# สาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม ของกลุ่มเจเนอเรชั่นวาย ในเขตกรุงเทพมหานครและปริมณฑล

**พงศ์พนธ์ ภาวศุทธิ์***

บริษัท ฟิกเจอร์ เมกเกอร์ จำกัด

***Correspondence:** pongpon.atc@gmail.com
doi: 10.14456/jisb.2019.1

วันที่รับบทความ: 14 พ.ย. 2561 วันแก้ไขบทความ: 28 พ.ย. 2561 วันตอบรับบทความ: 18 ธ.ค. 2561

## บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาถึงสาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม ของกลุ่มเจเนอเรชั่นวาย ในเขตกรุงเทพมหานครและปริมณฑล ว่ามีสาเหตุใดบ้างที่ส่งผลให้บุคคลที่ได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมในรูปแบบต่าง ๆ เช่น อีเมล เว็บไซต์ สื่อสังคมออนไลน์ เป็นต้น นั้นตัดสินใจกระทำตามสิ่งที่ผู้โจมตีต้องการและถูกโจมตี โดยงานวิจัยนี้เป็นการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research) ซึ่งเก็บข้อมูลด้วยการสัมภาษณ์เชิงลึก (In-Depth Interview) จากผู้ให้สัมภาษณ์ทั้งสิ้น 18 ท่าน ที่เคยมีประสบการณ์ได้รับสารสนเทศที่เป็นภัยคุกคามโดยมีเหตุการณ์ที่หลากหลายและแตกต่างกัน โดยคำถามที่ใช้ในการสัมภาษณ์เป็นคำถามแบบปลายเปิด เพื่อที่ผู้ให้สัมภาษณ์จะสามารถให้ข้อมูลเพิ่มเติมได้ ผลการวิจัยพบว่า สาเหตุที่ส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมนั้นสามารถแบ่งได้เป็น 2 กรณี คือ กรณีที่หนึ่งเป็นบุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมและถูกโจมตี จะมีปัจจัยที่ส่งผลได้แก่ การตัดสินใจอย่างไม่มีเหตุผล ที่เกิดขึ้นจาก ความอยากรู้อยากเห็น ความกลัว และความโลภ ซึ่งเป็นอารมณ์ความรู้สึกพื้นฐานของมนุษย์ โดยผู้โจมตีจะใช้ลักษณะเฉพาะของสารสนเทศ เช่น ช่องทาง เนื้อหา รูปแบบ และรูปภาพ ที่สร้างมาเพื่อให้ผู้ถูกโจมตีนั้นเกิดอารมณ์ความรู้สึกอย่างใดอย่างหนึ่งข้างต้นและตัดสินใจอย่างไม่มีเหตุผลจนส่งผลให้ถูกโจมตีได้ ส่วนกรณีที่สองเป็นบุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมในรูปแบบต่าง ๆ แต่ไม่ถูกโจมตี จะมีปัจจัยส่งผลได้แก่ การรับรู้ภัยคุกคามซึ่งเกิดขึ้นมาจาก ประสบการณ์ก่อนหน้า และการแจ้งเตือน โดยเมื่อบุคคล มีการรับรู้ภัยคุกคามมากเพียงพอแล้วจะมีการตัดสินใจที่ใช้เหตุผลไตร่ตรองมากยิ่งขึ้นและไม่ถูกโจมตี ข้อจำกัดของงานวิจัยนี้คือการที่อัตราส่วนผู้ให้สัมภาษณ์ของเพศหญิงมีมากกว่าเพศชาย โดยเป็นเพศหญิง 14 ท่าน และเพศชาย 4 ท่าน และผลของการวิจัยของผู้ให้สัมภาษณ์เพศชายที่พบว่าเหตุการณ์ส่วนใหญ่จะเป็นการได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมแต่ไม่ถูกโจมตี ดังนั้นการนำผลการวิจัยนี้ไปใช้อาจต้องคำนึงถึงเรื่องเพศด้วยเช่นกัน ในส่วนของข้อแนะนำสำหรับงานวิจัยต่อเนื่องนั้น เนื่องจากสาเหตุของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม สะท้อนให้เห็นว่า อารมณ์และความรู้สึกต่าง ๆ ส่งผลให้ผู้ถูกโจมตีตัดสินใจอย่างไม่มีเหตุผลและถูกโจมตีในที่สุด แต่การรับรู้ภัยคุกคามที่สูงนั้นจะสามารถยับยั้งการถูกโจมตีได้ จึงควรศึกษาหาแนวทางการป้องกันการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม โดยอาจศึกษาลึกลงไปในสาเหตุต่าง ๆ ว่าควรจะสร้างการรับรู้ภัยคุกคามและป้องกันอย่างไรให้ได้ประสิทธิภาพสูงที่สุด

**คำสำคัญ:** วิศวกรรมสังคม การรักษาความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคามทางคอมพิวเตอร์ การถูกโจมตี

# An in-depth study of the social engineering attacks of Generation Y in Bangkok and Metropolitan

**Pongpon Pawasut***

Fixture Maker Co., Ltd

***Correspondence:** pongpon.atc@gmail.com
doi: 10.14456/jisb.2019.1

Received: 14 Nov 2018 Revised: 28 Nov 2018 Accepted: 18 Dec 2018

## Abstract

The purpose of this study is to identify factors affecting the causes of social engineering attacks of Y generation in Bangkok and Metropolitan. This study differs from other studies by emphasizing on in-depth factors. This research is a qualitative research. Data has been collected from 18 people both male and female by in-depth interview. The analyzing results can be classified by participants into two groups The first group is people who make decision unreasonably. They are more likely to be attacked by social engineering and unhesitatingly clicking through attractive information such as format, content, photo, and channel. They focus on their basic emotions like curiosity, fear, and greed. The second group is people who perceive threats of social engineering. These people will certainly not click through the links or messages they got from attackers because of their prior experience and earlier warning about this issue. Therefore, they will make decision reasonably before they access to any social medias. The limitation of this research is the ratio of interviewees. The ratio between male and female is totally different. There are fourteen females who share experiences while only four males provide information about social engineering issue. Moreover, most of males who were interviewed is subjected to the second group which perceived threats and not click through links or messages. Hence, gender is also essential factor for referring this issue. In term of suggestion, this issue reflects that emotion can bring people to face with threat of social engineering. However, it can be effectively prevented if people perceived about threats. Future research may study more deeply through the reason of each cause in order to increase awareness of threats and decrease number of victims.

**Keywords:** Social engineering, Cybersecurity, Computer threats, Attacks

## 1. บทนำ

### 1.1 ความสำคัญและที่มาของปัญหา

ปัจจุบันเทคโนโลยีอินเทอร์เน็ตพัฒนาขึ้นอย่างก้าวกระโดดและได้เข้ามามีบทบาทอย่างมากในชีวิตของมนุษย์ตั้งแต่เรื่องส่วนตัว เรื่องการทำงาน และเรื่องอื่นๆ (Hendricks, 2017) ทำให้ผู้ใช้งานอินเทอร์เน็ตเพิ่มสูงขึ้นอย่างต่อเนื่อง (John, 2017) และจากปริมาณผู้ใช้งานจำนวนมากนั้นย่อมส่งผลให้ภัยคุกคามจากอินเทอร์เน็ตมีอัตราการเกิดเพิ่มสูงขึ้นและมีความรุนแรงมากขึ้น (Gammons, 2017) โดยปัญหาภัยคุกคามส่วนใหญ่นั้นมักจะเกิดจากความไม่ระวังของผู้ใช้งานเอง (Dascalescu, 2018) เมื่อผู้ใช้งานไม่ตระหนักถึงภัยคุกคาม ก็เป็นเหตุทำให้ภัยคุกคามต่างๆ นั้นเกิดขึ้นได้ง่ายขึ้น ซึ่งภัยคุกคามที่เกิดขึ้นมากในช่วงปี 2017 ที่ผ่านมาก็คือ แรนซัมแวร์ หรือโปรแกรมเรียกค่าไถ่ (Crowe, 2018) โดยการระบาดของแรนซัมแวร์นั้นจะระบาดทางอีเมลเป็นส่วนใหญ่ (Mason, 2018) โดยจะทำเป็นอีเมลหลอก หรือที่เรียกว่า ฟิชชิ่ง ซึ่งมักจะปลอมแปลงเป็นหน่วยงานหรือบุคคลที่น่าเชื่อถือแล้วส่งอีเมลที่มี URL ให้เหยื่อคลิก นอกจากนี้ยังมีการโจมตีโดยการทำฟิชชิ่งบนอินเทอร์เน็ตในรูปแบบอื่นๆ นอกจากอีเมลอีกด้วย เช่น ในสื่อสังคมออนไลน์ เฟซบุ๊ก ทวิตเตอร์ เป็นต้น (Institute of Information Security, 2014) โดยการทำฟิชชิ่งนั้นจะประสบความสำเร็จได้ยาก หากผู้โจมตีไม่มีทักษะวิศวกรรมสังคม ซึ่งวิศวกรรมสังคม คือศิลปะทางการสื่อสารอย่างหนึ่งที่ใช้เพื่อหลอกลวงผู้คนเพื่อให้ได้ผลประโยชน์ตามที่ผู้โจมตีต้องการ โดยจะอาศัยจุดอ่อน ความไม่รู้ ความประมาทของผู้ถูกโจมตี ทำให้วิธีการทางวิศวกรรมสังคมเป็นการโจมตีที่ได้ผลดีมากเมื่อเทียบกับการโจมตีรูปแบบอื่นๆ โดยเฉพาะเมื่อใช้กับผู้ที่ไม่มีความรู้หรือไม่ตระหนักถึงความมั่นคงปลอดภัย โดยผู้โจมตีอาจจะสร้างสถานการณ์ต่างๆ ขึ้นมา เช่น สถานการณ์ฉุกเฉิน ปลอมตัวเป็นบุคคลที่น่าเชื่อถือ กล่าวถึงเหตุการณ์ในปัจจุบันเพื่อความสมจริง อำพรางปลอมแปลง URL ให้คล้ายๆ กับของจริง เป็นต้น ในปัจจุบันผู้โจมตีนั้นมีเทคนิคในการหลอกลวงที่หลากหลายและแนบเนียนกว่าในอดีตมาก (Sophos, 2016) หรือกล่าวโดยสรุปได้ว่าการทำวิศวกรรมสังคมจะทำให้การโจมตีง่ายขึ้นและมีประสิทธิภาพมากกว่าวิธีการโจมตีอื่นๆ

เมื่อทราบถึงโอกาสและความรุนแรงในการถูกโจมตีรวมไปถึงวิธีการในการโจมตีแล้ว ในการป้องกันนั้นกลับทำได้ยากยิ่งกว่า งานวิจัยของ Junger et al. (2017) ระบุว่า การบอกให้ทราบและแจ้งเตือนไม่สามารถป้องกันการโจมตีด้วยวิธีทางวิศวกรรมสังคมอย่างได้ผล ซึ่งในบทวิจัยได้ทดลองกับกลุ่มตัวอย่างจำนวน 290 คนในประเทศเนเธอร์แลนด์ โดยถามคำถามทั่วไป หลังจากนั้นก็จะแจ้งเตือนเรื่องการเปิดเผยข้อมูลส่วนบุคคลและการทำฟิชชิ่งในรูปแบบต่างๆ และสุดท้ายก็จะเป็นส่วนคำถามข้อมูลส่วนตัวให้กรอกเช่น อีเมล เลขที่บัญชี เว็บไซต์ที่ซื้อของออนไลน์ เป็นต้น พบว่าร้อยละ 80 ของกลุ่มตัวอย่างยอมเปิดเผยข้อมูลส่วนบุคคลถึงแม้จะได้รับการแจ้งเตือนเกี่ยวกับเรื่องการเปิดเผยข้อมูลส่วนบุคคลและการทำฟิชชิ่งในรูปแบบต่างๆ จึงสรุปได้ว่าผู้คนนั้นไว้ใจผู้อื่นและมีแนวโน้มที่จะเปิดเผยข้อมูลส่วนบุคคลโดยง่าย ซึ่งเป็นจุดอ่อนและสาเหตุให้เกิดการโจมตีโดยใช้เทคนิคทางวิศวกรรมสังคม นอกจากนี้ยังมีงานวิจัยอื่นๆ เกี่ยวกับการแจ้งเตือนซึ่งไม่ได้ผลเช่น งานวิจัยของ Krol et al. (2012) ที่พบว่าร้อยละ 81.7 ของผู้ที่ดาวน์โหลดไฟล์ PDF ละเลยการแจ้งเตือน และงานวิจัยของ Wu et al. (2006) ที่กล่าวว่าผู้ใช้งานจะเพิกเฉยต่อแถบการแจ้งเตือน สุดท้ายนี้ Benenson (2016) ยังกล่าวว่าร้อยละ 78 ของกลุ่มตัวอย่าง ทราบถึงความเสี่ยงของ URL ที่ไม่รู้จักในอีเมล แต่ก็มีร้อยละ 45 ที่ยังคลิก URL นั้นแม้จะทราบถึงความเสี่ยงและภัยคุกคาม

