ความสัมพันธ์ระหว่างการตระหนักถึงความมั่นคงทางสารสนเทศกับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

พิชญ์สินี โกศลานันท์

คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

***Correspondence:** pichsinee-kos64@tbs.tu.ac.th

วันที่รับบทความ: วันแก้ไขบทความ: วันตอบรับบทความ:

บทคัดย่อ

ปัจจุบันภัยไซเบอร์ขยายวงเพิ่มขึ้นหลายเท่าตัว โดยเฉพาะภัยคุกคามในภาคการเงิน ซึ่งก่อให้เกิดความเดือดร้อนให้แก่ผู้ที่ทำธุรกรรมทางการเงินจำนวนมาก งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาความสัมพันธ์ระหว่างการตระหนักถึงความมั่นคงทางสารสนเทศกับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม โดยประยุกต์แนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม แนวคิดเกี่ยวกับประสิทธิภาพของตนเอง ทัศนคติการรักษาความมั่นคงปลอดภัยทางสารสนเทศ บรรทัดฐานจิตวิสัย การรับรู้การควบคุมพฤติกรรม และงานวิจัยที่เกี่ยวข้องในอดีตมาเป็นแนวทางในการสร้างกรอบแนวคิดการวิจัย งานวิจัยนี้ศึกษากับกลุ่มตัวอย่างซึ่งเป็นบุคคลทั่วไปที่เคยประสบภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม เช่น การได้รับโทรศัพท์ การได้รับข้อความสั้น (SMS) เข้ามาหลอกลวง หรือการหลอกลวงผ่านทางอินเทอร์เน็ตผ่านการเข้าใช้งาน ไม่ว่าจะเป็นช่องทาง เว็บไซต์ อีเมล และแชท อย่างน้อย 1 ครั้ง ภายในระยะเวลา 12 เดือน และมีประสบการณ์การทำงานมากกว่า 1 ปี โดยผู้วิจัยได้ส่งแบบสอบถามผ่านทางผ่านสื่อสังคมออนไลน์และได้ข้อมูลผู้ตอบแบบสอบถามจำนวนทั้งหมด 227 ราย หลังจากทำการตรวจสอบความถูกต้องก่อนนำไปวิเคราะห์ผลทางสถิติ พบว่ามีจำนวนผู้ตอบแบบสอบถามคงเหลือที่ 202 ราย และนำข้อมูลที่ได้มาประมวลด้วยโปรแกรมสำเร็จรูปทางสถิติ เพื่อวิเคราะห์ความสัมพันธ์กับปัจจัยต่าง ๆ จากทฤษฎีและกรอบแนวคิดการวิจัยที่กล่าวมาข้างต้น

ผลการวิจัยพบว่า การตระหนักด้านความมั่นคงทางสารสนเทศมีความสัมพันธ์กับประสิทธิภาพของตนเอง ทัศนคติในการรักษาความมั่นคงทางสารสนเทศ บรรทัดฐานจิตวิสัยและการรับรู้การควบคุมพฤติกรรม รวมถึงผลการวิเคราะห์ทางสถิติระหว่าง ทัศนคติในการรักษาความมั่นคงทางสารสนเทศ และการรับรู้การควบคุมพฤติกรรมมีความสัมพันธ์กับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคมอย่างมีนัยสำคัญ ผู้บริหารฝ่ายทรัพยากรมนุษย์สามารถนำผลวิจัยนี้ไปประยุกต์ใช้ในการพัฒนาโปรแกรมการอบรมให้ความรู้ความเข้าใจกับพนักงาน หรือกำหนดนโยบายและขั้นตอนการปฏิบัติงานที่ชัดเจนเพื่อป้องกันภัยคุกคามประเภทวิศวกรรมสังคม และหน่วยงานภาครัฐสามารถนำผลวิจัยนี้ไปใช้ในการสร้างการตระหนักรู้ให้แก่บุคคลทั่วไปในสังคมที่มีโอกาสพบกับภัยคุกคามทางไซเบอร์ฯ ได้

คำสำคัญ: การตระหนักถึงความมั่นคงทางสารสนเทศ; ประสิทธิภาพของตนเอง; ทัศนคติในการรักษาความมั่นคงทางสารสนเทศ; บรรทัดฐานจิตวิสัย; การรับรู้การควบคุมพฤติกรรม; ความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

The Relationship Between Information Security Awareness and Intention to Resist Social Engineering Threats

Pichsinee Kosalanun*

Thammasat Business School, Thammasat University

***Correspondence:** pichsinee-kos64@tbs.tu.ac.th

Abstract

Cyber threats are currently escalating significantly, causing widespread harm to those conducting financial transactions. This study aims to investigate the relationship between information security awareness and the intention to combat cyber threats. Social engineering is a quantitative study. And apply the concepts of network threats, social engineering types, concepts of Self Efficacy, concepts of Attitude, concepts of Information Security Awareness. Concepts of subjective Norm, concepts of Perceived Behavior Control and related research are guidelines for establishing a research framework. By studying a sample of individuals who have encountered social engineering network threats, such as answering and receiving calls. SMS fraud or internet fraud, whether through channels, websites, emails, or chats, at least once within 12 months, at least 1 year of social media work experience 227 respondents conducted validation before analyzing the statistical results, and the remaining number of respondents was 202. And use ready-made statistical programs to process data to analyze the relationship with various factors. Based on the above research theory and framework.

The results indicate that information security awareness is related to its own performance and attitude towards maintaining information security. Statistical analysis results between psychological norms and behavioral control awareness, including information security attitudes. Spiritual norms the awareness of behavior control is closely related to the intention to resist social engineering network threats. Human resource management personnel can apply the research findings to develop training plans, educate employees, or formulate policies and clear operational procedures to prevent social engineering threats. This includes raising awareness among the public who have the opportunity to encounter cyber threats in society.

Keywords: Information Security Awareness; Self Efficacy; Attitude; Subjective Norm; Perceived Behavior Control; Intention to resist social engineering

1. บทนำ

1.1 ความสำคัญและที่มาของปัญหาการวิจัย

ในปัจจุบันเทคโนโลยีได้เข้ามามีบทบาทอย่างมากในชีวิตของมนุษย์ ไม่ว่าจะเป็นการทำงาน เรื่องส่วนตัว หรือเรื่องอื่น ๆ จากรายงานสถิติและพฤติกรรมผู้ใช้งานอินเทอร์เน็ต (Internet) ทั่วโลกประจำไตรมาสหนึ่งของปี 2020 ของ Kemp (2020) พบว่าจำนวนประชากรทั้งโลกอยู่ที่ 7,750 ล้านคนและเป็นคนที่อยู่ในเมืองร้อยละ 55 มีคนใช้อินเทอร์เน็ต 4,540 ล้านคน คิดเป็นร้อยละ 59 ของจำนวนประชากรทั้งหมด และมีบัญชีโซเชียลมีเดีย (Social Media) 3,800 ล้านบัญชี คิดเป็นร้อยละ 49 ของประชากรทั้งหมด มีคนใช้อินเทอร์เน็ต มากขึ้นร้อยละ 7 และโซเชียลมีเดีย มากขึ้นร้อยละ 9.2 จากปีที่ผ่านมา อย่างไรก็ตามแม้จะมีมาตรการรักษาความมั่นคงที่เข้มงวด แต่การโจมตีทางอินเทอร์เน็ตจำนวนมากยังคงโจมตีโดยใช้ประโยชน์จากช่องโหว่ของการออกแบบแอปพลิเคชัน การหลอกลวง หรือวิธีการทางเทคนิคขั้นสูง ทำให้เกิดความกังวลอย่างมากต่อความมั่นคงทางสารสนเทศและความเป็นส่วนตัวของผู้ใช้ (Abroshan et al., 2021) ในบรรดาวิธีการโจมตีเหล่านี้เป็นการหลอกลวง ก่อนที่จะมีคอมพิวเตอร์และอินเทอร์เน็ต ซึ่งการหลอกลวงเหล่านี้จัดเป็นการโจมตีประเภทวิศวกรรมสังคม (Social Engineering) การโจมตีเหล่านี้ใช้ประโยชน์จากจุดอ่อนในการปฏิสัมพันธ์ของมนุษย์และโครงสร้างเชิงพฤติกรรมและวัฒนธรรม (Indrajit, 2017; Wang et al., 2021) โดยส่วนใหญ่มักใช้การโน้มน้าวใจทางจิตวิทยา เพื่อให้ได้มาซึ่งข้อมูลที่สำคัญ เอกสาร และข้อมูลที่ผู้ไม่หวังดีไม่ควรเข้าถึง (Washo, 2021) การโจมตีทางวิศวกรรมสังคมมักมีรูปแบบหรือวิธีการ เช่น การได้รับโทรศัพท์ การได้รับข้อความสั้น (SMS) เข้ามาหลอกลวงว่าท่านคือผู้โชคดีที่ได้รับรางวัล และส่งช่องทางการเข้าถึงข้อมูลสำคัญหรือข้อมูลส่วนตัวของผู้ใช้งาน เพื่อให้ผู้ใช้งานหลงเชื่อและปฏิบัติตามคำแนะนำ จากนั้นจะถูกขโมยข้อมูลและนำไปสู่ความเสียหายทางทรัพย์สิน หรือการหลอกลวงผ่านทางอินเทอร์เน็ตผ่านการเข้าใช้งาน ไม่ว่าจะเป็นช่องทาง เว็บไซต์ อีเมล และแชท ซึ่งเป้าหมายก็ไม่ทราบว่ากำลังถูกโจมตีหรือได้รับอิทธิพลจากผู้กระทำความผิด เนื่องจากลักษณะเฉพาะของการโจมตีแบบพื้นฐานทางวิศวกรรมสังคมที่คลุมเครือ

ปัจจุบันภัยไซเบอร์ขยายวงเพิ่มขึ้นหลายเท่าตัว โดยเฉพาะภัยคุกคามในภาคการเงิน ซึ่งก่อให้เกิดความเดือดร้อนให้แก่ผู้ที่ทำธุรกรรมทางการเงินจำนวนมาก โดยเฉพาะจากการถูกโจรกรรมข้อมูล (Data Theft) นอกจากนี้กลุ่มมิจฉาชีพทำการสุ่มข้อมูลบัตรและนำไปสวมรอยทำธุรกรรมผ่านร้านค้าออนไลน์ต่างประเทศ โดยมีบัญชีบัตรเดบิตและบัตรเครดิตที่ถูกโจรกรรมรวม 10,700 บัตร เป็นมูลค่าความเสียหาย 131 ล้านบาท (ศูนย์วิจัยกสิกรไทย, 2564) รวมถึงการระบาดครั้งใหญ่ของไวรัสโควิด-19 ได้ทำให้อาชญากรไซเบอร์โอกาสในการโจมตีมากขึ้นกว่าเดิม เนื่องจากการล็อคดาวน์ (lockdown) และมาตรการรักษาระยะห่าง (social distancing) ของทั่วโลก ทำให้หลายบริษัทต้องมีการเปลี่ยนแปลงระบบการทำงานจากที่บ้าน แล้วเข้ามาทำงานผ่านออนไลน์ ซึ่งเป็นช่องทางที่หลายบริษัทอ่อนไหวต่อการถูกคุกคามทางไซเบอร์ เพราะมันมีช่องโหว่ของการเข้าถึงข้อมูลได้อย่างง่ายมากยิ่งขึ้นหากระบบรักษาความปลอดภัยของบริษัทไม่แข็งแรงพอที่จะป้องกันภัยคุกคามทางไซเบอร์

