

ระดับคะแนน	การแปลความหมาย
1.00 - 1.80	มีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ต่ำที่สุด
1.81 – 2.60	มีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ต่ำ
2.61 – 3.40	มีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ปานกลาง
3.41 – 4.20	มีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์มาก
4.21 – 5.00	มีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์มากที่สุด

สำหรับส่วนที่ 3 ข้อเสนอแนะ เป็นคำถามปลายเปิด เพื่อให้ผู้ตอบแบบสอบถามสามารถแสดงความคิดเห็นเพิ่มเติมเกี่ยวกับความสำคัญของการตระหนักรู้ด้านไซเบอร์ต่อการทำงานในวิชาชีพบัญชี

การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลเชิงพรรณนา โดยวิเคราะห์ค่าสถิติประกอบกับการแจกแจงความถี่ ค่าร้อยละ ค่าเฉลี่ย และค่าส่วนเบี่ยงเบนมาตรฐาน มาทำการวิเคราะห์ข้อมูลเชิงปริมาณของข้อมูลทั่วไปด้านประชากรศาสตร์จากผู้ตอบแบบสอบถาม ผู้ศึกษาใช้การวิเคราะห์ข้อมูลทางสถิติด้วยโปรแกรมสำเร็จรูปทางสถิติซึ่งการวิเคราะห์ข้อมูลทั่วไปและวิเคราะห์ข้อมูลระดับการให้ความสำคัญของแต่ละปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ การวิเคราะห์ข้อมูลเชิงอนุมานโดยวิเคราะห์การทดสอบสมมติฐานของกลุ่มตัวอย่าง 2 กลุ่มที่เป็นอิสระจากกัน และสถิติการวิเคราะห์ความแปรปรวนทางเดียว โดยใช้วิธีผลต่างนัยสำคัญน้อยที่สุดในการทดสอบรายคู่ด้วยวิธี LSD ในการทดสอบสมมติฐานได้กำหนดให้มีระดับความมีนัยสำคัญเท่ากับ 0.05 การวิเคราะห์ข้อมูลข้อเสนอแนะเพิ่มเติม จากที่ผู้ตอบแบบสอบถามแสดงความคิดเห็นเพิ่มเติมเกี่ยวกับความสำคัญของการตระหนักรู้ความมั่นคงปลอดภัยทางไซเบอร์ต่อการทำงานในวิชาชีพบัญชี ซึ่งใช้การรวบรวมข้อมูลและการวิเคราะห์เนื้อหา

ผลการศึกษา

ผลการศึกษาแบ่งเป็น 3 ส่วน ได้แก่ ผลการวิเคราะห์ข้อมูลโดยสถิติเชิงพรรณนา ผลการวิเคราะห์ข้อมูลโดยสถิติเชิงอนุมาน และผลการวิเคราะห์ข้อมูลข้อเสนอแนะเพิ่มเติม ดังนี้

ผลการวิเคราะห์ข้อมูลโดยสถิติเชิงพรรณนา

จากการศึกษาครั้งนี้ผู้ศึกษาได้ทำการเก็บรวบรวมข้อมูลจากแบบสอบถามและนำมาประมวลผลทางสถิติโดยผลการตอบกลับแบบสอบถามมีทั้งหมด 305 ชุด คิดเป็นร้อยละ 79.22 ของจำนวนตัวอย่างที่ต้องการ ซึ่งอธิบายผลการวิเคราะห์จากข้อมูลทั่วไปของผู้ตอบแบบสอบถาม และวิเคราะห์ปัจจัยที่มีผลกระทบต่อระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของผู้ประกอบวิชาชีพบัญชี ทั้งนี้ จำนวนตัวอย่างที่เก็บรวบรวมได้จริงไม่เป็นไปตามเป้าหมายที่กำหนดไว้ แต่ผู้ศึกษา ได้พิจารณาถึงความเหมาะสมและความเป็นตัวแทนของกลุ่มตัวอย่างที่ได้มา โดยกลุ่มตัวอย่างที่เข้าร่วมการศึกษาในครั้งนี้ มีความรู้และประสบการณ์ทำงานเกี่ยวกับวิชาชีพบัญชีและครอบคลุมลักษณะของประชากรที่ศึกษา ซึ่งทำให้ผลการศึกษาที่ได้ยังคงมีความน่าเชื่อถือและมีคุณภาพสูง สามารถสะท้อนความเห็น และประสบการณ์ที่เกี่ยวข้องกับหัวข้อในการศึกษา จึงถือว่ากลุ่มตัวอย่างเป็นตัวแทนที่ดีของประชากรได้

ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม การศึกษาส่วนนี้เป็นการวิเคราะห์ข้อมูลเบื้องต้นโดยใช้สถิติเชิงพรรณนาดังที่ปรากฏในตารางที่ 2

ตารางที่ 2 จำนวนและร้อยละของกลุ่มตัวอย่างโดยแจกแจงข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม	จำนวน	ร้อยละ
1. เพศ		
(1) ชาย	135	44.3
(2) หญิง	170	55.7
รวม	**305**	**100**
2. อายุ		
(1) 21 – 30 ปี	180	59.0
(2) 31 – 40 ปี	92	30.2
(3) 41 – 50 ปี	14	4.6
(4) 50 – 60 ปี	16	5.2
(5) มากกว่า 60 ปี	3	1.0
รวม	**305**	**100**
3. ระดับการศึกษา		
(1) ปริญญาตรี	242	79.3
(2) สูงกว่าปริญญาตรี	63	20.7
รวม	**305**	**100**
4. ใบอนุญาตประกอบวิชาชีพ		
(1) ไม่มี	198	64.9
(2) CPA	81	26.6
(3) CIA	10	3.3
(4) TA	10	3.3
(5) อื่น ๆ	2	0.7
(6) CPA และ อื่น ๆ	4	1.3
รวม	**305**	**100**

ตารางที่ 2 (ต่อ)

ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม	จำนวน	ร้อยละ
5. ประเภทหน่วยงานที่สังกัด		
(1) สำนักงานสอบบัญชี	66	21.6
(2) หน่วยงานราชการ	68	22.3
(3) บริษัทเอกชน	110	36.1
(4) รับงานอิสระ	61	20.0
รวม	**305**	**100**
6. สาขาที่เชี่ยวชาญ		
(1) การทำบัญชี	113	37.0
(2) การสอบบัญชี	98	32.1
(3) การบัญชีภาษีอากร	48	15.7
(4) การบัญชีบริหาร	22	7.2
(5) การวางระบบบัญชี	12	3.9
(6) อื่น ๆ	12	3.9
รวม	**305**	**100**
7. ประสบการณ์ในการทำงานเกี่ยวกับวิชาชีพบัญชี		
(1) 1 – 5 ปี	124	40.7
(2) 6 – 10 ปี	112	36.7
(3) 11 – 15 ปี	34	11.1
(4) 16 – 20 ปี	12	3.9
(5) มากกว่า 20 ปี	23	7.5
รวม	**305**	**100**

จากตารางที่ 2 แสดงข้อมูลทั่วไปของผู้ตอบแบบสอบถาม จำนวน 305 คน สรุปได้ว่าผู้ตอบแบบสอบถามส่วนมากเป็นเพศหญิง 170 คน (คิดเป็นร้อยละ 55.7) มีช่วงอายุ 21 – 30 ปี จำนวน 180 คน (คิดเป็นร้อยละ 59) มีระดับการศึกษาสูงสุด คือ ปริญญาตรี จำนวน 242 คน (คิดเป็นร้อยละ 79.3) ผู้ตอบแบบสอบถามไม่มีใบอนุญาตประกอบวิชาชีพ จำนวน 198 คน (คิดเป็นร้อยละ 64.9) รองลงมาเป็น มีใบอนุญาตประกอบวิชาชีพ CPA เพียงอย่างเดียว จำนวน 81 คน (คิดเป็นร้อยละ 26.6) ซึ่งอยู่ในบริษัทเอกชน จำนวน 110 คน (คิดเป็นร้อยละ 36.1) สาขาที่เชี่ยวชาญ คือ การทำบัญชี จำนวน 113 คน (คิดเป็นร้อยละ 37) และมีประสบการณ์การทำงานเกี่ยวกับวิชาชีพบัญชี 1 – 5 ปี จำนวน 124 คน (คิดเป็นร้อยละ 40.7) และ 6 – 10 ปี จำนวน 112 คน (คิดเป็นร้อยละ 36.7) ตามลำดับ

การวิเคราะห์ระดับการให้ความสำคัญแต่ละปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

การศึกษาส่วนนี้เป็นการวิเคราะห์ระดับการให้ความสำคัญของแต่ละปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ ประกอบไปด้วย 4 ปัจจัย ได้แก่ (1) ด้านความรู้พื้นฐาน (2) ด้านการฝึกอบรม (3) ด้านทัศนคติ และ (4) ด้านพฤติกรรม โดยใช้สถิติพรรณนาในการอธิบายถึงค่าร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และความหมายของระดับความสำคัญที่ได้วิเคราะห์ทางสถิติ ดังที่ปรากฏในตารางที่ 3

ตารางที่ 3 ระดับการให้ความสำคัญแต่ละปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

