ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร

โดย

นายสุธาเทพ รุณเรศ

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
หลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชานโยบายและการบริหารเทคโนโลยีสารสนเทศ
วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2561

ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร

โดย

นายสุธาเทพ รุณเรศ

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
หลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชานโยบายและการบริหารเทคโนโลยีสารสนเทศ
วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2561

FACTORS AFFECTING AWARENESS OF CYBER-THREATS BY INTERNET USERS IN BANGKOK

BY

MR SUTHATHEP RUNNARES

AN INDEPENDENT STUDY SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE

INFORMATION TECHNOLOGY POLICY AND MANAGEMENT

COLLEGE OF INNOVATION

THAMMASAT UNIVERSITY

ACADEMIC YEAR 2018

มหาวิทยาลัยธรรมศาสตร์
วิทยาลัยนวัตกรรม

การค้นคว้าอิสระ

ของ

นายสุธาเทพ รุณเรศ

เรื่อง

ปัจจัยที่ผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์
ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร

ได้รับการตรวจสอบและอนุมัติ ให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต

เมื่อ วันที่ 15 ธันวาคม พ.ศ. 2561

ประธานกรรมการสอบการค้นคว้าอิสระ _____
(ผู้ช่วยศาสตราจารย์ ดร. สุวรรณ จันทิวาสารกิจ)

กรรมการและอาจารย์ที่ปรึกษาการค้นคว้าอิสระ _____
(ผู้ช่วยศาสตราจารย์ ดร. จิรพล สังข์โพธิ์)

กรรมการสอบการค้นคว้าอิสระ _____
(ดร. มานิต สาธิตสมิตพงษ์)

คณบดี _____
(ผู้ช่วยศาสตราจารย์ ดร. ประวิทย์ เขมะสุนันท์)

หัวข้อการค้นคว้าอิสระ	ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร
ชื่อผู้เขียน	นายสุธาเทพ รุณเรศ
ชื่อปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา/คณะ/มหาวิทยาลัย	นโยบายและการบริหารเทคโนโลยีสารสนเทศ วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาการค้นคว้าอิสระ	ผู้ช่วยศาสตราจารย์ ดร. จิรพล สังข์โพธิ์
ปีการศึกษา	2561

บทคัดย่อ

การวิจัย เรื่อง “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร”การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยทางด้านลักษณะทางประชากร ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ และความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

การวิจัยนี้เป็นการวิจัยเชิงสำรวจ ประชากร คือ ผู้ใช้อินเทอร์เน็ตที่มีอายุ 15 ปีขึ้นไป และอยู่ในเขตกรุงเทพมหานคร ขนาดตัวอย่าง 400 คน ใช้การสุ่มตัวอย่างแบบบังเอิญและแบบสโนว์บอล โดยให้กลุ่มตัวอย่างกรอกแบบสอบถามด้วยตนเองทางออนไลน์

ผลการวิจัยจะช่วยให้หน่วยงานที่เกี่ยวข้องสามารถนำไปใช้ในการวางแผนสร้างความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ให้กับผู้ใช้อินเทอร์เน็ตต่อไป

ผลการวิจัย พบว่า

1. ปัจจัยทางด้านลักษณะทางประชากรด้านอายุ ระดับการศึกษาสูงสุด และรายได้ส่วนตัวต่อเดือน มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต แต่ปัจจัยทางด้านลักษณะทางประชากรด้านเพศ ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

2. ปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

3. ปัจจัยทางด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

ผลการวิจัยจะช่วยให้หน่วยงานที่เกี่ยวข้องสามารถนำไปใช้ในการวางแผนสร้างความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ให้กับผู้ใช้อินเทอร์เน็ตต่อไป

คำสำคัญ : ความปลอดภัยทางไซเบอร์ ภัยคุกคามทางไซเบอร์ ผู้ใช้อินเทอร์เน็ต ความตระหนัก

Independent Study Title	RESEARCH TOPIC: FACTORS AFFECTING AWARENESS OF CYBER-THREATS BY INTERNET USERS IN BANGKOK
Author	Mr. Suthathep Runnares
Degree	Master of Science
Major Field/Faculty/University	IT Policies and Management College of Innovation Thammasat University
Independent Study Advisor	Assistant Professor Jirapon Sunkpho, Ph.D.
Academic Year	2018

ABSTRACT

The objective of the research is to study internet users' demographic profile, experience of cyber-threats, and knowledge about such threats and how they affect their awareness of the issue.

This is a survey research. The population consists of 400 internet users aged 15 years and above living in Bangkok. Accidental sampling is used with a snowball sampling technique in which the samples are asked to answer self-administered questionnaire online.

The findings reveal the following:

1. With regard to the demographic profile, age, highest education level, and personal monthly income affect the internet users' awareness of cyber-threats, while sex has no impact on such awareness.

2. Experience about cyber-threats does not affect the internet users' awareness.

3. Knowledge about cyber-threats affect the internet users' awareness.

The research findings will help and enable agencies concerned to plan how to build awareness about cyber-threats for internet users.

Keywords: cyber-safety, cyber-threats, internet users, awareness

กิตติกรรมประกาศ

ในการจัดทำค้นคว้าอิสระเล่มนี้สามารถสำเร็จลุล่วงไปได้ด้วยดี ทางผู้วิจัยขอขอบคุณความกรุณาที่ปรึกษาจาก ผู้ช่วยศาสตราจารย์ ดร. จิรพล สังข์โพธิ์ เป็นอย่างสูง ณ ที่นี้ ที่ท่านได้ความกรุณา เสียสละเวลาแนะนำแนวทาง ความรู้พร้อมให้คำปรึกษาในการดำเนินการวิจัย

ขอกราบขอบพระคุณประธานกรรมการ ผู้ช่วยศาสตราจารย์ ดร. สุวรรณ จันทิวาสารกิจ และกรรมการสอบค้นคว้าอิสระ ดร.มานิต สาธิตสมิตพงษ์ ที่ให้คำแนะนำกับผู้วิจัยในการปรับปรุงและตรวจสอบช่วยเหลือดำเนินงานวิจัยให้เหมาะสมมากยิ่งขึ้น เพื่อให้ค้นคว้าอิสระ เล่มนี้มีความสมบูรณ์ อีกทั้งขอขอบพระคุณอาจารย์ประจำหลักสูตรทุกท่าน ที่ได้ให้ความรู้ จนทำให้ผู้วิจัยประสบความสำเร็จ

ขอขอบคุณผู้มีส่วนร่วมในการตอบแบบสอบถาม เพื่อให้สามารถนำข้อมูลมาวิเคราะห์ผลสรุปเพื่อให้งานวิจัยนี้ได้เสร็จสมบูรณ์และเพื่อนๆ CIO ในรุ่น 8 ที่เป็นกำลังใจในการทำงานวิจัยและมิตรภาพตลอดระยะเวลาการศึกษาหลักสูตรนี้ที่ได้ร่วมศึกษามาด้วยกันและคอยช่วยเหลือกันเป็นอย่างดี

ขอขอบคุณวิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์ที่ได้ให้โอกาสศึกษาความรู้ที่จะสามารถพัฒนาศักยภาพของนักศึกษา

ขอขอบคุณผู้บริหาร บริษัท เฟรทเวย์ อินเตอร์เนชั่นแนล จำกัด และเจ้าที่ทุกท่านที่ให้การสนับสนุนการพัฒนาความรู้ ความสามารถด้านเทคโนโลยีของผู้วิจัยมาโดยตลอดและผู้ที่ให้การสนับสนุนการศึกษาส่งผลให้การค้นคว้าอิสระนี้สามารถประสบความสำเร็จ

นายสุธาเทพ รุณเรศ

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

ในปัจจุบันที่อินเทอร์เน็ต (Internet) เป็นเสมือนปัจจัยที่ 5 ของการดำเนินชีวิตของมนุษย์ทั่วโลก ไม่เว้นแม้แต่คนไทย ทั้งนี้ผลการสำรวจล่าสุดของ We Are Social (2016) ดิจิทัลเอเจนซี่ชื่อดังของประเทศสิงคโปร์ได้ออกรายงานชื่อ Digital in 2016 ซึ่งมีสถิติเกี่ยวกับพฤติกรรมการใช้อินเทอร์เน็ตของคนไทย พบว่า ในกลุ่มประชากรคนไทยทั้งหมด 68.05 ล้านคนนั้น เป็นผู้ใช้อินเทอร์เน็ตมากกว่าครึ่งหนึ่ง หรือประมาณ 38 ล้านคน โดยทั้งหมดนั้นใช้สื่อสังคมออนไลน์ (Social Media) โดยมีจำนวนหมายเลขโทรศัพท์เคลื่อนที่ซึ่งเปิดใช้งานถึง 82.78 ล้านคนซึ่งมากกว่าจำนวนประชากรทั้งหมด และมีผู้ใช้สื่อสังคมออนไลน์ผ่านโทรศัพท์เคลื่อนที่ถึง 34 ล้านคน ดังแผนภาพ

ภาพที่ 1.1 สถิติเกี่ยวกับพฤติกรรมการใช้อินเทอร์เน็ตของคนไทย. ที่มา MarketingOOPS!, 2561.

เมื่อศึกษาลึกลงไปถึงเวลาในการใช้สื่อต่าง ๆ พบว่า คนไทยใช้อินเทอร์เน็ตผ่านเครื่องคอมพิวเตอร์ตั้งโต๊ะ (PC) หรือแท็บเล็ต (Tablet) ถึงวันละ 4 ชั่วโมง 45 นาที ใช้อินเทอร์เน็ตผ่านโทรศัพท์เคลื่อนที่ถึงวันละ 3 ชั่วโมง 53 นาที ใช้สื่อสังคมออนไลน์ไม่ว่าจะผ่านช่องทางใดถึงวันละ 2 ชั่วโมง 52 นาที ซึ่งมากกว่าการชมโทรทัศน์ที่ใช้วันละ 2 ชั่วโมง 27 นาทีอย่างไรก็ตาม แม้ว่าการใช้อินเทอร์เน็ตและสื่อสังคมออนไลน์จะมีประโยชน์มากมาย แต่ก็สามารถสร้างความเสียหายต่อตนเองและผู้อื่น โดยมาจากพฤติกรรมของผู้ใช้เองหรือการโจมตี การจารกรรมข้อมูลทางคอมพิวเตอร์ของผู้ไม่ประสงค์ดี โดยเป็นอาชญากรรมทางคอมพิวเตอร์ที่เป็นภัยคุกคามทางด้านเทคโนโลยีสารสนเทศได้เช่นกัน ทั้งนี้โดนัลด์ ทรัมป์ ประธานาธิบดีสหรัฐอเมริกาคนปัจจุบันกล่าวว่า “การจารกรรมในโลกออนไลน์เป็นอาชญากรรมที่เติบโตขึ้นอย่างรวดเร็วในสหรัฐอเมริกาตอนนี้” ซึ่งสอดคล้องกับความคิดของสตีฟ มอร์แกน (Steve Morgan) ผู้ก่อตั้ง Cyber Security Ventures (2016) ได้คาดการณ์ถึงแนวโน้มทางสถิติสำหรับความปลอดภัยในโลกออนไลน์ (Cyber Security) ใน 2021 ปี ดังต่อไปนี้ (Morgan, 2016)

- คาดการณ์ว่าในปี ค.ศ. 2021 จะเกิดความเสียหายจากอาชญากรรมคอมพิวเตอร์มากถึง 6 ล้านล้านดอลลาร์ หรือประมาณ 216 ล้านล้านบาทซึ่งเพิ่มขึ้นถึง 100% เมื่อเทียบกับปีที่ผ่านมาที่มีมูลค่าความเสียหายที่ 3 ล้านล้านดอลลาร์

- การลงทุนทางด้านความปลอดภัยในโลกออนไลน์ (Cyber Security) จะใช้เงินจำนวนมากถึง 1 ล้านล้านดอลลาร์จากปี ค.ศ.2017 ถึง 2021 ตามผลสำรวจของการ์เนอร์ (Gartner, 2016) ระบุว่า จากการเติบโตของอาชญากรรมออนไลน์จะเป็นแรงผลักดันให้เกิดการลงทุนด้านความปลอดภัยในโลกออนไลน์ทั้งในธุรกิจผลิตภัณฑ์หรือบริการซึ่งมีมูลค่ามากกว่า 80,000 ล้านดอลลาร์ หรือประมาณ 2.9 ล้านล้านบาท

- ความต้องการบุคลากรความปลอดภัยในโลกออนไลน์ (Cyber Security) จะเพิ่มขึ้นถึง 1.5 ล้านตำแหน่งในปี ค.ศ.2019 และขณะนี้ทั่วโลกกาลังขาดแคลนบุคลากรผู้เชี่ยวชาญด้านนี้

- ในปี ค.ศ. 2020 ที่ทั่วโลกกำลังเข้าสู่ยุคดิจิทัลส่งผลให้มนุษย์กลายเป็นเป้าหมายของอาชญากรทางคอมพิวเตอร์แทนอุปกรณ์ทางคอมพิวเตอร์ โดยบริษัทไมโครซอฟต์ (Microsoft) คาดการณ์ไว้ว่า ในปี ค.ศ.2020 จะมีผู้ใช้บริการในโลกออนไลน์จำนวน 4,000 ล้านคน ซึ่งมากกว่าในปัจจุบันถึง 2 เท่าและกลายเป็นเหยื่อให้แฮ็คเกอร์ (Hacker) เลือกที่จะโจมตีได้

- ในปี ค.ศ. 2020 คาดการณ์ว่าจะมีอุปกรณ์เหล่านี้เป็นจำนวนมากถึง 200,000 ล้านเครื่อง เพิ่มขึ้นจาก 15,000 ล้านเครื่องในปี ค.ศ.2015 ถึง 13 เท่า นั่นหมายความว่า แฮ็คเกอร์มีช่องทางให้เลือกโจมตีมากขึ้นอย่างมหาศาลในอีก 5 ปีข้างหน้า นอกจากนี้ Microsoft และภายในปี ค.ศ. 2020 ปริมาณข้อมูลที่อยู่ในโลกออนไลน์จะเพิ่มขึ้นมากกว่าปัจจุบันถึง 50 เท่า

ปัจจุบันในเครือข่ายอินเทอร์เน็ตและเครือข่ายสื่อสังคมออนไลน์ทั่วโลกและในประเทศไทยพบการกระทำที่เป็นการคุกคามมากมาย เช่น การปลอมอินสตราแกรม ของ หญิง รฐา โพธิ์งาม และแตงโม นิดา พัชรวีระพงษ์ เพื่อนำไปขายสินค้าหรือรับงานโชว์ตัวโดยหลอกผู้เสียหายมากมายถึงพันกว่ารายรวมมูลค่าความเสียหายหลายรายหลายล้านบาท (ไทยรัฐออนไลน์, 2560)

นอกจากนั้นยังมีการขโมยตัวตน (Identity Theft) ซึ่งการขโมยตัวตนในโลกออนไลน์นั้นมักจะทำร่วมกับสิ่งที่ไม่ชอบมาพากลอื่น ๆ เช่น การปลอมแปลงเว็บไซต์เพื่อที่จะหลอกดักข้อมูลชื่อผู้ใช้และรหัสผ่านจากผู้ใช้แล้วนาข้อมูลที่ได้มาปลอมแปลงอีกครั้ง เพื่อนำไปหลอกลวงผู้ใช้งานอื่น ๆ อีกทอดหนึ่งไปจนถึงการทำให้ได้รับความเสื่อมเสียชื่อเสียง อับอาย และเสียทรัพย์สินหรือตกเป็นผู้ต้องสงสัยในคดีอาญา บางกรณีบรรดาแฮกเกอร์ก็ใช้วิธีการคาดเดารหัสผ่านที่มีคาดเดาได้ง่าย ซึ่งก็เป็นอีกวิธีที่ทำให้ผู้ใช้บริการถูกขโมยตัวตนทางออนไลน์ไปใช้แบบไม่รู้ตัว เช่น ตั้งรหัสจากตัวเลข วัน/เดือน/ปีเกิดหรือจะเป็นกรณีการละเลยจากตนเองปล่อยให้มีการเข้าสู่ระบบ (Login) คอมพิวเตอร์ในเว็บไซต์ต่าง ๆ ทิ้งไว้ในร้านคอมพิวเตอร์หรือคอมพิวเตอร์สาธารณะ โทรศัพท์มือถือและเมื่อมีผู้ไม่ประสงค์ดีมาพบข้อมูลของเราก็จะถูกขโมยไปต่อเนื่องไปจนถึงการถูกสวมรอยเพื่อเข้าถึงบัญชีธนาคารหรือการทำธุรกรรมที่ผิดกฎหมาย

ดังนั้นผู้ใช้อินเทอร์เน็ตจึงควรตระหนักถึงภัยคุกคามทางไซเบอร์ เพื่อความมั่นปลอดภัยทางไซเบอร์ ทำให้ผู้วิจัยสนใจศึกษาว่า การตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตเกิดมาจากปัจจัยใดบ้าง เพื่อนำไปใช้ประโยชน์ในการวางแผนเพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ให้กับผู้ใช้อินเทอร์เน็ตต่อไป

1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาปัจจัยทางด้านลักษณะทางประชากรที่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต
2. เพื่อศึกษาปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ที่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต
3. เพื่อศึกษาปัจจัยทางด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

1.3 สมมติฐานการวิจัย

1. ปัจจัยทางด้านลักษณะทางประชากรมีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

2. ปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

3. ปัจจัยทางด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

1.4 ขอบเขตของการวิจัย

การวิจัยนี้ได้กำหนดขอบเขตของการวิจัยไว้ ดังนี้

1. ขอบเขตด้านเวลา : การวิจัยนี้จะเก็บรวบรวมข้อมูลในช่วงเดือนมิถุนายน-กรกฎาคม พ.ศ. 2561

2. ขอบเขตด้านสถานที่/ประชากร : การวิจัยนี้จะศึกษากับผู้ใช้อินเทอร์เน็ตที่มีอายุ 15 ปีขึ้นไปและที่อยู่ในเขตกรุงเทพมหานครเท่านั้น

3. ขอบเขตด้านตัวแปร : การวิจัยนี้มีตัวแปรที่ศึกษา คือ

1) ลักษณะทางประชากร

2) ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

3) ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

4) ความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์

1.5 นิยามศัพท์

ลักษณะทางประชากร หมายถึง เพศ อายุ ระดับการศึกษาสูงสุด และรายได้ส่วนตัวต่อเดือนของผู้ใช้อินเทอร์เน็ต

ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ หมายถึง การเคยประสบกับปัญหาในการใช้งานทางไซเบอร์ ซึ่งเป็นภัยคุกคามที่ส่งผลต่อความปลอดภัยของผู้ใช้งาน

ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ หมายถึง ความสามารถในการทราบได้ว่า การกระทำใดเป็นการกระทำที่ปลอดภัยหรือเป็นการกระทำที่มีความเสี่ยง ซึ่งเป็นภัยคุกคามทางไซเบอร์

ความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ หมายถึง การแสดงออกซึ่งความรู้สึก ความเห็น ความสำนึก เกี่ยวกับลักษณะและผลของภัยคุกคามทางไซเบอร์ใน 6 ด้าน ได้แก่ ด้านความปลอดภัย การยั่วโมโห การข่มขู่ใส่ร้าย การแอบอ้าง การเผยแพร่ออกนอกกลุ่ม และการกีดกัน

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้ได้องค์ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อสามารถนำไปประยุกต์ใช้หรือทำวิจัยในประเด็นที่เกี่ยวข้องต่อไป

2. หน่วยงานที่เกี่ยวข้องสามารถนำผลการวิจัยไปใช้ในการวางแผนสร้างความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ให้กับผู้ใช้อินเทอร์เน็ตต่อไป

บทที่ 2

วรรณกรรมและงานวิจัยที่เกี่ยวข้อง

การวิจัย เรื่อง “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร” นี้ ได้ทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง เพื่อสร้างกรอบแนวคิดของงานวิจัย ดังหัวข้อต่อไปนี้

2.1 แนวคิดและทฤษฎีด้านประชากรศาสตร์
2.2 แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)
2.3 แนวคิดเกี่ยวกับการคุมคามทางไซเบอร์ (Cyber Threat)
2.4 แนวคิดเกี่ยวกับการกลั่นแกล้งทางไซเบอร์ (Cyber Bullying)
2.5 แนวคิดและทฤษฎีเกี่ยวกับความรู้ (Knowledge)
2.6 แนวคิดเกี่ยวกับความตระหนัก (Awareness)
2.7 งานวิจัยที่เกี่ยวข้อง
2.8 กรอบแนวคิดของการวิจัย

2.1 แนวคิดเกี่ยวข้องกับประชากรศาสตร์ (Demography)

มีรากฐานของคำศัพท์ภาษากรีก มาจากคำ ว่า “Demo” หมายถึง “People” ที่แปลว่า ประชากร หรือประชาชน และคำ ว่า “Graphy” หมายถึง “Description” มีความหมายว่า ลักษณะ ซึ่งการนำคำศัพท์ทั้งสองมารวมกันก็จะได้ความหมายว่า วิชาที่เกี่ยวกับประชากร (ชัยวัฒน์ ปัญจพงษ์และณรงค์ เทียนสงค์,2521อ้างถึงใน วศิน สันหกรณ์,2557) นอกจากนี้แนวความคิดด้านประชากรศาสตร์ เป็นทฤษฎีที่เกี่ยวข้องกับหลักการเป็นเหตุเป็นผล ซึ่งเป็นพฤติกรรมของมนุษย์ที่อาจจะเกิดขึ้นจากปัจจัยภายนอก เช่น แรงบังคับจากภายนอกมากระตุ้น และเมื่อกล่าวถึงประชากรที่แตกต่างกันก็จะนำไปสู่พฤติกรรมและการตัดสินใจที่แตกต่างกันไปด้วย (ยุบล เบ็ญจรงค์กิจ, 2542 อ้างถึงใน วศินสันหกรณ์,2557) ส่วนแนวความคิดด้านประชากรศาสตร์นั้น จะสามารถจำแนกประชากรออกเป็นกลุ่มๆได้จากลักษณะ และพฤติกรรม อย่างเช่น กลุ่มคนที่มีลักษณะและบุคลิกใกล้เคียงกันจะอยู่ในกลุ่มเดียวกันรวมไปถึงบุคคลที่อยู่ในชนชั้นทางสังคมเดียวกันก็จะตอบสนองถึงข่าวสารความต้องการ

ไปในทิศทางเดียวกัน และมากไปกว่า นั้น ปัจจัยการเปลี่ยนแปลงของประชากรอาจจะมาจากปัจจัยยังทางเศรษฐกิจ สังคมและวัฒนธรรมอีกด้วย นอกจากนี้แนวความคิดของประชากรศาสตร์สามารถจำแนกและอธิบายถึงคุณสมบัติเฉพาะตนของคนนั้น ๆ ซึ่งมีผลต่อกับการสื่อสารกับผู้รับสารในสถานการณ์ต่างๆ และในการสื่อสารแต่ละครั้งถ้าผู้รับสารมีจำนวนอยู่ก็อาจจะไม่ส่งผลให้เกิดปัญหาได้เพราะเราสามารถวิเคราะห์ผู้รับสารได้ทุกคนแต่ถ้าในทางกลับกัน บางสถานการณ์ผู้รับสารมีจำนวนมากเราจะไม่สามารถวิเคราะห์ผู้รับสารได้อย่างละเอียดถี่ถ้วน ดั้งนั้นการจำแนกผู้รับสารออกเป็นกลุ่มๆ ก็อาจทำ ให้ง่ายต่อการสื่อสารมากขึ้นโดย ซึ่งสามารถจำแนกตามลักษณะประชากร(Demographic Characteristics) ได้ด้วยดังนี้

- เพศ
- อายุ
- การศึกษา
- สถานะทางสังคม
- ศาสนา

ปัจจัยเหล่านี้อาจส่งผลกระทบต่อ การตีความ การรับรู้ ความเข้าใจในการสื่อสาร ข้อมูลด้านประชากรจะมีประสิทธิภาพและเข้าถึงมากที่สุดก็ต่อเมื่อกำหนดกลุ่มเป้าหมายที่ชัดเจน ซึ่งคนที่มีลักษณะทางประชากรต่างกันก็จะมีลักษณะทางจิตวิทยาต่างกัน

2.2 แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช. หรือ NSTDA) ให้ความหมายของ ไซเบอร์ (Cyber) ว่าเป็น คำที่กร่อนมาจากคำว่าไซเบอร์เนติกส์ (Cybernetics) และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต (Internet) และยังมีการให้ความหมาย “สารสนเทศ (Virtual) เสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง” (www.nstda.or.th, 2557)

โดยรวมแล้ว Cyber- จึงเป็นความหมายในเชิงนามธรรม หมายถึง ขอบเขตที่เกี่ยวข้องกับการใช้งานของระบบเครือข่ายคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ ซึ่งจะครอบคลุมมากกว่าคอมพิวเตอร์ ซึ่งมีความหมายในเชิงรูปธรรมของอุปกรณ์ระบบคอมพิวเตอร์ทั่วไป

ตามพจนานุกรม Cyberspace Operations Lexicon ของกระทรวงกลาโหมสหรัฐอเมริกา กำหนดให้ Cyber Security คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความมั่นคงปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ (ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ) ความมั่นคงปลอดภัยของระบบและเครือข่ายที่ใช้

ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูล ทั้งนี้ Cyber Security ยังรวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม อุบัติเหตุ และความผิดพลาดต่าง ๆ (www.enwikipedia.org, 2557)

ความเสี่ยงของ Cyber Security อาจรวมถึงสิ่งต่าง ๆ ที่ทำลายความเชื่อมั่นและความไว้วางใจของผู้มีส่วนได้เสีย (Stakeholder) ผลกระทบที่มีต่อการเก็บรักษาและการเติบโตของกลุ่มลูกค้า การละเมิดการป้องกันข้อมูลส่วนตัวของกลุ่มลูกค้าและผู้ถือหุ้น การรบกวนการทำงานหรือการดำเนินธุรกรรม ผลกระทบที่เป็นปฏิปักษ์ต่อชีวิตและสุขภาพของผู้ปฏิบัติงาน และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ

2.3 แนวคิดเกี่ยวกับการคุกคามทางไซเบอร์ (Cyber Threat)

การคุกคามทางไซเบอร์สามารถเกิดขึ้นได้หลายรูปแบบ แต่ละรูปแบบสามารถสร้างความเสียหายให้แก่บุคคล เศรษฐกิจ ไปจนถึงโครงสร้างพื้นฐานของประเทศต่าง ๆ ภัยคุกคามอาจเป็นการก่อวินาศกรรม การจารกรรมข้อมูลหรือรหัสสำคัญ การปล่อยข้อมูลลวง การทำลายชื่อเสียงของประเทศ องค์กร หรือบุคคล การเผยแพร่ข่าวสารอันเป็นเท็จ รวมถึงการทำลายระบบปฏิบัติการของเซิร์ฟเวอร์ คอมพิวเตอร์ส่วนบุคคล และอุปกรณ์เคลื่อนที่ เช่น แท็บเล็ต หรือโทรศัพท์แบบสมาร์ตโฟน เป็นต้น

2.3.1 ประเภทของการเกิดภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ สามารถแบ่งออกเป็น 5 กลุ่ม ดังนี้

1. ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์

โปรแกรมประยุกต์ (application-based threats) ที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนคอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ อาจจะถูกแอบแฝงมาด้วยโปรแกรมที่เป็นภัยคุกคาม ภัยคุกคามประเภทนี้เรียกว่า มัลแวร์ (malware) ซึ่งเป็นโปรแกรมที่ถูกออกแบบมาเพื่อทำอันตรายต่อข้อมูลในคอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ ทำให้เกิดความขัดข้องหรือเสียหายกับระบบปฏิบัติการ นอกจากนี้โปรแกรมที่ติดมัลแวร์ยังส่งข้อความที่ไม่พึงประสงค์ออกไปยังผู้อื่น หรือขโมยข้อมูลสำคัญออกไป ตัวอย่างโปรแกรมในกลุ่มนี้ ได้แก่ Virus, Worm, Trojan, Botnet หรือ Spyware เป็นต้น

2. ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์

ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ (web-based threats) เป็นภัยคุกคามที่เกิดจากการที่ผู้ใช้คอมพิวเตอร์ หรืออุปกรณ์พกพา เปิดเว็บไซต์ขึ้นมาใช้งาน ซึ่งเว็บไซต์ที่เรียกมาใช้อาจเป็นเว็บไซต์ฟิชชิ่ง (Phishing) ซึ่งถูกออกแบบให้มีลักษณะคล้ายคลึงกับเว็บไซต์จริงเพื่อหลอกให้ผู้ใช้กรอกข้อมูลเข้าสู่ระบบของผู้ไม่หวังดี เช่น หลอกให้ผู้ใช้งานล็อกอินเข้าอีเมล เฟซบุ๊ก หรือเว็บไซต์ที่เกี่ยวข้องกับธุรกรรมทางการเงิน ซึ่งจะคอยดักจับรหัสล็อกอินของผู้ใช้งานนั้น ๆ ทำให้ข้อมูลหรือบัญชีการใช้งานนั้น ๆ มีความเสี่ยงที่จะโดนขโมยข้อมูลออก

3. ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย

ปัจจุบันมีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก มีทั้งที่น่าเชื่อถือและที่ไม่น่าเชื่อถือ รวมถึงผู้ที่แอบแฝงเพื่อวัตถุประสงค์อื่น ดังนั้นผู้ใช้คอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่าง ๆ อาจได้รับผลกระทบโดยตรง รวมถึงยังสามารถเป็นต้นตอของผลกระทบไปยังอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ของผู้อื่นด้วยเช่นกัน โดยผู้ใช้เครือข่ายไร้สายอาจถูกโจมตีด้วยมัลแวร์ผ่านข้อบกพร่องของระบบปฏิบัติการ และถูกเปลี่ยนสถานะมาเป็นผู้โจมตีโดยการส่งต่อหรือแพร่กระจายมัลแวร์เหล่านี้ไปยังอุปกรณ์อื่นผ่านเครือข่ายไร้สาย หรือบลูทูธ นอกจากนี้การใช้เครือข่ายไร้สายยังเปิดโอกาสให้ผู้ไม่ประสงค์ดีดักจับข้อมูลสำคัญ หรือรหัสผ่านบนเครือข่ายไร้สายได้อีกด้วย

4. ภัยคุกคามที่เกิดจากการถูกโจมตีแบบเจาะจงเป้าหมาย

ภัยคุกคามที่เกิดการโจมตีแบบเจาะจงเป้าหมาย (targeted attack) ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตี หรือแฮกเกอร์ (hackers) ในประเทศต่าง ๆ จะใช้การโจมตีแบบเจาะจงเป้าหมายอย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐาน สถาบันการเงิน และองค์กรอื่น ๆ ของภาครัฐ และภาคเอกชนในหลายประเทศ อาชญากรไซเบอร์เหล่านี้จะใช้มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามประเภทนี้จัดว่า เป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

