การรับรู้ภัยทางไซเบอร์ส่งผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ของประชากรในจังหวัดกรุงเทพมหานคร

Perception of Cyber Threats Affects the Cyber Security Awareness Of the Population in Bangkok

ประสพ เชาว์ศิลป์[1],อรไท ชั้วเจริญ[2]

บทคัดย่อ

การวิจัยนี้ได้มีวัตถุประสงค์เพื่อศึกษา 1) เพื่อศึกษาการรับรู้ภัยทางไซเบอร์และการตระหนักด้านความปลอดภัยทางไซเบอร์ของประชากรในจังหวัดกรุงเทพมหานคร 2) เพื่อเปรียบเทียบการตระหนักด้านความปลอดภัยทางไซเบอร์จำแนกตามปัจจัยส่วนบุคคล 3) เพื่อศึกษาความสัมพันธ์ระหว่างการรับรู้ภัยทางไซเบอร์กับการตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของ ประชากรในจังหวัดกรุงเทพมหานคร โดยเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างจำนวน 403 คน ในพื้นที่กรุงเทพมหานครด้วยวิธีการใช้แบบสอบถาม ข้อมูลที่ได้ถูกนำมาวิเคราะห์ด้วยสถิติเชิงพรรณนาเพื่ออธิบายข้อมูลส่วนบุคคลและระดับความเห็นต่างๆ และสถิติเชิงอนุมาน เช่น t-test , One-Way ANOVA ,ทดสอบเปรียบเทียบความแตกต่างเป็นรายคู่วิธี LSD และการวิเคราะห์ถดถอยพหุคูณเพื่อทดสอบสมมติฐาน

ผลการศึกษาพบว่า การรับรู้ภัยคุกคามทางไซเบอร์และการตระหนักด้านความปลอดภัยทางไซเบอร์ของประชากรในกรุงเทพมหานคร สอดคล้องกับวัตถุประสงค์ข้อที่ 1 ผู้ตอบแบบสอบถามมีการรับรู้ภัยคุกคามโดยภาพรวมอยู่ในระดับปานกลาง แต่มีการตระหนักด้านความปลอดภัยโดยภาพรวมอยู่ในระดับมาก วัตถุประสงค์ข้อที่ 2 เพื่อเปรียบเทียบการตระหนักตามปัจจัยส่วนบุคคล พบว่า เพศที่แตกต่างกันมีการตระหนักด้านความปลอดภัยทางไซเบอร์ไม่ต่างกัน ขณะที่อายุ, ระดับการศึกษา และอาชีพ ที่แตกต่างมีการตระหนักด้านความปลอดภัยทางไซเบอร์ที่ต่างกัน สำหรับวัตถุประสงค์ข้อที่ 3 พบว่า การรับรู้ภัยทางไซเบอร์ที่มีอิทธิพลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ มี 2 ด้านคือ ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ และการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ ที่มีนัยสำคัญทางสถิติที่ระดับ 0.05

คำสำคัญ : การรับรู้ภัยทางไซเบอร์, การตระหนักด้านความปลอดภัยทางไซเบอร์,ประชากรในกรุงเทพมหานคร

---

[1] นักศึกษาปริญญาโท หลักสูตรบริหารธุรกิจมหาบัณฑิต โครงการพิเศษหลักสูตรบริหารธุรกิจมหาบัณฑิต (Visionary Leaders) รุ่นที่ 26 มหาวิทยาลัยรามคำแหง

[2] อาจารย์ประจำมหาวิทยาลัยรามคำแหง

Abstract

This research aimed to 1) study the perception of cyber threats and cyber security awareness of the population in Bangkok; 2) compare cyber security awareness classified by personal factors; 3) investigate the relationship between the perception of cyber threats and cyber security awareness of the population in Bangkok. Data was collected from a sample group of 403 individuals in Bangkok using questionnaires. The data was analyzed using descriptive statistics to explain personal information and different levels of opinions, and inferential statistics such as t-tests, One-Way ANOVA, LSD post hoc tests, and multiple regression analysis to test hypotheses.

The study found that the perception of cyber threats and cyber security awareness of the population in Bangkok aligned with the first objective. Overall, respondents had a moderate level of cyber threat perception but a high level of cyber security awareness. Regarding the second objective, comparing awareness based on personal factors revealed no difference in cyber security awareness between genders, while age, education level, and occupation showed differences in cyber security awareness. For the third objective, two aspects of cyber threat perception influenced cyber security awareness: knowledge about cyber threats and cyber security training, both with a statistical significance level of 0.05.

Keywords: Cyber Threat Awareness, Cybersecurity Awareness, Bangkok Population.

