ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร

นายณศรัณย์ ขำหาญ

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567

ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร

นายณศรัณย์ ขำหาญ

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567

ใบรับรองการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร

โดย นายณศรัณย์ ขำหาญ

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

คณบดีบัณฑิตวิทยาลัย / หัวหน้าภาควิชา

คณะกรรมการสอบการค้นคว้าอิสระ

..... ประธานกรรมการ

(รองศาสตราจารย์ ดร.สุมิตรา นวลมีศรี)

..... อาจารย์ที่ปรึกษา

(ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์)

..... กรรมการ

(รองศาสตราจารย์ ดร.สุมิตรา นวลมีศรี)

ชื่อ : นายณศรัณย์ ขำหาญ
ชื่อการค้นคว้าอิสระ : ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร
สาขาวิชา : การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์
ปีการศึกษา : 2567

บทคัดย่อ

การศึกษาปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานครมีวัตถุประสงค์ 1) เพื่อศึกษาปัจจัยทางด้านลักษณะประชากรที่มีผลต่อความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และด้านประสบการณ์ภัยคุกคามไซเบอร์ ความตระหนักรู้ถึงภัยคุกคามทาง ไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ 2) เพื่อหาปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ วิธีการสุ่มตัวอย่างในงานวิจัยครั้งนี้เป็นการสุ่มเฉพาะเจาะจงโดยเป็นการเลือกกลุ่มตัวอย่างที่เคยมีประสบการณ์ใช้บริการธุรกรรมการเงินออนไลน์อย่างน้อย 1 ครั้ง จำนวนกลุ่มตัวอย่าง 450 คนในการเก็บแบบสอบถามและนำมาทดสอบทางสถิติ ผลการศึกษาพบว่า ปัจจัยอายุ ระดับการศึกษา ระดับรายได้ต่อเดือนของผู้ตอบแบบสอบถามมีความสัมพันธ์และส่งผลต่อการตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์โดยวัดที่ระดับนัยสำคัญทางสถิติที่ 0.05 ระดับความเชื่อมั่นทางสถิติร้อยละ 95 มีเพียงปัจจัยเพศของผู้ตอบแบบสอบถามไม่มีความสัมพันธ์และไม่ส่งผลต่อการตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์กลุ่มตัวอย่างของการศึกษามีความรู้ด้านภัยคุกคามทางไซเบอร์ของการทำธุรกรรมการเงินออนไลน์ โดยกลุ่มตัวอย่างส่วนใหญ่เข้าใจว่าการเข้าใช้เครือข่ายไร้สายสาธารณะ ทำให้ผู้ใช้บริการมีความเสี่ยงต่อการทำธุรกรรมออนไลน์ ควรมีการตั้งรหัสผ่านต่างๆ ที่มีความยาวมากช่วยลดโอกาสการเดารหัสผ่านหรือใช้เวลาในการคาดเดายากมากขึ้นและการบันทึกรหัสผ่านต่างๆ ไว้ในเครื่องที่เชื่อมต่อกับเครือข่ายไร้สายสาธารณะมีความเสี่ยงต่อภัยคุกคามโจมตีการทำธุรกรรม

(มีจำนวนทั้งสิ้น 76 หน้า)

คำสำคัญ : ความตระหนักรู้, ภัยคุกคามทางไซเบอร์, ธุรกรรมการเงินออนไลน์

_____ อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Mr. Nasarun Khamharn
Independent Study Title : Factors Affecting Cyber Threat Awareness among Online Financial Transaction Service Users in Bangkok
Major Field : Network and Information Security Management King Mongkut's University of Technology North Bangkok
Independent Study Advisor : Assistant Professor Dr. Pongsarun Boonyopakorn
Academic Year : 2024

ABSTRACT

The study aimed to investigate the factors influencing the awareness of cyber threats among users of online financial transaction services in Bangkok. The objectives were to explore how demographic factors such as age, education level, and income affect users' knowledge of cyber threats and their personal experiences with them, as well as to identify the specific factors that contribute to users' awareness of these threats in the context of online financial transactions. A purposive sampling method was used to select 450 participants who had used online financial transaction services at least once. The results showed that age, education level, and monthly income were significantly related to the awareness of cyber threats, with a statistical significance level of 0.05 and a 95% confidence level. However, the study found no significant relationship between gender and awareness of cyber threats. Additionally, the study revealed that the majority of participants had a solid understanding of cyber threats related to online financial transactions, particularly the risks of using public Wi-Fi networks. Most participants acknowledged that using public Wi-Fi for online transactions could expose them to cyber threats.

(Total 76 Pages)

Keywords: Awareness, Cyber Threat, Online Financial Transaction

_____ Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระนี้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลืออย่างดียิ่งของ ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์ และ อาจารย์ ดร.ธนวรรธน์ โยชะนัง อาจารย์ที่ปรึกษาการค้นคว้าอิสระที่ได้ให้ข้อคิดเห็นต่างๆ และให้ความช่วยเหลือชี้แนะแนวทางที่เป็นประโยชน์ต่อการทำวิจัยนี้มาโดยตลอด ผู้วิจัยขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอขอบพระคุณผู้เชี่ยวชาญ ดร.พนิดา ร้อยดวง ผู้อำนวยการส่วนวิจัยนโยบายหนี้สาธารณะ สำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง ที่ได้ให้ความช่วยเหลือและให้ความรู้และข้อคิดเห็นเกี่ยวกับการเงินและแบบสอบถามสำหรับเก็บข้อมูลจากกลุ่มตัวอย่าง

ขอขอบพระคุณผู้เชี่ยวชาญ ดร.วศิน พิพัฒนฉัตร ผู้จัดการโครงการหน่วยวิชาการเครือข่ายนักจัดการปัจจัยเสี่ยง มหาวิทยาลัยมหิดล และ ทนาย บริษัท นิติหาญ จำกัด ที่ได้ให้ความช่วยเหลือและให้ความรู้และข้อคิดเห็นเกี่ยวกับกฎหมายและแบบสอบถามสำหรับเก็บข้อมูลจากกลุ่มตัวอย่าง

ขอขอบพระคุณผู้เชี่ยวชาญ อาจารย์ศรัญญา แจ้งขำ คณะกรรมการบริหารความเสี่ยง มหาวิทยาลัยธนบุรี ที่ได้ให้ความช่วยเหลือและให้ความรู้และข้อคิดเห็นเกี่ยวกับการจัดการและบริหารความเสี่ยงและแบบสอบถามสำหรับเก็บข้อมูลจากกลุ่มตัวอย่าง

ขอขอบพระคุณผู้เชี่ยวชาญทั้ง 3 ท่าน ที่ให้ความร่วมมือ พร้อมทั้งสละเวลาอันมีค่าเพื่อให้ได้มาซึ่งข้อมูลประกอบการวิจัยในครั้งนี้

ท้ายที่สุดนี้ผู้วิจัยขอกราบขอบพระคุณบิดา มารดา และ อาจารย์ชลิตา ชยุตรากรณ์ ซึ่งสนับสนุนในด้านการเงิน และ ด้านความรู้ต่างๆ และ ให้กำลังใจแก่ผู้วิจัยเสมอมาจนสำเร็จการศึกษา

ณศรัณย์ ขำหาญ

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญรูปภาพ

สารบัญภาพ (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ประเทศไทยกำลังก้าวเข้าสู่ยุคดิจิทัลและผลักดันนโยบายเศรษฐกิจดิจิทัลด้วยการส่งเสริมให้มีการใช้ประโยชน์จากเทคโนโลยีสารสนเทศและการสื่อสารเทคโนโลยีดิจิทัลและนวัตกรรมในทุกภาคส่วนทั้งภาครัฐ ภาคอุตสาหกรรม ภาคเอกชนและประชาชนซึ่งเทคโนโลยีดิจิทัลที่มีการใช้งานมากที่สุดคือการใช้อินเตอร์เน็ตจนอาจกล่าวได้ว่าชีวิตในสังคมสารสนเทศ ทุกวันนี้เราทุกคนล้วนเกี่ยวข้องกับอินเตอร์เน็ตในทางใดทางหนึ่งแม้จะไม่ใช่ผู้ใช้อินเตอร์เน็ตโดยตรงก็ตาม ในขณะที่อินเตอร์เน็ตนำมาซึ่งโอกาสในการขับเคลื่อนไปสู่เศรษฐกิจดิจิทัลไม่ว่าจะเป็นการส่งเสริมการเรียนรู้การศึกษาการสร้างธุรกิจใหม่ การส่งเสริมด้านสุขภาพ ธุรกรรมการเงินและการขนส่งคมนาคมแล้ว อินเตอร์เน็ตก็ยังเป็นเครื่องมือในการก่อให้เกิดภัยคุกคามไซเบอร์และการก่ออาชญากรรมไซเบอร์ ซึ่งเป็นภัยคุกคามที่ไร้พรหมแดนและมีผลกระทบในทุกมิติไม่ว่าจะเป็นเศรษฐกิจสังคมและความมั่นคงของประเทศ ยิ่งไปกว่านั้นภัยคุกคามทางไซเบอร์เป็นปัญหาสำคัญที่กระทบต่อความปลอดภัยในภาคการเงินทั่วโลก แม้เทคโนโลยีดิจิทัลจะช่วยให้ผู้คนใช้ชีวิตประจำวันได้สะดวกสบายขึ้นทั้งการใช้สื่อโซเชียลและการซื้อสินค้าหรือการโอนเงินออนไลน์แต่ความเสี่ยงในการเกิดอาชญากรรมทางไซเบอร์ทั้งการโจรกรรมข้อมูล การยักยอกเงินจากอินเตอร์เน็ตแบงค์กิ้งและเงินดิจิทัลกลับเพิ่มมากขึ้น และเป็นความเสี่ยงสำคัญของระบบการเงินโลกการดูแลความปลอดภัยทางไซเบอร์จึงเป็นเรื่องสำคัญ (World Economic Forum,2023) จัดเรื่องภัยคุกคามทางไซเบอร์เป็น 1 ใน 5 ความเสี่ยงสำคัญระดับโลก ซึ่งภาคการเงินเป็นเป้าหมายหลักของการถูกโจมตี ดังปรากฏในข่าวอยู่บ่อยครั้ง เช่น กรณีธนาคารกลางแห่งหนึ่งในเอเชียใต้ที่ถูกยักยอกเงินสำรองระหว่างประเทศกว่า 81 ล้านดอลลาร์สหรัฐอเมริกาจากการถูกเจาะเข้าระบบการโอนเงินเมื่อปี 2559 เช่นเดียวกับอีกธนาคารกลางหนึ่งในอาเซียนที่ประสบเหตุคล้ายกันแต่โชคดีที่พบความผิดปกติได้ทันเวลา ภัยไซเบอร์ที่มีแนวโน้มจะเกิดมากขึ้น หน่วยงานกำกับดูแลและองค์กรทั่วโลกจึงตื่นตัวกับการเร่งยกระดับการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างจริงจัง โดยมีการออกกฎหมายและแนวทางการกำกับดูแลเพื่อลดความเสี่ยงดังกล่าว เช่น สหภาพยุโรปออกกรอบการดูแลความปลอดภัยไซเบอร์ของภาคอุตสาหกรรมในยุโรป (Directive on Security of Network and Information Systems) และกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลของพลเมืองสหภาพยุโรป (General Data Protection Regulation) ขณะที่สหรัฐอเมริกาได้จัดทำกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของสหรัฐอเมริกา

(National Institute of Standards and Technology Cyber Security Framework) ซึ่งเป็นกรอบมาตรฐานสากลที่ถูกนำมาใช้อย่างแพร่หลายในองค์กรต่างๆ ทั่วโลกรวมรวมถึงในประเทศไทยด้วย

ปัจจุบันการทำธุรกรรมทางการเงินสามารถทำผ่านช่องทางการให้บริการทางการเงินได้หลากหลาย เช่น สาขาอิเล็กทรอนิกส์ช่องทางดิจิทัลเพื่ออำนวยความสะดวกต่อผู้ใช้บริการให้เข้าถึงบริการทางการเงิน และ การชำระค่าสินค้าบริการได้หลากหลายรูปแบบ สะดวก รวดเร็ว และครอบคลุมพื้นที่การใช้บริการมากขึ้น ธนาคารแห่งประเทศไทย (2566) ได้เผยแพร่ความรู้รูปแบบภัยทางการเงินด้วยกลโกงออนไลน์ประเภทต่างๆ พบว่ารูปแบบกลโกงออนไลน์มีหลายรูปแบบ จำแนกได้เป็น 1) หลอกให้ติดตั้งมัลแวร์ในอุปกรณ์โดยส่วนใหญ่การโจมตีด้วยมัลแวร์นี้ มิจฉาชีพมักจะส่ง SMS หรือ อีเมลล์ โดยแนบลิงค์ที่แฝงมัลแวร์ไว้และใช้ข้อความหลอกล่อให้คลิกลิงค์แนบเพื่อที่จะฝังมัลแวร์ลงบนอุปกรณ์ของเรา เช่น คอมพิวเตอร์หรือสมาร์ตโฟน 2) ฟิชชิง (Phishing) สร้างอีเมลล์และเว็บไซต์ปลอมขึ้นมาเพื่อหลอกเอาข้อมูลจากเหยื่อหรือหลอกขอรหัสผ่านการใช้งานบัญชีอีเมลล์ มิจฉาชีพจะส่งอีเมลล์แอบอ้างเป็นผู้ให้บริการบัญชีอีเมลล์ หลอกขอชื่อบัญชีผู้ใช้งาน (Email Address) และรหัสผ่าน (Password) โดยอ้างว่าเจ้าของอีเมลล์จะต้องยืนยันการใช้งานอีเมลล์และใช้รหัสผ่านที่ได้มาเข้าใช้งานบัญชีอีเมลล์แทนเจ้าของอีเมลล์นั้นซึ่งถือได้ว่าเป็นเหยื่อคนที่ หนึ่ง เมื่อเข้าใช้งานในบัญชีอีเมลล์ของเจ้าของบัญชีอีเมลล์ที่กลายเป็นเหยื่อคนที่หนึ่งได้แล้ว มิจฉาชีพก็จะส่งอีเมลล์ไปหาเพื่อนของเจ้าของบัญชีอีเมลล์แล้วหลอกขอให้เพื่อนโอนเงินให้ เช่น อ้างว่าเจ้าของบัญชีอีเมลล์ไปต่างประเทศแล้วกระเป๋าเงินหาย จึงต้องการความช่วยเหลือเรื่องเงินโดยด่วนโดยมักจะให้โอนเงินบริการรับโอนซึ่งไม่จำเป็นต้องมีเอกสารแสดงตนในการรับเงินในต่างประเทศซึ่งทำให้เจ้าหน้าที่ไม่สามารถติดตามจับคนร้ายได้และเพื่อนก็สูญเงินโดยไม่มีโอกาสได้คืนกลายเป็นเหยื่อคนที่สอง 3) โฆษณาปล่อยเงินกู้นอกระบบ มิจฉาชีพแอบอ้างเป็นผู้ให้บริการเงินกู้แล้วโฆษณผ่านเว็บไซต์ต่างๆ หรือส่งอีเมลล์หาเหยื่อโดยตรงว่าให้บริการเงินกู้นอกระบบดอกเบี้ยต่ำอนุมัติเงินเร็ว ไม่ต้องซื้อสินค้า ไม่ตรวจสอบเครดิตบูโร เมื่อเหยื่อติดต่อไปและขอกู้เงิน ผู้ให้กู้จะอ้างว่าจะส่งสัญญาให้กับผู้ขอกู้เพื่อลงลายมือชื่อ พร้อมทั้งขอให้เหยื่อโอนเงินชำระค่าทำสัญญา ค่าเอกสาร ค่ามัดจำ หรือดอกเบี้ยภายในเวลากำหนด เช่น ก่อน 18.00 น. เพื่อให้ผู้ให้กู้โอนเงินกู้ให้ก่อนเวลา 20.00 น. โดยสามารถยกเลิกและขอเงินโอนล่วงหน้าดังกล่าวคืนได้มิจฉาชีพมักโฆษณาว่าปล่อยกู้นอกระบบดอกเบี้ยต่ำเกินจริง หรือบางรายต่ำกว่าดอกเบี้ยเงินกู้ในระบบและให้ติดต่อผ่านโทรศัพท์หรืออีเมลล์เท่านั้น แม้กระทั่งขั้นตอนการทำสัญญาเงินกู้ ผู้ขอกู้ก็จะไม่มีโอกาสได้เจอผู้ให้กู้เลย เหยื่อส่วนมากมักจะรีบร้อนและกลัวว่าจะไม่ได้เงินกู้ จึงรีบโอนเงินให้กับผู้ให้กู้ในเวลาที่กำหนด แต่เมื่อติดต่อกลับผู้ให้กู้เพื่อขอรับเงินกู้ กลับไม่ได้รับการติดต่อผู้ให้กู้ได้อีกเลยและสูญเงินไปโดยไม่มีโอกาสได้เงินคืน และ 4) การขโมยตัวตนหรือ

แอบอ้างสวมรอยเป็นผู้อื่น เพื่อทำการหลอกลวงให้ทำธุรกรรมการเงินออนไลน์ให้แก่ บุคคลที่แอบอ้างสวมรอย ซึ่งการขโมยตัวตนในโลกออนไลน์นั้นมักจะทำร่วมกับสิ่งที่ไม่ดีอื่นๆแอบแฝง เช่น การปลอมแปลงเว็บไซต์เพื่อที่จะหลอกข้อมูลชื่อผู้ใช้และรหัสผ่านจากผู้ใช้แล้วนำข้อมูลที่ได้มาปลอมแปลงอีกครั้งเพื่อ นำไปหลอกลวงผู้ใช้งานอื่นๆ อีกทอดหนึ่งไปจนถึงการทำให้ได้รับความเสื่อมเสียชื่อเสียงอับอายและเสียทรัพย์สินหรือตกเป็นผู้ต้องสงสัยในคดีอาญา บางกรณีบรรดาแฮ็กเกอร์ก็ใช้วิธีการคาดเดารหัสผ่านที่มีการคาดเดาได้ง่ายซึ่งเป็นอีกวิธีที่ทำให้ผู้ใช้บริการถูกขโมยตัวตนทางออนไลน์ไปใช้แบบไม่รู้ตัว รหัสผ่านที่ตั้งรหัสจากตัวเลขวันเดือนปีเกิดหรือกรณีการละเลยจากตนเองปล่อยให้มีการเข้าสู่ระบบล็อคอินคอมพิวเตอร์ในเว็บไซต์ต่างๆทิ้งไว้ในร้านคอมพิวเตอร์ หรือคอมพิวเตอร์สาธารณะหรืออุปกรณ์อื่นๆ โทรศัพท์มือถือและเมื่อมีผู้ไม่สงค์ดีมาพบข้อมูลของเราก็จะถูกขโมยไปต่อเนื่องจนถึงการถูกสวมรอยเพื่อเข้าถึงบัญชีธนาคารหรือการทำธุรกรรมที่ผิดกฎหมาย

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีและสมาคมธนาคารไทย (2566) กล่าวว่า แนวโน้มภัยไซเบอร์มีอัตราการเติบโตแบบก้าวกระโดดและมีวิวัฒนาการไปตามเทคโนโลยี ซึ่งรูปแบบการหลอกลวงเริ่มตั้งแต่เงินสด โอนเงิน และไปสู่สกุลเงินคริปโตเคอร์เรนซี เป็นต้น ซึ่งมีการคาดการณ์ว่าภายใน 5 ปี ข้างหน้า การทุจริตที่เกิดจากภัยไซเบอร์จะขึ้นเป็นอันดับ 1 ของโลก และทวีความรุนแรงเพิ่มขึ้น ซึ่งในปัจจุบันต้องยอมรับว่าเทคโนโลยีที่มีความก้าวหน้ายังคงมีช่องโหว่ให้มิจฉาชีพและการตรวจจับยังตามหลังมิจฉาชีพ หากดูข้อมูลสถิติการแจ้งความออนไลน์สะสมนับตั้งแต่วันที่ 1 มี.ค. 2565 – 28 มิ.ย. 2566 พบว่ามีคดีออนไลน์ทั้งสิ้น 285,917 คดี แบ่งเป็นคดีที่เชื่อมโยงกันทั้งสิ้น 145,322 คดี และ คดีที่ไม่เชื่อมโยงกันอยู่ที่ 140,537 คดี ยอดมลูค่าความเสียหายอยู่ที่ราว 4 หมื่นล้านบาทโดยหากดูประเภทคดีที่เกิดขึ้นมากที่สุดตั้งแต่ 17 มี.ค. 2565 – 28 มิ.ย. 2566 ใน 5 อันดับแรก คือ 1) คดีหลอกซื้อขายสินค้าและบริการจำนวน 299 คดีต่อวัน มลูค่าความเสียหาย 4.3 ล้านบาทต่อวัน 2) คดีหลอกให้โอนเงินเพื่อทำงานหารายได้พิเศษ จำนวน 78 เรื่องต่อวัน มลูค่าความเสียหาย 9.8 ล้านบาทต่อวัน 3) คดีหลอกให้กู้เงิน จำนวน 65 คดีต่อวัน มลูค่าความเสียหาย 3 ล้านบาทต่อวัน 4) คดี Call Center จำนวน 36 คดีต่อวัน มลูค่าความเสียหาย 16.5 ล้านบาทต่อวัน และคดีประเภทอื่นๆ อาทิ หลอกเป็นผู้อื่นเพื่อยืมเงิน 9,664 คดี หลอกให้โอนเงินเพื่อรับรางวัล ฯ 8,697 คดี หลอกลวงซื้อสินค้าและบริการเป็นขบวนการ 8,107 คดี หลอกให้ติดตั้งโปรแกรมควบคุมระบบ ฯ 4,768 คดี หลอกให้ลงทุนตามพรบ.กู้ยืมเงิน 3,080 คดี กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ 2,972 คดี หลอกให้รักแล้วโอนเงิน 2,167 คดี หลอกเกี่ยวกับทรัพย์สินดิจิทัล 1,229 คดี เข้ารหัสคอมพิวเตอร์ของผู้อื่น 79 คดี

จากความสำคัญปัญหาภัยคุกคามทางไซเบอร์ของผู้ใช้ธุรกรรมการเงินออนไลน์ที่นับวันจะเพิ่มปัญหาจำนวนมากขึ้นในกลุ่มผู้ใช้บริการธุรกรรมการเงินออนไลน์ ทำให้ผู้วิจัยสนใจศึกษาปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ใน

กรุงเทพมหานครมีปัจจัยใดบ้าง เพื่อนำไปใช้ประโยชน์การวางแผนหรือการบริหารจัดการภัยทุจริตทางธุรกรรมการเงินต่อไป

1.2 วัตถุประสงค์

1.2.1 เพื่อศึกษาปัจจัยทางด้านลักษณะประชากรที่มีผลต่อความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และด้านประสบการณ์ภัยคุกคามไซเบอร์ ความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์

1.2.2 เพื่อหาปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์

1.3 สมมุติฐานการวิจัย

1.3.1 ปัจจัยทางด้านลักษณะประชากรส่งผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์

1.3.2 ปัจจัยทางลักษณะประชากรส่งผลต่อด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์

1.3.3 ปัจจัยทางลักษณะประชากรส่งผลต่อด้านด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์

1.4 ขอบเขตของการวิจัย

การวิจัยครั้งนี้กำหนดขอบเขตของการวิจัยดังนี้

1.4.1 ขอบเขตด้านเวลา : การวิจัยครั้งนี้เก็บรวบรวมข้อมูลในช่วงเดือน มกราคม – มีนาคม พ.ศ. 2567

1.4.2 ขอบเขตด้านประชากร : การวิจัยครั้งนี้ศึกษากับผู้ใช้บริการธุรกรรมการเงินออนไลน์ อายุ 15 ปี ขึ้นไปและอาศัยในเขตกรุงเทพมหานครเท่านั้น

1.4.3 ขอบเขตด้านตัวแปร : ตัวแปรที่ศึกษา คือ ลักษณะทางประชากร ความรู้ เกี่ยวกับภัยคุกคามทางไซเบอร์ ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ และ ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

1.5 นิยามศัพท์เฉพาะ

1.5.1 การทำธุรกรรมการเงิน หมายความว่า การทำธุรกรรมทางการเงินที่ผู้ให้บริการทางการเงินให้บริการ เช่น การเปิดบัญชีการสมัครใช้บริการการฝากเงิน การถอนเงิน การโอนเงิน และการชำระค่าสินค้า และบริการ โดยผ่านช่องทางการให้บริการครอบคลุม สาขาทั่วไป สาขาอิเล็กทรอนิกส์ ช่องทางดิจิทัล (Digital Channels) หรือ ช่องทางการให้บริการอื่นที่ธนาคารแห่งประเทศไทยอนุญาตเพิ่มเติมทั้งที่เป็นการทำธุรกรรมทางการเงินผ่านบัตร บริการเงินอิเล็กทรอนิกส์ หรือ ผ่านสื่ออื่น เช่น QR Code

1.5.2 สาขาอิเล็กทรอนิกส์ หมายความว่า ช่องทางการให้บริการที่มีสถานที่ตั้งหรือสถานที่ทำการแน่นอน ด้วยเครื่องอิเล็กทรอนิกส์ โดยผู้ใช้บริการดำเนินการด้วยตนเอง ซึ่งผู้ให้บริการทางการเงินอาจจัดให้มีพนักงาน คอยให้คำแนะนำหรือช่วยเหลือผู้อื่นผู้ใช้บริการในการใช้เครื่องอิเล็กทรอนิกส์ดังกล่าว เช่น เครื่องถอนเงินสดอัตโนมัติ (Automatic Teller Machine : ATM) หรือ เครื่องฝากเงินสดอัตโนมัติ (Cash Deposit Machine : CDM) ทั้งนี้ ไม่รวมถึงเครื่องอิเล็กทรอนิกส์ที่ให้บริการภายในหรือหน้าสาขาทั่วไป

1.5.3 ช่องทางดิจิทัล หมายความว่า ช่องทางให้บริการที่เป็นการให้บริการทางอินเตอร์เน็ต (Internet Banking) อุปกรณ์เคลื่อนที่ (Mobile Banking) และ ช่องทางดิจิทัลอื่นๆ ที่ธนาคารแห่งประเทศไทยอนุญาตเพิ่มเติม

1.6 กรอบแนวคิดการวิจัย

ตัวแปรอิสระ คือ ปัจจัยทางด้านลักษณะประชากร เช่น เพศ อายุ ระดับการศึกษา และรายได้ ส่งผลต่อตัวแปรตาม ได้แก่ ประสบการณ์ ความรู้ และ ความตระหนักรู้เกี่ยวกับภัยคุกคามไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ดังภาพที่ 1-1

ภาพที่ 1-1 กรอบแนวคิดการวิจัย

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1.7.1 สถาบันการเงินและหน่วยงานที่เกี่ยวข้องอื่นๆ สามารถนำผลการวิจัยไปใช้ในการวางแผนสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

1.7.2 สถาบันการเงินและหน่วยงานที่เกี่ยวข้องอื่นๆ สามารถนำผลการวิจัยไปใช้ในการบริหารจัดการภัยทุจริตจากการทำธุรกรรมการเงินออนไลน์

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

การวิจัยเรื่อง “ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร” นี้ ได้ทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง เพื่อสร้างกรอบแนวคิดของงานวิจัย ดังหัวข้อต่อไปนี้

2.1 แนวคิดและทฤษฎีเกี่ยวข้องกับด้านประชากรศาสตร์ (Demography)

2.2 แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

2.3 แนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์ (Cyber Threat)

2.4 แนวคิดและทฤษฎีเกี่ยวกับความรู้ (Knowledge)

2.5 แนวคิดเกี่ยวกับความตระหนักรู้ (Awareness)

2.6 งานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎีที่เกี่ยวข้องกับด้านประชากรศาสตร์ (Demography)

ประชากรศาสตร์ หมายถึง การทำความเข้าใจเกี่ยวกับมนุษย์ที่เกี่ยวข้องกับ ปัจจัยทางสังคม วัฒนธรรม เศรษฐกิจ และปัจจัยอื่นๆ ลักษณะทางประชากรศาสตร์ประกอบไปด้วย เพศ อายุ ระดับการศึกษา และ รายได้ ฯลฯ (สันทัด เสริมศรี, 2541 อ้างอิงใน สุธาเทพ รุณเรศ, 2561)