จากการที่พบว่าการเกิดภัยคุกคามทางคอมพิวเตอร์นั้น ส่วนใหญ่จะเกิดจากตัวผู้ใช้งานเอง โดยการโจมตีผ่านผู้ใช้งานที่ประสบความสำเร็จมากที่สุดก็คือการทำวิศวกรรมสังคม ซึ่งถึงแม้ว่าผู้ใช้งานจะมีความรู้เกี่ยวกับภัยคุกคามอยู่บ้าง ก็ยังคงมีโอกาสที่จะถูกโจมตีได้ และเนื่องจากการถูกโจมตีที่เป็นปัญหาในปัจจุบันยังไม่ทราบสาเหตุที่แน่ชัด จึงทำให้การป้องกันนั้นไม่ได้ผลดีเท่าที่ควร ซึ่งผู้วิจัยมีความสนใจที่จะศึกษาปัญหาที่เกิดขึ้น เพื่อหาสาเหตุเชิงลึกของปัญหานี้ โดยในเบื้องต้นจะนำทฤษฎีทางจิตวิทยา ทฤษฎีทางเทคโนโลยีสารสนเทศ รวมไปถึงกรอบแนวคิดจากงานวิจัยที่น่าสนใจที่เกี่ยวข้องมาพิจารณาในการวิจัย

### 1.2 วัตถุประสงค์ของการวิจัย

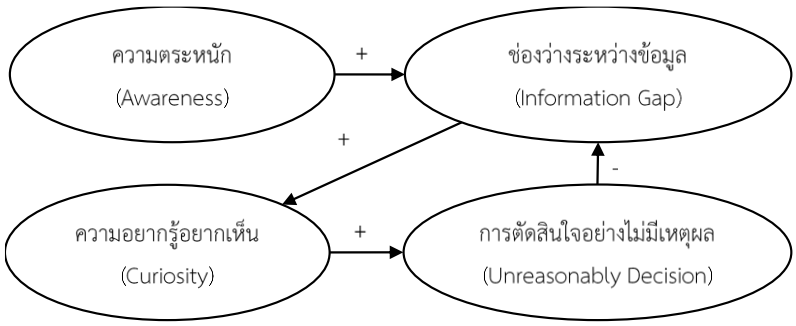
งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาถึงสาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม โดยมีรายละเอียดในการศึกษาถึงเหตุการณ์ที่เกิดขึ้นขณะถูกโจมตีด้วยวิธีทางวิศวกรรมสังคม ว่ามีสาเหตุใดบ้างที่ทำให้ผู้ถูกโจมตีนั้นถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม และสาเหตุที่ทำให้ผู้ถูกโจมตีนั้นละเลยการแจ้งเตือนความปลอดภัยและถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม รวมไปถึงปัญหาและผลกระทบของผู้ถูกโจมตีหลังจากการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม

## 2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

### 2.1 ทฤษฎีที่เกี่ยวข้องกับการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม

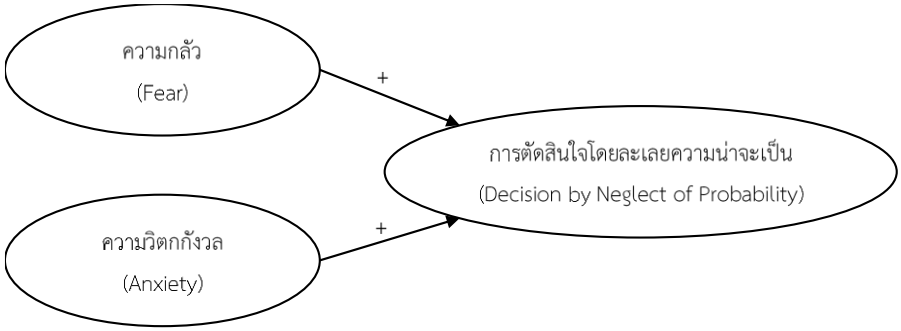
เนื่องจากการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมนั้นจะเกิดจากตัวผู้ใช้งานคอมพิวเตอร์เอง เพื่อหาสาเหตุเชิงลึกของปัญหานี้ งานวิจัยที่เกี่ยวข้องจึงเป็นทฤษฎีทางจิตวิทยาสังคม (Social psychology) ซึ่งเกี่ยวข้องกับการตัดสินใจของผู้ใช้งานคอมพิวเตอร์ที่ทำให้ถูกโจมตี ได้แก่ ทฤษฎีช่องว่างระหว่างข้อมูล แนวคิดการละเลยความน่าจะเป็น แนวคิดพฤติกรรมชั่ววูบ ทฤษฎีแรงจูงใจเพื่อป้องกัน

ทฤษฎีช่องว่างระหว่างข้อมูล พัฒนาโดย Loewenstein ในปี 1994 เป็นทฤษฎีทางจิตวิทยา ที่กล่าวว่า เมื่อบุคคลมีความตระหนักหรือเผชิญหน้ากับสิ่งใหม่ที่ไม่คุ้นเคย จะทำให้เกิดช่องว่างระหว่างข้อมูล (Information gap) ซึ่งจะส่งผลให้บุคคลเกิดความอยากรู้อยากเห็น และทำให้บุคคลแสดงพฤติกรรมเพื่อลดช่องว่างระหว่างข้อมูล ต่อมา Golman and Loewenstein (2016) ได้ทำการวิจัยต่อเนื่องเพื่อศึกษาทฤษฎีช่องว่างระหว่างข้อมูลกับการตัดสินใจภายใต้ความไม่แน่นอน โดยได้กล่าวว่าหากบุคคลที่มีช่องว่างของข้อมูลจะทำการตัดสินใจภายใต้ความเสี่ยงและความไม่แน่นอน บุคคลจะพยายามปิดช่องว่างระหว่างข้อมูลโดยการตัดสินใจอย่างไม่มีเหตุผลเพื่อจะทำให้ช่องว่างระหว่างข้อมูลมีความสำคัญมากขึ้นและหากบุคคลคาดว่าข้อมูลที่จะได้รับนั้นจะทำให้พึงพอใจ บุคคลก็จะตัดสินใจที่จะรับความเสี่ยงเพื่อปิดช่องว่างของข้อมูลนั้น ดังแสดงในภาพที่ 1



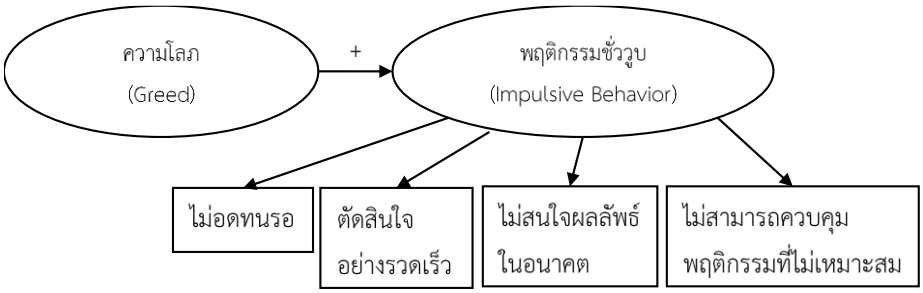

ภาพที่ 1 ทฤษฎีช่องว่างระหว่างข้อมูลกับการตัดสินใจภายใต้ความไม่แน่นอน

การละเลยความน่าจะเป็น เป็นแนวคิดเกี่ยวกับพฤติกรรมทางจิตวิทยาการรับรู้ ที่เกิดจากอคติของการรับรู้ (Cognitive bias) ต่อยอดมาจากทฤษฎีคาดหวัง (Prospect theory) และแนวคิดการหลีกเลี่ยงความสูญเสีย โดยแนวคิดการละเลยความน่าจะเป็นนั้นจะอธิบายเกี่ยวกับสาเหตุของการตัดสินใจอย่างไม่มีเหตุผลของบุคคลภายใต้ความไม่แน่นอนในสถานการณ์ต่าง ๆ โดยแนวคิดนี้กล่าวว่า เมื่อบุคคลเกิดอารมณ์ความรู้สึกเช่น ความกลัว ความวิตกกังวล จะมีผลต่อการตัดสินใจของบุคคลโดยส่งผลให้เกิดการตัดสินใจที่ไม่ใช้หลักเหตุผล ซึ่งในที่นี้คือการตัดสินใจโดยไม่มีการประเมินความน่าจะเป็น (Kahneman, 2011; Michel-Kerjan & Slovic, 2010) ดังแสดงในภาพที่ 2



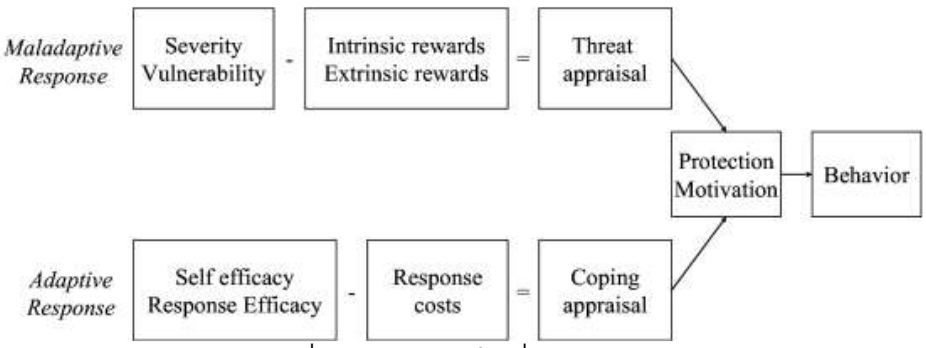

ภาพที่ 2 แนวคิดการละเลยความน่าจะเป็น

แนวคิดพฤติกรรมชั่ววูบ เป็นแนวคิดเกี่ยวกับการตัดสินใจและแสดงออกทางพฤติกรรมของบุคคลในทางจิตวิทยา ที่ใช้อธิบายพฤติกรรมการตัดสินใจอย่างรวดเร็วและไม่มีเหตุผลของบุคคล (Rook & Gardner, 1993) ซึ่งการเกิดพฤติกรรมชั่ววูบนั้นมีสาเหตุหลากหลาย และความโลภนั้นก็เป็นหนึ่งในสาเหตุ (Dijkstra, 2018; Seuntjens et al., 2015) โดยเมื่อบุคคลเกิดความโลภแล้วจะส่งผลให้บุคคลนั้นเกิดพฤติกรรมชั่ววูบ ดังแสดงในภาพที่ 3




ภาพที่ 3 แนวคิดพฤติกรรมชั่ววูบ

ทฤษฎีแรงจูงใจเพื่อป้องกัน (Protection Motivation Theory) พัฒนาขึ้นโดย Rogers ในปี 1975 เป็นทฤษฎีทางจิตวิทยาสังคม ที่พัฒนาขึ้นมาจากทฤษฎีความคาดหวังในความสามารถตนเอง (Self-efficacy theory) (Rogers, 1975) และแนวคิดความเชื่อด้านสุขภาพ (Health belief model) เพื่อศึกษาการรับรู้ของมนุษย์ที่นำไปสู่การป้องกันตนเองในทางสุขภาพ โดยพบว่าหลังจากบุคคลได้รับรู้ข้อมูลต่าง ๆ ไม่ว่าจะเป็นจากสภาพแวดล้อมได้แก่ ข่าวสารและการแจ้งเตือน หรือจากตนเองได้แก่ ประสบการณ์ ก็จะประเมินข้อมูลเหล่านั้นเพื่อตัดสินใจว่าจะเปลี่ยนแปลงพฤติกรรมหรือปรับตัวรับมือกับภัยคุกคามหรือไม่ โดยมีผลมาจากกระบวนการประเมิน 2 ส่วน ได้แก่ กระบวนการประเมินภัยคุกคาม (Threat appraisal) และกระบวนการประเมินการเผชิญปัญหา (Coping appraisal) ซึ่งจะส่งผลต่อแรงจูงใจ และพฤติกรรมต่อไป (Rogers, 1983) ดังแสดงในภาพที่ 4