เนื่องจากผู้คนอาศัยอยู่บ้านและทำงานจากที่บ้าน (working from home) มากขึ้น การทำงานจากที่บ้านหรือนอกสถานที่ที่ไม่ใช่ภายในองค์กรมักใช้อุปกรณ์ส่วนตัวในการทำงาน และ ล็อคอิน (log in) เข้าสู่ระบบในเว็บต่าง ๆ ผ่านเน็ตเวิร์ก (networks) ภายในบ้านหรือพื้นที่สาธารณะ โดยที่ไม่ได้รับการรักษาความมั่นคงทางไซเบอร์อย่างเต็มที่ซึ่งวิถีชีวิตของผู้คนที่เชื่อมต่อกันง่ายมากขึ้นนั้น ทำให้มิจฉาชีพมุ่งเน้นที่ข้อมูลส่วนบุคคล รายงาน Global Digital Trust Insights 2021 ของ PwC พบว่าร้อยละ 96 ขององค์กรทั่วโลก ได้หันมาปรับกลยุทธ์ด้านความมั่งคงปลอดภัยทางไซเบอร์ (Cybersecurity strategy) และลงทุนในโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ (IT infrastructure) ในช่วงการแพร่ระบาดของไวรัสโควิด-19 เพื่อรับมือกับความเสี่ยงที่เพิ่มขึ้นตามการเติบโตของการทำงานในแบบดิจิทัล

นอกจากนี้การใช้ชีวิตประจำวันของผู้คนในปัจจุบันล้วนแต่สื่อสารหรือดำเนินกิจกรรมผ่านช่องทางออนไลน์ ซึ่งมิจฉาชีพเองก็เริ่มใช้ช่องทางดังกล่าวเพื่อแสวงหาผลประโยชน์เช่นเดียวกัน โดยอาศัยข้อมูลจากแชทหรือโพสต์ต่าง ๆ เป็นตัวช่วยในการสวมรอยหรือปลอมแปลงข้อมูลเพื่อหลอกลวง ประชาชน ยกตัวอย่างเช่น การส่งข้อความแชทเพื่อ

หลอกให้โอนเงิน หรือการปลอมแปลงสลิปโอนเงินในการสั่งซื้อสินค้าออนไลน์ ซึ่งถ้าหากเราไม่ระวังอาจทำให้สูญเสียเงินหรือเสียผลประโยชน์ทางธุรกิจได้ การป้องกันภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคมนั้นสามารถใช้ เทคโนโลยีหรือ Security Control เข้ามาช่วย เช่น Reputation Filtering, URL Filtering, Anti-Malware, Email Security (Anti-Spam หรือ Email Gateway), และอื่น ๆ ในองค์กรขนาดใหญ่ ที่ระบบทางสารสนเทศมีความซับซ้อนมาก อาจต้องใช้เทคโนโลยีหลาย ๆ ตัวที่กล่าวมาเข้ามาช่วยในการป้องกัน โดยออกแบบในลักษณะ Multi-Layer Security หรือ Defense in Depth แต่ในองค์กรขนาดเล็กความซับซ้อนของระบบสารสนเทศน้อยกว่า อาจไม่ต้องใช้ Security Control มากนักในการป้องกัน นอกจาก Security Control ที่จำเป็นต้องมีแล้ว สิ่งสำคัญที่ขาดไม่ได้ คือ Awareness Training ที่จะต้องให้ความรู้ในระดับที่เหมาะสมกับผู้ใช้งาน เนื่องจาก ผู้ใช้งานบางกลุ่มไม่จำเป็นต้องรู้ถึงรายละเอียดที่ลึกมากจนเกินไป ซึ่งจะทำให้เกิดความสับสน หรือไม่เข้าใจในสิ่งที่พยายามสื่อให้ผู้ใช้งานรับรู้ เนื่องจากภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคมมีเหยื่อเป็นบุคคล

การให้ความรู้ความเข้าใจในเรื่องภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคมจึงเป็นสิ่งสำคัญ และสามารถระวังตนจากผู้ไม่หวังดีได้ โดยอาศัยการเป็นคนช่างสงสัย และมีสติ เมื่อสื่อสารกับคนแปลกหน้าไม่ว่าจะเป็นทางโทรศัพท์ ทางอีเมล หรือพูดคุยกันซึ่งหน้า ที่ต้องการข้อมูลส่วนบุคคล หรือข้อมูลภายในขององค์กร ซึ่งไม่ว่าคนแปลกหน้านั้นจะแสดงตนว่าเป็นบุคคลจากองค์กรใดก็ตาม ผู้มีส่วนเกี่ยวข้องควรมีการตรวจสอบกับองค์กรนั้นโดยตรงก่อนเสมอ และผู้ใช้งานควรติดตามข่าวสารสม่ำเสมอ ไม่ว่าจะเป็นด้านเทคโนโลยีหรือข่าวสารทั่วไป เพื่อให้ทราบถึงรูปแบบการโจมตีของมิจฉาชีพที่อาจจะเกิดขึ้นกับตน รวมทั้งวิธีการป้องกันจากการโจมตีในรูปแบบต่าง ๆ ทำให้สามารถรับมือและหลีกเลี่ยงภัยคุกคามที่จะเกิดขึ้นได้และสิ่งหนึ่งที่กิจการไม่ว่าขนาดใหญ่หรือเล็กจะนำมาใช้เพื่อบรรเทาความเสียหายจากภัยนี้ได้โดยไม่มุ่งเน้นเพียงการแก้ปัญหาที่อาศัยเทคโนโลยี นั่นคือการสร้างการตระหนักถึงความมั่นคงทางสารสนเทศงานวิจัยฉบับนี้จึงมุ่งที่จะศึกษาปัจจัยที่ส่งผลต่อความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคมของผู้ใช้งาน เพื่อทราบถึงแนวทางในการสร้างความตระหนักและสามารถกำหนดแนวนโยบายและขั้นตอนการปฏิบัติงานที่ชัดเจนเพื่อป้องกันภัยคุกคามประเภทวิศวกรรมสังคม (Social Engineering Threat) โดยผู้วิจัยได้กำหนดคำถามวิจัยไว้ดังนี้

“ปัจจัยใดบ้างที่มีความสัมพันธ์กับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม”

2. ทฤษฎีและงานวิจัยในอดีตที่เกี่ยวข้อง

2.1 วิศวกรรมสังคม (Social Engineering)

วิศวกรรมสังคมเป็นการหลอกลวงที่ใช้ประโยชน์จากจุดอ่อนของมนุษย์โดยจัดการผู้คนให้ดำเนินการที่เป็นประโยชน์ต่อผู้โจมตี มักใช้การโน้มน้าวใจทางจิตวิทยาซึ่งไม่มีรูปแบบการโจมตีหรือวิธีการโจมตีที่ชัดเจน เพื่อให้ได้มาซึ่งข้อมูลที่สำคัญ เอกสาร และข้อมูลที่ผู้ไม่หวังดีไม่ควรเข้าถึง วิศวกรรมสังคมในปัจจุบันเป็นภัยคุกคามด้านความมั่นคงที่สำคัญต่อองค์กร และมักใช้ช่องทางโซเชียลมีเดีย เช่น เฟซบุ๊ก อีเมล (ฟิชชิง) หรือโทรศัพท์ (การฉ้อโกงทางโทรศัพท์) เพื่อต่อสู้กับวิศวกรรมสังคม สิ่งสำคัญคือต้องเข้าใจว่าทำไมพนักงานบางคนจึงต่อต้านการโจมตีทางวิศวกรรมสังคมได้ดีกว่าคนอื่น ๆ วรรณกรรมเชิงทฤษฎีก่อนหน้านี้ได้เสนอสาเหตุที่ทำให้ปัจเจกบุคคลตกเป็นเหยื่อของวิศวกรรมสังคม ตัวอย่างเช่น พนักงานที่แสดงความไว้วางใจมากกว่ามักจะถูกหลอก ผู้กระทำผิดสามารถใช้สิ่งนี้เพื่อประโยชน์ของตนโดยแอบอ้างเป็นผู้ใช้ที่สำคัญ เช่น ผู้จัดการอาวุโสหรือสมาชิกทีมบริการไอทีเพื่อให้ได้รับความไว้วางใจจากเหยื่อ การใช้การเอ่ยชื่อ “เพื่อนร่วมงานทั่วไป” ยังสามารถนำมาใช้เพื่อให้ได้รับความไว้วางใจจากเหยื่อ และทำให้เหยื่อปฏิบัติตามคำขอที่ “เป็นอันตราย” ผู้กระทำผิดสามารถพยายามสร้างความสัมพันธ์ระหว่างบุคคลกับเหยื่อเพื่อสร้างความรู้สึกผูกพัน การพยายามทำให้เหยื่อตอบสนองต่อข้อเสนอที่ที่น่าสนใจนั้น เชื่อว่าจะทำให้เหยื่อปฏิบัติตามคำขอ “ที่เป็นอันตราย” เนื่องจากโดยทั่วไปแล้วผู้คนมักกระตือรือร้นที่จะซื้อสิ่งที่พิเศษและเสนอให้ในช่วงเวลาสั้นๆ (Flores & Ekstedt, 2016)

2.2 การตระหนักด้านความมั่นคงทางสารสนเทศ (Information Security Awareness)

