หัวข้อวิทยานิพนธ์	สาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม ของกลุ่มเจเนอเรชั่นวาย ในเขตกรุงเทพมหานครและปริมณฑล
ชื่อผู้เขียน	นายพงศ์พนธ์ ภาวศุทธิ์
ชื่อปริญญา	วิทยาศาสตรมหาบัณฑิต (ระบบสารสนเทศเพื่อการจัดการ)
สาขาวิชา/คณะ/มหาวิทยาลัย	ระบบสารสนเทศเพื่อการจัดการ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รองศาสตราจารย์ ดร.นิตยา วงศ์ภินันท์วัฒนา
ปีการศึกษา	2561

บทคัดย่อ

วัตถุประสงค์ของงานวิจัยนี้ เพื่อศึกษาถึงสาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม 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 จะมีปัจจัยที่ส่งผล ได้แก่ การตัดสินใจอย่างไม่มีเหตุผลที่เกิดขึ้นจาก ความอยากรู้อยากเห็น ความกลัว และความโลภ ซึ่งเป็นอารมณ์ความรู้สึกพื้นฐานของมนุษย์ โดยผู้โจมตีจะใช้ลักษณะเฉพาะของสารสนเทศ เช่น ช่องทาง เนื้อหา รูปแบบ และรูปภาพที่สร้างมาเพื่อให้ผู้ถูกโจมตีนั้นเกิดอารมณ์ความรู้สึกอย่างใดอย่างหนึ่งข้างต้นและตัดสินใจอย่างไม่มีเหตุผลจนส่งผลให้ถูกโจมตีได้ ส่วนกรณีที่สองเป็นบุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมในรูปแบบต่าง ๆ แต่ไม่ถูกโจมตี จะมีปัจจัยส่งผล ได้แก่ การรับรู้ภัยคุกคาม ซึ่งเกิดขึ้นมาจาก ประสบการณ์ก่อนหน้า และการแจ้งเตือน โดยเมื่อบุคคลมีการรับรู้ภัยคุกคามมากเพียงพอแล้วจะมีการตัดสินใจที่ใช้เหตุผลไตร่ตรองมากยิ่งขึ้นและไม่ถูกโจมตี

ข้อจำกัดของงานวิจัยนี้คือการที่อัตราส่วนผู้ให้สัมภาษณ์ของเพศหญิงมีมากกว่าเพศชาย โดยเป็นเพศหญิง 14 ท่าน และเพศชาย 4 ท่าน และผลของการวิจัยของผู้ให้สัมภาษณ์เพศชายที่พบว่าเหตุการณ์ส่วนใหญ่จะเป็นการได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคม แต่ไม่ถูกโจมตี ดังนั้นการนำผลการวิจัยนี้ไปใช้อาจต้องคำนึงถึงเรื่องเพศด้วยเช่นกัน ในส่วนของข้อแนะนำสำหรับงานวิจัยต่อเนื่องนั้น เนื่องจากสาเหตุของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมสะท้อนให้เห็นว่า อารมณ์และความรู้สึกต่าง ๆ ส่งผลให้ผู้ถูกโจมตีตัดสินใจอย่างไม่มีเหตุผลและถูกโจมตีในที่สุด แต่การรับรู้ภัยคุกคามที่สูงนั้นจะสามารถยับยั้งการถูกโจมตีได้ จึงควรศึกษาหาแนวทาง การป้องกันการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม โดยอาจศึกษาลึกลงไปในสาเหตุต่าง ๆ ว่าควรจะสร้างการรับรู้ภัยคุกคามและป้องกันอย่างไรให้ได้ประสิทธิภาพสูงที่สุด

คำสำคัญ: วิศวกรรมสังคม, การรักษาความมั่นคงปลอดภัยไซเบอร์, ภัยคุกคามทางคอมพิวเตอร์, การถูกโจมตี

Thesis Title	AN IN-DEPTH STUDY OF THE SOCIAL ENGINEERING ATTACKS OF GENERATION Y IN BANGKOK AND METROPOLITAN
Author	Mr. Pongpon Pawasut
Degree	Master of Science Program (Management Information Systems)
Major Field/Faculty/University	Management Information Systems Commerce and Accountancy Thammasat University
Thesis Advisor	Associate Professor Nitaya Wongpinunwatana, Ph.D.
Academic Years	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