ภาพที่ 4 ทฤษฎีแรงจูงใจเพื่อป้องกัน

**2.2 งานวิจัยที่เกี่ยวข้องกับการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม**

จากการศึกษางานวิจัยในอดีตยังทำให้พบปัจจัยที่มีความสำคัญต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม ซึ่งประกอบด้วย การตัดสินใจอย่างไม่มีเหตุผล ประสบการณ์ก่อนหน้า การแจ้งเตือน และลักษณะเฉพาะของสารสนเทศ

การตัดสินใจอย่างไม่มีเหตุผล งานวิจัยของ Ahmed and Omotunde (2012) กล่าวถึงการตัดสินใจที่ไม่ดี (Bad decision) ไว้ว่าเป็นการตัดสินใจที่จะส่งผลให้เกิดผลลัพธ์ที่ไม่ได้คาดคิด หรือเกิดผลลัพธ์เชิงลบ ซึ่งการตัดสินใจที่ไม่ดีเกิดขึ้นได้จากหลายสาเหตุ เช่น ไม่มีทางเลือก ไม่มีข้อมูล ไม่มีเวลาในการคิด ละเลยการประเมิน เป็นต้น ซึ่งสอดคล้องกับ ปกรณ์ คำกอง (2555) ที่ได้กล่าวว่า การรีบเร่งทำการตัดสินใจเป็นการตัดสินใจซึ่งไม่ได้มีการใช้เหตุผลประเมินทางเลือกต่างๆ ให้ดีก่อนทำการตัดสินใจ จะส่งผลต่อคุณภาพของการตัดสินใจ อีกทั้งงานวิจัยของ Arvai and Froschauer (2010) ที่ศึกษาเรื่องความสัมพันธ์ของคุณภาพการตัดสินใจกับผลลัพธ์ พบว่าการตัดสินใจจะมีคุณภาพมากยิ่งขึ้น ในกรณีที่ให้ผู้เข้าร่วมการวิจัยตัดสินใจโดยสนใจผลลัพธ์มากขึ้น

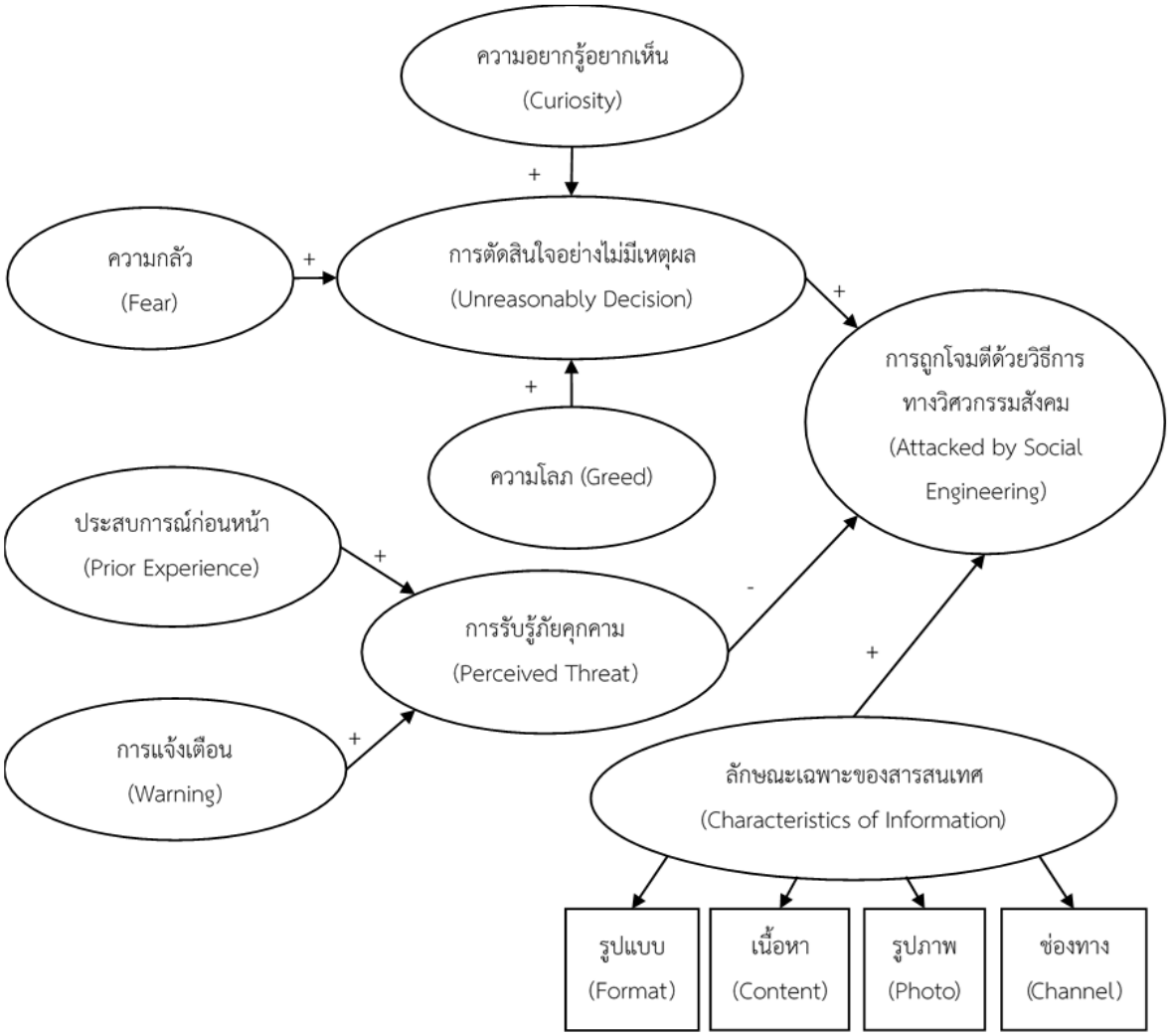
ประสบการณ์ก่อนหน้า งานวิจัยของ Safa et al. (2016) ซึ่งเป็นงานวิจัยที่ศึกษาว่ามีปัจจัยใดบ้างในองค์กรที่ส่งผลต่อการรักษาความมั่นคงปลอดภัยของพนักงานในองค์กร ซึ่งปัจจัยประสบการณ์เป็นปัจจัยหนึ่งที่ส่งผลต่อทัศนคติและพฤติกรรม โดยได้กล่าวเพิ่มเติมว่าประสบการณ์ก่อนหน้านั้นเกิดจากการที่แต่ละบุคคลได้รับรู้และสร้างทัศนคติของแต่ละบุคคลขึ้นมาเองจากประสบการณ์ส่วนตัวหรือจากการเรียนรู้ผ่านบุคคลอื่น โดยประสบการณ์ในด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ คือความคุ้นเคยกับภัยคุกคามหรือเหตุการณ์ที่เกิดขึ้นในอดีต กล่าวคือหากบุคคลเผชิญกับภัยคุกคามมาก่อนหน้าจะมีการรับรู้ภัยคุกคาม และพยายามหาทางป้องกันหรือรับมือกับภัยคุกคามที่จะเกิดขึ้นในอนาคตนั้น นอกจากนี้งานวิจัยของ Lee et al. (2016) ซึ่งเป็นงานวิจัยที่ศึกษาว่ามีปัจจัยใดบ้างในองค์กรที่ส่งผลต่อความตึงเครียดของการรักษาความมั่นคงปลอดภัยสารสนเทศ พบว่ามีปัจจัยเริ่มต้นได้แก่ ความรู้ก่อนหน้าเกี่ยวกับการรักษาความมั่นคงปลอดภัย และการรับรู้ภัยคุกคาม ซึ่งจะส่งผลต่อทัศนคติและพฤติกรรมต่อไป โดยได้อธิบายเพิ่มเติมในส่วนของความรู้ก่อนหน้าเกี่ยวกับการรักษาความมั่นคงปลอดภัยว่าเกิดขึ้นจากประสบการณ์ก่อนหน้าที่ถูกบันทึกไว้ในความทรงจำ และจะถูกใช้ในการกำหนดการรับรู้หรือทัศนคติเกี่ยวกับเรื่องและเหตุการณ์ต่างๆ เช่น พนักงานที่มีความรู้และประสบการณ์ก่อนหน้า ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยจะรู้ถึงภัยคุกคามและมีความตั้งใจที่จะปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยข้อมูลขององค์กร

การแจ้งเตือน มีงานวิจัยในอดีตจำนวนมากศึกษาเกี่ยวกับการแจ้งเตือนพบว่า บุคคลจะเชื่อและปรับพฤติกรรมตามการแจ้งเตือนอันตรายก็ต่อเมื่อบุคคลนั้นมีความเข้าใจถึงการแจ้งเตือนนั้น (Mileti & Sorensen, 1990) และมีความรู้เกี่ยวกับภัยคุกคาม (Ripberger et al., 2014) รวมไปถึงรับรู้ถึงผลกระทบที่อาจเกิดขึ้นด้วย (Perry & Lindell, 1990) โดยงานวิจัยของ Potter et al. (2018) ได้ศึกษากลุ่มตัวอย่างในประเทศนิวซีแลนด์ในเรื่องการรับรู้ภัยคุกคามจากสภาพอากาศผ่านการแจ้งเตือนเพื่อศึกษาว่าหลังจากแจ้งเตือนไปแล้วกลุ่มตัวอย่างนั้นมีการรับรู้ภัยคุกคามและปรับพฤติกรรมหรือไม่ ซึ่งพบว่ากลุ่มตัวอย่างที่ได้รับการแจ้งเตือนแบบผลกระทบจะมีการปรับเปลี่ยนพฤติกรรม เช่น หาข้อมูลเพิ่มเติม ทำความเข้าใจผลกระทบ รับรู้ภัยคุกคาม และเป็นกังวลเกี่ยวกับภัยคุกคามนั้นๆ ซึ่งแตกต่างจากกลุ่มตัวอย่างที่ได้รับการแจ้งเตือนแบบปรากฏการณ์ ซึ่งกลุ่มตัวอย่างไม่ได้มีการเปลี่ยนพฤติกรรมไปจากเดิม

ลักษณะเฉพาะของสารสนเทศ มีงานวิจัยที่ระบุว่าข้อมูลต่างๆ บนอินเทอร์เน็ตในปัจจุบันสามารถถูกสร้างขึ้นได้โดยง่ายและส่วนใหญ่นั้นไม่ได้มีการควบคุมแหล่งที่มาและความน่าเชื่อถือ จึงเป็นสาเหตุที่ทำให้ผู้ใช้งานจำเป็นต้องพิจารณาความน่าเชื่อถือของข้อมูลเหล่านั้นด้วยตนเอง (Li & Suh, 2015) โดยงานวิจัยของ Machackova and Smahel (2018) ได้ศึกษาเกี่ยวกับปัจจัยต่างๆ ที่ทำให้สารสนเทศมีความน่าเชื่อถือ โดยศึกษาจากความคิดเห็นของกลุ่มตัวอย่างที่เข้าชมเว็บไซต์เกี่ยวกับสุขภาพ ซึ่งผลการศึกษาพบว่า ปัจจัยที่ส่งผลต่อความน่าเชื่อถือของสารสนเทศนั้นประกอบด้วย ผู้เขียน เนื้อหา การตอบกลับ แหล่งอ้างอิง

## 3. กรอบแนวคิดการวิจัยเบื้องต้นและคำถามการวิจัย

จากกรอบแนวคิดการวิจัยเบื้องต้นของสาเหตุเชิงลึกที่ส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม ดังแสดงในภาพที่ 5 จะเห็นได้ว่าการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม (Attacked by social engineering) นั้นจะมีอิทธิพลมาจากการตัดสินใจอย่างไม่มีเหตุผล (Unreasonably decision) และลักษณะเฉพาะของสารสนเทศ (Characteristics of information) แต่สามารถลดลงได้ด้วยการรับรู้ภัยคุกคาม (Perceived threat) โดยปัจจัยที่ส่งผลให้บุคคลตัดสินใจอย่างไม่มีเหตุผลนั้นได้แก่ ความอยากรู้อยากเห็น (Curiosity) ความกลัว (Fear) และความโลภ (Greed) ซึ่งปัจจัยทั้งหมดนี้ส่งผลทางตรงต่อการตัดสินใจอย่างไม่มีเหตุผล ส่วนการรับรู้ภัยคุกคามนั้นจะมีปัจจัยที่ส่งผลได้แก่ ประสบการณ์ก่อนหน้า (Prior experience) และการแจ้งเตือน (Warning) ดังนั้นจึงสามารถกำหนดเป็นปัจจัยที่มีผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมได้ดังนี้