บทนำ

ความสำคัญของปัญหา

ในยุคปัจจุบัน เทคโนโลยีดิจิทัลได้กลายเป็นองค์ประกอบสำคัญของชีวิตมนุษย์ ไม่ว่าจะเป็นในด้านการใช้ชีวิตประจำวัน การทำงาน ธุรกิจ หรือแม้แต่บริการของภาครัฐ เทคโนโลยีเหล่านี้เข้ามามีบทบาทในการขับเคลื่อนสังคมและเศรษฐกิจ ทำให้โลกของเราก้าวสู่ยุคที่ทุกอย่างเชื่อมโยงถึงกันได้ง่ายขึ้น การสื่อสาร การทำธุรกรรมทางการเงิน การจัดเก็บข้อมูล การศึกษา การแพทย์ และการค้าขาย ล้วนได้รับอิทธิพลจากความก้าวหน้าทางเทคโนโลยี ซึ่งส่งผลให้เกิดความสะดวกสบาย ประสิทธิภาพที่เพิ่มขึ้น รวมถึงโอกาสใหม่ๆ ที่ไม่เคยเกิดขึ้นมาก่อน หนึ่งในตัวอย่างที่เห็นได้ชัดคือการสื่อสาร ปัจจุบันผู้คนสามารถติดต่อกันได้ง่ายดายผ่านแพลตฟอร์มออนไลน์ต่างๆ เช่น Facebook, Line, WhatsApp, Zoom และ Microsoft Teams การสนทนาไม่จำกัดเพียงแค่ข้อความหรือเสียงเท่านั้น แต่ยังสามารถทำการประชุมผ่านวิดีโอคอลได้แบบเรียลไทม์จากทุกมุมโลก เทคโนโลยีนี้ทำให้การทำงานร่วมกันของทีมที่อยู่ห่างไกลกันเป็นไปได้ง่ายขึ้น องค์กรหลายแห่งเริ่มใช้ระบบการทำงานแบบ Remote Work หรือ Hybrid Work ซึ่งช่วยลดค่าใช้จ่ายในการเดินทางและเพิ่มความยืดหยุ่นให้กับพนักงานมากขึ้น นอกจากนี้เทคโนโลยีทางการเงินหรือ FinTech ก็เป็นอีกหนึ่งปัจจัยสำคัญที่ช่วยเปลี่ยนแปลงพฤติกรรมของผู้คนจากเดิมที่ต้องพกเงินสดหรือทำธุรกรรมที่ธนาคาร มาเป็นการใช้ Mobile Banking และ E-Wallet อย่าง True Money, Prompt Pay, PayPal หรือ Apple Pay ซึ่งช่วยให้การใช้จ่ายสะดวก รวดเร็ว ทำให้ร้านค้าสามารถรองรับการจ่ายเงินผ่าน QR Code หรือแอปพลิเคชันต่างๆ ได้อย่างแพร่หลาย และยังมีเทคโนโลยีดิจิทัลที่ให้ในการจัดเก็บข้อมูลผ่านระบบคลาวด์ที่สามารถเข้าถึงได้ ไม่ว่าจะเป็นข้อมูลส่วนตัว ภาพถ่าย หรือเอกสารสำคัญ

เมื่อพิจารณาจากความท้าทายด้าน Cybersecurity ในยุคดิจิทัลและความแตกต่างด้านการรับรู้ภัยไซเบอร์ การตระหนักด้านความปลอดภัยทางไซเบอร์ของประชากรในจังหวัดกรุงเทพมหานครจำเป็นต้องได้รับการศึกษา เพื่อป้องกันผลกระทบที่จะสร้างความเสียหายทางการเงินให้กับบุคคล งานวิจัยนี้จึงมุ่งเน้นศึกษาความสัมพันธ์ระหว่างการรับรู้ภัยไซเบอร์ (Cyber Threat Awareness) และความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Awareness) เพื่อนำผลการศึกษามาเสนอแนะเป็นแนวทางในการสร้างระบบความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพได้ต่อไป และสามารถป้องกันตนเองจากภัยคุกคามทางไซเบอร์

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาการรับรู้ภัยทางไซเบอร์และการตระหนักด้านความปลอดภัยทางไซเบอร์ของประชากรในจังหวัดกรุงเทพมหานคร
2. เพื่อเปรียบเทียบการตระหนักด้านความปลอดภัยทางไซเบอร์จำแนกตามปัจจัยส่วนบุคคล

3. เพื่อศึกษาความสัมพันธ์ระหว่างการรับรู้ภัยทางไซเบอร์กับการตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของ ประชากรในจังหวัดกรุงเทพมหานคร