การตระหนักรู้	ระดับความคิดเห็น (ร้อยละ)					ระดับผลกระทบต่อการตระหนักรู้		
	ต่ำที่สุด	ต่ำ	ปานกลาง	มาก	มากที่สุด	ค่าเฉลี่ย	ส่วนเบี่ยงเบนมาตรฐาน	ความหมาย
1. ความรู้พื้นฐานต่อความมั่นคงปลอดภัยทางไซเบอร์								
1.1 ความมั่นคงปลอดภัยทางไซเบอร์ มีความจำเป็นในวิชาชีพบัญชี	0.0	0.0	1.3	17.0	81.6	4.80	0.43	มากที่สุด
1.2 ข้อกำหนดทางกฎหมายและข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ เช่น PDPA และ SOX มีความสำคัญสำหรับวิชาชีพบัญชี	0.0	0.0	3.9	31.5	64.6	4.61	0.56	มากที่สุด
1.3 ภัยคุกคามทางไซเบอร์ทั่วไป เช่น ฟิชชิง มัลแวร์ มีผลกระทบที่อาจเกิดขึ้นต่อข้อมูลทางการเงิน	0.0	0.7	4.6	34.4	60.3	4.54	0.62	มากที่สุด
1.4 การเข้ารหัส ไฟร์วอลล์ และซอฟต์แวร์ป้องกันไวรัส เป็นการควบคุมความมั่นคงปลอดภัยทางไซเบอร์ขั้นพื้นฐานสำคัญ	0.0	1.3	2.0	38.0	58.7	4.54	0.61	มากที่สุด
1.5 การตรวจสอบสิทธิ์แบบหลายปัจจัย เป็นการรักษาความปลอดภัยของการเข้าถึงระบบทางการเงิน	0.0	1.3	1.3	30.2	67.2	4.63	0.58	มากที่สุด
1.6 การอัปเดตและแก้ไขระบบเป็นประจำเป็นการป้องกันภัยคุกคามทางไซเบอร์	0.0	0.0	0.7	37.4	62.0	4.61	0.50	มากที่สุด
ภาพรวมด้านความรู้พื้นฐาน						**4.62**	**0.37**	**มากที่สุด**

ตารางที่ 3 (ต่อ)

การตระหนักรู้	ระดับความคิดเห็น (ร้อยละ)					ระดับผลกระทบต่อการตระหนักรู้		
	ต่ำที่สุด	ต่ำ	ปานกลาง	มาก	มากที่สุด	ค่าเฉลี่ย	ส่วนเบี่ยงเบนมาตรฐาน	ความหมาย
2. ด้านการฝึกอบรมต่อความมั่นคงปลอดภัยทางไซเบอร์								
2.1 แผนรับมือเหตุการณ์สำหรับการละเมิดความมั่นคงปลอดภัยทางไซเบอร์มีความสำคัญต่อองค์กรและผู้ประกอบวิชาชีพบัญชี	0.0	0.7	1.3	28.2	69.8	4.67	0.54	มากที่สุด
2.2 การฝึกอบรมการตระหนักรู้และระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์เป็นประจำมีความจำเป็นต่อองค์กรและผู้ประกอบวิชาชีพบัญชี	0.0	0.0	3.3	33.4	63.3	4.60	0.55	มากที่สุด
2.3 การประเมินหรือการตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์เป็นประจำมีความสำคัญต่อองค์กรและผู้ประกอบวิชาชีพบัญชี เพื่อให้มั่นใจว่ามีการปฏิบัติตามข้อกำหนด	0.0	0.0	3.9	31.1	64.9	4.61	0.56	มากที่สุด
2.4 ความพร้อมในการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้นในการทำงานมีความจำเป็นต่อองค์กรและผู้ประกอบวิชาชีพบัญชี	0.0	0.7	2.6	32.1	64.6	4.61	0.58	มากที่สุด
2.5 การติดตามข้อมูลล่าสุดเกี่ยวกับการละเมิดความมั่นคงปลอดภัยทางไซเบอร์มีความสำคัญต่อองค์กรและผู้ประกอบวิชาชีพบัญชี	0.0	0.0	4.6	28.2	67.2	4.63	0.57	มากที่สุด
ภาพรวมด้านการฝึกอบรม						**4.62**	**0.43**	มากที่สุด

ตารางที่ 3 (ต่อ)

การตระหนักรู้	ระดับความคิดเห็น (ร้อยละ)					ระดับผลกระทบต่อการตระหนักรู้		
	ต่ำที่สุด	ต่ำ	ปานกลาง	มาก	มากที่สุด	ค่าเฉลี่ย	ส่วนเบี่ยงเบนมาตรฐาน	ความหมาย
3. ด้านทัศนคติต่อความมั่นคงปลอดภัยทางไซเบอร์								
3.1 ควรมีการสำรองข้อมูลคอมพิวเตอร์เป็นประจำ มีความสำคัญต่อการรักษาข้อมูลทางการเงิน	0.0	3.9	3.3	32.8	60.0	4.49	0.74	มากที่สุด
3.2 ควรมีการอัปเดตระบบปฏิบัติการ (OS) และเวอร์ชั่นของโปรแกรมบนอุปกรณ์ เช่น คอมพิวเตอร์ โทรศัพท์ อย่างสม่ำเสมอ	0.0	0.7	5.9	32.8	60.7	4.53	0.64	มากที่สุด
3.3 องค์กรควรให้การฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์เพิ่มเติม ให้แก่ผู้ประกอบวิชาชีพบัญชี	0.0	2.0	5.9	27.9	64.3	4.54	0.70	มากที่สุด
3.4 องค์กรควรมีการกำหนดสิทธิ์การเข้าถึงข้อมูล และระบบต่าง ๆ ตามความจำเป็นของแต่ละบุคคลและตรวจสอบและปรับปรุงสิทธิ์การเข้าถึงเป็นประจำ	0.0	0.7	2.6	34.8	62.0	4.58	0.58	มากที่สุด
3.5 ควรมีการเปลี่ยนรหัสผ่านทุก 3-6 เดือน หรือทันทีที่สงสัยว่ารหัสผ่านอาจรั่วไหล	2.0	2.0	4.6	27.2	64.3	4.50	0.84	มากที่สุด
3.6 องค์กรควรมีการกำหนดนโยบายการตั้งรหัสผ่านที่มีความยาวอย่างน้อย 8 ตัวอักษร ประกอบด้วยตัวอักษรผสมกัน ทั้งตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และสัญลักษณ์พิเศษ	0.0	0.7	2.6	28.2	68.5	4.65	0.57	มากที่สุด
3.7 ควรมีการจดรหัสผ่านลงบนกระดาษ หรือบันทึกไว้ในไฟล์ที่ไม่มีการเข้ารหัสผ่าน เพื่อเพิ่มความสะดวกในการเข้าใช้ข้อมูลทางการเงิน	69.2	18.4	4.6	3.3	4.6	1.56	1.04	มากที่สุด
ภาพรวมด้านทัศนคติ						**4.12**	**0.41**	มากที่สุด

ตารางที่ 3 (ต่อ)

การตระหนักรู้	ระดับความคิดเห็น (ร้อยละ)					ระดับผลกระทบต่อการตระหนักรู้		
	ต่ำที่สุด	ต่ำ	ปานกลาง	มาก	มากที่สุด	ค่าเฉลี่ย	ส่วนเบี่ยงเบนมาตรฐาน	ความหมาย
4. ด้านพฤติกรรมต่อความมั่นคงปลอดภัยทางไซเบอร์								
4.1 มีการเปิดอีเมล รวมถึงไฟล์แนบที่ส่งมาจากบัญชีผู้ใช้ที่ไม่รู้จัก	66.2	23.3	3.3	4.6	2.6	1.54	0.95	ต่ำที่สุด
4.2 มีการดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่ปลอดภัย	54.1	34.1	5.2	3.3	3.3	1.68	0.96	ต่ำที่สุด
4.3 มีการใช้งานผ่านเว็บไซต์ที่ขึ้นต้นด้วย https เท่านั้น	0.7	1.3	6.6	28.2	63.3	4.52	0.73	มากที่สุด
4.4 มีการเปิดใช้งาน Multi-Factor Authentication เพิ่มความปลอดภัยอีกชั้นด้วยการยืนยันตัวตนหลายขั้นตอน เช่น การใช้รหัสผ่านร่วมกับ OTP	0.0	2.6	5.2	27.2	64.9	4.54	0.72	มากที่สุด
4.5 มีการตรวจสอบชื่อและความปลอดภัยของเครือข่าย Wi-Fi ก่อนเชื่อมต่อทุกครั้ง หากจำเป็นต้องเชื่อมต่อ Wi-Fi สาธารณะ	0.0	3.9	4.6	28.5	63.0	4.50	0.76	มากที่สุด
4.6 มีการใช้ VPN บนอุปกรณ์ขององค์กร หากจำเป็นต้องเชื่อมต่อ Wi-Fi สาธารณะ	2.6	3.3	3.3	23.6	67.2	4.50	0.91	มากที่สุด
ภาพรวมด้านพฤติกรรม						**3.55**	**0.44**	**มาก**
ภาพรวมทั้งหมด 4 ด้าน						**4.21**	**0.32**	**มากที่สุด**

จากตารางที่ 3 แสดงระดับการให้ความสำคัญของแต่ละปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ ในภาพรวมกลุ่มตัวอย่างมีระดับการตระหนักรู้มากที่สุด มีค่าเฉลี่ยเท่ากับ 4.21 พิจารณาเป็นรายปัจจัยดังนี้

1. ด้านความรู้พื้นฐาน ในภาพรวมผู้ตอบแบบสอบถามมีความคิดเห็นเกี่ยวกับระดับผลกระทบต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์มากที่สุด มีค่าเฉลี่ยเท่ากับ 4.62 เมื่อพิจารณาเป็นรายข้อ พบว่า เรื่องที่มีผลกระทบมากที่สุด คือ (1.1) ความมั่นคงปลอดภัยทางไซเบอร์มีความจำเป็นในวิชาชีพบัญชี มีค่าเฉลี่ยเท่ากับ 4.80 และเรื่องที่มีผลกระทบน้อยที่สุด คือ (1.3) ภัยคุกคามทางไซเบอร์ทั่วไปมีผลกระทบที่อาจเกิดขึ้นต่อข้อมูลทางการเงิน และ (1.4) การเข้ารหัสและซอฟต์แวร์ป้องกันไวรัสเป็นการควบคุมความมั่นคงปลอดภัยทางไซเบอร์ขั้นพื้นฐานที่สำคัญ มีค่าเฉลี่ยเท่ากับ 4.54