ภาพที่ 5 กรอบแนวคิดการวิจัยเบื้องต้นของสาเหตุเชิงลึกที่ส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม

จากที่มาและความสำคัญของปัญหาและจากทฤษฎีและงานวิจัยที่เกี่ยวข้องทำให้สามารถตั้งคำถามการวิจัยว่าทำไมและอย่างไรที่ทำให้ผู้ถูกโจมตีนั้นถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม

## 4. วิธีการดำเนินการวิจัย

### 4.1 การวิจัยเชิงคุณภาพและการสัมภาษณ์เชิงลึก

งานวิจัยนี้เป็นงานวิจัยเชิงคุณภาพ โดยทำการสัมภาษณ์เชิงลึกในการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมว่าประกอบไปด้วยสาเหตุอะไรบ้าง พร้อมทั้งวิเคราะห์เหตุการณ์ต่าง ๆ ของการถูกโจมตี เพื่อให้ได้ข้อมูลที่เหมาะสมสอดคล้องกับวัตถุประสงค์งานวิจัยอย่างแท้จริง และสามารถตอบคำถามการวิจัยต่าง ๆ ในกรอบแนวคิดการวิจัยเบื้องต้นได้ โดยผู้วิจัยเปิดรับสมัครผู้เข้าร่วมการวิจัยทางสื่อสังคมออนไลน์รวมถึงโฆษณาประชาสัมพันธ์การเปิดรับสมัครผ่านสื่อสังคมออนไลน์ ทำให้มีผู้ที่เคยได้รับสารสนเทศที่เกี่ยวข้องกับการโจมตีด้วยวิธีการทางวิศวกรรมสังคมสนใจสมัครมาทั้งสิ้น 48 ท่าน ต่อมาผู้วิจัยคัดกรองผู้สมัครเพื่อเลือกเป็นผู้ให้สัมภาษณ์แบบมีวัตถุประสงค์ (Purposeful sampling) ด้วยการสอบถามรายละเอียดเกี่ยวกับเหตุการณ์การถูกโจมตีเบื้องต้น ตรวจสอบความรู้ความเข้าใจของผู้สมัคร ซึ่งได้ผู้สมัครที่มีคุณลักษณะที่จะเป็นผู้ให้สัมภาษณ์ที่เข้าร่วมการวิจัยทั้งสิ้น 18 ท่าน เป็นเพศหญิง 14 ท่าน เพศชาย 4 ท่าน และผู้วิจัยได้แบ่งผู้ให้สัมภาษณ์ออกเป็นสองกลุ่ม ตามการตัดสินใจของผู้ให้สัมภาษณ์ในเหตุการณ์การถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม ได้แก่บุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมในรูปแบบต่าง ๆ และถูกโจมตี มีผู้ให้สัมภาษณ์ทั้งสิ้น 14 ท่าน และบุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมในรูปแบบต่าง ๆ แต่ไม่ถูกโจมตี มีผู้ให้สัมภาษณ์ทั้งสิ้น 4 ท่าน โดยกลุ่มบุคคลทั้งสองจะต้องเป็นบุคคลในกลุ่มเจเนอเรชั่นวาย ซึ่งหมายถึงบุคคลที่เกิดในปี พ.ศ. 2521-2540 (Mitrakul & Kongchan, 2016) ซึ่งอาศัยในเขตกรุงเทพมหานครและปริมณฑล และมีความรู้ความเข้าใจเบื้องต้นในเรื่องของคอมพิวเตอร์ รู้จักภัยคุกคามทางคอมพิวเตอร์ แต่ไม่ได้ทำงานในสายงานคอมพิวเตอร์ และผู้ให้สัมภาษณ์นั้นได้แสดงความสมัครใจให้ความร่วมมือในการทำวิจัย

ในการสร้างแนวทางการสัมภาษณ์เชิงลึก ผู้วิจัยได้จัดสร้างชุดคำถามสัมภาษณ์กึ่งโครงสร้าง (Semi-structured interview questions) ขึ้นตามวัตถุประสงค์ของงานวิจัย จากกรอบแนวคิดของการวิจัยเบื้องต้น โดยเขียนแนวคำถามให้มีลักษณะเป็นคำถามปลายเปิด โดยข้อคำถามจะอยู่ในขอบเขตดังนี้ (1) คำถามเกี่ยวกับเหตุการณ์การถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมอย่างละเอียด (ช่องทาง ลักษณะ และรายละเอียดต่าง ๆ) (2) คำถามเกี่ยวกับความรู้เกี่ยวกับภัยคุกคามทางคอมพิวเตอร์อย่างละเอียด (การรับรู้ภัยคุกคาม การแจ้งเตือน ประสบการณ์ก่อนหน้า) (3) คำถามเกี่ยวกับความรู้สึก ความคิด และการตัดสินใจอย่างละเอียด (4) คำถามเกี่ยวกับสาเหตุของการตัดสินใจที่ทำให้ถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม (กรณีถูกโจมตี) หรือสาเหตุของการตัดสินใจที่ทำให้ไม่ถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม (กรณีไม่ถูกโจมตี) (5) คำถามเกี่ยวกับผลกระทบที่เกิดขึ้นจากการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม (6) คำถามอื่นๆ (ถ้ามี)

### 4.2 การประเมินความน่าไว้วางใจของการวิจัย

ในการดำเนินงานวิจัยนี้ ผู้วิจัยคำนึงถึงประเด็นเรื่องความน่าไว้วางใจของงานวิจัย เพื่อให้มั่นใจว่างานวิจัยที่ได้ดำเนินการนั้นได้รับการรวบรวมและวิเคราะห์ประเด็นที่สำคัญของงานวิจัยอย่างครบถ้วนและสามารถตอบคำถามงานวิจัยได้อย่างถูกต้องเหมาะสม ผู้วิจัยได้ใช้แนวคิดเกี่ยวกับความน่าเชื่อถือของงานวิจัยจากหนังสือการวิจัยเชิงคุณภาพของนิศา ชูโต (2545) ซึ่งกล่าวว่างานวิจัยที่น่าเชื่อถือจะประกอบไปด้วยเรื่องดังนี้ (1) ความเชื่อถือได้ (Creditability) งานวิจัยนี้ผู้วิจัยได้ให้ผู้เชี่ยวชาญซึ่งปฏิบัติงานในสายงานเทคโนโลยีในระดับหัวหน้างานของบริษัทเอกชนแห่งหนึ่งที่ทำธุรกิจให้บริการรักษาความปลอดภัยขนส่งทรัพย์สินมีค่าทั้งภายในประเทศและต่างประเทศ เป็นเวลามากกว่า 10 ปี และมีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางคอมพิวเตอร์เป็นอย่างดี ในการยืนยันผลจากการวิเคราะห์ของผู้วิจัย โดยผู้วิจัยจะส่งผลการวิเคราะห์ให้ผู้เชี่ยวชาญอ่านและแสดงความคิดเห็นเพิ่มเติมเกี่ยวกับผลการวิเคราะห์ หลังจากนั้นผู้วิจัยจะปรับแก้ไขผลการวิเคราะห์ตามความเหมาะสม และให้ผู้เชี่ยวชาญยืนยันผลการวิจัย (2) การถ่ายโอนผลการวิจัย (Transferability) งานวิจัยนี้ผู้วิจัยใช้วิธีการสัมภาษณ์และวิเคราะห์ข้อมูลอย่างต่อเนื่อง เพื่อให้ได้ประเด็นที่น่าสนใจในการสัมภาษณ์เชิงลึกครั้งต่อ ๆ ไป ทั้งนี้ผู้ให้สัมภาษณ์เริ่มเห็นการให้ข้อมูล

ที่ซ้ำกันเมื่อการสัมภาษณ์ดำเนินมาถึงผู้ให้สัมภาษณ์คนที่ 8 อย่างไรก็ตาม ผู้ให้สัมภาษณ์ยังคงดำเนินการสัมภาษณ์ต่อไปอีกเพื่อให้มั่นใจว่าไม่มีประเด็นเพิ่มเติมแล้ว จึงหยุดการสัมภาษณ์ที่เดือนตุลาคม 2561 เมื่อดำเนินการสัมภาษณ์ผู้ให้สัมภาษณ์ไปทั้งสิ้น 18 คน (3) การพึ่งพากับเกณฑ์อื่น (Dependability) งานวิจัยนี้ผู้วิจัยจัดทำแบบทดสอบความรู้ความเข้าใจไว้ในแบบฟอร์มรับสมัครผู้เข้าร่วมการวิจัย เพื่อเป็นการยืนยันให้แน่ใจว่าผู้ให้สัมภาษณ์ที่เข้าร่วมการสัมภาษณ์นั้นมีความเข้าใจในเรื่องที่ให้สัมภาษณ์เป็นอย่างดี นอกจากนี้ผู้วิจัยยังได้ติดต่อผู้เข้าร่วมวิจัยที่สมัครเข้ามาเพื่อสอบถามรายละเอียดเบื้องต้นและยืนยันคำตอบกับแบบฟอร์มรับสมัครผู้เข้าร่วมการวิจัยเพื่อให้แน่ใจอีกครั้งก่อนที่จะเข้าสัมภาษณ์ (4) การยืนยันผลการวิจัย (Conformability) นอกจากการยืนยันผลการวิจัยกับผู้เชี่ยวชาญแล้ว งานวิจัยนี้ยังใช้โปรแกรมจัดกลุ่มคำสำหรับวิจัยเชิงคุณภาพ ในการให้รหัสคำ จัดกลุ่มและวิเคราะห์บทสัมภาษณ์ของผู้ให้สัมภาษณ์ด้วย

## 5. ผลการวิจัย

### 5.1 รายละเอียดของผู้ให้สัมภาษณ์

ในการศึกษาครั้งนี้ เป็นการสัมภาษณ์ผู้ให้สัมภาษณ์ที่เคยประสบกับเหตุการณ์การถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมทั้งสิ้น 18 ท่าน เป็นเพศหญิง 14 ท่าน เพศชาย 4 ท่าน ช่วงอายุที่พบมากคือ 23-25 ปี และมีอาชีพที่หลากหลาย ซึ่งเหตุการณ์ที่พบจะเป็นการโจมตีทางอีเมล์ 11 เหตุการณ์ ทางสื่อสังคมออนไลน์ 7 เหตุการณ์ ทางเว็บไซต์ 5 เหตุการณ์ และทาง SMS 1 เหตุการณ์ โดยมีรายละเอียดของผู้ให้สัมภาษณ์เบื้องต้น ดังแสดงในตารางที่ 1

