ปัจจัยทางบุคลิกภาพที่มีผลต่อความเสี่ยงในการโจมตีระบบสารสนเทศด้วยวิศวกรรมสังคม

สุทธิรักส์ ศุขเขษม[1*]

[1]สาขาวิชาระบบสารสนเทศ คณะบริหารธุรกิจและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก
[*]sutthirak@cpc.ac.th

บทคัดย่อ

งานวิจัยนี้ได้ศึกษาปัจจัยทางบุคลิกภาพที่มีผลต่อการโจมตีระบบสารสนเทศด้วยวิศวกรรมสังคม (Social Engineering) โดยทำการศึกษาความสัมพันธ์ของบุคลิกภาพ 4 ด้าน ตามแบบทดสอบ MBTI ได้แก่ บุคลิกใช้ความคิด (Thinking) กับบุคลิกใช้ความรู้สึก (Feeling) บุคลิกตัดสิน (Judging) กับบุคลิกรับรู้ (Perceiving) บุคลิกแสดงตัว (Extroversion) กับบุคลิกเก็บตัว (Introversion) และบุคลิกใช้ประสาทสัมผัส (Sensing) กับบุคลิกหยั่งรู้ (Intuition) รวมถึงปัจจัยด้านเพศและการทำงานด้านเทคโนโลยีสารสนเทศ พิจารณากับปัจจัยที่ผู้โจมตีใช้หลักทางจิตวิทยาในการชักจูงผู้ใช้ให้กระทำการให้เกิดความเสียหายแก่ระบบสารสนเทศหรือวิศวกรรมสังคม (Social Engineering) 3 ด้านได้แก่ ความอยากรู้อยากเห็น (Curiosity) ความกลัว (Fear) และความโลภ (Greedy) มีผู้ตอบแบบสอบถามจากทั้ง 4 วิทยาเขต จำนวน 53 คน เป็นเพศชายจำนวน 24 คน เพศหญิงจำนวน 29 คน เป็นคนที่ทำงานทางด้านเทคโนโลยีสารสนเทศ 21 คน และไม่ได้ทำงานด้านเทคโนโลยีสารสนเทศ 32 คน บุคลิกใช้ความคิด จำนวน 32 คน บุคลิกใช้ความรู้สึก จำนวน 21 คน บุคลิกตัดสิน จำนวน 21 คน บุคลิกรับรู้ จำนวน 32 คน บุคลิกแสดงตัว จำนวน 32 คน บุคลิกเก็บตัว จำนวน 21 คน บุคลิกใช้ประสาทสัมผัส จำนวน 24 คน และบุคลิกหยั่งรู้ จำนวน 29 คน จากการวิจัยนี้ได้ข้อสรุปว่าผู้ใช้ที่มีบุคลิกตัดสินมีโอกาสที่จะถูกชักจูงด้วยวิศวกรรมสังคมจากความอยากรู้อยากเห็นมากกว่าบุคลิกรับรู้ และผู้ใช้ที่มีบุคลิกตัดสินมีโอกาสที่จะถูกชักจูงด้วยวิศวกรรมสังคมจากความกลัวมากกว่าบุคลิกรับรู้ บุคลิกใช้ความคิดมีโอกาสที่จะถูกชักจูงด้วยวิศวกรรมสังคมจากความกลัวมากกว่าบุคลิกใช้ความรู้สึก เพศชายมีโอกาสที่จะถูกชักจูงด้วยวิศวกรรมสังคมจากความโลภมากกว่าเพศหญิง คนทำงานทางด้านเทคโนโลยีสารสนเทศมีโอกาสที่จะถูกชักจูงด้วยวิศวกรรมทางสังคมจากความกลัวน้อยกว่าคนที่ไม่ได้ทำงานด้านเทคโนโลยีสารสนเทศ อย่างมีนัยสำคัญ จากผลการวิจัยองค์กรสามารถจัดการอบรมทางด้านการรักษาความปลอดภัยของระบบสารสนเทศโดยเน้นที่กลุ่มคนเหล่านี้มากเป็นพิเศษ เพื่อสร้างประสบการณ์และความตระหนักรู้ในด้านความปลอดภัยของระบบสารสนเทศ จะได้รู้เท่าทันการใช้วิศวกรรมสังคมและไม่ถูกโจมตีโดยผู้ประสงค์ร้าย

คำสำคัญ: บุคลิกภาพ ความปลอดภัยของระบบสารสนเทศ วิศวกรรมสังคม

Personality Factors to the Risk of Information Systems from Social Engineering Attack

Sutthirak Sookkhasem[1,*]

[1] Department of Information System Faculty of Business Administration and Information Technology
Rajamangala University of Technology Tawan-ok
*sutthirak@cpc.ac.th

Abstract

This research studies the personality factors that affect the information system attack using social engineering. The research has studied the relationship of 4 aspects of personality according to the MBTI test consist of Thinking personality versus Feeling personality, Judging versus Perceiving, Extroversion versus Introversion and Sensing versus Intuition. And has considered in gender factors including to work about information technology. The Researcher consider factors that attackers use psychological principles to persuade users to cause damage to information systems or social engineering in three areas: Curiosity Fear and Greedy. There are 53 respondents from 4 campuses, consisting of 24 males and 29 females, 21 people worked in information technology, 32 did not work in information technology, 32 Thinking personalities ,21 Feeling personalities, 21 Judging personalities, 32 Perceiving personalities, 32 personalities (Extroversion) 32 persons, introverted personality, 21 Introversion personalities, 24 Sensing personalities and 29 Intuition personalities. From this research, I can concluded that users with Judging personalities are more likely to be influenced by social engineering from curiosity than Thinking personality. And users with Judging personalities are more likely to be influenced by social engineering from fear than Perceiving personalities. Thinking personalities are more likely to be influenced by social engineering from fear than Feeling personalities. Males are more likely to be influenced by social engineering than greed than females. Information technology workers are less likely to be influenced by social engineering than people who do not work in information technology. From this research, the researcher has brought the results to develop the curriculum of information system security based on personality factors. According to the research results, the organization is able to provide training on information technology security, with particular emphasis on these groups. The training create experience and awareness in information technology security. Resulting in users being informed of social engineering techniques and not be attacked by malicious attacker.