2. ด้านการฝึกอบรม ในภาพรวมผู้ตอบแบบสอบถามมีความคิดเห็นเกี่ยวกับระดับผลกระทบต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์มากที่สุด มีค่าเฉลี่ยเท่ากับ 4.62 เมื่อพิจารณาเป็นรายข้อ พบว่า เรื่องที่มีผลกระทบมากที่สุด คือ (2.1) แผนรับมือเหตุการณ์สำหรับการละเมิดความมั่นคงปลอดภัยทางไซเบอร์มีความสำคัญต่อองค์กรและผู้ประกอบวิชาชีพบัญชี มีค่าเฉลี่ยเท่ากับ 4.67 และเรื่องที่มีผลกระทบน้อยที่สุด คือ (2.2) การฝึกอบรมการตระหนักรู้และระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์เป็นประจำมีความจำเป็นต่อองค์กรและผู้ประกอบวิชาชีพบัญชี มีค่าเฉลี่ยเท่ากับ 4.60

3. ด้านทัศนคติ ในภาพรวมผู้ตอบแบบสอบถามมีความคิดเห็นเกี่ยวกับระดับผลกระทบต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์มาก มีค่าเฉลี่ยเท่ากับ 4.12 เมื่อพิจารณาเป็นรายข้อ พบว่า เรื่องที่มีผลกระทบมากที่สุด คือ (3.6) องค์กรควรมีการกำหนดนโยบายการตั้งรหัสผ่านที่มีความยาวอย่างน้อย 8 ตัวอักษร ประกอบด้วยตัวอักษรผสมกัน มีค่าเฉลี่ยเท่ากับ 4.65 และเรื่องที่มีผลกระทบน้อยที่สุด คือ (3.7) ควรมีการจดรหัสผ่านลงบนกระดาษ หรือบันทึกไว้ในไฟล์ที่ไม่มีการเข้ารหัสผ่าน มีค่าเฉลี่ยเท่ากับ 1.56

4. ด้านพฤติกรรม ในภาพรวมผู้ตอบแบบสอบถามมีความคิดเห็นเกี่ยวกับระดับผลกระทบต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์มาก มีค่าเฉลี่ยเท่ากับ 3.55 เมื่อพิจารณาเป็นรายข้อ พบว่า เรื่องที่มีผลกระทบมากที่สุด คือ (4.4) มีการเปิดใช้งาน Multi-Factor Authentication เพิ่มความปลอดภัยอีกชั้นด้วยการยืนยันตัวตนหลายขั้นตอน มีค่าเฉลี่ยเท่ากับ 4.54 และเรื่องที่มีผลกระทบน้อยที่สุด คือ (4.1) มีการเปิดอีเมล รวมถึงไฟล์แนบที่ส่งมาจากบัญชีผู้ใช้ที่ไม่รู้จัก มีค่าเฉลี่ยเท่ากับ 1.54

ผลการวิเคราะห์ข้อมูลโดยสถิติเชิงอนุมาน

การศึกษาส่วนนี้เป็นการวิเคราะห์ข้อมูลโดยเน้นการเปรียบเทียบความแตกต่างและทดสอบสมมติฐานว่าข้อมูลทั่วไปของผู้ตอบแบบสอบถามมีต่อระดับการให้ความสำคัญของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ ดังนี้

H_0 : ข้อมูลทั่วไปของผู้ตอบแบบสอบถามที่ต่างกันมีต่อระดับการให้ความสำคัญของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์***ไม่แตกต่างกัน***

H_1 : ข้อมูลทั่วไปของผู้ตอบแบบสอบถามที่ต่างกันมีต่อระดับการให้ความสำคัญของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์***แตกต่างกัน***

การทดสอบสมมติฐานข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ได้แก่ เพศ อายุ ระดับการศึกษา ใบอนุญาตประกอบวิชาชีพ ประเภทหน่วยงานที่สังกัด สาขาที่เชี่ยวชาญ และประสบการณ์ในการทำงานเกี่ยวกับวิชาชีพบัญชี โดยใช้สถิติเชิงอนุมานในการวิเคราะห์ ผลการวิเคราะห์ข้อมูลจะมิได้แสดงข้อมูลทั่วไปด้านเพศ และระดับการศึกษาไม่มีผลต่อระดับการตระหนักรู้อย่างมีนัยสำคัญทางสถิติ

ข้อมูลทั่วไป เรื่อง อายุ

ตารางที่ 4 ผลการเปรียบเทียบระดับการให้ความสำคัญของปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ จำแนกตามอายุ โดยใช้วิธี One-way ANOVA

การตระหนักรู้	Sum of Squares	df	Mean Square	F	p-value
1.ด้านความรู้พื้นฐาน					
ระหว่างกลุ่ม	1.434	4	0.359	2.725	**0.03***
ภายในกลุ่ม	39.47	300	0.132		
รวม	40.904	304			
2.ด้านการฝึกอบรม					
ระหว่างกลุ่ม	0.415	4	0.104	0.553	0.697
ภายในกลุ่ม	56.185	300	0.187		
รวม	56.599	304			
3.ด้านทัศนคติ					
ระหว่างกลุ่ม	2.387	4	0.597	3.683	**0.006***
ภายในกลุ่ม	48.614	300	0.162		
รวม	51.001	304			

ตารางที่ 4 (ต่อ)

การตระหนักรู้	Sum of Squares	df	Mean Square	F	p-value
4.ด้านพฤติกรรม					
ระหว่างกลุ่ม	0.746	4	0.186	0.949	0.436
ภายในกลุ่ม	58.914	300	0.196		
รวม	59.66	304			
ภาพรวม					
ระหว่างกลุ่ม	0.986	4	0.246	2.476	**0.044***
ภายในกลุ่ม	29.855	300	0.100		
รวม	30.840	304			

หมายเหตุ *ระดับนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 4 พบว่าค่า p-value ของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมมีค่าเท่ากับ 0.044 ซึ่งน้อยกว่าระดับนัยสำคัญทางสถิติที่ 0.05 จึงสรุปผลได้ว่า ผู้ตอบแบบสอบถามที่มีอายุแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมแตกต่างกัน ในขณะที่หากพิจารณาเป็นรายด้าน พบว่าค่า p-value ในด้านการฝึกอบรม และด้านพฤติกรรม มากกว่าระดับนัยสำคัญทางสถิติ จึงสรุปผลได้ว่า ผู้ตอบแบบสอบถามที่มีอายุแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในด้านการฝึกอบรม และด้านพฤติกรรมต่อความมั่นคงปลอดภัยทางไซเบอร์ไม่แตกต่างกัน ส่วนด้านความรู้พื้นฐาน และด้านทัศนคติ พบว่ามีค่า p-value น้อยกว่าระดับนัยสำคัญทางสถิติ จึงสรุปได้ว่า ผู้ตอบแบบสอบถามที่มีอายุแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในด้านความรู้พื้นฐานและด้านทัศนคติแตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ 0.05 และผู้ศึกษาได้วิเคราะห์เปรียบเทียบค่าเฉลี่ยเป็นรายคู่ ในภาพรวม ดังตารางที่ 5

ตารางที่ 5 ผลการเปรียบเทียบระดับการให้ความสำคัญของปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ในภาพรวม จำแนกตามอายุ และมีการเปรียบเทียบค่าเฉลี่ยเป็นรายคู่

อายุ	ค่าเฉลี่ย	21 - 30 ปี	31 - 40 ปี	41 - 50 ปี	51 - 60 ปี	มากกว่า 60
		p-value	p-value	p-value	p-value	p-value
21 - 30 ปี	4.237	-	0.008*	-	-	-
31 - 40 ปี	4.129	-	-	-	-	-
41 - 50 ปี	4.196	-	-	-	-	-
51 - 60 ปี	4.297	-	-	-	-	-
มากกว่า 60	4.430	-	-	-	-	-

หมายเหตุ *ระดับนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 5 พบว่าผู้ตอบแบบสอบถามที่มีอายุระหว่าง 21 – 30 ปี มีการให้ระดับความสำคัญที่ค่าเฉลี่ย 4.237 ซึ่งมีระดับการให้ความสำคัญของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวม มากกว่าผู้ที่มีอายุระหว่าง 31 – 40 ปี อย่างมีนัยสำคัญทางสถิติที่ 0.05

ข้อมูลทั่วไป เรื่อง ใบอนุญาตประกอบวิชาชีพ

ตารางที่ 6 ผลการเปรียบเทียบระดับการให้ความสำคัญของปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ จำแนกตามใบอนุญาตประกอบวิชาชีพ โดยใช้วิธี One-way ANOVA

การตระหนักรู้	Sum of Squares	df	Mean Square	F	p-value
1.ด้านความรู้พื้นฐาน					
ระหว่างกลุ่ม	2.919	5	0.584	4.595	**<0.001***
ภายในกลุ่ม	37.985	299	0.127		
รวม	40.904	304			
2.ด้านการฝึกอบรม					
ระหว่างกลุ่ม	5.728	5	1.146	6.733	**<0.001***
ภายในกลุ่ม	50.872	299	0.170		
รวม	56.599	304			