ตารางที่ 1 รายละเอียดผู้ให้สัมภาษณ์สำหรับงานวิจัย

| | ข้อมูลเบื้องต้นของผู้ให้สัมภาษณ์ | รายละเอียดเบื้องต้นของเหตุการณ์ | การตัดสินใจ |
|---|---|---|---|
| ผู้ให้สัมภาษณ์คนที่ 1 | เพศหญิง อายุ 23 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาตรี อาชีพพนักงานบริษัทเอกชน ตำแหน่ง Project Coordinator | ลิงก์หลอกให้กดยกเลิกรายการซื้อแอปพลิเคชันผ่านทางอีเมลที่ถูกปลอมแปลงให้คล้ายกับ Apple | ตัดสินใจคลิกและกรอกข้อมูล (ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 2 | เพศหญิง อายุ 24 ปี อาศัยอยู่จังหวัดปทุมธานี การศึกษาระดับปริญญาตรี อาชีพพยาบาลวิชาชีพ (โรงพยาบาลรัฐ) | ลิงก์หลอกที่แชร์มาจากเพื่อนผ่านทางหน้าฟีดข่าวและกล่องข้อความของสื่อสังคมออนไลน์ (เฟซบุ๊ก) | ตัดสินใจคลิก (ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 3 | เพศหญิง อายุ 24 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาตรี อาชีพพนักงานบริษัทเอกชน (น้ำมัน) ตำแหน่ง Fleet Card Operation | Phishing Email ทดสอบในที่ทำงาน (เป็นการสร้างอีเมลฟิชชิ่งในที่ทำงานจากฝ่ายไอทีเพื่อส่งไปยังพนักงาน เพื่อทดสอบว่าพนักงานมีความตระหนักถึงภัยคุกคามมากน้อยเพียงใด) | ตัดสินใจคลิก (ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 4 | เพศหญิง อายุ 24 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาตรี อาชีพธุรกิจส่วนตัว (ขายสินค้าทางออนไลน์) | ลิงก์หลอกให้กดยกเลิกรายการซื้อแอปพลิเคชันผ่านทางอีเมลที่ถูกปลอมแปลงให้คล้ายกับ Apple และ หลอกว่าเพจในสื่อสังคมออนไลน์ (เฟซบุ๊ก) ของตนเองจะถูกปิด | ตัดสินใจคลิกและกรอกข้อมูล (ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 5 | เพศหญิง อายุ 24 ปี อาศัยอยู่จังหวัดปทุมธานี การศึกษาระดับปริญญาตรี อาชีพพนักงานประจำหน่วยงานราชการตำแหน่งนักวิเคราะห์นโยบายและแผน | ลิงก์ข่าวหลอกที่แชร์ผ่านทางหน้าฟีดข่าวของสื่อสังคมออนไลน์ (เฟซบุ๊ก) | ตัดสินใจคลิก (ถูกโจมตี) |

ตารางที่ 1 รายละเอียดผู้ให้สัมภาษณ์สำหรับงานวิจัย (ต่อ)

| | ข้อมูลเบื้องต้นของผู้ให้สัมภาษณ์ | รายละเอียดเบื้องต้นของเหตุการณ์ | การตัดสินใจ |
|---|---|---|---|
| ผู้ให้สัมภาษณ์คนที่ 6 | เพศหญิง อายุ 23 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาตรี อาชีพพนักงานธนาคารเอกชน ตำแหน่ง เจ้าหน้าที่สินเชื่อ | ลิงก์หลอกให้ลุ้นรางวัลผ่านทางอีเมลที่ถูกปลอมแปลงให้คล้ายกับอีเมลของบริษัทตนเอง | ตัดสินใจคลิกและกรอกข้อมูล (ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 7 | เพศหญิง อายุ 20 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาตรี อาชีพนักศึกษา | SMS หลอกว่าได้รับรางวัล | ตัดสินใจคลิกและกรอกข้อมูล (ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 8 | เพศหญิง อายุ 23 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาโท อาชีพพนักงานบริษัทเอกชน (สินค้าโภคภัณฑ์) ตำแหน่ง เจ้าหน้าที่ส่งออก | Phishing Email ทดสอบในที่ทำงาน (เป็นการสร้างอีเมลฟิชชิ่งในที่ทำงานจากฝ่ายไอทีเพื่อส่งไปยังพนักงาน เพื่อทดสอบว่าพนักงานมีความตระหนักถึงภัยคุกคามมากน้อยเพียงใด) | ตัดสินใจคลิก (ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 9 | เพศหญิง อายุ 25 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาโท อาชีพนักศึกษา | ลิงก์หลอกให้กดยกเลิกรายการซื้อแอปพลิเคชันผ่านทางอีเมลที่ถูกปลอมแปลงให้คล้ายกับ Apple | ตัดสินใจตอบกลับอีเมล (ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 10 | เพศหญิง อายุ 24 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาตรี อาชีพพนักงานบริษัทเอกชน (รถยนต์) ตำแหน่ง วิศวกรออกแบบ | ลิงก์หลอกทางอีเมล และ ลิงก์โฆษณาหลอกตามเว็บไซต์และสื่อสังคมออนไลน์ | ตัดสินใจไม่คลิก (ไม่ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 11 | เพศหญิง อายุ 24 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาตรี อาชีพพนักงานบริษัทเอกชน (ให้เช่ารถยนต์) ตำแหน่ง เจ้าหน้าที่วิเคราะห์ข้อมูล | ลิงก์หลอกทางเว็บไซต์ดาวน์โหลดหนังสือละเมิดลิขสิทธิ์ และ ลิงก์หลอกทางอีเมล | ตัดสินใจคลิกและดาวน์โหลดไฟล์ (ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 12 | เพศหญิง อายุ 24 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาตรี อาชีพพนักงานบริษัทเอกชน (โรงแรม) ตำแหน่ง พนักงานต้อนรับ | ลิงก์หลอกที่แชร์ผ่านทางหน้าฟีดข่าวของสื่อสังคมออนไลน์ (เฟซบุ๊ก) และเว็บไซต์ต่าง ๆ | ตัดสินใจคลิก (ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 13 | เพศชาย อายุ 22 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาตรี อาชีพพนักงานบริษัทเอกชน (สินค้าโภคภัณฑ์) ตำแหน่ง เจ้าหน้าที่การเงินและงบประมาณ | ลิงก์หลอกที่แชร์ผ่านทางหน้าฟีดข่าวของสื่อสังคมออนไลน์ (เฟซบุ๊ก) และเว็บไซต์ต่าง ๆ | ตัดสินใจคลิก (ถูกโจมตี) |

ตารางที่ 1 รายละเอียดผู้ให้สัมภาษณ์สำหรับงานวิจัย (ต่อ)

| | ข้อมูลเบื้องต้นของผู้ให้สัมภาษณ์ | รายละเอียดเบื้องต้นของเหตุการณ์ | การตัดสินใจ |
|---|---|---|---|
| ผู้ให้สัมภาษณ์คนที่ 14 | เพศหญิง อายุ 26 ปี อาศัยอยู่จังหวัดปทุมธานี การศึกษาระดับปริญญาโทอาชีพพนักงานโรงพยาบาลรัฐ ตำแหน่งนักวิเคราะห์นโยบายและแผน | อีเมลหลอกที่ส่งมาจากอีเมลจริงของคนรู้จักที่ถูกแฮกอีเมลและไลน์ที่ถูกปลอมให้เหมือนคนรู้จักที่ส่งมาเพื่อขอให้โอนเงินช่วยเหลือ และ ลิงก์หลอกที่แชร์มาจากเพื่อนผ่านทางกล่องข้อความของสื่อสังคมออนไลน์ (เฟซบุ๊ก) และ ลิงก์หลอกให้กดยกเลิกรายการซื้อแอปพลิเคชันผ่านทางอีเมลที่ถูกปลอมแปลงให้คล้ายกับ Apple และลิงก์หลอกให้แก้ปัญหาธุรกรรมออนไลน์ผ่านทางอีเมลที่ถูกปลอมแปลงให้คล้ายกับธนาคาร SCB | ตัดสินใจสอบถามก่อนและทราบว่าเป็นการหลอก (ไม่ถูกโจมตี)<br><br>ตัดสินใจไม่คลิก (ไม่ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 15 | เพศหญิง อายุ 25 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาโท อาชีพพนักงานบริษัทเอกชน (การทำบัญชี) ตำแหน่ง เจ้าหน้าที่ตรวจสอบบัญชี | ลิงก์หลอกให้แก้ปัญหารายการซื้อสินค้าออนไลน์จากเว็บไซต์ Lazada ผ่านทางอีเมลที่ถูกปลอมแปลงให้คล้ายกับธนาคาร Kbank | ตัดสินใจไม่คลิก (ไม่ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 16 | เพศชาย อายุ 27 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาโท อาชีพพนักงานบริษัทเอกชนตำแหน่ง เจ้าหน้าที่วิเคราะห์ข้อมูล | ลิงก์หลอกให้ยืนยันการปรับปรุงข้อมูลบัญชีธนาคารผ่านทางอีเมลที่ถูกปลอมแปลงให้คล้ายกับธนาคารแห่งหนึ่ง | ตัดสินใจไม่คลิก (ไม่ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 17 | เพศชาย อายุ 27 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาโท อาชีพพนักงานธนาคารเอกชนตำแหน่ง เจ้าหน้าที่วางแผนกลยุทธ์ | ลิงก์หลอกทางเว็บไซต์ดาวน์โหลดเพลงละเมิดลิขสิทธิ์ | ตัดสินใจคลิก (ถูกโจมตี) |
| ผู้ให้สัมภาษณ์คนที่ 18 | เพศชาย อายุ 24 ปี อาศัยอยู่จังหวัดกรุงเทพมหานคร การศึกษาระดับปริญญาตรี อาชีพพนักงานบริษัทเอกชน (ร้านค้าปลีก) ตำแหน่ง นักวิเคราะห์พฤติกรรมลูกค้า | Phishing Email ทดสอบในที่ทำงาน (เป็นการสร้างอีเมลฟิชชิ่งในที่ทำงานจากฝ่ายไอทีเพื่อส่งไปยังพนักงาน เพื่อทดสอบว่าพนักงานมีความตระหนักถึงภัยคุกคามมากน้อยเพียงใด) | ตัดสินใจคลิก (ถูกโจมตี) |

### 5.2 การวิเคราะห์ผลสำหรับคำถามการวิจัย

งานวิจัยนี้นำข้อมูลที่ได้จากการสัมภาษณ์เชิงลึกจากผู้ที่เคยมีประสบกับเหตุการณ์การถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมทั้งสิ้น 18 ท่าน มาวิเคราะห์ผลตามกรอบแนวคิดการวิจัยเบื้องต้น และสามารถแยกตามปัจจัยต่างๆ ดังนี้

#### 5.2.1 ความอยากรู้อยากเห็นส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผล

ผู้ให้สัมภาษณ์ที่ได้รับสารสนเทศซึ่งเป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมและถูกโจมตี 9 ท่านได้แสดงให้เห็นว่าความอยากรู้อยากเห็นนั้นส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผล โดยผู้ให้สัมภาษณ์กล่าวถึงความสงสัยและความอยากรู้อยากเห็นในสารสนเทศที่ผู้โจมตีหลอกผู้ให้สัมภาษณ์ โดยสารสนเทศที่ส่งผลให้เกิดความอยากรู้อยากเห็นนั้นจะเป็นข้อมูลที่ผู้ให้สัมภาษณ์สนใจ เช่น ข่าวสาร ดารา ดวง และมีความเกี่ยวข้องกับตนเอง เช่น เรื่องงาน เป็นต้น ทั้งนี้ผู้ให้สัมภาษณ์จะทำการตัดสินใจคลิกอย่างไม่มีเหตุผลและไม่ตระหนักถึงภัยคุกคามเมื่อเกิดความอยากรู้อยากเห็นขึ้น ดังประโยคที่ผู้ให้สัมภาษณ์กล่าวไว้ว่า

> “รู้สึกอยากรู้ เลยกดอย่างเดียวเลย คืออยากรู้ แค่นั้นแหละ (หัวเราะ)”
> “มีความสงสัย อยากรู้อยากเห็นอะไรประมาณนี้ค่ะ ก็เลยคลิกเข้าไป”

**5.2.2 ความกลัวส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผล**

ผู้ให้สัมภาษณ์ที่ได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมและถูกโจมตี 4 ท่านแสดงให้เห็นว่าความกลัวนั้นส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผล โดยผู้ให้สัมภาษณ์กล่าวถึงความตกใจ และความกลัวในสารสนเทศที่ผู้โจมตีหลอกผู้ให้สัมภาษณ์ โดยสารสนเทศที่ส่งผลให้ผู้ให้สัมภาษณ์เกิดความกลัวนั้นจะทำให้รู้สึกกลัวว่าจะเกิดความผิดพลาดและจะเกิดความเสียหาย กลัวว่าจะต้องสูญเสียเงิน เป็นต้น โดยผู้ให้สัมภาษณ์จะทำการตัดสินใจคลิกอย่างไม่มีเหตุผลและไม่ตระหนักถึงภัยคุกคามเมื่อเกิดความกลัวขึ้น ดังประโยคที่ผู้ให้สัมภาษณ์กล่าวไว้ว่า

> “ตกใจค่ะ แล้วก็ขาดสติยั้งคิด เราไม่คิดอะไรแล้ว แล้วก็แบบไม่รู้ว่าจะแก้ยังไงด้วย แล้วก็คลิกไปเลยตามที่เขาให้มา”
> “ที่กดก็เพราะกลัว เรากลัวว่ามันจะมีปัญหาจริงๆ กลัวว่าจะต้องมีปัญหาตามมา”

