การพัฒนาแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน

Development of Deception Risk Assessment on Digital Media Using Communication-Based Model

ดำรงศักดิ์ สัตบุตร[1] และ กัญญรัตน์ หงส์วรนันท์[2]
Damrongsak Sattabut and Kanyarat Hongworranun
Corresponding author, E-mail: 625156060028@dpu.ac.th

Received : *February 12, 2021*
Revised : *September 16, 2021*
Accepted : *December 11, 2021*

บทคัดย่อ

การศึกษาครั้งนี้มีวัตถุประสงค์ 1) เพื่อสร้างแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน และ 2) เพื่อทดสอบคุณภาพแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล

โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน โดยทดสอบความตรงเชิงประจักษ์ ความตรงเชิงเนื้อหา ความตรงเชิงโครงสร้าง และความเชื่อมั่น กลุ่มตัวอย่างที่ใช้ในการศึกษา ได้แก่ ผู้รับสารกลุ่มดิจิทัลเนทีฟไทย จำนวน 400 คน ซึ่งได้มาจากการเลือกตัวอย่างแบบเฉพาะเจาะจง โดยมีเครื่องมือที่ใช้ในการวิจัย คือแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน ที่ผู้วิจัยพัฒนาขึ้นจากกระบวนการสร้างเครื่องมือวิจัย ประกอบไปด้วย 9 หมวด รวมทั้งสิ้น 36 ข้อคำถาม โดยมีค่าความเชื่อมั่นเท่ากับ .85

ผลการวิจัยพบว่า 1) การพัฒนาแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน มีตัวแปรที่เกี่ยวข้องทั้งหมด 9 ตัวแปร 2) คุณภาพแบบวัด ความตรงของแบบวัด ได้ค่าดัชนีความตรงตามเนื้อหาเท่ากับ .87 ความเชื่อมั่นของแบบวัดเท่ากับ .85 และมีความตรงเชิงโครงสร้าง ซึ่งตรวจสอบโดยใช้การวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis : EFA) สามารถจัดข้อคำถามที่มีความสัมพันธ์อยู่ในปัจจัยเดียวกันได้ 9 ปัจจัย ได้แก่ อ้างเป็นบุคคลสำคัญ การสร้างความน่าเชื่อถือ กระตุ้นความสนใจ กระตุ้นความต้องการ สร้างความคาดหวัง ความกลัว ความโลภ ความอยากรู้อยากเห็น และการตัดสินใจอย่างไม่มีเหตุผล

คำสำคัญ: การพัฒนาแบบวัด, การสื่อสาร, ภัยไซเบอร์, ฟิชชิ่ง

Abstract

The study aimed to 1) construct a deception risk assessment on digital media using a communication-based model, and 2) examine the empirical validity, content validity, construct validity, as well as the reliability of the deception risk assessment on digital media using the communication-based model. The sample group was 400 Thai digital native recipients determined by using a purposive sampling method. The instrument used in this study was the deception risk assessment on digital media developed by the researcher employing the communication-based model.

[1, 2] คณะนิเทศศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์
Faculty of Communication arts, Dhurakij Pundit University

The instrument consisted of 9 aspects with 36 question items, and its reliability was at .85.

The findings revealed that 1) the development of deception risk assessment on digital media using the communication-based model was associated with 9 factors, and 2) the quality of the instrument in terms of content validity index and reliability were .87 and .85 respectively. As the researcher performed an exploratory factor analysis (EFA), the question items that appeared in the assessment could be classified into 9 related factors including, key-person impersonation, credibility building, attention gaining, needs stimulation, expectation, fear, greed, as well as curiosity and unreasonable decision making.

Keywords: Assessment Development, Communication, Cyberthreat, Phishing

บทนำ

เทคโนโลยีอินเทอร์เน็ต นับได้ว่าเป็นจิ๊กซอว์ตัวสำคัญทางดิจิทัลที่ได้เข้ามาเติมเต็มสรรค์สร้างสังคมทุกมิติ ตั้งแต่การใช้ชีวิตประจำวัน การศึกษา การดำเนินธุรกิจ รวมถึงเป็นกลไกสำคัญในการขับเคลื่อนเศรษฐกิจทั้งในระดับจุลภาคและมหภาค แต่อินเทอร์เน็ตยังสามารถส่งผลเสีย และถูกใช้เป็นเครื่องมือในการกระจายภัยคุกคาม นิตยสารด้านความปลอดภัยทางคอมพิวเตอร์ ประเทศสหรัฐอเมริกาทำนายว่าในปี 2564 อาชญากรรมไซเบอร์ (Cybercrime) จะก่อให้เกิดความเสียหายทั่วโลกรวมกันสูงถึง 6 ล้านล้านดอลลาร์สหรัฐ ซึ่งเพิ่มขึ้น 3 ล้านล้านดอลลาร์จากปี 2558 สะท้อนให้เห็นการถ่ายโอนความมั่งคั่งทางเศรษฐกิจในตลาดมืด ซึ่งเป็นแรงจูงใจดึงดูดผู้ไม่หวังดีให้ก่ออาชญากรรมทางไซเบอร์เพราะเป็นการลงทุนที่น้อย แต่สามารถทำกำไรได้มากกว่าการค้ายาเสพติดทั่วโลกรวมกัน (Cybersecurity Ventures, 2020) ภัยไซเบอร์มุ่งโจมตีทั้งตัวบุคคล ภาครัฐ และภาคเอกชน โดยในปี 2018 ต้นทุนรักษาความปลอดภัยไซเบอร์ในการโจมตีประเภทต่าง ๆ มีแนวโน้มพุ่งสูงขึ้นอย่างเห็นได้ชัด เป็นผลมาจากการพัฒนารุดหน้าของเทคโนโลยี ในขณะที่ประเทศไทย จากการรายงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทยหรือ ไทยเซิร์ต (2563) พบว่า คนไทยเสี่ยงต่อถูกการโจมตีประเภท Malicious Code การติดตั้งโปรแกรมที่มีคำสั่งที่สร้างความเสียหายต่อเครื่องผู้ใช้ เช่น การสอดแนมหรือขโมยข้อมูลของผู้ใช้งานมากที่สุด ตามด้วย Fraud การใช้ข้อมูลโดยไม่ได้รับอนุญาต การละเมิดลิขสิทธิ์ รวมไปถึงการโจมตีที่ปลอมตัวเป็นนิติบุคคลหนึ่งที่ได้รับประโยชน์จากการปลอมตัวเป็นนิติบุคคลอื่น (The European Computer Security Incident Response Team Network, 2003) การปลอมแปลงเป็นบุคคลอื่นเพื่อหลอกเอาข้อมูลจากผู้ใช้งานนั้นมีมาตั้งแต่ปี 2538 โดยนิยมใช้วิธีที่เรียกว่า ฟิชชิ่ง (Phishing) ซึ่งมักจะปลอมแปลงเป็นบุคคล หน่วยงาน หรือแหล่งข้อมูลที่น่าเชื่อถือส่ง URL ให้เหยื่อคลิก เข้าถึง และกรอกข้อมูล โดยการทำฟิชชิ่งยังสามารถโจมตีผ่านทางช่องทางอื่นได้ อาทิ โทรศัพท์ สื่อสังคมออนไลน์ เฟซบุ๊ก ทวิตเตอร์ เว็บไซต์ต่าง ๆ เป็นต้น (พงศ์พนธ์ ภาวศุทธิ์, 2561)

