



ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูล
สารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศ
และการสื่อสารขององค์กรภาครัฐแห่งหนึ่ง

RELATIONSHIP BETWEEN BIG 5 PERSONALITY TRAITS
AND INFORMATION SECURITY BEHAVIOR OF EMPLOYEES
AT INFORMATION AND COMMUNICATION TECHNOLOGY
OF A SELECTED PUBLIC ORGANIZATION

ศิริพร ลิ้มรังษี
SIRIPORN LIMRUNGSI

การค้นคว้าอิสระเสนอต่อมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาบริหารธุรกิจมหาบัณฑิต
ปีการศึกษา 2561



ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูล
สารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศ
และการสื่อสารขององค์กรภาครัฐแห่งหนึ่ง

RELATIONSHIP BETWEEN BIG 5 PERSONALITY TRAITS
AND INFORMATION SECURITY BEHAVIOR OF EMPLOYEES
AT INFORMATION AND COMMUNICATION TECHNOLOGY
OF A SELECTED PUBLIC ORGANIZATION

ศิริพร ลิ้มรังษี

SIRIPORN LIMRUNGSI

การค้นคว้าอิสระเสนอต่อมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาบริหารธุรกิจมหาบัณฑิต

ปีการศึกษา 2561

ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

ชื่อการค้นคว้าอิสระ ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบ กับพฤติกรรมกรมกรใช้ข้อมูล
สารสนเทศอย่างปลอดภัย ของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศ
และการสื่อสารขององค์การภาครัฐแห่งหนึ่ง

ชื่อ นามสกุล นางสาวศิริพร ลิ้มรังษี

ชื่อปริญญา บริหารธุรกิจมหาบัณฑิต

กลุ่มวิชา การจัดการ

คณะ บริหารธุรกิจ

อาจารย์ที่ปรึกษา ดร.สุจิตรา ไชยกุลสินธุ์

คณะกรรมการสอบการค้นคว้าอิสระได้ให้ความเห็นชอบการค้นคว้าอิสระฉบับนี้แล้ว



..... ประธานกรรมการ

(ดร.ชัยเสฏฐ์ พรหมศรี)



..... กรรมการ

(ดร.ณัฐชา อ่างโชติ)



..... กรรมการ

(ดร.สุจิตรา ไชยกุลสินธุ์)

คณะบริหารธุรกิจ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร อนุมัติให้นับการค้นคว้าอิสระ

ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรบริหารธุรกิจมหาบัณฑิต

มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร



..... คณบดีคณะบริหารธุรกิจ

(ดร.รัตนาวลี ไม้สัก)

วันที่ 27 เดือน กุมภาพันธ์ พ.ศ. 2562

ชื่อการค้นคว้าอิสระ

ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบ
กับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย
ของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศ
และการสื่อสารขององค์การภาครัฐแห่งหนึ่ง

ชื่อ สกุล

ศิริพร ลิ้มรังษี

ชื่อปริญญา

บริหารธุรกิจมหาบัณฑิต

กลุ่มวิชา

การจัดการ

คณะ

บริหารธุรกิจ

ปีการศึกษา

2561

บทคัดย่อ

การศึกษาเรื่อง ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภาครัฐแห่งหนึ่ง มีวัตถุประสงค์เพื่อศึกษาบุคลิกภาพห้าองค์ประกอบของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ศึกษาพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และ ศึกษาความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย จำแนกตามลักษณะส่วนบุคคล ประชากรที่ใช้ในการศึกษาคั้งนี้ คือ พนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทั้งหมดจำนวน 65 คน โดยใช้แบบสอบถามในการเก็บรวบรวมข้อมูล พารามิเตอร์ที่ใช้สำหรับวิเคราะห์ข้อมูล ได้แก่ ค่าความถี่ ค่าร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน

ผลการวิเคราะห์ข้อมูลพบว่า ส่วนใหญ่เป็นเพศหญิงอายุ 20-30 ปี มีระดับการศึกษาปริญญาตรี มีตำแหน่งเป็นพนักงานราชการ ประสบการณ์ในการทำงาน 5 ปี/เท่ากับ 5 ปี ระยะเวลาการทำงานในตำแหน่งปัจจุบันน้อยกว่า 5 ปี รายได้เฉลี่ยสูงสุดอยู่ที่ 20,001 บาทขึ้นไป และผู้ตอบแบบสอบถามส่วนใหญ่มีบุคลิกภาพห้าองค์ประกอบ โดยภาพรวม พบว่า บุคลิกภาพแบบมีจิตสำนึกมีค่าเฉลี่ยสูงสุด บุคลิกภาพแบบเปิดประสบการณ์ บุคลิกภาพแบบประนีประนอม บุคลิกภาพแบบแสดงตัวมีค่าเฉลี่ยอยู่ในระดับมาก และบุคลิกภาพแบบหวั่นไหวมีค่าเฉลี่ยอยู่ใน

ระดับปานกลาง ผลวิเคราะห์พฤติกรรมการใช้ข้อมูลสารสนเทศ พบว่า พฤติกรรมการใช้รหัสผ่าน ค่าเฉลี่ยสูงสุดคือท่านได้บอกรหัสผ่านกับผู้อื่น พฤติกรรมการใช้โปรแกรมซอฟต์แวร์ไม่พึงประสงค์ ค่าเฉลี่ยสูงสุดมีการติดตั้งโปรแกรม Antivirus, Firewall, และโปรแกรมป้องกันการสอดส่องการใช้งานคอมพิวเตอร์ของ พฤติกรรมการถูกลอกลวงค่าเฉลี่ยสูงสุดพบว่าพนักงานในสังกัดมั่นใจว่าไม่ใช่เหยื่อของการถูกลอกลวงเนื่องจากเป็นบุคคลทั่วไปที่ไม่ใช่เป้าหมาย พฤติกรรมในด้านการโจมตีทางวิศวกรรมสังคม ค่าเฉลี่ยสูงสุด คือ ท่านเต็มใจที่จะปฏิบัติตามข้อกำหนดหรือข้อบังคับที่กำหนดโดยบุคคลที่มีอำนาจรับผิดชอบ และสุดท้ายพฤติกรรมการถูกลอกลวงทางออนไลน์ ค่าเฉลี่ยสูงสุด คือ ไว้ใจข้อมูลของคนแปลกหน้าบนอินเทอร์เน็ต สำหรับความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับการใช้ข้อมูลสารสนเทศอย่างปลอดภัย พบว่า บุคลิกภาพแบบเปิดประสบการณ์มีความสัมพันธ์กับพฤติกรรมการใช้ซอฟต์แวร์ที่ไม่พึงประสงค์ พฤติกรรมการถูกลอกลวง บุคลิกภาพแบบประนีประนอมมีความสัมพันธ์กับพฤติกรรมการถูกลอกลวง และบุคลิกภาพแบบมีจิตสำนึกมีความสัมพันธ์กับพฤติกรรมการถูกลอกลวง

คำสำคัญ : บุคลิกภาพห้าองค์ประกอบ, พฤติกรรมการใช้ข้อมูลสารสนเทศ



Independent Study Title	Relationship between big 5 Personality Traits and Information Security Behavior of Employees at Information and Communication Technology of a selected Public Organization
Author	Siriporn Limrungsi
Degree	Master of Business Administration
Field Study	Management
Academic Year	2018

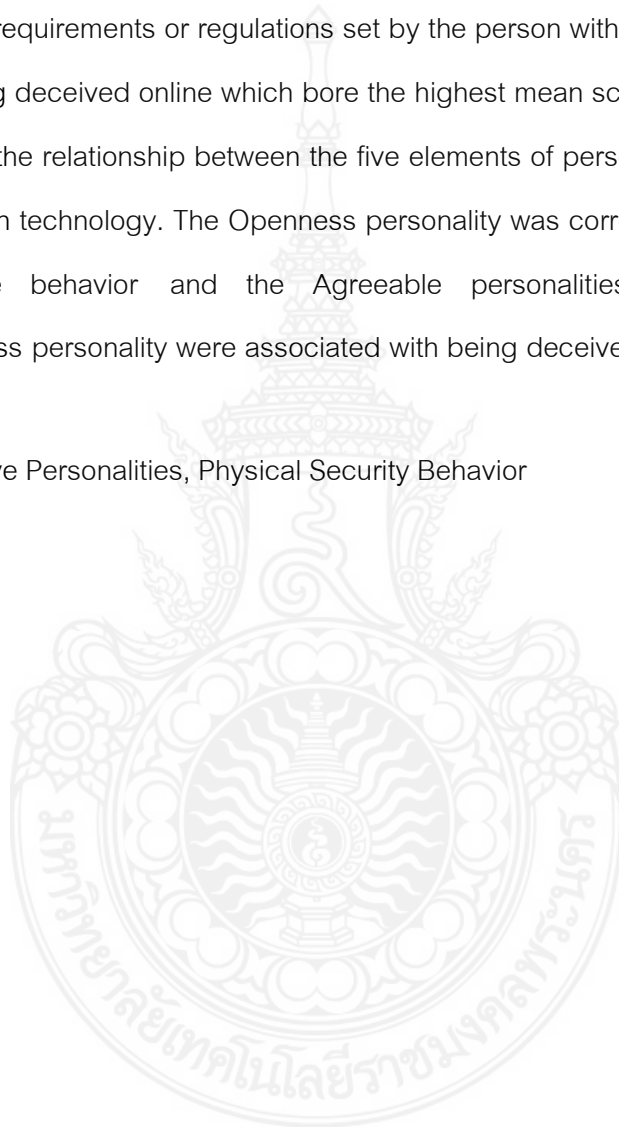
Abstract

The study was destined to investigate the Relationship between big 5 personality traits and information security behavior of employees at information and communication technology of a selected public organization. The population used in this study was 65 employees working in Information and Communication Technology center who responded to the questionnaire for the data collection. The statistics used for the data analysis included frequency, percentage, mean, and standard deviations.

The results of the data analysis showed that most of the respondents were females aged between 20 and 30 years old holding bachelor's degrees. They had experience working government officers for five years but had been in the position for less than five years. Their highest average income was 20,001 baht or more. Concerning the five personality elements, the overall respondents had the highest mean of the Conscientiousness personality. Openness, Agreeableness, and Extraversion personality had high level of mean scores while Neuroticism personality was in moderate level. The analysis of IT use behavior showed that average password usage behavior was the highest in telling others their passwords. In case of the behavior using unwanted software programs, the highest mean was relevant to the installation of

antivirus, firewall, and protection programs used to monitor the computer usage. Regarding the deception behavior, it can be found that employees were at the highest confident that they were not victims of fraud for they were only general not the targeted ones. As for social engineering attacks, the highest mean fell onto the willingness to comply with the requirements or regulations set by the person with authority. Finally, the behavior of being deceived online which bore the highest mean score on trusting online strangers while the relationship between the five elements of personality and the safely use of information technology. The Openness personality was correlated with unwanted software usage behavior and the Agreeable personalities as well as the Conscientiousness personality were associated with being deceived behavior.

Keywords: Big five Personalities, Physical Security Behavior



กิตติกรรมประกาศ

การค้นคว้าอิสระเล่มนี้ สำเร็จสมบูรณ์ได้ด้วยความช่วยเหลืออย่างสูงจาก ดร.สุจิตรา ไชยกุลสินธุ์ อาจารย์ที่ปรึกษาการค้นคว้าอิสระ ดร.ชัยเสฏฐ์ พรหมศรี และ ดร.ณัฐชา อัมรังโชติ คณะกรรมการค้นคว้าอิสระ ที่ได้กรุณาใช้เวลาอันมีค่า ให้คำปรึกษา แนะนำ และให้แนวทางในการปรับปรุงการค้นคว้าอิสระเล่มนี้ ให้มีความถูกต้องสมบูรณ์ครบถ้วนด้วยความเอาใจใส่โดยตลอด ผู้วิจัยขอกราบขอบพระคุณอย่างสูงมา ณ โอกาสนี้

ขอขอบพระคุณผู้ที่ให้ข้อมูลทุก ๆ ท่าน ผู้ที่มีชื่อในบรรณานุกรม คณาจารย์ เจ้าหน้าที่ เพื่อน ๆ และบิดามารดา พี่น้อง ที่ช่วยชี้แนะแนวทาง และเป็นกำลังใจด้วยดีตลอดมา

คุณค่าและประโยชน์อันพึงเกิดจากการค้นคว้าอิสระเล่มนี้ ขอมอบให้แก่บิดา มารดา ครู อาจารย์ เพื่อน ๆ ปริญญาโทคณะบริหารธุรกิจ และผู้ที่สนใจที่จะศึกษาค้นคว้าเรื่อง ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสารขององค์การภาครัฐแห่งหนึ่ง ซึ่งอาจก่อให้เกิดประโยชน์ในการปฏิบัติงานที่ดียิ่งขึ้นไป

ศิริพร ลิ้มรังษี



สารบัญ

	หน้า
บทคัดย่อ	ก
ABSTRACT	ค
กิตติกรรมประกาศ	จ
สารบัญ	ฉ
สารบัญตาราง	ช
สารบัญภาพ	ญ
1. บทนำ	
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์	3
1.3 ขอบเขตของการวิจัย	3
1.4 ประโยชน์ของการวิจัย	4
1.5 นิยามศัพท์เฉพาะ	5
2. เอกสารและงานวิจัยที่เกี่ยวข้อง	
2.1 ความหมายของความปลอดภัยบนระบบคอมพิวเตอร์	8
2.2 แนวคิดและทฤษฎีที่เกี่ยวกับบุคลิกภาพ	18
2.3 แนวคิดและทฤษฎีที่เกี่ยวกับบุคลิกภาพ 5 องค์ประกอบ	19
2.4 แนวคิดทฤษฎีเกี่ยวกับพฤติกรรมกรใช้สารสนเทศอย่างปลอดภัย	25
2.5 งานวิจัยที่เกี่ยวข้อง	28
2.6 ค ำถามการวิจัย	33
2.7 กรอบแนวคิดในการวิจัย	33

สารบัญ (ต่อ)

	หน้า
3. วิธีดำเนินการวิจัย	
3.1 ประชากรและกลุ่มตัวอย่าง	34
3.2 เครื่องมือที่ใช้ในการรวบรวมข้อมูล	35
3.3 การทดสอบคุณภาพของเครื่องมือที่ใช้ในการศึกษา	39
3.4 การเก็บรวบรวมข้อมูล	41
3.5 การวิเคราะห์ข้อมูล	42
4. ผลการวิจัย	
4.1 ผลการวิเคราะห์ข้อมูลลักษณะส่วนบุคคล	44
4.2 ผลการวิเคราะห์ข้อมูลบุคลิกภาพห้าองค์ประกอบ	44
4.3 ผลการวิเคราะห์พฤติกรรมการใช้ข้อมูลสารสนเทศ อย่างปลอดภัย	47
4.4 ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบ กับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย	57
5. สรุปผลการวิจัย การอภิปรายผล และข้อเสนอแนะ	
5.1 สรุปผลการวิจัย	62
5.2 อภิปรายผล	64
5.3 ข้อเสนอแนะจากการวิจัย	68
บรรณานุกรม	70
ภาคผนวก	75
ประวัติการศึกษาและการทำงาน	84

สารบัญตาราง

ตาราง	หน้า	
2.1	ลักษณะบุคลิกภาพ	19
2.2	ลักษณะบุคลิกภาพแบบห้วนไหว	20
2.3	ลักษณะบุคลิกภาพแบบแสดงตัว	21
2.4	ลักษณะบุคลิกภาพแบบเปิดประสบการณ์	21
2.5	ลักษณะบุคลิกภาพแบบประนีประนอม	22
2.6	ลักษณะบุคลิกภาพแบบมีจิตสำนึก	23
3.1	ข้อคำถามเกี่ยวกับจำนวนประชากรที่ใช้ในการวิจัย	35
3.2	ตารางแสดงค่าสัมประสิทธิ์แอลฟาของบุคลิกภาพ 5 องค์ประกอบ	40
3.3	ตารางแสดงค่าสัมประสิทธิ์แอลฟาของพฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	41
4.1	จำนวน (ความถี่) และร้อยละ จำแนกตามลักษณะส่วนบุคคล	44
4.2	ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานของบุคลิกภาพห้าองค์ประกอบ ในภาพรวม	47
4.3	ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานพฤติกรรมที่ตั้งรหัสผ่าน	48
4.4	ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานพฤติกรรมการใช้โปรแกรม ซอฟต์แวร์ที่ไม่พึงประสงค์	49
4.5	ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานพฤติกรรมการถูกลอกหลวง	51
4.6	ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานด้านการโจมตีทางวิศวกรรมสังคม	53
4.7	ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานพฤติกรรมการถูกลอกหลวง ทางออนไลน์	55
4.8	ผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ระหว่างบุคลิกภาพ แบบเปิดประสบการณ์กับพฤติกรรมการใช้ข้อมูลสารสนเทศ	57
4.9	ผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ระหว่างบุคลิกภาพแบบ ประนีประนอมกับพฤติกรรมการใช้ข้อมูลสารสนเทศ	58
4.10	ผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ระหว่างบุคลิกภาพแบบ ห้วนไหวกับพฤติกรรมการใช้ข้อมูลสารสนเทศ	59

สารบัญตาราง(ต่อ)

ตาราง	หน้า
4.11 ผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ระหว่างบุคลิกภาพแบบ แสดงตัวกับพฤติกรรมการใช้ข้อมูลสารสนเทศ	60
4.12 ผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ระหว่างบุคลิกภาพแบบ มีจิตสำนึกกับพฤติกรรมการใช้ข้อมูลสารสนเทศ	61



สารบัญภาพ

ภาพ		หน้า
2.1	กรอบแนวคิดในการวิจัย	33



บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันการพัฒนาเทคโนโลยีนำความก้าวหน้ามาสู่ประเทศไทยอย่างรวดเร็ว และมีแนวโน้มการเปลี่ยนแปลงอย่างต่อเนื่อง รวมไปถึงการพัฒนาในระบบออนไลน์ ไม่ว่าจะเป็น การติดต่อสื่อสารกันในโลกออนไลน์ในยุคปัจจุบัน อาจส่งผลกระทบต่อความปลอดภัย ในการป้องกันความปลอดภัยของข้อมูลในระบบคอมพิวเตอร์ส่วนบุคคล อาจส่งผลกระทบต่อ ความปลอดภัย ในข้อมูลส่วนบุคคล เพื่อให้เห็นถึงความสำคัญและตระหนักถึงความปลอดภัย ของข้อมูลส่วนบุคคล สาเหตุที่มาจากพฤติกรรมของความไม่ปลอดภัยในการใช้งานระบบ ออนไลน์นั้น อาจนำมาซึ่งความสูญเสีย อาจเกิดขึ้นได้ทั้งทางตรงและทางอ้อม เช่น เสียทรัพย์สิน หรือรายได้ เสียชื่อเสียง รวมไปถึงการสูญเสียคนรอบข้างและสูญเสียสภาพทางด้านจิตใจ นอกจากนี้ อาจเกิดจากบุคคลใกล้ชิด ที่ขาดจิตใต้สำนึก หรือแค่สนุก โดยไม่คำนึงถึงความ ปลอดภัยของข้อมูลส่วนตัวของผู้อื่น หรือตัวบุคคลนั้นอาจ ใฝ่ใจคนใกล้ชิด ขาดความเข้าใจในการ รักษาความปลอดภัยของข้อมูล เช่น เข้าระบบ Facebook ในคอมพิวเตอร์สาธารณะ การเข้ารหัส หรือการตั้งรหัสผ่านที่จดจำง่าย มีการจดบันทึกรหัสผ่านไว้กับหน้าจอคอมพิวเตอร์ เพื่อสะดวก ในการใช้งานอาจมีการใช้ Internet ในการเข้าเว็บไซต์หรือใช้สื่อต่าง ๆ โดยไม่ได้ออกจากระบบ โดยไม่คำนึงว่าจะมีคนใกล้ชิดหรือใกล้ตัวเข้ามาใช้งานในระบบของเราโดยไม่ได้รับอนุญาต

แนวโน้มความปลอดภัยบนโลกไซเบอร์ (Cyber Security) แนวโน้มและแนวทางที่จะ เกิดขึ้นด้านความปลอดภัย ทุกวันนี้ เราคงจะหลีกเลี่ยงไม่ได้ ถ้าพูดถึงอินเทอร์เน็ตนั้น มีอยู่รอบตัว เราถือได้ว่าเป็นอุปกรณ์ที่เราแทบจะขาดไม่ได้เลยอย่างเช่น โทรศัพท์มือถือ (Smartphone) ที่ใกล้ ตัวเรามากในยุคสมัยนี้ ซึ่งในปัจจุบันมีอุปกรณ์หลายอย่าง มีการพัฒนา ให้เชื่อมต่อกันได้ จึงมี ปัญหาทางด้านความปลอดภัยที่คุกคามผู้ใช้อินเทอร์เน็ตมากมาย ไม่ว่าจะเป็นวิธีการหลอกลวง ทางอินเทอร์เน็ตโดยการส่งข้อความให้แก่ผู้รับผ่านทางอินเทอร์เน็ต เพื่อหลอกลวงเอาข้อมูล

สำคัญต่างๆ เมื่อผู้รับเมลหลอกลวง และให้ข้อมูลส่วนตัวที่สำคัญทางเว็บไซต์หลอกลวงเหล่านั้น นอกจากนั้นในบางครั้งผู้ใช้งานรู้เท่าไม่ถึงการณ์ติดตั้งโปรแกรมแปลกปลอมหรือเข้าใช้งานโดยไม่ระวังระบบของผู้ใช้งาน เป็นสาเหตุที่ทำให้การรักษาความปลอดภัยนั้น ก่อให้เกิดช่องว่างเข้ามาทำลายระบบของผู้ใช้งานอย่างง่ายดาย (ฐิติมา มานิตพร, 2560 : 68-69)

พฤติกรรมในการใช้คอมพิวเตอร์นั้น ที่มีผลต่อความปลอดภัยทางสารสนเทศบนระบบคอมพิวเตอร์ ความเสี่ยงในด้านสารสนเทศ รวมไปถึงการใช้ Internet ในการเข้าระบบหรือหน้าเว็บเบราว์เซอร์ต่าง ๆ ไวรัที่จคอมพิวเตอร์ในสถานที่ทำงาน หรือคอมพิวเตอร์สาธารณะ โดยไม่มีการออกจากระบบเพื่อเลิกใช้ ผู้ใช้งานอาจจะคาดไม่ถึงสิ่งเหล่านี้อาจมีใครที่เข้าถึงข้อมูลของบุคคลอื่นโดยง่าย อย่างไรก็ตามพฤติกรรมทางด้านความปลอดภัยในการใช้สารสนเทศของแต่ละบุคคลแตกต่างกันออกไป มีการศึกษาด้านจิตวิทยาที่เกี่ยวข้องกับบุคลิกภาพ ได้แก่ จิตวิทยาที่ศึกษาเกี่ยวกับความแตกต่างของบุคคล ซึ่งนักจิตวิทยาสนใจเฉพาะลักษณะทั่วไปของในแต่ละบุคคลที่มีบุคลิกภาพที่มีความคงที่และมีความต่อเนื่อง ในปัจจุบันแบบทดสอบในการวัดบุคลิกภาพ เป็นที่นิยมอย่างแพร่หลาย คือ แบบทดสอบวัดบุคลิกภาพห้าองค์ประกอบ (Big 5 Personality) ของคอสตาและแมคเคร (Costa and McCrae, 1992) ซึ่งผู้วิจัยจึงนำแบบทดสอบบุคลิกภาพห้าองค์ประกอบมาประยุกต์ใช้เป็นแบบสอบถาม จากที่ได้มีการศึกษาและสังเกตลักษณะบุคลิกภาพของพนักงานในสังกัดของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารที่ผู้วิจัยนั้นได้ทำงานอยู่ในสังกัดนี้ ที่สังเกตได้ในภาพรวมของบุคลิกภาพแต่ละบุคคลนั้นมีความสอดคล้องและตรงตามแบบทดสอบของคอสตาและแมคเคร

ผลกระทบในปัญหาต่าง ๆ มีทั้งปัจจัยที่เกิดจากพฤติกรรมของบุคคลเอง ความสัมพันธ์ในตัวบุคคลเองบ้างรวมไปถึงบุคลิกภาพต่าง ๆ ทั้งแบบเปิดเผยและไม่เปิดเผย ซึ่งเป็นปัญหาของการละเมิดสิทธิความเป็นส่วนตัวเป็นส่วนตัวของบุคคล ทำให้ความคิดและพฤติกรรมความสัมพันธ์ในตัวบุคคลเปลี่ยนไป และเป็นที่มาของปัญหาอื่นๆ อีกหลายประการ ทั้งนี้ทั้งนั้น สาเหตุทั้งหมดทั้งปวงที่เกิดขึ้นและมองเห็นเป็นรูปธรรมและนามกระทำนั้นล้วนแล้วเกิดจากพฤติกรรมหรือรวมไปกับองค์ประกอบต่าง ๆ หรือปัจจัยอื่น ๆ ที่ส่งผลต่อการเกิดพฤติกรรมในการเข้าถึงข้อมูลส่วนบุคคล ซึ่งอาจส่งผลให้มีการนำข้อมูลต่าง ๆ ไปใช้ในทางที่ผิด นำไปใช้ในการกระจายข่าวสาร

หลอกลวงผู้อื่นหรือนำข้อมูลไปแอบอ้างในการค้าหรือการเอาเปรียบผู้อื่น รวมถึงการโพสต์ข้อความที่ไม่พึงประสงค์ต่อที่สาธารณะ พฤติกรรมเหล่านี้ล้วนแต่ไม่คำนึงถึงเจ้าของข้อมูลว่าพึงพอใจหรือรับรู้ในสิ่งที่เกิดขึ้นมากน้อยเพียงใด

ด้วยเหตุนี้ งานวิจัยนี้จึงมุ่งศึกษา ในเรื่องของบุคลิกภาพห้าองค์ประกอบ ที่มีความสัมพันธ์กับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย เพื่อศึกษาว่าบุคลิกภาพแบบใดมีความสัมพันธ์กับพฤติกรรมอย่างไร โดยเน้นการศึกษาในเรื่องของพฤติกรรม ที่มีความสัมพันธ์ในบุคลิกภาพและปัจจัยต่าง ๆ ที่เกี่ยวข้องกับการวิจัย อย่างไรก็ตามในการวิจัยครั้งนี้เพื่อทำให้เกิดความเข้าใจและชัดเจนในบุคลิกและพฤติกรรมของแต่ละบุคคลในองค์กร

1.2 วัตถุประสงค์ของการวิจัย

การวิจัยเรื่อง “ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ในองค์กรภาครัฐแห่งหนึ่ง” มีวัตถุประสงค์ในการวิจัย ดังนี้

1.2.1 เพื่อศึกษาบุคลิกภาพห้าองค์ประกอบของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

1.2.2 เพื่อศึกษาพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

1.2.3 เพื่อศึกษาความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย

1.3 ขอบเขตของการวิจัย

1.3.1 ขอบเขตเนื้อหา ผู้วิจัยมุ่งศึกษาตัวแปร ดังนี้

ตัวแปรอิสระ (Independent Variable) คือ บุคลิกภาพห้าองค์ประกอบประกอบด้วย

- บุคลิกภาพแบบเปิดรับประสบการณ์
- บุคลิกภาพแบบประนีประนอม
- บุคลิกภาพแบบหัวน้ไหว
- บุคลิกภาพแบบแสดงตัว
- บุคลิกภาพแบบมีจิตสำนึก

ตัวแปรตาม (Dependent Variable) คือ พฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย

1. การใช้รหัสผ่าน
2. การใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์
3. การถูกหลอกลวง
4. ด้านการโจมตีทางวิศวกรรมสังคม
5. การถูกหลอกลวงทางออนไลน์

1.3.2 ขอบเขตประชากร

ประชากรที่ใช้ในการศึกษาคั้งนี้ คือ พนักงานศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร องค์การภาครัฐแห่งหนึ่ง จำนวน 65 คน (ที่มา: ข้อมูลบุคลากร ฝ่ายบริหารงานทั่วไป ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ณ วันที่ 1 ตุลาคม พ.ศ. 2560)

1.4 ประโยชน์ของการวิจัย

1.4.1 คาดว่าสามารถนำไปใช้ในการวางแผนในด้านความปลอดภัยของข้อมูลสารสนเทศได้อย่างมีประสิทธิภาพ

1.4.2 คาดว่านำผลการวิจัยไปประยุกต์ใช้ในการออกข้อบังคับหรือกฎระเบียบในการใช้สารสนเทศของหน่วยงาน