การตระหนักด้านความมั่นคงทางสารสนเทศ หมายถึง การรับรู้ของแต่ละบุคคลเกี่ยวกับความรู้ทั่วไปเกี่ยวกับมาตรการการควบคุมภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม และการรับรู้ด้านนโยบายหรือแนวทางของภาครัฐและภาคเอกชนหรือหน่วยงานต่างๆ เกี่ยวกับมาตรการดังกล่าวข้างต้น (Flores & Ekstedt, 2016) จากการศึกษาว่าความตระหนักของพนักงานเกี่ยวกับนโยบายด้านความมั่นคงมีความเกี่ยวข้องกับความเชื่อที่รับรู้ของพนักงานเกี่ยวกับความง่าย สะดวก และง่ายดายในการปกป้อง ระบบข้อมูลจากภัยคุกคามด้านความปลอดภัย ซึ่งการรับรู้ถึงความมั่นคงของข้อมูลเป็นส่วนสำคัญของโปรแกรมการจัดการความมั่นคงของข้อมูลในทางปฏิบัติและมีประสิทธิภาพ ช่วยป้องกันการใช้คอมพิวเตอร์ในทางที่ผิด (Koohang et al., 2020) ซึ่งการรับรู้ถึงความมั่นคงของข้อมูลสามารถกำหนดรูปแบบได้จากความสนใจและประสบการณ์ของพนักงานเอง หรือโดยการแทรกแซงที่ดำเนินการโดยกลุ่มการจัดการความมั่นคงของข้อมูลขององค์กร รวมถึงสภาพแวดล้อมที่สนับสนุนซึ่งวัฒนธรรมการรักษาความปลอดภัยข้อมูลสร้างขึ้นมีความเกี่ยวข้องโดยตรงกับการรับรู้ถึงความปลอดภัยของข้อมูล ทัศนคติ และความเชื่อเชิงบรรทัดฐานเกี่ยวกับภัยคุกคามความมั่นคงของข้อมูลของพนักงาน (Flores & Ekstedt, 2016) หากองค์กรพยายามที่จะส่งเสริมวัฒนธรรมย่อยของการรักษาความมั่นคงข้อมูล กิจกรรมทั้งหมดจะต้องดำเนินการในลักษณะที่สอดคล้องกับแนวปฏิบัติด้านความมั่นคงของข้อมูลที่ดี ดังนั้นการมีความรู้เพียงพอเกี่ยวกับความมั่นคงของข้อมูลจึงเป็นข้อกำหนดเบื้องต้นในการดำเนินกิจกรรมตามปกติในลักษณะที่มั่นคง วัฒนธรรมการรักษาความมั่นคงของข้อมูลเป็นวัฒนธรรมย่อยขององค์กรที่สนับสนุนกิจกรรมทั้งหมดในลักษณะที่ความมั่นคงของข้อมูลกลายเป็นลักษณะธรรมชาติในกิจกรรมประจำวันของพนักงานทุกคน โดยการปรับปรุงพฤติกรรมการรักษาความมั่นคงข้อมูลของพนักงาน เป็นวัฒนธรรมที่ส่งเสริมพฤติกรรมด้านความมั่นคงและมีส่วนทำให้บรรลุเป้าหมายโดยรวมขององค์กร (Nasir et al., 2019)

2.3 ประสิทธิภาพของตนเอง (Self-Efficacy)

ประสิทธิภาพของตนเอง หมายถึง ระดับความรู้ ทักษะ หรือความสามารถส่วนบุคคลเกี่ยวกับภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม (Flores & Ekstedt, 2016) ตามทฤษฎีของพฤติกรรมที่วางแผนไว้ ความเชื่อในการรับรู้ความสามารถของตนเองจะกลั่นกรองผลกระทบของความตั้งใจต่อพฤติกรรมในทางบวก (Flores & Ekstedt, 2016) การที่คนอเมริกันพยายามเพื่อให้ได้ผลลัพธ์ที่รวดเร็วภายในสถานที่ทำงาน ประกอบกับความจริงที่ว่าคนอเมริกันมีความคิดที่ “ทำได้” อาจทำให้พวกเขาเชื่ออย่างแรงกล้าว่าพวกเขาสามารถทำนายพฤติกรรมของตนได้อย่างแม่นยำตามการรับรู้ของแต่ละคน ในขณะที่บุคคลเชิงปฏิบัติมากขึ้นตระหนักถึงข้อจำกัดของตนและคาดการณ์พฤติกรรมของพวกเขาแตกต่างกัน (Flores et al., 2015)

2.4 ทัศนคติการรักษาความมั่นคงสารสนเทศ (Attitude)

ทัศนคติการรักษาความมั่นคงทางสารสนเทศ หมายถึง ระดับที่บุคคลมีความรู้สึกเชิงบวกเกี่ยวกับมาตรการการควบคุมภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม (Samhan, 2017) การประเมิน (ทัศนคติ) เชิงบวกของผู้ใช้เกี่ยวกับคอมพิวเตอร์ของตนที่ติดมัลแวร์ จะเพิ่มความตั้งใจที่จะใช้โปรแกรมป้องกันมัลแวร์ ดังนั้น ทันทีที่พวกเขาพิจารณาว่าซอฟต์แวร์ป้องกันมัลแวร์มีประสิทธิภาพในการเพิ่มความมั่นคงและความเป็นส่วนตัวของระบบ (Vafaei-Zadeh et al., 2019) แสดงให้เห็นว่าการตระหนักด้านความมั่นคงของข้อมูลที่เพิ่มขึ้นส่งผลดีต่อทัศนคติของผู้ใช้ในการปฏิบัติตามข้อกำหนดด้านความมั่นคงของข้อมูล (Grassegger & Nedbal, 2021) และยังเป็นปัจจัยหลักในการสร้างความตั้งใจเชิงพฤติกรรมของผู้ใช้ในการใช้เทคโนโลยีการป้องกัน (Dinev & Hu, 2007)

2.5 บรรทัดฐานจิตวิสัย (Subjective Norm)

บรรทัดฐานจิตวิสัย หมายถึง ความเชื่อของบุคคลว่าคนอื่นๆ ที่มีความสำคัญสำหรับเขาต้องการให้เขาหลีกเลี่ยงผลเสียหายจากภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม (Dinev & Hu, 2007) ยิ่งระดับการรับรู้ในหมู่สมาชิกของกลุ่มทางสังคมสูงขึ้นเท่าใด บรรทัดฐานจิตวิสัยของกลุ่มเกี่ยวกับการใช้เทคโนโลยีการป้องกันก็จะยิ่งแข็งแกร่งขึ้นเท่านั้น

(Dinev & Hu, 2007) กล่าวอีกนัยหนึ่ง บุคคลที่มีความสำคัญต่อประชาชนส่งผลกระทบต่อบุคคลหรือสังคมในการดำเนินการ (Vafaei-Zadeh et al., 2019)

2.6 การรับรู้การควบคุมพฤติกรรม (Perceived behavior control)

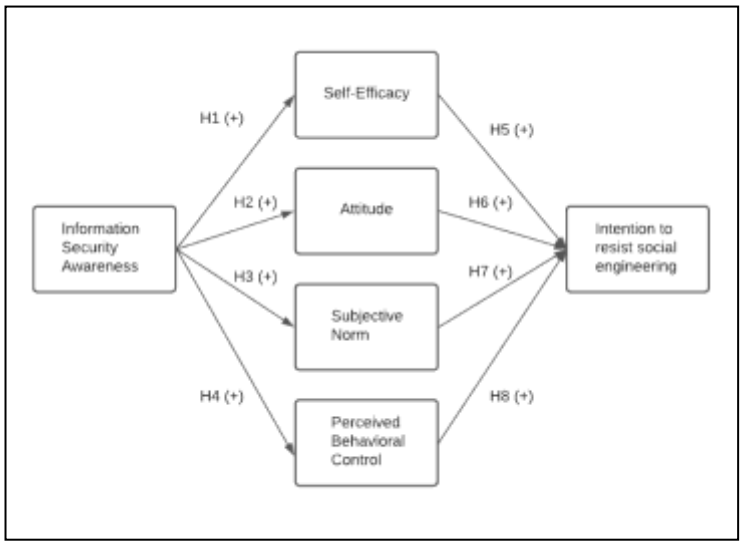
การรับรู้การควบคุมพฤติกรรม หมายถึง ระดับความมั่นใจในความสามารถการกระทำของตนเองและการมีทรัพยากร (เช่น เงิน และเวลา) เพื่อใช้ในการควบคุมภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม (Vafaei-Zadeh et al., 2018) สำหรับปัจจัยที่รับรู้การควบคุมพฤติกรรม เป็นสิ่งสำคัญที่พนักงานจะต้องตระหนักถึงภัยคุกคามต่อความปลอดภัยของข้อมูล เพื่อให้สามารถระบุเทคนิควิศวกรรมสังคมทั่วไปและตอบสนองต่อมัน การรับรู้ถึงการควบคุมพฤติกรรมในที่นี้ถูกมองว่าเป็นขอบเขตของการควบคุมที่บุคคลนั้นคิดว่าตนมีต่อการต่อต้านเทคนิควิศวกรรมสังคมและการตระหนักด้านความมั่นคงของข้อมูล ยังเป็นปัจจัยสำคัญในการเพิ่มการรับรู้การควบคุมพฤติกรรมของพนักงาน (Grassegger & Nedbal, 2021) กล่าวคือเป็นการรับรู้ถึงความง่ายหรือความยากลำบากในการแสดงพฤติกรรมและความรู้สึกส่วนตัวในการควบคุมพฤติกรรม การรับรู้ความสามารถของตนเองหมายถึงการตัดสินของแต่ละคนเกี่ยวกับทักษะและความสามารถในการปฏิบัติตามพฤติกรรม ความสามารถในการควบคุมหมายถึง การตัดสินใจของแต่ละบุคคลเกี่ยวกับความพร้อมของทรัพยากรและโอกาสในการดำเนินการ (Dinev & Hu, 2007)

2.7 ความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม (Intention to resist social engineering)

ความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม หมายถึง การคาดการณ์ หรือการวางแผนที่จะปฏิเสธ ยับยั้ง หยุดยั้ง การกระทำของบุคคลที่ไม่รู้จักหรือบุคคลที่ไม่ได้รับอนุญาต อันก่อให้เกิดความเสียหายต่อข้อมูลส่วนตัวหรือข้อมูลที่สำคัญ (Flores & Ekstedt, 2016) การศึกษาถึงการรับรู้ของพนักงานแต่ละคนเกี่ยวกับความรู้ทั่วไปเกี่ยวกับความมั่นคงของข้อมูลและการรับรู้ถึงนโยบายการรักษาความมั่นคงของข้อมูลมีความสัมพันธ์ต่อการรับรู้ประสิทธิภาพตนเองของพนักงานเกี่ยวกับทักษะ ความรู้ หรือความสามารถส่วนบุคคลเกี่ยวกับการต่อต้านวิศวกรรมสังคม (Flores & Ekstedt, 2016) วิศวกรรมสังคมเป็นรูปแบบหนึ่งของการโจมตีที่บุคคลถูกจัดการโดยเจตนาเพื่อเปิดเผยข้อมูลที่เป็นความลับหรือเพื่อดำเนินการตามที่ผู้โจมตีต้องการซึ่งคุกคามความมั่นคงปลอดภัยของบุคคลหรือบริษัท จึงจำเป็นเพื่อส่งเสริมความตระหนักในความปลอดภัยของข้อมูลของพนักงาน (Grassegger & Nedbal, 2021)

3. กรอบแนวคิดการวิจัยและสมมติฐานการวิจัย

ผู้วิจัยได้ทำการทบทวนวรรณกรรมที่เกี่ยวข้อง รวมทั้งทฤษฎีและแนวคิดที่เกี่ยวข้องพบว่าปัจจัยการตระหนักด้านความมั่นคงทางสารสนเทศมีความสัมพันธ์ทางอ้อมหรือมีค่าความสัมพันธ์ทางตรงกับปัจจัยความตั้งใจในการต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคมน้อยมากและจากการทบทวนวรรณกรรมที่เกี่ยวข้องพบว่าปัจจัยการตระหนักด้านความมั่นคงทางสารสนเทศควรมีปัจจัยที่นำส่งไปยังปัจจัยความตั้งใจในการต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม ซึ่งจากการทบทวนวรรณกรรมที่เกี่ยวข้องพบว่ามีปัจจัยที่เกี่ยวข้อง ได้แก่ ปัจจัยด้านประสิทธิภาพของตนเอง ปัจจัยด้านทัศนคติการรักษาความมั่นคงทางสารสนเทศ ปัจจัยบรรทัดฐานจิตวิสัย และปัจจัยด้านการรับรู้การควบคุมพฤติกรรม ในการวิจัยครั้งนี้จึงศึกษาปัจจัยที่นำส่งปัจจัยการตระหนักด้านความมั่นคงทางสารสนเทศไปยังปัจจัยความตั้งใจในการต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม



ภาพที่ 1 กรอบแนวคิดของความสัมพันธ์ระหว่างการตระหนักถึงความมั่นคงทางสารสนเทศ (Information Security Awareness) กับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม (Intention to resist social engineering)

3.1 สมมติฐานวิจัย

3.1.1 ความสัมพันธ์ระหว่างการตระหนักด้านความมั่นคงทางสารสนเทศกับประสิทธิภาพของตนเอง

เมื่อพนักงานรับรู้ถึงภัยคุกคามทางไซเบอร์ฯ และความรับรู้เกี่ยวกับนโยบายการป้องกันภัยดังกล่าวขององค์กร ทำให้เขาเหล่านั้นมีทักษะ ระดับความรู้ หรือความสามารถในจัดการการป้องกันภัยคุกคามทางไซเบอร์ฯ (Flores & Ekstedt, 2016) สอดคล้องกับ การให้ความรู้ในการจัดการกับสินทรัพย์ข้อมูลแก่พนักงานทุกคนในองค์กรเพื่อเพิ่มการรับรู้ ความเข้าใจในการจัดการสินทรัพย์แก่พวกเขา ทำให้ปรับปรุงและพัฒนาความเข้าใจ รวมถึงยกระดับทักษะ ความรู้ความสามารถด้านการปกป้องสินทรัพย์ข้อมูลของพนักงาน (Nasir et al., 2019) การรับรู้และการฝึกอบรมที่รวมถึงบทบาทและความรับผิดชอบของพนักงานเกี่ยวกับการรปกป้องข้อมูลก่อให้เกิดความเข้าใจในระดับที่สูงขึ้นมีรวมถึงช่วยเพิ่มทักษะหรือความสามารถที่จะปฏิบัติตามข้อกำหนดหรือนโยบายขององค์กร (Koohang et al., 2020) ดังนั้น หากบุคคลยิ่งมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ฯ มาก ทำให้เขาเหล่านั้นมีความมั่นใจในระดับความรู้และทักษะพอเพียงที่จะสามารถนำความรู้เหล่านั้นไปใช้ในการป้องกันภัยคุกคามทางไซเบอร์ฯ ได้

สมมติฐานที่ 1: การตระหนักด้านความมั่นคงทางสารสนเทศมีอิทธิพลเชิงบวกต่อประสิทธิภาพของตนเอง

3.1.2 ความสัมพันธ์ระหว่างการตระหนักด้านมั่นคงทางสารสนเทศกับทัศนคติในการรักษาความมั่นคงทางสารสนเทศ

เมื่อพนักงานมีการรับรู้เกี่ยวกับการภัยคุกคามทางไซเบอร์ฯ จากการให้ความรู้ภายในองค์กร ทำให้เขาเหล่านั้นรับรู้ถึงผลเสียหายของภัยคุกคามดังกล่าว และเกิดความคิดที่จะปฏิเสธภัยคุกคามทางไซเบอร์ (Flores & Ekstedt, 2016) สอดคล้องกับ การให้ความรู้เกี่ยวกับบทบาทและความรับผิดชอบของพนักงานบ่อยครั้ง เพื่อให้พวกเขารับรู้เกี่ยวกับแนวทางในการปฏิบัติหน้าที่ ทำให้พวกเขาเกิดความรู้สึกว่าต้องปฏิบัติตามแนวทางนั้น (Grassegger & Nedbal, 2021) รวมไปถึงการรับรู้เทคโนโลยีของแต่ละบุคคลเมื่อพวกเขารับรู้ถึงความน่าเชื่อถือของเทคโนโลยีที่ต่ำ รวมถึงรับรู้อันตรายของการป้องกันภัยคุกคามที่มาจากเทคโนโลยีที่ไม่เพียงพอทำให้พวกเขามีความรู้สึกว่าศักยภาพของเทคโนโลยีไม่เป็นที่น่าพอใจสำหรับเขา (Dinev & Hu, 2002) ดังนั้น เมื่อบุคคลยิ่งมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ฯ มาก ทำให้พวกเขาเข้าใจถึงความเสียหายที่จะเกิดขึ้นจากภัยคุกคามนั้น จึงทำให้มีความรู้สึกว่าการป้องกันภัยคุกคามาทางไซเบอร์ฯ เป็นสิ่งที่ควรกระทำ และทำให้ความคิดในการป้องกันภัยทางไซเบอร์ฯ สูงขึ้นไปด้วย

สมมติฐานที่ 2: การตระหนักด้านความมั่นคงทางสารสนเทศมีอิทธิพลเชิงบวกต่อทัศนคติในการรักษาความมั่นคงทางสารสนเทศ

3.1.3 ความสัมพันธ์ระหว่างการตระหนักด้านความมั่นคงทางสารสนเทศกับบรรทัดฐานจิตวิสัย

การให้ความรู้แก่ผู้ใช้งานอินเทอร์เน็ตและกลุ่มสังคมเพื่อให้การสื่อสารเป็นไปอย่างกว้างขวางเกี่ยวกับใช้เทคโนโลยีป้องกันซอฟต์แวร์ดักจับข้อมูลภายในเครื่องคอมพิวเตอร์ ทำให้เกิดความเชื่อที่คล้อยตามกันเกี่ยวกับการใช้เทคโนโลยีเพื่อป้องกันซอฟต์แวร์ดักจับ (Dinev & Hu, 2007) สอดคล้องกับ การให้ความรู้เกี่ยวกับบทบาทและความรับผิดชอบของพนักงานในการป้องกันภัยคุกคามทางไซเบอร์ฯ เพื่อเกิดความรู้ไปสู่วงสังคมของพวกเขาและมีความเห็นไปทิศทางเดียวกันว่าภัยคุกคามทางไซเบอร์เป็นสิ่งที่ไม่ดี (Grassegger & Nedbal, 2021) ดังนั้น การที่บุคคลยิ่งมีความรู้ ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ฯ มาก และเชื่อว่าคนรอบข้างที่สำคัญต่อตนเองเห็นด้วยว่าภัยคุกคามทางไซเบอร์เป็นการกระทำที่ไม่พึงประสงค์นั้น ยิ่งทำให้บุคคลเชื่อว่าภัยคุกคามทางไซเบอร์ฯ เป็นสิ่งที่ไม่ดีหรือควรต่อต้าน

สมมติฐานที่ 3: การตระหนักด้านความมั่นคงทางสารสนเทศมีอิทธิพลเชิงบวกต่อบรรทัดฐานจิตวิสัย

3.1.4 ความสัมพันธ์ระหว่างการตระหนักด้านความมั่นคงทางสารสนเทศกับการรับรู้การควบคุมพฤติกรรม

เมื่อผู้ใช้งานเทคโนโลยีมีความรู้เกี่ยวกับความจำเป็นในการป้องกันภัยคุกคามจากเทคโนโลยี ยิ่งผู้ใช้มีความรู้มากขึ้นเกี่ยวกับปัญหาและผลที่ตามมาของการภัยคุกคาม รวมถึงทราบวิธีป้องกันภัยคุกคามจากเทคโนโลยี ทำให้พวกเขายิ่งมีความมั่นใจในการใช้เทคโนโลยีเพื่อป้องกันภัยคุกคาม (Dinev & Hu, 2007) สอดคล้องกับ เมื่อพนักงานในองค์กรถูกส่งเสริมในความรู้เกี่ยวกับการป้องกันภัยคุกคาม ทำให้เพิ่มความมั่นใจต่อเขาเหล่านั้นในการปกป้องบริษัทจากการโจมตีที่อาจเกิดขึ้น (Grassegger & Nedbal, 2021) ดังนั้น การที่บุคคลยิ่งมีความรู้มากเกี่ยวกับภัยคุกคามทางไซเบอร์ฯ รวมถึงวิธีการป้องกัน ทำให้พวกเขายิ่งมีความมั่นใจในความสามารถที่จะจัดหาทรัพยากรในการป้องกันภัยคุกคามทางไซเบอร์ฯ

สมมติฐานที่ 4: การตระหนักด้านความมั่นคงทางสารสนเทศมีอิทธิพลเชิงบวกต่อการรับรู้การควบคุมพฤติกรรม

3.1.5 ความสัมพันธ์ระหว่างประสิทธิภาพของตนเองกับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

เมื่อพนักงานมีความมั่นใจในทักษะ ความรู้ หรือความสามารถของตนเองเกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์ฯ จากนโยบายหรือแนวปฏิบัติขององค์กร ทำให้พวกเขาเหล่านั้นเกิดความตั้งใจที่จะปกป้องภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม (Flores & Ekstedt, 2016) ความมั่นใจในตนเองของแต่ละบุคคลในความสามารถในการจัดการและปฏิบัติพฤติกรรมบางอย่างที่จำเป็นเพื่อให้บรรลุตามที่ต้องการ หากครูสอนภาษาอังกฤษไม่มีความรู้ที่ถูกต้องหรือไม่มั่นใจในการใช้นวัตกรรมทางเทคโนโลยีในชั้นเรียนภาษาอังกฤษ ทำให้ครูผู้นั้นจะหลีกเลี่ยงการใช้เทคโนโลยีในการสอน (Jung, 2018) สอดคล้องกับ เมื่อพนักงานมีความมั่นใจในทักษะ และความสามารถในการหลีกเลี่ยงฟิชชิงเมลเป็นอย่างมาก ยิ่งทำให้พวกเขาสามารถปฏิเสธฟิชชิงเมลได้เป็นอย่างดี (Flores et al., 2015) ดังนั้น เมื่อบุคคลมีความมั่นใจในความรู้ ความสามารถว่าการป้องกันภัยคุกคามทางไซเบอร์ฯ เป็นสิ่งที่ดีและควรกระทำ จึงทำให้เขาเหล่านั้นมีการคาดการณ์ว่าจะกระทำสิ่งนั้น

สมมติฐานที่ 5: ประสิทธิภาพของตนเองมีอิทธิพลเชิงบวกต่อความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

3.1.6 ความสัมพันธ์ระหว่างทัศนคติในการรักษาความมั่นคงทางสารสนเทศความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

ในสถานศึกษาที่มีการใช้เทคโนโลยีในการดำเนินกิจกรรมการเรียนการสอน โดยผู้ที่ใช้คือครูผู้สอน หากพวกเขาความรู้สึกที่ดีต่อผลิตภัณฑ์เดิมที่มีอยู่ เขาเหล่านั้นจึงมีความคิดว่าจะใช้ผลิตภัณฑ์ที่มีอยู่ต่อไปจนกว่าจะพังและจะปฏิเสธผลิตภัณฑ์ที่เป็นนวัตกรรมใหม่ ในทางกลับกันหากครูที่มีทัศนคติเชิงลบต่อผลิตภัณฑ์เดิมที่มีอยู่ จะเต็มใจ