กระบวนการสื่อสารตามทฤษฎีของ Berlo ระบุว่ามีองค์ประกอบพื้นฐาน 4 ประการ ได้แก่ ผู้ส่งสาร (Sender) เนื้อหาสาร (Messages) ช่องทางการสื่อสาร (Channel) และผู้รับสาร (Receiver) ซึ่งองค์ประกอบ

ทั้ง 4 นับได้ว่าเป็นส่วนสำคัญที่ทำให้การโจมตีด้วยวิธีฟิชชิ่งในแต่ละครั้งสำเร็จผล เช่น ในด้านของผู้ส่งสาร (Sender) หากผู้ส่งเป็นบุคคลสำคัญ มีการสร้างความน่าเชื่อถือ ก็จะทำให้การโจมตีสำเร็จผลได้ ในด้านของเนื้อหาสาร (Messages) หากมีเนื้อหาที่กระตุ้นความสนใจ กระตุ้นความต้องการ หรือสร้างความคาดหวัง ก็ทำให้ผู้อ่านสนใจและตกเป็นเหยื่อได้ง่ายมากยิ่งขึ้น ช่องทางการสื่อสาร (Channel) เป็นส่วนสำคัญที่ทำให้เกิดการแพร่กระจายของฟิชชิ่ง โดยเฉพาะสื่อดิจิทัล ที่สามารถสื่อสารกับคนจำนวนมากในเวลาเดียวกันได้อย่างรวดเร็ว และในด้านของ

ผู้รับสาร (Receiver) หากผู้รับสารมีความกลัว ความโลภ ความอยากรู้อยากเห็น และการตัดสินใจอย่างไม่มีเหตุผล

ก็จะเป็นการเพิ่มโอกาสให้การโจมตีสำเร็จได้มากยิ่งขึ้น จากปัญหาดังกล่าวจะเห็นได้ว่าวิธีการล่อลวงบนสื่อดิจิทัลเป็นอาชญากรรมทางไซเบอร์ที่ร้ายแรงระดับโลก ซึ่งประเทศไทยก็ตกเป็นเป้าการโจมตีอย่างต่อเนื่องทั้งฟิชชิ่งที่มาจากต่างประเทศ และฟิชชิ่งภายในประเทศ การใช้ซอฟต์แวร์ในการป้องกันเพียงอย่างเดียวไม่สามารถที่จะป้องกันได้อย่างมีประสิทธิภาพ เนื่องจากผู้ไม่หวังดีจะเลือกใช้กลวิธีต่าง ๆ เพื่อทำให้เหยื่อหลงเชื่อ โดยมุ่งเน้นไปที่ปัจเจกบุคคลไม่ใช่ตัวระบบ ซึ่งผู้วิจัยมีความสนใจที่จะพัฒนาแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล

โดยมุ่งประเด็นไปที่การสื่อสาร เพื่อจะได้เครื่องมือที่เหมาะสม และเป็นประโยชน์ในการประเมินความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล และงานวิจัยอื่น ๆ ต่อไป

วัตถุประสงค์ของการวิจัย

1. เพื่อสร้างแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน

2. เพื่อทดสอบคุณภาพแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน โดยทดสอบความตรงเชิงประจักษ์ ความตรงเชิงเนื้อหา ความตรงเชิงโครงสร้าง และความเชื่อมั่น

ประโยชน์ที่ได้รับ

1. ประโยชน์ในเชิงวิชาการ ทำให้เข้าใจถึงองค์ประกอบของปัจจัยการสื่อสารว่ามีผลต่อการถูกล่อลวงบนสื่อดิจิทัลอย่างไรและช่วยกระตุ้นให้เกิดการศึกษาวิจัยด้านภัยไซเบอร์สอดคล้องกับบริบทสังคมที่มีความเป็นพลวัตต่อไป

2. ประโยชน์ในทางวิชาชีพ ช่วยให้องค์กรภาครัฐ ภาคเอกชน ตลอดจนผู้มีส่วนเกี่ยวข้องเกิดความเข้าใจและสามารถประเมินความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัลได้ง่ายมากยิ่งขึ้น

กรอบแนวคิดในการวิจัย

การวิจัยเรื่อง “การพัฒนาแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน” ใช้แนวคิดการสื่อสารของ Berlo ประกอบกับการทบทวนวรรณกรรมเกี่ยวกับภัยไซเบอร์ การโจมตีด้วยวิธีวิศวกรรมสังคม และเหตุการณ์ฟิชชิ่งที่เกิดขึ้นในประเทศไทย

นิยามเชิงปฏิบัติการ

ผู้วิจัยได้กำหนดนิยามเชิงปฏิบัติการของตัวแปรต่าง ๆ ดังนี้

อ้างเป็นบุคคลสำคัญ หมายถึง การแอบอ้าง สวมรอย ปลอมแปลงเป็นบุคคลหรือองค์กรที่น่าเชื่อถือ

การสร้างความน่าเชื่อถือ หมายถึง สถานภาพที่ถูกสร้างขึ้น จากองค์ประกอบต่าง ๆ ตั้งแต่พฤติกรรม

การใช้ภาษา รวมไปถึงลักษณะที่ปรากฏบนโลกออนไลน์

กระตุ้นความสนใจ หมายถึง การสร้างสถานการณ์ เหตุการณ์ รวมไปถึงการใช้คุณลักษณะทางด้านภาษาเพื่อดึงดูดให้ผู้รับสารสนใจข้อมูลที่ต้องการนำเสนอ