ขอบเขตของการวิจัย

1. ขอบเขตด้านประชากรและกลุ่มตัวอย่าง การวิจัยครั้งนี้ศึกษากลุ่มตัวอย่างที่เป็นคนไทยที่อาศัยอยู่ในจังหวัดกรุงเทพมหานคร จำนวน 403 คน

2. ขอบเขตด้านเครื่องมือวิจัย ใช้แบบสอบถาม (Questionnaire) เป็นเครื่องมือหลักในการเก็บรวบรวมข้อมูล โดยประกอบด้วยคำถามเกี่ยวกับการรับรู้ภัยทางไซเบอร์ (Cyber Threat Awareness) และการตระหนักด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Awareness)

3. ขอบเขตด้านพื้นที่และเวลา การเก็บข้อมูลจะดำเนินการใน พื้นที่กรุงเทพมหานคร โดยมีระยะเวลาในการเก็บข้อมูลระหว่าง เดือนกุมภาพันธ์ ถึงเดือนเมษายน ปี พ.ศ. 2568

4. ขอบเขตด้านเนื้อหา การวิจัยมุ่งเน้นศึกษาความสัมพันธ์ระหว่างการรับรู้ภัยทางไซเบอร์กับการตระหนักด้านความปลอดภัยทางไซเบอร์ของกลุ่มตัวอย่างจำแนกตามปัจจัยส่วนบุคคล

สมมติฐานของการวิจัย

1. ปัจจัยส่วนบุคคลที่แตกต่างกันจะมีการตระหนักด้านความปลอดภัยทางไซเบอร์ที่แตกต่างกัน
2. ศึกษาความสัมพันธ์ระหว่างการรับการรับรู้ภัยทางไซเบอร์กับการตระหนักด้านความปลอดภัยทางไซเบอร์

วรรณกรรม และงานวิจัยที่เกี่ยวข้อง

ความรู้ทั่วไปด้านไซเบอร์

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศมีบทบาทสำคัญในทุกภาคส่วนของสังคม การรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศเป็นสิ่งที่ไม่อาจมองข้ามได้ Cybersecurity หรือการรักษาความปลอดภัยทางไซเบอร์ จึงเป็นเรื่องที่ควรให้ความสำคัญอย่างยิ่ง

Cybersecurity หมายถึง การป้องกันข้อมูล ระบบเครือข่าย และโปรแกรมต่างๆ จากการโจมตีทางไซเบอร์ ซึ่งอาจเป็นการเข้าถึงโดยไม่ได้รับอนุญาต การทำลาย หรือการเปลี่ยนแปลงข้อมูลและระบบ โดยมีวัตถุประสงค์เพื่อปกป้องความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

แนวความคิดเกี่ยวกับการรับรู้ภัยทางไซเบอร์

อาชญากรรมคอมพิวเตอร์ (Computer Crime)

อาชญากรรมคอมพิวเตอร์หมายถึง การกระทำใดๆ ที่เกี่ยวข้องกับการใช้คอมพิวเตอร์ ทำให้ผู้ใช้คอมพิวเตอร์นั้นได้รับความเสียหาย เช่น การลักทรัพย์อุปกรณ์คอมพิวเตอร์ เป็นต้น นอกจากนี้ยังหมายรวมถึงการกระทำใดๆ ที่เป็นความผิดทางอาญา ซึ่งจะต้องใช้ความรู้เกี่ยวกับ คอมพิวเตอร์ในการกระทำความผิดนั้น เช่น การบิดเบือนข้อมูล (Extortion) การเผยแพร่รูปอนาจาร ผู้เยาว์ (Child pornography) การฟอกเงิน (Money Laundering) ฉ้อโกง (Fraud) การถอดรหัส โปรแกรมคอมพิวเตอร์ โดยไม่รับอนุญาต แล้วเผยแพร่ให้ผู้อื่นดาวน์โหลดได้ บางครั้งเรียกว่า การ โจรกรรมโปรแกรม (Software Pirating) และการขโมยข้อมูลความลับทางการค้าของบริษัท (Corporate Espionage) เป็นต้น (Shelly & Vermaat, 2010) อาชญากรรมคอมพิวเตอร์เป็นความผิดที่กระทำขึ้นต่อปัจเจกบุคคลหรือกลุ่มของปัจเจก บุคคลด้วยเหตุจูงใจทางอาญา ที่เจตนาทำให้เหยื่อเสื่อมเสียชื่อเสียง หรือทำร้ายร่างกายหรือจิตใจของ เหยื่อ ทั้งทางตรงหรือทางอ้อม โดยใช้เครือข่ายโทรคมนาคมสมัยใหม่ อาทิ อินเทอร์เน็ต (ห้องแช็ต อีเมล กระดานประกาศ และกลุ่มข่าว) และโทรศัพท์เคลื่อนที่ (เอสเอ็มเอส/ เอ็มเอ็มเอส) (Halder, Jaishankar, & Jaishankar, 2012) ปัจจุบันอาชญากรรมทางคอมพิวเตอร์ถือเป็นอาชญากรรมทาง เศรษฐกิจ หรืออาชญากรรมทางธุรกิจรูปแบบหนึ่งที่มีความสำคัญ เนื่องจากได้ก่อให้เกิดความ เสียหายต่อเศรษฐกิจของประเทศจำนวนมหาศาล

