การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

STRENGTHENING CYBERSECURITY AWARENESS FOR PERSONNEL IN AERONAUTICAL RADIO OF THAILAND CO., LTD.

สุทธิพันธุ์ ชวลิตเลขา

SUTTIPHAN CHAVALITLEKHA

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม
ปีการศึกษา 2564

ลิขสิทธิ์ของมหาวิทยาลัยศรีปทุม

การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

สุทธิพันธุ์ ชวลิตเลขา

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม
ปีการศึกษา 2564
ลิขสิทธิ์ของมหาวิทยาลัยศรีปทุม

STRENGTHENING CYBERSECURITY AWARENESS FOR PERSONNEL IN AERONAUTICAL RADIO OF THAILAND CO., LTD.

SUTTIPHAN CHAVALITLEKHA

A THEMATIC SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
SCHOOL OF INFORMATION TECHNOLOGY
SRIPATUM UNIVERSITY
ACADEMIC YEAR 2021
COPYRIGHT OF SRIPATUM UNIVERSITY

หัวข้อสารนิพนธ์	การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด STRENGTHENING CYBERSECURITY AWARENESS FOR PERSONNEL IN AERONAUTICAL RADIO OF THAILAND CO., LTD.
นักศึกษา	สุทธิพันธุ์ ชวลิตเลขา รหัสประจำตัว 64502585
หลักสูตร	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะ	เทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
อาจารย์ที่ปรึกษาสารนิพนธ์	ดร.สุรชัย ทองแก้ว
อาจารย์ที่ปรึกษาสารนิพนธ์ร่วม	ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง

คณะกรรมการการสอบสารนิพนธ์

.....ประธานกรรมการ

(รองศาสตราจารย์.ดร.ทศนัย ชุ่มวัฒนะ)

.....กรรมการ

(ผู้ช่วยศาสตราจารย์.ดร.ปราลี มณีรัตน์)

.....กรรมการ

(ดร.สุรชัย ทองแก้ว)

คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม อนุมัติให้นับสารนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณบดีคณะเทคโนโลยีสารสนเทศ

.....

(ผู้ช่วยศาสตราจารย์ ดร.ธนา สุขวารี)

วันที่ 15 เดือน สิงหาคม พ.ศ. 2565 ..

สารนิพนธ์เรื่อง การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด
คำสำคัญ ความตระหนักรู้, ความมั่นคงปลอดภัยไซเบอร์, ความเสี่ยงด้านไซเบอร์
นักศึกษา สุทธิพันธุ์ ชวลิตเลขา
อาจารย์ที่ปรึกษาสารนิพนธ์ ดร.สุรชัย ทองแก้ว
อาจารย์ที่ปรึกษาสารนิพนธ์ร่วม ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง
หลักสูตร วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะ เทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
พ.ศ. 2564

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์ดังนี้ 1) เพื่อศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย และ 2) เพื่อพัฒนาแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินฯ กลุ่มตัวอย่างคือ บุคลากรในบริษัทวิทยุการบินฯ เครื่องมือที่ใช้ในการวิจัย ได้แก่ แบบสัมภาษณ์แบบกึ่งโครงสร้าง และแบบสอบถามปลายปิด ผลการวิจัยพบว่า บุคลากรในบริษัทวิทยุการบินฯ มีการกำหนดกลยุทธ์ด้านภัยคุกคามทางไซเบอร์ ผู้บังคับบัญชาให้ความสำคัญกับนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ มีการระบุภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อการปฏิบัติงานโดยตรง ภาพรวมความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับมากที่สุด ในส่วนการพัฒนาแนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์พบว่าบุคลากรในบริษัทวิทยุการบินฯ ต้องการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ด้วยวิธีการเรียนรู้แบบออนไลน์และวิธีการเรียนโดยใช้วีดิทัศน์ผสมผสานกัน จากผลการวิจัยนี้ ผู้วิจัยได้นำข้อมูลมาสร้างแอปพลิเคชันสำหรับการเสริมสร้างและประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และทำการการติดตั้งภายในระบบเครือข่าย Intranet ของบริษัทวิทยุการบินฯ ด้วยแพลตฟอร์ม AEROTHAI Learning Management Systems (AEROTHAI LMS)

THEMATIC TITLE STRENGTHENING CYBERSECURITY AWARENESS FOR PERSONNEL IN AERONAUTICAL RADIO OF THAILAND CO.,LTD.
KEYWORDS AWARENESS, CYBERSECURITY, CYBER RISK
STUDENT SUTTIPHAN CHAVALITLEKHA
ADVISOR DR.SURACHAI THONGKAEW
CO-ADVISOR PROFESSOR DR.PRASONG PRANEETPOLGRANG
LEVEL OF STUDY MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
FACULTY SCHOOL OF INFORMATION TECHNOLOGY, SRIPATUM UNIVERSITY
ACADEMIC YEAR 2021

ABSTRACT

The objectives of this research are as follows : 1) To study the problem conditions and usage behavior in the world cyber of personnel in Aeronautical Radio of Thailand Co., Ltd. who are at risk of cybersecurity, 2) To develop a guidelines to raise awareness among personnel in Aeronautical Radio of Thailand Co., Ltd. The sample group in the study was personnel in Aeronautical Radio of Thailand Co., Ltd. Research tools include structured interview forms, questionnaires. The results showed that Personnel in Aeronautical Radio of Thailand Co., Ltd. found that cyber threats have been formulated. Supervisors focus on cybersecurity policies. Cyber threats that directly affect operations are identified as well as having an awareness of cybersecurity behavior overall, it's at the highest level. From developing an awareness-raising approach by creating a digital platform to raise awareness of cybersecurity to train personnel and created an application to assess the level of cybersecurity awareness for personnel in Aeronautical Radio of Thailand Limited. Overall, it's at a highest level. Researcher found that the personnel in the Aeronautical Radio of Thailand Co., Ltd. want to raise awareness of cybersecurity through a combination of online learning and video learning methods. From the results to created an application for enhancing and assessing the level of cybersecurity awareness and installed with the AEROTHAI Learning Management System (AEROTHAI LMS) Intranet platform.

กิตติกรรมประกาศ

ความสำเร็จของสารนิพนธ์ฉบับนี้ ผู้วิจัยได้รับความกรุณาเป็นอย่างยิ่ง จากท่านศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง อาจารย์ที่ปรึกษา ที่ได้ให้เวลาและโอกาสในการปรึกษาพร้อมทั้งให้คำชี้แนะอันเป็นประโยชน์อย่างมากต่อการพัฒนาผลงานสารนิพนธ์ที่ได้ไปนำเสนอในงานประชุมวิชาการทั้งระดับชาติและนานาชาติของผู้วิจัย คอยตรวจสอบแก้ไขข้อบกพร่องต่าง ๆ ติดตามการทำสารนิพนธ์ของผู้วิจัยอย่างใกล้ชิด และคอยตรวจสอบในทุกทางเพื่อให้สารนิพนธ์นี้ออกมาอย่างดีและสมบูรณ์ที่สุด ผู้วิจัยได้เรียนรู้ประสบการณ์มากมายจากท่านอาจารย์ ซึ่งได้ให้ความช่วยเหลือการผ่านความยากลำบากเพื่อทำให้ผู้วิจัยได้มีพื้นฐานและรากฐานที่มั่นคงในการทำวิจัย มุ่งมั่นที่จะผลิตงานทางวิชาการที่มีคุณค่าต่อสังคม ถึงแม้ช่วงเวลาแห่งการเรียนรู้ในบางครั้ง ต้องแลกมาซึ่งความทุกข์ยากก็ตาม ร่วมอดหลับอดนอน ทุ่มเททุกอย่าง ทุกวิถีทาง จนสารนิพนธ์ฉบับนี้แล้วเสร็จ

ผู้วิจัยขอขอบพระคุณท่าน ดร.สุรชัย ทองแก้ว อาจารย์ที่ปรึกษา ที่ได้ให้แนวคิด ข้อเสนอแนะแนวทางในการทำวิจัย และประสบการณ์การเรียนรู้ให้แก่ผู้วิจัยให้มีความถูกต้องสมบูรณ์

ผู้วิจัยขอขอบพระคุณท่าน ผู้ช่วยศาสตราจารย์ ดร.ธนา สุขวารี คณบดีคณะเทคโนโลยีสารสนเทศ ผู้ช่วยศาสตราจารย์ ดร. ปราลี มณีรัตน์ ผู้อำนวยการหลักสูตรวิทยาศาสตรมหาบัณฑิต และผู้บริหารทุกท่านของมหาวิทยาลัยศรีปทุม ที่ได้ประสิทธิ์ประสาทความรู้ ซึ่งส่งผลให้สารนิพนธ์ฉบับนี้สามารถสำเร็จได้อย่างราบรื่นตามกรอบเวลาที่กำหนด มา ณ โอกาสนี้

ผู้วิจัยขอขอบพระคุณท่านผู้เชี่ยวชาญทุกท่านที่ได้ให้คำแนะนำตรวจสอบแบบสอบถาม และขอขอบพระคุณคณะผู้บริหารและพนักงานของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่ได้เสียสละเวลาให้สัมภาษณ์เชิงลึก ตอบแบบสอบถาม ทำให้สารนิพนธ์ฉบับนี้ประสบความสำเร็จอย่างดียิ่ง

ผู้วิจัยขอบพระคุณพี่น้องร่วมหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ รุ่นที่ 26 ทุกคน ที่ได้ร่วมให้ความรู้ คำแนะนำ และเป็นกำลังใจซึ่งกันและกัน

สุดท้ายนี้ ผู้วิจัยขอขอบคุณ นายสุทิน ชวลิตเลขา บิดา นางวรรณกนก ชวลิตเลขา มารดา นางสาวนันทิรัตน์ ชวลิตเลขา น้องสาว และนางภารณี ชวลิตเลขา คู่สมรส ที่คอยให้ความสนับสนุนช่วยเหลือในทุกสิ่ง คอยอยู่เคียงข้างกันและเป็นกำลังใจให้กันตลอดมา จวบจนสารนิพนธ์นี้สมบูรณ์

สุทธิพันธุ์ ชวลิตเลขา

สิงหาคม 2565

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ

บทที่ 1

บทนำ

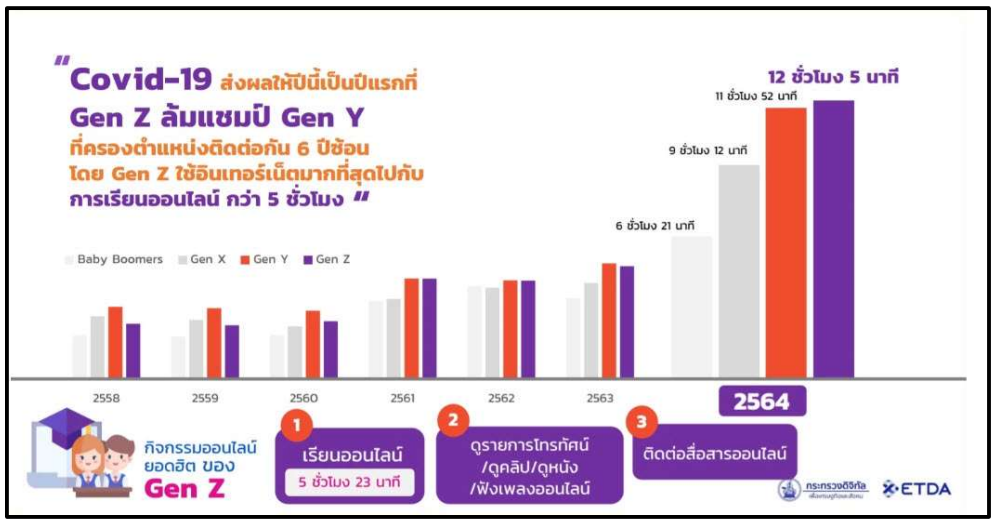
1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันโลกอินเทอร์เน็ตเป็นส่วนสำคัญในการดำรงชีวิตทั้งในมิติด้านเศรษฐกิจและสังคม การรักษาความมั่นคงและการป้องกันประเทศการสื่อสารโทรคมนาคมและการควบคุมดูแลโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญและจะทวีความสำคัญยิ่งขึ้นในอนาคต เนื่องจากความสามารถในการพัฒนาทางเทคโนโลยีที่รวดเร็วและความสามารถในการพัฒนาและการเข้าถึงเทคโนโลยีของประเทศที่มีความก้าวหน้าทางเทคโนโลยีในระดับรองลงมา ซึ่งความก้าวหน้าทางเทคโนโลยีจะตอบสนองต่อการใช้งานเครือข่ายเทคโนโลยีสารสนเทศของคนได้เป็นจำนวนมากทั้งกลุ่มที่เป็นผู้ใช้งานอินเทอร์เน็ตโดยตรง หรือผู้ที่ได้รับประโยชน์จากการใช้เครือข่ายเทคโนโลยีสารสนเทศในทางอ้อมซึ่งจะช่วยประหยัดเวลาและลดต้นทุนในการดำเนินการ (สุธาเทพ รุณเรศ, 2561)

ประเทศไทยในการก้าวสู่ยุคไทยแลนด์ 4.0 ที่รัฐมีเป้าหมายส่งเสริมให้มีการใช้วิทยาศาสตร์เทคโนโลยี วิจัยและพัฒนา อีกทั้งนวัตกรรมในทุกสาขาของภาคการผลิตและบริการโดยเฉพาะเทคโนโลยีดิจิทัลเพื่อยกระดับด้านเศรษฐกิจและสังคมของประเทศ ตามที่กำหนดไว้ในร่างยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561-2580) ยุทธศาสตร์ที่ 2 ด้านการสร้างความสามารถในการแข่งขัน ตามแนวโน้มความเสี่ยงของภัยคุกคามทางไซเบอร์ที่มีต่อเศรษฐกิจของโลก และยังพบว่าจากสถานการณ์โควิด-19 จึงทำให้ปีนี้เป็นปีแรกที่ กลุ่ม Gen Z (อายุน้อยกว่า 21 ปี) ทุบสถิติใช้งานอินเทอร์เน็ตมากที่สุด เฉลี่ยวันละ 12 ชั่วโมง 5 นาที ชนะกลุ่ม Gen Y (อายุ 21-40 ปี) อดีตแชมป์ 6 สมัยที่ใช้อินเทอร์เน็ตสูงที่สุด ซึ่งที่ปีนี้ Gen Y ใช้อินเทอร์เน็ตเฉลี่ยวันละ 11 ชั่วโมง 52 นาที ส่วน Gen X (อายุ 41-56 ปี) ใช้เฉลี่ยวันละ 9 ชั่วโมง 12 นาที และปิดท้ายด้วย Baby Boomer (อายุ 57-75 ปี) ใช้น้อยที่สุด เฉลี่ยวันละ 6 ชั่วโมง 21 นาที ตามลำดับ สำหรับกิจกรรมออนไลน์ที่กลุ่ม Gen Z ใช้เวลากับอินเทอร์เน็ตมากที่สุดคือเรียนออนไลน์เฉลี่ยวันละ 5 ชั่วโมง 23 นาที รองลงมาคือดูรายการโทรทัศน์ ดูคลิป ดูหนัง ฟังเพลงออนไลน์ เฉลี่ยวันละ 4 ชั่วโมง 11 นาที และติดต่อสื่อสารออนไลน์เฉลี่ยวันละ 3 ชั่วโมง 39 นาที ตามลำดับ (ฐานเศรษฐกิจดิจิทัล, 2564)

ด้วยความเสี่ยงของภัยคุกคามไซเบอร์ต่อเศรษฐกิจของโลกข้างต้น และจากการที่สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union : ITU) ได้มีการสำรวจประเทศต่าง ๆ ทั่วโลก 193 ประเทศ รวมทั้งประเทศไทยด้วย ในเรื่องของความมุ่งมั่นของการจัดการความมั่นคงปลอดภัยไซเบอร์ระดับชาติ (National Cyber security Commitments) โดยผลการสำรวจในปี พ.ศ. 2560 พบว่า ประเทศไทยมีคะแนนจากการสำรวจที่เรียกว่า Global Cybersecurity Index (GCI) Score ต่ำกว่าประเทศสิงคโปร์ มาเลเซีย ออสเตรเลีย ญี่ปุ่น เกาหลีใต้ และนิวซีแลนด์ซึ่งอยู่ในภูมิภาคเอเชียแปซิฟิกเช่นเดียวกัน โดยอยู่ในอันดับที่ 22 ซึ่งยังต่ำกว่าเป้าหมายที่กำหนดไว้ในแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ 12 (พ.ศ. 2560 - 2564) ที่กำหนดว่า อันดับความเสี่ยง

จากการโจมตีด้านไซเบอร์ตามดัชนี ITU ของประเทศไทยจะต้องต่ำกว่าอันดับที่ 10 ของโลก ด้วยเหตุนี้หากประเทศไทยต้องการบรรลุเป้าหมาย ก็เป็นเรื่องจำเป็นที่จะต้องศึกษารายละเอียดหลักเกณฑ์ที่ต้องมีการดำเนินการเพื่อนำมาปรับปรุงและยกระดับการดำเนินการด้านการสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศให้เป็นไปตามเป้าหมายที่กำหนดไว้ต่อไป (International Telecommunication Union, 2017)



ภาพประกอบที่ 1.1 สถิติการใช้งานอินเทอร์เน็ตของกลุ่มบุคคลแต่ละช่วงวัย (กระทรวงดิจิทัล, 2564.)

ระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบไอซีทีมีประโยชน์ต่อการพัฒนาประเทศให้เจริญก้าวหน้าโดยเป็นเรื่องที่เกี่ยวกับวิถีความเป็นอยู่ของสังคมสมัยใหม่ ก่อให้เกิดการเปลี่ยนแปลงวิถีชีวิตรวมถึงกลายเป็นสิ่งสำคัญและจำเป็นในการปฏิบัติงานของทุกองค์กรไม่ว่าจะเป็นการดำเนินธุรกิจอุตสาหกรรม การให้บริการโทรคมนาคม การท่องเที่ยว การทหาร และการศึกษา เป็นต้น หรือกล่าวได้ว่าโลกเข้าสู่สังคมฐานความรู้ (Knowledge-based Society) ที่มีการเชื่อมโยงข้อมูลเป็นระบบเครือข่าย โดยเฉพาะอย่างยิ่งเครือข่ายอินเทอร์เน็ตได้ถูกนำมาใช้อย่างแพร่หลายในทุกบริบทของสังคม (พงษ์ศักดิ์ ผกามาศ, 2553) อีกทั้งโครงสร้างพื้นฐานวิกฤต (Critical Infrastructure) ที่อยู่รอบตัวเรา เช่น ระบบไฟฟ้า น้ำประปา การคมนาคมขนส่ง ระบบธนาคาร และระบบสื่อสารโทรคมนาคม ล้วนมีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตแทบทั้งสิ้น การแพร่หลายของเครือข่ายนี้ได้เปลี่ยนวิถีการดำรงชีวิตของมนุษย์แทบทุกด้าน เช่น การใช้เว็บไซต์ การรับส่งอีเมล การซื้อขายสินค้าไปจนถึงการทำธุรกรรมทางอิเล็กทรอนิกส์ เช่น ระบบ Internet Banking ระบบ GFMIS ของรัฐบาล และระบบการชำระภาษี เป็นต้น แนวโน้มในอนาคตของมนุษยชาติย่อมหลีกเลี่ยงไม่ได้กับการใช้งานระบบเครือข่ายสากล (Universal Network) ที่เพิ่มมากขึ้น ตามการเปลี่ยนแปลงทั้งทางด้านวิทยาศาสตร์และเทคโนโลยี รวมถึงการเชื่อมโยงกันระหว่างประเทศในโลกยุคเศรษฐกิจดิจิทัล (Digital Economy)

พัฒนาการและการเปลี่ยนแปลงของระบบไอซีทีได้ส่งผลกระทบต่อกิจการและการดำเนินงานทางการเมือง การทหาร เศรษฐกิจ และสังคมจิตวิทยาของทุกประเทศในโลกเป็นอย่างมาก ผลจากการพัฒนาด้านวิทยาศาสตร์และเทคโนโลยีในหลายทศวรรษที่ผ่านมาทำให้เกิดการปฏิวัติสารสนเทศ (Information Revolution) ซึ่งเกี่ยวข้องกับการประมวลผลและกระจายสารสนเทศอย่างกว้างขวาง จนนำมาสู่การพัฒนาในสาขาคอมพิวเตอร์และการติดต่อสื่อสารอย่างก้าวกระโดดจนก่อให้เกิดพื้นที่มิติใหม่ที่เรียกว่า “โลกไซเบอร์” (Cyberspace) ด้วยเหตุนี้ความมั่นคงแห่งชาติ (National Security) จึงได้รับผลกระทบจากการปฏิวัติและปรากฏการณ์ของโลกไซเบอร์นี้โดยตรง เห็นได้จากมีผู้กล่าวถึง “ความมั่นคงด้านไซเบอร์” (Cybersecurity)ในบริบทของความมั่นคงแห่งชาติมากขึ้น อีกทั้งยังมีผู้กล่าวถึงคุณลักษณะของโลกไซเบอร์ ความล่อแหลมที่มีอยู่ภายใน ภัยคุกคามที่เป็นไปได้ด้านไซเบอร์ รวมถึงประเด็นที่เกี่ยวข้องกับการป้องกัน (Defense) การยับยั้ง (Deterrence) และการโจมตี (Attack) ในโลกไซเบอร์มากขึ้น แม้ว่าในปัจจุบันจะยังไม่มีหลักเกณฑ์ที่แน่นอนและชัดเจนที่จะกำหนดได้ว่า“การโจมตีด้านไซเบอร์เป็นอาชญากรรม” ในขณะเดียวกันยังไม่มีกลไกทางกฎหมายระหว่างประเทศใดที่จะสามารถระบุและควบคุมความสัมพันธ์ระหว่างรัฐในโลกไซเบอร์นี้ได้ ดังนั้นนานาอารยะประเทศรวมถึงประเทศไทยยังคงต้องค้นหารูปแบบและวิธีการที่เหมาะสมในการจัดการกับภัยคุกคามนี้อย่างต่อเนื่องจนถึงปัจจุบัน ทั้งนี้เพื่อให้เกิดความมั่นคงในการใช้ประโยชน์จากระบบ ไอซีที เพื่อการพัฒนาประเทศชาติอย่างแท้จริง (ราชิต อรุณรังสี, พลตรี, 2561)