ตารางที่ 6 (ต่อ)

การตระหนักรู้	Sum of Squares	df	Mean Square	F	p-value
3.ด้านทัศนคติ					
ระหว่างกลุ่ม	5.766	5	1.153	7.622	**<0.001***
ภายในกลุ่ม	45.235	299	0.151		
รวม	51.001	304			
4.ด้านพฤติกรรม					
ระหว่างกลุ่ม	4.222	5	0.844	4.555	**<0.001***
ภายในกลุ่ม	55.437	299	0.185		
รวม	59.660	304			
ภาพรวม					
ระหว่างกลุ่ม	3.658	5	0.732	8.048	**<0.001***
ภายในกลุ่ม	27.182	299	0.091		
รวม	30.840	304			

หมายเหตุ *ระดับนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 6 พบว่าค่า p-value ของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวม มีค่าน้อยกว่า 0.001 ซึ่งน้อยกว่าระดับนัยสำคัญทางสถิติที่ 0.05 จึงสรุปผลได้ว่า ผู้ตอบแบบสอบถามที่มีใบอนุญาตประกอบวิชาชีพแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมแตกต่างกัน หากพิจารณาเป็นรายด้าน พบว่า ค่า p-value ทั้ง 4 ด้าน ได้แก่ ด้านความรู้พื้นฐาน ด้านการฝึกอบรม ด้านทัศนคติ และด้านพฤติกรรม น้อยกว่าระดับนัยสำคัญทางสถิติ จึงสรุปผลได้ว่า ผู้ตอบแบบสอบถามที่มีใบอนุญาตประกอบวิชาชีพแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในด้านความรู้พื้นฐาน การฝึกอบรม ด้านทัศนคติ และด้านพฤติกรรม แตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ 0.05 และผู้ศึกษาได้วิเคราะห์เปรียบเทียบค่าเฉลี่ยเป็นรายคู่ในภาพรวม ดังตารางที่ 4.6

ตารางที่ 7 ผลการเปรียบเทียบระดับการให้ความสำคัญของปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ในภาพรวม จำแนกตามใบอนุญาตประกอบวิชาชีพและมีการเปรียบเทียบค่าเฉลี่ยเป็นรายคู่

ใบอนุญาตประกอบวิชาชีพ	ค่าเฉลี่ย	ไม่มี	CPA	CIA	TA	อื่น ๆ	CPA และอื่น ๆ
		p-value	p-value	p-value	p-value	p-value	p-value
ไม่มี	4.178	-	0.001*	-	-	-	<0.001*
CPA	4.316	-	-	-	-	-	<0.001*
CIA	4.125	-	-	-	-	-	<0.001*
TA	4.333	-	-	-	-	-	<0.001*
อื่น ๆ	4.042	-	-	-	-	-	0.026*
CPA และอื่น ๆ	3.458	-	-	-	-	-	-

หมายเหตุ *ระดับนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 7 พบว่าผู้ตอบแบบสอบถามที่มีใบอนุญาตประกอบวิชาชีพ CPA เพียงอย่างเดียว มีการให้ระดับความสำคัญที่ค่าเฉลี่ย 4.316 ซึ่งมีระดับการให้ความสำคัญของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมมากกว่าผู้ที่ไม่มีใบอนุญาตประกอบวิชาชีพ อย่างมีนัยสำคัญทางสถิติที่ 0.05 และผู้ตอบแบบสอบถามที่มีใบอนุญาตประกอบวิชาชีพ CPA และอื่น ๆ มีการให้ระดับความสำคัญที่ค่าเฉลี่ย 3.458 ซึ่งมีระดับการให้ความสำคัญของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวม น้อยที่สุดเมื่อเทียบกับกลุ่มต่าง ๆ ได้แก่ ผู้ที่ไม่มีใบอนุญาตประกอบวิชาชีพ ผู้ที่มีใบอนุญาตประกอบวิชาชีพ CPA CIA TA และอื่น ๆ อย่างมีนัยสำคัญทางสถิติ

ข้อมูลทั่วไป เรื่อง ประเภทหน่วยงานที่สังกัด

ตารางที่ 8 ผลการเปรียบเทียบระดับการให้ความสำคัญของปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ จำแนกตามประเภทหน่วยงานที่สังกัด โดยใช้วิธี One-way ANOVA

การตระหนักรู้	Sum of Squares	df	Mean Square	F	p-value
1.ด้านความรู้พื้นฐาน					
ระหว่างกลุ่ม	4.091	3	1.364	11.149	**<0.001***
ภายในกลุ่ม	36.813	301	0.122		
รวม	40.904	304			
2.ด้านการฝึกอบรม					
ระหว่างกลุ่ม	6.438	3	2.146	12.877	<0.001*
ภายในกลุ่ม	50.162	301	0.167		
รวม	56.599	304			

ตารางที่ 8 (ต่อ)

การตระหนักรู้	Sum of Squares	df	Mean Square	F	p-value
3.ด้านทัศนคติ					
ระหว่างกลุ่ม	1.936	3	0.645	3.96	**0.009***
ภายในกลุ่ม	49.065	301	0.163		
รวม	51.001	304			
4.ด้านพฤติกรรม					
ระหว่างกลุ่ม	2.104	3	0.701	3.668	**0.013***
ภายในกลุ่ม	57.555	301	0.191		
รวม	59.66	304			
ภาพรวม					
ระหว่างกลุ่ม	2.798	3	0.933	10.01	**<0.001***
ภายในกลุ่ม	28.042	301	0.093		
รวม	30.84	304			

หมายเหตุ *ระดับนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 8 พบว่าค่า p-value ของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวม มีค่าน้อยกว่า 0.001 ซึ่งน้อยกว่าระดับนัยสำคัญทางสถิติที่ 0.05 จึงสรุปผลได้ว่า ผู้ตอบแบบสอบถามที่มีหน่วยงานสังกัดแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมแตกต่างกัน หากพิจารณาเป็นรายด้าน พบว่าค่า p-value ทั้ง 4 ด้าน ได้แก่ ด้านความรู้พื้นฐาน ด้านการฝึกอบรม ด้านทัศนคติ และด้านพฤติกรรม น้อยกว่าระดับนัยสำคัญทางสถิติ จึงสรุปผลได้ว่า ผู้ตอบแบบสอบถามที่มีหน่วยงานสังกัดแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในด้านความรู้พื้นฐาน การฝึกอบรม ด้านทัศนคติ และด้านพฤติกรรมแตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ 0.05 และผู้ศึกษาได้วิเคราะห์เปรียบเทียบค่าเฉลี่ยเป็นรายคู่ในภาพรวม ดังตารางที่ 4.8

ตารางที่ 9 ผลการเปรียบเทียบระดับการให้ความสำคัญของปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ ในภาพรวม จำแนกตามหน่วยงานสังกัดและมีการเปรียบเทียบเป็นรายคู่

หน่วยงานที่สังกัด	ค่าเฉลี่ย	สำนักงานสอบบัญชี	หน่วยงานราชการ	บริษัทเอกชน	รับงานอิสระ
		p-value	p-value	p-value	p-value
สำนักงานสอบบัญชี	4.352	-	-	-	-
หน่วยงานราชการ	4.102	<0.001*	-	-	0.001*
บริษัทเอกชน	4.149	<0.001*	-	-	0.01*
รับงานอิสระ	4.275	-	-	-	-

หมายเหตุ *ระดับนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 9 พบว่าผู้ตอบแบบสอบถามที่ทำงานในสำนักงานสอบบัญชี และผู้ที่รับงานอิสระ มีการให้ระดับความสำคัญที่ค่าเฉลี่ย 4.352 และ 4.275 ตามลำดับ ซึ่งมีระดับการให้ความสำคัญของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวม มากกว่าผู้ที่ทำงานในบริษัทเอกชน และในหน่วยงานราชการ อย่างมีนัยสำคัญทางสถิติที่ 0.05

ข้อมูลทั่วไป เรื่อง ประสบการณ์การทำงาน (อายุงาน)

ตารางที่ 10 ผลการเปรียบเทียบระดับการให้ความสำคัญของปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ จำแนกตามอายุงาน โดยใช้วิธี One-way ANOVA

การตระหนักรู้	Sum of Squares	df	Mean Square	F	p-value
1.ด้านความรู้พื้นฐาน					
ระหว่างกลุ่ม	1.678	4	0.419	3.208	**0.013***
ภายในกลุ่ม	39.226	300	0.131		
รวม	40.904	304			
2.ด้านการฝึกอบรม					
ระหว่างกลุ่ม	2.843	4	0.711	3.967	**0.004***
ภายในกลุ่ม	53.756	300	0.179		
รวม	56.599	304			
3.ด้านทัศนคติ					
ระหว่างกลุ่ม	1.931	4	0.483	2.952	**0.020***
ภายในกลุ่ม	49.07	300	0.164		
รวม	51.001	304			

ตารางที่ 10 (ต่อ)

การตระหนักรู้	Sum of Squares	df	Mean Square	F	p-value
4.ด้านพฤติกรรม					
ระหว่างกลุ่ม	0.746	4	0.186	0.949	0.436
ภายในกลุ่ม	58.914	300	0.196		
รวม	59.66	304			
ภาพรวม					
ระหว่างกลุ่ม	1.452	4	0.363	3.706	**0.006***
ภายในกลุ่ม	29.388	300	0.098		
รวม	30.84	304			