1.5 นิยามศัพท์เฉพาะ

การศึกษาในครั้งนี้ ผู้วิจัยจึงกำหนดความหมายและขอบเขตของคำต่าง ๆ ไว้ดังนี้

พนักงาน คือ พนักงานระดับปฏิบัติการในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จำนวน 65 คน

ลักษณะทั่วไปของบุคคล คือ ลักษณะทั่วไปที่มีความแตกต่างของบุคคล ได้แก่ เพศ อายุ สถานภาพ ระดับการศึกษา ตำแหน่งงาน รายได้ และประสบการณ์ในการทำงาน

บุคลิกภาพห้าองค์ประกอบ หมายถึง ลักษณะของบุคลิกภาพห้าองค์ประกอบตามแนวคิดของคอสตาและแมคครี (Costa & McCrae, 1992) ประกอบไปด้วย บุคลิกภาพแบบเปิดรับประสบการณ์ บุคลิกภาพแบบประนีประนอม บุคลิกภาพแบบหวั่นไหว บุคลิกภาพแบบมีจิตสำนึก และบุคลิกภาพแบบแสดงตัว

- บุคลิกภาพแบบเปิดรับประสบการณ์ คือ บุคลิกภาพแบบเปิดรับสิ่งใหม่ ๆ อยู่เสมอ มีจินตนาการมีความคิดสร้างสรรค์ที่จะเรียนรู้ในสิ่งแปลกใหม่

- บุคลิกภาพแบบประนีประนอม คือ บุคลิกภาพที่มีความสุภาพอ่อนโยน มีน้ำใจต่อบุคคลรอบข้าง มีเหตุมีผลในการตัดสินใจและแก้ไขความขัดแย้งที่มีต่อผู้อื่น

- บุคลิกภาพแบบหวั่นไหว คือ บุคลิกภาพที่มีแต่ความวิตกกังวล คิดมากกับเรื่องต่าง ๆ มีความหวั่นไหวต่ออารมณ์ไม่สามารถจัดการกับอารมณ์ได้เท่าที่ควร

- บุคลิกภาพแบบมีจิตสำนึก คือ บุคลิกภาพที่มีความรับผิดชอบต่อเรื่องต่าง ๆ ที่ได้รับมอบหมาย หรือเรื่องที่ต้องรับผิดชอบ ปฏิบัติยึดถือตามข้อควรปฏิบัติหรือกฎระเบียบต่าง ๆ

- บุคลิกภาพแบบแสดงตัว คือ ผู้ที่มีบุคลิกภาพที่มีความเป็นตัวของตัวเองสูง ชอบเข้าสังคม ช่างพูดช่างเจรจา เป็นกันเอง แสดงออกอย่างตรงไปตรงมา

ความปลอดภัย หมายถึง การจัดการดูแลและการป้องกัน ไม่ให้เกิดภัยคุกคาม หรือสิ่งที่ไม่ก่อให้เกิดอันตรายต่าง ๆ รวมไปถึงความปลอดภัยในด้านการป้องกันข้อมูลส่วนบุคคลในสารสนเทศ

ข้อมูล หมายถึง ข้อเท็จจริง หรือเหตุการณ์ที่เกี่ยวข้องกับสิ่งต่าง ๆ เกี่ยวกับบุคคล หรือรายละเอียดที่อาจเป็นในรูปแบบของ ตัวเลข ภาพ เสียง แสง เป็นต้น ที่มีการค้นหาจากหลายแหล่งที่มาเพื่อได้มาซึ่งข้อมูลนั้น ๆ

สารสนเทศ หมายถึง ข้อมูลหรือสิ่งที่ได้จากการนำข้อมูลมาประมวลผลหรือมีการเปลี่ยนแปลง เพื่อนำมาใช้ประโยชน์ (วิเศษศักดิ์ โคตรอาษา, 2542)

ความปลอดภัยด้านข้อมูลสารสนเทศ (Information Security) คือ การกำหนดนโยบายหรือข้อปฏิบัติต่าง ๆ ในองค์กรหรือหน่วยงานนั้น ๆ เพื่อป้องกันการคุกคามจากการใช้สารสนเทศ

พฤติกรรม หมายถึง การกระทำต่าง ๆ ของบุคคลที่สามารถสังเกตได้จากการแสดงออกหรือกระทำกิจกรรมที่จะเกี่ยวข้องกับการใช้ข้อมูลสารสนเทศอย่างปลอดภัย

การตั้งรหัสผ่าน หมายถึง พฤติกรรมในการป้องกันข้อมูลในการใช้คอมพิวเตอร์หรือการใช้รหัสผ่านในการเข้าใช้ระบบสารสนเทศที่มีผลต่อความปลอดภัยในข้อมูลส่วนบุคคลในระบบสารสนเทศ

การใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์ คือ เป็นพฤติกรรมการใช้โปรแกรมหรือการดาวน์โหลดโปรแกรมที่ไม่ต้องเสียค่าใช้จ่าย และนอกจากนี้ยังรวมไปถึงเรื่องของการเปิดไฟล์เอกสารแนบที่รับจากเมลของคนแปลกหน้า

การถูกหลอกหลวง คือ การตกเป็นเหยื่อของผู้ไม่หวังดีที่แอบแฝงมาทางข้อมูลอีเมลหรือจากทางเว็บไซต์ การคลิกลิงก์ต่าง ๆ ในการเข้าใช้งาน และนอกจากนี้ยังง่ายต่อการถูกหลอกหลวงทางออนไลน์ ที่ส่งผลกระทบต่อพฤติกรรมจากการคลิกเข้าไปตอบคำถามเพื่อชิงเงินรางวัล หรือการรู้จักนัดพบจากคนแปลกหน้าที่รู้จักกันทางโลกออนไลน์ รวมไปถึงการถูกหลอกให้โอนเงินหรือแอบอ้างที่ทำให้มีความน่าเชื่อถือ

ด้านการโจมตีทางวิศวกรรมสังคม คือ การหลอกหลวงหรือใช้เล่ห์กลอุบายเพื่อแสวงหาผลประโยชน์จากผู้ใช้งานที่ไม่ระมัดระวัง โดยอาศัยช่องโหว่หรือจุดอ่อนของผู้ใช้งานที่มีความรู้ทางด้านของ ความมั่นคงปลอดภัยน้อยหรือรู้เท่าไม่ถึงการณ์มีความประมาทในเรื่องของความ

มั่นคงปลอดภัย เช่น การหลงเชื่อจากข้อมูลที่ได้รับทางโทรศัพท์ หรือการหลอกลวงให้ทำธุรกรรมทางการเงิน



บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

ในการศึกษาวิจัยนี้ ผู้วิจัยได้ศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง ดังนี้

- 2.1 ความหมายของความปลอดภัยบนระบบคอมพิวเตอร์
- 2.2 แนวคิดและทฤษฎีเกี่ยวกับบุคลิกภาพ
- 2.3 แนวคิดและทฤษฎีบุคลิกภาพ 5 องค์ประกอบ
- 2.4 แนวคิดและทฤษฎีเกี่ยวกับพฤติกรรมการใช้สารสนเทศอย่างปลอดภัย
- 2.5 งานวิจัยที่เกี่ยวข้อง
- 2.6 คำถามการวิจัย
- 2.7 กรอบแนวคิดในการวิจัย

2.1 ความหมายของความปลอดภัยบนระบบคอมพิวเตอร์

ความหมายและความสำคัญของ Cyber Security

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช. หรือ NSTDA) ให้ความหมายของไซเบอร์ (Cyber) คือ คำที่มาจากคำว่าไซเบอร์เนติกส์ (Cybernetics) และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต (Internet) และยังให้ความหมาย สารสนเทศ เสมือนจริง (Virtual) ที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง ไซเบอร์เนติกส์ (Cybernetics) เป็นวิชาการเกี่ยวกับระบบควบคุม เช่น ระบบประสาทของสิ่งมีชีวิตเพื่อนำไปใช้พัฒนาระบบอิเล็กทรอนิกส์

ตามพจนานุกรม Cyberspace Operations Lexicon ของ กท.สหรัฐ กำหนดให้ Cyber Security คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อให้องค์กรปราศจากความเสียหายและความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ(ทั้งทางอิเล็กทรอนิกส์

และทางกายภาพ) ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผลและกระจายข้อมูล ทั้งนี้ Cyber Security ยังรวมถึงการระวังป้องกันต่อการเกิดอาชญากรรม การโจมตี บ่อนทำลาย การโจรกรรม อุบัติเหตุ และความผิดพลาดต่าง ๆ ความเสี่ยงของ Cyber Security อาจรวมถึงสิ่งต่าง ๆ ที่ทำลายความเชื่อมั่น และความไว้วางใจของผู้ถือผลประโยชน์ร่วม (Stakeholder) ผลกระทบที่มีต่อการเก็บรักษาและการเติบโตของกลุ่มลูกค้า การละเมิดการป้องกันข้อมูลส่วนตัวของกลุ่มลูกค้าและผู้ถือหุ้น การรบกวนการทำงานหรือการดำเนินธุรกรรมที่เป็นต่อชีวิตและสุขภาพของผู้ปฏิบัติงาน และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ แม้ว่าปัจจุบันการกำหนดความหมายและห่วงของไซเบอร์ยังไม่มี ความชัดเจน แต่ความสำคัญในการทำความเข้าใจในไซเบอร์ยังคงเป็นสิ่งจำเป็นในการปฏิบัติการของทุกหน่วยงาน โดยเฉพาะหน่วยงานที่มีผลกระทบกับความมั่นคงของประเทศ การรักษาความปลอดภัยและการปฏิบัติการ ยังเป็นที่ต้องปฏิบัติเพื่อเป็นหลักประกันในความสำเร็จของหน่วยงาน ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในปัจจุบันและอนาคต (นิวัติ เนียมพลอย, 2560)

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union : ITU) ได้ให้ความหมายของคำว่า ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) คือ ภาพรวมของเครื่องมือ (Tools) นโยบาย (Policies) แนวคิดการรักษาความปลอดภัย (Security Concepts) การรักษาความปลอดภัย (Security Safeguards) แนวทาง (Guidelines) วิธีการบริหารความเสี่ยง (Risk Management Approaches) การปฏิบัติ (Actions) การอบรม (Training) วิธีปฏิบัติที่เป็นเลิศ (Best Practices) การรับประกัน (Assurance) และเทคโนโลยี (Technologies) ที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กร และสินทรัพย์ของผู้ใช้งาน ได้แก่ อุปกรณ์ สำหรับเชื่อมต่อ คอมพิวเตอร์ ข้อมูลส่วนตัว โครงสร้างพื้นฐาน แอปพลิเคชัน บริการ ระบบสารสนเทศ และภาพรวมของการส่งผ่านหรือเก็บข้อมูลในไซเบอร์

ทศพนธ์ นรทัศน์ (2560 : 66) กล่าวว่า ความเสี่ยงด้านความปลอดภัยไซเบอร์ในภูมิภาคเอเชีย แปซิฟิก ในปี 2017 และแนวโน้มเชิงนโยบายการรักษาความปลอดภัยไซเบอร์ของประเทศ ไทย แนวโน้มเชิงนโยบาย การรักษาความปลอดภัยไซเบอร์ของประเทศไทยเพื่อประกอบการ

วางแผนรับมือภัยคุกคามไซเบอร์ขององค์กรรวมถึงการรับมือภัยคุกคามไซเบอร์ในระดับประเทศ และระดับบุคคล ความปลอดภัยไซเบอร์เป็นเรื่อง ที่มีความสำคัญอย่างยิ่ง ทั้งในระดับประเทศ องค์กร และระดับบุคคล โดยเฉพาะการพัฒนาสู่ความเป็นดิจิทัลขององค์กร (Digital Transformation) ดังที่ Greg Bell, Co-Leader ของ Global Cyber Security KPMG International ได้ระบุว่า องค์กรจะต้องวางความปลอดภัย ไซเบอร์ไว้ทุก ๆ ส่วน การตัดสินใจมีความสำคัญ จะต้องคำนึงถึงความปลอดภัยไซเบอร์ร่วมกันเสมอและต้องมั่นใจว่าทุกคนในองค์กรมีความรู้ ความเข้าใจกับประเด็นในด้านของไซเบอร์ และมีแผนรองรับอย่างชัดเจน เพื่อให้บุคลากรรับรู้และ เข้าใจ ซึ่งจะช่วยให้เกิดความปลอดภัยไซเบอร์ (ฐิติมา มานิตพร, 2560 : 68 - 69) แนวโน้มความปลอดภัยบนโลกไซเบอร์ (Cyber Security Trend by E-rong, 2017) แนวโน้มและแนวทางที่จะ เกิดขึ้นด้านความปลอดภัยในทุกวันนี้เราคงปฏิเสธไม่ได้เลยว่า อินเทอร์เน็ตนั้นอยู่รอบ ๆ ตัวเรา สำหรับอุปกรณ์ ที่เราแทบจะขาดไม่ได้เลย เช่น โทรศัพท์มือถือคือ Smartphone ที่พาเราเข้าสู่โลก อินเทอร์เน็ตได้อย่างง่ายดาย และใกล้ตัวเรามากที่สุด ซึ่งในปัจจุบันมีอุปกรณ์หลายอย่าง ที่มีการ พัฒนาให้เชื่อมโยงถึงกันได้ สำหรับปัญหาในด้านของความปลอดภัยที่คุกคามผู้ใช้อินเทอร์เน็ต มากมาย คือเป็นวิธีการหลอกลวงอย่างหนึ่งทางอินเทอร์เน็ต โดยการส่งข้อความให้แก่ผู้รับผ่าน ทางอินเทอร์เน็ตเพื่อหลอกลวงเอาข้อมูลสำคัญเมื่อผู้รับเมลหลอกลวงหลงเชื่อกดเข้าเว็บไซต์ที่ หลอกลวง ผู้ใช้งานในบางครั้งอาจรู้เท่าไม่ถึงการณ์ที่อาจเผลอไปติดตั้งโปรแกรมแปลกปลอมหรือ เข้าใช้งานโดยไม่ระมัดระวัง อาจเป็นหนึ่งสาเหตุที่ทำให้การรักษาความปลอดภัยนั้นเกิดช่องว่าง เข้ามาทำลายได้

สุพิชญา อาชวีรดา (2560) ได้อธิบาย ปัจจัยหลักที่ส่งผลกระทบต่อระดับการรักษาความ มั่นคงปลอดภัยของระบบสารสนเทศภายในองค์กร สองประการสำคัญ ดังนี้

1. การรับรู้ถึงภัยคุกคาม (Perceived Threats) หมายถึง การทราบถึงความรุนแรง หรือผลกระทบของอันตรายที่จะเกิดขึ้น ซึ่งแสดงให้เห็นถึงความกลัวต่อความรุนแรง และการรับรู้ ถึงภัยคุกคามจะส่งผลต่อความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ
2. ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Insight into the Security of Information Systems) หมายถึง การที่บุคคลที่มีความทรงจำในเรื่องราว ข้อเท็จจริง

รายละเอียดต่าง ๆ และความสามารถในการนำความรู้มาประยุกต์ใช้ดัดแปลง อธิบาย เปรียบเทียบในเรื่องนั้น ๆ ได้อย่างมีเหตุผล ในเรื่องของระบบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศภายในองค์กร

การรักษาความปลอดภัยทางกายภาพ (Physical Security) หมายถึง มาตรการที่ใช้ในการป้องกันทรัพยากรจากภัยคุกคามทางกายภาพทั้งโดยเจตนาและไม่เจตนา ซึ่งเป็นหนึ่งในวิธีที่ช่วยลดความเสี่ยง ด้านความปลอดภัย โดยการจำกัดให้เฉพาะผู้ที่จำเป็นต้องใช้งาน เช่น ผู้ดูแลระบบเท่านั้นที่สามารถ เข้าถึงส่วนควบคุมของระบบปกติแล้วระบบที่เป็นเซิร์ฟเวอร์ ผู้ใช้ทั่วไปไม่จำเป็นต้องใช้งาน แต่สามารถใช้โปรแกรมประเภท Secure Shell (SSH) เพื่อทำการติดต่อเข้าไป ใช้งานยังเครื่องเซิร์ฟเวอร์ได้ เหตุผลที่ไม่ควรให้ผู้ทั่วไปเข้าถึงส่วนควบคุมระบบนั้น เนื่องจากผู้ที่ เข้าใช้สามารถทำการเปิด-ปิดเครื่อง ทำให้สามารถเปลี่ยนรหัสผ่านได้ นอกจากนี้การเข้าถึงยังสามารถทำอะไรได้ตามต้องการ เช่น การเข้าสู่ระบบได้โดยไม่จำเป็นต้องทราบรหัสผ่านทั้งๆ ที่ไม่มีซีดีรอมที่สามารถบูตได้ด้วย และยังเป็น การป้องกันอุปกรณ์ เป็นต้น เพื่อให้ปราศจากการเข้าถึง โดยไม่ได้รับอนุญาต และการใช้งานที่ไม่ถูกต้อง เช่น การตั้งรหัสผ่านเข้าใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล สร้างห้องปฏิบัติการสำหรับระบบคอมพิวเตอร์และเครือข่าย การจัดให้มีการพิสูจน์ตัวตนก่อนเข้าถึงระบบการใช้งาน แนวคิดเกี่ยวกับความปลอดภัยทางกายภาพในเครื่องคอมพิวเตอร์ (กิตติศักดิ์ จีวรรัตนกุล, 2545)

เสฐฐวุฒิ แสนนาม (2555) อธิบายว่า สำหรับการใช้งานผ่านคอมพิวเตอร์สาธารณะนั้นมีความมั่นคงปลอดภัยต่ำ ในคอมพิวเตอร์เครื่องนั้นอาจมีผู้ไม่หวังดีติดตั้งโปรแกรมที่ก่อให้เกิดความเสียหายของข้อมูล แต่ในบางสถานการณ์เราอาจมีความจำเป็นต้องใช้คอมพิวเตอร์สาธารณะในการเข้าถึงข้อมูล ในการใช้ข้อมูลในส่วนที่สำคัญ เช่น การ Log In เพื่อตรวจสอบ E-mail หรือในบางครั้งอาจจำเป็นต้องการในการแก้ไขงานต่าง ๆ หรือเอกสารที่มีความสำคัญอย่างยิ่ง อันตรายจากการใช้คอมพิวเตอร์สาธารณะที่อาจส่งผลกระทบต่อผู้ใช้งาน ดังนั้น เพื่อให้มีความมั่นคงปลอดภัยยิ่งขึ้นในการใช้คอมพิวเตอร์สาธารณะ เสฐฐวุฒิ แสนนาม (2555) ให้ข้อแนะนำต่าง ๆ อาจช่วยในการป้องกันข้อมูลสำคัญได้ ดังนี้

1. เลือกเครื่องที่ไม่มีผู้คนเดินผ่านไปมาบ่อย เพื่อป้องกันการทำ (Shoulder Surfing) การแอบมองหน้าจอ และไม่ควรเลือกเครื่องที่วางอยู่ในตำแหน่งที่มีวัตถุที่สามารถสะท้อนแสงจากหน้าจอได้ เช่น กระจก หรือ โลหะ เป็นต้น

2. ตรวจสอบ Key logger หรือที่เรียกกันว่าภัยร้ายบนแป้นพิมพ์ซึ่งผู้ไม่หวังดีจะมีการบันทึกการกดแป้นพิมพ์คอมพิวเตอร์ของคุณที่ได้มีการพิมพ์รหัสผ่านต่าง ๆ ด้วยแป้นพิมพ์ ซึ่งการตรวจสอบ Key logger นั้นจะมีทั้งที่เป็นอุปกรณ์ฮาร์ดแวร์ (Hardware) หรือที่เป็นโปรแกรมซอฟต์แวร์ (Software) อุปกรณ์เหล่านี้ จะตรวจสอบและสอดส่องในพฤติกรรมของผู้ที่ใช้งานคอมพิวเตอร์

3. บู๊ตเครื่องโดยใช้ Bootable CD หรือ Bootable USB หากเครื่องคอมพิวเตอร์สามารถบู๊ต จาก Bootable CD หรือ Bootable USB ได้ การบู๊ตเครื่องด้วยวิธีดังกล่าว สามารถช่วยป้องกันภัยคุกคามจากซอฟต์แวร์ไม่พึงประสงค์ได้

4. เพื่อป้องกัน Spyware พวก Key logger เราอาจใช้โปรแกรมประเภท On-Screen Keyboard ในการพิมพ์ Username และ Password ในหน้าเว็บไซต์ต่าง ๆ ได้

5. ใช้งานเบราว์เซอร์ในโหมด Private Browsing ซึ่งจะเป็นการตั้งค่าให้เบราว์เซอร์ไม่เก็บข้อมูล การใช้งานอินเทอร์เน็ตไว้ในเครื่อง เช่น Cache History หรือ Cookie เป็นต้น

6. ไม่ใช้งานธนาคารออนไลน์หรือทำธุรกรรมที่เกี่ยวข้องกับการเงินออนไลน์ เนื่องจากเครื่องคอมพิวเตอร์สาธารณะและเครือข่ายที่เชื่อมต่ออยู่นั้น ไม่สามารถแน่ใจในความมั่นคงปลอดภัยทางคอมพิวเตอร์ได้ผู้ใช้งานจึงไม่ควรประมาท

นอกจากนี้ เสกฐิฐุฒิ แสนนาม (2555) ยังกล่าวถึง อีกหนึ่งความสำคัญ คือ การพิสูจน์ตัวตนเป็นวิธีการที่ใช้ในการตรวจสอบผู้ที่มาใช้งานระบบเครือข่ายอินเทอร์เน็ต โดยระบบจะทำการตรวจสอบจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ว่ามีความถูกต้องครบถ้วนหรือไม่ จุดประสงค์หลักในการพิสูจน์ตัวตน คือพิสูจน์ตัวบุคคลว่าบุคคลที่เข้าใช้งานระบบเครือข่ายนั้นคือใคร พร้อมทั้งทำการตรวจสอบว่าผู้ใช้งานระบบเครือข่ายของบุคคลนั้นๆ มีสิทธิ์ใช้งานได้นานเพียงใด ซึ่งระบบนั้นจะทำการตัดผู้ใช้ออกไปจากการให้บริการทันทีที่เวลาหมดอีกทั้งยังสามารถกำหนดเวลาและความเร็วได้ตามความเหมาะสมด้วย และยังทำการบันทึกข้อมูลการ

ใช้งานระบบเครือข่าย ซึ่งจุดประสงค์หลักของขบวนการนี้เพื่อรายงานการใช้ระบบเครือข่ายอินเทอร์เน็ต จะทำการยืนยันการบันทึกข้อมูลในการใช้งานระบบเครือข่ายอินเทอร์เน็ตไว้อย่างละเอียดโดยสามารถทำรายงานสรุปได้ตามความต้องการในการพิสูจน์ตัวตน (Authentication) นั้น ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน

1. การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใคร เช่น ชื่อผู้ใช้

2. การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคล ที่กล่าวอ้างจริง การแสดงการพิสูจน์ตัวตนผู้ใช้สามารถแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนเป็นหลักฐานทางอิเล็กทรอนิกส์ที่บ่งบอกข้อมูลของบุคคลนั้น เช่น บัญชีชื่อผู้ใช้ กลไกของการพิสูจน์ตัวตนแบ่งออกได้ 4 คุณลักษณะ

2.1 สิ่งที่คุณมี (Possession Factor) เช่น กุญแจหรือเครดิตการ์ด

2.2 สิ่งที่คุณรู้ (Knowledge Factor) เช่น รหัสผ่าน (Passwords) หรือการใช้พิน (PINs)

2.3 สิ่งที่คุณเป็น (Biometric Factor) เช่น ลายนิ้วมือ รูปแบบเรตินา (Retinal Patterns) หรือใช้รูปแบบเสียงหรือรูปภาพ

2.4 สิ่งที่คุณสร้างขึ้นเอง (Produce Factor) เช่น การสร้างลายเซ็น การวาดภาพ เป็นต้น

สำหรับกระบวนการพิสูจน์ตัวตนนั้นจะนำ 4 ลักษณะข้างต้นมาเพื่อใช้ในการยืนยันหลักฐานที่นำมากล่าวอ้าง ทั้งนี้ขึ้นอยู่กับระบบ วิธีการที่นำมาใช้เพียงลักษณะใดลักษณะหนึ่ง (Single-factor Authentication) นั้นมีข้อจำกัดในการใช้ เช่น สิ่งที่คุณมี (Possession Factor) นั้น อาจสูญหายหรือถูกขโมยได้ ในสิ่งที่คุณรู้ (Knowledge Factor) อาจจะถูกดักฟัง ถูกคาดเดา หรือถูกขโมยจากเครื่องคอมพิวเตอร์ และนอกจากนี้แนวคิดหรือความรู้เกี่ยวกับความปลอดภัยของข้อมูล (Informational Security) ข้อมูลและสารสนเทศเป็นทรัพยากรที่สำคัญต่อบุคคลหรือองค์กรที่เป็นผู้ประมวลผลหรือรับส่งข้อมูลสารสนเทศนั้น ๆ ด้วยเหตุนี้อาจตกเป็นเป้าหมายหลักที่สำคัญของการโจมตีของผู้ไม่หวังดี เช่น การเปิดเผยความลับ การแก้ไขข้อมูลโดยไม่มีสิทธิ์และ

การทำให้ข้อมูลนั้นๆ ไม่สามารถเข้าถึงได้ เช่น การถูกลบ การเปลี่ยนแปลงสิทธิ์หรือการถูกเข้ารหัสเพื่อเรียกหรือก่อให้เกิดความเสียหายทางข้อมูลส่วนบุคคล เป็นต้น การรักษาความปลอดภัยของข้อมูล หมายถึง การทำให้มั่นใจได้ว่าทรัพยากรข้อมูลสารสนเทศที่มีอยู่มีความถูกต้องสมบูรณ์ และพร้อมใช้งานสำหรับผู้ใช้งานที่ได้รับสิทธิ์ในการเข้าถึงข้อมูลนั้น ๆ ในที่นี้จะยกตัวอย่างการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลซึ่งจัดเก็บข้อมูลที่อาจมีข้อมูล ที่ไม่ต้องการให้ผู้อื่นล่วงรู้ ตลอดจนต้องการรักษาความครบถ้วนสมบูรณ์ของไฟล์ต่าง ๆ ที่ถูกจัดเก็บไว้ในคอมพิวเตอร์ไม่ให้ถูกทำลายโดยรูปแบบการโจมตีต่าง ๆ และอาจส่งผลทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ การรักษาความปลอดภัยในเบื้องต้นอาจทำได้โดย การตั้ง Password เพื่อควบคุมการเข้าถึงเครื่องคอมพิวเตอร์ การติดตั้งซอฟต์แวร์ตรวจจับคอมพิวเตอร์ไวรัส และเปิดการใช้งาน Firewall ส่วนบุคคล (เสกฐวุฒิ แสนนาม, 2555)

ในส่วนของความปลอดภัยข้อมูลสารสนเทศที่มีส่วนเกี่ยวข้องนั้น คือ รหัสผ่าน (Password) เป็นส่วนหนึ่งที่มีความสำคัญในการรักษาความปลอดภัยของบัญชีผู้ใช้งานหรือในระบบที่ต้องการความปลอดภัยซึ่งรหัสผ่านถือเป็นสิ่งที่ใช้สำหรับยืนยันความถูกต้องของตัวบุคคลนั้นๆ การใช้งานรหัสผ่านจึงช่วยป้องกัน ความปลอดภัย การเข้าถึงข้อมูลโดยมิชอบได้ หากผู้ใช้งานไม่ให้ความสำคัญในการตั้งรหัสผ่านก็จะทำให้ ผู้ไม่หวังดีสามารถคาดเดารหัสผ่านและเข้าถึงข้อมูลของท่านได้อย่างง่ายดาย โดยแนวทางและข้อแนะนำ ในการตั้งรหัสผ่านให้ปลอดภัย รหัสผ่านเป็นสิ่งสำคัญ เป็นสิ่งจำเป็นที่จะยืนยันตัวตนในการเข้าถึงข้อมูลที่มีการป้องกันระบบหรือ เครือข่ายอื่นที่เป็นข้อมูลสำคัญที่ผู้ใช้จำเป็นต้องมีการจัดการและรักษาความปลอดภัยที่มีประสิทธิภาพในการบริหารจัดการรหัสผ่านให้มีประสิทธิภาพที่ดีนั้น ทางด้านของระบบต้องมีข้อกำหนด ในการสร้างรหัสผ่านที่มีความปลอดภัยสูงสุด (ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2553)