ยอมรับการเปลี่ยนแปลงในการใช้ผลิตภัณฑ์ใหม่ (Jung, 2018) สอดคล้องกับพนักงานของโรงพยาบาลมองว่าการเปลี่ยนแปลงเป็นกระบวนการที่จะทำให้พวกเขาสูญเสียการควบคุมวิธีการเข้าถึงผลการตรวจทางห้องปฏิบัติการ การตัดสินใจทางการรักษา และการดำเนินงานโดยทั่วไป การรับรู้นี้ทำให้พวกเขาต้องการปฏิเสธการเปลี่ยนแปลงเพื่อหลีกเลี่ยงการประสบกับอารมณ์ด้านลบในการทำงาน (Amarantou et al., 2018) สอดคล้องกับ เมื่อผู้ให้บริการด้านการแพทย์มีความจำเป็นต้องใช้ระบบ EMR เพื่อดึงข้อมูลประวัติทางการแพทย์ของผู้ป่วย แต่ไม่ต้องการป้อนข้อมูลใหม่ลงในแบบฟอร์ม เนื่องจากทำให้การทำงานล่าช้า พวกเขาจึงเกิดความคิดในเชิงลบต่อระบบ EMR ทำให้เขาเหล่านั้นมีคาดว่าที่จะหลีกเลี่ยงการใช้ระบบ EMR เพื่อหลีกเลี่ยงการทำงานที่ล่าช้า (Samhan, 2017) ดังนั้น เมื่อบุคคลมีความคิดว่าการป้องกันภัยคุกคามทางไซเบอร์ฯ เป็นสิ่งที่ดี ทำให้พวกเขาเหล่านั้นมีความตั้งใจที่จะกระทำในสิ่งที่เห็นว่าดี

สมมติฐานที่ 6: ทัศนคติในการรักษาความมั่นคงทางสารสนเทศมีอิทธิพลเชิงบวกต่อความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

3.1.7 ความสัมพันธ์ระหว่างบรรทัดฐานจิตวิสัยกับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

พฤติกรรมของพนักงานจะสามารถเปลี่ยนแปลงตามความเชื่อในการปกป้องบริษัทจากการถูกภัยคุกคามทางไซเบอร์ฯ จากสภาพแวดล้อมของสังคมภายในองค์กรที่พวกเขาอยู่ ทำให้พวกเขามีการคาดการณ์ว่าจะปกป้องภัยคุกคามทางไซเบอร์ฯ ภายในบริษัท (Grassegger & Nedbal, 2021) สอดคล้องกับนโยบายในเชิงบวกที่เกี่ยวข้องกับการใช้บริการขนส่งสาธารณะ KMRT ของรัฐบาลทำให้ประชาชนส่วนใหญ่คล้อยตามและคาดว่าที่จะเปลี่ยนความตั้งใจในการใช้รถส่วนบุคคลไปใช้ขนส่งธารณะ (Chen & Chao, 2011) สอดคล้องกับเมื่อผู้ให้บริการอินเทอร์เน็ต ผู้ผลิตคอมพิวเตอร์ และบริษัทซอฟต์แวร์ รับรู้ถึงเหตุการณ์ที่เกี่ยวข้องกับมัลแวร์และความเสียหายที่จะเกิดขึ้นกับข้อมูลที่เป็นความลับและเชื่อว่าความเสียหายเหล่านั้นมีผลกระทบกับสังคมหรือบุคคลอื่น จึงพยายามแจ้งแก่องค์กรต่าง ๆ และเครือข่ายสังคมรับทราบในวงกว้าง เพื่อลดผลกระทบที่จะเกิดขึ้นทางสังคม (Vafaei-Zadeh et al., 2019) ดังนั้น การที่บุคคลเชื่อว่าคนรอบข้างที่มีความสำคัญต่อตนเองมีความเห็นคล้อยตามว่าภัยคุกคามทางไซเบอร์ฯ เป็นสิ่งที่ไม่ดีและควรป้องกัน ซึ่งเป็นการเน้นย้ำว่าการป้องกันภัยคุกคามไซเบอร์เป็นสิ่งที่ควรกระทำ ทำให้บุคคลมีความตั้งใจในการต่อต้านหรือป้องกันภัยคุกคามทางไซเบอร์ฯ

สมมติฐานที่ 7: บรรทัดฐานจิตวิสัยมีอิทธิพลเชิงบวกต่อความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

3.1.8 ความสัมพันธ์ระหว่างการรับรู้การควบคุมพฤติกรรมกับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

บุคคลมีการรับรู้ถึงระดับความง่ายในการใช้เครื่องมือป้องกันมัลแวร์ ทำให้พวกเขามีแนวโน้มที่จะใช้เครื่องมือป้องกันมัลแวร์ หากพวกเขาเชื่อว่ามีความสามารถในการทำงานและทรัพยากรที่มีอยู่เพียงพอต่อการใช้งาน ทำให้พวกเขาเหล่านั้นมีความตั้งใจที่ใช้เครื่องมือเพื่อป้องกันมัลแวร์ (Vafaei-Zadeh et al., 2019) สอดคล้องกับเมื่อผู้ใช้งานรู้สึกว่าเทคโนโลยีที่ใช้อยู่นั้นมีความง่ายการใช้งาน แต่ก็ยังรู้สึกว่าตนไม่สามารถควบคุมขั้นตอนการใช้งานได้ ทำให้พวกเขาไม่อยากใช้งานต่อ หรือหลีกเลี่ยงการใช้งานกับเทคโนโลยีนั้น (Dinev & Hu, 2007) ดังนั้น การที่บุคคลมั่นใจในความรู้และความสามารถในการจัดหาทรัพยากรในการป้องกันภัยคุกคามภัยทางไซเบอร์ฯ มาก และเห็นว่าการป้องกันภัยคุกคามทางไซเบอร์เป็นสิ่งที่ดี ทำให้เขาเหล่านั้นมีความตั้งใจที่จะกระทำสิ่งนั้น

สมมติฐานที่ 8: การรับรู้การควบคุมพฤติกรรมมีอิทธิพลเชิงบวกต่อความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

4. วิธีการวิจัย

งานวิจัยนี้เป็นวิจัยเชิงปริมาณ (Quantitative Research) โดยการใช้แบบสอบถามออนไลน์ (Online Questionnaire) เป็นเครื่องมือที่ช่วยในการจัดเก็บรวบรวมข้อมูลต่าง ๆ และนำข้อมูลที่ได้จากกลุ่มตัวอย่างมาวิเคราะห์ด้วยสถิติในการทดสอบสมมติฐานตามกรอบแนวคิดการวิจัย ประชากรที่ใช้ในการศึกษาในงานวิจัยนี้คือ ผู้ที่เคยประสบภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม เช่น การได้รับโทรศัพท์ การได้รับ SMS เข้ามาหลอกลวง หรือการหลอกลวงผ่านทางอินเทอร์เน็ตผ่านการเข้าใช้งาน ไม่ว่าจะเป็นช่องทาง เว็บไซต์ อีเมล และแชท อย่างน้อย 1 ครั้ง ภายในระยะเวลา 12 เดือน และมีประสบการณ์การทำงานมากกว่า 1 ปี ผู้ตอบแบบสอบถามจำเป็นต้องมีความรู้ ความเข้าใจ เกี่ยวกับคำศัพท์เฉพาะในข้อคำถาม ซึ่งคำถามที่ใช้ในงานวิจัยนี้มีทั้งสิ้น 33 คำถาม ดังนั้นต้อง เก็บข้อมูลจากกลุ่มตัวอย่างอย่างน้อย 165 ตัวอย่าง

ผู้วิจัยใช้ Simple Linear Regression Analysis และ Multiple Linear Regression Analysis ในการวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรอิสระและตัวแปรตาม

5. ผลการวิจัยและอภิปรายผล

กลุ่มตัวอย่างที่ใช้ศึกษาในงานวิจัยเป็นบุคคลทั่วไปที่เคยประสบภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม เช่น การได้รับโทรศัพท์ การได้รับข้อความสั้น (SMS) เข้ามาหลอกลวง หรือการหลอกลวงผ่านทางอินเทอร์เน็ตผ่านการเข้าใช้งาน ไม่ว่าจะเป็นช่องทาง เว็บไซต์ อีเมล และแชท อย่างน้อย 1 ครั้ง ภายในระยะเวลา 12 เดือน และมีประสบการณ์การทำงานมากกว่า 1 ปี ดังนั้นจึงมีการใช้คำถามเพื่อกรองกลุ่มผู้ตอบแบบสอบถาม โดยมีผู้ตอบแบบสอบถามทั้งหมดจำนวน 227 ชุด ซึ่งผู้ตอบแบบสอบถามที่ผ่านคุณสมบัติของกลุ่มตัวอย่างตามงานวิจัยทั้งสิ้น 202 ชุด และในระหว่างปัจจัยมีค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างข้อคำถามไม่อยู่ในระหว่าง 0.3 – 0.8 จึงทำการตัดข้อคำถามใน 2 ตัวแปร ทำให้เหลือข้อคำถามทั้งหมด 31 ข้อ จากการวิเคราะห์องค์ประกอบด้วยวิธีการหมุนแกน พบว่ามี 4 องค์ประกอบ ซึ่งผลการวิเคราะห์ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟาของครอนบาชของตัวแปรทั้งหมด ดังนี้

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟาของครอนบาชของตัวแปรทั้งหมด

ปัจจัย		ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 1: การตระหนักด้านความมั่นคงทางสารสนเทศ (% OF VARIANCE = 62.352, CRONBACH'S ALPHA = 0.876)				
ISA 1	ฉันมีความรู้ ความเข้าใจเกี่ยวกับผลเสียหายที่เกิดจากภัยทางไซเบอร์ฯ	4.36	0.671	0.810
ISA 2	ฉันพูดคุยกับเพื่อนและบุคคลที่รู้จักเกี่ยวกับเทคโนโลยีการป้องกันภัยทางไซเบอร์ฯ	4.24	0.721	0.830
ISA 3	ฉันคอยติดตามข่าวสารเกี่ยวกับภัยทางไซเบอร์ฯ	4.28	0.671	0.796
ISA 4	ฉันมีส่วนร่วมในการแบ่งปันความรู้เกี่ยวกับการปกป้องผลเสียหายที่เกิดจากภัยทางไซเบอร์ฯ เพื่อให้ฉันได้รับข้อมูลล่าสุดอยู่เสมอ	4.18	0.704	0.803
ISA 5	ฉันทราบวิธีการควบคุมภัยทางไซเบอร์ฯ	4.11	0.718	0.758

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟาของครอนบาชของตัวแปรทั้งหมด (ต่อ)