กระตุ้นความต้องการ หมายถึง การสร้างสถานการณ์ เหตุการณ์ รวมไปถึงการใช้คุณลักษณะทางด้านภาษาเพื่อดึงดูดให้ผู้รับสารรู้สึกยากที่จะปฏิเสธข้อเสนอเหล่านั้น

สร้างความคาดหวัง หมายถึง การสร้างความรู้สึก ความคิดเห็น การรับรู้ โดยคาดหวังหรือต้องการให้ผู้รับสารนั้นประพฤติปฏิบัติในสิ่งที่ตนต้องการ หรือคาดหวังเอาไว้

ความกลัว หมายถึง อารมณ์หรือการตอบสนองที่ผู้รับสาร สามารถรับรู้ได้ถึงภัยคุกคามหรืออันตรายที่จะมาทำร้ายตน

ความโลภ หมายถึง ความรู้สึกที่สะท้อนถึงความต้องการ ความอยากได้ ซึ่งอาจนำไปสู่การแสวงหาทรัพย์สินที่ต้องการด้วยวิธีทุจริต

ความอยากรู้อยากเห็น หมายถึง สภาวะทางอารมณ์หรือความรู้สึกของผู้รับสารที่ปรารถนาอย่างแรงกล้าที่จะลองหรือเรียนรู้อะไรบางอย่าง

การตัดสินใจอย่างไม่มีเหตุผล หมายถึง กระบวนการที่ปราศจากเหตุผลในการเลือกหรือกระทำการสิ่งใดสิ่งหนึ่ง ซึ่งกระทำไปโดยใช้ความรู้สึกและเป็นการตัดสินใจที่เกิดขึ้นทันทีหลังจากสิ่งเร้าปรากฏ

วิธีดำเนินการวิจัย

เป็นการวิจัยเพื่อพัฒนาเครื่องมือวิจัย (Scale development research) โดยใช้วิธีการเชิงปริมาณแบ่งการศึกษาออกเป็น 2 ระยะ คือ ระยะที่ 1 การพัฒนาแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน และ ระยะที่ 2 การทดสอบคุณภาพแบบวัดการสื่อสาร

1. การพัฒนาแบบวัดการสื่อสาร เป็นการศึกษาจากวัตถุประสงค์ของการวิจัยที่กล่าวว่า “เพื่อสร้างแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน” โดยผู้วิจัยดำเนินการรวบรวมปัจจัยจากเอกสาร ตำรา งานวิจัยที่เกี่ยวข้องกับเกี่ยวกับภัยไซเบอร์ การโจมตีด้วยวิธีวิศวกรรมสังคม และเหตุการณ์ฟิชชิ่งที่เกิดขึ้นในประเทศไทย และนำปัจจัยที่ได้ไปพัฒนาเป็นแบบวัด โดยใช้มาตรวัดของลิเคอร์ท (Likert scale) 5 ระดับ ประกอบด้วย เห็นด้วยที่สุด เห็นด้วย ไม่แน่ใจ ไม่เห็นด้วย ไม่เห็นด้วยที่สุด

2. การทดสอบคุณภาพแบบวัดการสื่อสาร เป็นการศึกษาจากวัตถุประสงค์ของการวิจัยที่กล่าวว่า “เพื่อทดสอบคุณภาพแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน โดยทดสอบความตรงเชิงประจักษ์ ความตรงเชิงเนื้อหา ความตรงเชิงโครงสร้าง และความเชื่อมั่น” โดยผู้วิจัยได้ดำเนินการทดสอบดังต่อไปนี้

2.1 ความตรงเชิงประจักษ์ ผู้วิจัยนำแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน ไปให้อาจารย์ในคณะนิเทศศาสตร์ เพื่อตรวจให้ข้อเสนอแนะเกี่ยวกับหลักการใช้ภาษา ความถูกต้องของเนื้อหา และทำการปรับปรุงตามข้อเสนอแนะ

2.2 ความตรงตามเนื้อหา ผู้วิจัยนำแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน ไปให้ผู้ทรงคุณวุฒิ ที่มีความเชี่ยวชาญด้านความปลอดภัยบนระบบคอมพิวเตอร์ การโจมตีบนโลกออนไลน์ จำนวน 5 ท่าน เพื่อตรวจความตรงตามเนื้อหา และนำผลการตรวจสอบดังกล่าวมาคำนวณหาดัชนีความตรงตามเนื้อหา ทั้งแบบรายข้อ (I-CVI) และความตรงทั้งฉบับ (S-CVI) พร้อมทั้งปรับปรุงเครื่องมือให้มีความชัดเจนตามข้อคิดเห็นและข้อเสนอของผู้ทรงคุณวุฒิ

2.3 ความตรงเชิงโครงสร้าง ผู้วิจัยนำแบบวัดการสื่อสารที่ผ่านการตรวจสอบความตรงเชิงประจักษ์ ความตรงเชิงเนื้อหาเสร็จเรียบร้อยแล้ว ไปทดลองใช้กับผู้รับสารที่มีคุณลักษณะคล้ายกลุ่มตัวอย่างจำนวน 30 คน จากนั้นนำข้อมูลที่ได้มาคำนวณหาค่าความเชื่อมั่นของเครื่องมือ และวิเคราะห์รายข้อ คัดเลือกคำถามที่มีค่าความสัมพันธ์ระหว่างข้อคำถาม (Correlation item total correlation) ตั้งแต่ +0.30 ขึ้นไปมาจัดทำเป็นแบบวัด หลังจากนั้นนำแบบวัดไปเก็บจริงจากกลุ่มตัวอย่างจำนวน 400 คน และนำผลที่ได้มาวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory factor analysis) เพื่อศึกษาความสัมพันธ์ระหว่างตัวแปร ลดจำนวนข้อคำถามในแบบประเมิน โดยกำหนดเกณฑ์ของค่าน้ำหนักปัจจัยของคำถาม (Factor Loading) ตั้งแต่ .03 ขึ้นไป ในการคัดเข้าร่วมปัจจัย

ประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้ในการวิจัยครั้งนี้ คือ ผู้รับสารกลุ่มดิจิทัลเนทีฟไทย ซึ่งหมายถึง บุคคลที่มีอายุระหว่าง