Keywords: Personality , Information Security , Social Engineering

1. บทนำ

ปัจจุบันหน่วยงานหรือองค์กร ต่างๆไม่ว่าจะเป็นภาครัฐหรือเอกชนมีการนำระบบสารสนเทศเข้ามาใช้งานตั้งแต่ในระดับปฏิบัติงานที่ใช้ในการบันทึกและติดตามการดำเนินการ ไปจนถึงผู้บริหารระดับสูงที่ใช้ในการช่วยสนับสนุนการตัดสินใจในการกำหนดนโยบายในการบริหารงานขององค์กร ทำให้ระบบสารสนเทศมีความสำคัญต่อองค์กรมากขึ้นเรื่อยๆ

เนื่องจากระบบสารสนเทศมีความสำคัญต่อองค์กร ดังนั้นระบบสารสนเทศจึงเป็นเป้าหมายที่สำคัญในการโจมตีจากคู่แข่งหรือผู้ไม่ประสงค์ดี โดยบุคคลหรือกลุ่มบุคคลที่ทำการโจมตีให้เกิดความเสียหายจะอาศัยเทคนิคต่างๆทางคอมพิวเตอร์เพื่อแสวงหาประโยชน์จากความเสียหายของระบบสารสนเทศ ถึงแม้ว่าปัจจุบันจะมีการพัฒนาเครื่องมือในการรักษาความปลอดภัยของระบบสารสนเทศให้มีความก้าวหน้ามากขึ้น แต่ผู้โจมตีก็ยังสามารถเข้ามาทำให้เกิดความเสียหายแก่ระบบสารสนเทศได้ งานวิจัยทางด้านความปลอดภัยของระบบสารสนเทศหลายงานจะบอกตรงกันว่าจุดอ่อนที่สำคัญที่สุดในด้านการรักษาความปลอดภัยของระบบสารสนเทศคือผู้ใช้ (user) โดยผู้ใช้อาจจะรู้เท่าไม่ถึงการณ์ หรือถูกชักจูงให้ทำอะไรบางอย่างที่จะเกิดความเสียหายแก่ระบบสารสนเทศในองค์กร ซึ่งการชักจูงนั้นจะอาศัยเทคนิคทางจิตวิทยาเพื่อจูงใจให้ผู้ใช้ภายในองค์กรทำอะไรบางอย่างที่จะก่อให้เกิดความเสียหายแก่ระบบสารสนเทศ วิธีการจูงใจทางจิตวิทยานี้จะถูกเรียกว่าวิศวกรรมสังคม (Social Engineering)

พงศ์พนธ์ ภาวศุทธิ์ ได้ทำวิจัยในหัวเรื่อง สาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมของกลุ่มเจเนอเรชั่นวาย ในเขตกรุงเทพมหานครและปริมณฑล ได้สรุปว่าผู้โจมตีจะอาศัยการตัดสินใจที่ไม่มีเหตุผลโดยอาศัยความรู้สึกพื้นฐานของมนุษย์ได้แก่ ความอยากรู้อยากเห็น ความกลัว และความโลภ โดยผู้โจมตีจะอาศัยความรู้สึกเหล่านี้เป็นเครื่องมือในการแสวงหาประโยชน์ เช่น เอา Flash Drive ที่มีโปรแกรมประสงค์ร้าย (Malware) ไปทิ้ง เมื่อเป้าหมายเก็บได้ ก็จะอยากรู้ว่ามีข้อมูลอะไรอยู่ภายใน อาจจะเพื่อส่งคือเจ้าของหรือเพื่อเอาไปใช้ประโยชน์เอง เมื่อผู้ใช้เอา Flash Drive ไปเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์ก็จะเป็นการกระตุ้นให้โปรแกรมประสงค์ร้ายทำงาน ทำให้คอมพิวเตอร์เกิดความเสียหาย หรือผู้โจมตีใช้ประโยชน์จากความกลัวด้วยการส่งอีเมล์ที่ดูเหมือนอีเมล์ที่ดูเหมือนส่งจากธนาคารไปให้ลูกค้าของธนาคาร โดยแจ้งว่าธนาคารกำลังจะปรับปรุงระบบฐานข้อมูลลูกค้า ซึ่งการดำเนินการนี้อาจจะทำให้ข้อมูลลูกค้าสูญหายได้ ดังนั้นเพื่อป้องกันไม่ให้ข้อมูลลูกค้าสูญหาย ทางธนาคารจึงขอให้ลูกค้าสำรองข้อมูล โดยกรอกข้อมูลตามลิงค์ที่แนบมากับอีเมล์นี้ เมื่อลูกค้ากลัวว่าข้อมูลจะสูญหายก็จะกดลิงค์แล้วก็จะเห็นเว็บไซต์ที่ดูเหมือนกับเว็บไซต์ของธนาคาร ถ้าลูกค้าเข้าไปกรอกข้อมูลก็จะทำให้ผู้โจมตีได้ข้อมูลสำคัญของลูกค้าแล้วนำไปหาประโยชน์ต่อไปได้ หรือผู้โจมตีใช้ประโยชน์จากความโลภด้วยการให้ผู้ใช้สามารถใช้โปรแกรมบางอย่างได้ฟรีโดยไม่มีค่าใช้จ่าย แต่โปรแกรมนั้นก็จะมีการดักจับข้อมูลสำคัญต่างๆภายในเครื่องของผู้ใช้ เป็นต้น