2.3.2 ประเภทของผู้คุกคามทางไซเบอร์

ผู้คุกคามทางไซเบอร์ หรือกลุ่มบุคคลและ/หรือองค์กรที่มีความชำนาญในการปฏิบัติการภัยไซเบอร์สามารถแบ่งออกเป็น 5 กลุ่ม (นงรัตน์ สายเพชร, 2556) ดังนี้

1. ประเทศที่มีความประสงค์ร้าย

กลุ่มนี้ ได้แก่ รัฐบาลของบางประเทศที่มุ่งโจมตีกลุ่มงานความมั่นคงหรือกองทัพ โดยมีจุดมุ่งหมายที่จะสร้างความเสียหายให้เกิดขึ้น กับประเทศเป้าหมาย ซึ่งอาจเป็นการก่อกวนเว็บไซต์

ของหน่วยงานต่าง ๆ การจารกรรมข้อมูลสำคัญ รวมถึงการสร้างความเสียหายให้กับโครงสร้างพื้นฐานของประเทศเป้าหมาย

2. ผู้ก่อการร้าย

กลุ่มนี้ ได้แก่ ผู้ก่อการร้ายหรือผู้ไม่หวังดี ซึ่งมีจุดประสงค์ที่จะทำลายผลประโยชน์ของชาติเป้าหมาย กลุ่มผู้ก่อการร้ายเหล่านี้ใช้ไซเบอร์เป็นช่องทางการสื่อสาร โดยจะสร้างแบบแผนเพื่อหาเงินทุน หรือเพื่อเผยแพร่แนวความคิดที่เป็นภัยต่อประเทศเป้าหมาย

3. สายลับภาคเอกชน/องค์กรอาชญากรรม

กลุ่มนี้ ได้แก่ สายลับภาคเอกชน หรือองค์กรอาชญากรรมซึ่งมีการใช้ไซเบอร์เป็นช่องทางในการบุกรุก และโจมตีระบบ โดยมีเป้าหมายเพื่อจารกรรมข้อมูลสำคัญ รวมถึงทรัพย์สินจากองค์กรภาครัฐ และภาคเอกชนต่าง ๆ กลุ่มนี้อาจเป็นกลุ่มปฏิบัติการของหน่วยงานความมั่นคงของบางประเทศ หรืออาจเป็นเพียงอาชญากรที่ต้องการนำข้อมูลสำคัญไปหารายได้

4. แฮกเกอร์

กลุ่มแฮกเกอร์ (hackers) คือ กลุ่มผู้ที่พยายามหาช่องโหว่ของระบบ ลักลอบเจาะเข้าสู่ระบบเพื่ออ่านข้อมูลข่าวสาร เพื่อขโมย หรือเพื่อทำลายข้อมูลข่าวสารสำคัญเหล่านั้น ซึ่งจะทำให้เกิดความเสียหายแก่องค์กรเป้าหมาย แฮกเกอร์สามารถมาได้จากประเทศต่าง ๆ ทั่วโลก การป้องกัน หรือการสืบหาตัวผู้กระทำความผิดค่อนข้างยาก

5. แฮกทิวิส

กลุ่มแฮกทิวิส (hacktivists) คือ กลุ่มแฮกเกอร์ที่มีแรงจูงใจทางการเมือง เป็นกลุ่มที่ต้องการผลักดันให้เกิดความเปลี่ยนแปลงทางการเมือง กลุ่มนี้มุ่งเน้นที่จะนำเสนอแนวคิดผ่านทางไซเบอร์ และสร้างมูลเหตุที่ส่งผลต่อการเมืองและสังคมมากกว่าการสร้างความเสียหายให้กับโครงสร้างพื้นฐาน

2.3.3 ประเภทของภัยคุกคามทางไซเบอร์

หน่วยงาน The European Computer Security Incident Response Team (eCSIRT)

ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงาน CSIRT ในสหภาพยุโรปได้จำแนกตามประเภทของภัยคุกคามทางไซเบอร์ออกเป็น 10 ประเภท ดังนี้ (ไทยเซิร์ต, “การตรวจจับภัยคุกคามและอาชญากรรมไซเบอร์ในประเทศไทย”, 2556)

1. บอตเน็ต (Botnet) คือ โปรแกรมไม่พึงประสงค์ติดตั้งอยู่ในคอมพิวเตอร์ซึ่งสามารถโจมตีได้โดยอัตโนมัติ หรือรับคำสั่งจากผู้ควบคุมผ่านเครือข่ายอินเทอร์เน็ตได้จากระยะไกล

2. สแปม (Spam) คือ การส่งจดหมายอิเล็กทรอนิกส์ออกไปยังผู้รับจำนวนมากโดยผู้ที่ได้รับจดหมายเหล่านั้น ไม่ได้มีความประสงค์ที่จะได้รับ ส่วนมากเป็นการโฆษณาสินค้าและบริการ

3. โอเพ่นดีเอ็นเอสรีโซลเวอร์ (Open DNS Resolver) คือ การตั้งค่าเครื่องให้บริการดีเอ็นเอส (DNS) อย่างไม่เหมาะสม ทำให้ผู้อื่นสามารถส่งข้อมูลโดเมนเนมหลอกลวงให้กับเครื่องบริการดีเอ็นเอส เพื่อใช้หลอกลวงผู้ใช้งาน

4. บรูตฟอร์ซ (Brute Force) คือ โปรแกรมที่เจาะระบบเป้าหมายด้วยวิธีการสุ่มข้อมูลตาม

อัลกอริทึมที่ผู้โจมตีคิดค้น เพื่อให้ได้ข้อมูลสำคัญหรือข้อมูลลับของระบบเป้าหมาย เช่น บัญชีชื่อผู้ใช้งาน และรหัสผ่าน

5. มัลแวร์ยูอาร์แอล (Malware URL) คือ การที่ผู้ไม่ประสงค์ดีบุกรุกเข้าไปยังเว็บไซต์ของผู้อื่น และใช้พื้นที่ของเว็บไซต์นั้นในการเผยแพร่โปรแกรมไม่พึงประสงค์

6. สแกนนิ่ง (Scanning) คือ การตรวจสอบข้อมูลของบริการของเครื่องแม่ข่ายโดยใช้วิธีส่งข้อมูลไปสู่ระบบที่เป็นเป้าหมาย และรวบรวมข้อมูลที่ได้จากการสแกนนิ่ง เพื่อใช้เป็นข้อมูลในการเจาะระบบ

7. โอเพ่นพร็อกซี่เซิร์ฟเวอร์ (Open Proxy Server) คือ การตั้งค่าบริการเว็บพร็อกซี่ (web proxy) ไม่เหมาะสมที่ยินยอมให้ผู้ใช้งานทั่วไปเรียกใช้งาน เพื่อเข้าถึงบริการเว็บในเครือข่ายอินเทอร์เน็ตได้โดยไม่มีระบบยืนยันตัวตน (authentication)

8. ฟิชชิ่ง (Phishing) คือ เว็บไซต์ปลอมที่ต้องการหลอกลวงเพื่อขโมยข้อมูลสำคัญของผู้ใช้งาน เช่น บัญชีผู้ใช้หรือรหัสผ่าน เป็นต้น

9. สตอร์มเวิร์ม (Storm Worm) คือ โปรแกรมไม่พึงประสงค์ในลักษณะเวิร์ม (Worm) ซึ่งสามารถแพร่กระจายได้ด้วยตัวเอง สตอร์มเวิร์มมีลักษณะการทำงานในรูปแบบบอตเน็ต ต่างกันที่บอตเน็ตทั่วไปมีโครงสร้างการทำงานที่มีเครื่องที่ทำหน้าที่ควบคุม

10. ดีดอส (DDoS) คือ โปรแกรมที่โจมตีสภาพความพร้อมใช้งานของระบบเพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้

2.3.4 ลักษณะและผลของภัยคุกคามทางไซเบอร์

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

1. เนื้อหาที่เป็นภัยคุกคาม (abusive content) เป็นการใช้ข้อมูล หรือเผยแพร่ข้อมูลที่ไม่เป็นจริง หรือไม่เหมาะสม เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อก่อให้เกิดความไม่สงบหรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย การหมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่าง ๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้น ๆ

2. การโจมตีสภาพความพร้อมใช้งานของระบบ (availability) เป็นการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อสร้างความเสียหายให้แก่ระบบให้บริการต่าง ๆ เช่น ทำให้เกิดความล่าช้า จนถึงขั้นที่ระบบไม่สามารถให้บริการต่อไปได้ อาจเป็นการโจมตีระบบโดยตรง เช่น การโจมตีประเภท DoS (Denial of Service) หรือเป็นการโจมตีโครงสร้างพื้นฐาน เช่น การให้บริการระบบไฟฟ้า น้ำประปา หรือระบบโทรศัพท์ เป็นต้น

3. การฉ้อฉล ฉ้อโกง หรือหลอกลวง เพื่อผลประโยชน์ (fraud) เป็นความพยายามที่จะหาผลประโยชน์ด้วยการฉ้อโกง หรือหลอกลวง สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบ หรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาต เพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้า หรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์

4. ความพยายามรวบรวมข้อมูลของระบบ (information gathering) เป็นความพยายามในการรวบรวมข้อมูลระบบของผู้ไม่ประสงค์ดีด้วยการเรียกใช้บริการต่าง ๆ ที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน ชื่ออีเมล รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (sniffing) และการล่อลวงต่างๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ

5. การเจาะระบบได้สำเร็จ (intrusions) เป็นความพยายามที่สามารถเจาะเข้าระบบได้สำเร็จ และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

6. ความพยายามจะบุกรุกเข้าระบบ (intrusion attempts) เป็นความพยายามจะเจาะเข้าระบบผ่านจุดอ่อน หรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (Common Vulnerabilities and Exposures: CVE) หรือผ่านจุดอ่อนหรือช่องโหว่ใหม่ที่ยังไม่เคยพบมาก่อน เพื่อการเข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่าง ๆ ของระบบ รวมถึงความพยายามจะเจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน ด้วยวิธีการสุ่มข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกค่า (brute force)

7. โค้ดมุ่งร้าย (malicious code or malware) คือ โค้ดมุ่งร้ายหรือเป็นอันตรายต่อระบบ ขโมยข้อมูล และ/หรือยังส่งต่อไปยังเครื่องผู้อื่น ตัวอย่างโปรแกรมในกลุ่มนี้ ได้แก่ Virus, Worm, Trojan, Botnet, Horse, Spyware หรือ Web Scripts เป็นต้น

8. การเข้าถึง/เปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต (information security) เป็นภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (unauthorized access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (unauthorized modification) ได้

2.4 แนวคิดเกี่ยวกับการกลั่นแกล้งทางไซเบอร์ (Cyber Bullying)

2.3.1 ความหมายของการกลั่นแกล้งทางไซเบอร์

Payne (2007) กล่าวว่า การกลั่นแกล้งทางไซเบอร์ หมายถึง การรังแกและคุกคามผ่านอุปกรณ์อิเล็กทรอนิกส์ เช่น อีเมล์ โทรศัพท์มือถือ ข้อความโต้ตอบแบบทันที (IM) ข้อความสั้น (SMS) บล็อก และเว็บไซต์ ซึ่งทำให้เกิดอาชญากรรมคอมพิวเตอร์ได้ การกลั่นแกล้งทางไซเบอร์เป็นการกระทำโดยเจตนาและนำไปสู่ความตึงเครียดทางอารมณ์ ทำให้เกิดความทุกข์อย่างซ้ำ ๆ จากข้อความอิเล็กทรอนิกส์หนึ่งข้อความ การกลั่นแกล้งทางไซเบอร์ อาจรวมถึง การคุกคามและกล่าวถึงเรื่องทางเพศ การใช้คำพูดที่รุนแรง การดูถูกดูแคลน รวมทั้งการส่งอีเมลไปรบกวนผู้อื่นที่ไม่ต้องการติดต่อกับผู้ส่งด้วย

Smith (2008) กล่าวว่า การกลั่นแกล้งทางไซเบอร์ หมายถึง พฤติกรรมความก้าวร้าวของบุคคลหรือกลุ่มบุคคลที่เจตนาใช้เครื่องมืออิเล็กทรอนิกส์ ทำร้ายเหยื่อ ซึ่งยากที่จะป้องกันตนเอง โดยกระทาอย่างซ้ำ ๆ ซึ่งการกลั่นแกล้งทางไซเบอร์นั้นเพิ่งเกิดขึ้นในช่วงไม่กี่ปีที่ผ่านมา โดยเกิดขึ้นอย่างมาก โดยเฉพาะทางโทรศัพท์มือถือและอินเทอร์เน็ต

2.3.2 ลักษณะของการกลั่นแกล้งทางไซเบอร์

การกลั่นแกล้งโดยทั่วไปหลายแบบที่มีความแตกต่างกันออกไป เช่น การพูดจาหมิ่นประมาท การทำร้ายร่างกาย ซึ่งต่างจากการกลั่นแกล้งทางโลกไซเบอร์อย่างมาก โดยการกลั่นแกล้งทางไซเบอร์มีลักษณะดังนี้

1. การข่มขู่ใส่ร้าย (Harassment) เป็นการกลั่นแกล้งโดยการส่งข้อความโจมตีในทางเสียหายด้วยความคึกคะนองไปยังบุคคลอื่นหรือกลุ่มคนและทำซ้ำเป็นประจำหลาย ๆ ครั้ง ทั้งนี้การพูดคุยในโลกไซเบอร์ (Cyberstalking) เป็นอีกรูปแบบหนึ่งของการข่มขู่ที่ใช้ข้อความข่มขู่และหยาบคาย และนำไปสู่การทำร้ายร่างกายในโลกแห่งความเป็นจริง

2. การยั่วโมโห (Flaming) มีความคล้ายคลึงกับการข่มขู่ใส่ร้าย แต่จะมีการโต้ตอบกันทางอีเมล ข้อความโต้ตอบ หรือห้องแชท เป็นการกลั่นแกล้งประเภทหนึ่งที่เผยแพร่สู่สาธารณะโดยบ่อยครั้งมีการใช้ภาษาหรือภาพที่ส่อถึงบุคคลคนใดคนหนึ่งเป็นพิเศษ

3. การกีดกัน (Exclusion) การกีดกันเป็นการกระทำที่แยกบุคคลหนึ่งจากกลุ่มที่ออนไลน์ เช่น การสนทนาโดยส่งข้อความทันที การแชท ทั้งนี้ในกลุ่มจะมีการวิพากษ์วิจารณ์ในแง่ร้ายและข่มขู่จนกว่าบุคคลนั้นจะถอนตัวออกไป

4. การเผยแพร่ออกนอกกลุ่ม (Outing) การเผยแพร่ออกนอกกลุ่ม คือ การกลั่นแกล้งโดยแบ่งการเอาข้อมูล ภาพ คลิปวิดีโอส่วนบุคคลหรือข้อมูลส่วนตัวของบุคคลหนึ่งไปเผยแพร่สู่สาธารณะ โดยบุคคลที่เป็นคนที่ออกจากกลุ่มไปแล้ว ผู้ที่ออกนอกกลุ่มไปแล้ว (Outed) จะรู้ว่าข้อมูลของเขาถูกนำเผยแพร่จะรู้ตัวหลังจากกระจายทั่วอินเทอร์เน็ตแล้ว

5. การแอบอ้าง (Masquerading) การแอบอ้างเสแสร้งเป็นสถานการณ์เป็นการกลั่นแกล้งโดยสร้างเรื่องตลกที่มาจากลักษณะเฉพาะตัวที่เกี่ยวข้องกับบุคคลที่ถูกข่มขู่ โดยปิดบังชื่อนอกจากจะสร้างเรื่องตลก ยังมีการกลั่นแกล้งโดยปลอมเป็นบุคคลอื่น เพื่อส่งข้อความประสงค์ร้ายต่อเหยื่อด้วย

2.5 แนวคิดและทฤษฎีเกี่ยวกับความรู้ (Knowledge)

2.5.1 ทฤษฎีความรู้ในเชิงปรัชญา

เป็นเรื่องของญาณวิทยา (Epistemology) ซึ่งเกี่ยวข้องกับการกำเนิดของความรู้ โครงสร้างความรู้ วิธีการของความรู้และความเที่ยงตรงถูกต้องของความรู้ ความรู้ในเชิงญาณวิทยาจึงไม่มีโครงร่างเชิงวัตถุ ซึ่งเป็นการยากที่จะนำตัวความรู้ไปจัดการต่างกับความรู้ในเชิงเทคโนโลยีที่มองความรู้เป็นข้อเท็จจริง ในรูปแบบที่สามารถนำไปประมวลทางคณิตศาสตร์ได้ เช่น ความรู้ที่อยู่ในรูปของสูตร สมการ กฎ ทฤษฎีกระบวนการ และคำอธิบายให้เกิดความเข้าใจ ดังนั้นตามแนวทางนี้ความรู้จึงสามารถนำไปจัดการได้ความรู้มีอยู่ทั่วไปในส่วนที่ฝังอยู่ในตัวคนและอยู่ภายนอกตัวคน ในส่วนที่อยู่ภายนอกตัวคนซึ่ง

ได้มีการบันทึกเก็บไว้ในหน่วยบันทึกความรู้ในรูปแบบต่าง ๆ เช่นคู่มือ ตำราหรือ แฝงอยู่ในองค์การ ตัวผลิตภัณฑ์ และกระบวนการทำงานและการเรียนรู้ ซึ่งความรู้เหล่านี้จะมีคุณค่าก็ต่อเมื่อถูกนำไปใช้ให้เกิดประโยชน์ต่อบุคคล สถาบันและสังคมในบรรดาปัจจัยที่จำเป็นสำหรับการพัฒนานั้น ความรู้ทั้งในส่วนที่เป็นของปัจเจกบุคคลและของสถาบัน ถือเป็นปัจจัยที่มีความสำคัญอย่างยิ่ง การมีการบริหารจัดการความรู้ที่ดีย่อมทำให้บุคคล สถาบัน และสังคมได้รับประโยชน์จากความรู้อย่างเต็มที่ และในการที่จะบริหารจัดการความรู้ให้มีประสิทธิภาพนั้น จำเป็นอย่างยิ่งที่จะต้องรู้และเข้าใจในธรรมชาติของความรู้ โดยต้องเข้าใจความหมายของความรู้และประเภทของความรู้ ดังนี้

2.5.2 ความหมายของความรู้ (Knowledge)

การแบ่งประเภทของความรู้ มองได้หลายมิติ แต่มิติที่ได้รับความนิยมมากที่สุดคือมองในด้าน “รูปแบบที่มองเห็น” ซึ่ง ชู (Choo,2000 : 26 – 28) ได้แบ่งความรู้เป็น 3 ประเภท คือ

2.5.2.1 ความรู้โดยนัย (Tacit หรือ Implicit Knowledge) หมายความถึงเป็นความรู้เฉพาะตัวที่เกิดจากประสบการณ์ การศึกษา การสนทนา การฝึกอบรม ความเชื่อ เจตคติของแต่ละบุคคล เป็นความรู้บวกกับสติปัญญา และประสบการณ์ ซึ่งถือได้ว่าเป็นองค์รวมของความรู้ของแต่ละบุคคล ซึ่งเป็นความรู้ที่ไม่อยู่นิ่ง จะปรับเปลี่ยนไปตามสถานการณ์ของการใช้ความรู้ของแต่ละคน ซึ่งก็คือความรู้ที่ผ่านกระบวนการขัดเกลาทางสังคม ซึ่งถือว่าเมื่อคนปฏิบัติงานนาน ๆจนเกิดความช่ำชอง ความรู้ประเภทนี้ถือเป็นความรู้ไม่เป็นทางการจัดระบบหรือจัดหมวดหมู่ไม่ได้ แต่สามารถแลกเปลี่ยนหรือนำมาเล่าสู่กันฟัง สามารถถ่ายทอดแบ่งปันความรู้นี้ได้และสามารถสังเกตและเลียนแบบได้ ซึ่งองค์การต้องพยายามปรับเปลี่ยนความรู้โดยนัย ให้เป็นความรู้ที่ปรากฏเพื่อเป็นความรู้ที่ฝังกับองค์การ (Embedded Knowledge) ไม่ยึดติดกับตัวบุคคล

2.5.1.2 ความรู้ที่ปรากฏ (Explicit Knowledge) เป็นความรู้ที่ได้รับการถ่ายทอดจากบุคคลออกมาในรูปของบันทึกในรูปแบบต่าง ๆ ซึ่งก็คือ สารสนเทศนั่นเอง เช่น หนังสือ บทความ เอกสาร มาตรฐาน ลิขสิทธิ์ สิทธิบัตร เครื่องหมายการค้า ความลับทางการค้า รายงานประจำปี สื่อโสตทัศน์ เช่น วีดีโอ ซีดี สื่ออิเล็กทรอนิกส์ เช่นไปรษณีย์อิเล็กทรอนิกส์ อินเทอร์เน็ต เว็บไซต์อี-บุค ความรู้ที่ปรากฏถือได้ว่ามีการใช้สัญลักษณ์ ไม่ว่าจะเป็นภาษาพูด ภาษาเขียนเพื่อบันทึกความรู้นั้น ๆ ทำให้คนเข้าใจได้กว้างขวาง และสะดวกยิ่งขึ้นความรู้ที่มีการสะสมกันมานานเป็นความรู้ที่ใช้ประโยชน์ได้อย่างมีประสิทธิภาพและมีการตรวจสอบอย่างเป็นระบบ

2.5.3 ความรู้ที่เกิดจากวัฒนธรรม (Culture Knowledge)

เป็นความรู้ที่เกิดจากความเชื่อศรัทธา ซึ่งจะเกิดจากผลสะท้อนกลับของตัวความรู้ และสภาพแวดล้อมขององค์การ องค์การที่พัฒนามาเป็นระยะเวลานานจะมีการพัฒนาความเชื่อร่วมกันในเรื่องที่เกี่ยวกับธรรมชาติขององค์การ ความสามารถหลักขององค์การ (Core Competency) ซึ่งก็คือวัฒนธรรมขององค์การนั่นเอง

(Good, 1973, p. 325) กล่าวว่า ความรู้เป็นข้อเท็จจริง (Fact) ความจริง (Truth) เป็นข้อมูลที่มนุษย์ได้รับและเก็บรวบรวมจากประสบการณ์ต่าง ๆ การที่บุคคลยอมรับหรือปฏิเสธสิ่งใดสิ่งหนึ่งได้อย่างมีเหตุผล บุคคลควรจะต้องรู้เรื่องเกี่ยวกับสิ่งนั้น เพื่อประกอบการตัดสินใจ นั่นคือ บุคคลจะมีข้อเท็จจริงหรือข้อมูลต่าง ๆ ที่สนับสนุนและให้คำตอบข้อสงสัยที่มีอยู่ สามารถชี้แจงให้เกิดความเข้าใจและมีทัศนคติอันดี ตลอดจนเกิดความตระหนัก ความเชื่อ และค่านิยมต่าง ๆ ด้วย

เบอร์กูน (Burgoon, 1974, p. 64) กล่าวว่า การที่ผู้รับสารมีระดับการศึกษา หรือเคยศึกษาในสาขาวิชาที่ต่างกัน ตลอดจนได้รับการศึกษาในยุคสมัยที่แตกต่างกัน จะส่งผลให้มีความรู้ความนึกคิด และอุดมการณ์ที่แตกต่างกัน โดยช่วงเวลาของการเปิดรับสารมีอิทธิพลต่อความรู้ของผู้รับสาร

สุชาติ วงษ์หุ่น (2539, น.28) กล่าวว่า ความรู้เป็นพฤติกรรมเบื้องต้นที่ผู้เรียนสามารถจดจำได้หรือระลึกได้ โดยการมองเห็นหรือได้ยิน ซึ่งความรู้ในที่นี้คือข้อเท็จจริง กฎเกณฑ์ คำจำกัดความ เป็นต้น โดยขั้นนี้ความรู้จึงเป็นพฤติกรรมขั้นต้นที่คนเราเพียงแต่จำได้ อาจจะโดยการนึกได้ ความรู้ขั้นนี้ ได้แก่ ความรู้ที่เกี่ยวกับคำจำกัดความ ความหมาย ข้อเท็จจริง ทฤษฎี กฎโครงสร้าง และวิธีการแก้ปัญหา ดังนั้น อาจกล่าวรวม ๆ ได้ว่า ความรู้ หมายถึง การเรียนรู้ที่เน้นความจำ และการระลึกถึงได้ของคนเราที่มีต่อความคิด ปรากฏการณ์ หรือวัตถุต่าง ๆ ความจำนี้อาจเริ่มจากสิ่งที่ง่ายไม่ซับซ้อนไปจนถึงเรื่องยุ่งยากซับซ้อนหลายขั้นได้

ความรู้ เป็นการรับรู้เบื้องต้น ซึ่งบุคคลส่วนมากจะได้รับผ่านประสบการณ์ โดยการเรียนรู้จากการตอบสนองต่อสิ่งเร้า (Stimulus-Response) แล้วจัดระบบเป็นโครงสร้างของความรู้ที่ผสมผสานระหว่างความจำ (ข้อมูล) กับสภาพจิตวิทยา ดังนั้น ความรู้ จึงเป็นความจำที่เลือกสรร ให้สอดคล้องกับสภาพจิตใจของตนเอง ความรู้จึงเป็นกระบวนการภายใน อย่างไรก็ตามความรู้ก็อาจส่งผลต่อพฤติกรรมที่แสดงออกของมนุษย์ อาจปรากฏได้จากจากสาเหตุ 5 ประการ คือ (สุรพงษ์ โสธนะเสถียร, 2533, น. 120-121)

1. การตอบข้อสงสัย (Ambiguity Resolution) การสื่อสารมักสร้างความสับสนให้สมาชิกในสังคม ผู้รับสารจึงมักแสวงหาสารสนเทศโดยอาศัยสื่อทั้งหลาย เพื่อตอบข้อสงสัยและความสับสนของตน

2. การสร้างทัศนะ (Attitude Formation) ผลกระทบเชิงความรู้ต่อการปลูกฝังทัศนะนั้นส่วนมากนิยมใช้กับสารสนเทศที่เป็นนวัตกรรม เพื่อสร้างทัศนคติให้คนยอมรับการแพร่นวัตกรรมนั้น ๆ (ในฐานะความรู้)

3. การกำหนดวาระ (Agenda Setting) เป็นผลกระทบเชิงความรู้ที่สื่อกระจายออกไปเพื่อให้ประชาชนตระหนักและผูกพันกับประเด็นวาระที่สื่อกำหนดขึ้น หากตรงกับภูมิหลังของปัจเจกชนและค่านิยมของสังคมแล้ว ผู้รับสารก็จะเลือกสารสนเทศนั้น

4. การพอกพูนระบบความเชื่อ (Expansion of The Belief System) การสื่อสารสังคมมักกระจายความเชื่อ ค่านิยม และอุดมการณ์ด้านต่าง ๆ ไปสู่ประชาชน จึงทำให้ผู้รับสารรับทราบระบบความเชื่อถือหลากหลาย และลึกซึ้งไว้ในความเชื่อของตนมากขึ้นเรื่อย ๆ

5. การรู้แจ้งต่อค่านิยม (Value Clarification) ความขัดแย้งในเรื่องค่านิยมและอุดมการณ์เป็นภาวะปกติของสังคม สื่อมวลชนที่นำเสนอข้อเท็จจริงในประเด็นเหล่านี้ ย่อมทำให้ประชาชนผู้รับสารเข้าใจถึงค่านิยมเหล่านั้นแจ้งชัดขึ้น

บลูม และคณะ (Bloom et al., 1956, p. 28} อ้างถึงใน อรวรรณ ปิลันธน์โอวาท, 2549, น. 36-37) ได้แยกการประเมินระดับความรู้ไว้ 6 ระดับ ดังนี้

1. ระดับที่ระลึกได้ (Recall) หมายถึง การเรียนรู้ในลักษณะที่จำเรื่องเฉพาะ วิธีปฏิบัติ กระบวนการ และแบบแผนได้ ความสำเร็จในระดับนี้ คือ ความสามารถในการดึงข้อมูลจากความจำออกมาได้

2. ระดับที่รวบรวมสาระสำคัญได้ (Comprehension) หมายถึง บุคคลสามารถทำบางสิ่งบางอย่างได้มากกว่าการจำเนื้อหาที่ได้รับ สามารถเขียนข้อความนั้นได้ ด้วยถ้อยคำของตนเอง สามารถแสดงให้เห็นได้ด้วยภาพ ให้ความหมาย แปลความหมาย และเปรียบเทียบความคิดอื่น ๆ หรือคาดคะเนผลที่เกิดขึ้นต่อไปได้

3. ระดับของการนำไปใช้ (Application) สามารถนำเอาข้อเท็จจริงและความคิดเห็นที่เป็นนามธรรม (Abstract) ไปปฏิบัติการจริงอย่างเป็นรูปธรรม

4. ระดับของการวิเคราะห์ (Analysis) สามารถให้ความคิดเห็นในรูปของการนำความคิดมาแยกเป็นส่วน เป็นประเภท หรือการนำข้อมูลมาประกอบกันเพื่อการปฏิบัติของตนเอง

5. ระดับของการสังเคราะห์ (Synthesis) คือ การนำเอาข้อมูล แนวความคิด มาประกอบกัน แล้วนำไปสู่การสร้างสรรค์ (Creative) สิ่งใหม่ที่แตกต่างไปจากเดิม

6. ระดับของการประเมินผล (Evaluation) คือ ความสามารถในการใช้ข้อมูลเพื่อตั้งเกณฑ์ (Criteria) การรวบรวมผล และวัดข้อมูลตามมาตรฐาน เพื่อให้ตั้งข้อตัดสินถึงระดับของประสิทธิผลของกิจกรรมแต่ละอย่าง

2.6 แนวคิดเกี่ยวกับความตระหนัก (Awareness)

2.6.1 ความหมายของความตระหนัก

พจนานุกรมราชบัณฑิตสถาน พ.ศ. 2542 (2546) ได้ให้ความหมาย “ความตระหนักว่าเป็นการรู้ประจักษ์ชัด รู้ชัดแจ้ง” โดยสอดคล้องกับพจนานุกรม ของ Good (1973, p. 54) โดยได้ให้ความหมายว่า “การแสดงออกจากการระลึกได้หรือจดจำได้” นอกจากนั้น ยังมีผู้นิยามไว้อีก ดังนี้

Bloom (1971, p. 271 อ้างถึงใน สุพัตรา ถนอมวงค์, 2551, น.10) ได้ให้นิยามว่า “ความตระหนักคือ ภาคต่ำสุดทางภาคอารมณ์ซึ่งความตระหนักนั้นคล้ายกับอารมณ์ความรู้สึก (Affective Domain) แต่ความตระหนักต่างกับความรู้สึกตรงที่ความตระหนักไม่จำเป็นต้องเน้นปรากฏการณ์หรือสิ่งหนึ่งสิ่งใด แต่ความตระหนักจะเกิดขึ้นเมื่อมีสิ่งเร้าให้เกิดความตระหนัก”