นอกจากนี้แนวความคิดด้านประชากรศาสตร์ เป็นทฤษฎีที่เกี่ยวข้องกับหลักการเป็นเหตุผล ซึ่งเป็นพฤติกรรมของมนุษย์ที่อาจจะเกิดขึ้นจากปัจจัยภายนอกได้ เช่น แรงบังคับจากภายนอกมากระตุ้น และเมื่อกล่าวถึงประชากรที่แตกต่างกันจะนำไปสู่พฤติกรรมและการตัดสินใจที่แตกต่างกันไปด้วย (วศินสันหกรณ์,2557 อ้างอิงใน สุธาเทพ รุณเรศ,2561) ส่วนแนวคิดด้านประชากรศาสตร์นั้น จะสามารถจำแนกประชากรออกเป็นกลุ่มๆได้จากลักษณะ และ พฤติกรรม เช่น กลุ่มคนที่มีลักษณะและบุคลิกใกล้เคียงกันจะอยู่ในกลุ่มเดียวกันรวมไปถึงบุคคลที่อยู่ในชนชั้นทางสังคมเดียวกันก็มีแนวโน้มที่จะตอบสนองถึงข่าวสารความต้องการไปในทิศทางเดียวกัน และ ปัจจัยการเปลี่ยนแปลงของประชากรอาจจะมาจากปัจจัยทางเศรษฐกิจ สังคมและวัฒนธรรมอีกด้วย ซึ่งอาจกล่าวได้ว่า แนวความคิดของประชากรศาสตร์สามารถจำแนกและอธิบายถึงคุณสมบัติเฉพาะตนของคนนั้นๆ ซึ่งมีผลต่อกับการสื่อสารกับผู้รับสารในสถานการณ์ต่างๆและในการสื่อสารแต่ละครั้งถ้าผู้รับสารมีจำนวนอยู่ก็อาจจะไม่ส่งผลให้เกิดปัญหาได้เพราะเราสามารถวิเคราะห์ผู้รับสารได้ทุกคนแต่ถ้าในทางกลับกัน บางสถานการณ์ผู้รับสารมีจำนวนมากเราจะไม่สามารถวิเคราะห์ผู้รับสารได้อย่างละเอียดถี่ถ้วน ดังนั้น

การจำแนกผู้รับสารออกเป็นกลุ่มๆ มีแนวโน้มทำให้ง่ายต่อการสื่อสารมากขึ้นโดย สามารถจำแนกตามลักษณะประชากร (Demographic Characteristics) ได้ดังนี้

- เพศ
- อายุ
- ระดับการศึกษา
- รายได้

ปัจจัยเหล่านี้อาจส่งผลกระทบต่อ การตีความ การรับรู้ ความเข้าใจในการสื่อสาร ข้อมูล ด้านประชากรจะมีประสิทธิภาพและเข้าถึงมากที่สุดก็ต่อเมื่อกำหนดกลุ่มเป้าหมายที่ชัดเจน ซึ่งคนที่มีลักษณะทางประชากรที่แตกต่างกันก็จะมีลักษณะทางจิตวิทยาที่ต่างกันได้

2.2 แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ให้ความหมาย “การรักษาความมั่นคงปลอดภัยไซเบอร์” ไว้หมายความว่า “มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ” (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ Electronic Transactions Development Agency, 2560)

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช. หรือ NSTDA) ให้ความหมายไซเบอร์ ว่าเป็น คำที่กร่อนมาจากคำว่าไซเบอร์เนติกส์ (Cybernetics) และ มีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเตอร์เน็ต (Internet) และยังมีการให้ความหมาย “สารสนเทศ (Virtual) เสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง” (www.nstda.or.th, 2557)

โดยรวมแล้วความมั่นคงปลอดภัยจึงเป็นความหมายในเชิงนามธรรม หมายถึง ขอบเขตที่เกี่ยวข้องกับการใช้งานของระบบเครือข่ายคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ ซึ่งจะครอบคลุมมากกว่าคอมพิวเตอร์ซึ่งมีความหมายในเชิงรูปธรรมของอุปกรณ์ระบบคอมพิวเตอร์ทั่วไป

ตามพจนานุกรมพื้นที่การปฏิบัติการไซเบอร์ของกระทรวงกลาโหมสหรัฐอเมริกา กำหนดให้ ความมั่นคงปลอดภัย คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความมั่นคงปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ (ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ) ความมั่นคงปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง

ประมวลผล และกระจายข้อมูล ทั้งนี้ ความมั่นคงปลอดภัยยังรวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม อุบัติเหตุ และความผิดพลาดต่างๆ

ความเสี่ยงของความมั่นคงปลอดภัยทางไซเบอร์อาจรวมถึงสิ่งต่างๆ ที่ทำลายความเชื่อมั่นและความไว้วางใจของผู้มีส่วนได้ส่วนเสีย (Stakeholder) ผลกระทบที่มีต่อการเก็บรักษาและการเติบโตของกลุ่มลูกค้า การละเมิดการป้องกันข้อมูลส่วนตัวของกลุ่มลูกค้าและผู้ถือหุ้น การรบกวนการทำงานหรือการดำเนินธุรกรรมผลกระทบที่เป็นปฏิปักษ์ต่อชีวิตและสุขภาพของผู้ปฏิบัติงาน และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ (สุธาเทพ รุณเรศ, 2561)

2.3 แนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์ (Cyber Threat)

การคุกคามทางไซเบอร์สามารถเกิดขึ้นได้หลากหลายรูปแบบ แต่ละรูปแบบสามารถสร้างความเสียหายให้แก่บุคคล เศรษฐกิจ ไปจนถึงโครงสร้างพื้นฐานของแต่ละประเทศ ภัยคุกคามอาจจะทำให้เกิดการก่อวินาศกรรม การจารกรรมข้อมูลหรือรหัสสำคัญ การปล่อยข้อมูลลวง การทำลายชื่อเสียงของประเทศ องค์กร หรือบุคคล การเผยแพร่ข่าวสารอันเป็นเท็จ รวมถึงการทำลายระบบปฏิบัติการของคอมพิวเตอร์แม่ข่าย คอมพิวเตอร์ส่วนบุคคล และอุปกรณ์เคลื่อนที่

2.3.1 รูปแบบการโจมตีทางไซเบอร์

2.3.1.1 มัลแวร์ เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อรบกวนหรือขโมยข้อมูลจากระบบคอมพิวเตอร์ เครือข่าย หรือ คอมพิวแม่ข่าย โดยแฮกเกอร์มักล่อลวงเป้าหมายด้วยวิธีการต่างๆ แล้วฝังมัลแวร์ลงไปในอุปกรณ์เปิดทางเข้าถึงข้อมูลหรือเข้าควบคุมระบบของเป้าหมายได้ การใช้ มัลแวร์โจมตีเป็นวิธีการหนึ่งที่แฮกเกอร์นิยมใช้ ซึ่ง มัลแวร์ มีหลายประเภทและมีคุณสมบัติต่างกัน ได้แก่

2.3.1.1.1 ไวรัสคอมพิวเตอร์ (Viruses) เป็นโปรแกรมชนิดหนึ่งที่ทำงานเหมือน “เชื้อไวรัส” ที่ไปติดไฟล์อื่นๆในคอมพิวเตอร์ ในคอมพิวเตอร์ สามารถเพิ่มจำนวนตัวเองและทำให้อุปกรณ์ที่ติดเชื้อทำงานช้าลงหรือทำลายไฟล์ข้อมูล การแพร่กระจายเชื้อไวรัสไปยังอุปกรณ์อื่นๆ นั้นจำต้องอาศัยไฟล์พาหะ เช่น อีเมลล์ที่แนบเอกสารไฟล์ที่มีไวรัส หรือ การทำสำเนา (Copy) ไฟล์ที่ติดไวรัสไว้บนคอมพิวเตอร์แม่ข่าย เป็นต้น

2.3.1.1.2 ม้าโทรจันคอมพิวเตอร์ (Trojans) เป็นโปรแกรมที่ซ่อนตัวอยู่ในรูปแบบโปรแกรมทั่วไป เพื่อหลอกให้คนดาวน์โหลดมาใช้งาน และทันทีที่มีการใช้งานโปรแกรมจะเข้าทำลายไฟล์ข้อมูล หรือเปิดประตูให้ผู้ไม่สงค์ดีเข้าควบคุมเครื่องจากระยะไกลได้

2.3.1.1.3 หนอนคอมพิวเตอร์ (Worm) เป็นโปรแกรมที่ถูกออกแบบมาให้แพร่กระจายตัวเองจากคอมพิวเตอร์เครื่องหนึ่งผ่านระบบเครือข่ายส่วนใหญ่หนอนคอมพิวเตอร์จะถูกฝังอยู่ในไฟล์แนบของอีเมลล์และสามารถสำเนาตัวเองเพื่อส่งต่อไปยังรายชื่อ (Contact) ที่อยู่ใน

อีเมลล์ของเครื่องคอมพิวเตอร์ที่ติดเชื้อ ทำให้หนอนคอมพิวเตอร์แพร่ได้อย่างรวดเร็ว สร้างความเสียหายรุนแรงกว่าไวรัสได้

2.3.1.1.4 แรนซัมแวร์ (Ransomware) เป็นมัลแวร์อีกประเภทหนึ่งที่ใช้ปิดกั้นการเข้าถึงข้อมูลสำคัญหรือระบบของเหยื่อ เพื่อทำการข่มขู่เรียกค่าไถ่หากไม่จ่าย แฮกเกอร์จะลบข้อมูลหรือปิดกั้นการใช้งานระบบ ก่อให้เกิดความเสียหายทั้งชื่อเสียงและเงินขององค์กรที่ตกเป็นเหยื่อ

2.3.1.1.5 สปายแวร์ (Spyware) เป็นโปรแกรมประเภทหนึ่งที่ถูกแอบติดตั้งไว้ในคอมพิวเตอร์เพื่อรวบรวมข้อมูลของผู้ใช้งาน แฮกเกอร์สามารถใช้ข้อมูลเหล่านี้เพื่อแบล็คเมลล์ หรือใช้ดาวน์โหลดหรือติดตั้งมัลแวร์ตัวอื่นๆ จากเว็บไซต์ เพื่อแสวงประโยชน์ต่อไป

2.3.1.2 ฟิชชิ่ง (Phishing) เป็นการหลอกลวงในโลกออนไลน์ที่พบได้มากที่สุด มีเป้าหมายเพื่อขอข้อมูลสำคัญด้วยวิธีการต่างๆ เช่น อีเมลล์ปลอม ข้อความหลอกลวงผ่านข้อความหรือเว็บไซต์ปลอม เป็นต้น โดยทั่วไปแล้ว ฟิชชิ่ง มี 3 รูปแบบ ได้แก่

2.3.1.2.1 สเปียร์ฟิชชิ่ง (Spear Phishing) กำหนดกลุ่มเป้าหมายการโจมตีเป็นบริษัทหรือบุคคลแบบเฉพาะเจาะจง

2.3.1.2.2 วาฬลิ่ง (Whaling) โจมตีเป้าหมายที่เป็นผู้บริหารระดับสูง หรือ ผู้ที่มีส่วนได้ส่วนเสียขององค์กรเป้าหมาย

2.3.1.2.3 ฟาร์มมิ่ง (Pharming) เป็นรูปแบบที่แฮกเกอร์เข้าไปโจมตีคอมพิวเตอร์แม่ข่ายของเว็บไซต์ต่างๆ แล้วเปลี่ยนลิงค์เว็บไซต์

2.3.1.3 การโจมตีแบบคนกลาง (Man in the Middle Attack) เป็นการที่ผู้ประสงค์ร้ายเข้ามาแทรกกลางระหว่างการสนทนา หรือทำธุรกรรมออนไลน์ของคนสองคน และทำหน้าที่เป็นตัวกลางรับส่งข้อมูลโดยที่ทั้งคู่ไม่รู้ตัว โดยทั่วไปแล้วผู้โจมตีแบบเป็นคนกลางมักจะใช้ช่องโหว่จากเครือข่าย Wi-Fi สาธารณะ และแทรกตัวอยู่ระหว่างผู้ใช้งานกับเครือข่ายต่างๆ เพื่อหลอกเอาข้อมูลสำคัญนอกจากนั้นแฮกเกอร์หลายรายมักใช้วิธี การโจมตีแบบคนกลางเพื่อส่งต่อ ฟิชชิ่ง หรือ มัลแวร์

2.3.1.4 การปฏิเสธการให้บริการแบบกระจาย (Distributed Denial of Service) เป็นการโจมตีระบบเป้าหมายด้วยการส่งคำขอเข้าไปจำนวนมาก จนทำให้ระบบปฏิบัติการหรือแอปพลิเคชั่นทำงานล่าช้าหรือหยุดชะงักชั่วคราวเหมือนกัน เพียงแต่การโจมตีแบบการปฏิเสธการให้บริการ นั้นเป็นการส่งคำขอเข้าระบบจำนวนมากจากคอมพิวเตอร์แค่เครื่องเดียว แต่ การปฏิเสธการให้บริการแบบกระจาย จะส่งคำขอจำนวนมากด้วยเครื่องคอมพิวเตอร์หลายเครื่องด้วย หุ่นยนต์ที่โดนควบคุมการโจมตี ซึ่งในระหว่างการโจมตีนั้น แฮกเกอร์อาจฝังมัลแวร์ เพื่อเจาะเข้าระบบหรือข้อมูลสำคัญขององค์กรด้วย ที่ผ่านมามีแอปพลิเคชั่นชื่อดังเคยถูกการปฏิเสธการให้บริการแบบกระจายมาแล้ว เช่น ทวิตเตอร์ และ ซาวคลาว์ เป็นต้น

2.3.1.5 การแทรกคำสั่งฐานข้อมูล (SQL Injection) เว็บไซต์ส่วนใหญ่ใช้ ฐานข้อมูล เก็บข้อมูลสำคัญ เช่น การเข้างานใช้งานระบบ รหัสผ่าน และ ข้อมูลบัญชี เป็นต้น ดังนั้น แฮกเกอร์อาศัยช่องโหว่ของโปรแกรมหรือเว็บไซต์แอบใส่คำสั่งฐานข้อมูล เข้าไปทางช่องกรอกข้อมูลเพื่อหลอกฐานข้อมูล แล้วดึงข้อมูลออกไป นอกจากนี้ยังสามารถใช้คำสั่ง เพิ่ม, อัพเดท, ลบ, ทิ้ง หรืออื่นๆ กับฐานข้อมูลได้อีกด้วย

2.3.1.6 การโจมตีจากช่องโหว่ที่ศูนย์วัน (Zero-day Exploit & Attack) เป็นการโจมตีระบบด้วยการแอบเข้าไปปล่อยมัลแวร์ผ่านช่องโหว่ที่มีอยู่ในซอฟแวร์ / เครือข่าย / ฮาร์ทแวร์ ที่แม้แต่ผู้พัฒนาหรือเจ้าของซอฟแวร์เองก็ไม่รู้ส่วนการโจมตีจากช่องโหว่ที่ศูนย์วัน หมายถึงการที่แฮกเกอร์ใช้ช่องโหว่ที่ศูนย์วัน สร้างความเสียหายหรือโจรกรรมข้อมูลจากอุปกรณ์ที่มีช่องโหว่ บริษัทเทคโนโลยียักษ์ใหญ่อย่าง ไมโครซอฟท์ กูเกิ้ล และ แอปเปิ้ล ต่างเคยต้องแก้ข้อผิดพลาดหรือช่องโหว่ในระบบหรือ ซอฟแวร์ มาแล้วทั้งนั้น

2.3.1.7 โจมตีรหัสผ่าน (Password Attack) เป็นการโจมตีทางไซเบอร์ ด้วยการเดารหัสผ่านหรือใช้วิธีการล่อลวงให้เป้าหมายเปิดเผยรหัสผ่าน โดยทั่วไปแล้ว โจมตีรหัสผ่านมี 3 รูปแบบได้แก่

2.3.1.7.1 โจมตีรหัสผ่านคาดเดาง่าย (Password Spraying Attack) เป็นการโจมตีกลุ่มเป้าหมายที่ใช้รหัสผ่าน ที่คาดเดาง่าย และเป็นที่นิยมอย่าง “123456” แล้วไล่โจมตีบัญชี (Account) ที่มีอยู่ทีละบัญชี ถ้าผ่านก็จะจดบันทึกไว้และไล่จนครบทุกบัญชีที่มีอยู่ในระบบรายชื่อ

2.3.1.7.2 การโจมตีแบบคาดเดารหัสผ่าน (Brute Force Attack) เป็นการสุ่มรหัสผ่านแบบลองผิดลองถูกไปเรื่อยๆ จนกว่าจะได้รหัสผ่านที่ตรงกับบุคคลหรือองค์กรเป้าหมาย

2.3.1.7.3 การหลอกลวงข้อมูล(Social Engineering) เป็นวิธีการที่แฮกเกอร์ใช้หลักจิตวิทยาหลอกล่อเป้าหมายให้บอกรหัสผ่าน เช่น การแจ้งเตือนผ่านแอป ฯ หลอกล่อให้ใส่ ชื่อผู้ใช้และ รหัสผ่าน หรืออีเมลล์ฟิชชิ่ง และ คอลเซ็นเตอร์ ที่โทรมาหลอกให้ทำธุรกรรมการเงิน เป็นต้น

2.3.1.8 การโจมตีแบบต้องมีการขับเคลื่อน (Drive by Attack) การโจมตีทางไซเบอร์ส่วนใหญ่จะสำเร็จได้นั้นต้องให้เป้าหมายดำเนินการบางอย่าง เช่น กดคลิกลิงค์ หรือ กดดาวน์โหลดไฟล์เอกสารแนบ แต่ การโจมตีแบบต้องมีการขับเคลื่อน นั้นจะแทรกคำสั่งที่เป็นอันตรายไปยังเว็บไซต์ ซึ่งอาจจะอยู่ในรูปแบบของเว็บลิงค์ เพียงคุณคลิกเปิดขึ้นมาอุปกรณ์ของคุณก็จะถูกติดตั้ง มัลแวร์ โดยไม่รู้ตัว

2.3.1.9 อินเตอร์เน็ตของสรรพสิ่ง (Internet of Things) เมื่อโลกมีการเชื่อมโยงกันมากขึ้นด้วยอินเตอร์เน็ตทำให้อุปกรณ์ต่างๆ เช่น ลำโพงอัจฉริยะ สมาร์ททีวี หรือแม้แต่กล้องวงจรปิด ตกเป็นเป้าหมายของแฮกเกอร์ เพื่อขโมยข้อมูลจากอุปกรณ์หรือใช้อุปกรณ์เหล่านั้นเป็น หุ่นยนต์ควบคุมการโจมตี เพื่อใช้ในการโจมตีเป้าหมายแบบ การปฏิเสธการให้บริการแบบกระจาย โดยทั่วไปแล้วอุปกรณ์

อินเตอร์เน็ตของสรรพสิ่ง ส่วนใหญ่ไม่มีการอัพเดท โปรแกรมป้องกันไวรัสคอมพิวเตอร์ ทำให้ติดตั้งมัลแวร์ และควบคุมจากระยะไกลได้ง่าย

2.3.1.10 การปลอมแปลงระบบชื่อโดเมน (DNS Spoofing) เป็นการปลอมแปลง ชื่อโดเมนเพื่อนำจราจรเครือข่ายที่พยายามเข้าเว็บไซต์ที่ถูกต้องส่งต่อไปยังเว็บไซต์ปลอมหรือเว็บไซต์มัลแวร์ หน้าตาของเว็บไซต์หลอกจะเหมือนเว็บไซต์จริงมาก เพื่อหลอกให้ผู้ใช้งานป้อนข้อมูลส่วนตัวที่สำคัญ แฮกเกอร์บางรายมักใช้การโจมตีรูปแบบนี้เป็นส่วนหนึ่งในการก่อวินาศกรรมองค์กรเป้าหมาย เช่น เปลี่ยนเส้นทางเว็บไซต์ขององค์กรไปยังเว็บไซต์อนาจารเพื่อสร้างความอับอาย เป็นต้น (ธนาคารแห่งประเทศไทย, 2565)

2.3.2 ลักษณะและผลของภัยคุกคามทางไซเบอร์

เอกสาร บทความความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Articles) 2012 ของไทยเซิร์ต ได้มีการจำแนกลักษณะและผลของภัยคุกคามทางไซเบอร์ไว้ 8 ด้าน ดังนี้ (สรณันท์ จิวะสุรัตน์ และชัยชนะ มิตรพันธ์,2555)

2.3.2.1 เนื้อหาที่เป็นภัยคุกคาม (Abusive Content) เป็นการใช้ข้อมูล หรือเผยแพร่ข้อมูลที่ไม่เป็นจริง หรือเป็นเท็จ หรือไม่เหมาะสม เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อก่อให้เกิดความไม่สงบหรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย การหมิ่นประมาท รวมถึงการโฆษณาขายสินค้าและบริการต่างๆ ทางอีเมลล์ที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้นๆ

2.3.2.2 การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability) เป็นการโจมตีเพื่อให้ระบบไม่อยู่ในสภาพความพร้อมใช้งาน เพื่อสร้างความเสียหายให้แก่ระบบให้บริการต่างๆ เช่น ทำให้เกิดความล่าช้า จนถึงขั้นที่ระบบไม่สามารถให้บริการต่อไปได้ อาจเป็นการโจมตีระบบโดยตรง เช่น การโจมตีแบบการปฏิเสธการให้บริการ หรือ เป็นการโจมตีที่โครงสร้างพื้นฐาน เช่น การให้บริการระบบไฟฟ้า ระบบน้ำประปา หรือ ระบบโทรศัพท์ เป็นต้น

2.3.2.3 การฉ้อโกง หรือ หลอกลวง เพื่อผลประโยชน์ (Fraud) เป็นความพยายามที่จะหาผลประโยชน์ด้วยการฉ้อโกง หรือ หลอกลวง สามารถเกิดในหลายลักษณะ เช่น การลักลอบใช้งานระบบ หรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาต เพื่อแสวงหาผลประโยชน์ หรือ การขายสินค้าหรือ ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ เป็นต้น

2.3.2.4 การรวบรวมข้อมูลของระบบ (Information Gathering) เป็นความพยายามในการรวบรวมข้อมูลระบบของผู้ไม่ประสงค์ดีหรือผู้โจมตีด้วยการเรียกใช้บริการต่างๆ ที่อาจเปิดไว้ในระบบ เช่นข้อมูลเกี่ยวกับระบบปฏิบัติการระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน ชื่ออีเมลล์ รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงต่างๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ

2.3.2.5 การบุกรุกระบบได้สำเร็จ (Intrusions) เป็นความพยายามที่สามารถเจาะเข้าระบบได้สำเร็จ และ ระบบถูกครอบครองหรือถูกบุกรุกโดยผู้ที่ไม่ได้รับอนุญาต

2.3.2.6 การเขียนโปรแกรมมุ่งร้าย (Malicious Code of Malware) คือ การเขียนโปรแกรมมุ่งร้ายหรือเป็นอันตรายต่อระบบ เช่น ขโมยข้อมูล และ/หรือส่งต่อไปยังเครื่องผู้อื่น ตัวอย่างโปรแกรมในกลุ่มนี้ ได้แก่ ไวรัสคอมพิวเตอร์ หนอนคอมพิวเตอร์ สปายแวร์ เป็นต้น

2.3.2.7 การเข้าถึง/เปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาตเป็นภัยคุกคามที่เกิดจากการที่ผู้ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized Access) หรือ เปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized Modification) ได้

2.4 แนวคิดและทฤษฎีเกี่ยวกับความรู้ (Knowledge)

เป็นเรื่องของญาณวิทยา (Epistemology) ซึ่งเกี่ยวข้องกับการกำเนิดของความรู้โครงสร้างความรู้ วิธีการของความรู้และความเที่ยงตรงถูกต้องของความรู้ ความรู้ในเชิงญาณวิทยาจึงไม่มีโครงร่างเชิงวัตถุ ซึ่งเป็นการยากที่จะนำตัวความรู้ไปจัดการต่างกับความรู้ในเชิงเทคโนโลยีที่มองความรู้เป็นข้อเท็จจริง ในรูปแบบที่สามารถนำไปประมวลทางคณิตศาสตร์ได้ เช่น ความรู้ที่อยู่ในรูปแบบของ สูตร สมการ กฎ ทฤษฎีกระบวนการ และ คำอธิบายให้เกิดความเข้าใจ ดังนั้น ตามแนวทางนี้ความรู้จึงสามารถนำไปจัดการความรู้มีอยู่ทั่วไปในส่วนที่ฝังอยู่ในตัวคนและอยู่ภายนอกตัวคน ในส่วนที่อยู่ภายนอกตัวคนซึ่ง

ได้มีการบันทึกเก็บไว้ในหน่วยบันทึกความรู้ในรูปแบบต่างๆ เช่น คู่มือ ตำราหรือ แฝง อยู่ในองค์การ ตัวผลิตภัณฑ์ และกระบวนการทำงานและการเรียนรู้ ซึ่งความรู้เหล่านี้จะมีคุณค่าก็ต่อเมื่อสามารถถูกนำไปใช้ให้เกิดประโยชน์ต่อบุคคล สถาบันและสังคมในบรรดาปัจจัยที่จำเป็นสำหรับการพัฒนานั้น ความรู้ทั้งในส่วนที่เป็นของปัจเจกบุคคลและของสถาบัน ถือเป็นปัจจับที่มีความสำคัญอย่างยิ่ง การมีการบริหารจัดการความรู้ที่ดีย่อมทำให้บุคคล สถาบัน และสังคมได้รับประโยชน์จากความรู้อย่างเต็มที่ และในการที่จะบริหารจัดการความรู้ให้มีประสิทธิภาพนั้น จำเป็นอย่างยิ่งที่จะต้องรู้และเข้าใจในธรรมชาติของความรู้ โดยต้องเข้าใจความหมายของความรู้และประเภทของความรู้ ดังนี้

ความหมายของความรู้ การแบ่งประเภทของความรู้ มองได้หลายมิติ แต่มิติที่ได้รับความนิยมมากที่สุด ได้แก่มองในด้าน “รูปแบบที่มองเห็น” ซึ่ง ชู (Choo,2000 : 26-28) ได้แบ่งความรู้เป็น 3 ประเภท ได้แก่

2.4.1 ความรู้โดยนัย (Tacit or Implicit Knowledge) หมายความถึงเป็นความรู้เฉพาะตัวที่เกิดจากประสบการณ์ การศึกษา การสนทนา การฝึกอบรม ความเชื่อ เจตคติของแต่ละบุคคล เป็นความรู้บวกกับสติปัญญา และประสบการณ์ ซึ่งถือได้ว่าเป็นองค์รวมของความรู้ของแต่ละบุคคล ซึ่งเป็นความรู้ที่ไม่อยู่นิ่ง จะปรับเปลี่ยนไปตามสถานการณ์ของการใช้ความรู้ของแต่ละคน ซึ่งความรู้ที่ผ่าน

กระบวนการขัดเกลาทางสังคม ถือว่าเมื่อคนปฏิบัติงานนานๆ จนเกิดความช่ำชอง ความรู้ประเภทนี้ถือเป็นความรู้ไม่เป็นทางการจัดระบบหรือจัดหมวดหมู่ไม่ได้ แต่สามารถแลกเปลี่ยนหรือนำมาเล่าสู่กันฟัง สามารถถ่ายทอดแบ่งปันความรู้นี้ได้และสามารถสังเกตและเลียนแบบได้ ซึ่งองค์การต้องพยายามปรับเปลี่ยนความรู้โดยนัย ให้เป็นความรู้ที่ปรากฏเพื่อเป็นความรู้ที่ฝังกับองค์การ (Embedded Knowledge) ไม่ยึดติดกับบุคคล