จากที่กล่าวมาจะเห็นว่าความรู้สึกพื้นฐานของมนุษย์ได้แก่ ความอยากรู้อยากเห็น ความกลัว และความโลภ เป็นเครื่องมือสำคัญที่ผู้โจมตีนำมาใช้ในการหาประโยชน์เพื่อให้ผู้ใช้ทำอะไรบางอย่างให้เกิดความเสียหายแก่ระบบสารสนเทศ แต่ถึงกระนั้นการตอบสนองต่อความอยากรู้อยากเห็น ความกลัว และความโลภของผู้ใช้แต่ละคนจะแตกต่างกันขึ้นอยู่กับพื้นฐานทางบุคลิกภาพและประสบการณ์ของแต่ละคน การทำความเข้าใจเรื่องบุคลิกภาพและประสบการณ์ของแต่ละคน จะช่วยให้องค์กรทำความเข้าใจผู้ใช้และวางแผนในการจัดอบรมเพื่อป้องกันไม่ให้ผู้ใช้ตกเป็นเหยื่อจากวิธีการวิศวกรรมสังคมได้

ปัจจุบันมีแบบทดสอบบุคลิกภาพอยู่หลายแบบ โดยแต่ละแบบก็จะมีการจำแนกประเภทของบุคลิกภาพที่แตกต่างกัน หนึ่งในนั้นคือแบบทดสอบ MBIT (Mayers-Briggs Type Indicator) ซึ่งเป็นแบบทดสอบบุคลิกภาพที่เกี่ยวข้องกับการทำงานในองค์กร เพราะเป็นแบบทดสอบที่นิยมใช้สำหรับแนะนำอาชีพที่เหมาะกับบุคลิกภาพของแต่ละคน ทางผู้วิจัยจึงมีความคิดที่จะนำแบบทดสอบ MBTI มาใช้ในการวัดบุคลิกภาพของผู้ใช้ แล้วนำมาหาความสัมพันธ์กับความรู้สึกพื้นฐานของมนุษย์ได้แก่ ความอยากรู้อยากเห็น ความกลัว และความโลภ เพื่อที่จะได้ทำความเข้าใจว่าบุคลิกภาพในกลุ่มไหนมีความเสี่ยงต่อการใช้ความรู้สึกแบบไหน เพื่อที่จะได้นำไปวางแผนการอบรมและสร้างความตระหนักรู้ต่อการโจมตีด้วยวิศวกรรมสังคม และก่อให้เกิดความปลอดภัยในการใช้งานระบบสารสนเทศ

2. วัตถุประสงค์ของงานวิจัย

2.1 เพื่อศึกษาพฤติกรรมการใช้งานระบบสารสนเทศ โดยจำแนกกลุ่มผู้ใช้ตามแบบทดสอบบุคลิกภาพ MBTI

2.2 เพื่อศึกษาพฤติกรรมของบุคลิกภาพตามแบบทดสอบบุคลิกภาพ MBTI กลุ่มต่างๆว่ามีพฤติกรรมการใช้งานที่เป็นความเสี่ยงต่อการโจมตีวิศวกรรมสังคมประเภทใด

3. เอกสารและงานวิจัยที่เกี่ยวข้อง

จตุชัย แพงจันทร์ (2558) ได้อธิบายถึงการรักษาความมั่นคงของระบบสารสนเทศ เพื่อปกป้องรักษาคุณสมบัติ 3 ด้าน ได้แก่

1. ความลับ (Confidentiality) คือ การทำให้ข้อมูลสามารถเข้าถึงหรือดูได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น ผู้ที่ไม่ได้รับอนุญาตจะไม่สามารถเข้าถึงหรือดูข้อมูลได้ การรักษาความลับของข้อมูลคือการอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ หรือการป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้ โดยกลไกในการรักษาความลับจะอาศัยการเข้ารหัสลับ (Encryption) ซึ่งจะต้องใช้กุญแจ (Key) ในการเข้ารหัสลับ และถอดรหัสลับ (Decryption) นอกจากนั้นและกลไกที่ใช้รักษาความลับอีกประการคือการควบคุมการเข้าถึง (Access Control) โดยจะอาศัยการพิสูจน์ทราบตัวตน (Authentication) เพื่อดูว่าผู้ใช้งานมีสิทธิเข้าถึงข้อมูลหรือไม่ ซึ่งปกติที่นิยมใช้ก็คือการ Login เข้าสู่ระบบ

2. ความถูกต้อง(Integrity) คือการรักษาความคงสภาพของข้อมูลจากแหล่งที่มา หรือไม่ให้ถูกแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต หรือถ้าถูกแก้ไขจะต้องสามารถรู้ได้ว่าถูกแก้ไข ความถูกต้องของข้อมูลประกอบด้วย 2 ส่วนคือ ความถูกต้องของเนื้อหาและความถูกต้องของแหล่งที่มาของข้อมูล

3. ความพร้อมใช้งาน (Availability) คือ การทำให้ผู้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้เมื่อต้องการ ซึ่งระบบสารสนเทศที่ถูกผู้ไม่ประสงค์ดีโจมตีจะทำให้ระบบหยุดการทำงาน ทำให้ไม่สามารถให้บริการตามที่ผู้ใช้ต้องการได้ การจะทำให้ระบบมีความพร้อมในการใช้งานต้องมีการป้องกันผู้ไม่ประสงค์ดีเข้ามาโจมตีระบบ รวมถึงป้องกันโปรแกรมประสงค์ร้ายต่างๆ

Katharina (2015) ได้ศึกษาบทความวิจัยทางด้านวิศวกรรมสังคมแล้วสังเคราะห์จนได้ข้อสรุปเกี่ยววิธีการโจมตีด้วยวิศวกรรมสังคม ช่องทางในการโจมตี และวิธีการดำเนินการ ดังนี้

