



ความตระหนักรู้เท่าทันกลลวงหลอกขอข้อมูลทางไซเบอร์ (Phishing) ของ
กลุ่มคนช่วงวัย Gen Z

โดย

ปภาดา บุณนาค

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

วิทยาศาสตรมหาบัณฑิต

สาขาวิชาการแปรรูปธุรกิจทางดิจิทัล

วิชาเอกนโยบายและการบริหารดิจิทัล

วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์

ปีการศึกษา 2567

AWARENESS OF CYBER PHISHING SCAMS AMONG GENERATION Z

BY

PHAPADA BUNNAG



A INDEPENDENT STUDY SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE
DIGITAL BUSINESS TRANSFORMATION
DIGITAL POLICY AND MANAGEMENT
COLLEGE OF INNOVATION
THAMMASAT UNIVERSITY
ACADEMIC YEAR 2024

มหาวิทยาลัยธรรมศาสตร์

วิทยาลัยนวัตกรรมการ

การค้นคว้าอิสระ

ของ

ปภาดา บุนนาค

เรื่อง

ความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคนช่วงวัย Gen Z

ได้รับการตรวจสอบและอนุมัติ ให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

วิทยาศาสตรมหาบัณฑิต

เมื่อ วันที่ 2 มิถุนายน พ.ศ. 2568

ประธานกรรมการสอบการค้นคว้าอิสระ

ดร. มานิต สาคิตสมิตพงษ์

(ดร. มานิต สาคิตสมิตพงษ์)

กรรมการและอาจารย์ที่ปรึกษาการค้นคว้าอิสระ

ดร. วศินี หนูนุกัฏ

(ผู้ช่วยศาสตราจารย์ ดร. วศินี หนูนุกัฏ)

คณบดี

ดร. ชัยกฤต อัครวิธานนท์

(ผู้ช่วยศาสตราจารย์ ดร. ชัยกฤต อัครวิธานนท์)

หัวข้อการค้นคว้าอิสระ	ความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคนช่วงวัย Gen Z
ชื่อผู้เขียน	ปภาดา บุณนาค
ชื่อปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา/คณะ/มหาวิทยาลัย	การแปรรูปธุรกิจทางดิจิทัล วิชาเอกนโยบายและการบริหารดิจิทัล วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาการค้นคว้าอิสระ	ผู้ช่วยศาสตราจารย์ ดร. วศินี หนูนักดี
ปีการศึกษา	2567

บทคัดย่อ

การค้นคว้าอิสระนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่มีอิทธิพลต่อความตระหนักรู้เท่าทัน และการระวังภัยการถูกกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z ซึ่งเป็นกลุ่มคนที่ถือว่าเกิดและเติบโตมาพร้อมกับยุคที่เทคโนโลยีมีการพัฒนาอย่างก้าวไกลและไม่หยุดยั้ง งานวิจัยนี้ เป็นงานวิจัยเชิงปริมาณ ดำเนินการเก็บข้อมูลกลุ่มตัวอย่าง Gen Z ทั้งหมด 400 คน ผ่านการแจกแบบสอบถามออนไลน์ และนำข้อมูลที่ได้มาทำการวิเคราะห์ โดยใช้สถิติเชิงพรรณนา ในการหาค่าเฉลี่ย ร้อยละ และส่วนเบี่ยงเบนมาตรฐาน และใช้สถิติเชิงอนุมาน ได้แก่ วิธีการวิเคราะห์สมการถดถอยพหุคูณ หรือ Multiple Regression เพื่อให้ได้มาซึ่งปัจจัยที่ส่งผลและมีอิทธิพลต่อความตระหนักรู้และระวังภัยของกลุ่มตัวอย่าง

ผลการศึกษาพบว่าปัจจัยที่ส่งผลต่อความตระหนักรู้เท่าทันภัยกลลวงหลอกขโมยข้อมูล ได้แก่ ปัจจัยด้านประชากรศาสตร์ (เพศ, ช่วงอายุ) พฤติกรรมการใช้งานช่องทางออนไลน์ด้านการจัดการความเป็นส่วนตัวของช่องทางออนไลน์ พฤติกรรมเกี่ยวกับการป้องกันตัวจากภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ และประสบการณ์การรับรู้เกี่ยวกับกลลวงหลอกขโมยข้อมูลทางไซเบอร์ โดยสามารถทำนายความตระหนักรู้เท่าทันได้อย่างมีนัยสำคัญทางสถิติ และมีค่าความแปรปรวนหรือ Adjusted R Square อยู่ที่ร้อยละ 21

คำสำคัญ: ความตระหนักรู้ด้านความมั่นคงทางไซเบอร์, กลลวงหลอกขโมยข้อมูลทางไซเบอร์, ประสบการณ์และการรับรู้, พฤติกรรมการใช้งาน, กลุ่มคนช่วงวัย Gen Z

Independent Study Title	AWARENESS OF CYBER PHISHING SCAMS AMONG GENERATION Z
Author	Phapada Bunnag
Degree	Master of Science
Department/Faculty/University	Digital Business Transformation Digital Policy and Management College of Innovation Thammasat University
Independent Study Advisor	Assistant Professor Wasinee Noonpakdee, Ph.D.
Academic Year	2024

ABSTRACT

This independent study aims to examine the key factors influencing awareness of cyber phishing scams among Generation Z—a demographic born and raised in an era of rapid and continuous technological advancement. This study employs a quantitative research approach, with data collected from a sample of 400 Gen Z individuals through an online survey. The collected data were analyzed using both descriptive and inferential statistical methods. Descriptive statistics, including mean, percentage, and standard deviation, were used to summarize the findings, inferential statistics, specifically multiple regression analysis, were conducted to identify the factors that significantly influence the awareness and precautionary behaviors of the respondents.

The findings reveal that factors influencing awareness of cyber scams include demographic factors (gender, age group), self-protection behavior against cyber scams, and experience. These factors significantly predict awareness, with an adjusted R-squared value of 21%.

Keywords: Cybersecurity Awareness, Phishing, Experience and Perception, Usage Behavior, Gen Z Demographic

กิตติกรรมประกาศ

ข้าพเจ้าขอขอบพระคุณอาจารย์วศินี หนูนุกัคดี อาจารย์ที่ปรึกษาการค้นคว้าอิสระในครั้งนี้ที่คอยชี้แนะแนวทางในการศึกษาให้แก่ข้าพเจ้ามาเสมอ ท่านเป็นผู้ที่อยู่ข้างข้าพเจ้าตั้งแต่วันแรกที่เราเริ่มทำการศึกษาวิจัยมาจนถึงโค้งสุดท้ายในการพิมพ์เพื่อให้ได้มาซึ่งคำตอบตามสมมติฐานที่ตั้งไว้

การค้นคว้าอิสระครั้งนี้จะไม่สามารถประสบความสำเร็จและเสร็จสิ้นได้หากข้าพเจ้าขาดคำชี้แนะจากเหล่าคุณอาจารย์ ความช่วยเหลือในการกรอกแบบสอบถามของทุกท่าน กำลังใจจากครอบครัวและเพื่อนสนิทรอบตัว รวมไปถึงการสนับสนุนทั้งในทุกเรื่องและทุกเวลาที่ข้าพเจ้าต้องการ

สุดท้ายนี้ ข้าพเจ้าขอขอบคุณตัวของข้าพเจ้าเองที่ตั้งใจ ใส่ใจ และมุ่งมั่นในการศึกษาค้นคว้าจนทำให้การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงได้ในที่สุด หากงานค้นคว้าอิสระในครั้งนี้มีข้อผิดพลาด หรือจุดผิดประการใด ข้าพเจ้าต้องขออภัยมา ณ ที่นี้ด้วย และจะขอน้อมรับทุกคำแนะนำติชม เพื่อปรับปรุงให้ดีขึ้นในครั้งถัด ๆ ไป

ปภาดา บุนนาค

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	(1)
บทคัดย่อภาษาอังกฤษ	(2)
กิตติกรรมประกาศ	(3)
สารบัญตาราง	(6)
สารบัญภาพ	(7)
บทที่ 1 บทนำ	1
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์การวิจัย	3
1.3 ขอบเขตการวิจัย	3
1.4 นิยามศัพท์เฉพาะ	5
1.5 ประโยชน์ที่คาดว่าจะได้รับ	9
บทที่ 2 เอกสารและงานวิจัยที่เกี่ยวข้อง	10
2.1 แนวคิดและทฤษฎีด้านประชากรศาสตร์ (Demographic Characteristics Concept)	10
2.2 แนวคิดเกี่ยวกับ Generation Z และลักษณะของ Generation Z	12
2.3 แนวคิดและทฤษฎีเกี่ยวกับการรับรู้ข่าวสาร	13
2.4 แนวคิดและทฤษฎีเกี่ยวกับความตระหนักรู้และการรับรู้ความเสี่ยง	14
2.5 แนวคิดและทฤษฎีเกี่ยวกับการระงับภัยคุกคามทางไซเบอร์	15
2.6 แนวคิดและทฤษฎีเกี่ยวกับเครือข่ายสังคมออนไลน์	16

2.7 แนวคิดและทฤษฎีเกี่ยวกับกลโกงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing)	17
2.8 แนวคิดทฤษฎีเกี่ยวกับวิศวกรรมสังคม	18
2.9 แนวคิดเกี่ยวกับปัจจัยที่ส่งผลต่อความตระหนักรู้	19
2.10 ผลสรุปแนวคิดและงานวิจัยที่เกี่ยวข้อง	20
 บทที่ 3 วิธีดำเนินการวิจัย	 22
3.1 ประชากรและกลุ่มตัวอย่าง	22
3.2 เครื่องมือที่ใช้ในการรวบรวมข้อมูล	23
3.3 การเก็บรวบรวมข้อมูล	25
3.4 การวิเคราะห์ข้อมูล	25
3.5 สถิติที่ใช้ในการวิเคราะห์ข้อมูล	25
 บทที่ 4 ผลการวิจัยและอภิปรายผล	 26
4.1 ผลการตรวจสอบเครื่องมือที่ใช้ในการวิจัย	27
4.2 ผลการวิจัย	43
4.3 อภิปรายผลการวิจัย	60
 บทที่ 5 สรุปผลการวิจัยและข้อเสนอแนะ	 63
5.1 สรุปผลการวิจัย	64
5.2 ข้อเสนอแนะ	65
 รายการอ้างอิง	 66
 ภาคผนวก	
แบบสอบถามการศึกษา ความตระหนักรู้เท่าทันกลโกงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคนช่วงวัย Gen Z	70

สารบัญตาราง

ตารางที่	หน้า
1.3.1 การจัดเกณฑ์ในการศึกษาประเภทของกลลวงหลอกขอลข้อมูลทางไซเบอร์ (Phishing)	4
2.10 สรุปตัวแปรที่ได้จากการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง	20
4.1.1 แสดงผลการตรวจสอบค่าความเที่ยงตรงของแบบสอบถาม	29
4.2.1.1 ข้อมูลทางประชากรศาสตร์ของกลุ่มตัวอย่าง	43
4.2.1.2 ระดับความรู้เกี่ยวกับกลลวงหลอกขอลข้อมูลทางไซเบอร์ของกลุ่มตัวอย่าง	44
4.2.1.3 ระดับคะแนนพฤติกรรมการระวังภัยกลลวงหลอกขอลข้อมูลทางไซเบอร์ในการใช้งานช่องทางออนไลน์	46
4.2.1.4 ระดับคะแนนประสบการณ์และการรับรู้ในเรื่องของภัยกลลวงหลอกขอลข้อมูลทางไซเบอร์	48
4.2.1.5 ระดับคะแนนความตระหนักรู้เกี่ยวกับกลลวงหลอกขอลข้อมูลทางไซเบอร์	48
4.2.1.6 ข้อเสนอแนะต่อแนวทางการจัดทำข้อมูลสำหรับการป้องกันภัยกลลวงหลอกขอลข้อมูลทางไซเบอร์	50
4.2.2.1.1 ค่าความแปรปรวนของความตระหนักรู้เท่าทัน จำแนกตามตัวแปรเพศ	52
4.2.2.1.2 ค่าความแปรปรวนของความตระหนักรู้เท่าทัน จำแนกตามตัวแปรอายุ	53
4.2.2.1.3 ค่าความแปรปรวนของความตระหนักรู้เท่าทัน จำแนกตามตัวแปรการศึกษา	55
4.2.2.2.1 ผลลัพธ์ในการสรุปรูปแบบสมการถดถอย (Model Summary)	56
4.2.2.2.2 ตาราง ANOVA เพื่อวิเคราะห์ค่าปัจจัยที่มีอิทธิพลต่อความตระหนักรู้เท่าทัน	57
4.2.2.2.3 ตารางการวิเคราะห์ Multiple Regression	58

สารบัญภาพ

ภาพที่	หน้า
1.4.5 ตัวอย่างจดหมายอิเล็กทรอนิกส์ที่มีการแอบอ้างเป็นบริษัทที่มีชื่อเสียงอย่าง PayPal	6
1.4.6 ตัวอย่างจดหมายอิเล็กทรอนิกส์ที่ส่งจากบัญชีของ Faculty of Arts and Science มหาวิทยาลัยฮาวาร์ดที่ถูกแฮคข้อมูล	7
1.4.7 ตัวอย่าง SMS Phishing ที่หลอกขอข้อมูล Apple ID ของผู้ใช้งาน	8



บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ชีวิตประจำวันของคนในยุคปัจจุบันถูกทำให้สะดวกสบายขึ้นโดยการเพิ่มความสามารถในการจัดการเรื่องราวต่าง ๆ ผ่านช่องทางออนไลน์ พฤติกรรมของคนคุ้นชินกับการติดต่อผ่าน Social Media, การสืบค้นคว้าข้อมูลต่าง ๆ เพื่อการศึกษา, การทำธุรกิจซื้อขายแลกเปลี่ยนสินค้า, การประชาสัมพันธ์โฆษณา หรือการทำธุรกรรมทางการเงิน เป็นต้น ด้วยเหตุนี้เองทำให้ในหนึ่งวันมีข้อมูลจำนวนมหาศาลที่ถูกส่งผ่านอยู่ในโลกออนไลน์ ทั้งข้อมูลที่เป็นข้อความ ข้อมูลรูปภาพ ข้อมูลเสียง และข้อมูลตัวเลข ข้อมูลเหล่านี้ครอบคลุมในทุก ๆ เรื่องของเหล่าผู้ใช้งานไม่แม้กระทั่งข้อมูลส่วนบุคคล ซึ่งเป็นข้อมูลต่าง ๆ ที่จะสามารถระบุไปยังตัวตนของบุคคลผู้นั้นได้ ไม่ว่าจะเป็นทางตรงหรือทางอ้อม อย่างชื่อนามสกุล ที่อยู่ อีเมล เบอร์โทรศัพท์ วันเดือนปีที่เกิด สัญชาติ ข้อมูลระบุทรัพย์สินส่วนบุคคล หรือรหัสตัวเลขที่สามารถอ้างอิงถึงเจ้าของข้อมูลนั้น ๆ ได้ และยังมีข้อมูลส่วนบุคคลที่มีความอ่อนไหว กล่าวคือเป็นข้อมูลที่มีความเสี่ยงต่อการถูกนำไปใช้ในทางที่ไม่เหมาะสมได้ เช่น ความคิดเห็น ข้อมูลเกี่ยวกับพฤติกรรมของบุคคล หรือข้อมูลสุขภาพ จากช่องโหว่ของความปลอดภัยระมัดระวังในการปกป้องข้อมูลส่วนตัวของบุคคลหรือการรู้ไม่เท่าทันกลโกงรูปแบบต่าง ๆ ที่มีความใกล้เคียง อาจเป็นช่องทางที่ทำให้กลุ่มผู้ไม่ประสงค์ดี (Phisher) เล็งเห็นช่องว่างที่จะใช้กลวิธีในการหลอกล่อเพื่อให้ได้มาซึ่งข้อมูลและนำเอาข้อมูลเหล่านั้นไปใช้ประโยชน์ในทางที่ไม่เหมาะสมได้ โดยวิธีในการหลอกล่อเพื่อให้ได้มาซึ่งข้อมูลสามารถทำได้หลากหลายวิธี ได้แก่ การหลอกล่อผ่านการใช้ช่องทางจดหมายอิเล็กทรอนิกส์ (E-mail), หลอกล่อโดยเจาะจงเฉพาะที่ตัวบุคคลหรือองค์กร, หลอกล่อข้อมูลจากผู้บริหารระดับสูง, หลอกล่อขอข้อมูลผ่านทางโทรศัพท์, หลอกล่อขอข้อมูลผ่านทาง Social Media, หลอกล่อผ่านการแจ้งเตือนทาง Website ต่าง ๆ, หลอกล่อผ่านทาง Wi-Fi Hotspot หรือการหลอกล่อโดยแอบอ้างเป็นองค์กรหรือบุคคลที่มีชื่อเสียงและมีความน่าเชื่อถือ ซึ่งเห็นได้ว่าแต่ละช่องทางเป็นช่องทางที่เป็นส่วนหนึ่งของกิจกรรมในชีวิตประจำวันของผู้ใช้งานออนไลน์ทั่วไป หากบุคคลนั้น ๆ ไม่มีความตระหนักรู้เท่าทัน ไม่เห็นความสำคัญของการเก็บรักษาข้อมูลส่วนบุคคลและยังมีพฤติกรรมเคยชินบางอย่างที่เป็นจุดอ่อนก็อาจเกิดจุดเอื้อประโยชน์ให้กลุ่มผู้ไม่หวังดีเหล่านี้ทำงานได้อย่างสะดวกง่ายดายมากยิ่งขึ้น

ประชากรที่เกิดในช่วงปีพ.ศ.2540-2555 ถูกเรียกว่าเป็นคนในยุคช่วงวัย Gen Z ซึ่งถือเป็น Generation ที่เกิดมาพร้อมกับความแพร่หลายของอินเทอร์เน็ตรวมถึงเป็นยุคที่เทคโนโลยีต่าง ๆ ถูกพัฒนาขึ้นอย่างต่อเนื่อง พวกเขาส่วนมากมองว่าเทคโนโลยีและอินเทอร์เน็ตถือเป็นส่วนประกอบสำคัญส่วนหลักในชีวิต เนื่องจากทุกคนสามารถที่จะเข้าถึงข้อมูลทุกอย่างจากเพียงปลายนิ้วมือ สามารถติดต่อสื่อสารกันได้ง่ายดายผ่านการยกหูโทรศัพท์ หรือแม้กระทั่งสามารถทำกิจกรรมและธุรกรรมต่าง ๆ ผ่านช่องทางออนไลน์ได้อย่างไม่จำกัด (Philip Kotler, 2564) ดังนั้นจึงไม่ใช่เรื่องแปลกหากจะกล่าวว่าคนในช่วงวัยนี้ค่อนข้างมีความคุ้นเคยกับเทคโนโลยีเป็นอย่างมาก หากเทียบกับช่วงวัยอื่น ๆ จึงก่อให้เกิดแนวคิดสำคัญในการศึกษาวิจัยเรื่องนี้ว่า คนที่เกิดในช่วง Gen Z ซึ่งมีความคุ้นเคยกับเทคโนโลยีเป็นอย่างดีจนเรียกได้ว่าเป็นกลุ่มคนที่เกิดมาพร้อมกับโลกที่มีอินเทอร์เน็ตและเทคโนโลยีอยู่แล้วนั้นมีลักษณะพฤติกรรมในการใช้งานเทคโนโลยีในชีวิตประจำวันและมีประสบการณ์ รวมถึงข้อมูลความรู้เท่าทันต่อภัยไซเบอร์เป็นอย่างไร ท้ายที่สุดแล้ว พฤติกรรมเหล่านี้ส่งผลต่อการตระหนักรู้เท่าทันกลลวงหลอกขอลข้อมูลทางไซเบอร์สำหรับคนในช่วงวัย Gen Z ให้มีการระวังตัวที่จะไม่โดนหลอกนำเอาข้อมูลไปใช้ในทางที่ไม่ดีมากนักน้อยเพียงใด ทั้งนี้ยังสามารถนำเอาข้อมูลที่ได้เหล่านี้มาวิเคราะห์ถึงแนวทางในการป้องกันภัยกลลวงหลอกขอลข้อมูลทางไซเบอร์ (Phishing) ได้อย่างมีประสิทธิภาพมากขึ้นในอนาคต

1.2 วัตถุประสงค์การวิจัย

การศึกษาวิจัยครั้งนี้ มีวัตถุประสงค์ในการวิจัย ดังนี้

1.2.1 เพื่อศึกษาปัจจัยและอิทธิพลที่เกี่ยวกับการตระหนักรู้เท่าทันและระวังภัยการใช้กลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) กรณีศึกษา กลุ่มคนช่วงวัย Gen Z

1.2.2 เพื่อเสนอแนะแนวทางและรูปแบบในการจัดทำข้อมูลในการป้องกันภัยจากการใช้กลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ในอนาคตที่มีประสิทธิภาพต่อการรับรู้และสร้างความตระหนักให้คนในสังคมได้มากยิ่งขึ้น

1.3 ขอบเขตการวิจัย

การศึกษาวิจัยครั้งนี้ มีขอบเขตในการวิจัย ดังนี้

1.3.1 ขอบเขตด้านเนื้อหา

ผู้วิจัยมีความต้องการศึกษา ความตระหนักรู้เท่าทันและระวังภัยการใช้กลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) โดยจะทำการศึกษากลโกงทางไซเบอร์ทั้งหมด 5 ประเภท ได้แก่

- E-mail Phishing หรือการหลอกลวงขโมยข้อมูลทางอีเมล
- Spear Phishing หรือการหลอกลวงขโมยข้อมูลโดยเจาะจงไปที่ตัวบุคคลหรือองค์กรโดยตรง
- Smishing Phishing หรือการหลอกลวงขโมยข้อมูลทางข้อความโทรศัพท์
- Vishing Phishing หรือการหลอกลวงขโมยข้อมูลผ่านการโทรศัพท์
- Angler Phishing หรือการหลอกลวงขโมยข้อมูลทาง social media

โดยมีเกณฑ์ในการเลือกหัวข้อของกลลวงหลอกขอข้อมูล (Phishing) ที่กลุ่ม
กรณีศึกษาจะได้พบบ่อยในชีวิตประจำวันดังต่อไปนี้

ตารางที่ 1.3.1 การจัดเกณฑ์ในการศึกษาประเภทของกลลวงหลอกขอข้อมูลทางไซเบอร์ (Phishing)

ประเภทของกลลวง หลอกขอข้อมูล (Phishing)	กลุ่มเป้าหมายที่ต้องการ โจมตี	ช่องทางการโจมตี
E-mail Phishing	กลุ่มบุคคล	ผ่านทางอีเมลส่วนตัว
Spear Phishing	กลุ่มบุคคลใดบุคคลหนึ่ง	ผ่านทางอีเมลองค์กรหรือส่วนตัว
Smishing Phishing	บุคคล	ผ่านทางข้อความทางโทรศัพท์ส่วนตัว
Vishing Phishing	บุคคล	ผ่านทางโทรศัพท์ส่วนตัว
Angler Phishing	บุคคล	ผ่านทางโซเชียลมีเดียส่วนตัว
Search Engine Phishing	บุคคล	ผ่านทาง SEO
Whaling Phishing	บุคคลระดับสูง	ผ่านทางอีเมล
CEO Fraud Phishing	บุคคลระดับสูง	ผ่านทางอีเมล
Web Phishing	บุคคล	เว็บไซต์ที่เป็นสแปม

1.3.2 ของเขตด้านระยะเวลา

ผู้วิจัยมีระยะเวลาในการเก็บและรวบรวมข้อมูลเป็นระยะเวลาทั้งสิ้น 3 เดือน ตั้งแต่
เดือนธันวาคม – กุมภาพันธ์

1.3.3 ขอบเขตด้านพื้นที่

ผู้วิจัยมุ่งเน้นศึกษาไปที่ประชากรที่มีอายุระหว่าง 18-28 ปี หรือผู้ที่เกิดอยู่ในช่วง
พ.ศ.2540 – 2550 อาศัยอยู่ในประเทศไทย

1.4 นิยามศัพท์เฉพาะ

การศึกษาวิจัยครั้งนี้ มีนิยามศัพท์เฉพาะ ดังนี้

1.4.1 การตระหนักรู้เท่าทัน

การรับรู้ในระดับความรู้สึกก็นึกคิดและการให้ความสนใจต่อประเด็นใดประเด็นหนึ่งที่
ต้องการศึกษา

1.4.2 การระวังภัย

การตอบสนองต่อการคิดค้นหาวิธีการที่จะเป็นการปกป้องตนเองจากสถานการณ์ที่อาจ
ส่งผลกระทบที่ไม่ดีต่อตัวบุคคล

1.4.3 กลุ่มคนช่วงวัย Gen Z

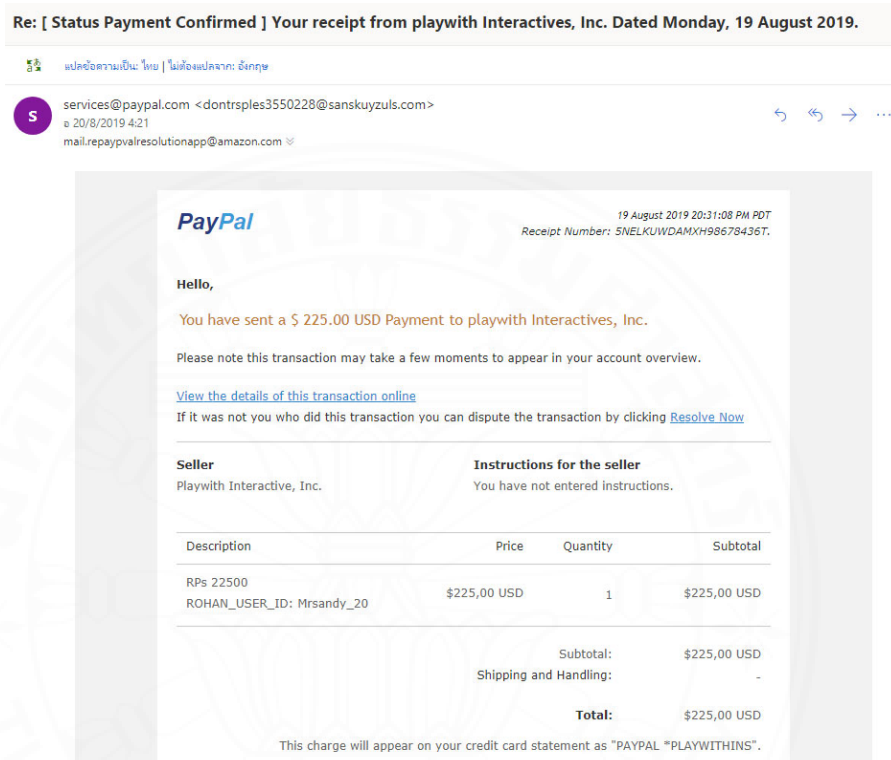
ประชากรที่เกิดในปีพ.ศ.2540-2550 หรือมีอายุตั้งแต่ 18-28 ปี