2.4.2 ความรู้ที่ปรากฏ (Explicit Knowledge) เป็นความรู้ที่ได้รับการถ่ายทอดจากบุคคลออกมาในรูปของบันทึกในรูปแบบต่างๆ ซึ่งก็คือ สารสนเทศ เช่น หนังสือ บทความ เอกสาร มาตรฐาน ลิขสิทธิ์ สิทธิบัตร เครื่องหมายการค้า ความลับทางการค้า รายงานประจำปี สื่อ โสตทัสน์ เช่น วิดิโอ สื่ออิเล็กทรอนิกส์ ซีดี เช่น ไปรษณีย์อิเล็กทรอนิกส์ อินเตอร์เน็ต เว็บไซต์อีบุค ความรู้ที่ปรากฏถือได้ว่ามีการใช้สัญลักษณ์ ไม่ว่าจะเป็นภาษาพูด ภาษาเขียนเพื่อบันทึกความรู้นั้นๆ ทำให้คนเข้าใจได้กว้างขวาง และสะดวกยิ่งขึ้นความรู้ที่มีการสะสมกันมานานเป็นความรู้ที่ใช้ประโยชน์ได้อย่างมีประสิทธิภาพและมีการตรวจสอบอย่างเป็นระบบ

2.4.3 ความรู้ที่เกิดจากวัฒนธรรม (Culture Knowledge) เป็นความรู้ที่เกิดจากความเชื่อความศรัทธา ซึ่งจะเกิดจากผลสะท้อนกลับของตัวความรู้ และ สภาพแวดล้อมขององค์การ องค์การที่พัฒนามาเป็นระยะเวลานานจะมีการพัฒนาความเชื่อร่วมกันในเรื่องที่เกี่ยวกับธรรมชาติขององค์การ ความสามารถหลักขององค์การ (Core Competency) ซึ่งก็คือวัฒนธรรมขององค์การ

สุชาติ วงษ์หุ่น (2539, น.28) กล่าวว่า ความรู้เป็นพฤติกรรมเบื้องต้นที่ผู้เรียนสามารถจดจำได้หรือระลึกได้ โดยการมองเห็นหรือได้ยิน ซึ่งความรู้ในที่นี้คือข้อเท็จจริง กฎเกณฑ์ คำจำกัดความ เป็นต้น โดยขั้นนี้ความรู้จึงเป็นพฤติกรรมขั้นต้นที่คนเราเพียงแต่จำได้ อาจจะโดยการนึกด้วยความรู้ขั้นนี้ ได้แก่ ความรู้เกี่ยวกับคำจำกัดความ ความหมาย ข้อเท็จจริง ทฤษฎี กฎโครงสร้าง และ วิธีการแก้ปัญหา ดังนั้น อาจกล่าวรวมๆ ได้ว่า ความรู้ หมายถึง การเรียนรู้ที่เน้นความจำ และ การระลึกถึงได้ของคนเราที่มีต่อความคิด ปรากฏการณ์ หรือวัตถุต่างๆ ความจำนี้อาจเริ่มจากสิ่งที่ง่ายไม่ซับซ้อนไปจนถึงเรื่องยุ่งยากซับซ้อนหลายขั้นได้ ซึ่ง ความรู้ เป็นการรับรู้เบื้องต้น ซึ่งบุคคลส่วนมากจะได้รับผ่านประสบการณ์ โดยการ เรียนรู้จากการตอบสนองต่อสิ่งเร้า (Simulus-Response) แล้วจัดระบบเป็นโครงสร้างของความรู้ที่ผสมผสานระหว่างความจำ (ข้อมูล) กับ สภาพจิตวิทยา ดังนั้น ความรู้ จึงเป็นความจำที่เลือกสรร ให้สอดคล้องกับสภาพจิตใจของตนเอง ความรู้จึงเป็นกระบวนการภายใน อย่างไรก็ตามความรู้อาจส่งผลต่อพฤติกรรมที่แสดงออกของมนุษย์ อาจปรากฏได้จากสาเหตุ 5 ประการ คือ (สุรพงษ์ โสธนะเสถียร, 2533, น. 120-121)

2.4.3.1 การตอบข้อสงสัย (Ambiguity Resolution) การสื่อสารมักสร้างความสับสนให้สมาชิกในสังคม ผู้รับสารจึงมักแสวงหาสารสนเทศโดยอาศัยสื่อทั้งหลาย เพื่อตอบข้อสงสัยและความสับสนของตน

2.4.3.2 การสร้างทัศนะ (Attitude Formation) ผลกระทบเชิงความรู้ต่อการปลูกฝังทัศนะนั้นส่วนมากนิยมใช้กับสารสนเทศที่เป็นนวัตกรรม เพื่อสร้างทัศนคติให้คนยอมรับการแพร่นวัตกรรมนั้นๆ(ในฐานะความรู้)

2.4.3.3 การกำหนดวาระ (Agenda Setting) เป็นผลกระทบเชิงความรู้ที่สื่อกระจายออกไปเพื่อให้ประชาชนตระหนักและผูกพันกับประเด็นวาระที่สื่อกำหนดขึ้น หากตรงกับภูมิหลังของปัจเจกชนและค่านิยมของสังคมแล้ว ผู้รับสารก็จะเลือกสารสนเทศนั้น

2.4.3.4 การพอกพูนระบบความเชื่อ (Expansion of The Belief System) การสื่อสารสังคมมักกระจายความเชื่อ ค่านิยม และอุดมการณ์ด้านต่างๆ ไปสู่ประชาชน จึงทำให้ผู้รับสารรับทราบระบบ ความเชื่อถือหลากหลาย และลึกซึ้งไว้ในความเชื่อของตนมากขึ้นเรื่อยๆ

2.4.3.5 การรู้แจ้งต่อค่านิยม (Value Clarification) ความขัดแย้งในเรื่องค่านิยมและอุดมการณ์เป็นภาวะปกติของสังคม สื่อมวลชนที่นำเสนอข้อเท็จจริงในประเด็นเหล่านี้ ย่อมทำให้เกิดประชาชนผู้รับสารเข้าใจถึงค่านิยมเหล่านั้นแจ้งชัดขึ้น

2.5 แนวคิดเกี่ยวกับความตระหนักรู้ (Awareness)

2.5.1 ความหมายของความตระหนักรู้

พจนานุกรมราชบัณฑิตสถาน พ.ศ.2542 ได้ให้ความหมาย “ความตระหนักว่า เป็นการรู้ประจักษ์ชัด รู้ชัดแจ้ง” นอกจากนั้น ยังมีผู้นิยามไว้อีก ดังนี้

กุลวดี ราชภักดี (2545, น.38) ได้ให้นิยามว่า “ความตระหนัก หมายถึง การที่บุคคลเกิดความรู้สึก นึกคิด ความคิดเห็นหรือประสบการณ์แล้วเกิดความเข้าใจแล้วประเมินสถานการณ์ที่เกี่ยวกับตนเองด้จากสภาวะจิตที่ยอมรับและเกิดแสดงพฤติกรรมตอบสนองต่อเหตุการณ์”

อนุสรณ์ กาลดิษฐ์ (2548, น.19) ได้ให้นิยามว่า “ความตระหนัก หมายถึง ความสำนึกของแต่ละบุคคลเคยมีการรับรู้หรือเคยมีความรู้มาก่อน มีสิ่งเร้ามากระตุ้นจนเกิดความตระหนักจากการประเมินค่า”

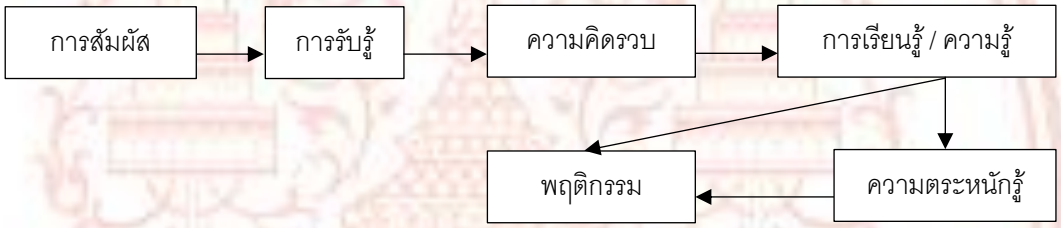
วีระชน ขาวผ่อง (2551, น.42) ได้ให้นิยามว่า “ความตระหนัก คือ สภาวการณ์มีผลให้เกิดความรู้สึก การรับรู้มุ่งสู่สภาวะจิตแห่งตน คือ ทัศนคติ ความคิด ความเชื่อ ความสมัครใจ อันจะก่อให้เกิดความตระหนักและจิตสำนึก”

พงษ์ชัย เฉลิมกลิ่น (2551, น.50) ได้ให้นิยามว่า “ความตระหนัก คือ พฤติกรรมที่แสดงถึงความรับผิดชอบต่อสิ่งใดสิ่งหนึ่งหรือเหตุการณ์ใดเหตุการณ์หนึ่ง ซึ่งเป็นอารมณ์ความรู้สึกด้านทัศนคติ ค่านิยม ความชอบ หรือไม่ชอบ ดีหรือไม่ดี ที่ได้จากการประเมินสิ่งเร้าต่างๆ ของบุคคลนั้น”

ทั้งนี้สามารถสรุปได้ว่า ความตระหนัก (Awareness) คือ การรับรู้แบบฉุกคิดขึ้นมากะทันหันต่อสิ่งใดสิ่งหนึ่งหรือเหตุการณ์ใดเหตุการณ์หนึ่งซึ่งเป็นอารมณ์ความรู้สึกโดยอาศัยองค์ประกอบจากสิ่งแวดล้อม ประสบการณ์ และสิ่งที่ส่งผลกับอารมณ์และความรู้สึกได้

2.5.2 ปัจจัยที่ทำให้เกิดความตระหนักรู้

กระบวนการเกิดความตระหนักมาจากกระบวนการทางปัญญา (Cognitive Process) ทั้งนี้เมื่อบุคคลได้รับการกระตุ้นจากสิ่งเร้าหรือรับสัมผัสจากสิ่งเร้าหรือประสบการณ์แล้วจะเกิดการรับรู้จากนั้นจะเข้าใจในสิ่งเร้านั้น และเกิดเป็นความคิดรวบยอด และทำให้มีความรู้และเมื่อมีความรู้ในสิ่งนั้นก็จะนำไปสู่การเกิดความตระหนัก ทั้งนี้ ความรู้ความตระหนักนี้ต่างก็จำนำไปสู่การกระทำ (Action) หรือการแสดงพฤติกรรมของบุคคลต่อสิ่งเร้านั้นๆ ดังภาพที่ 2-1



ภาพที่ 2-1 ขั้นตอนของกระบวนการเกิดความตระหนักรู้

ในลักษณะเช่นนี้นั้น ความตระหนักจึงเป็นผลของกระบวนการทางปัญญา กล่าวได้ว่า เมื่อบุคคลได้รับการกระตุ้นจากสิ่งเร้าแล้ว หรือ รับสัมผัสจากสิ่งเร้าแล้วเกิดการรับรู้ขึ้นแล้วจะนำไปสู่การเกิดความเข้าใจในสิ่งเร้านั้น และนำไปสู่การเรียนรู้เป็นขั้นตอนต่อไป และเมื่อบุคคลเกิดมีความรู้ในสิ่งนั้นแล้วก็จะมีผลไปสู่ความตระหนักในที่สุด ซึ่งทั้งความรู้และความตระหนักจะนำไปสู่การกระทำหรือพฤติกรรมของบุคคลที่มีต่อสิ่งเร้านั้นๆ ต่อไป

วิธีการสร้างความตระหนักรู้ทำได้ด้วยวิธีดังต่อไปนี้

1) การเผยแพร่ข้อมูล

2) สร้างข้อความที่มีผลกระทบสูง หรือ ข้อความที่กระตุ้นอารมณ์

3) สร้างข้อความที่เชื่อมต่อทัศนคติกับพฤติกรรมที่ผ่านมา

ลักษณะเฉพาะของแต่ละบุคคลมีผลต่อการรับรู้และการเกิดความตระหนักรู้ที่มุ่งเน้นการเปลี่ยนแปลงการรับรู้เกี่ยวกับกลุ่มหรือต่อวัตถุ รวมทั้งจะเกิดความตระหนักรู้ต่อสถานการณ์ที่จะส่งเสริมการเปลี่ยนแปลงทัศนคติต่างกัน

2.6 งานวิจัยที่เกี่ยวข้อง

นันท์ณิภัค นันทวัฒน์วงษ์ (2561) วิจัยเรื่อง “ความตระหนักความมั่นคงปลอดภัยด้านระบบสารสนเทศของหน่วยงานด้านการบิน กรณีศึกษา ท่าอากาศยานนานาชาติอุดรธานี กรมท่าอากาศยาน กระทรวงคมนาคม” พบว่า กลุ่มตัวอย่างส่วนใหญ่เป็นเพศชาย มีอายุระหว่าง 20-29 ปี ระดับการศึกษาปริญญาตรี เป็นบุคลากรชั่วคราว และมีอายุงานระหว่าง 1-5 ปี ความตระหนักความมั่นคงปลอดภัยด้านระบบสารสนเทศโดยภาพรวม อยู่ในระดับมาก โดยด้านที่มีค่าเฉลี่ยสูงสุด คือ ด้านความร่วมมือของเจ้าหน้าท่าอากาศยานนานาชาติอุดรธานี รองลงมาคือ ด้านทัศนคติความปลอดภัยระบบสารสนเทศ ด้านพฤติกรรมในการเข้าใช้ระบบสารสนเทศ ด้านความรู้ความเข้าใจความมั่นคงปลอดภัยระบบสารสนเทศ และ ด้านการรับรู้ข่าวสารด้านความปลอดภัยระบบสารสนเทศตามลำดับ โดยผลการทดสอบสมมติฐานพบว่า เจ้าหน้าที่ของท่าอากาศยานนานาชาติอุดรธานีที่มีอายุ และประเภทบุคลากรแตกต่างกัน มีความตระหนักความมั่นคงปลอดภัยด้านระบบสารสนเทศแตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

วิลาส วิถีไพร (2561) ได้วิจัยเรื่อง “การพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเตอร์เน็ตประสานสรรพสิ่ง” ผลการวิจัย จากการวิเคราะห์ความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเตอร์เน็ตประสานสรรพสิ่ง พบว่ามีความเสี่ยงมาก และการรักษาความมั่นคงปลอดภัยของหน่วยงานที่ใช้อินเตอร์เน็ตประสานสรรพสิ่งมีความเสี่ยงอยู่ในระดับปานกลาง จากข้อมูลที่ได้นำมาพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเตอร์เน็ตประสานสรรพสิ่ง ประกอบด้วย ฟังค์ชั่นหลัก 6 ด้าน 1.การกำหนดมาตรการด้านความมั่นคงปลอดภัย 2.การปกป้องดูแลด้านความมั่นคงปลอดภัย 3.การตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์ 4.การรับมือภัยคุกคามทางไซเบอร์ 5.การกู้คืน 6.การกำหนดมาตรฐานและฟังค์ชั่นย่อย สำหรับใช้ในการประเมินความเสี่ยงด้านไซเบอร์สำหรับอินเตอร์เน็ตประสานสรรพสิ่งในองค์กรโดยใช้แอปพลิเคชั่นระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเตอร์เน็ตประสานสรรพสิ่ง เพื่อให้บุคลากรขององค์กรนั้น ประเมินถึงมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเตอร์เน็ตประสานสรรพสิ่งที่ใช้อยู่ในองค์กรมีความเหมาะสมหรือมีความเสี่ยงมากน้องเพียงใด และนำผลการประเมินที่ได้มาเป็นข้อปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยขององค์กรต่อไป

สุธาเทพ รุณเรศ (2561) วิจัย เรื่อง “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเตอร์เน็ตในกรุงเทพมหานคร” พบว่าปัจจัยทางด้านลักษณะทางประชากรด้านอายุ ระดับการศึกษาสูงสุด และรายได้ส่วนตัวต่อเดือน มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเตอร์เน็ต แต่ปัจจัยทางด้านลักษณะทางประชากรด้านเพศ ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเตอร์เน็ต และเพื่อให้ทราบผลทางลักษณะประชากรที่ส่งผลต่อความตระหนัก

ภัยคุกคาม ที่ระบุได้จากกลุ่มตัวอย่าง ตรงกับสมมุติฐา และนำไปสร้างแนวทางกำหนดกลุ่มเป้าหมาย ถึงวิธีป้องกันและลดความเสี่ยงจากภัยคุกคามของการโจมตีทางไซเบอร์ สามารถสร้างความตระหนักและความเข้าใจที่จะเกิดผลกระทบต่อตนเองจากอุปกรณ์ต่างๆในการเข้าถึงอินเตอร์เน็ตนอกจากนี้ยังพบว่า ปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเตอร์เน็ต เนื่องจาก การโจมตีทางไซเบอร์มีรูปแบบการพัฒนาการโจมตีช่องโหว่ทางอินเตอร์เน็ตหลากหลายรูปแบบทำให้ผู้ใช้อินเตอร์เน็ตไม่สามารถระวังได้ถึงภัยคุกคามทางไซเบอร์และไม่สามารถป้องกันการโจมตีที่ไม่เหมือนเดิมและได้รับความเสียหายไม่คาดคิดแตกต่างจากครั้งก่อนทำให้ไม่สามารถประเมินสถานการณ์ที่จะเกิดความเสียหายขึ้นได้ นอกจากนี้ยังพบว่า ปัจจัยทางด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเตอร์เน็ต เนื่องจาก ผู้ที่มีความรู้ทราบถึงภัยคุกคามทางไซเบอร์ส่งผลกระทบต่อตนเอง สามารถเข้าใจถึงปัญหาที่จะเกิดความเสียหาย จากภัยคุกคามทางไซเบอร์ขึ้นล่วงหน้า ไม่ว่าจะเป็นการเปิดเผยข้อมูลบนสาธารณะ การทำธุรกรรมออนไลน์ การป้องกันให้ผู้อื่นไม่ทราบข้อมูลส่วนตัว และการติดตามข้อมูลข่าวสารการโจมตีรูปแบบใหม่ๆ การดาวโหลดโปรแกรมที่ถูกต้องมาจากผู้ผลิตโดยตรง ป้องกันความเสี่ยงการฝังไวรัสที่ไม่คาดคิดติดมากับโปรแกรมและสามารถป้องกันภัยคุกคามจากผู้ไม่หวังดีที่จะเกิดผลกระทบความเสียหายโดยไม่คาดคิดได้

กัลยา ชินาธิวร (2562) วิจัย เรื่อง “ปัจจัยความสำเร็จของสิงค์โปร์ : กรณีศึกษาเพื่อประกอบการพัฒนาแนวทางการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย ” ผลการวิจัย ปัจจัยที่ทำให้สิงค์โปรมีวิสัยทัศน์กว้างไกล เล็งเห็นถึงปัญหาและภัยคุกคามไซเบอร์ที่จะมาบั่นทอนโอกาสในการพัฒนาเศรษฐกิจและสังคมที่ต้องขับเคลื่อนด้วยการใช้เทคโนโลยีดิจิทัลและนวัตกรรมจึงได้ให้ความสำคัญกับเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีการดำเนินการอย่างจริงจัง ต่อเนื่องและเป็นระบบ โดยมีการดำเนินการในด้านต่างๆ ที่เป็นปัจจัยสำคัญของความสำเร็จ 5 ด้าน ได้แก่ ด้านกฎหมาย ด้านเทคนิค ด้านองค์กร ด้านการเสริมสร้างศักยภาพ ด้านความร่วมมือ

สกาวฟ้า จันทภาโส (2563) ได้วิจัยเรื่อง “การพัฒนาแอปพลิเคชั่น เพื่อสร้างความตระหนักรู้ เรื่องการระรานทางไซเบอร์ สำหรับนักเรียนชั้นมัธยมศึกษาปีที่ 1 ” ผลการวิจัย แอปพลิเคชั่น เพื่อสร้างความตระหนักรู้ เรื่องการระรานทางไซเบอร์ผู้วิจัยพัฒนาขึ้นมีประสิทธิภาพตามเกณฑ์ที่กำหนดไว้ นอกจากนี้ ผลการศึกษาผลสัมฤทธิ์ทางการเรียนของนักเรียนชั้นมัธยมศึกษาปีที่ 1 จากการเรียนรู้ผ่านแอปพลิเคชั่นเพื่อสร้างความตระหนักรู้เรื่องการระรานทางไซเบอร์ พบว่า คะแนนเฉลี่ยหลังเรียนสูงกว่าก่อนเรียนอย่างมีนัยสำคัญทางสถิติที่ระดับ0.01 และ พบว่านักเรียนมีความตระหนักรู้อยู่ในระดับมาก ร้อยละ 83.94 ค่าเฉลี่ย 4.20

สุรชัย ฉัตรเฉลิมพันธุ์ และ เทอดพงษ์ แดงสี (2563) ได้วิจัยเรื่อง “การเสริมสร้างความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในองค์กร : กรณีจำลองการโจมตีด้วยฟิชชิ่ง” ผลการวิจัย จากผล

การศึกษาในครั้งที่ 1 ที่จำลองการโจมตีนั้นพบว่า บุคลากรในองค์กรมีระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ที่ยังไม่จัดได้ว่าอยู่ในเกณฑ์ดี เพราะยังมีพนักงานหรือบุคลากรขององค์กรจำนวนหนึ่งที่ยังขาดความตระหนักถึงความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ อย่างไรก็ดีเมื่อมีการดำเนินการถ่าย ทอดความรู้เรื่องความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์ให้แก่บุคลากร แล้วทำการศึกษาซ้ำในครั้งที่ 2 พบว่าบุคลากรในองค์กรมีระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ที่ดีขึ้นอย่างชัดเจน คืออยู่ในเกณฑ์ดี แสดงว่าการถ่ายทอดความรู้เรื่องความตระหนักรู้เท่าทันภัยทางไซเบอร์ให้แก่บุคลากรที่ดำเนินการไปให้ผลลัพธ์ที่ดี และสามารถนำรูปแบบการดำเนินการที่ได้บรรยายไว้ในบทความนี้ไปประยุกต์ใช้ในการยกระดับความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์ในองค์อื่นๆ เพื่อเพิ่มความมั่นคงปลอดภัยทางไซเบอร์และบุคลากรในองค์กรอย่างไรก็ตามการยกระดับความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์ด้วยการจำลองการโจมตีด้วยอีเมลล์ฟิชชิ่งเพียงอย่างเดียวอาจไม่เพียงพอ ผู้บริหารจำเป็นที่จะต้องดำเนินการอย่างต่อเนื่องและครอบคลุมภัยทางไซเบอร์รูปแบบอื่นๆ ด้วย เช่น การโจมตีด้วยไวรัสเรียกค่าไถ่ ตลอดจนการโจมตีด้วยมัลแวร์ทุกรูปแบบ

กริน ธัญญาวิกรม และ ธีระ กุลสวัสดิ์ (2564) วิจัย เรื่อง “การจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ กรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย” ผลการวิจัย พบว่า ปัจจุบันการทำธุรกรรมทางการเงินของธนาคารพาณิชย์นั้น ได้ถูกขับเคลื่อนด้วยระบบดิจิทัลแบงกิ้ง (Digital Banking) แต่สิ่งที่มาพร้อมกับเทคโนโลยี คือ ภัยคุกคามไซเบอร์ ที่เพิ่มขึ้นอย่างรวดเร็วและมีความซับซ้อนมากขึ้น ส่งผลกระทบต่อทุกภาคส่วน จนเป็นปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญระดับชาติ ในด้านความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์และความพร้อมในการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ และจากมาตรการกำกับดูแลของรัฐ การดำเนินการและมาตรการต่างๆ ของธนาคารพาณิชย์ ในการรองรับปัญหาดังกล่าว

สุทธิพันธุ์ ชวลิตเลขา (2564) ได้วิจัยเรื่อง “การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด” พบว่า ปัจจัยด้านข้อมูลทั่วไปด้านประชากรไม่มีผลต่อการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ ซึ่งได้ข้อมูลจากการสัมภาษณ์เชิงลึกด้วยแบบสัมภาษณ์แบบกึ่งโครงสร้าง กับ การทำแบบสอบถามแบบปลายปิด โดยออกแบบคำถามออกเป็น 3 ส่วน ได้แก่ส่วนที่ 1 ข้อมูลทั่วไปบุคคลากรของกลุ่มตัวอย่าง ส่วนที่ 2 พฤติกรรมการใช้งานระบบอินเตอร์เน็ต ส่วนที่ 3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

สุพิตรา ศรีบุรินทร์ และ ทัชชกร แสงทองดี(2564) วิจัยเรื่อง “การตระหนักรู้ในการป้องกันตนเองบนโลกไซเบอร์ของประชาชนในเขตเทศบาลตำบลอ้อมใหญ่” ผลการวิจัย พบว่า ระดับการตระหนักรู้ในการป้องกันตนเองบนโลกไซเบอร์ของประชาชนในเขตเทศบาลตำบลอ้อมใหญ่ โดยภาพรวมอยู่ใน

ระดับมาก เมื่อพิจารณาเป็นรายด้านพบว่าด้านที่มีระดับความคิดเห็นสูงสุด คือ ด้านสติปัญญาพื้นฐาน รองลงมาคือ ด้านการตอบสนองทางอารมณ์ และด้านที่มีความคิดเห็นน้อยที่สุด ด้านพฤติกรรม ตามลำดับ นอกจากนี้ ผลการเปรียบเทียบปัจจัยส่วนบุคคลกับการตระหนักรู้ในการป้องกันตนเองบนโลกไซเบอร์ของประชาชนในเขตเทศบาลตำบลอ้อมใหญ่ เมื่อจำแนกตาม ภูมิลำเนา พบว่า ภาพรวมไม่แตกต่างกัน จำแนกตาม เพศ อายุ อาชีพ และระยะเวลาในการใช้อินเตอร์เน็ตต่อวัน พบว่า โดยภาพรวมแตกต่างกัน อย่างมีนัยสำคัญทางสถิติ

เมธาพร ธรรมศิริ และ ศิรภัสสรศ์ วงศ์ทองดี (2565) ได้วิจัยเรื่อง “ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพ” พบว่าบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครมีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์อยู่ในระดับมาก โดยเมื่อจำแนกตามปัจจัยส่วนบุคคลพบว่าบุคลากรในบริษัทเอกชนแห่งนี้ที่มี เพศ อายุ และประสบการณ์การทำงาน ที่ต่างกันมีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่ไม่แตกต่างกัน และในส่วนบุคลากรที่มีระดับการศึกษาสูงสุด แผนกที่สังกัด และประสบการณ์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ที่ต่างกัน มีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่แตกต่างกันอย่างมีนัยสำคัญทางสถิติ

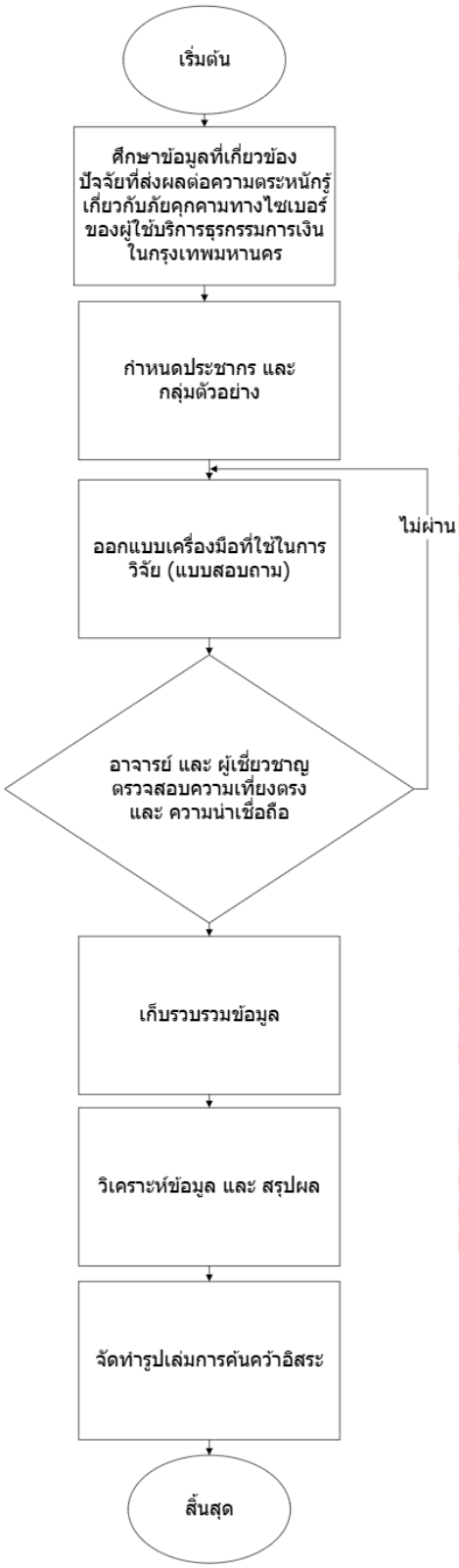
บทที่ 3
วิธีการวิจัย

การศึกษาเรื่อง “ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร” การวิจัยนี้เป็นการวิจัยเชิงปริมาณ (Quantitative Research) ด้วยการวิจัยเชิงสำรวจ (Survey Research) ผู้วิจัยรวบรวมข้อมูลจากการทบทวนวรรณกรรม บทความ วิชาการหนังสือและเอกสารที่มีความเกี่ยวข้องเพื่อให้การดำเนินวิจัยนำไปสู่วัตถุประสงค์ที่ตั้งไว้