วิธีการในการโจมตี แบ่งได้ 5 ประเภท ได้แก่

1. วิธีการทางทางกายภาพ เป็นการกระทำเพื่อเก็บรวบรวมข้อมูลของเหยื่อในอนาคต เช่น การค้นข้อมูลจากถังขยะ (Dumpster Diving)
2. วิธีการทางสังคม เป็นวิธีการที่ประสบความสำเร็จอย่างมากในการทำวิศวกรรมสังคม โดยสร้างความสัมพันธ์กับเหยื่อด้วยการให้เชื่อว่าเป็นกลุ่มสังคมเดียวกันจนทำให้เหยื่อเกิดความเชื่อใจ
3. วิศวกรรมย้อนรอยทางสังคม (Reverse Social Engineering) เป็นแนวทางที่ผู้โจมตีไม่ได้เข้าไปหาเหยื่อโดยตรง แต่จะทำให้เหยื่อเกิดปัญหาอะไรบางอย่าง แล้วทำตัวให้เหยื่อเชื่อว่าตัวเองจะแก้ปัยหาให้เหยื่อได้ เช่น ทำให้คอมพิวเตอร์ในองค์กรไม่สามารถใช้อินเตอร์เน็ตได้ แล้วหาหน้าม้ามาแนะนำว่าผู้โจมตีเป็นผู้เชี่ยวชาญที่สามารถแก้ปัญหานี้ได้
4. วิธีการทางเทคนิค โดยทั่วไปจะทำผ่านอินเตอร์เน็ต เช่นผู้ใช้ไม่ได้ระวังในการเปิดเผยข้อมูลส่วนตัว และมีการนำข้อมูลส่วนตัวเหล่านั้นมาใช้เป็นรหัสผ่านในการเข้าสู้ระบบต่างๆ ซึ่งทำให้ผู้โจมตีสามารถเดารหัสผ่านแล้วเข้าสู่ระบบได้โดยง่าย

5. วิธีการทางสังคมและเทคนิค เป็นวิธีการที่อาศัยทั้งวิธีการทางสังคมและทางเทคนิค เช่น การทำ Flash Drive ตกแล้วให้เหยื่อมาเก็บไป โดยที่ผ่านใน Flash Drive มีการติดตั้งโปรแกรมประสงค์ร้ายเอาไว้

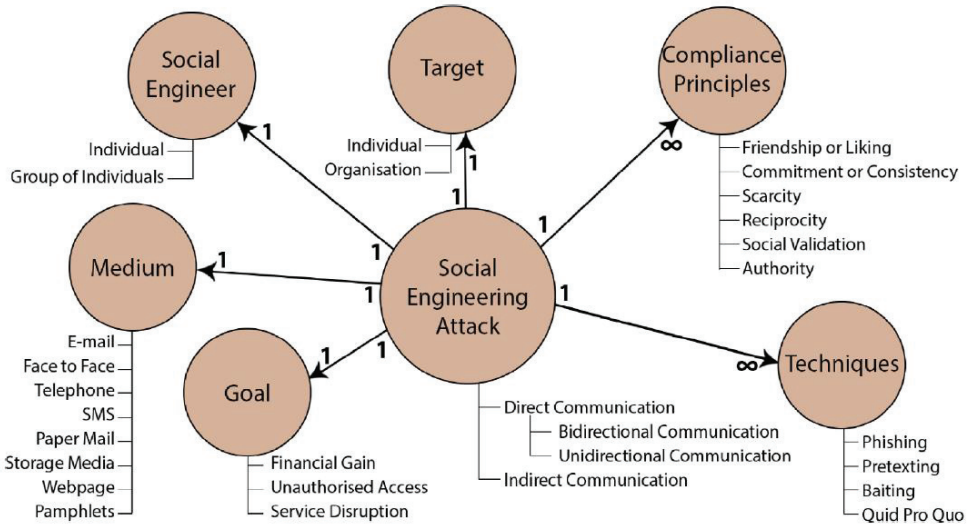
ช่องทางในการโจมตี ได้แก่

1. อีเมล์ เป็นช่องทางที่ถูกใช้มากที่สุดสำหรับการทำฟิชชิ่ง (Phishing) และวิศวกรรมย้อนรอยทางสังคม
2. ระบบส่งข้อความทันที (Instant Massager) เป็นช่องทางที่ได้รับความนิยมในการทำฟิชชิ่ง (Phishing) และวิศวกรรมย้อนรอยทางสังคมเช่นกัน เป็นสิ่งที่ถูกนำไปใช้ในการขโมยอัตลักษณ์ (Identity Theft) ด้วยวิธีการง่ายๆ
3. โทรศัพท์ เป็นช่องทางที่พื้นฐานที่สุดในการส่งข้อมูลที่ความอ่อนไหว (Sensitive)
4. เครือข่ายสังคม เป็นอีกช่องทางหนึ่งที่ถูกนำมาใช้ เพราะสามารถปลอมอัตลักษณ์ (Fake Identity) ได้ง่าย
5. การให้บริการกลุ่มเมฆ (Cloud) จะอาศัยการแบ่งปันไฟล์ของผู้ใช้ในการทำงานร่วมกัน ซึ่งผู้ใช้อาจจะขาดการตระหนักรู้ในเรื่องความปลอดภัย
6. เว็บไซต์ เป็นการสร้างเว็บไซต์ที่การฝังสคริปต์บางอย่างที่เป็นอันตรายถ้าผู้ใช้เข้าไปเยี่ยมชม