1.4.4 กลลวงหลอกขอลข้อมูล (Phishing)

หนึ่งในรูปแบบของการใช้วิธีต่าง ๆ ปลอมแปลงหรือแอบอ้างเพื่อหลอกลวงให้บุคคลเกิด
ความหลงเชื่อและทำให้ได้มาซึ่งข้อมูลส่วนบุคคลของบุคคลใดบุคคลหนึ่ง และนำเอาข้อมูล
ส่วนบุคคลเหล่านั้นไปใช้ในทางที่ไม่เหมาะสมซึ่งอาจก่อให้เกิดผลกระทบต่อเจ้าของข้อมูลได้
ไม่ว่าทั้งด้านความเป็นส่วนตัว ด้านผลกระทบทางการเงิน หรือ ด้านความปลอดภัย เป็นต้น

1.4.5 Email Phishing

รูปแบบการหลอกลวงโดยการส่งจดหมายอิเล็กทรอนิกส์ไปยังหลายผู้ใช้งานไม่ได้มีการเจาะจงเป็นพิเศษเพื่อหวังให้ผู้ใช้งานเชื่อและทำการคลิกลิงก์หรือทำการดาวน์โหลดไฟล์ดังกล่าวที่มีความอันตรายต่อข้อมูลส่วนบุคคล

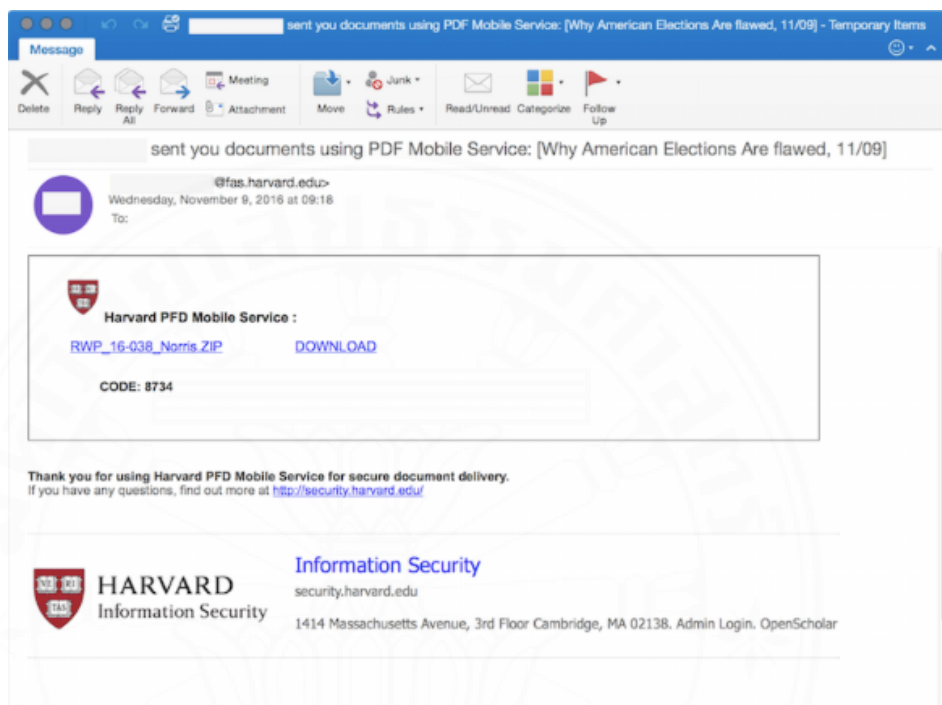


ภาพที่ 1.4.5 : ตัวอย่างจดหมายอิเล็กทรอนิกส์ที่มีการแอบอ้างเป็นบริษัทที่มีชื่อเสียงอย่าง PayPal

ที่มา : บทความเรื่อง “Phishing คืออะไร ป้องกันอย่างไร” (บรรณศักดิ์ ยุวมิตร, 2563)

1.4.6 Spear Phishing

รูปแบบการหลอกลวงที่ส่งจดหมายอิเล็กทรอนิกส์แบบมุ่งเป้าหมายที่ตัวบุคคลโดยเฉพาะ อาจแอบอ้างเป็นคนที่รู้จักหรือมีการระบุข้อมูลส่วนตัวบางอย่างของบุคคลเพื่อให้เกิดความน่าเชื่อถือ



ภาพที่ 1.4.6 : ตัวอย่างจดหมายอิเล็กทรอนิกส์ที่ส่งจากบัญชีของ Faculty of Arts and Sciences

มหาวิทยาลัยฮาร์วาร์ดที่ถูกแฮคข้อมูล

ที่มา : บทความเรื่อง “กลุ่มอาชญากรไซเบอร์เริ่มแคมเปญ SPEAR-PHISHING หลังทรัมป์รับเลือกเป็นประธานาธิบดี” (Techtalkthai,2559)

1.4.7 Smishing phishing

รูปแบบการหลอกลวงโดยใช้กลวิธีการโจมตีผ่านทางข้อความ SMS โดยหวังให้บุคคลกดลิงค์ที่มีการแนบมากับตัวเนื้อหา



1.4.8 Vishing phishing

รูปแบบการหลอกลวงโดยใช้กลวิธีผ่านทางโทรศัพท์เพื่อทำการสอบถามข้อมูลส่วนตัว อาจใช้การโทรศัพท์โดยแอบอ้างว่าตนเองเป็นเจ้าของหน้าที่หรือคนรู้จักของคุณ

1.4.9 Angler Phishing

รูปแบบการหลอกลวงแบบที่จะมีการเฝ้าจับตามองพฤติกรรมของคุณจากการใช้งาน Social Media ต่าง ๆ เพื่อให้ได้มาซึ่งข้อมูลของคุณและนำมาเป็นข้อมูลในการพูดคุยเพื่อหลอกล่อขอข้อมูลของคุณ

1.4.10 กลุ่มผู้ไม่ประสงค์ดี (Phisher)

กลุ่มบุคคลที่ใช้โอกาสและช่องโหว่ทางโลกออนไลน์ในการใช้กลวิธีการหลอกลวงบุคคล เพื่อให้ได้มาซึ่งข้อมูลต่าง ๆ และนำเอาข้อมูลเหล่านั้นไปใช้ในทางไม่เหมาะสม

1.5 ประโยชน์ที่คาดว่าจะได้รับ

การศึกษาวิจัยครั้งนี้ มีประโยชน์ที่คาดว่าจะได้รับ ดังนี้

1.5.1 ทำให้เกิดความรู้และความเข้าใจเกี่ยวกับประเด็นหลักคือความตระหนักรู้เรื่องของ
กลโกงจากโลกไซเบอร์

1.5.2 สามารถสรุปแนวทาง วิธีการป้องกันรวมถึงการลดอัตราความเสี่ยงในการถูก
หลอกลวงขอข้อมูลในอนาคตได้มากขึ้น

บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

การศึกษาวิจัยเรื่อง “ความตระหนักรู้เท่าทันกลลวงหลอกลวงขอข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคนช่วงวัย Gen Z” ได้มีการศึกษาค้นคว้าข้อมูลโดยที่ผู้จัดทำได้ทำการศึกษารวบรวมแนวคิด หลักการทฤษฎี และงานวิจัยที่เกี่ยวข้องกับหัวข้อ ดังต่อไปนี้

2.1 แนวคิดและทฤษฎีด้านประชากรศาสตร์ (Demographic Characteristics Concept)

กอบกาญจน์ เจริญทอง (2556) ได้กล่าวถึงแนวคิดและทฤษฎีด้านประชากรศาสตร์ว่า หมายถึง ศาสตร์ที่ศึกษาเกี่ยวข้องกับประชากรเป็นหลัก โดยนำเอาคำศัพท์ว่า “Demo” หมายถึง ประชากร รวมกับคำว่า “Graphy” ซึ่งมีความหมายเกี่ยวกับ ลักษณะ ดังนั้นเมื่อทั้งสองคำนำมารวมกันจะได้ความหมายเกี่ยวกับ การศึกษาข้อมูลต่าง ๆ ที่มีความเกี่ยวข้องกับประเด็นของประชากร อันได้แก่ ปัจจัยอายุ เพศ การศึกษา สถานภาพทางสังคม อาชีพ รายได้ หรือเชื้อชาติ เป็นต้น

ยุบล เบ็ญจรงค์กิจ (2543) ได้กล่าวไว้ว่า ทฤษฎีประชากรศาสตร์คือแนวคิดที่ประกอบไปด้วยปัจจัยต่าง ๆ ได้แก่ อายุ เพศ การศึกษา สถานะทางสังคม และอื่น ๆ โดยถ้าประชากรมีความแตกต่างกันก็สามารถที่จะส่งผลไปยังพฤติกรรมหรือการรับรู้เรื่องต่าง ๆ ที่แตกต่างกันอีกด้วย

ศิริวรรณ เสรีรัตน์ (2538) ได้ให้ความหมายของ ลักษณะทางประชากรศาสตร์ ไว้ว่า ประกอบไปด้วย อายุ เพศ การศึกษา ลักษณะของครอบครัว เงินเดือน รายได้ โดยองค์ประกอบปัจจัยเหล่านี้มักจะถูกนำมาใช้เป็นเกณฑ์ส่วนแบ่งทางการตลาด เนื่องจากลักษณะของประชากรที่แตกต่างกันย่อมมีอิทธิพลต่อการกำหนดกลุ่มของประชากรที่มีความแตกต่างกันในด้านของความรู้สึกนึกคิด พฤติกรรม ความสนใจ และลักษณะทางจิตวิทยา ที่ง่ายต่อการวัดผลมากกว่าตัวแปรอื่น ๆ โดยปัจจัยของตัวแปรด้านประชากรศาสตร์ที่มีความสำคัญ ได้แก่

- เพศ เป็นตัวแปรที่สามารถส่งผลให้เกิดความแตกต่างไม่เหมือนกันของพฤติกรรมในการรับสารประเด็นต่าง ๆ หรือการตระหนักรู้คิดในประเด็นต่าง ๆ ได้นอกจากแต่ละเพศที่มีความแตกต่างในแง่ของกายภาพแล้ว ก็ยังมีปัจจัยอื่น ๆ อย่างค่านิยม ทัศนคติส่วนตัว การอบรมเลี้ยงดู หรือกรอบแนวคิดที่สังคมวัฒนธรรมได้กำหนดบทบาทที่แตกต่างกันเอาไว้

- อายุ การที่ประชากรมีอายุแตกต่างกันก็สามารถส่งผลให้การตอบสนอง ความต้องการ หรือ แนวความคิดของแต่ละช่วงวัยมีความแตกต่างกันออกไป เนื่องจากแต่ละยุคสมัยกลุ่มคนในแต่ละช่วงวัยก็ได้รับการเติบโตเลี้ยงดูปลูกฝังมาจากสภาพแวดล้อมทางสังคมที่มีความแตกต่างกัน ชุดความคิด ทักษะของแต่ละช่วงวัยก็ย่อมแตกต่างกันตามไปด้วยเช่นกัน
- รายได้ เงินเดือน อาชีพ ถือเป็นปัจจัยสำคัญในการกำหนดและจำแนกกลุ่มของประชากร เนื่องจากปัจจัยเหล่านี้มีผลกระทบต่อพฤติกรรม รูปแบบในการดำเนินชีวิต รสนิยม การเสพ ข้อมูลข่าวสารที่แตกต่างกันออกไป
- ระดับการศึกษา การศึกษาที่แตกต่างกันจะส่งผลต่อความคิดและพฤติกรรม รวมถึงการรับมือกับสถานการณ์ต่าง ๆ ได้ต่างกัน บุคคลที่มีระดับการศึกษาที่สูงอาจมีโอกาสนในการเปิดกว้างทางการรับรู้ข้อมูลในประเด็นต่าง ๆ ได้มากกว่า

จากแนวคิดและทฤษฎีเกี่ยวกับประชากรศาสตร์สามารถสรุปได้ว่าปัจจัยต่าง ๆ ที่แตกต่างกันออกไปย่อมมีผลต่อพฤติกรรม ความคิดอ่าน และการรับมือกับสถานการณ์ที่ต่างกันไปด้วย ดังนั้นผู้ศึกษาจึงมีความสนใจที่จะศึกษาลักษณะของประชากรศาสตร์ในประเด็นของ เพศ อายุ และการศึกษาเป็นหลัก เนื่องจากกลุ่มเป้าหมายของงานวิจัยฉบับนี้เป็นกลุ่มคนในช่วงวัย Gen Z มีความน่าจะเป็นที่จะได้รับการปลูกฝังข้อมูลเนื้อหาทางด้านเทคโนโลยี โลกไซเบอร์มาเป็นอย่างดี

2.2 แนวคิดเกี่ยวกับ Generation Z และลักษณะของ Generation Z

Mannheim (2495) และ Zemke (2554) ได้มีแนวคิดที่สอดคล้องกันเกี่ยวกับหัวข้อของการกำหนดและแบ่งแยกบุคคลตามช่วงอายุ โดยเสนอว่า การที่จะแบ่งคนออกเป็นกลุ่มตามช่วงวัยจะต้องมีปัจจัยในการแบ่ง ได้แก่ ลักษณะทางประชากรศาสตร์และประสบการณ์ที่คนในช่วงวัยนั้น ๆ ได้ประสบพบเจอร่วมกันมา ปัจจัยเหล่านี้จะเป็นสิ่งที่ทำให้คนในแต่ละกลุ่มมีความแตกต่างกันออกไปในเรื่องของ ความคิด ทักษะ มุมมองต่อเรื่องราวต่างๆ จึงก่อให้เกิดพฤติกรรมร่วมในกลุ่มคนที่มีอายุใกล้เคียงกันเช่นเดียวกับ Glass (2550) ได้กล่าวว่ากลุ่มคนช่วงวัย Generation Z คือบุคคลที่เกิดระหว่างปี พ.ศ.2540-2555 โดยจะมีอายุอยู่ระหว่าง 13-28 ปี คนกลุ่มช่วงวัยนี้ถือกำเนิดมาพร้อมๆกับโลกที่มีการพัฒนาด้านเทคโนโลยีที่ก้าวหน้าอย่างต่อเนื่อง ส่งผลให้กลุ่มคน Generation Z มีความใกล้ชิดกับการใช้งานเทคโนโลยีในชีวิตประจำวันเป็นทุนเดิมและสามารถวิ่งตามกระแสการพัฒนาเทคโนโลยีใหม่ ๆ ได้อย่างรวดเร็ว Howe & Strauss (2551)

คณัญญา อิมใจ (2565) ได้กล่าวว่า ด้วยความที่ Generation Z เป็นกลุ่มคนที่เกิดมาในโลกยุคที่เทคโนโลยีมีความก้าวหน้าและมีการพัฒนาอย่างเปิดกว้าง จึงส่งผลให้คนกลุ่มนี้มีลักษณะเฉพาะที่แตกต่างจากกลุ่มคนจาก Generation อื่นๆ กล่าวคือ เป็นกลุ่มคนที่ให้ความสำคัญกับเทคโนโลยีเป็นอย่างมากและไม่สามารถใช้ชีวิตโดยที่ไม่มีเทคโนโลยีได้ ทำให้คนกลุ่มนี้ต้องวิ่งตามการพัฒนาใหม่ๆ อยู่เสมอ ต้องการความรวดเร็วในการรับรู้ข้อมูลหรือข่าวสาร ต้องการที่จะแบ่งปันข้อมูลทั้งความชอบ หรือกิจวัตรประจำวันของตนเองผ่านทางโลกโซเชียลมีเดียเพื่อสื่อสารพูดคุยกับผู้อื่นอยู่ตลอดเวลา เป็นกลุ่มคนที่ใช้เวลาอยู่กับโลกอินเทอร์เน็ตต่อวันค่อนข้างมากโดยเฉลี่ย 6-8 ชั่วโมง จากการที่ชีวิตเกือบแทบทุกมิติอยู่ในโลกออนไลน์ทำให้คนกลุ่มนี้มีความจำเป็นจะต้องแชร์ข้อมูลส่วนตัวของตนเองลงในช่องทางต่างๆ อยู่ตลอดจึงอาจเป็นเหตุให้เกิดความละเลยในการระวังตัว รวมถึงมีความเสี่ยงสูงในการถูกภัยคุกคามจากผู้อื่นในโลกออนไลน์ได้ง่าย

2.3 แนวคิดและทฤษฎีเกี่ยวกับการรับรู้ข่าวสาร

Charles k. Atkin (1973) ได้กล่าวว่าผู้ที่มีการเปิดรับข่าวสารในจำนวนมาก จะเป็นผู้ที่มีความรู้กว้างขวาง มีความเข้าใจสถานการณ์และสภาพแวดล้อมเป็นอย่างดี และย่อมมีความทันสมัยมากกว่าผู้ที่ไม่รับข้อมูลข่าวสารใดแต่อย่างไกรก็ตาม โดยธรรมชาติของบุคคลแล้วจะเลือกรับเฉพาะข่าวสารหรือข้อมูลที่คิดว่ามีความสำคัญและมีประโยชน์ต่อส่วนตนเท่านั้น ไม่ได้รับข้อมูลทั้งหมดที่ผ่านเข้ามา โดยข้อมูลต่าง ๆ ที่หมุนเวียนอยู่รายล้อมตัวเราจะถูกนำเข้ากระบวนการคัดเลือกอยู่ตลอดเวลา ให้มีความตอบสนองต่อความอยากรู้และมีความเหมาะสมตามความรู้สึกนึกคิดของผู้รับ กล่าวโดย กิติมา สุรสนธิ (2533) และกระบวนการในการคัดเลือกข้อมูลข่าวสารของบุคคลนั้นย่อมมีความแตกต่างกันไปตามปัจจัยส่วนตัวหรือปัจจัยด้านจิตวิทยา โดย Klapper, J.T. (1960) ได้กล่าวว่า กระบวนการดังกล่าวจะประกอบไปด้วย 4 ขั้นตอนดังนี้

- การเปิดรับ (Selective Exposure) บุคคลจะมีทางเลือกในการเลือกเปิดรับข้อมูลและข่าวสารต่าง ๆ จากหลายแหล่งที่มา โดยยึดตามความสนใจและทักษะความชำนาญในการใช้ช่องทางนั้น ๆ
- การเลือกให้ความสนใจ (Selective Attention) บุคคลจะเลือกทุ่มความสนใจไปยังข้อมูลข่าวสารจากแหล่งใดแหล่งหนึ่งตามความเห็น ทศนคติส่วนตัวของตนเองเพื่อให้ได้รับข้อมูลที่มาสสนับสนุนแนวคิดเดิมและเพื่อไม่ให้เกิดความไม่สอดคล้องทางความเข้าใจหรือความไม่สะดวกใจในการรับรู้
- การเลือกรับรู้และตีความหมาย (Selective Perception and Interpretation) แต่ละบุคคลจะตีความข้อมูลที่ได้รับแตกต่างกันออกไปตามลักษณะส่วนตัว และอาจมีการบิดเบือนเนื้อหาบางส่วนเพื่อให้ตอบสนองต่อความพอใจส่วนบุคคลในการรับรู้อีกด้วย
- การเลือกจดจำ (Selective Retention) บุคคลจะเลือกจดจำข้อมูลข่าวสารแค่เพียงเฉพาะในส่วนที่ตนเองมีความสนใจและสนับสนุนกับแนวคิดดั้งเดิมของตนที่มี

ขวัญเรือน กิติวัดน์ (2531) และ Wilbur Schramm (1973) ได้กล่าวว่าปัจจัยและองค์ประกอบทางสังคมต่าง ๆ ไม่ว่าจะเป็น เพศ อายุ อาชีพ การศึกษา สภาพแวดล้อม รวมถึงภูมิหลังที่แตกต่างกัน มีอิทธิพลต่อเนื้อหาของข้อมูลข่าวสารที่แตกต่างกัน ความสามารถในการรับรู้ที่แตกต่างกัน และประสิทธิภาพในการประเมินสาระประโยชน์จากข่าวสารข้อมูลนั้น ๆ ได้อย่างแตกต่างกัน

2.4 แนวคิดและทฤษฎีเกี่ยวกับความตระหนักและการรับรู้ความเสี่ยง

Schiffman & Kanuk (2000) ได้ให้คำจำกัดความของความตระหนักรู้ไว้ว่า เป็นกระบวนการที่แต่ละบุคคลจะมีการคิดสรรและตีความความหมายของสิ่งต่าง ๆ ออกมา

นวลศิริ เปาโรหิตย์ (2532) ได้กล่าวว่า การตระหนักรู้เป็นวิธีลำดับขั้นตอนในการแปลความหมายของสิ่งที่มากระทบต่อประสาทสัมผัสของบุคคล และในการตีความออกมาจะขึ้นอยู่กับประสบการณ์และปัจจัยด้านจิตวิทยาของแต่ละบุคคล

บรรยงค์ โตจินดา (2543) ได้ให้ความหมายของการรับรู้ไว้ว่า เมื่อใดก็ตามที่บุคคลได้ทำการแปลความหมายและสร้างปฏิกิริยาตอบโต้ต่อสถานการณ์ที่เกิดขึ้น การรับรู้นั้นจะสามารถเกิดขึ้นโดยการเห็น ได้ยิน หรือการทำและผนวกกับการคิดวิเคราะห์ถอดความหมายออกมาทำให้เกิดการเรียนรู้ในตอนท้าย

ศิริวรรณ เสรีรัตน์และคณะ (2541) ได้กล่าวถึงขั้นตอนในการรับรู้หรือ Perception Process โดยมีการแบ่งออกเป็น 4 ลำดับ ได้แก่

- การเปิดรับข้อมูล (Information Exposure) คือการที่บุคคลเปิดกว้างที่จะรับข้อมูลเข้ามา
- การตั้งรับข้อมูล (Information Attention) คือการที่เลือกสรรข้อมูลเฉพาะในส่วนที่ตนเองสนใจ
- การตีความข้อมูล (Information Interpretation) ขั้นตอนนี้จะขึ้นอยู่กับทัศนคติ ประสบการณ์ที่ผ่านมาในอดีต หรือความรู้สึกนึกคิดของแต่ละคน ในการที่ได้รับข้อมูลเรื่องเดียวกันบางคนอาจทำการตีความหมายออกมาในรูปแบบที่ไม่เหมือนกันก็ย่อมเป็นไปได้
- การเก็บรักษาข้อมูล (Information Retention) เกิดสุดท้ายหลังจากที่บุคคลได้รับข้อมูลนั้น ๆ เรียบร้อยแล้ว โดยบุคคลจะเลือกทำการจดจำข้อมูลไว้เพียงบางส่วนเท่านั้น

Cunningham (1967) ได้กล่าวถึงการรับรู้ความเสี่ยงว่า คือความไม่แน่นอนที่บุคคลสามารถรับรู้ได้ว่าอาจจะเกิดขึ้นกับสถานการณ์นั้น ๆ ได้ โดยเรื่องนั้นอาจก่อให้เกิดผลกระทบในเชิงลบต่อการใช้งาน

Heng, Hock-Hai & Bernard (2005) ได้กล่าวว่า การรับรู้ความเสี่ยงสามารถถูกแบ่งออกเป็น 4 ด้าน ได้แก่ ด้านเศรษฐกิจ, ด้านการกระทำ, ด้านบุคคล และด้านความเป็นส่วนตัว

Martin & Camarero (2008) ได้กล่าวถึงการรับรู้ความเสี่ยงว่าขึ้นอยู่กับการศึกษาความมั่นคงปลอดภัยของข้อมูลส่วนตัวของบุคคลให้เหมาะสม หากทำได้จะทำให้ความเสี่ยงเหล่านั้นมีอัตราเกิดที่ต่ำลง

2.5 แนวคิดและทฤษฎีเกี่ยวกับการระงับภัยคุกคามทางไซเบอร์

ยรรยงวรกร ทองแย้ม (2563) ได้กล่าวว่าเป็นเรื่องจำเป็นอย่างยิ่งที่จะต้องมีการสร้างความตระหนักในการใช้ช่องทางออนไลน์เพื่อให้บุคคลเกิดพฤติกรรมที่สามารถช่วยลดอัตราความเสี่ยงและสามารถช่วยเพิ่มความฉลาดทางดิจิทัลให้กับผู้ใช้งานได้มากขึ้น กล่าวคือหากบุคคลใดที่มีการระแวดระวังกับประเด็นของภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้ก็ย่อมส่งเสริมให้บุคคลผู้นั้นมีทักษะการป้องกันตัวจากภัยคุกคามออนไลน์ มีการคิดวิเคราะห์ในการบริหารจัดการข้อมูลส่วนตัว และมีการยกระดับทักษะในการรักษาความปลอดภัยของตนเองเมื่อใช้งานโลกออนไลน์อยู่เสมอ รวมไปถึงปัจจัยที่อาจช่วยกระตุ้นการรู้เท่าทันได้ ได้แก่ อิทธิพลจากครอบครัวและข่าวสารต่าง ๆ ที่ถูกคัดกรองแล้ว

สุภิญญา กลางณรงค์ และ ผศ. ดร.ณภัทร เรืองนภากุล (2564) ได้กล่าวว่าประชากรในยุคปัจจุบันที่ถือเป็นยุคของการขับเคลื่อนด้วยดิจิทัลจำเป็นที่จะต้องมีความรู้ของพลเมืองยุคดิจิทัล โดยเฉพาะในเรื่องของการรู้เท่าทันภัยทางโลกออนไลน์และสามารถระมัดระวังระดับคุณภาพชีวิตและช่วยให้ตนเองรับมือกับภัยร้ายเหล่านั้นได้ท่ามกลางสังคมที่เต็มไปด้วยการแพร่กระจายของข้อมูลข่าวสารในจำนวนมหาศาลอย่างไม่หยุดนิ่ง การตั้งใจที่จะบิดเบือนข้อมูลเพื่อให้เกิดความเชื่อใจและหลงเชื่อ ถือว่าเป็นเรื่องที่ใกล้ตัวทุกคนในสังคมมากและหากขาดความรู้หรือทักษะในการดูแลป้องกันตัวเองที่ดีมากพอจะเป็นการเปิดช่องว่างให้ผู้ประสงค์ร้ายใช้พื้นที่นี้ในการเล่นงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