ภัยคุกคามทางไซเบอร์ (Cyber Threat)

จาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 3 บัญญัติ ความหมายภัยคุกคามไซเบอร์ ไว้ว่า "การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นๆที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง"

แนวความคิดเกี่ยวกับการตระหนักด้านความปลอดภัยทางไซเบอร์

แนวคิดเกี่ยวกับความตระหนัก (Awareness)

พจนานุกรมราชบัณฑิตสถาน พ.ศ. 2542 (2546) ได้ให้ความหมาย "ความตระหนักว่า เป็นการรู้ประจักษ์ชัด รู้ชัดแจ้ง" โดยลอดคล้องกับพจนานุกรม ของ Good (1973, p. 54) โดยได้ให้ ความหมายว่า "การแสดงออกจากการระลึกได้หรือจดจำได้" นอกจากนั้น ยังมีผู้นิยามไว้อีก ดังนี้

Bloom (1971, p. 271 อ้างถึงใน สุพัตรา ถนอมวงค์, 2551, น.10) ได้ให้นิยามว่า "ความตระหนักคือ ภาคต่ำสุดทางภาคอารมณ์ซึ่งความตระหนักนั้นคล้ายกับอารมณ์ความรู้สึก (Affective

Domain) แต่ความตระหนักต่างกับความรู้สึกตรงที่ความตระหนักไม่จำเป็นต้องเน้น ปรากฏการณ์หรือสิ่งหนึ่งสิ่งใด แต่ความตระหนักจะเกิดขึ้นเมื่อมีสิ่งเร้าให้เกิดความตระหนัก"

แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช. หรือ NSTDA) ให้ความหมายของไซเบอร์ (Cyber) ว่าเป็น คำที่กร่อนมาจากคำว่าไซเบอร์เนติกส์ (Cybernetics) และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต (Internet) และยังมีการให้ความหมาย "สารสนเทศ (Virtual) เสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง" (www.nstda.or.th, 2557)

โดยรวมแล้ว Cyber จึงเป็นความหมายในเชิงนามธรรม หมายถึง ขอบเขตที่เกี่ยวข้องกับการใช้งานของระบบเครือข่ายคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ ซึ่งจะครอบคลุมมากกว่าคอมพิวเตอร์ ซึ่งมีความหมายในเชิงรูปธรรมของอุปกรณ์ระบบคอมพิวเตอร์ทั่วไป

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์

จาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 3 บัญญัติความหมายภัยคุกคามไซเบอร์ ไว้ว่า

“การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นๆ ที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง”

วิธีการดำเนินการวิจัย

ประชากรและขนาดกลุ่มตัวอย่าง

ประชากรที่ใช้ในการวิจัยครั้งนี้ คือประชากรในกรุงเทพมหานคร ใช้วิธีการสุ่มตัวอย่างแบบง่าย และได้ทำการเก็บข้อมูลตัวอย่างจำนวน 403 ตัวอย่าง

เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลการวิจัยครั้งนี้ คือ แบบสอบถามเพื่อการวิจัย (Questionnaire) เรื่อง การรับรู้ภัยทางไซเบอร์ส่งผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ของประชากรในจังหวัดกรุงเทพมหานคร สร้างขึ้นจากกรอบแนวคิดที่พัฒนาจากวรรณกรรมและงานวิจัยที่เกี่ยวข้อง โดยคำนึงถึงวัตถุประสงค์ของการวิจัยเป็นหลัก เนื้อหาของแบบสอบถามประกอบด้วย 3 ส่วน ดังนี้ คือ

ส่วนที่ 1 แบบสอบถามเกี่ยวกับปัจจัยส่วนบุคคล ได้แก่ เพศ อายุ ระดับการศึกษา และอาชีพ