**5.2.3 ความโลภส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผล**

ผู้ให้สัมภาษณ์ที่ได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมและถูกโจมตี 5 ท่านได้แสดงให้เห็นว่าความโลภนั้นส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผล โดยผู้ให้สัมภาษณ์กล่าวถึงความอยากได้ และความโลภในสิ่งที่ผู้โจมตีนำมาหลอกผู้ให้สัมภาษณ์ โดยสารสนเทศที่ส่งผลให้เกิดความโลภนั้นจะทำให้รู้สึกต้องการบางสิ่งบางอย่างที่ผู้โจมตีนำมาหลอก เช่น เพลง หนังสือ โปรแกรม ซึ่งเป็นเนื้อหาละเมิดลิขสิทธิ์ หรืออยากลุ้นชิงโชครางวัลหลอกว่าได้รับรางวัล เป็นต้น โดยผู้ให้สัมภาษณ์จะทำการตัดสินใจคลิกอย่างไม่มีเหตุผลและไม่ตระหนักถึงภัยคุกคามเมื่อเกิดความโลภขึ้น ดังประโยคที่ผู้ให้สัมภาษณ์กล่าวไว้ว่า

> “ด้วยความที่เราอยากได้หนังสือมากๆ เราก็พยายามที่จะทำทุกวิถีทางให้ได้หนังสือมา”
> “ตอนนั้นคือกดโหลดไปเพราะอยากได้เพลง”

**5.2.4 การตัดสินใจอย่างไม่มีเหตุผลส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม**

สำหรับผู้ให้สัมภาษณ์ที่ได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมและถูกโจมตี 14 ท่านแสดงให้เห็นว่าการตัดสินใจอย่างไม่มีเหตุผลนั้นส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม โดยผู้ให้สัมภาษณ์กล่าวถึงการตัดสินใจโดยไม่คิด ไม่ไตร่ตรอง ไม่รู้ ขาดสติ เป็นต้น โดยเมื่อผู้ให้สัมภาษณ์ตัดสินใจอย่างไม่มีเหตุผลแล้วจะเชื่อและทำตามสิ่งที่ผู้โจมตีต้องการและถูกโจมตีด้วยวิธีการวิศวกรรมสังคมในที่สุด ดังประโยคที่ผู้ให้สัมภาษณ์ กล่าวไว้ว่า

> “ก็ไม่อะ ก็คลิก แล้วก็กรอก ส่ง ไม่ได้คิด เอ๊ะ อะไรต่อ ไม่ได้คิดว่ามันจะหลอก ไม่ได้คิดเลย ไม่มีความคิดอยู่ในหัวว่าเป็นเมลหลอก”
> “ขาดสติยั้งคิด เราไม่คิดอะไรแล้ว แล้วก็แบบไม่รู้ว่าจะแก้ยังไงด้วย แล้วก็คลิกไปเลยตามที่เขาให้มา”

ส่วนผู้ให้สัมภาษณ์ที่ได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมและไม่ถูกโจมตี 4 ท่านกล่าวว่าการที่ผู้ให้สัมภาษณ์รับรู้ภัยคุกคามที่สูงนั้นจะทำให้ตัดสินใจอย่างมีเหตุผลและตรวจสอบให้ดีเสียก่อนจึงไม่ถูกโจมตี ดังประโยคที่ผู้ให้สัมภาษณ์กล่าวไว้ว่า

> “พอเราดูข้อมูลรายละเอียดหลายๆ อย่างแล้วเราก็ตัดสินใจว่าจะไม่เข้า แล้วเราก็รู้ว่าเป็นอีเมลหลอกอะไรแบบนี้ครับ”
> “เป็นเมลมาเราก็คิดว่ามันใช่รึเปล่า แล้วเราก็พยายามดูว่ามันเป็นของจริงไหมด้วยการที่บอก ไม่แน่ใจก็ไปเสิร์ชในกูเกิลว่ามีคนโดนหลอกแบบนี้รึเปล่าเป็นเมลข้อความประมานนี้ ก็ไม่คลิก”

**5.2.5 ประสบการณ์ก่อนหน้าส่งผลต่อการรับรู้ภัยคุกคาม**

ผู้ให้สัมภาษณ์ 17 ท่านกล่าวว่าประสบการณ์ก่อนหน้านั้นส่งผลต่อการรับรู้ภัยคุกคาม เนื่องจากจะตระหนักถึงภัยคุกคาม โดยประสบการณ์ก่อนหน้าของผู้ให้สัมภาษณ์ส่วนใหญ่จะเป็นเรื่องของไวรัส มัลแวร์ มีผู้ให้สัมภาษณ์ส่วนน้อยที่เคยถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมมาก่อน แต่อย่างไรก็ดีผู้ให้สัมภาษณ์แสดงให้เห็นว่าการที่มีประสบการณ์ก่อนหน้านั้นจะทำให้ผู้ให้สัมภาษณ์รู้สึกว่าจะต้องมีความระมัดระวังมากยิ่งขึ้น ดังประโยคที่ผู้ให้สัมภาษณ์กล่าวไว้ว่า

> “เคยตัดสินใจคลิกเมื่อนานมาแล้ว ครั้งที่โดนอะไม่ได้คิด แต่ว่าหลังจากนั้นมาก็คือเวลาเข้าเมลก็จะเช็คก่อนก็จะระวัง ก็รู้แล้วว่าเออมันมีแบบประมาณนี้ แล้วก็ไม่คลิกไง”

แต่ผู้ให้สัมภาษณ์บางท่านกล่าวว่าตนเองไม่ได้ระวังมากเท่าที่ควร โดยมองว่าเป็นเรื่องไกลตัวและผลกระทบไม่ได้ร้ายแรง หรือไม่มีประสบการณ์มาก่อน

**5.2.6 การแจ้งเตือนส่งผลต่อการรับรู้ภัยคุกคาม**

ผู้ให้สัมภาษณ์ 18 ท่านแสดงให้เห็นว่าการแจ้งเตือนนั้นส่งผลต่อการรับรู้ภัยคุกคาม โดยผู้ให้สัมภาษณ์ได้กล่าวถึงการตระหนักและรับรู้ถึงภัยคุกคาม โดยการแจ้งเตือนของผู้ให้สัมภาษณ์จะมาจากเพื่อนและคนรู้จัก ข่าวสารจากสื่อสังคมออนไลน์ ข่าวสารทางการ และจากบริษัท โดยผู้ให้สัมภาษณ์แสดงให้เห็นว่าการได้รับการแจ้งเตือนนั้นทำให้ผู้ให้สัมภาษณ์รับรู้และรู้จักกับภัยคุกคามมากยิ่งขึ้น ดังประโยคที่ผู้ให้สัมภาษณ์กล่าวไว้ว่า

> “พอหลังๆ มีคนมาเตือนหรือว่ามาบอก ก็เริ่มจะรู้บ้างแล้วว่า สมัยนี้ ตอนนี้มีเรื่องภัยคุกคามทางด้านคอมพิวเตอร์มากขึ้น”

แต่ผู้ให้สัมภาษณ์บางท่านกล่าวว่าตนเองไม่ได้สนใจการแจ้งเตือนมากเท่าที่ควร โดยมองว่าเป็นเรื่องไกลตัวและผลกระทบไม่ได้ร้ายแรง

**5.2.7 การรับรู้ภัยคุกคามส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม**

สำหรับผู้ให้สัมภาษณ์ที่ได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมและถูกโจมตี 14 ท่านกล่าวว่าการรับรู้ภัยคุกคามนั้นส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม แต่การรับรู้ภัยคุกคามนั้นมีไม่มากพอที่จะยับยั้งการตัดสินใจอย่างไม่มีเหตุผลได้ โดยการตัดสินใจอย่างไม่มีเหตุผล เช่น การตัดสินใจโดยไม่คิด ไม่ไตร่ตรอง ไม่รู้ ขาดสติ มากกว่าการรับรู้ภัยคุกคาม ทำให้ตัดสินใจเชื่อและทำตามสิ่งที่ผู้โจมตีต้องการและถูกโจมตีด้วยวิธีการวิศวกรรมสังคมในที่สุด นอกจากนี้ยังมีผู้ให้สัมภาษณ์บางส่วนที่กล่าวว่าตนเองไม่ได้สนใจเรื่องของภัยคุกคามเนื่องจากเป็นเรื่องไกลตัวและผลกระทบไม่ได้ร้ายแรง ดังประโยคที่ผู้ให้สัมภาษณ์กล่าวไว้ว่า

> “เหมือนรับรู้นะคะ แต่ก็ไม่ได้ทำให้เหมือนแบบยับยั้งการกดของเรา เหมือนพอถึงเวลานั้นจริงๆ มันกลัวแล้วแบบ เฮ้ย อะไรอะ เออก็กดไป”
>
> “ก็คือรู้ แต่ว่าไม่ได้สนใจเลย เพราะแบบว่า ไม่รู้วิธีที่จะแบบป้องกันชัดเจน หรือมันมีอะไรชัดเจนที่แบบจะส่งผลเสียหายยิ่งใหญ่ขนาดนั้นค่ะ”

ส่วนผู้ให้สัมภาษณ์ที่ได้รับสารสนเทศที่เป็นภัยคุกคามด้วย วิธีการทางวิศวกรรมสังคมและไม่ถูกโจมตี 4 ท่านได้แสดงให้เห็นว่าการรับรู้ภัยคุกคามนั้นส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมเช่นกัน แต่จะเป็นการที่การรับรู้ภัยคุกคามนั้นมีมากเพียงพอที่จะยับยั้งการตัดสินใจอย่างไม่มีเหตุผลได้ ซึ่งจะทำให้ผู้ให้สัมภาษณ์นั้นตัดสินใจอย่างมีเหตุผลและตรวจสอบให้ดีเสียก่อนจึงไม่ถูกโจมตี ดังประโยคที่ผู้ให้สัมภาษณ์กล่าวไว้ว่า

"ส่งผลให้รับรู้ เพราะว่าเมื่อแบบได้รู้ข่าวมาแล้วเราก็จะระวังตัวเองมากขึ้น พยายามไม่กดไม่อะไร แบบเขาเรียกว่าอะไรอะ พยายามไม่ไปกดมัน ระวังตัวเองมากขึ้นนั่นแหละ เพราะไม่อยากโดน"

"ตระหนักมากขึ้นนะครับ ก็จะระวัง ถ้าเกิดช่วงไหนที่มีคนมาเน้นย้ำเป็นพิเศษ ช่วงนั้นก็จะไม่ใช้งานเลย ไม่ใช้งานตัวที่มีความเสี่ยง ที่เราคิดว่ามีความเสี่ยง เราก็จะไม่ใช้ ไม่เข้าไป"

**5.2.8 ลักษณะเฉพาะของสารสนเทศส่งผลต่อความอยากรู้อยากเห็น**

ผู้ให้สัมภาษณ์ 9 ท่านระบุว่าความอยากรู้อยากเห็นส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผล นอกจากนี้ช่องทาง เนื้อหา รูปแบบ และรูปภาพ ซึ่งเป็นลักษณะเฉพาะของสารสนเทศที่ส่งมาจะทำให้เกิดความอยากรู้อยากเห็นด้วยเช่นกัน โดยข้อมูลเหล่านั้นจะมาจากช่องทางที่น่าเชื่อถือ เช่น ส่งมาจากเพื่อน ส่งมาในอีเมลที่ทำงาน หรือมีเนื้อหาและรูปแบบที่น่าสนใจ เช่น เป็นข่าวสาร มีรูปภาพประกอบ เป็นต้น ทำให้ผู้รับสารสนเทศนั้นเกิดความอยากรู้อยากเห็นขึ้น ดังประโยคที่ผู้ให้สัมภาษณ์กล่าวไว้ว่า

"คือเพื่อนแชร์มา เพื่อนส่งมาให้เรา เราก็เลยอยากจะเข้าไปอ่าน ถ้าเกิดทางแชทบ็อกซ์เราก็คือจะคลิก การตัดสินใจอาจจะคลิกได้ง่ายกว่า แชร์ทั่วๆ ไป"

"พอเราเห็นเนื้อหาเราก็อยากรู้ไง เราก็เลือกที่จะ ไหนลองดูซิ"