18 - 36 ปี และใช้งานอินเทอร์เน็ตเป็นประจำอย่างน้อย 5 ปีติดต่อกัน ซึ่งมีจำนวนทั้งสิ้น 4,387,062 คน (ITU, 2013) โดยเลือกเก็บข้อมูลจากผู้รับสารกลุ่มดิจิทัลเนทีฟที่อาศัยอยู่ในเขตกรุงเทพมหานคร เนื่องจากมีสัดส่วนประชากร ผู้ใช้งานอินเทอร์เน็ตสูงที่สุดถึงร้อยละ 85.3 เมื่อเทียบกับทุกภูมิภาค (สำนักงานสถิติแห่งชาติ, 2562) ผู้วิจัยจึงคาดว่าจะพบความหลากหลายของรูปแบบการดำเนินชีวิตและเคยประสบเหตุหรือพบเห็นการถูกล่อลวงบนสื่อดิจิทัลได้มากกว่าพื้นที่อื่นในประเทศไทย โดยทำการสุ่มตัวอย่างแบบไม่อาศัยหลักความน่าจะเป็น (Unprovability random sampling) ซึ่งใช้การเลือกตัวอย่างแบบเฉพาะเจาะจง (Purposive Sampling) เพื่อให้ได้กลุ่มตัวอย่างที่มีคุณลักษณะตรงตามวัตถุประสงค์ของการวิจัย จำนวนรวมทั้งสิ้น 400 คน และเลือกใช้วิธีสุ่มอย่างง่ายสำหรับการทดสอบและหาคุณภาพเครื่องมือ โดยกลุ่มตัวอย่างสำหรับการนำเครื่องมือไปทดลองใช้เบื้องต้น (Preliminary item try out) จำนวน 30 คน

เครื่องมือที่ใช้ในการวิจัย

แบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน ที่ผู้วิจัยพัฒนาขึ้นจากกระบวนการสร้างเครื่องมือวิจัย ประกอบไปด้วย 9 หมวด รวมทั้งสิ้น 36 ข้อ โดยมีลักษณะของแบบวัดเป็นมาตรวัดของลิเคอร์ท (Likert scale) 5 ระดับมีค่าคะแนนของคำตอบตั้งแต่ 1 - 5 โดย 5 คะแนน หมายถึงเห็นด้วยมากที่สุด และ 1 หมายถึง ไม่เห็นด้วยมากที่สุด

การวิเคราะห์ข้อมูล

การศึกษาครั้งนี้ ทำการวิเคราะห์ข้อมูลด้วยโปรแกรมทางสถิติ SPSS โดยมีรายละเอียดดังนี้

1. ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม อาทิ อายุ เพศ รายได้ การศึกษา ใช้การวิเคราะห์ด้วยสถิติเชิงพรรณนา (Descriptive Statistics) โดยการแจกแจงความถี่ ร้อยละ ค่าเฉลี่ย และค่าเบี่ยงเบนมาตรฐาน
2. วิเคราะห์ปัจจัยของแบบวัด โดยใช้วิธีการวิเคราะห์ปัจจัยเชิงสำรวจ (Exploratory factor analysis)
3. วิเคราะห์คำถามรายข้อ
4. ทั้งยังใช้วิธีการคำนวณ ค่าความเชื่อมั่นของเครื่องมือ โดยหาค่าสัมประสิทธิ์แอลฟาของครอนบัค (Cronbach's alpha coefficient)

ผลการวิจัย

การพัฒนาแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน ได้จากการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้องซึ่งค้นพบตัวแปรดังนี้ ตัวแปรที่เกี่ยวข้องกับผู้ส่งสารประกอบด้วย อ้างเป็นบุคคลสำคัญ และการสร้างความน่าเชื่อถือ ตัวแปรที่เกี่ยวข้องกับเนื้อหาสารประกอบด้วย กระตุ้นความสนใจ, กระตุ้นความต้องการ และสร้างความคาดหวัง ตัวแปรที่เกี่ยวข้องกับผู้รับสารประกอบด้วย ความกลัว, ความโลภ, ความอยากรู้อยากเห็น และ การตัดสินใจอย่างไม่มีเหตุผล รวมทั้งสิ้น 9 ตัวแปร ได้ข้อคำถามรวม 45 ข้อคำถาม

ความตรงเชิงประจักษ์ ผู้วิจัยได้ดำเนินการปรับปรุงข้อคำถามตามคำแนะนำของอาจารย์คณะนิเทศศาสตร์ สำหรับความตรงตามเนื้อหาผู้วิจัยได้นำแบบวัดไปตรวจสอบโดยผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้านความปลอดภัยบนระบบคอมพิวเตอร์ การโจมตีบนโลกออนไลน์ จำนวน 5 ท่าน พิจารณาให้คะแนนแต่ละข้อความตั้งแต่ 1 - 4 คะแนน โดยผู้วิจัยนำคะแนนมาคำนวณค่าดัชนีความตรงตามเนื้อหา (Content validity index : CVI) ทั้งแบบรายข้อ (I-CVI) และทั้งฉบับ (S-CVI) โดยได้ค่า I-CVI

อยู่ระหว่าง 0.6 - 1.0 และค่า S-CVI เท่ากับ .87 ผู้วิจัยได้ปรับปรุงข้อคำถาม การใช้ภาษาให้มีความชัดเจนมากยิ่งขึ้นตามความคิดเห็นและข้อเสนอจากผู้ทรงคุณวุฒิ และได้ปรับลดข้อคำถามจาก 45 ข้อคำถาม เหลือ 37 ข้อคำถาม แบ่งเป็น 9 หมวด ดังนี้

หมวดที่ 1 อ้างเป็นบุคคลสำคัญ จำนวน 4 ข้อ (ข้อ 1 - 4)

หมวดที่ 2 การสร้างความน่าเชื่อถือ จำนวน 4 ข้อ (ข้อ 5 - 8)

หมวดที่ 3 กระตุ้นความสนใจ จำนวน 4 ข้อ (ข้อ 9 - 12)

หมวดที่ 4 กระตุ้นความต้องการ จำนวน 4 ข้อ (ข้อ 13 - 16)

หมวดที่ 5 สร้างความคาดหวัง จำนวน 4 ข้อ (ข้อ 17 - 20)

หมวดที่ 6 ความกลัว จำนวน 5 ข้อ (ข้อ 21 - 25)

หมวดที่ 7 ความโลภ จำนวน 4 ข้อ (ข้อ 26 - 29)