ส่วนที่ 2 ข้อมูลเกี่ยวกับการรับรู้ภัยทางไซเบอร์ เพื่อดูว่าประชากรมีระดับความคิดเห็นต่อภัยทางไซเบอร์ มากน้อยพียงใด ประกอบด้วย 3 ด้าน ได้แก่ ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ ประสบการณ์ส่วนตัวเกี่ยวกับภัยไซเบอร์ และการฝึกอบรมด้านความปลอดภัยทางไซเบอร์

ส่วนที่ 3 ข้อมูลการตระหนักด้านความปลอดภัยทางไซเบอร์ เพื่อดูว่าบุคลากรมีระดับความคิดเห็นต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ มากน้อยพียงใด ประกอบด้วย 3 ด้าน ได้แก่ ความเข้าใจในแนวทางปฏิบัติที่ปลอดภัย การปฏิบัติตามมาตรการความปลอดภัย พฤติกรรมการใช้งานระบบไอทีอย่างปลอดภัย

ช่วงเวลาในการเก็บรวบรวมข้อมูล

ตั้งแต่ช่วงเดือนกุมภาพันธ์พ.ศ. 2568 ถึงเดือนเมษายน พ.ศ. 2568

สถิติที่ใช้ในการวิเคราะห์ข้อมูล

1. การแจกแจงค่าความถี่ และหาค่าร้อยละค่าร้อยละ (Percentage) เพื่อใช้อธิบายข้อมูลที่ได้จากแบบสอบถามของส่วนที่ 1 เกี่ยวกับปัจจัยส่วนประชากรในจังหวัดกรุงเทพมหานคร ได้แก่ อายุ เพศ ระดับการศึกษา และอาชีพ

2. ค่าเฉลี่ย (Mean) และส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) เพื่อใช้อธิบายข้อมูลที่ได้จากแบบสอบถามของส่วนที่ 2 เกี่ยวกับระดับความคิดเห็นการรับรู้ภัยทางไซเบอร์ของประชากรในจังหวัดกรุงเทพมหานคร และส่วนที่ 3 ระดับความคิดเห็นการตระหนักด้านความปลอดภัยทางไซเบอร์ของประชากรในจังหวัดกรุงเทพมหานคร

3. วิเคราะห์ข้อมูลเปรียบเทียบความแตกต่าง ของปัจจัยส่วนบุคคลและการรับรู้ทางไซเบอร์มีผลต่อตระหนักด้านความปลอดภัยทางไซเบอร์ โดยใช้วิธีการเปรียบเทียบความแตกต่างระหว่างตัวแปรมากกว่า 2 ตัวแปร ด้วยการวิเคราะห์ความแปรปรวนทางเดียว One - way ANOVA (F-test) และเปรียบเทียบความแตกต่างเป็นรายคู่วิธี Least - Significant Different (LSD) และทดสอบสมมติฐานที่ระดับนัยสำคัญทางสถิติเท่ากับ 0.05

4. การวิเคราะห์ความสัมพันธ์ การรับรู้ภัยทางไซเบอร์ กับการตระหนักด้านความปลอดภัยทางไซเบอร์ โดยใช้การวิเคราะห์สัมประสิทธิ์สหสัมพันธ์เพียร์สัน (Pearson’s Correlation) เพื่อศึกษาว่ามีความสัมพันธ์เชิงเส้นตรงกันในระดับใด และมีทิศทางของความสัมพันธ์เป็นไปในอาจจะปรับเป็น ไปในทางเดี่ยวกันหรือตรงกันข้าม

5. การสร้างสมการถดถอยเชิงเส้น จากการวิเคราะห์ข้อมูลการรับรู้ภัยทางไซเบอร์ส่งผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ ของประชากรในจังหวัดกรุงเทพมหานคร ใช้การวิเคราะห์การถดถอยแบบพหุคูณ (Multiple Regression Analysis) กำหนดระดับนัยสำคัญทางสถิติที่ 0.05

ผลการวิเคราะห์ข้อมูล

สรุปผลการทดสอบสมมติฐาน

สรุปผลการทดสอบสมมติฐานปัจจัยส่วนบุคคลที่แตกต่างกันจะมีผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ที่ต่างกัน

การตระหนักด้านความปลอดภัยทางไซเบอร์	ปัจจัยส่วนบุคคล			
	เพศ	อายุ	ระดับการศึกษา	อาชีพ
ความเข้าใจในแนวทางปฏิบัติที่ปลอดภัย	✓	✓	×	✓
การปฏิบัติตามมาตรการความปลอดภัย	✓	×	✓	×
พฤติกรรมการใช้งานระบบไอทีอย่างปลอดภัย	✓	×	✓	✓
การตระหนักด้านความปลอดภัยทางไซเบอร์ด้านภาพรวม	✓	×	×	×