**5.2.9 ลักษณะเฉพาะของสารสนเทศส่งผลต่อความกลัว**

ผู้ให้สัมภาษณ์ 4 ท่านระบุว่าความกลัวส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผล นอกจากนี้ช่องทาง เนื้อหา รูปแบบ และรูปภาพ ซึ่งเป็นลักษณะเฉพาะของสารสนเทศที่ส่งมาจะทำให้เกิดความกลัวด้วยเช่นกัน โดยข้อมูลเหล่านั้นจะมาจากช่องทางที่น่าเชื่อถือ เช่น เป็นอีเมลที่ส่งมาถึงตนเองโดยตรง หรือมีเนื้อหาที่น่าเชื่อถือ เช่น เป็นการแจ้งปัญหาเพื่อให้ตอบสนองอย่างเร่งด่วน หรือมีรูปแบบที่ดูน่าเชื่อถือ เช่น ปลอมแปลงอีเมลให้เหมือนอีเมลของทางการจริงๆ หรือเหมือนเว็บไซต์ซื้อสินค้าออนไลน์หรือธนาคารต่างๆ มีรูปภาพประกอบ เป็นต้น ซึ่งจะทำให้ผู้รับสารสนเทศนั้นเกิดความกลัวขึ้น ดังประโยคที่ผู้ให้สัมภาษณ์กล่าวไว้ว่า

"เป็นลักษณะของการที่เป็น Apple คือเป็นเอาชื่อบริษัทมาอ้างแล้วก็เหมือนรู้สึกตอนนั้นจะมีรูปแอพขึ้นมาให้ดูแล้วก็มีประโยคเชิญชวน ให้ดูว่าเราซื้อไปแล้วนะ แล้วก็ในราคาที่ค่อนข้างจะสูง ถ้าตีเป็นเงินไทยประมาณห้าพันก็เลยคิดว่าไม่ๆ แบบคือมันเงินจำนวนมาก ก็เลยแบบรู้สึกตกใจ แล้วแพนิค"

"กลัวว่าที่เราทำไปมันผิดอะไรรึเปล่า เกี่ยวกับงาน เหมือนแบบเราทำงานผิดรึเปล่า"

**5.2.10 ลักษณะเฉพาะของสารสนเทศส่งผลต่อความโลภ**

ผู้ให้สัมภาษณ์ 5 ท่านระบุว่าความโลภส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผล นอกจากนี้ช่องทาง เนื้อหา รูปแบบ และรูปภาพ ซึ่งเป็นลักษณะเฉพาะของสารสนเทศที่ส่งมาจะทำให้เกิดความโลภด้วยเช่นกัน โดยข้อมูลเหล่านั้นจะมาจากช่องทางที่น่าเชื่อถือ เช่น เป็นเว็บไซต์ เป็น SMS เป็นอีเมลที่ส่งมาถึงตนเองโดยตรง หรือมีเนื้อหาที่ดึงดูด เช่น สามารถดาวน์โหลดไฟล์ได้ทันที คุณได้รับรางวัลหรือลุ้นรางวัล หรือมีรูปแบบที่ดูน่าสนใจและน่าเชื่อถือ เช่น เว็บไซต์ที่จัดวางหน้าอย่างดี ไม่รก มีรูปภาพประกอบ เป็นต้น ซึ่งจะทำให้ผู้รับสารสนเทศนั้นเกิดความโลภขึ้น ดังประโยคที่ผู้ให้สัมภาษณ์กล่าวไว้ว่า

"คำพูดใน Message มันดูน่าเชื่อถือ มันเหมือนเขาพิมพ์มาเหมือนแบบเราเป็นผู้โชคดีแบบจริงๆ นั่นแหละ"

"มีเรื่องชิงโชค อะไรอย่างเงี้ย แล้วแต่ที่เขาจะเอามาให้เราอยากได้"

จากการวิเคราะห์บทสัมภาษณ์จากผู้ให้สัมภาษณ์ทั้ง 18 ท่าน ทำให้ได้คำตอบคำถามงานวิจัยดังนี้

**คำถามงานวิจัย:** ทำไมและอย่างไรที่ทำให้ผู้ถูกโจมตีนั้นถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม โดยสามารถแบ่งคำตอบนี้ได้เป็น 2 ส่วน คือ

**(1) บุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมในรูปแบบต่าง ๆ และถูกโจมตี**

บุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมทางสังคมในรูปแบบต่าง ๆ และถูกโจมตี มีทั้งสิ้น 14 คน โดยผู้ให้สัมภาษณ์ทั้ง 14 คน เห็นว่าปัจจัยการตัดสินใจอย่างไม่มีเหตุผลนั้นส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม โดยที่ปัจจัยที่จะส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผลนั้นอาจจะมีความแตกต่างกันออกไปได้ตามบุคคล เช่น ผู้ให้สัมภาษณ์จำนวน 8 คนจาก 14 คน เห็นว่าปัจจัยความอยากรู้อยากเห็นส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผล ผู้ให้สัมภาษณ์จำนวน 4 คนจาก 14 คน เห็นว่าปัจจัยความกลัวส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผล และผู้ให้สัมภาษณ์จำนวน 5 คนจาก 14 คน เห็นว่าปัจจัยความโลภส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผล โดยปัจจัยทั้งสามซึ่งได้แก่ ความอยากรู้อยากเห็น ความกลัว ความโลภนั้นเป็นอารมณ์ความรู้สึกที่เป็นพื้นฐานของมนุษย์ที่ล้วนแต่ส่งผลต่อการตัดสินใจ ซึ่งผู้โจมตีจะใช้ลักษณะเฉพาะของสารสนเทศ เช่น ช่องทาง เนื้อหา รูปแบบ และรูปภาพ ที่ถูกสร้างมาเพื่อให้ผู้ถูกโจมตีนั้นเกิดอารมณ์ความรู้สึกอย่างใดอย่างหนึ่งข้างต้นและตัดสินใจอย่างไม่มีเหตุผลจนส่งผลให้ถูกโจมตีได้ โดยสามารถสรุปได้ดังตารางที่ 2

ตารางที่ 2 สาเหตุที่ส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม

| ผู้ให้สัมภาษณ์ | ปัจจัยที่ส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม | | | | |
|---|---|---|---|---|---|
| **ผู้ให้สัมภาษณ์คนที่ 1** | | ความกลัว | - | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |
| **ผู้ให้สัมภาษณ์คนที่ 2** | | - | - | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |
| **ผู้ให้สัมภาษณ์คนที่ 3** | | ความกลัว | - | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |
| **ผู้ให้สัมภาษณ์คนที่ 4** | | ความกลัว | - | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |
| **ผู้ให้สัมภาษณ์คนที่ 5** | | - | ความโลภ | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |
| **ผู้ให้สัมภาษณ์คนที่ 6** | | - | ความโลภ | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |
| **ผู้ให้สัมภาษณ์คนที่ 7** | | - | ความโลภ | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |
| **ผู้ให้สัมภาษณ์คนที่ 8** | | - | - | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |
| **ผู้ให้สัมภาษณ์คนที่ 9** | | ความกลัว | - | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |

ตารางที่ 2 สาเหตุที่ส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม (ต่อ)

| ผู้ให้สัมภาษณ์ | ปัจจัยที่ส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม | | | | |
|---|---|---|---|---|---|
| **ผู้ให้สัมภาษณ์คนที่ 11** | | - | ความโลภ | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |
| **ผู้ให้สัมภาษณ์คนที่ 12** | | - | - | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |
| **ผู้ให้สัมภาษณ์คนที่ 13** | | - | - | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |
| **ผู้ให้สัมภาษณ์คนที่ 17** | | - | ความโลภ | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |
| **ผู้ให้สัมภาษณ์คนที่ 18** | | - | - | การตัดสินใจอย่างไม่มีเหตุผล | ลักษณะเฉพาะของสารสนเทศ |
| **สรุป (%)** | **57** | **29** | **36** | **100** | **100** |

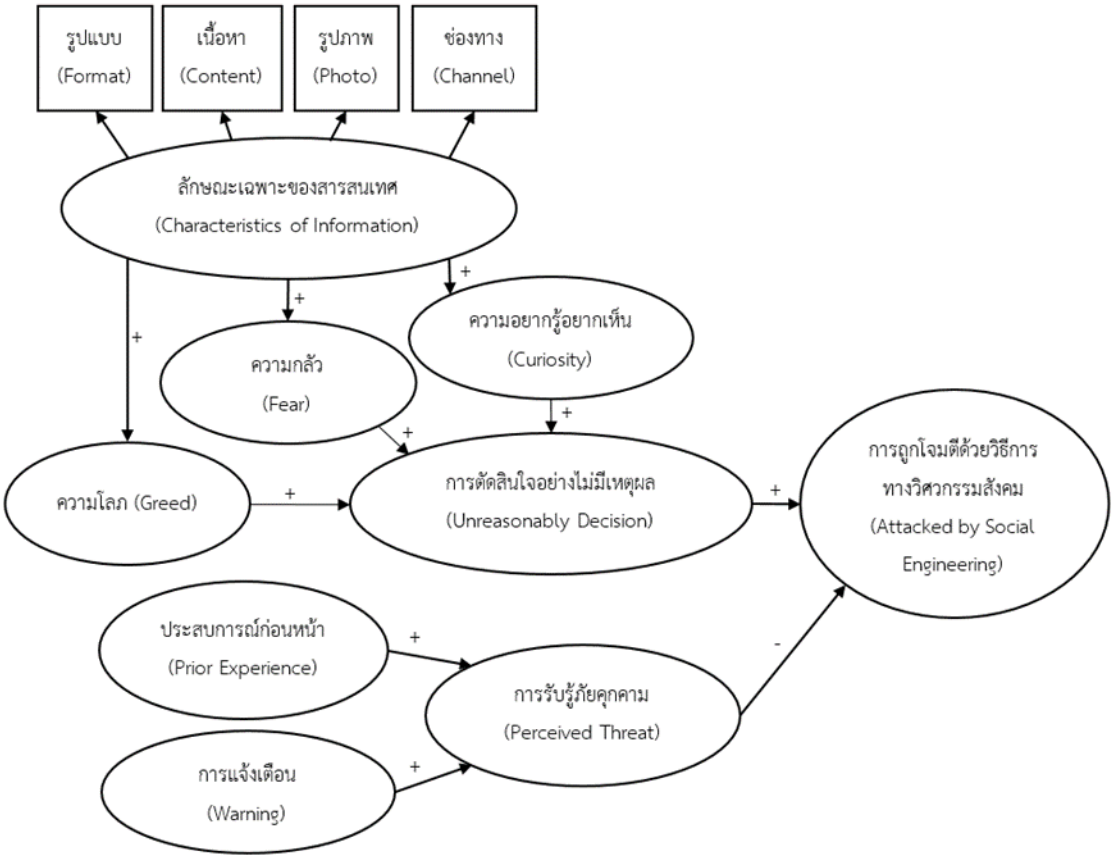
**(2) บุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมในรูปแบบต่าง ๆ แต่ไม่ถูกโจมตี**

บุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมทางสังคมในรูปแบบต่าง ๆ และถูกโจมตีมีทั้งสิ้น 4 คน โดยผู้ให้สัมภาษณ์ทั้งหมดเห็นว่าปัจจัยการรับรู้ภัยคุกคามนั้นส่งผลให้ไม่ถูกโจมตีด้วยวิธีการวิศวกรรมสังคม โดยที่ปัจจัยที่จะส่งผลต่อการรับรู้ภัยคุกคามนั้นจะเกิดขึ้นจากปัจจัยประสบการณ์ก่อนหน้าและการแจ้งเตือน โดยผู้ให้สัมภาษณ์ทั้งหมดเห็นว่าปัจจัยประสบการณ์ก่อนหน้าส่งผลต่อการรับรู้ภัยคุกคาม และผู้ให้สัมภาษณ์ทั้งหมดเห็นว่าการแจ้งเตือนส่งผลต่อการรับรู้ภัยคุกคาม ทั้งนี้การที่บุคคลที่จะมีการรับรู้ภัยคุกคามมากเพียงพอ ที่จะไม่ถูกโจมตีด้วยวิธีการทางวิศวกรรมทางสังคมได้นั้น จะเป็นบุคคลที่มีประสบการณ์ก่อนหน้ามาอย่างชัดเจนในเรื่องการถูกโจมตีด้วยวิธีการทางวิศวกรรมทางสังคมมาก่อนหน้า หรือได้รับการแจ้งเตือนมาอย่างละเอียดถี่ถ้วนมากเพียงพอ