หมวดที่ 8 ความอยากรู้อยากเห็น จำนวน 4 ข้อ (ข้อ 30 - 33)

หมวดที่ 9 การตัดสินใจอย่างไม่มีเหตุผล จำนวน 4 ข้อ (ข้อ 34 - 37)

โดยมีลักษณะของแบบวัดเป็นมาตรวัดของลิเคอร์ท (Likert scale) 5 ระดับ มีค่าคะแนนของคำตอบตั้งแต่ 1 - 5 โดย 5 คะแนน หมายถึงเห็นด้วยมากที่สุด และ 1 หมายถึง ไม่เห็นด้วยมากที่สุด การแปลผลคะแนนหากผลคะแนนรวมมากแสดงว่ามีความเสี่ยงสูงที่จะถูกล่อลวงบนสื่อดิจิทัล

ความเชื่อมั่นของแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน ทดสอบโดยกลุ่มตัวอย่างจำนวน 30 คน ที่มีลักษณะใกล้เคียงกับกลุ่มประชากร โดยมีอายุระหว่าง 22 - 25 ปี

ร้อยละ 60.00 จบการศึกษาระดับปริญญาตรี ร้อยละ 84.00 ประกอบอาชีพพนักงานบริษัทเอกชน ร้อยละ 65.00

มีรายได้เฉลี่ยต่อเดือนอยู่ที่ 15,001 - 20,000 บาท ร้อยละ 43.00 คำนวณหาค่าความสอดคล้องภายในเครื่องมือ (Farnsworth, 1928) ได้ค่าเท่ากับ .85 และได้ค่าสัมประสิทธิ์แอลฟ่าของครอนบัค (Cronbach's Alpha coefficient) ของข้อคำถามแต่ละหมวดดังนี้

หมวดที่ 1 อ้างเป็นบุคคลสำคัญ ค่า Cronbach's alpha = .87

หมวดที่ 2 การสร้างความน่าเชื่อถือ ค่า Cronbach's alpha = .88

หมวดที่ 3 กระตุ้นความสนใจ ค่า Cronbach's alpha = .92

หมวดที่ 4 กระตุ้นความต้องการ ค่า Cronbach's alpha = .85

หมวดที่ 5 สร้างความคาดหวัง ค่า Cronbach's alpha = .91

หมวดที่ 6 ความกลัว ค่า Cronbach's alpha = .88

หมวดที่ 7 ความโลภ ค่า Cronbach's alpha = .91

หมวดที่ 8 ความอยากรู้อยากเห็น ค่า Cronbach's alpha = .88

หมวดที่ 9 การตัดสินใจอย่างไม่มีเหตุผล ค่า Cronbach's alpha = .79

การตรวจสอบคุณภาพแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน กลุ่มตัวอย่างจำนวน 400 คน โดยมีอายุระหว่าง 26 - 29 ปี ร้อยละ 64.25 จบการศึกษาระดับปริญญาตรี

ร้อยละ 67.50 ประกอบอาชีพพนักงานบริษัทเอกชน ร้อยละ 62.50 มีรายได้เฉลี่ยต่อเดือนอยู่ที่ 25,001 - 30,000 บาท ร้อยละ 55.00 ได้ค่าความเชื่อมั่นเท่ากับ .85 และค่าสัมประสิทธิ์แอลฟ่าของครอนบัค (Cronbach's Alpha coefficient) ของข้อคำถามแต่ละหมวดดังนี้

หมวดที่ 1 อ้างเป็นบุคคลสำคัญ ค่า Cronbach's alpha = .85

หมวดที่ 2 การสร้างความน่าเชื่อถือ ค่า Cronbach's alpha = .88

หมวดที่ 3 กระตุ้นความสนใจ ค่า Cronbach's alpha = .80

หมวดที่ 4 กระตุ้นความต้องการ ค่า Cronbach's alpha = .84

หมวดที่ 5 สร้างความคาดหวัง ค่า Cronbach's alpha = .91

หมวดที่ 6 ความกลัว ค่า Cronbach's alpha = .90

หมวดที่ 7 ความโลภ ค่า Cronbach's alpha = .88

หมวดที่ 8 ความอยากรู้อยากเห็น ค่า Cronbach's alpha = .84

หมวดที่ 9 การตัดสินใจอย่างไม่มีเหตุผล ค่า Cronbach's alpha = .75

ค่าความสัมพันธ์ระหว่างข้อคำถาม (Correlation item total correlation) อยู่ระหว่าง .25 ถึง .52 ยกเว้นข้อคำถาม rec17 "ท่านไม่สนใจคำเตือนไวรัสที่ปรากฏบนหน้าจอ" ที่พบมีค่าความสัมพันธ์เพียง .08 โดยที่ค่าความสัมพันธ์ตั้งแต่ .25 ขึ้นไป ถือว่าแบบวัดนั้น ๆ มีความสอดคล้องภายใน (Jirojanakul & Skevington, 2000)

ความตรงเชิงโครงสร้าง ของแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการ

สื่อสารเป็นฐาน ใช้การวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis : EFA) ด้วยวิธีการหมุนแกนปัจจัยแบบ Varimax with Kaiser Normalization โดยใช้ข้อมูลจากกลุ่มตัวอย่าง 400 คน ผลการทดสอบข้อตกลงเบื้องต้นพบว่า ค่า KMO and Bartlett's Test มีค่าเท่ากับ 0.65 และค่า Bartlett's Test of Sphericity เท่ากับ $\chi 2 = 5733.96$, p .000) หมายความว่า ตัวแปรคู่ต่าง ๆ มีความสัมพันธ์กัน สามารถนำตัวแปรทั้งหมดมาทำการทดสอบวิเคราะห์องค์ประกอบได้ (สุดารัตน์ แสงแก้ว, 2558)