ในส่วนของ บริษัทวิทยุการบินแห่งประเทศไทย จำกัด พบสถิติภัยคุกคามไซเบอร์ ตั้งแต่เดือนมกราคม พ.ศ. 2562 – พฤษภาคม พ.ศ. 2563 มีจำนวนทั้งสิ้น 57,902 ครั้ง โดยภัยคุกคามประเภท Attempted Information Leak มีสถิติเป็นอันดับ 1 คิดเป็นร้อยละ 41.52 ตามมาด้วย Potential Corporte Policy Violation คิดเป็นร้อยละ 19.53 (วิทยา จุลวัฒนานนท์, 2563) รายละเอียดตามตารางที่ 1.1

ตารางที่ 1.1 สถิติภัยคุกคามทางไซเบอร์ของ บริษัทวิทยุการบินแห่งประเทศไทย จำกัด

ลำดับ	ประเภทภัยคุกคาม	จำนวน	ร้อยละ
1.	Attempted Information Leak (โจมตีการรั่วไหลข้อมูล)	23,705	41.52
2.	Potential Corporte Policy Violation (การละเมิดนโยบายองค์กร)	11,155	19.53
3.	A Network Trojan was Detected (ตรวจพบโทจันในเครือข่าย)	9,117	15.97
4.	Attempted Administrator Privilege Gain (ความพยายามเข้าถึงสิทธิผู้ดูแลระบบ)	6,283	11.01
5.	Web Application Attack (การโจมตีเว็บแอพพลิเคชั่น)	3,010	5.27

ตารางที่ 1.1 (ต่อ)

6.	Attempted User Privilege Gain (ความพยายามรับสิทธิผู้ใช้งาน)	2,787	4.88
7.	Misc Attack (การโจมตีอื่น)	1,020	1.79
8.	Attempted Denial of Service (พยายามปฏิเสธการให้บริการ)	6	0.01
9.	Misc Activity (กิจกรรมอื่น ๆ)	5	0.01
10.	Detection of Denial-of-Service Attack ตรวจจับการปฏิเสธการโจมตีระบบ	4	0.01
	รวม	**57,092**	**100**

ที่มา : กองบริหารระบบเทคโนโลยีสารสนเทศ บริษัทวิทยุการบินแห่งประเทศไทย จำกัด

จากปัญหาดังกล่าวผู้วิจัยได้เล็งเห็นความสำคัญของปัญหา จากสถิติภัยคุกคามทางไซเบอร์กอปรกับสถานการณ์โรคระบาด COVID-19 ที่มีมาตรการรักษาระยะห่างทางสังคม ทำให้ต้องเกิดการทำงานจากที่บ้าน Work from Home (WFH) ยิ่งเป็นการเพิ่มความเสี่ยงที่จะทำให้มีโอกาสเกิดภัยคุกคามทางไซเบอร์ได้มากยิ่งขึ้น ดังนั้นการป้องกันภัยคุกคามทางไซเบอร์ด้วยการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์เป็นวิธีที่สะดวก ประหยัดงบประมาณ และความตระหนักรู้นี้จะเป็นสิ่งที่ป้องกันภัยคุกคามทางไซเบอร์ให้กับพนักงานและบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ได้อย่างดีและยั่งยืน จึงสนใจศึกษาแนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด และนำผลวิจัยไปนำเสนอแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์ เพื่อให้มีความเหมาะสมและทันกับการเปลี่ยนแปลงของเทคโนโลยีและภัยคุกคามทางไซเบอร์รูปแบบใหม่ รวมทั้งจัดทำแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ต่อไป

1.2 คำถามการวิจัย

1. พฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างไร
2. แนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์ ควรเป็นอย่างไร
3. แอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด สามารถทำได้อย่างไร

1.3 วัตถุประสงค์ของการวิจัย

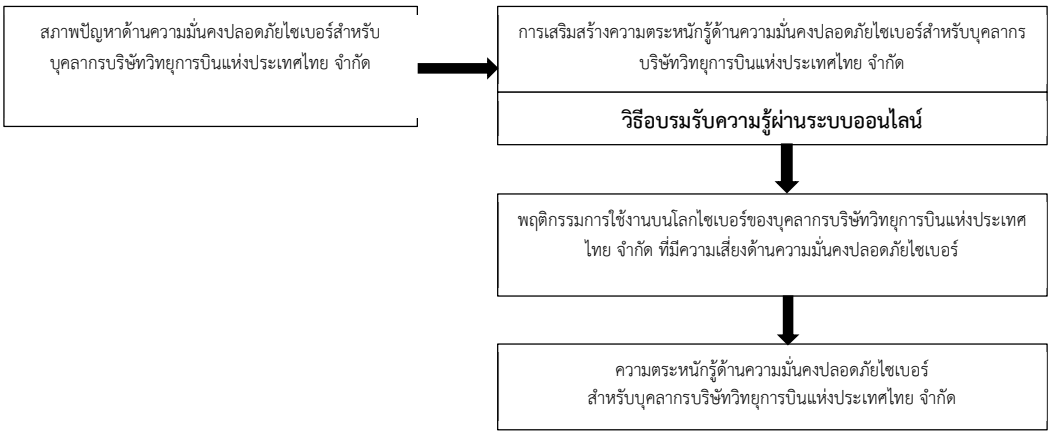
1. เพื่อศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
2. เพื่อพัฒนาแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์
3. เพื่อจัดทำแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

1.4 สมมติฐานการวิจัย

1. พฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อยู่ในระดับมาก
2. แนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์ที่ผู้วิจัยได้จัดทำขึ้นมีความเหมาะสมอยู่ในระดับมาก
3. แอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด มีค่าการยอมรับอยู่ในระดับมาก

1.5 กรอบแนวคิดในการวิจัย

จากการศึกษาแนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง เพื่อวิเคราะห์และออกแบบสอบถามในการสอบถามประชากรบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ในเรื่องของความรู้ ความเข้าใจ เพื่อศึกษาพฤติกรรมและความพร้อมของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ในการรับมือกับภัยคุกคามทางไซเบอร์ จากนั้นสรุปข้อมูล เพื่อเป็นแนวทางในการกำหนดวิธีการที่เหมาะสมในการสร้างการตระหนักรู้ โดยมีกรอบแนวคิดในการวิจัย ดังภาพประกอบที่ 1.2



ภาพประกอบที่ 1.2 กรอบแนวคิดในการวิจัย

1.6 ขอบเขตของการวิจัย

งานวิจัยเรื่อง “การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ” มีขอบเขตเนื้อหาในการวิจัยดังนี้

1. ขอบเขตด้านเวลา : ระยะเวลาในการทำวิจัยจากการศึกษา วิเคราะห์ ออกแบบและสรุปแนวทางในการกำหนดนโยบาย ใช้เวลา 1 ปีการศึกษา ตั้งแต่เดือนกันยายน พ.ศ. 2564 ถึงเดือสิงหาคม พ.ศ. 2565
2. ขอบเขตด้านสถานที่/ประชากร : บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด
3. ขอบเขตด้านเนื้อหาของการทำงานวิจัย ได้แก่ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.2560-2564 แนวคิดทฤษฎีและงานวิจัยที่เกี่ยวข้อง

1.7 ประโยชน์ที่ได้รับจากการวิจัย

1. สามารถลดความเสี่ยงและความเสียหายจากการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ในด้านความมั่นคงปลอดภัยไซเบอร์
2. การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด จากการใช้งานบนโลกไซเบอร์ เป็นประโยชน์ต่อบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด และสามารถให้ความรู้ต่อบุคคลใกล้ตัวได้
3. สามารถใช้เป็นต้นแบบวิธีการประเมินความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ได้

1.8 นิยามศัพท์

1. ไซเบอร์ (Cyber) คือ มีความหมายว่าเกี่ยวข้องกับคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ หรืออินเทอร์เน็ตหรือความเป็นจริงเสมือน (Virtual Reality) เช่น ไซเบอร์สเปซ (Cyberspace) หมายถึง สภาพแวดล้อมสมมติในเครือข่ายอินเทอร์เน็ต (ราชบัณฑิตสาขาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ, 2559)
2. ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) หมายถึง ความรู้แจ้งชัดเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เช่น ความเสี่ยง ภัยคุกคาม การระราน การแอบอ้าง การกีดกัน การโจมตี การก่อการร้าย ฯลฯ ในระบบ (ราชบัณฑิตสาขาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ, 2562)
3. ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) หมายถึง ภาวะพ้นจากภัยคุกคามที่มีต่อเครือข่ายระบบคอมพิวเตอร์ โปรแกรม และข้อมูล เพื่อรักษาไว้ซึ่งลักษณะสำคัญ 3 ประการ คือ ความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน ภาวะดังกล่าวจะเกิดขึ้นได้ ต้องอาศัยบุคลากร ประบวนการทำงาน และเครื่องมือที่เหมาะสม (ราชบัณฑิตสาขาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ, 2558)

1.9 สรุป

ในบทที่ 1 ผู้วิจัยได้นำเสนอความเป็นมาและความสำคัญของปัญหา คำถามการวิจัย วัตถุประสงค์ของการวิจัย สมมติฐานการวิจัย กรอบแนวคิดในการวิจัย ขอบเขตของการวิจัย ประโยชน์ที่คาดว่าจะได้รับ และนิยามศัพท์เฉพาะ ซึ่ง ทฤษฎี แนวคิด และงานวิจับที่เกี่ยวข้องจะได้นำเสนอต่อไปในบทที่ 2

บทที่ 2

แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

การวิจัย เรื่อง “การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด” นี้ ผู้วิจัยได้ศึกษาแนวคิด ทฤษฎี เอกสารทางวิชาการ และศึกษาเอกสารงานวิจัยที่เกี่ยวข้องเพื่อเป็นแนวทางในการวิจัย ดังนี้

2.1 การใช้อินเทอร์เน็ตและระบบดิจิทัลในประเทศไทย

2.2 แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)

2.3 แนวคิดเกี่ยวกับการคุกคามทางไซเบอร์ (Cyber Threat)

2.4 แนวคิดเกี่ยวกับการกลั่นแกล้งทางไซเบอร์ (Cyber Bullying)

2.5 กรอบการรักษาความมั่นคงปลอดภัย (NIST Cybersecurity Framework)

2.6 งานวิจัยที่เกี่ยวข้อง

2.7 สรุป

2.1 การใช้อินเทอร์เน็ตและระบบดิจิทัลในประเทศไทย

2.1.1 สถิติการใช้อินเทอร์เน็ตและระบบดิจิทัลในประเทศไทย

ประเทศไทยมีการใช้ประโยชน์จากอินเทอร์เน็ตและระบบดิจิทัลมากขึ้น โดยจากสถิติของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center : NECTEC) พบว่า ในปี พ.ศ. 2559 มีผู้ใช้อินเทอร์เน็ตในไทยเกือบ 40 ล้านคน เพิ่มขึ้นจาก ปี พ.ศ. 2557 ที่มีผู้ใช้ประมาณ 30 ล้านคน คิดเป็นร้อยละ 16 ของจำนวนผู้ใช้อินเทอร์เน็ตในภูมิภาคเอเชียตะวันออกเฉียงใต้ ซึ่งมีจำนวนโดยประมาณ 250 ล้านคน นอกจากนี้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้ทำการสำรวจข้อมูลการใช้อินเทอร์เน็ต พบว่าในปี พ.ศ. 2558 ประเทศไทยมีประชากรใช้อินเทอร์เน็ตอายุ ตั้งแต่ 6 ปีขึ้นไป โดยประชากร 1 คนจะใช้เวลาโดยเฉลี่ย 41.4 ชั่วโมงต่อสัปดาห์ ในการใช้อินเทอร์เน็ต โดยการใช้งานผ่าน Smart Phone ซึ่งเป็นช่องทางที่นิยมใช้กันมากที่สุด คิดเป็นร้อยละ 80.9 และการใช้คอมพิวเตอร์แบบตั้งโต๊ะ (Desktop) และการใช้คอมพิวเตอร์แบบพกพา (Laptop) เป็นที่นิยมเป็นอันดับสองและสามตามลำดับ และส่วนใหญ่ใช้งานอินเทอร์เน็ตในส่วนของสื่อสังคมออนไลน์ ได้แก่ YouTube Facebook และ LINE มากที่สุด และในปี พ.ศ. 2561 พบว่าการใช้งานอินเทอร์เน็ตของคนไทยมีเพิ่มขึ้นจากปี พ.ศ. 2560 เฉลี่ย 3 ชม. ต่อวัน โดยส่วนใหญ่ใช้งานอินเทอร์เน็ตในช่วงวันหยุด โดยพบในกลุ่ม Gen Y (อายุระหว่าง 18–37 ปี) และ Gen Z (อายุน้อยกว่า 18 ปี) มากที่สุด สำหรับสถานที่

ที่มีการใช้งานอินเทอร์เน็ตมากที่สุด คือ ระหว่างเดินทางและในที่สาธารณะ คิดเป็นร้อยละ 33.2 และร้อยละ 20.8 ตามลำดับ และกิจกรรมที่ใช้งานอินเทอร์เน็ตเพิ่มขึ้นจากปี พ.ศ. 2560 คือ อ่านหนังสือออนไลน์ คิดเป็นร้อยละ 48.27 รองลงมาเป็นขายสินค้าและบริการ คิดเป็นร้อยละ 24.48 และ จองโรมแรม คิดเป็นร้อยละ 20.65 จะเห็นว่าการเข้าถึงระบบเครือข่ายสารสนเทศและอินเทอร์เน็ตทำได้ง่าย และสะดวกสบายต่อการใช้ชีวิตประจำวัน แต่ในขณะเดียวกันก็ทำให้เกิดความเสี่ยงต่อการนำไปใช้ในทางที่ผิดและเสี่ยงที่จะ เกิดภัยคุกคามต่อชีวิตเพิ่มขึ้นอีกด้วย กล่าวคือ ภัยที่เกิดจากมิจฉาชีพหรือผู้ไม่ประสงค์ดีใช้อินเทอร์เน็ตใน การก่ออาชญากรรมและแสวงผลประโยชน์ในรูปแบบต่าง ๆ ภัยที่จะเกิดต่อระบบควบคุมดูแลการใช้งานอินเทอร์เน็ตและระบบปฏิบัติการที่เกี่ยวข้องกับโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญ ซึ่งก่อให้เกิดผลกระทบต่อการใช้ชีวิตของประชาชนและภาคธุรกิจเอกชน ทั้งในยามปกติและยามเกิดเหตุฉุกเฉิน ภัยที่ส่งผลกระทบต่อสังคมวัฒนธรรม และธรรมเนียมประเพณีอันดีงามทั้งต่อบุคคลทั่วไป เด็ก สตรี และเยาวชน (กระทรวงคมนาคม, 2562)

สำนักงานสถิติแห่งชาติ, (2564) ได้ทำการสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือนได้จัดทำเป็นครั้งแรกในปี พ.ศ. 2544 และตั้งแต่ พ.ศ. 2546 เป็นต้นมา สำนักงานสถิติแห่งชาติได้ทำการสำรวจต่อเนื่องเป็นประจำทุกปี เพื่อให้ทราบจำนวนประชาชนที่ใช้โทรศัพท์มือถือ อินเทอร์เน็ต คอมพิวเตอร์ลักษณะและพฤติกรรมในการใช้อุปกรณ์เทคโนโลยีต่าง ๆ รวมทั้งจำนวนครัวเรือนที่มีอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร เช่น โทรศัพท์พื้นฐานเครื่องคอมพิวเตอร์ และการเชื่อมต่ออินเทอร์เน็ตในครัวเรือน เป็นต้น

การสำรวจใช้วิธีสัมภาษณ์หัวหน้าครัวเรือน และสมาชิกในครัวเรือนที่มีอายุ 6 ปีขึ้นไป จากครัวเรือนตัวอย่างทั้งสิ้น 83,880 ครัวเรือน ผลการสำรวจสรุปได้ดังนี้ ผลการสำรวจประชาชนอายุ 6 ปีขึ้นไป ประมาณ 63.8 ล้านคน พบว่ามีผู้ใช้โทรศัพท์มือถือ 60.5 ล้านคน (ร้อยละ 94.8) ผู้ใช้อินเทอร์เน็ต 49.7 ล้านคน (ร้อยละ 77.8) และผู้ใช้คอมพิวเตอร์16.8 ล้านคน (ร้อยละ 26.4)

การใช้โทรศัพท์มือถือ สำหรับการใช้โทรศัพท์มือถือของประชาชนอายุ 6 ปีขึ้นไป ซึ่งมีผู้ใช้โทรศัพท์มือถือ ร้อยละ 94.8 เมื่อจำแนกตามเขตการปกครอง พบว่า ในเขตเทศบาลมีผู้ใช้โทรศัพท์มือถือ ร้อยละ 95.8 นอกเขตเทศบาลมีผู้ใช้โทรศัพท์มือถือร้อยละ 94.0

รูปแบบการใช้โทรศัพท์มือถือ เมื่อพิจารณารูปแบบการใช้โทรศัพท์มือถือ พบว่า ประชาชนใช้โทรศัพท์มือถือแบบ Smart Phone มากที่สุดคือ ร้อยละ 86.4 รองลงมาคือใช้โทรศัพท์มือถือแบบ Feature Phone ร้อยละ 12.7 และใช้โทรศัพท์มือถือทั้งแบบ Smart Phone และ Feature Phone ร้อยละ 0.9

การใช้อินเทอร์เน็ตและคอมพิวเตอร์ เมื่อพิจารณาแนวโน้มการใช้อินเทอร์เน็ตและคอมพิวเตอร์ในช่วงระหว่างปี 2559–2563 พบว่า ในระยะเวลา 5 ปีนี้ ประเทศไทยมีผู้ใช้อินเทอร์เน็ตเพิ่มขึ้นโดยผู้ใช้อินเทอร์เน็ตเพิ่มขึ้นจากร้อยละ 47.5 (29.8 ล้านคน) ในปี 2559 เป็นร้อยละ 77.8 (49.7 ล้านคน) ในปี 2563 ในขณะที่สัดส่วนของผู้ใช้คอมพิวเตอร์มีแนวโน้มลดลงในปี 2559 ถึง 2562 แต่ในปี 2563 เพิ่มขึ้นเล็กน้อยคิดเป็นร้อยละ 26.4 (16.8 ล้านคน)

สำหรับการใช้เทคโนโลยีสารสนเทศและการสื่อสารของประชาชนที่อาศัยอยู่ในเขตเทศบาลและนอกเขตเทศบาล ระหว่างปี 2559–2563 พบว่าผู้ใช้อินเทอร์เน็ตมีแนวโน้มเพิ่มขึ้นทั้งในเขต

เทศบาลและนอกเขตเทศบาล คือในเขตเทศบาลจากร้อยละ 57.4 ในปี 2559 เป็นร้อยละ 83.6 ในปี 2563ส่วนนอกเขตเทศบาลจากร้อยละ 39.5 ในปี 2559 เป็นร้อยละ 73.2 ในปี 2563

สำหรับผู้ใช้คอมพิวเตอร์ที่อยู่ในเขตเทศบาลและนอกเขตเทศบาลมีแนวโน้มลดลงในปี 2559–2562 แต่ในปี 2563 ผู้ใช้คอมพิวเตอร์เพิ่มขึ้นทั้งในเขตเทศบาลและนอกเขตเทศบาลร้อยละ 32.8และร้อยละ 21.2 ตามลำดับ

เมื่อพิจารณาผู้ใช้โทรศัพท์มือถือ อินเทอร์เน็ต และคอมพิวเตอร์เป็นรายภาค พบว่า กรุงเทพมหานครมีผู้ใช้โทรศัพท์มือถือสูงที่สุดคือ ร้อยละ 97.2 รองลงมาคือ ภาคกลาง ร้อยละ 95.0 และใช้ต่ำที่สุดคือ ภาคตะวันออกเฉียงเหนือร้อยละ 94.0

สำหรับการใช้อินเทอร์เน็ต พบว่า กรุงเทพมหานครมีผู้ใช้อินเทอร์เน็ตสูงที่สุดเช่นเดียวกันคือ ร้อยละ 91.4 รองลงมาคือ ภาคกลาง ร้อยละ 81.2 และใช้ต่ำที่สุดคือ ภาคตะวันออกเฉียงเหนือร้อยละ 70.9 ในขณะที่การใช้คอมพิวเตอร์กรุงเทพมหานครยังมีผู้ใช้คอมพิวเตอร์ สูงที่สุดเช่นเดียวกันคือ ร้อยละ 43.4 รองลงมาคือ ภาคกลาง ร้อยละ 26.7 และใช้ต่ำที่สุดคือ ภาคตะวันออกเฉียงเหนือ ร้อยละ 20.9

2.1.2 ลักษณะและพฤติกรรมการใช้อินเทอร์เน็ต

สำนักงานสถิติแห่งชาติ, (2564) ได้รายงานลักษณะและพฤติกรรมการใช้อินเทอร์เน็ต ดังนี้

เมื่อเปรียบเทียบการใช้อินเทอร์เน็ตระหว่างเพศชายและหญิงในปี 2559–2563 ไม่แตกต่างกันมากนัก โดยปี 2563 พบว่า ผู้ชายใช้อินเทอร์เน็ต ร้อยละ 79.0 ผู้หญิงใช้ ร้อยละ 76.8 เมื่อพิจารณาการใช้อินเทอร์เน็ตตามกลุ่มอายุต่าง ๆ ในปี 2559–2563 ทุกกลุ่มอายุมีแนวโน้มใช้อินเทอร์เน็ตสูงขึ้น โดยในปี 2563 พบว่า กลุ่มอายุ 15-24 ปี มีการใช้อินเทอร์เน็ตสูงที่สุด ร้อยละ 98.4 รองลงมาคือ กลุ่มอายุ 25-34 ปีร้อยละ 97.3 และกลุ่มอายุ 35-49 ปีร้อยละ 90.6