การดำเนินการ อาศัย 2 อย่าง ได้แก่

1. ผู้คน เป็นการดำเนินการโดยอาศัยคนดำเนินการโดยตรง จะเป็นวิธีการที่มีความสามารถต่ำกว่าการใช้ซอฟต์แวร์
2. ซอฟต์แวร์ เป็นการดำเนินการโดยอาศัยซอฟต์แวร์โดยตรง เช่น Spear Phishing จะมีการทำเหมืองข้อมูลเพื่อวิเคราะห์ข้อมูลของเป้าหมาย แล้วมีการส่งเว็บปลอมผ่านทางอีเมล์

Francois (2016) ได้ศึกษาบทความวิจัยทางด้านวิศวกรรมสังคมแล้วสังเคราะห์แล้วนำเสนอกรอบงานของการโจมตีด้วยวิศวกรรมสังคม ซึ่งสามารถสรุปประเด็นที่เกี่ยวข้องกับการโจมตีด้วยวิศวกรรมสังคม ได้แก่ วิธีการวิศวกรรมสังคม เป้าหมาย หลักการที่ทำให้เกิดการยอมทำตาม เทคนิคในการทำวิศวกรรมสังคม สื่อกลางในการทำวิศวกรรมสังคม แล้วเป้าหมายในการกระทำ



รูปที่ 1 กลไกการโจมตีด้วยวิศวกรรมสังคม

ที่มา: Social engineering attack examples, templates and scenarios

มนัสนันท์ หัตถศักดิ์ และ ศุภชัย อิทธิปาทานันท์ (2545) ศึกษาเชิงบรรยายมีวัตถุประสงค์เพื่อศึกษาบุคลิกภาพของนักศึกษามหาวิทยาลัยกรุงเทพ ตามแบบวัดบุคลิกภาพของไมเยอร์ บริกจ์(MBTI) และเปรียบเทียบแบบของบุคลิกภาพของนักศึกษามหาวิทยาลัยกรุงเทพ โดยจำแนก คณะ และเพศ โดยมีตัวอย่างทั้งหมด 815 คน จากนักศึกษาคณะมนุษยศาสตร์

บริหารธุรกิจ และนิติศาสตร์ ภาคการศึกษาที่1 ปีการศึกษา 2545 ซึ่งได้จากการสุ่มตัวอย่างอย่างง่าย เครื่องมือที่ใช้ในการทำวิจัยเป็นแบบวัดบุคลิกภาพของไมเยอร์ บริกจ์ ฟอร์ม จี(MBTI Form G) การวิเคราะห์ข้อมูลใช้ โปรแกรมสำเร็จรูป SPSS ในการคำนวณค่าร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน วิเคราะห์ความแตกต่างโดยใช้ค่าที(t-test) วิเคราะห์ความแปรปรวนทางเดียว ANOVA

ผลการวิจัยสามารถสรุปได้ว่า

1. นักศึกษามหาวิทยาลัยกรุงเทพมีบุคลิกภาพตามแบบทดสอบ MBTI ในแบบ ESTJ มากที่สุด

2. นักศึกษาหญิงกับนักศึกษาชายมีบุคลิกภาพตามแบบทดสอบ MBTI ต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01

3. นักศึกษาที่มีคณะต่างกันมีบุคลิกภาพตามแบบทดสอบ MBTI แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

Sherly (2010) ได้ทำการสังเคราะห์บทความวิจัยจากวารสาร Virus Bulletin เกี่ยวกับโปรแกรมประสงค์ร้ายซึ่งถูกทำให้แพร่กระจายด้วยวิศวกรรมสังคม โดยให้ข้อสรุปไว้ว่าเครื่องมือที่ถูกใช้เพื่อทำวิศวกรรมสังคมมากที่สุดคืออีเมล์ รองลงมาคือเว็บไซต์ โปรแกรมเครือข่ายสังคม และอุปกรณ์จัดเก็บข้อมูลเคลื่อนที่ ตามลำดับ โดยการโจมตีจะอาศัยพื้นฐานทางจิตวิทยา 3 ประการได้แก่ความอยากรู้อยากเห็น ความกล้ว และความโลภ เป้าหมายในการโจมตี ได้แก่ นักศึกษาในมหาวิทยาลัย ผู้บริหารองค์กร องค์กรทางศาสนา

พงศ์พนธ์ (2562) ได้ทำการศึกษาสาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมของกลุ่มเจเนอเรชั่นวาย ในเขตกรุงเทพมหานครและปริมณฑล โดยสัมภาษณ์เชิงลึกผู้ที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามจำนวน 18 คน พบว่าสาเหตุที่ส่งผลต่อการถูกโจมตีด้วยวิธีการวิศวกรรมทางสังคมนั้นสามารถแบ่งได้เป็น 2 กรณีคือ กรณีที่หนุ่งเป็นบุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมและถูกโจมตี โดยมีปัจจัยที่ส่งผลต่อการตัดสินใจอย่างไม่มีเหตุผลคือความอยากรู้อยากเห็น ความกลัวและความโลภ ส่วนกรณีที่สองเป็นบุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมในรูปแบบต่าง ๆ แต่ไม่ถูกโจมตี มีสาเหตุมาจากการรับรู้ภัยคุกคามซึ่งเกิดขึ้นมาจาก ประสบการณ์ก่อนหน้าและการแจ้งเตือน มีการรับรู้ภัยคุกคามมากเพียงพอแล้วจะมีการตัดสินใจที่ใช้เหตุผลไตร่ตรองมากยิ่งขึ้นและไม่ถูกโจมตี

4. วิธีดำเนินการวิจัย

ผู้วิจัยได้ดำเนินการวิจัยดังนี้

4.1 สร้างแบบสอบถาม

ผู้วิจัยได้ใช้แบบสอบถามเพื่อวัดบุคลิกภาพตามแบบทดสอบ MBTI โดยอาศัยแบบทดสอบจากเอกสารประกอบการบรรยายของผู้ช่วยศาสตราจารย์ ดร.มณฑิรา อินจ่าย ภาควิชาสังคมวิทยาและมานุษยวิทยา คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร จากการบรรยายหัวข้อจิตวิทยาการให้คำปรึกษาสำหรับผู้ดูแลนิสิต และสร้างแบบสอบถามเพื่อวัดพฤติกรรมการใช้งานระบบสารสนเทศ รวมทั้งวัดความตระหนักถึงความปลอดภัยในการใช้งานระบบสารสนเทศ โดยอาศัยผู้เชี่ยวชาญด้านความปลอดภัยของระบบสารสนเทศเป็นผู้ออกแบบสอบถาม