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

อนุสรณ์ กาลดิษฐ์ (2548, น.51) ได้ให้นิยามว่า “ความตระหนัก หมายถึง ความสำนึกของแต่ละบุคคลเคยมีการรับรู้หรือเคยมีความรู้มาก่อน มีสิ่งเร้ามากระตุ้นจนเกิดความตระหนักจากการประเมินค่า”

ประพล มิลินทจินดา (2542, น.19) ได้ให้นิยามว่า “ความตระหนัก คือ การแสดงความรู้สึก นึกคิด ความคิดเห็น ที่บุคคลเข้าใจและประเมินสถานการณ์ที่เกิดขึ้นเกี่ยวกับตนเองจากประสบการณ์ จากช่วงระยะเวลา จากเหตุการณ์ และจากสภาพแวดล้อม เป็นปัจจัยทำให้มนุษย์มีความตระหนัก”

วีระชน ขาวผ่อง (2551,น.42) ได้ให้นิยามว่า “ความตระหนัก คือ สภาวการณ์มีผลให้เกิด ความรู้สึก การรับรู้มุ่งสู่สภาวะจิตแห่งตนคือ ทัศนคติ ความคิด ความเชื่อ ความสนใจ อันจะก่อให้เกิดความตระหนักและจิตสำนึก”

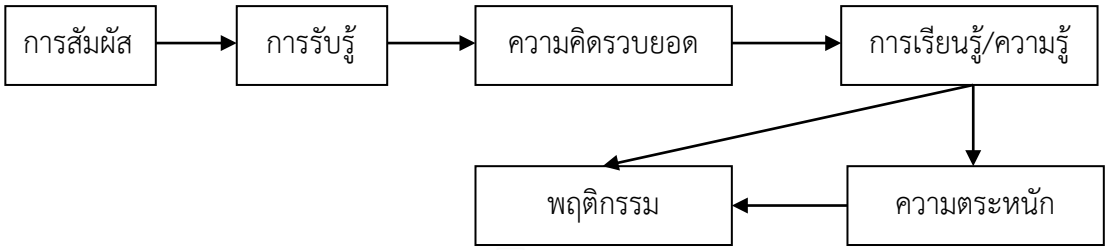
พงษ์ชัย เฉลิมกลิ่น (2551,น. 50) ได้ให้นิยามว่า “ความตระหนัก คือ พฤติกรรมที่แสดงถึงความรับผิดชอบต่อสิ่งใดสิ่งหนึ่งหรือเหตุการณ์ใดเหตุการณ์หนึ่ง ซึ่งเป็นอารมณ์ความรู้สึกด้านทัศนคติ ค่านิยม ความชอบหรือไม่ชอบ ดีหรือไม่ดี ที่ได้จากการประเมินสิ่งเร้าต่าง ๆ ของบุคคลนั้น”

ทั้งนี้สามารถสรุปได้ว่า ความตระหนัก (Awareness) คือ การรับรู้แบบฉุกคิดขึ้นมากะทันหันต่อสิ่งใดสิ่งหนึ่งหรือเหตุการณ์ใดเหตุการณ์หนึ่งซึ่งเป็นอารมณ์ความรู้สึกโดยอาศัยองค์ประกอบจากสิ่งแวดล้อม ประสบการณ์ และสิ่งที่ส่งผลกับอารมณ์และความรู้สึก

2.4.2 ปัจจัยที่ทำให้เกิดความตระหนัก

กระบวนการเกิดความตระหนักมาจากกระบวนการทางปัญญา (Cognitive process) ทั้งนี้เมื่อบุคคลได้รับการกระตุ้นจากสิ่งเร้าหรือรับสัมผัสจากสิ่งเร้าหรือประสบการณ์แล้วจะเกิดการรับรู้ จากนั้นจะเข้าใจในสิ่งเร้านั้น และเกิดเป็นความคิดรวบยอด และทำให้มีความรู้ (Knowledge) และเมื่อมีความรู้ในสิ่งนั้นก็จะนำไปสู่การเกิดความตระหนัก ทั้งนี้ความรู้และความตระหนักนี้ต่างก็จะนำไปสู่การกระทำ (Action) หรือการแสดงพฤติกรรมของบุคคลต่อสิ่งเร้านั้น ๆ

พจนานุกรม ของ Good (1973) ได้ประมวลขั้นตอนของกระบวนการเกิดความตระหนัก ดังนี้ (Good, 1973 อ้างถึงใน สุธาสินี อินทร์ผูก, 2548)



ภาพที่ 2.1 ขั้นตอนของกระบวนการเกิดความตระหนัก

ในลักษณะเช่นนี้ ความตระหนักจึงเป็นผลของกระบวนการทางปัญญา กล่าวคือ เมื่อบุคคลได้รับการกระตุ้นจากสิ่งเร้า หรือรับสัมผัสจากสิ่งเร้าแล้วเกิดการรับรู้ขึ้นแล้วจะนำไปสู่การเกิดความเข้าใจในสิ่งเร้านั้น และนำไปสู่การเรียนรู้เป็นขั้นตอนต่อไป และเมื่อบุคคลเกิดมีความรู้ในสิ่งนั้นแล้วก็จะมีผลไปสู่ความตระหนักในที่สุด ซึ่งทั้งความรู้และความตระหนักจะนำไปสู่การกระทำหรือพฤติกรรมของบุคคลที่มีต่อสิ่งเร้านั้น ๆ ต่อไป และจากการศึกษาของทนงศักดิ์ ประสบกิตติคุณ (ม.ป.ป. อ้างถึงใน พัฒนศักดิ์ บุบผาสุวรรณ, 2546) กล่าวถึง ปัจจัยทางพฤติกรรมศาสตร์ที่มีผลต่อความตระหนัก ประกอบด้วย ประสบการณ์ที่มีต่อการรับรู้ ความเคยชินต่อสภาพแวดล้อม ถ้าบุคคลใดไม่เคยชินต่อสภาพแวดล้อมนั้นก็จะทำให้บุคคลนั้นไม่ตระหนักต่อสิ่งที่เกิดขึ้น ความใส่ใจและการให้คุณค่า ถ้ามนุษย์มีความใส่ใจในเรื่องใดมากก็จะมีความตระหนักในเรื่องนั้นมาก ลักษณะและรูปแบบของสิ่งเร้า ถ้าสิ่งเร้านั้นสามารถทำให้ผู้พบเห็นเกิดความสนใจย่อมทำให้ผู้พบเห็นเกิดการรับรู้และความตระหนักขึ้น ระยะเวลาและความถี่ในการรับรู้ ถ้ามนุษย์ได้รับรู้บ่อยครั้งเท่าใดก็ยิ่งทำให้มีโอกาสเกิดความตระหนักได้มากขึ้นเท่านั้น

สำหรับวิธีการสร้างความตระหนักทำได้ด้วยวิธีดังต่อไปนี้

1) การเผยแพร่ข้อมูล

2) สร้างข้อความที่มีผลกระทบสูง หรือข้อความที่กระตุ้นอารมณ์

3) สร้างข้อความที่เชื่อมต่อทัศนคติกับพฤติกรรมที่ผ่านมา

อย่างไรก็ตาม ลักษณะเฉพาะของแต่ละบุคคลมีผลต่อการรับรู้และการเกิดความตระหนักที่มุ่งเน้นการเปลี่ยนแปลงการรับรู้เกี่ยวกับกลุ่มหรือต่อวัตถุ รวมทั้งจะเกิดความตระหนักต่อสถานการณ์ที่จะส่งเสริมการเปลี่ยนแปลงทัศนคติต่างกัน

นอกจากนี้ Herek, G. (1986,pp99 -104) กล่าวว่า ปัจจัยด้านสถานการณ์ที่ทำให้บุคคลมีความตระหนักมากขึ้นส่วนหนึ่งมาจากการรับรู้ข่าวสาร อย่างไรก็ตามยังไม่อาจสามารถสรุปได้ว่า ทัศนคติและความตระหนักมีผลโดยตรงทำให้เกิดการเปลี่ยนแปลงพฤติกรรม แต่เป็นเพียงปัจจัยที่มีส่วนให้เกิดการเปลี่ยนแปลงพฤติกรรมเท่านั้น เช่นเดียวกันกับ Kim, M. s., & Hunter, J. e. (1993,pp. 331 - 364) อธิบายว่า ความตระหนักรู้ทำหน้าที่เป็นตัวกลางในการมีปฏิสัมพันธ์เชิงทัศนคติและพฤติกรรม ความตระหนักรู้สร้างความเต็มใจในการมีส่วนร่วมกับพฤติกรรมต่างๆ

2.7 งานวิจัยที่เกี่ยวข้อง

ฐิตารีย์ จันทพันธ์ (2559) วิจัย เรื่อง “การศึกษาผลกระทบการรับรู้ความเสี่ยงในการใช้งานการระบุตำแหน่ง (Location - Based Services: LBS) บนสื่อสังคมออนไลน์ ต่อความเป็นส่วนตัวของผู้ใช้งานในเขตกรุงเทพมหานคร” ผลการวิจัย พบว่า ปัจจัยการรับรู้ความเสี่ยงด้านความปลอดภัย และการรับรู้ความเสี่ยงด้านความไว้วางใจ ในการใช้งานการระบุตำแหน่ง (Location - Based Services: LBS) บนสื่อสังคมออนไลน์ ส่งผลกระทบต่อความเป็นส่วนตัวของผู้ใช้งานในเขตกรุงเทพมหานคร โดยที่ปัจจัยการรับรู้ความเสี่ยงด้านความปลอดภัย ส่งผลกระทบต่อความเป็นส่วนตัวของผู้ใช้งานในเขตกรุงเทพมหานครมากที่สุด ในขณะที่ปัจจัยการรับรู้ความเสี่ยงด้านความไว้วางใจ ด้านอิทธิพลทางสังคม ไม่ส่งผลกระทบต่อความเป็นส่วนตัวของผู้ใช้งานในเขตกรุงเทพมหานคร

ปิยะภัสร์ โรจน์รัตนวาณิชย์ (2557) วิจัย เรื่อง “แนวทางการคุ้มครองข้อมูลใน Big Data: ความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูล” ผลการวิจัย พบว่า ยังไม่กฎหมายที่บัญญัติขึ้นเป็นการเฉพาะเรื่องความเป็นส่วนตัว รวมถึงการรักษาความมั่นคงปลอดภัยของข้อมูลของผู้ใช้บริการต่าง ๆ แม้ว่าจะมีการนำกฎหมายที่มีผลบังคับใช้ในปัจจุบันไปใช้ในกรณีการละเมิดความเป็นส่วนตัวจากการใช้ Big Data ก็ตาม แต่ก็ยังไม่ได้บัญญัติไว้ครอบคลุมถึงการคุ้มครองความเป็นส่วนตัว และความปลอดภัยของข้อมูลในกรณี Big Data ดังนั้นผู้วิจัยจึงมีความเห็นว่า ควรเร่งให้มีการออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลที่มีอยู่ในความครอบครองของภาคเอกชนเป็นการทั่วไป และเพื่อเป็นการวางมาตรการในเชิงป้องกันการละเมิดความเป็นส่วนตัวในข้อมูลส่วนบุคคล และความปลอดภัยของข้อมูล และเพื่อระบุถึงสิทธิหน้าที่ของผู้ที่เกี่ยวข้องกับ Big Data ให้มีความชัดเจนแน่นอน ผู้เขียนเห็นว่าควรจะพยายามตีความกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลให้ครอบคลุมมาถึงความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูลกรณี Big Data ด้วย แล้วอาศัยอำนาจแห่งกฎหมายดังกล่าวออกกฎหมายลำดับรอง เพื่อวางแนวทางในการคุ้มครองความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูลกรณี Big Data เป็นการเฉพาะ

อุบลวรรณ ภีระเป็ง (2558) วิจัยเรื่อง “การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ : ศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ” ทั้งนี้งานวิจัยนี้มีจุดประสงค์เพื่อศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศว่าสามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธในฐานะเป็นวิธีการและปัจจัยในการสู้รบที่เกิดขึ้นใหม่ได้หรือไม่เพียงใด

อนึ่ง กฎหมายมนุษยธรรมระหว่างประเทศเป็นกฎหมายระหว่างประเทศบังคับใช้เมื่อมีการสู้รบหรือสถานการณ์การขัดกันทางอาวุธเกิดขึ้นประกอบด้วยหลักเกณฑ์เกี่ยวกับปฏิบัติการทางทหารรวมทั้งการให้ความคุ้มครองพลเรือน จากการศึกษาวิจัยพบว่า แม้ว่าการโจมตีทางไซเบอร์จะเป็นวิธีการและปัจจัยในการสู้รบใหม่และไม่ปรากฏข้อบทที่เกี่ยวข้องกับการใช้เทคโนโลยีตามกฎหมายมนุษยธรรมระหว่างประเทศ แต่กฎหมายมนุษยธรรมระหว่างประเทศสามารถยืดหยุ่นครอบคลุมกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอันเป็นการนำเอาเทคโนโลยีสารสนเทศและคอมพิวเตอร์หรือไซเบอร์มาใช้ในปฏิบัติการทางทหารและการสู้รบได้

อย่างไรก็ตาม ด้วยลักษณะความเชื่อมต่อของเทคโนโลยีที่ใช้ในทางทหารและพลเรือน อีกทั้งการโจมตีทางไซเบอร์ยังเป็นการกระทำภายในห้วงไซเบอร์ที่ไม่มีลักษณะทางกายภาพก่อให้เกิดข้อท้าทายในบังคับใช้หลักการสำคัญตามกฎหมายมนุษยธรรมระหว่างประเทศ ไม่ว่าจะเป็นหลักการแยกแยะเป้าหมาย หลักความได้สัดส่วนในการโจมตี หลักการใช้ความระมัดระวังในการโจมตีอย่างมีนัยสำคัญจำเป็นจะต้องอาศัยความร่วมมือจากผู้ที่มีส่วนเกี่ยวข้องทั้งภาคประชาสังคม ภาครัฐ และความร่วมมือระหว่างประเทศในการพัฒนาแนวทางการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่จะนำไปสู่แนวทางปฏิบัติของรัฐที่ชัดเจนต่อไป เพื่อให้กฎหมายมนุษยธรรมระหว่างประเทศสามารถรองรับวิธีการและปัจจัยในการสู้รบใหม่ซึ่งมีความซับซ้อนของเทคโนโลยีสารสนเทศและคอมพิวเตอร์ทวีขึ้นไปตามกาลเวลาได้อย่างมีประสิทธิภาพ

ศิวลีย์ สิริโรจน์บริรักษ์ (2558) วิจัยเรื่อง “การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม” มีวัตถุประสงค์เพื่อศึกษานโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. ศึกษามาตรฐานการดำเนินงานด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ในระดับสากล และเพื่อเสนอแนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ของ กห. ให้ได้มาตรฐานระดับสากล โดยการศึกษาครั้งนี้ใช้วิธีการสัมภาษณ์กลุ่มผู้ให้ข้อมูลสำคัญ (Key Informants) และการ ค้นคว้าข้อมูลจากเอกสารทางวิชาการต่าง ๆ ที่มีเนื้อหาเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. และมาตรฐาน การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล ผลการศึกษา พบว่า

1) กรอบนโยบาย ยุทธศาสตร์ และการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกระทรวง กลาโหม ได้แก่ พ.ร.บ.ว่าด้วยการจัดระเบียบราชการด้านเทคโนโลยีสารสนเทศและการ

สื่อสารของ กห. พ.ศ. 2551, นโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กห. พ.ศ. 2554, ยุทธศาสตร์ กห. อิเล็กทรอนิกส์ (e-Defence), แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของ กห. ฉบับที่ 3 พ.ศ. 2557 – 2561, การจัดตั้งศูนย์บัญชาการไซเบอร์ กห.

2) มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล ได้แก่ มาตรฐาน U.S. DoD, มาตรฐาน ISO 27001: 2005, มาตรฐาน FIPS PUB 200, มาตรฐาน NIST 800 – 14, มาตรฐาน COBIT, และ มาตรฐาน IT BPM 3) แนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กห. ให้ได้มาตรฐานใน ระดับสากล เชิงนโยบาย ได้แก่ ส่วนบังคับการ ต้องเปิดอัตรานายทหารสงครามข้อมูลข่าวสาร เพื่อดำเนินการตอบสนองต่อ

ภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ (Cyber Threat) เป็นประเด็นปัญหาที่ทำให้ประเทศต่าง ๆ ทั่วโลก เกิดการตื่นตัวและตระหนักถึงปัญหา ดังจะเห็นได้จาก ปรากฏการณ์ที่ก่อให้เกิดความเปลี่ยนแปลงในโลกอาหรับ หรือที่รู้จักโดยทั่วไปว่าปรากฏการณ์ “Arab Spring” หรือแม้แต่กลุ่มก่อการร้าย ISIS ซึ่งใช้เครือข่ายสังคมออนไลน์ เช่น Twitter, Facebook ฯลฯ เป็นเครื่องมือสำคัญในการปลุก ระดมมวลชน เป็นต้น จากรายงานของ World Economic Forum แสดงให้เห็นว่า ทั่วโลกำลังวิตกกังวลกับภัยคุกคาม ความมั่นคงปลอดภัยไซเบอร์เป็นอย่างมาก โดยภัยคุกคาม ความมั่นคงปลอดภัยไซเบอร์ถูกจัดให้อยู่ในอันดับที่ 4 ใน 10 Trends ของโลก ประกอบกับผลการศึกษาของสถาบัน The Business Continuity Institute (BCI) ซึ่งเป็นสถาบันอันดับ หนึ่งของโลกด้านการบริหารความต่อเนื่องทางธุรกิจ ยังแสดง ให้เห็นว่า Cyber Attack เป็นประเด็นอันดับต้น ๆ ที่องค์กร ให้ความสนใจมากที่สุด

วิภารัตน์ ปทักขินัง (2557) วิจัยเรื่อง “การพัฒนาระบบสารสนเทศสำหรับการประเมินระดับความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภยัทางไซเบอร์ ขององค์กร” พบว่า การวิจัยนี้มีวัตถุประสงค์เพื่อวิเคราะห์ความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ การนำเสนอตัวแบบการประเมินความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์และการพัฒนาระบบสารสนเทศสำหรับประเมินด้านความมั่นคงปลอดภัยไซเบอร์ ผู้วิจัยได้ใช้กรณีศึกษาของวิทยาลัยเทคโนโลยีสยาม และได้เก็บรวมรวบข้อมูลจากผู้ที่ทำหน้าที่ เกี่ยวข้องกับไอซีทีเป็นกลุ่มตัวอย่าง ผลการวิจัยพบว่า องค์ประกอบความพร้อมด้านความมั่นคง ปลอดภัยทางไซเบอร์จะประกอบไปด้วย 7 ด้าน ได้แก่

1. ด้านยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์
2. ด้านกฎระเบียบที่เกี่ยวข้อง
3. ด้านศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์
4. ด้านการป้องกันอาญากรรมไซเบอร์

5. ด้านการพัฒนาด้านไซเบอร์

6. ด้านงบประมาณการวิจัย

7. ด้านความร่วมมือกับหน่วยงานอื่น ๆ

สำหรับตัวแบบการประเมิน ความเสี่ยงจะประกอบไปด้วย 4 ด้าน ได้แก่

1. กำหนดหัวข้อการบริหารจัดการความเสี่ยง

2. การวิเคราะห์ความเสี่ยง

3. การวางแผนการลดความเสี่ยง

4. การรายงานและการประเมินผล

นอกจากนั้น เมื่อนำตัวแบบดังกล่าวไปทำการประเมินวิทยาลัยเทคโนโลยีสยามแล้ว พบว่าระดับความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรอยู่ในระดับที่มีความพร้อมมากที่สุด ส่วนการวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ขององคกร์อยู่ในระดับที่มีความเสี่ยงน้อย เมื่อแยกความเสี่ยงแต่ละด้านพบดังนี้

ด้านยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ มีระดับความพร้อมอยู่ในระดับมีความพร้อมมาก โดยมีค่าเฉลี่ย = 4.19 แสดงให้เห็นว่าองค์กรมีการกาหนดนโยบายและยุทธศาสตร์ด้านความมั่นคงปลอดภัย มีการประกาศให้บุคลากรได้ทราบถึงยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์รวมถึงมีผู้ดูแลรับผิดชอบ

ด้านบุคลากร มีความมั่นคงปลอดภัยอยู่ในระดับปานกลาง โดยมีค่าเฉลี่ย = **2.91** แสดงว่าบุคลากรของสถาบันการพลศึกษา เห็นว่าควรหน่วยงานมีการ คัดเลือกบุคลากรกาหนดเงื่อนไขการจ้างงาน การส่งมอบงานและตรวจสอบทรัพย์สิน ยกเลิกสิทธิ การจัดอบรมและสร้างความตระหนักให้กับบุคลากรเกี่ยวกับความมั่นคงปลอดภัยอยู่ในระดับปานกลาง

ด้านศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีระดับความพร้อมอยู่ในระดับมีความพร้อมมาก โดยมีค่าเฉลี่ย = 3.96 แสดงให้เห็นว่า องค์กรมีศูนย์ประสานงานหรือการตอบสนองต่อการแจ้งเหตุภัยคุกคามทางไซเบอร์ มีการประสานงานเพื่อแลกเปลี่ยนข้อมูลสารสนเทศและซอฟต์แวร์ระหว่างหน่วยงาน มีการควบคุมข้อมูลสารสนเทศ กรณีส่งผ่านทางอีเมล์ เอสเอ็มเอสและอื่นๆ

ด้านการป้องกันอาญากรรมไซเบอร์ ระดับความพร้อมอยู่ในระดับมีความพร้อมมาก โดยมีค่าเฉลี่ย = **3**.99 แสดงให้เห็นว่า องค์กรมีนโยบายด้านการป้องกันข้อมูลสารสนเทศอย่างเข้มแข็ง มีระบบจัดเก็บสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต หรือการนาไปใช้ในทางที่ผิด มีบุคลากรคอยตรวจจับและตอบโต้การคุกคาม มีการแจ้งเตือนผู้ใช้ให้ระมัดระวังการโจมตีจากภัยคุกคาม และ จากัดการเข้าถึงสารสนเทศตามนโยบายการป้องกันข้อมูลสารสนเทศ

ด้านการพัฒนากำลังพลต่อความมั่นคงปลอดภัยไซเบอร์ ระดับความพร้อมอยู่ในระดับมีความพร้อมมาก โดยมีค่าเฉลี่ย = 4.13 แสดงให้เห็นว่า องค์กรมีการพัฒนาบุคลากรโดยการส่งไปฝึกอบรม หรือ ดูงานด้านความมั่นคงปลอดภัยไซเบอร์ นอกสถานที่ บุคลากรขององค์กรเข้าใจในบทบาท หน้าที่และความรับผิดชอบของตน และ ปลุกจิตสานึก ให้ความรู้ และเตือนความจา เกี่ยวกับเรื่องความมั่นคงปลอดภัยทางไซเบอร์ ให้แก่บุคลากรทุกคน

ด้านงบประมาณสนับสนุนการวิจัยพื้นฐานและวิจัยเชิงประยุกต์ ระดับความพร้อมอยู่ในระดับมีความพร้อมมาก โดยมีค่าเฉลี่ย = 3.88 แสดงให้เห็นว่า องค์กรสนับสนุนการวิจัยพื้นฐานและวิจัยเชิงประยุกต์ด้านความมั่นคงปลอดภัยไซเบอร์ มีงบประมาณสนับสนุนในการตีพิมพ์บทความการวิจัยและมีงบประมาณสนับสนุนในการจัดสัมมนาทางด้านความมั่นคงปลอดภัยไซเบอร์

ด้านความร่วมมือกับหน่วยงานอื่น ๆ ระดับความพร้อมอยู่ในระดับมีความพร้อมมาก โดยมีค่าเฉลี่ย = 4.09 แสดงให้เห็นว่า องค์กรมีความพร้อมด้านความร่วมมือกับองค์กรภายนอกสถาบันเกี่ยวกับความมั่นคงปลอดภัย มีการจัดตั้งศูนย์ด้านความมั่นคงปลอดภัยเพื่อแลกเปลี่ยนข้อมูลกับหน่วยงานอื่นๆ และมีการจัดบุคลากรเพื่อรับผิดชอบและประสานงานด้านความมั่นคงปลอดภัยไซเบอร์

อรรถพล ป้อมสถิตย์ (2559) วิจัยเรื่อง “การเพิ่มประสิทธิภาพระบบตรวจจับการบุกรุกในการรักษาความมั่นคงทางไซเบอร์ด้วยฮันนี่พอท” พบว่า การบุกรุกเครือข่ายโดยใช้ฮันนี่พอทในการหลอกล่อ หน่วงเวลา หรือเบี่ยงเบน ผู้บุกรุกไม่ให้โจมตีไปที่เครื่องแม่ข่าย ในการโจมตีรูปแบบการปฏิเสธการมีการให้บริการ 3 รูปแบบได้แก่ TCP Flood, UDP Flood และ ICMP Flood โดยฮันนี่พอทจะใช้โปรแกรม Honeyd ในการจำลองเครื่องคอมพิวเตอร์หรือเครื่องแม่ข่ายให้อยู่ในแผนผังเครือข่ายที่ต้องการจะรักษาความปลอดภัยโดยกำหนดให้ไม่มีการใช้งานไฟร์วอล์และการรักษาความปลอดภัยรูปแบบอื่นๆ ซึ่งจะใช้ระบบป้องกันการบุกรุกและฮันนี่พอทเท่านั้นในการรักษาความปลอดภัยเครือข่าย

ส่วนระบบตรวจจับการบุกรุกเครือข่ายจะใช้โปรแกรม Snort โดยโปรแกรมทั้งหมดจะพัฒนาในรูปแบบ Open Source อยู่บนระบบปฏิบัติการ Linux จากผลการทดสอบการโจมตีจากระบบเครือข่ายภายใน และภายนอกของงานวิจัยนี้ทำให้ได้วิธีการเพิ่มประสิทธิภาพระบบตรวจจับการบุกรุกในการรักษาความมั่นคงทางไซเบอร์เมื่อนำฮันนี่พอททำงานร่วมกับระบบตรวจจับการบุกรุกโดยการโจมตีผ่านระบบเครือข่ายแลน มีความเสี่ยงในการถูกโจมตีใกล้เคียงระบบเครือข่ายแลนไร้สาย และการโจมตีแบบ TCP Flood มีอัตราการตรวจจับการบุกรุกได้สูงสุดเมื่อเปรียบเทียบกับการโจมตีแบบ ICMP Flood ที่มีอัตราการตรวจจับการบุกรุกในการโจมตีผ่านระบบเครือข่ายภายในต่างกัน 33.75% และโจมตีผ่านระบบเครือข่ายภายนอกต่างกัน 53.47% นั่นหมายถึงในการรักษาความมั่นคง

ทางไซเบอร์ จะต้องมีการป้องกันการโจมตีแบบ TCP Flood และการโจมตีจากภายในซึ่งมีอันตรายมากที่สุด

สรุปได้ว่า การโจมตีแบบปฏิเสธการให้บริการจากภายในมีจำนวนการตรวจจับการบุกรุกที่มากกว่าการโจมตีจากภายนอกเฉลี่ยรวมประมาณ 48.3% นั้นหมายถึงการใช้เราท์เตอร์เพื่อแยกระบบเครือข่ายออกเป็นส่วนๆ แม้ไม่การใช้ไฟร์วอลล์และกำหนดคุณสมบัติด้านความปลอดภัยใดๆกับเราท์เตอร์สามารถลดโอกาสในการโจมตีแบบปฏิเสธการให้บริการจากผู้ประสงค์ร้ายต่อเครื่องแม่ข่ายได้อย่างมาก และการโจมตีแบบ TCP Flood สามารถตรวจจับการบุกรุกได้มากที่สุดนั้นเป็นเพราะ TCP โพรโทคอลเป็นได้รับความนิยม การให้บริการ และมีการใช้งานของเครื่องแม่ข่ายโดยทั่วไปจำนวนมาก จึงทำให้ระบบตรวจจับการบุกรุกสามารถตรวจจับการบุกรุกได้แตกต่างมากกว่าโพรโทคอลอื่นๆ และในส่วนการโจมตีแบบปฏิเสธการให้บริการผ่านระบบแลน และแลนไร้สายที่มีค่าใกล้เคียงกันในทุกการทดลองเป็นเพราะจำนวนรวมเครื่องลูกข่ายของแลนไร้สายมีจำนวนไม่เกิน 3 เครื่อง

ดังนั้นหากในกรณีที่จำนวนรวมเครื่องลูกข่ายของแลนไร้สายมีจำนวนมากกว่า 100 เครื่อง ผลลัพธ์ของการทดลองระหว่างแลน และแลนไร้สายจะมีค่าต่างกัน โดยการตรวจจับในเครือข่ายแลนไร้สายจะมีค่าน้อยกว่าเครือข่ายแลนเนื่องจากกลไกการสื่อสารของแลนไร้สายเป็นแบบ Carrier Sent Multiple Access/Collision Avoidance (CSMA/CA) (Alshami, I.H., Ahmad, N.A. and Sahibuddin, S., 2014)

ซึ่งเป็นการสื่อสารของอุปกรณ์ไร้สายแบบ Half Duplex กล่าวคือจะต้องใช้การหลีกเลี่ยงการชนของสัญญาณที่มีการเสียเวลาในการรอคอยช่องสัญญาณจำนวนมาก อีกทั้งยังอาจเกิดปัญหาการรบกวนสัญญาณ หรือการสูญหายของสัญญาณระหว่างการสื่อสารไร้สาย จึงทำให้มีผลลัพธ์ของการโจมตีที่มีความล่าช้า กว่าการสื่อสารในเครือข่ายแลนซึ่งใช้กลไกการสื่อสารแบบ Full Duplex กล่าวคือไม่ต้องหลีกเลี่ยงการชนของสัญญาณในช่องสัญญาณที่จำกัด และที่สำคัญจะเห็นได้ว่าเมื่อมีการใช้ระบบตรวจจับการบุกรุกร่วมกับฮันนี่พอทจะมีจำนวนการตรวจจับได้มากกว่ากรณีไม่มีฮันนี่พอทในทุกการทดลองโดยเฉลี่ยต่างกันประมาณ 7% นั้นเป็นการยืนยันได้ว่าฮันนี่พอทสามารถเพิ่มประสิทธิภาพในการรักษาความมั่นคงทางไซเบอร์โดยช่วยหลอกล่อผู้ประสงค์ร้ายในการโจมตีเครื่องแม่ข่ายได้เป็นอย่างดี