จิตสุภา ฤทธิผลิน (2564) ได้กล่าวว่าการที่มีทักษะและมีการเตรียมความพร้อมในการที่จะรับมือกับสถานการณ์ต่าง ๆ ที่อาจจะเกิดขึ้นทางโลกไซเบอร์ เรียนรู้ที่จะมีวิธีแก้ไขหรือเยียวยาจากสถานการณ์นั้น ๆ เรียกได้ว่าเป็นกระบวนการคืนสภาพได้ทางไซเบอร์ โดยลักษณะเด่นที่สำคัญควรมีความคล่องตัวและมีความทนทานต่อภัยคุกคามต่าง ๆ เพราะจะทำให้เกิดการตอบสนองต่อการระงับภัยทางไซเบอร์ได้อย่างดีและมีประสิทธิภาพมากยิ่งขึ้น

2.6 แนวคิดและทฤษฎีเกี่ยวกับเครือข่ายสังคมออนไลน์

ภิเชก ชัยนิรันดร์ (2553) ได้ทำการกำหนดความหมายและจำแนกประเภทของสื่อสังคมออนไลน์ ว่าเป็นสังคมที่อยู่บนแพลตฟอร์มออนไลน์และในการปฏิสัมพันธ์เชิงสังคมภายในเครือข่ายจะใช้ social media ที่อาจอยู่ในรูปแบบของข้อความ ภาพ เสียง ภาพเคลื่อนไหว สอดคล้องกับ กานดา รุณนะพงศา (2557) ที่กล่าวไว้ว่าเครือข่ายสังคมออนไลน์ สามารถเรียกได้ว่าเป็นการอยู่ร่วมกันเป็นกลุ่มเป็นก้อนและมีการปฏิสัมพันธ์ในสังคมโดยใช้เครื่องมือและช่องทางทางออนไลน์เป็นตัวกลางในการแลกเปลี่ยน สื่อสารซึ่งกันและกัน

สุภาวรรณ นวลนิล (2557) ได้กล่าวว่าเครือข่ายสังคมออนไลน์เป็นช่องทางที่เชื่อมโยงบุคคลหลายบุคคลเข้าไว้ด้วยกันจนเกิดเป็นเครือข่ายสังคมขึ้นมา

พิจิตร วิจิตรบุญรักษ์ (2554) กล่าวว่าเครือข่ายสังคมออนไลน์เป็นที่ที่ผู้ส่งสารสามารถทำการแบ่งปันส่งต่อข้อมูลในรูปแบบต่าง ๆ แลกเปลี่ยนกันไปมาระหว่างผู้รับสาร และสามารถมีการโต้ตอบกันได้อีกด้วย

Wertime & Fenwick (2008) ได้ให้คำอธิบายถึงเครือข่ายสังคมออนไลน์ว่าเป็นพื้นที่สำหรับให้บุคคลที่มีความสนใจหรือมีความต้องการคล้ายคลึงกันมารวมตัวกัน โดยที่ผู้ใช้งานภายในเครือข่ายแต่ละคนจะมีการให้ข้อมูลส่วนตัวของตนเอง

เอมิกา เหมมินทร์ (2556) กล่าวว่า เครือข่ายสังคมออนไลน์จะถูกประกอบไปด้วยผู้ใช้งานหลายบุคคล โดยจะมีการสื่อสารข้อมูล เนื้อหา ข้อความ รูปภาพ วิดีโอ แลกเปลี่ยนแบ่งปันให้กับผู้ใช้งานอื่นในเครือข่ายอยู่ตลอดเวลา

Kommers (2001) ได้อธิบายถึงขอบข่ายของเครือข่ายสังคมออนไลน์ว่าเป็นตัวกลางที่กระตุ้นให้เกิดการปฏิสัมพันธ์ระหว่างบุคคลผ่านทางสื่อเทคโนโลยี มีการสร้างเครือข่ายที่หลากหลายและสามารถเชื่อมต่อกันได้จากทั่วทุกมุมโลก ไม่ว่าจะเป็น เครือข่ายด้านอาชีพหรือธุรกิจ เครือข่ายของบุคคลที่มีความชื่นชอบสิ่งเดียวกัน หรือแม้กระทั่งเครือข่ายของบุคคลที่ทำงานร่วมกันในบริษัท

เศรษฐพงศ์ มะลิสุวรรณ (2554) กล่าวว่าเครือข่ายสังคมบนโลกออนไลน์นั้นถือได้ว่าเป็นเปรียบเสมือนกับสังคมบนโลกของความเป็นจริง เพราะบุคคลสามารถมีการพูดคุยและโต้ตอบกันไปมาได้ปกติ สามารถแลกเปลี่ยนข้อมูลต่าง ๆ ได้อย่างไม่จำกัด รวมไปถึงสามารถทำกิจกรรมหรือธุรกรรมต่าง ๆ ได้ผ่านช่องทางนี้อีกด้วย

2.7 แนวคิดและทฤษฎีเกี่ยวกับกลโกงหลอกขอลงข้อมูลทางไซเบอร์ (Phishing)

อลิษา สายแผ้ว (2556) ได้กล่าวถึงกระบวนการของการหลอกล่อเพื่อลวงข้อมูลทางไซเบอร์ไว้ว่าสามารถกระทำโดยการที่ผู้ไม่ประสงค์ดีใช้ปัจจัยความรู้ความเชี่ยวชาญในด้านของเทคโนโลยีมาสร้างข้อกำหนดหรือเงื่อนไขต่าง ๆ ในการหลอกลวงบุคคลให้หลงเชื่อและยินยอมที่จะให้ข้อมูลส่วนตัวเหล่านั้นผ่านช่องทางต่าง ๆ ยกตัวอย่างเช่น จดหมายอิเล็กทรอนิกส์ที่แอบอ้างหรือปลอมแปลงลิงค์ หรือกลอุบายอื่น

ศักดิ์ชัย อัครวินอนันท์ (2559) ได้อธิบายรูปแบบของการโกงในยุคปัจจุบันที่มีความซับซ้อนเป็นอย่างมากว่า อาจจะมีการฉ้อโกงในลักษณะเดียวกับที่เคยเกิดขึ้นในอดีต และในขณะเดียวกันนี้ประชาชนอาจจะรู้ไม่เท่าทันกับภัยที่เกิดขึ้น จึงทำให้หลงเชื่อและตกเป็นเหยื่อของการสร้างเครือข่ายองค์กรอาชญากรรมที่นำเทคโนโลยีมาใช้ในการฉ้อโกงมากขึ้น

สำหรับรูปแบบการฉ้อโกงในยุคปัจจุบันสามารถประมวลได้ 8 รูปแบบ ซึ่งสามารถเตือนภัยแก่ผู้คนทั่วไปได้ดังนี้ คือ

- การฉ้อโกงโดยหลอกลวงให้ร่วมลงทุนในลักษณะของการแชร์ลูกโซ่
- การฉ้อโกงโดยหลอกลวงให้ทำรายการที่ตู้เอทีเอ็ม
- การฉ้อโกงโดยส่งอีเมลมาทำความรู้จักคุ้นเคยและหลอกลวงให้โอนเงินเข้าบัญชี
- การฉ้อโกงโดยปลอมตัวและปลอมที่อยู่อีเมลมาหลอกลวงให้โอนเงินผิดบัญชี
- การฉ้อโกงโดยอ้างการรักษาพยาบาลมาหลอกลวงเอาเงิน
- การฉ้อโกงโดยอ้างการเรียกรับเงินไปช่วยเหลือทางราชการหรือผู้ด้อยโอกาส
- การฉ้อโกงโดยใช้ศาสนาเป็นเครื่องมือในการหลอกลวง
- การฉ้อโกงโดยอ้างว่าเป็นเจ้าหน้าที่ในกระบวนการยุติธรรมและหลอกลวงเอาเงิน

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร คณะทำงานการจัดการความรู้ สำนักงานเลขาธิการวุฒิสภา ได้ให้ข้อมูลในเอกสารองค์ความรู้ เรื่องการป้องกันภัยคุกคามทางคอมพิวเตอร์ว่า กลโกงหลอกขอลงข้อมูลทางไซเบอร์ หรือ Phishing คือการหลอกลวงผ่านทางอินเทอร์เน็ตโดยที่มีผู้ไม่ประสงค์ดีหวังที่จะขอข้อมูลสำคัญของบุคคล เช่น รหัสผ่าน หมายเลขบัตรเครดิต เลขที่บัญชี เป็นต้น โดยอาจใช้ช่องทางต่าง ๆ แอบอ้างเป็นบุคคลหรือองค์กรที่น่าเชื่อถือส่งข้อความมาหลอกให้บุคคลเปิดเข้าไปเพื่อใส่ข้อมูลนั้น ๆ

2.8 แนวคิดและทฤษฎีเกี่ยวกับวิศวกรรมสังคม

ภูวดล แสงทองได้ให้คำอธิบายของวิศวกรรมสังคม หรือ Social Engineering ว่าเป็นกลวิธีในการโจมตีทางโลกไซเบอร์ในรูปแบบที่ค่อนข้างง่ายและไม่ซับซ้อน โดยที่ผู้ประสงค์ร้ายไม่ได้มีความจำเป็นต้องมีความรู้ความสามารถมากในระดับสูงแต่สามารถออกแบบการโจมตีที่ได้ประสิทธิภาพที่ดีได้ วิศวกรรมสังคมมักจะเป็นการใช้กลลวงในการล่อให้บุคคลกดเข้ามาในระบบเพื่อที่จะสามารถให้บุคคลนั้น ๆ กรอกข้อมูลส่วนตัวหรือข้อมูลที่ไม่ประสงค์ดีต้องการจะทราบไม่จำเป็นที่จำต้องเจาะระบบและใช้จุดอ่อนเกี่ยวข้องกับความสัมพันธ์ ไม่ระมัดระวังของคนเพื่อให้ได้มาซึ่งข้อมูล ส่วนมากผู้หลอกลวงข้อมูลมักใช้วิธีการในการแอบอ้าง บิดเบือนข้อมูลของตนเองให้ดูน่าเชื่อถือหรือได้รับมอบหมายอำนาจในการดำเนินการมาเพื่อให้เกิดความเชื่อใจในตัวผู้หลอกลวงและไม่เคลือบแคลงใจที่จะมอบข้อมูลให้

กรีน ธัญญวิกรม และธีระ กุลสวัสดิ์ (2564) ได้กล่าวว่าวิศวกรรมสังคมเป็นรูปแบบการโจมตีที่ใช้พื้นฐานของทฤษฎีจิตวิทยาสังคมเข้ามาประกอบ มีการใช้กลลวง ใช้อุบายต่าง ๆ เพื่อบิดเบือนความจริงและหลอกล่อให้บุคคลเปิดเผยข้อมูลสำคัญของตนเอง

วุฒิชัย สุขจรจิต (2561) กล่าวว่า วิศวกรรมสังคมถือว่าเป็นรูปแบบของศิลปะการหลอกลวงโดยเน้นการใช้จุดอ่อนของความไม่รู้เท่าทันและความไม่ระมัดระวังของตัวบุคคล และยังรวมถึงการบิดเบือนตัวตนที่แท้จริงเพื่อสร้างความเข้าใจที่ผิดให้กับบุคคลนั้น ๆ

คณาธิป ทองรวีวงศ์ (2564) ได้กล่าวว่า การที่เหล่าผู้ไม่ประสงค์ดีใช้การค้นคว้าหาข้อมูลจากที่ต่าง ๆ มาเป็นส่วนประกอบในการใช้เพื่อหลอกลวงและใช้เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลของผู้อื่นเป็นรูปแบบของหลักการวิศวกรรมทางสังคม หรือ Social Engineering

กิตติคุณ มีทองจันทร์ และ วงศ์ยศ เกิดศรี (2564) ได้กล่าวว่าวิศวกรรมทางสังคมคือปัจจัยที่ก่อให้เกิดอาชญากรรมทางไซเบอร์ โดยมีพฤติกรรมการณ์ไม่รู้เท่าทัน ความไม่ระมัดระวัง รวมถึงความพลอยปละละเลยที่เป็นส่วนประกอบหลักให้เกิดการโจมตีความมั่นคงทางไซเบอร์ได้

สามารถสรุปได้ว่า หนึ่งในกลวิธีที่กลุ่มผู้ไม่ประสงค์ดีได้เลือกใช้เพื่อนำมาหลอกลวงขอข้อมูลบุคคลอื่น ได้แก่ พฤติกรรมการณ์หลอกลวงขอข้อมูลทางไซเบอร์ หรือที่เรียกกันว่า Phishing นั้นเอง โดยกลวิธีในการหลอกลวงต่าง ๆ ก็สามารถแบ่งประเภทออกได้เป็นหลายประเภทโดยยึดจากช่องทางที่ใช้ในการโจมตี กลุ่มเป้าหมายที่ต้องการโจมตี หรือวิธีที่ใช้ในการโจมตี

2.9 แนวคิดเกี่ยวกับปัจจัยที่ส่งผลต่อความตระหนักรู้

Rui & Sushil (2566) ได้กล่าวว่า ตัวแปรที่มีอิทธิพลสามารถก่อให้เกิดความเสี่ยงจากการใช้งานโซเชียลมีเดียได้ คือ พฤติกรรมในการใช้งานของบุคคลนั้นๆ ทักษะคติ และข้อมูลพื้นฐานในการเตรียมรับความเสี่ยง

Rutger Leukfeldt (2560) ได้ศึกษาพบว่าตัวแปรสำคัญที่ส่งผลกระทบให้เกิดการถูกละเมิดทางไซเบอร์หรือตกเป็นเหยื่อของอาชญากรรมทางไซเบอร์ คือพฤติกรรมของมนุษย์ อันประกอบไปด้วย ความมั่งง่าย (ปล่อยปละละเลยและไม่ให้ความสำคัญ) ความรู้เท่าไม่ถึงการณ์ (ไม่ได้คำนึงถึงผลกระทบที่จะตามมาหรือไม่ทราบถึงผลกระทบที่อาจจะเกิดขึ้นได้) และความประมาท

วงศ์ยศ เกิดศรี (2561) ได้สรุปผลการวิจัยออกมาได้ว่า สิ่งที่มีอิทธิพลต่อการก่อให้เกิดอาชญากรรมทางไซเบอร์นั้นประกอบไปด้วย 4 ปัจจัย อันได้แก่ ข้อมูลส่วนตัว พฤติกรรมในการใช้งานโซเชียลมีเดีย ความรู้ความเข้าใจในเรื่องของกลลวงต่างๆ ในโลกไซเบอร์ และการตระหนักรู้เกี่ยวกับเทคโนโลยีสารสนเทศ

วิหวัธ สุขชีพ และ จริญญา แสนราช (2566) ได้ทำการสำรวจและได้อภิปรายผลการวิจัยว่า อายุและประสบการณ์ของบุคคลที่มีความแตกต่างกันออกไปย่อมส่งผลกระทบต่อระดับของความตระหนักรู้เท่าทันภัยไซเบอร์ที่แตกต่างกัน โดยบุคคลที่มีประสบการณ์รู้จักหรือเคยถูกรบกวนโดยภัยคุกคามทางไซเบอร์มาก่อนจะมีการระวังภัยและมีกลวิธีในการปกป้องตัวเองมากขึ้นจึงเป็นเรื่องสำคัญที่ควรจะต้องมีการจัดทำข้อมูลเพื่อให้ความรู้ ความเข้าใจเกี่ยวกับเรื่องภัยหรืออาชญากรรมทางไซเบอร์ให้ครอบคลุมและทั่วถึงเพื่อให้คนในสังคมเกิดให้ความสำคัญกับเรื่องเหล่านี้มากยิ่งขึ้นและปรับพฤติกรรมในการใช้งานอินเทอร์เน็ตให้มีความปลอดภัยเพิ่มขึ้น

กิตติยา วิสิฐพงศ์พันธ์ และคณะ ได้ทำการวิจัยและอภิปรายผลการศึกษาว่า ปัจจัยที่ส่งผลต่อการเกิดความตระหนักรู้ความปลอดภัยจากภัยทางไซเบอร์ ได้แก่ การที่บุคคลมีความรู้และมีการทำความเข้าใจเรื่องภัยคุกคามทางไซเบอร์ ความปลอดภัยและมั่นคงของอุปกรณ์และเครือข่าย และพฤติกรรมในการใช้งาน หากบุคคลมีความรู้เท่าทันและมีการศึกษาข้อมูลผลกระทบเกี่ยวกับประเด็นภัยคุกคามทางไซเบอร์จะทำให้เกิดความรู้เท่าทันรูปแบบของภัยต่างๆ ที่อาจเกิดขึ้นกับตัวบุคคลได้ รวมถึงยังสามารถที่จะหลีกเลี่ยงการทำพฤติกรรมที่ก่อให้เกิดความเสี่ยงในการเกิดอาชญากรรมทางไซเบอร์ได้อีกด้วย

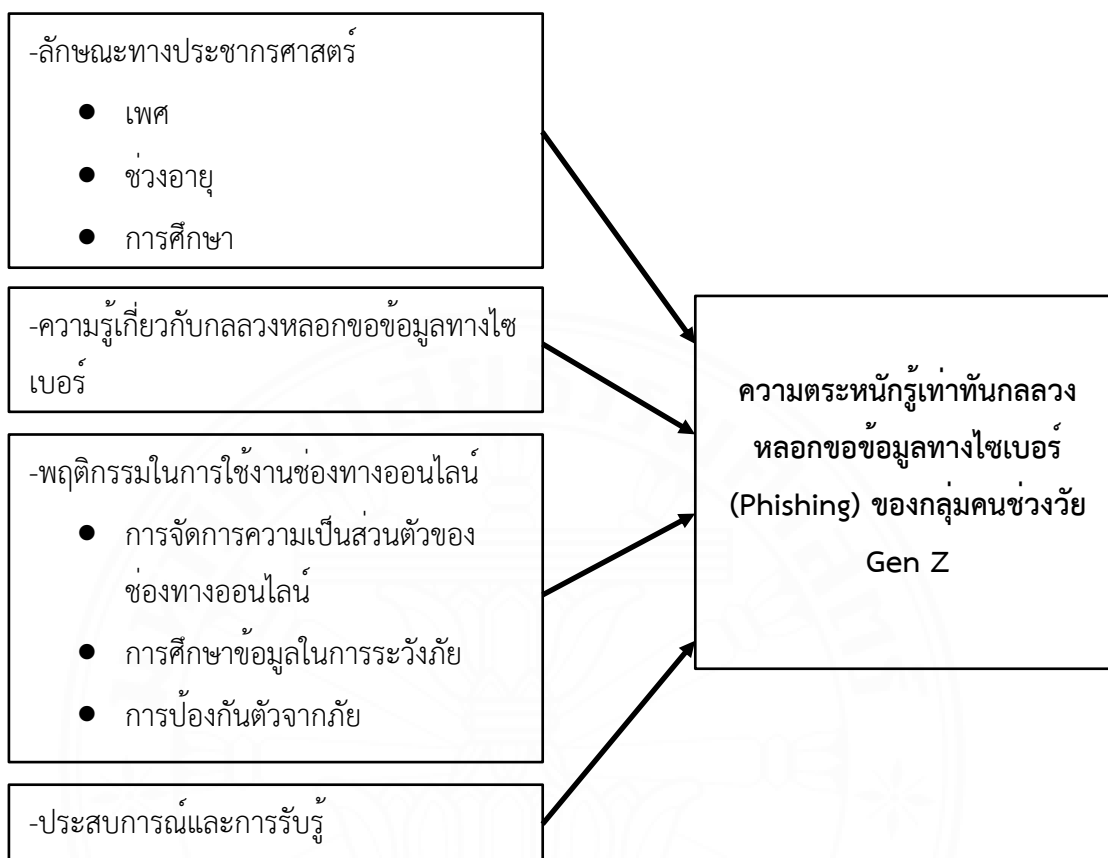
2.10 ผลสรุปแนวคิดและงานวิจัยที่เกี่ยวข้อง

จากการที่ผู้วิจัยได้ทำการทบทวนวรรณกรรมรวมถึงงานวิจัยที่เกี่ยวข้อง สามารถสรุปปัจจัยและตัวแปรที่มีอิทธิพลต่อความตระหนักรู้เท่าทันภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ได้แก่ เพศ ช่วงอายุ การศึกษา ความรู้ พฤติกรรมการใช้งาน ประสบการณ์และการรับรู้

ตารางที่ 2.10 แสดงตารางสรุปตัวแปรที่ได้จากการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง

ผู้วิจัย	ปัจจัยและตัวแปรที่มีอิทธิพลต่อความตระหนักรู้					
	เพศ	ช่วงอายุ	การศึกษา	ความรู้	พฤติกรรมการใช้งาน	ประสบการณ์และการรับรู้
ยุบล เป็ญจรงค์กิจ (2543)	✓	✓	✓			
ศิริวรรณ เสรีรัตน์ (2538)	✓	✓	✓			
Howe & Strauss (2551)		✓				
คณัญญา อิมใจ (2565)		✓				
Charles k. Atkin (1973)				✓		✓
Cunningham (1967)						✓
Martin & Camarero (2008)						✓
ยรรยงวรกร ทองแย้ม (2563)						✓
สุภิญญา กลางณรงค์ และ ผศ.ดร.ณภัทร เรืองนภากุล (2564)				✓		
จิตสุภา ฤทธิผลิน (2564)				✓		✓
อลิษา สายแผ้ว (2556)				✓		
ภูวดล แสงทอง (2565)					✓	
วุฒิชัย สุขจรจิต (2561)					✓	
กิตติคุณ มีทองจันทร์ และ วงศ์ยศ เกิดศรี (2564)					✓	✓
Rui & Sushil (2566)				✓	✓	✓
Rutger Leukfeldt (2560)					✓	
วงศ์ยศ เกิดศรี (2561)				✓	✓	
วิทวัส สุขชีพ และจรรย์ แสนราช (2566)		✓				✓
กิตติยา วิสิฐพงศ์พันธ์ และคณะ (2568)				✓	✓	

กรอบงานวิจัย



สมมติฐานการวิจัย

1. ลักษณะทางประชากรศาสตร์ (เพศ ช่วงอายุ การศึกษา) ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกลวงขอข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z
2. ความรู้เกี่ยวกับภัยกลลวงหลอกลวงขอข้อมูลทางไซเบอร์ ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกลวงขอข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z
3. พฤติกรรมในการใช้งานช่องทางออนไลน์ของบุคคล ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกลวงขอข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z
4. ประสบการณ์และรับรู้ภัยกลลวงหลอกลวงขอข้อมูลทางไซเบอร์ ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกลวงขอข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z

บทที่ 3

วิธีดำเนินการวิจัย

การศึกษาวิจัยเรื่อง “ความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคนช่วงวัย Gen Z” เป็นการวิจัยเชิงปริมาณ (Quantitative Research) ได้มีวิธีการดำเนินการศึกษาวิจัย ดังต่อไปนี้

3.1 ประชากรและกลุ่มตัวอย่าง

3.1.1 ประชากร

กำหนดให้ประชากร คือ ประชากรชาวไทยที่มีอายุอยู่ในช่วงกลุ่ม Gen Z ซึ่งมีเกณฑ์อายุอยู่ระหว่าง 18-28 ปี หรือเกิดในพ.ศ.2540 – 2550 นับตามระยะเวลาที่ทำการศึกษาค้นคว้าข้อมูล (พ.ศ.2567) โดยจะต้องมีคุณสมบัติ ดังต่อไปนี้

- มีอายุอยู่ในช่วงระหว่าง 18-28 ปี
- อาศัยอยู่ในประเทศไทย
- เป็นเพศชาย เพศหญิง หรือเพศทางเลือก

3.1.2 กลุ่มตัวอย่าง

กำหนดให้กลุ่มตัวอย่าง จำนวน 400 คน อ้างอิงจากสูตรการคำนวณหาขนาดของประชากรกลุ่มตัวอย่างของ Taro Yamane

$$n = \frac{N}{1 + Ne^2}$$

3.2 เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล

3.2.1 การสร้างแบบสอบถามออนไลน์ จำนวน 400 ชุด

แบบสอบถามประกอบไปด้วย 6 ส่วน ได้แก่

- ส่วนที่ 1 คำถามเกี่ยวกับลักษณะทางประชากรศาสตร์ (เพศ ช่วงอายุ การศึกษา)
- ส่วนที่ 2 คำถามเกี่ยวกับความรู้เกี่ยวกับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing)
- ส่วนที่ 3 คำถามเกี่ยวกับพฤติกรรมในการใช้งานช่องทางออนไลน์ต่างๆ และการป้องกันภัย
- ส่วนที่ 4 คำถามเกี่ยวกับประสบการณ์และการรับรู้เกี่ยวกับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์
- ส่วนที่ 5 คำถามเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์
- ส่วนที่ 6 ข้อเสนอแนะต่อแนวทางการป้องกันภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์

เบอร์

3.2.2 แบบสอบถามเพื่อสำรวจข้อมูลสำหรับงานวิจัยในครั้งนี้

ผู้วิจัยจะเริ่มต้นจากการคัดกรองผู้ตอบแบบสอบถามให้ได้เฉพาะกลุ่มเป้าหมาย ซึ่งเป็น กลุ่มคน Gen Z เมื่อจบการคัดกรองจึงนำไปสู่แบบสอบถามในส่วนต่างๆ ต่อไป

ส่วนที่ 1 คำถามเกี่ยวกับลักษณะทางประชากรศาสตร์ (เพศ ช่วงอายุ การศึกษา)

คำถามเกี่ยวกับลักษณะทางประชากรศาสตร์ ผู้วิจัยเลือกใช้ลักษณะคำถามปลายปิด โดยมีตัวเลือกคำตอบให้ผู้ตอบแบบสอบถามเลือกตอบได้เพียงคำตอบเดียวเท่านั้น

ส่วนที่ 2 คำถามเกี่ยวกับความรู้เกี่ยวกับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing)

คำถามเกี่ยวกับความรู้เกี่ยวกับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ผู้วิจัยเลือกใช้ลักษณะคำถามปลายปิด โดยมีตัวเลือกคำตอบให้ผู้ตอบแบบสอบถามเลือกตอบที่ถูกต้องได้เพียงคำตอบเดียวเท่านั้น โดยแต่ละข้อคำถามจะมีตัวเลือกคำตอบทั้งหมด 4 ตัวเลือก