## 6. สรุปผลการวิจัย

### 6.1 อภิปรายผลการวิจัย

ผลการวิจัยสามารถนำมาสร้างกรอบแนวคิดการวิจัยสำหรับสาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม โดยกรอบแนวคิดการวิจัยนี้มีความแตกต่างจากกรอบแนวคิดการวิจัยเบื้องต้นที่สร้างไว้จากการทบทวนวรรณกรรมเล็กน้อย โดยความแตกต่างแสดงในส่วนของลักษณะเฉพาะของสารสนเทศที่จะส่งผลให้เกิดความรู้สึกต่างๆ เช่น ความอยากรู้อยากเห็น ความกลัว หรือความโลภ ก่อนที่จะส่งผลให้เกิดการตัดสินใจอย่างไม่มีเหตุผลและถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม ดังแสดงในภาพที่ 7




ภาพที่ 7 กรอบแนวคิดการวิจัยของสาเหตุเชิงลึกที่ส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม

### 6.2 ข้อเสนอแนะในเชิงปฏิบัติ

งานวิจัยนี้แสดงให้เห็นถึงสาเหตุเชิงลึกที่ส่งผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม โดยสาเหตุหลักจะเกิดจากการตัดสินใจอย่างไม่มีเหตุผล ซึ่งเกิดขึ้นจากอารมณ์และความรู้สึกต่างๆ ประกอบด้วย ความกลัว ความโลภ และความอยากรู้อยากเห็น ข้อมูลจากการสัมภาษณ์แสดงให้เห็นว่าการที่ผู้ถูกโจมตีรับรู้ภัยคุกคามที่ต่ำจะส่งผลให้ถูกโจมตีได้ง่าย แต่หากผู้ถูกโจมตีรับรู้ถึงภัยคุกคามมากขึ้นจากการได้รับการแจ้งเตือนและการมีประสบการณ์ก่อนหน้าจนมากกว่าการตัดสินใจอย่างไม่มีเหตุผล การตัดสินใจจะเปลี่ยนไปและจะไม่ถูกโจมตี ดังนั้นบริษัทเอกชน ภาครัฐ หน่วยงานต่างๆ ควรสร้างการรับรู้ถึงภัยคุกคามทางคอมพิวเตอร์ให้มากยิ่งขึ้น ยกตัวอย่างเช่น การจำลองสถานการณ์ให้บุคลากรในองค์กรได้รับรู้ว่าภัยคุกคามจากการโจมตีด้วยวิธีการทางวิศวกรรมสังคมสามารถเข้ามาจากช่องทางใดบ้าง มีลักษณะอย่างไร และการจัดการกับปัญหาทำอย่างไร โดยการเน้นให้บุคลากรมีส่วนร่วมในการสร้างการรับรู้ภัยคุกคาม ไม่ใช่เพียงกล่าวแจ้งเตือนเพียงอย่างเดียว เนื่องจากไม่สามารถสร้างการรับรู้ภัยคุกคามได้อย่างมีประสิทธิภาพเท่าที่ควร ส่วนการแสดงให้บุคลากรในองค์กรทราบว่าภัยคุกคามสามารถมาจากรูปแบบใดได้บ้าง รวมไปถึงการมีตัวอย่างเหตุการณ์ให้เข้าใจถึงผลกระทบ จะทำให้การถูกโจมตีทางวิศวกรรมสังคมลดลงได้อย่างมีประสิทธิภาพ

### 6.3 ข้อจำกัดของงานวิจัย

จากการที่ผู้วิจัยเปิดรับสมัครผู้เข้าร่วมการวิจัยทางสื่อสังคมออนไลน์รวมถึงโฆษณาประชาสัมพันธ์การเปิดรับสมัครผ่านสื่อสังคมออนไลน์ ทำให้มีผู้ที่เคยได้รับสารสนเทศที่เกี่ยวข้องกับการโจมตีด้วยวิธีการทางวิศวกรรมสังคมสนใจสมัครมาทั้งสิ้น 48 ท่าน เป็นเพศหญิง 29 ท่าน และเป็นเพศชาย 19 ท่าน การที่อัตราส่วนเพศหญิงมากกว่าเพศชายอาจเป็นเพราะเพศชายไม่ต้องการที่จะเปิดเผยข้อมูล ซึ่งเป็นลักษณะนิสัยพื้นฐานของเพศชายที่มักจะไม่ชอบเล่าปัญหาของตนเองให้ผู้อื่นฟัง (Edwards, n.d.; Hsu, 2012) ผู้วิจัยได้คัดเลือกผู้ให้สัมภาษณ์จากคุณสมบัติต่างๆ ที่เหมาะสมกับ

งานวิจัย และสัมภาษณ์ผู้ร่วมวิจัยจำนวนทั้งสิ้น 18 ท่าน เป็นเพศหญิง 14 ท่าน และเพศชาย 4 ท่าน โดยเพศชาย ส่วนใหญ่จะพบเหตุการณ์การได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมแต่ไม่ถูกโจมตี กล่าวคือเพศชายอาจจะมีความรอบคอบมากกว่าเพศหญิง (Edwards, n.d.) ทำให้หาผู้ให้สัมภาษณ์เพศชายที่ถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมได้ยากกว่า ดังนั้นการนำผลการวิจัยไปใช้อาจต้องคำนึงถึงเพศด้วยเช่นกัน

**6.4 ข้อเสนอแนะสำหรับงานวิจัยต่อเนื่อง**

จากสาเหตุของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม สะท้อนให้เห็นว่า อารมณ์และความรู้สึกต่าง ๆ ของผู้ถูกโจมตี ส่งผลให้ผู้ถูกโจมตีตัดสินใจอย่างไม่มีเหตุผลและถูกโจมตีในที่สุด แต่การรับรู้ภัยคุกคามที่สูงนั้นจะสามารถยับยั้งการถูกโจมตีได้ ผู้วิจัยจึงขอเสนอหัวข้อที่น่าสนใจเพื่อเป็นงานวิจัยต่อเนื่อง คือ แนวทางการป้องกันการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม โดยอาจศึกษาลึกลงไปในสาเหตุต่าง ๆ ว่าควรจะสร้างการรับรู้ภัยคุกคามและป้องกันอย่างไรให้ได้ประสิทธิภาพสูงที่สุด

## บรรณานุกรม


นิศา ชูโต. (2545). *การวิจัยเชิงคุณภาพ*. กรุงเทพฯ: บริษัท แม็ทส์ปอยท์ จำกัด.

ปกรณ์ คำกอง. (2555). แนวคิดการตัดสินใจ. ดึงข้อมูลวันที่ 6 กรกฎาคม 2561, สืบค้นจาก https://www.gotoknow.org/posts/284784%5C.

Dijkstra, J. (2018). *Relation between Dispositional Greed and Impulsive Buying Tendency: Role of Cognitive Reflection.* Tilburg: Tilburg press.

Golman, R. & Loewenstein, G. (2016). *An Information-Gap Theory of Feelings about Uncertainty.* Pennsylvania: Academic press.

Kahneman, D. (2011). *Thinking, Fast and Slow.* Toronto: Doubleday Canada.

Michel-Kerjan, E. & Slovic, P. (2010). *The Irrational Economist: Making Decisions in a Dangerous World.* New York: Public Affairs Press.

Rogers, R. W. (1983). *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation.* New York: Guilford.

Ahmed, M. T. & Omotunde, H. (2012). Theories and Strategies of Good Decision Making. International *Journal of Scientific & Technology Research, 1*(10), 51-54.

Arvai, J. L. & Froschauer, A. (2010). Good decisions, bad decisions: the interaction of process and outcome in evaluations of decision quality. *Journal of Risk Research, 13*(7), 845-859.

Junger, M., Montoya, L. & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior, 66*, 75-87.

Krol, K., Moroz, M. & Sasse, M. A. (2012). Don't work. Can't work? Why it's time to rethink security warnings. *Risk and Security of Internet and Systems (CRiSIS), 2012 7th International Conference,* Malaysia, 59-72.

Lee, C., Lee, C. C. & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computer & Security, 59*, 60-70.

Li, R. & Suh, A. (2015). Factors Influencing Information credibility on Social Media Platforms: Evidence from Facebook Pages. *Procedia Computer Science, 72*, 314–328.

Loewenstein, G. (1994). The psychology of curiosity: A review and reinterpretation. *Psychological Bulletin, 116(*1), 75–98.

Machackova, H. & Smahel, D. (2018). The perceived importance of credibility cues for the assessment of the trustworthiness of online information by visitors of health-related websites: The role of individual factors. *Telematics and Informatics, 35*, 1534–1541.

Mileti, D. S. & Sorensen, J. H. (1990). Communication of Emergency Public Warnings – A Social Science Perspective and State-of-the-art Assessment. *Oak Ridge National Laboratory,* 2(4), 166.

Mitrakul, S. & Kongchan, A. (2016). Generation Y in the Workplace: A Study of the Relationship between Value Congruence and Organizational Commitment. *Journal of Management Sciences, 33*, 51-75.

Perry, R. W. & Lindell, M. K., (1990). Predicting long-term adjustment to volcano hazard. *International Journal of Mass Emergencies and Disasters, 8*(2), 177-136.

Potter, S. H., Kreft, P. V., Milojev, P., Noble, C., Montz, B., Dhellemmes, A., Woods, R. J. & Gauden-Ing, S. (2018). The influence of impact-based severe weather warnings on risk perceptions and intended protective actions. *International Journal of Disaster Risk Reduction*, 4(2), 54-72.

Ripberger, J. T., Silva, C. L., Jenkins-Smith, H. C. & James, M. (2014). The influence of consequence-based messages on public responses to tornado warnings. *Bulletin of the American Meteorological Society, 96*(4), 577-590.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology, 91*(1), 93-114.

Rook, D. W. & Gardner, M. P. (1993). In the mood: Impulse buying's affective antecedents. *Research in Consumer Behavior, 6*(7), 1–28.

Safa, N. S., Solms, R. V. & Furnell, S. (2016). Information security policy compliance model in organizations. *Computer & Security, 56*, 20-82.

Seuntjens, T. G., Zeelenberg, M., Van de Ven, N. & Breugelmans, S. M. (2015). Dispositional greed. *Journal of Personality and Social Psychology, 108*(6), 917–933.

Wu, M., Miller, R. C. & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks?. *Proceedings of the SIGCHI conference on human factors in computing systems*, Montreal, Quebec, Canada, 32-54.

Benenson, Z. (2016). One in two users click on links from unknown senders. Retrieved April 18, 2018, from https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders.

Crowe, J. (2018). 10 Must-Know Cybersecurity Statistics for 2018. Retrieved April 18, 2018, from https://blog.barkly.com/2018-cybersecurity-statistics.

Dascalescu, A. (2018). 10+ Critical Corporate Cyber Security Risks – A Data Driven List [Update 2018]. Retrieved April 17, 2018, from https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list.

Edwards, V. (n.d.). 6 Fascinating Gender Differences Between Men and Women in the Workplace. Retrieved October 17, 2018, from https://www.scienceofpeople .com/gender-differences.

Gammons, B. (2017). 6 Must-Know Cybersecurity Statistics for 2017. Retrieved April 17, 2018, from https://blog.barkly.com/cyber-security-statistics-2017.

Hendricks, D. (2017). 3 Ways the Internet Has Changed the World – And Created New Opportunities?. Retrieved April 17, 2018, fromhttps://smallbiztrends.com/2017/07/impact-the-internet-has-on-society.html.

Hsu, C. (2012). Scientists Reveal Why Most Men Refuse to Ask for Directions Even When They're Lost. Retrieved October 17, 2018, from https://www.medical daily.com/scientists-reveal-why-most-men-refuse-ask-directions-even-when-theyre-lost-242596.

Institute of Information Security. (2014). Phishing & Social Media Phishing. Retrieved April 17, 2018, from http://iisecurity.in/blog/phishing-social-media-phishing.

John, G. (2017). Internet User Growth Over the Next Five Years. Retrieved April 17, 2018, from https://www.huffingtonpost.com/john-garrity/internet-user-growth-over_b_10603196.html.

Mason, J. (2018). Cyber Security Statistics. Retrieved April 17, 2018, from https://thebestvpn.com/cyber-security-statistics-2018.

Sophos. (2016). What is… social engineering?. Retrieved April 17, 2018, from https://news.sophos.com/en-us/2016/08/08/what-is-social-engineering.