เสกฐวุฒิ แสนนาม (2555) ได้กล่าวถึงพฤติกรรมในการตั้งรหัสหรือใส่รหัสผ่านนั้น ส่วนใหญ่จะใช้คำศัพท์ทั่วไปจากพจนานุกรม โดยใช้ซอฟต์แวร์ในการใส่คำศัพท์เพื่อคาดเดารหัสผ่านของผู้ใช้งาน โดยรหัสผ่านที่มีความยาวของตัวอักษรน้อยจะถูกพบได้ง่ายกว่ารหัสผ่านที่มีตัวอักษรที่เยอะและยาว สำหรับรหัสผ่านจำแนกออกได้หลายรูปแบบ ดังนี้

- Password Synchronization หมายถึง กระบวนการในการจัดการกับรหัสผ่านของผู้ใช้งานระบบ ให้เป็นรหัสผ่านเดียวกัน วิธีนี้จะมีประโยชน์สำหรับผู้ดูแลระบบ Single Sign-On คือผู้ใช้งานชื่อเข้าใช้งานระบบเพียงครั้งเดียว สำหรับการจัดการรหัสผ่านในลักษณะนี้จะทำให้ไม่จำเป็นที่จะต้องมีการตรวจสอบรหัสผ่านแบบ Single Sign-On

- Local Password Management หมายถึง การจัดการสิทธิ์ในการเข้าใช้งานระบบกับเครื่องคอมพิวเตอร์แต่ละเครื่องโดยอาศัยการใช้ซอฟต์แวร์ในการช่วยในการจัดการสิทธิ์และอาจมีการแยกรหัสผ่านของการใช้งานแยกกับเครื่องคอมพิวเตอร์เช่น แฟลชไดรฟ์ เพื่อเพิ่มความปลอดภัยมากยิ่งขึ้น สำหรับรหัสผ่านแบบครั้งเดียว คือ รหัสผ่านที่ใช้ได้หนึ่งครั้ง เมื่อใช้แล้วรหัสผ่านเดิม จะไม่สามารถใช้งานได้อีก ต้องใช้รหัสผ่านตัวใหม่ หรือรหัสผ่านที่เปลี่ยนแปลงตลอดเวลาหรือตามช่วงเวลาที่กำหนดมี 2 ประเภทคือ แบบใช้อุปกรณ์และไม่ใช้อุปกรณ์ แบบใช้อุปกรณ์ (Hardware) คือรหัสผ่านแบบครั้งเดียวที่มีอุปกรณ์ สำหรับใช้ตรวจสอบรหัสผ่านปัจจุบัน ซึ่งจากการที่รหัสผ่านถูกเปลี่ยนแปลงตลอดเวลาหรือตามช่วงเวลาที่กำหนด วิธีการนี้จึงจำเป็นต้องใช้อุปกรณ์เช่น Token – Synchronization Mobile Phone Smart Card เป็นต้น สำหรับการตรวจสอบรหัสผ่านปัจจุบัน ในกรณีของการใช้โทรศัพท์มือถืออาจสั่งการให้ระบบส่งรหัสผ่านด้วยการส่งข้อความ SMS ให้ผู้ใช้งานได้ทราบรหัสผ่าน สำหรับข้อดี มีความปลอดภัยมากแต่จะมีข้อเสีย คือ ใช้งานลำบากเพราะต้องพกพาอุปกรณ์ต่าง ๆ และแบบไม่ใช้อุปกรณ์ คือ ใช้ Software เป็นสื่อกลางที่ทำให้ทราบรหัสผ่านปัจจุบัน เช่น การสร้างรูปแบบของคำถามที่เปลี่ยนแปลงตลอดเวลาซึ่งผู้ใช้งานจะรู้ว่าต้องตอบอะไร หรือใช้ส่วนไหนของคำตอบมาเป็นรหัสผ่าน

- ความมั่นคงปลอดภัยส่วนบุคคล (Personal Security) เพื่อเป็นการรักษาบุคลากรหรือกลุ่มของผู้ใช้งานที่มีสิทธิ์ให้เข้าถึงข้อมูลได้อย่างมั่นคงปลอดภัย เช่น การกำหนดสิทธิ์ให้กับเจ้าหน้าที่ตามความรับผิดชอบ โดยกำหนดให้เจ้าหน้าที่ทั่วไปไม่สามารถอ่านข้อมูลที่ถูกสร้างขึ้นโดยหัวหน้าผู้รับผิดชอบงานสามารถแก้ไขและตรวจสอบผู้ที่กระทำการแก้ไขข้อมูลนั้น ๆ โดยบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านเมื่อเข้าใช้งานระบบในครั้งแรกและทุก ๆ สามเดือน เป็นต้น

นอกจากนี้ กรกช วิไลลักษณ์ (2560) กล่าวว่า ความมั่นคงปลอดภัยของข้อมูลข่าวสาร (Information Security) เพื่อรักษาความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ของ

องค์ประกอบต่างๆ ที่ถูกผนวกเข้าเป็นระบบสารสนเทศนับตั้งแต่กระบวนการสร้าง ประมวลผล และการรับส่งข้อมูลสารสนเทศนั้นๆ

กนกวรรณ ตาลเสียน (2560) กล่าวถึงแนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศของกลุ่มอุตสาหกรรมความมั่นคงปลอดภัยของคอมพิวเตอร์ ได้กำหนดแนวคิดหลักของความมั่นคงปลอดภัยของคอมพิวเตอร์ขึ้น ประกอบด้วย

- 1) ความลับ Confidentiality
- 2) ความสมบูรณ์ Integrity
- 3) ความพร้อมใช้ Availability
- 4) ความถูกต้องแม่นยำ Accuracy
- 5) เป็นของแท้ Authenticity
- 6) ความเป็นส่วนตัว Privacy

กนกวรรณ ตาลเสียน (2560) อธิบายว่า

ความลับ Confidentiality เป็นการรับประกันว่าผู้มีสิทธิ์ และได้รับอนุญาตเท่านั้นที่จะสามารถเข้าถึงข้อมูลได้ องค์การต้องมีมาตรการนโยบายป้องกันการเข้าถึงข้อมูลสารสนเทศที่เป็นความลับ เช่น การจัดประเภทของข้อมูลสารสนเทศ การรักษาความปลอดภัยกับแหล่งจัดเก็บข้อมูลและการกำหนดนโยบายรักษาความมั่นคงปลอดภัย ประกอบกับความต้องการความสะดวกรบาย

ความสมบูรณ์ (Integrity) คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลกปลอมสำหรับสารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้อง ครบถ้วน สารสนเทศจะขาดความสมบูรณ์ ก็ต่อเมื่อสารสนเทศนั้นถูกนำไปเปลี่ยนแปลงด้วยสารสนเทศอื่น ถูกทำให้เสียหาย ถูกทำลาย หรือถูกกระทำในรูปแบบอื่น ๆ เพื่อขัดขวางการพิสูจน์การเป็นสารสนเทศ

ความพร้อมใช้ (Availability) คือ สารสนเทศที่ตอบสนองความต้องการของผู้ใช้งานที่จะเข้าถึงหรือเรียกใช้งานระบบได้อย่างราบรื่นจะเป็นผู้ใช้งานระบบที่ได้รับอนุญาตเท่านั้นแต่

หากเป็นผู้ที่ไม่ได้รับอนุญาต ในการเข้าถึงหรือเรียกใช้งานจะถูกขัดขวางและล้มเหลวในการเข้าระบบนั้น ๆ

ความเป็นของแท้ (Authenticity) คือ สารสนเทศที่ถูกจัดทำขึ้นมาจากผู้ดูแลระบบเพียงเท่านั้น และไม่มีผู้อื่นทำซ้ำโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบหรือจากแหล่งที่ไม่คุ้นเคย

ความเป็นส่วนตัว (Privacy) คือ สารสนเทศที่ถูกรวบรวมและจัดเก็บโดยองค์กร ที่มีวัตถุประสงค์ให้ผู้เป็นเจ้าของข้อมูลสารสนเทศรับทราบ ในขณะที่มีการรวบรวมข้อมูลสารสนเทศนั้น มิฉะนั้นจะถือว่าการละเมิดสิทธิส่วนบุคคลด้านสารสนเทศ

กนกวรรณ ตาลเสียน (2560) อธิบายถึง อุปสรรคของงานความมั่นคงปลอดภัยของสารสนเทศ โดยมีรายละเอียดดังนี้

- 1) ความมั่นคงปลอดภัย คือ ความไม่สะดวก เนื่องจากต้องเสียเวลาในการป้อน Password และกระบวนการอื่น ๆ ในการพิสูจน์ตัวตนของผู้เข้าใช้งาน
- 2) มีความซับซ้อนบางอย่างในคอมพิวเตอร์ที่ผู้ใช้ทั่วไปไม่ทราบ เช่น Registry Port Service เหล่านี้จะเป็นที่ทราบกันดีในแวดวงของ Programmer หรือผู้ดูแลระบบ
- 3) ผู้ใช้คอมพิวเตอร์ไม่ระแวดระวัง เช่น การบันทึกรหัสทิ้งไว้ ไม่ Log Out จากระบบ และไม่ Log หน้าจอเมื่อไม่ใช้งาน เป็นต้น
- 4) การพัฒนาซอฟต์แวร์ไม่คำนึงถึงความปลอดภัยภายหลัง
- 5) แนวโน้มเทคโนโลยีสารสนเทศคือการแบ่งปันไม่ใช้การป้องกัน
- 6) มีการเข้าถึงข้อมูลได้จากทุกสถานที่

สรุปได้ว่า ความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ มีความสำคัญและมีความจำเป็น ซึ่งในปัจจุบันมีภัยคุกคามทางคอมพิวเตอร์มากมาย ไม่ว่าจะเป็นภัยคุกคามจากแฮ็กเกอร์ การละเมิดสิทธิส่วนบุคคล หรือข้อมูลต่าง ๆ ของบุคคลอื่นบนระบบคอมพิวเตอร์ การรักษาความมั่นคงปลอดภัยทางไซเบอร์จึงมีความจำเป็นต้องคำนึงถึงการคุ้มครองความเป็นส่วนตัวและความสะดวกสบาย ในการเข้าถึงระบบของแต่ละบุคคลด้วยเช่นกัน ความเป็นส่วนตัวถือว่าเป็นเรื่องที่มีความสำคัญที่แต่ละบุคคลควรคำนึงถึงในการใช้งานระบบคอมพิวเตอร์ สำหรับปัจจัยที่ส่งผลต่อความมั่นคงปลอดภัยของสารสนเทศนั้น ขึ้นอยู่กับความรู้ความเข้าใจในความ

ปลอดภัยและการรับรู้ถึงภัยคุกคามที่ก่อให้เกิดความเสียหายต่อข้อมูลบุคคลหรือองค์กรเองนั้น ในความมั่นคงปลอดภัยของสารสนเทศมีความสำคัญและมีความจำเป็นที่จะต้องรักษาข้อมูลให้ เป็นความลับเพื่อความปลอดภัยในการใช้ข้อมูลสารสนเทศ

2.2 แนวคิดและทฤษฎีเกี่ยวกับบุคลิกภาพ

ความหมายของบุคลิกภาพ เออร์เนส อาร์ ฮิลการ์ด (1962 อ้างถึงใน ธนพร วัฒนศรานนท์, 2555 : 27) บุคลิกภาพเป็นลักษณะส่วนรวมของบุคคล และแสดงออกทางพฤติกรรม

ริชาร์ด ซี บูทชินและคณะ (1991 อ้างถึงใน ธนพร วัฒนศรานนท์, 2555 : 27) บุคลิกภาพ เป็นลักษณะนิสัยและรูปแบบของความคิด ความรู้สึก และการประพฤติปฏิบัติของแต่ละบุคคล

ศรีเรือน แก้วกังวาล (2554 : 7) กล่าวถึงความหมายของบุคลิกภาพ คือ ลักษณะเฉพาะบุคคลที่มีทั้งภายในและภายนอก ลักษณะที่จะแสดงออกหรือเก็บซ่อนไว้ภายใน เช่น กริยาท่าทางการเจรจา การแต่งตัว เป็นต้น ลักษณะเหล่านี้จะนำไปสู่พฤติกรรมที่แสดงออกในแต่ละบุคคล

จากความหมายของบุคลิกภาพที่กล่าวมาทั้งหมด สรุปได้ว่า บุคลิกภาพนั้นอาจสังเกตเห็นได้ด้วยตา หรือมองเห็นด้วยการแสดงออกในตัวบุคคลที่ทำให้ผู้อื่นเห็นว่ามีบุคลิกอย่างไรที่บ่งบอกถึงความเป็นตัวตน นอกจากนี้ ปัจจัยในการแสดงออกของบุคลิกภาพอาจเกิดจากสังคม สิ่งแวดล้อม และสิ่งต่าง ๆ ที่บีบบังคับ ให้แสดงออกของบุคลิกนั้นออกมา

Stephen P. Robbin (1989) ได้กล่าวถึงแนวคิดตามคุณลักษณะ (Traits Theory) ไว้ว่า บุคลิกภาพของบุคคลเกิดจากพฤติกรรมที่บุคคลแสดงมาในสถานการณ์ต่าง ๆ ซึ่งเป็นพฤติกรรมหรือลักษณะที่แสดงออกบ่อย ๆ หรือซ้ำ ๆ กันในสถานการณ์ที่ต่างกันออกไป ซึ่งพฤติกรรมเหล่านี้ จะแสดงออกค่อนข้างที่จะคงที่จนเป็นลักษณะของบุคคลหรือคุณสมบัติประจำตัวของบุคคลนั้น โดย แนวคิดนี้ สามารถนำไปสังเกตพฤติกรรมของบุคคลได้ ดังนี้

ตาราง 2.1 ตารางแสดงบุคลิกภาพ

	กังวลสูง (High anxiety)	กังวลต่ำ (Low anxiety)
เปิดเผย (Extrovert)	ซีกังวล/เปิดเผย	ไม่กังวล/เปิดเผย
เก็บตัว (Introvert)	ซีกังวล/เก็บตัว	ไม่กังวล/เก็บตัว

ที่มา: Stephen P. Robbins, (1989)

จากตารางสามารถจัดกลุ่มบุคลิกภาพออกเป็น 4 กลุ่ม คือ

- พวกที่ชอบกังวลและเปิดเผย จะมีลักษณะชอบสังคม ชอบอุ่น น่ารัก ชอบสังคม แต่จะซีกังวล ตื่นเต้นง่าย และจะมีความรู้สึกที่ไม่มั่นคง
- พวกที่ชอบกังวลและชอบเก็บตัว มักจะซีฉลาด อาย เย็นชา มีความเครียด ชอบความตื่นเต้น และไม่ค่อยมีความมั่นคง
- พวกที่ชอบเปิดเผยจะไม่มี ความกังวล จะมีความมั่นคงจริงใจ มีความซื่อสัตย์ ปรับตัวได้ดี มีความอบอุ่น ชอบเข้าสังคมและรักอิสระ
- พวกที่ชอบเก็บตัวไม่มีความกังวล มักเป็นคนที่มีความเชื่อมั่น มีความใจเย็น ไร้วางใจได้ปรับตัวได้ดี สงบ เย็นชาและไม่ชอบเกาะกลุ่ม

2.3 แนวคิดและทฤษฎีเกี่ยวกับบุคลิกภาพ 5 องค์ประกอบ

ลักษณะบุคลิกภาพ 5 องค์ประกอบ ศึกษาตามแนวคิดของ คอสตาและแมคเคร Costa and McCrae (1992 อ้างถึงใน นิภาพร พวงมี, 2554 : 15) มีความเชื่อว่าบุคลิกภาพทั้งห้า องค์ประกอบเปรียบเสมือนลักษณะนิสัยย่อย ๆ ของมนุษย์ที่คล้ายคลึงกันซึ่งในงานวิจัยนำเสนอ

รายละเอียดตามแนวคิดของ (Costa and McCrae, 1992 as cited in Feist and Feist, 2006 : 451 - 417) ซึ่งระบุรายละเอียดไว้ดังนี้

1. บุคลิกภาพแบบหวั่นไหว (Neuroticism) หมายถึงเป็นผู้ที่มีความวิตกกังวล (Worry) เป็นคนโกรธง่าย (Anger) ความท้อแท้ (Discouragement) การคำนึงถึงแต่ตนเอง (Self Consciousness) การมีความกระตุ้นรุนแรง (Impulsiveness) และมีอารมณ์เปราะบาง (Vulnerability)

ตาราง 2.2 ลักษณะของบุคลิกภาพแบบหวั่นไหว

ลักษณะบุคลิกภาพ	ลักษณะของผู้ที่ได้คะแนนต่ำ	ลักษณะผู้ที่ได้คะแนนสูง
แบบหวั่นไหว	สงบ โกรธง่าย อารมณ์ไม่ฉุนเฉียวง่าย รู้สึกอึดอัด ทนต่อสิ่งที่มากระตุ้นได้ เผชิญกับความตึงเครียดได้เป็นอย่างดี	วิตกกังวล โกรธง่าย อารมณ์แปรปรวน รู้สึกอึดอัดง่าย ถูกยั่วยุต่อสิ่งที่มากระตุ้นได้ง่าย รับมือกับความตึงเครียดไม่ค่อยง่าย ลำบาก

ที่มา : Costa and McCrae, 1992 as cited in Feist and Feist, (2006)

2. บุคลิกภาพแบบแสดงตัว (Extraversion) หมายถึง เป็นผู้ที่มีความอบอุ่น (Warmth) ชอบอยู่ร่วมกับผู้อื่น (Gregariousness) แสดงออกแบบตรงไปตรงมา (Assertiveness) ชอบมีกิจกรรม (Activity) ชอบแสวงหาความตื่นเต้น (Excitement-Seeking) และมีอารมณ์ด้านบวก (Positive-Emotions)

ตาราง 2.3 ลักษณะบุคลิกภาพแบบแสดงตัว

ลักษณะบุคลิกภาพ	ลักษณะของผู้ที่ได้คะแนนต่ำ	ลักษณะของผู้ที่ได้คะแนนสูง
แบบแสดงตัว	รักสันโดษ ไม่ชอบเข้าสังคม จริงจัง ไม่ต้องการความตื่นเต้น ไม่ค่อยแสวงหาความต้องการ ไม่ค่อยร่าเริง	เป็นมิตรและสนิทสนม ชอบเข้าสังคม แสดงออก เป็นผู้นำ ชอบความตื่นเต้น ชอบทำกิจกรรม กระฉับกระเฉง ร่าเริง มองโลกในแง่ดี

ที่มา : Costa and McCrae, 1992 as cited in Feist and Feist, (2006)

3. บุคลิกภาพแบบเปิดรับประสบการณ์ (Openness to Experience) หมายถึง การเป็นคนช่างฝัน (Fantasy) ความซาบซึ้งในความงาม (Aesthetics) การเปิดเผยความรู้สึก (Feelings) การปฏิบัติ (Actions) การมีความคิด (Ideas) และการยอมรับค่านิยม (Values)

ตาราง 2.4 ลักษณะบุคลิกภาพแบบเปิดรับประสบการณ์

ลักษณะบุคลิกภาพ	ลักษณะของผู้ที่ได้คะแนนต่ำ	ลักษณะของผู้ที่ได้คะแนนสูง
แบบเปิดประสบการณ์	ตรงไปตรงมา ไม่คิดสร้างสรรค์ เพิกเฉย ไม่สนใจ ไม่ใฝ่เรียนรู้ ทำในสิ่งที่เคยชิน เน้นการใช้เหตุผลในมุมมองแคบ ๆ ไม่ยอมรับค่านิยมใหม่ ๆ	มีจินตนาการ มองอนาคต คิดสร้างสรรค์ ใฝ่เรียนรู้ ชอบความหลากหลาย ลองสิ่งใหม่ เน้นการใช้เหตุผลในมุมมองกว้าง พร้อมที่จะลองค่านิยมใหม่ ๆ

ที่มา : Costa and McCrae, 1992 as cited in Feist and Feist, (2006)

4. บุคลิกภาพแบบประนีประนอม (Agreeableness) หมายถึง การเป็นผู้ใจกว้างใจผู้อื่น (Trust) ความตรงไปตรงมา (Straightforwardness) ความรู้สึกเอื้อเฟื้อ (Altruism) การยอมตามผู้อื่น (Compliance) ความสุภาพ (Modesty) และการมีจิตใจอ่อนโยน (Tender-Mindedness)

ตาราง 2.5 ลักษณะองค์ประกอบบุคลิกภาพแบบประนีประนอม

ลักษณะบุคลิกภาพ	ลักษณะของผู้ที่ได้คะแนนต่ำ	ลักษณะผู้ที่ได้คะแนนสูง
แบบประนีประนอม	ชอบวิจารณ์คนอื่น ระแวงระแวง พุดเกินความจริง ไม่เต็มใจที่จะช่วยเหลือผู้อื่น ก้าวร้าว ชอบแข่งขัน รู้ว่าตนเองเหนือผู้อื่น ไม่มีเมตตา	เห็นว่าผู้อื่นซื่อสัตย์ เจตนาดี ตรงไปตรงมา จริงใจ เต็มใจที่จะช่วยเหลือผู้อื่น คล้อยตามผู้อื่น มีความอดทน จิตใจอ่อนโยน

ที่มา : Costa and McCrae, 1992 as cited in Feist and Feist, (2006)

5. บุคลิกภาพแบบมีจิตสำนึก (Conscientiousness) หมายถึง การมีความสามารถ (Competence) ความเป็นระเบียบ (Order) การมีความรับผิดชอบต่อหน้าที่ (Dutifulness) ความต้องการสัมฤทธิ์ผล (Achievement Striving) ความมีวินัยในตนเอง (Self-Discipline) และความคิดที่ใช้ปฏิบัติงาน (Deliberation) ลักษณะองค์ประกอบบุคลิกภาพแบบมีจิตสำนึกสำหรับบุคลิกภาพแบบมีจิตสำนึก

ตาราง 2.6 ลักษณะของบุคลิกภาพแบบมีจิตสำนึก

องค์ประกอบบุคลิกภาพ	ลักษณะของผู้ที่ได้คะแนนต่ำ	ลักษณะของผู้ที่ได้คะแนนสูง
แบบมีจิตสำนึก	<p>ประมาท</p> <p>ไม่เป็นระเบียบ ไม่มีระบบ</p> <p>ไม่เอาใจใส่ต่อหน้าที่</p> <p>มีความต้องการผลสัมฤทธิ์ต่ำ</p> <p>ทนต่อสิ่งที่ไม่กระตุ้นได้</p> <p>ผลัดวันประกันพรุ่ง</p> <p>ปฏิบัติโดยปราศจากการไตร่ตรอง</p>	<p>มีความสามารถ</p> <p>เป็นระเบียบเรียบร้อย</p> <p>มีจิตสำนึกรับผิดชอบต่อหน้าที่</p> <p>มีความพยายามเพื่อให้สำเร็จตามเป้าหมาย</p> <p>มุ่งเน้นการปฏิบัติภารกิจให้สำเร็จ</p> <p>คิดอย่างรอบคอบก่อนปฏิบัติ</p>

ที่มา : Costa and McCrae, 1992 as cited in Feist and Feist, (2006)

คอสตาและแมคครี (Costa and McCrae, 1987 as cited in Schultz and Schultz, 2005 : 284) กล่าวว่า บุคลิกภาพห้าองค์ประกอบ หมายถึง การอธิบายลักษณะของมนุษย์เป็น 5 องค์ประกอบ คือ บุคลิกภาพแบบหวั่นไหว (Neuroticism) บุคลิกภาพแบบแสดงตัว (Extraversion) บุคลิกภาพแบบเปิดรับประสบการณ์ (Openness) บุคลิกภาพแบบประนีประนอม (Agreeableness) และบุคลิกภาพแบบมีจิตสำนึก (Conscientiousness)

โกลด์เบิร์ก Goldberg, 1990 as cited in Quilty et al (2006 อ้างถึงใน มงคล อุดมชัย พัฒนาการ, 2557 : 20-21) บุคลิกภาพห้าองค์ประกอบ หมายถึง การอธิบายบุคลิกลักษณะด้วยการใช้คำคุณศัพท์ และจัดกลุ่มบุคลิกภาพออกเป็น 5 ปัจจัย คือ

ความมั่นคงทางอารมณ์ (Emotional Stability) การแสดงตัว (Extraversion) สติปัญญา (Intellect) ประนีประนอม (Agreeableness) และการมีจิตสำนึก (Conscientiousness)

สรุปได้ว่า บุคลิกภาพห้าองค์ประกอบ หมายถึง ลักษณะของบุคลิกภาพอันได้แก่ 1. บุคลิกภาพแบบหวั่นไหว 2. บุคลิกภาพแบบแสดงตัว 3. บุคลิกภาพแบบเปิดรับประสบการณ์ 4. บุคลิกภาพแบบประนีประนอม และ 5. บุคลิกภาพแบบมีจิตสำนึก ทั้งนี้เป็นสิ่งที่กำหนดพฤติกรรมหรือสิ่งที่ออกมาจากในแต่ละบุคคลที่แสดงออกมาอย่างชัดเจน

Costa & McCrae (1992) ได้กล่าวถึงลักษณะบุคลิกภาพ 5 องค์ประกอบ ไว้ว่า

1. บุคลิกภาพแบบหวั่นไหว (Neuroticism: N) เป็นลักษณะบุคลิกภาพแบบมั่นคงทางอารมณ์ (Emotional Stability) บุคคลที่มีบุคลิกภาพแบบหวั่นไหวสูงมีแนวโน้มที่จะมีความวิตกกังวล อารมณ์แปรปรวน คำนึงถึงแต่ตนเอง อุนเฉียว สำหรับบุคคลที่มีบุคลิกภาพแบบหวั่นไหวต่ำหรือเรียกว่าเป็นผู้มีความมั่นคงในอารมณ์ (Emotional Stability) จะเป็นคนที่สุขุมเยือกเย็น (Clam) พึงพอใจในตนเอง (Self-satisfied) และอารมณ์ไม่อุนเฉียว (Extroversion: E)
2. บุคลิกภาพแบบแสดงตัว (Extroversion: E) เป็นลักษณะบุคลิกภาพของบุคคลที่สนใจในสิ่งต่าง ๆ รอบตัวและสิ่งต่าง ๆ ภายในตัวบุคคล ดังนั้นบุคคลที่มีบุคลิกภาพแบบแสดงตัวตนสูงมีแนวโน้มที่จะเป็นคนมีเสน่ห์ (Affectionate) สนุกสนานร่าเริง ช่างพูด ชอบเข้าสังคม มองโลกในแง่ดี ในทางตรงข้ามบุคคลที่มีบุคลิกภาพแบบแสดงตัวต่ำมักจะเป็นคนเก็บตัว (Reserved) เงียบขรึม (Quiet)
3. บุคลิกภาพแบบเปิดรับประสบการณ์ (Open to Experience : O) เป็นลักษณะของบุคคลที่ชอบความหลากหลาย สังเกตได้จากบุคคลประเภทนี้จะต้องการให้มีการแสดงความคิดเห็นในกิจกรรมต่าง ๆ และ มีความสุขในการคบค้าสมาคมกับบุคคลหรือสิ่งต่าง ๆ ที่คุ้นเคย เป็นบุคคลที่มักค้นหาประสบการณ์แปลกใหม่ นั่นคือบุคคลที่มีบุคลิกภาพแบบเปิดประสบการณ์สูง จะมีความคิดสร้างสรรค์ (Creative) มีจินตนาการสูง จะนำเสนอตัวเองเพื่อเข้าร่วมกิจกรรมต่าง ๆ ในทางตรงกันข้ามบุคคลที่มีบุคลิกภาพที่ไม่เปิดรับสิ่งใหม่
4. บุคลิกภาพแบบประนีประนอม (Agreeableness: A) เป็นลักษณะของบุคคลใจอ่อน มีความเมตตา ไว้วางใจผู้อื่นง่าย (Trusting) คล้อยตามผู้อื่น ในทางตรงกันข้ามถ้ามีบุคลิกภาพในระดับต่ำ มักจะเป็นคนที่ขี้สงสัยในเรื่องทั่ว ๆ ไป (Generally suspicious) และชอบวิจารณ์ผู้อื่น (Critical)
5. บุคลิกภาพแบบมีจิตสำนึก (Conscientiousness : C) เป็นลักษณะของบุคคลที่มักจะมีความเป็นระเบียบ (Ordered) ควบคุม (Controlled) มีระบบระเบียบวินัยในตนเอง (Self-Disciplined) ดังนั้น บุคคลที่มีบุคลิกภาพแบบมีจิตสำนึกสูงจึงเป็นคนชอบทำงานหนัก มีจิตสำนึก