ส่วนที่ 3 คำถามเกี่ยวกับพฤติกรรมในการใช้งานช่องทางออนไลน์ต่างๆ และการป้องกันภัย

คำถามเกี่ยวกับความรู้เกี่ยวกับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ผู้วิจัยเลือกใช้ลักษณะคำถามแบบตารางตัวเลือกหลายข้อ (Multiple choice grid) ให้ผู้ตอบ

แบบสอบถามเลือกตอบเพียงข้อเดียว โดยมีเกณฑ์ในการวัดระดับของคำตอบทั้งหมด 5 ระดับ ได้แก่ 5 = มากที่สุด 4 = มาก 3 = ปานกลาง 2 = น้อย และ 1 = น้อยที่สุด

ส่วนที่ 4 คำถามเกี่ยวกับประสบการณ์และการรับรู้เกี่ยวกับภัยกลลวงหลอกขอข้อมูลทางไซเบอร์

คำถามเกี่ยวกับความรู้เกี่ยวกับภัยกลลวงหลอกขอข้อมูลทางไซเบอร์ (Phishing) ผู้วิจัยเลือกใช้ลักษณะคำถามแบบตารางตัวเลือกหลายข้อ (Multiple choice grid) ให้ผู้ตอบแบบสอบถามเลือกตอบเพียงข้อเดียว โดยมีเกณฑ์ในการวัดระดับของคำตอบทั้งหมด 5 ระดับ ได้แก่ 5 = มากที่สุด 4 = มาก 3 = ปานกลาง 2 = น้อย และ 1 = น้อยที่สุด

ส่วนที่ 5 คำถามเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยกลลวงหลอกขอข้อมูลทางไซเบอร์

คำถามเกี่ยวกับความรู้เกี่ยวกับภัยกลลวงหลอกขอข้อมูลทางไซเบอร์ (Phishing) ผู้วิจัยเลือกใช้ลักษณะคำถามแบบตารางตัวเลือกหลายข้อ (Multiple choice grid) ให้ผู้ตอบแบบสอบถามเลือกตอบเพียงข้อเดียว โดยมีเกณฑ์ในการวัดระดับของคำตอบทั้งหมด 5 ระดับ ได้แก่ 5 = มากที่สุด 4 = มาก 3 = ปานกลาง 2 = น้อย และ 1 = น้อยที่สุด

ส่วนที่ 6 ข้อเสนอแนะต่อแนวทางการป้องกันภัยกลลวงหลอกขอข้อมูลทางไซเบอร์

คำถามเกี่ยวกับข้อเสนอแนะต่อแนวทางการป้องกันภัยกลลวงหลอกขอข้อมูลทางไซเบอร์ ผู้วิจัยเลือกใช้ลักษณะคำถามปลายปิด โดยมีตัวเลือกคำตอบให้ผู้ตอบแบบสอบถามเลือกตอบได้เพียงคำตอบเดียวเท่านั้น

3.3 การเก็บรวบรวมข้อมูล

การเก็บรวบรวมข้อมูลดำเนินการตามขั้นตอน ดังนี้

3.3.1 จัดทำร่างแบบสอบถาม

3.3.2 ดำเนินการตรวจสอบวัดคุณภาพของเครื่องมือคำถามที่จะใช้ในการศึกษาวิจัย โดยการให้ผู้เชี่ยวชาญ จำนวนทั้งหมด 3 ท่านร่วมทำการประเมินวิเคราะห์การหาค่าดัชนีความเที่ยงตรงของแบบสอบถาม (IOC : Index of item objective congruence) โดยกำหนดเกณฑ์ของความเที่ยงตรง ดังนี้

ข้อคำถามที่ได้รับค่าดัชนีความเที่ยงตรงตั้งแต่ 0.50-1.00 ถือว่าสามารถใช้งานได้ มีความสอดคล้องต่อวัตถุประสงค์

หากข้อคำถามใดที่ได้รับค่าดัชนีความเที่ยงตรงต่ำกว่า 0.50 ถือว่าไม่สามารถใช้งานได้ จำเป็นต้องได้รับการปรับปรุงให้สอดคล้องกับวัตถุประสงค์ในการศึกษาวิจัย

3.3.3 ดำเนินการสร้างแบบสอบถามออนไลน์ทาง Google Form

3.3.4 เริ่มดำเนินการในการเก็บข้อมูล โดยทำการแจกแบบสอบถามให้กับกลุ่มตัวอย่าง จำนวน 400 ชุด

3.4 การวิเคราะห์ข้อมูล

3.4.1 ใช้โปรแกรมสำเร็จรูปสำหรับการวิเคราะห์ข้อมูลการวิจัยทางสังคมศาสตร์

3.5 สถิติที่ใช้ในการวิเคราะห์ข้อมูล

3.5.1 ใช้สถิติพรรณนา (Descriptive Statistics) ในการอธิบายคุณลักษณะต่างๆ ทางประชากรของกลุ่มตัวอย่างในงานวิจัย

3.5.2 วิเคราะห์สถิติเชิงอนุมานเพื่อทำการวิเคราะห์ค่าความแปรปรวนทางเดียว (One-way ANOVA) และสมการถดถอยพหุคูณ (Multiple Regression Analysis)

บทที่ 4

ผลการวิจัยและอภิปรายผล

งานค้นคว้าอิสระหัวข้อ “ความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคนช่วงวัย Gen Z” ได้เจาะจงกลุ่มตัวอย่างที่ต้องการสอบถามข้อมูล คือ กลุ่มคน Gen Z ที่มีอายุระหว่าง 18-28 ปี หรือเกิดในช่วง พ.ศ.2540-2550 ที่อาศัยอยู่ในประเทศไทย โดยมีการตั้งข้อคำถามในเรื่องของข้อมูลทางประชากรศาสตร์ ความรู้เบื้องต้นเกี่ยวกับกลลวงหลอกขโมยข้อมูลทางไซเบอร์ พฤติกรรมการใช้งานและการป้องกันภัย ประสบการณ์และการรับรู้เกี่ยวกับกลลวงหลอกขโมยข้อมูลทางไซเบอร์ ความตระหนักรู้เกี่ยวกับกลลวงหลอกขโมยข้อมูลทางไซเบอร์ และข้อเสนอแนะที่เป็นประโยชน์ต่อการป้องกันภัยทางไซเบอร์ในอนาคต โดยผู้ศึกษาวิจัยได้ทำการแจกจ่ายแบบสอบถามผ่านทางช่องทางออนไลน์ และได้รับการตอบแบบสอบถามจำนวนทั้งหมด 400 ชุด และจึงนำมาดำเนินการต่อในการวิเคราะห์ข้อมูล ดังนี้

4.1 ผลการตรวจสอบเครื่องมือที่ใช้ในการวิจัย

4.2 ผลการวิจัย

4.2.1 ผลการวิจัยเชิงพรรณนา

- 4.2.1.1 ข้อมูลทางประชากรศาสตร์ของกลุ่มตัวอย่าง
- 4.2.1.2 ระดับความรู้ของกลุ่มตัวอย่างในเรื่องของกลลวงหลอกขโมยข้อมูล
- 4.2.1.3 ระดับพฤติกรรมการระวังภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ในการใช้งานช่องทางออนไลน์
- 4.2.1.4 ระดับประสบการณ์และการรับรู้ในเรื่องกลลวงหลอกขโมยข้อมูล
- 4.2.1.5 ระดับความตระหนักรู้เกี่ยวกับกลลวงหลอกขโมยข้อมูลทางไซเบอร์
- 4.2.1.6 ข้อเสนอแนะต่อแนวทางการป้องกันภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์

4.2.2 ผลการวิจัยเชิงอนุมาน

- 4.2.2.1 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรข้อมูลทางประชากรศาสตร์กับความตระหนักรู้เท่าทันภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์
- 4.2.2.2 ผลการวิเคราะห์ปัจจัยที่มีอิทธิพลต่อความตระหนักรู้เกี่ยวกับกลลวงหลอกขโมยข้อมูลทางไซเบอร์ ของกลุ่มคน Gen Z

4.3 อภิปรายผลการวิจัย

4.1 ผลการตรวจสอบเครื่องมือที่ใช้ในการวิจัย

ผลการตรวจสอบความเที่ยงตรงของแบบสอบถาม (Index of item Objective Congruence - IOC)

ในการออกแบบและสร้างแบบสอบถามสำหรับงานวิจัยฉบับนี้ ทางผู้จัดทำได้มีการนำเสนอแบบสอบถามให้แก่ผู้เชี่ยวชาญ จำนวน 3 ท่าน เพื่อเป็นการตรวจสอบความเที่ยงตรงและค่าน้ำหนักของเนื้อหาให้ตรงตามวัตถุประสงค์ของงานวิจัยที่ตั้งไว้ก่อนสามารถนำมาใช้เก็บข้อมูลจริง โดยทางผู้จัดทำได้นำเสนอข้อคำถามทั้งหมด 6 ส่วน ประกอบด้วย ส่วนที่ 1 คำถามเกี่ยวกับลักษณะทางประชากรศาสตร์ (เพศ ช่วงอายุ การศึกษา) / ส่วนที่ 2 คำถามเกี่ยวกับความรู้เกี่ยวกับภัยกลวงหลอกขอข้อมูลทางไซเบอร์ (Phishing) / ส่วนที่ 3 คำถามเกี่ยวกับพฤติกรรมในการใช้งานช่องทางออนไลน์ต่างๆ และการป้องกันภัย / ส่วนที่ 4 คำถามเกี่ยวกับประสบการณ์และการรับรู้เกี่ยวกับภัยกลวงหลอกขอข้อมูลทางไซเบอร์ / ส่วนที่ 5 คำถามเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยกลวงหลอกขอข้อมูลทางไซเบอร์ และ ส่วนที่ 6 ข้อเสนอแนะต่อแนวทางการป้องกันภัยกลวงหลอกขอข้อมูลทางไซเบอร์

ผู้เชี่ยวชาญที่ทำการร่วมตรวจสอบค่าความเที่ยงตรงของแบบสอบถามในวิจัยฉบับนี้ ได้แก่

1. อาจารย์สังกัดภาควิชาวิทยาการวิจัยและนวัตกรรมทางแพทย์ มหาวิทยาลัยนวมินทราธิราช
2. ผู้อำนวยการสำนักพัฒนาการเรียนรู้ มหาวิทยาลัยกรุงเทพ
3. ผู้อำนวยการสำนักความเสี่ยงและควบคุมภายในการทำเรือแห่งประเทศไทย

ทางผู้เชี่ยวชาญทั้ง 3 ท่านมีการใช้เกณฑ์ในการร่วมตรวจสอบพิจารณาความเที่ยงตรงของข้อคำถาม ดังนี้

- +1 หมายถึงแน่ใจว่าคำถามมีความสอดคล้องและเหมาะสมกับวัตถุประสงค์
- 0 หมายถึงไม่แน่ใจว่าคำถามมีความสอดคล้องและเหมาะสมกับวัตถุประสงค์
- 1 หมายถึงคำถามไม่มีความสอดคล้องและไม่เหมาะสมกับวัตถุประสงค์

หลังจากได้ผลคะแนนจากผู้เชี่ยวชาญทั้ง 3 ท่านเป็นที่เรียบร้อยแล้ว ทางผู้จัดทำได้มีการคำนวณหาค่า IOC โดยการนำผลคะแนนทั้ง 3 ชุดมาทำการเฉลี่ยตามเกณฑ์การประเมินมาตรฐาน ข้อคำถามที่ได้รับค่าตั้งแต่ 0.50-1.00 สามารถใช้งานได้ มีความสอดคล้องต่อวัตถุประสงค์ ข้อคำถามใดที่ได้รับค่าต่ำกว่า 0.50 ไม่สามารถใช้งานได้ จำเป็นต้องได้รับการปรับปรุงให้สอดคล้องกับวัตถุประสงค์ในการศึกษาวิจัย

จากผลคะแนนหัวข้อคำถามสามารถนำไปใช้งานต่อไปได้อีก โดยนำข้อเสนอแนะจากผู้เชี่ยวชาญ
ปรับให้คำถามมีความเข้าใจง่ายต่อผู้ตอบมากขึ้นและปรับรูปแบบของคำถามส่วนข้อเสนอแนะให้มีทั้ง
ประเภทการเลือกตอบและปลายเปิดเพื่อให้ได้มาซึ่งข้อมูลที่หลากหลายมากยิ่งขึ้น



ตารางที่ 4.1.1 แสดงผลการตรวจสอบค่าความเที่ยงตรงของแบบสอบถาม

ข้อ	คำถาม	ความคิดเห็นผู้เชี่ยวชาญ				การแปลผลและข้อเสนอแนะ
		1	2	3	IOC	
ส่วนที่ 1 คำถามเกี่ยวกับลักษณะทางประชากรศาสตร์ (เพศ ช่วงอายุ การศึกษา)						
ใช้ลักษณะคำถามปลายปิด โดยมีตัวเลือกคำตอบให้ผู้ตอบแบบสอบถามเลือกตอบได้เพียงคำตอบเดียวเท่านั้น						
วัตถุประสงค์ : เพื่อศึกษาและเก็บรวบรวมข้อมูลทางประชากรศาสตร์ของผู้ตอบแบบสอบถามที่ส่งผลกระทบต่อความตระหนักรู้เท่าทันกลลวงหลอกขอข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z						
1.1	อายุ ท่านเป็นกลุ่มคนที่มีอายุระหว่าง 13-28 ปี หรือเกิดในช่วงระหว่างพ.ศ.2540-2550 ใช่หรือไม่ [1] ใช่ [2] ไม่ใช่ (จบแบบสอบถาม)	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : อาจพิจารณาเพิ่มช่วงอายุที่ละเอียดขึ้นแทนการถามเพียงว่าอยู่ในช่วงอายุ 13-28 ปีหรือไม่ เช่น แบ่งเป็น 13-18, 19-23, 24-28 จะทำให้สามารถวิเคราะห์ช่วงอายุน้อยใน Gen Z ได้ชัดเจนยิ่งขึ้น 2 : คำถามชัดเจนและจำเป็นเพื่อตรวจสอบว่าผู้ตอบเป็นกลุ่มเป้าหมาย Gen Z หรือไม่ 3 : ช่วงอายุค่อนข้างกว้าง หากแบ่งช่วงอายุละเอียดมากขึ้น อาจจะส่งผลที่ดีต่อการตีความแบบสอบถาม
1.2	เพศ [1] เพศชาย [2] เพศหญิง [3] เพศทางเลือก	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : มีความเกี่ยวข้องกับการวิเคราะห์ทางสถิติ แต่ควรเพิ่มตัวเลือก "ไม่ระบุ" สำหรับความเป็นกลาง 3 : สอดรับกับกระแสสังคมดี
1.3	ระดับการศึกษา [1] ประถมศึกษา [2] มัธยมศึกษา [3] ปวช./ ปวส./ อนุปริญญา [4] ปริญญาตรี [5] ปริญญาโทหรือสูงกว่า	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : อาจพิจารณาเพิ่ม "กำลังศึกษา" ต่อท้ายแต่ละระดับ เนื่องจากกลุ่ม Gen Z หลายคนอาจยังอยู่ในระหว่างการศึกษ 2 : คำตอบครอบคลุมดีอยู่แล้ว

ข้อ	คำถาม	ความคิดเห็นผู้เชี่ยวชาญ				การแปลผลและข้อเสนอแนะ
		1	2	3	IOC	
ส่วนที่ 2 คำถามเกี่ยวกับความรู้เกี่ยวกับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing)						
ลักษณะคำถามปลายปิด โดยมีตัวเลือกคำตอบให้ผู้ตอบแบบสอบถามเลือกตอบที่ถูกต้องได้เพียงคำตอบเดียวเท่านั้น โดยแต่ละข้อคำถามจะมีตัวเลือกคำตอบทั้งหมด 4 ตัวเลือก						
วัตถุประสงค์ : เพื่อวัดระดับความรู้เกี่ยวกับกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของผู้ตอบแบบสอบถามที่อาจส่งผลกระทบต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ของกลุ่มคน Gen Z						
2.1	หากท่านได้รับข้อความทางโทรศัพท์โดยมีการอ้างว่าท่านมีพัสดุที่ตกค้างอยู่และต้องการให้ท่านคลิกลิงค์เพื่อกรอกข้อมูลส่วนตัวในระบบ ถือเป็นการภัยคุกคามทางไซเบอร์รูปแบบใด [1] ภัยคุกคามจากภายใน (Insider Threat) [2] ฟิชซิง (Phishing) [3] รูทคิท (Rootkit) [4] สปายแวร์ (Spyware)	+1	+1	+1	1	สามารถใช้ได้ 1: สอดคล้องและเหมาะสม แต่ตัวเลือกอาจมีความใกล้เคียงกันสำหรับผู้ที่ไม่มีความรู้ด้านไซเบอร์ ควรพิจารณาเพิ่มคำอธิบายสั้นๆ ในแต่ละตัวเลือก 2 : คำถามมีความชัดเจนและเกี่ยวข้องโดยตรงกับความเข้าใจเกี่ยวกับ Phishing 3 : คำถาม ร่วมสมัย และเป็นกรณีที่เกิดขึ้นจริงในปัจจุบัน คำตอบ อาจเพิ่มในส่วน of คำอธิบาย เนื่องจากเป็น technical term
2.2	ข้อใดเป็นข้อมูลที่เสี่ยงต่อการโดนหลอกลวงขโมยข้อมูลทางไซเบอร์ [1] วันเดือนปีเกิด [2] บัญชีธนาคาร [3] ชื่อเพื่อนสนิท [4] ถูกทุกข้อ	+1	+1	+1	1	สามารถใช้ได้ 1 : ตัวเลือกข้อ 4 "ถูกทุกข้อ" อาจทำให้ผู้ตอบเลือกโดยไม่พิจารณาตัวเลือกอื่นอย่างถี่ถ้วน อาจพิจารณาปรับเป็นการถามให้จัดลำดับความเสี่ยงของข้อมูลแต่ละประเภท 2 : คำตอบครอบคลุมดีอยู่แล้ว

2.3	เว็บไซต์ใดต่อไปนี้เป็นเว็บไซต์ที่มีความน่าเชื่อถือมากที่สุดในการกรอกข้อมูล [1] https://www.youtube.co.th [2] https://docs.google.go.th/forms/d/1X0Td3HBnbfOBEP0tYIvLfSvF7tRhMB_P9hVGG6fVEV0/edit [3] http://d6s.me/JSdte [4] http://adidas.co.th	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : อาจพิจารณาปรับโจทย์และตัวเลือกให้มีความชัดเจนมากขึ้นเนื่องจากเว็บไซต์ที่มี https:// ก็อาจถูกปลอมแปลงได้ และ URL ยาวๆ ใน Google Forms อาจเป็น URL ที่ถูกต้อง 2 : คำถามดี ช่วยให้ประเมินความรู้เกี่ยวกับ URL และความปลอดภัยทางไซเบอร์ 3 : คำถาม ยังมีความคลุมเครือ อาจจะปรับ wording ให้สะท้อนกับวัตถุประสงค์มากขึ้น คำตอบค่อนข้างอ่านยาก และขาดความชัดเจน
2.4	ข้อใดเป็นนโยบายในการป้องกันการถูกหลอกขอข้อมูลภายในองค์กรที่มีประสิทธิภาพมากที่สุด [1] พนักงานบริษัททุกคนต้องทำการเปลี่ยนรหัสผ่านทุก 45 วัน [2] พนักงานทุกคนต้องแจ้งรหัสผ่านให้เพื่อนสนิทรับทราบ [3] หัวหน้างานต้องส่งลิงค์เปลี่ยนรหัสผ่านให้ลูกน้องโดยการใช้ช่องทางออนไลน์ส่วนตัว [4] หากได้รับอีเมลขู่ว่าจะส่งไฟล์สำคัญให้รีบกดลิงค์เพื่อกู้ข้อมูลทันทีไม่ว่าจะมาจากผู้ส่งคนไหนก็ตาม	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามเหมาะสม

2.5	พฤติกรรมในข้อใดที่เสี่ยงต่อการถูกหลอกขอข้อมูลประเภทสังเกต พฤติกรรมทางโซเชียล (Angler Phishing) มากที่สุด [1] บ่นและอัปเดตทุกเรื่องในชีวิตลงเฟซบุ๊กส่วนตัว [2] ค้นหาข้อมูลที่สนใจใน www.google.com [3] รีบกดชำระเงินในเว็บไซต์เพราะกลัวสินค้าหมด [4] คุยเรื่องงานกับเพื่อนร่วมงานผ่านทางโทรศัพท์	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : อธิบายเพิ่มเติมว่า Angler Phishing คืออะไร เนื่องจากผู้ตอบอาจไม่คุ้นเคยกับคำศัพท์เฉพาะทาง 2 : คำถามมีความเกี่ยวข้องโดยตรงและช่วยวัดระดับความรู้ของผู้ตอบ 3 : ตัดส่วนของ technical term ออก อาจทำให้ผู้ตอบแบบสอบถามเข้าใจง่ายขึ้น
2.6	ข้อใดไม่ถือเป็นการละเมิด พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล [1] โรงพยาบาลทำการส่งข้อมูลการรักษาของคนไข้ให้แก่แพทย์เจ้าของไข้ที่ทำการรักษา [2] พนักงานในองค์กรแอบส่งข้อมูลส่วนตัวของลูกค้าให้คนนอกองค์กร [3] คาเฟ่ชื่อดังนำภาพและประวัติการซื้อของลูกค้ามาลงเพจเฟซบุ๊ก [4] เจ้าหน้าที่บริษัทเครือข่ายโทรศัพท์เอารายชื่อและเบอร์ติดต่อของลูกค้าไปขาย	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามเหมาะสมและเกี่ยวข้องกับนโยบายคุ้มครองข้อมูลส่วนบุคคล 3 : คำตอบครอบคลุมกับช่วงอายุของกลุ่มตัวอย่างที่จะตอบแบบสอบถามดี

2.7	หากมีเบอร์ที่แค้นโทรเข้ามาอ้างว่าเป็นเจ้าหน้าที่จากแบรนด์ดังที่คุณใช้ประจำและแจ้งว่าคุณเป็นผู้โชคดีที่ได้รับการสุ่มเลือกให้ได้รับของรางวัลพิเศษ โดยต้องทำการแอดไลน์เพื่อรับของรางวัล ถือว่าเสี่ยงที่จะเป็นกลโกง หลอกขอข้อมูลในประเภทใด [1] E-mail Phishing [2] Vishing Phishing [3] CEO Fraud Phishing [4] Web Phishing	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามดี ช่วยให้เข้าใจประเภทของ Phishing ที่พบบ่อย 3 : คำตอบ อาจต้องเพิ่มคำอธิบาย หรือ อาจใช้เป็นคำศัพท์ที่รู้จักในวงกว้าง
2.8	หากมีอีเมลส่งเข้ามาจาก TikTok ด้วยชื่อเมล Tiktokthailand@tiktok.co.th ให้คุณทำการอัปเดตข้อมูลส่วนตัวและอีเมลอีกครั้งไม่อย่างนั้นจะถูกระงับการใช้งาน ถือว่าเสี่ยงที่จะเป็นกลโกง หลอกขอข้อมูลในประเภทใด [1] E-mail Phishing [2] Vishing Phishing [3] CEO Fraud Phishing [4] Web Phishing	+1	+1	+1	1	<u>สามารถใช้ได้</u>

2.9	หากมีอีเมลที่อ้างเป็นเพื่อนร่วมงานในองค์กรส่งไฟล์มาให้ดาวน์โหลด โดยที่เป็นอีเมลที่คล้ายคลึงกับอีเมลขององค์กร ถือว่าเสี่ยงที่จะเป็นกลโกงหลอกขอข้อมูลในประเภทใด [1] E-mail Phishing [2] Vishing Phishing [3] Spear Phishing [4] Web Phishing	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : สอดคล้อง แต่คำถามยังไม่ระบุชัดเจนว่า "ชื่ออีเมลที่คล้ายคลึง" นั้นแตกต่างจากอีเมลขององค์กรอย่างไร ควรเพิ่มเติมอย่างประกอบ 2 : คำถามดี และเกี่ยวข้องกับการโจมตีแบบ Spear Phishing โดยเฉพาะกลุ่มคนทำงาน
2.10	หากท่านได้รับข้อความที่อ้างว่าส่งจากเฟซบุ๊กให้รีบดำเนินการเปลี่ยนรหัสผ่านเพื่อให้บัญชีของท่านสามารถใช้งานได้อีก ท่านจะตัดสินใจดำเนินการอย่างไร [1] กดลิงค์เพื่อตรวจสอบว่าเป็นลิงค์จากเฟซบุ๊กจริงๆ ใช่มั้ยหรือไม่ [2] รีบเปลี่ยนรหัสผ่านเนื่องจากกลัวถูกระงับการใช้ [3] ส่งอีเมลตอบกลับว่าได้ทำการเปลี่ยนรหัสผ่านแล้ว [4] ตรวจสอบให้มั่นใจโดยไม่คลิกลิงค์ใด ๆ และรีบลบอีเมลออกทันที	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามดี วัดพฤติกรรมการตอบสนองต่อภัย Phishing