3.1 แผนผังวิธีการวิจัย
3.2 ประชากรและกลุ่มตัวอย่าง
3.3 เครื่องมือที่ใช้ในการวิจัย
3.4 ความเที่ยงตรงและความน่าเชื่อถือ
3.5 การเก็บรวบรวมข้อมูล
3.6 การวิเคราะห์ข้อมูล

3.1 แผนผังวิธีการวิจัย

ศึกษาข้อมูลที่เกี่ยวข้องกับปัจจัยที่ส่งผลต่อความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินในกรุงเทพมหานคร และ ได้มีการกำหนดเป้าหมาย หรือ ประชากร ที่จะใช้ในการเก็บข้อมูล และ ก็มีใช้ทฤษฎีในการหาขนาดกลุ่มตัวอย่างในกรณีที่ไม่ทราบขนาดประชากร ในการกำหนดขนาดกลุ่มประชากร ซึ่งจะอยู่ในหัวข้อที่ 3.2 จากนั้นจะทำการออกแบบเครื่องมือที่ใช้ในการวิจัย อยู่ในหัวข้อที่ 3.3 และได้มีการให้อาจารย์ และ ผู้เชี่ยวชาญในการตรวจสอบความเที่ยงตรงและความน่าเชื่อถือ เพื่อปรับแก้ไขแบบสอบถามตามคำแนะนำของอาจารย์และผู้เชี่ยวชาญ ซึ่งจะอยู่ในหัวข้อที่ 3.4 เมื่อแก้ไขจนแบบสอบถามพร้อมแล้ว ก็จะทำการเก็บรวบรวมข้อมูล ซึ่งจะตรงกับหัวข้อที่ 3.5 เมื่อเก็บรวบรวมข้อมูลแบบสอบถามตามจำนวนขนาดประชากรแล้ว ก็นำข้อมูลมาวิเคราะห์ผล และ สรุปผล ดังภาพที่ 3-1



ภาพที่ 3-1 แผนผังวิธีการวิจัย

3.2 ประชากรและกลุ่มตัวอย่าง

ประชากร คือ ผู้ใช้บริการธุรกรรมทางการเงินออนไลน์ อายุ 15 ปีขึ้นไปและอาศัยในเขตกรุงเทพมหานคร มีประสบการณ์ในการใช้บริการธุรกรรมการเงินออนไลน์ เช่น ธนาคารบนมือถือ (Mobile Banking) บริการธนาคารทางอินเตอร์เน็ต (Internet Banking) และ กระเป๋าเงินอิเล็กทรอนิกส์ (E-Wallet)

กลุ่มตัวอย่าง คือ ใช้การสุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) โดยการเลือกกลุ่มตัวอย่างที่มีการใช้งานธุรกรรมการเงินออนไลน์เป็นประจำ จำนวนกลุ่มตัวอย่างคำนวณจากสูตรของ Yamene (1967) โดยกำหนดระดับความเชื่อมั่นที่ 95% และค่าความคลาดเคลื่อนที่ยอมรับได้ที่ 95%

$$n = \frac{P(1-P)Z^2}{e^2} \qquad (1)$$

โดย กำหนดให้

n คือ ขนาดตัวอย่าง

P คือ สัดส่วนของประชากรที่ผู้วิจัยกำลังสุ่ม กำหนดไว้ที่ 0.5 เนื่องจากกรณีที่ไม่ทราบขนาดของประชากรจากสูตร (มีค่าเท่ากับ 0.5)

Z คือ ค่าสถิติ Z ที่ระดับความเชื่อมั่นร้อยละ 95 หรือค่า Z-Score (มีค่าเท่ากับ 1.96)

e คือ ค่าความคลาดเคลื่อนจากการสุ่มตัวอย่างที่ยอมให้เกิดขึ้นได้ (มีค่าเท่ากับ 0.05) เนื่องจากใช้ระดับความเชื่อมั่นร้อยละ 95 ซึ่งค่าที่ยอมรับความคลาดเคลื่อนได้อยู่ที่ 0.05

แทนค่าในสมการที่ 1

$$n = \frac{(0.50)(1-0.50)(1.96)^2}{(0.05)^2}$$

$$= \frac{(0.5)(0.5)(3.8416)}{0.0025}$$

$$= \frac{0.9604}{0.0025}$$

$$= 384.16 \text{ คน}$$

จากการคำนวณแทนค่าในสมการที่ 1 มีค่าเท่ากับ 384.16 ในงานวิจัยครั้งนี้ จะใช้กลุ่มตัวอย่าง 385 คนวิธีการสุ่มตัวอย่างในงานวิจัยครั้งนี้เป็นการสุ่มเฉพาะเจาะจง โดยเป็นการเลือกกลุ่มตัวอย่างที่

เคยมีประสบการณ์ใช้บริการธุรกรรมการเงินออนไลน์อย่างน้อย 1 ครั้ง จากการคำนวณคาดว่าจะใช้กลุ่มตัวอย่างประมาณ 400 คน เพื่อให้ได้ข้อมูลเพียงพอสำหรับการวิเคราะห์ทางสถิติ

3.3 เครื่องมือที่ใช้ในการวิจัย

การเก็บรวบรวมข้อมูล โดยการใช้แบบสอบถาม (Questionnaire) ในการเก็บรวบรวมข้อมูลข้อคิดเห็นของกลุ่มตัวอย่างโดยจะสอบถามกลุ่มตัวอย่างด้วยคำถามแบบลักษณะปลายปิด (Close Questionnaire) โดยให้กลุ่มตัวอย่างเป็น ผู้ตอบแบบสอบถามด้วยตนเองโดยประกอบไปด้วยข้อคำถามจำนวน 4 ตอน ดังนี้

ตอนที่ 1 ลักษณะประชากร ได้แก่ เพศ อายุ อาชีพ ระดับการศึกษา รายได้ต่อเดือน

ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

ตอนที่ 3 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

ตอนที่ 4 ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

3.4 ความเที่ยงตรงและความน่าเชื่อถือ

แบบสอบถามที่ผู้วิจัยสร้างขึ้นจะนำมาทดสอบความเที่ยงตรงและความน่าเชื่อถือดังนี้ ความเที่ยงตรงผู้วิจัยได้นำร่างแบบสอบถามที่สร้างขึ้นให้อาจารย์ที่ปรึกษาตรวจสอบความเที่ยงตรงเชิงเนื้อหาและนำข้อคิดเห็นของอาจารย์ที่ปรึกษามาปรับแก้ก่อนและนอกจากนี้ยังมีการทำดัชนีหาความสอดคล้องของข้อมูลกับวัตถุประสงค์ (Index of item objective congruence : IOC) โดยให้ผู้เชี่ยวชาญ จำนวน 3 ท่านโดยเป็นผู้เชี่ยวชาญทางกฎหมาย 1 ท่าน, ผู้เชี่ยวชาญทางด้านความเสี่ยง 1 ท่าน และ ผู้เชี่ยวชาญทางด้านการเงิน 1 ท่านได้ดำเนินตรวจสอบและได้นำข้อคิดเห็นของผู้เชี่ยวชาญมาปรับแก้ไขและเก็บข้อมูลจริงต่อไป โดยดัชนีหาความสอดคล้องของข้อมูลกับวัตถุประสงค์จะเป็นการวัดความสัมพันธ์หรือความสอดคล้องกันของข้อมูล ซึ่งจะมีการแบ่งเกณฑ์การให้ความสัมพันธ์หรือการสอดคล้องกันของข้อมูลดังนี้

คะแนน -1 หมายถึง ความสัมพันธ์หรือความสอดคล้องที่ตรงข้ามกับข้อมูล

คะแนน 0 หมายถึง ความสัมพันธ์ที่เป็นกลาง

คะแนน 1 หมายถึง ความสัมพันธ์หรือความสอดคล้องที่เชิงบวกกับข้อมูล

3.5 การเก็บรวบรวมข้อมูล

ข้อมูลปฐมภูมิคือข้อมูลที่ได้จากแบบสอบถามแบบออนไลน์ถึงปัจจัย 4 ด้าน ได้แก่ด้านลักษณะทางประชากร ด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ ด้านความรู้เกี่ยวกับภัยคุกคามทาง

ไซเบอร์ ด้านความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์โดยเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างตามที่กำหนดของประชากร

ข้อมูลทุติยภูมิคือข้อมูลที่ได้จากแหล่งที่รวบรวมข้อมูลไว้แล้วหรือหน่วยงานที่มีการบันทึกเก็บรวบรวมสถิติต่างๆหรือเรียบเรียงไว้เรียบร้อยแล้วนำข้อมูลเหล่านั้นมาใช้เป็นในการวิเคราะห์อ้างอิง ผู้วิจัยจะทำการเก็บรวบรวมจากการทบทวนวรรณกรรมแนวคิดทฤษฎีและงานวิจัยที่เกี่ยวข้องรวมถึงการสืบค้นทางอินเตอร์เน็ตจากเว็บไซต์ที่เกี่ยวข้องกับปัจจัยที่มีผลต่อการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์เพื่อเป็นข้อมูลประกอบการวิเคราะห์งานวิจัย

3.6 การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลด้วยการใช้สถิติการวิเคราะห์ข้อมูลที่ได้รับจากการเก็บรวบรวมข้อมูลที่ผู้วิจัยได้จากกลุ่มตัวอย่างของงานวิจัย โดยจะนำข้อมูลที่ได้มาวิเคราะห์ประมวลผลทางสถิติ แบ่งออกเป็น

3.6.1 สถิติเชิงพรรณาคือการนำข้อมูลที่เก็บได้จากกลุ่มตัวอย่างมาแสดงรายละเอียดของข้อมูลเพื่อทีจะอธิบายค่าของข้อมูลโดยแจกแจงความถี่แบบค่าร้อยละแบบคำนวณค่าเฉลี่ยและแบบค่าเบี่ยงเบนมาตรฐานในการพัฒนาข้อมูลของกลุ่มตัวอย่างเกี่ยวกับลักษณะทางประชากร ประสบการณ์เกี่ยวกับภัยคุกคามทาง ไซเบอร์ ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ ซึ่งก็จะมีการแบ่งเกณฑ์ตามสัดส่วนคะแนน เช่น

1.00 – 1.49 คะแนน หมายถึง มีความตระหนักรู้ระดับน้อยมาก
1.50 – 2.49 คะแนน หมายถึง มีความตระหนักรู้ระดับน้อย
2.50 – 3.49 คะแนน หมายถึง มีความตระหนักรู้ระดับปานกลาง
3.50 – 4.49 คะแนน หมายถึง มีความตระหนักรู้ระดับมาก
4.50 – 5.00 คะแนน หมายถึง มีความตระหนักรู้ระดับมากที่สุด

3.6.2 สถิติเชิงอนุมานคือการนำข้อมูลที่ได้มาจากกลุ่มตัวอย่างมาทดสอบหาความสัมพันธ์ระหว่างตัวแปรอิสระกับตัวแปรตามโดยใช้ การทดสอบทีแบบอิสระ (Independent Sample T-Test) ในการทดสอบสมมุติฐาน และ การทดสอบเอฟโดยรวม (Overall F-test)

3.6.3 การวิเคราะห์ถดถอยเชิงเส้น (Linear Regression Analysis) เป็นเทคนิคทางสถิติที่ใช้ในการประมาณค่าความสัมพันธ์ระหว่างตัวแปรโดยกำหนดให้ตัวแปรหนึ่งเป็นตัวแปรที่ทราบค่าเรียกว่าตัวแปรอิสระ (Independent Variable: X) ในขณะที่ตัวแปรหนึ่งเป็นตัวแปรที่ต้องการทราบค่าเรียกว่าตัวแปรตาม (Dependent Variable: Y) มีวัตถุประสงค์เพื่อพยากรณ์และวิเคราะห์ความสัมพันธ์เชิงเส้นระหว่างตัวแปรอิสระกับตัวแปรตาม ในการศึกษาครั้งนี้ผู้วิจัยวิเคราะห์ความสัมพันธ์เชิงเส้นระหว่างตัวแปรด้านประชากรที่ส่งผลต่อประสบการณ์ภัยคุกคามทางไซเบอร์ ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ และความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ การถดถอย

เชิงเส้นของ เกาส์ (Gauss) และ เลเจนเดอ (Legendre) ซึ่งได้พัฒนาวิธีการกำลังสองน้อยที่สุด (Least Squares Method) รูปแบบทั่วไปของโมเดลการถดถอยเชิงเส้นอย่างง่ายดังสมการที่ 2

$$Y = \beta 0 + \beta 1(X) + \epsilon \quad (2)$$

โดยที่

Y = ตัวแปรตามที่ต้องการพยากรณ์

X = ตัวแปรอิสระที่ใช้ในการทำนาย

$\beta 0$ = ค่าคงที่หรือตัดแกน (Intercept)

$\beta 1$ = ค่าสัมประสิทธิ์ความชัน (Slope) แสดงถึงอัตราการเปลี่ยนแปลงของ Y ต่อ X

ϵ = ค่าความคลาดเคลื่อนของโมเดล

ในกรณีของการถดถอยเชิงเส้นพหุคูณ โมเดลจะถูกขยายให้ครอบคลุมตัวแปรพยากรณ์หลายตัว จากการศึกษาวิจัยเกี่ยวกับโมเดลการถดถอยเชิงเส้น มีข้อค้นพบสำคัญ ได้แก่

3.6.3.1 ตัวประมาณค่าที่ดีที่สุดและไม่มีอคติ (BLUE) : ตามทฤษฎี เกาส์-มาร์คอฟ (Gauss-Markov) วิธีการประมาณค่าด้วยกำลังสองน้อยที่สุด (OLS) จะให้ค่าประมาณที่ดีที่สุดและไม่มีอคติภายใต้ข้อสมมติของความเป็นเส้นตรง ความสม่ำเสมอของความแปรปรวน (Homoscedasticity) การไม่มีปัญหาความสัมพันธ์กันระหว่างตัวแปรอิสระ (Multicollinearity) และการไม่มีเชื่อมโยงกันของค่าคลาดเคลื่อน (Autocorrelation)

3.6.3.2 การประยุกต์ใช้ในสาขาต่างๆ โมเดลการถดถอยเชิงเส้นถูกนำไปใช้กันอย่างแพร่หลายในเศรษฐศาสตร์ การเงิน สังคมศาสตร์ และ การเรียนรู้ของเครื่องเพื่อการพยากรณ์และการวิเคราะห์เชิงอนุมานความสัมพันธ์

การตีความผลลัพธ์ที่สำคัญ การตีความความผลลัพธ์ของโมเดลการถดถอยเชิงเส้นประกอบไปด้วย

1) ค่าประมาณสัมประสิทธิ์ (Coeffcient Estimates) : แสดงขนาดและทิศทางของความสัมพันธ์ระหว่างตัวแปรอิสระและตัวแปรตาม

2) ค่าความแปรผันของตัวแปรตอบสนองที่สามารถอธิบายได้ (R-Squared) และ ค่าสัมประสิทธิ์ของการพยากรณ์ปรับปรุง(Adjusted R-Squared) ใช้ในการวัดสัดส่วนของความแปรปรวนที่สามารถอธิบายได้โดยโมเดล ค่ายิ่งสูงแสดงว่าโมเดลมีความสามารถในการอธิบายข้อมูลได้ดีขึ้น

3) ค่าพี (P – Value) และนัยสำคัญทางสถิติ ใช้ในการทดสอบสมมติฐานเพื่อตรวจสอบว่าสัมประสิทธิ์แตกต่างจากศูนย์อย่างมีนัยสำคัญหรือไม่ ซึ่งช่วยในการคัดเลือกตัวแปร

4) การวิเคราะห์ค่าความคลาดเคลื่อน (Residual Analysis) : ตรวจสอบค่าความคลาดเคลื่อนเพื่อให้แน่ใจว่าข้อสมมติของโมเดลยังคงเป็นจริง และทำการแก้ไขหากจำเป็น กล่าวโดยสรุป โมเดลการถดถอยเชิงเส้นยังคงเป็นรากฐานสำคัญของการสร้างแบบจำลองทางสถิติ ด้วยการพัฒนาอย่างต่อเนื่องทั้งในด้านวิธีการและการประยุกต์ใช้งาน แม้ว่าจะเป็นโมเดลที่เรียบง่าย แต่ให้ข้อมูลเชิงลึกที่สำคัญและเป็นพื้นฐานสำหรับโมเดลที่ซับซ้อนมากขึ้นในด้านการวิเคราะห์ข้อมูลความสัมพันธ์ของตัวแปรต่างๆ การวิเคราะห์การถดถอยถูกนำมาใช้กันอย่างแพร่หลายในด้านความปลอดภัยทางไซเบอร์เพื่อการตรวจจับภัยคุกคามการประเมินความเสี่ยง และ การคาดการณ์ความผิดปกติ โมเดลการถดถอยเชิงเส้น และ โลจิสติก (Logistic Regression) สามารถช่วยระบุรูปแบบของทราฟฟิกของเครือข่ายที่อาจเป็นภัยคุกคามทางไซเบอร์ การสร้างแบบจำลอง เชิงพยากรณ์สามารถใช้ในการจำแนกพฤติกรรมเครือข่ายว่าเป็นปกติหรือเป็นอันตรายโดยอ้างอิง จากข้อมูลเหตุการณ์โจมตีในอดีต สามารถใช้พยากรณ์ค่าตัวแปรตามในอนาคตจากค่าของตัวแปรอิสระช่วยให้เข้าใจว่าตัวแปรอิสระมีผลต่อการเปลี่ยนแปลงของตัวแปรตามมากน้อยเพียงใด การวิเคราะห์การถดถอย (Simple Regression) เป็นรากฐานของการวิเคราะห์การถดถอยพหุคูณ (Multiple Regression) สามารถขยายไปสู่โมเดลที่ซับซ้อน เช่น การถดถอยพหุคูณ (Multiple Regression) การถดถอยลาสโซ่ (Lasso Regression) และ โครงข่ายประสาทเทียม (Neural Networks) สามารถใช้วิเคราะห์ข้อมูลเชิงสถิติ เช่น การทดสอบสมมติฐานว่า X มีผลต่อ Y อย่างมีนัยสำคัญทางสถิติหรือไม่ และสามารถช่วยให้องค์กรและนักวิจัยสนับสนุนการตัดสินใจที่มีหลักฐานเชิงตัวเลข

บทที่ 4
ผลการวิจัย

การวิจัยเรื่อง “ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร” เป็นการวิจัยเชิงปริมาณ โดยใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูล ทำการแจกแบบสอบถามแก่ผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร หลังจากการเก็บข้อมูลเรียบร้อยจากกลุ่มตัวอย่าง ผู้วิจัยทำการวิเคราะห์ข้อมูลและนำเสนอผลการวิจัยแบ่งเป็น 4 ส่วนดังนี้

4.1 ผลการวิจัยข้อมูลทางประชากร

4.2 ผลการวิจัยความรู้เกี่ยวกับภัยคุกคามไซเบอร์

4.3 ผลการวิจัยประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

4.4 ผลการวิจัยความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

4.5 ผลการวิจัยความสัมพันธ์ระหว่างตัวแปรข้อมูลทางประชากรต่อความรู้เกี่ยวกับภัยคุกคามไซเบอร์ของการใช้บริการธุรกรรมเงินออนไลน์

4.6 ผลการวิจัยความสัมพันธ์ระหว่างตัวแปรข้อมูลทางประชากรต่อประสบการณ์เกี่ยวกับภัยคุกคามไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

4.7 ผลการวิจัยความสัมพันธ์ระหว่างตัวแปรข้อมูลทางประชากรต่อความตระหนักรู้เกี่ยวกับภัยคุกคามไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

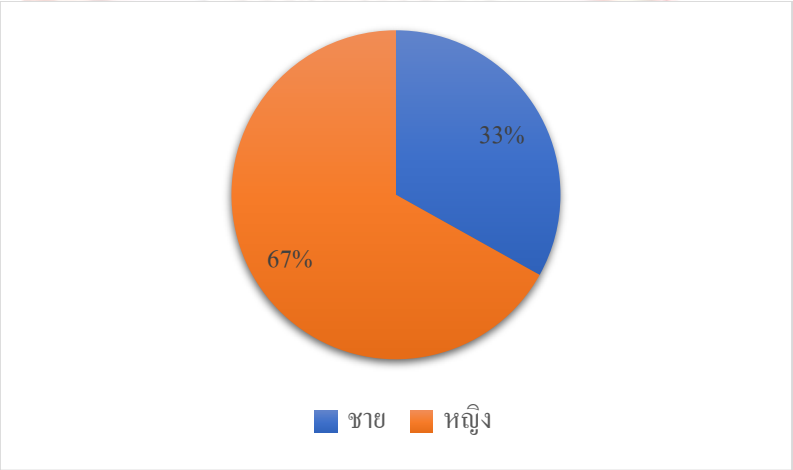
4.8 ผลการวิจัยการหาความสัมพันธ์ของตัวแปรต้นและตัวแปรตาม

4.1 ผลการวิจัยข้อมูลทางประชากร

การวิจัยเรื่อง “ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร” เป็นการวิจัยเชิงปริมาณ โดยใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูล ทำการแจกแบบสอบถามแก่ผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร โดยใช้วิธีการสุ่มตัวอย่างแบบเจาะจงผู้ที่เคยใช้บริการธุรกรรมการเงินแบบออนไลน์ จากการเก็บแบบสอบถามจากกลุ่มตัวอย่างครั้งนี้จำแนกตามเพศได้ดังตารางที่ 4-1

ตารางที่ 4-1 จำนวนและร้อยละของผู้ตอบแบบสอบถาม จำแนกตามเพศ

เพศ	จำนวน(คน)	ร้อยละ
หญิง	301	66.9
ชาย	149	33.1
รวม	450	100



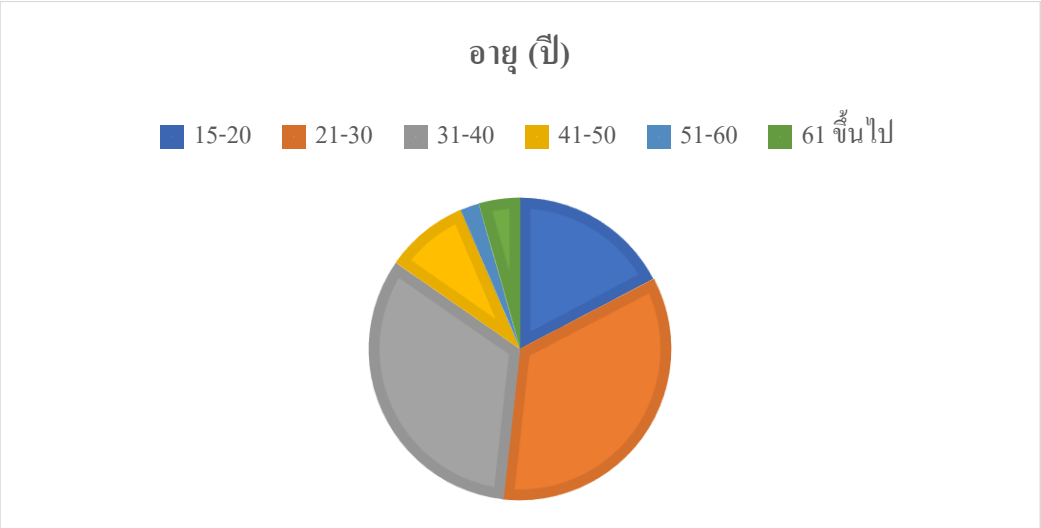
ภาพที่ 4-1 จำนวนและร้อยละของผู้ตอบแบบสอบถาม จำแนกตามเพศ

จำนวนผู้ตอบแบบสอบถามของกลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิง จำนวน 301 คน คิดเป็นร้อยละ 67 และเพศชายจำนวน 149 คน คิดเป็นร้อยละ 33 ตามลำดับ

จากการเก็บแบบสอบถามจากกลุ่มตัวอย่างครั้งนี้จำแนกตามอายุจำนวน 450 คน แบ่งเป็นช่วงอายุได้ดังตารางที่ 4-2

ตารางที่ 4-2 จำนวนและร้อยละของผู้ตอบแบบสอบถาม จำแนกตามอายุ

อายุ	จำนวน(คน)	ร้อยละ
15-20 ปี	78	17.3
21-30 ปี	155	34.4
31-40 ปี	148	32.9
41-50 ปี	40	8.9
51-60 ปี	9	2
61 ปีขึ้นไป	20	4.4
รวม	450	100



ภาพที่ 4-2 จำนวนและร้อยละของผู้ตอบแบบสอบถาม จำแนกตามอายุ

จากผลการวิเคราะห์อายุผู้ตอบแบบสอบถามของกลุ่มตัวอย่างส่วนใหญ่อยู่ในช่วงอายุ 21-30 ปี จำนวน 155 คน คิดเป็นร้อยละ 34.4 รองลงมาช่วงอายุ 31 – 40 ปี จำนวน 148 คน คิดเป็นร้อยละ 32.9 กลุ่มอายุ15-20 ปีจำนวน 78 คน คิดเป็นร้อยละ17.3 ช่วงอายุ 41-50 ปี จำนวน 40 คน คิดเป็นร้อยละ 8.9 และในกลุ่มช่วงอายุผู้สูงวัย อายุ 61 ปีขึ้นไป จำนวน 20 คน คิดเป็นร้อยละ 4.4 และกลุ่มอายุ 51 – 60 ปี จำนวน 9 คน คิดเป็นร้อยละ 2 ของกลุ่มตัวอย่างทั้งหมด ตามลำดับ

จากการเก็บแบบสอบถามจากกลุ่มตัวอย่างครั้งนี้จำแนกตามระดับการศึกษาของกลุ่มตัวอย่าง จำนวน 450 คน แบ่งเป็นช่วงอายุได้ดังตารางที่ 4-3

ตารางที่ 4-3 จำนวนและร้อยละของผู้ตอบแบบสอบถาม จำแนกตามระดับการศึกษา

ระดับการศึกษา	จำนวน(คน)	ร้อยละ
ต่ำกว่ามัธยมศึกษา	5	1.1
มัธยมศึกษาตอนต้น	35	7.8
มัธยมศึกษาตอนปลายหรือเทียบเท่า	64	14.2
ปริญญาตรี	269	59.8
ปริญญาโท	67	14.9
ปริญญาเอก	10	2.2
รวม	450	100

จากตารางที่ 4-3 ระดับการศึกษาของผู้ตอบแบบสอบถามส่วนใหญ่มีระดับการศึกษาปริญญาตรี จำนวน 269 คน คิดเป็นร้อยละ 59.8 รองลงมา ปริญญาโท จำนวน 67 คน ร้อยละ 14.9 มัธยมศึกษา

ตอนปลายหรือเทียบเท่า จำนวน 64 คน ร้อยละ 14.2 มัธยมศึกษาตอนต้น จำนวน 35 คน ร้อยละ 7.8 ปริญญาเอก จำนวน 10 คน ร้อยละ 2.2 และต่ำกว่ามัธยมศึกษา จำนวน 5 คน ร้อยละ 1.1 ตามลำดับ

จากการเก็บแบบสอบถามจากกลุ่มตัวอย่างครั้งนี้จำแนกตามระดับรายได้ต่อเดือนจำนวน 450 คน แบ่งเป็นระดับรายได้ต่อเดือนของกลุ่มตัวอย่าง ได้ดังตารางที่ 4-4

ตารางที่ 4-4 จำนวนและร้อยละของผู้ตอบแบบสอบถาม จำแนกตามระดับรายได้ต่อเดือน

รายได้ต่อเดือน (บาท)	จำนวน(คน)	ร้อยละ
ไม่เกิน 15,000	183	40.7
15,001 – 30,000	173	38.4
30,001 – 45,000	50	11.1
45,001 – 50,000	11	2.4
50,001 ขึ้นไป	33	7.3
รวม	450	100