รับผิดชอบในทางตรงกันข้าม ถ้ามีบุคลิกภาพแบบมีจิตสำนึกในระดับต่ำจะเป็นคนที่ไม่ม่ระบบระเบียบ (Disorganized) ประมาท (Negligent) ชี้เกียจ (Lazy)

สรุปได้ว่า ระหว่างบุคลิกภาพ 5 องค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย ล้วนแสดงออกจากพฤติกรรมในการใช้สารสนเทศของแต่ละบุคคล ที่มีความชัดเจนและบ่งบอกถึงตัวตนของบุคคลนั้นอาจจะเกี่ยวข้องกับความปลอดภัยในการใช้ข้อมูล ทั้งนี้ทั้งนั้น ปัจจัยที่เกิดจากบุคลิกภาพส่วนบุคคลเอง ความสัมพันธ์ในตัวเอง รวมไปถึงพฤติกรรมต่างๆ ที่นำมาซึ่งเป็นปัญหาของการละเมิดสิทธิส่วนบุคคล ทำให้ความคิดและพฤติกรรมความสัมพันธ์ในตัวบุคคลเปลี่ยนไป และเป็นที่มาของปัญหาอื่นๆ อีกหลายประการ ทั้งนี้ทั้งนั้น สาเหตุทั้งหมดทั้งปวงที่เกิดขึ้นและมองเห็นเป็นรูปธรรมและนามกระทำนั้น อาจเกิดจากบุคลิกภาพ 5 องค์ประกอบที่มีความสัมพันธ์กับพฤติกรรมในการใช้ข้อมูลสารสนเทศอย่างปลอดภัย

2.4 แนวคิดและทฤษฎีที่เกี่ยวข้องกับพฤติกรรมการใช้สารสนเทศ

กรรข วิไลลักษณ์ (2560) ข้อมูลและสารสนเทศเป็นทรัพยากรที่สำคัญต่อบุคคลหรือองค์กรที่เป็นผู้สร้าง ประมวลผล และรับส่งข้อมูลสารสนเทศนั้นๆ ด้วยเหตุนี้ทรัพยากรนี้จึงเป็นเป้าหมายหลักของการโจมตีของผู้ไม่ประสงค์ดีโดยความเสียหายที่เกิดขึ้นมักเกิดขึ้นในลักษณะที่สำคัญ คือ การเปิดเผยความลับ การแก้ไขข้อมูลโดยไม่มีสิทธิ์และการทำให้ข้อมูลนั้นๆ ไม่สามารถเข้าถึงได้ เช่น ถูกลบ เปลี่ยนแปลงหรือถูกเข้ารหัสลับเพื่อเรียกค่าไถ่ เป็นต้น

พฤติกรรมการใช้ระบบสารสนเทศในองค์กร (Behavior) หมายถึง ความตั้งใจของบุคลากรที่จะปฏิบัติตามมาตรการ การรักษาความมั่นคงปลอดภัยจากทัศนคติ กฎเกณฑ์ ความเชื่อและการรับรู้ถึงมาตรการที่ควรปฏิบัติตาม ซึ่งพฤติกรรมดังกล่าวส่งผลกระทบต่อความปลอดภัยของการใช้ระบบสารสนเทศในองค์กร ซึ่งพฤติกรรมการใช้ระบบสารสนเทศในองค์กรจะส่งผลต่อระดับความมั่นคงปลอดภัย

พฤติกรรม หมายถึงการกระทำหรือการแสดงออกโดยมีพื้นฐานมาจากการรับรู้ ความรู้ และทัศนคติ ของตัวบุคคลนั้น ซึ่งบุคคลมีพฤติกรรมที่แตกต่างกันออกไป เนื่องจากทัศนคติและ

การรับรู้ที่ต่างกัน อาจเกิดขึ้นจากประสบการณ์หรือสังคมที่พบเจอ สิ่งเหล่านี้ส่งผลต่อพฤติกรรมของบุคคล

นักทฤษฎีองค์การจะให้ความสนใจกับการศึกษาพฤติกรรมของแต่ละบุคคลเพื่อนำไปปรับใช้องค์ประกอบต่าง ๆ ขององค์กร ในการศึกษาพฤติกรรมบุคคลที่เข้าใจถึงองค์ประกอบภายนอกของบุคคล เช่น สิ่งแวดล้อม เหตุการณ์ต่าง ๆ เป็นต้น

ดังนั้น ในการศึกษาพฤติกรรมการใช้ข้อมูลสารสนเทศของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสารนั้น จึงเป็นการศึกษาพฤติกรรมภายนอกที่เป็นผลจากการถูกผลักดันด้วยความต้องการข้อมูลสารสนเทศ

สมใจ ศรีปานเงิน (2540 : 16-17) กล่าวถึง พฤติกรรมของบุคคลไม่ได้จะเกิดขึ้นเฉย ๆ แต่เกิดขึ้น เพราะมีสิ่งใดสิ่งหนึ่งมากระทบต่อร่างกาย สามารถแบ่งพฤติกรรมออกเป็น 3 ชนิด ดังนี้

1. พฤติกรรมที่เกิดจากกล้ามเนื้อ เกิดจากการเคลื่อนไหวจนทำให้เกิดเป็นกิจกรรม เช่น การพูด การเดิน หรือกิจกรรมต่าง ๆ เป็นต้น
2. พฤติกรรมที่เป็นความรู้สึก ความคิดและความรู้สึก ภาวะปกติในการรับรู้ เข้าใจ และตอบสนอง ต่อสิ่งเร้าภายนอก เช่น อาการเจ็บปวด การได้ยิน เป็นต้น
3. พฤติกรรมที่เป็นอารมณ์ การแสดงออกของภาวะจิตใจที่ได้รับการกระตุ้นให้เกิดการแสดงออก เช่น ความอยากรู้อยากเห็น ความโกรธ ความกลัว ความยินดี เป็นต้น

พจนานุกรมฉบับราชบัณฑิตยสถาน (2546 : 1182) ได้ให้คำจำกัดความของคำว่า สารสนเทศ คือ สาร และ สนเทศ คำว่า สาร หมายความว่า แก่นสาร ส่วนสำคัญ ใจความ และในส่วนของคำว่า สนเทศ หมายความว่า คำที่แสดง คำที่จำแนกออก หรือชี้แจง ทั้งนี้คำว่า สารสนเทศ หมายถึง แก่นหรือเนื้อหาที่สำคัญ ที่แสดงออกให้เห็นแก่นแท้หรือเนื้อหาที่อาจเป็นข้อมูล หรือ ข้อเท็จจริง ข่าวสาร ความรู้ เรื่องราวทั่วไป ความรู้ทางวิชาการหรือศาสตร์ ความรู้สึก ความคิด ประสบการณ์ ซึ่งได้มีการกลั่นกรอง ประมวลและเรียบเรียง โดยใช้ภาษาพูด ภาษาเขียน และสัญลักษณ์ต่าง ๆ โดยการบันทึก หรือการแสดงออกโดยกรรมวิธีต่าง ๆ ที่สามารถมองเห็นได้ ฟังได้ มีรูปแบบเป็นสื่อที่ถ่ายทอดให้ผู้อื่นได้รับรู้ อาจสรุปสั้นๆ ได้ว่าเป็นข้อมูลที่ผ่านการประมวลผลแล้วด้วยวิธีการใดวิธีการหนึ่ง เพื่อทำให้เกิดประโยชน์ในการใช้ข้อมูลนั้น

เพ็ญพันธ์ เพชรคร (2554 : 1-2) อธิบายว่า การใช้สารสนเทศ หมายถึง ความรู้ความสามารถของบุคคลในการเข้าถึงสารสนเทศ เช่น การค้นคว้าข้อมูล ค้นหาแหล่งสารสนเทศ เป็นต้น ในการใช้สารสนเทศทำให้ผู้ใช้ตระหนักถึงความสำคัญ รู้จักแหล่งสารสนเทศ สามารถนำสารสนเทศมาใช้ให้เกิดประโยชน์สูงสุดและ สามารถนำข้อมูลสารสนเทศมาสื่อสารกับผู้อื่นได้อย่างมีประสิทธิภาพ

พฤติกรรมการใช้สารสนเทศ คือ การใช้สารสนเทศหรือการนำข้อมูลสารสนเทศไปใช้เพื่อให้เกิดประโยชน์ ขึ้นอยู่กับบุคคล แต่ละบุคคลย่อมมีวัตถุประสงค์ในการใช้สารสนเทศที่แตกต่างกันไป เช่น การนำสารสนเทศเพื่อใช้ประกอบการเรียน การทำรายงานตามที่ได้รับมอบหมาย หรือในวัยทำงานจำเป็นที่จะต้องใช้สารสนเทศในการจัดทำข้อมูลหรือจัดทำโปรเจกต์เพื่อนำเสนอหัวหน้างานหรือลูกค้าทั้งนี้สามารถจำแนกเหตุผล ในการใช้สารสนเทศ ออกเป็น 5 ประการ

1. เพื่อสนองความต้องการส่วนบุคคล เช่น ใช้แก้ปัญหาประจำวัน ปรับตัวให้อยู่รอดในภาวะวิกฤติ ติดตามข้อมูลข่าวสารและเหตุการณ์ในปัจจุบันและสร้างความสุขความบันเทิง
2. เพื่อการศึกษาและการเรียนรู้ ช่วยเพิ่มพูนความรู้หรือข้อมูลให้ลึกซึ้งและกว้างไกลมากยิ่งขึ้น
3. เพื่อประกอบอาชีพและการปฏิบัติงาน และช่วยส่งเสริมการปฏิบัติงานให้มีประสิทธิภาพและบรรลุตามเป้าหมายและเกิดประโยชน์สูงสุด สำหรับเทคโนโลยีสารสนเทศกับการปฏิบัติงาน ในปัจจุบันมนุษย์ นำเทคโนโลยีมาประยุกต์ใช้เพื่อเป็นตัวช่วยในการทำงาน การใช้เทคโนโลยีสารสนเทศในสำนักงานเพื่อให้เกิดความสะดวกรวดเร็ว
4. เพื่อถ่ายทอดข้อมูลสารสนเทศไปยังบุคคลอื่น เช่น นักเขียน นักเอกสาร นักสารสนเทศ เป็นต้น
5. เพื่อวัตถุประสงค์อื่นๆ เช่น การแลกเปลี่ยนวัฒนธรรม การแลกเปลี่ยนทางวิทยาศาสตร์ และเทคโนโลยี ความบันเทิง ความเพลิดเพลิน การติดต่อสื่อสารจากบุคคลหนึ่งไปยังบุคคลหนึ่ง เป็นต้น

สรุปได้ว่าพฤติกรรมการใช้สารสนเทศ หมายถึง การกระทำหรือการแสดงผลออกในการแสวงหาความรู้ ข้อมูลข่าวสาร และความต้องการอื่น ๆ เช่น สำหรับวัตถุประสงค์อื่นของการใช้สารสนเทศ ได้แก่ ตอบสนองความต้องการของแต่ละบุคคล เพื่อการค้นคว้าหาข้อมูล รวบรวม

ข้อมูล เพื่อการศึกษา รวมไปถึงการแสวงหาความบันเทิง ความเพลิดเพลินและการติดต่อสื่อสาร เป็นต้น

2.5 งานวิจัยที่เกี่ยวข้อง

คณิน อุดมสุขประเสริฐ (2555) อ้างถึงในการศึกษาพฤติกรรมการตั้งรหัสผ่านของผู้ใช้งานอินเทอร์เน็ตด้วยทำงานในประเทศไทย พฤติกรรมการตั้งรหัสผ่านและการใช้งานอินเทอร์เน็ต พบว่ากลุ่มตัวอย่างส่วนใหญ่มีพฤติกรรมที่มีความเสี่ยงในการใช้รหัสผ่าน เนื่องจากการตั้งรหัสผ่านจะมีการตั้งโดยใช้ข้อมูลที่อยู่ใกล้ตัว มีการตั้งรหัสผ่านเดียวกันในหลาย ๆ บัญชี มีการจดจำรหัสหรือจดบันทึกรหัสผ่านโดยไม่คำนึงถึงความปลอดภัย และนอกจากนี้กลุ่มตัวอย่างนิยมใช้อินเตอร์ที่บ้านและที่ทำงาน ซึ่งผู้ใช้งานเหล่านี้มีความเสี่ยงในการถูกขโมยข้อมูลได้ง่าย จากผลสำรวจของบุคลากรในมหาวิทยาลัยพรินซ์ตัน ประเทศสหรัฐอเมริกาผู้ใช้งานส่วนใหญ่นิยมจดจำรหัสผ่านมากกว่าการจดบันทึก

จากการสำรวจของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) พบว่ากลุ่มผู้ใช้งานอินเทอร์เน็ตในประเทศไทยส่วนใหญ่อยู่ในช่วงอายุ 30-39 ปี รองลงมาเป็นช่วงอายุ 20-29 ปี ช่วงอายุ 50-59 ปี และช่วงอายุ 15-19 ปี มีการกระจายความทั่วถึงของอินเทอร์เน็ตภายในประเทศคิดเป็นร้อยละ 32.5% และการป้องกันและแก้ไขปัญหาคอมพิวเตอร์หรืออินเทอร์เน็ต รหัสผ่าน เป็นชุดตัวอักษร ที่ผู้ใช้งาน ถือเป็นกุญแจสำหรับการใช้งานระบบหรือบริการใด ๆ เช่น อีเมล เป็นต้น แต่จะให้ดี รหัสผ่านควรประกอบไปด้วยตัวเลขและตัวอักษรเล็กใหญ่ ผู้ใช้งานอินเทอร์เน็ตด้วยทำงานส่วนใหญ่ไม่เคยเปลี่ยนรหัสผ่านเลย รองลงมาการเปลี่ยนรหัสผ่าน 1 ปี ต่อครั้ง 3 เดือนต่อครั้ง 6 เดือนต่อครั้ง 1 เดือนต่อครั้งและ 1 สัปดาห์ต่อครั้งตามลำดับ โดยมีผู้ตอบแบบสอบถามบางส่วนไม่ทราบหรือไม่แน่ใจช่วงเวลาในการเปลี่ยนรหัสผ่านในแต่ละครั้งนั้นผู้ใช้งานอินเทอร์เน็ตด้วยทำงานจะมีการนำตัวอักษรหรือตัวเลขทั้งสองอย่างมาใช้เป็นส่วนประกอบของรหัสผ่าน ผู้ที่มีการนำอักษรหรือตัวเลขมาใช้อย่างใดอย่างหนึ่งและผู้ที่ไม่ใช้ทั้งอักขระพิเศษและตัวเลขมีสัดส่วนใกล้เคียงกัน ผู้ใช้งานอินเทอร์เน็ตด้วยทำงานส่วนใหญ่เคยลืมรหัสผ่าน โดยกลุ่มที่ลืมรหัสผ่านใช้กระบวนการในการกู้รหัสผ่านมากที่สุด รองลงมา

เป็นวิธีติดต่อผู้ให้บริการบัญชี สมัครงบบัญชีใหม่ดูที่บันทึกไว้ และอื่น ๆ ผู้ใช้งานอินเทอร์เน็ตช่วยทำงานส่วนใหญ่ไม่เคยถูกขโมยรหัสผ่าน โดยกลุ่มที่เคยถูกขโมยรหัสผ่านใช้กระบวนการในการกู้รหัสผ่านมากที่สุด รองลงมาเป็นวิธีติดต่อผู้ให้บริการบัญชีสมัครงบบัญชีใหม่ และเปลี่ยนรหัสผ่าน พฤติกรรมการตั้งรหัสผ่านและการใช้งานอินเทอร์เน็ต ส่วนใหญ่มีพฤติกรรมที่มีความเสี่ยงต่อการใช้งานรหัสผ่านโดยมีการตั้งรหัสผ่านจากข้อมูลที่อยู่ใกล้ตัว เช่น วันเดือนปีเกิด หมายเลขโทรศัพท์ หรือชื่อของผู้ใช้เองหรือชื่อคนใกล้ตัว เป็นต้น มีการใช้รหัสผ่านเดียวกันหลาย ๆ บัญชี และมีการจดบันทึกรหัสผ่านโดยไม่คำนึงถึงความปลอดภัย

การตั้งรหัสผ่านที่ง่ายต่อการคาดเดาซึ่งได้ผลลัพธ์ใกล้เคียงกับงานวิจัยของ Shirley และ Edward ที่ทำการสำรวจ พบว่าผู้ใช้งานมักจะใช้วิธีที่ง่ายที่สุดสำหรับการใช้งานรหัสผ่าน เช่น การจดจำรหัสผ่านมากกว่าการจดบันทึก การใช้รหัสผ่านเดียวกันในหลายบัญชีเพื่อการใช้งาน เป็นต้น จากข้อมูลที่สำรวจพบว่ากลุ่มตัวอย่างนิยมใช้อินเทอร์เน็ตที่บ้านและที่ทำงาน ทำให้ผู้ใช้งานส่วนใหญ่มีความเสี่ยงในด้านการถูกขโมยข้อมูล รหัสผ่านจากไวรัสหรือเครื่องมือที่ดักจับข้อมูลน้อยกว่าผู้ใช้เครื่องคอมพิวเตอร์สาธารณะเป็นประจำ (มนชัย เทียนทอง, 2548) การลืมรหัสผ่าน การถูกขโมยรหัสผ่าน และทัศนคติต่อความปลอดภัยบนระบบคอมพิวเตอร์ ความปลอดภัยบนระบบคอมพิวเตอร์ สำหรับผู้ใช้งานทั่วไป อาจเป็นเรื่องยาก และซับซ้อนจนส่งผลทำให้ผู้ใช้ไม่กล้าที่จะแก้ไขการตั้งค่าการใช้งาน

ธีรยุทธ เอกภูณ (2558) การศึกษาอิทธิพลของรูปแบบการใส่รหัสผ่านและประเภทของรหัสผ่าน ต่อการพิสูจน์ตัวตนด้วยรหัสผ่านตัวอักษรร่วมกับตารางกริดและรูปภาพในการทบทวนวรรณกรรมของงานวิจัยนี้มีความสอดคล้องกับงานวิจัยของ คณิน อุดมสุขประเสริฐ (2555) ที่ได้ศึกษาพฤติกรรมการตั้งรหัสผ่านของผู้ใช้อินเทอร์เน็ตวัยทำงานในประเทศไทย จากกลุ่มตัวอย่างทั้งหมด 494 คน มีพฤติกรรมในการตั้งรหัสผ่านโดยใช้ข้อมูลที่ใกล้ตัว เช่น วันเดือนปีเกิด เบอร์โทรศัพท์ บ้านเลขที่ เป็นต้น และนอกจากนี้ยังมีการตั้งรหัสผ่านเดียวกันในหลาย ๆ บัญชี

สุภกิจ มหิทธิบุรินทร์ (2557) ได้ศึกษาเกี่ยวกับการพิสูจน์ตัวตนเป็นวิธีการที่ใช้ในการตรวจสอบ ผู้ที่มาใช้งานระบบเครือข่ายอินเทอร์เน็ต โดยระบบจะทำการตรวจสอบจาก ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ว่าถูกอ้างหรือไม่ ซึ่งจุดประสงค์หลักของการพิสูจน์

ตัวตน คือ พิสูจน์ตัวบุคคลว่าผู้ที่เข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตนั้นเป็นใคร พร้อมทั้งตรวจสอบสิทธิว่าผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตนั้น มีสิทธิใช้ได้นานเท่าไร การใช้งานระบบเครือข่ายอินเทอร์เน็ต ซึ่งจุดประสงค์หลักของขบวนการนั้น เพื่อทำรายงานการให้ระบบเครือข่ายอินเทอร์เน็ต จะทำการยืนยัน บันทึกข้อมูลในการใช้งานระบบเครือข่ายอินเทอร์เน็ตโดยสามารถรายงานสรุปและสถิติต่างๆ ได้ตามความต้องการ ซึ่งการพิสูจน์ตัวตน (Authentication) ในการพิสูจน์ตัวตนนั้นมีความสัมพันธ์ถึงความปลอดภัยในการใช้ข้อมูลสารสนเทศ เมื่อตั้งคำถามถึงการรักษาความมั่นคงปลอดภัยบนระบบคอมพิวเตอร์ อาจให้คำนิยามด้วยภาพของการเข้าสู่ระบบปฏิบัติการหรือการเข้าสู่หน้าเว็บไซต์ด้วยชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นอย่างแรกเนื่องจากเป็นวิธีการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์แบบหนึ่งที่ได้พบได้บ่อยครั้งเมื่อมีความต้องการเข้าใช้งาน

ข้อมูลที่เป็นส่วนตัวหรือเป็นความลับ สำหรับความปลอดภัยในการใช้งานกับระบบหรือบริการต่าง ๆ ควรมีพฤติกรรมด้านความมั่นคงปลอดภัยโดยให้เปลี่ยนรหัสผ่านส่วนตัวให้เป็นรหัสผ่านที่มีความซับซ้อน ประกอบไปด้วยตัวเลขกับตัวอักษร โดยอาจจะมีหลักเกณฑ์ เช่น กำหนดความยาวของรหัสผ่านมากกว่า 8 ตัวอักษร โดยทั่วไปการระบุตัวตนสามารถตรวจสอบได้ผ่านทางชื่อผู้ใช้ และรหัสผ่านเป็นการกำหนดด้วยตนเอง ซึ่งส่วนใหญ่แล้วมาจากความคิดหรือสิ่งที่อยู่ใกล้ ๆ ตัวของผู้ใช้งาน เช่น เบอร์โทรศัพท์ เลขบัตรประชาชน เลขที่บ้าน วัน เดือน ปี เกิด เป็นต้น ปกติแล้วรหัสผ่าน ไม่ว่าจะเป็นการใช้ตัวอักษรหรือตัวเลขได้ถูกนำมาใช้ในการตรวจสอบการเข้าใช้ระบบ แต่ระบบดังกล่าวอาจมีปัญหาในเรื่องของความปลอดภัย การพิสูจน์ตัวตนด้วยภาพเป็นทางเลือกที่ดีอีกทางหนึ่ง เนื่องจากการตรวจสอบอีกขั้นต่อจากรหัสผ่านแบบปกติและง่ายต่อการจดจำ และมีความยากต่อการคาดเดา และมีความปลอดภัยมากขึ้น

ศรวิทย์ สนิธิ (2557) ศึกษาเรื่องความรู้ ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษา ข้าราชการ กองบัญชาการกองทัพไทย ในการศึกษางานวิจัยนี้ในการรักษาความมั่นคงปลอดภัยสารสนเทศนั้น คือ การรักษาความปลอดภัยทางข้อมูลที่เกิดจากการใช้ระบบของนโยบายหรือระเบียบที่ใช้ในการปฏิบัติการพิสูจน์ทราบ ควบคุมและป้องกันการเปิดเผยข้อมูลในงานวิจัยนี้ศึกษาเกี่ยวกับพฤติกรรมการใช้ระบบสารสนเทศของกองบัญชาการ

กองทัพไทย สำหรับความปลอดภัยคอมพิวเตอร์เป็นบทความเรื่อง ความมั่นคงปลอดภัยสารสนเทศของคณะวิทยาศาสตร์ มหาวิทยาลัยพาร์อิสเทิร์น ความมั่นคงปลอดภัยทางสารสนเทศ ความมั่นคงปลอดภัยทางกายภาพ (Physical Security) ความมั่นคงปลอดภัยส่วนบุคคล ความมั่นคงปลอดภัยในการปฏิบัติงาน ความมั่นคงปลอดภัยในการติดต่อสื่อสาร ความมั่นคงปลอดภัยของระบบเครือข่ายและความมั่นคงปลอดภัยของสารสนเทศ สำหรับอุปสรรคของงานความมั่นคงปลอดภัย คือความไม่สะดวก เนื่องจากต้องเสียเวลาในการป้อน Passwords ผู้ใช้ไม่ระมัดระวังในการใช้คอมพิวเตอร์ มีการเข้าถึงข้อมูลได้จากทุกสถานที่ เป็นต้น การศึกษาในครั้งนี้แสดงให้เห็นว่าการใช้งานคอมพิวเตอร์ของกลุ่มตัวอย่างการวิจัยในครั้งนี้มีจุดประสงค์เพื่อศึกษาพฤติกรรมในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของกองบัญชาการกองทัพไทย

ดลลักษณ์ พลเสนา (2556) ความสัมพันธ์บุคลิกภาพห้าองค์ประกอบและพฤติกรรมที่เป็นปัญหาของวัยรุ่นกับการเสพติดอินเทอร์เน็ตเกมส์ ผลการวิเคราะห์ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบ กับการเสพติดอินเทอร์เน็ตเกมส์ พบว่า 1.บุคลิกภาพห้าองค์ประกอบที่มีความสัมพันธ์ทิศทางตรงกันข้าม กับการเสพติดอินเทอร์เน็ตเกมส์ในระดับต่ำ คือ บุคลิกภาพแบบมีจิตสำนึก 2.บุคลิกภาพห้าองค์ประกอบ ที่มีความสัมพันธ์ในระดับต่ำมาก คือ บุคลิกภาพแบบสุภาพอ่อนโยน 3.บุคลิกภาพองค์ประกอบที่ไม่มีความสัมพันธ์กับการเสพติดอินเทอร์เน็ตเกมส์ ประกอบด้วย บุคลิกภาพแบบแสดงตัว บุคลิกภาพภาพมั่นคง ทางอารมณ์ และบุคลิกภาพแบบสติปัญญาในการศึกษาวิจัยการเสพติดอินเทอร์เน็ตเกมส์ของกลุ่มตัวอย่างนี้ มีความสอดคล้องกับความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับการใช้ข้อมูลสารสนเทศ

วิจัย สมอ้าย (2554) ศึกษาพฤติกรรมการใช้สารสนเทศของพนักงานบริษัท ทูมูฟ จำกัด ในเขตภาคตะวันออกเฉียงเหนือ พบว่า พฤติกรรมทั่วไปในการใช้สารสนเทศของพนักงานในตำแหน่งปฏิบัติงานของบริษัททูมูฟ ส่วนใหญ่ที่ใช้สารสนเทศมากที่สุดเพื่อใช้ในการทำงาน รองลงมาใช้ข้อมูลสารสนเทศ เพื่อความบันเทิงและอันดับสุดท้ายใช้เพื่อเป็นการติดต่อสื่อสารสรุปในภาพรวมได้ว่า พนักงานมีการ ใช้สารสนเทศอยู่ในระดับปานกลาง เมื่อพิจารณาเป็นด้าน ๆ พบว่ามีการใช้งานด้านสำนักงานมากที่สุด รองลงมาเป็นการใช้งานในด้านการติดต่อสื่อสารอยู่ในระดับปานกลางและอันดับสุดท้ายเป็นการใช้สารสนเทศในด้านของความบันเทิงซึ่งสอดคล้องกับ

วัตถุประสงค์ของผู้วิจัยที่ผู้วิจัยได้ทำการศึกษาพฤติกรรมการใช้สารสนเทศของพนักงานในสังกัด ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ธนบูรณ์ เย็นอุทก (2556) ศึกษาพฤติกรรมการใช้สารสนเทศของพนักงาน บริษัท โตโยต้า มอเตอร์ ประเทศไทย จำกัด และเพื่อเปรียบเทียบพฤติกรรมการใช้สารสนเทศระหว่างพนักงานชายและพนักงานหญิง ในบริษัทโตโยต้า มอเตอร์ ประเทศไทย จำกัด ประชากรที่ใช้สำหรับการศึกษาในครั้งนี้ คือ พนักงานชายและพนักงานหญิงที่ปฏิบัติงานในบริษัทโตโยต้า มอเตอร์ ประเทศไทย จำกัด ประกอบไปด้วยฝ่ายบริการลูกค้า ฝ่ายตัวถังและสี ฝ่ายบริการด้านเทคนิค ฝ่ายบริหารกลาง ฝ่ายส่งเสริมความพึงพอใจลูกค้า ฝ่ายปฏิบัติการบริการลูกค้า ฝ่ายพัฒนาลูกค้าสัมพันธ์ส่งเสริมกิจกรรมไคเซ็น จำนวน 225 คน แบ่งเป็น เพศชาย 145 คน เพศหญิง 80 คน เครื่องมือที่ใช้ในการวิจัยเป็นแบบสอบถามเก็บรวบรวมข้อมูลของประชากร โดยจำแนกเป็น ข้อมูลทั่วไป พฤติกรรมการใช้สารสนเทศ ผลการวิจัยพฤติกรรมการใช้เทคโนโลยีสารสนเทศของพนักงานบริษัท พบว่า พฤติกรรมในด้านการสืบค้นข้อมูลนั้นอยู่ในระดับปานกลาง ด้านการใช้งานสำนักงานเฉลี่ยแล้วอยู่ในระดับมากเป็นการใช้เทคโนโลยีเพื่อจัดทำแผนงาน จากพฤติกรรม การใช้เทคโนโลยีสารสนเทศของพนักงานชายและหญิงของบริษัทโตโยต้า มอเตอร์ ประเทศไทย จำกัด มีค่าเบี่ยงเบนมาตรฐาน ที่สูงทั้ง 3 ด้าน ได้แก่ ด้านการใช้งานสำนักงาน ด้านการติดต่อสื่อสาร ด้านการสืบค้นข้อมูล