หมายเหตุ เครื่องหมาย ✓ หมายถึง ไม่ต่างกัน, เครื่องหมาย × หมายถึง ต่างกัน

ผลการวิจัย พบว่าปัจจัยด้านเพศเป็นปัจจัยเดียวที่ไม่มีผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ในทุกด้าน ปัจจัยด้านอายุที่แตกต่างไม่ส่งผลต่อด้านความเข้าใจในแนวทางปฏิบัติที่ปลอดภัย แต่มีผลต่อด้านอื่นๆ ระดับการศึกษาที่ต่างกันไม่ส่งผลต่อการปฏิบัติตามมาตรการและพฤติกรรมการใช้งานระบบไอทีอย่างปลอดภัย อาชีพที่ต่างกันไม่มีผลต่อความเข้าใจในแนวทางปฏิบัติที่ปลอดภัยและพฤติกรรมการใช้งานระบบไอทีอย่างปลอดภัย

สรุปผลการทดสอบสมมติฐานการรับรู้ภัยทางไซเบอร์ที่แตกต่างกันจะมีผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ที่ต่างกัน

การตระหนักด้านความปลอดภัยทางไซเบอร์	การรับรู้ภัยทางไซเบอร์		
	ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์	ประสบการณ์ส่วนตัวเกี่ยวกับภัยไซเบอร์	การฝึกอบรมด้านความปลอดภัยทางไซเบอร์
ความเข้าใจในแนวทางปฏิบัติที่ปลอดภัย	✓	×	×
การปฏิบัติตามมาตรการความปลอดภัย	×	×	×
พฤติกรรมการใช้งานระบบไอทีอย่างปลอดภัย	✓	×	×
การตระหนักด้านความปลอดภัยทางไซเบอร์ด้านภาพรวม	×	×	×

หมายเหตุ เครื่องหมาย ✓ หมายถึง ไม่ต่างกัน, เครื่องหมาย × หมายถึง ต่างกัน

ผลการวิจัย พบว่าการรับรู้ภัยทางไซเบอร์ด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่แตกต่างกันไม่ส่งพลต่อ ความเข้าใจในแนวทางปฏิบัติที่ปลอดภัยและพฤติกรรมการใช้งานระบบไอทีอย่างปลอดภัย ด้านประสบการณ์ส่วนตัวเกี่ยวกับภัยไซเบอร์ที่แตกต่างกันส่งผลการตระหนักด้านความปลอดภัยทางไซเบอร์ทุกด้าน การรับรู้ภัยทางไซเบอร์ด้านการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ส่งผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ในทุกด้าน

ผลการวิจัย

ประชากรผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง อายุ 37-45 ปี มีระดับการศึกษาปริญญาตรี และ มีอาชีพเป็นพนักงานเอกชน

ผู้ตอบแบบสอบถามมีภาพรวมการรับรู้ภัยคุกคามทางไซเบอร์ อยู่ในระดับปานกลาง เมื่อพิจารณาเป็นรายด้านพบว่า ผู้ตอบแบบสอบถามมีการรับรู้ภัยทางไซเบอร์ในระดับปานกลางมี 2 ด้าน เรียงตามลำดับ ได้แก่ ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ และการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ ส่วนการรับรู้ภัยคุกคามทางไซเบอร์ที่อยู่ในระดับน้อย ได้แก่ ประสบการณ์ส่วนตัวเกี่ยวกับภัยไซเบอร์

ผู้ตอบแบบสอบถามมีการตระหนักด้านความปลอดภัยทางไซเบอร์ อยู่ในระดับมาก เมื่อพิจารณาเป็นรายด้านพบว่า ผู้ตอบแบบสอบถามการตระหนักด้านความปลอดภัยทางไซเบอร์ในระดับมากที่สุด 1 ด้าน ได้แก่ ความเข้าใจในแนวทางปฏิบัติที่ปลอดภัย ส่วนการตระหนักด้านความปลอดภัยทางไซเบอร์ที่อยู่ในระดับมากมี 2 ด้าน เรียงตามลำดับ ได้แก่ พฤติกรรมการใช้ระบบไอทีอย่างปลอดภัย และการปฏิบัติตามมาตรการความปลอดภัยทางไซเบอร์

อภิปรายผลการวิจัย

ผลการศึกษาปัจจัยส่วนบุคคลกับการตระหนักด้านความปลอดภัยทางไซเบอร์

ผลการศึกษาปัจจัยส่วนบุคคลแตกต่างกันจะมีการตระหนักด้านความปลอดภัยทางไซเบอร์ที่แตกต่าง พบว่า