การสร้างแบบสอบถามเพื่อประเมินความเสี่ยงผู้วิจัยอาศัยพื้นฐานแนวคิดจากงานวิจัยของพงศ์พนธ์ ภาวศุทธิ์ เรื่อง สาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม ของกลุ่มเจเนอเรชั่นวาย ในเขตกรุงเทพมหานครและปริมณฑล โดยงานวิจัยได้ระบุถึงการตัดสินใจอย่างไม่มีเหตุผลเกิดขึ้นจากความอยากรู้อยากเห็น ความกลัว และโลภ ถ้าผู้ถูกโจมตีมีความรู้มากพอจะไม่ถูกโจมตี และงานวิจัยระบุว่าตัวอย่างในงานวิจัยมีสัดส่วนของเพศหญิงมากกว่าเพศชาย จึงเป็นสาเหตุให้ผู้วิจัยพิจารณาประเด็นด้านการทำงานทางด้านเทคโนโลยีสารสนเทศกับประเด็นเรื่องเพศเพิ่มเติมจากบุคลิกภาพ 4 ด้านตามแบบทดสอบ MBTI

แบบสอบถามพิจารณา 6 ประเด็นได้แก่

1. บุคลิกใช้ความคิด (Thinking) กับบุคลิกใช้ความรู้สึก (Feeling)
2. บุคลิกตัดสิน (Judging) กับบุคลิกรับรู้ (Perceiving)
3. บุคลิกแสดงตัว (Extroversion) กับบุคลิกเก็บตัว (Introversion)
4. บุคลิกใช้ประสาทสัมผัส (Sensing) กับบุคลิกหยั่งรู้ (Intuition)
5. การทำงานด้านเทคโนโลยีสารสนเทศ (IT) กับการไม่ได้ทำงานด้านเทคโนโลยีสารสนเทศ (Non – IT)
6. เพศชายกับเพศหญิง

โดยพิจารณา 6 ประเด็นนี้กับอารมณ์พื้นฐาน 3 ประการ ได้แก่ ความอยากรู้อยากเห็น ความกลัว และความโลภ ว่าประเด็นทั้ง 6 มีความสัมพันธ์กับอารมณ์พื้นฐาน 3 ประการอย่างไร

ผู้วิจัยได้นำเสนอแบบสอบถามให้แก่ผู้เชี่ยวชาญด้านความปลอดภัยของระบบสารสนเทศจำนวน 6 ท่าน โดยผู้เชี่ยวชาญทั้ง 6 ท่านได้อ่านแบบสอบถาม ให้คำแนะนำซึ่งนำไปสู่การปรับปรุง แล้วนำไปใช้จริง ตัวอย่างคำถาม เช่น เมื่อเก็บ flash drive ได้ท่านจะพยายามหาทางส่งคืนเจ้าของ , ท่านมีความกังวลเมื่อมี pop up ขึ้นมาว่าเครื่องคอมพิวเตอร์ของท่านมีความเสี่ยงที่จะติดไวรัส และ ท่านยอมให้ข้อมูลบางส่วนเพื่อให้ได้ของฟรีหรือของลดราคา

4.2 เผยแพร่แบบสอบถามทั้งด้านบุคลิกภาพและแบบประเมินความเสี่ยง

ผู้วิจัยดำเนินการทดสอบบุคลิกภาพบุคลากรของราชมงคลตะวันออกทั้ง 4 วิทยาเขต โดยใช้แบบทดสอบบุคลิกภาพและสอบถามพฤติกรรมการใช้งานระบบสารสนเทศตามที่ได้สร้างแบบทดสอบเอาไว้ ซึ่งเป็นการเลือกกลุ่มตัวอย่างแบบสุ่ม

4.3 วิเคราะห์ผลการตอบแบบสอบถาม

วิเคราะห์ความสัมพันธ์ระหว่างบุคลิกภาพประเภทต่างๆกับความเสี่ยงในการใช้งานระบบสารสนเทศโดยการเขียนโปรแกรมด้วยภาษ Python เพื่อวิเคราะห์ข้อมูลทางสถิติ โดยใช้โปรแกรม Winpython เป็นเครื่องมือในการเขียนโปรแกรมเพื่อวิเคราะห์ข้อมูล

4.4 สรุปผลการวิเคราะห์ข้อมูล

ผู้วิจัยได้ทำการวิเคราะห์ทางสถิติเพื่อพิจารณาความแตกต่างของ 6 ประเด็นที่พิจารณากับอารมณ์พื้นฐาน 3 ประการว่ามีความแตกต่างกันอย่างมีนัยสำคัญหรือไม่