หมายเหตุ *ระดับนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 10 พบว่าค่า p-value ของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวม มีค่าเท่ากับ 0.006 ซึ่งน้อยกว่าระดับนัยสำคัญทางสถิติที่ 0.05 จึงสรุปผลได้ว่า ผู้ตอบแบบสอบถามที่มีอายุงานแตกต่างกัน มีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมแตกต่างกัน ในขณะที่หากพิจารณาเป็นรายด้าน พบว่าค่า p-value ในด้านพฤติกรรม มากกว่าระดับนัยสำคัญทางสถิติ จึงสรุปผลได้ว่า ผู้ตอบแบบสอบถามที่มีอายุงานแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในด้านพฤติกรรมต่อความมั่นคงปลอดภัยทางไซเบอร์ไม่แตกต่างกัน ส่วนด้านความรู้พื้นฐาน การฝึกอบรม และด้านทัศนคติ พบว่ามีค่า p-value น้อยกว่าระดับนัยสำคัญทางสถิติ จึงสรุปได้ว่า ผู้ตอบแบบสอบถามที่มีอายุงานแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในด้านความรู้พื้นฐานการฝึกอบรม และด้านทัศนคติแตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ 0.05 และผู้ศึกษาได้วิเคราะห์เปรียบเทียบค่าเฉลี่ยเป็นรายคู่ในภาพรวม ดังตารางที่ 4.10

ตารางที่ 11 ผลการเปรียบเทียบระดับการให้ความสำคัญของปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ ในภาพรวม จำแนกตามอายุงานและมีการเปรียบเทียบเป็นรายคู่

อายุงาน	ค่าเฉลี่ย	1 - 5 ปี	6 - 10 ปี	11 - 15 ปี	16 - 20 ปี	มากกว่า 20
		p-value	p-value	p-value	p-value	p-value
1 - 5 ปี	4.185	-	-	0.025*	-	-
6 - 10 ปี	4.252	-	-	0.001*	-	-
11 - 15 ปี	4.049	-	-	-	-	-
16 - 20 ปี	4.264	-	-	0.042*	-	-
มากกว่า 20	4.317	-	-	0.002*	-	-

หมายเหตุ *ระดับนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 11 พบว่าผู้ตอบแบบสอบถามที่มีอายุงานระหว่าง 11 – 15 ปี มีการให้ระดับความสำคัญที่ค่าเฉลี่ย 4.049 ซึ่งมีระดับการให้ความสำคัญของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวม น้อยที่สุดเมื่อเทียบกับกลุ่มต่าง ๆ ได้แก่ ผู้ที่มีอายุงานระหว่าง 1 – 5 ปี อายุงาน 6 – 10 ปี อายุงาน 16 – 20 ปี และอายุงานมากกว่า 20 ปีขึ้นไป อย่างมีนัยสำคัญทางสถิติที่ 0.05

ข้อมูลทั่วไป เรื่อง สาขาที่เชี่ยวชาญ

ตารางที่ 12 ผลการเปรียบเทียบระดับการให้ความสำคัญของปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ จำแนกตามสาขาที่เชี่ยวชาญ โดยใช้วิธี One-way ANOVA

การตระหนักรู้	Sum of Squares	df	Mean Square	F	p-value
1.ด้านความรู้พื้นฐาน					
ระหว่างกลุ่ม	2.987	5	0.597	4.711	**0.0003***
ภายในกลุ่ม	37.917	299	0.127		
รวม	40.904	304			
2.ด้านการฝึกอบรม					
ระหว่างกลุ่ม	3.100	5	0.620	3.465	**0.005***
ภายในกลุ่ม	53.499	299	0.179		
รวม	56.599	304			

ตารางที่ 12 (ต่อ)

การตระหนักรู้	Sum of Squares	df	Mean Square	F	p-value
3.ด้านทัศนคติ					
ระหว่างกลุ่ม	0.859	5	0.172	1.024	0.404
ภายในกลุ่ม	50.143	299	0.168		
รวม	51.001	304			
4.ด้านพฤติกรรม					
ระหว่างกลุ่ม	4.265	5	0.853	4.604	0.0005*
ภายในกลุ่ม	55.395	299	0.185		
รวม	59.660	304			
ภาพรวม					
ระหว่างกลุ่ม	1.791	5	0.358	3.687	0.003*
ภายในกลุ่ม	29.049	299	0.097		
รวม	30.840	304			

หมายเหตุ *ระดับนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 12 พบว่าค่า p-value ของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมมีค่าเท่ากับ 0.003 ซึ่งน้อยกว่าระดับนัยสำคัญทางสถิติที่ 0.05 จึงสรุปผลได้ว่า ผู้ตอบแบบสอบถามที่มีสาขาเชี่ยวชาญแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมแตกต่างกัน ในขณะที่หากพิจารณาเป็นรายด้าน พบว่า ค่า p-value ในด้านทัศนคติ มากกว่าระดับนัยสำคัญทางสถิติ จึงสรุปผลได้ว่า ผู้ตอบแบบสอบถามที่มีสาขาเชี่ยวชาญแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในด้านทัศนคติต่อความมั่นคงปลอดภัยทางไซเบอร์ไม่แตกต่างกัน ส่วนด้านความรู้พื้นฐาน การฝึกอบรม และด้านพฤติกรรม พบว่ามีค่า p-value น้อยกว่าระดับนัยสำคัญทางสถิติ จึงสรุป ได้ว่า ผู้ตอบแบบสอบถามที่มีสาขาเชี่ยวชาญแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในด้านความรู้พื้นฐาน การฝึกอบรม และด้านพฤติกรรมแตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ 0.05 และผู้ศึกษาได้วิเคราะห์เปรียบเทียบค่าเฉลี่ยเป็นรายคู่ในภาพรวม ดังตารางที่ 13

ตารางที่ 13 ผลการเปรียบเทียบระดับการให้ความสำคัญของปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ในภาพรวม จำแนกตามสาขาที่เชี่ยวชาญ

สาขาที่เชี่ยวชาญ	ค่าเฉลี่ย	การทำบัญชี	การสอบบัญชี	การบัญชีภาษีอากร	การบัญชีบริหาร	การวางระบบบัญชี	อื่น ๆ
		p-value	p-value	p-value	p-value	p-value	p-value
การทำบัญชี	4.252	-	-	0.0004*	-	0.046*	-
การสอบบัญชี	4.258	-	-	0.0004*	-	0.042*	-
การบัญชีภาษีอากร	4.063	-	-	-	-	-	-
การบัญชีบริหาร	4.193	-	-	-	-	-	-
การวางระบบบัญชี	4.063	-	-	-	-	-	-
อื่น ๆ	4.139	-	-	-	-	-	-

หมายเหตุ *ระดับนัยสำคัญทางสถิติที่ 0.05

จากตารางที่ 13 พบว่าผู้ตอบแบบสอบถามที่เชี่ยวชาญสาขาการสอบบัญชี และการทำบัญชี มีการให้ระดับความสำคัญที่ค่าเฉลี่ย 4.258 และ 4.252 ตามลำดับ ซึ่งมีระดับการให้ความสำคัญของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวม มากกว่าผู้ที่เชี่ยวชาญสาขาการบัญชีภาษีอากร และสาขาการวางระบบบัญชี อย่างมีนัยสำคัญทางสถิติที่ 0.05

ผลการวิเคราะห์ข้อมูลข้อเสนอแนะเพิ่มเติม

ผู้ตอบแบบสอบถามส่วนใหญ่เห็นว่าการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์มีความสำคัญอย่างยิ่ง เนื่องจากข้อมูลทางการเงินและบัญชีในปัจจุบันถูกจัดเก็บในระบบอินเทอร์เน็ต การรั่วไหลของข้อมูลที่ยังไม่ควรเปิดเผยอาจก่อให้เกิดปัญหาต่าง ๆ ตามมา และความปลอดภัยทางไซเบอร์ไม่ใช่หน้าที่ของฝ่ายสาระสนเทศเพียงฝ่ายเดียว แต่เป็นส่วนสำคัญของการทำงาน ในวิชาชีพบัญชีโดยตรง อย่างไรก็ตาม บางความเห็นระบุว่านักบัญชีไม่จำเป็นต้องมีความรู้ลึกซึ้งเกี่ยวกับเทคโนโลยี เพียงแค่มีความรู้พื้นฐานและหลีกเลี่ยงความเสี่ยง โดยไม่จำเป็นต้องเข้าใจเรื่องเทคนิคเฉพาะทางอย่างไฟร์วอลล์ ซึ่งสะท้อนว่ายังมีช่องว่างในการพัฒนาความตระหนักรู้ด้านไซเบอร์สำหรับผู้ประกอบวิชาชีพบัญชี

อภิปรายผลการศึกษา ข้อเสนอแนะ และสรุปผลการศึกษา

อภิปรายผลการศึกษา

การให้ความสำคัญของแต่ละปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของผู้ประกอบวิชาชีพบัญชี การศึกษาครั้งนี้พบว่าภาพรวมกลุ่มตัวอย่างมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์มากที่สุด สะท้อนว่าผู้ประกอบวิชาชีพบัญชีตระหนักถึงความสำคัญของความมั่นคงปลอดภัยไซเบอร์ต่อวิชาชีพของตนอย่างมาก ซึ่งสอดคล้องกับ Thammasiri and Wongthongdee (2022) พบว่ากลุ่มตัวอย่างมีการตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ในภาพรวมอยู่ในระดับมากเช่นเดียวกัน นอกจากนี้ ปัจจัยที่กลุ่มตัวอย่างเห็นว่ามีผลกระทบมากที่สุด คือ ด้านความรู้ และด้านการฝึกอบรม รองลงมา คือ ด้านทัศนคติ และด้านพฤติกรรม ตามลำดับ กล่าวคือ ผู้ประกอบวิชาชีพบัญชีส่วนใหญ่เห็นพ้องต้องกันว่าการมีความรู้พื้นฐานที่ถูกต้องและการได้รับการฝึกอบรมเป็นประจำมีความจำเป็นอย่างยิ่งต่อความมั่นคงปลอดภัยทางไซเบอร์ในงานบัญชี ตามมาด้วยการมีทัศนคติที่ดีต่อแนวปฏิบัติด้านความปลอดภัย ทั้งนี้ ด้านพฤติกรรมถูกประเมินว่า มีความสำคัญน้อยกว่าปัจจัยอื่น ๆ ซึ่งสอดคล้องกับการที่กลุ่มตัวอย่างบางส่วนยังมีพฤติกรรมเสี่ยงอยู่บ้าง หากพิจารณาเป็นรายปัจจัย ดังนี้