ข้อ	คำถาม	ความคิดเห็นผู้เชี่ยวชาญ				การแปลผลและข้อเสนอแนะ
		1	2	3	IOC	
ส่วนที่ 3 คำถามเกี่ยวกับพฤติกรรมในการใช้งานช่องทางออนไลน์ต่างๆ และการป้องกันภัย						
ลักษณะคำถามแบบตารางตัวเลือกหลายข้อ (Multiple choice grid) ให้ผู้ตอบแบบสอบถามเลือกตอบเพียงข้อเดียว โดยมีเกณฑ์ในการวัดระดับของคำตอบทั้งหมด 5 ระดับ ได้แก่ 5 = มากที่สุด 4 = มาก 3 = ปานกลาง 2 = น้อย และ 1 = น้อยที่สุด						
วัตถุประสงค์ : เพื่อศึกษาและเก็บข้อมูลพฤติกรรมในการใช้งานช่องทางออนไลน์ของผู้ตอบแบบสอบถามที่อาจส่งผลกระทบต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z						
3.	ท่านมีพฤติกรรมอย่างไรเกี่ยวกับกลลวงหลอกขโมยข้อมูลทางไซเบอร์					
	พฤติกรรมด้านการจัดการความเป็นส่วนตัวของช่องทางออนไลน์					
3.1	ท่านไม่ทำการแชร์ข้อมูลส่วนตัวหรือบุคคลรอบตัวลงในช่องทางออนไลน์	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามเหมาะสม สอดคล้องกับแนวทางป้องกันภัยไซเบอร์
3.2	ท่านมักจะตั้งค่าความเป็นส่วนตัวของช่องทางออนไลน์ทั้งหมดให้มีความปลอดภัยมากที่สุด (ยืนยันตัวตนด้วยอีเมลหรือเบอร์โทรศัพท์ ตั้งค่าการแจ้งเตือนเมื่อมีคนพยายามล่อคอนิน ไม่เปิดบัญชีให้เป็นสาธารณะ เป็นต้น)	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามดี ควรเพิ่มตัวอย่าง เช่น ใช้ 2FA หรือการจำกัดผู้เข้าถึงข้อมูล
	พฤติกรรมด้านการศึกษาข้อมูลในการระงับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์					
3.3	ท่านให้ความสำคัญกับการค้นคว้าข่าวสาร ข้อมูลและวิธีในการระงับภัยกลโกงหลอกขโมยข้อมูลทางออนไลน์จากช่องทางต่างๆ	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : สอดคล้อง แต่ควรระบุประเภทของแหล่งข้อมูลที่ศึกษาเพิ่มเติม เช่น สื่อสังคมออนไลน์ เว็บไซต์ทางการ หรือการอบรม 2 : คำถามสำคัญเกี่ยวกับการรักษาความปลอดภัยข้อมูลส่วนตัว
3.4	ท่านให้ความสำคัญกับเนื้อหาของนโยบายความเป็นส่วนตัวของข้อมูลก่อนที่จะใช้งานแอปพลิเคชันต่างๆเสมอ	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามดี เหมาะสม
3.5	ท่านศึกษาข้อมูลเกี่ยวกับภัยกลโกงหลอกขโมยข้อมูลทางไซเบอร์อยู่เสมอ	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามตรงประเด็น เหมาะสม
3.6	ท่านเคยเข้าอบรมวิธีการระงับตนเองจากภัยกลโกงหลอกขโมยข้อมูลทางไซเบอร์	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามตรงประเด็น เหมาะสม

พฤติกรรมด้านการป้องกันตัวจากภัยกลลวงหลอกขอข้อมูลทางไซเบอร์						
3.7	ท่านมีการโหลดแอปพลิเคชันในการตรวจสอบมิจฉาชีพ หรือไม่การเช็ค ชื่อเมล เบอร์โทรที่ส่งมาก่อนเสมอ	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามดี เหมาะสม
3.8	ท่านไม่ดาวน์โหลดหรือคลิกลิงค์ที่ไม่ทราบที่มาที่ไปแม้อูกลงจากอีเมล ของบุคคลที่รู้จัก	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามสำคัญเกี่ยวกับ Malware และ Spear Phishing
3.9	ท่านทำการบล็อกเบอร์โทรศัพท์ที่เป็นมิจฉาชีพ	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามดีเกี่ยวกับมาตรการป้องกัน

ข้อ	คำถาม	ความคิดเห็นผู้เชี่ยวชาญ				การแปลผลและข้อเสนอแนะ
		1	2	3	IOC	
ส่วนที่ 4 คำถามเกี่ยวกับประสบการณ์และการรับรู้เกี่ยวกับภัยกลลวงหลอกขอข้อมูลทางไซเบอร์						
ลักษณะคำถามแบบตารางตัวเลือกหลายข้อ (Multiple choice grid) ให้ผู้ตอบแบบสอบถามเลือกตอบเพียงข้อเดียว โดยมีเกณฑ์ในการวัดระดับของคำตอบทั้งหมด 5 ระดับ ได้แก่ 5 = มากที่สุด 4 = มาก 3 = ปานกลาง 2 = น้อย และ 1 = น้อยที่สุด						
วัตถุประสงค์ : เพื่อศึกษาและเก็บข้อมูลประสบการณ์และการรับรู้เกี่ยวกับเรื่องกลลวงหลอกขอข้อมูลทางไซเบอร์ของผู้ตอบแบบสอบถามที่อาจส่งผลกระทบต่อความตระหนักรู้เท่าทันกลลวงหลอกขอข้อมูลทางไซเบอร์ ของกลุ่มคน Gen Z						
4.	ท่านมีประสบการณ์และการรับรู้เกี่ยวกับกลลวงหลอกขอข้อมูลทางไซเบอร์					
4.2	ท่านหรือบุคคลรอบตัวเคยมีประสบการณ์ถูกหลอกขอข้อมูลทางไซเบอร์ จากช่องทางข้อความ	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1: สอดคล้อง แต่ไม่ชัดเจนว่าหมายถึงตัวผู้ตอบถูกหลอกสำเร็จหรือเพียงได้รับข้อความหลอกกลลวง 2 : คำถามตรงประเด็น เหมาะสม 3 : เพื่อเพิ่มความชัดเจนของคำตอบ อาจถามเพิ่มว่า เคยมีประสบการณ์ร่วม หรือ แคเคยได้รับและไม่มีประสบการณ์ร่วม
4.2	ท่านหรือบุคคลรอบตัวเคยมีประสบการณ์ถูกหลอกขอข้อมูลทางไซเบอร์ จากช่องทางอีเมลล์	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : สอดคล้อง แต่มีปัญหาเช่นเดียวกับข้อ 4.2 2 : คำถามตรงประเด็น เหมาะสม 3 : เพื่อเพิ่มความชัดเจนของคำตอบ อาจถามเพิ่มว่า เคยมีประสบการณ์ร่วม หรือ แคเคยได้รับและไม่มีประสบการณ์ร่วม
4.3	ท่านหรือบุคคลรอบตัวเคยมีประสบการณ์ถูกหลอกขอข้อมูลทางไซเบอร์ จากช่องทางโทรศัพท์	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : สอดคล้อง แต่มีปัญหาเช่นเดียวกับข้อ 4.2 2 : คำถามตรงประเด็น เหมาะสม 3 : เพื่อเพิ่มความชัดเจนของคำตอบ อาจถามเพิ่มว่า เคยมีประสบการณ์ร่วม หรือ แคเคยได้รับและไม่มีประสบการณ์ร่วม

4.4	ท่านมีการคำนึงถึงความเสี่ยงของการถูกนำเอาข้อมูลส่วนตัวไปใช้ในทางที่ไม่ดีอยู่เสมอ	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : สอดคล้อง แต่เป็นการวัดทัศนคติมากกว่าประสบการณ์ ควรย้ายไปส่วนที่ 5 2 : คำถามตรงประเด็น เหมาะสม 3 : คำถามสอดคล้องกับ ส่วนที่ 5 เรื่องการสร้างความตระหนัก
4.5	ท่านคิดว่าความรู้และประสบการณ์ส่งผลให้ความเสี่ยงที่จะถูกหลอกขอข้อมูลทางไซเบอร์มีน้อยลง	0	+1	+1	0.67	<u>สามารถใช้ได้</u> 1 : เป็นการวัดทัศนคติมากกว่าประสบการณ์ ควรย้ายไปส่วนที่ 5 2 : คำถามตรงประเด็น เหมาะสม 3 : คำถามสอดคล้องกับ ส่วนที่ 5 เรื่องการสร้างความตระหนัก

ข้อ	คำถาม	ความคิดเห็นผู้เชี่ยวชาญ				การแปลผลและข้อเสนอแนะ
		1	2	3	IOC	
ส่วนที่ 5 คำถามเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยกลลวงหลอกขอข้อมูลทางไซเบอร์						
ลักษณะคำถามแบบตารางตัวเลือกหลายข้อ (Multiple choice grid) ให้ผู้ตอบแบบสอบถามเลือกตอบเพียงข้อเดียว โดยมีเกณฑ์ในการวัดระดับของคำตอบทั้งหมด 5 ระดับ ได้แก่ 5 = มากที่สุด 4 = มาก 3 = ปานกลาง 2 = น้อย และ 1 = น้อยที่สุด						
วัตถุประสงค์ : เพื่อศึกษาและเก็บข้อมูลเกี่ยวกับความตระหนักรู้เรื่องกลลวงหลอกขอข้อมูลทางไซเบอร์ของผู้ตอบแบบสอบถามและสามารถนำข้อมูลมาเปรียบเทียบวิเคราะห์หาความเชื่อมโยงกับปัจจัยต่างๆที่มีอิทธิพล						
5.	ท่านมีความตระหนักรู้เกี่ยวกับกลลวงหลอกขอข้อมูลทางไซเบอร์อย่างไร					
5.1	ท่านคิดว่าความไม่รอบคอบส่วนบุคคลส่งผลต่อการถูกหลอกขอข้อมูลทางไซเบอร์	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : ควรปรับเป็น "ท่านคิดว่าการขาดความรอบคอบ..." 2 : คำถามตรงประเด็น เหมาะสม
5.2	ท่านคิดว่าความไม่ทันระวังหรือการไม่สังเกตรายละเอียดมากพอส่งผลต่อการถูกหลอกขอข้อมูลทางไซเบอร์	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : สอดคล้อง แต่มีปัญหาเช่นเดียวกับข้อ 5.1 ในการใช้คำปฏิเสธ 2 : คำถามตรงประเด็น เหมาะสม
5.3	ท่านคิดว่าความประมาทที่คิดว่าข้อมูลที่ให้หรือกรอกไปนั้นไม่ได้สำคัญส่งผลต่อการถูกหลอกขอข้อมูลทางไซเบอร์	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : สอดคล้อง แต่การใช้คำว่า "ความประมาท" มีความหมายกว้างและอาจซ้ำซ้อนกับข้อ 5.1 และ 5.2 2 : คำถามตรงประเด็น เหมาะสม
5.4	ท่านคิดว่าความการมีเวลาที่จำกัดส่งผลต่อการถูกหลอกขอข้อมูลทางไซเบอร์ (ถูกเร่งให้กรอกข้อมูลในระยะเวลาที่กำหนด)	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามตรงประเด็น เหมาะสม
5.5	ท่านคิดว่าการถูกกลลวงหลอกขอข้อมูลทางไซเบอร์ส่งผลกระทบต่อด้านการเงิน (สูญเสียเงิน / มีเงินเข้าและออกจากบัญชีอย่างผิดปกติ)	+!	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามตรงประเด็น เหมาะสม

5.6	ท่านคิดว่าการถูกกลวงหลอกขอข้อมูลทางไซเบอร์ส่งผล กระทบต่อด้านความเป็นส่วนตัว (ถูกนำเอาข้อมูลไปเผยแพร่)	+1	+1	+1	1	<u>สามารถใช้ได้</u> 2 : คำถามตรงประเด็น เหมาะสม
5.7	ท่านคิดว่าการถูกกลวงหลอกขอข้อมูลทางไซเบอร์ส่งผล กระทบต่อด้านความปลอดภัยและทรัพย์สิน (มีคนติดตามหรือ ติดต่อเพื่อข่มขู่)	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : สอดคล้อง แต่ควรแยกแยะระหว่างความปลอดภัยทางดิจิทัล กับความปลอดภัยทางกายภาพให้ชัดเจน 2 : คำถามตรงประเด็น เหมาะสม
5.8	ท่านคิดว่าการศึกษาข้อมูลและวิธีระวังภัยจากกลโกงหลอกขอ ข้อมูลมีความสำคัญมาก	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : สอดคล้อง แต่คำถามกว้างเกินไป ควรเจาะจงถึงประเภท ของข้อมูลหรือวิธีระวังภัยที่มีประสิทธิภาพ 2 : คำถามตรงประเด็น เหมาะสม
5.9	ท่านคิดว่ากลวงหลอกขอข้อมูลทางไซเบอร์เป็นเรื่องใกล้ตัวที่ สามารถพบเจอในชีวิตประจำวันได้	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : ควรระบุว่าเป็นเรื่องใกล้ตัวในบริบทใด เช่น การใช้งาน โซเชียลมีเดีย หรือการทำธุรกรรมออนไลน์ 2 : คำถามตรงประเด็น เหมาะสม
5.10	ท่านคิดว่ากรณีความตระหนักรู้ที่มากพอส่งผลให้ความเสี่ยงที่ จะถูกหลอกขอข้อมูลทางไซเบอร์มีน้อยลง	+1	+1	+1	1	<u>สามารถใช้ได้</u> 1 : ควรเจาะจงประเภทของการตระหนักรู้ เช่น ความรู้เชิง เทคนิค หรือการระมัดระวังในการใช้งาน 2 : คำถามตรงประเด็น เหมาะสม

ข้อ	คำถาม	ความคิดเห็นผู้เชี่ยวชาญ				การแปลผลและข้อเสนอแนะ
		1	2	3	IOC	
ส่วนที่ 6 ข้อเสนอแนะต่อแนวทางการป้องกันภัยกลลวงหลอกขอข้อมูลทางไซเบอร์						
ลักษณะคำถามแบบปลายเปิด						
วัตถุประสงค์ : เพื่อเสนอแนะแนวทางและรูปแบบในการจัดทำข้อมูลเกี่ยวกับการระงับภัยกลลวงหลอกขอข้อมูลทางไซเบอร์ที่มีประสิทธิภาพมากยิ่งขึ้นในอนาคต						
6.	ท่านคิดว่าเนื้อหาและรูปแบบของข้อมูลการระงับภัยแบบใดที่มีประสิทธิภาพต่อท่านมากที่สุด	+1	+1	+1	1	สามารถใช้ได้ 1 : สอดคล้องกับวัตถุประสงค์ แต่คำถามกว้างเกินไป ควรแยกเป็นประเด็นย่อยๆ เช่น รูปแบบสื่อ (วิดีโอ บทความ อินโฟกราฟิก) เนื้อหา (กรณีศึกษา คำแนะนำทั่วไป เทคนิคเฉพาะทาง) และช่องทางการเผยแพร่ (โซเชียลมีเดีย เว็บไซต์ การอบรม) 2 : คำถามตรงประเด็น เหมาะสม 3 : เพิ่มส่วนของคำตอบ เพื่อ scope ที่เล็กลง และสะท้อนมากขึ้น

เมื่อผู้วิจัยได้ทำการวิเคราะห์ค่า IOC เสร็จสิ้นแล้ว จึงมีการนำเอาข้อเสนอแนะจากผู้เชี่ยวชาญทั้ง 3 ท่านมาปรับแบบสอบถามอีกครั้งเพื่อการตอบวัตถุประสงค์ที่ตั้งใจศึกษา โดยผลสรุปจากการออกแบบข้อคำถามสำหรับการเก็บแบบสอบถามออนไลน์จึงได้เป็นแบบสอบถามที่สมบูรณ์ตามรายละเอียดในภาคผนวก



4.2 ผลการวิจัย

4.2.1 ผลการวิจัยเชิงพรรณนา

4.2.1.1 ข้อมูลทางประชากรศาสตร์ของกลุ่มตัวอย่าง

ข้อมูลลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่างทั้ง 400 คน เป็นเพศหญิงมีสัดส่วนมากที่สุด คิดเป็นร้อยละ 59.3 เป็นเพศชาย คิดเป็นร้อยละ 27.3 และเป็นเพศทางเลือก คิดเป็นร้อยละ 13.5 ตามลำดับ กลุ่มตัวอย่างส่วนมากมีอายุอยู่ในช่วง 24-26 ปี คิดเป็นร้อยละ 54.3 ถัดมาคือช่วงอายุ 21-23 ปี คิดเป็นร้อยละ 23 ช่วงอายุ 27-28 ปี คิดเป็นร้อยละ 15.8 และอยู่ในช่วงอายุระหว่าง 18-20 ปี คิดเป็นร้อยละ 7 ระดับการศึกษาที่กลุ่มตัวอย่างเลือกตอบมากที่สุด ได้แก่ ปริญญาตรี หรือกำลังศึกษา คิดเป็น ร้อยละ 70.8 รองลงมาคือระดับ ปริญญาโท หรือสูงกว่า คิดเป็นร้อยละ 26.5 มัธยมศึกษาหรือกำลังศึกษาคิดเป็นร้อยละ 2.3 และน้อยที่สุดคือระดับ ปวช. / ปวส. อนุปริญญา หรือกำลังศึกษา คิดเป็นร้อยละ 0.5

ตารางที่ 4.2.1.1 ข้อมูลทางประชากรศาสตร์ของกลุ่มตัวอย่าง

		จำนวน (คน)	ร้อยละ
เพศ	เพศชาย	109	27.3
	เพศหญิง	237	59.3
	เพศทางเลือก	54	13.5
	รวม	400	100
ช่วงอายุ	18-20 ปี	28	7
	21-23 ปี	92	23
	24-26 ปี	217	54.3
	27-28 ปี	63	15.7
	รวม	400	100
การศึกษา	มัธยมศึกษา หรือกำลังศึกษา	9	2.3
	ปวช. / ปวส. / อนุปริญญา หรือกำลังศึกษา	2	0.5
	ปริญญาตรี หรือกำลังศึกษา	283	70.8
	ปริญญาโท หรือสูงกว่า	106	26.5
	รวม	400	100

4.2.1.2 ระดับความรู้ของกลุ่มตัวอย่างในเรื่องของกลลวงหลอกขอลข้อมูล

ข้อคำถามวัดความรู้เกี่ยวกับกลลวงทางไซเบอร์ (Phishing) ที่ผู้ตอบแบบสอบถามตอบถูกจำนวนมากที่สุด ได้แก่ ข้อที่ 4 ข้อใดเป็นนโยบายในการป้องกันการถูกหลอกขอลข้อมูลภายในองค์กรที่มีประสิทธิภาพมากที่สุด ตอบถูก 393 คน คิดเป็นร้อยละ 98.3 ข้อที่ 6 ข้อใดไม่ถือเป็นการละเมิด พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ตอบถูก 388 คน คิดเป็นร้อยละ 97 และข้อ 1 หากท่านได้รับข้อความทางโทรศัพท์โดยมีการอ้างว่าท่านมีพัสดุที่ตกค้างอยู่และต้องการให้ท่านคลิกลิงค์เพื่อกรอกข้อมูลส่วนตัวในระบบ ถือเป็นการหลอกลวงทางไซเบอร์รูปแบบใด ตอบถูก 384 คน คิดเป็นร้อยละ 96 ตามลำดับ

ตารางที่ 4.2.1.2 ระดับความรู้เกี่ยวกับกลลวงหลอกขอลข้อมูลทางไซเบอร์ของกลุ่มตัวอย่าง

ข้อคำถาม	ตอบถูก		ตอบผิด	
	จำนวน (คน)	ร้อยละ	จำนวน (คน)	ร้อยละ
1.หากท่านได้รับข้อความทางโทรศัพท์โดยมีการอ้างว่าท่านมีพัสดุที่ตกค้างอยู่และต้องการให้ท่านคลิกลิงค์เพื่อกรอกข้อมูลส่วนตัวในระบบ ถือเป็นการหลอกลวงทางไซเบอร์รูปแบบใด	384	96	16	4.1
2.ข้อใดเป็นข้อมูลที่เสี่ยงต่อการโดนหลอกขอลข้อมูลทางไซเบอร์	362	90.5	38	9.6
3.เว็บไซต์ใดต่อไปนี้ถือเป็นเว็บไซต์ที่มีความน่าเชื่อถือมากที่สุดในการกรอกข้อมูล	310	77.5	90	22.5
4.ข้อใดเป็นนโยบายในการป้องกันการถูกหลอกขอลข้อมูลภายในองค์กรที่มีประสิทธิภาพมากที่สุด	393	98.3	7	1.3

5.พฤติกรรมในข้อใดที่เสี่ยงต่อการถูกผู้ไม่ประสงค์ดีหลอกขอข้อมูลจากการสังเกตพฤติกรรมทางช่องทางโซเชียล (Angler Phishing) มากที่สุด	366	91.5	34	8.6
6.ข้อใดไม่ถือเป็นการละเมิด พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล	388	97	12	3.1
7.หากมีเบอร์ที่ไม่คุ้นโทรเข้ามาอ้างว่าเป็นเจ้าหน้าที่จากแบรนด์ดังที่คุณใช้ประจำและแจ้งว่าคุณเป็นผู้โชคดีที่ได้รับการสุ่มเลือกให้ได้รับของรางวัลพิเศษ โดยต้องทำการแอดไลน์เพื่อรับของรางวัล ถือว่าเสี่ยงที่จะเป็นกลโกงหลอกขอข้อมูลในประเภทใด	358	89.5	42	10.6
8.หากมีอีเมลส่งเข้ามาจาก TikTok ด้วยชื่อเมล Tiktokthailand@tiktok.co.th ให้คุณทำการอัปเดตข้อมูลส่วนตัวและอีเมลอีกครั้งไม่อย่างนั้นจะถูกระงับการใช้งาน ถือว่าเสี่ยงที่จะเป็นกลโกงหลอกขอข้อมูลในประเภทใด	378	94.5	22	5.5
9.หากมีอีเมลที่อ้างเป็นเพื่อนร่วมงานในองค์กรส่งไฟล์มาให้ดาวน์โหลด โดยที่เป็นชื่อเมลที่คล้ายคลึงกับอีเมลขององค์กร (เปลี่ยนจาก @ชื่อบริษัท.com เป็น @ชื่อบริษัท.co.th) ถือว่าเสี่ยงที่จะเป็นกลโกงหลอกขอข้อมูลในประเภทใด	318	79.5	82	20.5
10. หากท่านได้รับข้อความที่อ้างว่าส่งจากเพชบุ๊คให้รีบดำเนินการเปลี่ยนรหัสผ่านเพื่อให้บัญชีของท่านสามารถใช้งานได้ต่อ ท่านจะตัดสินใจดำเนินการอย่างไร	367	91.8	33	8.2

4.2.1.3 ระดับพฤติกรรมการระงับภัยกลวงหลอกขอข้อมูลทางไซเบอร์ในการใช้งานช่องทางออนไลน์

ผลการเก็บข้อมูลและวิเคราะห์ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน พบว่า กลุ่มตัวอย่างที่เป็น Gen Z มีพฤติกรรมการใช้งานช่องทางออนไลน์และมีพฤติกรรมในการระงับภัยกลวงหลอกทางไซเบอร์ อยู่ในระดับมาก โดยมีค่าเฉลี่ยรวมอยู่ที่ 3.95 และจากการวิเคราะห์ข้อมูลในพฤติกรรมการใช้งานช่องทางออนไลน์ของกลุ่มคน Gen Z แบบรายด้าน พบว่า กลุ่มคน Gen Z มีพฤติกรรมด้านการป้องกันตัวจากภัยกลวงหลอกขอข้อมูลทางไซเบอร์มากที่สุด มีค่าเฉลี่ยอยู่ที่ 4.41 ถัดมาคือพฤติกรรมด้านการศึกษาข้อมูลมีค่าเฉลี่ยอยู่ที่ 3.92 และพฤติกรรมด้านการจัดการความเป็นส่วนตัวของช่องทางออนไลน์ ค่าเฉลี่ยอยู่ที่ 3.31 ตามลำดับ

ตารางที่ 4.2.1.3 ระดับคะแนนพฤติกรรมการระงับภัยกลวงหลอกขอข้อมูลทางไซเบอร์ในการใช้งานช่องทางออนไลน์

ข้อคำถาม	ระดับความคิดเห็น		
	ค่าเฉลี่ย	S.D.	การแปลความ
พฤติกรรมด้านการจัดการความเป็นส่วนตัวของช่องทางออนไลน์			
1. ท่านไม่ทำการแชร์ข้อมูลส่วนตัวหรือบุคคลรอบตัวลงในช่องทางออนไลน์	4.23	0.78	มาก
2. ท่านมักจะตั้งค่าความเป็นส่วนตัวของช่องทางออนไลน์ทั้งหมดให้มีความปลอดภัยมากที่สุด (ยืนยันตัวตนด้วยอีเมลหรือเบอร์โทรศัพท์ ตั้งค่าการแจ้งเตือนเมื่อมีคนพยายามล่อลวง ไม่เปิดบัญชีให้เป็นสาธารณะ ใช้เครื่องมือ 2FA เพื่อจำกัดการเข้าถึงข้อมูล เป็นต้น)	4.39	0.68	มาก
ค่าเฉลี่ยรวมด้านการจัดการความเป็นส่วนตัวของช่องทางออนไลน์	3.31	0.73	ปานกลาง
พฤติกรรมด้านการศึกษาข้อมูลในการระงับภัยกลวงหลอกขอข้อมูลทางไซเบอร์			
3. ท่านให้ความสำคัญกับการค้นคว้าข่าวสาร ข้อมูลและวิธีการระงับภัยกลวงหลอกขอข้อมูลทางออนไลน์จากช่องทางต่างๆ (สื่อสังคมออนไลน์ เว็บไซต์ของทางการ)	4.14	0.72	มาก

4. ท่านให้ความสำคัญกับเนื้อหาของนโยบายความเป็นส่วนตัว ส่วนตัวของข้อมูลก่อนที่จะใช้งานแอปพลิเคชันต่างๆ เสมอ	3.79	0.93	มาก
5. ท่านศึกษาข้อมูลเกี่ยวกับภัยกลโกงหลอกขอข้อมูล ทางโซเชียลมีเดียอยู่เสมอ	4.05	0.79	มาก
6. ท่านเคยเข้าอบรมวิธีการระวังตนเองจากภัยกลโกง หลอกขอข้อมูลทางโซเชียลมีเดียหรือไม่	3.72	2.30	มาก
ค่าเฉลี่ยรวมด้านการศึกษาข้อมูลในการระวังภัย	3.92	1.18	มาก
พฤติกรรมด้านการป้องกันตัวจากภัยกลโกงหลอกขอข้อมูลทางโซเชียลมีเดีย			
7. ท่านมีการโหลดแอปพลิเคชันในการตรวจสอบ มีจฉฉฉ หรือมีการเช็คชื่อเมล เบอร์โทรที่ส่งมาก่อน เสมอ	4.30	0.82	มาก
8. ท่านไม่ดาวน์โหลดหรือคลิกลิงค์ที่ไม่ทราบที่มาที่ไปแม้ ถูกส่งจากอีเมลของบุคคลที่รู้จัก	4.46	0.68	มาก
9. ท่านทำการบล็อกเบอร์โทรศัพท์ที่เป็นมีจฉฉฉ	4.47	0.74	มาก
ค่าเฉลี่ยรวมด้านการป้องกันตัว	4.41	0.75	มาก
เฉลี่ยรวม	3.95	0.94	มาก