5. ผลการวิจัย

จากการส่งแบบสอบถามผ่านสื่อเครือข่ายสังคมของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก มีผู้ตอบแบบสอบถามทั้งหมด 53 คน เป็นเพศชายจำนวน 24 คน เพศหญิงจำนวน 29 คน เป็นคนที่ทำงานทางด้านเทคโนโลยีสารสนเทศ 21 คน และไม่ได้ทำงานด้านเทคโนโลยีสารสนเทศ 32 คน บุคลิกใช้ความคิด จำนวน 32 คน บุคลิกใช้ความรู้สึก จำนวน 21 คน บุคลิกตัดสิน จำนวน 21 คน บุคลิกรับรู้ จำนวน 32 คน บุคลิกแสดงตัว จำนวน 32 คน บุคลิกเก็บตัว จำนวน 21 คน บุคลิกใช้ประสาทสัมผัส จำนวน 24 คน และบุคลิกหยั่งรู้ จำนวน 29 คน เพื่อพิจารณาความแตกต่างของ 6 ประเด็นที่พิจารณา ได้แก่ บุคลิกใช้ความคิด (Thinking) กับบุคลิกใช้ความรู้สึก (Feeling) , บุคลิกตัดสิน (Judging) กับบุคลิกรับรู้ (Perceiving) , บุคลิกแสดงตัว (Extroversion) กับบุคลิกเก็บตัว (Introversion) , บุคลิกใช้ประสาทสัมผัส (Sensing) กับบุคลิกหยั่งรู้ (Intuition) , การทำงานทางด้านเทคโนโลยีสารสนเทศกับไม่ได้ทำงานด้านเทคโนโลยีสารสนเทศ และเพศชายกับ

เพศหญิง กับอารมณ์พื้นฐาน 3 ประการได้แก่ ความอยากรู้อยากเห็น ความกลัว และความโลภ ว่ามีความแตกต่างกันอย่างมีนัยสำคัญหรือไม่ ได้ Z Score ตามตารางที่ 1

ตารางที่ 1 Z Score จากผลการทดสอบความแตกต่างระหว่าง 6 ประเด็นที่พิจารณากับอารมณ์พื้นฐาน 3 ประการ

	Male-Female	IT – Non IT	I-E	S-N	J-P	T-F
Curiosity	0.69	0.05	-0.23	1.24	2.25	0.30
Fear	0.05	-1.33	-0.52	0.50	1.65	1.51
Greedy	1.57	-0.01	-0.30	-1.24	0.23	0.34

จากการทดสอบสมมติฐานทั้งหมดได้ข้อสรุปคือ

1. บุคลิกใช้ความคิด (T) มีความกลัวมากกว่าบุคลิกใช้ความรู้สึก (F) ที่ระดับนัยสำคัญ 0.1
2. เพศชายมีความโลภมากกว่าเพศหญิง ที่ระดับนัยสำคัญ 0.1
3. คนทำงานทางด้านเทคโนโลยีสารสนเทศ (IT) มีความกลัวน้อยกว่าคนที่ไม่ได้ทำงานด้านเทคโนโลยีสารสนเทศ (Non-IT) ที่ระดับนัยสำคัญ 0.1
4. บุคลิกตัดสิน (J) มีความอยากรู้อยากเห็นมากกว่าบุคลิกรับรู้ (P) ที่ระดับนัยสำคัญ 0.05
5. บุคลิกตัดสิน (J) มีความกลัวมากกว่าบุคลิกรับรู้ (P) ที่ระดับนัยสำคัญ 0.10

จากผลการวิเคราะห์นี้สามารถนำไปใช้กับองค์กรในการป้องกันความเสี่ยงจากวิศวกรรมสังคมโดยนำบุคลากรมาทำแบบทดสอบบุคลิกภาพเพื่อหาว่าพนักงานในองค์กรแต่ละคนมีบุคลิกภาพอยู่ในกลุ่มใด ถ้าพบว่าพนักงานมีบุคลิกตัดสิน (ESTJ , ISTJ , ESFJ , ISFJ , ENTJ , INTJ ,ENFJ หรือ INFJ) แสดงว่าพนักงานมีโอกาสจะถูกชักจูงจากวิศวกรรมสังคมโดยอาศัยความอยากรู้อยากเห็นและความกลัวมาก ถ้าพบว่าพนักงานมีบุคลิกใช้ความคิด (ESTJ , ISTJ , ESTP , ISTP , ENTJ , INTJ ,ENTP หรือ INTP) แสดงว่าพนักงานมีโอกาสจะถูกชักจูงจากวิศวกรรมสังคมโดยอาศัยความกลัวมาก โดยเฉพาะอย่างยิ่งพนักงานที่มีบุคลิกภาพที่ผสมกันกันบุคลิกใช้ความคิดและบุคลิกตัดสิน (ESTJ , ISTJ , ENTJ หรือ INTJ) จะยิ่งต้องระวังจากการถูกชักจูงด้วยวิศวกรรมสังคมโดยอาศัยความกลัวเป็นอย่างมาก นอกจากนั้นแล้วพนักงานเพศชายมีโอกาสถูกชักจูงด้วยวิศวกรรมสังคมโดยอาศัยความโลภมาก พนักงานที่ไม่ได้ทำงานด้านเทคโนโลยีสารสนเทศมีโอกาสจะถูกชักจูงจากวิศวกรรมสังคมโดยอาศัยความกลัวมาก ดังนั้นองค์กรจึงควรจัดการอบรมทางด้านการรักษาความปลอดภัยของระบบสารสนเทศโดยเน้นที่กลุ่มคนเหล่านี้มากเป็นพิเศษ เพื่อสร้างประสบการณ์และความตระหนักรู้ในด้านความปลอดภัยของระบบสารสนเทศ จะได้รู้เท่าทันการใช้วิศวกรรมสังคมและไม่ถูกโจมตีโดยผู้ประสงค์ร้าย

6. สรุปผลการวิจัยและข้อเสนอแนะ

จากผลการวิจัยแสดงให้เห็นว่าผู้ใช้บางกลุ่มบุคลิกมีความเสี่ยงจากการชักจูงด้วยวิศวกรรมสังคมมากกว่ากลุ่มอื่นอย่างมีนัยสำคัญ โดยเฉพาะผู้ใช้ที่มีบุคลิกตัดสินจะมีความเสี่ยงจากการชักจูงโดยอาศัยความอยากรู้อยากเห็นและความกลัว ผู้ใช้ที่มีบุคลิกใช้ความคิด จะมีความเสี่ยงจากการชักจูงโดยอาศัยความกลัว นอกจากนั้นแล้วปัจจัยเรื่องเพศและการทำงานก็มีผลต่อการชักจูงด้วยวิศวกรรมสังคมด้วยเช่นกันโดยผู้ใช้เพศชายจะมีความเสี่ยงจากการชักจูงโดยอาศัยความโลภ และผู้ใช้ที่ไม่ได้ทำงานทางด้านเทคโนโลยีสารสนเทศจะมีความเสี่ยงจากการชักจูงโดยอาศัยความกลัว