จากตารางที่ 4-4 กลุ่มรายได้ต่อเดือนของผู้ตอบแบบสอบถามส่วนใหญ่อยู่ที่ ไม่เกิน 15,000 บาท ต่อเดือน จำนวน 183 คน ร้อยละ 40.7 ระดับรายได้ 15,001 – 30,000 บาทต่อเดือน จำนวน 173 คน คิดเป็นร้อยละ 38.4 ระดับรายได้ 30,001 – 45,000 บาทต่อเดือน จำนวน 50 คน ร้อยละ 11.1 รายได้ 50,001 ขึ้นไป จำนวน 33 คน ร้อยละ 7.3 และรายได้ 45,001 – 50,000 บาท จำนวน 11 คน ร้อยละ 2.4 ตามลำดับ

4.2 ผลการวิจัยความรู้เกี่ยวกับภัยคุกคามไซเบอร์

ในส่วนความรู้เกี่ยวกับภัยคุกคามไซเบอร์ของผู้ตอบแบบสอบถามมีการให้กลุ่มตัวอย่างเลือกตอบคำถาม ใช่หรือไม่ใช่ จำนวน 10 คำถาม ข้อคำถามเกี่ยวกับอันตรายหรือความเสี่ยงที่อาจจะเกิดขึ้นจากการโจมตีทางเทคโนโลยีสารสนเทศ อาทิ การเจาะระบบ การแพร่กระจายมัลแวร์ซอฟต์แวร์ที่เป็นอันตราย เช่น ไวรัส แรนซัมแวร์ และการขโมยข้อมูล การหลอกลวงข้อมูลเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลสำคัญ และการหลอกให้เหยื่อกรอกข้อมูลส่วนตัวผ่านอีเมลหรือเว็บไซต์ปลอม นำมาซึ่งผลกระทบ ความสูญเสียที่จะเกิดขึ้นต่อบุคคลผู้ใช้บริการธุรกรรมการเงินออนไลน์ แบ่งข้อคำถามออกเป็น 1) คำถามที่ตอบว่าใช่จะเป็นคำตอบที่ถูกต้อง จำนวน 5 คำถาม และ2) คำถามที่ตอบว่าไม่ใช่จะเป็นคำตอบที่ถูกต้องจำนวน 5 คำถาม โดยมีผลดังตารางที่ 4-5

ตารางที่ 4-5 จำนวนและร้อยละของความรู้เกี่ยวกับภัยคุกคามไซเบอร์ของผู้ตอบแบบสอบถาม

ข้อคำถาม	คำตอบ				รวม	
	ใช่ (คน)	ร้อยละ	ไม่ใช่ (คน)	ร้อยละ	ทั้งหมด (คน)	ร้อยละ
ข้อคำถามที่ตอบใช่ คือ ตอบถูก						
2.การเข้าใช้เครือข่ายไร้สาย (Wifi) สาธารณะ ทำให้ผู้ใช้มีความเสี่ยงต่อการทำธุรกรรมออนไลน์	342	76	108	24	450	100
3.การติดตามข่าวสารรูปแบบการโจมตีทางไซเบอร์ต่างๆ สามารถช่วยให้รับมือกับการโจมตีทางไซเบอร์ที่เกิดขึ้นได้	399	88.7	51	11.3	450	100
5.การตั้งรหัสผ่าน (Password) ต่างๆ ที่มีความยาวมาก ช่วยลดโอกาสการเดารหัสผ่านหรือใช้เวลาในการเดามากขึ้น	402	89.3	48	10.7	450	100
7.การบันทึกรหัสผ่าน (Password) ต่างๆ ไว้ในเครื่องที่เชื่อมต่อกับเครือข่ายไร้สาย (Wifi) สาธารณะ มีความเสี่ยงต่อการทำธุรกรรมออนไลน์	395	87.8	55	12.2	450	100
10.การเข้าเว็บไซต์ Https มีความปลอดภัยมากกว่า Http	298	66.2	152	33.8	450	100
ข้อคำถามที่ตอบใช่ คือ ตอบผิด						
1.การให้ข้อมูลส่วนตัวบนเครือข่ายสังคม (Social Media) สาธารณะ ทำให้ผู้ให้ข้อมูลส่วนตัวไม่มีความเสี่ยงต่อการทำธุรกรรมออนไลน์	196	43.6	254	56.4	450	100
4.การโหลดแอปพลิเคชั่น (Application) จากแหล่งต่างๆ เช่น เว็บไซต์ที่ไม่มีความน่าเชื่อถือ ทำให้มีความปลอดภัยจากการโดนโจรกรรมข้อมูล	211	46.9	239	53.1	450	100
6.การตั้งรหัสผ่าน (Password) ใน อุปกรณ์ต่างๆ ควรจะตั้งเหมือนๆกัน	152	33.8	298	66.2	450	100
8.การคลิกเปิดลิงค์ (Link) ในจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ได้รับ จากแหล่งหรือบุคคลที่ไม่รู้จัก ไม่ทำให้เกิดความเสี่ยงต่อการทำธุรกรรมออนไลน์	251	55.8	199	44.2	450	100
9.การใช้รหัสผ่าน (Password) หลายชั้น และหลากหลาย เช่น ชั้นที่ 1 รหัสผ่านที่ตั้งขึ้นมา กับชั้นที่ 2 มีการยืนยัน OTP ทำให้มีความเสี่ยงต่อการทำธุรกรรมออนไลน์เพิ่มขึ้น	198	44	252	56	450	100

จากตารางที่ 4-5 พบว่า ผู้ตอบแบบสอบถาม กลุ่มข้อความที่ตอบใช่คือตอบถูกนั้น มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ การตั้งรหัสผ่านต่างๆ ควรที่มีความยาวมาก ซึ่งจะช่วยในการลดโอกาสการเดารหัสผ่านหรือใช้เวลาในการเดามากขึ้น ได้มากที่สุด จำนวน 402 คน คิดเป็นร้อยละ 89.3 รองลงมา การติดตามข่าวสารรูปแบบการโจมตีทางไซเบอร์ต่างๆ สามารถช่วยให้รับมือกับการโจมตีทางไซเบอร์ที่เกิดขึ้นได้ จำนวน 399 คน คิดเป็นร้อยละ 88.7 การบันทึกรหัสผ่านต่างๆ ไว้ในเครื่องที่เชื่อมต่อกับเครือข่ายไร้สายสาธารณะ มีความเสี่ยงต่อการทำธุรกรรมออนไลน์ จำนวน 395 คน คิดเป็นร้อยละ 87.8 การเข้าใช้เครือข่ายไร้สายสาธารณะ ทำให้ผู้ใช้มีความเสี่ยงต่อการทำธุรกรรมออนไลน์ จำนวน 342 คน คิดเป็นร้อยละ 76 การเข้าเว็บไซต์ Https มีความปลอดภัยมากกว่า Http จำนวน 298 คน คิดเป็นร้อยละ 66.2 ตามลำดับ ซึ่งจะเห็นได้ว่า ผู้ตอบแบบสอบถามส่วนมากมีความรู้ความเข้าใจเกี่ยวกับรหัสผ่านในการป้องกันความเสี่ยง และ รู้จักความเสี่ยงต่อธุรกรรมออนไลน์ในการใช้เครือข่ายไร้สายสาธารณะอีกด้วย

จากตาราง พบว่า ผู้ตอบแบบสอบถาม กลุ่มข้อความที่ตอบใช่คือตอบผิดนั้น มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ การคลิกเปิดลิงค์ (Link) ในจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ได้รับ จากแหล่งหรือบุคคลที่ไม่รู้จัก ไม่ทำให้เกิดความเสี่ยงต่อการทำธุรกรรมออนไลน์ มากที่สุด จำนวน 251 คน คิดเป็นร้อยละ 55.8 รองลงมา การโหลดแอปพลิเคชั่น (Application) จากแหล่งต่างๆ เช่น เว็บไซต์ที่ไม่มีความน่าเชื่อถือ ทำให้มีความปลอดภัยจากการโดนโจรกรรมข้อมูล จำนวน 211 คน คิดเป็นร้อยละ 46.9 การใช้รหัสผ่านหลายชั้น และ หลากหลาย เช่น ชั้นที่ 1 รหัสผ่านที่ตั้งขึ้นมา กับ ชั้นที่ 2 มีการยืนยัน OTP ทำให้มีความเสี่ยงต่อการทำธุรกรรมออนไลน์เพิ่มขึ้น จำนวน 198 คน คิดเป็นร้อยละ 44 การให้ข้อมูลส่วนตัวบนเครือข่ายสังคมออนไลน์สาธารณะ ทำให้ผู้ให้ข้อมูลส่วนตัวไม่มีความเสี่ยงต่อการทำธุรกรรมออนไลน์ จำนวน196 คน คิดเป็นร้อยละ 43.6 การตั้งรหัสผ่านในอุปกรณ์ต่างๆ ควรจะตั้งเหมือนๆกัน จำนวน 152 คน คิดเป็นร้อยละ 33.8 ตามลำดับ

4.3 ผลการวิจัยประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

ปัจจุบันธุรกรรมการเงินออนไลน์ (เช่น ธนาคารบนมือถือ บริการธนาคารทางอินเตอร์เน็ต กระเป๋าเงินอิเล็กทรอนิกส์) ได้รับความนิยมมากขึ้น แต่ก็มาพร้อมกับภัยคุกคามไซเบอร์ที่หลากหลาย เช่น ฟิชชิ่ง มัลแวร์ การขโมยข้อมูล เป็นต้น ในการศึกษาครั้งนี้แบบสอบถามที่ใช้กับกลุ่มตัวอย่างเก็บข้อมูลของกลุ่มตัวอย่างเกี่ยวกับ ประสบการณ์เคยหรือไม่เคยแก่กลุ่มตัวอย่างให้เลือกตอบ จำนวน 10 ข้อคำถาม ในข้อคำถามจะครอบคลุมประสบการณ์หลากหลายด้าน อาทิ กรณีฟิชชิ่ง มัลแวร์ การขโมยข้อมูล วิศวกรรมสังคม และ การโจมตีแบบการปฏิเสธการให้บริการแบบกระจายในระบบเครือข่ายทำให้ไม่สามารถใช้บริการธุรกรรมการเงินออนไลน์ได้

ตารางที่ 4-6 จำนวนและร้อยละของผู้ตอบแบบสอบถามมีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

ประสบการณ์	เคย (คน)	ร้อยละ	ไม่เคย (คน)	ร้อยละ	รวม (คน)	ร้อยละ
1.ท่านเคยได้รับผลกระทบจากโปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมา เพื่อทำอันตรายกับข้อมูลในระบบ (Malware) เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ มีการขโมยหรือทำลายข้อมูลหรืออาจจะเปิดช่องทางให้กับผู้ไม่หวังดีเข้ามาควบคุมเครื่องคอมพิวเตอร์ ทำให้ข้อมูลส่วนตัวรั่วไหล เป็นต้น ซึ่งทำให้มีบุคคลอื่นสามารถใช้บริการธุรกรรมการเงินของท่านได้	178	39.6	272	60.4	450	100
2.ท่านเคยได้รับการก่อกวน เช่น DDOS ในระบบเครือข่ายทำให้ไม่สามารถใช้บริการธุรกรรมการเงินออนไลน์ได้	134	29.8	316	70.2	450	100
3.ท่านเคยติดตั้งโปรแกรมหรือแอปพลิเคชั่นที่คิดว่าปลอดภัยแต่มี โปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมาเพื่อทำอันตรายกับข้อมูลในระบบ (Malware) แฝงตัวมา ทำให้มีบุคคลอื่น สามารถทำธุรกรรมการเงินของท่านได้	167	37.1	283	62.9	450	100
4.ท่านเคยถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์หรือโทรศัพท์โดยที่ท่านไม่รู้ตัว	159	35.3	291	64.7	450	100
5.ท่านเคยถูกหลอกให้ลงทุนและได้ทำธุรกรรมการเงิน	148	32.9	302	67.1	450	100
6.ท่านเคยถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าสู่ระบบ	172	38.2	278	61.8	450	100
7.ท่านเคยได้รับจดหมายอิเล็กทรอนิกส์ (E-Mail) หลอกลวงให้ทำธุรกรรมการเงิน	239	53.1	211	46.9	450	100
8.ท่านเคยถูกคอลเซ็นเตอร์ (Call Center) มิจฉาชีพ หลอกลวงให้ทำธุรกรรมการเงิน	255	56.7	195	43.3	450	100
9.ท่านเคยถูกหลอกให้ซื้อขายสินค้าหรือบริการทางเครือข่ายสังคม (Social Media)	203	45.1	247	54.9	450	100
10.ท่านเคยถูกหลอกให้รักและให้ทำธุรกรรมการเงิน	100	22.2	350	77.8	450	100

จากตารางที่ 4-6 พบว่า ผู้ตอบแบบสอบถามมีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมออนไลน์ เคยถูกคอลเซ็นเตอร์ มิจฉาชีพ หลอกลวงให้ทำธุรกรรมการเงิน มากที่สุด จำนวน 255 คน คิดเป็นร้อยละ 56.7 รองลงมา คือ เคยได้รับจดหมายอิเล็กทรอนิกส์ หลอกลวงให้ทำธุรกรรมการเงิน จำนวน 239 คน คิดเป็นร้อยละ 53.1 เคยถูกหลอกให้ซื้อขายสินค้าหรือบริการทางเครือข่ายสังคม จำนวน 203 คน คิดเป็นร้อย 45.1 เคยได้รับผลกระทบจากโปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมา เพื่อทำอันตรายกับข้อมูลในระบบ เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ มีการขโมยหรือทำลายข้อมูลหรืออาจจะเปิดช่องทางให้กับผู้ไม่หวังดีเข้ามาควบคุมเครื่องคอมพิวเตอร์ ทำให้ข้อมูลส่วนตัวรั่วไหล เป็นต้น ซึ่งทำให้มีบุคคลอื่นสามารถใช้บริการธุรกรรมการเงินได้ จำนวน 178 คน คิดเป็นร้อยละ 39.6 เคยถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าสู่ระบบ จำนวน 172 คิดเป็นร้อยละ 38.2 เคยติดตั้งโปรแกรมหรือแอปพลิเคชั่นที่คิดว่าปลอดภัยแต่มี โปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมาเพื่อทำอันตรายกับข้อมูลในระบบแฝงตัวมา ทำให้มีบุคคลอื่น สามารถทำธุรกรรมการเงินของท่านได้ จำนวน 167 คิดเป็นร้อยละ 37.1 เคยถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์หรือโทรศัพท์โดยที่ท่านไม่รู้ตัว จำนวน 159 คน คิดเป็นร้อยละ 35.3 เคยถูกหลอกให้ลงทุนและได้ทำธุรกรรมการเงิน จำนวน 148 คน คิดเป็นร้อยละ 32.9 เคยได้รับการก่อกวน เช่น การปฏิเสธการให้บริการแบบกระจายในระบบเครือข่ายทำให้ไม่สามารถใช้บริการธุรกรรมการเงินออนไลน์ได้ จำนวน 134 คน คิดเป็นร้อยละ 29.8 เคยถูกหลอกให้รักและให้ทำธุรกรรมการเงิน จำนวน 100 คน คิดเป็นร้อยละ 22.2 ตามลำดับ

4.4 ผลการวิจัยความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

การเก็บแบบสอบถามของกลุ่มตัวอย่างเพื่อต้องการข้อมูลความตระหนักรู้ทางไซเบอร์ เพื่อทราบว่ากลุ่มตัวอย่างมีความเข้าใจและการรับรู้ ถึงภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นจากการทำธุรกรรมออนไลน์ และการมี พฤติกรรมที่ปลอดภัย เพื่อป้องกันตนเองจากการถูกโจมตีทางไซเบอร์ โดยเฉพาะในปัจจุบัน ธุรกรรมการเงินออนไลน์ได้กลายเป็นส่วนสำคัญในชีวิตประจำวัน ไม่ว่าจะเป็น ธนาคารบนมือถือ บริการธนาคารทางอินเตอร์เน็ต กระเป๋าเงินอิเล็กทรอนิกส์ หรือการใช้ ระบบจ่ายเงินด้วยคิวอาร์โค้ดอย่างไรก็ตาม การใช้งานเหล่านี้ก็มี ความเสี่ยงด้านภัยคุกคามไซเบอร์ ที่ผู้ใช้บริการธุรกรรมการเงินออนไลน์ควรตระหนักรู้และป้องกันความเสี่ยงที่อาจจะเกิดขึ้นจากการใช้บริการธุรกรรมการเงินออนไลน์ จำนวนและร้อยละของผู้ตอบแบบสอบถามรายละเอียดดังตารางที่ 4-7

ตารางที่ 4-7 จำนวนและร้อยละของผู้ตอบแบบสอบถามมีความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

ประเด็น	Mean	S.D.	ระดับความตระหนักรู้
1. ด้านความมั่นคงปลอดภัย (Security)			
1.1ควรตั้ง Password ให้มีความยาวมากๆ เพื่อให้ใช้เวลาในการคาดเดารหัสผ่านยากขึ้น (Brute Force)	4.49	0.03	ระดับมาก
1.2ควรหาทางป้องกันการถูกหลอกให้กรอกข้อมูลส่วนตัวทางเว็บไซต์ปลอม	4.66	0.03	ระดับมากที่สุด
1.3ควรหาทางป้องกันโปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมาเพื่อทำอันตรายกับข้อมูลในระบบ (Malware) เช่น โปรแกรม Anti – Virus เป็นต้น	4.61	0.02	ระดับมากที่สุด
2. ด้านการแอบอ้าง (Masquerading)			
2.1ไม่ควรแอบอ้างชื่อหรือภาพผู้อื่นผ่าน Social Media เพื่อทำธุรกรรมการเงิน	4.67	0.02	ระดับมากที่สุด
2.2ไม่ควรมีการแอบอ้างชื่อหรือภาพผู้อื่นผ่านการโทร เพื่อทำธุรกรรมการเงิน	4.65	0.03	ระดับมากที่สุด
2.3ไม่ควรมีการแอบอ้างชื่อหรือภาพผู้อื่นผ่านการใช้ AI ในการทำ Deep Fake เพื่อทำธุรกรรมการเงิน	4.67	0.02	ระดับมากที่สุด
3. ด้านกฎหมาย (Legal)			
3.1ข้อมูลอิเล็กทรอนิกส์ และ ข้อมูลที่เป็นกระดาษสามารถนำไปใช้ตามกฎหมายได้เหมือนกัน	4.37	0.04	ระดับมาก
3.2กฎหมาย PDPA สามารถใช้กับกรณีที่เกิดข้อมูลรั่วไหลได้	4.35	0.04	ระดับมาก
3.3กฎหมาย E-Payment สามารถรองรับระบบภาษี และเอกสารธุรกรรมทางการอิเล็กทรอนิกส์ได้	4.48	0.03	ระดับมาก
4. ด้านการหลอกลวงข้อมูล (Social Engineering)			
4.1ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านทางเครือข่ายสังคม (Social Media)	3.71	0.06	ระดับปานกลาง
4.2ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านทางจดหมายอิเล็กทรอนิกส์ (E-Mail)	3.74	0.07	ระดับปานกลาง
4.3ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านช่องทางการโทร	3.72	0.06	ระดับปานกลาง

ตารางที่ 4-7 (ต่อ)

ประเด็น	Mean	S.D.	ระดับความตระหนักรู้
5.ด้านการตอบสนอง (Response)			
5.1เมื่อพบว่าได้ให้ข้อมูลส่วนตัวกับมิจฉาชีพ ควรเปลี่ยนรหัสผ่าน (Password) ใหม่ทั้งหมด และระงับการใช้งานบัตรเดบิต / บัตรเครดิต ทันที	4.62	0.02	ระดับมาก
5.2เมื่อพบว่าได้ให้ข้อมูลส่วนตัวกับมิจฉาชีพ ควรเตือนผู้ใกล้ชิดทั้งหมดและระมัดระวังการหลอกลวงจากมิจฉาชีพมากขึ้น	4.66	0.03	ระดับมาก
5.3เมื่อเกิดเหตุโดนหลอกให้ข้อมูลส่วนตัวหรือทำธุรกรรมการเงินให้มิจฉาชีพไป ควรรวบรวมหลักฐานเพื่อแจ้งความและติดต่อธนาคาร	4.63	0.02	ระดับมาก

จากตารางที่ 4-7 พบว่าในภาพรวมผู้ตอบแบบถามมีความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ในระดับมาก (4.40) โดยด้านที่มีกลุ่มตัวอย่างมีความตระหนักในระดับมากที่สุดมี 2 ด้าน

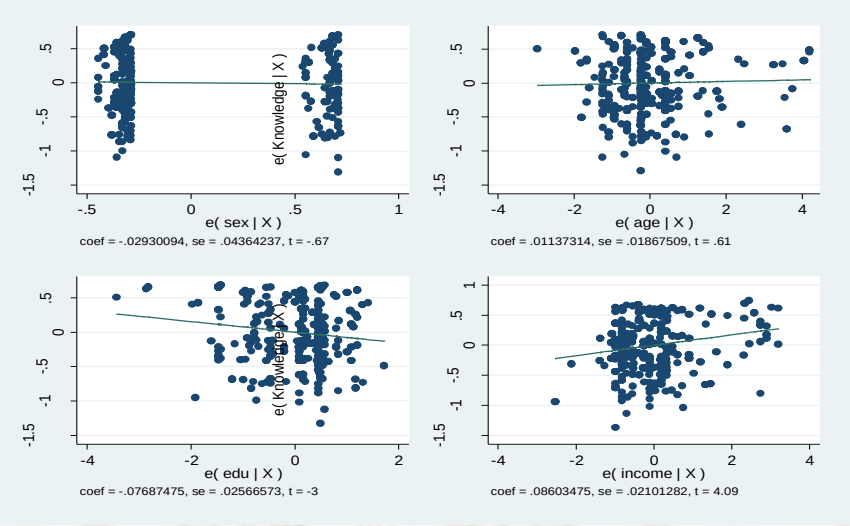
4.5 ผลการวิจัยความสัมพันธ์ระหว่างตัวแปรข้อมูลทางประชากรต่อความรู้เกี่ยวกับภัยคุกคามไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

จากข้อมูลที่เก็บได้จากกลุ่มตัวอย่างจำนวน 450 คน นำมาทดสอบความสัมพันธ์ระหว่างตัวแปรข้อมูลทางประชากร อาทิ เพศ อายุ ระดับการศึกษา รายได้ต่อเดือน ที่ส่งผลต่อความรู้เกี่ยวกับภัยคุกคามไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ โดยทดสอบระดับความเชื่อมั่นทางสถิติ ที่ร้อยละ 95 รายละเอียดดังภาพที่ 4-3

```
. reg Knowledge sex age edu income

      Source |       SS           df       MS      Number of obs   =       450
-------------+----------------------------------   F(4, 445)       =      5.59
       Model |  4.21167932         4  1.05291983   Prob > F        =    0.0002
    Residual |  83.8404335       445  .188405469   R-squared       =    0.0478
-------------+----------------------------------   Adj R-squared   =    0.0393
       Total |  88.0521128       449  .196107156   Root MSE        =    .43406

------------------------------------------------------------------------------
   Knowledge |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
         sex |  -.0293009   .0436424    -0.67   0.502    -.1150717    .0564698
         age |   .0113731   .0186751     0.61   0.543    -.0253292    .0480755
         edu |  -.0768747   .0256657    -3.00   0.003    -.1273158   -.0264337
      income |   .0860347   .0210128     4.09   0.000     .0447381    .1273314
       _cons |   4.512333   .0962834    46.87   0.000     4.323106     4.70156
------------------------------------------------------------------------------
```

ภาพที่ 4-3 ผลลัพธ์ความสัมพันธ์ระหว่างปัจจัยทางลักษณะประชากรส่งผลต่อความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

จากภาพที่ 4-3 พบว่าปัจจัยเพศและปัจจัยอายุของผู้ตอบแบบสอบถามไม่มีความสัมพันธ์และไม่ส่งผลต่อความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ โดยวัดที่ระดับนัยสำคัญทางสถิติที่ 0.05 ไม่มีระดับนัยสำคัญทางสถิติ ระดับความเชื่อมั่นทางสถิติร้อยละ 95 ในขณะที่ปัจจัยระดับการศึกษาละปัจจัยทางรายได้ของผู้ตอบแบบสอบถามมีความสัมพันธ์ต่อ ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ในทิศทางเดียวกันเมื่อระดับการศึกษาสูงขึ้นจะส่งผลต่อการตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกร รมการเงินออนไลน์เพิ่มขึ้นเช่นเดียวกันกับระดับรายได้ที่สูงขึ้นจะส่งผลต่อ ความรู้ฯที่เพิ่มขึ้น โดยวัดที่ระดับนัยสำคัญทางสถิติที่ 0.05 มีระดับนัยสำคัญทางสถิติ ที่ระดับความเชื่อมั่นทางสถิติร้อยละ 95 โดยที่ค่า รากที่สองค่าเฉลี่ยความคลาดเคลื่อนกำลังสอง (Root Mean Square Error) มีค่าเท่ากับ 0.44 โดยเฉลี่ยตัวแปรข้อมูลทางประชากรทำนายความสัมพันธ์เชิงเส้นกับความรู้ เกี่ยวกับภัยคุกคามทางไซเบอร์คลาดเคลื่อนไปเพียง 0.44 หน่วย กล่าวโดยสรุปปัจจัยทางด้านประชากรมีความสัมพันธ์เชิงเส้นกับความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ดังแสดงในภาพที่ 4-4



ภาพที่ 4-4 ความสัมพันธ์เชิงเส้นของตัวแปรข้อมูลทางประชากรต่อต่อความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

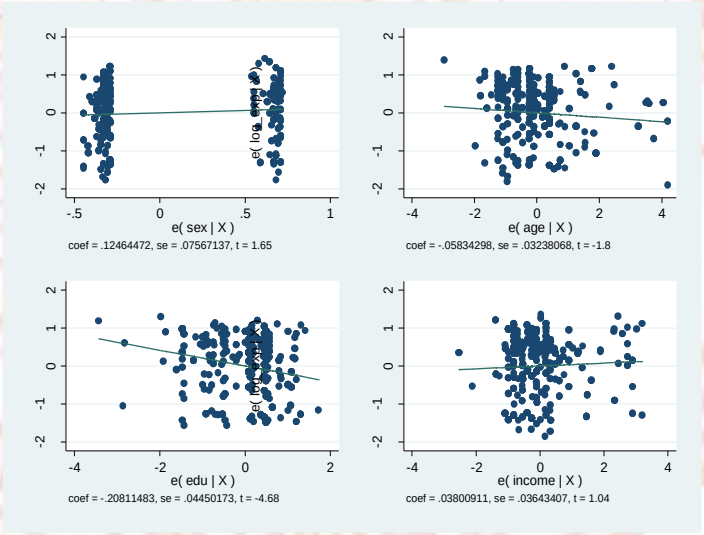
4.6 ผลการวิจัยความสัมพันธ์ระหว่างตัวแปรข้อมูลทางประชากรต่อประสบการณ์เกี่ยวกับภัยคุกคามไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

จากข้อมูลที่เก็บได้จากกลุ่มตัวอย่างจำนวน 450 คน นำมาทดสอบความสัมพันธ์ระหว่างตัวแปรข้อมูลทางประชากร อาทิ เพศ อายุ ระดับการศึกษา รายได้ต่อเดือน ที่ส่งผลต่อประสบการณ์เกี่ยวกับภัยคุกคามไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ โดยทดสอบระดับความเชื่อมั่นทางสถิติที่ร้อยละ 95 รายละเอียดดังภาพที่ 4-5

```
. reg log_exp sex age edu income

      Source |       SS           df       MS      Number of obs   =       450
-------------+----------------------------------   F(4, 445)       =      8.15
       Model |  18.4623385         4  4.61558461   Prob > F        =    0.0000
    Residual |  252.057812       445   .56642205   R-squared       =    0.0682
-------------+----------------------------------   Adj R-squared   =    0.0599
       Total |  270.520151       449   .602494768   Root MSE        =    .75261

------------------------------------------------------------------------------
     log_exp |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
         sex |   .1246447   .0756714     1.65   0.100    -.0240729    .2733624
         age |   -.058343   .0323807    -1.80   0.072     -.121981    .0052951
         edu |  -.2081148   .0445017    -4.68   0.000    -.2955745   -.1206552
      income |   .0380091   .0364341     1.04   0.297    -.0335951    .1096133
       _cons |   2.167398   .1669455    12.98   0.000     1.839298    2.495497
------------------------------------------------------------------------------
```