วรัญญา สอาด (2557) วิจัยเรื่อง “ผลกระทบของระบบความปลอดภัยของข้อมูลที่มีต่อความได้เปรียบของข้อมูลของธุรกิจโรงพยาบาลเอกชนในประเทศไทย” ทั้งนี้งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาผลกระทบของระบบความปลอดภัยของข้อมูลที่มีต่อความได้เปรียบของข้อมูลของธุรกิจโรงพยาบาลเอกชนในประเทศไทย โดยทาการการเก็บรวบรวมข้อมูลจากผู้บริหารฝ่ายเทคโนโลยี

สารสนเทศธุรกิจโรงพยาบาลเอกชน จำนวน 207 คน และใช้แบบสอบถามเป็นเครื่องมือ สถิติที่ใช้ในการวิเคราะห์ข้อมูล ได้แก่ การวิเคราะห์สหสัมพันธ์พหุคูณ และการวิเคราะห์ความถดถอยแบบพหุคูณ

ผลการวิจัย พบว่า

1) ระบบความปลอดภัยของข้อมูล ด้านการคงสภาพข้อมูล (0.474) มีความสัมพันธ์และผลกระทบเชิงบวกต่อความได้เปรียบของข้อมูลโดยรวม เนื่องจาก การคงสภาพข้อมูลเป็นการสร้างความถูกต้องของข้อมูลในฐานข้อมูล ในส่วนของฐานข้อมูลเชิงสัมพันธ์มีการกำหนดกฎเกณฑ์ของข้อมูลเพื่อรักษาความถูกต้องของข้อมูลความสัมพันธ์ระหว่างข้อมูลต่างๆ และเป็นการป้องกันความเสียหายที่อาจเกิดกับฐานข้อมูลภายในองค์กรซึ่งสอดคล้องกับกับแนวคิดของ รุจกา สถิรางกูล (2553 : 1-16) กล่าวไว้ว่า ความคงสภาพของข้อมูล (Data Integrity) เป็นกระบวนการที่มีจุดประสงค์หลักคือป้องกันความผิดพลาดที่เกิดจากการเพิ่มข้อมูลลงในฐานข้อมูลรักษาความถูกต้องของข้อมูลเมื่อมีการเปลี่ยนแปลงข้อมูลในฐานข้อมูล ทาให้ข้อมูลต่าง ๆ ในฐานข้อมูลมีความถูกต้องตรงกัน และทาให้ระบบจัดการฐานข้อมูล สามารถตัดสินใจได้ว่า จะจัดการกับข้อมูล ณ ตำแหน่งต่าง ๆ ในฐานข้อมูลอย่างไร เช่น เลือกตำแหน่ง ในการเก็บข้อมูล และสอดคล้องกับแนวคิดของ จตุชัย แพงจันทร์ (2553 : 10) กล่าวไว้ว่า หลักการทางาน ที่สำคัญของความได้เปรียบของข้อมูล มี 3 ประการดังนี้ คือ การรักษาไว้ซึ่งความลับ การรักษาความลับในที่นี้ คือ การทำให้ข้อมูลหรือสารสนเทศต่างๆในระบบเทคโนโลยีสารสนเทศของบุคคลหรือองค์กร สามารถเปิดเผยหรือเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตแล้วเท่านั้น ในส่วนของความคงสภาพนั้นจะพูดถึงการทาให้ข้อมูลหรือสารสนเทศต่าง ๆ ที่จัดเก็บไว้ให้มีความน่าเชื่อถือมากที่สุด และในส่วนของ ความพร้อมใช้งาน เป็นการให้บริการข้อมูลที่พร้อมใช้งานตลอดเวลา มีการปรับปรุงข้อมูลอย่างสม่ำเสมอ สาหรับให้บริการกับผู้ที่ได้รับอนุญาตในการเข้าถึงข้อมูลนั้น

2) ระบบความปลอดภัยของข้อมูล ด้านการสร้างตารางข้อมูลเสมือน (0.149) มีความสัมพันธ์และผลกระทบเชิงบวกต่อความได้เปรียบของข้อมูลโดยรวม เนื่องจาก องค์กรสามารถกำหนดได้ว่าต้องการแสดงข้อมูลให้บุคคลทั้งภายในและภายนอกขององค์กรเข้าถึงข้อมูลได้ในระดับใด จึงสร้างตารางข้อมูลเสมือนเพื่อกำหนดการเข้าถึงข้อมูลของบุคคลในแต่ละระดับ วิธีการนี้จะช่วยให้ข้อมูลเป็นความลับและป้องการการแก้ไขข้อมูลจากบุคคลอื่น สิ่งนี้จะช่วยสร้างความน่าเชื่อถือให้กับองค์กรได้ ซึ่งสอดคล้องกับแนวคิดของ นวรัตน์ ธนะรุ่งรักษ์ (2550 : เว็บไซต์) กล่าวว่า ตารางข้อมูลเสมือน เป็นข้อมูลที่ถูกคัดลอกออกมาจากฐานข้อมูลเพื่อเป็นการป้องกันและรักษาความปลอดภัยในระบบการจัดการฐานข้อมูล ซึ่งตารางข้อมูลเสมือนจะช่วยรักษาความปลอดภัยในการปรับปรุงข้อมูลทั้งการเพิ่ม ลบ แก้ไขข้อมูลโดยไม่กระทบกับข้อมูลเดิม ทาให้มีความถูกต้องและสมบูรณ์ของข้อมูล เพราะข้อมูลถูกเรียกใช้ผ่านตารางเสมือน ไม่ได้ผ่านข้อมูลจริง จึงไม่ส่งผลกระทบใดๆ กับข้อมูลจริง และตารางเสมือนจะช่วยจากัดผู้ใช้ไม่ให้เข้าถึงข้อมูลจริงที่องค์กรไม่ต้องการเปิดเผยได้ และสอดคล้อง

กับงานวิจัยของ เชาวิวัฒน์ นันทพัฒน์สิริ (2555 : บทคัดย่อ) พบว่า การพัฒนาระบบบัญชีเสมือนและเงินเสมือน สาหรับเว็บไซต์ อี-คอมเมิร์ซ ช่วยเพิ่มความสะดวก ในการใช้งานเว็บไซต์พาณิชย์อิเล็กทรอนิกส์ (E-Commerce Website) สาหรับการขายสินค้า หรือสั่งซื้อสินค้า จะมีการบริการเพื่อเพิ่มความน่าเชื่อถือ ความมั่นใจ สาหรับการเก็บรักษาข้อมูลที่เป็นความลับของผู้ใช้บริการ โดยใช้การพิสูจน์ตัวตนด้วย ยูสเซอร์เนม (Username) พาสเวิร์ด (Password) สาหรับการเข้าใช้งานเว็บไซต์ และเมื่อมีการสั่งซื้อสินค้าผ่านเพย์เมนท์ เกตเวย์ (Payment Gateway) จะมีการยืนยันตัวตน ด้วยการล็อคอินเข้าสู่ระบบเพื่อยืนยันการชำระค่าสินค้า

ดังนั้น ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศธุรกิจโรงพยาบาลเอกชน ควรมีการส่งเสริมระบบความปลอดภัยของข้อมูลในด้านการคงสภาพข้อมูล และด้านการสร้างตารางข้อมูลเสมือน เพื่อสร้างความได้เปรียบของข้อมูลให้กับองค์กรและธุรกิจต่อไป

ชิษณุพงศ์ ธนูทอง (2557) วิจัยเรื่อง “การพัฒนาการรักษาความมั่นคงในระบบเครือข่ายหน่วยงานภาครัฐ” งานวิจัยนี้มุ่งเน้นทางด้านการวิเคราะห์การรักษาความมั่นคงในเครือข่ายคอมพิวเตอร์ของหน่วยงานภาครัฐโดยการศึกษาและวิเคราะห์การจัดการความมั่นคงของเทคโนโลยีสารสนเทศที่ใช้อยู่ในปัจจุบันและแนวโน้มการเกิดการจารกรรมบนเครือข่ายหน่วยงานภาครัฐของประเทศไทยเพื่อใช้ในการวิเคราะห์มาตรฐานความมั่นคงในเครือข่ายอย่างมีประสิทธิภาพ ผลจากการศึกษาจะนามาซึ่งแนวทางการพัฒนาระบบและแนวทางการบริหารจัดการทางเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐในด้านการรักษาความมั่นคงบนเครือข่ายให้มีประสิทธิภาพมากยิ่งขึ้น

งานวิจัยนี้ ได้สรุปแนวทางการแก้ไขปัญหาด้านการพัฒนาการรักษาความมั่นคงของระบบเครือข่ายหน่วยงานภาครัฐไว้ดังนี้

1. การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยการทางานในลักษณะรวมศูนย์นั่นคือการจัดตั้ง National Cyber Security Agency โดยมีหน้าที่รับผิดชอบดำเนินการดังต่อไปนี้

ก. รับผิดชอบในส่วนที่เกี่ยวข้องกับความมั่นคงปลอดภัยในโลกไซเบอร์ การให้ความรู้ความเข้าใจ คำปรึกษาและประสานงานกับผู้ที่รับผิดชอบงานด้านความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงานอื่น ๆ

ข. การดำเนินการเรื่องการตรวจสอบและประเมิน (Compliance and monitoring) การประเมินความเสี่ยงของระบบสารสนเทศ (ICT Risk Assessment) ในระดับประเทศ โดยมีกลไกประสานเชื่อมโยงกับคณะกรรมการนโยบายระดับชาติที่เกี่ยวข้อง ได้แก่ คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสารแห่งชาติ คณะกรรมการธุรกรรรมทางอิเล็กทรอนิกส์ สภาความมั่นคงแห่งชาติ เป็นต้น

ค. จัดฝึกอบรมให้แก่บุคลากรในหน่วยงานภาครัฐ

ง. รวมรวม incident และปัญหาของหน่วยงานต่าง ๆ ทั้งในระดับท้องถิ่น ภูมิภาคและส่วนกลาง

จ. หาวิธีการแก้ไข incident และปัญหาต่าง ๆ

ฉ. ส่งเสริมสร้างความตระหนักรู้แก่หน่วยงานต่าง ๆ ประชาชน และผู้เกี่ยวข้อง

ช. การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยทางไซเบอร์

ซ. การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์

ฌ. การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์

2. การดำเนินการของหน่วยงานภาครัฐโดยทั่วไป

ก. จัดทำนโยบายด้านความมั่นคงปลอดภัยโดยยึดหลักมาตรฐานนานาชาติ เพื่อจัดให้มีทิศทางและการสนับสนุนด้านความมั่นคงปลอดภัยของสารสนเทศที่จาเป็นตามกฎหมายและระเบียบข้อบังคับที่สอดคล้องเป็นแผนเดียวกัน โดยปัจจุบันได้ใช้ ISO 27001 ซึ่งได้มีการประยุกต์ใช้ในหลายประเทศ ประเทศไทยได้มีการบังคับใช้เช่นกัน แต่ในทางปฏิบัติการบังคับใช้ดังกล่าวยังไม่ประสบผลสาเร็จเนื่องจากยังขาดบทลงโทษและการผลักดันที่มีประสิทธิภาพ ดังนั้นการจัดทำนโยบายด้านความมั่นคงของระบบเครือข่ายจะต้องดำเนินการดังนี้

- ดำเนินการส่งเสริมให้ความรู้และจัดพิมพ์จาหน่ายมาตรฐาน ISO 27001 ให้เป็นภาษาไทยเพื่อใช้เป็นฐานในการกาหนดนโยบายและดำเนินการ

- จัดทำคู่มือการกำหนดนโยบายด้านความมั่นคงของระบบเครือข่ายในระดับหน่วยงาน

- จัดฝึกอบรมและสัมมนาเผยแพร่นโยบายและการดำเนินการตามนโยบาย ข.จัดทำแผนปฏิบัติงานของแต่ละหน่วยงาน โดยดำเนินการดังนี้

- จัดทำการประเมินความพร้อมของหน่วยงานภาครัฐด้านความมั่นคงของระบบเครือข่ายสารสนเทศ

- สร้างความตระหนักรู้ด้านความมั่นคงของระบบเครือข่าย โดยสร้างจิตสานึกให้คนในองค์กรตระหนักถึงอันตรายอันเกิดจากการละเลยด้าน Security แนะนามาตรฐาน ISO 27001 และให้หน่วยงานต่าง ๆ ปฏิบัติตามมาตรฐานดังกล่าวด้วย

- การพัฒนาบุคลากรและถ่ายทอดเทคโนโลยี

- การบริหารจัดการทางด้านเทคโนโลยีสารสนเทศที่ดี

- การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยทางไซเบอร์

- การเตรียมความพร้อมทั้งในส่วน Database, Software, Hardware, และ Network

Wajeb Gharibi and Maha Shaabi (2012) วิจัยเรื่อง “Cyber Threats in Social Networking Websites” พบว่า เครือข่ายทางสังคมเป็นโครงสร้างทางสังคมที่ประกอบด้วยบุคคล

หรือองค์กรที่มีความเกี่ยวพันกัน เช่น มิตรภาพ ความสนใจร่วมกันและการแลกเปลี่ยนทางการเงิน ความสัมพันธ์ระหว่างความเชื่อ ความรู้และศักดิ์ศรี

ทั้งนี้ภัยคุกคามในโลกไซเบอร์สามารถเกิดขึ้นได้ทั้งโดยไม่เจตนาและโดยเจตนา มีเป้าหมายหรือไม่มีเป้าหมายและอาจมาจากหลายแหล่ง รวมทั้งประเทศต่าง ๆ ที่ทำงานในหน่วยสืบราชการลับ ปัจจุบันสงครามข้อมูลมีอาชญากรที่เป็นทั้งแฮกเกอร์ ผู้สร้างไวรัส พนักงานที่ไม่พอใจในองค์กร และผู้รับเหมาที่ทำงานภายในองค์กร ผู้ดูแลเว็บไซต์เครือข่ายสังคม และเมื่อมีการสื่อสารหรือมีปฏิสัมพันธ์กับผู้อื่นทั่วโลกจึงต้องพัฒนาระบบการรักษาความปลอดภัยที่มีประสิทธิภาพสำหรับการส่งเสริมธุรกิจ

สำหรับงานวิจัยนี้ ผู้วิจัยจะตรวจสอบและศึกษาถึงภัยคุกคามไซเบอร์ในเว็บไซต์เครือข่ายสังคม ตั้งแต่ประวัติการจัดเก็บของเว็บไซต์โซเชียลออนไลน์ การแบ่งประเภท รวมถึงภัยคุกคามในโลกไซเบอร์ และจะนำมาสร้างแนวทางแนะนำกลยุทธ์การต่อต้านการคุกคาม นอกจากนี้ยังดูภาพแนวโน้มในอนาคตของเว็บไซต์ที่ได้รับความนิยมด้วยวิธีการศึกษาเอกสาร

จากการศึกษานำมาเสนอแนวทางการป้องกันความเสี่ยงและความเสี่ยงที่อาจเกิดขึ้นซึ่งที่จะช่วยให้ผู้ใช้เครือข่ายสังคมสามารถใช้งานได้โดยปฏิบัติดังนี้

- มีรหัสผ่านที่เข้มงวดมากในอีเมลและเว็บไซต์ทางสังคมอื่น ๆ ของคุณ
- เก็บข้อมูลในเว็บไซต์สังคมได้มากเท่าที่คุณสามารถทำได้
- เปลี่ยนรหัสผ่านของคุณเป็นประจำเพื่อให้ข้อมูลของคุณปลอดภัย แฮกเกอร์เข้าถึงได้ยาก
- ให้ข้อมูลให้น้อยที่สุด เวลาใช้เว็บไซต์และอินเทอร์เน็ต เนื่องจากมีการเผยแพร่ข้อมูลอินเทอร์เน็ตจะเพิ่มความเสี่ยงในการถูกล้วงข้อมูล
- อย่าไว้ใจผู้อื่นที่รู้จักทางออนไลน์และอย่าตอบคำถามพิเศษจากผู้ใช้หรือบริษัทที่ไม่รู้จัก
- ตรวจสอบนโยบายความเป็นส่วนตัวและป้องกันการเข้าถึงของอีเมลและลิงก์ที่ไม่รู้จัก
- ป้องกันการตรวจจับที่อยู่อีเมลโดยใช้เทคนิคสแปมเมอร์ให้เขียนอีเมล เช่น xyz@hotmail.com เป็น xyz ที่ Hotmail.com แทน

แม้ว่าเว็บไซต์เครือข่ายสังคมจะนำเสนอเทคโนโลยีและการติดต่อสื่อสารที่ทันสมัย แต่พวกเขาก็ยังต้องเผชิญกับความท้าทายใหม่ ๆ เกี่ยวกับประเด็นเรื่องความเป็นส่วนตัวและความปลอดภัย ในงานวิจัยนี้ผู้วิจัยเชื่อว่าความก้าวหน้าของเทคโนโลยีใหม่ ๆ ในเว็บไซต์ทั่วไปและสังคมจะนำความเสี่ยงด้านความปลอดภัยใหม่ ๆ ที่อาจเป็นโอกาสสำหรับผู้สร้างไวรัส และผู้บุกรุก

อย่างไรก็ตามผู้เชี่ยวชาญด้านความปลอดภัยข้อมูล เจ้าหน้าที่ของรัฐและหน่วยข่าวกรองอื่น ๆ ต้องพัฒนาเครื่องมือใหม่ ๆ เพื่อป้องกันและปรับตัวให้เข้ากับความเสี่ยงและภัยคุกคามใน

อนาคต นอกจากนี้ยังต้องพัฒนาให้ระบบสามารถจัดการกับข้อมูลจำนวนมากได้อย่างปลอดภัยในอินเทอร์เน็ตและในเว็บไซต์ทางสังคมด้วย

Jaeseung Hong, Jongwung Kim, Jeonghun Cho (2010) วิจัยเรื่อง “The Trend of the Security Research for the Insider Cyber Threat” พบว่า ความปลอดภัยภายในเป็นหนึ่งในประเด็นที่ใหญ่ที่สุดในด้านความปลอดภัยของเครือข่าย จากการสำรวจและวิเคราะห์ปัญหาของการศึกษาก่อนหน้านี้ ผู้วิจัยมุ่งค้นคว้าและรวบรวมข้อมูลเพื่อเสนอแนวทางที่มีประสิทธิภาพ สำหรับการวิจัยที่ผ่านมาพบว่า มีประมาณ 90% ของเหตุการณ์การรั่วไหลของข้อมูลที่มาจากการกระทำโดยคนภายในองค์กรซึ่นับว่าเป็นปัญหาร้ายแรงกว่าการโจมตีจากภายนอก

จากเหตุการณ์การรั่วไหลของข้อมูลทำให้องค์กรหรือบริษัท ไม่ใช่เพียงสูญเสียข้อมูลเพียงอย่างเดียว แต่ยังส่งผลกระทบต่อภาพอย่างมาก ดังนั้นเพื่อป้องกันความสูญเสียทางเศรษฐกิจและความเสียหายในอนาคต องค์กรจำเป็นต้องมีการวิจัยและพัฒนาเพื่อหาทางออกที่มีประสิทธิภาพ อย่างไรก็ตาม งานวิจัยนี้พบว่าผลของการแก้ปัญหาด้านความปลอดภัยภายในยังไม่เป็นที่น่าพอใจ แต่องค์กรส่วนใหญ่กลับไปเน้นการรักษาความปลอดภัยภายนอก

นอกจากนี้ปัญหาใหญ่ที่สุดของการแก้ไขปัญหาด้านความปลอดภัยภายใน คือ การพัฒนาข้อมูลภายในที่มีข้อมูลเกี่ยวกับองค์กรและเข้าใจโครงสร้างขององค์กรภายในให้มีความปลอดภัยและเสริมสร้างความจงรักภักดีต่อองค์กร เพราะคนในองค์กรไม่เพียงแต่รู้ว่าข้อมูลที่ต้องการคืออะไร แต่ยังมีความรู้เพียงพอเกี่ยวกับระบบรักษาความปลอดภัยภายในอีกด้วย และเมื่อคนภายในคนหนึ่งมีเจตนาที่ประสงค์ร้ายในการรับข้อมูลที่เป็นความลับจึงไม่ใช่เรื่องยากที่จะกระทำ ทั้งนี้ถือเป็นความท้าทายและเป็นการยากที่จะปกป้องทรัพยากรภายในจากภายในโดยใช้เทคนิคและเทคนิคที่ยอดเยี่ยม โดยเฉพาะอย่างยิ่งเป็นไปไม่ได้ที่จะป้องกันเหตุการณ์ความปลอดภัยภายในโดยผู้จัดการระบบ เนื่องจากผู้จัดการระบบจัดการระบบทั้งหมดรวมทั้งระบบรักษาความปลอดภัยภายใน หากมีเจตนาร้ายเจตนาร้ายมันเป็นภัยคุกคามภายในที่ใหญ่ที่สุด

จากการศึกษา ผู้วิจัยเสนอว่า เพื่อป้องกันภัยคุกคามจากภายใน องค์กรจำเป็นต้องมีระบบรักษาความปลอดภัยซึ่งไม่เพียงแต่จะปกป้องทรัพยากรภายในเท่านั้น แต่ยังต้องเข้าใจถึงรูปแบบพฤติกรรมหรือความมุ่งหมายภายในของบริษัท นอกจากนี้หากเกิดเหตุการณ์ที่คุกคามความปลอดภัยภายในเกิดขึ้นระบบรักษาความปลอดภัยจะต้องเข้าใจสาเหตุและติดตามผู้โจมตี รวมทั้งให้ผู้จัดการระบบโดเมนจัดการและต้องให้แบ่งการใช้งานระบบตามงานที่เกี่ยวข้องและธุรกิจโดยต้องมีการพึ่งพาระหว่างกันเพื่อป้องกันไม่ให้บุคคลนั้นได้รับข้อมูลและเข้าถึงระบบเป็นจำนวนมากเกินไป

สาเหตุที่คนในองค์กรคุกคามความปลอดภัยของระบบมาจากการเป็นสายลับ หรือเป็นบุคคลที่ไม่พอใจด้วยเหตุผลหลายประการ เนื่องจากการจ้างงานค่าแรงและการส่งเสริมการขาย เป็นต้น ยิ่งความไม่พอใจเหล่านี้เติบโตขึ้นเท่าไหร่ก็ยิ่งภายในมากขึ้นจะมีเจตนาที่เป็นอันตรายมากขึ้น

ดังนั้นแม้ว่าการสร้างระบบรักษาความปลอดภัยภายในที่มีประสิทธิภาพเป็นสิ่งสำคัญ แต่ทางองค์กรจะต้องมีระบบการประเมินผลที่ดีและการชดเชยที่เหมาะสมตามความสามารถทางธุรกิจให้แก่คนในองค์กร มีการสร้างความสัมพันธ์ระหว่างกันและกันระหว่างองค์กรภายในและองค์กรเพื่อลดความเป็นไปได้ที่ภัยคุกคามภายในให้ได้มากที่สุด

Axel Tanner (2015) วิจัยเรื่อง “Gaining an Edge in Cyberspace with Advanced Situational Awareness” พบว่า องค์กรภาคธุรกิจมีการพึ่งพาระบบคอมพิวเตอร์ที่มีนำมาใช้วางระบบต้องเผชิญกับวิกฤตการคุกคามทางไซเบอร์ องค์กรต่าง ๆ มีภารกิจสำคัญในการพัฒนาระบบรักษาความปลอดภัยในโลกไซเบอร์โดยใช้แนวคิดการตระหนักรู้ในสถานการณ์ (situational awareness: SA) มาประยุกต์ใช้ทำให้ต้องมีการวิเคราะห์สถานการณ์ มีการจำลองสถานการณ์ขั้นสูงโดยสร้างเป็นระบบ OODA (สังเกต (observe) ปรับทิศทาง (orient) ตัดสินใจ (decide) การลงมือทำ (act)) เพื่อสร้างทำแผนรองรับสถานการณ์ ทำความรู้ความเข้าใจในแบบเรียลไทม์ใกล้เคียงกับสภาพแวดล้อมขององค์กร และภัยคุกคามทางไซเบอร์จะส่งผลกระทบทางธุรกิจที่อาจเกิดขึ้น

ทั้งนี้ภัยคุกคามในโลกไซเบอร์เป็นภัยคุกคามระดับชาติซึ่งปัจจุบันมีการพึ่งพาระบบไซเบอร์ในการควบคุมระบบระบบสาธารณูปโภค จากเหตุการณ์คุกคามความปลอดภัยในปี 2007 มีธนาคารเอสโตเนีย รัฐสภา กระทรวงหนังสือพิมพ์และสถานีโทรทัศน์ ทั้งนี้ยังเกิดวิกฤตปี 2013 เหตุการณ์ Red October นอกจากนี้บริษัทอเมซอนและอีเบย์ (Amazon and eBay) ยอมลงทุนนับล้านดอลล่าห์เมื่อระบบบริการลูกค้าเกิดเหตุขัดข้อง ซึ่งสาเหตุอาจจะมาจากการคุกคามทางไซเบอร์ ขณะที่ในระดับโลก ทุกประเทศพยายามมีมาตรการควบคุมและรักษาความปลอดภัยใต้โลกไซเบอร์ด้วยการวางกลยุทธ์การต่อต้านภัยคุกคามในโลกไซเบอร์ ดังนั้นการขาดการประเมินสถานการณ์ทางไซเบอร์เป็นปัญหาสำคัญในระบบสารสนเทศ องค์กรทางธุรกิจจำนวนมากมองว่า ระบบรักษาความปลอดภัยในโลกไซเบอร์มีความสำคัญแต่ขาดการประเมินสถานการณ์ทางไซเบอร์จึงทำให้ขาดมาตรการรุกในการป้องกันปัญหาภัยคุกคามในโลกไซเบอร์

การตระหนักรู้ในสถานการณ์เป็นขั้นตอนพื้นฐานของทหารในการรักษาความปลอดภัยโดยนำมาประเมินสถานการณ์ในโลกไซเบอร์ในระบบของกองทัพ ขณะที่ในองค์กรภาคธุรกิจและเอกชาถือเป็นสิ่งแปลกใหม่และเพิ่มต้นทุนให้กับองค์กร ทั้งในด้านบุคคลากร เงินทุน รวมทั้งระบบปฏิบัติการ โดยการวิเคราะห์ระบบสารสนเทศขององค์กรธุรกิจที่มีการให้บริการนับพันและมีกลุ่มลูกค้านับล้านคนในการเข้าถึงการบริการ รวมทั้งการเผชิญกับภัยคุกคาม อาทิ มัลแวร์ และการถูกขโมยข้อมูลที่สำคัญ การคอร์รัปชั่นในบริษัท การโจมตีเหล่านี้อาจจะใช้วิธีการให้ระบบไม่ทำงาน ระบบซอฟแวร์ทำงานผิดพลาด การปฏิเสธรับโค้ดคำสั่ง ซึ่งสถานการณ์เหล่านี้เป็นสถานการณ์ที่

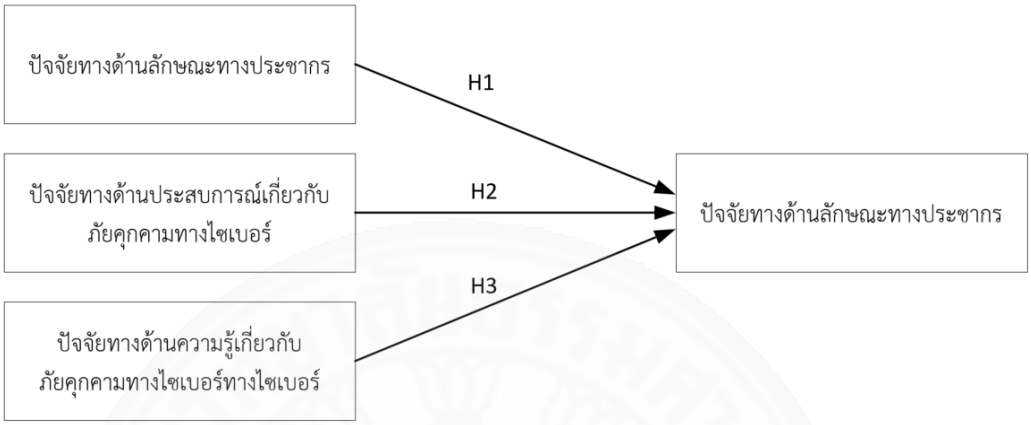
เกิดขึ้นในปัจจุบัน ดังนั้นบริษัท หลายแห่งที่ต้องการตรวจตราและป้องกันการโจมตีระบบไซเบอร์ขององค์กรเพื่อลดผลกระทบทางธุรกิจและต้องการให้ดำเนินธุรกิจได้อย่างต่อเนื่องและปลอดภัย

Ram Herkanaidu, Steven Furnell และ Maria Papadaki (2017) วิจัยเรื่อง “Online Risk Awareness and Exposure of Young People in Thailand” โดยได้ศึกษานักเรียนในโรงเรียนในจังหวัดหนองคายในภาคอีสานของประเทศไทยจำนวน 206 คน เกี่ยวกับการมีปฏิสัมพันธ์ทางออนไลน์ของพวกเขา ศึกษาสถานที่เชื่อมต่อ วัตถุประสงค์ในการใช้อินเทอร์เน็ตความถี่และสอบถามถึงประสบการณ์ในการใช้อินเทอร์เน็ตในแง่ลบ จากผลการวิจัยพบว่า กลุ่มตัวอย่างมีอายุระหว่าง 12 -18 ปี โดยมาจาก 2 โรงเรียน และมีครูเข้าร่วมในการวิจัยครั้งนี้จำนวน 2 คน ซึ่งเป็นผู้คอยช่วยจัดการและดูแลกลุ่มตัวอย่าง ทั้งนี้อยู่ในอำเภอเมือง จำนวน 83 คน และอยู่ในอำเภอโพนพิสัย จำนวน 120 คน และพบว่า ครอบครัวส่วนใหญ่เป็นชาวนาและปศุสัตว์ ทำงานตามร้านค้าและพนักงานในร้านอาหาร เด็กหลายคนหลังจากกลับจากโรงเรียนก็จะทำไปทำงานต่อด้วย ได้แก่ การทำงานในร้านอาหารของครอบครัวในตอนเย็น