ตารางที่ 1 ค่า Factor Loading และการจัดข้อคำถามเข้าในปัจจัยจากการวิเคราะห์ปัจจัย

ปัจจัยที่ 1	**จำนวนข้อคำถาม 6 คำถาม**	**Factor Loading**
sen03	ท่านรู้สึกตื่นตระหนกหากได้รับการติดต่อจากหน่วยงานด้านความมั่นคงของประเทศ	.759
sen02	ท่านจะดำเนินการตามข้อความที่ปรากฏในอีเมล หากส่งมาจากบริษัทที่ติดต่อประจำและสามารถระบุข้อมูลเบื้องต้นของท่านได้ถูกต้อง	.729
sen04	ท่านได้รับการติดต่อจากกรมสรรพากร ผ่านช่องทางแชทให้ท่านเสียภาษี ท่านจะรีบดำเนินการทันที	.684
sen01	ท่านเชื่อถือข้อมูลเหล่านั้นทันที หากส่งมาจากบุคคลที่รู้จัก	.650
mes06	ท่านยินดีบอกข้อมูลให้กับทนายอาสาบนโลกออนไลน์ที่บอกว่าจะช่วยให้ท่านไม่ถูกดำเนินคดี	.559
mes09	ท่านรู้สึกดีใจหากได้รับข้อความว่า “ได้รับเงินช่วยเหลือสวัสดิการจากภาครัฐ”	.520
ปัจจัยที่ 2	**จำนวนข้อคำถาม 4 คำถาม**	**Factor Loading**
sen07	ท่านจะเชื่อถือบุคคลที่อ้างตนว่าเป็นเจ้าหน้าที่ของรัฐจากโปรไฟล์โซเชียลและภาพถ่าย	.749
sen05	ท่านจะเชื่อถือข้อความในสื่อออนไลน์ หากเขียนด้วยภาษาทางการ	.710
sen06	ท่านจะเชื่อถือการรีวิว หากเนื้อหาเป็นไปในทิศทางเดียวกันจำนวนมาก	.682
sen08	ท่านเชื่อถือลิงก์ที่นามสกุล (โดเมน) ไม่รู้จัก หากส่งมาโดยคนรู้จัก	.625
ปัจจัยที่ 3	**จำนวนข้อคำถาม 5 คำถาม**	**Factor Loading**
mes02	ท่านรู้สึกตื่นเต้นเมื่อได้รับข้อความว่า “ท่านเป็นผู้โชคดี”	.924
rec08	ท่านจะกรอกข้อมูลบนแอปฯ ที่ไม่รู้จัก หากแอปฯ นั้นระบุว่าจะมอบส่วนลดของร้านค้าชื่อดังให้	.862
mes04	ท่านมักจะให้ความสนใจกับข้อความที่จำกัดระยะเวลา เช่น “ดูด่วนก่อนโดนลบ”	.780
mes01	ท่านรู้สึกกังวลทุกครั้งเมื่อเห็นคำว่า “เฟซโดนแฮ็ก”, “กู้คืนบัญชีโดยด่วน” ในอีเมล	.745
mes03	ท่านจะไม่ส่งต่อข้อมูลเหล่านั้น หากพบว่าเป็นข่าวปลอม แชร์ลูกโซ่	.702
ปัจจัยที่ 4	**จำนวนข้อคำถาม 3 คำถาม**	**Factor Loading**
mes05	ท่านจะบอกหมายเลขบัญชีให้กับหน่วยงานที่บอกว่าจะโอนเงินรางวัลพิเศษให้	.624
mes08	ท่านมักจะคลิกลิงก์เพื่อทำความสะอาดกล่องข้อความ ตามคำแนะนำที่ระบุไว้ในอีเมล	.620
mes07	ท่านยินดีโอนค่ามัดจำให้กับเว็บไซต์ที่ระบุว่าจะทำให้ท่านได้สินค้าราคาถูกกว่าท้องตลาด	.529

ปัจจัยที่ 5	จำนวนข้อคำถาม 3 คำถาม	Factor Loading
mes10	ท่านยินดีชำระค่าธรรมเนียม เพื่อรับเงินสกุลดิจิทัลที่มีมูลค่าสูงจากต่างประเทศ	.773
mes12	ท่านจะตรวจสอบข้อมูลจากหน่วยงานต้นสังกัดก่อนทำธุรกรรมด้วยเสมอ	.743
mes11	ท่านพิจารณาอย่างถี่ถ้วนเกี่ยวกับส่วนลดที่ได้จากการร่วมกิจกรรม	.659
ปัจจัยที่ 6	**จำนวนข้อคำถาม 5 คำถาม**	**Factor Loading**
rec03	ท่านรู้สึกกลัว เมื่อมีผู้อ้างว่าครอบครองภาพลับของท่านไว้	.887
rec04	ท่านรู้สึกกลัวหากได้รับข้อความว่า “บัญชีของท่านเข้าข่ายการฟอกเงิน”	.765
rec01	ท่านรู้สึกกลัวข้อมูลในเครื่องคอมพิวเตอร์อาจถูกขโมยจึงดำเนินการสำรองข้อมูลอย่างสม่ำเสมอ	.675
rec05	ท่านรู้สึกกลัวหากได้รับข้อความว่า “เป็นหนี้บัตรเครดิตในจำนวนที่สูง”	.637
rec02	ท่านรู้สึกกลัว เมื่อมีคนรู้จักทักว่าเดือดร้อนต้องการขอยืมเงิน	.629
ปัจจัยที่ 7	**จำนวนข้อคำถาม 3 คำถาม**	**Factor Loading**
rec09	ท่านรู้สึกพิเศษ เมื่อได้รับข้อความที่ระบุว่ามอบสิทธิพิเศษให้เฉพาะคุณเท่านั้น	.723
rec06	ท่านให้ข้อมูลส่วนตัว อาทิ ชื่อ ที่อยู่ เบอร์โทรศัพท์ กับเว็บไซต์ที่สัญญาว่าจะให้รางวัล	.662
rec07	ท่านจะกดรหัสสั้น (USSD) เพื่อลุ้นรับรางวัลใหญ่กับหน่วยงานที่ท่านไม่รู้จัก	.599
ปัจจัยที่ 8	**จำนวนข้อคำถาม 4 คำถาม**	**Factor Loading**
rec13	ท่านกดยอมรับข้อตกลงการใช้งานเว็บไซต์ทันที โดยไม่ได้อ่านข้อมูลทั้งหมด	.850
rec12	ท่านดาวน์โหลดไฟล์ที่ไม่เกี่ยวข้องกับงานในเวลางาน	.768
rec11	ท่านคลิกลิงก์ในแอปสนทนาซึ่งได้รับจากบุคคลที่ไม่รู้จัก	.675
rec10	ท่านเปิดไฟล์แนบในอีเมลที่ได้รับจากบุคคลที่ไม่รู้จัก	.637
ปัจจัยที่ 9	**จำนวนข้อคำถาม 3 คำถาม**	**Factor Loading**
rec14	ท่านใช้อีเมลของบริษัทเพื่อลงทะเบียนในเว็บไซต์ต่าง ๆ	.850
rec16	ท่านทดลองคลิกลิงก์ไปเรื่อย ๆ เพื่อค้นหาไฟล์ที่ท่านต้องการดาวน์โหลด	.768
rec15	ท่านเขียนหรือบันทึกรหัสผ่าน (Password) ไว้ในสถานที่ที่ผู้อื่นพบได้ง่าย	.675