ภาพที่ 4-5 ผลลัพธ์ความสัมพันธ์ระหว่างปัจจัยทางลักษณะประชากรส่งผลต่อประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

จากภาพที่ 4-5 พบว่าปัจจัยระดับการศึกษาของผู้ตอบแบบสอบถามมีความสัมพันธ์และส่งผลต่อประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ โดยวัดที่ระดับนัยสำคัญทางสถิติที่ 0.05 มีระดับนัยสำคัญทางสถิติ ระดับความเชื่อมั่นทางสถิติร้อยละ 95 สำหรับปัจจัยระดับการศึกษามีความสัมพันธ์ต่อประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ในทิศทางตรงกันข้ามหมายความว่า กลุ่มผู้ตอบแบบสอบถามที่ระดับการศึกษาที่น้อยยิ่งมีการพบเจอประสบการณ์ของภัยคุกคามทางไซเบอร์เพิ่มขึ้น ในขณะที่ปัจจัยทางรายได้ เพศและอายุของผู้ตอบแบบสอบถามไม่มีความสัมพันธ์ต่อประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ โดยวัดที่ระดับนัยสำคัญทางสถิติที่ 0.05 มีระดับนัยสำคัญทางสถิติ ที่ระดับความเชื่อมั่นทางสถิติร้อยละ 95 โดยที่ค่า รากที่สองค่าเฉลี่ยความคลาดเคลื่อนกำลังสอง มีค่าเท่ากับ 0.75 โดยเฉลี่ยตัวแปรข้อมูลทางประชากรทำนายความสัมพันธ์เชิงเส้นกับประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์คลาดเคลื่อนไปเพียง 0.75 หน่วย กล่าวโดยสรุป ปัจจัยทางด้านประชากรมีความสัมพันธ์เชิงเส้นกับประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ ดังแสดงในภาพที่ 4-6



ภาพที่ 4-6 ความสัมพันธ์เชิงเส้นของตัวแปรข้อมูลทางประชากรต่อประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

4.7 ผลการวิจัยความสัมพันธ์ระหว่างตัวแปรข้อมูลทางประชากรต่อความตระหนักรู้เกี่ยวกับภัยคุกคามไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

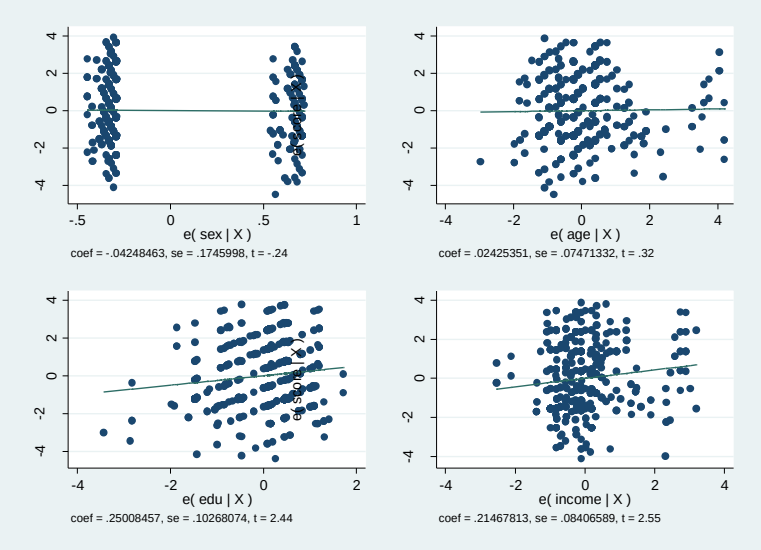
จากข้อมูลที่เก็บได้จากกลุ่มตัวอย่างจำนวน 450 คน นำมาทดสอบความสัมพันธ์ระหว่างตัวแปรข้อมูลทางประชากร อาทิ เพศ อายุ ระดับการศึกษา รายได้ต่อเดือน ที่ส่งผลต่อการตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ โดยทดสอบระดับความเชื่อมั่นทางสถิติที่ร้อยละ 95 รายละเอียดดังภาพที่ 4-7 ตามลำดับ

```
. reg score sex age edu income

      Source |       SS           df       MS      Number of obs   =       450
-------------+----------------------------------   F(4, 445)       =      5.94
       Model |  71.6980131         4  17.9245033   Prob > F        =    0.0001
    Residual |   1341.9131       445  3.01553505   R-squared       =    0.0507
-------------+----------------------------------   Adj R-squared   =    0.0422
       Total |  1413.61111       449  3.14835437   Root MSE        =    1.7365

------------------------------------------------------------------------------
       score |      Coef.   Std. Err.      t    P>|t|     [95% Conf. Interval]
-------------+----------------------------------------------------------------
         sex |  -.0424846   .1745998    -0.24   0.808    -.3856272     .300658
         age |   .0242535   .0747133     0.32   0.746    -.1225813    .1710883
         edu |   .2500846   .1026807     2.44   0.015     .0482852     .451884
      income |   .2146781   .0840659     2.55   0.011     .0494627    .3798936
       _cons |   5.106639   .3852006    13.26   0.000     4.349601    5.863678
------------------------------------------------------------------------------
```

ภาพที่ 4-7 ผลลัพธ์ความสัมพันธ์ระหว่างปัจจัยทางลักษณะประชากรส่งผลต่อความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

จากภาพที่ 4-7 พบว่าปัจจัยเพศและปัจจัยอายุของผู้ตอบแบบสอบถามไม่มีความสัมพันธ์และไม่ส่งผลต่อการตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ โดยวัดที่ระดับนัยสำคัญทางสถิติที่ 0.05 ไม่มีระดับนัยสำคัญทางสถิติ ระดับความเชื่อมั่นทางสถิติร้อยละ 95 ในขณะที่ปัจจัยระดับการศึกษาละปัจจัยทางรายได้ของผู้ตอบแบบสอบถามมีความสัมพันธ์ต่อการตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ในทิศทางเดียวกัน เมื่อระดับการศึกษาสูงขึ้นจะส่งผลต่อการตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์เพิ่มขึ้นเช่นเดียวกันกับระดับรายได้ที่สูงขึ้นจะส่งผลต่อการตระหนักรู้ฯที่เพิ่มขึ้น โดยวัดที่ระดับนัยสำคัญทางสถิติที่ 0.05 มีระดับนัยสำคัญทางสถิติ ที่ระดับความเชื่อมั่นทางสถิติร้อยละ 95 โดยที่ค่า รากที่สองค่าเฉลี่ยความคลาดเคลื่อนกำลังสอง มีค่าเท่ากับ 1.73 โดยเฉลี่ยตัวแปรข้อมูลทางประชากรทำนายความสัมพันธ์เชิงเส้นกับความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์คลาดเคลื่อนไปเพียง 1.73 หน่วย กล่าวโดยสรุปปัจจัยทางด้านประชากรมีความสัมพันธ์เชิงเส้น

กับความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ ดังแสดงในภาพที่ 4-8



ภาพที่ 4-8 ความสัมพันธ์เชิงเส้นของตัวแปรข้อมูลทางประชากรต่อความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

4.8 ผลการวิจัยความสัมพันธ์ของตัวแปรต้นและตัวแปรตาม

ตัวแปรต้น หรือ ข้อมูลทางลักษณะประชากรด้านแก่ เพศ, อายุ, ระดับการศึกษา, รายได้ต่อเดือน ส่วนตัวแปรตาม ได้แก่ ความรู้ฯ, ประสบการณ์ฯ, ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์จะมีความสัมพันธ์กันโดยที่

✓ หมายถึง ตัวแปรต้นกับตัวแปรตามมีความสัมพันธ์ต่อกัน

X หมายถึง ตัวแปรต้นกับตัวแปรตามไม่มีความสัมพันธ์ต่อกัน

ดังตารางที่ 4-8

ตารางที่ 4-8 ความสัมพันธ์ของตัวแปรต้นและตัวแปรตาม

ตัวแปรตาม / ตัวแปรต้น	ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์	ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์	ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์
เพศ	X	X	X
อายุ	X	X	X
ระดับการศึกษา	✓	✓	✓
รายได้ต่อเดือน	✓	X	✓

จากตารางที่ 4-8 พบว่า เพศและอายุไม่มีความสัมพันธ์ต่อความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ และ ไม่มีความสัมพันธ์ต่อประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ และ ไม่มีความสัมพันธ์ต่อความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ และยังพบว่า ระดับการศึกษา มีความสัมพันธ์กับความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ และ มีความสัมพันธ์กับประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ และ มีความสัมพันธ์กับความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ นอกจากนี้ยังพบว่า รายได้ต่อเดือน มีความสัมพันธ์กับความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ และ มีความสัมพันธ์กับความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ แต่ไม่มีความสัมพันธ์กับประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

บทที่ 5
อภิปรายผล

5.1 อภิปรายผล

จากการดำเนินการวิจัยตามวัตถุประสงค์ของการศึกษาในครั้งนี้เพื่อศึกษาปัจจัยทางด้านลักษณะประชากรที่มีผลต่อความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และด้านประสบการณ์ภัยคุกคามไซเบอร์ความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์และเพื่อหาปัจจัยที่ส่งผลกระทบต่อการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ ทำให้พบว่าปัจจัยอายุ ระดับการศึกษา ระดับรายได้ต่อเดือนของผู้ตอบแบบสอบถามมีความสัมพันธ์และส่งผลต่อการตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์โดยวัดที่ระดับนัยสำคัญทางสถิติที่ 0.05 ระดับความเชื่อมั่นทางสถิติร้อยละ 95 มีเพียงปัจจัยเพศของผู้ตอบแบบสอบถามไม่มีความสัมพันธ์และไม่ส่งผลต่อการตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ สอดคล้องกับการศึกษาของสุธาเทพ รุณเรศ (2561) วิจัยเรื่อง “ปัจจัยที่มีผลต่อการตระหนักรู้ถึงภัยคุกคามไซเบอร์ของผู้ใช้อินเตอร์เน็ตในกรุงเทพมหานคร” ผลการวิจัยพบว่า ปัจจัยทางด้านลักษณะประชากร อายุ ระดับการศึกษาสูงสุด และรายได้ล้วนส่งผลต่อความรู้ถึงภัยคุกคามของผู้ใช้อินเตอร์เน็ต มีเพียงปัจจัยเพศที่ไม่ส่งผล เมธาพร ธรรมศิริและศิรภัสสรศ์ วงศ์ทองดี (2565) ศึกษาเรื่อง “ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร” พบว่าบุคลากรในบริษัทเอกชนปัจจัยทางประชากร เพศ อายุ ประสบการณ์ทำงานที่ต่างกันมีระดับความตะหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่ไม่แตกต่างกัน และในบุคคลที่มีระดับการศึกษาที่สูงมีผลต่อการตระหนักรู้ภัยคุกคามอย่างมีนัยยะสำคัญทางสถิติเช่นเดียวกับการศึกษาของสุทธิพันธ์ ชวลิตเลขา (2564)

อย่างไรก็ตามจากผลการศึกษาในครั้งนี้ยังพบว่ากลุ่มตัวอย่างของการศึกษามีความรู้ด้านภัยคุกคามทางไซเบอร์ของการทำธุรกรรมการเงินออนไลน์ โดยส่วนใหญ่เข้าใจว่าการเข้าใช้เครือข่ายไร้สายสาธารณะ ทำให้ผู้ใช้มีความเสี่ยงต่อการทำธุรกรรมออนไลน์ ควรมีการตั้งรหัสผ่านต่างๆ ที่มีความยาวมาก ช่วยลดโอกาสการคาดเดารหัสผ่านหรือใช้เวลาในการคาดเดายากมากขึ้นและการบันทึกรหัสผ่านต่างๆ ไว้ในเครื่องที่เชื่อมต่อกับเครือข่ายไร้สายสาธารณะมีความเสี่ยงต่อภัยคุกคามโจมตีการทำธุรกรรมออนไลน์สูงมาก ทั้งนี้การเข้าเว็บไซต์ Https มีความปลอดภัยมากกว่า ในขณะที่กลุ่มตัวอย่างเองยังขาดความตระหนักรู้ว่า 1) การให้ข้อมูลส่วนตัวบนเครือข่ายสังคมออนไลน์สาธารณะทำให้ผู้ให้ข้อมูลส่วนตัวมีความเสี่ยงต่อการทำธุรกรรมออนไลน์

2) การโหลดแอปพลิเคชั่นจากแหล่งต่างๆ เช่น เว็บไซต์ที่ไม่มีความน่าเชื่อถือ ทำให้มีความเสี่ยงจากการโดนโจรกรรมข้อมูล 3) การตั้งรหัสผ่านในอุปกรณ์ต่างๆที่มีลักษณะการตั้งรหัสผ่านเหมือนกันในทุกอุปกรณ์ 4) ขาดความเข้าใจการใช้รหัสผ่านหลายชั้นจะมีความปลอดภัยมากกว่ามีความเข้าใจว่าไม่จำเป็นต้องมีการใช้รหัสผ่านครั้งเดียว (One Time Password: OTP) และ 5) การคลิกเปิดลิงค์ในจดหมายอิเล็กทรอนิกส์ที่ได้รับจากแหล่งหรือบุคคลที่ไม่รู้จักก่อให้เกิดความเสี่ยงต่อการทำธุรกรรมออนไลน์ ยังมีความเข้าใจคลาดเคลื่อน ด้านประสบการณ์ที่เคยประสบพบของการคุกคามด้านธุรกรรมส่วนใหญ่จะเคย 1)ได้รับจดหมายอิเล็กทรอนิกส์หลอกลวงให้ทำธุรกรรมการเงินไลน์ 2) เคยถูกคอลเซ็นเตอร์มิจฉาชีพหลอกลวงให้ทำธุรกรรมการเงินออนไลน์และ 3) เคยถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าสู่ระบบ นอกจากนี้มีประสบการณ์บ้างในการถูกคุกคามในรูปแบบอื่น อาทิเช่น 1) เคยได้รับผลกระทบจากโปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมาเพื่อทำอันตรายกับข้อมูลในระบบ เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติมีการขโมยหรือทำลายข้อมูลหรืออาจจะเปิดช่องทางให้กับผู้ไม่หวังดีเข้ามาควบคุมเครื่องคอมพิวเตอร์ทำให้ข้อมูลส่วนตัวรั่วไหล เป็นต้น ซึ่งทำให้มีบุคคลอื่นสามารถใช้บริการธุรกรรมการเงินของท่านได้ 2) เคยติดตั้งโปรแกรมหรือแอปพลิเคชั่นที่คิดว่าปลอดภัยแต่มี โปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมาเพื่อทำอันตรายกับข้อมูลในระบบแฝงตัวมา ทำให้มีบุคคลอื่น สามารถทำธุรกรรมการเงินของท่านได้ 3) เคยได้รับการก่อกวน เช่น การปฏิเสธการให้บริการแบบกระจายในระบบเครือข่ายทำให้ไม่สามารถใช้บริการธุรกรรมการเงินออนไลน์ได้ 4) เคยถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์หรือโทรศัพท์โดยที่ไม่รู้ตัว และ5) เคยถูกหลอกให้รักและให้ทำธุรกรรมการเงินออนไลน์ตลอดจนหลอกให้ซื้อขายสินค้าหรือบริการทางเครือข่ายสังคมออนไลน์

5.2 ข้อเสนอแนะ

ควรจะมีการศึกษาเพิ่มเติมด้วยวิธีวิจัยเชิงคุณภาพเพิ่มเติมด้วยการสัมภาษณ์เชิงลึกหรือการสัมภาษณ์แบบกลุ่มเพื่อสะท้อนปัญหาที่เกิดขึ้นอย่างแท้จริงนำมาสู่การหาวิธีป้องกันและแก้ปัญหาให้กับประชาชนที่ถูกภัยคุกคามทางไซเบอร์ต่อการทำธุรกรรมการเงินออนไลน์และให้ความรู้ด้านภัยคุกคามทางไซเบอร์แก่ประชาชนอย่างทั่วถึงเพื่อจะมีทักษะในการป้องกันและรับมือกับปัญหาเหล่านี้ได้

5.3 ข้อจำกัด

การศึกษาครั้งนี้มีข้อจำกัดในด้านระยะเวลาในการค้นคว้า การเก็บแบบสอบถามและงบประมาณจำกัดซึ่งอาจจะทำให้ยังมีปัจจัยแฝงอื่นๆที่ส่งผลต่อภัยคุกคามทางไซเบอร์ อาจจะยังไม่ครอบคลุมทุกปัจจัย

บรรณานุกรม

(ภาษาไทย)

กริน ธัญญวิกรม และธีระ กุลสวัสดิ์. (2564). **การจัดการความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ กรณีศึกษาการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย.** วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยบูรพา.

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลนี. (2566). **สถิติแจ้งความออนไลน์.** สืบค้นออนไลน์เมื่อ 24 พฤศจิกายน 2566, จาก https://ccid4.ccib.go.th

กัลยา ชินาธิวร. (2562). **ปัจจัยความสำเร็จของสิงค์โปร: กรณีศึกษาเพื่อประกอบการพัฒนาแนวทางดำเนินการตามนโยบายการรักษาความปลอดภัยไซเบอร์ของไทย.** รายงานการศึกษาส่วนบุคคล หลักสูตรนักบริหารการทูต สถาบันการต่างประเทศเทวะวงศ์วโรปการ, กระทรวงการต่างประเทศ

ธนาคารแห่งประเทศไทย. (2566). **กลโกงธนาคารออนไลน์.** สืบค้นออนไลน์เมื่อ 24 พฤศจิกายน 2566, จาก https://www.bot.or.th/th/satang-story/fraud/online-fraud.html

ธนาคารแห่งประเทศไทย. (2566). **แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมการเงิน.** สืบค้นออนไลน์เมื่อ 24 พฤศจิกายน 2566, จาก https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2566/ThaiPDF/25660066.PDF

ธนาคารแห่งประเทศไทย. (2566). **ภัยทางการเงิน กลโกงออนไลน์รูปแบบอื่นๆ.** สืบค้นออนไลน์เมื่อ 24 พฤศจิกายน 2566, จาก https://www.bot.or.th/th/satang-story/fraud/online-crime.html

นันท์ณิภัค นันทวัฒน์วงษ์. (2561). **ความตระหนักความมั่นคงปลอดภัยด้านระบบสารสนเทศของหน่วยงานด้านการบิน กรณีศึกษา ท่าอากาศยานนานาชาติอุดรธานี กรมท่าอากาศยาน.** วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์.

เมธาพร ธรรมศิริ และ ศิรภัสสรศ์ วงศ์ทองดี. (2565). **ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพ.วารสารวิชาการไทยวิจัยและการจัดการ**

ราชบัณฑิตสถาน. (2562). **พจนานุกรมศัพท์คอมพิวเตอร์และเทคโนโลยีสารสนเทศ**. กรุงเทพฯ : สำนักงานราชบัณฑิตยสภา.

วราภรณ์ เพลิดเพลิน. (2565). **การพัฒนาทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ.** การศึกษาค้นคว้าอิสระรัฐประศาสนศาตรมหาบัณฑิต, มหาวิทยาลัยรามคำแหง

วิลาส วิถีไพร. (2561). **การพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเตอร์เน็ตประสานสรรพสิ่ง.**การค้นคว้าอิสระมหาบัณฑิต, มหาวิทยาลัยศรีปทุม

สกาวฟ้า จันทภาโส. (2563). **การพัฒนาแอปพลิเคชั่น เพื่อสร้างความตระหนักรู้ เรื่องการระราน ทางไซเบอร์ สำหรับนักเรียนชั้นมัธยมศึกษาปีที่ 1**.การค้นคว้าอิสระบัณฑิต, มหาวิทยาลัยศรีนครินทรวิโรฒ.

สมาคมธนาคารไทย. (2566). **ธปท. สมาคมธนาคารไทย และสมาคมสถาบันการเงินของรัฐจับมือยกระดับการจัดการภัยทุจริตทางการเงิน.** สืบค้นออนไลน์เมื่อ 27 พฤศจิกายน 2566, จาก https://www.tba.or.th/financial-fraud/

สมาคมธนาคารไทย. (2566). **เปิดความเสียหายภัยการเงิน 4 หมื่นล้าน ธปท. งัดมาตราการเผาบัญชีม้า.** สืบค้นออนไลน์เมื่อ 27 พฤศจิกายน 2566, จาก https://www.tba.or.th/

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2560). Electronic Transections Development Agency.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2564). **CS101 ความมั่นคงปลอดภัยไซเบอร์เบื้องต้น.** สืบค้นออนไลน์เมื่อ 27 พฤศจิกายน 2566, จาก https://www.etda.or.th/th/Useful-Resource/Knowledge-Sharing/Articles/Cybersecurity-101.aspx

สุทธิพันธ์ ชวลิตเลขา. (2564). **การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรภายในบริษัทวิทยุการบินแห่งประเทศไทยจำกัด.** สารนิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ, มหาวิทยาลัยศรีปทุม.

สุธาเทพ รุณเรศ. (2561). **ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเตอร์เน็ตในกรุงดทพมหานคร.** การศึกษาค้นคว้าอิสระวิทยาศาสตรมหาบัณฑิต, สาขาวิชานโยบายและการบริหารเทคโนโลยีสารสนเทศ, มหาวิทยาลัยธรรมศาสตร์.

สุพิตรา ศรีบุรินทร์ และ พัชชกร แสงทองดี. (2564). **การตระหนักรู้ในการป้องกันตนเองบนโลกไซเบอร์ของประชาชนในเขตเทศบาลตำบลอ้อมใหญ่.** *Crime and Safety Journal*, *3* (1), 63–74.

สุรชัย ฉัตรเฉลิมพันธุ์ และ เทอดพงษ์ แดงสี. (2563). **การเสริมสร้างความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในองค์กร : กรณีจำลองการโจมตีด้วยฟิชชิ่ง.** สารนิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม.

(ภาษาอังกฤษ)

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

Draper, N. R., & Smith, H. (1998). ***Applied regression analysis*** **(3rd ed.)**. Wiley.

Hastie, T., Tibshirani, R., & Friedman, J. (2009). ***The elements of statistical learning: Data mining, inference, and prediction*** **(2nd ed.)**. Springer.

World Economic Forum. (2023). **Global Cybersecurity Outlook 2023.** Retrieved from https://www.weforum.org/publications/global-cybersecurity-outlook-2023/.

ภาคผนวก ก.
แบบสอบถาม ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร และประวัติผู้เชี่ยวชาญ

แบบสอบถาม “ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร”

คำชี้แจง 1.แบบสอบถามนี้เป็นส่วนหนึ่งของหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

<u>วัตถุประสงค์</u> แบบสอบถามนี้มีจุดประสงค์เพื่อศึกษาถึงปัจจัยและเก็บรวบรวมข้อมูลและนำข้อมูลไปใช้ในการวิเคราะห์ ในงานวิจัย เรื่อง “ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร” ทั้งนี้ผลที่ได้จากแบบสอบถาม ผู้วิจัยจะนำเป็นแนวทางเพื่อทำให้ทราบถึงปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานครให้เกิดประสิทธิภาพสูงสุด

2.แบบสอบถามชุดนี้แบ่งออกเป็น 4 ตอน ดังนี้

•ตอนที่ 1 ลักษณะทางประชากร

•ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

•ตอนที่ 3 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

•ตอนที่ 4 ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

3.หากท่านมีข้อสงสัยเกี่ยวกับคำถามสัมภาษณ์ กรุณาติดต่อผู้วิจัย นาย ณศรัณย์ ขำหาญ

Email : <u>icenasarun@gmail.com</u> / s6507031858237@email.kmutnb.ac.th

ตอนที่ 1 ลักษณะทางประชากร

คำอธิบาย : คำถามต่อไปนี้เกี่ยวข้องกับข้อมูลส่วนตัวของท่านกรุณาเลือกคำตอบที่ตรงกับความคิดเห็นและข้อเท็จจริงมากที่สุด

1. เพศ

❍ 1. ชาย

❍2. หญิง

2. อายุ

❍1. 15-20 ปี

❍2. 21-30 ปี

❍3. 31-40 ปี

❍4. 41-50 ปี

❍5. 51-60 ปี

❍6. 61 ปีขึ้นไป

3. ระดับการศึกษาสูงสุด

❍1. ต่ำกว่ามัธยมศึกษา

❍2. มัธยมศึกษาตอนต้น

❍3. มัธยมศึกษาตอนปลาย หรือเทียบเท่า

❍4. ปริญญาตรี

❍5. ปริญญาโท

❍6. ปริญญาเอก

4. รายได้

❍1.ไม่เกิน 15,000 บาท

❍2. 15,001 – 30,000 บาท

❍3. 30,001 – 45,000 บาท

❍4. 45,001 – 50,000 บาท

❍5. 50,001 บาทขึ้นไป

ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

คำอธิบาย : คำถามต่อไปนี้เกี่ยวข้องกับปัจจัย ความรู้ การใช้งาน การทำธุรกรรม และ การกระทำกิจกรรมต่างๆ ของท่านกรุณา เลือกคำตอบ ใช่ หรือ ไม่ใช่ ที่ตรงกับความคิดเห็นและข้อเท็จจริงมากที่สุด

ประกอบไปด้วยคำถาม จำนวน 10 ข้อ ได้แก่

(ตอบได้ข้อละหนึ่งคำตอบ)

ข้อความ	ใช่	ไม่ใช่
1.การให้ข้อมูลส่วนตัวบนเครือข่ายสังคม (Social Media) สาธารณะ ทำให้ผู้ให้ข้อมูลส่วนตัวไม่มีความเสี่ยงต่อการทำธุรกรรมออนไลน์		
2.การเข้าใช้เครือข่ายไร้สาย (Wifi) สาธารณะ ทำให้ผู้ใช้มีความเสี่ยงต่อการทำธุรกรรมออนไลน์		
3.การติดตามข่าวสารรูปแบบการโจมตีทางไซเบอร์ต่างๆ สามารถช่วยให้รับมือกับการโจมตีทางไซเบอร์ที่เกิดขึ้นได้		
4.การโหลดแอปพลิเคชั่น (Application) จากแหล่งต่างๆ เช่น เว็บไซต์ที่ไม่มีความน่าเชื่อถือ ทำให้มีความปลอดภัยจากการโดนโจรกรรมข้อมูล		
5.การตั้งรหัสผ่าน (Password) ต่างๆ ที่มีความยาวมาก ช่วยลดโอกาสการเดา Password หรือใช้เวลาในการเดามากขึ้น		
6.การตั้งรหัสผ่าน (Password) ใน Device ต่างๆ ควรจะตั้งเหมือนๆกัน		
7.การบันทึกรหัสผ่าน (Password) ต่างๆ ไว้ในเครื่องที่เชื่อมต่อกับเครือข่ายไร้สาย (Wifi) สาธารณะ มีความเสี่ยงต่อการทำธุรกรรมออนไลน์		
ข้อความ	ใช่	ไม่ใช่
8.การคลิกเปิดลิงค์ (Link) ในจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ได้รับ จากแหล่งหรือบุคคลที่ไม่รู้จัก ไม่ทำให้เกิดความเสี่ยงต่อการทำธุรกรรมออนไลน์		
9.การใช้รหัสผ่าน (Password) หลายชั้น และ หลากหลาย เช่น ชั้นที่ 1 รหัสผ่านที่ตั้งขึ้นมา กับ ชั้นที่ 2 มีการยืนยัน OTP ทำให้มีความเสี่ยงต่อการทำธุรกรรมออนไลน์เพิ่มขึ้น		
10.การเข้าเว็บไซต์ Https มีความปลอดภัยมากกว่า Http		

เกณฑ์การให้คะแนนคือ

ข้อที่ตอบ ใช่ แล้วได้ 1 คะแนน ได้แก่ข้อ 2,3,5,7,10

ข้อที่ตอบ ไม่ใช่ แล้วได้ 1 คะแนน ได้แก่ข้อ 1,4,6,8,9

หลังจากนั้นจะนำคะแนนที่ได้ ซึ่งตอบถูกตามเฉลยข้างต้น มารวมเป็นคะแนนความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อใช้ในการทดสอบสมมติฐาน