ผลการวิจัยยังพบว่า 90% ของผู้ตอบแบบสอบถามเป็นผู้ใช้สมาร์ตโฟนที่ใช้แอปพลิเคชั่นในโลกออนไลน์ในการปฏิสัมพันธ์กันผ่าน Facebook และ Facebook Messenger ซึ่งเป็นเครือข่ายทางสังคมที่โดดเด่นและแพลตฟอร์มการรับส่งข้อความโต้ตอบแบบทันที ทั้งนี้พบว่า มีนักเรียนจำนวน 2 ใน 3 ของนักเรียนทั้งหมดรู้สึกไม่พอใจจากการใช้สื่อออนไลน์ โดยพบว่า มีผู้ที่ถูกกลั่นแกล้งในโลกออนไลน์ 71% และมีผู้ที่เคยกลั่นแกล้งผู้อื่นจำนวน 44% โดยมีเนื้อหาที่เกี่ยวกับการพูดคุยวิพากษ์วิจารณ์เกี่ยวกับลักษณะตัวตนของแต่ละคนซึ่งเป็นเรื่องที่อ่อนไหวและอันตรายมาก ส่วนหนึ่งมาจากพฤติกรรมที่มีความเสี่ยง ได้แก่ การรับเพื่อนที่ไม่รู้จัก แต่เป็นเพื่อนของเพื่อนในบัญชีเพื่อนมีจำนวน 52% ของกลุ่มตัวอย่างทั้งหมด ซึ่งเป็นเพศหญิง และจำนวน 58% เป็นเพศชายมีจำนวน 46% ทั้งนี้ยังพบว่า มีการพูดคุยหรือส่งภาพที่เกี่ยวกับเพศ ส่งข้อความที่สร้างความเกลียดชัง โดย 1 ใน 5 ยังส่งรูปถ่ายหรือวิดีโอให้คนแปลกหน้าดู รวมทั้งใช้รหัสผ่านคนอื่น และยังพบว่า ผู้ปกครองและครูเป็นผู้ช่วยไกล่เกลี่ยและคอยช่วยเหลือเวลาที่นักเรียนถูกกลั่นแกล้งในโลกออนไลน์ และผู้ปกครองและครูเป็นผู้สร้างความตระหนักถึงพฤติกรรมเสี่ยงของการใช้สื่อออนไลน์ จากการศึกษานี้ ผู้วิจัยเสนอว่า ควรจะมีการวางหลักสูตรการศึกษาและสร้างความตระหนักถึงอันตรายของการกลั่นแกล้งในโลกออนไลน์ในกลุ่มเยาวชนต่อไป

2.8 กรอบแนวคิดของการวิจัย

กรอบแนวคิดของการวิจัย สามารถแสดงได้ดังแผนภาพต่อไปนี้



ภาพที่ 2.2 กรอบแนวคิดของการวิจัย

บทที่ 3

ระเบียบวิธีวิจัย

การศึกษาเรื่อง “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร” การวิจัยนี้เป็นการวิจัยเชิงปริมาณ (Quantitative Research) ด้วยการวิจัยเชิงสำรวจ (Survey Research) ผู้วิจัยรวบรวมข้อมูลจากการทบทวนวรรณกรรม บทความวิชาการหนังสือและเอกสารที่มีความเกี่ยวข้องเพื่อให้การดำเนินวิจัยนำไปสู่วัตถุประสงค์ที่ตั้งไว้ โดยผู้วิจัยได้ดำเนินการศึกษาวิจัยตามขั้นตอน ดังนี้

3.1 ประชากรและกลุ่มตัวอย่าง

3.2 เครื่องมือที่ใช้ในการวิจัย

3.3 ความเที่ยงตรงและความน่าเชื่อถือ

3.4 การเก็บรวบรวมข้อมูล

3.5 การวิเคราะห์ข้อมูล

3.1 ประชากรและกลุ่มตัวอย่าง

ประชากรและกลุ่มตัวอย่างของงานวิจัยหัวข้อ “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร” การกำหนดกลุ่มประชากรและกลุ่มตัวอย่างที่ใช้ในการศึกษาวิจัย โดยมีรายละเอียดดังต่อไปนี้

3.1.1 ประชากรที่นำมาศึกษาในงานครั้งนี้

ประชากร คือ ผู้ใช้อินเทอร์เน็ตที่มีอายุ 15 ปีขึ้นไปและอยู่ในเขตกรุงเทพมหานคร

3.1.2 การกำหนดขนาดกลุ่มตัวอย่าง

ขนาดตัวอย่างในการวิจัยครั้งนี้ ได้คำนวณจากสูตรของ Cochran (1977) กรณีที่ไม่ทราบขนาดประชากร ดังนี้

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

เมื่อ n แทน ขนาดตัวอย่าง

P แทน สัดส่วนของประชากรที่ผู้วิจัยกำลังสุ่ม (ในที่นี้กำหนดไว้ที่ 0.50)

Z แทน ค่าสถิติ Z ที่ระดับความเชื่อมั่นร้อยละ 95 (มีค่าเท่ากับ 1.96)

e แทน ค่าความคลาดเคลื่อนจากการสุ่มตัวอย่างที่ยอมให้เกิดขึ้นได้
(ในที่นี้กำหนดไว้ที่ร้อยละ 5 หรือ 0.05)

แทนค่าในสูตร

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

$$= 384.16$$

จากการคำนวณจะได้ขนาดตัวอย่าง 384 คน แต่ในการวิจัยครั้งนี้จะใช้ขนาดตัวอย่าง 400 คน

3.1.3 วิธีการสุ่มตัวอย่าง

วิธีการสุ่มตัวอย่างได้ใช้การสุ่มตัวอย่างแบบไม่ใช่หลักความน่าจะเป็น (Non-Probability Sampling) ด้วยวิธีการสุ่มตัวอย่างแบบบังเอิญ (Accidental Sampling) และวิธีการสุ่มตัวอย่างแบบสโนว์บอล (Snowball Sampling)

3.1.3.1 การสุ่มตัวอย่างโดยไม่ใช้ความน่าจะเป็น (Non-probability sampling)

เป็นการเลือกตัวอย่างโดยไม่คำนึงว่าตัวอย่างแต่ละหน่วยมีโอกาสถูกเลือกมากน้อยเท่าไร

3.1.3.2 การเลือกกลุ่มตัวอย่างแบบบังเอิญ (Accidental sampling)

เป็นการเลือกกลุ่ม ตัวอย่างเพื่อให้ได้จำนวนตามต้องการโดยไม่มีหลักเกณฑ์ กลุ่มตัวอย่างจะเป็นใครก็ได้ที่สามารถให้ข้อมูล

3.1.3.3 วิธีการสุ่มตัวอย่างแบบสโนว์บอล (Snowball Sampling)

เป็นการบอกต่อของผู้ตอบแบบสอบถามจนกว่าจะได้จำนวนที่ต้องการ

3.2 เครื่องมือที่ใช้ในการวิจัย

งานวิจัยเรื่อง “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร”ครั้งนี้จะใช้แบบสอบถาม (Questionnaire) ในการเก็บรวบรวมข้อมูล ข้อคิดเห็นของกลุ่มตัวอย่าง โดยจะสอบถามกลุ่มตัวอย่างแบบคำถามลักษณะปลายปิด (Close end questionnaire) โดยให้กลุ่มตัวอย่างเป็นผู้ตอบแบบสอบถามด้วยตนเอง (Self-Administered) โดยประกอบไปด้วยข้อคำถาม จำนวน 4 ตอน ดังนี้ ในเก็บรวบรวมข้อมูล

ตอนที่ 1 ลักษณะทางประชากร ประกอบไปด้วยข้อคำถาม 4 ข้อ ได้แก่

1. เพศ แบ่งออกเป็น 2 กลุ่ม คือ
    1. ชาย
    2. หญิง
2. อายุ แบ่งออกเป็น 6 กลุ่ม คือ
    1. ไม่เกิน 20 ปี
    2. 21-30 ปี
    3. 31-40 ปี
    4. 41-50 ปี
    5. 51-60 ปี
    6. 61 ปีขึ้นไป
3. ระดับการศึกษาสูงสุด แบ่งออกเป็น 4 กลุ่ม คือ
    1. ต่ำกว่าปริญญาตรี
    2. ปริญญาตรี
    3. ปริญญาโท
    4. สูงกว่าปริญญาโท
4. รายได้ส่วนตัวต่อเดือน แบ่งออกเป็น 5 กลุ่ม คือ
    1. ไม่เกิน 15,000 บาท
    2. 15,001-30,000 บาท
    3. 30,001-45,000 บาท
    4. 45,001-60,000 บาท
    5. 60,001 บาทขึ้นไป

ตอนที่ 2 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ ประกอบไปด้วยข้อคำถามแบบตอบได้มากกว่าหนึ่งคำตอบ (Multiple Responses) จำนวน 10 ข้อ ได้แก่

1. ท่านเคยได้รับผลกระทบจากไวรัสทำให้ไฟล์หรือโปรแกรมคอมพิวเตอร์เกิดความเสียหาย
2. ท่านได้รับการก่อกวนในระบบเครือข่ายทำให้ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ
3. ท่านติดตั้งโปรแกรมที่คิดว่าปลอดภัย แต่มีโปรแกรมอันตรายแฝงตัวมา
4. ท่านถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของได้โดยท่านไม่รู้ตัว
5. ท่านถูกแอบดูพฤติกรรมหรือบันทึกการเข้าใช้งานคอมพิวเตอร์

6. ท่านโดนขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน

7. ท่านไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นจะได้รับข้อความ “เรียกค่าไถ่”

8. ท่านถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าระบบ

9. ท่านเคยได้รับจดหมายอิเล็กทรอนิกส์หลอกลวง

10. ท่านเคยได้รับโฆษณาที่ไม่พึงประสงค์จะได้รับ

เกณฑ์การให้คะแนน คือ

มีประสบการณ์ = 1

ไม่มีประสบการณ์ = 0

หลังจากนั้นจะรวมคะแนนทั้ง 10 ข้อ เป็นคะแนนรวมประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำไปใช้ในการทดสอบสมมติฐาน

อย่างไรก็ตาม ได้นำคะแนนรวมนั้นมาแบ่งระดับประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์เป็น 3 ระดับ ดังนี้

0-3 คะแนน หมายถึง มีประสบการณ์น้อย

4-6 คะแนน หมายถึง มีประสบการณ์ปานกลาง

7-10 คะแนน หมายถึง มีประสบการณ์มาก

ตอนที่ 3 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ ประกอบไปด้วยข้อคำถาม จำนวน 10 ข้อ ได้แก่

1. การเข้าเว็บไซต์ https มีความปลอดภัยมากกว่า http

2. การเปิดเผยระบุตำแหน่งตัวตนบนเครือข่ายสังคมออนไลน์สาธารณะที่มีผู้ใช้ทั่วไปมีความปลอดภัย

3. การให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะไม่มีความเสี่ยง

4. การเข้าใช้เครือข่ายไร้สายสาธารณะมีความเสี่ยงต่อการทำธุรกรรมออนไลน์

5. การติดตามข่าวสารรูปแบบโจมตีทางไซเบอร์สามารถป้องกันความเสียหายที่จะเกิดขึ้นได้

6. การตั้งรหัสผ่าน (Password) ควรตั้งให้ปนกันทั้งตัวอักษรใหญ่-เล็ก ตัวเลข สัญลักษณ์พิเศษ และยาวอย่างน้อย 8 ตัวอักษร

7. การตั้งรหัสผ่าน (Password) สำหรับเครื่องมือและเว็บไซต์ต่าง ๆ ควรจะเหมือนกัน

8. การใช้โปรแกรมถูกลิขสิทธิ์มีความเสี่ยงพอ ๆ กับโปรแกรมที่ไม่ถูกลิขสิทธิ์

9. การสำรองข้อมูลและตั้งรหัสเข้าใช้ทำให้มีความปลอดภัยมากขึ้น

10. การโหลดแอปพลิเคชันที่มีชื่อเหมือนกับโปรแกรมที่มีชื่อเสียงจะมีความปลอดภัย

ข้อความที่ถูก หรือต้องตอบว่า ใช่ จึงได้ 1 คะแนน คือ ข้อ 1 4 5 6 9

ข้อความที่ผิด หรือต้องตอบว่า ไม่ใช่ จึงได้ 1 คะแนน คือ ข้อ 2 3 7 8 10

ในกรณีที่ตอบว่า ไม่แน่ใจ จะไม่ได้คะแนนในทุกข้อ

หลังจากนั้นจะนำคะแนนที่ได้ ซึ่งตอบถูกตามเฉลยข้างต้น มารวมเป็นคะแนนความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อใช้ในการทดสอบสมมติฐาน

อย่างไรก็ตาม ได้นำคะแนนรวมนั้นมาแบ่งระดับความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เป็น 3 ระดับ ดังนี้

0-3 คะแนน หมายถึง มีความรู้น้อย

4-6 คะแนน หมายถึง มีความรู้ปานกลาง

7-10 คะแนน หมายถึง มีความรู้มาก

ตอนที่ 4 ความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ ประกอบไปด้วยข้อคำถามแบบมาตราส่วนประมาณค่า (Rating Scale) ทั้งหมด 6 ด้าน ด้านละ 3 ข้อ จำนวนรวม 18 ข้อ ได้แก่

1. ความปลอดภัย (Security)

1.1 ควรหาทางป้องกันการถูกโปรแกรมคอมพิวเตอร์ที่ไม่พึงประสงค์ทำความเสียหายข้อมูลในระบบ

1.2 ควรหาทางป้องกันการถูกหลอกให้กรอกข้อมูลส่วนตัวทางเว็บไซต์ปลอม

1.3 ควรหาทางป้องกันการถูกลักลอบเจาะเข้าสู่ระบบเพื่ออ่านหรือทำลายข้อมูล

2. การยั่วโมโห (Flaming)

2.1 ไม่ควรมีการกล่าวถึงผู้อื่นให้ได้รับความอับอายหรือเสื่อมเสียชื่อเสียงผ่านทางไซเบอร์

2.2 ไม่ควรมีการใช้ถ้อยคำหรือข้อความที่หยาบคายด่าว่าผู้อื่นผ่านทางไซเบอร์

2.3 ไม่ควรมีการล้อเลียนรูปร่างหน้าตาของผู้อื่นผ่านทางไซเบอร์

3. การข่มขู่ใส่ร้าย (Harassment)

3.1 ไม่ควรมีการใส่ร้ายผู้อื่นให้บุคคลที่สามเกลียดชังผ่านทางไซเบอร์

3.2 ไม่ควรมีการนำภาพหรือคลิปวิดีโอที่เสื่อมเสียของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์

3.3 ไม่ควรมีการเผยแพร่ข่าวลือในทางลบของผู้อื่นผ่านทางไซเบอร์

4. การแอบอ้าง (Masquerading)

4.1 ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นในการสนทนาผ่านทางไซเบอร์

4.2 ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อผลประโยชน์ให้ตนเองผ่านทางไซเบอร์

4.3 ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อให้ร้ายบุคคลที่สามผ่านทางไซเบอร์

5. การเผยแพร่ออกนอกกลุ่ม (Outing)

5.1 ไม่ควรมีการนำชื่อพ่อแม่หรือญาติพี่น้องของผู้อื่นไปเปิดเผยผ่านทางไซเบอร์โดยไม่ได้รับ

อนุญาต

5.2 ไม่ควรมีการนำที่อยู่ของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต

5.3 ไม่ควรมีการนำเบอร์โทรศัพท์ของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต

6. การกีดกัน (Exclusion)

6.1 ไม่ควรมีการบล็อกข้อความสนทนาทางไซเบอร์ของบุคคลที่ไม่ชอบ

6.2 ไม่ควรมีการลบรายชื่อบุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางไซเบอร์

6.3 ไม่ควรมีการกดดันให้บุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางไซเบอร์

เกณฑ์การให้คะแนน คือ

เห็นด้วยอย่างยิ่ง	=	5
เห็นด้วย	=	4
ไม่แน่ใจ	=	3
ไม่เห็นด้วย	=	2
ไม่เห็นด้วยอย่างยิ่ง	=	1

หลังจากนั้นจะเฉลี่ยคะแนนทั้ง 18 ข้อ เป็นคะแนนเฉลี่ยความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำไปใช้ในการทดสอบสมมติฐาน

อย่างไรก็ตาม ได้นำคะแนนเฉลี่ยนั้นมาแบ่งระดับความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์เป็น 5 ระดับ ดังนี้

คะแนนเฉลี่ย	1.00-1.49	หมายถึง	ตระหนักน้อยที่สุด
คะแนนเฉลี่ย	1.50-2.49	หมายถึง	ตระหนักน้อย
คะแนนเฉลี่ย	2.50-3.49	หมายถึง	ตระหนักปานกลาง
คะแนนเฉลี่ย	3.50-4.49	หมายถึง	ตระหนักมาก
คะแนนเฉลี่ย	4.50-5.00	หมายถึง	ตระหนักมากที่สุด

3.3 ความเที่ยงตรงและความน่าเชื่อถือ

แบบสอบถามที่ผู้วิจัยสร้างขึ้นจะนำมาทดสอบความเที่ยงตรงและความน่าเชื่อถือ ดังนี้

3.3.1 ความเที่ยงตรง (Validity) ผู้วิจัยได้นำร่างแบบสอบถามที่สร้างขึ้นให้อาจารย์ที่ปรึกษาตรวจสอบความเที่ยงตรงเชิงเนื้อหา และนำข้อคิดเห็นของอาจารย์ที่ปรึกษามาปรับแก้ ก่อนนำไปทดสอบความน่าเชื่อถือและเก็บข้อมูลจริงต่อไป

3.3.2 ความน่าเชื่อถือ (Reliability) ผู้วิจัยได้เก็บแบบสอบถามมาจำนวน 30 ชุด และนำมาหาค่าสัมประสิทธิ์อัลฟาของครอนบาช (Cronbach's Alpha Coefficient) ซึ่งพบว่าแบบสอบถามตอนความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ ได้ค่าอัลฟา (α) เท่ากับ .880 ซึ่งไม่ต่ำกว่า 0.70 จึงจะถือว่า แบบสอบถามมีความน่าเชื่อถือ สามารถนำไปใช้ในการเก็บข้อมูลจริงได้

3.4 การเก็บรวบรวมข้อมูล

งานวิจัยหัวข้อ "ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร" ได้ศึกษาขั้นตอนในการเก็บรวบรวมข้อมูล ดังต่อไปนี้

3.4.1 ข้อมูลปฐมภูมิ (Primary Data) คือ ข้อมูลที่ได้จากแบบสอบถามแบบออนไลน์ (Online Questionnaire) ถึงปัจจัย 4 ด้าน ได้แก่ ด้านลักษณะทางประชากร ด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ ด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ ด้านความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ โดยเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง ของประชากรผู้ใช้อินเทอร์เน็ตในเขตกรุงเทพมหานคร โดยมี

3.4.2 ข้อมูลทุติยภูมิ (Secondary Data) คือ ข้อมูลที่ได้จากแหล่งที่รวบรวมข้อมูลไว้แล้ว หรือหน่วยงานที่มีการบันทึกทำการเก็บรวบรวมสถิติต่าง ๆ หรือเรียบเรียงไว้เรียบร้อยแล้ว สามารถนำข้อมูลเหล่านั้นมาใช้อ้างอิงได้เลย ผู้วิจัยได้ทำการเก็บรวบรวมจากการทบทวนวรรณกรรม แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง รวมทั้งการสืบค้นทางอินเทอร์เน็ตจากเว็บไซต์ที่เกี่ยวข้อง กับปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ เพื่อเป็นข้อมูลประกอบการวิเคราะห์งานวิจัย

3.5 การวิเคราะห์ข้อมูล

การวิจัยนี้ จะใช้สถิติการวิเคราะห์ข้อมูลที่ได้รับจากการเก็บรวบรวมข้อมูลที่ผู้วิจัยได้จากกลุ่มตัวอย่างของงานวิจัย “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร” โดยจะนำข้อมูลที่ได้มาวิเคราะห์ประมวลผลทางสถิติ และสามารถแบ่งการวิเคราะห์ข้อมูลได้ 2 ประเภท ดังต่อไปนี้

3.5.1 สถิติเชิงพรรณนา (Descriptive Statistics) คือ การนำข้อมูลที่เก็บได้มาจากกลุ่มตัวอย่างมาแสดงรายละเอียดของข้อมูลเพื่อที่จะอธิบายค่าของข้อมูล โดยแจกแจงความถี่ (Frequency) แบบค่าร้อยละ (Percentage) แบบคำนวนค่าเฉลี่ย (Mean) และแบบค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) ในการพรรณนาข้อมูลของกลุ่มตัวอย่างเกี่ยวกับลักษณะทางประชากร ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ และความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์

3.5.2 สถิติเชิงอนุมาน (Inferential Statistics) คือ การนำข้อมูลที่ได้มาจากกลุ่มตัวอย่าง มาทดสอบหาความสัมพันธ์ระหว่างตัวแปรอิสระ (Independent Variables) กับตัวแปรตาม(Dependent Variables) โดยใช้ Independent Samples T Test / Oneway ANOVA และ Pearson Correlation ในการทดสอบสมมติฐาน

บทที่ 4

ผลการวิจัย

การวิจัย เรื่อง “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร” เป็นการวิจัยเชิงปริมาณ (Quantities Research) โดยใช้แบบสอบถาม (Questionnaires) เป็นเครื่องมือในการเก็บรวบรวมข้อมูล ทำการแจกแบบสอบถามแก่ผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร ผู้วิจัยได้ทำการวิเคราะห์ข้อมูล และได้เสนอการวิเคราะห์ข้อมูลผลการวิจัย โดยแบ่งเป็น 4 ตอน ดังต่อไปนี้

4.1 ลักษณะทางประชากร

4.2 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

4.3 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

4.4 ความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์

4.5 การทดสอบสมมติฐาน

สัญลักษณ์ที่ใช้ในการวิเคราะห์ข้อมูล

X	หมายถึง ค่าเฉลี่ยเลขคณิต (Mean)
S.D.	หมายถึงค่าเฉลี่ยส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation)
SS	หมายถึง ผลบวกกำลังสอง (Sum of Squares)
Df	หมายถึงองศาอิสระ (degree of freedom)
MS	หมายถึง ผลบวกกำลังสองเฉลี่ย (Sum of Squares)
F	หมายถึงค่าสถิติทดสอบF(F-value)
p	หมายถึงค่าความน่าจะเป็นทางสถิติ (p-value)
R	หมายถึงค่าสัมประสิทธิ์สหสัมพันธ์ (Correlation Coefficient)
R2	หมายถึงค่าสัมประสิทธิ์การตัดสินใจ (Coefficient of Determination)
AdjR2	หมายถึงค่า R2 ที่ปรับแก้ (Adjusted R Square)
B	หมายถึงค่าสัมประสิทธิ์ความถดถอย
S.E.	หมายถึง ค่าความคลาดเคลื่อนมาตรฐาน (Standard Error)
β	หมายถึงสัมประสิทธิ์ความถดถอยเชิงส่วน (Partial Regression Coefficient)

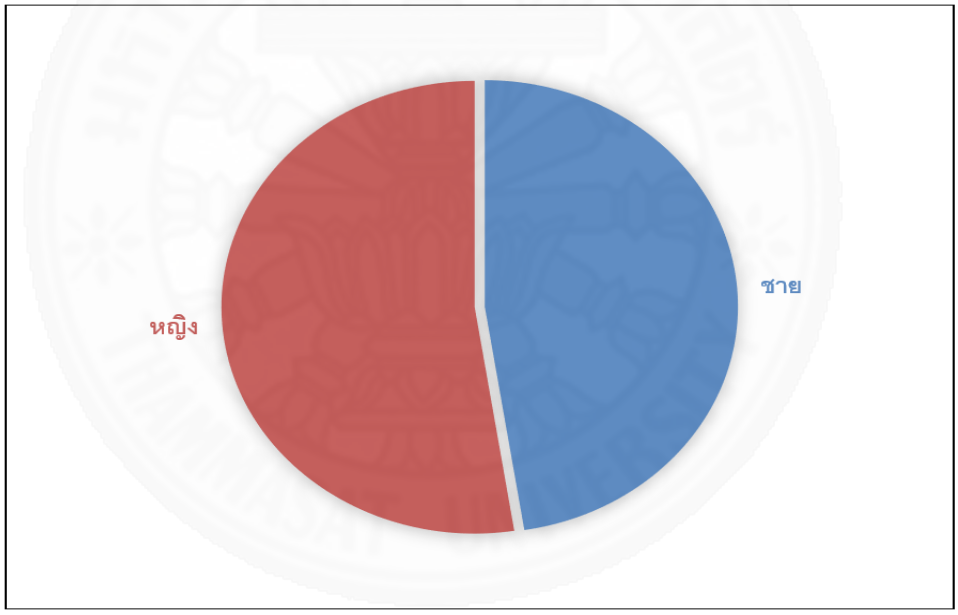
t หมายถึงค่าสถิติ (t-value)

Sig หมายถึง ระดับนัยสำคัญ (Level of significance)

4.1 ข้อมูลลักษณะทางประชากร

ตารางที่ 4.1 *จำนวนและค่าร้อยละของผู้ตอบแบบสอบถาม จำแนกตามเพศ*

เพศ	จำนวน (คน)	ร้อยละ
ชาย	190	47.5
หญิง	210	52.5
รวม	400	100.0



ภาพที่ 4.1 แสดงจำนวนร้อยละของลักษณะทางประชากรของผู้ตอบแบบสอบถามในด้านเพศ

จากตารางที่ 4.1 พบว่าผู้ตอบแบบสอบถามส่วนมากเป็นเพศหญิง จำนวน 210 คน คิดเป็นร้อยละ 52.5 และเป็นเพศหญิง จำนวน 190 คน คิดเป็น ร้อยละ 47.5 ตามลำดับ

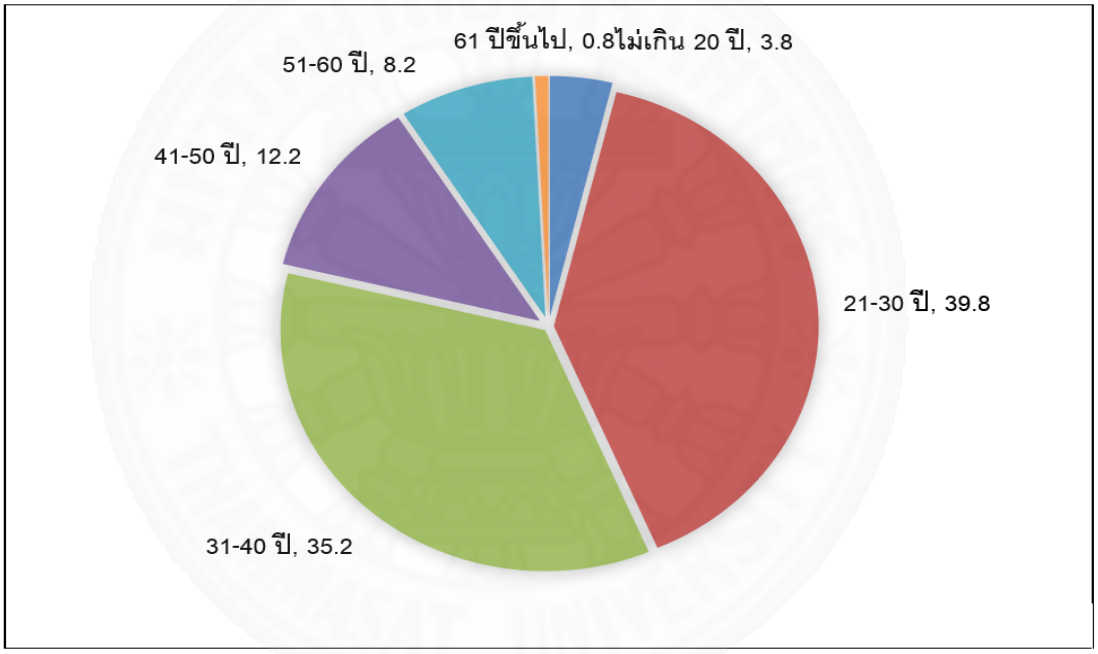
ตารางที่ 4.2 *จำนวนและค่าร้อยละของผู้ตอบแบบสอบถาม จำแนกตามอายุ*

อายุ	จำนวน (คน)	ร้อยละ
ไม่เกิน 20 ปี	15	3.8

21-30 ปี	159	39.8

ตารางที่ 4.2 *จำนวนและค่าร้อยละของผู้ตอบแบบสอบถาม จำแนกตามอายุ (ต่อ)*

อายุ	จำนวน (คน)	ร้อยละ
31-40 ปี	141	35.2
41-50 ปี	49	12.2
51-60 ปี	33	8.2
61 ปีขึ้นไป	3	0.8
รวม	400	100.0

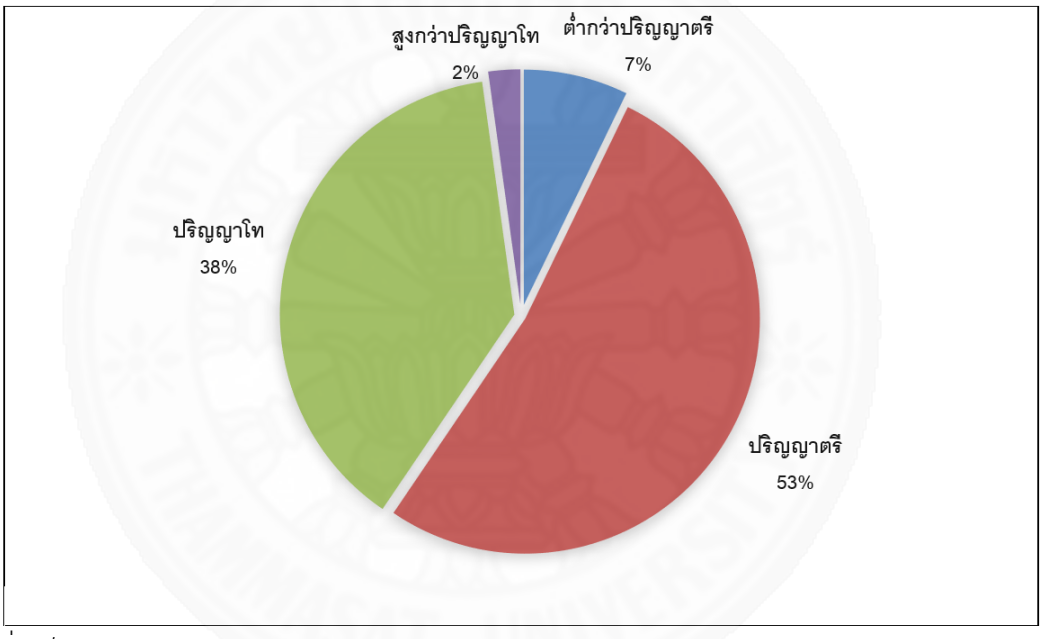


ภาพที่ 4.2 แสดงจำนวนร้อยละของลักษณะทางประชากรของผู้ตอบแบบสอบถามในด้านอายุ

จากตารางที่ 4.2 พบว่า ผู้ตอบแบบสอบถามส่วนมาก มีอายุ 21-30 ปี มีจำนวน 159 คน คิดเป็นร้อยละ 39.8 รองลงมา มีอายุ 31-40 ปี มีจำนวน 141 คน คิดเป็นร้อยละ 35.2 อายุ 41-50 ปี มีจำนวน 49 คน คิดเป็น ร้อยละ 12.2 อายุ 51-60 ปี มีจำนวน 33 คน คิดเป็น ร้อยละ 8.2 อายุไม่เกิน 20 ปี มีจำนวน 15 คน คิดเป็น ร้อยละ 3.8 อายุ 61 ปีขึ้นไป มีจำนวน 3 คน คิดเป็นร้อยละ 0.8 ตามลำดับ