ปัจจัย		ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 1: การตระหนักด้านความมั่นคงทางสารสนเทศ (% OF VARIANCE = 62.352, CRONBACH'S ALPHA = 0.876)				
ISA 6	ฉันทราบนโยบายหรือแนวทางการป้องกันภัยทางไซเบอร์ฯ ขององค์กรหรือหน่วยงานต่าง ๆ	4.03	0.831	0.736
ปัจจัย 2: ประสิทธิภาพของตนเอง (% OF VARIANCE = 16.096, CRONBACH'S ALPHA = 0.830)				
SE 1	ฉันสามารถป้องกันบุคคลที่ไม่รู้จักหรือบุคคลที่ไม่ได้รับอนุญาตจากการเข้าถึงข้อมูลส่วนตัวหรือข้อมูลที่สำคัญของฉัน	4.09	0.717	0.671
SE 2	ฉันมั่นใจว่าฉันพร้อมที่จะป้องกันไม่ให้บุคคลที่ไม่รู้จักหรือบุคคลที่ไม่ได้รับอนุญาต ติดตั้งซอฟต์แวร์ที่เป็นอันตรายบนคอมพิวเตอร์ที่ทำงานของฉัน	4.10	0.81	0.802
SE 3	ฉันสามารถระบุตัวตนของบุคคลที่ไม่รู้จักบุคคลที่น่าสงสัย หรือบุคคลที่ไม่ได้รับอนุญาต จากการสอบถามข้อมูลส่วนตัวหรือข้อมูลที่สำคัญของฉัน	3.87	0.991	0.697
SE 5	ฉันมีทักษะที่จำเป็นอย่างเพียงพอต่อการป้องกันภัยทางไซเบอร์ฯ	4.09	0.83	0.863
ปัจจัย 3: ทัศนคติการรักษาความมั่นคงทางสารสนเทศ (% OF VARIANCE = 25.170, CRONBACH'S ALPHA = 0.938)				
ATT 1	ฉันคิดว่าฉันควรป้องกันไม่ให้บุคคลที่ไม่รู้จักหรือไม่ได้รับอนุญาตเข้าถึงข้อมูลส่วนตัวหรือข้อมูลที่สำคัญ	4.41	0.658	0.818
ATT 2	ฉันคิดว่าฉันควรป้องกันไม่ให้บุคคลต่าง ๆ ติดตั้งซอฟต์แวร์ที่เป็นอันตรายบนคอมพิวเตอร์ที่ทำงานของฉัน	4.40	0.728	0.878
ATT 3	ฉันคิดว่าองค์กรหรือหน่วยงานควรสามารถระบุตัวตนผู้ทำให้เกิดภัยทางไซเบอร์ฯ ว่าเกิดจากใคร	4.32	0.706	0.823
ATT 4	ฉันคิดว่าติดตั้งซอฟต์แวร์ป้องกันอันตรายบนคอมพิวเตอร์เป็นประโยชน์ต่อฉัน	4.37	0.756	0.830
ATT 5	ฉันคิดว่าฉันควรล้างไวรัสจากคอมพิวเตอร์อยู่เสมอ	4.39	0.699	0.821

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟาของครอนบาชของตัวแปรทั้งหมด (ต่อ)

ปัจจัย		ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 4: บรรทัดฐานจิตวิสัย (% OF VARIANCE = 19.764, CRONBACH'S ALPHA = 0.867)				
SN 1	คนรอบข้างที่มีความสำคัญต่อฉัน (เช่น พ่อ แม่ พี่ น้อง เพื่อนสนิท เป็นต้น) คิดว่าฉันควรล้างไวรัสออกจากคอมพิวเตอร์ของฉัน เพิ่มคำกำกับ (เช่น พ่อ แม่ พี่ น้อง เพื่อนสนิท เป็นต้น)	4.00	0.723	0.767
SN 2	คนรอบข้างที่มีความสำคัญต่อฉัน (เช่น พ่อ แม่ พี่ น้อง เพื่อนสนิท เป็นต้น) คิดว่าฉันควรป้องกันไม่ให้ไวรัสทำงานบนคอมพิวเตอร์ของฉัน	4.09	0.728	0.760
SN 3	คนรอบข้างที่มีความสำคัญต่อฉัน (เช่น พ่อ แม่ พี่ น้อง เพื่อนสนิท เป็นต้น) คิดว่าฉันควรให้ฉันใช้ซอฟต์แวร์ป้องกันอันตรายบนคอมพิวเตอร์ของฉัน	4.02	0.708	0.828
SN 4	คนรอบข้างที่มีความสำคัญต่อฉัน (เช่น พ่อ แม่ พี่ น้อง เพื่อนสนิท เป็นต้น) คิดว่าฉันควรสามารถระบุตัวตนผู้ทำให้เกิดภัยทางไซเบอร์ฯ เกิดจากใคร	3.97	0.788	0.757
SN 5	คนรอบข้างที่มีความสำคัญต่อฉัน (เช่น พ่อ แม่ พี่ น้อง เพื่อนสนิท เป็นต้น) คิดว่าฉันควรป้องกันไม่ให้บุคคลที่ไม่รู้จักหรือไม่ได้รับอนุญาต เข้าถึงข้อมูลส่วนตัวหรือข้อมูลที่สำคัญ	4.21	0.71	0.782
ปัจจัย 5: การรับรู้การควบคุมพฤติกรรม (% OF VARIANCE = 14.869, CRONBACH'S ALPHA = 0.90)				
PBC 1	ฉันมั่นใจว่าฉันมีกำลังทรัพย์เพียงพอที่จะจัดหาซอฟต์แวร์ป้องกันอันตรายบนคอมพิวเตอร์ของฉัน เพิ่มคำว่าคอมพิวเตอร์ของฉัน	4.15	0.771	0.803
PBC 4	การล้างไวรัสจากคอมพิวเตอร์ของฉันโดยใช้ซอฟต์แวร์เรื่องที่ง่ายสำหรับฉัน	4.08	0.971	0.833
PBC 5	ฉันมั่นใจว่าฉันสามารถปฏิเสธการหลอกลวงอันเกิดจากภัยทางไซเบอร์ฯ	4.36	0.755	0.769
ปัจจัย 6: ความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม (% OF VARIANCE = 66.414, CRONBACH'S ALPHA = 0.913)				
INT 1	ฉันจะไม่เปิดโอกาสให้บุคคลที่ไม่รู้จักหรือไม่ได้ รับอนุญาต ติดตั้งซอฟต์แวร์ในเครื่องของฉัน	4.54	0.573	0.849
INT 2	ฉันจะไม่เปิดเผยรหัสผ่านคอมพิวเตอร์ของฉันให้กับบุคคลที่ไม่รู้จักหรือไม่ได้รับอนุญาต	4.50	0.566	0.812

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบและค่าสัมประสิทธิ์แอลฟาของครอนบาชของตัวแปรทั้งหมด (ต่อ)

ปัจจัย		ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัย 6: ความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม (% OF VARIANCE = 66.414, CRONBACH'S ALPHA = 0.913)				
INT 3	ฉันจะไม่เปิดโอกาสให้บุคคลที่น่าสงสัยเข้าถึงข้อมูลส่วนตัวหรือข้อมูลที่สำคัญของฉัน	4.55	0.631	0.871
INT 4	ฉันจะไม่เปิดเผยรหัสผ่านคอมพิวเตอร์ของฉันให้กับบุคคลที่น่าสงสัยว่าจะมาสร้างภัยทางไซเบอร์ฯ	4.60	0.558	0.835
INT 5	ฉันจะตรวจสอบการตั้งค่าคอมพิวเตอร์เป็นระยะ ๆ เพื่อป้องกันอันตรายบนคอมพิวเตอร์	4.44	0.697	0.727
INT 6	ฉันจะอัปเดตหรือติดตั้งซอฟต์แวร์ที่ถูกต้องตามกฎหมายเพื่อป้องกันอันตรายบนคอมพิวเตอร์	4.44	0.668	0.813
INT 7	ฉันจะหลีกเลี่ยงภัยทางไซเบอร์ฯ ให้มากที่สุด	4.59	0.594	0.790

5.1 การทดสอบสมมติฐานการวิจัย (Regression Analysis)

งานวิจัยฉบับนี้ใช้การวิเคราะห์เพื่อคาดการณ์ตัวแปรตามด้วยค่าสัมประสิทธิ์การถดถอย (Regression Coefficient) เพื่อบอกถึงอิทธิพลของตัวแปรตามที่เกิดขึ้น ซึ่งในงานวิจัยเลือกใช้การวิเคราะห์การถดถอยอย่างง่าย (Simple Regression Analysis) และการวิเคราะห์การถดถอยเชิงเส้นพหุคูณ (Multiple Linear Regression) โดยใช้ค่า p-value ที่น้อยกว่าหรือเท่ากับ 0.05 เป็นตัวกำหนดนัยสำคัญทางสถิติ (Significant Level) โดยมีผลการทดสอบ ดังนี้

5.1.1 ความสัมพันธ์ระหว่างการตระหนักด้านความมั่นคงทางสารสนเทศกับประสิทธิภาพของตนเอง

ผลของการวิเคราะห์การถดถอย พบว่าตัวแปรอิสระ คือ การตระหนักด้านความมั่นคงทางสารสนเทศ และตัวแปรตาม คือ ประสิทธิภาพของตนเอง พบว่า การตระหนักด้านความมั่นคงทางสารสนเทศมีความสัมพันธ์กับประสิทธิภาพของตนเองอย่างมีนัยสำคัญทางสถิติที่ 0.05 เมื่อพิจารณาจากค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) พบว่า การตระหนักด้านความมั่นคงทางสารสนเทศและประสิทธิภาพของตนเอง มีค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) เท่ากับ 0.551 โดยมีค่า p-value ที่น้อยกว่า 0.01

5.1.2 ความสัมพันธ์ระหว่างการตระหนักด้านความมั่นคงทางสารสนเทศกับทัศนคติในการรักษาความมั่นคงทางสารสนเทศ

ผลของการวิเคราะห์การถดถอย พบว่าตัวแปรอิสระ คือ การตระหนักด้านความมั่นคงทางสารสนเทศ และตัวแปรตาม คือ ทัศนคติในการรักษาความมั่นคงทางสารสนเทศ พบว่า การตระหนักด้านความมั่นคงทางสารสนเทศมีความสัมพันธ์กับทัศนคติในการรักษาความมั่นคงทางสารสนเทศ อย่างมีนัยสำคัญทางสถิติที่ 0.05 เมื่อพิจารณาจากค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) พบว่า การตระหนักด้านความมั่นคงทางสารสนเทศและประสิทธิภาพของตนเอง มีค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) เท่ากับ 0.404 โดยมีค่า p-value ที่น้อยกว่า 0.01

5.1.3 ความสัมพันธ์ระหว่างการตระหนักด้านความมั่นคงทางสารสนเทศกับบรรทัดฐานจิตวิสัย

ผลของการวิเคราะห์การถดถอย พบว่าตัวแปรอิสระ คือ การตระหนักด้านความมั่นคงทางสารสนเทศ และตัวแปรตาม คือ บรรทัดฐานจิตวิสัย พบว่า การตระหนักด้านความมั่นคงทางสารสนเทศมีความสัมพันธ์กับบรรทัดฐานจิตวิสัยอย่างมีนัยสำคัญทางสถิติที่ 0.05 เมื่อพิจารณาจากค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) พบว่า การตระหนักด้าน