1. ด้านความรู้พื้นฐาน ในภาพรวมผู้ตอบแบบสอบถามให้ความสำคัญมากที่สุดกับความจำเป็นของความมั่นคงปลอดภัยทางไซเบอร์ในวิชาชีพบัญชี ซึ่งสอดคล้องกับการศึกษาของ Zwilling at al. (2022) ที่พบความสัมพันธ์เชิงบวกระหว่างระดับความรู้และการตระหนักรู้ เรื่องที่ได้ความสำคัญรองลงมาคือการตรวจสอบสิทธิ์แบบหลายปัจจัยเพื่อรักษาความปลอดภัยของระบบทางการเงิน ขณะที่เรื่องที่ได้ความสำคัญน้อยสุดคือผลกระทบของภัยคุกคามต่อข้อมูลทางการเงินและเครื่องมือควบคุมความปลอดภัยขั้นพื้นฐาน

2. ด้านการฝึกอบรม ในภาพรวมผู้ตอบแบบสอบถามเห็นความสำคัญสูงสุดของแผนรับมือเหตุการณ์สำหรับการละเมิดความปลอดภัยทางไซเบอร์ รองลงมาคือการติดตามข้อมูลล่าสุดเกี่ยวกับการละเมิดความปลอดภัย ซึ่งสอดคล้องกับแนวคิดของ Swain (2014) และ Fattah et al. (2023) เกี่ยวกับความสำคัญของการฝึกอบรมต่อเนื่อง อย่างไรก็ตาม การฝึกอบรมการตระหนักรู้และระเบียบปฏิบัติเป็นประจำได้ความสำคัญน้อยสุด ซึ่งอาจเนื่องมาจากข้อจำกัดด้านเวลาและทรัพยากร

3. ด้านทัศนคติ ในภาพรวมผู้ตอบแบบสอบถามให้ความสำคัญสูงสุดกับการกำหนดนโยบายรหัสผ่านที่รัดกุม รองลงมาคือการกำหนดสิทธิ์การเข้าถึงข้อมูลตามความจำเป็น ซึ่งสอดคล้องกับการศึกษาของ Ifinedo (2014) เกี่ยวกับบทบาทของทัศนคติต่อการปฏิบัติตามนโยบาย และเข้ากับกรอบแนวคิดของทฤษฎีพฤติกรรมตามแผนของ Ajzen (1991) เรื่องที่ได้ความสำคัญน้อยสุดคือการจดรหัสผ่านลงกระดาษหรือไฟล์ที่ไม่เข้ารหัส ซึ่งแสดงการตระหนักที่ดีเกี่ยวกับความเสี่ยงของการปฏิบัติดังกล่าว

4. ด้านพฤติกรรม ในภาพรวมผู้ตอบแบบสอบถามให้ความสำคัญสูงสุดกับการเปิดใช้งาน Multi-Factor Authentication รองลงมาคือการใช้งานเว็บไซต์ที่ขึ้นต้นด้วย https เท่านั้น ซึ่งสอดคล้องกับการศึกษาของ Felt et al. (2017) เกี่ยวกับความสำคัญของโปรโตคอล HTTPS ในการป้องกันข้อมูลอ่อนไหว เรื่องที่ได้ความสำคัญน้อยสุด คือ การเปิดอีเมล รวมถึงไฟล์แนบที่ส่งมาจากบัญชีผู้ใช้ที่ไม่รู้จัก ซึ่งแสดงให้เห็นถึงการตระหนักที่ดีเกี่ยวกับความเสี่ยงของการปฏิบัติดังกล่าว

การศึกษาข้อมูลทั่วไปด้านประชากรศาสตร์ที่ส่งต่อระดับการให้ความสำคัญของการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ จากการทดสอบสมมติฐานว่าปัจจัยข้อมูลทั่วไปของผู้ตอบแบบสอบถามใดบ้างมีต่อระดับการให้ความสำคัญของการตระหนักรู้ สามารถสรุปได้ดังนี้

1. ผู้ตอบแบบสอบถามที่มีอายุแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์แตกต่างกัน โดยกลุ่มอายุ 21-30 ปีมีระดับการตระหนักรู้สูงกว่ากลุ่มอายุ 31-40 ปี อย่างมีนัยสำคัญทางสถิติ ผลการศึกษานี้สอดคล้องกับการศึกษาของ Branley-Bell et al. (2022) ที่พบความสัมพันธ์ที่ไม่เป็นเส้นตรงระหว่างอายุกับการตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ ผู้ประกอบวิชาชีพบัญชีรุ่นใหม่มีระดับการตระหนักรู้สูงกว่าอาจเนื่องมาจากการได้รับการศึกษาเกี่ยวกับความปลอดภัยทางไซเบอร์ในหลักสูตรที่ทันสมัยกว่า

2. ผู้ตอบแบบสอบถามที่มีใบอนุญาตประกอบวิชาชีพแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมแตกต่างกัน โดยผู้ที่มีใบอนุญาตประกอบวิชาชีพ CPA เพียงอย่างเดียวมีระดับการตระหนักรู้สูงกว่าผู้ที่ไม่มีใบอนุญาตประกอบวิชาชีพอย่างมีนัยสำคัญทางสถิติ ซึ่งสอดคล้องกับการศึกษาของ Hasan et al. (2024) ที่ระบุว่าระดับความเชี่ยวชาญและคุณสมบัติทางวิชาชีพมีผลต่อระดับการตระหนักรู้และความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

3. ผู้ตอบแบบสอบถามที่มีประเภทหน่วยงานที่สังกัดแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมแตกต่างกัน โดยผู้ที่ทำงานในสำนักงานสอบบัญชีและผู้รับงานอิสระมีระดับการตระหนักรู้สูงกว่าผู้ที่ทำงานในบริษัทเอกชนและหน่วยงานราชการอย่างมีนัยสำคัญทางสถิติ ผู้ศึกษาเห็นว่าผู้ประกอบวิชาชีพบัญชีในสำนักงานสอบบัญชีและผู้รับงานอิสระต้องรับผิดชอบข้อมูลของลูกค้าหลายราย ทำให้มีความเสี่ยงในการถูกโจมตีทางไซเบอร์สูงกว่า ประกอบกับสำนักงานสอบบัญชีโดยเฉพาะรายใหญ่มีงบประมาณและโอกาสในการฝึกอบรมด้านความปลอดภัยทางไซเบอร์มากกว่าหน่วยงานอื่น

4. ผู้ตอบแบบสอบถามที่มีประสบการณ์ในการทำงาน (อายุงาน) แตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมแตกต่างกัน โดยผู้ที่มีประสบการณ์การทำงาน 11-15 ปีมีระดับการตระหนักรู้น้อยที่สุดเมื่อเทียบกับกลุ่มประสบการณ์อื่นอย่างมีนัยสำคัญทางสถิติ ปรากฏการณ์นี้สอดคล้องกับทฤษฎี Dunning-Kruger Effect ที่อธิบายว่าบุคคลที่มีความรู้ระดับปานกลางมักประเมินความสามารถของตนเองสูงเกินจริง กลุ่มนี้อาจอยู่ในช่วงเปลี่ยนผ่านระหว่างเทคโนโลยีเก่าและใหม่ โดยไม่ได้รับการฝึกอบรมพื้นฐานด้านความปลอดภัยไซเบอร์อย่างเข้มข้นเหมือนกลุ่มที่เพิ่งเข้าสู่วิชาชีพในยุคปัจจุบัน

5. ผู้ตอบแบบสอบถามที่มีสาขาที่เชี่ยวชาญแตกต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมแตกต่างกัน โดยผู้เชี่ยวชาญสาขาการสอบบัญชีและการทำบัญชีมีระดับการตระหนักรู้สูงกว่าผู้เชี่ยวชาญสาขาการบัญชีภาษีอากรและการวางระบบบัญชีอย่างมีนัยสำคัญทางสถิติ ผลการศึกษานี้สอดคล้องกับการศึกษาของ Mamade and Dabala (2021) ที่พบว่าสาขาวิชาที่ศึกษามีอิทธิพลต่อระดับการตระหนักรู้ลักษณะงานและความรับผิดชอบของผู้สอบบัญชีที่ต้องรับผิดชอบข้อมูลการเงินที่มีความอ่อนไหวสูงส่งผลให้มีระดับการตระหนักรู้ที่สูงกว่าสาขาอื่น

6. ผู้ตอบแบบสอบถามที่มีเพศและระดับการศึกษาที่ต่างกันมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมไม่แตกต่างกัน สอดคล้องกับการศึกษาของ Branley-Bell et al. (2022) ที่พบว่าความแตกต่างทางเพศไม่มีผลต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างมีนัยสำคัญ สำหรับระดับการศึกษา ผู้ศึกษาเห็นว่าการที่ไม่พบความแตกต่างอย่างมีนัยสำคัญอาจเป็นเพราะความรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ไม่ได้ขึ้นอยู่กับระดับการศึกษาในระบบ แต่ขึ้นอยู่กับการฝึกอบรมเฉพาะทางและประสบการณ์มากกว่า