นิชนันท์ ก่อกุลกิตติการ (2559) การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาพฤติกรรมการใช้สารสนเทศของผู้ผลิตรายการโทรทัศน์ ตัวแปรในการศึกษา เพศ อายุ ระดับการศึกษา ตำแหน่งงาน ฝ่ายงานที่ปฏิบัติ และประสบการณ์การทำงาน โดยใช้แบบสอบถามในการเก็บรวบรวมข้อมูลจากผู้ผลิตรายการโทรทัศน์ของสถานีโทรทัศน์ จำนวน 150 คน ในการวิเคราะห์ข้อมูลใช้โปรแกรมสำเร็จรูป เพื่อหาค่าความถี่ ค่าร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน ส่วนการทดสอบสมมติฐาน โดยการเปรียบเทียบความแตกต่าง ของค่าเฉลี่ยสองกลุ่มโดยใช้สถิติ การวิเคราะห์ความแปรปรวนแบบทางเดียว และการทดสอบความแตกต่างค่าเฉลี่ยเป็นรายคู่และการสัมภาษณ์ผู้ผลิตรายการโทรทัศน์ จำนวน 6 คน ผลการวิจัยสรุปได้ ดังนี้กลุ่มตัวอย่างซึ่งเป็นผู้ผลิตรายการโทรทัศน์มีพฤติกรรมใช้บริการสารสนเทศโดยรวมและรายด้านอยู่ในระดับมาก โดย

ผู้ผลิตรายการใช้สารสนเทศเพื่อเพิ่มศักยภาพของตนเองเพื่อการวางแผนและการเรียนรู้วิทยาการใหม่ๆ

2.6 คำถามการวิจัย

พฤติกรรมในการใช้ข้อมูลสารสนเทศกับบุคลิกภาพห้าองค์ประกอบมีความสัมพันธ์กันอย่างไร

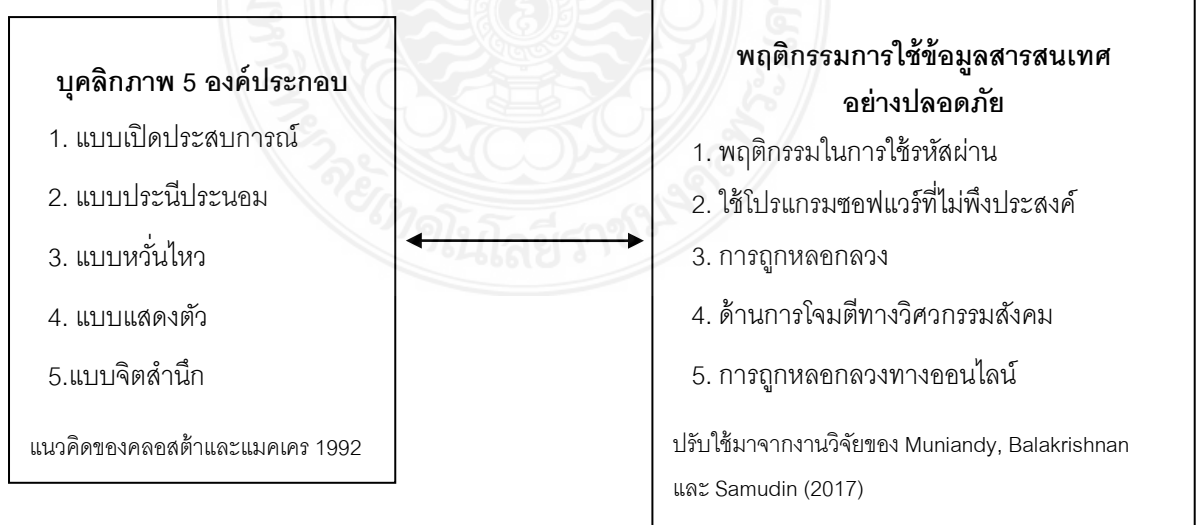
2.7 กรอบแนวความคิดในการวิจัย

การวิจัยเรื่อง ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสารขององค์การภาครัฐแห่งหนึ่ง โดยศึกษาความสัมพันธ์ระหว่างตัวแปรอิสระ คือ บุคลิกภาพห้าองค์ประกอบ และตัวแปรตาม คือ พฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย

ภาพ 2.1 กรอบแนวความคิดในการวิจัย

ตัวแปรอิสระ (Independent Variable)

ตัวแปรตาม (Dependent Variable)



บทที่ 3

วิธีดำเนินการวิจัย

ในการวิจัยครั้งนี้เป็นการวิจัยที่มุ่งศึกษา เรื่อง ความสัมพันธ์ระหว่างบุคลิกภาพ
ห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัด
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภาครัฐแห่งหนึ่ง ผู้วิจัยได้ดำเนินการ
ศึกษาค้นคว้าตามลำดับ ดังต่อไปนี้

- 3.1 ประชากรและกลุ่มตัวอย่าง
- 3.2 เครื่องมือที่ใช้ในการรวบรวมข้อมูล
- 3.3 การทดสอบคุณภาพของเครื่องมือที่ใช้ในการศึกษา
- 3.4 การเก็บรวบรวมข้อมูล
- 3.5 การวิเคราะห์ข้อมูล

3.1 ประชากรและกลุ่มตัวอย่าง

3.1.1 ประชากร

ประชากรที่ใช้ในการศึกษาค้นคว้าครั้งนี้ คือ บุคลากรในสังกัดศูนย์เทคโนโลยีสารสนเทศ
และการสื่อสาร จำนวน 65 คน (ที่มา: ข้อมูลจากฝ่ายบริหารงานทั่วไป ณ วันที่ 1 ตุลาคม พ.ศ.
2560)

3.1.2 กลุ่มตัวอย่าง

ผู้วิจัยได้กำหนดขนาดของกลุ่มตัวอย่างเป็นจำนวนเท่ากับจำนวนประชากรทั้งหมด
ที่มีอยู่ คือ บุคลากรในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จำนวน 65 คน (ที่มา:
ข้อมูลจากฝ่ายบริหารงานทั่วไป ณ วันที่ 1 ตุลาคม พ.ศ. 2560)

3.2 เครื่องมือที่ใช้ในการรวบรวมข้อมูล

เครื่องมือที่ใช้ในการวิจัยครั้งนี้ คือ แบบสอบถามบุคลิกภาพห้าองค์ประกอบพัฒนามา จากวิทยานิพนธ์ของ สุขยา ชูแสง (2557) และแบบสอบถามพฤติกรรมการใช้ข้อมูลสารสนเทศ อย่างปลอดภัยพัฒนามาจากงานวิจัยของ Muniandy, Balakrishnan และ Samudin (2017)

โดยผู้วิจัยได้ทำการดำเนินการสร้างแบบสอบถามออกเป็น 3 ตอน รวมจำนวน 68 ข้อ ดังนี้

ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม เป็นแบบสอบถามเกี่ยวกับลักษณะส่วนบุคคลของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีลักษณะคำถามแบบสำรวจรายการ (Check List) ประกอบด้วย เพศ อายุ ระดับการศึกษา สถานภาพ ตำแหน่ง รายได้ ประสบการณ์ในการทำงาน จำนวน 7 ข้อ

ตาราง 3.1 ข้อคำถามเกี่ยวกับจำนวนประชากรที่ใช้ในการวิจัย

ตัวแปร	ระดับการวัด	เกณฑ์การแบ่งกลุ่ม
1. เพศ	Nominal	1 = หญิง 2 = ชาย
2. อายุ	Ordinal	1 = 20-30 ปี 2 = 31-40 ปี 3 = 41-50 ปี 4 = 50 ปีขึ้นไป
3. ระดับการศึกษา	Ordinal	1 = ต่ำกว่าปริญญาตรี 2 = ปริญญาตรี 3 = สูงกว่าปริญญาตรี
4. สถานภาพ	Nominal	1 = โสด 2 = สมรส 3 = หย่าร้าง 4 = แยกกันอยู่ 5 = อื่น ๆ โปรดระบุ

ตาราง 3.1 แสดงคำถามเกี่ยวกับจำนวนประชากรที่ใช้ในการวิจัย(ต่อ)

ตัวแปร	ระดับการวัด	เกณฑ์การแบ่งกลุ่ม
5. ตำแหน่ง	Nominal	1 = ข้าราชการ 2 = พนักงานราชการ 3 = ลูกจ้างประจำ 4 = จ้างเหมาบริการ
6. รายได้	Ordinal	1 = น้อยกว่า/เท่ากับ 15,000 2 = 15,001 – 20,000 3 = 20,001ขึ้นไป
7. ประสบการณ์ในการทำงาน	Ordinal	1 = น้อยกว่า/เท่ากับ 5 ปี 2 = 6-10 ปี 3 = 11 ปีขึ้นไป

ตอนที่ 2 แบบสอบถามเกี่ยวกับบุคลิกภาพห้าองค์ประกอบ มีลักษณะเป็นมาตราส่วนประมาณค่า (Rating Scale) 5 ระดับ โดยมีข้อความเกี่ยวกับบุคลิกภาพห้าองค์ประกอบมี 5 ด้าน จำนวนทั้งสิ้น 20 ข้อ ดังนี้

1.บุคลิกภาพแบบเปิดประสบการณ์	จำนวนข้อความ	4	ข้อ
2.บุคลิกภาพแบบประนีประนอม	จำนวนข้อความ	4	ข้อ
3.บุคลิกภาพแบบหัวน้าว	จำนวนข้อความ	4	ข้อ
4.บุคลิกภาพแบบแสดงตัว	จำนวนข้อความ	4	ข้อ
5.บุคลิกภาพแบบจิตสำนึก	จำนวนข้อความ	4	ข้อ

ลักษณะแบบสอบถามเป็นมาตราส่วนประมาณค่า (Rating Scale) ตามมาตรวัดแบบ Likert Scale และกำหนดคะแนนความคิดเห็นแตกต่างกัน 5 ระดับ มีรายละเอียดการให้คะแนน ดังนี้

ระดับความคิดเห็น		ระดับคะแนน
มากที่สุด	หมายถึง	5
มาก	หมายถึง	4
ปานกลาง	หมายถึง	3
น้อย	หมายถึง	2
น้อยที่สุด	หมายถึง	1

สำหรับการวิเคราะห์ข้อมูลเป็นแบบมาตราส่วนประมาณค่า (Rating Scale) ในการวิจัยครั้งนี้จะใช้การวิเคราะห์ค่าเฉลี่ย (μ) และค่าส่วนเบี่ยงเบนมาตรฐาน (σ)

ค่าคะแนนเฉลี่ยตั้งแต่ 4.50 – 5.00 หมายถึง มีค่าอยู่ในระดับมากที่สุด

ค่าคะแนนเฉลี่ยตั้งแต่ 3.50 – 4.49 หมายถึง มีค่าอยู่ในระดับมาก

ค่าคะแนนเฉลี่ยตั้งแต่ 2.50 – 3.49 หมายถึง มีค่าอยู่ในระดับปานกลาง

ค่าคะแนนเฉลี่ยตั้งแต่ 1.50 – 2.49 หมายถึง มีค่าอยู่ในระดับน้อย

ค่าคะแนนเฉลี่ยตั้งแต่ 1.00 - 1.49 หมายถึง มีค่าอยู่ในระดับน้อยที่สุด

การแปลความหมายของค่าเฉลี่ยน้ำหนัก แบ่งเป็น 5 ระดับ ตามแนวคิดของ Likert Scale (เมธี ไพรัชิต, 2556) ดังนี้

เกณฑ์การพิจารณาค่าสัมประสิทธิ์ โดยทั่วไปอาจใช้เกณฑ์ ดังนี้

ระดับความสัมพันธ์กันในระดับต่ำมาก 0.01 – 0.30

ระดับความสัมพันธ์ในระดับต่ำ 0.30 – 0.50

ระดับความสัมพันธ์ในระดับปานกลาง 0.50 – 0.70

ระดับความสัมพันธ์กันในระดับสูง 0.70 - 0.90

ระดับความสัมพันธ์กันสูงมาก 0.90 – 1.00

ตอนที่ 3 แบบสอบถามเกี่ยวกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย มีลักษณะเป็นมาตราส่วนประมาณค่า (Rating Scale) 4 ระดับ โดยมีข้อคำถามเกี่ยวกับพฤติกรรม การใช้ข้อมูลสารสนเทศอย่างปลอดภัยมี 5 ด้าน จำนวนทั้งสิ้น 48 ข้อ ดังนี้

1. การใช้รหัสผ่าน	จำนวนข้อคำถาม	10 ข้อ
2. ใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์	จำนวนข้อคำถาม	8 ข้อ
3. การถูกหลอกลวง	จำนวนข้อคำถาม	10 ข้อ
4. ด้านการโจมตีทางวิศวกรรมสังคม	จำนวนข้อคำถาม	10 ข้อ
5. การถูกหลอกลวงทางออนไลน์	จำนวนข้อคำถาม	10 ข้อ

ลักษณะแบบสอบถามเป็นมาตราส่วนประมาณค่า (Rating Scale) กำหนดคะแนน ความคิดเห็นแตกต่างกัน 4 ระดับ มีรายละเอียดการให้คะแนน ดังนี้

คะแนนความคิดเห็น		ระดับพฤติกรรม
3 คะแนน	หมายถึง	ทำเป็นประจำ
2 คะแนน	หมายถึง	ทำบ่อยครั้ง
1 คะแนน	หมายถึง	ทำบ้างเป็นบางครั้ง
0 คะแนน	หมายถึง	ไม่เคยทำ

เกณฑ์การแปลความหมายของค่าเฉลี่ยน้ำหนักโดยอาศัยเกณฑ์กำหนด ดังนี้ ตามวิธี ของ Linkert. (1932, อ้างถึงใน ชเนตตี ชยนาพันธ์, 2555 : 38)

คะแนนความคิดเห็น		ระดับพฤติกรรม
3 คะแนน	หมายถึง	ทำเป็นประจำ
2 คะแนน	หมายถึง	ทำเป็นบ่อยครั้ง
1 คะแนน	หมายถึง	ทำบ้างเป็นบางครั้ง
0 คะแนน	หมายถึง	ไม่เคยทำ

$$\begin{aligned}
 \text{ความกว้างของอันตรภาคชั้น} &= \frac{\text{คะแนนสูงสุด} - \text{คะแนนต่ำสุด}}{\text{จำนวนชั้น}} \\
 &= \frac{3 - 0}{4} \\
 &= 0.75
 \end{aligned}$$

ซึ่งจะได้ค่าเฉลี่ยแต่ละระดับห่างกัน 0.75 และกำหนดความหมายของค่าเฉลี่ยแต่ละระดับ ดังนี้

ค่าคะแนนเฉลี่ยตั้งแต่ 2.26 - 3.00 หมายถึง พฤติกรรมที่แสดงออกในระดับมาก

ค่าคะแนนเฉลี่ยตั้งแต่ 1.51 - 2.25 หมายถึง พฤติกรรมที่แสดงออกในระดับปานกลาง

ค่าคะแนนเฉลี่ยตั้งแต่ 0.76 - 1.50 หมายถึง พฤติกรรมที่แสดงออกในระดับน้อย

ค่าคะแนนเฉลี่ยตั้งแต่ 0.01 - 0.75 หมายถึง พฤติกรรมที่แสดงออกในระดับน้อยที่สุด

3.3 การทดสอบคุณภาพของเครื่องมือที่ใช้ในการศึกษา

ในการศึกษาครั้งนี้ ได้มีวิธีการเก็บข้อมูลดังต่อไปนี้

1. การสร้างแบบสอบถาม

1.1 ศึกษาค้นคว้าจากตำรา เอกสาร บทความ ทฤษฎีหลักการ และงานวิจัยที่เกี่ยวข้องเพื่อนำไปกำหนดขอบเขตการวิจัยและสร้างเครื่องมือในการวิจัย คือ แบบสอบถามที่ครอบคลุมวัตถุประสงค์ที่ศึกษา

1.2 นำข้อมูลที่ได้มาสร้างแบบสอบถาม

1.3 นำแบบสอบถามที่สร้างขึ้นให้อาจารย์ที่ปรึกษาตรวจสอบความถูกต้องของเนื้อหาและภาษาที่ใช้ให้มีความถูกต้องสมบูรณ์ก่อนนำแบบสอบถามนำไปทดลองใช้

1.4 นำแบบสอบถามฉบับสมบูรณ์ที่ได้ไปสอบถามกับประชากร

2. การทดสอบคุณภาพของเครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการศึกษาครั้งนี้ ได้ทำการทดสอบความตรงเชิงเนื้อหาของแบบสอบถามก่อนนำแบบสอบถามไปหาค่าความเชื่อมั่น (Reliability) ดังนี้

2.1 การตรวจสอบค่าความตรงเชิงเนื้อหา (Content Validity)

เพื่อตรวจสอบความตรงเชิงเนื้อหา (Content Validity) และภาษาที่ใช้ให้ครอบคลุมและตรงกับนิยามที่กำหนด และทำการแก้ไขแบบสอบถามตามข้อเสนอแนะ โดยการปรึกษากับอาจารย์ที่ปรึกษาเพื่อพิจารณาความสอดคล้องระหว่างนิยามศัพท์และวัตถุประสงค์การเรียนรู้กับข้อคำถาม

2.2 การทดสอบความเชื่อมั่น (Reliability)

การทดสอบความเชื่อมั่น (Reliability) ผู้วิจัยได้นำแบบสอบถามที่สร้างขึ้นมา และปรับปรุงแก้ไขแล้วไปทดลองก่อน (try – out) จำนวน 20 ชุด กับประชากรที่ไม่ใช่กลุ่มตัวอย่าง เพื่อหาค่าความเชื่อมั่น (Reliability) โดยใช้วิธีการหาค่าสัมประสิทธิ์แอลฟา (α - Coefficient) ตามวิธีของ Cronbach's alpha coefficient ถ้าค่าสัมประสิทธิ์ใกล้ 1.00 มากดี น้อยกว่า .60 ไม่ดี และถ้าได้ค่า .70 ขึ้นไปถือว่าดียอมรับได้ (บุญชม ศรีสะอาด, 2556 : 116-119) ซึ่งผลจากการคำนวณค่าสัมประสิทธิ์แอลฟาได้เท่ากับ 0.757 แสดงว่าแบบสอบถามมีความน่าเชื่อถือนำไปเก็บรวบรวมข้อมูลต่อไปได้ ดังตารางต่อไปนี้

ตาราง 3.2 ตารางแสดงค่าสัมประสิทธิ์แอลฟาของบุคลิกภาพ 5 องค์ประกอบ

บุคลิกภาพ 5 องค์ประกอบ	Alpha
1. บุคลิกภาพแบบเปิดประสบการณ์	0.772
2. บุคลิกภาพแบบประนีประนอม	0.678
3. บุคลิกภาพแบบหัวนไหว	0.851
4. บุคลิกภาพแบบแสดงตัว	0.605
5. บุคลิกภาพแบบมีจิตสำนึก	0.819

จากตาราง 3.2 เมื่อพิจารณาค่าสัมประสิทธิ์แอลฟาในภาพรวม พบว่า ค่าสัมประสิทธิ์ของบุคลิกภาพ 5 องค์ประกอบอยู่ในเกณฑ์ที่ยอมรับได้ สามารถแบ่งออกเป็นรายชื่อได้ ดังนี้ บุคลิกภาพแบบเปิดประสบการณ์เท่ากับ 0.772, บุคลิกภาพแบบประนีประนอมเท่ากับ 0.678,

บุคลิกภาพแบบหวั่นไหวเท่ากับ 0.851, บุคลิกภาพแบบแสดงตัวเท่ากับ 0.605, และบุคลิกภาพแบบมีจิตสำนึกเท่ากับ 0.819

ตาราง 3.3 ตารางแสดงค่าสัมประสิทธิ์แอลฟาของพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย

พฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย	Alpha
1. การใช้รหัสผ่าน	0.611
2. การใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์	0.596
3. การถูกหลอกลวง	0.792
4. การถูกโจมตีทางวิศวกรรมสังคม	0.755
5. การถูกหลอกลวงทางออนไลน์	0.754

จากตาราง 3.3 เมื่อพิจารณาค่าสัมประสิทธิ์แอลฟาในภาพรวม พบว่า ค่าสัมประสิทธิ์ของพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยอยู่ในเกณฑ์ที่ยอมรับได้ สามารถแบ่งออกเป็นรายชื่อได้ ดังนี้ การใช้รหัสผ่านเท่ากับ 0.611, การใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์เท่ากับ 0.596, การถูกหลอกลวงเท่ากับ 0.795, การโจมตีด้านวิศวกรรมสังคมเท่ากับ 0.755, และ การถูกหลอกลวงทางออนไลน์เท่ากับ 0.754

3.4 การเก็บรวบรวมข้อมูล

การศึกษาวิจัยครั้งนี้เป็นการวิจัยแบบบรรยาย (Descriptive Research) เพื่อศึกษาถึงความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผู้วิจัยได้ดำเนินการเก็บรวบรวมข้อมูล ดังนี้

3.4.1. ข้อมูลปฐมภูมิ (Primary Data) เป็นการเก็บรวบรวมข้อมูลโดยใช้แบบสอบถามที่ผ่านการตรวจสอบคุณภาพมาใช้ในการเก็บข้อมูลจำนวน 65 ชุด ซึ่งจะดำเนินการเก็บรวบรวมข้อมูลจนครบตามจำนวนโดยขอความร่วมมือจากพนักงานในสังกัด ซึ่งได้กำหนดไว้ในขั้นตอนการตอบแบบสอบถามโดยให้ผู้ตอบเป็นผู้ตอบแบบสอบถามเองและผู้วิจัยนำแบบสอบถามที่ผ่านการตรวจสอบความถูกต้องและครบถ้วนตามจำนวนที่ทำการนำส่งแบบสอบถามไปแล้วนั้นได้รับแบบสอบถามคืนครบทั้งหมด 65 ชุดจึงนำไปวิเคราะห์ข้อมูลทางสถิติด้วยโปรแกรมสำเร็จรูปทางคอมพิวเตอร์

3.4.2. ข้อมูลทุติยภูมิ (Secondary Data) เป็นข้อมูลที่เก็บรวบรวมและค้นคว้ามาจากหนังสือ เอกสาร ตำราวิชาการ งานวิจัยที่เกี่ยวข้อง

3.5 การวิเคราะห์ข้อมูล

การวิจัยครั้งนี้ผู้ศึกษาได้ใช้ค่าพารามิเตอร์มาใช้ในการวิเคราะห์ข้อมูล โดยการใช้การแจกแจงความถี่ (Frequency) ค่าร้อยละ (Percentage) ในการวิเคราะห์ข้อมูลลักษณะส่วนบุคคล ประกอบด้วยค่าเฉลี่ย (μ) ส่วนเบี่ยงเบนมาตรฐาน (σ) ในการวิเคราะห์ข้อมูลระดับของบุคลิกภาพห้าองค์ประกอบและใช้ค่า Rho (ρ) เพื่อทดสอบสัมประสิทธิ์สหสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย

บทที่ 4

ผลการวิจัย

การศึกษาเรื่อง ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย ผู้วิจัยทำการวิจัยกลุ่มประชากรทั้งหมด 65 คน โดยการแจกแบบสอบถามไปกลุ่มประชากร จำนวน 65 ชุด ได้รับแบบสอบถามคืนมา จำนวน 65 ชุด จากนั้นผู้วิจัยได้นำข้อมูลที่ได้จากการทำแบบสอบถามมาวิเคราะห์เพื่อศึกษาความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศ โดยจำแนกตามลักษณะส่วนบุคคล โดยนำเสนอผลการวิจัยดังนี้

4.1 ผลการวิเคราะห์ข้อมูลลักษณะส่วนบุคคลของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ภาครัฐแห่งหนึ่ง ได้แก่ เพศ อายุ ระดับการศึกษา สถานภาพ ตำแหน่ง รายได้ ประสบการณ์ในการทำงาน โดยการแจกแจงความถี่ (Frequency) ค่าร้อยละ (Percentage) ค่าเฉลี่ย (μ) และส่วนเบี่ยงเบนมาตรฐาน (σ)

4.2 ผลการวิเคราะห์ข้อมูลระดับบุคลิกภาพห้าองค์ประกอบของบุคลากรในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

4.3 ผลการวิเคราะห์ข้อมูลระดับพฤติกรรมการใช้ข้อมูลสารสนเทศของบุคลากรในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

4.4 ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย

สัญลักษณ์ที่ใช้ในการวิเคราะห์และแปรผลข้อมูล มีดังนี้

μ	แทน	ค่าเฉลี่ยของประชากร
σ	แทน	ค่าเบี่ยงเบนมาตรฐานของประชากร
ρ	แทน	ค่าสัมประสิทธิ์สหสัมพันธ์ (Rho)
N	แทน	จำนวนประชากร

4.1 ผลการวิเคราะห์ข้อมูลลักษณะส่วนบุคคล

ผลการวิเคราะห์ข้อมูลลักษณะส่วนบุคคลของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้แก่ เพศ อายุ ระดับการศึกษา สถานภาพ ตำแหน่ง รายได้ ประสบการณ์ในการทำงาน โดยการแจกแจงความถี่ (Frequency) และคำนวณหาค่าร้อยละ (Percentage) นำเสนอในรูปของตาราง 4.1

ตาราง 4.1 จำนวน (ความถี่) และร้อยละ จำแนกตามลักษณะส่วนบุคคล (N = 65)

ปัจจัยส่วนบุคคล	จำนวน (คน)	ร้อยละ
เพศ		
หญิง	33	50.8
ชาย	32	49.2
อายุ		
20-30 ปี	25	38.5
31-40 ปี	18	27.6
41-50 ปี	17	26.2
50 ปีขึ้นไป	5	7.7
สถานภาพ		
โสด	41	63.1
สมรส	20	30.7
หย่าร้าง	4	6.2
แยกกันอยู่	0	0
ระดับการศึกษา		
ต่ำกว่าปริญญาตรี	8	12.3
ปริญญาตรี	47	72.3
สูงกว่าปริญญาตรี	10	15.4

ตาราง 4.1 (ต่อ)

ปัจจัยส่วนบุคคล	จำนวน (คน)	ร้อยละ
ตำแหน่ง		
ข้าราชการ	23	35.4
พนักงานราชการ	33	50.7
ลูกจ้างประจำ	7	10.8
จ้างเหมาบริการ	2	3.1
รายได้		
น้อยกว่า/เท่ากับ 15,000	8	12.3
15,001 – 20,000	19	29.2
20,001ขึ้นไป	38	58.5
ประสบการณ์ในการทำงาน		
น้อยกว่า/เท่ากับ 5 ปี	33	50.8
6 – 10 ปี	9	13.8
11 ปีขึ้นไป	23	35.4

จากตาราง 4.1 พบว่าผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง จำนวน 33 คน คิดเป็นร้อยละ 50.8 เป็นเพศชาย จำนวน 32 คน คิดเป็นร้อยละ 49.2 ตามลำดับ

ผู้ตอบแบบสอบถามส่วนใหญ่มีช่วงอายุ 20-30 ปี จำนวน 25 คน คิดเป็นร้อยละ 38.5 รองลงมาคือช่วงอายุ 31-40 ปี จำนวน 18 คน คิดเป็นร้อยละ 27.6 ช่วงอายุ 41-50 ปี จำนวน 17 คน คิดเป็นร้อยละ 26.2 และช่วงอายุที่น้อยที่สุด คือ ช่วงอายุ 50 ปีขึ้นไป จำนวน 5 คน คิดเป็นร้อยละ 7.7 ตามลำดับ