4.2.1.4 ระดับประสบการณ์และการรับรู้ในเรื่องกลโกงหลอกขอข้อมูล

ผลการเก็บข้อมูลและวิเคราะห์ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน พบว่ากลุ่มตัวอย่างที่เป็น Gen Z มีประสบการณ์และการรับรู้เกี่ยวกับเรื่องกลโกงหลอกขอข้อมูลทางโซเชียลมีเดีย อยู่ในระดับน้อย โดยมีค่าเฉลี่ยอยู่ที่ 1.92 โดยส่วนมากกลุ่มตัวอย่างและคนรอบข้างเคยมีประสบการณ์ถูกหลอกสำเร็จผ่านการใช้กลโกงหลอกขอข้อมูลทางโทรศัพท์ ค่าเฉลี่ยอยู่ที่ 2.01 ผ่านช่องทางข้อความ ค่าเฉลี่ยอยู่ที่ 1.93 และน้อยที่สุดคือการถูกหลอกสำเร็จผ่านช่องทางอีเมล ค่าเฉลี่ยอยู่ที่ 1.83

ตารางที่ 4.2.1.4 ระดับประสบการณ์และการรับรู้ในเรื่องกลวงหลอกขอข้อมูลทางไซเบอร์

ข้อคำถาม	ระดับความคิดเห็น		
	ค่าเฉลี่ย	S.D.	การแปลความ
1.ท่านหรือบุคคลรอบตัวเคยมีประสบการณ์ถูกหลอกขอข้อมูลทางไซเบอร์ จากช่องทางข้อความสำเร็จ	1.93	1.40	น้อย
2.ท่านหรือบุคคลรอบตัวเคยมีประสบการณ์ถูกหลอกขอข้อมูลทางไซเบอร์ จากช่องทางอีเมลสำเร็จ	1.83	1.24	น้อย
3.ท่านหรือบุคคลรอบตัวเคยมีประสบการณ์ถูกหลอกขอข้อมูลทางไซเบอร์ จากช่องทางโทรศัพท์สำเร็จ	2.01	1.37	น้อย
เฉลี่ยรวม	1.92	1.34	น้อย

4.2.1.5 ระดับความตระหนักรู้เกี่ยวกับกลวงหลอกขอข้อมูลทางไซเบอร์

ผลการเก็บข้อมูลและวิเคราะห์ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน พบว่า กลุ่มตัวอย่างที่เป็น Gen Z มีระดับความตระหนักรู้เกี่ยวกับเรื่องกลวงหลอกขอข้อมูลทางไซเบอร์ อยู่ในระดับมาก โดยกลุ่มตัวอย่างมีความคิดเห็นว่า การมีความตระหนักรู้ที่มากพอ เช่น ความรู้เกี่ยวกับภัยไซเบอร์ หรือการระมัดระวังในการใช้งานช่องทางออนไลน์ ส่งผลให้ความเสี่ยงที่จะถูกหลอกขอข้อมูลทางไซเบอร์มีน้อยลง มีค่าเฉลี่ยคิดเป็น 4.59 รองลงมาคือ คิดว่ากลวงหลอกขอข้อมูลทางไซเบอร์เป็นเรื่องใกล้ตัวที่สามารถพบเจอในชีวิตประจำวันได้ (การใช้งานช่องทางออนไลน์ การทำธุรกรรมทางการเงินออนไลน์ การสั่งซื้อสินค้าออนไลน์) มีค่าเฉลี่ยอยู่ที่ 4.58 และคิดว่าการไม่ทันระวัง หรือการไม่สังเกตรายละเอียดมากพอส่งผลต่อการถูกหลอกขอข้อมูลทางไซเบอร์ มีค่าเฉลี่ย อยู่ที่ 4.51

ตารางที่ 4.2.1.5 ระดับคะแนนของความตระหนักรู้เกี่ยวกับกลวงหลอกขอข้อมูลทางไซเบอร์

ข้อคำถาม	ระดับความคิดเห็น		
	ค่าเฉลี่ย	S.D.	การแปลความ
1.ท่านมีการคำนึงถึงความเสี่ยงของการถูกนำเอาข้อมูลส่วนตัวไปใช้ในทางที่ไม่ดีอยู่เสมอ	4.36	0.68	มาก
2.ท่านคิดว่าการขาดความรอบคอบส่วนบุคคลส่งผลต่อการถูกหลอกขอข้อมูลทางไซเบอร์	4.45	0.86	มาก
3.ท่านคิดว่าการขาดความรู้และประสบการณ์เกี่ยวกับภัยไซเบอร์ส่งผลต่อการถูกหลอกขอข้อมูลทางไซเบอร์	4.40	0.85	มาก

4. ท่านคิดว่าการไม่ทันระว่างหรือการไม่สังเกต รายละเอียดมากพอส่งผลต่อการถูกหลอกขอข้อมูลทาง ไซเบอร์	4.51	0.63	มากที่สุด
5. ท่านคิดว่าการคิดว่าข้อมูลที่ให้หรือกรอกไปนั้นไม่ได้ สำคัญส่งผลต่อการถูกหลอกขอข้อมูลทางไซเบอร์	4.14	1.05	มาก
6. ท่านคิดว่าความการมีเวลาที่จำกัดส่งผลต่อการถูก หลอกขอข้อมูลทางไซเบอร์ (ถูกเร่งให้กรอกข้อมูลใน ระยะเวลาที่กำหนด)	4.33	0.74	มาก
7. ท่านคิดว่าการถูกกลลวงหลอกขอข้อมูลทางไซเบอร์ ส่งผลกระทบต่อด้านการเงิน (สูญเสียเงิน / มีเงินเข้า และออกจากบัญชีอย่างผิดปกติ)	4.45	0.65	มาก
8. ท่านคิดว่าการถูกกลลวงหลอกขอข้อมูลทางไซเบอร์ ส่งผลกระทบต่อด้านความเป็นส่วนตัว (ถูกนำเอาข้อมูล ไปเผยแพร่)	4.50	0.66	มาก
9. ท่านคิดว่าการถูกกลลวงหลอกขอข้อมูลทางไซเบอร์ ส่งผลกระทบต่อด้านความปลอดภัยทางกายภาพและ ทรัพย์สิน (มีคนติดตามหรือติดต่อเพื่อข่มขู่)	4.07	0.89	มาก
10. ท่านคิดว่าการศึกษาข้อมูลเตือนภัยและวิธีระวังภัย จากกลโกงหลอกขอข้อมูลมีความสำคัญมาก	4.43	0.62	มาก
11. ท่านคิดว่ากลลวงหลอกขอข้อมูลทางไซเบอร์เป็น เรื่องใกล้ตัวที่สามารถพบเจอในชีวิตประจำวันได้ (การ ใช้งานช่องทางออนไลน์ การทำธุรกรรมทางการเงิน ออนไลน์ การสั่งซื้อสินค้าออนไลน์)	4.58	0.58	มากที่สุด
12. ท่านคิดว่าการมีความตระหนักรู้ที่มากพอ เช่น ความรู้เกี่ยวกับภัยไซเบอร์ หรือการระมัดระวังในการใช้ งานช่องทางออนไลน์ ส่งผลให้ความเสี่ยงที่จะถูกหลอก ขอข้อมูลทางไซเบอร์มีน้อยลง	4.59	0.61	มากที่สุด
เฉลี่ยรวม	4.40	0.74	มาก

4.2.1.6 ข้อเสนอแนะต่อแนวทางการป้องกันภัยกลวงหลอกขอข้อมูลทางไซเบอร์

พบว่ากลุ่มตัวอย่างที่เป็นคน Gen Z มีความคิดเห็นต่อการเสนอแนะให้จัดทำข้อมูลการระวังภัยกลวงหลอกขอข้อมูลทางไซเบอร์ โดยใช้เนื้อหาของเกร็ดความรู้ที่เข้าใจง่าย เพื่อให้รู้หลักการและวิธีป้องกันภัย คิดเป็นร้อยละ 44 และจัดทำในรูปแบบของอินโฟกราฟฟิกสรุปข้อมูล คิดเป็นร้อยละ 40 เผยแพร่ในช่องทางสื่อสังคมออนไลน์ (เฟซบุ๊ก ไลน์ เอกซ์ อินสตราแกรม ยูทูบ) คิดเป็นร้อยละ 62.5

ตารางที่ 4.2.1.6 ข้อเสนอแนะต่อแนวทางการจัดทำข้อมูลสำหรับการป้องกันภัยกลวงหลอกขอข้อมูลทางไซเบอร์

ข้อคำถาม	จำนวน (คน)	ร้อยละ
1.ท่านคิดว่าเนื้อหาของข้อมูลการระวังภัยแบบใดที่มีประสิทธิภาพต่อท่านมากที่สุด		
กรณีศึกษาจากผู้ที่มีประสบการณ์	75	18.8
คำแนะนำทั่วไปในการใช้งานสื่อสังคมออนไลน์อย่างปลอดภัย	82	20.5
การให้ความรู้เกี่ยวกับเทคนิคเฉพาะทางที่เกี่ยวข้องกับภัยทางไซเบอร์	67	16.8
เกร็ดความรู้ที่เข้าใจง่ายเพื่อให้รู้หลักการและวิธีป้องกันภัย	176	44
รวม	400	100
2.ท่านคิดว่ารูปแบบของข้อมูลการระวังภัยแบบใดที่มีประสิทธิภาพต่อท่านมากที่สุด		
วิดีโอให้ความรู้	122	30.5
บทความ	89	22.2
อินโฟกราฟฟิกสรุปข้อมูล	160	40
การสัมภาษณ์ผู้เชี่ยวชาญ	29	7.5
รวม	400	100
3.ท่านคิดว่าช่องทางในการเผยแพร่ข้อมูลการระวังภัยช่องทางใดที่มีประสิทธิภาพต่อท่านมากที่สุด		
ช่องทางสื่อสังคมออนไลน์ (เฟซบุ๊ก ไลน์ เอกซ์ อินสตราแกรม ยูทูบ)	250	62.5
เว็บไซต์ของหน่วยงานที่เป็นทางการ	51	12.7
อินฟลูเอนเซอร์	59	14.7
ช่องทางโทรทัศน์ หนังสือพิมพ์ หรือวิทยุ	40	10
รวม	400	100

ข้อเสนอแนะเพิ่มเติมในการจัดทำข้อมูลสำหรับการระงับภัยทางไซเบอร์

ควรเป็นเนื้อหาที่สั้น กระชับ เข้าใจง่ายน่าจะส่งผลให้คนอ่านเกิดความอยากอ่านมากขึ้น

ผู้สูงอายุมักจะถูกโดนหลอกง่ายอยากให้ทางสื่อโทรทัศน์ หรือ TikTok ทำข้อมูลออกมาบ่อยๆ แบบ เวอร์ชันเข้าใจง่าย

เน้นการใช้ภาพมากกว่าข้อความเพื่อดึงความสนใจ

ควรเป็นวิดีโอและมี infographic ควบคู่

ควรใช้ภาษาเข้าใจง่ายเพื่อให้คนที่อ่านไม่เก่ง

ข่าวเรื่องมีฉ้อฉลส่วนมาก เวลาที่คนโดน ทุกคนก็จะบอกว่า "เห็นข่าวนี้มาก็เยอะ เราเองก็ระวัง ไม่คิดว่าจะเป็นตัวเอง" เลยมองว่า เรื่องนี้ไม่ว่าคนจะระวังขนาดไหน หรือ ว่ามีความรู้แค่ไหน มันก็ผิดพลาดและโดนหลอกได้ จะดาราคนดัง คนฉลาดแค่ไหนก็โดนได้เหมือนกัน เลยมองว่าทางที่ดีคือ ไม่คุยกับมีฉ้อฉลแต่แรก ส่วนมากคนที่โดนก็จะโดนต่อเป็นทอดๆ

มีตัวอย่างข้อความหรือรูปภาพประกอบ เพื่ออนาคตเกิดเหตุการณ์กับตัวผู้อ่าน จะได้เตรียมตัวและตั้งรับได้อย่างมีสติมากขึ้น

อัปเดตข้อมูลให้ทันสมัย – ภัยคุกคามทางไซเบอร์เปลี่ยนแปลงตลอดเวลา จึงควรมีการปรับปรุงข้อมูลให้เป็นปัจจุบัน

ทำเป็น Tiktok คลิปสั้นๆ

4.2.2 ผลการวิจัยเชิงอนุมาน

4.2.2.1 การวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรข้อมูลทางประชากรศาสตร์กับความตระหนักรู้เท่าทันภัยกลลวงหลอกขอลข้อมูลทางไซเบอร์

ในการวิเคราะห์หาความสัมพันธ์ของตัวแปรอิสระด้านข้อมูลทางประชากรศาสตร์ทางผู้วิจัยเลือกใช้วิธีการทดสอบด้วยวิธีการวิเคราะห์ความแปรปรวนทางเดียว หรือ One-way ANOVA ในการทดสอบตัวแปรด้านข้อมูลทางประชากรศาสตร์แต่ละกลุ่มโดยจะเริ่มจากการตรวจค่าความแปรปรวนของแต่ละตัวแปรด้วยการใช้วิธี Levene Test ก่อน หากผลการวิเคราะห์ได้ค่าแปรปรวนที่เท่ากันให้ทดสอบต่อด้วย F-Test หากผลการวิเคราะห์ได้ค่าแปรปรวนของข้อมูลอย่างน้อย 2 กลุ่มที่แตกต่างกัน จึงทดสอบต่อด้วยการใช้ Welch หลังจากนั้นหากพบว่าค่าเฉลี่ยของแต่ละกลุ่มมีความแตกต่างกันจึงทดสอบการหา Post Hoc. Multiple Comparisons ต่อไป

4.2.2.1.1 ตารางแสดงค่าความแปรปรวนของความตระหนักรู้เท่าทันกลวงหลอกขอข้อมูลทางไซเบอร์ จำแนกตามตัวแปร เพศ

ความตระหนักรู้เท่าทันกลวงหลอกขอข้อมูลทางไซเบอร์

Test of Homogeneity of Variances			
Levene Statistic	df1	df2	Sig.
4.115	2	397	.017*

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางการทดสอบด้วย Levene Test พบว่า ค่าความตระหนักรู้เท่าทันกลวงหลอกขอข้อมูลทางไซเบอร์ที่จำแนกด้วยตัวแปรเพศ มีค่า Sig. อยู่ที่ .017 ซึ่งมีค่าน้อยกว่านัยสำคัญทางสถิติ จึงทำการทดสอบด้วยการใช้ Welch

ความตระหนักรู้เท่าทันกลวงหลอกขอข้อมูลทางไซเบอร์

Robust Tests of Equality of Means				
	Statistic	df1	df2	Sig.
Welch	9.854	2	142.225	.000*

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางการทดสอบด้วย Welch พบว่า ค่าความตระหนักรู้เท่าทันกลวงหลอกขอข้อมูลทางไซเบอร์ที่จำแนกด้วยตัวแปรเพศ มีค่า Sig. อยู่ที่ .000 ซึ่งมีค่าน้อยกว่านัยสำคัญทางสถิติ จึงทำการทดสอบหาความแตกต่างด้วยการทำ Post Hoc. Multiple Comparisons: Games-Howell ดังตารางหน้าถัดไป

ความตระหนักรู้เท่าทันกลลวงหลอกของข้อมูลทางไซเบอร์

Multiple Comparisons: Games-Howell				
เพศ	เพศ (เปรียบเทียบ)	Mean Difference	Std. Error	Sig.
เพศชาย	เพศหญิง	.01553	.03784	.911
	เพศทางเลือก	-.20261	.05308	.001*
เพศหญิง	เพศชาย	-.01553	.03784	.911
	เพศทางเลือก	.03784	.05011	.000*
เพศทางเลือก	เพศชาย	.20261	.05308	.001*
	เพศหญิง	.21814	.05011	.000*

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางการทดสอบ Post Hoc. ด้วยวิธีของ Games-Howell พบว่า ระดับความตระหนักรู้เท่าทันกลลวงหลอกของข้อมูลทางไซเบอร์ของตัวแปรเพศทางเลือกมีความแตกต่างกับตัวแปรเพศชายและเพศหญิง โดยมีนัยสำคัญเชิงสถิติ และมีค่า Sig. อยู่ที่ .001 และ .000 ตามลำดับ

4.2.2.1.2 ค่าความแปรปรวนของความตระหนักรู้เท่าทัน จำแนกตามตัวแปรอายุ

ความตระหนักรู้เท่าทันกลลวงหลอกของข้อมูลทางไซเบอร์

Test of Homogeneity of Variances			
Levene Statistic	df1	df2	Sig.
.469	3	396	.704

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางการทดสอบด้วย Levene Test พบว่า ค่าความตระหนักรู้เท่าทันกลลวงหลอกของข้อมูลทางไซเบอร์ที่จำแนกด้วยตัวแปรช่วงอายุ มีค่า Sig. อยู่ที่ .704 ซึ่งมีความมากกว่านัยสำคัญทางสถิติ จึงทำการวิเคราะห์ข้อมูลต่อด้วยการหาค่า F

ความตระหนักรู้เท่าทันกลลวงหลอกของข้อมูลทางไซเบอร์

ANOVA					
ความแปรปรวน	SS	df	MS	F	Sig.
ระหว่างกลุ่ม	1.674	3	.588	4.625	.003*
ภายในกลุ่ม	47.762	396	.121		
รวม	49.436	399			

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตาราง ANOVA พบว่า ค่าความตระหนักรู้เท่าทันกลลวงหลอกของข้อมูลทางไซเบอร์ที่จำแนกด้วยตัวแปรอายุ มีค่า Sig. อยู่ที่ .003 ซึ่งมีค่าน้อยกว่านัยสำคัญทางสถิติ จึงทำการทดสอบหาค่าความแตกต่างด้วยการทำ Post Hoc. Multiple Comparisons: LSD

ความตระหนักรู้เท่าทันกลลวงหลอกของข้อมูลทางไซเบอร์

Multiple Comparisons: LSD				
ช่วงอายุ	ช่วงอายุ (เปรียบเทียบ)	Mean Difference	Std. Error	Sig.
18-20 ปี	21-23 ปี	.04645	.07496	.536
	24-26 ปี	.13767	.06974	.049*
	27-28 ปี	-.02315	.07888	.769
21-23 ปี	18-20 ปี	-.04645	.07496	.536
	24-26 ปี	.09122	.04321	.035*
	27-28 ปี	-.06960	.05679	.221
24-26 ปี	18-20 ปี	-.13767	.06974	.049*
	21-23 ปี	-.09122	.04321	.035*
	27-28 ปี	-.16082	.04970	.001*
27-28 ปี	18-20 ปี	.02315	.07888	.769
	21-23 ปี	.06960	.05679	.221
	24-26 ปี	.16082	.04970	.001*

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางการทดสอบ Post Hoc. ด้วยวิธีของ LSD พบว่า ระดับความตระหนักรู้เท่าทันกลวงหลอกขอข้อมูลทางไซเบอร์ ที่จำแนกด้วยตัวแปรช่วงอายุ มีความแตกต่างกันโดย ช่วงอายุ 18-20 ปี และ 21-23 ปี มีความแตกต่างกับช่วงอายุ 24-26 ปี มีค่า Sig. อยู่ที่ .049 และ .035 ตามลำดับ และช่วงอายุ 24-26 ปี มีความแตกต่างกับช่วงอายุ 27-28 ปี อยู่ที่ .001

4.2.2.1.3 ตารางแสดงค่าความแปรปรวนของความตระหนักรู้เท่าทันกลวงหลอกขอข้อมูลทางไซเบอร์ จำแนกตามตัวแปร การศึกษา
ความตระหนักรู้เท่าทันกลวงหลอกขอข้อมูลทางไซเบอร์

Test of Homogeneity of Variances			
Levene Statistic	df1	df2	Sig.
2.764	3	396	.042*

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางการทดสอบด้วย Levene Test พบว่า ค่าความตระหนักรู้เท่าทันกลวงหลอกขอข้อมูลทางไซเบอร์ที่จำแนกด้วยตัวแปรการศึกษา มีค่า Sig. อยู่ที่ .042 ซึ่งมีค่าน้อยกว่า นัยสำคัญทางสถิติ จึงทำการทดสอบด้วยการใช้ Welch

ความตระหนักรู้เท่าทันกลวงหลอกขอข้อมูลทางไซเบอร์

Robust Tests of Equality of Means				
	Statistic	df1	df2	Sig.
Welch	.231	3	4.442	.871

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

จากตารางการทดสอบด้วย Welch พบว่า ค่าความตระหนักรู้เท่าทันกลวงหลอกขอข้อมูลทางไซเบอร์ที่จำแนกด้วยตัวแปรการศึกษา มีค่า Sig. อยู่ที่ .871 ซึ่งมีค่ามากกว่านัยสำคัญทางสถิติ ไม่พบความแตกต่าง

4.2.2.2 ผลการวิเคราะห์ปัจจัยที่มีอิทธิพลต่อความตระหนักรู้เกี่ยวกับกลวงหลอกขอข้อมูลทางโซเชียล ของกลุ่มคน Gen Z

ผู้จัดทำได้ทำการวิเคราะห์ความสัมพันธ์ระหว่างปัจจัยความรู้เกี่ยวกับกลวงหลอกขอข้อมูลทางโซเชียล พฤติกรรมการใช้งานช่องทางออนไลน์ ด้านการจัดการความเป็นส่วนตัวของช่องทางออนไลน์ พฤติกรรมด้านการศึกษาข้อมูลเกี่ยวกับการระงับภัย พฤติกรรมเกี่ยวกับการป้องกันตัวจากภัยกลวงหลอกขอข้อมูลทางโซเชียล และประสบการณ์การรับรู้เกี่ยวกับกลวงหลอกขอข้อมูลทางโซเชียล ที่มีอิทธิพลต่อความตระหนักรู้เท่าทันของกลุ่มคน Gen Z ด้วยวิธีการวิเคราะห์แบบถดถอยพหุคูณ หรือ Multiple Regression Analysis โดยสามารถสรุปผลการวิเคราะห์ข้อมูลออกมาได้ดังนี้

ตารางที่ 4.2.2.2.1 ผลลัพธ์ในการสรุปรูปแบบสมการถดถอย (Model Summary)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.469 ^a	.220	.210	.31293

- a. Predictors: (Constant), ความรู้เกี่ยวกับกลวงหลอกขอข้อมูลทางโซเชียล, พฤติกรรมด้านการจัดการความเป็นส่วนตัว, พฤติกรรมการศึกษาข้อมูล, พฤติกรรมการป้องกันตัว, ประสบการณ์การรับรู้

จากตารางที่ 4.2.2.2.1 พบว่าปัจจัยทั้ง 5 ด้านอันประกอบด้วยความรู้เกี่ยวกับกลวงหลอกขอข้อมูลทางโซเชียล พฤติกรรมการใช้งานช่องทางออนไลน์ ด้านการจัดการความเป็นส่วนตัวของช่องทางออนไลน์ พฤติกรรมด้านการศึกษาข้อมูลเกี่ยวกับการระงับภัย พฤติกรรมเกี่ยวกับการป้องกันตัวจากภัยกลวงหลอกขอข้อมูลทางโซเชียล และประสบการณ์การรับรู้เกี่ยวกับกลวงหลอกขอข้อมูลทางโซเชียล มีความสัมพันธ์กับระดับความตระหนักรู้เท่าทันกลวงหลอกขอข้อมูลทางโซเชียลของกลุ่ม Gen Z อย่างมีนัยสำคัญทางสถิติ และมีอิทธิพลในการพยากรณ์ระดับความตระหนักรู้เท่าทันอยู่ที่ ร้อยละ 21 โดยมีค่า Adjusted R Square อยู่ที่ .210

ตารางที่ 4.2.2.2 ตาราง ANOVA เพื่อวิเคราะห์หาค่าปัจจัยที่มีอิทธิพลต่อความตระหนักรู้เท่าทันกลลวงหลอกขอข้อมูลทางไซเบอร์ของกลุ่มคน Gen Z

ANOVA						
Model		SS	df	MS	F	Sig.
1	ระหว่างกลุ่ม	10.852	5	2.170	22.164	.000 ^b
	ภายในกลุ่ม	38.584	394	.098		
	รวม	49.436	399			

*มีนัยสำคัญทางสถิติที่ระดับ 0.05

- a. Dependent Variable: ความตระหนักรู้เท่าทันกลลวงหลอกขอข้อมูลทางไซเบอร์
- b. Predictors: (Constant), ความรู้เกี่ยวกับกลลวงหลอกขอข้อมูลทางไซเบอร์, พฤติกรรมด้านการจัดการความเป็นส่วนตัว, พฤติกรรมการศึกษาข้อมูล, พฤติกรรมการป้องกันตัว, ประสบการณ์การรับรู้

จากตารางดังกล่าว พบว่า ปัจจัยที่มีอิทธิพลต่อความตระหนักรู้เท่าทันกลลวงหลอกขอข้อมูลทางไซเบอร์ของกลุ่มคน Gen Z มีค่า F อยู่ที่ 22.164 และมีค่า Sig. อยู่ที่ 0.000 โดยมีค่าน้อยกว่าระดับนัยสำคัญทางสถิติ สามารถทำการสรุปข้อมูลได้ว่า ปัจจัยความรู้เกี่ยวกับกลลวงหลอกขอข้อมูลทางไซเบอร์ พฤติกรรมการใช้งานช่องทางออนไลน์ ด้านการจัดการความเป็นส่วนตัวของช่องทางออนไลน์ พฤติกรรมด้านการศึกษาข้อมูลเกี่ยวกับการระวังภัย พฤติกรรมเกี่ยวกับการป้องกันตัวจากภัยกลลวงหลอกขอข้อมูลทางไซเบอร์ และประสบการณ์การรับรู้เกี่ยวกับกลลวงหลอกขอข้อมูลทางไซเบอร์ ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขอข้อมูลทางไซเบอร์ อย่างน้อย 1 ตัวแปร จึงมีการทดสอบ T-Test เพื่อหาความสัมพันธ์ของแต่ละตัวแปรกับความตระหนักรู้เท่าทันสำหรับการตอบสมมติฐานของงานวิจัยในครั้งนี้

ตารางที่ 4.2.2.3 ตารางการวิเคราะห์ Multiple Regression เพื่อหาค่า Coefficients ของปัจจัยที่มีอิทธิพลต่อความตระหนักรู้เท่าทันกลลวงหลอกขอข้อมูลทางไซเบอร์ของกลุ่มคน Gen Z