อย่างไรก็ตาม ได้นำคะแนนรวมนั้นมาแบ่งเป็นระดับความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เป็น 3 ระดับ ดังนี้

0 – 3 คะแนน หมายถึง มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับน้อย
4 – 6 คะแนน หมายถึง มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับปานกลาง
7 – 10 คะแนน หมายถึง มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับมาก

ตอนที่ 3 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

คำอธิบาย : คำถามต่อไปนี้เกี่ยวข้อกับผลกระทบจากภัยคุกคามทางไซเบอร์ ท่านเคยประสบปัญหาเหล่านี้หรือไม่กรุณาทำเครื่องหมาย ✓ ลงในช่องว่างที่ตรงกับความคิดเห็นและข้อเท็จจริงมากที่สุด ประกอบไปด้วยคำถามแบบตอบได้มากกว่าหนึ่งคำตอบ (Multiple Responses) จำนวน 10 ข้อ ได้แก่

(ตอบได้มากกว่าหนึ่งคำตอบ)

☐1.ท่านเคยได้รับผลกระทบจากโปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมา เพื่อทำอันตรายกับข้อมูลในระบบ (Malware) เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ มีการขโมยหรือทำลายข้อมูลหรืออาจจะเปิดช่องทางให้กับผู้ไม่หวังดีเข้ามาควบคุมเครื่องคอมพิวเตอร์ ทำให้ข้อมูลส่วนตัวรั่วไหล เป็นต้น ซึ่งทำให้มีบุคคลอื่นสามารถใช้บริการธุรกรรมการเงินของท่านได้

☐2.ท่านเคยได้รับการก่อกวน เช่น DDOS ในระบบเครือข่ายทำให้ไม่สามารถใช้บริการธุรกรรมการเงินออนไลน์ได้

☐3.ท่านเคยติดตั้งโปรแกรมหรือแอปพลิเคชั่นที่คิดว่าปลอดภัยแต่มี โปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมาเพื่อทำอันตรายกับข้อมูลในระบบ (Malware) แฝงตัวมา ทำให้มีบุคคลอื่น สามารถทำธุรกรรมการเงินของท่านได้

☐4.ท่านเคยถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์หรือโทรศัพท์โดยที่ท่านไม่รู้ตัว

☐5.ท่านเคยถูกหลอกให้ลงทุน และ ได้ทำธุรกรรมการเงิน

☐6.ท่านเคยถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าสู่ระบบ

☐7.ท่านเคยได้รับจดหมายอิเล็กทรอนิกส์ (E-Mail) หลอกลวงให้ทำธุรกรรมการเงิน

☐8.ท่านเคยถูกคอลเซ็นเตอร์ (Call Center) มิจฉาชีพ หลอกลวงให้ทำธุรกรรมการเงิน

☐9.ท่านเคยถูกหลอกให้ซื้อขายสินค้าหรือบริการทางเครือข่ายสังคม (Social Media)

☐10.ท่านเคยถูกหลอกให้รัก และ ให้ทำธุรกรรมการเงิน

เกณฑ์การให้คะแนน คือ

มีประสบการณ์ = 1
ไม่มีประสบกาณ์ = 0

หลังจากนั้นจะรวมคะแนนทั้ง 10 ข้อ เป็นคะแนนรวมประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ เพื่อนำไปใช้ในการทดสอบสมมติฐาน

อย่างไรก็ตาม ได้นำคะแนนรวมนั้นมาแบ่งระดับประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ เป็น 3 ระดับ ดังนี้

0 – 3 คะแนน หมายถึง มีประสบการณ์ระดับน้อย

4 – 6 คะแนน หมายถึง มีประสบการณ์ระดับปานกลาง

7 – 10 คะแนน หมายถึง มีประสบการณ์ระดับมาก

ตอนที่ 4 ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

คำอธิบาย : คำถามต่อไปนี้เกี่ยวข้องกับความคิดเห็นความตระหนักรู้ของท่านกรุณาเลือกคำตอบที่ตรงกับความคิดเห็นและข้อเท็จจริงมากที่สุด

•หมายเหตุ ความหมาย ของ Social Engineering คือ การหลอกลวง ล่อหลอกผู้อื่น ใช้หลักการพื้นฐานทางจิตวิทยาให้เหยื่อเปิดเผยข้อมูล เพื่อให้ได้ผลประโยชน์ตามที่ต้องการ โดยอาศัยจุดอ่อนความรู้เท่าไม่ถึงการณ์ ความไม่รู้ ความประมาท เป็นต้น

5 หมายถึง เห็นด้วยอย่างยิ่ง

4 หมายถึง เห็นด้วย

3 หมายถึง ไม่แน่ใจ

2 หมายถึง ไม่เห็นด้วย

1 หมายถึง ไม่เห็นด้วยอย่างยิ่ง

ประกอบไปด้วยคำถามแบบมาตราส่วนประมาณค่า (Rating Scale) ทั้งหมด 5 ด้าน ด้านละ 3 ข้อ จำนวน15ข้อ ได้แก่

(ตอบได้ข้อละหนึ่งคำตอบ)

ข้อความ	ระดับ				
	5	4	3	2	1
1.ด้านความมั่นคงปลอดภัย (Security)					
1.1ควรตั้ง Password ให้มีความยาวมากๆ เพื่อให้ใช้เวลาในการคาดเดารหัสผ่านมากขึ้น (Brute Force)					
1.2ควรหาทางป้องกันการถูกหลอกให้กรอกข้อมูลส่วนตัวทางเว็บไซต์ปลอม					
1.3ควรหาทางป้องกันโปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมาเพื่อทำอันตรายกับข้อมูลในระบบ (Malware) เช่น โปรแกรม Anti – Virus เป็นต้น					

ข้อความ	ระดับ				
	5	4	3	2	1
2.ด้านการแอบอ้าง (Masquerading)					
2.1ไม่ควรแอบอ้างชื่อหรือภาพผู้อื่นผ่าน Social Media เพื่อทำธุรกรรมการเงิน					
2.2ไม่ควรมีการแอบอ้างชื่อหรือภาพผู้อื่นผ่านการโทรเพื่อทำธุรกรรมการเงิน					
2.3ไม่ควรมีการแอบอ้างชื่อหรือภาพผู้อื่นผ่านการใช้ AI ในการทำ Deep Fake เพื่อทำธุรกรรมการเงิน					
3.ด้านกฎหมาย (Legal)					
3.1ข้อมูลอิเล็กทรอนิกส์ และ ข้อมูลที่เป็นกระดาษสามารถนำไปใช้ตามกฎหมายได้เหมือนกัน					
3.2กฎหมาย PDPA สามารถใช้กับกรณีที่เกิดข้อมูลรั่วไหลได้					
3.3กฎหมาย E-Payment สามารถรองรับระบบภาษี และ เอกสารธุรกรรมทางการอิเล็กทรอนิกส์ได้					
4.ด้านการหลอกลวง (Social Engineering)					
4.1ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านทางเครือข่ายสังคม (Social Media)					
4.2ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านทางจดหมายอิเล็กทรอนิกส์ (E-Mail)					
4.3ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านช่องทางการโทร					
5.ด้านการตอบสนอง (Response)					
5.1เมื่อพบว่าได้ให้ข้อมูลส่วนตัวกับมิจฉาชีพ ควรเปลี่ยนรหัสผ่าน (Password) ใหม่ทั้งหมด และระงับการใช้งานบัตรเดบิต / บัตรเครดิต ทันที					
5.2เมื่อพบว่าได้ให้ข้อมูลส่วนตัวกับมิจฉาชีพ ควรเตือนผู้ใกล้ชิดทั้งหมดและระมัดระวังการหลอกลวงจากมิจฉาชีพมากขึ้น					

ข้อความ	ระดับ				
	5	4	3	2	1
5.ด้านการตอบสนอง (Response)					
5.3เมื่อเกิดเหตุโดนหลอกให้ข้อมูลส่วนตัวหรือทำธุรกรรมการเงินให้มิจฉาชีพไป ควรรวบรวมหลักฐานเพื่อแจ้งความและติดต่อธนาคาร					

หลังจากนั้นจะเฉลี่ยคะแนนทั้ง 15 ข้อ เป็นคะแนนเฉลี่ยความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ เป็น 5 ระดับ ดังนี้

1.00 – 1.49 คะแนน	หมายถึง	มีความตระหนักรู้ระดับน้อย
1.50 – 2.49 คะแนน	หมายถึง	มีความตระหนักรู้ระดับปานกลาง
2.50 – 3.49 คะแนน	หมายถึง	มีความตระหนักรู้ระดับมาก
3.50 – 4.49 คะแนน	หมายถึง	มีความตระหนักรู้ระดับปานกลาง
4.50 – 5.00 คะแนน	หมายถึง	มีความตระหนักรู้ระดับมาก

2. ประวัติผู้เชี่ยวชาญที่ตรวจสอบ ดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์

2.1 ดร.พนิดา ร้อยดวง (ผู้เชี่ยวชาญที่ให้ปรึกษาด้านการเงิน)
ตำแหน่ง ผู้อำนวยการส่วนการวิจัยนโยบายหนี้สาธารณะ สำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง

2.2 ดร.วศิน พิพัฒนฉัตร (ผู้เชี่ยวชาญที่ให้ปรึกษาด้านการกฎหมาย)
ตำแหน่ง ผู้จัดการโครงการหน่วยวิชาการเครือข่ายนักจัดการปัจจัยเสี่ยง มหาวิทยาลัยมหิดล และ
ทนาย บริษัท นิติหาญ จำกัด

2.3 อาจารย์ศรัญญา แจ้งขำ (ผู้เชี่ยวชาญที่ให้ปรึกษาด้านการบริหารความเสี่ยง)
ตำแหน่ง คณะกรรมการบริหารความเสี่ยง มหาวิทยาลัยธนบุรี

ภาคผนวก ข.

เอกสารดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์

ร่างแบบสอบถามเพื่อการวิจัย (IOC)

เรื่อง แบบสอบถามสำหรับกลุ่มตัวอย่าง เพื่อศึกษาเรื่อง

"ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร"

คำชี้แจง

1. แบบสอบถามฉบับนี้ อยู่ในขั้นตอนการศึกษาปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร

2. แบบสอบถามฉบับนี้มุ่งตรวจสอบ เพื่อหาค่าความเที่ยงตรง (Validity) โดยการวิเคราะห์ดัชนีความสอดคล้อง (Index of item object congruence : IOC) ของแบบสอบถามและข้อเสนอแนะของผู้เชี่ยวชาญ เพื่อนำไปปรับปรุงแบบสอบถามให้สมบูรณ์ขึ้น

3. แบบสอบถามฉบับนี้มีทั้งหมด 4 ตอน

ตอนที่ 1 ลักษณะทางประชากร

ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

ตอนที่ 3 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

ตอนที่ 4 ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

4. ขอความกรุณาผู้ทรงคุณวุฒิหรือท่านผู้เชี่ยวชาญ ช่วยพิจารณาร่างแบบสอบถามว่ามีความสอดคล้องกับตัวแปรของการวิจัยเรื่องนี้หรือไม่ ด้วยการให้คะแนนในแต่ละข้อความในระบบ IOC โดยการทำเครื่องหมาย ✓ ลงในช่องว่าง

เกณฑ์การให้คะแนนในระบบ IOC

1) ให้ 1 คะแนน เมื่อแน่ใจว่าข้อนั้นมีเนื้อหาที่สอดคล้องกับตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา

2) ให้ 0 คะแนน เมื่อไม่แน่ใจว่าข้อนั้นมีเนื้อหาที่สอดคล้องตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา

3) ให้ -1 คะแนน เมื่อแน่ใจว่าข้อนั้นมีเนื้อหาที่ไม่สอดคล้องกับตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา

5. ผู้วิจัยขอความกรุณาท่านผู้ทรงคุณวุฒิและผู้เชี่ยวชาญ ให้ข้อเสนอแนะหรือความคิดเห็นเพิ่มเติมในประเด็นที่ยังไม่สมบูรณ์ โดยการเขียนข้อเสนอแนะไว้ท้ายข้อความนั้นๆ

ผู้วิจัยขอขอบพระคุณในความกรุณาของท่านมา ณ โอกาส นี้

นาย ณศรัณย์ ขำหาญ

นักศึกษาปริญญาโท (การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ)

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ภาพที่ ข-1 IOC จาก ดร.พนิดาส่วนที่ 1

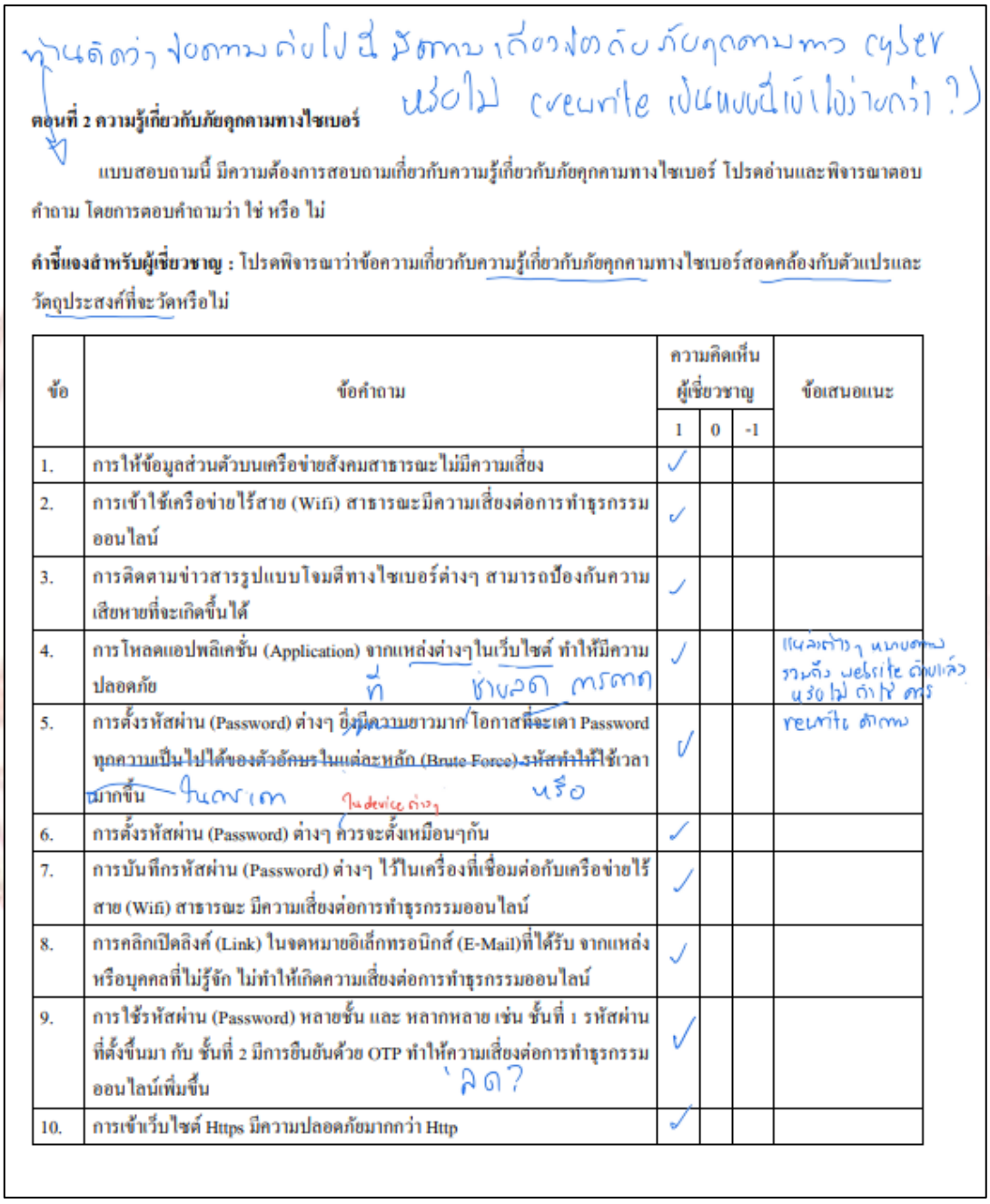
ตอนที่ 1 ลักษณะทางประชากร

คำชี้แจงของผู้ตอบแบบสอบถาม : กรุณาทำเครื่องหมาย ✓ ลงใน ( ) หรือเติมข้อความที่ตรงกับความเป็นจริง

คำชี้แจงสำหรับผู้เชี่ยวชาญ : โปรดพิจารณาว่าข้อความเกี่ยวกับลักษณะทางประชากรผู้ตอบเหมาะสมหรือไม่อย่างไร

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1.	เพศ ( ) ชาย ( ) หญิง	✓			
2.	อายุ ( ) ไม่เกิน 20 ปี ( ) 21 – 30 ปี ( ) 31 – 40 ปี ( ) 41 – 50 ปี ( ) 51 – 60 ปี ( ) 61 ปีขึ้นไป	✓			
3.	ระดับการศึกษาสูงสุด ( ) ต่ำกว่ามัธยมศึกษาตอนต้น ( ) มัธยมศึกษาตอนต้น ( ) มัธยมศึกษาตอนปลาย / ปวช. ( ) ปริญญาตรี ( ) สูงกว่าปริญญาโท	✓			
4.	รายได้ ( ) ไม่เกิน 15,000 บาท ( ) 15,001 – 30,000 บาท ( ) 30,001 – 45,000 บาท ( ) 45,001 – 50,000 บาท ( ) 50,001 บาทขึ้นไป	✓			

ภาพที่ ข-2 IOC จาก ดร.พนิดาส่วนที่ 2



ท่านคิดว่า ข้อความต่อไปนี้ มีความเกี่ยวข้องกับคุกคามทาง cyber หรือไม่ (rewrite เป็นแบบนี้เข้าใจง่ายกว่า ?)

ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

แบบสอบถามนี้ มีความต้องการสอบถามเกี่ยวกับความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ โปรดอ่านและพิจารณาตอบคำถาม โดยการตอบคำถามว่า ใช่ หรือ ไม่

คำชี้แจงสำหรับผู้เชี่ยวชาญ : โปรดพิจารณาว่าข้อความเกี่ยวกับความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์สอดคล้องกับตัวแปรและวัตถุประสงค์ที่จะวัดหรือไม่

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1.	การให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะไม่มีความเสี่ยง	✓			
2.	การเข้าใช้เครือข่ายไร้สาย (Wifi) สาธารณะมีความเสี่ยงต่อการทำธุรกรรมออนไลน์	✓			
3.	การติดตามข่าวสารรูปแบบโจมตีทางไซเบอร์ต่างๆ สามารถป้องกันความเสียหายที่จะเกิดขึ้นได้	✓			
4.	การโหลดแอปพลิเคชั่น (Application) จากแหล่งต่างๆในเว็บไซต์ ทำให้มีความปลอดภัย (ที่ ช่วยลด ความ)	✓			(แหล่งต่างๆ หมายความถึง website ดีพอแล้ว หรือไม่ ถ้าใช่ ควร rewrite ตาม)
5.	การตั้งรหัสผ่าน (Password) ต่างๆ ยิ่งมีความยาวมาก โอกาสที่จะเดา Password ทุกความเป็นไปได้ของตัวอักษรในแต่ละหลัก (Brute Force) รหัสก็จะใช้เวลามากขึ้น (ในความ ในแต่ละ device ต่างๆ หรือ)	✓			rewrite ตาม
6.	การตั้งรหัสผ่าน (Password) ต่างๆ ควรจะตั้งเหมือนๆกัน	✓			
7.	การบันทึกรหัสผ่าน (Password) ต่างๆ ไว้ในเครื่องที่เชื่อมต่อกับเครือข่ายไร้สาย (Wifi) สาธารณะ มีความเสี่ยงต่อการทำธุรกรรมออนไลน์	✓			
8.	การคลิกเปิดลิงค์ (Link) ในจดหมายอิเล็กทรอนิกส์ (E-Mail)ที่ได้รับ จากแหล่งหรือบุคคลที่ไม่รู้จัก ไม่ทำให้เกิดความเสี่ยงต่อการทำธุรกรรมออนไลน์	✓			
9.	การใช้รหัสผ่าน (Password) หลายชั้น และ หลากหลาย เช่น ชั้นที่ 1 รหัสผ่านที่ตั้งขึ้นมา กับ ชั้นที่ 2 มีการยืนยันด้วย OTP ทำให้ความเสี่ยงต่อการทำธุรกรรมออนไลน์เพิ่มขึ้น (ลด?)	✓			
10.	การเข้าเว็บไซต์ Https มีความปลอดภัยมากกว่า Http	✓			

ภาพที่ ข-3 IOC จาก ดร.พนิดาส่วนที่ 3

ตอนที่ 3 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

แบบสอบถามนี้ มีความต้องการสอบถามเกี่ยวกับประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ โปรดอ่านและพิจารณาตอบคำถาม โดยการตอบคำถามว่า เคย หรือ ไม่ เป็นคำถามแบบตอบได้มากกว่าหนึ่งคำตอบ (Multiple Responses) ประกอบไปด้วยจำนวน 10 ข้อ

คำชี้แจงผู้เชี่ยวชาญ : โปรดพิจารณาว่าข้อความเกี่ยวกับประสบการณ์ที่เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์สอดคล้องกับตัวแปร และ วัตถุประสงค์ที่จะวัดหรือไม่

คำชี้แจง : ถ้า เคยให้ ทำการ ✓ ในหัวข้อนั้น

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1.	ท่านเคยได้รับผลกระทบจากมัลแวร์ (Malware) ทำให้ข้อมูลส่วนตัวรั่วไหล ซึ่งทำให้มีบุคคลอื่นใช้บริการธุรกรรมการเงินของท่านได้	✓			
2.	ท่านได้รับการก่อกวนในระบบเครือข่ายทำให้ไม่สามารถใช้บริการธุรกรรมการเงินออนไลน์ได้	✓			
3.	ท่านติดตั้งโปรแกรมหรือแอปพลิเคชั่นที่คิดว่าปลอดภัย แต่มี มัลแวร์ (Malware) แฝงตัวมา ทำให้มีบุคคลอื่นใช้บริการธุรกรรมการเงินของท่านได้	✓			
4.	ท่านเคยถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์หรือโทรศัพท์โดยที่ท่านไม่รู้ตัว	✓			
5.	ท่านเคยถูกหลอกให้ลงทุน และ มีการทำธุรกรรมการเงินไป	✓			
6.	ท่านถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าสู่ระบบ	✓			
7.	ท่านเคยได้รับจดหมายอิเล็กทรอนิกส์ (E-Mail) หลอกลวงให้ทำธุรกรรมการเงิน	✓			
8.	ท่านเคยได้รับคอลเซ็นเตอร์ (Call Center) มิจฉาชีพ หลอกลวงให้ทำธุรกรรมการเงิน	✓			
9.	ท่านเคยถูกหลอกให้ซื้อขายสินค้าและบริการ	✓			
10.	ท่านเคยถูกหลอกให้รัก และ ให้ทำธุรกรรมการเงิน	✓			

ภาพที่ ข-4 IOC จาก ดร.พนิดาส่วนที่ 4

ตอนที่ 4 ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

แบบสอบถามนี้ มีความต้องการสอบถามเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ โปรดอ่านและพิจารณาตอบคำถาม โดยทำเครื่องหมาย ✓ ลงในในช่องระดับความคิดเห็นที่ตรงกับความคิดเห็นกับท่านมากที่สุด เพียง 1 เห็นด้วย / ไม่เห็นด้วย ?

คำชี้แจงสำหรับผู้เชี่ยวชาญ : โปรดพิจารณาว่าข้อความเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์สอดคล้องกับตัวแปรและวัตถุประสงค์ที่จะวัดหรือไม่ โปรดตอบโดยทำเครื่องหมาย

คำชี้แจง เขียนเครื่องหมาย ✓ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่านมากที่สุด

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1.	**ด้านความปลอดภัย (Security)**				
1.1	ควรตั้ง Password ให้มีความยาวมากๆ เพื่อให้ยากต่อการ Brute Force	✓			
1.2	ควรหาทางป้องกันการถูกหลอกให้กรอกข้อมูลส่วนตัวทางเว็บไซต์ปลอม	✓			
1.3	ควรหาทางป้องกันมัลแวร์ เช่น โปรแกรม Anti – Virus เป็นต้น	✓			
2.	**ด้านการแอบอ้าง (Masquerading)**				
2.1	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นผ่าน Social Media เพื่อใช้ประโยชน์ในการทำธุรกรรมการเงิน	✓			
2.2	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นผ่านการโทร เพื่อใช้ประโยชน์ในการทำธุรกรรมการเงิน	✓			
2.3	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นผ่านการใช้ AI ในการทำ Deep Fake เพื่อใช้ประโยชน์ในการทำธุรกรรมการเงิน	✓			
3	**ด้านกฎหมาย (Legal)** ปรับเปลี่ยนภาษาเป็นไทย				ตามกฎหมาย ?
3.1	ข้อมูลอิเล็กทรอนิกส์ มีผลเท่ากับ กระดาษ สามารถใช้ได้ในทางกฎหมาย	✓			
3.2	กฎหมาย PDPA สามารถใช้กับกรณีที่เกิดข้อมูลรั่วไหลได้	✓			
3.3	กฎหมาย E-Payment เกิดขึ้นเพื่อรองรับระบบภาษี และ เอกสารธุรกรรมทางการอิเล็กทรอนิกส์	✓			

ภาพที่ ข-5 IOC จาก ดร.พนิดาส่วนที่ 5

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ 1	0	-1	ข้อเสนอแนะ
4.	**ด้านวิศวกรรมสังคม (Social Engineering)**				
4.1	ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านทาง Social Media	✓			
4.2	ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านทาง E-Mail	✓			
4.3	ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านช่องทางการโทรศัพท์	✓			
5.	**ด้านการตอบสนอง (Response)**				
5.1	เมื่อเกิดเหตุโดนหลอกให้ข้อมูลกับมิจฉาชีพไป ควรทำการเปลี่ยนรหัสผ่านใหม่ทั้งหมด และ ระงับการใช้งานบัตรเดบิต / บัตรเครดิต ทันที	✓			
5.2	เมื่อเกิดเหตุโดนหลอกให้ข้อมูลหรือทำธุรกรรมการเงินให้มิจฉาชีพไป ควรติดต่อศูนย์ดูแลลูกค้าจากภัยออนไลน์	✓			
5.3	เมื่อเกิดเหตุโดนหลอกให้ข้อมูลหรือทำธุรกรรมการเงินให้มิจฉาชีพไป ควรรวบรวมหลักฐานเพื่อแจ้งความ และ ดำเนินการติดต่อธนาคาร	✓			

ข้อเสนอแนะของผู้เชี่ยวชาญ

1. ลองหา reference ปรับเล็บ หรือบทวิจารณ์หลายๆ มาเพิ่มเติม
2. ปรับคำชี้แจงแต่ละส่วนให้ชัดเจนว่าต้องทำยังไง
3. ผลวิจัยที่ได้ออกมาจะนำไปใช้อย่างไร เช่น แนวทางป้องกัน (สั้นๆ) ให้เห็นภาพ

อย่างไร : เป็นแค่ประเด็นตามแบบสอบถามคิด แต่ fact ที่ต้องรู้คืออะไรแน่

: ข้อคำถามข้างๆ ผู้วิจัยมีมาจาก reference ที่นำเสนอมา/ทางคณะต้านใช้แล้วหรือไม่

ลงชื่อ.....พนิตา ร้อยตวง.....

(.....พนิตา ร้อยตวง.....)