ผู้ตอบแบบสอบถามส่วนใหญ่มีระดับการศึกษาปริญญาตรี จำนวน 47 คน คิดเป็นร้อยละ 72.3 รองลงมาคือ ระดับการศึกษาสูงกว่าปริญญาตรี จำนวน 10 คน คิดเป็นร้อยละ 15.4 และระดับการศึกษาต่ำกว่าปริญญาตรี จำนวน 8 คน คิดเป็นร้อยละ 12.3 ตามลำดับ

ผู้ตอบแบบสอบถามส่วนใหญ่มีสถานะโสด จำนวน 41 คน คิดเป็นร้อยละ 63.1 รองลงมา คือ สมรสแล้ว จำนวน 20 คน คิดเป็นร้อยละ 30.7 และอันดับสุดท้ายหย่าร้าง จำนวน 4 คน คิดเป็นร้อยละ 6.2 ตามลำดับ

ผู้ตอบแบบสอบถามส่วนใหญ่มีตำแหน่งเป็นพนักงานราชการ จำนวน 33 คน คิดเป็นร้อยละ 50.8 รองลงมาคือ ข้าราชการ จำนวน 23 คน คิดเป็นร้อยละ 35.4 รองลงมา คือ ลูกจ้างประจำ จำนวน 7 คน คิดเป็นร้อยละ 10.8 และลำดับสุดท้ายคือ จ้างเหมาบริการ จำนวน 2 คน คิดเป็นร้อยละ 3.1 ตามลำดับ

ผู้ตอบแบบสอบถามส่วนใหญ่มีรายได้มากที่สุดคือ ตั้งแต่ 20,001 บาทขึ้นไป จำนวน 38 คน คิดเป็นร้อยละ 58.5 รองลงมารายได้ 15,001 – 20,000 บาท จำนวน 19 คน คิดเป็นร้อยละ 29.2 และรายได้ที่น้อยที่สุดคือ น้อยกว่า/เท่ากับ 15,000 บาท จำนวน 8 คน คิดเป็นร้อยละ 12.3 ตามลำดับ

ผู้ตอบแบบสอบถามส่วนใหญ่มีประสบการณ์ในการทำงานน้อยกว่า 5 ปี/เท่ากับ 5 ปี จำนวน 33 คน คิดเป็นร้อยละ 50.7 รองลงมาคือ ประสบการณ์ในการทำงาน 11 ปีขึ้นไป จำนวน 23 คน คิดเป็นร้อยละ 35.4 และประสบการณ์ในการทำงาน 6 – 10 ปี จำนวน 9 คน คิดเป็นร้อยละ 13.8 ตามลำดับ

4.2 ผลการวิเคราะห์ข้อมูลบุคลิกภาพห้าองค์ประกอบ

ผลการวิเคราะห์ข้อมูลระดับของบุคลิกภาพห้าองค์ประกอบนำมาวิเคราะห์โดยใช้สถิติหาค่าเฉลี่ย (μ) ส่วนเบี่ยงเบนมาตรฐาน (σ) นำเสนอในรูปแบบของตาราง 4.2 – 4.7

ตาราง 4.2 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานของบุคลิกภาพห้าองค์ประกอบในภาพรวม (N = 65)

บุคลิกภาพห้าองค์ประกอบ	μ	σ	ระดับ	ลำดับ
บุคลิกภาพแบบเปิดประสบการณ์	3.82	0.602	มาก	3
บุคลิกภาพแบบประนีประนอม	4.00	0.497	มาก	2
บุคลิกภาพแบบหวั่นไหว	2.95	0.796	ปานกลาง	5
บุคลิกภาพแบบแสดงตัว	3.78	0.495	มาก	4
บุคลิกภาพแบบมีจิตสำนึก	4.26	0.518	มากที่สุด	1
รวม	3.78	0.330	มาก	

จากตาราง 4.2 พบว่า ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานระดับบุคลิกภาพห้าองค์ประกอบในภาพรวมอยู่ระดับมาก ($\mu = 3.78$, $\sigma = 0.330$) เมื่อพิจารณาเป็นรายด้าน พบว่าค่าเฉลี่ยสูงสุดคือ บุคลิกภาพแบบมีจิตสำนึก ($\mu = 4.26$, $\sigma = 0.518$) รองลงมาคือ บุคลิกภาพแบบประนีประนอม ($\mu = 4.00$, $\sigma = 0.497$) บุคลิกภาพแบบเปิดประสบการณ์ ($\mu = 3.82$, $\sigma = 0.602$) บุคลิกภาพแบบแสดงตัว ($\mu = 3.78$, $\sigma = 0.495$) และบุคลิกภาพแบบหวั่นไหว ($\mu = 2.95$, $\sigma = 0.796$) ตามลำดับ

4.3 ผลการวิเคราะห์พฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย

ผลการวิเคราะห์ข้อมูลระดับของพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยนำมาวิเคราะห์โดยใช้สถิติหาค่าเฉลี่ย (μ) ส่วนเบี่ยงเบนมาตรฐาน (σ) นำเสนอในรูปแบบของตาราง 4.3 – 4.7

ตาราง 4.3 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานพฤติกรรมการใช้รหัสผ่าน (N = 65)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	μ	σ	ระดับ	ลำดับ
การใช้รหัสผ่าน(Passwords Usage)				
1. จดรหัสผ่านลงในกระดาษหรือสมุดโน้ตเพื่อถ่ายต่อ การจดจำ	1.47	0.920	น้อย	8
2. ท่านได้บอกรหัสผ่านกับผู้อื่น	2.07	0.756	ปานกลาง	1
3. ท่านใช้รหัสผ่านเดียวกันในการเข้าใช้งานระบบ	1.76	0.996	ปานกลาง	5
4. ตั้งรหัสผ่านของท่านมีตัวอักษรและตัวเลขมากกว่า 8 ตัวผสมกัน	1.92	0.940	ปานกลาง	2
5. ท่านไม่เคยเปลี่ยนรหัสผ่านของท่านเลย	1.83	1.069	ปานกลาง	4
6. รหัสผ่านของท่านประกอบไปด้วยตัวอักษรพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ	1.58	1.059	ปานกลาง	7
7. ตั้งรหัสผ่านจากข้อมูลส่วนบุคคล เช่น วัน เดือน ปี เกิด หมายเลขโทรศัพท์ เป็นต้น	1.67	0.953	ปานกลาง	6
8. ใช้งานตัวเลือก "การจดจำรหัสผ่าน"	1.89	1.017	ปานกลาง	3
9. ท่านใช้รหัสผ่านที่แตกต่างกันในการใช้งานระบบต่าง ๆ	1.36	0.858	น้อย	9
10. รหัสผ่านของท่านไม่ได้เป็นไปตามรูปแบบของแป้นพิมพ์	0.75	0.901	น้อยที่สุด	10
รวม	1.291	0.754	น้อย	

จากตาราง 4.3 เมื่อพิจารณาผลการวิเคราะห์พฤติกรรมการใช้รหัสผ่าน ในภาพรวม พฤติกรรมที่แสดงออกอยู่ในระดับน้อย ($\mu = 1.291$, $\sigma = 0.754$) เมื่อพิจารณาเป็นรายข้อ พบว่า ค่าเฉลี่ยสูงสุดคือ ท่านได้บอกรหัสผ่านกับผู้อื่น ($\mu = 1.92$, $\sigma = 0.940$) รองลงมาคือ การตั้งรหัสผ่านของท่านมีตัวอักษรและตัวเลขมากกว่า 8 ตัวผสมกัน ($\mu = 1.92$, $\sigma = 1.940$) ใช้งานตัวเดียว การจดจำรหัสผ่าน ($\mu = 1.89$, $\sigma = 1.017$) ท่านไม่เคยเปลี่ยนรหัสผ่านของท่านเลย ($\mu = 1.83$, $\sigma = 1.069$) ท่านใช้รหัสผ่านเดียวกันในการเข้าใช้งานระบบ ($\mu = 1.76$, $\sigma = 0.996$) ตั้งรหัสผ่านจากข้อมูลส่วนบุคคล เช่น วัน เดือน ปี เกิด หมายเลขโทรศัพท์ ($\mu = 1.67$, $\sigma = 0.953$) รหัสผ่านของท่านประกอบไปด้วยตัวอักษรพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ ($\mu = 1.58$, $\sigma = 1.059$) จดรหัสผ่านลงในกระดาษหรือสมุดโน้ตเพื่อง่ายต่อการจดจำ ($\mu = 1.47$, $\sigma = 0.920$) ใช้รหัสผ่านที่แตกต่างกันในการใช้งานระบบต่างๆ ($\mu = 1.36$, $\sigma = 0.858$) และรหัสผ่านของท่านไม่ได้เป็นไปตามรูปแบบของแป้นพิมพ์ ($\mu = 0.75$, $\sigma = 0.901$) ตามลำดับ

ตาราง 4.4 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานพฤติกรรมการใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์ (N = 65)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	μ	σ	ระดับ	ลำดับ
ใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์(Malware)				
1. ท่านมีความเต็มใจที่จะเปิดเอกสารแนบ E-mail จากบุคคลแปลกหน้า	0.83	0.782	น้อยที่สุด	7
2. มีหัวข้อของเอกสารที่น่าสนใจจึงเป็นสาเหตุที่ท่านต้องเปิดอ่าน E-mail	1.29	0.842	น้อย	4
3. ท่านมีการตรวจสอบสถานะของโปรแกรมป้องกันไวรัสในคอมพิวเตอร์อย่างสม่ำเสมอ	1.73	0.888	ปานกลาง	2

ตาราง 4.4 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานพฤติกรรมการใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์ (ต่อ)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	μ	σ	ระดับ	ลำดับ
4. ท่านเปิดเอกสารที่เป็นไฟล์แนบ มาโดยแนบเป็นไฟล์ประเภทที่ ใช้หลายนามสกุล	1.06	0.826	น้อย	5
5. ท่านดาวน์โหลดโปรแกรมฟรี จากอินเทอร์เน็ตลงใน คอมพิวเตอร์ของตน	1.41	0.845	น้อย	3
6. มีการติดตั้งโปรแกรม Antivirus, Firewall และ โปรแกรมป้องกันการสอดส่อง การใช้งานคอมพิวเตอร์ของคุณ	1.83	0.977	ปานกลาง	1
7. ท่านมีความเต็มใจที่จะดาวน์โหลด ข้อมูลจากเว็บไซต์ที่ไม่ ปลอดภัย	0.75	0.86	น้อยที่สุด	8
8. มีการนำโปรแกรมที่ใช้ป้องกัน จุดบกพร่องของโปรแกรม คอมพิวเตอร์เพื่อป้องกันการ โดนขโมยข้อมูล	1.00	0.883	น้อย	6
รวม	1.240	0.754	น้อย	

จากตาราง 4.4 เมื่อพิจารณาผลการวิเคราะห์พฤติกรรมการใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์โดยภาพรวมพฤติกรรมที่แสดงออกอยู่ในระดับน้อย ($\mu = 1.240$, $\sigma = 0.526$) เมื่อพิจารณาเป็นรายข้อ พบว่าค่าเฉลี่ยสูงสุดคือ มีการติดตั้งโปรแกรม Antivirus, Firewall, และโปรแกรมป้องกันการสอดส่องการใช้งานคอมพิวเตอร์ของคุณ ($\mu = 1.83$, $\sigma = 0.977$)

รองลงมาคือ ท่านมีการตรวจสอบสถานะของโปรแกรมป้องกันไวรัสในคอมพิวเตอร์อย่างสม่ำเสมอ ($\mu = 1.73$, $\sigma = 1.110$) ท่านดาวน์โหลดโปรแกรมฟรีจากอินเทอร์เน็ตลงในคอมพิวเตอร์ของตน ($\mu = 1.41$, $\sigma = 1.013$) มีหัวข้อของเอกสารที่น่าสนใจจึงเป็นสาเหตุที่ท่านต้องเปิดอ่านE-mail ($\mu = 1.29$, $\sigma = 0.671$) ท่านเปิดเอกสารที่เป็นไฟล์แนบมาโดยแนบเป็นไฟล์ประเภทที่ใช้หลายนามสกุล ($\mu = 1.06$, $\sigma = 0.747$) มีการนำโปรแกรมที่ใช้ป้องกันจุดบกพร่องของโปรแกรมคอมพิวเตอร์เพื่อป้องกันการโดนขโมยข้อมูล ($\mu = 1.00$, $\sigma = 0.883$) ท่านเปิดเอกสารที่เป็นไฟล์แนบมาโดยแนบเป็นไฟล์ท่านมีความเต็มใจที่จะเปิดเอกสารแนบ E-mail จากบุคคลแปลกหน้า ($\mu = 0.83$, $\sigma = 0.858$) และท่านมีความเต็มใจที่จะดาวน์โหลดข้อมูลจากเว็บไซต์ที่ไม่ปลอดภัย ($\mu = 0.75$, $\sigma = 0.886$) ตามลำดับ

ตาราง 4.5 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานพฤติกรรมกรถูกหลอกลวง(Phishing issue)
(N = 65)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	μ	σ	ระดับ	ลำดับ
การถูกหลอกลวง(Phishing issue)				
1.ท่านมีการอัปเดตความรู้เกี่ยวกับการถูกหลอกลวงทางคอมพิวเตอร์โดยการอ่านข้อมูลที่เกี่ยวข้อง	1.47	0.792	น้อย	3
2.ท่านมั่นใจว่าคุณไม่ใช่เหยื่อของการหลอกลวงเนื่องจากคุณเป็นบุคคลทั่วไป	1.50	0.953	น้อย	1
3.ท่านมีความสมัครใจในการจัดการข้อมูลที่น่าเชื่อถือของทุกประเภท	1.47	0.772	น้อย	4
4.ท่านมีความสมัครใจในการกด Hyperlink จากอีเมล	1.04	0.799	น้อย	9

ตาราง 4.5 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานพฤติกรรมกรถูกหลอกลวง(Phishing issue) (ต่อ)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	μ	σ	ระดับ	ลำดับ
5.มีความเชื่อในข้อความที่ส่งจาก อีเมลที่ส่งมาเกี่ยวกับการชิงเงิน รางวัลต่าง ๆ	0.61	0.842	น้อยที่สุด	10
6.ถ้าจะมีการส่ง ข้อมูลที่เป็น ความลับ ชนิดของ URL ต้องเป็น “https” เท่านั้น	1.29	0.896	น้อย	7
7.สัญลักษณ์กุญแจมีความจำเป็น ในการส่งผ่านข้อมูลสำคัญ	1.32	0.903	น้อย	6
8.ท่านชอบที่จะพิมพ์ URL ในเบราว์เซอร์แทนการคลิก Hyperlink เพื่อเชื่อมโยงหลายมิติ	1.49	0.889	น้อย	2
9.เมื่อท่านได้รับอีเมลที่น่าสงสัยคุณ จะติดต่อกับบุคคลที่เกี่ยวข้องใน การตรวจสอบ	1.07	0.889	น้อย	8
10.มีการตรวจสอบชนิดของ URL ก่อนที่จะทำธุรกรรมต่าง ๆ บน อินเทอร์เน็ต	1.46	0.936	น้อย	5
รวม	1.276	0.512	น้อย	

จากตาราง 4.5 เมื่อพิจารณาผลการวิเคราะห์พฤติกรรมกรถูกหลอกลวง โดยภาพรวมพฤติกรรมที่แสดงออกอยู่ระดับน้อย ($\mu = 1.276$, $\sigma = 0.512$) เมื่อพิจารณาเป็นรายข้อ พบว่าค่าเฉลี่ยสูงสุดคือ ท่านมั่นใจว่าท่านไม่ใช่เหยื่อของการถูกหลอกลวงเนื่องจากคุณเป็นบุคคลทั่วไป ($\mu = 1.50$, $\sigma = 0.953$) รองลงมาคือ ท่านชอบที่จะพิมพ์ URL ในเบราว์เซอร์แทนการคลิก Hyperlink เพื่อเชื่อมโยงหลายมิติ ($\mu = 1.49$, $\sigma = 0.889$) ท่านมีการอัปเดตความรู้เกี่ยวกับการ

ถูกหลอกลวงทางคอมพิวเตอร์โดยการอ่านข้อมูลที่เกี่ยวข้อง ($\mu = 1.47, \sigma = 0.792$) ท่านมีความ
 สนใจในการจัดการข้อมูลที่น่าเชื่อถือของทุกประเภท ($\mu = 1.47, \sigma = 0.772$) มีการตรวจสอบ
 ชนิดของ URL ก่อนที่จะทำธุรกรรมต่าง ๆ บนอินเทอร์เน็ต ($\mu = 1.46, \sigma = 0.936$) สัญลักษณ์
 กุญแจมีความจำเป็นในการส่งผ่านข้อมูลสำคัญ ($\mu = 1.32, \sigma = 0.903$) ถ้าจะมีการส่งข้อมูลที่เป็น
 ความลับ ชนิดของ URL ต้องเป็น “https” เท่านั้น ($\mu = 1.29, \sigma = 0.896$) เมื่อท่านได้รับอีเมล
 ที่น่าสงสัยคุณจะติดต่อกับบุคคลที่เกี่ยวข้องในการตรวจสอบ ($\mu = 1.07, \sigma = 0.889$) ท่านมี
 ความสนใจในการกด Hyperlink จากอีเมล ($\mu = 1.04, \sigma = 0.799$) และมีความเชื่อใน
 ข้อความที่ส่งจากอีเมลที่ส่งมาเกี่ยวกับการชิงเงินรางวัลต่าง ๆ ($\mu = 0.61, \sigma = 0.842$)

ตาราง 4.6 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานด้านการโจมตีทางวิศวกรรมสังคม (N = 65)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	μ	σ	ระดับ	ลำดับ
ด้านการโจมตีทางวิศวกรรมสังคม(Social Engineering)				
1.ท่านไม่สนใจในการอ่านข้อมูลที่เกี่ยวข้องกับการโจมตีแบบวิศวกรรมสังคม	1.06	0.845	น้อย	8
2.ท่านเปิดเผย Username และ Passwords ถึงบุคคลที่ถูกเรียกว่าเป็นผู้ดูแลระบบ	0.72	0.800	น้อยที่สุด	10
3. ท่านเชื่อว่าตนเองไม่ใช่เป้าหมายของการโจมตีแบบวิศวกรรมสังคมเนื่องจากเป็นบุคคลทั่วไป	1.38	1.010	น้อย	6
4. ท่านไม่ยินดีที่จะตอบรับโทรศัพท์, ข้อความ, หรืออีเมลจากคนแปลกหน้าที่เป็นมิตร/ไม่เป็นมิตร	1.49	1.001	น้อย	4
5. ท่านเต็มใจที่จะปฏิบัติตามข้อกำหนด/ข้อบังคับที่ถูกกำหนดโดยบุคคลที่มีอำนาจรับผิดชอบ	1.81	0.827	ปานกลาง	1

ตาราง 4.6 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานด้านการโจมตีทางวิศวกรรมสังคม (ต่อ)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	μ	σ	ระดับ	ลำดับ
6. ท่านเต็มใจที่จะให้ Passwords แก่โปรแกรมช่วยเหลือการทำงานที่ให้ความช่วยเหลือแก่ผู้ใช้ระบบ	1.00	0.728	น้อย	9
7. ตรวจสอบอำนาจความรับผิดชอบหรือลักษณะของบุคคลก่อนที่จะมีการพูดคุย	1.40	0.825	น้อย	5
8. ท่านรู้สึกว่าคุณเองหวาดหวั่นกับคำถามของคนแปลกหน้า	1.23	0.805	น้อย	7
9. ท่านไม่สื่อสารกับคนแปลกหน้าถึงแม้ว่าจะดูน่าไว้วางใจ	1.61	0.995	ปานกลาง	3
10. ท่านไม่เปิดเผยข้อมูลที่เป็นความลับในทุก ๆ สถานการณ์	1.78	1.082	ปานกลาง	2
รวม	1.350	0.502	น้อย	

จากตาราง 4.6 เมื่อพิจารณาผลการวิเคราะห์พฤติกรรมในด้านการโจมตีวิศวกรรมสังคม โดยภาพรวมการแสดงพฤติกรรมอยู่ในระดับน้อย ($\mu = 3.01$, $\sigma = 0.520$) เมื่อพิจารณาเป็นรายข้อ พบว่าค่าเฉลี่ยสูงสุดคือ ท่านเต็มใจที่จะปฏิบัติตามข้อกำหนด/ข้อบังคับที่ถูกกำหนดโดยบุคคลที่มีอำนาจรับผิดชอบ ($\mu = 1.81$, $\sigma = 0.827$) รองลงมาคือ ท่านไม่เปิดเผยข้อมูลที่เป็นความลับในทุก ๆ สถานการณ์ ($\mu = 1.78$, $\sigma = 1.082$) ท่านไม่สื่อสารกับคนแปลกหน้าถึงแม้ว่าจะดูน่าไว้วางใจ ($\mu = 1.61$, $\sigma = 0.995$) ท่านไม่ยินดีที่จะตอบรับโทรศัพท์ ข้อความ หรืออีเมลจากคนแปลกหน้าที่เป็นมิตร/ไม่เป็นมิตร ($\mu = 1.49$, $\sigma = 1.001$) ตรวจสอบอำนาจความรับผิดชอบ หรือลักษณะของบุคคลก่อนที่จะมีการพูดคุย ($\mu = 1.40$, $\sigma = 0.825$) ท่านเชื่อว่าตนเองไม่ใช่เป้าหมายของการโจมตีแบบวิศวกรรมทางสังคมเนื่องจากเป็นบุคคลทั่วไป ($\mu = 1.38$, $\sigma = 0.899$) ท่านรู้สึกว่าคุณเองหวาดหวั่นกับคำถามของคนแปลกหน้า ($\mu = 1.23$, $\sigma = 0.805$) ท่านเชื่อว่า

ตนเองไม่ใช่ ท่านไม่สนใจในการอ่านข้อมูลที่เกี่ยวข้องกับการโจมตีแบบวิศวกรรมสังคม ($\mu = 1.06$, $\sigma = 0.845$) ท่านเต็มใจที่จะให้ Passwords แก่โปรแกรมช่วยเหลือเหลือการทำงานที่ให้ความช่วยเหลือแก่ผู้ใช้ระบบ ($\mu = 1.00$, $\sigma = 0.728$) ท่านเต็มใจที่จะให้ Passwords กับโปรแกรมช่วยเหลือการทำงานที่ให้ความช่วยเหลือแก่ผู้ใช้ระบบ ($\mu = 1.00$, $\sigma = 0.728$) ท่านเปิดเผย Username และ Passwords และเข้าถึงบุคคลที่ถูกเรียกว่าเป็นผู้ดูแลระบบ (1.00, $\sigma = 0.800$) ตามลำดับ

ตาราง 4.7 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานการพฤติกรรมการถูกหลอกลวงทางออนไลน์ (N = 65)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	μ	σ	ระดับ	ลำดับ
การถูกหลอกลวงทางออนไลน์ (Online scam)				
1.ท่านสร้างความสัมพันธ์แบบไว้เนื้อ เชื้อใจบนโลกออนไลน์กับคนแปลก หน้า	0.76	0.805	น้อยที่สุด	6
2.ท่านเพิกเฉยต่ออีเมลหลอกลวงที่มี ชื่อเสียงที่ผิดปกติหรือเกินจริง	1.60	1.129	น้อย	3
3.ท่านตอบคำถามทางโทรศัพท์ที่ เกี่ยวข้องกับเงินรางวัลจำนวน มหาศาล	0.38	0.743	น้อยที่สุด	10
4.ท่านไว้ใจข้อมูลของคนแปลกหน้าที่ ได้รับบนอินเทอร์เน็ต	1.70	1.155	ปานกลาง	1
5.ท่านไม่เคยให้ความสนใจกับจำนวน เงินที่เสนอโดยเว็บไซต์ออนไลน์	1.69	1.184	ปานกลาง	2

ตาราง 4.7 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานการพฤติกรรมกรรณการถูกลอกลงทางออนไลน์ (ต่อ)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	μ	σ	ระดับ	ลำดับ
6.ท่านมีความเต็มใจที่จะโอนเงิน ให้แก่เพื่อนที่รู้จักกันทางโลก ออนไลน์	0.43	0.847	น้อยที่สุด	9
7.ท่านมีความตระหนักถึง และ สามารถระบุงการถูกลอกลงบน โลกออนไลน์ที่เกิดขึ้นล่าสุดได้	1.53	1.016	ปานกลาง	4
8.ท่านไว้วางใจ/เชื่อใจในรูปภาพของ คนแปลกหน้าทีโพสลงบน อินเทอร์เน็ต	0.58	0.766	น้อยที่สุด	8
9.ท่านยอมรับพัสดุหรือของขวัญจาก เพื่อนในอินเทอร์เน็ต	1.20	1.063	น้อย	5
10.ท่านไม่ลังเลที่จะพบหน้าแบบเห็น หน้าคร่ำตากับเพื่อนที่รู้จักกันทาง อินเทอร์เน็ต	0.66	0.834	น้อยที่สุด	7
รวม	1.056	0.540	น้อย	

จากตาราง 4.7 เมื่อพิจารณาผลการวิเคราะห์พฤติกรรมในการถูกลอกลงทางออนไลน์ โดยรวมการแสดงพฤติกรรมอยู่ระดับน้อย ($\mu = 1.056$, $\sigma = 0.540$) เมื่อพิจารณาเป็นรายข้อ พบว่าค่าเฉลี่ยสูงสุด คือ ท่านไว้ใจข้อมูลของคนแปลกหน้าที่ได้รับบนอินเทอร์เน็ต ($\mu = 1.70$, $\sigma = 1.155$) รองลงมาคือ ท่านไม่เคยให้ความสนใจกับจำนวนเงินที่เสนอโดยเว็บไซต์ออนไลน์ ($\mu = 1.69$, $\sigma = 1.184$) ท่านเพิกเฉยต่ออีเมลหลอกลงที่มีชื่อเสียงที่ผิดปกติหรือเกินจริง ($\mu = 1.60$, $\sigma = 1.129$) ท่านมีความตระหนักถึงและสามารถระบุงการถูกลอกลงบนโลกออนไลน์ที่เกิดขึ้นล่าสุดได้ ($\mu = 1.53$, $\sigma = 1.016$) ท่านยอมรับพัสดุหรือของขวัญจากเพื่อนในอินเทอร์เน็ต ($\mu = 1.20$, $\sigma = 1.063$) ท่านสร้างความสัมพันธ์แบบไว้เนื้อเชื่อใจบนโลกออนไลน์กับคนแปลก

หน้า ($\mu = 0.76$, $\sigma = 0.805$) ท่านไม่ลังเลที่จะพบหน้าแบบเห็นหน้าคร่ำคร่ากับเพื่อนที่รู้จักกันทาง อินเทอร์เน็ต ($\mu = 0.66$, $\sigma = 0.834$) ท่านไว้วางใจ/เชื่อใจในรูปภาพของคนแปลกหน้าที่โพสต์ ลงบนอินเทอร์เน็ต ($\mu = 0.58$, $\sigma = 0.766$) ท่านมีความเต็มใจที่จะโอนเงินให้แก่เพื่อนที่รู้จักกัน ทางโลกออนไลน์ ($\mu = 0.43$, $\sigma = 0.847$) และท่านตอบคำถามทางโทรศัพท์ที่เกี่ยวข้องกับเงิน รางวัลจำนวนมหาศาล ($\mu = 0.38$, $\sigma = 0.743$) ตามลำดับ

4.4 ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย

ตาราง 4.8 ผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ระหว่างบุคลิกภาพแบบเปิดประสบการณ์ กับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย ของพนักงานในสังกัดศูนย์เทคโนโลยี สารสนเทศและการสื่อสาร (N = 65)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	บุคลิกภาพแบบเปิดประสบการณ์		
	ρ	Sig.	ระดับความสัมพันธ์
1. การเข้ารหัสผ่าน	- 0.19	0.880	ไม่มีความสัมพันธ์
2. ใช้โปรแกรมซอฟต์แวร์ที่ไม่พึง ประสงค์	0.277*	0.026	ระดับต่ำมาก
3. การถูกหลอกลวง	0.294*	0.018	ระดับต่ำมาก
4. ด้านการโจมตีทางวิศวกรรม สังคม	0.014	0.910	ไม่มีความสัมพันธ์
5. การถูกหลอกลวงทาง ออนไลน์	0.068	0.589	ไม่มีความสัมพันธ์