สรุปผลและอภิปรายผล

การพัฒนาแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน เกิดจากการทบทวนวรรณกรรมและแนวคิดต่าง ๆ ที่เกี่ยวกับภัยไซเบอร์ การโจมตีด้วยวิธีวิศวกรรมสังคม และเหตุการณ์ฟิชชิ่งที่เกิดขึ้นในประเทศไทย ได้ข้อคำถามรวม 45 ข้อ ทำการตรวจสอบแบบวัด ความชัดเจน การใช้ภาษา โดยอาจารย์คณะนิเทศศาสตร์ และผู้ทรงคุณวุฒิจำนวน 5 ท่าน ได้รับคำแนะนำให้ลดข้อคำถามจาก 45 ข้อคำถาม เหลือ 37 ข้อคำถาม แบ่งเป็น 9 หมวด โดยนำไปทดลองใช้เบื้องต้นกับกลุ่มตัวอย่าง 30 คน หลังจากนั้นนำไปทดลองใช้จริงกับกลุ่มตัวอย่างจำนวน 400 คน

ความเชื่อมั่นของแบบวัด มีค่า Cronbach's Alpha เท่ากับ .85 สำหรับเครื่องมือที่พัฒนาขึ้นใหม่ หากมีค่า Cronbach's Alpha มากกว่า .70 ถือว่าเหมาะสมและแสดงให้เห็นว่าเครื่องมือนั้นมีความสอดคล้องภายใน (Nunnally & Bernstein, 1994)

ความตรงของแบบวัด ได้รับการตรวจสอบจากผู้ทรงคุณวุฒิ จำนวน 5 ท่าน ได้ค่าดัชนีความตรงตามเนื้อหา (Content validity index : CVI) เท่ากับ .87 ซึ่งเป็นค่าที่ยอมรับได้ (Polit & Hungler, 1999) แสดงให้เห็นว่าแบบวัดดังกล่าวได้รับความเห็นจากผู้ทรงคุณวุฒิว่ามีความตรงตามเนื้อหา ซึ่งสามารถนำไปใช้ในการวัดผลได้จริง

ความตรงเชิงโครงสร้าง ผลการวิเคราะห์ของแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐานมีองค์ประกอบของปัจจัย ซึ่งในการศึกษาครั้งนี้ สามารถจัดกลุ่มได้ทั้งสิ้น 9 ปัจจัย ประกอบด้วย

ปัจจัยที่ 1 เป็นปัจจัยที่มีข้อคำถามถูกจัดเข้าในกลุ่มมากที่สุด รวมทั้งสิ้น 6 ข้อคำถาม ซึ่งสามารถแบ่งได้เป็นข้อคำถามเกี่ยวกับการอ้างเป็นบุคคลสำคัญจำนวน 4 ข้อคำถาม และกระตุ้นความต้องการจำนวน 2 ข้อคำถาม ทั้งนี้เนื่องจากการอ้างเป็นบุคคลสำคัญจะทำให้เหยื่อหลงเชื่อและกระทำตามที่ตนต้องการได้ง่ายมากยิ่งขึ้น ดังนั้นปัจจัยที่ 1 จึงเป็น อ้างเป็นบุคคลสำคัญ และกระตุ้นความต้องการ

ปัจจัยที่ 2 มีจำนวนข้อคำถามทั้งหมด 4 ข้อคำถาม ซึ่งเป็นข้อความเกี่ยวข้องกับความน่าเชื่อถือทั้งหมด ดังนั้นปัจจัยที่ 2 จึงเป็น การสร้างความน่าเชื่อถือ

ปัจจัยที่ 3 มีจำนวนข้อคำถามทั้งหมด 5 ข้อคำถาม ซึ่งสามารถแบ่งได้เป็นข้อคำถามเกี่ยวกับการกระตุ้นความสนใจจำนวน 4 ข้อคำถาม และความโลภจำนวน 1 ข้อคำถาม ทั้งนี้เนื่องจากการสร้างข้อความล่อลวงจะต้องใช้ภาษาและเนื้อหาที่กระตุ้นความสนใจผู้อ่าน ดังนั้นปัจจัยที่ 3 จึงเป็น กระตุ้นความสนใจ

ปัจจัยที่ 4 มีจำนวนข้อคำถามทั้งหมด 3 ข้อคำถาม ซึ่งเป็นข้อความเกี่ยวข้องกับการกระตุ้นความต้องการทั้งหมด ดังนั้นปัจจัยที่ 4 จึงเป็น กระตุ้นความต้องการ

ปัจจัยที่ 5 มีจำนวนข้อคำถามทั้งหมด 3 ข้อคำถาม ซึ่งเป็นข้อความเกี่ยวข้องกับการสร้างความคาดหวังทั้งหมด ดังนั้นปัจจัยที่ 5 จึงเป็น สร้างความคาดหวัง

ปัจจัยที่ 6 มีจำนวนข้อคำถามทั้งหมด 5 ข้อคำถาม ซึ่งเป็นข้อความเกี่ยวข้องกับความกลัวทั้งหมด ดังนั้นปัจจัยที่ 6 จึงเป็น ความกลัว

ปัจจัยที่ 7 มีจำนวนข้อคำถามทั้งหมด 3 ข้อคำถาม ซึ่งเป็นข้อความเกี่ยวข้องกับความโลภทั้งหมด ดังนั้นปัจจัยที่ 7 จึงเป็น ความโลภ

ปัจจัยที่ 8 มีจำนวนข้อคำถามทั้งหมด 4 ข้อคำถาม ซึ่งเป็นข้อความเกี่ยวข้องกับความอยากรู้อยากเห็นทั้งหมด ดังนั้นปัจจัยที่ 8 จึงเป็น ความอยากรู้อยากเห็น