สำหรับสถานที่ใช้อินเทอร์เน็ต พบว่า ส่วนใหญ่ใช้ที่บ้าน/ที่พักอาศัยร้อยละ 95.6 รองลงมาคือ ใช้ตามสถานที่ต่าง ๆ ผ่านโทรศัพท์มือถือร้อยละ 89.6 และใช้ที่ทำงาน ร้อยละ 33.1

ส่วนกิจกรรมที่ใช้ส่วนใหญ่ใช้ Social Media เช่น Facebook, Twitter, LINE, WhatsApp เป็นต้น ร้อยละ 92.0 รองลงมาคือ ใช้โทรศัพท์ผ่าน Internet (VoIP) เช่น โทรผ่าน Line, Facebook, Facetime, WhatsApp เป็นต้น ร้อยละ 90.9 และใช้ในการดาวน์โหลดหรือสตรีมมิ่งรูปภาพ/หนัง/วิดีโอ/เพลง/เกมส์เล่นเกมส์ดูหนัง ร้อยละ 74.3

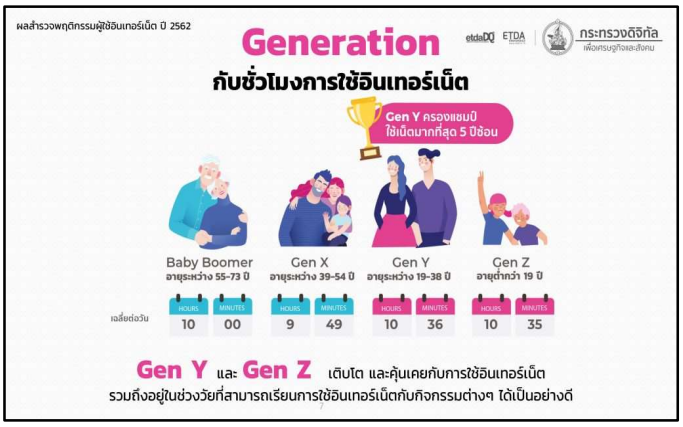
ในขณะที่ความถี่ในการใช้อินเทอร์เน็ต พบว่า มีผู้ใช้อินเทอร์เน็ตใช้ทุกวัน ร้อยละ 89.3 รองลงมาใช้อย่างน้อยสัปดาห์ละครั้ง ร้อยละ 10.1

ส่วนอุปกรณ์ในการเข้าถึงอินเทอร์เน็ตส่วนใหญ่ผู้ใช้อินเทอร์เน็ตใช้โทรศัพท์มือถือแบบ Smart Phone ในการเข้าถึงอินเทอร์เน็ตค่อนข้างสูงคือ ร้อยละ 99.2 รองลงมาใช้คอมพิวเตอร์ตั้งโต๊ะ ร้อยละ27.2 และใช้คอมพิวเตอร์พกพาร้อยละ 12.5

จากรายงานผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทยในปี 2562 โดย ETDA ได้รายงานรายงานพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ไว้ดังนี้

พฤติกรรมการใช้อินเทอร์เน็ตโดยเฉลี่ยคนไทยมีการใช้งานอินเทอร์เน็ต 10 ชั่วโมง 22 นาที ต่อวัน หากแยกตาม Generation พบว่า Gen Y และ Gen Z ครองแชมป์ผู้ที่ใช้งานอินเทอร์เน็ตสูง

ที่สุด เนื่องจาก Gen Y ส่วนมากเป็นวัยทำงานที่มีความจำเป็นต้องใช้อินเทอร์เน็ตประกอบการทำงานและจัดการธุระส่วนตัว ขณะที่ Gen Z ส่วนมากเป็นคนวัยเรียน ที่ต้องใช้อินเทอร์เน็ตประกอบการศึกษาหาความรู้และใช้ในช่วงเวลาว่างเป็นส่วนมาก อันดับ 1 Gen Y (อายุ 19 -38 ปี) มีอัตราการใช้อินเทอร์เน็ตต่อวันเฉลี่ยอยู่ที่ 10 ชั่วโมง 36 นาทีอันดับ 2 Gen Z (อายุน้อยกว่า 19 ปี) มีอัตราการใช้อินเทอร์เน็ตต่อวันเฉลี่ยอยู่ที่ 10 ชั่วโมง 35 นาที อันดับ 3 Baby Boom (อายุ 55 -73 ปี) มีอัตราการใช้อินเทอร์เน็ตต่อวันเฉลี่ยอยู่ที่ 10 ชั่วโมง อันดับ 4 Gen X (อายุ 39 -54 ปี) มีอัตราการใช้อินเทอร์เน็ตต่อวันเฉลี่ยอยู่ที่ 9 ชั่วโมง 49 นาที รายละเอียดแสดงในภาพประกอบที่ 2.1



ภาพประกอบที่ 2.1 รายงานพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย (ข้อมูลจาก ETDA)

การจำแนกตามเพศจะพบว่า กลุ่มเพศทางเลือกมีการใช้อินเทอร์เน็ตมากที่สุดเฉลี่ยอยู่ที่ 11 ชั่วโมง 20 นาทีต่อวัน รองลงมาคือเพศชายเฉลี่ยที่ 10 ชั่วโมง 25 นาทีต่อวัน และเพศหญิง เฉลี่ยที่ 10 ชั่วโมง 17 นาทีต่อวัน อัตราการใช้อินเทอร์เน็ตทั่วประเทศไทย ภาคเหนือครองแชมป์ แต่เฉลี่ยแล้วไม่ต่างกันมาก ปริมาณผู้ใช้งานอินเทอร์เน็ตในแต่ละภูมิภาคของประเทศไทย โดยเฉลี่ยไม่แตกต่างกันมากแสดงว่าอินเทอร์เน็ตภายในประเทศมีความครอบคลุมและทั่วถึง ทำให้ประชากรทั่วทุกพื้นที่สามารถใช้งานได้อย่างเท่าเทียมกัน โดยภูมิภาคที่มีการใช้งานอินเทอร์เน็ตมากที่สุดคือ อันดับ 1 ภาคเหนือ เฉลี่ย 10 ชั่วโมง 31 นาที อันดับ 2 ภาคตะวันออกเฉียงเหนือ เฉลี่ย 10 ชั่วโมง 28 นาที อันดับ 3 ภาคกลาง เฉลี่ย 10 ชั่วโมง 19 นาที อันดับ 4 กรุงเทพฯ เฉลี่ย 10 ชั่วโมง 19 นาที และอันดับ 5 ภาคใต้ เฉลี่ย 10 ชั่วโมง 17 นาที รายละเอียดแสดงในภาพประกอบที่ 2.2

ภาพประกอบที่ 2.2 รายงานพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย (ข้อมูลจาก ETDA)

การใช้อินเทอร์เน็ตเพื่อความบันเทิงเป็นส่วนใหญ่ โดยใช้งาน Social Media หรือแพลตฟอร์มออนไลน์อย่าง Facebook, Instagram, twitter มากถึง ร้อยละ 91.2 ครองอันดับ 1 ถึง 7 ปีซ้อน สื่อให้เห็นถึงพฤติกรรมการใช้งานอินเทอร์เน็ตที่เพิ่มมากขึ้นในทุก ๆ ปี โดยกิจกรรมการชำระเงินค่าสินค้าและบริการ ได้ติด 1 ใน 5 ของกิจกรรมยอดฮิตเป็นปีแรก แสดงถึงความเชื่อมั่นในความมั่นคงปลอดภัยของการทำธุรกรรมทางออนไลน์และพฤติกรรมการใช้จ่ายผ่านทางออนไลน์ที่เพิ่มมากขึ้นอีกด้วย ซึ่งกิจกรรมยอดฮิต 10 อันดับ ได้แก่ อันดับ 1 ใช้ Social Media เช่น Facebook, Instagram, twitter เฉลี่ยร้อยละ 91.2 อันดับ 2 ดูหนัง ฟังเพลง เฉลี่ยร้อยละ 71.2 อันดับ 3 ค้นหาข้อมูลออนไลน์ เฉลี่ยร้อยละ 70.7 อันดับ 4 รับ – ส่ง E-mail เฉลี่ยร้อยละ 62.5 อันดับ 5 ชำระเงินค่าสินค้าและบริการ เฉลี่ยร้อยละ 60.6 อันดับ 6 อ่านหนังสือออนไลน์ เฉลี่ยร้อยละ 57.1 อันดับ 7 ซื้อสินค้าและบริการ เฉลี่ยร้อยละ 57.0 อันดับ 8 ติดต่อสื่อสารออนไลน์ เฉลี่ยร้อยละ 50.0 อันดับ 9 เล่นเกมออนไลน์ เฉลี่ยร้อยละ 34.1 และอันดับ 10 Live สด เฉลี่ยร้อยละ 29.6 รายละเอียดแสดงในภาพประกอบที่ 2.3

ภาพประกอบที่ 2.3 รายงานพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย แยกตามกิจกรรม (ETDA)

สั่งอาหารออนไลน์เพิ่มมากขึ้น ร้อยละ 15.1 จากปี 2561 แสดงถึงพฤติกรรมที่ชื่นชอบความสะดวกสบายและบริการที่รวดเร็วโดยมีโซเชียลมีเดียเป็นสื่อกลาง ผ่านบริการจากบริษัท Food Delivery ที่เพิ่มมากขึ้นในปัจจุบัน โดยกิจกรรมที่สะท้อนถึงพฤติกรรมการซื้อสินค้าและบริการผ่านทางช่องทางออนไลน์ก็ติดอันดับกิจกรรมยอดนิยมที่มีการเติบโตมากที่สุดระหว่างปี 2561 -2562 อันดับ 1 บริการสั่งอาหาร เพิ่มขึ้น ร้อยละ 15.1 อันดับ 2 ชำระเงินค่าสินค้าและบริการออนไลน์ เพิ่มขึ้น ร้อยละ 11.4 อันดับ 3 รับ-ส่งสินค้าและพัสดุ เอกสารออนไลน์ เพิ่มขึ้น ร้อยละ 11.0 อันดับ 4 ดูหนังฟังเพลง เพิ่มขึ้น ร้อยละ 10.5 และอันดับ 5 ใช้บริการรถโดยสารออนไลน์ เพิ่มขึ้น ร้อยละ 9.3

การค้นหาข้อมูลของบริการ รีวิว และการค้นหาคำตอบ ชาวไทยใช้การ Search Engine หรือการค้นหาผ่านทาง Google มากเป็นอันดับ 1 ด้วยค่าเฉลี่ยที่ ร้อยละ 97.3 แสดงถึงพฤติกรรมที่เชื่อในการค้นหาข้อมูลการใช้งานจริงหรือรีวิวจากผู้ใช้งานก่อนจะเลือกใช้สินค้าหรือบริการ โดยแบ่งช่องทางค้นหายอดนิยมเป็น 5 อันดับ ดังนี้ อันดับ 1 Search Engine เฉลี่ยร้อยละ 97.3 อันดับ 2 YouTube เฉลี่ยร้อยละ 75.2 อันดับ 3 Facebook Fanpage เฉลี่ยร้อยละ 67.3 อันดับ 4 Website/Blog เฉลี่ยร้อยละ 44.4 อันดับ 5 Pantip เฉลี่ยร้อยละ 42.7

ช่องทางขายของออนไลน์ยอดนิยมในไทย Facebook Fanpage ครองอันดับ 1 ที่เจ้าของธุรกิจและพ่อค้าแม่ค้าออนไลน์นิยมเข้ามาเปิดร้านค้ามากที่สุด เฉลี่ยที่ ร้อยละ 64.0 ขณะที่ Shopee ตามมาเป็นอันดับที่ 2 ที่ ร้อยละ 43.1 และอันดับอื่น ๆ ดังนี้ อันดับ 1 Facebook Fanpage เฉลี่ยร้อยละ 64.0 อันดับ 2 Shopee เฉลี่ยร้อยละ 43.1 อันดับ 3 Line เฉลี่ยร้อยละ 39.5 อันดับ 4 Instagram เฉลี่ยร้อยละ 26.6 อันดับ 5 Lazada เฉลี่ยร้อยละ 24.8 อันดับ 6 Twitter เฉลี่ยร้อยละ 8.7

ช่องทางที่ร้านค้าเลือกเปิดร้านมาที่สุดจะเป็น Facebook Fanpage แต่ผู้บริโภคกลับไว้วางใจที่จะซื้อสินค้าผ่านแพลตฟอร์ม E-Commerce อย่าง Shopee เป็นอันดับ 1 สูงถึง ร้อยละ 75.6 รองลงมาคือ Lazada ร้อยละ 65.5 ในขณะที่ Facebook Fanpage ตกเป็นอันดับที่ 3 เฉลี่ยที่ ร้อยละ 47.5 และอันดับอื่น ๆ ดังนี้ อันดับ 1 Shopee เฉลี่ยร้อยละ 75.6 อันดับ 2 Lazada เฉลี่ยร้อยละ 65.5 อันดับ 3 Facebook Fanpage เฉลี่ยร้อยละ 47.5 อันดับ 4 Line เฉลี่ยร้อยละ 38.9 อันดับ 5 Instagram เฉลี่ยร้อยละ 21.8 อันดับ 6 Twitter เฉลี่ยร้อยละ 5.7 (Fillgoods, 2564)

จากการศึกษา ลักษณะและพฤติกรรมการใช้อินเทอร์เน็ต ผู้วิจัยสรุปได้ว่า พฤติกรรมการใช้อินเทอร์เน็ตของชาวไทยมีแนวโน้มการใช้งานเพิ่มมากขึ้นทุกปี เนื่องจากอินเทอร์เน็ตที่เปิดให้บริการอย่างครอบคลุม ทำให้ประชาชนสามารถเข้าถึงได้ง่าย โดย Social Media ที่มีการใช้งานมากเป็นอันดับต้น ๆ สะท้อนให้เห็นว่าในอนาคต Social Media จะเข้ามามีบทบาทกับในการใช้ชีวิตประจำวันมากขึ้น ไม่เพียงแค่การเสพสื่อบันเทิง ค้นคว้าหาความรู้ แต่จะรวมไปถึงการซื้อสินค้าอุปโภค บริโภค และการชำระค่าสินค้าผ่านทางช่องทางออนไลน์

2.2 แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช. หรือ NSTDA) ให้ความหมายของไซเบอร์ (Cyber) คือ คำที่กร่อนมาจากคำว่าไซเบอร์เนติกส์ (Cybernetics) และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต(Internet) และ

ยังมีการให้ความหมาย “สารสนเทศ (Virtual) เสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง” ไซเบอร์เนติกส์ (Cybernetics) เป็นวิชาการเกี่ยวกับระบบควบคุม เช่น ระบบประสาทของสิ่งมีชีวิต เพื่อนำไปใช้พัฒนาระบบอิเล็กทรอนิกส์ หรือ ระบบกลไกที่ทำงานคล้ายคลึงกัน วิชานี้เปรียบเทียบความคล้ายคลึงและต่างกันระหว่างสิ่งมีชีวิตกับสิ่งไม่มีชีวิต และยึดหลักการพื้นฐานทางด้านการสื่อสารและการควบคุมที่สามารถอธิบายการทำงานของทั้งสิ่งมีชีวิตและสิ่งไม่มีชีวิตได้ (ชนินทร เฉลิมทรัพย์, นาวาอากาศเอก, 2561)

จากความหมายของไซเบอร์ สรุปได้ว่า ไซเบอร์ (Cyber) คือ ระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต (Internet) รวมไปถึงสารสนเทศที่ใช้ในการสื่อสารต่าง ๆ ระหว่างบุคคล สื่อสารภายในหน่วยงานและองค์กรต่าง ๆ

ความมั่นคงปลอดภัยไซเบอร์ คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยงและความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูล ทั้งนี้ ความมั่นคงปลอดภัยไซเบอร์ยังรวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลายการจารกรรมและความผิดพลาดต่าง ๆ ซึ่งความเสี่ยงของความมั่นคงปลอดภัยไซเบอร์อาจรวมถึงสิ่งต่าง ๆ การละเมิดการป้องกัน ข้อมูลส่วนตัว การรบกวนการทำงานหรือการดำเนินธุรกรรม และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ (ชนินทร เฉลิมทรัพย์, นาวาอากาศเอก, 2561)

ความเสี่ยงของความมั่นคงปลอดภัยไซเบอร์อาจรวมถึงสิ่งต่าง ๆ ที่ทำให้ความเชื่อมั่นและความไว้วางใจของผู้มีส่วนได้เสีย (Stakeholder) ผลกระทบที่มีต่อการเก็บรักษาและการเติบโตของกลุ่มลูกค้าการละเมิดการป้องการข้อมูลส่วนตัวของลูกค้า การรบกวนการทำงานหรือการทำธุรกรรม ผลกระทบที่เป็นปฏิปักษ์และสุขภาพของผู้ปฏิบัติงาน และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ (สุธาเทพ รุณเรศ, 2561)

ปริญญา หอมเอนก, (2557) กล่าวว่า การรักษาความปลอดภัยไซเบอร์ ต้องมีการรักษาในปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสาร มีการพัฒนาและมีประยุกต์ใช้งานอย่างแพร่หลาย ข้อมูลสารสนเทศ การติดต่อสื่อสารและการใช้งานคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ต่าง ๆ เป็นสิ่งที่มีความสำคัญ จำเป็นที่จะต้องได้รับการป้องกันจากภัยไซเบอร์เพื่อให้ข้อมูลสารสนเทศและเครือข่ายต่าง ๆ มีความปลอดภัย สามารถทำงานได้อย่างมีเสถียรภาพ ปราศจากภัยคุกคาม และลดระดับความรุนแรงที่อาจเกิดขึ้นในการที่จะทำให้องค์กรสร้างความมั่นใจว่าการป้องกันและรักษาเป็นไปอย่างถูกต้องครบถ้วน ย่อมต้องมีมาตรฐานหรือแนวทางปฏิบัติที่มีประสิทธิภาพ ล่าสุดได้มีการกำหนดมาตรฐาน ISO/IEC 27001-2013 ซึ่งเกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศขึ้น โดยมีวัตถุประสงค์เพื่อบริหารจัดการกับความปลอดภัยไซเบอร์ ISO/IEC 27001-2013 เป็นมาตรฐานที่มุ่งเน้นด้านการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ เป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศที่หลายองค์กรยึดถือร่วมกัน มีการนำไปใช้อย่างแพร่หลายทั่วโลก และได้มีการปรับปรุงอย่างต่อเนื่อง มาตรฐานนี้มีความเกี่ยวข้องกับข้อมูลโดยตรงเนื่องจากการรักษาความปลอดภัยของข้อมูลซึ่งถือเป็นส่วนสำคัญส่วนหนึ่งขององค์กร มาตรฐานนี้เป็นมาตรฐานที่พัฒนามาจากมาตรฐานในตระกูล ISO/IEC 27000 โดยองค์กรมาตรฐาน International Organization for

Standardization (ISO) เป็นข้อกำหนดสำหรับการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) ระบบคุณภาพนี้กำหนดขึ้นเพื่อเป็นแนวทางในการจัดทำระบบบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศ ซึ่งเป็นมาตรฐานที่ยอมรับทั้งภาครัฐและเอกชนว่า เป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพ เป็นระบบที่อ้างอิงตัวแบบ PDCA (Plan, Do, Check, และ Act) ซึ่งเป็นโครงสร้างระบบบริหารที่เป็นสากลที่ใช้กันทั่วโลก สงครามไซเบอร์เป็นการปฏิบัติการในเครือข่ายที่สามารถทำลายข้อมูลหรือระบบคอมพิวเตอร์และอุปกรณ์อื่นที่อยู่บนเครือข่ายซึ่งการรบแบบนี้จะไม่มีการเผชิญหน้าแบบการรบในอดีต ทำให้เกิดความวิตกกังวล และความสับสนในการปฏิบัติงาน หากเกิดขึ้นกับทางทหาร จะมีความเสี่ยงสูงมากเพราะรูปแบบการเข้าโจมตีในสงครามไซเบอร์ก่อให้เกิดผลกระทบต่อศักยภาพในการปฏิบัติการรบ ระบบควบคุม การออกคำสั่ง หรือข้อมูลมีความผิดพลาด จึงต้องมีการเตรียมพร้อมเพื่อรับมือกับสงครามไซเบอร์ตลอดเวลา

จากการศึกษาการรักษาความปลอดภัยไซเบอร์สรุปได้ว่า การรักษาความปลอดภัยของข้อมูลซึ่งถือเป็นส่วนสำคัญส่วนหนึ่งขององค์กร มาตรฐานนี้เป็นมาตรฐานที่พัฒนามาจากมาตรฐานในตระกูล ISO/IEC 27000 โดยองค์กรมาตรฐาน International Organization for Standardization (ISO) เป็นข้อกำหนดสำหรับการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) ระบบคุณภาพนี้กำหนดขึ้นเพื่อเป็นแนวทางในการจัดทำระบบบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศ อินเทอร์เน็ตและสื่อออนไลน์ต่าง ๆ มีบทบาทต่อชีวิตประจำวันของเราเป็นอย่างมาก เพราะเป็นช่องทางสื่อสารและแลกเปลี่ยนข้อมูลกันได้รวดเร็วอีกทั้งยังสะดวกสบายต่อเรามาก รวมถึงธุรกิจห้างร้านที่ต้องใช้งานในการค้าขายใช้ธุรกรรมการเงินทางอินเทอร์เน็ต แต่ถ้าเราใช้อย่างไม่ระวังและยังไม่เห็นความสำคัญ ของการใช้งานอินเทอร์เน็ตที่ปลอดภัย ก็จะเกิดภัยคุกคามต่าง ๆได้เช่นโดนโจรกรรมข้อมูลส่วนตัวเพื่อขโมยเงินทางอินเทอร์เน็ตได้ หรือถูกหลอกหลวงเกี่ยวกับการค้า เป็นต้น