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตาราง 4.8 เมื่อพิจารณาผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ ระหว่างบุคลิกภาพ แบบเปิดประสบการณ์กับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย จะพบว่า บุคลิกภาพ แบบเปิดประสบการณ์มีความสัมพันธ์ทางบวกกับพฤติกรรมการใช้ซอฟต์แวร์ที่ไม่พึงประสงค์ ($\rho = 0.277$, $\text{sig} = 0.26$) แสดงให้เห็นว่าความสัมพันธ์สองตัวนี้อยู่ในระดับที่ต่ำมาก บ่งบอกได้ว่า

บุคลิกภาพเช่นนี้มีการเปิดรับสิ่งใหม่ๆ หรือสิ่งที่แปลกใหม่โดยไม่คำนึงในความปลอดภัยของข้อมูลสารสนเทศ และพฤติกรรมการถูกหลอกหลวงอยู่ในระดับที่ต่ำมาก ($p=0.294$, sig = 0.294) แสดงว่าบุคลิกภาพแบบเปิดประสบการณ์นั้นมีพฤติกรรมที่ไม่เกรงกลัวหรือไม่คำนึงถึงการถูกหลอกหลวงที่แอบแฝงมาในรูปแบบต่าง ๆ ในระบบคอมพิวเตอร์ ซึ่งบุคลิกภาพแบบเปิดประสบการณ์มีแนวโน้มที่จะถูกหลอกหลวงหรือถูกขโมยข้อมูลได้อย่างง่ายดาย

ตาราง 4.9 ผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ระหว่างบุคลิกภาพแบบประนีประนอมกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (N = 65)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	บุคลิกภาพแบบประนีประนอม		
	ρ	Sig.	ระดับความสัมพันธ์
1. การใช้อีเมลผ่าน	- 0.036	0.776	ไม่มีความสัมพันธ์
2. ใช้โปรแกรมซอฟต์แวร์ที่ไม่พึง ประสงค์	0.127	0.313	ไม่มีความสัมพันธ์
3. การถูกหลอกหลวง	0.364**	0.003	ระดับต่ำ
4. ด้านการโจมตีทางวิศวกรรม สังคม	0.152	0.227	ไม่มีความสัมพันธ์
5. การถูกหลอกหลวงทาง ออนไลน์	0.084	0.507	ไม่มีความสัมพันธ์

**มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตาราง 4.9 เมื่อพิจารณาผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ ระหว่างบุคลิกภาพแบบประนีประนอมกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย จะพบว่าบุคลิกภาพแบบประนีประนอมมีความสัมพันธ์ทางบวกกับพฤติกรรมการถูกหลอกหลวงในระดับต่ำ ($p = 0.364$, sig= 0.003) ซึ่งในภาพรวมบุคลิกภาพแบบประนีประนอมเป็นบุคลิกภาพที่มีความไว้วางใจผู้อื่นง่าย แต่ในบางครั้งมักจะเป็นคนที่ขี้สงสัย ดังนั้น บุคลิกภาพเช่นนี้อาจมีแนวโน้มที่เสี่ยงต่อการถูกหลอกหลวงได้ง่าย

ตาราง 4.10 ผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ระหว่างบุคลิกภาพแบบหวั่นไหวกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (N = 65)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	บุคลิกภาพแบบหวั่นไหว		
	ρ	Sig.	ระดับความสัมพันธ์
1. การใช้อีเมลผ่าน	- 0.168	0.181	ไม่มีความสัมพันธ์
2. ใช้โปรแกรมซอฟต์แวร์ที่ไม่พึง ประสงค์	0.031	0.805	ไม่มีความสัมพันธ์
3. การถูกหลอกลวง	- 0.138	0.273	ไม่มีความสัมพันธ์
4. ด้านการโจมตีทางวิศวกรรม สังคม	0.032	0.801	ไม่มีความสัมพันธ์
5. การถูกหลอกลวงทาง ออนไลน์	0.145	0.249	ไม่มีความสัมพันธ์

จากตาราง 4.10 เมื่อพิจารณาผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ ระหว่างบุคลิกภาพแบบหวั่นไหวกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย พบว่า ไม่มีพฤติกรรมใดที่มีความสัมพันธ์กับบุคลิกภาพแบบหวั่นไหว แสดงให้เห็นว่าบุคลิกภาพแบบหวั่นไหวมีความวิตกกังวลและมีความหวั่นไหวต่อสิ่งต่าง ๆ ไม่ว่าจะกำลังจะเกิดขึ้นหรือไม่เกิดขึ้นก็ตาม และบุคลิกภาพเช่นนี้คิดมากกับเรื่องต่าง ๆ ผลจากการวิเคราะห์ที่ได้จึงไม่มีแนวโน้มที่จะเกิดความเสียหายในด้านของพฤติกรรมต่าง ๆ ทางสารสนเทศ

ตาราง 4.11 ผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ระหว่างบุคลิกภาพแบบแสดงตัว กับ พฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร N = 65)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	บุคลิกภาพแบบแสดงตัว		
	ρ	Sig.	ระดับความสัมพันธ์
1. การใช้รหัสผ่าน	- 0.170	0.176	ไม่มีความสัมพันธ์
2. ใช้โปรแกรมซอฟต์แวร์ที่ไม่พึง ประสงค์	0.249*	0.057	ระดับต่ำ
3. การถูกหลอกลวง	0.210	0.094	ไม่มีความสัมพันธ์
4. ด้านการโจมตีทางวิศวกรรม สังคม	- 0.06	0.315	ไม่มีความสัมพันธ์
5. การถูกหลอกลวงทาง ออนไลน์	0.127		

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตาราง 4.11 เมื่อพิจารณาผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ ระหว่าง บุคลิกภาพแบบแสดงตัวกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย พบว่าบุคลิกภาพแบบแสดงตัวความสัมพันธ์ทางบวกพฤติกรรมการใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์ในระดับต่ำ ($\rho = 0.249$, sig= 0.057) ซึ่งในภาพรวมของบุคลิกภาพแบบแสดงตัวเป็นบุคลิกที่มีความเป็นตัวของตัวเองค่อนข้างสูง ชอบเข้าสังคมมีการแสดงออกอย่างชัดเจน บุคลิกภาพเช่นนี้มีความเสี่ยงในการถูกขโมยข้อมูลต่าง ๆ จากการดาวน์โหลดติดตั้งโปรแกรมที่ไม่มีค่าใช้จ่ายโดยไม่คำนึงว่าจะมีผู้ไม่หวังดีแอบแฝงหรือแอบแฝงมาในรูปแบบของ E-mail ที่มีความน่าเชื่อถือ

ตาราง 4.12 ผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ระหว่างบุคลิกภาพแบบมีจิตสำนึกกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (N = 65)

พฤติกรรมการใช้ข้อมูล สารสนเทศอย่างปลอดภัย	บุคลิกภาพแบบมีจิตสำนึก		
	ρ	Sig.	ระดับความสัมพันธ์
1. การใช้รหัสผ่าน	- 0.130	0.300	ไม่มีความสัมพันธ์
2. ใช้โปรแกรมซอฟต์แวร์ที่ไม่พึง ประสงค์	0.086	0.497	ไม่มีความสัมพันธ์
3. การถูกลอกลวง	0.303*	0.014	ระดับต่ำ
4. ด้านการโจมตีทางวิศวกรรม สังคม	0.127	0.314	ไม่มีความสัมพันธ์
5. การถูกลอกลวงทาง ออนไลน์	- 0.071	0.576	ไม่มีความสัมพันธ์

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตาราง 4.12 เมื่อพิจารณาผลการวิเคราะห์สัมประสิทธิ์สหสัมพันธ์ ระหว่างบุคลิกภาพแบบมีจิตสำนึกกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยจะพบว่าบุคลิกภาพแบบมีจิตสำนึกมีความสัมพันธ์ทางบวกกับพฤติกรรมการถูกลอกลวงในระดับต่ำ ($\rho = 0.303$, sig = 0.014) แสดงว่าบุคลิกภาพเช่นนี้มีแนวโน้มในการถูกลอกลวงได้น้อยมากเนื่องจากบุคลิกภาพแบบมีจิตสำนึกจะเป็นผู้ที่ปฏิบัติตามกฎระเบียบต่าง ๆ ที่ทางองค์กรหรือหน่วยงานจัดตั้งขึ้น

บทที่ 5

สรุปผลการวิจัย การอภิปรายผล และข้อเสนอแนะ

การศึกษา เรื่อง ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร องค์การภาครัฐแห่งหนึ่ง ได้ทำการศึกษาประชากรทั้งหมด ประชากรที่ใช้ในการศึกษาเป็นบุคลากรในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จำนวน 65 คน โดยใช้เครื่องมือในการเก็บรวบรวมข้อมูลเป็นแบบสอบถามที่สามารถทำได้ด้วยตนเอง โดยนำไปให้อาจารย์ที่ปรึกษาและผู้เชี่ยวชาญตรวจสอบความเที่ยงตรงของเนื้อหาและความเหมาะสมของภาษา โดยการหาค่าสัมประสิทธิ์แอลฟาทดสอบความเชื่อมั่น (Reliability) ของแบบสอบถาม การวิเคราะห์ข้อมูลโดยใช้สถิติเชิงพรรณนา ได้แก่ ความถี่ (Frequency) ค่าร้อยละ (Percentage) ค่าเฉลี่ย (μ) ส่วนเบี่ยงเบนมาตรฐาน (σ) และใช้สถิติทดสอบสัมประสิทธิ์สหสัมพันธ์ของบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศ ซึ่งในการศึกษาคั้งนี้ ได้กำหนดวัตถุประสงค์ของการศึกษา ดังนี้ เพื่อศึกษาบุคลิกภาพห้าองค์ประกอบของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อศึกษาพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และเพื่อศึกษาความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย

5.1 สรุปผลการวิจัย

ผลการวิเคราะห์ข้อมูลการศึกษา เรื่อง ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร องค์การภาครัฐแห่งหนึ่ง โดยทำการศึกษาประชากรทั้งหมด 65 คน สามารถสรุปผลการศึกษาได้ดังนี้

5.1.1 สรุปผลการวิเคราะห์ข้อมูลลักษณะส่วนบุคคล

ผลการวิเคราะห์ข้อมูลของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสารขององค์การภาครัฐแห่งหนึ่ง จากประชากรทั้งหมด จำนวน 65 คน พบว่า ส่วนใหญ่เป็นเพศหญิง จำนวน 33 คน คิดเป็นร้อยละ 50.8 มีช่วงอายุ 20-30 ปี จำนวน 25 คน คิดเป็นร้อยละ 38.5 มีสถานภาพโสด จำนวน 41 คน คิดเป็นร้อยละ 63.1 มีระดับการศึกษาปริญญาตรี จำนวน 47 คน คิดเป็นร้อยละ 72.3 มีตำแหน่งเป็นพนักงานราชการ จำนวน 33 คน คิดเป็นร้อยละ 50.8 มีรายได้ตั้งแต่ 20,001 บาทขึ้นไป จำนวน 38 คน คิดเป็นร้อยละ 58.5 และมีประสบการณ์ในการทำงานน้อยกว่า 5 ปี/เท่ากับ 5 ปี จำนวน 33 คน คิดเป็นร้อยละ 50.7

5.1.2 สรุปผลการวิเคราะห์บุคลิกภาพห้าองค์ประกอบ ดังนี้

จากผลการวิเคราะห์โดยภาพรวมของบุคลิกภาพห้าองค์ประกอบ พบว่า ประชากรส่วนใหญ่มีบุคลิกภาพห้าองค์ประกอบที่มีค่าเฉลี่ยอยู่ในระดับมาก เมื่อพิจารณาเป็นด้าน พบว่า ประชากรส่วนใหญ่มีบุคลิกภาพแบบมีจิตสำนึก ซึ่งมีค่าเฉลี่ยมากที่สุด รองลงมาคือ บุคลิกภาพแบบประนีประนอม ด้านบุคลิกภาพแบบเปิดประสบการณ์ บุคลิกภาพแบบแสดงตัว และบุคลิกภาพแบบหวั่นไหว ตามลำดับ

5.1.3 สรุปผลการวิเคราะห์พฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย ดังนี้

จากการศึกษาพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย พบว่า ประชากรมีพฤติกรรมในภาพรวมอยู่ในระดับน้อยที่สุด เมื่อพิจารณาเป็นผลการศึกษาในรายข้อคำถาม พบว่า ในด้านของการใช้รหัสผ่าน มีค่าเฉลี่ยอยู่ในระดับมากที่สุด รองลงมาคือ การถูกโจมตีทางด้านวิศวกรรมสังคม การใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์ ด้านการถูกหลอกหลวง และด้านการถูกหลอกหลวงทางออนไลน์ ตามลำดับ

5.1.4 สรุปผลการวิเคราะห์ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เมื่อพิจารณาเป็นรายด้าน พบว่า

5.1.4.1 ความสัมพันธ์ระหว่างบุคลิกภาพแบบเปิดประสบการณ์กับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย พบว่า บุคลิกภาพแบบเปิดประสบการณ์มีความสัมพันธ์กับพฤติกรรมการใช้ซอฟต์แวร์ที่ไม่พึงประสงค์ และมีความสัมพันธ์กับพฤติกรรมการถูกหลอกลวง

5.4.1.2 ความสัมพันธ์ระหว่างบุคลิกภาพแบบประนีประนอมกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย พบว่า บุคลิกภาพแบบประนีประนอมมีความสัมพันธ์กับพฤติกรรมการถูกหลอกลวง

5.4.1.3 ความสัมพันธ์ระหว่างบุคลิกภาพแบบแสดงตัวกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย พบว่า บุคลิกภาพแบบแสดงตัวมีความสัมพันธ์กับพฤติกรรมการใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์

5.4.1.4 ความสัมพันธ์ระหว่างบุคลิกภาพแบบมีจิตสำนึกกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย พบว่า บุคลิกภาพแบบมีจิตสำนึกมีความสัมพันธ์กับพฤติกรรมการถูกหลอกลวง

5.2 อภิปรายผล

จากผลการศึกษา บุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร องค์การภาครัฐแห่งหนึ่งสามารถอภิปรายผลได้ ดังนี้

5.2.1 ผลการศึกษามุมมองบุคลิกภาพห้าองค์ประกอบของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร องค์การภาครัฐแห่งหนึ่ง ในภาพรวม พบว่า พนักงานในสังกัดมีบุคลิกภาพแบบมีจิตสำนึก ซึ่งมีค่าเฉลี่ยอยู่ในระดับมากที่สุด เนื่องจากองค์กรเป็นหน่วยงานทางราชการ พนักงานทุกคนจำเป็นต้องยึดถือปฏิบัติตามกฎระเบียบหรือข้อบังคับต่าง ๆ ที่กำหนดขึ้นโดยผู้บังคับบัญชาการ นอกจากนี้พนักงานในสังกัดยังมีจิตสำนึกรับผิดชอบในหน้าที่และรับผิดชอบงานที่ได้รับมอบหมาย ซึ่งมีความสอดคล้องกับแนวคิดของคลอธตาและแมคเคอร์ที่กล่าวว่า ลักษณะของบุคลิกภาพแบบมีจิตสำนึกสูง เป็นผู้ที่มิระบระเบียบในการปฏิบัติงาน

มีความรับผิดชอบที่มุ่งเน้นต่อการปฏิบัติงานให้สำเร็จลุล่วง และมีจิตสำนึกรับผิดชอบต่อหน้าที่ เป็นผลทำให้พนักงานในสังกัดส่วนใหญ่มีลักษณะบุคลิกภาพแบบมีจิตสำนึกซึ่งลักษณะบุคลิกภาพเช่นนี้เป็นที่คาดหวังของผู้บริหารองค์กร

บุคลิกภาพแบบประนีประนอม พบว่า พนักงานในสังกัดมีบุคลิกภาพแบบประนีประนอมที่มีค่าเฉลี่ยอยู่ในระดับมากรองลงมาจากบุคลิกภาพแบบมีจิตสำนึก เนื่องจากพนักงานมีการถูกปลูกฝังในเรื่องของการทำงานร่วมกับผู้อื่นและการปฏิบัติงานในองค์กรมีการติดต่อประสานงานกับบุคคลภายในและภายนอกอยู่เสมอ ทำให้พนักงานเป็นคนที่มีความสุภาพอ่อนโยน มีเหตุมีผลในการตัดสินใจและแก้ไขปัญหาความขัดแย้ง และมีความเต็มใจที่จะช่วยเหลือผู้อื่น ซึ่งมีความสอดคล้องกับแนวคิดของคลอสตาและแมคเคอว่าด้วยลักษณะของผู้ที่มีบุคลิกภาพแบบประนีประนอมสูง เป็นผู้ที่มีความอ่อนโยน มีน้ำใจต่อบุคคลรอบข้างและมีเหตุมีผลในการตัดสินใจในการแก้ไขปัญหา สิ่งที่ถูกกล่าวมาข้างต้นจึงเป็นส่วนหนึ่งที่ทำให้พนักงานที่มีลักษณะบุคลิกภาพแบบประนีประนอมเป็นที่คาดหวังของผู้ร่วมงานและบุคคลอื่น ๆ ที่ต้องการร่วมงานด้วย

5.2.2 พฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัย แบ่งออกเป็นรายด้าน ได้แก่ พฤติกรรมการใช้รหัสผ่าน พฤติกรรมการถูกลอกลวง พฤติกรรมการใช้ซอฟต์แวร์ที่ไม่พึงประสงค์ พฤติกรรมในด้านการโจมตีทางวิศวกรรมสังคม และพฤติกรรมการถูกลอกลวงทางออนไลน์ สามารถอภิปรายผลโดยจำแนกออกเป็นรายชื่อ ดังนี้

พฤติกรรมการใช้รหัสผ่าน พบว่า มีค่าเฉลี่ยระดับพฤติกรรมที่แสดงออกอยู่ในระดับน้อย พนักงานในสังกัดส่วนใหญ่มีการตั้งรหัสผ่านโดยใช้ตัวอักษรและตัวเลขมากกว่า 8 ตัวผสมกัน ถือว่าเป็นการป้องกันการถูกขโมยรหัสผ่านจากผู้ไม่หวังดีที่นำไปแอบอ้างหรือนำไปใช้ในทางที่ไม่ดี เนื่องจากพนักงานในสังกัดบางส่วนมีประสบการณ์ในการถูกขโมยรหัสผ่านไปใช้ในทางที่ไม่ดี และพนักงานมีความรู้ความเข้าใจจากเจ้าหน้าที่ที่มีหน้าที่ในการดูแลระบบความปลอดภัย ข้อมูลของหน่วยงานที่ได้มีการแนะนำแนวทางและวิธีการป้องกันการถูกคาดเดารหัสผ่านโดยการใช้ตัวอักษรกับตัวเลขผสมกันและให้มีความยาวของการตั้งรหัสที่ยากต่อการคาดเดา ซึ่งสอดคล้องกับสุภกิจ มหิทธิบุรินทร์ (2557) ได้ศึกษาตัวแปรในการตั้งรหัสผ่าน ที่พบว่า พฤติกรรมการตั้งรหัสผ่านส่วนใหญ่มีการกำหนดความยาวของรหัสผ่านที่มีความยาวมากกว่า 8

ตัวอักษรและกำหนดรหัสผ่านโดยใช้ตัวอักษร ตัวเลข และอักขระพิเศษที่มีความปลอดภัยและยากต่อการคาดเดา ซึ่งเป็นผลสะท้อนถึงพฤติกรรมของพนักงานในสังกัดที่ตระหนักถึงความเสี่ยงต่อการถูกขโมยรหัสผ่าน

พฤติกรรมการใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์ พบว่า พนักงานในสังกัดส่วนใหญ่มีการติดตั้งโปรแกรม Antivirus, Firewall, และโปรแกรมป้องกันการสอดส่องการใช้งานคอมพิวเตอร์ ซึ่งมีค่าเฉลี่ยที่สูงที่สุด เนื่องด้วยองค์กรปฏิบัติงานเกี่ยวกับด้านสารสนเทศและองค์กรเคยถูกโจมตีจากผู้ไม่หวังดี นอกจากนี้พนักงานมีการรับรู้ข้อมูลข่าวสารเกี่ยวกับด้านของความปลอดภัยทางระบบคอมพิวเตอร์ จึงเป็นสาเหตุหนึ่งที่ทำให้พนักงานมีการติดตั้งโปรแกรม Antivirus, Firewall, และโปรแกรมป้องกันการสอดส่องการใช้งานคอมพิวเตอร์ เพื่อเป็นการป้องกันไวรัสที่แอบแฝงมาในรูปแบบต่าง ๆ ที่ไม่ทันได้ตั้งตัวและมีความตระหนักถึงความปลอดภัยของข้อมูลที่เกิดความเสียหายขององค์กร

พฤติกรรมการถูกหลอกลวง พบว่า พนักงานในสังกัดมีความมั่นใจว่าตนเองไม่ใช่เหยื่อของการถูกหลอกลวงเนื่องจากไม่ใช่เป้าหมายของการถูกหลอกลวง ซึ่งมีค่าเฉลี่ยที่พบอยู่ในระดับสูงที่สุด เนื่องจากการปฏิบัติงานของพนักงานมีความเกี่ยวข้องกับสารสนเทศ พนักงานจึงมีความรู้ความเข้าใจวิธีการป้องกันการตกเป็นเหยื่อของการถูกหลอกลวง นอกจากนี้องค์กรมีการส่งพนักงานเข้าร่วมสัมมนาต่าง ๆ ที่จัดขึ้นโดยหน่วยงานที่มีความรับผิดชอบและมีความเชี่ยวชาญในด้านของการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์โดยตรง ทั้งหมดที่กล่าวมานี้จึงทำให้พนักงานในสังกัดทุกคนมีวิธีการหลีกเลี่ยงไม่ให้ตกเป็นเหยื่อในการถูกหลอกลวง

การโจมตีทางด้านวิศวกรรมสังคม พบว่า พนักงานในสังกัดส่วนใหญ่มีความเต็มใจที่จะปฏิบัติตามข้อกำหนดหรือข้อบังคับที่ถูกกำหนดขึ้นโดยเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบหรือจากผู้บังคับบัญชา ซึ่งมีค่าเฉลี่ยที่พบอยู่ในระดับสูงที่สุด เนื่องจากองค์กรมีการปฏิบัติงานเกี่ยวข้องกับสารสนเทศอยู่แล้ว ดังนั้น วิธีหรือแนวทางการรักษาความปลอดภัยของข้อมูลซึ่งในองค์กรมีการตั้งนโยบายหรือกฎระเบียบข้อบังคับเพื่อควบคุม ดูแล และป้องกันการถูกโจมตีทางด้านวิศวกรรมสังคม ความปลอดภัยของข้อมูลล้วนเกิดจากการตั้งนโยบายหรือข้อบังคับที่มีในองค์กร และพนักงานในองค์กรยึดถือปฏิบัติ

การถูกหลอกลวงทางออนไลน์ พบว่า พนักงานในสังกัดมีความไวเนื้อเชื่อใจกับข้อมูลของคนแปลกหน้าที่ได้รับบนอินเทอร์เน็ตหรืออีเมล ซึ่งมีค่าเฉลี่ยที่พบอยู่ในระดับที่สูงที่สุด อาจเป็นสาเหตุที่ทำให้เกิดการถูกหลอกลวงทางออนไลน์ได้ เนื่องจากข้อมูลที่ได้รับจากคนแปลกหน้ามีความน่าสนใจ และมีข้อมูลที่กระตุ้นให้ผู้รับเชื่อถือมากยิ่งขึ้น พนักงานบางส่วนอาจไม่คำนึงถึงความปลอดภัยหรือรู้เท่าไม่ถึงการณ์หรือขาดความรู้ความเข้าใจกับข้อมูลหลอกลวงเหล่านั้น ที่ได้รับทางอินเทอร์เน็ต จึงเป็นสาเหตุเพียงเรื่องเดียวที่ส่งผลต่อการเกิดพฤติกรรมในการถูกหลอกลวงทางออนไลน์ของพนักงานในสังกัด

5.2.3 ผลการศึกษาความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศอย่างปลอดภัยของพนักงานในสังกัดศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สามารถอภิปรายผลโดยจำแนกออกเป็นรายด้าน ดังนี้

บุคลิกภาพแบบเปิดประสบการณ์มีความสัมพันธ์กับพฤติกรรมการใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์และพฤติกรรมการถูกหลอกลวง ซึ่งมีความสัมพันธ์กันในเชิงบวกและมีค่าเฉลี่ยอยู่ในระดับที่ต่ำมาก แสดงว่าพนักงานในสังกัดส่วนใหญ่มีการปฏิบัติตามข้อบังคับหรือกฎกติกาขององค์กร และเปิดรับข้อมูลข่าวสาร เปิดรับการเรียนรู้สิ่งใหม่ ๆ อยู่เสมอ ซึ่งสะท้อนให้เห็นถึงโอกาสที่เกิดช่องว่างในการถูกหลอกลวงหรือการเข้าใช้งานโปรแกรมซอฟต์แวร์ที่ไม่ได้รับอนุญาตได้น้อยมาก เนื่องจากบุคลิกภาพแบบเปิดประสบการณ์ส่วนใหญ่จะมีพฤติกรรมที่มีความตื่นตัว และเปิดรับข้อมูลข่าวสารอยู่เสมอ

บุคลิกภาพแบบแสดงตัวมีความสัมพันธ์กับพฤติกรรมการใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์อยู่ในระดับที่ต่ำ แสดงให้เห็นว่าพนักงานในสังกัดส่วนใหญ่มองโลกในแง่ดีและมีความสนใจในสิ่งต่าง ๆ รอบตัวอยู่เสมอ สะท้อนให้เห็นถึงแนวโน้มในการเกิดพฤติกรรมการใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์

บุคลิกภาพแบบประนีประนอมมีความสัมพันธ์กับพฤติกรรมการถูกหลอกลวง มีความสัมพันธ์อยู่ในระดับที่ต่ำ ซึ่งพนักงานที่มีบุคลิกภาพเช่นนี้มีเหตุมีความอยากรู้อยากเห็น มีความสงสัยในเรื่องต่าง ๆ ในบางครั้งแต่ในทางกลับกันผู้ที่มีบุคลิกภาพเช่นนี้เป็นผู้ที่มีเหตุมีผลในการตัดสินใจแก้ไขปัญหาต่าง ๆ และมีความพร้อมในการรับมือกับการถูกหลอกลวง

บุคลิกภาพแบบมีจิตสำนึกก็มีความสัมพันธ์กับพฤติกรรมการถูกละเมิด พบว่ามีความสัมพันธ์อยู่ในระดับที่ต่ำมาก อาจเป็นเพราะพนักงานส่วนใหญ่ที่มีบุคลิกภาพแบบมีจิตสำนึกจะยึดถือปฏิบัติในระเบียบหรือข้อบังคับที่องค์กรตั้งเพื่อความมั่นคงความปลอดภัยของข้อมูล ซึ่งแสดงให้เห็นว่ามีโอกาสที่จะเกิดพฤติกรรมในการการถูกละเมิดได้น้อยมาก เนื่องจากบุคลิกภาพแบบมีจิตสำนึกจะเป็นผู้ที่ปฏิบัติตามกฎและระเบียบต่าง ๆ ที่ทางองค์กรหรือหน่วยงานจัดตั้งขึ้น

5.3 ข้อเสนอแนะจากการวิจัย

5.3.1 ข้อเสนอแนะที่ได้จากการวิจัยครั้งนี้

1. ผู้บริหารและหัวหน้าฝ่าย/งานในองค์กรควรรักษาความสำคัญและตระหนักถึงความปลอดภัยในการใช้คอมพิวเตอร์ วางแผน จัดทำคู่มือและกำหนดนโยบายควบคุม กำกับดูแล และนำแนวทางไปพัฒนาส่งเสริมให้เกิดพฤติกรรมการป้องกันการถูกละเมิดหรือการถูกโจรกรรมทางคอมพิวเตอร์ เพื่อให้พนักงานสามารถเข้าถึงและยึดถือปฏิบัติที่เป็นไปในทิศทางเดียวกัน

2. ผู้บริหารให้การสนับสนุนการจัดกิจกรรมเสริมสร้างความรับรู้ให้เข้าใจถึงวิธีการป้องกันการถูกละเมิด การล้างความลับของข้อมูล การใช้สารสนเทศ ความปลอดภัยบนระบบคอมพิวเตอร์ การดาวน์โหลดหรือการนำเข้าโปรแกรมที่ไม่พึงประสงค์ รวมไปถึงการละเมิดสิทธิส่วนบุคคล

5.3.2 ข้อเสนอแนะสำหรับการวิจัยในครั้งต่อไป

1. การศึกษาในครั้งต่อไปควรเพิ่มขนาดของประชากร หรือกลุ่มตัวอย่างในสังกัดอื่น ๆ หรือหน่วยงานอื่นทั้งภาครัฐและภาคเอกชน เพื่อให้ได้ข้อมูลที่หลากหลายข้อมูลมีความน่าเชื่อถือ

2. ควรมีการศึกษาตัวแปรอื่น ๆ ที่เกี่ยวกับการป้องกันข้อมูลสารสนเทศอย่างปลอดภัยเช่น วิธีการป้องกันข้อมูล ตั้งแต่เรื่องใกล้ตัว คือ การตั้งรหัสผ่าน การใช้คอมพิวเตอร์

สาธารณะ รวมไปถึงวิธีการใช้งานคอมพิวเตอร์อย่างไรไม่ให้ถูกขโมยข้อมูล การนำระบบรักษาความปลอดภัยข้อมูลอื่นๆ เข้ามาใช้งานภายในหน่วยงาน

3. ควรมุ่งเน้นเฉพาะในเรื่องของพฤติกรรมการใช้ซอฟต์แวร์ที่ไม่พึงประสงค์และการถูกหลอกลวงทางออนไลน์ ซึ่งพฤติกรรมเหล่านี้มีความเกี่ยวข้องกับการถูกคุกคามทางคอมพิวเตอร์และมีความเสี่ยงในด้านความปลอดภัยของข้อมูลส่วนบุคคลและองค์กร จึงเป็นสิ่งที่ควรให้ความสำคัญอย่างยิ่ง



บรรณานุกรม

- กรกช วิไลลักษณ์. (2560). ความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สืบค้นเมื่อ 18 มิถุนายน 2561 จาก <http://www.stou.ac.th/Schools/sst/main/Subject96101/96101-14.pdf>.
- กนกวรรณ ตาลเสียน. (2560). ความมั่นคงปลอดภัยของระบบสารสนเทศ. สืบค้นเมื่อ 7 ตุลาคม 2560 จาก <https://sites.google.com/site/kanokwant5/khwam-mankhng-plxdphay-khxng-rabb-sarsnthes.html>.
- กิตติศักดิ์ จีรวรรณกุล, (2545). การรักษาความมั่นคงปลอดภัยทางกายภาพ. สืบค้นเมื่อ 10 มกราคม 2562 จาก : <http://research.it.mut.ac.th>.
- คณิน อุดมสุขประเสริฐ. (2555). การศึกษาพฤติกรรมการตั้งรหัสผ่านของผู้ใช้อินเทอร์เน็ตวัยทำงานในประเทศไทย. วิทยานิพนธ์มหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.
- ครรชิต มาลัยวงศ์. (2540). คอมพิวเตอร์กับการศึกษา วารสารศูนย์บริการนิตทางการศึกษา หน้า 4-8.
- ฐิติมา มานิตพร. (2560). แนวโน้มความปลอดภัยบนโลกไซเบอร์ Cyber Security Trend 2017 by E-rong. วารสาร Microcomputer March 2017 ปีที่ 34 ฉบับที่ 3805 หน้า 68-69.
- ชเนตตี ชยนานนท์. 2555. พฤติกรรมและปัญหาการใช้อินเทอร์เน็ตของนักศึกษาระดับปริญญาตรี มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ปริญญาโทมหาบัณฑิต มหาวิทยาลัยศรีนครินทรวิโรฒ.
- ดลลักษณ์ พลเสนา. (2556). ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบและพฤติกรรมที่เป็นปัญหาของวัยรุ่นกับการเสพติดอินเทอร์เน็ตเกม. วิทยานิพนธ์ปริญญาโทมหาบัณฑิต สาขาวิชาจิตวิทยาการให้คำปรึกษา คณะวิทยาศาสตร์ มหาวิทยาลัยรามคำแหง.
- ทศพนธ์ นรทัศน์. (2560). ภัยคุกคามไซเบอร์ในมุมมองของผู้ใช้อินเทอร์เน็ตในประเทศไทย. วารสาร Microcomputer March 2017 ปีที่ 35 ฉบับที่ 3806 หน้า 66.