ผู้ทรงคุณวุฒิ

ภาพที่ ข-6 IOC จาก ดร.พนิดาส่วนที่ 6

ร่างแบบสอบถามเพื่อการวิจัย (IOC)

เรื่อง แบบสอบถามสำหรับกลุ่มตัวอย่าง เพื่อศึกษาเรื่อง

"ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร"

คำชี้แจง

1. แบบสอบถามฉบับนี้ อยู่ในขั้นตอนการศึกษาปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร

2. แบบสอบถามฉบับนี้มุ่งตรวจสอบ เพื่อหาค่าความเที่ยงตรง (Validity) โดยการวิเคราะห์ดัชนีความสอดคล้อง (Index of item object congruence : IOC) ของแบบสอบถามและข้อเสนอแนะของผู้เชี่ยวชาญ เพื่อนำไปปรับปรุงแบบสอบถามให้สมบูรณ์ขึ้น

3. แบบสอบถามฉบับนี้มีทั้งหมด 4 ตอน

ตอนที่ 1 ลักษณะทางประชากร

ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

ตอนที่ 3 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

ตอนที่ 4 ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

4. ขอความกรุณาผู้ทรงคุณวุฒิหรือท่านผู้เชี่ยวชาญ ช่วยพิจารณาร่างแบบสอบถามว่ามีความสอดคล้องกับตัวแปรของการวิจัยเรื่องนี้หรือไม่ ด้วยการให้คะแนนในแต่ละข้อความในระบบ IOC โดยการทำเครื่องหมาย ✓ ลงในช่องว่าง

เกณฑ์การให้คะแนนในระบบ IOC

1) ให้ 1 คะแนน เมื่อแน่ในว่าข้อนั้นมีเนื้อหาที่สอดคล้องกับตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา

2) ให้ 0 คะแนน เมื่อไม่แน่ใจว่าข้อนั้นมีเนื้อหาที่สอดคล้องตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา

3) ให้ -1 คะแนน เมื่อแน่ใจว่าข้อนั้นมีเนื้อหาที่ไม่สอดคล้องกับตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา

5. ผู้วิจัยขอความกรุณาท่านผู้ทรงคุณวุฒิและผู้เชี่ยวชาญ ให้ข้อเสนอแนะหรือความคิดเห็นเพิ่มเติมในประเด็นที่ยังไม่สมบูรณ์ โดยการเขียนข้อเสนอแนะไว้ท้ายข้อความนั้นๆ

ผู้วิจัยขอขอบพระคุณในความกรุณาของท่านมา ณ โอกาส นี้

นาย ณศรัณย์ ขำหาญ

นักศึกษาปริญญาโท (การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ)

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ภาพที่ ข-7 IOC จาก ดร.วศินส่วนที่ 1

ตอนที่ 1 ลักษณะทางประชากร

คำชี้แจงของผู้ตอบแบบสอบถาม : กรุณาทำเครื่องหมาย ✓ ลงใน ( ) หรือเติมข้อความที่ตรงกับความเป็นจริง

คำชี้แจงสำหรับผู้เชี่ยวชาญ : โปรดพิจารณาว่าข้อความเกี่ยวกับลักษณะทางประชากรผู้ตอบเหมาะสมหรือไม่อย่างไร

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1.	เพศ ( ) ชาย ( ) หญิง	/			
2.	อายุ ( ) ไม่เกิน 20 ปี ( ) 21 – 30 ปี ( ) 31 – 40 ปี ( ) 41 – 50 ปี ( ) 51 – 60 ปี ( ) 61 ปีขึ้นไป	/			
3.	ระดับการศึกษาสูงสุด ( ) ต่ำกว่ามัธยมศึกษาตอนต้น ( ) มัธยมศึกษาตอนต้น ( ) มัธยมศึกษาตอนปลาย / ปวช. ( ) ปริญญาตรี ( ) สูงกว่าปริญญาโท		/		แล้วถ้าผู้ตอบจบปริญญาโท จะเลือกอันไหน ปรับเป็นปริญญาโท ปริญญาเอก ให้ชัดเจน
4.	รายได้ ( ) ไม่เกิน 15,000 บาท ( ) 15,001 – 30,000 บาท ( ) 30,001 – 45,000 บาท ( ) 45,001 – 50,000 บาท ( ) 50,001 บาทขึ้นไป	/			

ภาพที่ ข-8 IOC จาก ดร.วศินส่วนที่ 2

ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

แบบสอบถามนี้ มีความต้องการสอบถามเกี่ยวกับความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ โปรดอ่านและพิจารณาตอบคำถาม โดยการตอบคำถามว่า ใช่ หรือ ไม่

คำชี้แจงสำหรับผู้เชี่ยวชาญ : โปรดพิจารณาว่าข้อความเกี่ยวกับความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์สอดคล้องกับตัวแปรและวัตถุประสงค์ที่จะวัดหรือไม่

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1.	การให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะไม่มีความเสี่ยง		/		เสี่ยงอะไร อย่างไรน่าจะขยายความ
2.	การเข้าใช้เครือข่ายไร้สาย (Wifi) สาธารณะมีความเสี่ยงต่อการทำธุรกรรมออนไลน์		/		ไม่ชัดเจน ใครเสี่ยง คนใช้ หรือ WIFI สาธารณะเสี่ยง
3.	การติดตามข่าวสารรูปแบบโจมตีทางไซเบอร์ต่างๆ สามารถป้องกันความเสียหายที่จะเกิดขึ้นได้		/		เสียหายอย่างไร ไม่ชัดเจน
4.	การโหลดแอปพลิเคชั่น (Application) จากแหล่งต่างๆในเว็บไซต์ ทำให้มีความปลอดภัย		/		เข้าใจว่าเป็นคำถามหลอก ? อะไรคือทำให้มีความปลอดภัย อะไร อย่างไร
5.	การตั้งรหัสผ่าน (Password) ต่างๆ ยิ่งมีความยาวมาก โอกาสที่จะเดา Password ทุกความเป็นไปได้ของตัวอักษรในแต่ละหลัก (Brute Force) รหัสทำให้ใช้เวลามากขึ้น		/		ปลอดภัย ศัพท์เทคนิคเยอะไป เข้าใจยาก
6.	การตั้งรหัสผ่าน (Password) ต่างๆ ควรจะตั้งเหมือนๆกัน	/			
7.	การบันทึกรหัสผ่าน (Password) ต่างๆ ไว้ในเครื่องที่เชื่อมต่อกับเครือข่ายไร้สาย (Wifi) สาธารณะ มีความเสี่ยงต่อการทำธุรกรรมออนไลน์		/		เสี่ยงอะไร อย่างไร ไม่ชัดเจน
8.	การคลิกเปิดลิงก์ (Link) ในจดหมายอิเล็กทรอนิกส์ (E-Mail)ที่ได้รับ จากแหล่งหรือบุคคลที่ไม่รู้จัก ไม่ทำให้เกิดความเสี่ยงต่อการทำธุรกรรมออนไลน์		/		อะไร คือ เสี่ยงต่อการทำธุรกรรมออนไลน์
9.	การใช้รหัสผ่าน (Password) หลายชั้น และ หลากหลาย เช่น ชั้นที่ 1 รหัสผ่านที่ตั้งขึ้นมา กับ ชั้นที่ 2 มีการยืนยันด้วย OTP ทำให้ความเสี่ยงต่อการทำธุรกรรมออนไลน์เพิ่มขึ้น	/			
10.	การเข้าเว็บไซต์ Https มีความปลอดภัยมากกว่า Http	/			

ภาพที่ ข-9 IOC จาก ดร.วศินส่วนที่ 3

ตอนที่ 3 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

แบบสอบถามนี้ มีความต้องการสอบถามเกี่ยวกับประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ โปรดอ่านและพิจารณาตอบคำถาม โดยการตอบคำถามว่า เคย หรือ ไม่ เป็นคำถามแบบตอบได้มากกว่าหนึ่งคำตอบ (Multiple Responses) ประกอบไปด้วยจำนวน 10 ข้อ

คำชี้แจงผู้เชี่ยวชาญ : โปรดพิจารณาว่าข้อความเกี่ยวกับประสบการณ์ที่เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์สอดคล้องกับตัวแปร และ วัตถุประสงค์ที่จะวัดหรือไม่

คำชี้แจ้ง : ถ้า เคยให้ ทำการ ✓ ในหัวข้อนั้น

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1.	ท่านเคยได้รับผลกระทบจากมัลแวร์ (Malware) ทำให้ข้อมูลส่วนตัวรั่วไหล ซึ่งทำให้มีบุคคลอื่นใช้บริการธุรกรรมการเงินของท่านได้		/		มัลแวร์ คืออะไร
2.	ท่านได้รับการก่อกวนในระบบเครือข่ายทำให้ไม่สามารถใช้บริการธุรกรรมการเงินออนไลน์ได้		/		ก่อกวนอย่างไร
3.	ท่านติดตั้งโปรแกรมหรือแอปพลิเคชั่นที่คิดว่าปลอดภัย แต่มี มัลแวร์ (Malware) แฝงตัวมา ทำให้มีบุคคลอื่นใช้บริการธุรกรรมการเงินของท่านได้		/		
4.	ท่านเคยถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์หรือโทรศัพท์โดยที่ท่านไม่รู้ตัว	/			
5.	ท่านเคยถูกหลอกให้ลงทุน และ มีการทำธุรกรรมการเงินไป	/			
6.	ท่านถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าสู่ระบบ	/			
7.	ท่านเคยได้รับจดหมายอิเล็กทรอนิกส์ (E-Mail) หลอกลวงให้ทำธุรกรรมการเงิน	/			
8.	ท่านเคยโดนคอลเซ็นเตอร์ (Call Center) มิจฉาชีพ หลอกลวงให้ทำธุรกรรมการเงิน	/			
9.	ท่านเคยถูกหลอกให้ซื้อขายสินค้าและบริการ		/		จากแหล่งใด
10.	ท่านเคยถูกหลอกให้รัก และ ให้ทำธุรกรรมการเงิน		/		

ภาพที่ ข-10 IOC จาก ดร.วศินส่วนที่ 4

ตอนที่ 4 ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

แบบสอบถามนี้ มีความต้องการสอบถามเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ โปรดอ่านและพิจารณาตอบคำถาม โดยทำเครื่องหมาย ✓ ลงในในช่องระดับความคิดเห็นที่ตรงกับความคิดเห็นกับท่านมากที่สุด เพียง 1

คำชี้แจงสำหรับผู้เชี่ยวชาญ : โปรดพิจารณาว่าข้อความเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์สอดคล้องกับตัวแปรและวัตถุประสงค์ที่จะวัดหรือไม่ โปรดตอบโดยทำเครื่องหมาย

คำชี้แจง เขียนเครื่องหมาย ✓ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่านมากที่สุด

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1.	**ด้านความปลอดภัย (Security)**				
1.1	ควรตั้ง Password ให้มีความยาวมากๆ เพื่อให้ยากต่อการ Brute Force		/		อธิบายศัพท์เทคนิคด้วย
1.2	ควรหาทางป้องกันการถูกหลอกให้กรอกข้อมูลส่วนตัวทางเว็บไซต์ปลอม	/			
1.3	ควรหาทางป้องกันมัลแวร์ เช่น โปรแกรม Anti – Virus เป็นต้น	/			
2.	**ด้านการแอบอ้าง (Masquerading)**				
2.1	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นผ่าน Social Media เพื่อใช้ประโยชน์ในการทำธุรกรรมการเงิน	/			
2.2	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นผ่านการโทร เพื่อใช้ประโยชน์ในการทำธุรกรรมการเงิน	/			โทรทางไหน โทรศัพท์ไลน์ เมสเสนเจอร์
2.3	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นผ่านการใช้ AI ในการทำ Deep Fake เพื่อใช้ประโยชน์ในการทำธุรกรรมการเงิน		/		
3	**ด้านกฎหมาย (Legal)**				
3.1	ข้อมูลอิเล็กทรอนิกส์ มีผลเท่ากับ กระดาษ สามารถใช้ได้ในทางกฎหมาย			/	ไม่เข้าใจคำถามเลย
3.2	กฎหมาย PDPA สามารถใช้กับกรณีที่เกิดข้อมูลรั่วไหลได้	/			
3.3	กฎหมาย E-Payment เกิดขึ้นเพื่อรองรับระบบภาษี และ เอกสารธุรกรรมทางการอิเล็กทรอนิกส์		/		ชื่อย่อกฎหมายถูกต้อง ? ตรวจสอบชื่อย่อกฎหมาย

ภาพที่ ข-11 IOC จาก ดร.วศินส่วนที่ 5

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
4.	**ด้านวิศวกรรมสังคม (Social Engineering)**				
4.1	ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านทาง Social Media		/		อะไร คือ วิศวกรรมสังคม
4.2	ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านทาง E-Mail		/		
4.3	ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านช่องทางการโทรต่างๆ		/		
5.	**ด้านการตอบสนอง (Response)**				
5.1	เมื่อเกิดเหตุโดนหลอกให้ข้อมูลกับมิจฉาชีพไป ควรทำการเปลี่ยนรหัสผ่านใหม่ทั้งหมด และ ระงับการใช้งานบัตรเดบิต / บัตรเครดิต	/			
5.2	เมื่อเกิดเหตุโดนหลอกให้ข้อมูลหรือทำธุรกรรมการเงินให้มิจฉาชีพไป ควรติดต่อศูนย์ดูแลลูกค้าจากภัยออนไลน์		/		ที่ไหน ศูนย์ดูแลลูกค้า ?
5.3	เมื่อเกิดเหตุโดนหลอกให้ข้อมูลหรือทำธุรกรรมการเงินให้มิจฉาชีพไป ควรรวบรวมหลักฐานเพื่อแจ้งความ และ ดำเนินการติดต่อธนาคาร	/			

ข้อเสนอแนะของผู้เชี่ยวชาญ

ให้พิจารณา กลุ่มที่ไปเก็บข้อมูล ว่าเข้าใจศัพท์เทคนิค จากข้อคำถามหรือไม่ ปรับแบบสอบถาม

ให้ข้อความ หรือศัพท์เทคนิคให้เข้าใจมากขึ้น และคำกริยาต่างๆ ในประโยคควรมี กรรม มารองรับ เช่น "เสี่ยง" (อะไร อย่างไร)

ลงชื่อ.....

อ.ดร.วศิน พิพัฒนฉัตร

(.....)

ผู้ทรงคุณวุฒิ

ภาพที่ ข-12 IOC จาก ดร.วศินส่วนที่ 6

ร่างแบบสอบถามเพื่อการวิจัย (IOC)

เรื่อง แบบสอบถามสำหรับกลุ่มตัวอย่าง เพื่อศึกษาเรื่อง

"ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร"

คำชี้แจง

1. แบบสอบถามฉบับนี้ อยู่ในขั้นตอนการศึกษาปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร

2. แบบสอบถามฉบับนี้มุ่งตรวจสอบ เพื่อหาค่าความเที่ยงตรง (Validity) โดยการวิเคราะห์ดัชนีความสอดคล้อง (Index of item object congruence : IOC) ของแบบสอบถามและข้อเสนอแนะของผู้เชี่ยวชาญ เพื่อนำไปปรับปรุงแบบสอบถามให้สมบูรณ์ขึ้น

3. แบบสอบถามฉบับนี้มีทั้งหมด 4 ตอน

ตอนที่ 1 ลักษณะทางประชากร

ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

ตอนที่ 3 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

ตอนที่ 4 ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

4. ขอความกรุณาผู้ทรงคุณวุฒิหรือท่านผู้เชี่ยวชาญ ช่วยพิจารณาร่างแบบสอบถามว่ามีความสอดคล้องกับตัวแปรของการวิจัยเรื่องนี้หรือไม่ ด้วยการให้คะแนนในแต่ละข้อความในระบบ IOC โดยการทำเครื่องหมาย ✓ ลงในช่องว่าง

เกณฑ์การให้คะแนนในระบบ IOC

1) ให้ 1 คะแนน เมื่อแน่ในว่าข้อนั้นมีเนื้อหาที่สอดคล้องกับตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา

2) ให้ 0 คะแนน เมื่อไม่แน่ใจว่าข้อนั้นมีเนื้อหาที่สอดคล้องตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา

3) ให้ -1 คะแนน เมื่อแน่ใจว่าข้อนั้นมีเนื้อหาที่ไม่สอดคล้องกับตัวแปรและวัตถุประสงค์ที่ต้องการศึกษา

5. ผู้วิจัยขอความกรุณาท่านผู้ทรงคุณวุฒิและผู้เชี่ยวชาญ ให้ข้อเสนอแนะหรือความคิดเห็นเพิ่มเติมในประเด็นที่ยังไม่สมบูรณ์ โดยการเขียนข้อเสนอแนะไว้ท้ายข้อความนั้นๆ

ผู้วิจัยขอขอบพระคุณในความกรุณาของท่านมา ณ โอกาส นี้

นาย ณศรัณย์ ขำหาญ

นักศึกษาปริญญาโท (การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ)

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ภาพที่ ข-13 IOC จาก อ.ศรัญญาส่วนที่ 1

ตอนที่ 1 ลักษณะทางประชากร

คำชี้แจงของผู้ตอบแบบสอบถาม : กรุณาทำเครื่องหมาย ✓ ลงใน ( ) หรือเติมข้อความที่ตรงกับความเป็นจริง

คำชี้แจงสำหรับผู้เชี่ยวชาญ : โปรดพิจารณาว่าข้อความเกี่ยวกับลักษณะทางประชากรผู้ตอบเหมาะสมหรือไม่อย่างไร

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1.	เพศ ( ) ชาย ( ) หญิง	✓			
2.	อายุ ( ) ไม่เกิน 20 ปี ( ) 21 – 30 ปี ( ) 31 – 40 ปี ( ) 41 – 50 ปี ( ) 51 – 60 ปี ( ) 61 ปีขึ้นไป	✓			
3.	ระดับการศึกษาสูงสุด ( ) ต่ำกว่ามัธยมศึกษาตอนต้น ( ) มัธยมศึกษาตอนต้น ( ) มัธยมศึกษาตอนปลาย / ปวช. ( ) ปริญญญาตรี ( ) สูงกว่าปริญญาโท	✓			
4.	รายได้ ( ) ไม่เกิน 15,000 บาท ( ) 15,001 – 30,000 บาท ( ) 30,001 – 45,000 บาท ( ) 45,001 – 50,000 บาท ( ) 50,001 บาทขึ้นไป	✓			

ภาพที่ ข-14 IOC จาก อ.ศรัญญาส่วนที่ 2

ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

แบบสอบถามนี้ มีความต้องการสอบถามเกี่ยวกับความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ โปรดอ่านและพิจารณาตอบคำถาม โดยการตอบคำถามว่า ใช่ หรือ ไม่

คำชี้แจงสำหรับผู้เชี่ยวชาญ : โปรดพิจารณาว่าข้อความเกี่ยวกับความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์สอดคล้องกับตัวแปรและวัตถุประสงค์ที่จะวัดหรือไม่

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1.	การให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะไม่มีความเสี่ยง	✓			ควรมีแก้ไขตามคำแนะนำ
2.	การเข้าใช้เครือข่ายไร้สาย (Wifi) สาธารณะมีความเสี่ยงต่อการทำธุรกรรมออนไลน์	✓			
3.	การติดตามข่าวสารรูปแบบโจมตีทางไซเบอร์ต่างๆ สามารถป้องกันความเสียหายที่จะเกิดขึ้นได้	✓			
4.	การโหลดแอปพลิเคชั่น (Application) จากแหล่งต่างๆในเว็บไซต์ ทำให้มีความปลอดภัย	✓			
5.	การตั้งรหัสผ่าน (Password) ต่างๆ ยิ่งมีความยาวมาก โอกาสที่จะเดา Password ทุกความเป็นไปได้ของตัวอักษรในแต่ละหลัก (Brute Force) รหัสทำให้ใช้เวลามากขึ้น	✓			
6.	การตั้งรหัสผ่าน (Password) ต่างๆ ควรจะตั้งเหมือนๆกัน	✓			
7.	การบันทึกรหัสผ่าน (Password) ต่างๆ ไว้ในเครื่องที่เชื่อมต่อกับเครือข่ายไร้สาย (Wifi) สาธารณะ มีความเสี่ยงต่อการทำธุรกรรมออนไลน์	✓			
8.	การคลิกเปิดลิงค์ (Link) ในจดหมายอิเล็กทรอนิกส์ (E-Mail)ที่ได้รับ จากแหล่งหรือบุคคลที่ไม่รู้จัก ไม่ทำให้เกิดความเสี่ยงต่อการทำธุรกรรมออนไลน์	✓			ควรมีแก้ไขตามคำแนะนำ
9.	การใช้รหัสผ่าน (Password) หลายชั้น และ หลากหลาย เช่น ชั้นที่ 1 รหัสผ่านที่ตั้งขึ้นมา กับ ชั้นที่ 2 มีการยืนยันด้วย OTP ทำให้ความเสี่ยงต่อการทำธุรกรรมออนไลน์เพิ่มขึ้น	✓			
10.	การเข้าเว็บไซต์ Https มีความปลอดภัยมากกว่า Http	✓			

ภาพที่ ข-15 IOC จาก อ.ศรัญญาส่วนที่ 3

ตอนที่ 3 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

แบบสอบถามนี้ มีความต้องการสอบถามเกี่ยวกับประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ โปรดอ่านและพิจารณาตอบคำถาม โดยการตอบคำถามว่า เคย หรือ ไม่ เป็นคำถามแบบตอบได้มากกว่าหนึ่งคำตอบ (Multiple Responses) ประกอบไปด้วยจำนวน 10 ข้อ

คำชี้แจงผู้เชี่ยวชาญ : โปรดพิจารณาว่าข้อความเกี่ยวกับประสบการณ์ที่เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์สอดคล้องกับตัวแปร และ วัตถุประสงค์ที่จะวัดหรือไม่

คำชี้แจ้ง : ถ้า เคยให้ ทำการ ✓ ในหัวข้อนั้น

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1.	ท่านเคยได้รับผลกระทบจากมัลแวร์ (Malware) ทำให้ข้อมูลส่วนตัวรั่วไหล ซึ่งทำให้มีบุคคลอื่นใช้บริการธุรกรรมการเงินของท่านได้	✓			
2.	ท่านได้รับการก่อกวนในระบบเครือข่ายทำให้ไม่สามารถใช้บริการธุรกรรมการเงินออนไลน์ได้	✓			
3.	ท่านติดตั้งโปรแกรมหรือแอปพลิเคชั่นที่คิดว่าปลอดภัย แต่มี มัลแวร์ (Malware) แฝงตัวมา ทำให้มีบุคคลอื่นใช้บริการธุรกรรมการเงินของท่านได้	✓			
4.	ท่านเคยถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์หรือโทรศัพท์โดยที่ท่านไม่รู้ตัว	✓			
5.	ท่านเคยถูกหลอกให้ลงทุน และ มีการทำธุรกรรมการเงินไป	✓			
6.	ท่านถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าสู่ระบบ	✓			
7.	ท่านเคยได้รับจดหมายอิเล็กทรอนิกส์ (E-Mail) หลอกลวงให้ทำธุรกรรมการเงิน	✓			
8.	ท่านเคยโดนคอลเซ็นเตอร์ (Call Center) มิจฉาชีพ หลอกลวงให้ทำธุรกรรมการเงิน	✓			
9.	ท่านเคยถูกหลอกให้ซื้อขายสินค้าและบริการ	✓			
10.	ท่านเคยถูกหลอกให้รัก และ ให้ทำธุรกรรมการเงิน	✓			

ภาพที่ ข-16 IOC จาก อ.ศรัญญาส่วนที่ 4

ตอนที่ 4 ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์

แบบสอบถามนี้ มีความต้องการสอบถามเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์ โปรดอ่านและพิจารณาตอบคำถาม โดยทำเครื่องหมาย ✓ ลงในในช่องระดับความคิดเห็นที่ตรงกับความคิดเห็นกับท่านมากที่สุด เพียง 1

คำชี้แจงสำหรับผู้เชี่ยวชาญ : โปรดพิจารณาว่าข้อความเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ของการใช้บริการธุรกรรมการเงินออนไลน์สอดคล้องกับตัวแปรและวัตถุประสงค์ที่จะวัดหรือไม่ โปรดตอบโดยทำเครื่องหมาย

คำชี้แจง เขียนเครื่องหมาย ✓ ลงในช่องที่ตรงกับระดับความคิดเห็นของท่านมากที่สุด

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
1.	**ด้านความปลอดภัย (Security)**				
1.1	ควรตั้ง Password ให้มีความยาวมากๆ เพื่อให้ยากต่อการ Brute Force	✓			
1.2	ควรหาทางป้องกันการถูกหลอกให้กรอกข้อมูลส่วนตัวทางเว็บไซต์ปลอม	✓			
1.3	ควรหาทางป้องกันมัลแวร์ เช่น โปรแกรม Anti – Virus เป็นต้น	✓			
2.	**ด้านการแอบอ้าง (Masquerading)**				
2.1	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นผ่าน Social Media เพื่อใช้ประโยชน์ในการทำธุรกรรมการเงิน	✓			
2.2	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นผ่านการโทร เพื่อใช้ประโยชน์ในการทำธุรกรรมการเงิน	✓			
2.3	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นผ่านการใช้ AI ในการทำ Deep Fake เพื่อใช้ประโยชน์ในการทำธุรกรรมการเงิน	✓			
3	**ด้านกฎหมาย (Legal)**				
3.1	ข้อมูลอิเล็กทรอนิกส์ มีผลเท่ากับ กระดาษ สามารถใช้ได้ในทางกฎหมาย	✓			
3.2	กฎหมาย PDPA สามารถใช้กับกรณีที่เกิดข้อมูลรั่วไหลได้	✓			
3.3	กฎหมาย E-Payment เกิดขึ้นเพื่อรองรับระบบภาษี และ เอกสารธุรกรรมทางการอิเล็กทรอนิกส์	✓			

ภาพที่ ข-17 IOC จาก อ.ศรัญญาส่วนที่ 5

ข้อ	ข้อคำถาม	ความคิดเห็นผู้เชี่ยวชาญ			ข้อเสนอแนะ
		1	0	-1	
4.	**ด้านวิศวกรรมสังคม (Social Engineering)**				
4.1	ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านทาง Social Media	✓			
4.2	ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านทาง E-Mail	✓			
4.3	ผู้ไม่หวังดีสามารถใช้ Social Engineering ผ่านช่องทางการโทรต่างๆ	✓			
5.	**ด้านการตอบสนอง (Response)**				
5.1	เมื่อเกิดเหตุโดนหลอกให้ข้อมูลกับมิจฉาชีพไป ควรทำการเปลี่ยนรหัสผ่านใหม่ทั้งหมด และ ระงับการใช้งานบัตรเดบิต / บัตรเครดิต	✓			
5.2	เมื่อเกิดเหตุโดนหลอกให้ข้อมูลหรือทำธุรกรรมการเงินให้มิจฉาชีพไป ควรติดต่อศูนย์ดูแลลูกค้าจากภัยออนไลน์	✓			
5.3	เมื่อเกิดเหตุโดนหลอกให้ข้อมูลหรือทำธุรกรรมการเงินให้มิจฉาชีพไป ควรรวบรวมหลักฐานเพื่อแจ้งความ และ ดำเนินการติดต่อธนาคาร	✓			

ข้อเสนอแนะของผู้เชี่ยวชาญ

.....

.....

.....

.....

.....

.....

ลงชื่อ.....

(ศรัญญา แจ้งจำ)

ผู้ทรงคุณวุฒิ

ภาพที่ ข-18 IOC จาก อ.ศรัญญาส่วนที่ 6

ประวัติผู้เขียน

ชื่อ นายณศรัณย์ ขำหาญ

ชื่อการค้นคว้าอิสระ ปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้บริการธุรกรรมการเงินออนไลน์ในกรุงเทพมหานคร

สาขาวิชา การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

ประวัติ ปริญญาตรี: วิทยาลัยเทคโนโลยีอุตสาหกรรม (วทอ.)
สาขาการจัดการเทคโนโลยีการผลิตและสารสนเทศ
: มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

<u>ประวัติการทำงานและผลงาน</u>

- 2561 – 2562
  ปริญญานิพนธ์ สร้าง เครื่องทาเนยขนมปังกรอบ โดยใช้ Micro Controller
- 2562 – 2563
  บริษัท ปูนซิเมนต์ (ท่าหลวง) จำกัด และ บริษัท ปูนซิเมนซ์ (เขาวง) จำกัด
  ตำแหน่ง Internship (Maintenance Engineer)
- 2563 – 2564
  บริษัท กรุงไทยอาหาร จำกัด (มหาชน) โรงงานบ้านบึง KT2
  ตำแหน่ง SCADA Programmer
- 2564 – 2566
  บริษัท ไทยอกริฟู้ดส์ จำกัด (มหาชน) โรงงานกระทิอร่อยดี (สมุทรปราการ) และ สำนักงานใหญ่พระราม3
  ตำแหน่ง Programmer (Production)
- 2567 - ปัจจุบัน
  บริษัท บางมดเอ็นเตอร์ไพรส์ จำกัด
  ตำแหน่ง Cyber Security Analyst (CSOC)