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน), (2563) ให้ข้อมูลไว้ว่า บัญชี Social บนโลกออนไลน์ เช่น Facebook Twitter Line Instagram ฯลฯ คือสิ่งที่เรียกว่าเป็นตัวตน Digital ของเรา เพราะโปรไฟล์บน Social media ต่าง ๆ จำเป็นต้องใช้ข้อมูลส่วนตัวเพื่อใช้ระบุตัวตนของผู้ใช้งาน อาจดูเหมือนเป็นข้อมูลทั่ว ๆ ไปจนทำให้ผู้ใช้งานไม่ได้ใส่ใจมากนักเกี่ยวกับด้านความปลอดภัย แต่นี่คือข้อมูลที่แฮกเกอร์ต้องการ หากผู้ใช้งานละเลยอาจทำให้เกิดช่องโหว่จนนำไปสู่การโจรกรรมข้อมูลได้ง่าย จากสถิติภัยคุกคามในประเทศจาก Thaicert พบว่าตั้งแต่ต้นปีที่ผ่านมาจนถึงสิ้นเดือนมิถุนายน มีภัยคุกคามที่เกิดขึ้นกว่า 1,400 ครั้งและมีแนวโน้มจะสูงขึ้นเรื่อย ๆ เมื่อแฮกเกอร์ขโมยข้อมูลประจำตัว Digital ไปแล้ว มีโอกาสที่แฮกเกอร์จะนำข้อมูลที่ได้นำไปใช้หาประโยชน์ทางด้านอื่นอีก เช่นนำไปก่อภัยไซเบอร์ที่เรียกว่า Social Engineer หรือเอาไปทำ Phishing เป็นต้นซึ่งหากข้อมูลถูกขโมยไปแล้ว กว่าจะแก้ไขได้คงต้องใช้เวลานาน และความเสียหายอาจเป็นจำนวนที่มากจนคิดไม่ถึง ดังนั้นควรระมัดระวัง การใช้งานในโลกไซเบอร์ ในเรื่องดังนี้ ชื่อผู้ใช้และรหัสผ่าน การเรียกดูกิจกรรม เช่น การไลน์ หรือการแชร์ ประวัติการค้นหาของคุณ วันเกิด เลขบัตรประชาชน ข้อมูลบนโปรไฟล์

โซเชียลมีเดีย เพจที่คุณติดตามหรือโต้ตอบ คำร้องออนไลน์ที่คุณเคยลงชื่อไว้ และประวัติทางการแพทย์ ซึ่งมีตัวอย่างการขโมยข้อมูลตัวตนดิจิทัล ดังนี้

1. การโดนขโมย Online Account ไม่ว่าจะเป็น Social Network Account ต่าง ๆ หรือ Online Shopping Account เมื่อแฮกเกอร์สามารถเข้าถึง Account ของเราได้แล้ว ไม่ว่าจะความผิดพลาดจากตัวเราเอง (ใช้ Password ง่ายไปหรือใช้ซ้ำกับเว็บอื่น) หรือว่าผิดพลาดจากผู้ให้บริการ ถ้าระบบไม่รัดกุมเพียงพอ (โดน Hacker โจมตีที่ระบบ) ข้อมูลทั้งหมดของเราจะหลุดออกไปทันที เรียกว่าขโมยความเป็นตัวตนไปได้เลย กรณีนี้สร้างความเสียหายอย่างรุนแรง เพราะ Hacker สามารถนำเอาไปทำอะไรก็ได้ และยังสามารถนำไปสร้างความเสียหายอื่น ๆ ได้อีก
2. นำเอาข้อมูลของเด็กไปใช้ การนำข้อมูลของเด็กโพสขึ้นโซเชียลนั้นนอกจากจะกระทบกับสิทธิความเป็นส่วนตัวของเด็กแล้ว ข้อมูลที่พ่อแม่ หรือผู้ปกครอง นำไปเผยแพร่ในโซเชียลมีเดีย อาจถูกนำเอาข้อมูลเหล่านั้นไปใช้ในทางที่ผิดได้เช่นเดียวกัน แฮกเกอร์สามารถนำไปสร้างโปรไฟล์ออนไลน์ หรืออาจนำไปทำสิ่งที่เลวร้ายบนโลกออนไลน์ก็ได้เช่นกัน
3. การขโมยเลขบัตรประชาชน เลขบัตรประชาชนอาจดูเป็นข้อมูลที่ดูทั่วๆ ไป แต่จริง ๆ แล้วในหลาย ๆ ครั้งถูกนำเป็นข้อมูลเพื่อใช้ยืนยันตัวตน ควบคู่กับวันเดือนปีเกิด เช่น หลายครั้งที่มีคนถ่ายรูปบัตรประชาชนลงโพสต์ลง Social Media แบบสาธารณะ นั่นอาจทำให้ผู้ไม่หวังดีก็สามารถนำข้อมูลไปยืนยันตัวตนแทนเราได้แล้ว
4. การปลอมแปลงบัญชีของเหยื่อ ที่พบบ่อยที่สุดคือการโจรกรรมข้อมูลส่วนตัวจากโปรไฟล์ดิจิทัลต่าง ๆ ของเหยื่อ คือการสร้างบัญชีใหม่โดยใช้ข้อมูลที่ขโมยมา เพื่อนำไปหลอกลวงผู้อื่นด้วยวิธีที่หลากหลายหรือนำไปเปิดบัญชีธนาคาร เป็นต้น

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน), (2563) ให้ข้อมูลวิธีการปกป้องตัวตน Digital บนโลกออนไลน์ทำได้ ดังนี้

1. ตั้งรหัสผ่านที่เดายาก ไม่ใช้ซ้ำ และหมั่นเปลี่ยนอยู่เสมอ วิธีง่าย ๆ ที่เราสามารถทำได้คือการตั้งรหัสผ่านที่คาดเดายากและหลากหลาย มีความยาวอย่างน้อย 12-14 ตัวอักษร ประกอบไปด้วย ตัวอักษรใหญ่ ตัวอักษรเล็ก ตัวเลข และไม่ควรใช้ซ้ำกับ Online Account อื่น ๆ รวมถึงคอยตรวจสอบคำขอรีเซ็ตรหัสผ่านในบัญชีด้วย และที่สำคัญควรเปลี่ยนรหัสผ่านเป็นประจำทุก 3- 6 เดือน เพื่อป้องกันกรณีที่มีการรั่วไหลของข้อมูลโดยที่เราไม่รู้ตัว
2. หมั่น Update ระบบปฏิบัติการบนอุปกรณ์ หมั่นตรวจสอบการ Update ระบบปฏิบัติการและการตั้งค่าเบราว์เซอร์อุปกรณ์ต่างให้ทันสมัยอยู่เสมอ เช่น โทรศัพท์มือถือ คอมพิวเตอร์ แล็ปท็อป ฯลฯ เพราะ Patch ทุกเวอร์ชั่น ย่อมมีช่องโหว่ที่แฮกเกอร์สามารถเข้ามายังระบบได้ แต่เมื่อเราหมั่น Update Patch ก็จะช่วยปิดช่องโหว่นั้น ๆ และ เพิ่มฟีเจอร์ใหม่ ๆ ที่ช่วยให้มีความปลอดภัยระบบมากขึ้นหรือหากระบบปฏิบัติการผิดพลาดจนไม่สามารถใช้งานได้ เราจะได้แก้ไขอย่างทันท่วงที

3. หลีกเลี่ยงการใช้ Wi-Fi สาธารณะ พยายามหลีกเลี่ยงการใช้ Wi-Fi สาธารณะ ทางที่ดีควรใช้อินเทอร์เน็ตเครือข่ายมือถือของตัวเองเพราะเราไม่สามารถรู้ได้ว่า เครือข่าย Wi-Fi สาธารณะปลอดภัยจริงหรือไม่ เป็น Wi-Fi ปลอมที่แฮกเกอร์สร้างเพื่อดักจับข้อมูลเหยื่อหรือเปล่า หากไม่มีทางเลือกควรใช้ VPN (Virtual Private Networks) ด้วย เพื่อให้แน่ใจว่ากิจกรรมออนไลน์ทั้งหมดจะปลอดภัยตั้งแต่ ธนาคารออนไลน์ไปจนถึงข้อความส่วนตัว
4. อย่าแชร์ทุกอย่างที่คิด ก่อนแชร์ให้คิดก่อนเสมอ ในโลก Social media มีอันตรายแอบแฝงอยู่แล้ว ยิ่งถ้าเราใช้งานโดยการแชร์ทุกอย่างที่เกี่ยวข้องกับเราลงบนโลกออนไลน์ เช่น แชร์ข้อมูลส่วนตัวทั้งหมดแบบสาธารณะ แชร์ Location ที่อยู่อาศัยของตัวเอง ฯลฯ อาจเป็นการแบ่งปันข้อมูลให้กับแฮกเกอร์ หรือ คนแปลกหน้าก็ได้ ทางทีดีควรคิดก่อนแชร์เสมอ เพื่อความปลอดภัยของตัวเอง
5. จดบันทึกประวัติการใช้งานทางการเงิน จดบันทึกการใช้งานเครดิตอยู่เสมอว่าเราได้ใช้ทำอะไร ที่ไหน เวลาเท่าไหร่ และจดบันทึกการเปลี่ยนแปลงแม้จะเล็ก ๆ น้อย ๆ เพื่อป้องกันยอดเงินแปลก ๆ ที่หักเงินในบัตรเครดิตเราแบบที่ไม่รู้ตัวและที่สำคัญไม่ควรผูกเลขบัตรเครดิต เลขบัญชีธนาคารลงในเว็บไซต์ช้อปปิ้งออนไลน์ หรือ เว็บไซต์ Social ต่าง ๆ เพราะหากโดนแฮกบัญชี สิ่งพวกนี้คือเป้าหมายแรกของแฮกเกอร์ในการขโมยข้อมูล
6. ตรวจสอบประวัติการใช้งานอินเทอร์เน็ตเสมอ ตรวจสอบการใช้ซอฟต์แวร์เพื่อป้องกันการติดตามต่าง ๆ และป้องกันข้อมูลส่วนบุคคลบนโลก Social (ข้อมูลส่วนตัวที่คุณโชว์ไว้บน Profile Digital ต่าง ๆ) ของเราเพื่อรักษาตัวเองให้ปลอดภัยจากการติดตามออนไลน์ที่ถูกคุกคามโดยโฆษณาออนไลน์ต่าง ๆ ที่ไม่เหมาะสม
7. ใช้ระบบรักษาความปลอดภัยในทุกอุปกรณ์ที่เชื่อมต่อออนไลน์ ถ้าคอมพิวเตอร์หรืออุปกรณ์ชิ้นนั้น สามารถออกสู่โลกอินเทอร์เน็ตได้ ต้องป้องกันมันด้วย เช่น ถ้าเป็น PC หรือ มือถือ ก็จะต้องมี Antivirus เพื่อป้องกันการโดนไวรัส หรือว่าถ้าในอนาคตตู้เย็นส่งข้อมูลออกสู่โลกอินเทอร์เน็ตได้ ก็ควรจะต้องป้องกันมันด้วย เพราะทุกการเชื่อมต่อมีภัยแฝงเสมอ การเลือกระบบรักษาความปลอดภัยจึงเป็นเรื่องสำคัญ

จากการศึกษาแนวคิดเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ สรุปได้ว่า ความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งที่สำคัญต่อองค์กรต่าง ๆ ในด้านข้อมูล ดังนั้นควรให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ ดังนั้นเราสามารถปรับพฤติกรรมการใช้ไซเบอร์ การเข้าใช้อินเทอร์เน็ต การใช้งานสื่อสังคม การเข้าถึงสื่อออนไลน์ การใช้งานผ่านโปรแกรม การป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต อย่างปลอดภัยได้เพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์

จากการศึกษา ผู้วิจัยได้สังเคราะห์สรุปจากแนวคิดของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน), (2563) มากำหนดเป็นตัวแปรในการศึกษาครั้งนี้ เพื่อนำมาประกอบใช้ในการสร้างแบบสอบถาม เรื่องการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรใน

บริษัทวิทยุการบินแห่งประเทศไทย จำกัด ในส่วนที่ 2 พฤติกรรมการใช้งานระบบอินเทอร์เน็ต ได้แก่ ด้านพฤติกรรมการใช้อินเทอร์เน็ต ด้านพฤติกรรมการใช้งานสื่อสังคม ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์ ด้านพฤติกรรมการใช้งานผ่านโปรแกรม และ ด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต ซึ่งมีรายละเอียดดังนี้

1. ด้านพฤติกรรมการใช้อินเทอร์เน็ต ได้แก่ การใช้อีเมลตนเองในการสมัครบัญชีออนไลน์ การตั้งค่าบัญชีให้เป็นส่วนตัว การกรอกข้อมูลส่วนตัวตามอีเมลที่ส่งมา ดาวน์โหลดไฟล์โดยไม่ทราบแหล่งที่มาออนไลน์
2. ด้านพฤติกรรมการใช้งานสื่อสังคม ได้แก่ การเผยแพร่ข้อความ รูปภาพ วีดิทัศน์ ลงในสื่อสาธารณะ การอนุญาตให้บุคคลที่ไม่รู้จักเข้าถึงการใช้งานบน Social และไม่จำกัดการเข้าถึงข้อมูลส่วนตัวใจบัญชี Social Media
3. ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์ ได้แก่ การเข้าถึงสื่อออนไลน์ที่ไม่รู้จักมาก่อน การเข้าถึงสื่อที่มีโฆษณาเชิญชวนไปยังเว็บไซต์อื่น และการเข้าถึงสื่อออนไลน์ที่ไม่ได้รับการคัดกรอง
4. ด้านพฤติกรรมการใช้งานผ่านโปรแกรม ได้แก่ การใช้งานผ่านโปรแกรมที่ไม่มีลิขสิทธิ์ การโหลดโปรแกรมที่ไม่มีลิขสิทธิ์จากแหล่งต่าง ๆ การติดตั้งโปรแกรมต่าง ๆ จากบุคคลอื่น การติดตั้งโปรแกรมโดยไม่ศึกษารายละเอียด
5. ด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต ได้แก่ มีโปรแกรมป้องกัน Spyware การเปิดการใช้งานโปรแกรม Firewall มีการสำรอง (back up) ข้อมูลเป็นประจำ รวมทั้งมีโปรแกรมสำหรับลบไฟล์แบบถาวร (Files Shredder)

2.3 แนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์ (Cyber Threats)

2.3.1 ประเภทของภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ (Cyber threats) ถือเป็นภัยคุกคามสำคัญที่ส่งผลกระทบอย่างรุนแรงต่อผลประโยชน์ทางเศรษฐกิจ และความมั่นคงของประเทศ โดยมีลักษณะเป็นการโจมตีหลากหลายรูปแบบ อาทิการเจาะระบบคอมพิวเตอร์ (hacking) การสอดแนมข้อมูลคอมพิวเตอร์โดยสปายแวร์ การดักรับข้อมูลคอมพิวเตอร์ (sniffing) การโจมตีโดยชุดค าสั่งไม่พึงประสงค์ (Malicious Software : Malware) หรือการรุมสอบถามข้อมูลจนระบบล่ม (Denial of Service Attack : DOS) ซึ่งการโจมตีแต่ละครั้งล้วนสร้างความเสียหายอย่างมหาศาลทั้งต่อความมั่นคง ความปลอดภัยของระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ ตลอดจนระบบเศรษฐกิจและความมั่นคงของประเทศ (สุปรีดี ประวิตร, พลโท หม่อมหลวง, 2561)

ณรงค์เวตย์ เรืองจวง, นาวาอากาศเอก, (2560) ได้แบ่งประเภทของภัยคุกคามจากไซเบอร์สามารถจำแนกออกเป็น 2 กลุ่ม ได้แก่ การจำแนกตามประเภทของภัยคุกคาม และการจำแนกตามลักษณะ/ผลของภัยคุกคาม แต่ละกลุ่มมีรายละเอียดดังนี้

1. การจำแนกภัยคุกคามตามประเภทหน่วยงาน The European Computer Security Incident Response Team (eCSIRT) ซึ่งเป็นเครือข่ายความร่วมมือของ

หน่วยงาน CSIRT ในสหภาพยุโรปได้จำแนกตามประเภทของภัยคุกคามออกเป็น 10 ประเภท ประกอบด้วย

1.1 บอตเน็ต (Botnet)
1.2 สแปม (Spam)
1.3 โอเพ่นดีเอ็นเอสรีโซลเวอร์ (Open DNS Resolver)
1.4 บรูตฟอร์ซ (Brute Force)
1.5 มัลแวร์ยูอาร์แอล (Malware URL)
1.6 สแกนนิ่ง (Scanning)
1.7 โอเพ่นพร็อกซี่เซิร์ฟเวอร์ (Open Proxy Server)
1.8 ฟิชชิ่ง (Phishing)
1.9 สตอร์มเวิร์ม (Storm Worm)
1.10 ดีดอส (DDoS)

2. การจำแนกภัยคุกคามตามลักษณะ/ผลของภัยคุกคาม จากบทความเรื่องความเป็นมาของไทยเซิร์ตจากกระทรวงวิทย์สู่กระทรวง ICT ได้แสดงรายละเอียดของภัยคุกคามจำแนกตาม ลักษณะ/ผลของภัยคุกคามจำนวน 9 ด้าน ประกอบด้วย

2.1 เนื้อหาที่เป็นภัยคุกคาม (Abusive Content)
2.2 การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability)
2.3 การฉ้อฉล ฉ้อโกง หรือหลอกลวง เพื่อผลประโยชน์ (Fraud)
2.4 ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)
2.5 ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts)
2.6 การเจาะระบบได้สำเร็จ (Intrusions)
2.7 โค้ดมุ่งร้าย (Malicious code or malware)
2.8 การเข้าถึง/เปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต (Information Security)
2.9 ภัยคุกคามอื่นๆ (Other)

2.3.2 ประเภทของการเกิดภัยคุกคามทางไซเบอร์

ประเภทของการเกิดภัยคุกคามทางไซเบอร์ แบ่งออกเป็น 4 ประเภท (สุธาเทพ รุณเรศ, 2561) ดังนี้

1. ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ (Application-Based Threats) ที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนคอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ อาจจะถูกแอบแฝงมาด้วยโปรแกรมที่เป็นภัยคุกคามที่เรียกว่า มัลแวร์ (Malware) นอกจากนี้โปรแกรมที่ติดมัลแวร์ยังส่งข้อความที่ไม่พึงประสงค์ออกไปยังผู้อื่น หรือขโมยข้อมูลสำคัญออกไป ตัวอย่างโปรแกรมในกลุ่มนี้ได้แก่ Virus, Worm, Trojan, Botnet หรือ Spyware เป็นต้น

2. ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ (Web-Based Threats) เป็นภัยคุกคามที่เกิดจากการที่ผู้ใช้คอมพิวเตอร์หรืออุปกรณ์พกพาเปิดเว็บไซต์ขึ้นมาใช้งาน ซึ่งเว็บไซต์ที่เรียกมาใช้อาจเป็นเว็บไซต์ฟิชชิ่ง (Phishing) ซึ่งถูกออกแบบให้มีลักษณะคล้ายคลึงกับเว็บไซต์จริงเพื่อหลอกให้ผู้ใช้กรอกข้อมูลเข้าสู่ระบบของผู้ไม่หวังดี
3. ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย ปัจจุบันมีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก มีทั้งที่น่าเชื่อถือและที่ไม่น่าเชื่อถือ รวมถึงผู้ที่แอบแฝงเพื่อวัตถุประสงค์อื่น ดังนั้น ผู้ใช้คอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่าง ๆ อาจได้รับผลกระทบโดยตรง
4. ภัยคุกคามที่เกิดจากการถูกโจมตีแบบเจาะจงเป้าหมาย (Targeted Attack) ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตี หรือแฮกเกอร์ (Hackers) ในประเทศต่าง ๆ จะใช้การโจมตีแบบเจาะจงเป้าหมายอย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐานวิกฤติ สถาบันการเงิน และองค์กรอื่น ๆ ของภาครัฐ และภาคเอกชนในหลายประเทศ อาชญากรไซเบอร์เหล่านี้จะใช้มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามประเภทนี้จัดว่าเป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

2.3.3 ประเภทของผู้คุกคามทางไซเบอร์

ผู้คุกคามทางไซเบอร์หรือกลุ่มบุคคลและ/หรือองค์กรที่มีความชำนาญในการปฏิบัติการภัยไซเบอร์สามารถแบ่งออกเป็น 5 ประเภท (นงรัตน์ สายเพชร, 2556) ดังนี้

1. ประเทศที่มีความประสงค์ร้าย

กลุ่มนี้ได้แก่ รัฐบาลของบางประเทศที่มุ่งโจมตีกลุ่มงานความมั่นคงหรือกองทัพ โดยมีจุดมุ่งหมายที่จะสร้างความเสียหายให้เกิดขึ้น กับประเทศเป้าหมาย ซึ่งอาจเป็นการก่อกวนเว็บไซต์ของหน่วยงานต่าง ๆ การจารกรรมข้อมูลสำคัญ รวมถึงการสร้างความเสียหายให้กับโครงสร้างพื้นฐานของประเทศเป้าหมาย

2. ผู้ก่อการร้าย

กลุ่มนี้ได้แก่ ผู้ก่อการร้ายหรือผู้ไม่หวังดีซึ่งมีจุดประสงค์ที่จะทำลายผลประโยชน์ของชาติเป้าหมาย กลุ่มผู้ก่อการร้ายเหล่านี้ใช้ไซเบอร์เป็นช่องทางการสื่อสาร โดยจะสร้างแบบแผนเพื่อหาเงินทุน หรือเพื่อเผยแพร่แนวความคิดที่เป็นภัยต่อประเทศเป้าหมาย

3. สายลับภาคเอกชน/องค์กรอาชญากรรม

กลุ่มนี้ได้แก่ สายลับภาคเอกชน หรือองค์กรอาชญากรรมซึ่งมีการใช้ไซเบอร์เป็นช่องทางในการบุกรุก และโจมตีระบบ โดยมีเป้าหมายเพื่อจารกรรมข้อมูลสำคัญ รวมถึงทรัพย์สินจากองค์กรภาครัฐ และภาคเอกชนต่าง ๆ กลุ่มนี้อาจเป็นกลุ่มปฏิบัติการของหน่วยงานความมั่นคงของบางประเทศ หรืออาจเป็นเพียงอาชญากรที่ต้องการนำข้อมูลสำคัญไปหารายได้