บรรณานุกรม (ต่อ)

- ธนพร วัฒนศรานนท์. (2555). ปัจจัยด้านการปรับปรุงมาตรฐานในการให้บริการและด้านบุคลิกภาพที่ส่งผลต่อประสิทธิภาพการทำงานของบุคลากรโรงพยาบาลสมิติเวช สุขุมวิท. ปริญญาบริหารธุรกิจมหาบัณฑิต มหาวิทยาลัยศรีนครินทรวิโรฒ.
- ธนบูรณ์ เข็นอุทก. 2556. การศึกษาพฤติกรรมการใช้เทคโนโลยีสารสนเทศของพนักงาน บริษัท ไทโยต้า มอเตอร์ ประเทศไทย จำกัด. วิทยานิพนธ์ปริญญาโทมหาบัณฑิต. สาขาวิชาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ คณะครุศาสตร์อุตสาหกรรมมหาบัณฑิต มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี.
- ธีรยุทธ เอกภูณ. (2558). ในการประชุมวิชาการระดับนานาชาติเรื่อง อิทธิพลของรูปแบบการใส่รหัสผ่านและประเภทของรหัสผ่านต่อการพิสูจน์ตัวตนด้วยรหัสผ่านตัวอักษรร่วมกับการใช้ตารางกริดและรูปภาพ (น. 209-210). กรุงเทพฯ : คณะวิทยาการจัดการ มหาวิทยาลัยราชภัฏสวนสุนันทา
- นิชนันท์ ก่อกุลกิตติการ. (2559). พฤติกรรมสารสนเทศของผู้ผลิตรายการโทรทัศน์. วิทยานิพนธ์ปริญญาโทมหาบัณฑิต สาขาวิชาบรรณารักษศาสตร์และสารนิเทศศาสตร์ คณะศิลปศาสตร์ มหาวิทยาลัยรามคำแหง.
- นิภาพร พวงมี (2554). บุคลิกภาพห้าองค์ประกอบกับการรับรู้วัฒนธรรมองค์การ ของพยาบาลโรงพยาบาลมหาวิทยาลัยแห่งหนึ่ง. ปริญญาโทมหาบัณฑิต สาขาจิตวิทยาอุตสาหกรรมและองค์การ มหาวิทยาลัยธรรมศาสตร์.
- นิวัตติ เนียมพลอย. (2560). ไซเบอร์กับการรักษาความปลอดภัยและการปฏิบัติการ. สืบค้นเมื่อ 20 กุมภาพันธ์ 2561 จาก : <https://nniwat.wordpress.com/2013/11/08/ไซเบอร์กับการรักษาความปลอดภัย>.
- บุญชม ศรีสะอาด. (2556). วิธีการทางสถิติสำหรับการวิจัย (พิมพ์ครั้งที่ 5). กรุงเทพฯ: สุวีริยาสาส์น.
- ปณิชา นิตีพรมงคล. (2560). พฤติกรรมการใช้เครือข่ายสังคมออนไลน์ของคนวัยทำงานในเขตกรุงเทพมหานคร สืบค้นเมื่อ 18 พฤศจิกายน 2560, จาก : <http://spu.ac.th/commarts/files/2012/07/บทความ-ปณิชา.pdf>.

บรรณานุกรม (ต่อ)

- พรพรม ประกากิตติกุล. (2555). สัญญาอันตรายที่มากับรหัสผ่าน. สืบค้นเมื่อ 29 เมษายน 2561. จาก www.thaicert.or.th.
- เพ็ญพันธ์ เพชรสร. (2552). เอกสารประกอบการสอนวิชา 412102 ทักษะการรู้สารสนเทศ. พิมพ์ครั้งที่ 3 ขอนแก่น. สำนักวิชาการศึกษาทั่วไป มหาวิทยาลัยขอนแก่น.
- มงคล อุดมชัยพัฒนากิจ. (2557). ทักษะชีวิต บุคลิกภาพห้าองค์ประกอบ และบรรยากาศองค์กร ส่งผลต่อการมีส่วนร่วมในการพัฒนาและคุณภาพในการทำงานของพนักงานในบริษัทเอกชน ในเขตกรุงเทพมหานคร. บริหารธุรกิจมหาบัณฑิต มหาวิทยาลัยกรุงเทพ.
- มนต์ชัย เทียนทอง. (2548). สถิติและวิธีการวิจัยทางเทคโนโลยีสารสนเทศ. กรุงเทพฯ: วิทยุการพิมพ์. เมธี ไพรัชิต. (2556). การหาปัจจัยที่มีผลต่อการเสริมสร้างประสิทธิภาพในการปฏิบัติงานของพนักงาน กรณีศึกษา: บริษัท สุธานี จำกัด. สารนิพนธ์ปริญญาโทมหาบัณฑิต คณะวิทยาศาสตร์ มหาวิทยาลัยกรุงเทพธนบุรี.
- ราชบัณฑิตยสถาน. (2546). พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2542. กรุงเทพฯ : นานมีบุ๊คส์พับลิเคชั่นส์.
- วิจัย สมอ้าย. (2554). การศึกษาพฤติกรรมการใช้เทคโนโลยีสารสนเทศของพนักงานบริษัท ทูมูฟ จำกัด ในเขตภาคตะวันออกเฉียงเหนือ วิทยานิพนธ์ปริญญาโทมหาบัณฑิต สาขาวิชาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี.
- วิเศษศักดิ์ โคตรอาษา. (2542). เทคโนโลยีสารสนเทศเพื่อการเรียนรู้. กรุงเทพฯ: ธีรด์เวฟ เอ็ดดูเคชั่น. ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค) รายงานผลการสำรวจผู้ใช้อินเทอร์เน็ตในประเทศไทยประจำปี 2553. สืบค้นเมื่อ 18 ธันวาคม 2560. จาก : www.nstda.or.th/prs/index.php/53-4.
- ศรวิสัย สอนิ. (2557). ความรู้ ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษา: ข้าราชการกองบัญชาการกองทัพไทย สืบค้นเมื่อ 18 ธันวาคม 2560 จาก: <http://ilodoc.dpu.ac.th/thesis/155993.pdf>.

บรรณานุกรม (ต่อ)

- ศรีเรือน แก้วสังวาล. (2554). ทฤษฎีจิตวิทยาบุคลิกภาพ. (พิมพ์ครั้งที่ 15). กรุงเทพมหานคร: หมอชาวบ้าน.
- สถิติภัยคุกคาม ประจำปี. (พ.ศ. 2554-2559). Thailand Computer Emergency Response Team (ThaiCERT). สืบค้นข้อมูล : <https://www.thaicert.or.th/statistics/statistics.html>
- สมใจ ศรีปานเงิน. (2540). ความต้องการใช้และการใช้ทรัพยากรสารสนเทศของผู้ใช้ห้องสมุด เฉพาะสังกัดสำนักนายกรัฐมนตรี้. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะศิลปศาสตร์ สาขาวิชาบรรณารักษศาสตร์และสารนิเทศศาสตร์ มหาวิทยาลัยรามคำแหง.
- สุชญา ชูแสง. (2557). ความสัมพันธ์ระหว่างลักษณะบุคลิกภาพห้าองค์ประกอบและผลการเรียนรู้ เป็นที่มบุคลากรทางด้านการขนส่งสินค้าทางทะเลในเขตอำเภอหาดใหญ่ จังหวัดสงขลา. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะบริหารธุรกิจ มหาวิทยาลัยสงขลานครินทร์.
- สุพิชญา อาชวีรดา. (2560). ปัจจัยที่ส่งผลกระทบต่อระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร สืบค้นเมื่อ 15 มกราคม 2561. จาก : http://doi.nrct.go.th/ListDoi/Download/194401/dda2589f2436b85e194932f2c5d93242?Resolve_DOI=10.14456/jisb.2016.11.
- สุภกิจ มหิทธิบุรินทร์. (2557). การพิสูจน์ตัวตนแบบสองปัจจัยโดยใช้รหัสผ่านและภาพ. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะเทคโนโลยีสารสนเทศ สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.
- เสฏฐวุฒิ แสนนาม. (2555). ข้อเสนอแนะในการใช้งานอินเทอร์เน็ตผ่านคอมพิวเตอร์สาธารณะ สืบค้นเมื่อวันที่ 20 กันยายน 2560 จาก <https://www.thaicert.or.th>.
- อนรรทวงศ์ คุณมณี, (2547). คอมพิวเตอร์เบื้องต้น Network computer กรุงเทพฯ: สำนักพิมพ์ เอส.พี.ซี.บุ๊ก จำกัด.

บรรณานุกรม (ต่อ)

- Costa & McCrae. (1992). Revised NEO Personality Inventory (NEO-PI-R) and NEO Five-Factor Inventory (NEO-FFI) professional manual. Odessa FL: Psychological Assessment Resources.
- Feist, J and Feist, Gregory J. (2006). Theories of Personality. (6th ed) NewYork: McGrawhill.
- Lalitha Muniandy, Balakrishnan Muniandy and Zarina Samudin. (2017). Cyber Security Behaviour among Higher Education Students in Malaysia. Journal of information Assurance and Cybersecurity. From :
<http://www.ibm-publishing.com/journals/JICS/jiacs.html>.
- Schult, D.P. and Schult, S.E. (2005). Theories of Personality (8th ed.). USA: Wadsworth Thomson Learning, Inc.
- Stephen P. Robbins. (1989). Organizational Behavior concepts, controversies and applications (4th ed) Englewood Cliffs New Jersey: Prentice-Hall International, Inc.
- McCrae, R.R. and P. T. Costa. (1987). Validation of Five – Factor Model of Personality and Social Psychology.

ภาคผนวก



แบบสอบถามเพื่อการวิจัย

เรื่อง

ความสัมพันธ์ระหว่างบุคลิกภาพห้าองค์ประกอบกับพฤติกรรมการใช้ข้อมูลสารสนเทศ
อย่างปลอดภัย

คำชี้แจง แบบสอบถามชุดนี้ประกอบด้วย 3 ส่วน

ส่วนที่ 1 ลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม

ส่วนที่ 2 ข้อมูลเกี่ยวกับบุคลิกภาพ 5 องค์ประกอบ

ส่วนที่ 3 พฤติกรรมในการใช้งานข้อมูลสารสนเทศอย่างปลอดภัย

ส่วนที่ 1 ลักษณะส่วนบุคคลของผู้ตอบแบบสอบถาม

โปรดใส่เครื่องหมาย ✓ ลงในช่อง

เพศ

หญิง

ชาย

อายุ

20 – 30

31 – 40

41 – 50

50 ปีขึ้นไป

ระดับการศึกษา

ต่ำกว่าปริญญาตรี

ปริญญาตรี

สูงกว่าปริญญาตรี

สถานภาพ

โสด

สมรส

หย่าร้าง

แยกกันอยู่ อื่น ๆ โปรดระบุ.....

ตำแหน่ง

ข้าราชการ

พนักงานราชการ

ลูกจ้างประจำ

จ้างเหมาบริการ

อื่น ๆ โปรดระบุ.....

รายได้ น้อยกว่า/เท่ากับ 15,000

15,001 – 20,000

20,001 ขึ้นไป

ประสบการณ์ น้อยกว่า/เท่ากับ 5 ปี

ในการทำงาน 6 – 10 ปี

11 ปีขึ้นไป

ส่วนที่ 2 ข้อมูลเกี่ยวกับบุคลิกภาพ 5 องค์ประกอบ

โปรดใส่เครื่องหมาย ✓ ลงในช่อง ที่ตรงกับบุคลิกภาพในตัวท่านมากที่สุด

ระดับความคิดเห็น

คะแนน

มากที่สุด

5

มาก

4

ปานกลาง

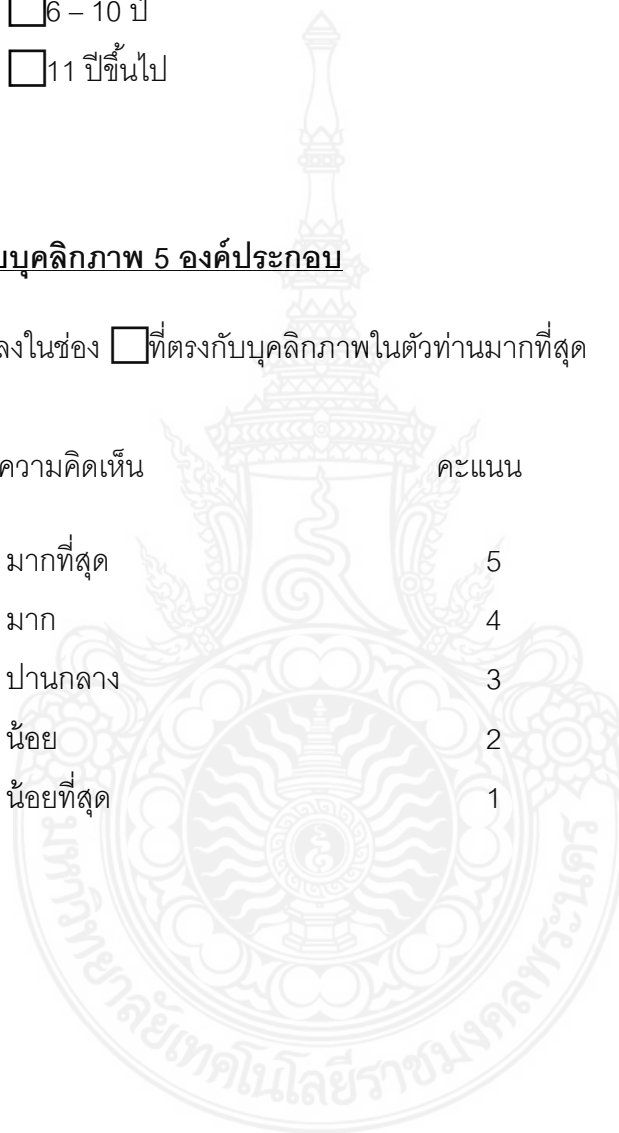
3

น้อย

2

น้อยที่สุด

1



ประเด็นคำถาม	ระดับความคิดเห็น				
	5 มากที่สุด	4 มาก	3 ปานกลาง	2 น้อย	1 น้อยที่สุด
บุคลิกภาพแบบเปิดประสบการณ์ (Extraversion)					
1. ท่านเป็นคนที่มีบุคลิกภาพเปิดรับสิ่งใหม่ ๆ อยู่เสมอ					
2. ท่านเป็นคนร่าเริง ช่างพูด ชอบเข้าสังคม					
3. ท่านเป็นคนอยากทำ อยากเห็น ชอบการเรียนรู้สิ่งใหม่ ๆ ตลอดเวลา					
4. ท่านเป็นคนมีจินตนาการ มีความคิดสร้างสรรค์					
บุคลิกภาพแบบประนีประนอม (Agreeableness)					
1. ท่านเป็นคนที่มีความสุภาพอ่อนโยน					
2. ท่านพร้อมที่จะยอมรับฟังและทำตามคำต่าาห์ของผู้อื่น					
3. ท่านช่วยเหลือคนรอบข้าง/เพื่อนร่วมงานด้วยความเต็มใจ					
4. ท่านมีความพร้อมในการแก้ไขปัญหา/ความขัดแย้งกับผู้อื่น					
แบบหวั่นไหว (Neuroticism)					
1. ฉันเป็นคนที่มีความวิตกกังวลอยู่เสมอ					
2. มีความเครียดในการทำงานหรือเหตุการณ์ต่าง ๆ ที่พบเจอ					
3. มีความหวั่นไหวกับความกดดันหรือคำพูดที่มากกระทบจิตใจ					
4. ไม่สามารถจัดการกับอารมณ์ได้เท่าที่ควร					

ประเด็นคำถาม	ระดับความคิดเห็น				
	5 มากที่สุด	4 มาก	3 ปานกลาง	2 น้อย	1 น้อยที่สุด
แบบแสดงตัว (Extraversion)					
1. มีความมุ่งมั่นในการทำงาน					
2. กล้าคิด กล้าทำ กล้าแสดงออก					
3. ชอบเข้าสังคม ช่างพูดช่างเจรจา					
4. ท่านเป็นคนมีจินตนาการ มีความคิดสร้างสรรค์					
แบบจิตสำนึก(Conscientiousness)					
1. เป็นผู้มีความรับผิดชอบต่อหน้าที่					
2. มีระเบียบวินัยในการปฏิบัติตามกฎระเบียบหรือข้อบังคับภายในหน่วยงาน					
3. ยึดมั่นในหลักการอย่างมีเหตุผล					
4. ท่านมีความพร้อมในการแก้ไขปัญหา/ความขัดแย้งกับผู้อื่น					

ส่วนที่ 3 พฤติกรรมในการใช้งานข้อมูลสารสนเทศอย่างปลอดภัย

โปรดใส่เครื่องหมาย ลงในช่อง ที่ตรงกับตัวท่านมากที่สุด

ระดับความคิดเห็น	คะแนน
ทำเป็นประจำอย่างสม่ำเสมอ	3
ทำทุกวัน	2
ทำบ้างเป็นบางครั้งคราว	1
ไม่เคยทำเลย	0

ประเด็นคำถาม	ระดับความคิดเห็น			
	3 ทำเป็นประจำ	2 ทำ บ่อยครั้ง	1 ทำบ้างเป็น บางครั้ง	0 ไม่เคยทำ
การใช้รหัสผ่าน (Password usage)				
1. จดรหัสผ่านลงในกระดาษหรือสมุดโน้ตเพื่อง่ายต่อการจดจำ				
2. ท่านได้บอกรหัสผ่านกับผู้อื่น				
3. ท่านใช้รหัสผ่านเดียวกันในการเข้าใช้งานระบบ				
4. ตั้งรหัสผ่านของท่านมีตัวอักษรและตัวเลขมากกว่า 8 ตัวผสมกัน				
5. ท่านไม่เคยเปลี่ยนรหัสผ่านของท่านเลย				
6. รหัสผ่านของท่านประกอบไปด้วยตัวอักษรพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ				
7. ตั้งรหัสผ่านจากข้อมูลส่วนบุคคล เช่น วัน เดือน ปี เกิด หมายเลขโทรศัพท์ เป็นต้น				
8. ใช้งานตัวเลือก “การจดจำรหัสผ่านของฉัน”				
9. ใช้รหัสผ่านที่แตกต่างกันในการใช้งานระบบต่างๆ				
10. รหัสผ่านของท่านไม่ได้เป็นไปตามรูปแบบของแป้นพิมพ์				
ใช้โปรแกรมซอฟต์แวร์ที่ไม่พึงประสงค์ (Malware)				
1. ท่านมีความเต็มใจที่จะเปิดเอกสารแนบ E-mail จากบุคคลแปลกหน้า				
2. มีหัวข้อของเอกสารที่น่าสนใจจึงเป็นสาเหตุที่ท่านต้องเปิดอ่านอีเมล				
3. ท่านมีการตรวจสอบสถานะของโปรแกรมป้องกันไวรัสในคอมพิวเตอร์อย่างสม่ำเสมอ				
4. ท่านเปิดเอกสารที่เป็นไฟล์แนบมาโดยแนบเป็นไฟล์ประเภทที่ใช้หลายนามสกุล				

5. ท่านดาวน์โหลดโปรแกรมฟรีจากอินเทอร์เน็ตลงในคอมพิวเตอร์ที่ท่านใช้งานอยู่ประจำ				
6. มีการติดตั้งโปรแกรม antivirus, Firewall, และโปรแกรมป้องกันการสอดส่องการใช้งานคอมพิวเตอร์ของคุณ				
7. ท่านมีความเต็มใจที่จะดาวน์โหลดข้อมูลจากเว็บไซต์ที่ไม่ปลอดภัย				
8. มีการนำโปรแกรมที่ใช้ป้องกันจุดบกพร่องของโปรแกรมคอมพิวเตอร์เพื่อป้องกันการโดนขโมยข้อมูล				
การถูกหลอกลวง (Phishing issue)				
1. ท่านมีการอัปเดตความรู้เกี่ยวกับการถูกหลอกลวงทางคอมพิวเตอร์โดยการอ่านจากข้อมูลที่เกี่ยวข้อง				
2. ท่านมั่นใจว่าคุณไม่ใช่เหยื่อของการหลอกลวงเนื่องจากคุณเป็นบุคคลทั่วไป				
3. มีความสนใจในการจัดการข้อมูลที่น่าเชื่อถือของทุกประเภทของอีเมล				
4. ท่านมีความสนใจในการกด Hyperlink จากอีเมล				
5. มีความเชื่อในข้อความที่ส่งจากอีเมลที่ส่งมาเกี่ยวกับการชิงเงินรางวัลต่าง ๆ				
6. ถ้าจะมีการส่งข้อมูลที่เป็นความลับ ชนิดของ URL ต้องเป็น "https" เท่านั้น				
7. สัญลักษณ์กุญแจมีความจำเป็นในการส่งผ่านข้อมูลที่สำคัญ				
8. ท่านชอบที่จะพิมพ์ URL ในบราวเซอร์แทนการคลิก Hyperlink เพื่อเชื่อมโยงหลายมิติ				
9. เมื่อท่านได้รับอีเมลที่น่าสงสัยคุณจะติดต่อกับบุคคลที่เกี่ยวข้องในการตรวจสอบ				
10. มีการตรวจสอบชนิดของ URL ก่อนที่จะทำธุรกรรมต่างๆ บนอินเทอร์เน็ต				

ด้านการโจมตีทางวิศวกรรมสังคม(Social engineering)				
1. ท่านไม่สนใจในการอ่านข้อมูลที่เกี่ยวข้องกับการโจมตีแบบวิศวกรรมสังคม				
2. ท่านเปิดเผย username และ passwords ถึงบุคคลที่ถูกเรียกว่าเป็นผู้ดูแลระบบ				
3. ท่านเชื่อว่าตนเองไม่ใช่เป้าหมายของการโจมตีแบบวิศวกรรมทางสังคมเนื่องจากเป็นบุคคลทั่วไป				
4. ท่านไม่ยินดีที่จะตอบรับโทรศัพท์, ข้อความ, หรืออีเมลจากคนแปลกหน้าที่เป็นมิตร/ไม่เป็นมิตร				
5. ท่านเต็มใจที่จะปฏิบัติตามข้อกำหนด/ข้อบังคับที่ถูกกำหนดโดยบุคคลที่มีอำนาจรับผิดชอบ				
6. ท่านเต็มใจที่จะให้ passwords แก่โปรแกรมช่วยเหลือการทำงานที่ให้ความช่วยเหลือแก่ผู้ใช้ระบบ				
7. ตรวจสอบอำนาจความรับผิดชอบหรือลักษณะของบุคคลก่อนที่จะมีการพูดคุยถึงประเด็นต่างๆ ผ่านระบบ				
8. ท่านไม่รู้สึกรว่าตนเองหวาดหวั่นกับคำถามของคนแปลกหน้า				
9. ท่านไม่สื่อสารกับคนแปลกหน้าถึงแม้ว่าจะดูน่าไว้วางใจ				
10. ท่านไม่เปิดเผยข้อมูลที่เป็นความลับในทุกๆ สถานการณ์				
การถูกหลอกลวงทางออนไลน์ (Online scam)				
1. ท่านสร้างความสัมพันธ์แบบไว้วางใจกับคนในโลกออนไลน์กับคนแปลกหน้า				
2. ท่านเพิกเฉยต่ออีเมลหลอกลวงที่มีชื่อเสียงที่ผิดปกติหรือเกินจริง				
3. ท่านตอบคำถามทางโทรศัพท์ที่เกี่ยวข้องกับเงินรางวัลจำนวนมหาศาล				

4. ท่านไม่ไว้ใจข้อมูลของคนแปลกหน้าที่ได้รับบนอินเทอร์เน็ต				
5. ท่านไม่เคยให้ความสนใจกับจำนวนเงินที่นำเสนอโดยเว็บไซต์ออนไลน์				
6. ท่านมีความเต็มใจที่จะโอนเงินให้แก่เพื่อนที่รู้จักกันทางโลกออนไลน์				
7. ท่านมีความตระหนักถึง และสามารถระงับการถูกลอกหลวงบนโลกออนไลน์ที่เกิดขึ้นล่าสุดได้				
8. ท่านไว้วางใจ/เชื่อใจในรูปภาพของคนแปลกหน้าที่โพสต์ ลงบนอินเทอร์เน็ต				
9. ท่านไม่ยอมรับพัสดุหรือของขวัญจากเพื่อนในอินเทอร์เน็ต				
10. ท่านไม่ลังเลที่จะพบหน้าแบบเห็นหน้าคร่ำคร่ากับเพื่อนที่รู้จักกันทางอินเทอร์เน็ต				

ชื่อเสนอแนะ.....

.....

.....