ตัวแปรอิสระ	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	B		
(Constant)	2.910	.195		14.939	.000*
ความรู้เกี่ยวกับกลลวงหลอกขอข้อมูลทางไซเบอร์	.067	.109	.029	.614	.540
พฤติกรรมการใช้งานช่องทางออนไลน์ ด้านการจัดการความเป็นส่วนตัวของช่องทางออนไลน์	.161	.029	.256	5.588	.000*
พฤติกรรมด้านการศึกษาข้อมูลเกี่ยวกับการระวังภัย	-.031	.030	-.053	-1.063	.288
พฤติกรรมเกี่ยวกับการป้องกันตัวจากภัยกลลวงหลอกขอข้อมูลทางไซเบอร์	.211	.032	.311	6.661	.000*
ประสบการณ์การรับรู้เกี่ยวกับกลลวงหลอกขอข้อมูลทางไซเบอร์	-.036	.014	-.123	-2.503	.013*

*มีนัยสำคัญทางสถิติที่ระดับ 0.05 / ระดับความเชื่อมั่น 95%

a. Dependent Variable: ความตระหนักรู้เท่าทันกลลวงหลอกขอข้อมูลทางไซเบอร์

จากตารางดังกล่าว สามารถสรุปผลการวิจัยได้ว่า ปัจจัยพฤติกรรมการใช้งานช่องทางออนไลน์ ด้านการจัดการความเป็นส่วนตัวของช่องทางออนไลน์ มีค่า Sig. อยู่ที่ 0.000 ปัจจัยพฤติกรรมเกี่ยวกับการป้องกันตัวจากภัยกลลวงหลอกขอข้อมูลทางไซเบอร์ มีค่า Sig. อยู่ที่ 0.000 และปัจจัยประสบการณ์การรับรู้เกี่ยวกับกลลวงหลอกขอข้อมูลทางไซเบอร์ เบอร์ มีค่า Sig. อยู่ที่ 0.013 ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญทางสถิติ 0.05

จากผลข้อมูลการวิเคราะห์สามารถสรุปการยอมรับต่อสมมติฐานการวิจัยได้ดังนี้

สมมติฐานในการวิจัย 1

ลักษณะทางประชากรศาสตร์ (เพศ ช่วงอายุ การศึกษา) ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z

ตัวแปรอิสระด้านประชากรศาสตร์ที่ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z ได้แก่ ตัวแปรเพศ และตัวแปรช่วงอายุ

ตัวแปรอิสระด้านประชากรศาสตร์ที่ไม่ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z ได้แก่ ตัวแปรการศึกษา

สมมติฐานในการวิจัย 2

ความรู้เกี่ยวกับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z

ตัวแปรอิสระด้านความรู้เกี่ยวกับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ ไม่ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z

สมมติฐานในการวิจัย 3

พฤติกรรมในการใช้งานช่องทางออนไลน์ของบุคคล ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z

ตัวแปรด้านปัจจัยพฤติกรรมการใช้งานช่องทางออนไลน์ ด้านการจัดการความเป็นส่วนตัวส่วนตัวของช่องทางออนไลน์ และ ปัจจัยพฤติกรรมเกี่ยวกับการป้องกันตัวจากภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z

ตัวแปรอิสระด้านพฤติกรรมด้านการศึกษาข้อมูลเกี่ยวกับการระวังภัยไม่ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z

สมมติฐานในการวิจัย 4

ประสบการณ์และรับรู้ภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z

ตัวแปรด้านปัจจัยประสบการณ์และรับรู้ภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z

4.3 อภิปรายผลการวิจัย

จากผลการศึกษาและเก็บรวบรวมข้อมูลสามารถทำการสรุปการอภิปรายผลของข้อมูลต่อสมมติฐานตั้งต้นได้ดังนี้

สมมติฐานที่ 1 ลักษณะทางประชากรศาสตร์ (เพศ ช่วงอายุ การศึกษา) ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z

จากการเก็บรวบรวมและวิเคราะห์ข้อมูลทำให้พบว่า ปัจจัยด้านประชากรศาสตร์ที่ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ ของกลุ่ม Gen Z มี 2 ปัจจัย ได้แก่ ตัวแปรเรื่องเพศ และตัวแปรเรื่องช่วงอายุ โดยมีนัยสำคัญทางสถิติอยู่ที่ 0.05 สอดคล้องกับงานของยุบล เบ็ญจรงค์กิจ (2543) และศิริวรรณ เสรีรัตน์ (2538) ที่กล่าวว่า อายุและเพศที่มีความแตกต่างกันย่อมมีผลกระทบต่อพฤติกรรมหรือการรับรู้เรื่องราวต่างๆ ได้ต่างกัน เนื่องจากความแตกต่างในเชิงกายภาพแล้ว การถูกอบรมเลี้ยงดู ค่านิยม หรือทัศนคติของแต่ละเพศหรือคนในแต่ละช่วงวัยก็ย่อมมีความแตกต่างกันออกไปในสังคม โดยจากกลุ่มตัวอย่างทั้งหมด 400 คนพบว่า เพศหญิงมีสัดส่วนมากที่สุด จึงมีความน่าจะเป็นสูงที่เพศหญิงอาจถูกปลุกฝังให้มีความระมัดระวังตัวในประเด็นต่างๆ มากกว่าเพศชายและเพศทางเลือก ทำให้เกิดความตระหนักรู้ในเรื่องของภัยไซเบอร์และมีความระมัดระวังในการใช้งานในชีวิตประจำวันมากกว่า และยังพบว่าช่วงอายุแม้จะเป็นการแบ่งกลุ่มระหว่างวัยที่ค่อนข้างแคบแต่ก็แสดงถึงความแตกต่างทางด้านทัศนคติและมุมมองต่อเรื่องของภัยทางไซเบอร์ให้เห็นเช่นกัน ซึ่งสอดคล้องกับงานของคณัญญา อิมใจ (2565) เนื่องจากกลุ่มคนวัย Gen Z ถือเป็นกลุ่มช่วงอายุที่มีลักษณะพิเศษที่ค่อนข้างมีความแตกต่างจากกลุ่มช่วงวัยอื่น ๆ กล่าวคือเป็นคนที่มีความสำคัญกับเรื่องราวเกี่ยวกับเทคโนโลยีและพยายามที่จะวิ่งตามการพัฒนาของเทคโนโลยีใหม่ๆ อยู่อย่างสม่ำเสมอ จึงทำให้คนกลุ่มวัยนี้มีความต้องการในการที่จะรับรู้ข้อมูล ข่าวสาร เกี่ยวกับเรื่องภัยไซเบอร์มากกว่าคนในช่วงวัยอื่น ๆ จึงทำให้ระดับการรับรู้ของคนในช่วงวัยนี้ค่อนข้างมีความหลากหลายตั้งแต่ยังอายุน้อย และทำให้มีการเปิดรับข่าวสารที่เพิ่มมากขึ้นตามอายุได้อีกด้วย

ตัวแปรที่ไม่ส่งผลต่อความตระหนักรู้ ได้แก่ การศึกษา ทำให้พบว่าระดับการศึกษาที่ต่างกันออกไปนั้นไม่ได้ส่งผลกระทบต่อความตระหนักรู้ เนื่องจากสังคมในปัจจุบันคนส่วนมากมักใช้เวลาอยู่ในช่องทางออนไลน์ ทำให้สามารถเข้าถึงข้อมูล ข่าวสาร หรือพบเจอเหตุการณ์เกี่ยวกับภัยทางไซเบอร์ได้ตลอดเวลาอยู่แล้ว ไม่จำเป็นต้องศึกษาจากการเรียนการสอนตามหลักสูตรมาตรฐานหรือตามสถาบันการเรียนการสอนใด ๆ สอดคล้องกับงานของเอมิกา เหมมินทร์ (2556) ที่กล่าวว่า

ปัจจุบัน โลกออนไลน์มีการแลกเปลี่ยนข้อมูล ข่าวสารจากผู้ใช้งานหนึ่งสู่อีกผู้ใช้งานหนึ่งอยู่ตลอดเวลา และไม่เคยหยุดนิ่ง และ Kommers (2001) ได้กล่าวว่า เครือข่ายของสังคมออนไลน์เป็นเครือข่ายที่กว้างขวางมาก ทุกคนสามารถเชื่อมต่อและแลกเปลี่ยนเรื่องราว ประสบการณ์ต่าง ๆ ในจากทั่วทุกมุมของโลกและสามารถทำได้อย่างไร้ขีดจำกัด

สมมติฐานในการวิจัย 2 ความรู้เกี่ยวกับภัยกลลวงหลอกขอข้อมูลทางไซเบอร์ ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขอข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z

จากการเก็บรวบรวมข้อมูล พบว่า ปัจจัยด้านความรู้เกี่ยวกับภัยกลลวงหลอกขอข้อมูลทางไซเบอร์ ของกลุ่ม Gen Z มีค่ามากกว่านัยสำคัญเชิงสถิติ 0.05 ต่อความตระหนักรู้เท่าทัน โดยกลุ่มตัวอย่างส่วนมากล้วนมีความรู้เบื้องต้นเกี่ยวกับภัยทางไซเบอร์อยู่ในเกณฑ์ที่ค่อนข้างสูง แต่กลับไม่มีอิทธิพลส่งผลต่อความตระหนักรู้เท่าทันที่มากขึ้น โดยมีความน่าจะเป็นว่าแม่คนในกลุ่มช่วงวัย Gen Z มีความรู้เบื้องต้นพื้นฐานเกี่ยวกับภัยทางไซเบอร์อยู่แล้ว แต่อาจเป็นแค่เพียงการรับรู้ที่ไม่ได้นำเอาความรู้เหล่านั้นมาประยุกต์กับชีวิตประจำวันได้จริง เนื่องด้วยวิถีชีวิตของสังคมปัจจุบันที่มีความรวดเร็วและมีการแลกเปลี่ยนข้อมูลกันอยู่ตลอดเวลา อาจทำให้การตระหนักรู้เท่าทันภัยร้ายทางไซเบอร์เหล่านี้ถูกละเลยไป และไม่ถูกให้การระมัดระวังมากเท่าที่ควร ซึ่งไม่สอดคล้องกับแนวคิดของ Charles k Atkin (1973) ที่กล่าวว่า ในกรณีที่บุคคลนั้นๆ มีการเปิดรับข้อมูลที่มาก ย่อมมีผลต่อการเข้าใจสถานการณ์ได้มากขึ้น และแนวคิดของขวัญเรือน กิตติวัฒน์ (2531) ว่าประสิทธิภาพของบุคคลในการประเมินสาระสำคัญหรือประโยชน์จากเรื่องใดเรื่องหนึ่งเกิดจากความสามารถในการรับรู้ข้อมูลที่ต่างกัน ในกรณีนี้จำเป็นที่จะต้องหาเหตุปัจจัยอื่นที่ส่งผลต่อการเสริมสร้างความตระหนักรู้มาช่วย ในขณะเดียวกันควรมีการกระตุ้นให้มีการฝึกประยุกต์เอาความรู้ด้านภัยไซเบอร์ มาใช้จริงในชีวิตประจำวันให้มากยิ่งขึ้น เพื่อให้อัตราความเสี่ยงในการถูกหลอกหลวงทางไซเบอร์มีน้อยลงตาม

สมมติฐานที่ 3 พฤติกรรมในการใช้งานช่องทางออนไลน์ของบุคคล ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขอข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z

ผลการศึกษาพบว่าพฤติกรรมการใช้งานช่องทางออนไลน์ ด้านการจัดการความเป็นส่วนตัวของช่องทางออนไลน์ เช่น การไม่แชร์ข้อมูลส่วนตัวลงช่องทางออนไลน์ การตั้งค่าบัญชีให้เป็นส่วนตัว และ พฤติกรรมเกี่ยวกับการป้องกันตัวจากภัยกลลวงหลอกขอข้อมูลทางไซเบอร์ เช่น การดาวน์โหลดแอปพลิเคชันในการตรวจสอบเบอร์มิฉฉาชีพ การบล็อกเบอร์มิฉฉาชีพ หรือการไม่คลิกลิงค์

ที่ไม่มีที่ไปที่ไปที่น่าเชื่อถือ ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z โดยมีความสอดคล้องกับแนวคิดของยรรยงวรกร ทองแย้ม (2563) ว่าการที่บุคคลใดมีพฤติกรรมที่ระมัดระวังในการใช้งานออนไลน์ก็จะสามารถลดความเสี่ยงและเพิ่มความฉลาดทางดิจิทัลให้แก่บุคคลผู้นั้นได้เพิ่มมากขึ้น และจากแนวคิดของ Rutger Leukfeldt (2560) กล่าวว่า สิ่งที่สำคัญที่สุดในการตกเป็นเหยื่อหรือถูกหลอกจากอาชญากรรมทางไซเบอร์คือ พฤติกรรมของมนุษย์นั่นเอง หากบุคคลนั้นประมาท ปล่อยปละละเลยหรือ ไม่เห็นความสำคัญของการระมัดระวังตัวขณะใช้งานช่องทางออนไลน์ก็จะทำให้เสี่ยงต่อการถูกหลอกได้เพิ่มมากขึ้น และหากผู้ใช้งานมีพฤติกรรมในการหลีกเลี่ยงความเสี่ยงก็สามารถทำให้ลดอัตราการเกิดอาชญากรรมทางไซเบอร์ได้ดี ตามแนวคิดของกิตติยา วิสิฐพงศ์พันธ์ และคณะ (2568)

ตัวแปรที่ไม่ส่งผลต่อความตระหนักรู้เท่าทัน ได้แก่ พฤติกรรมด้านการศึกษาข้อมูลในการระวังภัย ซึ่งมีความสอดคล้องกับสมมติฐานที่ 2 ในตัวแปรของปัจจัยด้านความรู้เกี่ยวกับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ ว่าแม้จะมีความรู้จากการศึกษาข้อมูล ข่าวสาร หรือเข้ารับการอบรมต่าง ๆ แต่กลุ่มคนในช่วงวัย Gen Z อาจยังขาดการนำมาประยุกต์ใช้ในชีวิตประจำวัน

สมมติฐานที่ 4 ประสบการณ์และรับรู้ภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z

ตัวแปรด้านปัจจัยประสบการณ์และรับรู้ภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ส่งผลต่อความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคน Gen Z เนื่องจากการเคยถูกหลอกสำเร็จถือเป็นการขาดความตระหนักรู้เท่าทันภัยกลลวงหลอกขโมยข้อมูล ดังนั้นจึงสามารถอธิบายได้ว่า หากกลุ่มตัวอย่างมีประสบการณ์กับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ที่เพิ่มขึ้นย่อมส่งผลต่อระดับความตระหนักรู้ที่น้อยลงอย่างมีนัยเชิงสถิติ

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

งานศึกษาค้นคว้าอิสระในหัวข้อ “ความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคนช่วงวัย Gen Z” ทางผู้ศึกษาวิจัยมีวัตถุประสงค์ในการจัดทำขึ้นเพื่อศึกษาประสบการณ์และความรู้เกี่ยวกับการตระหนักรู้เท่าทันและระวังภัยการใช้กลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) กรณีศึกษา กลุ่มคนช่วงวัย Gen Z และสามารถเสนอแนะแนวทางและรูปแบบในการจัดทำข้อมูลในการป้องกันภัยจากการใช้กลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ในอนาคตที่มีประสิทธิภาพต่อการรับรู้และสร้างความตระหนักให้คนในสังคมได้มากยิ่งขึ้น โดยหลังจากการเก็บข้อมูลและวิเคราะห์ข้อมูลเสร็จสิ้น สามารถกำหนดหัวข้อในการสรุปผลและเสนอแนะแนวทางเพิ่มเติม ได้ดังนี้

5.1 สรุปผลการวิจัย

5.2 ข้อเสนอแนะ

5.1 ผลการวิจัย

งานวิจัยหัวข้อ “ความตระหนักรู้เท่าทันกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) ของกลุ่มคนช่วงวัย Gen Z” เป็นงานวิจัยเชิงปริมาณ (Quantitative Research) โดยทางผู้จัดทำได้ทำการออกแบบเครื่องมือในการเก็บข้อมูล ด้วยการใช้แบบสอบถามออนไลน์ (Online Questionnaire) ทั้งหมด 400 ชุด ตัวแบบสอบถามประกอบไปด้วยข้อคำถาม 6 ส่วน ได้แก่ ส่วนที่ 1 คำถามเกี่ยวกับลักษณะทางประชากรศาสตร์ (เพศ ช่วงอายุ การศึกษา) เป็นคำถามปลายปิด เลือกตอบ จำนวน 3 ข้อ ส่วนที่ 2 คำถามเกี่ยวกับความรู้เกี่ยวกับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ (Phishing) เป็นคำถามปลายปิด เลือกตอบ จำนวน 10 ข้อ ส่วนที่ 3 คำถามเกี่ยวกับพฤติกรรมในการใช้งานช่องทางออนไลน์ต่างๆ และการป้องกันภัย ส่วนที่ 4 คำถามเกี่ยวกับประสบการณ์และการรับรู้เกี่ยวกับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ ส่วนที่ 5 คำถามเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ โดยในส่วนของแบบสอบถามส่วนที่ 3 ถึง 5 เป็นคำถามแบบตารางตัวเลือกหลายข้อ โดยมีการวัดระดับมาตรฐานทั้งหมด 5 ระดับ จำนวนทั้งหมด 24 ข้อ ส่วนที่ 6 ข้อเสนอแนะต่อแนวทางการป้องกันภัยกลลวงหลอกขโมยข้อมูลทางไซเบอร์ เป็นคำถามปลายปิดเลือกตอบ 3 ข้อ และคำถามปลายเปิดสำหรับเสนอแนะเพิ่มเติม 1 ข้อ

จากข้อคำถามทั้งหมดสามารถนำมาจัดประเภทเป็นปัจจัยที่ส่งผลต่อความตระหนักรู้เท่าทันภัยกลลวงหลอกขอลข้อมูลของกลุ่มคน Gen Z ได้ทั้งหมด 5 ตัวแปร ได้แก่ ปัจจัยด้านประชากรศาสตร์ ความรู้เกี่ยวกับภัยกลลวงหลอกขอลข้อมูล พฤติกรรมการใช้งานช่องทางออนไลน์ด้านการจัดการความเป็นส่วนตัว ส่วนตัวของช่องทางออนไลน์ พฤติกรรมเกี่ยวกับการป้องกันตัวจากภัยกลลวงหลอกขอลข้อมูลทางไซเบอร์ และประสบการณ์การรับรู้เกี่ยวกับกลลวงหลอกขอลข้อมูลทางไซเบอร์ มีวิธีดำเนินการวิเคราะห์ข้อมูลด้วยการวิเคราะห์ความแปรปรวนทางเดียว (One-way ANOVA) สำหรับตัวแปรด้านประชากรศาสตร์ และใช้วิธีการถดถอยพหุคูณ หรือ Multiple Regression Analysis สำหรับตัวแปรด้านอื่น ๆ โดยพบความสัมพันธ์ระหว่างตัวแปรอิสระ ด้านประชากรศาสตร์ ได้แก่ เพศ ช่วงอายุ และด้านอื่น ๆ ได้แก่ พฤติกรรมการใช้งานช่องทางออนไลน์ ด้านการจัดการความเป็นส่วนตัวของช่องทางออนไลน์ พฤติกรรมด้านการศึกษาข้อมูลเกี่ยวกับการระวังภัย พฤติกรรมเกี่ยวกับการป้องกันตัวจากภัยกลลวงหลอกขอลข้อมูลทางไซเบอร์ และประสบการณ์การรับรู้เกี่ยวกับกลลวงหลอกขอลข้อมูลทางไซเบอร์ ต่อตัวแปรต้น ความตระหนักรู้เท่าทันกลลวงหลอกขอลข้อมูลทางไซเบอร์ของกลุ่มคน Gen Z โดยสามารถอธิบายความแปรปรวนได้ร้อยละ 21

5.2 ข้อเสนอแนะ

5.2.1 แนวทางและรูปแบบในการจัดทำข้อมูลในการป้องกันภัยกลลวงหลอกขอลข้อมูลทางไซเบอร์ (Phishing)

5.2.1.1 เน้นย้ำการยกระดับความรู้และมาตรฐานในการสร้างความตระหนักรู้เท่าทันภัยกลลวงหลอกขอลข้อมูลทางไซเบอร์ให้มากขึ้น โดยต้องมีการดำเนินการที่เหมาะสมและมีประสิทธิภาพต่อคนในแต่ละกลุ่มเป้าหมาย เนื่องจากในการศึกษาวิจัยพบว่า ปัจจัยความรู้เกี่ยวกับกลลวงหลอกขอลข้อมูลทางไซเบอร์ ไม่ส่งผลต่อระดับความตระหนักรู้เท่าทันจึงควรเร่งหาวิธีการในการปรับเพื่อกระตุ้นความรู้และพัฒนากการประยุกต์ใช้ในชีวิตประจำวันให้ดียิ่งขึ้น เช่น การจัดกิจกรรม Phishing Simulator เพิ่มเติมเพื่อให้กลุ่มเป้าหมายได้ลองเผชิญหน้ากับสถานการณ์ที่อาจพบเจอในชีวิตประจำวัน เพื่อที่จะสามารถดึงองค์ความรู้ต่างๆ ที่มีมาใช้ในการป้องกันตัว

5.2.1.2 ปรับปรุงเนื้อหาและรูปแบบของข้อมูลเตือนภัยกลลวงหลอกขอลข้อมูลทางไซเบอร์ให้มีความเหมาะสมกับเพศและช่วงอายุของกลุ่มเป้าหมายมากยิ่งขึ้น เพื่อให้สอดคล้องกับผลการวิจัยที่ระบุว่าตัวแปรเพศและช่วงอายุมีผลต่อความตระหนักรู้เท่าทัน โดยจำเป็นอย่างยิ่งที่จะต้องมีการพิจารณาจากทั้งระดับความรู้ความเข้าใจเรื่องภัยไซเบอร์ที่แตกต่างกัน พฤติกรรมการใช้งานช่องทางออนไลน์ที่แตกต่างกัน และความสนใจเฉพาะกลุ่มของแต่ละเพศและช่วงวัย

5.2.1.3 จากผลการวิจัยเรื่องพฤติกรรมการใช้งานช่องทางออนไลน์มีอิทธิพลต่อความตระหนักรู้เท่าทัน จึงควรมีการเผยแพร่ข้อมูลเกี่ยวกับกลลวงหลอกขอลข้อมูลในรูปแบบที่เข้าใจง่าย โดยอาจเน้นการทำเนื้อหาที่ยกตัวอย่างพฤติกรรมที่ควรปฏิบัติ พฤติกรรมที่ควรหลีกเลี่ยง หรือ พฤติกรรมที่ช่วยเสริมความปลอดภัยในการใช้งานช่องทางออนไลน์ให้กับกลุ่มเป้าหมาย และสามารถจัดทำในรูปแบบของอินโฟกราฟฟิกหรือคลิปวิดีโอสั้นด้วยภาษาที่เข้าใจง่าย รวมถึงควรเผยแพร่ผ่านทางช่องทางที่หลากหลาย เช่น TikTok Instagram หรือช่องทางที่มีผู้คนใช้งานมาก

5.2.1.4 เน้นกิจกรรมการฝึกการป้องกันภัยในเชิงปฏิบัติมากยิ่งขึ้น โดยภายในสถานศึกษา หรือสถานประกอบการ อาจมีการฝึกให้กลุ่มเป้าหมายลองแยกแยะลิงค์ที่น่าเชื่อถือ ฝึกตั้งคำถาม ยืนยันตัวตนในช่องทางออนไลน์ หรือฝึกถอดรหัสผ่านเพื่อให้ทราบถึงความปลอดภัยของรหัสของตนเองในปัจจุบัน

5.2.1.5 พัฒนาและส่งเสริมให้องค์กรหรือช่องทางต่าง ๆ มีมาตรฐานในการตรวจสอบและป้องกันภัยทางไซเบอร์มากขึ้น เช่น มีช่องทางการแจ้งลิงค์ที่น่าเชื่อถือ ช่องทางตรวจสอบเบอร์มิจฉาชีพที่แม่นยำมากขึ้น หรือมีระบบในการช่วยผู้ใช้งานคัดกรองข้อความ อีเมล และลิงค์ที่น่าไว้วาง

5.2.2 ข้อเสนอแนะสำหรับงานวิจัยในอนาคต

5.2.2.1 ควรมีการขยายกลุ่มเป้าหมายในการวิจัยให้ครอบคลุมมากยิ่งขึ้น เนื่องจากในสังคมปัจจุบันเหยื่อจากภัยกลลวงหลอกขอลข้อมูลทางไซเบอร์ มีได้ทุกเพศทุกช่วงวัย จึงควรศึกษาพฤติกรรมหรือปัจจัยที่ส่งผลต่อความตระหนักรู้เท่าทันของแต่ละช่วงวัยเพื่อลดอัตราความเสี่ยงในการถูกหลอกได้มากยิ่งขึ้น

5.2.2.2 ในการศึกษาวิจัยในอนาคตนอกจากช่วงวัยที่สามารถขยายเพื่อให้ครอบคลุมมากยิ่งขึ้น ควรมีการศึกษาปัจจัยที่อาจส่งผลต่อความตระหนักรู้เพิ่มเติม เช่น วัฒนธรรมภายในองค์กรหรือสังคม อิทธิพลจากครอบครัว

รายการอ้างอิง

หนังสือและบทความในหนังสือ

Glass, A. (2007). Understanding generational differences for competitive success. *Industrial and Commercial Training*, 39(2), 98-103.

Rui Chena & Sushil K Sharmaa. (2013). Understanding Member Use of Social Networking Sites from a Risk Perspective. *Procedia Technology*, 9, 331-339.

บทความในวารสาร

กิตติคุณ มีทองจันทร์ และ วงศ์ยศ เกิดศรี. (2564). ปัจจัยที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑล. *วารสารวิชาการอาชญวิทยาและนิติวิทยาศาสตร์*, 7 (2).

กิตติยา วิสสุพงศ์พันธ์, ชูเกียรติ บุญก่อเกื้อ, กิตติพงศ์ อยู่นิรันดร์ และ นลินภัทร์ บำเพ็ญเพียร. (2565). *วารสารวิชาการวิทยาศาสตร์ มหาวิทยาลัยราชภัฏจันทรเกษม*. ปีที่ 32 ฉบับที่ 1 มกราคม-มิถุนายน 2568.

คณาธิป ทองรวีวงศ์. (2564). ผลกระทบทางลบอันเกิดจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562. *วารสารรัชต์ภาคย์*, 15 (38).