ปัจจัยที่ 9 มีจำนวนข้อคำถามทั้งหมด 3 ข้อคำถาม ซึ่งเป็นข้อความเกี่ยวข้องกับการตัดสินใจอย่างไม่มีเหตุผลทั้งหมด ดังนั้นปัจจัยที่ 9 จึงเป็น การตัดสินใจอย่างไม่มีเหตุผล

ผลการวิเคราะห์ปัจจัยพบว่ามี 1 ข้อคำถาม "ท่านไม่สนใจคำเตือนไวรัสที่ปรากฏบนหน้าจอ" (rec17) ความสัมพันธ์เท่ากับ .08 ในปัจจัยที่ 9 ไม่ถูกคัดเข้าร่วมในปัจจัยทั้ง 9 จึงสรุปได้ว่า ข้อคำถาม rec17 ท่านไม่สนใจคำเตือนไวรัสที่ปรากฏบนหน้าจอ มีคำตอบที่หลากหลาย ทำให้ไม่มีความสอดคล้องภายใน และมีความสัมพันธ์กับข้ออื่น ๆ ต่ำจนไม่ถูกจัดเข้าร่วมปัจจัยทั้ง 9 ผู้วิจัยจึงได้ดำเนินการตัดข้อคำถาม rec17 ออกจากแบบวัด ทำให้เหลือข้อคำถามในแบบวัดทั้งสิ้น 36 ข้อคำถาม

จึงได้แบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน ที่ได้ทำการพัฒนาและตรวจสอบคุณภาพ ทั้งความตรงเชิงประจักษ์ ความตรงเชิงเนื้อหา ความตรงเชิงโครงสร้าง และความเชื่อมั่น อยู่ในระดับที่ยอมรับได้ เพื่อสร้างความมั่นใจสำหรับผู้ที่ต้องการนำไปใช้หรือศึกษาต่อไป

ข้อเสนอแนะ

ข้อเสนอแนะในการนำไปใช้

1. แบบผลจากการวิจัยครั้งนี้ทำให้ได้เครื่องมือแบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล ซึ่งนำไปใช้วัดเพื่อเป็นข้อมูลในการจัดกิจกรรม ส่งเสริมความรู้ และการใช้งานอินเทอร์เน็ตให้ปลอดภัยมากยิ่งขึ้น

2. ในการนำแบบวัดไปใช้ควรมีการปรับสถานการณ์เหตุการณ์ของแบบวัดให้มีความเหมาะสมกับช่วงอายุของกลุ่มเป้าหมายที่ต้องการวัด

ข้อเสนอแนะในการวิจัย

1. แบบวัดความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้แนวคิดด้านการสื่อสารเป็นฐาน ศึกษาในกลุ่มเป้าหมายที่เฉพาะเจาะจง ดังนั้นผู้ที่สนใจนำแบบวัดดังกล่าวไปศึกษาต่อ ควรเปลี่ยนกลุ่มเป้าหมายและปรับรูปแบบของข้อคำถามให้มีความเหมาะสมกับบริบทของกลุ่มเป้าหมายที่เปลี่ยนไป และนำมาหาความเชื่อมั่นของแบบวัดอีกครั้ง

2. การศึกษาครั้งต่อไปควรทำการศึกษาวิจัยเชิงคุณภาพเพื่อนำข้อมูลเชิงลึกมาบูรณาการในการสร้างแบบวัดร่วมกับการทบทวนวรรณกรรมเพิ่มเติม

เอกสารอ้างอิง

ไทยเซิร์ต (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย). (2563). **สถิติภัยคุกคาม 2563**. สืบค้นเมื่อ 8 ตุลาคม 2564, จาก https://www.thaicert.or.th/statistics/statistics.html

พงศ์พนธ์ ภาวศุทธิ์. (2561). **สาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม ของกลุ่มเจเนอเรชั่นวาย ในเขตกรุงเทพมหานครและปริมณฑล**. วิทยาศาสตรมหาบัณฑิต,มหาวิทยาลัยธรรมศาสตร์.

สำนักงานสถิติแห่งชาติ. (2562). **สำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2562**. สืบค้นเมื่อ 8 ตุลาคม 2564, จาก http://www.nso.go.th/sites/2014/DocLib13/ด้านICT/เทคโนโลยีในครัวเรือน/2562/Pocketbook_2562.pdf

สุดารัตน์ แสงแก้ว. (2558). การพัฒนาแบบวัดการเปิดเผยตัวตนบนเครือข่ายสังคมออนไลน์ (เฟสบุ๊ค). **วารสารวิชาการคณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏลำปาง**. 8(2), 101-111.

Cybersecurity Ventures. (2018). **Official Annual Cybercrime Report**. Retrieved November 25, 2020, from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Farnsworth, P. R. (1928). **The Spearman-Brown prophecy formula and the Seashore tests**. Journal of Educational Psychology, 19(8), 586-588.

Inter Telecommunication Union [ITU]. (2013). **Measuring the information society**. Geneva: . Retrieved November 25, 2020, from https://www.itu.int/en/ITU-D/Statistics/Documents/publications/anapub/Youth_2008.pdf

Jirojanakul, Pragai & Skevington, Suzanne. (2010). Developing a quality of life measure for children aged 5-8 years. **British Journal of Health Psychology**. 5. 299-321.

เอกสารอ้างอิง

Nunnally, J.C. and Bernstein, I.H. (1994) The Assessment of Reliability. Psychometric Theory, 3, 248-292.

Polit, D. F., & Hungler, B. P. (1999). Nursing research: Principles and methods (6th ed.). Philadelphia: Lippincott.

The European Computer Security Incident Response Team Network. (2003). **WP4 Clearinghouse Policy**. Retrieved November 5, 2020, from http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html

National statistics office thailand. (2562). **The 2019 Household survey on the use of information and communication technology**. Retrieved Octorber 8, 2020, from http://www.nso.go.th/sites/2014/DocLib13/ด้านICT/เทคโนโลยีในครัวเรือน/2562/ Pocketbook_2562.pdf

Pongpon Pawasut. (2561). **An In-dept of the Social Engineering attarcks of generlation y in Bangkok and Metropolitan**. Master of Science Program, Thammasat University.

Sudarat sangkaew. (2558). Scale Development of Self-Disclosure Through Online Social Network (Facebook). **Industrial Technology Lampang Rajabhat University Journal**. 8(2), 101-111.

Thaicert (Thailand Computer Emergency Response Team). (2563). **Threat statistics 2563**. Retrieved Octorber 8, 2020, from https://www.thaicert.or.th/statistics/statistics.html