4. แฮกเกอร์

กลุ่มแฮกเกอร์ (hackers) คือ กลุ่มผู้ที่พยายามหาช่องโหว่ของระบบ ลักลอบเจาะเข้าสู่ระบบเพื่ออ่านข้อมูลข่าวสาร เพื่อขโมย หรือเพื่อทำลายข้อมูลข่าวสารสำคัญเหล่านั้น ซึ่งจะทำให้เกิดความ

เสียหายแก่องค์กรเป้าหมาย แฮกเกอร์สามารถมาได้จากประเทศต่าง ๆ ทั่วโลก การป้องกัน หรือ การสืบหาตัวผู้กระทำความผิดค่อนข้างทำได้ยาก

5. แฮกทิวิส

กลุ่มแฮกทิวิส (hacktivists) คือ กลุ่มแฮกเกอร์ที่มีแรงจูงใจทางการเมือง เป็นกลุ่มที่ต้องการผลักดันให้เกิดความเปลี่ยนแปลงทางการเมือง กลุ่มนี้มุ่งเน้นที่จะนำเสนอแนวคิดผ่านทางไซเบอร์และสร้างมูลเหตุที่ส่งผลต่อการเมืองและสังคมมากกว่าการสร้างความเสียหายให้กับโครงสร้างพื้นฐาน

2.4 แนวคิดเกี่ยวกับการกลั่นแกล้งทางไซเบอร์ (Cyber Bullying)

2.4.1 ความหมายของการกลั่นแกล้งทางไซเบอร์

Payne, (2007) กล่าวว่า การกลั่นแกล้งทางไซเบอร์ หมายถึง การรังแกและคุกคามผ่านอุปกรณ์ทางอิเล็กทรอนิกส์ เช่น อีเมล์ โทรศัพท์มือถือ ข้อความโต้ตอบแบบทันที(IM) ข้อความสั้น (SMS)บล็อก และเว็บไซต์ซึ่งทำให้เกิดอาชญากรรมคอมพิวเตอร์ได้ การกลั่นแกล้งทางไซเบอร์เป็นการกระทำโดยเจตนาและนำไปสู่ความตึงเครียดทางอารมณ์ทำให้เกิดความทุกข์อย่างช้า ๆ จากข้อความอิเล็กทรอนิกส์หนึ่งข้อความการกลั่นแกล้งทางไซเบอร์อาจรวมถึงการคุกคามและกล่าวถึงเรื่องทางเพศ การใช้คำพูดที่รุนแรง การดูถูกดูแคลน รวมทั้งการส่งอีเมล ไปรบกวนผู้อื่นที่ไม่ต้องการติดต่อกับผู้ส่งด้วย

Smith, (2008) กล่าวว่า การกลั่นแกล้งทางไซเบอร์ หมายถึง พฤติกรรมความก้าวร้าวของบุคคลหรือกลุ่มบุคคลที่เจตนาใช้เครื่องมืออิเล็กทรอนิกส์ทำร้ายเหยื่อ ซึ่งยากที่จะป้องกันตนเองโดยกระทำอย่างซ้ำ ๆ ซึ่งอิเล็กทรอนิกส์นั้นเพิ่งเกิดขึ้น โดยเกิดขึ้นอย่างมาก โดยเฉพาะทางโทรศัพท์มือถือและอินเทอร์เน็ต

จากการศึกษาความหมายของการกลั่นแกล้งทางไซเบอร์สรุปได้ว่า การกลั่นแกล้งทางไซเบอร์เป็นพฤติกรรมความก้าวร้าวของบุคคลหรือกลุ่มบุคคลที่เจตนาใช้เครื่องมืออิเล็กทรอนิกส์เช่น อีเมล์ โทรศัพท์มือถือ ข้อความโต้ตอบแบบทันที (IM) ข้อความสั้น (SMS) บล็อกและเว็บไซต์ซึ่งทำให้เกิดอาชญากรรมคอมพิวเตอร์ได้ การกลั่นแกล้งทางไซเบอร์เป็นการกระทำโดยเจตนาและนำไปสู่ความตึงเครียดทางอารมณ์ทำให้เกิดความทุกข์อย่างช้า ๆ

2.4.2 ลักษณะของการกลั่นแกล้งทางไซเบอร์

สุธาเทพ รุณเรศ, (2561). การกลั่นแกล้งโดยทั่วไปหลายแบบที่มีความแตกต่างกันออกไป เช่น การพูดจาหมิ่นประมาท การทำร้ายร่างกาย ซึ่งต่างจากการกลั่นแกล้งทางโลกไซเบอร์อย่างมาก โดยการกลั่นแกล้งทางไซเบอร์มีลักษณะดังนี้

1. การข่มขู่ใส่ร้าย (Harassment) เป็นการกลั่นแกล้งโดยการส่งข้อความโจมตีในทางเสียหายด้วยความคึกคะนองไปยังบุคคลอื่นหรือกลุ่มคนทำซ้ำเป็นประจำหลาย ๆ ครั้ง ทั้งนี้การพูดคุยในโลกไซเบอร์ (Cyberstalking) เป็นอีกรูปแบบหนึ่งของการข่มขู่ที่ใช้ข่มขู่และหยาบคาย และนำไปสู่การทำร้ายร่างกายในโลกแห่งความเป็นจริง

2. การยั่วโมโห (Flaming) มีความคล้ายคลึงกับการข่มขู่ใส่ร้าย แต่จะมีการโต้ตอบกันทางอีเมล ข้อความโต้ตอบ หรือห้องแชท เป็นการกลั่นแกล้งประเภทหนึ่งที่เผยแพร่สู่สาธารณะโดนบ่อยครั้ง มีการใช้ภาษาหรือภาพที่ส่อถึงบุคคลคนใดคนหนึ่งเป็นพิเศษ
3. การกีดกัน (Exclusion) การกีดกันเป็นการกระทำที่แยกบุคคลหนึ่งจากกลุ่มที่ออนไลน์ เช่น การสนทนาโดยส่งข้อความทันทีการแชท ทั้งนี้ในกลุ่มจะมีการวิพากษวิจารณ์ในแง่ร้ายและข่มขู่จนกว่าบุคคลนั้นจะถอนตัวออกไป
4. การเผยแพร่ออกนอกกลุ่ม (Outing) การเผยแพร่ออกนอกกลุ่ม คือ การกลั่นแกล้งโดยแบ่งการเอาข้อมูลภาพ คลิปวิดีโอส่วนบุคคลหรือข้อมูลส่วนตัวของบุคคลหนึ่งไปเผยแพร่สู่สาธารณะ โดยบุคคลที่เป็นคนที่ออกจากกลุ่มไปแล้ว ผู้ที่ออกนอกกกลุ่มไปแล้ว (Outed) จะรู้ว่าข้อมูลของเขาถูกนำเผยแพร่จะรู้ตัวหลังจากกระจายทั่วอินเทอร์เน็ตแล้ว
5. การแอบอ้าง (Masquerading) การแอบอ้างเสแสร้งเป็นสถานการณ์ เป็นการกลั่นแกล้งโดยการสร้างเรื่องตลกตลกที่มาจากลักษณะเฉพาะตัวที่เกี่ยวข้องกับบุคคลที่ถูกข่มขู่ โดยปิดบังชื่อนอกจากจะสร้างเรื่องตลก ยังมีการกลั่นแกล้งโดยปลอมเป็นบุคคลอื่น เพื่อประสงค์ร้ายต่อเหยื่อ

จากการศึกษาลักษณะของการกลั่นแกล้งทางไซเบอร์ สรุปได้ว่า การกลั่นแกล้งทางไซเบอร์มีลักษณะเป็นการแอบอ้าง การข่มขู่ใส่ร้าย การยั่วโมโห การกีดกัน (Exclusion) การกีดกันเป็นการกระทำที่แยกบุคคลหนึ่งจากกลุ่มที่ออนไลน์ เช่น การสนทนาโดยส่งข้อความทันทีการแชท ทั้งนี้ในกลุ่มจะมีการวิพากษวิจารณ์ในแง่ร้ายและข่มขู่จนกว่าบุคคลนั้นจะถอนตัวออกไป การเผยแพร่ออกนอกกลุ่ม (Outing) การเผยแพร่ออกนอกกลุ่ม คือ การกลั่นแกล้งโดยแบ่งการเอาข้อมูลภาพ คลิปวิดีโอส่วนบุคคลหรือข้อมูลส่วนตัวของบุคคลหนึ่งไปเผยแพร่สู่สาธารณะ และยังมีการกลั่นแกล้งโดยปลอมเป็นบุคคลอื่น เพื่อประสงค์ร้ายต่อเหยื่อ ซึ่งถือได้ว่าเป็นภัยคุกคามทางไซเบอร์

2.5 แนวคิดเกี่ยวกับความตระหนักรู้ (Awareness)

2.5.1 ความหมายของความตระหนักรู้

พจนานุกรมราชบัณฑิตสถาน พ.ศ. 2560 ได้ให้ความหมาย “ความตระหนักรู้ว่าเป็นการรู้ประจักษ์ชัด รู้ชัดแจ้ง” โดยสอดคล้องกับพจนานุกรม ของ Good, (1973) โดยได้ให้ความหมายว่า “การแสดงออกจากการระลึกได้หรือจดจำได้” นอกจากนี้ยังมีผู้นิยามไว้อีก ดังนี้

Bloom, (1971 p. 271 อ้างถึงใน สุพัตรา ถนอมวงค์, 2551, น.10) ได้ให้นิยามว่า “ความตระหนักรู้ คือ ภาคต่ำสุดทางภาคอารมณ์ซึ่งความตระหนักรู้นั้นคล้ายกับอารมณ์ความรู้สึก (Affective Domain) แต่ความตระหนักรู้ต่างกับความรู้สึกตรงที่ความตระหนักรู้ไม่จำเป็นต้องเน้นปรากฏการณ์หรือสิ่งหนึ่งสิ่งใด แต่ความตระหนักรู้จะเกิดขึ้นเมื่อมีสิ่งเร้าให้เกิดความตระหนักรู้”

กุลวดี ราชภักดี, (2545) ได้ให้นิยามว่า “ความตระหนักรู้ หมายถึง การที่บุคคลเกิดความรู้สึก นึกคิด ความคิดเห็นหรือประสบการณ์แล้วเกิดความเข้าใจแล้วประเมินสถานการณ์ที่เกี่ยวกับตนเองได้จากสภาวะจิตที่ยอมรับและเกิดแสดงพฤติกรรมตอบสนองต่อเหตุการณ์”

อนุสรณ์ กาลดิษฐ์, (2548) ได้ให้นิยามว่า “ความตระหนักรู้ หมายถึง ความสำนึกของแต่ละบุคคลเคยมีการรับรู้หรือเคยมีความรู้มาก่อน มีสิ่งเร้ามากระตุ้นจนเกิดความตระหนักรู้จากการประเมินค่า”

ประพล มิลินทจินดา, (2542) ได้ให้นิยามว่า “ความตระหนักรู้ คือ การแสดงความรู้สึก นึกคิด ความคิดเห็น ที่บุคคลเข้าใจและประเมินสถานการณ์ที่เกิดขึ้นเกี่ยวกับตนเองจากประสบการณ์จากช่วงระยะเวลา จากเหตุการณ์ และจากสภาพแวดล้อม เป็นปัจจัยทำให้มนุษย์มีความตระหนักรู้”

วีระชน ขาวผ่อง, (2551) กล่าวว่า ความตระหนักรู้เป็นสถานการณ์มีผลให้เกิดความรู้สึกการรับรู้มุ่งสู่สภาวะจิตแห่งตน คือ ทัศนคติ ความคิด ความเชื่อ ความสนใจ และอารมณ์ อันจะก่อให้เกิดความตระหนักรู้ และจิตสำนึก

ปรีดิ์ณัฐ ภาณุมนต์วาที, (2552) กล่าวว่า ความตระหนักรู้สภาวะของจิตใจที่เกี่ยวข้องกับความรู้สึก (Feeling) ความคิด (Idea) และความปรารถนาที่บุคคลมีต่อสิ่งหนึ่งสิ่งใด หรือปรากฏการณ์ใดปรากฏการณ์หนึ่ง ด้วยการพูด การเขียน หรือวิธีการอื่น โดยอาศัยระยะเวลาหรือประสบการณ์หรือสภาพแวดล้อมในชุมชน หรือสิ่งเร้าภายนอก เป็นปัจจัยที่ทำให้บุคคลมีความตระหนักรู้ขึ้น หรือความตระหนักรู้ก็คือ ความสำนึกต่อสิ่งใดสิ่งหนึ่งนั่นเอง

ปารวีร์ บุษบาศรี, (2555) ให้ความหมายไว้ว่า ความตระหนักรู้ หมายถึง การมีความสำนึกในบางสิ่งบางอย่างหรือเป็นการแสดงออกให้เห็นถึงการรับรู้และพิจารณาใคร่ครวญเหตุการณ์ ประสบการณ์ วัตถุหรือเหตุการณ์ที่ดาเนินไปบางอย่าง การใช้ความคิดจดจ่อเตือนตนเองได้ไม่ว่าจะอยู่ในสถานการณ์ใด

พงษ์ชัย เฉลิมกลิ่น, (2551) กล่าวว่า ความตระหนักรู้ เป็นพฤติกรรมที่แสดงถึงความรับผิดชอบหรือเหตุการณ์ใดเหตุการณ์หนึ่ง เป็นอารมณ์ความรู้สึกด้านทัศนคติค่านิยม ความชอบหรือไม่ชอบ ดีหรือไม่ดี ที่ได้จากการประเมินสิ่งเร้าต่าง ๆ ของบุคคลนั้น

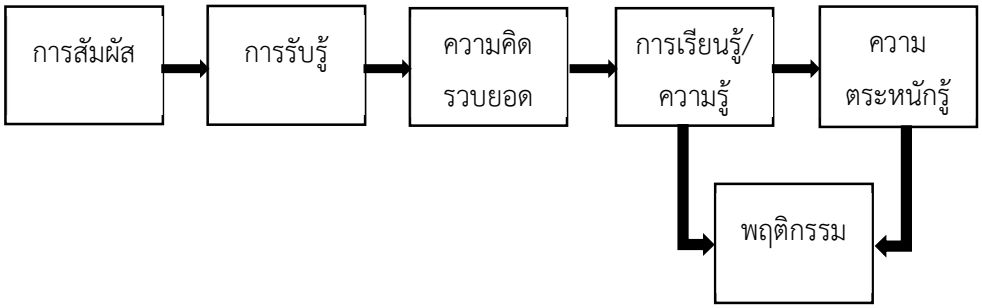
สกาวฟ้า จันทภาโส และคณะ, (2563) ได้สรุปประเด็นความตระหนักรู้จากการทบทวนวรรณกรรมที่เกี่ยวข้องกับงานวิจัยเรื่องการพัฒนาแอปพลิเคชัน เพื่อสร้างความตระหนักรู้ เรื่องการระรานทางไซเบอร์สำหรับนักเรียนชั้นมัธยมศึกษาปี ที่ 1 ไว้ว่า ความตระหนักรู้ หมายถึง ความสำนึกซึ่งบุคคลเคยมีการรับรู้ หรือเคยมีความรู้มาก่อน โดยเมื่อมีสิ่งเร้ามากระตุ้นจะทำให้เกิดความสำนึกขึ้นหรือเกิดความตระหนักรู้ขึ้น ความตระหนักรู้จึงเป็นภาวะทางจิตใจที่เกี่ยวข้องกับความรู้สึก ความคิดและความปรารถนาต่าง ๆ อันเกิดจากการรับรู้และความสำนึก ซึ่งเป็นภาวะที่บุคคลได้รับรู้ หรือได้รับประสบการณ์ต่าง ๆ มาแล้วโดยมีการประเมินค่าและตระหนักรู้ถึงความสำคัญของตนเองที่มีต่อสิ่งนั้น ๆ ความตระหนักรู้จึงเป็นการตื่นตัวทางจิตใจต่อเหตุการณ์ หรือสถานการณ์นั้น ๆ ซึ่งหมายความว่าระยะเวลาหรือประสบการณ์และสภาพแวดล้อมจะทำให้เกิดการรับรู้ (Perception) ขึ้น และนำไปสู่การเกิดความคิดรวบยอด การเรียนรู้และ ความตระหนักรู้ ตามลำดับ ซึ่งขั้นตอนและกระบวนการเกิดความตระหนักรู้เป็นผลมาจากกระบวนการทางปัญญา (Cognitive Process) กล่าวคือ เมื่อบุคคลได้รับการกระตุ้นจากสิ่งเร้าหรือได้รับการสัมผัสจากสิ่งเร้าแล้วจะเกิดการรับรู้และเมื่อรับรู้ในขั้นต่อ ๆ ไป ก็จะเข้าใจในสิ่งเร้านั้น คือ เกิดความคิดรวบยอดและนำไปสู่การเรียนรู้คือ มีความรู้ในสิ่งนั้นและนำไปสู่การเกิดความตระหนักรู้ในที่สุด ซึ่งความรู้และความตระหนักรู้ต่างก็นำไปสู่การกระทำหรือการแสดงพฤติกรรมของบุคคลต่อสิ่งเร้านั้น ๆ การที่บุคคลจะเกิดความตระหนักรู้ขึ้นได้นั้น บุคคลนั้น

จะต้องมีความรู้มาก่อน ดังนั้นการจัดการเรียนรู้เพื่อให้ผู้เรียนมองเห็นความสำคัญ ความรับผิดชอบและผลกระทบที่จะเกิดขึ้นตามมา จะส่งผลให้ผู้เรียนเกิดความตระหนักรู้ต่อสิ่งนั้น ๆ ต่อไปในที่สุด

2.5.2 ปัจจัยที่ทำให้เกิดความตระหนักรู้

กระบวนการเกิดความตระหนักรู้มาจากกระบวนการทางปัญญา (Cognitive process) ทั้งนี้เมื่อบุคคลได้รับการกระตุ้นจากสิ่งเร้าหรือรับสัมผัสจากสิ่งเร้าหรือประสบการณ์แล้วจะเกิดการรับรู้ จากนั้นจะเข้าใจในสิ่งเร้านั้น และเกิดเป็นความคิดรวบยอด และทำให้มีความรู้ (Knowledge) และเมื่อมีความรู้ในสิ่งนั้นก็จะนำไปสู่การเกิดความตระหนักรู้ ทั้งนี้ความรู้และความตระหนักรู้นี้ต่างก็จะนำไปสู่การกระทำ (Action) หรือการแสดงพฤติกรรมของบุคคลต่อสิ่งเร้านั้น ๆ

พจนานุกรม ของ Good, (1973) ได้ประมวลขั้นตอนของกระบวนการเกิดความตระหนักรู้ ดังภาพประกอบที่ 2.4 นี้ (Good, 1973 อ้างถึงใน สุธาสินี อินทร์ผูก, 2548)



ภาพประกอบที่ 2.4 ขั้นตอนของกระบวนการเกิดความตระหนักรู้

จากการศึกษาความหมายของการตระหนักรู้ สรุปได้ว่า ความตระหนักรู้ (Awareness) คือ การรับรู้แบบฉุกคิดขึ้นมาต่อสถานการณ์ใดสถานการณ์หนึ่ง หรือเหตุการณ์ใดเหตุการณ์หนึ่งซึ่งเป็นอารมณ์ความรู้สึกโดยอาศัยองค์ประกอบจากสิ่งแวดล้อม ประสบการณ์ และสิ่งที่ส่งผลต่ออารมณ์และความรู้สึก

2.5.3 การสร้างการตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

QuickServ, (2020). การสร้างการตระหนักรู้ด้านความมั่นคงปลอดภัยในการใช้ทรัพยากรสารสนเทศภายในองค์กร ช่วยให้องค์กรมีความพร้อมและสามารถปรับตัวให้เข้ากับการเปลี่ยนแปลง ทั้งยังลดโอกาสที่จะถูกโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ ได้มากขึ้น เนื่องด้วยสถานการณ์ด้านความปลอดภัยที่เปลี่ยนแปลงไปอย่างรวดเร็ว อาจเป็นเรื่องยากที่จะก้าวให้ทันกับข่าวของภัยคุกคามที่เกิดขึ้นล่าสุดสำหรับผู้ที่อยู่แนวหน้าซึ่งเกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร และมันก็ยังเป็นเรื่องที่ยากยิ่งกว่า สำหรับพนักงานที่ไม่ได้มีส่วนร่วมโดยตรงในการรักษาความปลอดภัยในโลกไซเบอร์ ในการที่จะทำให้พวกเขาต้องระมัดระวังมากยิ่งขึ้นกับสิ่งต่าง ๆ ที่เกี่ยวข้อง

กับมัลแวร์เรียกค่าไถ่ (Ransomware), การหลอกลวงในรูปแบบ Phishing และการละเมิดข้อมูล (Data Breach)

การฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์นั้น เป็นการให้ความรู้แก่พนักงานเกี่ยวกับภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ที่อาจเกิดขึ้น เพื่อให้พวกเขาสามารถหลีกเลี่ยงการโจมตีเหล่านั้นได้ แต่ทั้งนี้ก็ไม่ได้มีการรับประกันว่าเหล่าพนักงานที่ผ่านการอบรมมาแล้วจะไม่ทำพลาด แต่ด้วยการสร้างความตระหนักรู้ถึงวิธีการทั่วไปและวิธีการที่เกิดขึ้นใหม่ที่เหล่าแฮ็กเกอร์จะพยายามนำมาใช้หรือสืบข้อมูล จึงช่วยให้พวกเขาคำนึงถึงความมั่นคงและปลอดภัยทางไซเบอร์ เป็นอันดับแรกเสมอ การฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ควรมุ่งเน้นไปที่สาระสำคัญ 3 ประการ ประการแรกก็คือ เราควรนำเทคโนโลยีสารสนเทศและอุปกรณ์ต่าง ๆ มาใช้ในธุรกิจอย่างไร; ประการที่สองคือ สิ่งที่ดูเหมือนว่าจะเป็นภัยคุกคามด้านความปลอดภัยและประการที่สามคือ วิธีการโต้ตอบต่อกิจกรรมที่น่าสงสัยและการโจมตีทางไซเบอร์ จากเหตุการณ์ที่เกิดขึ้นจริง