ความมั่นคงทางสารสนเทศและประสิทธิภาพของตนเอง มีค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) เท่ากับ 0.296 โดยมีค่า p-value ที่น้อยกว่า 0.01

5.1.4 ความสัมพันธ์ระหว่างการตระหนักด้านความมั่นคงทางสารสนเทศกับการรับรู้การควบคุมพฤติกรรม

ผลของการวิเคราะห์การถดถอย พบว่าตัวแปรอิสระ คือ การตระหนักด้านความมั่นคงทางสารสนเทศ และตัวแปรตาม คือ การรับรู้การควบคุมพฤติกรรม พบว่า การตระหนักด้านความมั่นคงทางสารสนเทศมีความสัมพันธ์กับการรับรู้การควบคุมพฤติกรรม อย่างมีนัยสำคัญทางสถิติที่ 0.05 เมื่อพิจารณาจากค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) พบว่า การตระหนักด้านความมั่นคงทางสารสนเทศและประสิทธิภาพของตนเอง มีค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) เท่ากับ 0.471 โดยมีค่า p-value ที่น้อยกว่า 0.01

5.6.5 ความสัมพันธ์ระหว่างประสิทธิภาพของตนเองกับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

ผลของการวิเคราะห์การถดถอย พบว่าตัวแปรอิสระ คือ ประสิทธิภาพของตนเองและตัวแปรตาม คือ ความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม พบว่า ประสิทธิภาพของตนเองมีความสัมพันธ์กับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม อย่างไม่มีนัยสำคัญทางสถิติที่ 0.05 เมื่อพิจารณาจากค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) พบว่า ประสิทธิภาพของตนเองและความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม มีค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) เท่ากับ 0.058 โดยมีค่า p-value มากกว่า 0.05

ทั้งนี้อาจเกิดจากปัจจัยของลักษณะขององค์กร หรือขนาดของแต่ละองค์กร ที่มีรูปแบบการทำงานแตกต่างกันออกไป ทำให้ปัจจัยด้านประสิทธิภาพตนเองยังไม่เป็นผลเชิงประจักษ์ว่ามีความสัมพันธ์กับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคมอย่างมีนัยสำคัญ

5.1.6 ความสัมพันธ์ระหว่างทัศนคติในการรักษาความมั่นคงทางสารสนเทศกับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

ผลของการวิเคราะห์การถดถอย พบว่าตัวแปรอิสระ คือ ทัศนคติในการรักษาความมั่นคงทางสารสนเทศ และตัวแปรตาม คือ ความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม พบว่า ทัศนคติในการรักษาความมั่นคงทางสารสนเทศมีความสัมพันธ์กับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม อย่างมีนัยสำคัญทางสถิติที่ 0.05 เมื่อพิจารณาจากค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) พบว่า ทัศนคติในการรักษาความมั่นคงทางสารสนเทศและความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม มีค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) เท่ากับ 0.258 โดยมีค่า p-value น้อยกว่า 0.01

5.1.7 ความสัมพันธ์ระหว่างบรรทัดฐานจิตวิสัยกับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

ผลของการวิเคราะห์การถดถอย พบว่าตัวแปรอิสระ คือ บรรทัดฐานจิตวิสัย และตัวแปรตาม คือ ความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม พบว่า บรรทัดฐานจิตวิสัยมีความสัมพันธ์กับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม อย่างไม่มีนัยสำคัญทางสถิติที่ 0.05 เมื่อพิจารณาจากค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) พบว่า บรรทัดฐานจิตวิสัยและความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม มีค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) เท่ากับ 0.104 โดยมีค่า p-value มากกว่า 0.05

ทั้งนี้อาจมีเหตุผลมาจากอิทธิพลของบุคคลรอบข้างหรือเพื่อนร่วมงานมีการพูดคุยหรือแลกเปลี่ยนความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ฯ น้อย อาจเกิดจากการทำงานที่ไม่ค่อยเกี่ยวข้องเกี่ยวข้องกับระบบสารสนเทศ ทำให้ไม่เกิดความคิดที่สนับสนุนหรือคล้อยตาม ซึ่งส่งผลต่อการการคาดการณ์ หรือการวางแผนที่จะปฏิเสธภัยคุกคามทางไซเบอร์ฯ

5.1.8 ความสัมพันธ์ระหว่างการรับรู้การควบคุมพฤติกรรมกับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

ผลของการวิเคราะห์การถดถอย พบว่าตัวแปรอิสระ คือ การรับรู้การควบคุมพฤติกรรม และตัวแปรตาม คือ ความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม พบว่า การรับรู้การควบคุมพฤติกรรมมีความสัมพันธ์กับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม อย่างมีนัยสำคัญทางสถิติที่ 0.05 เมื่อพิจารณาจากค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) พบว่า การรับรู้การควบคุมพฤติกรรมและความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม มีค่าสัมประสิทธิ์ถดถอยมาตรฐาน (Beta) เท่ากับ 0.397 โดยมีค่า p-value น้อยกว่า 0.01

ตารางที่ 2 สรุปผลการทดสอบสมมติฐานงานวิจัย

ลำดับ	สมมติฐาน	ผลการทดสอบ
H1	การตระหนักด้านความมั่นคงทางสารสนเทศส่งผลต่อประสิทธิภาพของตนเอง	สนับสนุน
H2	การตระหนักด้านความมั่นคงทางสารสนเทศส่งผลต่อทัศนคติในการรักษาความมั่นคงทางสารสนเทศ	สนับสนุน
H3	การตระหนักด้านความมั่นคงทางสารสนเทศส่งผลต่อบรรทัดฐานจิตวิสัย	สนับสนุน
H4	การตระหนักด้านความมั่นคงทางสารสนเทศส่งผลต่อการรับรู้การควบคุมพฤติกรรม	สนับสนุน
H5	ประสิทธิภาพของตนเองส่งผลต่อความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม	ไม่สนับสนุน
H6	ทัศนคติในการรักษาความมั่นคงทางสารสนเทศส่งผลต่อความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม	สนับสนุน
H7	บรรทัดฐานจิตวิสัยส่งผลต่อความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม	ไม่สนับสนุน
H8	การรับรู้การควบคุมพฤติกรรมส่งผลต่อความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม	สนับสนุน

6. สรุปผลการวิจัยและข้อเสนอแนะ

งานวิจัยนี้มีแนวคิดจากการที่ผู้วิจัยพบเห็นเหตุการณ์ภัยคุกคามทางไซเบอร์หลากหลายรูปแบบยิ่งในปัจจุบันผู้คนทั่วไปและในองค์กรต่าง ๆ พบเจอเหตุการณ์ภัยคุกคามบ่อยครั้งทั้งในชีวิตประจำวัน โดยเฉพาะอย่างยิ่งในรูปแบบโทรศัพท์ ที่แอบอ้างเป็นหน่วยงานต่าง ๆ เพื่อสอบถามข้อมูลที่เป็นส่วนตัวหรือข้อมูลที่เป็นความลับ หรือในรูปแบบข้อความสั้น (SMS) แจ้งว่าเป็นผู้โชคดีได้รับรางวัลต่าง ๆ เพื่อหลอกให้เหยื่อหลงดีใจและกดเข้าไปตามที่อยู่ที่ระบุไว้ หรือในรูปแบบอีเมล มักถูกส่งมาในลักษณะองค์กรที่เกี่ยวข้องกับการทำงาน เพื่อหลอกให้เปิดไฟล์ที่แนบมากับอีเมลหรือเข้าถึงเว็บไซต์ที่มีมัลแวร์แฝงตัวอยู่ เป็นต้น ซึ่งผู้ไม่หวังดีที่ทำให้เกิดภัยคุกคามทางไซเบอร์นี้อาศัยเทคนิคพื้นฐานทางจิตวิทยาที่เรียกว่า “วิศวกรรมสังคม (Social Engineering)” ให้เหยื่อเปิดเผยข้อมูล เพื่อให้ได้ผลประโยชน์ตามที่ผู้ไม่หวังดีต้องการโดยอาศัยจุดอ่อน ความรู้เท่าไม่ถึงการณ์ ความไม่รู้ ความประมาท ซึ่งการโจมตีนี้จะได้ผลดีมากเมื่อเทียบกับการโจมตีทางไซเบอร์ฯ ลักษณะอื่น ๆ ในปัจจุบันและมีแนวโน้มจะเพิ่มขึ้นในอนาคต ซึ่งการป้องกันหรือกรหลีกเลี่ยงไม่ให้ตกเป็นเหยื่อของการหลอกลวงในรูปแบบดังกล่าวคือการสร้างความตระหนักรู้ถึงความมั่นคงทางสารสนเทศแก่บุคคลทั่วไปรวมถึงพนักงานในองค์กรต่าง ๆ ที่มีความสำคัญในการเก็บรักษาข้อมูลขององค์กร ดังนั้น

ผู้วิจัยจึงอยากศึกษาความสัมพันธ์ระหว่างการตระหนักถึงความมั่นคงทางสารสนเทศกับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม

งานวิจัยนี้ศึกษาโดยการเก็บข้อมูลผ่านแบบสอบถามอิเล็กทรอนิกส์กับกลุ่มตัวอย่าง โดยผู้วิจัยดำเนินการแจกแบบสอบถามในสื่อสังคมออนไลน์ และได้ข้อมูลผู้ตอบแบบสอบถามจำนวนทั้งหมด 227 ราย หลังจากทำการตรวจสอบความถูกต้องก่อนนำไปวิเคราะห์ผลทางสถิติ พบว่ามีจำนวนผู้ตอบแบบสอบถามคงเหลือที่ 202 ราย โดยมีผลการวิเคราะห์ทางสถิติ ดังนี้

ข้อมูลทางประชากรศาสตร์ของกลุ่มตัวอย่างในงานวิจัยประกอบด้วย เพศ อายุ ระดับการศึกษา และระดับรายได้ โดยผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิงจำนวน 135 ราย คิดเป็น ร้อยละ 66.8 อายุผู้ตอบแบบสอบถามส่วนใหญ่มีอายุระหว่าง 26-35 ปี จำนวน 135 ราย คิดเป็นร้อยละ 66.8 ผู้ตอบแบบสอบถามมีระดับการศึกษาส่วนใหญ่ระดับปริญญาตรี จำนวน 124 ราย คิดเป็นร้อยละ 61.4 สำหรับรายได้ต่อเดือนของผู้ตอบแบบสอบถามส่วนใหญ่มีรายได้ต่อเดือน 30,000 – 50,000 บาท จำนวน 80 ราย คิดเป็นร้อยละ 39.6 อาชีพของผู้ตอบแบบสอบถามส่วนใหญ่เป็นพนักงานบริษัทเอกชนจำนวน 113 ราย คิดเป็นร้อยละ 55.9

ผลการวิเคราะห์ทางสถิติระหว่างการตระหนักด้านความมั่นคงทางสารสนเทศมีความสัมพันธ์กับประสิทธิภาพของตนเอง ทัศนคติในการรักษาความมั่นคงทางสารสนเทศ บรรทัดฐานจิตวิสัยและการรับรู้การควบคุมพฤติกรรม รวมถึงผลการวิเคราะห์ทางสถิติระหว่าง ทัศนคติในการรักษาความมั่นคงทางสารสนเทศ และการรับรู้การควบคุมพฤติกรรมมีความสัมพันธ์กับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคมอย่างมีนัยสำคัญ