ถึงแม้ว่าบุคลิกภาพด้านอื่นจะไม่มีผลทางสถิติที่ยืนยันถึงความแตกต่างอย่างชัดเจน แต่บุคลิกภาพบางด้านก็มีคะแนน Z Score ในระดับที่สูงได้แก่ บุคลิกใช้ประสาทสัมผัส (S) กับบุคลิกหยั่งรู้ (I) ในด้านความอยากรู้อยากเห็น และบุคลิกใช้ประสาทสัมผัสกับบุคลิกหยั่งรู้ในด้านความโลภ โดยมีแนวโน้มที่ผู้ใช้ที่มีบุคลิกใช้ประสาทสัมผัสมีโอกาสที่จะถูกชักจูงด้วยวิศวกรรมทางสังคมจากความอยากรู้อยากเห็นมากกว่าบุคลิกหยั่งรู้ และมีแนวโน้มที่ผู้ใช้ที่มีบุคลิกหยั่งรู้มีโอกาสที่จะถูกชักจูง

ด้วยวิศวกรรมทางสังคมจากความโลภมากกว่าผู้ใช้ที่มีบุคลิกใช้ประสาทสัมผัส ซึ่งองค์กรไม่ควรละเลย โดยจัดลำดับความสำคัญให้อยู่ในลำดับรองลงมาจากกลุ่มบุคลิกที่มีผลทางสถิติอย่างมีนัยสำคัญ

ถึงแม้ว่าผู้ใช้กลุ่มบุคลิกอื่นจะไม่มีคะแนน Z Score สูง แต่ทางองค์กรก็ไม่ควรจะละเลยในการให้ความรู้เรื่องความปลอดภัยทางระบบสารสนเทศ โดยจัดลำดับความสำคัญรองลงมาจาก 2 กลุ่มแรก

งานวิจัยนี้ทำการวิเคราะห์โดยใช้สถิติอย่างง่าย ควรที่จะมีการใช้วิธีการเรียนรู้ของเครื่องจักร (Machine Learning) เพื่อหาความรู้เชิงลึก (Insight) จากข้อมูลที่เก็บรวบรวมได้ต่อไปในอนาคต

7. กิตติกรรมประกาศ

งานวิจัยนี้ได้รับทุนอุดหนุนการวิจัยงบประมาณแผ่นดินจากมหาวิทยาลัยราชมงคลตะวันออก ด้านการวิจัยประยุกต์สาขาเทคโนโลยีสารสนเทศและนิเทศศาสตร์โดยมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ได้เห็นความสำคัญของการพัฒนางานวิจัยของบุคลากรเพื่อพัฒนาศักนภาพการวิจัยของบุคลากรของมหาวิทยาลัย

ขอขอบคุณ ท่านอธิการมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออกที่ให้การสนับสนุนให้โครงการวิจัยนี้เกิดขึ้น ท่านผู้อำนวยการสำนักวิจัยและพัฒนาที่ให้ข้อเสนอแนะในการดำเนินการวิจัย และท่านคณบดีคณะบริหารธุรกิจและเทคโนโลยีที่ส่งเสริมและอำนวยความสะดวกต่อการดำเนินการโครงการวิจัยจนงานสำเร็จลุล่วงตามเป้าหมาย

ขอขอบคุณ ดร.ขจรศักดิ์ สังข์เจริญ ดร.ชาลี ธรรมรัตน์ อาจารย์สาโรช หว่างนุ่ม อาจารย์สิทธิศักดิ์ อรรจนานนท์ คุณเชียร เตชะภาณุปรีดา คุณเอกราช แก้วบุญจันทร์ และคุณทัศนัย เหมือนเสน ที่สละเวลาในการตรวจทานแบบสอบถามด้านวิศวกรรมสังคม และประเมินหลักสูตรความปลอดภัยในการใช้งานระบบสารสนเทศบนพื้นฐานปัจจัยทางบุคลิกภาพ

8. เอกสารอ้างอิง

จตุชัย แพงจันทร์. (2558). **Master in Security 3rd Edition**. กรุงเทพมหานคร: ไอดีซี พรีเมียร์.

มนัสนันท์ หัตถศักดิ์ และ ศุภชัย อิทธิปาทานันท์. (2547). การศึกษาบุคลิกภาพของนักศึกษามหาวิทยาลัยกรุงเทพ ตามแบบวัดบุคลิกภาพของไมเยอร์ บริกจ์ (MBTI).**วารสารวิชาการมหาวิทยาลัยกรุงเทพ** ,3 (1), 41-51.

พงศ์พนธ์ ภาวศุทธิ์. (2562). สาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมของกลุ่มเจเนอเรชั่นวาย ในเขตกรุงเทพมหานครและปริมณฑล. **วารสารระบบสารสนเทศด้านธุรกิจ** ,5 (1), 6-25.

Sherly Abraham, InduShobha Chengalur-Smith(2010). An overview of social engineering malware: Trends, tactics,and implications. **Technology in Society** ,32: 183-196.

Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl. (2015). Advanced social engineering attacks. **journal of information security and application** ,22 (6): 113-122.

Francois Mouton, Louise Leenen , H.S. Venter. (2016). Social engineering attack examples, templates and scenarios. **computers & security** ,59, 186-209.