ตารางที่ 4.3 *จำนวนและร้อยละของระดับการศึกษาสูงสุด*

ระดับการศึกษาสูงสุด	จำนวน (คน)	ร้อยละ
ต่ำกว่าปริญญาตรี	29	7.2
ปริญญาตรี	209	52.3
ปริญญาโท	153	38.3
สูงกว่าปริญญาโท	9	2.2
รวม	400	100.0

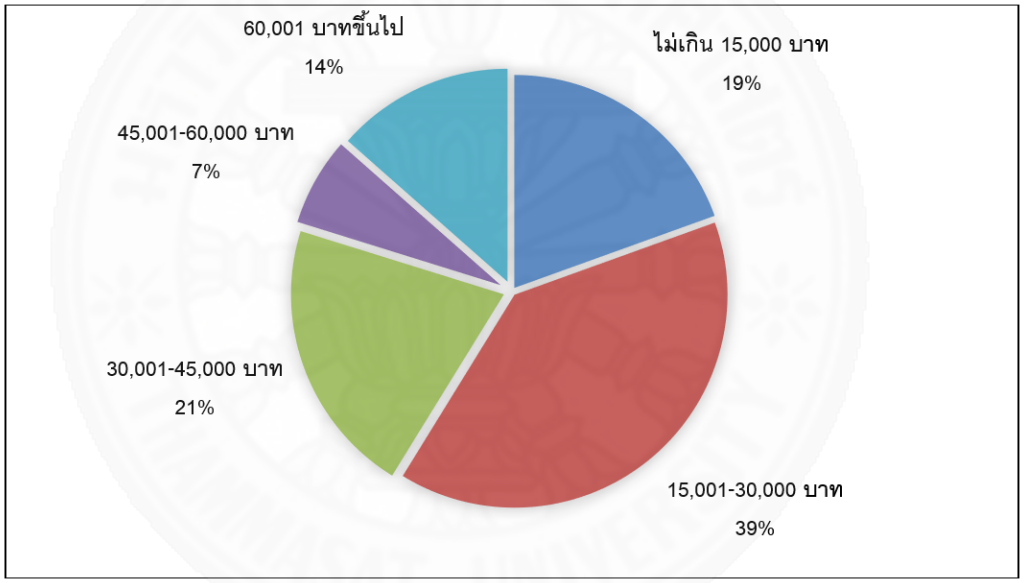


ภาพที่ 4.3 แสดงจำนวนร้อยละของลักษณะทางประชากรของผู้ตอบแบบสอบถามในด้านการศึกษา

จากตารางที่ 4.3 พบว่า ผู้ตอบแบบสอบถามส่วนมาก มีการศึกษาระดับปริญญาตรี จำนวน 209 คน คิดเป็น ร้อยละ 52.3 รองลงมา จบการศึกษาระดับปริญญาโท จำนวน 153 คน คิดเป็น ร้อยละ 38.3 มีการศึกษาระดับต่ำกว่าปริญญาตรี จำนวน 29 คน คิดเป็น ร้อยละ 7.2และมีการศึกษาสูงกว่าระดับปริญญาโท จำนวน 9 คน คิดเป็น ร้อยละ 2.2 ตามลำดับ

ตารางที่ 4.4 *จำนวนและร้อยละของรายได้ส่วนตัวต่อเดือน*

รายได้ส่วนตัวต่อเดือน	จำนวน (คน)	ร้อยละ
ไม่เกิน 15,000 บาท	78	19.5
15,001-30,000 บาท	157	39.3
30,001-45,000 บาท	84	21.0
45,001-60,000 บาท	27	6.7
60,001 บาทขึ้นไป	54	13.5
รวม	400	100.0



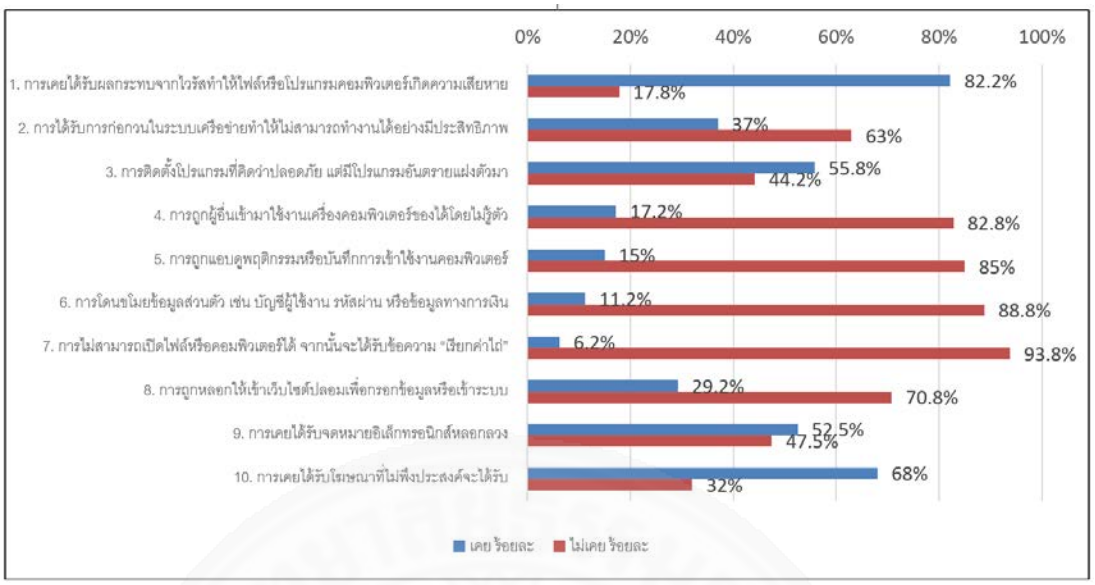
ภาพที่ 4.4 แสดงจำนวนร้อยละของลักษณะทางประชากรของผู้ตอบแบบสอบถามในด้านรายได้

จากตารางที่ 4.4 พบว่า ผู้ตอบแบบสอบถามส่วนมากมีรายได้ส่วนตัว 15,001-30,000 บาทต่อเดือน จำนวน 157 คน คิดเป็นร้อยละ 39.3 รองลงมา มีรายได้ส่วนตัว 30,001-45,000 บาท ต่อเดือน จำนวน 84 คน คิดเป็น ร้อยละ 21.0 มีรายได้ส่วนตัวไม่เกิน 15,000 บาท จำนวน 78 คน คิดเป็น ร้อยละ 19.5 มีรายได้ส่วนตัว 60,001 บาทขึ้นไป จำนวน 54 คน คิดเป็น ร้อยละ 13.5 และมีรายได้ส่วนตัว 45,001-60,000 บาทต่อเดือน จำนวน 27 คน คิดเป็น ร้อยละ 6.7 ตามลำดับ

4.2 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

ตารางที่ 4.5 *จำนวนและร้อยละของประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์*

ประเด็น	ประสบการณ์				รวม
	เคย	ร้อยละ	ไม่เคย	ร้อยละ	
1. การได้รับผลกระทบจากไวรัสทำให้ไฟล์หรือโปรแกรมคอมพิวเตอร์เกิดความเสียหาย	329	82.2	17	17.8	400 100.0
2. การได้รับการก่อกวนในระบบเครือข่ายทำให้ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ	148	37.0	252	63.0	400 100.0
3. การติดตั้งโปรแกรมที่คิดว่าปลอดภัย แต่มีโปรแกรมอันตรายแฝงตัวมา	223	55.8	177	44.2	400 100.0
4. การถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของได้โดยไม่รู้ตัว	69	17.2	331	82.8	400 100.0
5. การถูกแอบดูพฤติกรรมหรือบันทึกการเข้าใช้งานคอมพิวเตอร์	60	15.0	340	85.0	400 100.0
6. การโดนขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน	45	11.2	355	88.8	400 100.0
7. การไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้จากนั้นจะได้รับข้อความ “เรียกค่าไถ่”	25	6.2	375	93.8	400 100.0
8. การถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าระบบ	117	29.2	283	70.8	400 100.0
9. การเคยได้รับจดหมายอิเล็กทรอนิกส์หลอกลวง	210	52.5	190	47.5	400 100.0
10. การเคยได้รับโฆษณาที่ไม่พึงประสงค์จะได้รับ	272	68.0	128	32.0	400 100.0

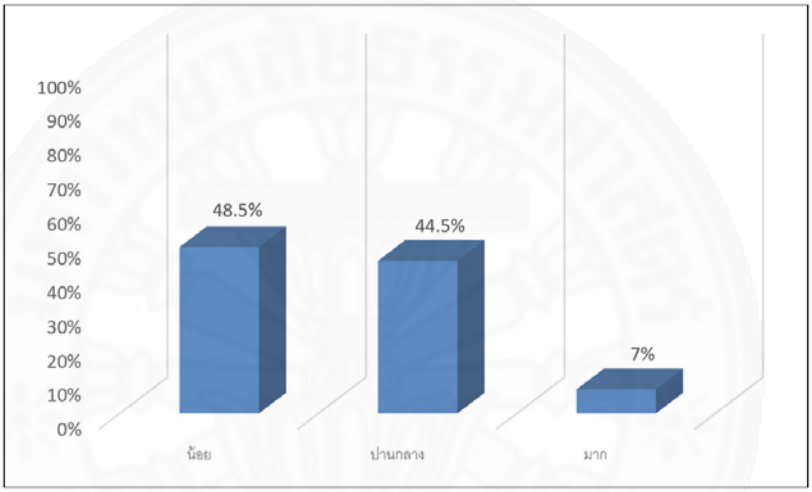


ภาพที่ 4.5 แสดงจำนวนร้อยละของลักษณะทางประชากรของผู้ตอบแบบสอบถามในด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

จากตารางที่ 4.5 พบว่า ผู้ตอบแบบสอบถามมีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ในประเด็น การเคยได้รับผลกระทบจากไวรัสทำให้ไฟล์หรือโปรแกรมคอมพิวเตอร์เกิดความเสียหาย มากที่สุด จำนวน 329 คิดเป็น ร้อยละ 82.2 รองลงมา คือ การเคยได้รับโฆษณาที่ไม่พึงประสงค์จะได้รับ จำนวน 272 คิดเป็น ร้อยละ 68.0 การติดตั้งโปรแกรมที่คิดว่าปลอดภัย แต่มีโปรแกรมอันตรายแฝงตัวมา จำนวน 223 คิดเป็น ร้อยละ 55.8 การเคยได้รับจดหมายอิเล็กทรอนิกส์หลอกลวง จำนวน 210 คิดเป็น ร้อยละ 52.5“การได้รับการก่อกวนในระบบเครือข่ายทำให้ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ จำนวน 148 คิดเป็น ร้อยละ 37.0 การถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าระบบ จำนวน 117 คิดเป็น ร้อยละ 29.2 การถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของได้โดยไม่รู้ตัว จำนวน 69 คิดเป็น ร้อยละ 17.2 การถูกแอบดูพฤติกรรมหรือบันทึกการเข้าใช้งานคอมพิวเตอร์ จำนวน 60 คิดเป็น ร้อยละ 15.0 การโดนขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน จำนวน 45 คิดเป็น ร้อยละ 11.2 และการไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นจะได้รับข้อความ เรียกค่าไถ่ จำนวน 25 คิดเป็น ร้อยละ 6.2 ตามลำดับ

ตาราง 4.6 *แสดงจำนวนร้อยละของลักษณะทางประชากรของผู้ตอบแบบสอบถามในด้านจัดกลุ่มระดับประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์*

ระดับประสบการณ์	จำนวน (คน)	ร้อยละ
น้อย	194	48.5
ปานกลาง	178	44.5
มาก	28	7.0
รวม	400	100.0



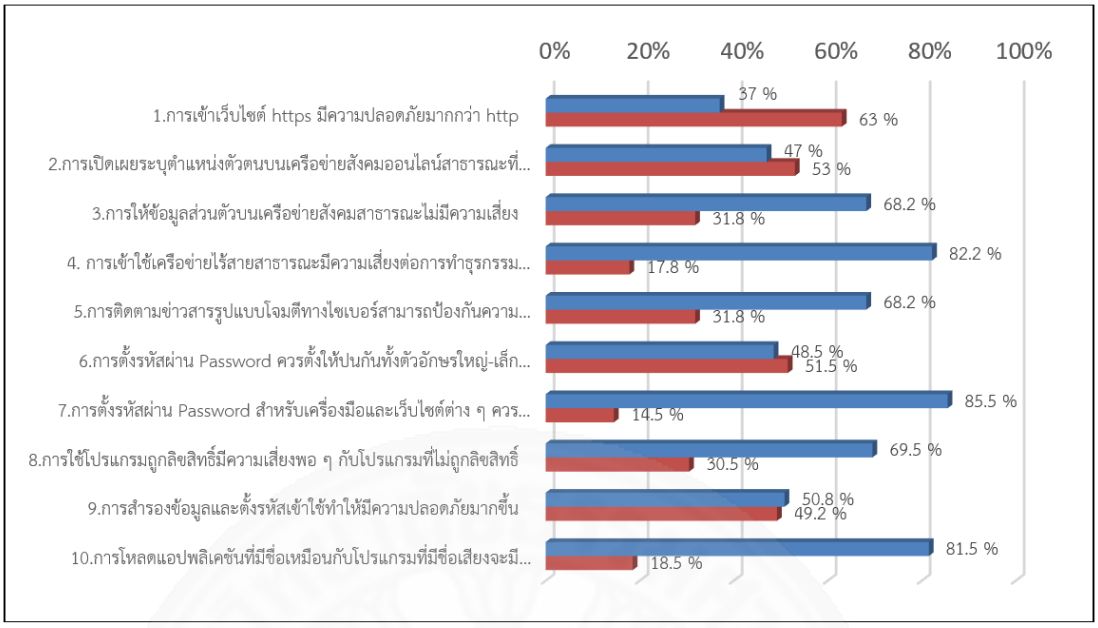
ภาพที่ 4.6 แสดงจำนวนร้อยละของลักษณะทางประชากรของผู้ตอบแบบสอบถามในด้านจัดกลุ่มระดับประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

จากตารางที่ 4.6 พบว่า หากจัดกลุ่มผู้ตอบแบบสอบถามประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ วัดค่าเป็น 3 ระดับคือ (น้อย,ปานกลาง,มาก) พบว่า ผู้ตอบแบบสอบถามส่วนมากมีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับน้อย จำนวน 194 คน คิดเป็น ร้อยละ 48.5 รองลงมา มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับปานกลาง จำนวน 178 คน คิดเป็นร้อยละ 44.5 และมีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับมาก จำนวน 28 คน คิดเป็นร้อยละ 7.0 ตามลำดับ

4.3 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

ตารางที่ 4.7 *จำนวนและร้อยละของความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์*

ประเด็น	คำตอบ				รวม
	ตอบถูก	ร้อยละ	ตอบผิด	ร้อยละ	
ข้อความที่ตอบคำถามถูก คือตอบถูก					
1. การเข้าเว็บไซต์ https มีความปลอดภัยมากกว่า http	148	37.0	252	63.0	400 100.0
4. การเข้าใช้เครือข่ายไร้สายสาธารณะมีความเสี่ยงต่อการทำธุรกรรมออนไลน์	273	68.2	127	31.8	400 100.0
5. การติดตามข่าวสารรูปแบบโจมตีทางไซเบอร์สามารถป้องกันความเสียหายที่จะเกิดขึ้นได้	194	48.5	206	51.5	400 100.0
6. การตั้งรหัสผ่าน Password ควรตั้งให้ปนกันทั้งตัวอักษรใหญ่-เล็ก ตัวเลข สัญลักษณ์พิเศษและยาวอย่างน้อย 8 ตัวอักษร	342	85.5	58	14.5	400 100.0
9. การสำรองข้อมูลและตั้งรหัสเข้าใช้ทำให้มีความปลอดภัยมากขึ้น	326	81.5	74	18.5	400 100.0
ข้อความที่ตอบคำถามถูก คือตอบผิด					
2. การเปิดเผยระบุตำแหน่งตัวตนบนเครือข่ายสังคมออนไลน์สาธารณะที่มีผู้ใช้ทั่วไปมีความปลอดภัย	273	68.2	127	31.8	400 100.0
3. การให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะไม่มีความเสี่ยง	329	82.2	71	17.8	400 100.0
7. การตั้งรหัสผ่าน Password สำหรับเครื่องมือและเว็บไซต์ต่าง ๆ ควรจะเหมือนกัน	278	69.5	122	30.5	400 100.0
8. การใช้โปรแกรมถูกลิขสิทธิ์มีความเสี่ยงพอ ๆ กับโปรแกรมที่ไม่ถูกลิขสิทธิ์	203	50.8	197	49.2	400 100.0
10. การโหลดแอปพลิเคชันที่มีชื่อเหมือนกับโปรแกรมที่มีชื่อเสียงจะมีความปลอดภัย	188	47.0	212	53.0	400 100.0



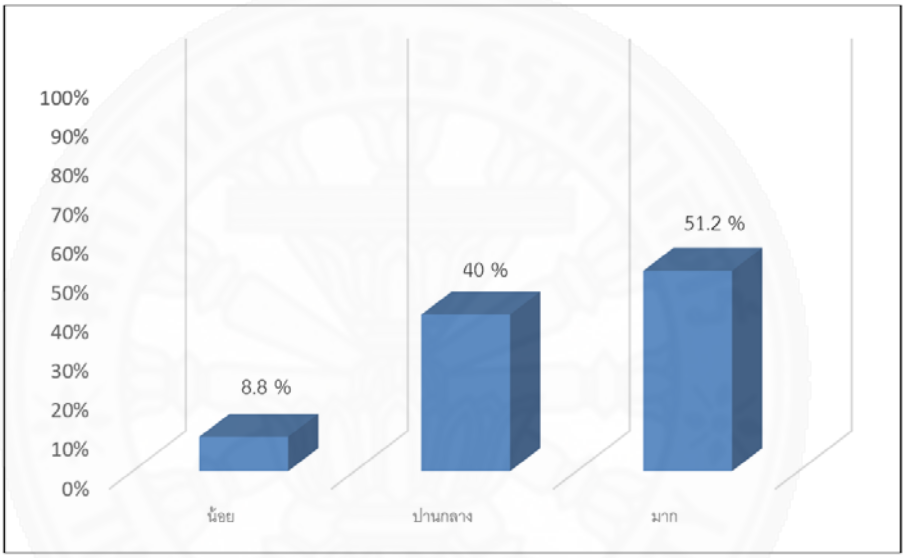
ภาพที่ 4.7 แสดงจำนวนร้อยละของผู้ตอบแบบสอบถามในด้านจัดกลุ่มระดับความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

จากตารางที่ 4.7 พบว่า ผู้ตอบแบบสอบถาม กลุ่มข้อความที่ตอบคำถามถูก มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ การตั้งรหัสผ่าน (Password) ควรตั้งให้ปนกันทั้งตัวอักษรใหญ่-เล็ก ตัวเลข สัญลักษณ์พิเศษ และยาวอย่างน้อย 8 ตัวอักษร มากที่สุด จำนวน 342 คน คิดเป็น ร้อยละ 85.5 รองลงมา การสำรองข้อมูลและตั้งรหัสเข้าใช้ทำให้มีความปลอดภัยมากขึ้น จำนวน 326 คน คิดเป็น ร้อยละ 81.5 การเข้าใช้เครือข่ายไร้สายสาธารณะมีความเสี่ยงต่อการทำธุรกรรมออนไลน์ จำนวน 273 คน คิดเป็น ร้อยละ 68.2 การติดตามข่าวสารรูปแบบโจมตีทางไซเบอร์สามารถป้องกันความเสียหายที่จะเกิดขึ้นได้ จำนวน 194 คน คิดเป็น ร้อยละ 48.5 การเข้าเว็บไซต์ https มีความปลอดภัยมากกว่า http จำนวน 148 คน คิดเป็น ร้อยละ 37 ตามลำดับ

จากตาราง พบว่า ผู้ตอบแบบสอบถาม กลุ่มข้อความที่ตอบคำถามถูก (คือตอบผิด) มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ การให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะไม่มีความเสี่ยงมากที่สุด จำนวน 329 คน คิดเป็น ร้อยละ 82.2 รองลงมา การตั้งรหัสผ่าน (Password) สำหรับเครื่องมือและเว็บไซต์ต่าง ๆ ควรจะเหมือนกัน จำนวน 278 คน คิดเป็น ร้อยละ 69.5 การเปิดเผยระบุตำแหน่งตัวตนบนเครือข่ายสังคมออนไลน์สาธารณะที่มีผู้ใช้ทั่วไปมีความปลอดภัย จำนวน 273 คน คิดเป็น ร้อยละ 68.2 การใช้โปรแกรมถูกลิขสิทธิ์มีความเสี่ยงพอ ๆ กับโปรแกรมที่ไม่ถูกลิขสิทธิ์ จำนวน 203 คน คิดเป็น ร้อยละ 50.8 การโหลดแอปพลิเคชันที่มีชื่อเหมือนกับโปรแกรมที่มีชื่อเสียงจะมีความปลอดภัย จำนวน 188 คน คิดเป็น ร้อยละ 47 ตามลำดับ

ตาราง 4.8 *แสดงจำนวนร้อยละของลักษณะทางประชากรของผู้ตอบแบบสอบถามในด้านจัดกลุ่มความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์*

ระดับความรู้	จำนวน (คน)	ร้อยละ
น้อย	35	8.8
ปานกลาง	160	40.0
มาก	205	51.2
รวม	400	100.0



ภาพที่ 4.8 แสดงจำนวนร้อยละของลักษณะทางประชากรของผู้ตอบแบบสอบถามในด้านจัดกลุ่มความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

จากตารางที่ 4.8 พบว่า หากจัดกลุ่มผู้ตอบแบบสอบถามความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ วัดค่าเป็น 3 ระดับคือ (น้อย,ปานกลาง,มาก) ผู้ตอบแบบสอบถามส่วนมาก มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับมาก จำนวน 205 คน คิดเป็น ร้อยละ 51.2 รองลงมา มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับปานกลาง จำนวน 160 คน คิดเป็น ร้อยละ 40.0 และมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับน้อย จำนวน 35 คน คิดเป็น ร้อยละ 8.8 ตามลำดับ

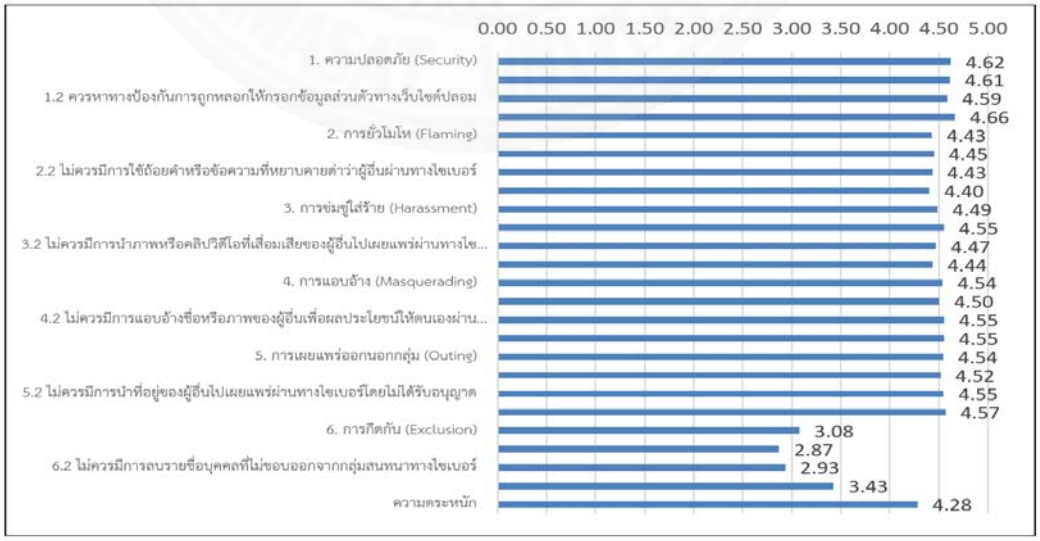
4.4 ความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์

ตารางที่ 4.9 *ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์*

ประเด็น	M	SD	ระดับ
1. ความปลอดภัย (Security)	4.62	0.64	มากที่สุด
1.1 ควรหาทางป้องกันการถูกโปรแกรมคอมพิวเตอร์ที่ไม่พึงประสงค์ทำความเสียหายต่อข้อมูลในระบบ	4.61	0.69	มากที่สุด
1.2 ควรหาทางป้องกันการถูกหลอกให้กรอกข้อมูลส่วนตัวทางเว็บไซต์ปลอม	4.59	0.73	มากที่สุด
1.3 ควรหาทางป้องกันการถูกลักลอบเจาะเข้าสู่ระบบเพื่ออ่านหรือทำลายข้อมูล	4.66	0.67	มากที่สุด
2. การยั่วโมโห (Flaming)	4.43	0.65	มาก
2.1 ไม่ควรมีการกล่าวถึงผู้อื่นให้ได้รับความอับอายหรือเสื่อมเสียชื่อเสียงผ่านทางไซเบอร์	4.45	0.74	มาก
2.2 ไม่ควรมีการใช้ถ้อยคำหรือข้อความที่หยาบคายด่าว่าผู้อื่นผ่านทางไซเบอร์	4.43	0.73	มาก
2.3 ไม่ควรมีการล้อเลียนรูปร่างหน้าตาของผู้อื่นผ่านทางไซเบอร์	4.40	0.78	มาก
3. การข่มขู่ใส่ร้าย (Harassment)	4.49	0.59	มาก
3.1 ไม่ควรมีการใส่ร้ายผู้อื่นให้บุคคลที่สามเกลียดชังผ่านทางไซเบอร์	4.55	0.62	มากที่สุด
3.2 ไม่ควรมีการนำภาพหรือคลิปวิดีโอที่เสื่อมเสียของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์	4.47	0.67	มาก
3.3 ไม่ควรมีการเผยแพร่ข่าวลือในทางลบของผู้อื่นผ่านทางไซเบอร์	4.44	0.69	มาก
4. การแอบอ้าง (Masquerading)	4.54	0.56	มากที่สุด
4.1 ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นในการสนทนาผ่านทางไซเบอร์	4.50	0.65	มากที่สุด
4.2 ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อผลประโยชน์ให้ตนเองผ่านทางไซเบอร์	4.55	0.59	มากที่สุด

ตารางที่ 4.9 *ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์(ต่อ)*

4.3 ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อให้ร้ายบุคคลที่สามผ่านทางไซเบอร์	4.55	0.59	มากที่สุด
5. การเผยแพร่ออกนอกกลุ่ม (Outing)	4.54	0.58	มากที่สุด
5.1 ไม่ควรมีการนำชื่อพ่อแม่หรือญาติพี่น้องของผู้อื่นไปเปิดเผยผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต	4.52	0.64	มากที่สุด
5.2 ไม่ควรมีการนำที่อยู่ของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต	4.55	0.62	มากที่สุด
5.3 ไม่ควรมีการนำเบอร์โทรศัพท์ของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต	4.57	0.62	มากที่สุด
6. การกีดกัน (Exclusion)	3.08	1.04	ปานกลาง
6.1 ไม่ควรมีการบล็อกข้อความสนทนาทางไซเบอร์ของบุคคลที่ไม่ชอบ	2.87	1.23	ปานกลาง
6.2 ไม่ควรมีการลบรายชื่อบุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางไซเบอร์	2.93	1.19	ปานกลาง
6.3 ไม่ควรมีการกดดันให้บุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางไซเบอร์	3.43	1.10	ปานกลาง
รวม	**4.28**	**0.46**	**มาก**



ภาพที่ 4.9 แสดงจำนวนค่าเฉลี่ยของผู้ตอบแบบสอบถามในด้านความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์

จากตารางที่ 4.9 พบว่า ในภาพรวมผู้ตอบแบบสอบถามมีความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ในระดับมาก (4.28) โดยด้านที่มีกลุ่มตัวอย่างมีความตระหนักในระดับมากที่สุดมี 3 ด้าน คือ ด้านความปลอดภัย (4.62) ด้านการแอบอ้าง (4.54) และด้านการเผยแพร่ออกนอกกลุ่ม (4.54) ส่วนด้านที่มีกลุ่มตัวอย่างมีความตระหนักในระดับมากมี 2 ด้าน คือ ด้านการข่มขู่ใส่ร้าย (4.49) และด้านการยั่วโมโห (4.43) สำหรับด้านที่มีกลุ่มตัวอย่างมีความตระหนักในระดับปานกลางมีเพียงด้านเดียว คือ ด้านการกีดกัน (3.08)

เมื่อพิจารณารายละเอียดในแต่ละด้าน พบว่า ด้านความปลอดภัย กลุ่มตัวอย่างมีความตระหนักในระดับมากที่สุดทุกประเด็น คือ ควรหาทางป้องกันการถูกลักลอบเจาะเข้าสู่ระบบเพื่ออ่านหรือทำลายข้อมูล (4.66) ควรหาทางป้องกันการถูกโปรแกรมคอมพิวเตอร์ที่ไม่พึงประสงค์ทำความเสียหายต่อข้อมูลในระบบ (4.61) และควรหาทางป้องกันการถูกหลอกให้กรอกข้อมูลส่วนตัวทางเว็บไซต์ปลอม (4.59)

ด้านการแอบอ้าง กลุ่มตัวอย่างมีความตระหนักในระดับมากที่สุดทุกประเด็น คือ ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อผลประโยชน์ให้ตนเองผ่านทางไซเบอร์ (4.55) ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อให้ร้ายบุคคลที่สามผ่านทางไซเบอร์ (4.55) และไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นในการสนทนาผ่านทางไซเบอร์ (4.50)

ด้านการเผยแพร่ออกนอกกลุ่ม กลุ่มตัวอย่างมีความตระหนักในระดับมากที่สุดทุกประเด็น คือ ไม่ควรมีการนำเบอร์โทรศัพท์ของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต (4.57) ไม่ควรมีการนำที่อยู่ของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต (4.55) และไม่ควรมีการนำชื่อพ่อแม่หรือญาติพี่น้องของผู้อื่นไปเปิดเผยผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต (4.52)

ด้านการข่มขู่ใส่ร้าย กลุ่มตัวอย่างมีความตระหนักในระดับมากที่สุดใน 1 ประเด็น คือ ไม่ควรมีการใส่ร้ายผู้อื่นให้บุคคลที่สามเกลียดชังผ่านทางไซเบอร์ (4.55) และกลุ่มตัวอย่างมีความตระหนักในระดับมากใน 2 ประเด็น คือ ไม่ควรมีการนำภาพหรือคลิปวิดีโอที่เสื่อมเสียของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์ (4.47) และไม่ควรมีการเผยแพร่ข่าวลือในทางลบของผู้อื่นผ่านทางไซเบอร์ (4.44)