1. เพศที่แตกต่างกันไม่มีผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์โดยภาพรวมและรายด้านทั้ง 3 ด้าน ไม่ต่างกันอย่างมีระดับนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับงานวิจัยของ คนัญญา อิ่มใจ (2565) เรื่องพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด ผลการวิจัยพบว่าไม่มีผลต่อพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ อย่างมีระดับนัยสำคัญทางสถิติที่ระดับ 0.05

2. อายุที่แตกต่างกัน จะมีผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ โดยภาพรวมและรายด้านทั้ง 2 ด้าน ได้แก่ การปฏิบัติตามมาตรการความปลอดภัยทางไซเบอร์ และพฤติกรรมการใช้

ระบบไอทีอย่างปลอดภัย ต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับงานวิจัยของ อภิญญา รัตนาตรานุรักษ (2559) เรื่องปัจจัยที่ส่งเสริมให้พนักงานในองค์กรแสดงออกถึงพฤติกรรม ในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัย

3. ระดับการศึกษาที่แตกต่างกัน จะมีผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ โดยภาพรวม และรายด้าน 1 ด้าน ได้แก่ ความเข้าใจในแนวทางปฏิบัติที่ปลอดภัย อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ซึ่งสอดคล้องกับงานวิจัยของ เมธาพร ธรรมศิริ (2565) เรื่องความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากร ในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร

4. อาชีพที่แตกต่างกัน จะมีผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ โดยภาพรวม และรายด้าน 1 ด้าน ได้แก่ การปฏิบัติตามมาตรการความปลอดภัยทางไซเบอร์ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

ผลการศึกษาแนวทางการสร้างการตระหนักด้านความปลอดภัยทางไซเบอร์

ผลการศึกษาแนวทางการสร้างการตระหนักด้านความปลอดภัยทางไซเบอร์ เป็นการนำเสนอตามแนวคิดของผู้วิจัยที่ว่า การตระหนักด้านความปลอดภัยทางไซเบอร์ ประกอบด้วย ความเข้าใจในแนวทางปฏิบัติที่ปลอดภัย ซึ่งเป็นการต่อยอดงานวิจัยของ กิตติศักดิ์ จันทร์นิเวศน์ (2566) เรื่องการวิเคราะห์องค์ประกอบของปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษา ความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่มน้ำมันและก๊าซ ที่แสดงให้เห็นว่า ปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่มน้ำมันและก๊าซ เมื่อนำมาวิจัยกับกลุ่มตัวอย่างในเขตกรุงเทพมหานคร ได้ผลไปในทางเดียวกันกับงานวิจัย ซึ่งสะท้อนให้เห็นว่า ความเข้าใจในแนวทางปฏิบัติที่ปลอดภัยนั้น เป็นส่วนสำคัญที่จะทำให้เกิดการตระหนักความปลอดภัยทางไซเบอร์

และในส่วนสุดท้ายที่ผู้วิจัยมีแนวคิดว่าเป็นองค์ประกอบของการตระหนักด้านความปลอดภัยทางไซเบอร์คือ พฤติกรรมการใช้งานระบบไอทีอย่างปลอดภัย ซึ่งเป็นการต่อยอดงานวิจัยของ คนัญญา อิ่มใจ (2565) เรื่องพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด ที่แสดงให้เห็นว่า กลุ่มเจเนอเรชั่นแซดมีพฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ในระดับมาก เมื่อนำมาขยายเมื่อนำมาวิจัยกับกลุ่มตัวอย่างในเขตกรุงเทพมหานครที่มีอายุหลากหลายมากขึ้น ครบทุกเจเนอเรชั่น จะเห็นว่าอายุที่แตกต่างกันจะมีผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ที่ต่างกัน นั่นหมายถึงทุกกลุ่มอายุที่มีการใช้เทคโนโลยีในชีวิตประจำวัน ย่อมมพฤติกรรมการปกป้องตนเองจากภัยคุกคามทางไซเบอร์ ทำให้เกิดการตระหนักความปลอดภัยทางไซเบอร์

ทำให้งานวิจัยนี้ แสดงให้เห็นว่าการตระหนักด้านความปลอดภัยทางไซเบอร์ เป็นสิ่งสำคัญที่จะทำให้ประชาชนมีการรับรู้ทางไซเบอร์ให้ครอบคลุมทุกด้าน ทั้งทางด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่ทำให้มีความรู้ที่เพิ่มขึ้น การมีประสบการณ์ส่วนตัวเกี่ยวกับภัยไซเบอร์ ที่จะทำให้มีความระมัดระวังในการใช้เทคโนโลยี และการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ ที่เพิ่มพูนความรู้ด้าน