6.1 ประโยชน์ของงานวิจัย

6.1.1 ประโยชน์ของงานวิจัยในภาคทฤษฎี

งานวิจัยนี้พัฒนากรอบแนวคิดการวิจัยมาจากทฤษฎีพฤติกรรมตามแผน (Theory of Planned Behavior: TPB) เป็นทฤษฎีที่เกี่ยวกับการเชื่อมโยงระหว่างทัศนคติและพฤติกรรมโดยนำไปใช้เพื่อศึกษาความสัมพันธ์ระหว่างทัศนคติ ความเชื่อ และการรับรู้ ที่นำไปสู่ความตั้งใจเชิงพฤติกรรม ทางผู้วิจัยได้ทำการทบทวนวรรณกรรมและงานวิจัยในอดีตที่เกี่ยวข้องกับความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม พบว่าปัจจัยที่จะส่งผลต่อ ทัศนคติในการรักษาความมั่นคงทางสารสนเทศ การรับรู้การควบคุมพฤติกรรม และนำไปสู่ความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรม คือปัจจัยการตระหนักรู้ด้านความมั่นคงทางสารสนเทศซึ่งองค์กรสามารถเสริม สร้างความรู้ ความเข้าใจเกี่ยวกับผลเสียหายที่เกิดจากภัยทางไซเบอร์ฯ เพื่อให้พนักงานเกิดความคิดและทัศนคติในการป้องกันภัยคุกคามทางไซเบอร์ฯ รวมถึงการแชร์ข่าวสารภายในองค์กรที่เกี่ยวข้องกับภัยไซเบอร์ฯ เพื่อให้มีการรับรู้ข้อมูลข่าวสารที่ล่าสุดอยู่เสมอนำไปสู่การแลกเปลี่ยนข้อมูลระหว่างพนักงานในองค์กร และทำให้พนักงานมีส่วนร่วมในการแบ่งปันความรู้ภายในองค์กร

6.1.2 ประโยชน์ของงานวิจัยทางภาคปฏิบัติ

จากผลการทดสอบทางสถิติของงานวิจัยฉบับนี้ทำให้ทราบว่าการตระหนักรู้ด้านความมั่นคงทางสารสนเทศ ส่งผลทางบวกต่อทัศนคติในการรักษาความมั่นคงทางสารสนเทศ ความเชื่อหรือบรรทัดฐานจิตวิสัย การรับรู้การควบคุมพฤติกรรม ซึ่งปัจจัยเหล่านี้จะนำไปสู่ความตั้งใจที่จะต่อต้านภัยคุกคามทางไซเบอร์ประเภทวิศวกรรมสังคม ซึ่งหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงทางสารสนเทศสามารถนำผลการศึกษาที่ได้มาวิเคราะ ห์และวางแผนเชิงกลยุทธ์เพื่อสื่อสารไปยังองค์กรต่าง ๆ หรือองค์กรที่อยู่ภายใต้กำกับดูแล เพื่อสร้างการตระหนักรู้ให้แก่พนักงานในองค์กร ผู้บริหารฝ่ายทรัพยากรมนุษย์สามารถพัฒนาโปรแกรมการอบรมให้ความรู้ความเข้าใจกับพนักงาน เช่น การจัดโปรแกรมการเรียนรู้ในเรื่องของภัยคุกคามทางไซเบอร์ฯ ให้มีเนื้อหาที่ทันสมัยเข้ากับภัยคุกคามทางไซเบอร์ในปัจจุบันและมีเนื้อหาเข้าใจง่าย เพื่อให้ง่ายต่อการรับรู้และเข้าใจ รวมถึงควรจัดให้มีการวัดประสิทธิภาพในการเรียน เช่น การจัดทำแบบทดสอบก่อนและหลังเรียน เพื่อวัดประสิทธิภาพและความรู้ ความเข้าใจของพนักงาน รวมถึงยังเป็นการประเมินประสิทธิภาพของโปรแกรมการเรียนดังกล่าวว่าเหมาะสมและมีประโยชน์แก่ผู้เรียนหรือไม่ และควรจัดให้มีการ

ทบทวนบทเรียนอยู่เสมอ เพื่อให้การเรียนรู้เหมาะสมแก่ผู้เรียนและรูปแบบภัยคุกคามทางไซเบอร์ฯ ที่เปลี่ยนแปลงไป หรืออาจจะมีการกำหนดนโยบาย และขั้นตอนการปฏิบัติงานที่ชัดเจนเพื่อป้องกันภัยคุกคามประเภทวิศวกรรมสังคม ซึ่งหน่วยงานที่มีบทบาททางสังคมทั้งภาครัฐและภาคเอกชนสามารถสร้างการตระหนักรู้ให้แก่บุคคลทั่วไปในสังคมที่มีโอกาสพบกับภัยคุกคามทางไซเบอร์ฯ เช่น การเผยแพร่ข้อมูลข่าวสารที่เกี่ยวของกับ ภัยคุกคามทางไซเบอร์ฯ และวิธีการป้องกันหรือข้อมูลเป็นประโยชน์ที่เกี่ยวข้อง รวมถึงองค์กรได้ตระหนักถึงเรื่องภัยคุกคามทางไซเบอร์ฯ และพัฒนาระบบสารสนเทศให้มั่นคงมากยิ่งขึ้น เพื่อเตรียมรับมือกับภัยคุกคามทางไซเบอร์ฯ ที่อาจเกิดขึ้นในอนาคต และลดผลกระทบ ความเสียหายที่อาจเกิดขึ้นกับระบบสารสนเทศ รวมถึงการดำเนินงานของธุรกิจ อีกทั้งยังสร้างความน่าเชื่อถือต่อพนักงาน ลูกค้า และผู้ใช้ระบบขององค์กร ในการป้องกันภัยคุกคามทางไซเบอร์ฯ ได้อย่างมีประสิทธิภาพ

6.2 ข้อจำกัดของงานวิจัยและงานวิจัยในอนาคต

งานวิจัยในอนาคตควรจะกำหนดปัจจัยในการประเมินเพื่อสร้างวัฒนธรรมและพฤติกรรมการรักษาความปลอดภัยแบบองค์รวม (Security Behavior and Culture Programs หรือ SBCPs) เนื่องจากเห็นว่า การปลูกฝังสร้างวัฒนธรรมให้พนักงานในองค์กรจะสามารถป้องกันภัยคุมคามทางไซเบอร์ในรูปแบบใหม่ ๆ ตามพฤติกรรมที่เปลี่ยนแปลงไปของสังคมและการพัฒนาของเทคโนโลยีในอนาคต และอาจเจาะจงกลุ่มตัวอย่างให้ชัดเจนมากขึ้น เช่น กลุ่มตัวอย่างที่ทำงานด้านสารสนเทศ หรือ กลุ่มลักษณะเฉพาะของการดำเนินงานขององค์กรต่าง ๆ เพื่อให้ได้ผลลัพธ์ที่ชัดเจนมากยิ่งขึ้น

บรรณานุกรม

ศูนย์วิจัยกสิกรไทย. (2 พฤศจิกายน 2564). *แฉเล่ห์กล ล่อ..ลวง...ล้วง ข้อมูลผ่านมือถือ/ซ้อปออนไลน์.* https://www.kasikornresearch.com/th/analysis/k-social-media/Pages/FB-02-11-21.aspx?fbclid=IwAR1iP0-YuZ9czlBZN-InGR8WNNWoxkoHkdaOxjSMySV4hI6Z_ffXrSEkE2M

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: the effects of human behaviors and demographics on each step of a phishing process. *IEEE Access*, *9*, 44928-44949. https://doi.org/10.1109/ACCESS.2021.3066383

Amarantou, V., Kazakopoulou, S., Chatzoudes, D., & Chatzoglou, P. (2018). Resistance to change: an empirical investigation of its antecedents. *Journal of Organizational Change Management*, *31*(2), 426-450. https://doi.org/10.1108/JOCM-05-2017-0196

Chen, C. F., & Chao, W. H. (2011). Habitual or reasoned? Using the theory of planned behavior, technology acceptance model, and habit to examine switching intentions toward public transit. *Transportation Research Part F: Traffic Psychology and Behaviour*, *14*(2), 128-137. https://doi.org/10.1016/j.trf.2010.11.006

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 23. f https://aisel.aisnet.org/jais/vol8/iss7/23

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*, 26-44. https://doi.org/10.1016/j.cose.2016.01.004

Flores, W. R., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information & Computer Security, 23*(2), 178-199. https://doi.org/10.1108/ICS-05-2014-0029

Global Digital Trust Insights. (2021). Global Digital Trust Insights Survey 2021. Pwc. 1-37. Retrieved 18 November 2024, https://www.pwc.es/es/publicaciones/digital/global-digital-trust-insights-2021.pdf

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, *181*, 59-66. https://doi.org/10.1016/j.procs.2021.01.103

Indrajit, R. E. (2017). Social engineering framework: Understanding the deception approach to human element of security. *International Journal of Computer Science Issues (IJCSI)*, *14*(2), 8. https://doi.org/10.20943/01201702.816

Jung, H. j. (2018). An Exploration of English Teachers' Resistance to Technological Innovation. *Multimedia-Assisted Language Learning*, *21*(1), 35-56. https://doi.org/10.15702/mall.2018.21.1.35

Kemp, S. (2020, January 30). *DIGITAL 2020: 3.8 BILLION PEOPLE USE SOCIAL MEDIA.* We Are Social. from https://wearesocial.com/uk/blog/2020/01/digital-2020-3-8-billion-people-use-social-media

Koohang, A., Anderson, J., Nord, J. H., & Paliszkiewicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, *120*(1), 231-247. https://doi.org/10.1108/IMDS-07-2019-0412

Nasir, A., Abdullah Arshah, R., & Ab Hamid, M. R. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal: A Global Perspective*, *28*(3), 55-80. https://doi.org/10.1080/19393555.2019.1643956

Samhan, B. (2017). Can cyber risk management insurance mitigate healthcare providers' intentions to resist electronic medical records? *International Journal of Healthcare Management*, 12-21. https://doi.org/10.1080/20479700.2017.1412558

Vafaei-Zadeh, A., Thurasamy, R., & Hanifah, H. (2019). Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior. *Kybernetes*, *48*(8), 1565-1585. https://doi.org/10.1108/K-05-2018-0226

Vafaei-Zadeh, A., Ramayah, T., Wong, W. P., & Md Hanifah, H. (2018). Modelling internet security software usage among undergraduate students: A necessity in an increasingly networked world. *VINE Journal of Information and Knowledge Management Systems*, *48*(1), 2-20. https://doi.org/10.1108/VJIKMS-09-2016-0052

Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, *9*, 11895-11910. https://doi.org/10.1109/ACCESS.2021.3051633

Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports, 4,* 100126. https://doi.org/10.1016/j.chbr.2021.100126