ด้านการยั่วโมโห กลุ่มตัวอย่างมีความตระหนักในระดับมากทุกประเด็น คือ ไม่ควรมีการกล่าวถึงผู้อื่นให้ได้รับความอับอายหรือเสื่อมเสียชื่อเสียงผ่านทางไซเบอร์ (4.45) ไม่ควรมีการใช้ถ้อยคำหรือข้อความที่หยาบคายด่าว่าผู้อื่นผ่านทางไซเบอร์ (4.43) ไม่ควรมีการล้อเลียนรูปร่างหน้าตาของผู้อื่นผ่านทางไซเบอร์ (4.40)

ด้านการกีดกัน กลุ่มตัวอย่างมีความตระหนักในระดับปานกลางทุกประเด็น คือ ไม่ควรมีการกดดันให้บุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางไซเบอร์ (3.43) ไม่ควรมีการลบรายชื่อบุคคลที่

ไม่ชอบออกจากกลุ่มสนทนาทางไซเบอร์ (2.93) ไม่ควรมีการบล็อกข้อความสนทนาทางไซเบอร์ของบุคคลที่ไม่ชอบ (2.87)

4.5 การทดสอบสมมติฐาน

4.5.1 ปัจจัยทางด้านลักษณะทางประชากรมีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

4.5.1.1 เพศไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

ตารางที่ 4.10 *การเปรียบเทียบความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต จำแนกตามเพศ*

เพศ	N	M	SD	t	p
ชาย	190	4.274	.501	-.303	.762
หญิง	210	4.288	.412		

จากตารางที่ 4.10 พบว่า ปฏิเสธสมมติฐานการวิจัย กล่าวคือ เพศไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตที่ระดับนัยสำคัญ .05 ($p<.05$)

4.5.1.2 อายุมีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

ตารางที่ 4.11 การวิเคราะห์ความแปรปรวนแบบทางเดียวของตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต จำแนกตามอายุ

แหล่งที่มา	SS	df	MS	F	p
ระหว่างกลุ่ม	4.837	4	1.209	6.126***	.000
ภายในกลุ่ม	77.969	395	.197		
รวม	82.806	399			

หมายเหตุ: ***มีนัยสำคัญทางสถิติที่ระดับ 0.001

จากตารางที่ 4.11 พบว่า ยอมรับสมมติฐานการวิจัย กล่าวคือ อายุมีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตที่ระดับนัยสำคัญ .001 (p<.001)

ตารางที่ 4.12 *การเปรียบเทียบความแตกต่างระหว่างความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต จำแนกตามอายุ*

อายุ		**ความแตกต่างของค่าเฉลี่ย**	**p**
ไม่เกิน 20 ปี	21-30 ปี	-.420*	.017
	31-40 ปี	-.357	.069
	41-50 ปี	-.582**	.001
	51 ปีขึ้นไป	-.523**	.006
21-30 ปี	ไม่เกิน 20 ปี	.420*	.017
	31-40 ปี	.062	.832
	41-50 ปี	-.162	.289
	51 ปีขึ้นไป	-.104	.810
31-40 ปี	ไม่เกิน 20 ปี	.357	.069
	21-30 ปี	-.062	.832
	41-50 ปี	-.225	.056
	51 ปีขึ้นไป	-.166	.408
41-50 ปี	ไม่เกิน 20 ปี	.582**	.001
	21-30 ปี	.162	.289
	31-40 ปี	.225	.056
	51 ปีขึ้นไป	.059	.985
51 ปีขึ้นไป	ไม่เกิน 20 ปี	.523**	.006
	21-30 ปี	.104	.810
	31-40 ปี	.166	.408
	41-50 ปี	-.059	.985

หมายเหตุ: *มีนัยสำคัญทางสถิติที่ระดับ 0.05

**มีนัยสำคัญทางสถิติที่ระดับ 0.01

จากตารางที่ 4.12 ผู้ใช้อินเทอร์เน็ตที่มีอายุ 21-30 ปี จะมีความตระหนักถึงภัยคุกคามทางไซเบอร์มากกว่าผู้ใช้อินเทอร์เน็ตที่มีอายุไม่เกิน 20 ปีที่ระดับนัยสำคัญ .05 (p<.05) และผู้ใช้

อินเทอร์เน็ตที่มีอายุ 41-50ปี และ 51 ปีขึ้นไป จะมีความตระหนักถึงภัยคุกคามทางไซเบอร์มากกว่าผู้ใช้อินเทอร์เน็ตที่มีอายุไม่เกิน 20 ปีที่ระดับนัยสำคัญ .01 (p<.01)

4.5.1.3 ระดับการศึกษาสูงสุดมีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

ตารางที่ 4.13 *การวิเคราะห์ความแปรปรวนแบบทางเดียวของตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินนเทอร์เน็ต จำแนกตามระดับการศึกษาสูงสุด*

แหล่งที่มา	SS	df	MS	F	p
ระหว่างกลุ่ม	2.142	2	1.071	5.270**	.006
ภายในกลุ่ม	80.664	397	.203		
รวม	82.806	399			

หมายเหตุ: **มีนัยสำคัญทางสถิติที่ระดับ 0.01

จากตารางที่ 4.13 พบว่า ยอมรับสมมติฐานการวิจัย กล่าวคือ ระดับการศึกษามีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตที่ระดับนัยสำคัญ .01 (p<.01)

ตารางที่ 4.14 *การเปรียบเทียบความแตกต่างระหว่างความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต จำแนกตามระดับการศึกษาสูงสุด*

ระดับการศึกษาสูงสุด		ความแตกต่างของค่าเฉลี่ย	p
ต่ำกว่าปริญญาตรี	ปริญญาตรี	-.274**	.009
	ปริญญาโทขึ้นไป	-.289**	.007
ปริญญาตรี	ต่ำกว่าปริญญาตรี	.274**	.009
	ปริญญาโทขึ้นไป	-.015	.951
ปริญญาโทขึ้นไป	ต่ำกว่าปริญญาตรี	.289**	.007
	ปริญญาตรี	.015	.951

หมายเหตุ: **มีนัยสำคัญทางสถิติที่ระดับ 0.01

จากตารางที่ 4.14 ผู้ใช้อินเทอร์เน็ตที่จบการศึกษาระดับปริญญาตรีและปริญญาโทขึ้นไป จะมีความตระหนักถึงภัยคุกคามทางไซเบอร์มากกว่าผู้ใช้อินเทอร์เน็ตที่มีจบการศึกษาระดับต่ำกว่าปริญญาตรีที่ระดับนัยสำคัญ .01 (p<.01)

4.5.1.4 รายได้ส่วนตัวต่อเดือนมีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

ตารางที่ 4.15 *การวิเคราะห์ความแปรปรวนแบบทางเดียวของตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต จำแนกตามรายได้ส่วนตัวต่อเดือน*

แหล่งที่มา	SS	df	MS	F	p
ระหว่างกลุ่ม	2.477	4	.619	3.044*	.017
ภายในกลุ่ม	80.330	395	.203		
รวม	82.806	399			

หมายเหตุ: *มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางที่ 4.15 พบว่า ยอมรับสมมติฐานการวิจัย กล่าวคือ รายได้ส่วนตัวต่อเดือนมีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตที่ระดับนัยสำคัญ .05 (p<.05)

ตารางที่ 4.16 *การเปรียบเทียบความแตกต่างระหว่างความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตจำแนกตามรายได้ส่วนตัวต่อเดือน*

รายได้ส่วนตัวต่อเดือน		ความแตกต่างของค่าเฉลี่ย	p
ไม่เกิน 15,000 บาท	15,001-30,000 บาท	-.046	.463
	30,001-45,000 บาท	-.184*	.010
	45,001-60,000 บาท	-.252*	.013
	60,001 บาทขึ้นไป	-.132	.099
15,001-30,000 บาท	ไม่เกิน 15,000 บาท	.046	.463
	30,001-45,000 บาท	-.138*	.024
	45,001-60,000 บาท	-.206*	.029
	60,001 บาทขึ้นไป	-.086	.227

ตารางที่ 4.16 *การเปรียบเทียบความแตกต่างระหว่างความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตจำแนกตามรายได้ส่วนตัวต่อเดือน (ต่อ)*

30,001-45,000 บาท	ไม่เกิน 15,000 บาท	.184*	.010
	15,001-30,000 บาท	.138*	.024
	45,001-60,000 บาท	-.069	.491
	60,001 บาทขึ้นไป	.052	.512
45,001-60,000 บาท	ไม่เกิน 15,000 บาท	.252*	.013
	15,001-30,000 บาท	.206*	.029
	30,001-45,000 บาท	.069	.491
	60,001 บาทขึ้นไป	.120	.258
60,001 บาทขึ้นไป	ไม่เกิน 15,000 บาท	.132	.099
	15,001-30,000 บาท	.086	.227
	30,001-45,000 บาท	-.052	.512
	45,001-60,000 บาท	.120	.258

หมายเหตุ: *มีนัยสำคัญทางสถิติที่ระดับ 005

จากตารางที่ 4.16 ผู้ใช้อินเทอร์เน็ตที่มีรายได้ส่วนตัว 30,001-45,000 บาทต่อเดือน จะมีความตระหนักถึงภัยคุกคามทางไซเบอร์มากกว่าผู้ใช้อินเทอร์เน็ตที่มีรายได้ส่วนตัวไม่เกิน 15,000 บาท และ 15,001-30,000 บาท นอกจากนั้นผู้ใช้อินเทอร์เน็ตที่มีรายได้ส่วนตัว 45,001-60000 บาท ต่อเดือน จะมีความตระหนักถึงภัยคุกคามทางไซเบอร์มากกว่าผู้ใช้อินเทอร์เน็ตที่มีรายได้ส่วนตัวไม่เกิน 15,000 บาท และ 15,001-30,000 บาท ที่ระดับนัยสำคัญ .05 ($p<.05$)

4.5.2 ปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

ตารางที่ 4.17 ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์กับความตระหนักถึงภัยคุกคามทางไซเบอร์

ตัวแปร	ความตระหนักถึงภัยคุกคามทางไซเบอร์	
	r	p
ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์	.073	.143

จากตารางที่ 4.17 พบว่า ปฏิเสธสมมติฐานการวิจัย กล่าวคือ ปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตที่ระดับนัยสำคัญ .05 (p>.05)

4.5.3 ปัจจัยทางด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

ตารางที่ 4.18 *ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์กับความตระหนักถึงภัยคุกคามทางไซเบอร์*

ตัวแปร	ความตระหนักถึงภัยคุกคามทางไซเบอร์	
	r	p
ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์	.376***	.000

หมายเหตุ: ***มีนัยสำคัญทางสถิติที่ระดับ 0.001

จากตารางที่ 4.18 พบว่า ยอมรับสมมติฐานการวิจัย กล่าวคือ ปัจจัยทางด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตที่ระดับนัยสำคัญ .001 (p<.001) โดยมีผลทางบวก กล่าวคือ ผู้ใช้อินเทอร์เน็ตที่มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์มาก จะมีความตระหนักถึงภัยคุกคามทางไซเบอร์มากด้วย

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

จากการศึกษางานวิจัยเรื่อง “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร” มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ เพื่อเสนอแนะผลกระทบที่จะเกิดขึ้นจากการใช้อินเทอร์เน็ต โดยกลุ่มตัวอย่างที่ผู้วิจัยใช้ศึกษาความคิดเห็นที่เกี่ยวข้องกับปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ คือ ประชากรที่อาศัยอยู่ในเขตกรุงเทพมหานคร โดยสามารถสรุปผลวิจัยเป็น 3 ส่วนได้ดั้งนี้

5.1 สรุปผลการวิจัย

5.2 ข้อเสนอแนะ

5.3 ข้อจำกัดในการวิจัย

5.1 สรุปผลการวิจัย

การวิจัย เรื่อง “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร” มีวัตถุประสงค์ของการวิจัย ดังนี้

1. เพื่อศึกษาปัจจัยทางด้านลักษณะทางประชากรที่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

2. เพื่อศึกษาปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ที่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

3. เพื่อศึกษาปัจจัยทางด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

การวิจัยนี้เป็นการวิจัยเชิงปริมาณ (Quantitative Research) ด้วยการวิจัยเชิงสำรวจ (Survey Research) ประชากร คือ ผู้ใช้อินเทอร์เน็ตที่มีอายุ 15 ปีขึ้นไปและอยู่ในเขตกรุงเทพมหานคร ขนาดตัวอย่าง 400 คน ใช้การสุ่มตัวอย่างแบบไม่ใช่หลักความน่าจะเป็น (Non-Probability Sampling) ด้วยวิธีการสุ่มตัวอย่างแบบบังเอิญ (Accidental Sampling) และวิธีการสุ่มตัวอย่างแบบสโนว์บอล (Snowball Sampling) เครื่องมือที่ใช้ในการวิจัย คือ แบบสอบถาม ใช้วิธีให้กลุ่มตัวอย่างกรอกแบบสอบถามด้วยตนเอง (Self-Administered Questionnaire) ทางออนไลน์ โดยใช้สถิติเชิงพรรณนาและสถิติเชิงอนุมานในการวิเคราะห์ข้อมูล

5.1.1 สรุปผลข้อมูลลักษณะทางประชากร

- กลุ่มตัวอย่างส่วนใหญ่ร้อยละ 52.5 เป็นเพศหญิง ส่วนที่เหลืออีกร้อยละ 47.5 เป็นเพศชาย

- กลุ่มตัวอย่างส่วนมากร้อยละ 39.8 มีอายุ 21-30 ปี รองลงมา ร้อยละ 35.2 มีอายุ 31-40 ปี ร้อยละ 12.2 มีอายุ 41-50 ปี ร้อยละ 8.2 มีอายุ 51-60 ปี ร้อยละ 3.8 มีอายุไม่เกิน 20 ปี และร้อยละ 0.8 มีอายุ 61 ปีขึ้นไป ตามลำดับ

- กลุ่มตัวอย่างส่วนใหญ่ ร้อยละ 52.3 จบการศึกษาระดับปริญญาตรี รองลงมา ร้อยละ 38.3 จบการศึกษาระดับปริญญาโท ร้อยละ 7.2 จบการศึกษาระดับต่ำกว่าปริญญาตรี และร้อยละ 2.2 จบการศึกษาสูงกว่าระดับปริญญาโท ตามลำดับ

- กลุ่มตัวอย่างส่วนมากร้อยละ 39.3 มีรายได้ส่วนตัว 15,001-30,000 บาทต่อเดือน รองลงมา ร้อยละ 21.0 มีรายได้ส่วนตัว 30,001-45,000 บาทต่อเดือน ร้อยละ 19.5 มีรายได้ส่วนตัวไม่เกิน 15,000 บาท ร้อยละ 13.5 มีรายได้ส่วนตัว 60,001 บาทขึ้นไป และร้อยละ 6.7 มีรายได้ส่วนตัว 45,001-60,000 บาทต่อเดือน ตามลำดับ

5.1.2 สรุปผลข้อมูลประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

กลุ่มตัวอย่างมีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ในประเด็น “การเคยได้รับผลกระทบจากไวรัสทำให้ไฟล์หรือโปรแกรมคอมพิวเตอร์เกิดความเสียหาย” สูงที่สุด (ร้อยละ 82.2) รองลงมา คือ “การเคยได้รับโฆษณาที่ไม่พึงประสงค์จะได้รับ” (ร้อยละ 68.0) “การติดตั้งโปรแกรมที่คิดว่าปลอดภัย แต่มีโปรแกรมอันตรายแฝงตัวมา” (ร้อยละ 55.8) “การเคยได้รับจดหมายอิเล็กทรอนิกส์หลอกลวง” (ร้อยละ 52.5) “การได้รับการก่อกวนในระบบเครือข่ายทำให้ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ” (ร้อยละ 37.0) “การถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าระบบ” (ร้อยละ 29.2) “การถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของได้โดยไม่รู้ตัว” (ร้อยละ 17.2) “การถูกแอบดูพฤติกรรมหรือบันทึกการเข้าใช้งานคอมพิวเตอร์” (ร้อยละ 15.0) “การโดนขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน” (ร้อยละ 11.2) และ “การไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นจะได้รับข้อความ เรียกค่าไถ่” (ร้อยละ 6.2) ตามลำดับ

หากจัดประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์เป็น 3 ระดับ พบว่า กลุ่มตัวอย่างส่วนมาก ร้อยละ 48.5 มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับน้อย รองลงมา ร้อยละ 44.5 มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับปานกลาง และร้อยละ 7.0 มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับมาก ตามลำดับ

5.1.3 สรุปผลข้อมูลความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

ประเด็นที่กลุ่มตัวอย่างมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์สูงสุด 3 อันดับแรก คือ

- การตั้งรหัสผ่าน (Password) ควรตั้งให้ปนกันทั้งตัวอักษรใหญ่-เล็ก ตัวเลข สัญลักษณ์พิเศษ และยาวอย่างน้อย 8 ตัวอักษร
- การให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะมีความเสี่ยง
- การสำรองข้อมูลและตั้งรหัสเข้าใช้ทำให้มีความปลอดภัยมากขึ้น

ประเด็นที่กลุ่มตัวอย่างมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ต่ำสุด 3 อันดับแรก คือ

- การเข้าเว็บไซต์ https มีความปลอดภัยมากกว่า http
- การโหลดแอปพลิเคชันที่มีชื่อเหมือนกับโปรแกรมที่มีชื่อเสียงจะไม่มีความปลอดภัย
- การติดตามข่าวสารรูปแบบโจมตีทางไซเบอร์สามารถป้องกันความเสียหายที่จะเกิดขึ้นได้

หากจัดความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์เป็น 3 ระดับ พบว่า กลุ่มตัวอย่างส่วนใหญ่ ร้อยละ 51.2 มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับมาก รองลงมา ร้อยละ 40.0 มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับปานกลาง และร้อยละ 8.8 มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับน้อย ตามลำดับ

5.1.4 สรุปผลข้อมูลความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์

ในภาพรวมกลุ่มตัวอย่างมีความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ในระดับมาก (4.28) โดยด้านที่มีกลุ่มตัวอย่างมีความตระหนักในระดับมากที่สุดมี 3 ด้าน คือ ด้านความปลอดภัย (4.62) ด้านการแอบอ้าง (4.54) และด้านการเผยแพร่ออกนอกกลุ่ม (4.54) ส่วนด้านที่มีกลุ่มตัวอย่างมีความตระหนักในระดับมากมี 2 ด้าน คือ ด้านการข่มขู่ใส่ร้าย (4.49) และด้านการยั่วโมโห (4.43) สำหรับด้านที่มีกลุ่มตัวอย่างมีความตระหนักในระดับปานกลางมีเพียงด้านเดียว คือ ด้านการกีดกัน (3.08)

เมื่อพิจารณารายละเอียดในแต่ละด้าน พบว่า

ด้านความปลอดภัย กลุ่มตัวอย่างมีความตระหนักในระดับมากที่สุดทุกประเด็น คือ ควรหาทางป้องกันการถูกลักลอบเจาะเข้าสู่ระบบเพื่ออ่านหรือทำลายข้อมูล (4.66) ควรหาทางป้องกันการถูกโปรแกรมคอมพิวเตอร์ที่ไม่พึงประสงค์ทำความเสียหายต่อข้อมูลในระบบ (4.61) และควรหาทางป้องกันการถูกหลอกให้กรอกข้อมูลส่วนตัวทางเว็บไซต์ปลอม (4.59)

ด้านการแอบอ้าง กลุ่มตัวอย่างมีความตระหนักในระดับมากที่สุดทุกประเด็น คือ ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อผลประโยชน์ให้ตนเองผ่านทางไซเบอร์ (4.55) ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อให้ร้ายบุคคลที่สามผ่านทางไซเบอร์ (4.55) และไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นในการสนทนาผ่านทางไซเบอร์ (4.50)

ด้านการเผยแพร่ออกนอกกลุ่ม กลุ่มตัวอย่างมีความตระหนักในระดับมากที่สุดทุกประเด็น คือ ไม่ควรมีการนำเบอร์โทรศัพท์ของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต (4.57) ไม่ควรมีการนำที่อยู่ของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต (4.55) และไม่ควรมีการนำชื่อพ่อแม่หรือญาติพี่น้องของผู้อื่นไปเปิดเผยผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต (4.52)

ด้านการข่มขู่ใส่ร้าย กลุ่มตัวอย่างมีความตระหนักในระดับมากที่สุดใน 1 ประเด็น คือ ไม่ควรมีการใส่ร้ายผู้อื่นให้บุคคลที่สามเกลียดชังผ่านทางไซเบอร์ (4.55) และกลุ่มตัวอย่างมีความตระหนักในระดับมากใน 2 ประเด็น คือ ไม่ควรมีการนำภาพหรือคลิปวิดีโอที่เสื่อมเสียของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์ (4.47) และไม่ควรมีการเผยแพร่ข่าวลือในทางลบของผู้อื่นผ่านทางไซเบอร์ (4.44)

ด้านการยั่วโมโห กลุ่มตัวอย่างมีความตระหนักในระดับมากทุกประเด็น คือ ไม่ควรมีการกล่าวถึงผู้อื่นให้ได้รับความอับอายหรือเสื่อมเสียชื่อเสียงผ่านทางไซเบอร์ (4.45) ไม่ควรมีการใช้ถ้อยคำหรือข้อความที่หยาบคายด่าว่าผู้อื่นผ่านทางไซเบอร์ (4.43) ไม่ควรมีการล้อเลียนรูปร่างหน้าตาของผู้อื่นผ่านทางไซเบอร์ (4.40)

ด้านการกีดกัน กลุ่มตัวอย่างมีความตระหนักในระดับปานกลางทุกประเด็น คือ ไม่ควรมีการกดดันให้บุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางไซเบอร์ (3.43) ไม่ควรมีการลบรายชื่อบุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางไซเบอร์ (2.93) ไม่ควรมีการบล็อกข้อความสนทนาทางไซเบอร์ของบุคคลที่ไม่ชอบ (2.87)

5.1.5 สรุปผลข้อมูลการทดสอบสมมติฐาน

ผลการทดสอบสมมติฐาน พบว่า

1. ปัจจัยทางด้านลักษณะทางประชากรด้านอายุ ระดับการศึกษาสูงสุด และรายได้ส่วนตัวต่อเดือน มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต แต่ปัจจัยทางด้านลักษณะทางประชากรด้านเพศ ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต กล่าวคือ เพื่อให้ทราบผลทางลักษณะประชากรที่ส่งผลต่อความตระหนักภัยคุกคาม ที่ระบุได้จากกลุ่มตัวอย่าง ตรงกับสมมุติฐาน และนำไปสร้างแนวทางกำหนดกลุ่มเป้าหมายถึงวิธีป้องกัน

และลดความเสี่ยงจากภัยคุกคามของการโจมตีทางไซเบอร์ สามารถสร้างความตระหนักและความเข้าใจ ที่จะเกิดผลกระทบต่อตนเองจากอุปกรณ์ต่าง ๆ ในการเข้าถึงอินเทอร์เน็ต

2. ปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต กล่าวคือ การโจมตีทางไซเบอร์มีรูปแบบการพัฒนาการโจมตีหาช่องโหว่ทางอินเทอร์เน็ตหลากหลายรูปแบบทำให้ผู้อินเทอร์เน็ตไม่สามารถระวังได้ถึงภัยคุกคามทางไซเบอร์และไม่สามารถป้องกันการโจมตีที่ไม่เหมือนเดิมและได้รับความเสียหายไม่คาดคิดแตกต่างจากครั้งก่อนทำให้ไม่สามารถประเมินสถานการณ์ที่จะเกิดความเสียหายขึ้นได้

3. ปัจจัยทางด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต กล่าวคือ ทำให้ทราบถึงผู้ที่มีความรู้ทราบถึงภัยคุกคามทางไซเบอร์ส่งผลกระทบต่อตนเอง สามารถความเข้าใจถึงปัญหาที่จะเกิดความเสียหาย จากภัยคุกคามทางไซเบอร์ขึ้นล่วงหน้า ไม่ว่าจะเป็นการเปิดเผยข้อมูลบนสาธารณะ การทำธุรกรรมออนไลน์ การป้องกันให้ไม่ผู้อื่นทราบข้อมูลส่วนตัว และการติดตามข้อมูลข่าวสารการโจมตีรูปแบบใหม่ๆ การดาวโหลดโปรแกรมที่ถูกต้องมาจากผู้ผลิตโดยตรงป้องกันความเสี่ยงการฝั่งไวรัสที่ไม่คาดคิดติดมากับโปรแกรมและสามารถป้องกันภัยคุกคามจากผู้ไม่หวังดีที่จะเกิดผลกระทบความเสียหายโดยไม่คาดคิดได้

5.2 ข้อเสนอแนะ

ในการวิจัยครั้งต่อไป ถ้าจะทำการวิจัยเกี่ยวกับภัยคุกคามทางไซเบอร์ มีข้อเสนอแนะดังนี้ 1. ควรศึกษาปัจจัยทางสังคมที่อาจจะมีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตด้วย 2. ควรจะใช้การวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยการสัมภาษณ์กลุ่ม (Focus Group Interview) หรือการสัมภาษณ์เจาะลึก (In-depth Interview) เพื่อศึกษาความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในเชิงลึก และข้อมูลที่รอบด้านครบทุกมิติมากยิ่งขึ้น 3. ควรมีการศึกษานโยบายของรัฐ และองค์กรต่าง ๆ เกี่ยวกับการป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต

5.3 ข้อจำกัดในการวิจัย

การศึกษาในครั้งนี้มีข้อจำกัดด้านระยะเวลาในการค้นคว้า ทบทวน วรรณกรรม ซึ่งอาจทำให้การศึกษาปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์หาข้อมูลเชิงลึกได้อย่างไม่เพียงพอตามที่ผู้วิจัยได้ทำการศึกษามาและอาจทำให้การวิเคราะห์ประเด่นต่างๆ ไม่สามารถครอบคลุมถึงส่วนที่สำคัญ

รายการอ้างอิง

งานวิจัย/วิทยานิพนธ์

กุลวดี ราชภักดี. (2545). ความตระหนักและการปฏิบัติตนเกี่ยวกับการประหยัดพลังงานไฟฟ้าของนักศึกษาในหอพักสถาบันอุดมศึกษา เขตกรุงเทพมหานคร สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ.

พัฒนศักดิ์ บุบผาสุวรรณ. ร.ต.อ. (2546). ความตระหนักของนิสิตมหาวิทยาลัยเกษตรศาสตร์ต่ออาชญากรรมบนอินเทอร์เน็ตมหาวิทยาลัยเกษตรศาสตร์.

อนุสรณ์ กาลดิษฐ์. (2548). การศึกษาความรู้ และความตระหนักของนักศึกษาที่มีต่อปัญหาสิ่งแวดล้อมในห้องปฏิบัติการ วิศวอุตสาหการ คณะวิศวกรรมศาสตร์ในเขตกรุงเทพมหานคร. ปริญญานิพนธ์มหาวิทยาลัยศรีนครินทรวิโรฒ.

สุธาสินี อินทร์ผูก. (2548). ความตระหนักในปัญหาการจัดการมูลฝอยกับพฤติกรรมการนำมูลฝอยแห้งกลับมาใช้ซ้ำของประชาชนในเขตเทศบาลนครลำปาง การค้นคว้าแบบอิสระมหาวิทยาลัยเชียงใหม่.

อรวรรณ ปิลันธน์โอวาท. (2549). การสื่อสารเพื่อการโน้มน้าวใจ กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

ปารวีร์ บุษบาศรี. (2555). ความตระหนักรู้และทัศนคติของผู้บริหารและพนักงานต่อการประชาสัมพันธ์ภายในของบริษัทจัดการและพัฒนาทรัพยากรน้ำภาคตะวันออก จำกัด (มหาชน) การค้นคว้าอิสระมหาวิทยาลัยหอการค้าไทย.

เอกลักษณ์ ธนเจริญพิศาล. (2554). ความตระหนักและการยอมรับการนำระบบการจัดการสิ่งแวดล้อม (ISO 14001) มาใช้ในองค์การภาครัฐ:ศึกษากรณี สำนักงาน นโยบายและแผนทรัพยากรธรรมชาติและสิ่งแวดล้อมคณะพัฒนาสังคมและสิ่งแวดล้อม สถาบันบัณฑิตพัฒนาบริหารศาสตร์.

ปิยะภัสร์ โรจน์รัตนวาณิชย์. (2557). แนวทางการคุ้มครองข้อมูลใน Big Data: ความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูล มหาวิทยาลัยกรุงเทพ.

วิภารัตน์ ปทักขินัง. (2557). การพัฒนาระบบสารสนเทศสำหรับการประเมินระดับความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ ขององค์กร มหาวิทยาลัยศรีปทุม.

ชิษณุพงศ์ ธนูทอง. (2557). การพัฒนาการรักษาความมั่นคงในระบบเครือข่ายหน่วยงานภาครัฐ มหาลัยธรรมศาสตร์.

อุบลวรรณ ภีระเป็ง. (2558). การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ : ศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ”คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

ศิวลีย์ สิริโรจน์บริรักษ์. (2558). วิจัยเรื่อง การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ.

ฐิตารีย์ จันทพันธ์. (2559). วิจัย เรื่อง “การศึกษาผลกระทบการรับรู้ความเสี่ยงในการใช้งานการระบุตำแหน่ง (Location - Based Services: LBS) บนสื่อสังคมออนไลน์ ต่อความเป็นส่วนตัวของผู้ใช้งานในเขตกรุงเทพมหานคร” มหาวิทยาลัยกรุงเทพ.

อรรถพล ป้อมสถิต. (2559). การเพิ่มประสิทธิภาพระบบตรวจจับการบุกรุกในการรักษาความมั่นคงทางไซเบอร์ด้วยฮันนี่พอท มหาวิทยาลัยราชภัฏพระนคร.

Wajeb Gharibi and Maha Shaabi (2012) วิจัยเรื่อง “Cyber Threats in Social Networking Websites” College of Computer Science & Information SystemsJazan University, Kingdom of Saudi Arabia

Jaeseung Hong, Jongwung Kim, Jeonghun Cho (2010) “The Trend of the Security Research for the Insider Cyber Threat” University. Jeong Hoon Cho

Axel Tanner (2015) วิจัยเรื่อง “Gaining an Edge in Cyberspace with Advanced Situational Awareness” IBM Research

เว็บไซต์

น.ท.นิวัติ เนียมพลอย, ต.ค.-พ.ย.๕๖.ไซเบอร์ กับการรักษาความปลอดภัย และการปฏิบัติการ :โรงเรียนนายเรืออากาศ, นนอ.๓๗ สืบค้นเมื่อวันที่ 12 เมษายน 2561
จาก https://nniwat.wordpress.com/2013/11/08/2013/11/08/ไซเบอร์-กับการรักษาความ/

Pigabyte. (2561). MarketingOOPS!. สืบค้นเมื่อวันที่ 12 เมษายน 2561
จาก https://www.marketingoops.com/reports/behaviors/thailand-digital-in-2018/

หนังสือและบทความในหนังสือ

นงรัตน์ สายเพชร. (2556). ความมั่นคงไซเบอร์ของสหรัฐอเมริกา American Cyber Security: จุลสารความมั่นคงศึกษา สถาบันการข่าวกรองสำนักข่าวกรองแห่งชาติ.