จิตสุภา ฤทธิผลิน. (2564). กลยุทธ์การคืนสภาพได้ทางไซเบอร์: แนวทางสำคัญในการดำเนินงานขององค์กรในยุคดิจิทัล. *วารสารวิชาการ กสทช. ประจำปี 2564*.

ยรรยงวรกร ทองแย้ม. (2563). การสร้างความตระหนักรู้ความฉลาดทางดิจิทัลด้วยสัญญาณภาพยนตร์สั้นกับนักศึกษาวิทยาศาสตร์ชั้นปีที่ 1 มหาวิทยาลัยราชภัฏพิบูลสงคราม. *วารสารการบริหารนิติบุคคลและนวัตกรรมท้องถิ่น*, 6 (5), 189-190.

วรพิน นามไกววัล. (2557). ปัจจัยที่มีอิทธิพลต่อการยอมรับนวัตกรรมหนังสืออิเล็กทรอนิกส์ของผู้บริโภคชาวไทย. *วารสารวิชาการบริหารธุรกิจ สมาคมสถาบันอุดมศึกษาเอกชนแห่งประเทศไทย (สสอท.)*, 3 (2), 64.

วงศ์ยศ เกิดศรี. (2561). การสำรวจตัวแปรที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดียในประเทศไทย. การประชุมวิชาการเสนอผลงานวิจัยระดับชาติ “GRADUATE SCHOOL CONFERENCE 2018”.

วุฒิชัย สุขจิต. (2561). อาชญากรรมคอมพิวเตอร์: ศึกษากรณีปัจจัยที่มีผลต่อการเกิดอาชญากรรมบนระบบ electronic banking. การประชุมวิชาการเสนอผลงานวิจัยระดับชาติ “GRADUATE SCHOOL CONFERENCE 2018”.

วิวัฒน์ สุขชีพ และ จรรย์ แสนราช. (2566). การตระหนักรู้ถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์. Industrial Technology Journal, 8 (1), มกราคม-มิถุนายน 2566.

เอกสารอื่น ๆ

คนัญญา อิมใจ. (2565). พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจนเนอเรชั่นแซต. (สารนิพนธ์, มหาวิทยาลัยศรีนครินทรวิโรฒ, ศิลปศาสตรมหาบัณฑิต).

ครองรัตน์ ดุลลาพันธ์. (2561). พฤติกรรมการใช้เครือข่ายสังคมออนไลน์และปัจจัยทางจิตที่พยากรณ์ภาวะโรคซึมเศร้า. (วิทยานิพนธ์ปริญญามหาบัณฑิต).

จิรภา รุ่งเรืองศักดิ์. (2558). การศึกษาการยอมรับและการรับรู้ความเสี่ยงที่ส่งผลต่อความไว้วางใจในการใช้บริการระบุตำแหน่ง (Location-based Services: LBS) ของผู้ใช้บริการในเขตกรุงเทพมหานคร. (การศึกษาค้นคว้าอิสระ, มหาวิทยาลัยกรุงเทพ, บัณฑิตวิทยาลัย).

ณภัทร เรืองนภากุล และ สุภิญญา กลางณรงค์. (2564). ความเป็นพลเมืองยุคดิจิทัลกับการรับมือด้านมืดออนไลน์ในวิถีปรกติใหม่. สืบค้นเมื่อวันที่ 2 มีนาคม 2565 จากเว็บไซต์ <https://blog.cofact.org/digitalcitizen/>

นิภาพร แสงทวี และ สมนึก พ่วงพรพิทักษ์. (2559). การวิเคราะห์ความปลอดภัยและความมั่นคงสำหรับระบบธนาคารผ่านโทรศัพท์มือถือในประเทศไทย. สืบค้นจาก <https://www.thaiscience.info/journals/Article/JSMU/10985196.pdf>

ภัทรดนัย พริยะธนภัทร. (2559). การศึกษาปัจจัยด้านประชากรศาสตร์ ด้านพฤติกรรม ผู้บริโภคและปัจจัยด้านเว็บไซต์พระเครื่องพาณิชย์อิเล็กทรอนิกส์ที่มีผลต่อการตัดสินใจเช่าหรือ ประมูลพระเครื่องออนไลน์. (การศึกษาค้นคว้าอิสระ, มหาวิทยาลัยกรุงเทพ, บัณฑิตวิทยาลัย).

ภูวดล แสงทอง. Information Security. สืบค้นเมื่อวันที่ 9 มีนาคม 2565 จาก เว็บไซต์ http://www1.udd.go.th/WEB_CIT/File/InformationSecurity.pdf

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร คณะทำงานการจัดการความรู้ สำนักงาน เลขาธิการวุฒิสภา. การป้องกันภัยคุกคามทางคอมพิวเตอร์. สืบค้นเมื่อวันที่ 6 มีนาคม 2565 จาก เว็บไซต์ <https://www.senate.go.th/assets/portals/49/news/87/km11-59.pdf>

สุภวัฒน์ สงวนนาม. (2557). ปัจจัยที่ส่งผลต่อพฤติกรรมการเลือกรับชมรายการข่าวของ สถานีโทรทัศน์ของผู้ชมในเขตกรุงเทพมหานคร. (มหาวิทยาลัยเนชั่น).

อลิษา สายแผ้ว. (2556). ประสิทธิภาพของกฎหมายไทยในการรับมือกับอาชญากรรมข้ามชาติในรูปแบบฟิชซิง (Phishing). (การศึกษาค้นคว้าอิสระ, มหาวิทยาลัยธรรมศาสตร์, บัณฑิตวิทยาลัย).

Howe, N., & Strauss, W. (2008). Millennials & K-12 school: LifeCourse Associates.

Mannhiem, K. (1952). Essays on the sociology of knowledge. London: Routledge and Kegan Paul.

Rutger Leukfeldt. (2017). Research agenda the human factor in cybercrime and cybersecurity. Eleven International Publishing



ภาคผนวก

คำชี้แจง แบบสอบถามชุดนี้จะประกอบไปด้วยคำถามทั้งหมด 5 ส่วน ได้แก่

- ส่วนที่ 1 คำถามเกี่ยวกับลักษณะทางประชากรศาสตร์ (เพศ ช่วงอายุ การศึกษา)
- ส่วนที่ 2 คำถามเกี่ยวกับความรู้เกี่ยวกับภัยกลวงหลอกขอข้อมูลทางโซเชียล (Phishing)
- ส่วนที่ 3 คำถามเกี่ยวกับพฤติกรรมในการใช้งานช่องทางออนไลน์ต่างๆ และการป้องกันภัย
- ส่วนที่ 4 คำถามเกี่ยวกับประสบการณ์และการรับรู้เกี่ยวกับภัยกลวงหลอกขอข้อมูลทางโซเชียล
- ส่วนที่ 5 คำถามเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยกลวงหลอกขอข้อมูลทางโซเชียล
- ส่วนที่ 6 ข้อเสนอแนะต่อแนวทางการป้องกันภัยกลวงหลอกขอข้อมูลทางโซเชียล

คำชี้แจง ให้ทำเครื่องหมาย ✓ หน้าหมายเลขของคำตอบในช่องว่างที่ต้องการเลือกตอบ
ท่านเป็นกลุ่มคนที่มียุระหว่าง 18-28 ปี หรือเกิดในช่วงระหว่างพ.ศ.2540-2550 ใช่หรือไม่
[1] ใช่ [2] ไม่ใช่ (จบแบบสอบถาม)

ส่วนที่ 1 คำถามเกี่ยวกับลักษณะทางประชากรศาสตร์

คำชี้แจง ให้ทำเครื่องหมาย ✓ หน้าหมายเลขของคำตอบในช่องว่างที่ต้องการเลือกตอบ

1.1 เพศ

[1] เพศชาย [2] เพศหญิง [3] เพศทางเลือก

1.2 อายุ

[1] 18-20 પૈ [2] 21-23 પૈ [3] 24-26 પૈ [4] 27-28 પૈ

1.3 ระดับการศึกษา

- [1] มัธยมศึกษา หรือกำลังศึกษา
- [2] ปวช./ ปวส./ อนุปริญญา หรือกำลังศึกษา
- [3] ปริญญาตรี หรือกำลังศึกษา
- [4] ปริญญาโทหรือสูงกว่า

ส่วนที่ 2 คำถามเกี่ยวกับความรู้เกี่ยวกับภัยกลวงหลอกขอข้อมูลทางไซเบอร์ (Phishing)

คำชี้แจง ให้ทำเครื่องหมาย ✓ หน้าหมายเลขของคำตอบในช่องว่างที่ต้องการเลือกตอบ

2.1 หากท่านได้รับข้อความทางโทรศัพท์โดยมีการอ้างว่าท่านมีพัสดุที่ตกค้างอยู่และต้องการให้ท่านคลิกลิงค์เพื่อกรอกข้อมูลส่วนตัวในระบบ ถือเป็นภัยคุกคามทางไซเบอร์รูปแบบใด

- [1] ภัยคุกคามทางไซเบอร์จากบุคคลภายใน (Insider Threat)
- [2] ภัยคุกคามทางไซเบอร์โดยการหลอกขอข้อมูล หรือฟิชชิ่ง (Phishing)
- [3] ภัยจากการใช้โปรแกรมแฝงที่มีอันตราย หรือรูทคิท (Rootkit)
- [4] การใช้ซอฟต์แวร์ในการดักจับข้อมูล หรือสปายแวร์ (Spyware)

2.2 ข้อใดเป็นข้อมูลที่เสี่ยงต่อการโดนหลอกขอลงขอข้อมูลทางไซเบอร์

- [1] วันเดือนปีเกิด
- [2] บัญชีธนาคาร
- [3] ชื่อเพื่อนสนิท
- [4] ถูกทุกข้อ

2.3 เว็บไซต์ใดต่อไปนี้เป็นเว็บไซต์ที่มีความน่าเชื่อถือมากที่สุดในการกรอกข้อมูล

- [1] <http://www.youtube.co.th>
- [2] http://docs.google.go.th/forms/d/1X0Td3HBnbFOBEp0tYivLfSvF7tRhMB_P9hVGG6fVEV0/edit
- [3] <http://d6s.me/JSDte>
- [4] <https://adidas.co.th>

2.4 ข้อใดเป็นนโยบายในการป้องกันการถูกหลอกขอข้อมูลภายในองค์กรที่มีประสิทธิภาพมากที่สุด

- [1] พนักงานบริษัททุกคนต้องทำการเปลี่ยนรหัสผ่านทุก 45 วัน
- [2] พนักงานทุกคนต้องแจ้งรหัสผ่านให้เพื่อนสนิทรับทราบ
- [3] หัวหน้างานต้องส่งลิงค์เปลี่ยนรหัสผ่านให้ลูกน้องโดยการใช้ช่องทางออนไลน์ส่วนตัว
- [4] หากได้รับอีเมลชู้ลปไฟล์สำคัญให้รีบกดลิงค์เพื่อกู้ข้อมูลทันทีไม่ว่าจะมาจากผู้ส่งคนไหนก็ตาม

2.5 พฤติกรรมในข้อใดที่เสี่ยงต่อการถูกผู้ไม่ประสงค์ดีหลอกขอข้อมูลจากการสังเกตพฤติกรรมทางช่องทางโซเชียล (Angler Phishing) มากที่สุด

- [1] บ่นและอัปเดตทุกเรื่องในชีวิตลงเฟซบุ๊กส่วนตัว
- [2] ค้นหาข้อมูลที่สนใจใน www.google.com
- [3] รีบกดชำระเงินในเว็บไซต์เพราะกลัวสินค้าหมด
- [4] คุยเรื่องงานกับเพื่อนร่วมงานผ่านทางโทรศัพท์

2.6 ข้อใดไม่ถือเป็นการละเมิด พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

- [1] โรงพยาบาลทำการส่งข้อมูลการรักษาของคนไข้ให้แก่แพทย์เจ้าของไข้ที่ทำการรักษา
- [2] พนักงานในองค์กรแอบส่งข้อมูลส่วนตัวของลูกค้าให้คนนอกองค์กร
- [3] คาเฟ่ชื่อดังนำภาพและประวัติการซื้อของลูกค้ามาลงเพจเฟซบุ๊ก
- [4] เจ้าหน้าที่บริษัทเครือข่ายโทรศัพท์เอารายชื่อและเบอร์ติดต่อของลูกค้าไปขาย

2.7 หากมีเบอร์ที่ไม่คุ้นโทรเข้ามาอ้างว่าเป็นเจ้าหน้าที่จากแบรนด์ดังที่คุณใช้ประจำและแจ้งว่าคุณเป็นผู้โชคดีที่ได้รับการสุ่มเลือกให้ได้รับของรางวัลพิเศษ โดยต้องทำการแอดไลน์เพื่อรับของรางวัล ถือว่าเสี่ยงที่จะเป็นกลโกงหลอกขอข้อมูลในประเภทใด

- [1] E-mail Phishing
- [2] Vishing Phishing
- [3] CEO Fraud Phishing
- [4] Web Phishing

2.8 หากมีอีเมลส่งเข้ามาจาก TikTok ด้วยชื่อเมล Tiktokthailand@tiktok.co.th ให้คุณทำการอัปเดตข้อมูลส่วนตัวและอีเมลอีกครั้งไม่อย่างนั้นจะถูกระงับการใช้งาน ถือว่าเสี่ยงที่จะเป็นกลโกงหลอกขโมยข้อมูลในประเภทใด

- [1] E-mail Phishing
- [2] Vishing Phishing
- [3] CEO Fraud Phishing
- [4] Web Phishing

2.9 หากมีอีเมลที่อ้างเป็นเพื่อนร่วมงานในองค์กรส่งไฟล์มาให้ดาวน์โหลด โดยที่เป็นชื่อเมลที่คล้ายคลึงกับอีเมลขององค์กร (เปลี่ยนจาก @ชื่อบริษัท.com เป็น @ชื่อบริษัท.co.th) ถือว่าเสี่ยงที่จะเป็นกลโกงหลอกขโมยข้อมูลในประเภทใด

- [1] E-mail Phishing
- [2] Vishing Phishing
- [3] Spear Phishing
- [4] Web Phishing

2.10 หากท่านได้รับข้อความที่อ้างว่าส่งจากเฟซบุ๊กให้รีบดำเนินการเปลี่ยนรหัสผ่านเพื่อให้บัญชีของท่านสามารถใช้งานได้ต่อ ท่านจะตัดสินใจดำเนินการอย่างไร

- [1] กดลิงค์เพื่อตรวจสอบว่าเป็นลิงค์จากเฟซบุ๊กจริงๆ ใช่หรือไม่
- [2] รีบเปลี่ยนรหัสผ่านโดยใช้ลิงค์นั้นเนื่องจากกลัวถูกระงับการใช้
- [3] ส่งอีเมลตอบกลับว่าได้ทำการเปลี่ยนรหัสผ่านแล้ว
- [4] ตรวจสอบให้มั่นใจโดยไม่คลิกลิงค์ใด ๆ และรีบลบอีเมลออกทันที

ส่วนที่ 3 คำถามเกี่ยวกับพฤติกรรมในการใช้งานช่องทางออนไลน์ต่างๆ และการป้องกันภัย

คำชี้แจง ให้ทำเครื่องหมาย ✓ หน้าหมายเลขของคำตอบในช่องว่างที่ต้องการเลือกตอบ

5 = มากที่สุด 4 = มาก 3 = ปานกลาง 2 = น้อย 1 = น้อยที่สุด

3. ท่านมีพฤติกรรมอย่างไรเกี่ยวกับกลลวงหลอกขอข้อมูลทางโซเชียล	ระดับความคิดเห็น				
	5 มากที่สุด	4 มาก	3 ปานกลาง	2 น้อย	1 น้อยที่สุด
พฤติกรรมด้านการจัดการความเป็นส่วนตัวของช่องทางออนไลน์					
3.1 ท่านไม่ทำการแชร์ข้อมูลส่วนตัวหรือบุคคลรอบตัวลงในช่องทางออนไลน์					
3.2 ท่านมักจะตั้งค่าความเป็นส่วนตัวของช่องทางออนไลน์ทั้งหมดให้มีความปลอดภัยมากที่สุด (ยืนยันตัวตนด้วยอีเมลหรือเบอร์โทรศัพท์ ตั้งค่าการแจ้งเตือนเมื่อมีคนพยายามล่อลวง ไม่เปิดบัญชีให้เป็นสาธารณะ ใช้เครื่องมือ 2FA เพื่อจำกัดการเข้าถึงข้อมูล เป็นต้น)					
พฤติกรรมด้านการศึกษาข้อมูลในการระวังภัยกลลวงหลอกขอข้อมูลทางโซเชียล					
3.3 ท่านให้ความสำคัญกับการค้นคว้าข่าวสาร ข้อมูลและวิธีการระวังภัยกลลวงหลอกขอข้อมูลทางออนไลน์จากช่องทางต่างๆ (สื่อสังคมออนไลน์ เว็บไซต์ของทางการ)					
3.4 ท่านให้ความสำคัญกับเนื้อหาของนโยบายความเป็นส่วนตัวของข้อมูลก่อนที่จะใช้งานแอปพลิเคชันต่างๆเสมอ					
3.5 ท่านศึกษาข้อมูลเกี่ยวกับภัยกลลวงหลอกขอข้อมูลทางโซเชียลอยู่เสมอ					
3.6 ท่านเคยเข้าอบรมวิธีการระวังตนเองจากภัยกลลวงหลอกขอข้อมูลทางโซเชียล					
พฤติกรรมด้านการป้องกันตัวจากภัยกลลวงหลอกขอข้อมูลทางโซเชียล					
3.7 ท่านมีการโหลดแอปพลิเคชันในการตรวจสอบมิจฉาชีพ หรือมีการเช็คชื่อเมล เบอร์โทรที่ส่งมาก่อนเสมอ					
3.8 ท่านไม่ดาวน์โหลดหรือคลิกลิงค์ที่ไม่ทราบที่มาที่ไปแม้อ้างส่งจากอีเมลของบุคคลที่รู้จัก					
3.9 ท่านทำการบล็อกเบอร์โทรศัพท์ที่เป็นมิจฉาชีพ					

ส่วนที่ 4 คำถามเกี่ยวกับประสบการณ์และการรับรู้เกี่ยวกับภัยกลวงหลอกขอข้อมูลทางไซเบอร์

คำชี้แจง ให้ทำเครื่องหมาย ✓ หน้าหมายเลขของคำตอบในช่องว่างที่ต้องการเลือกตอบ

5 = มากที่สุด 4 = มาก 3 = ปานกลาง 2 = น้อย 1 = น้อยที่สุด

4. ท่านมีประสบการณ์และการรับรู้เกี่ยวกับภัยกลวงหลอกขอข้อมูลทางไซเบอร์	ระดับความคิดเห็น				
	5 มาก ที่สุด	4 มาก	3 ปาน กลาง	2 น้อย	1 น้อย ที่สุด
4.1 ท่านหรือบุคคลรอบตัวเคยมีประสบการณ์ถูกหลอกขอข้อมูลทางไซเบอร์ จากช่องทางข้อความสำเร็จ					
4.2 ท่านหรือบุคคลรอบตัวเคยมีประสบการณ์ถูกหลอกขอข้อมูลทางไซเบอร์ จากช่องทางอีเมลสำเร็จ					
4.3 ท่านหรือบุคคลรอบตัวเคยมีประสบการณ์ถูกหลอกขอข้อมูลทางไซเบอร์ จากช่องทางโทรศัพท์สำเร็จ					

ส่วนที่ 5 คำถามเกี่ยวกับความตระหนักรู้เกี่ยวกับภัยกลลวงหลอกขอข้อมูลทางไซเบอร์

คำชี้แจง ให้ทำเครื่องหมาย ✓ หน้าหมายเลขของคำตอบในช่องว่างที่ต้องการเลือกตอบ

5 = มากที่สุด 4 = มาก 3 = ปานกลาง 2 = น้อย 1 = น้อยที่สุด

5. ท่านมีความตระหนักรู้เกี่ยวกับกลลวงหลอกขอข้อมูลทางไซเบอร์อย่างไร	ระดับความคิดเห็น				
	5 มาก ที่สุด	4 มาก	3 ปาน กลาง	2 น้อย	1 น้อย ที่สุด
5.1 ท่านมีการคำนึงถึงความเสี่ยงของการถูกนำเอาข้อมูลส่วนตัวไปใช้ในทางที่ไม่ดีอยู่เสมอ					
5.2 ท่านคิดว่าการขาดความรอบคอบส่วนบุคคลส่งผลต่อการถูกหลอกขอข้อมูลทางไซเบอร์					
5.3 ท่านคิดว่าการขาดความรู้และประสบการณ์เกี่ยวกับภัยไซเบอร์ส่งผลต่อการถูกหลอกขอข้อมูลทางไซเบอร์					
5.4 ท่านคิดว่าความไม่ทันระวังหรือการไม่สังเกตรายละเอียดมากพอส่งผลต่อการถูกหลอกขอข้อมูลทางไซเบอร์					
5.5 ท่านคิดว่าความคิดว่าข้อมูลที่ให้หรือรอกไปนั้นไม่ได้สำคัญส่งผลต่อการถูกหลอกขอข้อมูลทางไซเบอร์					
5.6 ท่านคิดว่าความการมีเวลาจำกัดส่งผลต่อการถูกหลอกขอข้อมูลทางไซเบอร์ (ถูกเร่งให้กรอกข้อมูลในระยะเวลาที่กำหนด)					
5.7 ท่านคิดว่าการถูกกลลวงหลอกขอข้อมูลทางไซเบอร์ส่งผลกระทบต่อด้านการเงิน (สูญเสียเงิน / มีเงินเข้าและออกจากบัญชีอย่างผิดปกติ)					
5.8 ท่านคิดว่าการถูกกลลวงหลอกขอข้อมูลทางไซเบอร์ส่งผลกระทบต่อด้านความเป็นส่วนตัว (ถูกนำเอาข้อมูลไปเผยแพร่)					
5.9 ท่านคิดว่าการถูกกลลวงหลอกขอข้อมูลทางไซเบอร์ส่งผลกระทบต่อด้านความปลอดภัยทางกายภาพและทรัพย์สิน (มีคนติดตามหรือติดต่อเพื่อข่มขู่)					
5.10 ท่านคิดว่าการศึกษาข้อมูลเตือนภัยและวิธีระวังภัยจากกลโกงหลอกขอข้อมูลมีความสำคัญมาก					
5.11 ท่านคิดว่ากลลวงหลอกขอข้อมูลทางไซเบอร์เป็นเรื่องใกล้ตัวที่สามารถพบเจอในชีวิตประจำวันได้ (การใช้งานช่องทางออนไลน์ การทำธุรกรรมทางการเงินออนไลน์ การสั่งซื้อสินค้าออนไลน์)					
5.12 ท่านคิดว่าการมีความตระหนักรู้ที่มากพอ เช่น ความรู้เกี่ยวกับภัยไซเบอร์ หรือการระมัดระวังในการใช้งานช่องทางออนไลน์ ส่งผลให้ความเสี่ยงที่จะถูกหลอกขอข้อมูลทางไซเบอร์มีน้อยลง					

ส่วนที่ 6 ข้อเสนอแนะต่อแนวทางการป้องกันภัยกลลวงลอกขโมยข้อมูลทางไซเบอร์

คำชี้แจง ให้ทำเครื่องหมาย ✓ หน้าหมายเลขของคำตอบในช่องว่างที่ต้องการเลือกตอบ

6.1 ท่านคิดว่าเนื้อหาของข้อมูลการระวังภัยแบบใดที่มีประสิทธิภาพต่อท่านมากที่สุด

- [1] กรณีศึกษาจากผู้มีประสบการณ์
- [2] คำแนะนำทั่วไปในการใช้งานสื่อสังคมออนไลน์อย่างปลอดภัย
- [3] การให้ความรู้เกี่ยวกับเทคนิคเฉพาะทางที่เกี่ยวข้องกับภัยทางไซเบอร์
- [4] เกร็ดความรู้เบื้องต้นที่เข้าใจง่ายเพื่อให้รู้หลักการและวิธีป้องกันภัย

6.2 ท่านคิดว่ารูปแบบของข้อมูลการระวังภัยแบบใดที่มีประสิทธิภาพต่อท่านมากที่สุด

- [1] วิดีโอให้ความรู้
- [2] บทความ
- [3] อินโฟกราฟฟิกสรุปข้อมูล
- [4] การสัมภาษณ์ผู้เชี่ยวชาญ

6.3 ท่านคิดว่าช่องทางในการเผยแพร่ข้อมูลการระวังภัยช่องทางใดที่มีประสิทธิภาพต่อท่านมากที่สุด

- [1] ช่องทางสื่อสังคมออนไลน์ (เฟซบุ๊ก ไลน์ เอกซ์ อินสตราแกรม ยูทูบ)
- [2] เว็บไซต์ของหน่วยงานที่เป็นทางการ
- [3] อินฟลูเอนเซอร์
- [4] ช่องทางโทรทัศน์ หนังสือพิมพ์ หรือวิทยุ

6.4 ข้อเสนอแนะเพิ่มเติมสำหรับการจัดทำข้อมูลในการระวังภัยทางไซเบอร์ที่ท่านคิดว่าสามารถเสริมสร้างประสิทธิภาพให้กับผู้อ่านได้มากยิ่งขึ้น (ถ้ามี)

เฉลยคำตอบแบบสอบถามส่วนที่ 2 คำถามเกี่ยวกับความรู้เกี่ยวกับภัยกลวงหลอกขอข้อมูลทางไซเบอร์ (Phishing)

- 2.1 [2] ภัยคุกคามทางไซเบอร์โดยการหลอกขอข้อมูล หรือฟิชชิ่ง (Phishing)
- 2.2 [4] ถูกทุกข้อ
- 2.3 [4] <https://adidas.co.th>
- 2.4 [1] พนักงานบริษัททุกคนต้องทำการเปลี่ยนรหัสผ่านทุก 45 วัน
- 2.5 [1] บ่นและอัปเดตทุกเรื่องในชีวิตลงเฟซบุ๊กส่วนตัว
- 2.6 [1] โรงพยาบาลทำการส่งข้อมูลการรักษาของคนไข้ให้แก่แพทย์เจ้าของไข้ที่ทำการรักษา
- 2.7 [2] Vishing Phishing
- 2.8 [1] E-mail Phishing
- 2.9 [3] Spear Phishing
- 2.10 [4] ตรวจสอบให้มั่นใจโดยไม่คลิกลิงค์ใดๆ และรีบิลบอีเมล์ออกทันที