ความปลอดภัย เมื่อทั้ง 3 ส่วนนี้ประกอบกัน จะทำให้ประชาชนมีการตะหนักด้านความปลอดภัยทางไซเบอร์มากขึ้น

ข้อเสนอแนะ

ข้อเสนอแนะในการนำไปใช้

การวิจัยเรื่องการรับรู้ภัยทางไซเบอร์ส่งผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ของประชากรในจังหวัดกรุงเทพมหานคร ทำให้ทราบถึงปัจจัยการรับรู้ทางไซเบอร์ที่มีผลต่อการตระหนักด้านความปลอดภัยทางไซเบอร์ และเป็นสำรวจจากประชากรในจังหวัดกรุงเทพมหานคร ทำให้เห็นถึงภาพใหญ่ของคนทั้งจังหวัด องค์กร หรือหน่วยงาน หรือเขตท้องถิ่นต่างๆ สามารถนำผลการวิจัยไปประยุกต์ใช้ โดยการให้จัดโครงการเพื่อให้ความรู้ จะได้มีการรับรู้ทางไซเบอร์เพิ่มขึ้น เพราะว่าไม่ว่าจะจัดโครงการให้ความรู้ในระดับใดก็ตาม การตระหนักด้านปลอดภัยทางไซเบอร์ที่เพิ่มมากขึ้น จะทำให้ไม่ถูกหลอก และเป็นเหยื่อของมิจฉาชีพที่แฝงตัวเข้ามาทางช่องทางต่างๆ จากความรู้ที่เพิ่มมากขึ้น ยังสมารถช่วยหน่วยงานราชการ สังเกต สอดส่อง บุคคลที่อาจเป็นมิจฉาชีพ เพื่อเข้าสู่กระบวนการลงโทษต่อไป

ข้อเสนอแนะเพื่อการศึกษาครั้งถัดไป

1. ควรศึกษาวิจัยเกี่ยวกับการตระหนักความปลอดภัยทางไซเบอร์ไปยังกลุ่มตัวอย่างในแบบอื่นๆ เช่น ในจังหวัดอื่น ภูมิภาคอื่น หรือเฉพาะบางหน่วยงาน หรือบางองค์กร เพื่อนำผลมาศึกษาใช้ในการวางแผน ต่อยอดการให้ความรู้กลุ่มต่างๆ
2. ควรศึกษาวิจัยเกี่ยวกับการตระหนักความปลอดภัยทางไซเบอร์ ที่มาจากปัจจัยอื่นๆ หรือเจาะจงรูปแบบเทคนิค หรือธุรกิจเฉพาะ เช่น เฉพาะกลุ่มที่ใช้ธุรกรรมทางการเงินออนไลน์ผ่านโทรศัพท์ (Mobile Banking) บุคคลที่มีความจำเป็นต้องมีการเก็บข้อมูลบน Cloud และการค้าขายผ่านช่องทางออนไลน์ เป็นต้น เพื่อให้เกิดความครอบคลุม และมีการชี้เฉพาะกลุ่มเพื่อได้ศึกษาปัญหา และสามารถให้ความรู้ หรือปรับแก้ปัญหาเฉพาะจุด ให้เกิดการตระหนักในระยะยาวได้

เอกสารอ้างอิง

กิตติศักดิ์ จันทร์นิเวศน์ .(2566). การวิเคราะห์องค์ประกอบของปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษา ความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่มน้ำมันและก๊าซ

คณัญญา อิ่มอำไพ .(2565). พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด

เมธาพร ธรรมศิริ .(2565). ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร

อภิญญา รัตนาตรานุรักษ์ .(2559). ปัจจัยที่ส่งเสริมให้พนักงานในองค์กรแสดงออกถึงพฤติกรรม ในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัย ทางด้านสารสนเทศ

Bloom (1971, p. 271 อ้างถึงใน สุพัตรา ถนอมวงค์, 2551, น.10)

เรียนรู้ “การใช้คอมพิวเตอร์อย่างปลอดภัย” https://www.boonjit.ac.th/security/internetsecurity3.pdf

รู้เข้าใจและตระหนัก “อาชญากรรมทางไซเบอร์” (Cybercrime) ป้องกันภัยคุกคามใกล้ตัว https://www.chula.ac.th/news/138291/

ราชกิจจานุเบกษา, ‘พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562’ <http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF> สืบค้นเมื่อ 27 พฤษภาคม 2562.

“อาชญากรรมทางไซเบอร์ (Cyber Crime) ภัยคุกคามตัวร้ายในโลกยุคดิจิทัล” https://www.bangkokbankinnohub.com/th/what-is-cyber-crime/