วรัญญา สะอาด. (2557). ผลกระทบของระบบความปลอดภัยของข้อมูลที่มีต่อความได้เปรียบของข้อมูลของธุรกิจโรงพยาบาลเอกชนในประเทศไทย.

Herek, G.M. (1986) 'The Instrumentality of Attitudes: Toward a Neofunctional ... 42, 2, pp. 99-114.

Kim, M. s., & Hunter, J. e. Relationships Among Attitudes, Behavioral Intentions, and Behavior A Meta-Analysis of Past Research (1993),pp. 331 – 364.

ภาคผนวก

แบบสอบถาม “ปัจจัยที่มีผลต่อการตระหนักของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร”	
คำชี้แจ้ง	1.แบบสอบถามนี้เป็นส่วนหนึ่งของหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชานโยบายและการบริหารเทคโนโลยีสารสนเทศวิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์ **<u>วัตถุประสงค์</u>** แบบสอบถามนี้มีจุดประสงค์เพื่อศึกษาถึงปัจจัยและเก็บรวบรวมข้อมูลและนำข้อมูลไปใช้ในการวิเคราะห์ ในงานวิจัยเรื่อง “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร” ทั้งนี้ผลที่ได้จากแบบสอบถาม ผู้วิจัยจะนำไปเป็นแนวทางเพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตให้เกิดประสิทธิภาพสูงสุด
	2.แบบสอบถามชุดนี้แบ่งออกเป็น 4 ตอน ดังนี้ • ตอนที่ 1 ลักษณะทางประชากร • ตอนที่ 2 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ • ตอนที่ 3 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ • ตอนที่ 4 ความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์
	3.หากท่านมีข้อสงสัยเกี่ยวกับคำถามสัมภาษณ์ กรุณาติดต่อผู้วิจัย นาย สุธาเทพ รุณเรศ หมายเลขโทรศัพท์ : 087-675-7761 E-mail : <u>suthathep@outlook.com</u>

ตอนที่ 1 ลักษณะทางประชากร

คำอธิบาย :คำถามต่อไปนี้เกี่ยวข้องกับข้อมูลส่วนตัวของท่านกรุณาทำเครื่องหมาย ✓ลงในช่องว่างที่ตรงกับความคิดเห็นและข้อเท็จจริงมากที่สุด

1. เพศ

☐ 1. ชาย ☐ 2. หญิง

2. อายุ

☐ 1. ไม่เกิน 20 ปี ☐ 2. 21-30 ปี ☐ 3. 31-40 ปี

☐ 4. 41-50 ปี ☐ 5. 51-60 ปี ☐ 6. 61 ปีขึ้นไป

3. ระดับการศึกษาสูงสุด

☐ 1. ต่ำกว่าปริญญาตรี ☐ 2. ปริญญาตรี

☐ 3. ปริญญาโท ☐ 4. สูงกว่าปริญญาโท

4. รายได้ส่วนตัวต่อเดือน

☐ 1. ไม่เกิน 15,000 บาท

☐ 2. 15,001-30,000 บาท

☐ 3. 30,001-45,000 บาท

☐ 4. 45,001-60,000 บาท

☐ 5. 60,001 บาทขึ้นไป

ตอนที่ 2 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

คำอธิบาย :คำถามต่อไปนี้เกี่ยวข้องกับผลกระทบจากภัยคุกคามทางไซเบอร์ ท่านเคยประสบปัญหาเหล่านี้หรือไม่กรุณาทำเครื่องหมาย ✓ลงในช่องว่างที่ตรงกับความคิดเห็นและข้อเท็จจริงมากที่สุด

(ตอบได้มากกว่าหนึ่งคำตอบ)

☐ 1.ท่านเคยได้รับผลกระทบจากไวรัสทำให้ไฟล์หรือโปรแกรมคอมพิวเตอร์เกิดความเสียหาย

☐ 2.ท่านได้รับการก่อกวนในระบบเครือข่ายทำให้ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ

☐ 3.ท่านติดตั้งโปรแกรมที่คิดว่าปลอดภัย แต่มีโปรแกรมอันตรายแฝงตัวมา

☐ 4.ท่านถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของได้โดยท่านไม่รู้ตัว

☐ 5.ท่านถูกแอบดูพฤติกรรมหรือบันทึกการเข้าใช้งานคอมพิวเตอร์

☐ 6.ท่านโดนขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน

☐ 7.ท่านไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นจะได้รับข้อความ “เรียกค่าไถ่”

☐ 8.ท่านถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าระบบ

☐ 9.ท่านเคยได้รับจดหมายอิเล็กทรอนิกส์หลอกลวง

☐ 10.ท่านเคยได้รับโฆษณาที่ไม่พึงประสงค์จะได้รับ

ตอนที่ 3 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

คำอธิบาย :คำถามต่อไปนี้เกี่ยวข้องกับปัจจัยความรู้ การใช้งาน การทำธุรกรรม และการกระทำกิจกรรมต่างๆ บนอิเล็คทรอนิกส์ของท่านกรุณาทำเครื่องหมาย ✓ลงในช่องว่างที่ตรงกับความคิดเห็นและข้อเท็จจริงมากที่สุด

ท่านคิดว่า ข้อความต่อไปนี้ใช่หรือไม่ใช่

(ตอบได้ข้อละหนึ่งคำตอบ)

ข้อความ	ใช่	ไม่ใช่	ไม่แน่ใจ
1.การเข้าเว็บไซต์ https มีความปลอดภัยมากกว่า http			
2.การเปิดเผยระบุตำแหน่งตัวตนบนเครือข่ายสังคมออนไลน์สาธารณะที่มีผู้ใช้ทั่วไปมีความปลอดภัย			
3.การให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะไม่มีความเสี่ยง			
4.การเข้าใช้เครือข่ายไร้สายสาธารณะมีความเสี่ยงต่อการทำธุรกรรมออนไลน์			
5.การติดตามข่าวสารรูปแบบโจมตีทางไซเบอร์สามารถป้องกันความ			

ข้อความ	ใช่	ไม่ใช่	ไม่แน่ใจ
เสียหายที่จะเกิดขึ้นได้			
6.การตั้งรหัสผ่าน (Password) ควรตั้งให้ปนกันทั้งตัวอักษรใหญ่-เล็ก ตัวเลข สัญลักษณ์พิเศษ และยาวอย่างน้อย 8 ตัวอักษร			
7.การตั้งรหัสผ่าน (Password) สำหรับเครื่องมือและเว็บไซต์ต่าง ๆ ควรจะเหมือนกัน			
8.การใช้โปรแกรมถูกลิขสิทธิ์มีความเสี่ยงพอ ๆ กับโปรแกรมที่ไม่ถูกลิขสิทธิ์			
9.การสำรองข้อมูลและตั้งรหัสเข้าใช้ทำให้มีความปลอดภัยมากขึ้น			
10.การโหลดแอปพลิเคชันที่มีชื่อเหมือนกับโปรแกรมที่มีชื่อเสียงจะมีความปลอดภัย			

<u>ตอนที่ 4 ความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์</u>

คำอธิบาย :คำถามต่อไปนี้เกี่ยวข้องกับความคิดเห็นความตระหนักของท่านกรุณาทำเครื่องหมาย ✓ ลงในช่องว่างที่ตรงกับความคิดเห็นและข้อเท็จจริงมากที่สุด

5	หมายถึง	เห็นด้วยอย่างยิ่ง
4	หมายถึง	เห็นด้วย
3	หมายถึง	ไม่แน่ใจ
2	หมายถึง	ไม่เห็นด้วย
1	หมายถึง	ไม่เห็นด้วยอย่างยิ่ง

<u>(ตอบได้ข้อละหนึ่งคำตอบ)</u>

ข้อความ	ระดับ				
	5	4	3	2	1
1. ความปลอดภัย (Security)					
1.1 ควรหาทางป้องกันการถูกโปรแกรมคอมพิวเตอร์ที่ไม่พึงประสงค์ทำความเสียหายต่อข้อมูลในระบบ					
1.2 ควรหาทางป้องกันการถูกหลอกให้กรอกข้อมูลส่วนตัวทางเว็บไซต์ปลอม					
1.3 ควรหาทางป้องกันการถูกลักลอบเจาะเข้าสู่ระบบเพื่ออ่านหรือทำลาย					

ข้อความ	ระดับ				
	5	4	3	2	1
ข้อมูล					
2. การยั่วโมโห (Flaming)					
2.1 ไม่ควรมีการกล่าวถึงผู้อื่นให้ได้รับความอับอายหรือเสื่อมเสียชื่อเสียงผ่านทางไซเบอร์					
2.2 ไม่ควรมีการใช้ถ้อยคำหรือข้อความที่หยาบคายด่าว่าผู้อื่นผ่านทางไซเบอร์					
2.3 ไม่ควรมีการล้อเลียนรูปร่างหน้าตาของผู้อื่นผ่านทางไซเบอร์					
3. การข่มขู่ใส่ร้าย (Harassment)					
3.1 ไม่ควรมีการใส่ร้ายผู้อื่นให้บุคคลที่สามเกลียดชังผ่านทางไซเบอร์					
3.2 ไม่ควรมีการนำภาพหรือคลิปวิดีโอที่เสื่อมเสียของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์					
3.3 ไม่ควรมีการเผยแพร่ข่าวลือในทางลบของผู้อื่นผ่านทางไซเบอร์					
4. การแอบอ้าง (Masquerading)					
4.1 ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นในการสนทนาผ่านทางไซเบอร์					
4.2 ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อผลประโยชน์ให้ตนเองผ่านทางไซเบอร์					
4.3 ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อให้ร้ายบุคคลที่สามผ่านทางไซเบอร์					
5. การเผยแพร่ออกนอกกลุ่ม (Outing)					
5.1 ไม่ควรมีการนำชื่อพ่อแม่หรือญาติพี่น้องของผู้อื่นไปเปิดเผยผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต					
5.2 ไม่ควรมีการนำที่อยู่ของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต					
5.3 ไม่ควรมีการนำเบอร์โทรศัพท์ของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต					
6. การกีดกัน (Exclusion)					
6.1 ไม่ควรมีการบล็อกข้อความสนทนาทางไซเบอร์ของบุคคลที่ไม่ชอบ					

ข้อความ	ระดับ				
	5	4	3	2	1
6.2 ไม่ควรมีการลบรายชื่อบุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางไซเบอร์					
6.3 ไม่ควรมีการกดดันให้บุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางไซเบอร์					

การประมวลผลข้อมูล SPSS

ผลข้อมูลการวิเคราะห์ค่าความถี่ร้อยละ Frequencies

เพศ

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ชาย	190	47.5	47.5	47.5
	หญิง	210	52.5	52.5	100.0
	Total	400	100.0	100.0	

อายุ

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เกิน20ปี	15	3.8	3.8	3.8
	21-30ปี	159	39.8	39.8	43.5
	31-40ปี	141	35.3	35.3	78.8
	41-50ปี	49	12.3	12.3	91.0
	51-60ปี	33	8.3	8.3	99.3
	61ปีขึ้นไป	3	.8	.8	100.0
	Total	400	100.0	100.0	

ระดับการศึกษาสูงสุด

	Frequency	Percent	Valid Percent	Cumulative Percent

Valid	ต่ำกว่าป.ตรี	29	7.2	7.2	7.2
	ป.ตรี	209	52.3	52.3	59.5
	ป.โท	153	38.3	38.3	97.8
	สูงกว่าป.โท	9	2.3	2.3	100.0
	Total	400	100.0	100.0	

รายได้ส่วนตัวต่อเดือน

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เกิน 15,000 บาท	78	19.5	19.5	19.5
	15,001-30,000 บาท	157	39.3	39.3	58.8
	30,001-45,000 บาท	84	21.0	21.0	79.8
	45,001-60,000 บาท	27	6.8	6.8	86.5
	60,001 บาทขึ้นไป	54	13.5	13.5	100.0
	Total	400	100.0	100.0	

1.ท่านเคยได้รับผลกระทบจากไวรัสทำให้ไฟล์หรือโปรแกรมคอมพิวเตอร์เกิดความเสียหาย

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เคย	71	17.8	17.8	17.8
	เคย	329	82.3	82.3	100.0
	Total	400	100.0	100.0	

2.ท่านได้รับการก่อกวนในระบบเครือข่ายทำให้ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เคย	252	63.0	63.0	63.0
	เคย	148	37.0	37.0	100.0
	Total	400	100.0	100.0	

3.ท่านติดตั้งโปรแกรมที่คิดว่าปลอดภัย แต่มีโปรแกรมอันตรายแฝงตัวมา

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เคย	177	44.3	44.3	44.3
	เคย	223	55.8	55.8	100.0
	Total	400	100.0	100.0	

4.ท่านถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของได้โดยท่านไม่รู้ตัว

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เคย	331	82.8	82.8	82.8
	เคย	69	17.3	17.3	100.0
	Total	400	100.0	100.0	

5.ท่านถูกแอบดูพฤติกรรมหรือบันทึกการเข้าใช้งานคอมพิวเตอร์

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เคย	340	85.0	85.0	85.0
	เคย	60	15.0	15.0	100.0
	Total	400	100.0	100.0	

6.ท่านโดนขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เคย	355	88.8	88.8	88.8
	เคย	45	11.3	11.3	100.0
	Total	400	100.0	100.0	

7.ท่านไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นจะได้รับข้อความ "เรียกค่าไถ่"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เคย	375	93.8	93.8	93.8
	เคย	25	6.3	6.3	100.0
	Total	400	100.0	100.0	

8.ท่านถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าระบบ

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เคย	283	70.8	70.8	70.8
	เคย	117	29.3	29.3	100.0
	Total	400	100.0	100.0	

9.ท่านเคยได้รับจดหมายอิเล็กทรอนิกส์หลอกลวง

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เคย	190	47.5	47.5	47.5
	เคย	210	52.5	52.5	100.0
	Total	400	100.0	100.0	

10.ท่านเคยได้รับโฆษณาไม่พึงประสงค์

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ไม่เคย	128	32.0	32.0	32.0
	เคย	272	68.0	68.0	100.0
	Total	400	100.0	100.0	

1.การเข้าเว็บไซต์ https มีความปลอดภัยมากกว่า http

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ตอบผิด	252	63.0	63.0	63.0
	ตอบถูก	148	37.0	37.0	100.0
	Total	400	100.0	100.0	

2.การเปิดเผยระบุตำแหน่งตัวตนบนเครือข่ายสังคมออนไลน์ปลอดภัย

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ตอบผิด	127	31.8	31.8	31.8
	ตอบถูก	273	68.3	68.3	100.0
	Total	400	100.0	100.0	

3.การให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะไม่มีความเสี่ยง

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ตอบผิด	206	51.5	51.5	51.5
	ตอบถูก	194	48.5	48.5	100.0
	Total	400	100.0	100.0	

4.การเข้าใช้เครือข่ายไร้สายสาธารณะมีความเสี่ยงต่อการทำธุรกรรมออนไลน์

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ตอบผิด	58	14.5	14.5	14.5
	ตอบถูก	342	85.5	85.5	100.0
	Total	400	100.0	100.0	

5.การติดตามข่าวสารรูปแบบโจมตีทางไซเบอร์สามารถป้องกันความเสียหาย

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ตอบผิด	74	18.5	18.5	18.5
	ตอบถูก	326	81.5	81.5	100.0
	Total	400	100.0	100.0	

6.การตั้งรหัสผ่าน (**Password**) ควรตั้งให้ปนกันทั้งตัวอักษรใหญ่-เล็ก

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ตอบผิด	127	31.8	31.8	31.8
	ตอบถูก	273	68.3	68.3	100.0
	Total	400	100.0	100.0	

7.การตั้งรหัสผ่าน (**Password**) สำหรับเครื่องมือและเว็บไซต์ต่าง ๆ ควรจะเหมือนกัน

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ตอบผิด	71	17.8	17.8	17.8
	ตอบถูก	329	82.3	82.3	100.0
	Total	400	100.0	100.0	

8.การใช้โปรแกรมลูกลิขสิทธิ์มีความเสี่ยงพอ ๆ กับโปรแกรมที่ไม่ลูกลิขสิทธิ์

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ตอบผิด	122	30.5	30.5	30.5
	ตอบถูก	278	69.5	69.5	100.0
	Total	400	100.0	100.0	

9.การสำรองข้อมูลและตั้งรหัสเข้าใช้ทำให้มีความปลอดภัยมากขึ้น

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ตอบผิด	197	49.3	49.3	49.3
	ตอบถูก	203	50.7	50.7	100.0
	Total	400	100.0	100.0	

10.การโหลดแอพที่มีชื่อเหมือนกับโปรแกรมที่มีชื่อเสียงจะมีความปลอดภัย

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ตอบผิด	212	53.0	53.0	53.0
	ตอบถูก	188	47.0	47.0	100.0
	Total	400	100.0	100.0	

ประสบการณ์(กลุ่ม)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	น้อย	194	48.5	48.5	48.5
	ปานกลาง	178	44.5	44.5	93.0
	มาก	28	7.0	7.0	100.0
	Total	400	100.0	100.0	

ความรู้(กลุ่ม)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	น้อย	35	8.8	8.8	8.8
	ปานกลาง	160	40.0	40.0	48.8
	มาก	205	51.2	51.2	100.0
	Total	400	100.0	100.0	

ผลข้อมูลการวิเคราะห์ค่าเฉลี่ย Descriptives

Descriptive Statistics			
	N	Mean	Std. Deviation
1. ความปลอดภัย (Security)	400	4.62	.64
1.1 ควรหาทางป้องกันการถูกโปรแกรมคอมพิวเตอร์ที่ไม่พึงประสงค์ทำความเสียหายต่อข้อมูลในระบบ	400	4.61	.69
1.2 ควรหาทางป้องกันการถูกหลอกให้กรอกข้อมูลส่วนตัวทางเว็บไซต์ปลอม	400	4.58	.73
1.3 ควรหาทางป้องกันการถูกลักลอบเจาะเข้าสู่ระบบเพื่ออ่านหรือทำลายข้อมูล	400	4.66	.67
2. การยั่วโมโห (Flaming)	400	4.43	.65
2.1 ไม่ควรมีการกล่าวถึงผู้อื่นให้ได้รับความอับอายหรือเสื่อมเสียชื่อเสียงผ่านทางไซเบอร์	400	4.45	.74
2.2 ไม่ควรมีการใช้ถ้อยคำหรือข้อความที่หยาบคายด่าว่าผู้อื่นผ่านทาง ไซเบอร์	400	4.43	.73
2.3 ไม่ควรมีการล้อเลียนรูปร่างหน้าตาของผู้อื่นผ่านทางไซเบอร์	400	4.40	.78
3. การข่มขู่ไส่ร้าย (Harassment)	400	4.49	.59
3.1 ไม่ควรมีการใส่ร้ายผู้อื่นให้บุคคลที่สามเกลียดชังผ่านทางไซเบอร์	400	4.55	.62
3.2 ไม่ควรมีการนำภาพหรือคลิปวิดีโอที่เสื่อมเสียของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์	400	4.47	.67
3.3 ไม่ควรมีการเผยแพร่ข่าวลือในทางลบของผู้อื่นผ่านทางไซเบอร์	400	4.44	.69
4. การแอบอ้าง (Masquerading)	400	4.54	.56
4.1 ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นในการสนทนาผ่านทาง ไซเบอร์	400	4.50	.65
4.2 ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อผลประโยชน์ให้ตนเองผ่านทางไซเบอร์	400	4.55	.59
4.3 ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อให้ร้ายบุคคลที่สามผ่านทางไซเบอร์	400	4.55	.59
5. การเผยแพร่ออกนอกกลุ่ม (Outing)	400	4.54	.58
5.1 ไม่ควรมีการนำชื่อพ่อแม่หรือญาติพี่น้องของผู้อื่นไปเปิดเผยผ่านทาง	400	4.52	.64
5.2 ไม่ควรมีการนำที่อยู่ของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต	400	4.55	.62

ผลข้อมูลการวิเคราะห์ค่าเฉลี่ย Descriptives (ต่อ)

5.3 ไม่ควรมีการนำเบอร์โทรศัพท์ของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์โดยไม่ได้รับอนุญาต	400	4.57	.62
6. การกีดกัน (Exclusion)	400	3.08	1.04
6.1 ไม่ควรมีการบล็อกข้อความสนทนาทางไซเบอร์ของบุคคลที่ไม่ชอบ	400	2.87	1.23
6.2 ไม่ควรมีการลบรายชื่อบุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางไซเบอร์	400	2.93	1.19
6.3 ไม่ควรมีการกดดันให้บุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางไซเบอร์	400	3.43	1.10
ความตระหนัก	400	4.28	.46
Valid N (listwise)	400		

ผลข้อมูลการ5วิเคราะห์ค่าความแตกต่างของค่าเฉลี่ย T-Test

Group Statistics

	เพศ	N	Mean	Std. Deviation	Std. Error Mean
ความตระหนัก	ชาย	190	4.2743	.50075	.03633
	หญิง	210	4.2881	.41152	.02840

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means					
								95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
ความพึงพอใจ	Equal variances assumed	2.456	.118	-.303	398	.762	-.01383	.04566	-.10360	.07595
	Equal variances not assumed			-.300	366.721	.764	-.01383	.04611	-.10450	.07685

ผลข้อมูลการวิเคราะห์ค่าความแปรปรวน F-Test

Descriptives

ความตระหนัก

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
ไม่เกิน20ปี	15	3.8704	.69695	.17995	3.4844	4.2563	2.17	5.00
21-30ปี	159	4.2900	.47683	.03781	4.2153	4.3647	2.17	5.00
31-40ปี	141	4.2277	.41448	.03491	4.1587	4.2967	3.17	5.00
41-50ปี	49	4.4524	.40572	.05796	4.3358	4.5689	3.56	5.00
51ปีขึ้นไป	36	4.3935	.30671	.05112	4.2897	4.4973	3.72	5.00
Total	400	4.2815	.45556	.02278	4.2367	4.3263	2.17	5.00

ANOVA

ความตระหนัก

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4.837	4	1.209	6.126	.000
Within Groups	77.969	395	.197		
Total	82.806	399			

Multiple Comparisons

Dependent Variable: ความตระหนัก

Scheffe

(I) อายุก	(J) อายุก	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
ไม่เกิน20ปี	21-30ปี	-.41964*	.12000	.017	-.7910	-.0482
	31-40ปี	-.35737	.12066	.069	-.7308	.0161
	41-50ปี	-.58201*	.13110	.001	-.9878	-.1763
	51ปีขึ้นไป	-.52315*	.13654	.006	-.9457	-.1006
21-30ปี	ไม่เกิน20ปี	.41964*	.12000	.017	.0482	.7910
	31-40ปี	.06227	.05139	.832	-.0968	.2213
	41-50ปี	-.16237	.07259	.289	-.3870	.0623
	51ปีขึ้นไป	-.10351	.08200	.810	-.3573	.1503
31-40ปี	ไม่เกิน20ปี	.35737	.12066	.069	-.0161	.7308
	21-30ปี	-.06227	.05139	.832	-.2213	.0968
	41-50ปี	-.22464	.07368	.056	-.4527	.0034
	51ปีขึ้นไป	-.16578	.08296	.408	-.4225	.0910
41-50ปี	ไม่เกิน20ปี	.58201*	.13110	.001	.1763	.9878
	21-30ปี	.16237	.07259	.289	-.0623	.3870
	31-40ปี	.22464	.07368	.056	-.0034	.4527
	51ปีขึ้นไป	.05886	.09753	.985	-.2430	.3607
51ปีขึ้นไป	ไม่เกิน20ปี	.52315*	.13654	.006	.1006	.9457
	21-30ปี	.10351	.08200	.810	-.1503	.3573
	31-40ปี	.16578	.08296	.408	-.0910	.4225
	41-50ปี	-.05886	.09753	.985	-.3607	.2430

*. The mean difference is significant at the 0.05 level.

ความตระหนัก

Scheffe[a,b]

อายุก	N	Subset for alpha = 0.05	
		1	2
ไม่เกิน20ปี	15	3.8704	
31-40ปี	141		4.2277
21-30ปี	159		4.2900
51ปีขึ้นไป	36		4.3935
41-50ปี	49		4.4524
Sig.		1.000	.291

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 38.991.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

Descriptives

ความตระหนัก

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
ต่ำกว่าป.ตรี	29	4.0211	.58483	.10860	3.7986	4.2435	2.17	5.00
ป.ตรี	209	4.2953	.43838	.03032	4.2355	4.3551	2.17	5.00
ป.โทขึ้นไป	162	4.3104	.43962	.03454	4.2421	4.3786	3.17	5.00
Total	400	4.2815	.45556	.02278	4.2367	4.3263	2.17	5.00

ANOVA

ความตระหนัก

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2.142	2	1.071	5.270	.006
Within Groups	80.664	397	.203		
Total	82.806	399			

Multiple Comparisons

Dependent Variable: ความตระหนัก

Scheffe

(I) ระดับการศึกษาสูงสุดก	(J) ระดับการศึกษาสูงสุดก	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
ต่ำกว่าป.ตรี	ป.ตรี	-.27425*	.08932	.009	-.4937	-.0548
	ป.โทขึ้นไป	-.28928*	.09089	.007	-.5126	-.0660
ป.ตรี	ต่ำกว่าป.ตรี	.27425*	.08932	.009	.0548	.4937
	ป.โทขึ้นไป	-.01504	.04718	.951	-.1310	.1009
ป.โทขึ้นไป	ต่ำกว่าป.ตรี	.28928*	.09089	.007	.0660	.5126
	ป.ตรี	.01504	.04718	.951	-.1009	.1310

*. The mean difference is significant at the 0.05 level.

ความตระหนัก

Scheffe[a,b]

ระดับการศึกษาสูงสุดก	N	Subset for alpha = 0.05	
		1	2
ต่ำกว่าป.ตรี	29	4.0211	
ป.ตรี	209		4.2953
ป.โทขึ้นไป	162		4.3104
Sig.		1.000	.982

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 66.021.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

Descriptives

ความตระหนัก

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
ไม่เกิน 15,000 บาท	78	4.1902	.50835	.05756	4.0756	4.3048	2.17	5.00
15,001-30,000 บาท	157	4.2360	.46377	.03701	4.1629	4.3091	2.17	5.00
30,001-45,000 บาท	84	4.3737	.46779	.05104	4.2722	4.4752	3.33	5.00
45,001-60,000 บาท	27	4.4424	.32957	.06343	4.3120	4.5728	3.78	5.00
60,001 บาทขึ้นไป	54	4.3220	.33340	.04537	4.2310	4.4130	3.72	5.00
Total	400	4.2815	.45556	.02278	4.2367	4.3263	2.17	5.00

ANOVA

ความตระหนัก

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2.477	4	.619	3.044	.017
Within Groups	80.330	395	.203		
Total	82.806	399			

Multiple Comparisons

Dependent Variable: ความตระหนัก

LSD

(I) รายได้ส่วนตัวต่อเดือน	(J) รายได้ส่วนตัวต่อเดือน	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
ไม่เกิน 15,000 บาท	15,001-30,000 บาท	-.04585	.06247	.463	-.1687	.0770
	30,001-45,000 บาท	-.18351*	.07091	.010	-.3229	-.0441
	45,001-60,000 บาท	-.25222*	.10069	.013	-.4502	-.0543
	60,001 บาทขึ้นไป	-.13185	.07983	.099	-.2888	.0251
15,001-30,000 บาท	ไม่เกิน 15,000 บาท	.04585	.06247	.463	-.0770	.1687
	30,001-45,000 บาท	-.13765*	.06096	.024	-.2575	-.0178
	45,001-60,000 บาท	-.20636*	.09395	.029	-.3911	-.0217
	60,001 บาทขึ้นไป	-.08599	.07114	.227	-.2259	.0539
30,001-45,000 บาท	ไม่เกิน 15,000 บาท	.18351*	.07091	.010	.0441	.3229
	15,001-30,000 บาท	.13765*	.06096	.024	.0178	.2575
	45,001-60,000 บาท	-.06871	.09977	.491	-.2648	.1274
	60,001 บาทขึ้นไป	.05166	.07866	.512	-.1030	.2063
45,001-60,000 บาท	ไม่เกิน 15,000 บาท	.25222*	.10069	.013	.0543	.4502
	15,001-30,000 บาท	.20636*	.09395	.029	.0217	.3911
	30,001-45,000 บาท	.06871	.09977	.491	-.1274	.2648
	60,001 บาทขึ้นไป	.12037	.10629	.258	-.0886	.3293
60,001 บาทขึ้นไป	ไม่เกิน 15,000 บาท	.13185	.07983	.099	-.0251	.2888
	15,001-30,000 บาท	.08599	.07114	.227	-.0539	.2259
	30,001-45,000 บาท	-.05166	.07866	.512	-.2063	.1030
	45,001-60,000 บาท	-.12037	.10629	.258	-.3293	.0886

*. The mean difference is significant at the 0.05 level.

ผลข้อมูลการวิเคราะห์ค่าสหสัมพันธ์ Pearson

Correlations

		ประสบการณ์	ความตระหนัก
ประสบการณ์	Pearson Correlation	1	.073
	Sig. (2-tailed)		.143
	N	400	400
ความตระหนัก	Pearson Correlation	.073	1
	Sig. (2-tailed)	.143	
	N	400	400

ล

Correlations

		ความรู้	ความตระหนัก
ความรู้	Pearson Correlation	1	.376**
	Sig. (2-tailed)		.000
	N	400	400
ความตระหนัก	Pearson Correlation	.376**	1
	Sig. (2-tailed)	.000	
	N	400	400

**. Correlation is significant at the 0.01 level (2-tailed).

ประวัติผู้เขียน

ชื่อ	นาย สุธาเทพ รุณเรศ	
วันเดือนปีเกิด	26 สิงหาคม พ.ศ.2527	
ตำแหน่ง	ผู้ดูแลระบบเทคโนโลยีสารสนเทศ	
ประสบการณ์ทำงาน	2553-2555	เจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศ บริษัท สมาร์ท แอนด์ สไมล์ จำกัด
	2553 –2555	เจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศ บริษัท แสงทองผ้าใบ จำกัด
	2553 – ปัจจุบัน	เจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศ บริษัท เฟรทเวย์อินเตอร์เนชั่นแนล จำกัด
	2560 – ปัจจุบัน	เจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศ มูลนิธิ ไร้ท์ ทู เพลย์ ประเทศไทย