องค์กรส่วนใหญ่ควรจะมีนโยบายขององค์กรที่เกี่ยวกับวิธีการใช้อุปกรณ์ ไม่ว่าจะเป็นอุปกรณ์ขององค์กรหรืออุปกรณ์ส่วนบุคคล นอกจากนี้ Shadow IT หรืออุปกรณ์และแอพพลิเคชั่นธุรกิจที่พนักงานนำมาใช้งานโดยไม่ได้รับอนุญาตหรือไม่ได้แจ้งให้ทางฝ่าย IT ทราบนั้น ก็ยังก่อให้เกิดปัญหาทางด้านความปลอดภัยที่อาจจะทำให้ธุรกิจมีความเสี่ยงได้ ดังนั้น จึงถือได้ว่าเป็นเรื่องสำคัญที่จะต้องมีการกำหนดและสนับสนุนความต้องการอย่างสม่ำเสมอ ในสิ่งที่พนักงานสามารถนำไปใช้งานได้และข้อจำกัดต่าง ๆ โดยเฉพาะอย่างยิ่ง ในขณะที่พวกเขาทำการเชื่อมต่อกับเครือข่ายขององค์กร ช่วยให้พนักงานทันต่อเหตุการณ์อยู่เสมอในเรื่องของสิ่งที่ดูเหมือนว่าจะเป็นภัยคุกคามด้านความปลอดภัยนั้นเป็นสิ่งสำคัญอีกประการหนึ่งสำหรับการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยในการใช้ทรัพยากรสารสนเทศภายในองค์กร เพราะเรื่องนี้สามารถนำมาใช้ประโยชน์ได้กับทุก ๆ เรื่อง ตั้งแต่พื้นฐานของสิ่งที่ต้องระวังสำหรับ Phishing Email ไปจนถึงแนวคิดของเทคโนโลยีที่ดีที่สุดเกี่ยวกับสภาพแวดล้อมที่มั่นคงปลอดภัยบนโลกไซเบอร์

การฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอจะช่วยให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์ ถูกหล่อหลอมจนกลายเป็นส่วนหนึ่งในวัฒนธรรมขององค์กร นอกจากนี้ การมีจิตสำนึกต่อส่วนรวมก็ยังเป็นเครื่องมือที่ทรงพลังและมีความสำคัญอย่างมากสำหรับองค์กรธุรกิจที่มีการ เข้า-ออก ของพนักงานในอัตราที่สูง หากพนักงานมีความระมัดระวังเกี่ยวกับอีเมลที่พวกเขาได้รับ หรือแม้แต่รหัสผ่านที่พวกเขาตั้งขึ้นมา ตลอดจนวิธีการแบ่งปันข้อมูลทั้งภายในและภายนอกองค์กร ความเสี่ยงที่จะเกิดจากความผิดพลาดอย่างไร้เหตุผลที่จะส่งผลกระทบร้ายแรงต่อธุรกิจก็จะลดลงอย่างมาก

ข้อดีอย่างหนึ่งที่เห็นได้ชัดเลยก็คือ การฝึกอบรมเป็นประจำจะช่วยให้มีการปฏิบัติตามข้อกำหนดเพิ่มขึ้น หากมีการละเมิดข้อมูลเกิดขึ้นควรแสดงให้เห็นว่าคุณมีการฝึกอบรมอย่างเพียงพอและมีผลบังคับใช้ ซึ่งจะกลายเป็นส่วนสำคัญในการนำมาพิจารณาความผิดพลาดที่เกิดขึ้นกับธุรกิจ อย่างไรก็ตาม องค์กรก็ยังสามารถพบกับความเสี่ยงได้อยู่เสมอ เพราะการให้ความสำคัญกับการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยที่มากเกินไปนั้น อาจจะทำให้พนักงาน

รู้สึกเบื่อหน่ายกับเรื่องภัยคุกคามที่อาจเกิดขึ้นได้ ไม่ต่างกันกับสัญญาณเตือนไฟไหม้ที่เกิดขึ้นถี่จนเกินไปนั่นเอง

การฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านมั่นคงความปลอดภัยไซเบอร์บางรูปแบบอาจมีค่าใช้จ่ายที่ค่อนข้างสูง โดยเฉพาะการฝึกอบรมภาคปฏิบัติและการฝึกอบรมในห้องเรียน ซึ่งมักจะมีประสิทธิภาพมากกว่าหลักสูตรออนไลน์หรือการบรรยายสรุปสั้น ๆ จากองค์กร แต่ค่าใช้จ่ายในการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านมั่นคงความปลอดภัยไซเบอร์นั้น ควรจะมีความสมดุลกับต้นทุนทางการเงินและชื่อเสียง (Reputational Cost) ในระยะยาวที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ที่ประสบความสำเร็จ อย่างไรก็ตาม การฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความปลอดภัยจะไม่เกิดประโยชน์ หากพนักงานมีเจตนาที่จะทำในสิ่งที่เป็นอันตราย แต่ความจริงก็คือ พวกเขาจะไม่สามารถปฏิเสธได้เลยว่า พวกเขาไม่มีความรู้เกี่ยวกับนโยบายและขั้นตอนการปฏิบัติ หากองค์กรมีการเน้นย้ำเป็นประจำในเรื่องของการฝึกอบรม

2.5.4 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ในชีวิตประจำวัน

กรรมการราชบัณฑิตสาขาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ, (2562) อธิบาย ความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) หมายถึง ความรู้แจ้งชัดเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เช่น ความเสี่ยง ภัยคุกคาม การระราน การแอบอ้าง การกีดกัน การโจมตี การก่อการร้าย ฯลฯ ในระบบ

ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ จึงเป็นการสร้างความรู้ ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามทางไซเบอร์ให้ปลอดภัยจากภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ เพื่อให้บุคลากรสามารถดูแลรักษาและใช้งานทรัพยากรสารสนเทศขององค์กรได้อย่างปลอดภัย ระวัง ป้องกันภัยต่อการอาชญากรรม การโจมตี การทำลาย และความผิดพลาดต่าง ๆ ที่อาจเกิดขึ้น โดยคำนึงถึงความปลอดภัยของทรัพย์สินเป็นอันดับแรก และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน ไม่ว่าวันนั้นจะเป็นวันทำงานหรือวันพักผ่อน ซึ่งมีหน่วยงานและผู้กล่าวถึงความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ในชีวิตประจำวัน (สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), 2564) ดังนี้

1. ความตระหนักรู้ด้านการใช้คอมพิวเตอร์ (Computer) เป็นสิ่งที่ควรตระหนักรู้เกี่ยวกับสิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ได้แก่ ควรมีการแยก User ใช้งานกันของแต่ละบุคคล ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์ ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ และมีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น
2. ความตระหนักรู้ด้านการใช้พาสเวิร์ด (Password) โดยการใช้ Password ที่ดี คือ ควรมีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #) ควร มีความยาวของ Password อย่างน้อย 8 ตัวอักษร ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น

password, 123456, วันเกิด, หมายเลขโทรศัพท์ ควรมีการเปลี่ยน Password อย่างสม่ำเสมอ ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้ ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ รวมทั้งไม่ควรบอก Password แก่ผู้อื่น

3. ความตระหนักรู้ด้านการใช้อีเมล (E-mail) โดยสิ่งที่ควรตระหนักรู้ในสิ่งที่ควรปฏิบัติในการใช้อีเมลเพื่อความปลอดภัย คือ ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค และเรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านทางช่องทางอื่น ๆ เพิ่มเติม
4. ความตระหนักรู้ด้านการเข้าเว็บไซต์ (Website) โดยสิ่งที่ควรตระหนักรู้การเข้าเว็บไซต์เพื่อความปลอดภัย ได้แก่ ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ ไม่ควรทำการบันทึก Password ต่าง ๆ บน Browser เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น การใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ และในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing รวมทั้งควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ
5. ความตระหนักรู้ด้านการใช้ (Messaging) โดยสิ่งที่ควรตระหนักรู้เพื่อความปลอดภัยในการใช้ คือ ไม่ควรบันทึก Password ไว้ที่โปรแกรม กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง มีความตระหนักรู้ก่อนเปิด Link หรือไฟล์ต่าง ๆ ที่ได้รับมา มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ รวมทั้งไม่ควรแชร์ข้อมูลหรือข่าวสารต่าง ๆ โดยไม่ทราบที่มาของข้อมูล
6. ความตระหนักรู้เกี่ยวข่าวปลอมในโลกไซเบอร์ (Fake News) ข่าวปลอม เป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือ ซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น ดังนั้นวิธีการสังเกตข่าวปลอม ได้แก่ มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ ระบุที่มาของข่าวไม่ได้ มักจะไม่ระบุวันที่และเวลาที่เกิดเหตุการณ์ สำนวนการเขียนออกแนวการโฆษณา
7. ความตระหนักรู้ด้านการเก็บข้อมูลบนเครื่อง Server (Cloud Storage) สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ควรแยก User ในการใช้งานของแต่ละบุคคล ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ ควรมีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ รวมทั้งควรมีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

8. ความตระหนักรู้ด้านเข้าประชุมทางออนไลน์ (Conference) สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ ใช้สถานที่เหมาะสมกับการประชุมทางออนไลน์ ในการประชุมทางออนไลน์ควรมีแต่ผู้ที่เกี่ยวข้อง การแชร์เอกสารต่าง ๆ อย่างระมัดระวัง การใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน ควรมีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ และควรมีการขออนุญาตผู้เข้าร่วมประชุมทางออนไลน์ ก่อนที่จะบันทึกภาพและเสียงในการประชุม
9. ความตระหนักรู้ในการใช้มือถือ (Mobile) สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ควรเปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์ ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา กำหนด Application permission ให้เหมาะสม มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ และควรมีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

2.5.5 รูปแบบการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความปลอดภัย

QuickServ, (2020) ส่วนใหญ่แล้ว การฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความปลอดภัยจะเป็นการเน้นให้เห็นถึงพฤติกรรมที่ไม่ดีที่พนักงานอาจจะกำลังทำอยู่ พร้อมทั้งสร้างความตระหนักรู้ถึงผลที่จะตามมา เรามี 4 วิธีหลัก ๆ ที่องค์กรจะสามารถนำไปปรับใช้ในการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความปลอดภัย สำหรับปรับปรุงบางส่วนของช่องโหว่ (Vulnerability) ด้วยวิธีง่าย ๆ ดังนี้

1. วิธีการสอนในรูปแบบของห้องเรียน (Classroom-Style) เป็นวิธีการที่พนักงานจะรวมตัวกันทั้งภายในห้องหรือภายนอกห้องก็ได้ เพื่อเข้าร่วมการฝึกอบรมโดยเฉพาะ โดยเรื่องนี้สามารถยกให้เป็นหน้าที่ของสมาชิกด้าน IT หรือทีมรักษาความปลอดภัย (Security Team) หรืออาจจะเป็นการว่าจ้างบริษัทฝึกอบรมจากภายนอกองค์กรก็สามารถทำได้เช่นกัน
2. การฝึกอบรมจากหลักสูตรออนไลน์ (Online Course) เป็นวิธีการที่สามารถนำมาใช้ได้กับพนักงานทั้งที่เป็นพนักงานมาใหม่และพนักงานประจำ ซึ่งหลักสูตรออนไลน์หรือวิดีโอการฝึกอบรมในรูปแบบที่ว่านี้ มักจะนำมาใช้สำหรับการฝึกอบรมเพื่อการปฏิบัติตามกฎระเบียบที่เกี่ยวกับความปลอดภัยจากอัคคีภัยและอื่น ๆ อีกมากมาย นอกจากนี้ยังสามารถนำมาใช้ได้อย่างง่ายดาย เพื่อสร้างการตระหนักรู้ถึงความปลอดภัย แม้ว่าจะไม่มีการรับประกันว่าพนักงานมีส่วนร่วมอย่างไรในการทำหลักสูตรออนไลน์ แต่พวกเขาก็สามารถเรียนรู้ได้ในทันทีสำหรับผู้ที่มาใหม่ และยังสามารถทำแบบทดสอบในตอนท้ายได้อย่างครบถ้วน เพื่อทดสอบความเข้าใจในเรื่องนี้ Internal Test ก็เป็นอีกหนึ่งวิธีที่ได้รับความนิยมมากขึ้น โดยบริษัทต่าง ๆ จะส่งการโจมตีแบบฟิชชิ่งไปยังพนักงานของพวกเขาเอง ซึ่งผู้ที่ทำหน้าที่รักษาความปลอดภัย (Security Staff) สามารถกำหนดผู้ที่จะตกเป็นเหยื่อของการโจมตีแบบฟิชชิ่งได้ และยังสามารถใช้สิ่งเหล่านี้เพื่อการฝึกอบรมเพิ่มเติมได้หากจำเป็น และเมื่อเร็ว ๆ นี้ ผู้มีอำนาจในท้องถิ่นของ Bristol ก็ยังส่งการโจมตีแบบฟิชชิ่งเป็นระยะ ๆ

ให้กับเพื่อนร่วมงานของพวกเขา เพื่อส่งผู้ที่คลิกไปที่ลิงค์ไปยังไซต์ฝึกอบรมที่ได้ทำการระบุไว้แล้ว

3. การแจ้งเตือนเป็นประจำ (Frequent Reminders) การแจ้งเตือนเป็นประจำเช่น โปสเตอร์ที่สามารถติดไว้ในที่ที่มองเห็นได้ชัดในสำนักงานพร้อมกับประกาศด้านสุขภาพและความปลอดภัย, หรืออีเมลของบริษัทที่สร้างขึ้นเฉพาะ ซึ่งทั้งสองอย่างนี้สามารถนำมาใช้เพื่อให้ครอบคลุมเนื้อหาสาระ ทั้งในส่วนของลักษณะของอีเมลที่น่าสงสัย, วิธีการตรวจสอบลิงค์และความสำคัญของรหัสผ่านที่ปลอดภัย
4. กุญแจสำคัญในการฝึกอบรมเรืองการตระหนักรู้ (Awareness Training) ในทุก ๆ รูปแบบก็คือ การทำอย่างสม่ำเสมอ ซึ่งผลการวิจัยระดับโลกจาก Vanson Bourne พบว่าในขณะนี้มีองค์กรเพียง 11% ที่ทำการฝึกอบรมพนักงานของพวกเขาอย่างต่อเนื่องเกี่ยวกับวิธีการโจมตีทางไซเบอร์ และมีองค์กรจำนวน 52% ที่ทำการฝึกซ้อมเป็นรายไตรมาสหรือเพียงปีละครั้งเท่านั้นและนั่นก็หมายความว่า การฝึกอบรมประจำปีอาจส่งผลให้สมาชิกใหม่ของทีมสามารถทำพลาดซ้ำ ๆ ได้นานกว่า 11 เดือน โดยที่ไม่มีการฝึกอบรมด้านความปลอดภัยใด ๆ เพิ่มเติม นับว่าเป็นการเพิ่มความเสี่ยงให้กับองค์กรของพวกเขาได้อย่างมหาศาล ซึ่งอาจจะเป็นการคลิกอีเมลที่เป็นอันตรายโดยไม่ได้ตั้งใจหรืออาจจะเป็นอะไรที่แย่กว่านั้น เนื่องจากการโจมตีมีวิวัฒนาการอย่างรวดเร็ว นั่นจึงเป็นการเน้นย้ำว่าการฝึกอบรมอย่างต่อเนื่องเป็นวิธีที่ดีที่สุด รวมถึงการปลูกฝังความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ให้เข้าไปเป็นส่วนหนึ่งของวัฒนธรรมองค์กร ก็จะช่วยให้พนักงานทันต่อเหตุการณ์กับสิ่งที่ต้องระวังได้มากยิ่งขึ้น

2.6 กรอบการรักษาความมั่นคงปลอดภัย (NIST Cybersecurity Framework)

Framework Core Functions for Cyber security แบ่งออกเป็นกรอบงานหลัก 5 functions ซึ่งเป็นกิจกรรมงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ ได้แก่

1. การระบุ (Identify) เป็นขั้นตอนแรกในการศึกษาทำความเข้าใจบริบท ทรัพยากรและกิจกรรมงานสำคัญ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบทรัพย์สิน ข้อมูล และขีดความสามารถ
2. การป้องกัน (Protect) เป็นการจัดทำและดำเนินการตามมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการโครงสร้างพื้นฐานสำคัญโดยมีวัตถุประสงค์เพื่อจำกัดระดับผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งครอบคลุมการฝึกอบรมและการสร้างความตระหนักรู้มาตรการควบคุมการเข้าถึงและมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี
3. การตรวจจับ (Detect) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวังหรือตรวจติดตามต่อเนื่อง

4. การตอบสนอง (Respond) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสารการวิเคราะห์ การลดความเสี่ยง และการปรับปรุง (จิราพัชร์ พันธุ์ถาวรชัย, 2561, หน้า 6-13)

Cybersecurity Framework ออกแบบมาเพื่อลดความเสี่ยงโดยการปรับปรุงการจัดการของความเสี่ยงด้านความปลอดภัยทางไซเบอร์ต่อวัตถุประสงค์ขององค์กร ตามหลักการแล้ว องค์กรที่ใช้กรอบการทำงานจะสามารถวัดและกำหนดค่าความเสี่ยงพร้อมกับต้นทุนและประโยชน์ของขั้นตอนที่ดำเนินการเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ยิ่งองค์กรสามารถวัดความเสี่ยง ต้นทุนและประโยชน์ของกลยุทธ์และขั้นตอนในการรักษาความปลอดภัยทางไซเบอร์ ก็จะยิ่งมีประสิทธิภาพมากขึ้น ซึ่งการพัฒนาตัวชี้วัดประสิทธิภาพการรักษาความปลอดภัยทางไซเบอร์ องค์กรควรจะรอบคอบสร้างสรรค์ และระมัดระวังเกี่ยวกับวิธีการใช้การวัดเพื่อเพิ่มประสิทธิภาพใช้ในขณะที่หลีกเลี่ยงการพึ่งพาตัวบ่งชี้สถานะปัจจุบันและความคืบหน้าในการปรับปรุงการจัดการความเสี่ยงด้านควาปลอดภัยทางไซเบอร์ นอกจากนี้การตัดสินความเสี่ยงทางไซเบอร์ต้องมีระเบียบวินัยและควรได้รับการทบทวนอย่างสม่ำเสมอ ในทุกครั้งที่มีการใช้การวัดเป็นส่วนหนึ่งของกระบวนการกรอบงานองค์กรควรระบุอย่างชัดเจนและรู้ว่าเหตุใดการวัดเหล่านี้จึงเป็นเช่นนั้นสำคัญและจะมีส่วนช่วยในการจัดการความเสี่ยงด้านความปลอดภัยในโลกไซเบอร์โดยรวมได้อย่างไร (National Institute of Standards and Technology, 2018, หน้า 5-27)

2.7 งานวิจัยที่เกี่ยวข้อง

ศุภวิชญ์ สาตราวาหะ, กีรติสรรพ์ ผลละออ, วิชากร ต่ายทอง, (2560) ศึกษาเรื่องการวิเคราะห์พฤติกรรมการป้องกันภัยคุกคามทางโทรศัพท์มือถือของคนไทยด้วยโปรแกรม RapidMiner ได้ทำการ Data Mining โดยใช้ RapidMiner ผลสำรวจที่ได้ทำการแจกจ่ายผ่านทาง Google Drive ให้กับประชาชนแบบสุ่มจำนวน 400 ชุด เพื่อทำการหาความสัมพันธ์ของพฤติกรรมการใช้งานต่อความเสี่ยงในการคุกคามทางด้านไซเบอร์ จากนั้นนำความสัมพันธ์ที่ได้มาทำ Web Application ให้ประชาชนมาทำแบบทดสอบความเสี่ยง และทำให้ทราบความเสี่ยงของตนเอง

A. Alarifi, H. Tootell, P. Hyland, (2012) ได้ทำวิจัยเรื่อง “A Study of Information Security Awareness and Practices in Saudi Arabia” ศึกษาเรื่องรูปแบบการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยแก่ประชาชนในประเทศ Saudi Arabia โดยการสร้างแบบสอบถามเพื่อสำรวจความคิดเห็นของประชาชนจำนวน 462 คน ถึงรูปแบบวิธีการสร้างความตระหนักรู้ที่คิดว่ามีประสิทธิภาพมากที่สุดระหว่าง Web portals, Newspaper, Advertisements, Documentaries, Billboard/Posters, E-books/Magazines และ Seminars ผลวิจัยพบว่ารูปแบบที่มีประสิทธิภาพสูงที่สุดคือ Web portals และต่ำที่สุดคือ Seminars

สุรชัย ฉัตรเฉลิมพันธุ์ และ เทอดพงษ์ แดงสี, (2563) จากผลการศึกษาด้วยการจำลองการโจมตีโดยใช้อีเมลฟิชชิ่งในบริษัทแห่งหนึ่งเกี่ยวกับประเด็นด้านความมั่นคงปลอดภัยทางไซเบอร์ในครั้งนี้ สามารถสรุปจากผลการศึกษาในครั้งที่ 1 ได้ว่า บุคลากรในองค์กรมีระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ที่ยังไม่จัดได้ว่าอยู่ในเกณฑ์ดี (74.48 %) เพราะยังมีพนักงานหรือบุคลากรขององค์กร

จำนวนหนึ่งที่ยังขาดความตระหนักรู้ถึงความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ อย่างไรก็ดีเมื่อมีการดำเนินการถ่ายทอดความรู้เรื่องความตระหนักรู้เท่าทันภัยทางไซเบอร์ให้แก่บุคลากรแล้วทำการศึกษาซ้ำในครั้งที่ 2 พบว่า บุคลากรในองค์กรมีระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ที่ดีขึ้นอย่างชัดเจน คืออยู่ในเกณฑ์ดี (88.80 %) แสดงว่าการถ่ายทอดความรู้เรื่องความตระหนักรู้เท่าทันภัยทางไซเบอร์ให้แก่บุคลากรที่ดำเนินการไปให้ผลลัพธ์ที่ดี และสามารถนำรูปแบบการดำเนินการที่ได้บรรยายไว้ในบทความนี้ไปประยุกต์ใช้ในการยกระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ในองค์กรอื่น ๆ ได้ เพื่อเพิ่มความมั่นคงปลอดภัยทางไซเบอร์และของบุคลากรในองค์กร