กล่าวโดยสรุปผลการศึกษาครั้งนี้ชี้ให้เห็นว่าผู้ประกอบวิชาชีพบัญชีในประเทศไทยมีระดับการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในระดับสูงมาก โดยมีปัจจัยด้านความรู้พื้นฐานและการฝึกอบรมเป็นปัจจัยสำคัญที่สุด รองลงมาคือด้านทัศนคติและพฤติกรรม ซึ่งสอดคล้องกับงานของ Fattah et al. (2023) และ Zwilling et al. (2022) ที่ย้ำว่าความรู้และการฝึกอบรมอย่างต่อเนื่องเป็นแรงขับเคลื่อนสำคัญของการตระหนักรู้ด้านไซเบอร์ สำหรับงานบัญชีซึ่งเกี่ยวข้องกับข้อมูลทางการเงินที่มีความอ่อนไหวสูง ผลลัพธ์นี้สะท้อนถึงความจำเป็นในการบูรณาการความรู้ด้านไซเบอร์ทั้งในระดับการปฏิบัติงานและในหลักสูตรการศึกษา

ผลการศึกษายังแสดงให้เห็นว่าปัจจัยด้านประชากรศาสตร์ เช่น อายุ ใบอนุญาตประกอบวิชาชีพ หน่วยงานที่สังกัด สาขาที่เชี่ยวชาญ และประสบการณ์การทำงาน มีผลต่อระดับการตระหนักรู้ ขณะที่เพศและระดับการศึกษาไม่ส่งผล ซึ่งสอดคล้องกับ Branley-Bell et al. (2022) ที่พบว่าอายุมีอิทธิพลต่อพฤติกรรมด้านไซเบอร์แต่เพศไม่มี นอกจากนี้การที่ผู้ถือใบอนุญาต CPA มีระดับการตระหนักรู้สูงกว่าผู้ไม่มีใบอนุญาต สะท้อนว่าการสอบใบอนุญาตและมาตรฐานทางวิชาชีพ มีบทบาทเสริมสร้างมุมมองด้านความมั่นคงปลอดภัย อย่างไรก็ตาม กลุ่มที่มีใบอนุญาตหลายประเภทกลับมีระดับการตระหนักรู้ต่ำกว่า อาจเนื่องจากการขาดการบูรณาการด้านความมั่นคงปลอดภัยในหลักสูตรต่อเนื่อง

เมื่อจำแนกตามประเภทหน่วยงาน พบว่าผู้ทำงานในสำนักงานสอบบัญชีและผู้รับงานอิสระมีระดับการตระหนักรู้สูงกว่าผู้ทำงานในบริษัทเอกชนและหน่วยงานราชการ ซึ่งอาจสะท้อนถึงแรงกดดันด้านกฎระเบียบและความเสี่ยงจากลูกค้าที่ผู้ตรวจสอบต้องเผชิญโดยตรง ตลอดจนความรับผิดชอบต่อวิชาชีพ ข้อมูลนี้สอดคล้องกับ Trim and Lee (2019) ที่ชี้ว่าสภาพแวดล้อมองค์กรส่งผลต่อพฤติกรรมการป้องกันภัยไซเบอร์

ด้านประสบการณ์การทำงาน ผลลัพธ์บ่งชี้ว่าผู้ที่มีอายุงานระดับกลาง (11–15 ปี) มีการตระหนักรู้ต่ำกว่ากลุ่มอายุน้อยและอาวุโส ซึ่งอาจสะท้อนถึงวงจรการเรียนรู้ด้านเทคโนโลยี โดยกลุ่มอายุน้อยได้รับการศึกษาใหม่ล่าสุด ขณะที่กลุ่มอาวุโสมีประสบการณ์ตรงกับความเสี่ยงไซเบอร์มากกว่า ส่วนกลุ่มอายุงานกลางอาจมีภาระงานสูงและเข้าถึงการฝึกอบรมน้อยลง

ในทางปฏิบัติ ผลการศึกษาที่ชี้ถึงบทบาทสำคัญของการฝึกอบรม สนับสนุนแนวทางการพัฒนาโปรแกรมฝึกอบรมเชิงจำลองสถานการณ์ เช่น การจำลอง phishing หรือ ransomware การทำให้ผู้ประกอบวิชาชีพบัญชีเป็น “แนวป้องกันมนุษย์” มีความสำคัญต่อการปกป้องข้อมูลทางการเงิน อีกทั้งการบรรจุเนื้อหาไซเบอร์ในหลักสูตรบัญชีระดับปริญญาตรีตามข้อเสนอของ Swain (2014) จะช่วยเสริมสร้างพฤติกรรมที่ปลอดภัยตั้งแต่ต้น

โดยสรุป งานวิจัยนี้ได้เติมเต็มช่องว่างทางวิชาการ โดยขยายการศึกษาด้านความมั่นคงปลอดภัยทางไซเบอร์ไปสู่กลุ่มผู้ประกอบวิชาชีพบัญชี ซึ่งในอดีตมักถูกมองข้าม และยังเป็นหลักฐานเชิงประจักษ์ที่ยืนยันว่าปัจจัยด้านประชากรศาสตร์และองค์กรมีบทบาทไม่ยิ่งหย่อนไปกว่าปัจจัยด้านทัศนคติและพฤติกรรมของบุคคล

ข้อเสนอแนะ

จากผลการศึกษา สามารถนำไปสู่ข้อเสนอแนะเชิงนโยบายและแนวทางการปฏิบัติเพื่อยกระดับการตระหนักรู้และการป้องกันความเสี่ยงทางไซเบอร์ในสายวิชาชีพบัญชีได้ ดังนี้

1. การพัฒนาหลักสูตรฝึกอบรมเฉพาะด้าน องค์กรที่เกี่ยวข้องควรจัดทำหลักสูตรฝึกอบรมที่ครอบคลุมภัยคุกคามทางไซเบอร์ เทคโนโลยีป้องกัน การตอบสนองเหตุการณ์ฉุกเฉิน และการตั้งค่าความปลอดภัยพื้นฐาน โดยเน้นรูปแบบ e-learning ที่ยืดหยุ่นสำหรับองค์กรขนาดเล็กและผู้รับงานอิสระ

2. การบูรณาการความรู้ในหลักสูตรระดับปริญญาตรี สถาบันการศึกษาควรเพิ่มเนื้อหาด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับนักบัญชีในหลักสูตรบัญชี ครอบคลุมทั้งแนวคิดเชิงเทคนิคและเชิงจริยธรรม พร้อมสร้างความร่วมมือกับบริษัทบัญชีเพื่อให้นักศึกษาได้สัมผัสกับแนวปฏิบัติจริง

3.การส่งเสริมวัฒนธรรมองค์กรองค์กรควรกำหนดนโยบายความปลอดภัยด้านไอทีอย่างเป็นรูปธรรมจัดการอบรมภายในอย่างสม่ำเสมอ และประเมินพฤติกรรมเสี่ยงด้านไซเบอร์ของพนักงานเพื่อป้องกันช่องโหว่

4. การส่งเสริมความร่วมมือระหว่างสภาวิชาชีพ สถาบันการศึกษา และหน่วยงานรัฐ เพื่อให้แนวทางด้านความมั่นคงปลอดภัยทางไซเบอร์ในสายวิชาชีพบัญชีมีความครอบคลุมและยั่งยืน

5. ข้อเสนอเฉพาะจากผลการวิเคราะห์ตามข้อมูลทั่วไปด้านประชากรศาสตร์

5.1 ด้านใบอนุญาตประกอบวิชาชีพ: ผู้ที่ไม่มีใบประกอบวิชาชีพ ควรได้รับการสนับสนุนการฝึกอบรมด้านไซเบอร์ในราคาย่อมเยา เพื่อส่งเสริมให้ตระหนักและปฏิบัติตามมาตรฐาน และบูรณาการเนื้อหาด้านความมั่นคงปลอดภัยทางไซเบอร์เข้ากับการพัฒนาความรู้ต่อเนื่องทางวิชาชีพ

5.2 ด้านสาขาที่เชี่ยวชาญ: กลุ่มผู้เชี่ยวชาญสาขาการสอบบัญชีและการทำบัญชี มีระดับการตระหนักรู้สูง ควรมีบทบาทเป็นผู้นำในการแบ่งปันความรู้และประสบการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ให้กับผู้ประกอบวิชาชีพบัญชีในสาขาอื่น และมีส่วนร่วมในการพัฒนาเครื่องมือประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับวิชาชีพบัญชี

ข้อจำกัดและข้อเสนอแนะเกี่ยวกับประเด็นที่ควรศึกษาในครั้งต่อไป

การศึกษาครั้งนี้มีข้อจำกัดสำคัญประการหนึ่งคือขนาดกลุ่มตัวอย่างจำนวน 305 คน แม้จะเป็นจำนวนที่เพียงพอต่อการวิเคราะห์ทางสถิติ แต่อาจไม่สามารถเป็นตัวแทนของผู้ประกอบวิชาชีพบัญชีในประเทศไทยทั้งหมดได้อย่างสมบูรณ์ นอกจากนี้ การใช้แบบสอบถามที่ผู้ตอบรายงานด้วยตนเองอาจมีความเสี่ยงจากอคติด้านความต้องการทางสังคมหรืออคติในการตอบคำถาม นอกจากนั้น งานวิจัยนี้ยังมีข้อจำกัดที่ควรพิจารณาเมื่อแปลผลลัพธ์ กล่าวคือ แบบสอบถามบางข้อที่มีทิศทางตรงข้ามมิได้ปรับค่าคะแนนย้อนกลับ (reverse score) ทำให้ผลการคำนวณค่าเฉลี่ยและการทดสอบ ANOVA อาจมีความคลาดเคลื่อนบ้าง แม้ผู้วิจัยตั้งใจคงความเรียบง่ายในการวิเคราะห์ แต่ประเด็นนี้อาจมีผลกระทบต่อความถูกต้องเชิงสถิติกลุ่มตัวอย่างบางกลุ่มมีจำนวนผู้ตอบค่อนข้างน้อย เช่น ผู้ที่มีอายุมากกว่า 60 ปี หรือผู้ถือใบอนุญาตวิชาชีพบางประเภท ซึ่งอาจส่งผลต่อความน่าเชื่อถือของการวิเคราะห์ โดยเฉพาะในการเปรียบเทียบระหว่างกลุ่ม นอกจากนั้น การทดลองใช้แบบสอบถาม (pilot test) แม้จะเป็นประโยชน์ต่อการตรวจสอบความชัดเจนของคำถามและความเหมาะสมของโครงสร้าง แต่ก็อาจไม่สะท้อนมุมมองของกลุ่มเป้าหมายจริงที่อยู่ในวิชาชีพบัญชี สุดท้าย การเก็บข้อมูลผ่านช่องทางออนไลน์ แม้จะมีการใช้คำถามคัดกรองเพื่อจำกัดผู้ตอบให้ตรงตามคุณสมบัติ แต่ก็ยังมีความเป็นไปได้ที่ผู้ตอบบางส่วนอาจไม่ใช่ผู้ประกอบวิชาชีพบัญชีโดยตรง ซึ่งอาจมีผลกระทบต่อความน่าเชื่อถือของข้อมูลและการตีความผลการวิจัยโดยรวม

การศึกษาครั้งต่อไปควรพิจารณาการใช้กลุ่มตัวอย่างที่มีขนาดใหญ่ขึ้นและหลากหลายมากขึ้น รวมทั้งการใช้วิธีการวิจัยเชิงคุณภาพ เช่น การสัมภาษณ์หรือการสนทนากลุ่มเพื่อให้ได้ข้อมูลเชิงลึกเกี่ยวกับทัศนคติและพฤติกรรมของผู้ประกอบวิชาชีพบัญชี ควรมีการเปรียบเทียบกับผู้เชี่ยวชาญในสาขาอื่นเพื่อให้ได้มุมมองที่กว้างขึ้น และควรพิจารณาปัจจัยอื่นที่อาจมีอิทธิพล เช่น นโยบายองค์กร โครงสร้างพื้นฐานด้านความปลอดภัยทางไซเบอร์ และภัยคุกคามรูปแบบใหม่

สรุปผลการศึกษา

การศึกษาพบว่าปัจจัยสำคัญที่ส่งผลต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของผู้ประกอบวิชาชีพบัญชีประกอบด้วยความรู้พื้นฐาน การฝึกอบรม ทัศนคติ และพฤติกรรม โดยความรู้พื้นฐานและการฝึกอบรมมีผลกระทบสูงสุด ชี้ให้เห็นถึงความจำเป็นของการมีความรู้ที่ถูกต้องและการฝึกอบรมอย่างต่อเนื่อง ด้านประชากรศาสตร์ พบว่าอายุ ใบอนุญาตประกอบวิชาชีพ ประเภทหน่วยงานที่สังกัด ประสบการณ์การทำงาน และสาขาที่เชี่ยวชาญมีผลต่อระดับการตระหนักรู้ ขณะที่เพศและระดับการศึกษาไม่มีผลอย่างมีนัยสำคัญ ผลการศึกษาสามารถนำไปใช้ในเชิงปฏิบัติได้โดยองค์กรควรให้ความสำคัญกับการพัฒนาความรู้พื้นฐานและการฝึกอบรมด้านความปลอดภัยทางไซเบอร์อย่างต่อเนื่อง โดยปรับให้เหมาะสมกับแต่ละกลุ่มเป้าหมาย สถาบันการศึกษาควรบูรณาการเนื้อหาด้านความปลอดภัยทางไซเบอร์เข้ากับหลักสูตรบัญชี ขณะที่สภาวิชาชีพบัญชีควรกำหนดให้ความรู้และทักษะด้านไซเบอร์เป็นส่วนหนึ่งของมาตรฐานวิชาชีพ การสร้างเครือข่ายความร่วมมือระหว่างสภาวิชาชีพ สถาบันการศึกษา และหน่วยงานรัฐเพื่อพัฒนาแนวปฏิบัติที่เหมาะสมกับบริบทวิชาชีพบัญชีไทยจะช่วยยกระดับการตระหนักรู้และการป้องกันความเสี่ยงทางไซเบอร์ให้มีประสิทธิภาพมากขึ้น

ผลการศึกษานี้มีข้อเสนอเชิงนัยสำคัญหลายประการ สำหรับผู้ประกอบวิชาชีพบัญชี ควรเข้าร่วมการพัฒนาอย่างต่อเนื่องที่เน้นทั้งความรู้เชิงเทคนิคและพฤติกรรมที่ช่วยลดความเสี่ยงไซเบอร์ สำหรับ หน่วยงานกำกับดูแลและองค์กรวิชาชีพ เช่น สภาวิชาชีพบัญชี ควรกำหนดให้การตระหนักรู้ด้านไซเบอร์เป็นส่วนหนึ่งของเกณฑ์การสอบใบอนุญาตและการศึกษาต่อเนื่อง สำหรับสถาบันการศึกษาควรบรรจุวิชาหรือโมดูลด้านไซเบอร์ในหลักสูตรบัญชี เพื่อให้บัณฑิตมีความพร้อมรับมือกับความเสี่ยงตั้งแต่เข้าสู่วิชาชีพ และสำหรับ องค์กรและนายจ้าง ควรสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับไซเบอร์ เช่น การฝึกอบรม การจำลองสถานการณ์ และการกำหนดนโยบายที่เข้มแข็ง เพื่อให้บุคลากรทุกระดับมีความตระหนักรู้และพร้อมปกป้องข้อมูลทางการเงินขององค์กร

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring age and gender differences in ICT cybersecurity behaviour. *Human Behavior and Emerging Technologies*, 2022, 1–10. https://doi.org/10.1155/2022/2693080

Charoenpichet, Chanida (2023) *The relationship between cybersecurity awareness and behavior of certified public accountants in Thailand* (Independent study, Master of Accountancy). Thammasat University.

Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). John Wiley & Sons.

Cronbach, L. J. (1990). *Essentials of psychological testing* (5th ed.). Harper & Row.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*(1), 32–64. https://doi.org/10.1518/001872095779049543

Fattah, A., Wagimin, W., & Nurlia, N. (2023). Enhancing cybersecurity awareness among university students: A study on the relationship between knowledge, attitude, behavior, and training. *JSI: Jurnal Sistem Informasi (E-Journal), 15*(1). https://doi.org/10.18495/jsi.v15i1.21812

Felt, A. P., Barnes, R., King, A., Palmer, C., Bentzel, C., & Tabriz, P. (2017). Measuring HTTPS adoption on the web. In *Proceedings of the 26th USENIX Security Symposium* (pp. 1323–1338). USENIX Association.

European Parliament (2016). *General data protection regulation (GDPR) – Legal text*. https://gdpr-info.eu/

Hasan, L., Hossain, M. Z., Johora, F. T., & Hasan, M. H. (2024). Cybersecurity in accounting: Protecting financial data in the digital age. *European Journal of Applied Science, Engineering and Technology, 2*(6), 64–80. https://doi.org/10.59324/ejaset.2024.2(6).06

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

International Organization for Standardization & International Electrotechnical Commission. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.* International Organization for Standardization. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Katz, D. (1960). The functional approach to the study of attitudes. *Public Opinion Quarterly, 24*(2), 163–204. https://doi.org/10.1086/266945

Mamade, B. K., & Dabala, D. M. (2021). Exploring the correlation between cybersecurity awareness, protection measures and the state of victimhood: The case study of Ambo University's academic staffs. *Journal of Cyber Security and Mobility, 10*(4), 419–439. https://doi.org/10.13052/jcsm2245-1439.1044

National Cyber Security Agency (NCSA). (2025). *Threat statistics.* https://www.ncsa.or.th/policy/threat-statistics

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Royal Gazette. (2004). *Accounting Profession Act B.E. 2004.* https://www.tfac.or.th/upload/9414/BQnA6YI6XE.pdf

Royal Gazette. (2017). *Computer Crime Act (No. 2) B.E. 2017*. https://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF

Royal Gazette. (2019). *Personal Data Protection Act B.E. 2562*. https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

SEC. (2018). Commission statement and guidance on public company cybersecurity disclosures. https://www.sec.gov/rules/interp/2018/33-10459.pdf

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Swain, N. (2014). A multi-tier approach to cyber security education, training, and awareness in the undergraduate curriculum (CSETA). In *2014 ASEE Annual Conference & Exposition Proceedings* (pp. 24.72.1–24.72.9). American Society for Engineering Education. https://doi.org/10.18260/1-2--19964

Thammasiri, M., & Wongthongdee, S. (2022). Cyber security awareness of employees in one private company in Bangkok area. *Thai Research and Management Journal, 3*(2), 1–17.

Trim, P. R. J., & Lee, Y.-I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management, 83*, 224–238. https://doi.org/10.1016/j.indmarman.2019.04.003

World Economic Forum. (2024). *The global risks report 2024* (19th ed.). https://www.weforum.org/publications/global-risks-report-2024/

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