สุธาเทพ รุณเรศ, (2561) ได้วิจัยเรื่อง “ปัจจัยที่มีผลต่อการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร” การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยทางด้านลักษณะทางประชากร ประสบการณเกี่ยวกับภัยคุก คามทางไซเบอร์ และความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่มีผลต่อความตระหนักรู้ถึงภัย คุกคามทางไซเบอร์ของผู้ใช้ อินเทอร์เน็ต การวิจัยนี้เป็นการวิจัยเชิงสำรวจ ประชากร คือ ผู้ใช้อินเทอร์เน็ตที่มีอายุ 15 ปีขึ้นไป และอยู่ในเขตกรุงเทพมหานคร ขนาดตัวอย่าง 400 คน ใช้การสุ่มตัวอย่างแบบบังเอิญและแบบสโนว์บอล โดยให้กลุ่มตัวอย่างกรอกแบบสอบถามด้วยตนเองทางออนไลน์ ผลการวิจัยจะช่วยให้หน่วยงานที่เกี่ยวข้องสามารถนำไปใช้ในการวางแผนสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ให้กับผู้ใช้อินเทอร์เน็ตต่อไป ผลการวิจัย พบว่า 1. ปัจจัยทางด้านลักษณะทางประชากรด้านอายุ ระดับการศึกษาสูงสุด และรายได้ส่วนตัวต่อเดือน มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต แต่ปัจจัยทางด้านลักษณะทางประชากรด้านเพศ ไม่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต 2. ปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ไม่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต 3. ปัจจัยทางด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตผลการวิจัยจะช่วยให้หน่วยงานที่เกี่ยวข้องสามารถนำไปใช้ในการวางแผนสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ให้กับผู้ใช้อินเทอร์เน็ตต่อไป

เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี, (2565) ได้วิจัยเรื่อง ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร โดยมีวัตถุประสงค์เพื่อศึกษาระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร และเพื่อเปรียบเทียบระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร โดยจำแนกตามปัจจัยส่วนบุคคล ผลการศึกษาพบว่า บุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร มีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์อยู่ในระดับมาก เมื่อจำแนกตามปัจจัยด้านบุคคลผลวิจัยพบว่าบุคลากรในบริษัทเอกชนแห่งนี้ที่มี เพศ อายุ และประสบการณ์การทำงาน (อายุงาน) ที่ต่างกันมีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่ไม่แตกต่างกัน และในส่วนบุคลากรที่มีระดับการศึกษาสูงสุด แผนกที่สังกัด และประสบการณ์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่ต่างกัน มีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่แตกต่างกันอย่างมีนัยสำคัญทางสถิติ

ชนินทร เฉลิมทรัพย์, นาวาอากาศเอก, (2561) ได้วิวิจัยเรื่อง แนวทางการบูรณาการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ ผู้วิจัยได้ศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กร

การบูรณาการการบริหารจัดการและการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งศึกษาค้นคว้านโยบายยุทธศาสตร์และการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหมและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จากการวิจัยนี้ได้มีข้อเสนอแนะว่าสำหรับแนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ คือ

1) การจัดการความรู้และการบริหารความเสี่ยง (Knowledge Management & Risk) เพื่อให้ผู้นำองค์กร ผู้กำหนดนโยบายและผู้ปฏิบัติ ได้ตระหนักรู้ เก็บสะสมองค์ความรู้ และประสบการณ์เพื่อเป็นประโยชน์ต่อไป

2) มีการทำงานแบบเครือข่ายเชื่อมโยงตามประเด็นยุทธศาสตร์ร่วม (Common Agenda) ปฏิบัติงานตามมาตรฐานการปฏิบัติทางเทคโนโลยีและจัดตั้งศูนย์การศึกษาการวิจัยการพัฒนาด้านความมั่นคงปลอดภัยทางไซเบอร์ต่อไป

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

สุรพงศ์ ทรัพยาคม และ อรรถพล ป้อมสถิต, (2563) ได้ศึกษาการวิเคราะห์การรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พบว่าธนาคารพาณิชย์จะต้องมีการปรับปรุงพัฒนาเพื่อสร้างความเข้มแข็งในด้านเทคโนโลยีสารสนเทศให้ครบทั้ง 3 ด้านคือ 1) การใช้เทคโนโลยีที่เหมาะสมสำหรับการบูรณาการในด้านเทคนิคเช่นการยืนยันตัวบุคคลอย่างบูรณาการ ไฮเปอร์คอนเวอจ์อินฟราสตรัคเจอร์หรือการพัฒนาคลังข้อมูลกลาง 2) มีการสร้างแบบนโยบายหรือแนวทางปฏิบติสำหรับกำกับผู้ปฏิบัติงานเพื่อลดความเสี่ยงหรือภัยคุกคามที่มาจากความผิดพลาดของมนุษย์ และ 3) มีการเตรียมความพร้อมหรือมีมาตราการรองรับสำหรับด้านภัยหรือสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้น ทั้งนี้สามารถสรุปแนะแนวทางการป้องกันภัยคุกคามให้สอดคล้องกับตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

Wajeb Gharibi and Maha Shaabi, (2012) เรื่อง Cyber Threats in Social Networking Websites ศึกษาเรื่องภัยคุกคามทางไซเบอร์ในเครือข่ายสังคมออนไลน์ เว็บไซต์ โซเชียลออนไลน์ โดยการจำแนกประเภทภัยคุกคามทางไซเบอร์ แนะนำกลยุทธ์ต่อต้านภัยคุกคามและคาดการณ์แนวโน้มในอนาคตของเว็บไซต์ยอดนิยม แม้ว่าเว็บไซต์ เครือข่ายสังคมออนไลน์จะมีเทคโนโลยีขั้นสูงในการโต้ตอบและการสื่อสาร ซึ่งก่อให้เกิดความท้าทายใหม่ ๆ เกี่ยวกับเรื่องความลอดภัยของความเป็นส่วนตัว ผู้เขียนสรุปว่า ความก้าวหน้าของเทคโนโลยีใหม่โดยทั่วไปและเว็บไซต์โซเชียลโดยเฉพาะ จะนำมาซึ่งความเสี่ยงด้านความปลอดภัยในรูปแบบใหม่ ๆ ที่อาจเปิดโอกาสสำหรับผู้มุ่งร้าย ผู้บันทึกคีย์ ม้าโทรจัน ฟิชชิ่ง

สายลับ ไวรัส และผู้โจมตี ดังนั้น ผู้เชี่ยวชาญด้านความปลอดภัยของข้อมูล ข้าราชการและหน่วยข่าวกรองอื่น ๆ ต้องพัฒนาเครื่องมือใหม่ที่ป้องกันและปรับให้เข้ากับความเสี่ยงและภัยคุกคามที่อาจเกิดขึ้นในอนาคต และสามารถจัดการกับข้อมูลในอินเทอร์เน็ตและในเว็บไซต์โซเชียลได้อย่างปลอดภัยด้วย

Ikhsan & Ramli, (2019) ได้ทำการศึกษาด้วยแบบสอบถามเกี่ยวกับพฤติกรรมเพื่อวัดระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ของเจ้าพนักงานในหน่วยงานรัฐในประเทศอินโดนีเซียจำนวนมากกว่า 7,300 คนทั่วประเทศ จากการศึกษาพบว่า เจ้าพนักงานในหน่วยงานรัฐในหน่วยงานดังกล่าวซึ่งตอบแบบสอบถาม 736 คน มีความตระหนักรู้เท่าทันภัยทางไซเบอร์ในระดับ 79.32 % เมื่อ 60 % - 79 % คือ ปานกลาง และ 80 % - 100 % คือ ดี

Tero Haukilehto, (2019) เนื่องจากการปฏิรูปด้านสุขภาพ บริการสังคม และรัฐบาลระดับภูมิภาคสร้างความคาดหวังอย่างมากสำหรับเทคโนโลยีใหม่และการประหยัดที่จะเกิดขึ้น ความสำคัญของความปลอดภัยในโลกไซเบอร์ก็เพิ่มขึ้น เมื่อฝึกอบรมการรักษาความปลอดภัยทางไซเบอร์สำหรับบุคลากรของเขตโรงพยาบาล South Ostrobothnia ข้อบกพร่องในการตระหนักรู้ด้านความปลอดภัยในโลกไซเบอร์ก็ปรากฏขึ้น เนื่องจากการปรับปรุงการรับรู้เป็นวิธีที่ง่ายเร็ว และถูกที่สุดในการปรับปรุงระดับความปลอดภัยในโลกไซเบอร์ในองค์กร การตระหนักรู้ด้านความปลอดภัยในโลกไซเบอร์ในปัจจุบันจึงมีคุณค่าต่อการวัดผลในองค์กรต่าง ๆ ภายใต้การปฏิรูปในภูมิภาค South Ostrobothnia การศึกษาได้ตรวจสอบระดับปัจจุบันของการรับรู้ความปลอดภัยในโลกไซเบอร์และเหตุผลที่มีผลกระทบต่อมัน ส่วนทางทฤษฎีกล่าวถึงการพึ่งพาและความท้าทายของการรักษาความปลอดภัยในโลกไซเบอร์และโครงสร้างพื้นฐานที่สำคัญ โดยเฉพาะอย่างยิ่งจากมุมมองของการดูแลสุขภาพ การศึกษาความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ได้รับการศึกษาด้วยการสำรวจที่แตกต่างกันสามแบบ การสำรวจสองครั้งแรกจัดขึ้นโดยเป็นส่วนหนึ่งของบทเรียนความปลอดภัยทางไซเบอร์สำหรับบุคลากรของ Hospital District of South Ostrobothnia การสำรวจครั้งที่ 3 ดำเนินการในรูปแบบการสำรวจทางอินเทอร์เน็ตสำหรับองค์กรทั้งหมดที่เกี่ยวข้องกับการปฏิรูปใน South Ostrobothnia มีการวิเคราะห์คำตอบมากกว่า 1,200 คำตอบ โดยใช้การวิเคราะห์เนื้อหาตามเนื้อหาผลลัพธ์ที่ได้ทำให้สามารถสร้างมุมมองโดยรวมของระดับปัจจุบันของการรับรู้ความปลอดภัยในโลกไซเบอร์ในองค์กร ความครอบคลุมของการศึกษา และเหตุผลที่มีผลกระทบต่อพวกเขา จากผลการศึกษาพบว่าบุคลากรและผู้บริหารในองค์กรเป้าหมายยังขาดความตระหนักรู้และความรู้ด้านความปลอดภัยทางไซเบอร์ ควรปรับปรุงความตระหนักรู้ด้านความปลอดภัยในโลกไซเบอร์โดยรวมในองค์กรเป้าหมายทั้งหมด

Therdpong Daengsi et al., (2021) การรักษาความปลอดภัยทางไซเบอร์มีความสำคัญในปัจจุบัน เนื่องจากภัยคุกคามทางไซเบอร์ (เช่น ฟิชชิ่ง) กลายเป็นเรื่องธรรมดาในชีวิตประจำวัน การทบทวนวรรณกรรมพบว่าไม่มีการศึกษาเกี่ยวกับความตระหนักรู้เรื่องความปลอดภัยในโลกไซเบอร์ซึ่งเกี่ยวข้องกับกลุ่มใหญ่ จำนวนผู้ใช้ชาวไทย ดังนั้น งานวิจัยนี้จึงเน้นที่ความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของพนักงานทั่วประเทศประมาณ 20,000 คนในสถาบันการเงินขนาดใหญ่ในประเทศไทยการศึกษาประกอบด้วย 3 ระยะ คือ การโจมตีแบบฟิชชิ่งครั้งแรก การถ่ายทอดความรู้ผ่านวิธีการผสมและการโจมตีแบบฟิชชิงครั้งที่สองที่มีเนื้อหาต่างกัน หลังจากการตรวจสอบข้อมูลและวิเคราะห์ผล พบว่า ระดับความปลอดภัยทางไซเบอร์ความตระหนักรู้ของพนักงานดีขึ้นอย่างมาก

จำนวนพนักงานผู้ที่เปิดอีเมลฟิชชิ่งลดลง 71.5% ดังนั้น แนวทางนี้สามารถนำไปปรับใช้กับการเพิ่มประสิทธิภาพการรักษาความปลอดภัยทางไซเบอร์ในองค์กรและภาคส่วนอื่น ๆ/ ในอุตสาหกรรม นอกจากนี้ ยังพบว่าเพศมีบทบาทสำคัญในความปลอดภัยทางไซเบอร์ ความตระหนักรู้ในระบบนิเวศความปลอดภัยทางไซเบอร์ของไทยตั้งแต่พนักงานหญิงไทย พบว่ามีความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ในระดับที่สูงกว่าพนักงานชาย นอกจากนี้ ยังพบว่าพนักงานชาวไทยรุ่นต่าง ๆ (Generations Y และ X และ Baby Boomers) ไม่ส่งผลต่อการรับรู้ความปลอดภัยในโลกไซเบอร์

2.7 สรุป

ในบทที่ 2 เป็นการนำเสนอแนวคิดในด้านต่าง ๆ ประกอบด้วย การใช้อินเทอร์เน็ตและระบบดิจิทัลในประเทศไทย แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) แนวคิดเกี่ยวกับการคุกคามทางไซเบอร์ (Cyber Threats) แนวคิดเกี่ยวกับการกลั่นแกล้งทางไซเบอร์ (Cyber Bullying) แนวคิดเกี่ยวกับความรู้ (Awareness) กรอบการรักษาความมั่นคงปลอดภัย (NIST Cybersecurity Framework) และ งานวิจัยที่เกี่ยวข้อง ทั้งนี้ผู้วิจัยจะนำเสนอวิธีดำเนินการวิจัยในบทที่ 3 ต่อไป

บทที่ 3

วิธีดำเนินการวิจัย

การวิจัยเรื่อง “การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด” มีวัตถุประสงค์ 3 ข้อ ได้แก่ 1) เพื่อศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ 2) เพื่อพัฒนาแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์ 3) เพื่อจัดทำแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ซึ่งงานวิจัยนี้เป็นการวิจัยแบบผสมผสาน (Mixed Method) กล่าวคือเป็นการวิจัยเชิงคุณภาพ (Qualitative Research) และการวิจัยเชิงปริมาณ (Quantitative Research) โดยมีรายละเอียดดังต่อไปนี้

3.1 ประชากรและกลุ่มตัวอย่าง

3.2 การเก็บรวบรวมข้อมูล

3.3 เครื่องมือที่ใช้ในการวิจัย

3.4 การวิเคราะห์ข้อมูล

3.5 การวิเคราะห์ข้อมูล ออกแบบและพัฒนาแอปพลิเคชัน

3.6 ระยะเวลาในการดำเนินงาน

3.7 สรุป

3.2 ประชากรและกลุ่มตัวอย่าง

3.2.1 ประชากรที่ใช้ในการวิจัย

ประชากรและกลุ่มตัวอย่างที่ของงานวิจัยครั้งนี้ คือ บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด จำนวน 3,169 คน

3.2.2 การกำหนดขนาดกลุ่มตัวอย่าง

ขนาดกลุ่มตัวอย่างของงานวิจัยนี้ ใช้การกำหนดขนาดกลุ่มตัวอย่างตามตารางสำเร็จของทาโรยามาเน่ (Yamane, 1973) โดยที่ระดับความเชื่อมั่น 95% ค่าความคลาดเคลื่อนที่ผู้วิจัยยอมรับได้เท่ากับ 10% ตามตารางที่ 3.1

ตารางที่ 3.1 แสดงขนาดของกลุ่มตัวอย่าง

ขนาดประชากร	ขนาดของกลุ่มตัวอย่างที่ระดับความคลาดเคลื่อน (e)					
	$\pm$ 1%	$\pm$ 2%	$\pm$ 3%	$\pm$ 4%	$\pm$ 5%	$\pm$ 10%
500	*	*	*	*	222	83
1,000	*	*	*	385	286	91
1,500	*	*	638	441	316	94
2,000	*	*	714	476	333	95
2,500	*	1,250	769	500	345	96
3,000	*	1,364	811	517	353	97
3,500	*	1,458	843	530	359	97
4,000	*	1,538	870	541	364	98
4,500	*	1,607	891	549	367	98
5,000	*	1,667	909	556	370	98
6,000	*	1,765	938	566	375	98
7,000	*	1,842	959	574	378	99
8,000	*	1,905	976	580	381	99
9,000	*	1,957	989	584	383	99
10,000	5,000	2,000	1,000	588	385	99
15,000	6,000	2,143	1,034	600	390	99
20,000	6,667	2,222	1,053	606	392	100
25,000	7,143	2.273	1,064	610	394	100
50,000	8,333	2,381	1,087	617	397	100
100,000	9,091	2,439	1,099	621	398	100
∞	10,000	2,500	1,111	625	400	100

* หมายถึง ขนาดตัวอย่างไม่เหมาะสมที่จะคาดคะเนให้เป็นการกระจายแบบปกติ จึงไม่สามารถใช้สูตรคำนวณหาขนาดของกลุ่มตัวอย่างได้

3.1.3 วิธีการสุ่มตัวอย่าง

ผู้วิจัยใช้วิธีการสุ่มตัวอย่างแบบไม่ใช่หลักความน่าจะเป็น (Non-Probability Sampling) เป็นการเลือกกลุ่มตัวอย่างโดยไม่คำนึงว่าตัวอย่างแต่ละหน่วยมีโอกาสถูกเลือกมากน้อยเท่าไหร่ ด้วยวิธีการสุ่มตัวอย่างแบบบังเอิญ (Accidental Sampling) ตัวอย่างจะเป็นใครก็ได้ที่สามารถให้ข้อมูลได้ และวิธีการสุ่มตัวอย่างแบบสโนว์บอล (Snowball Sampling) เป็นการบอกต่อของผู้ตอบแบบสอบถามจนกว่าจะได้จำนวนที่ต้องการ

3.2 การเก็บรวบรวมข้อมูล

งานวิจัยนี้เป็นการวิจัยแบบผสมผสาน มีการเก็บรวบรวมข้อมูล ดังนี้

การวิจัยเชิงคุณภาพ ใช้แบบสัมภาษณ์แบบกึ่งโครงสร้าง ทำการสัมภาษณ์เชิงลึก (In-depth Interview) ผู้บริหารและผู้เชี่ยวชาญด้านระบบสารสนเทศของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด โดยผู้วิจัยสัมภาษณ์ด้วยตนเองโดยการบันทึกข้อมูลด้วยการจดบันทึกและ/หรือบันทึกด้วยเครื่องบันทึกเสียงและ/หรือภาพเคลื่อนไหวและการสัมภาษณ์ผ่านสื่อออนไลน์ สำหรับการเก็บรวบรวมข้อมูล

การวิจัยเชิงปริมาณ ใช้แบบสอบถามปลายปิด (Close-end Questionnaire) โดยการทำแบบสอบถามออนไลน์ และให้กลุ่มตัวอย่างที่กำหนดไว้เป็นผู้ตอบคำถามเอง (Self-Administered) ด้วย Google Forms ซึ่งสามารถรองรับผู้ตอบแบบสอบถามได้ไม่จำกัดและข้อมูลจะถูกเก็บโดยอัตโนมัติไว้ที่ Google Spreadsheet ซึ่งเป็นวิธีที่ดี รวดเร็ว และสะดวก เหมาะสมกับสถานการณ์โรคระบาด COVID-19 ในปัจจุบัน ที่ต้องหลีกเลี่ยงการสัมผัสกับชุมชน และยังสามารถแชร์ แบ่งปันแบบสอบถามไปยังประชากรกลุ่มตัวอย่างได้ง่าย

3.3 เครื่องมือที่ใช้ในการวิจัย

งานวิจัยนี้เป็นการวิจัยแบบผสมผสาน จะใช้เครื่องมือการวิจัย ดังนี้

3.3.1 แบบสัมภาษณ์แบบกึ่งโครงสร้าง

สำหรับการวิจัยเชิงคุณภาพ ผู้วิจัยใช้แบบสัมภาษณ์แบบกึ่งโครงสร้าง ทำการสัมภาษณ์เชิงลึก (In-depth Interview) ผู้บริหารและผู้เชี่ยวชาญด้านระบบสารสนเทศของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด เพื่อดำเนินการตามวัตถุประสงค์ข้อที่ 1 “เพื่อศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์” และตามวัตถุประสงค์ข้อที่ 2 “เพื่อพัฒนาแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์”

3.3.2 แบบสอบถามปลายปิด

สำหรับการวิจัยเชิงปริมาณ ผู้วิจัยได้ออกแบบสอบถามปลายปิดจากการกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ NIST Cybersecurity Framework การวิเคราะห์ข้อมูลจากแบบสัมภาษณ์เชิงลึก และสังเคราะห์จากการศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้องพิจารณาจากงานวิจัยที่ด้รับการตีพิมพ์ในวารสารทางวิชาการที่เชื่อถือได้ และกำหนดหัวข้อคำถามนำเสนออาจารย์ที่ปรึกษาเพื่อตรวจสอบความถูกต้องและความเหมาะสมของภาษาและข้อคำถามที่ใช้ จำนวน 2 ชุด ดังนี้

แบบสอบถามชุดที่ 1 สำหรับการเก็บรวบรวมข้อมูลสำหรับการสำรวจพฤติกรรมและระดับความตระหนักรู้ เพื่อดำเนินการตามวัตถุประสงค์ข้อที่ 1 “เพื่อศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์” และตามวัตถุประสงค์ข้อที่ 2 “เพื่อพัฒนาแนวทางการเสริมสร้างความ

ตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์” โดยแบบสอบถามนี้ประกอบด้วยข้อคำถาม จำนวน 3 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลทั่วไปบุคลากรของกลุ่มตัวอย่าง

ส่วนที่ 2 พฤติกรรมการใช้งานระบบอินเทอร์เน็ต ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

ส่วนที่ 3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

แบบสอบถามชุดที่ 2 ใช้สำหรับการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ หลังจากการได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์แล้ว โดยแบบสอบถามนี้ประกอบด้วยข้อคำถาม จำนวน 4 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลทั่วไปบุคลากรของกลุ่มตัวอย่าง

ส่วนที่ 2 พฤติกรรมการใช้งานระบบอินเทอร์เน็ต ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

ส่วนที่ 3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

ส่วนที่ 4 ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์

สามารถแสดงภาพรวมข้อคำถามในแบบสอบถาม ซึ่งเป็นเครื่องมือของการวิจัยเชิงปริมาณได้ดังตารางที่ 3.2

ตารางที่ 3.2 ตารางแสดงภาพรวมข้อคำถามที่ใช้ในแบบสอบถาม

ข้อ	มิติของตัวแปรแฝง	ปัจจัยที่ส่งผลต่อความตั้งใจที่จะใช้ประกันภัยไซเบอร์
ด้านพฤติกรรมการใช้อินเทอร์เน็ต INTERNET (INT) (5 ข้อ)		
1	INT1	การใช้อีเมลตนเองในการสมัครบัญชีออนไลน์
2	INT2	การตั้งค่าบัญชีให้เป็นส่วนตัว
3	INT3	การกรอกข้อมูลส่วนตัวตามอีเมลที่ส่งมา
4	INT4	การดาวน์โหลดไฟล์โดยไม่ทราบแหล่งที่มาออนไลน์
5	INT5	การเข้าเว็บไซต์ที่ไม่เหมาะสม
6	INT6	การใช้อีเมลตนเองในการสมัครบัญชีออนไลน์
ด้านพฤติกรรมการใช้งานสื่อสังคม SOCIAL (SCL) (3 ข้อ)		
7	SCL1	การเผยแพร่ข้อความ รูปภาพ วิดิทัศน์ ลงในสื่อสาธารณะ
8	SCL2	อนุญาตให้บุคคลที่ไม่รู้จักเข้าถึงการใช้งานบน Social Media ของตนเอง

ตารางที่ 3.2 (ต่อ)

9	SCL3	ไม่จำกัดการเข้าถึงข้อมูลส่วนตัวในบัญชี Social Media
ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์ ON-LINE (ONL) (4 ข้อ)		
11	ONL1	การเข้าถึงสื่อออนไลน์ที่ไม่รู้จักมาก่อน
12	ONL2	การเข้าถึงสื่อที่มีโฆษณาเชิญชวนไปยังเว็บไซต์อื่น
13	ONL3	การเข้าถึงสื่อออนไลน์ที่ไม่ได้รับการคัดกรอง
14	ONL4	การเข้าสื่อออนไลน์ที่ให้เปิดเผยข้อมูลส่วนตัวมากเกินไป
ด้านพฤติกรรมการใช้งานผ่านโปรแกรม PROGRAM (PRG) (4 ข้อ)		
15	PRG1	การใช้งานผ่านโปรแกรมที่ไม่มีลิขสิทธิ์
16	PRG2	การโหลดโปรแกรมที่ไม่มีลิขสิทธิ์จากแหล่งต่าง ๆ
17	PRG3	การติดตั้งโปรแกรมต่าง ๆ จากบุคคลอื่น
18	PRG4	การติดตั้งโปรแกรมโดยไม่ศึกษารายละเอียด
ด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต Cybersecurity Threats (CST) (4 ข้อ)		
19	CST1	มีโปรแกรมป้องกัน Spyware
20	CST2	การเปิดการใช้งานโปรแกรม Firewall
21	CST3	มีการสำรอง (Backup) ข้อมูลเป็นประจำ
22	CST4	มีโปรแกรมสำหรับลบไฟล์แบบถาวร (Files Shredder)
ความตระหนักรู้ด้านการใช้คอมพิวเตอร์ Computer (COM) (5 ข้อ)		
23	COM1	มีการแยก User ใช้งานกันของแต่ละบุคคล
24	COM2	Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
25	COM3	ติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
26	COM4	มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
27	COM5	มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
ความตระหนักรู้ด้านการใช้พาสเวิร์ด Password (PWD) (5 ข้อ)		
28	PWD1	พาสเวิร์ดมีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #) และมีความยาวของ Password อย่างน้อย 8 ตัวอักษร
29	PWD2	มีการหลีกเลี่ยงใช้ Common Password หรือ Default Password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น password, 123456, วันเกิด, หมายเลขโทรศัพท์
30	PWD3	มีการเปลี่ยน Password อย่างสม่ำเสมอ ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
31	PWD4	ไม่ใช้ Password ซ้ำกันในแต่ละระบบ รวมทั้งไม่ควรบอก Password แก่ผู้อื่น

ตารางที่ 3.2 (ต่อ)

32	PWD5	ไม่จด Password และติด Password ไว้ที่หน้าจอ
ความตระหนักรู้ด้านการใช้อีเมล E-mail (EML) (4 ข้อ)		
33	EML1	ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
34	EML2	ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
35	EML3	ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจสอบ
36	EML4	เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการตรวจสอบผ่านทางช่องทางอื่น ๆ เพิ่มเติม
ความตระหนักรู้ด้านการเข้าเว็บไซต์ Website (WEB) (4 ข้อ)		
37	WEB1	ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ
38	WEB2	ไม่ทำการบันทึก Password ต่าง ๆ บน Browser เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือหากมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS และการใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox
39	WEB3	มีการ Update Version ของ Browser อย่างสม่ำเสมอ
40	WEB4	มีการใช้งาน Browser ในโหมด Safe Web Browsing รวมทั้งได้ติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ
ความตระหนักรู้ด้านการใช้ Messaging (MSG) (3 ข้อ)		
41	MSG1	ไม่บันทึก Password ไว้ที่โปรแกรม
42	MSG2	กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง
43	MSG3	มีความตระหนักรู้ก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา
ความตระหนักรู้เกี่ยวข่าวปลอมในโลกไซเบอร์ Fake News (FAK) (2 ข้อ)		
44	FAK1	ไม่อ่านข่าวที่ไม่ได้ระบุที่มาของข่าวไม่ได้
45	FAK2	ไม่อ่านข่าวที่ไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
ความตระหนักรู้ด้านการเก็บข้อมูลบนเครื่อง Server (Cloud Storage) (CLD) (3 ข้อ)		
46	CLD1	ควรแยก User ในการใช้งานของแต่ละบุคคล
47	CLD2	ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็น และปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
48	CLD3	ควรติดตั้ง Anti-Malware และ Update อย่างสม่ำเสมอ และควรมีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ
ความตระหนักรู้ด้านเข้าประชุมทางออนไลน์ Conference (CON) (3 ข้อ)		
49	CON1	การใช้สถานที่เหมาะสมกับการประชุม (Conference)
50	CON2	การประชุม (Conference) ควรมีแต่ผู้ที่เกี่ยวข้อง

ตารางที่ 3.2 (ต่อ)

51	CON3	ควรมีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ และควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม
ความตระหนักรู้ในการใช้มือถือ Mobile (MOB) (4 ข้อ)		
52	MOB1	ควรเปิดการใช้งาน PIN / Password, Face Scan หรือ Fingerprint
53	MOB2	การเข้าใช้งานอุปกรณ์ ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
54	MOB3	การกำหนด Application permission ให้เหมาะสม
55	MOB4	ควรมีการ Update Patch ระบบปฏิบัติการ (OS) และมีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
ความมั่นคงปลอดภัย Security (SEC) (4 ข้อ)		
56	SEC1	ควรมีการติดตั้งโปรแกรมป้องกัน Malware ในคอมพิวเตอร์ส่วนตัว
57	SEC2	ควรมีการป้องกันและตรวจสอบแหล่งที่มาของข้อมูลก่อนการกรอกข้อมูลส่วนตัว หรือคลิก Link ต่าง ๆ
58	SEC3	ควรหาทางวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กรจะถูกลักลอบเจาะเข้าสู่ระบบเพื่อแสวงประโยชน์
การส่งข้อความซึ่งเต็มไปด้วยความโกรธ Flaming (FLA) (4 ข้อ)		
59	FLA1	ไม่ควรกล่าวถึงหรือกล่าวหาผู้อื่นในทางเสียหายหรือทำให้ได้รับความอับอายในสื่อสังคมออนไลน์
60	FLA2	ไม่ควรใช้ข้อความหรือถ้อยคำที่หยาบคายในสื่อสังคมออนไลน์
61	FLA3	ไม่ควรล้อเลียนพฤติกรรม รูปร่างหน้าตาของผู้อื่นในสื่อสังคมออนไลน์
62	FLA4	ไม่ยั่วยุหรือปะทะคารมให้เกิดความเสียหายแก่ตนเองและผู้อื่นบนโลกออนไลน์
การคุกคามหรือล่วงละเมิด Harassment (HAR) (3 ข้อ)		
63	HAR1	ไม่ควรเผยแพร่ข่าวลือในด้านลบหรือข่าวเท็จของผู้อื่นผ่านทางสื่อสังคมออนไลน์
64	HAR2	ไม่ควรข่มขู่หรือใส่ร้ายผู้อื่นให้บุคคลที่สามเกลียดชังกันผ่านทางสื่อสังคมออนไลน์
65	HAR3	ไม่ควรนำภาพหรือคลิปวิดีโอของผู้อื่นที่จะก่อให้เกิดเสื่อมเสียไปเผยแพร่ผ่านทางสื่อสังคมออนไลน์
การปลอมตัวหรือแอบอ้าง Masquerading (MAS) (3 ข้อ)		
66	MAS1	ไม่ควรมีการปลอมแปลงชื่อหรือภาพของผู้อื่นเพื่อให้ร้ายบุคคลที่สามผ่านทางสื่อสังคมออนไลน์

ตารางที่ 3.2 (ต่อ)

67	MAS2	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นในการสนทนาผ่านทางสื่อสังคมออนไลน์
68	MAS	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อผลประโยชน์ให้ตนเองผ่านทางสื่อสังคมออนไลน์
การเผยแพร่ออกนอกกลุ่ม Outing (OUT) (3 ข้อ)		
69	OUT1	ไม่ควรนำชื่อบุพการีหรือญาติพี่น้องของผู้อื่นไปเปิดเผยผ่านทางสื่อสังคมออนไลน์โดยไม่ได้รับอนุญาต
70	OUT2	ไม่ควรนำที่อยู่หรือข้อมูลส่วนตัวของผู้อื่นไปเผยแพร่ผ่านทางสื่อสังคมออนไลน์โดยไม่ได้รับอนุญาต
71	OUT3	ไม่ควรนำเบอร์โทรศัพท์และข้อมูลการทำงานของผู้อื่นไปเผยแพร่ผ่านทางสื่อสังคมออนไลน์โดยไม่ได้รับอนุญาต
การกีดกัน Exclusion (EXC) (3 ข้อ)		
72	EXC1	ไม่ควรปิดกั้นหรือบล็อกข้อความสนทนาของบุคคลที่ไม่ชอบในกลุ่มสนทนาทางสื่อสังคมออนไลน์
73	EXC2	ไม่ควรกดดันหรือลบรายชื่อบุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางสื่อสังคมออนไลน์
74	EXC3	ไม่สร้างกลุ่มเฉพาะออกมาโจมตีบุคคลที่ไม่ชอบทางสื่อสังคมออนไลน์

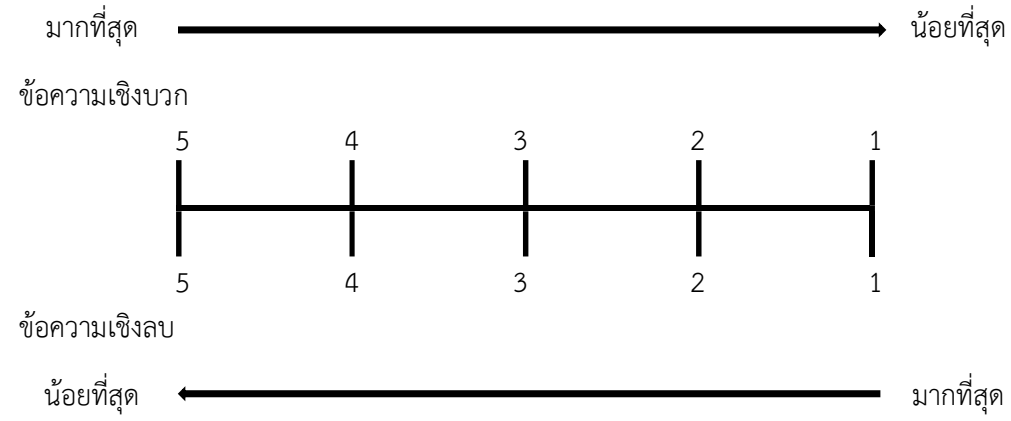
ตัวแปรและคำถามทั้งหมดที่นำมาศึกษาในการวิจัยนี้ ผู้วิจัยได้ศึกษาจากแนวคิด ทฤษฎี ซึ่งประกอบด้วยการใช้อินเทอร์เน็ตและระบบดิจิทัลในประเทศไทย,แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์, แนวคิดเกี่ยวกับการคุกคามทางไซเบอร์, แนวคิดเกี่ยวกับการกลั่นแกล้งทางไซเบอร์, แนวคิดเกี่ยวกับความตระหนักรู้ และงานวิจัยที่เกี่ยวข้อง ทั้งนี้ได้ปรึกษากับอาจารย์ที่ปรึกษาและมีการนำแบบสอบถามให้ผู้เชี่ยวชาญตรวจสอบค่า IOC เพื่อดูความสอดคล้องของตัวแปรกับวัตถุประสงค์การวิจัย ซึ่งสามารถแสดงความสัมพันธ์ระหว่างตัวแปรกับแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องได้ดังตารางที่ 3.3

ตารางที่ 3.3 ความสัมพันธ์ระหว่างตัวแปรที่ใช้กับทฤษฎีและงานวิจัยที่เกี่ยวข้อง

แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง	ตัวแปร
1. แนวคิดเกี่ยวกับการสร้างการตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์(Cybersecurity Awareness) 2. แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) 3. แนวคิดเกี่ยวกับการคุกคามทางไซเบอร์ (Cyber Threat) 4. แนวคิดเกี่ยวกับการกลั่นแกล้งทางไซเบอร์ (Cyber Bullying) 5. แนวคิดเกี่ยวกับความตระหนักรู้ (Awareness) 6. กรอบการรักษาความมั่นคงปลอดภัย (NIST Cybersecurity Framework) 7. อ้างอิงจากงานวิจัยของชนินทร เฉลิมทรัพย์, นาวาอากาศเอก. (2561) 8. อ้างอิงจากงานวิจัยของราชิต อรุณรังสี, พลตรี. (2561) 9. อ้างอิงจากงานวิจัยของณรงค์เวตย์ เรืองจวง, นาวาอากาศเอก. (2560) 10. อ้างอิงจากงานวิจัยของวิทยา จุลวัฒนานนท์. (2563) 11. อ้างอิงจากงานวิจัยของศุภวิชญ์ สาตราวาหะ, กีรติสรรพ์ ผลละออ และวิชากร ต่ายทอง. (2560) 12. อ้างอิงจากงานวิจัยของสุรพงศ์ ทรัพยาคม และ อรรถพล ป้อมสถิต. (2563) 13. อ้างอิงจากงานวิจัยของMichael Hanna. (2020)	ด้านพฤติกรรมการใช้อินเทอร์เน็ต
	ด้านพฤติกรรมการใช้งานสื่อสังคม
	ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์
	ด้านพฤติกรรมการใช้งานผ่านโปรแกรม
	ด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต
	ความตระหนักรู้ด้านการใช้คอมพิวเตอร์
	ความตระหนักรู้ด้านการใช้พาสเวิร์ด
	ความตระหนักรู้ด้านการใช้อีเมล
	ความตระหนักรู้ด้านการเข้าเว็บไซต์
	ความตระหนักรู้ด้านการใช้ Messaging
	ความตระหนักรู้เกี่ยวข่าวปลอมในโลกไซเบอร์
	ความตระหนักรู้ด้านการเก็บข้อมูลบนเครื่อง Server
	ความตระหนักรู้ด้านเข้าประชุมทางออนไลน์
	ความตระหนักรู้ในการใช้มือถือ
	ความมั่นคงปลอดภัย
	การส่งข้อความซึ่งเต็มไปด้วยความโกรธ
	การคุกคามหรือล่วงละเมิด
	การปลอมตัวหรือแอบอ้าง
	การเผยแพร่ออกนอกกลุ่ม
	การกีดกัน

เกณฑ์การให้คะแนน แบบสอบถามชุดที่ 1 ในส่วนที่ 2 และ ส่วนที่ 3 และแบบสอบถามชุดที่ 2 ในส่วนที่ 2 ส่วนที่ 3 และ ส่วนที่ 4 ใช้การประเมินให้คะแนนในลักษณะของการใช้มาตราส่วนประเมินค่า (Rating Scale) ของลิเคิร์ท (Likert Scale) ซึ่งเป็นมาตรวัดชนิดประมาณค่าจากค่าน้อยที่สุดถึงค่ามากที่สุด มาตรวัดแบบประมาณค่า คือ การวัดแบบจัดอันดับ ชนิด 5 ระดับ โดยมีระยะห่างระหว่างแต่ละจุดของสเกลจะมีค่าเท่ากัน โดยมีเกณฑ์ดังนี้

ระดับความตระหนักรู้	**คะแนน**
เห็นด้วยอย่างยิ่ง	5
เห็นด้วย	4
ไม่แน่ใจ	3
ไม่เห็นด้วย	2
ไม่เห็นด้วยอย่างยิ่ง	1



ภาพประกอบที่ 3.1 วิธีการประมาณค่าตามมาตรวัดของ Likert Scale

การคำนวณหาค่าพิสัยเพื่อจัดระยะห่างของช่วงชั้นออกเป็น 5 ระดับคือมากที่สุด มาก ปานกลาง น้อย และน้อยที่สุด ตามสมการดังนี้

$$\text{อันตรภาคชั้น} = \frac{\text{พิสัย}}{\text{จำนวนชั้น}}$$

$$= \frac{\text{คะแนนสูงสุด} - \text{คะแนนต่ำสุด}}{\text{จำนวนชั้น}}$$

$$\text{แทนค่าในสมการ} = \frac{\mathbf{5-1}}{\mathbf{5}}$$

$$= 0.8$$

การพิจารณาอันตรภาคชั้นของช่วงระดับคะแนน สามารถกำหนดระดับคะแนน ดังนี้

ค่าเฉลี่ย 4.21 – 5.00 หมายถึง มีระดับพฤติกรรม หรือ มีระดับความตระหนักรู้ มากที่สุด

ค่าเฉลี่ย 3.21 – 4.20 หมายถึง มีระดับพฤติกรรม หรือ มีระดับความตระหนักรู้ มาก

ค่าเฉลี่ย 2.61 – 3.40 หมายถึง มีระดับพฤติกรรม หรือ มีระดับความตระหนักรู้ ปานกลาง

ค่าเฉลี่ย 1.81 – 2.60 หมายถึง มีระดับพฤติกรรม หรือ มีระดับความตระหนักรู้ น้อย
ค่าเฉลี่ย 1.00 – 1.80 หมายถึง มีระดับพฤติกรรม หรือ มีระดับความตระหนักรู้ น้อยที่สุด

3.3.3 การตรวจสอบคุณภาพของแบบสอบถาม

3.3.3.1 การตรวจสอบค่าความเที่ยงตรง (Validity) โดยการสร้างแบบสอบถามฉบับร่างเสนอต่ออาจารย์ที่ปรึกษา เพื่อพิจารณาตรวจสอบความถูกต้องในเนื้อหา (Content validity) ทำการปรับปรุงแก้ไขแบบสอบถามตามข้อเสนอแนะของอาจารย์ที่ปรึกษา และตรวจสอบค่าความเที่ยงตรงตามเกณฑ์ที่เกี่ยวข้อง โดยนำแบบสอบถามไปให้ผู้ทรงคุณวุฒิตรวจสอบความเที่ยงตรงเพื่อวิเคราะห์หาค่าดัชนีความสอดคล้อง (Index of Item Objective Congruence : IOC) ของข้อคำถามกับวัตถุประสงค์ ซึ่งมีเกณฑ์การให้คะแนนข้อคำถาม ดังต่อไปนี้

แน่ใจว่ามีความสอดคล้องหรือวัดได้ มีระดับคะแนนเท่ากับ 1
ไม่แน่ใจว่ามีความสอดคล้องหรือวัดได้ มีระดับคะแนนเท่ากับ 0
แน่ใจว่าไม่มีความสอดคล้องหรือวัดได้ มีระดับคะแนนเท่ากับ -1

หลังจากนั้นนำแบบสอบถามที่ผู้ทรงคุณวุฒิประเมินความสอดคล้องแล้ว นำมาหาค่าดัชนีความสอดคล้องโดยใช้สมการ ดังนี้

$$IOC = \frac{\sum R}{n}$$

โดยที่ R คือ คะแนนของผู้ทรงคุณวุฒิ
$\sum R$ คือ ผลรวมของคะแนนผู้ทรงคุณวุฒิแต่ละคน
n คือ จำนวนผู้ทรงคุณวุฒิ

ในการพิจารณาความคิดเห็นของผู้ทรงคุณวุฒิ การหาค่าดัชนีความสอดคล้อง (IOC) ในทุกข้อคำถามนั้นต้องมีค่า IOC ตั้งแต่ 0.50 - 1.00 จึงจะถือว่าเกณฑ์มาตรฐานและสามารถนำข้อคำถามนั้นไปใช้สำรวจความคิดเห็นจากกลุ่มตัวอย่างได้ แต่หากว่าข้อคำถามใดที่มีค่า IOC ต่ำกว่า 0.50 จะต้องนำมาพิจารณาปรับปรุงข้อคำถามใหม่หรือจะตัดทิ้งก็ได้ตามความเหมาะสมและความคิดเห็นของอาจารย์ที่ปรึกษาในการวิจัย (ธีระ กุลสวัสดิ์ 2558) ในงานวิจัยนี้ได้รับความอนุเคราะห์จากผู้ทรงคุณวุฒิจำนวน 5 ท่าน ช่วยตรวจสอบเครื่องมือวิจัย ดังนี้

1. อาจารย์ สำราญ ไชยคำวัง
2. อาจารย์ บุญชม สุดจิตต์
3. นายเกรียงไกร ภูวณิชย์
4. นายเทพฤทธิ์ พระเทพ
5. นางสาววิรัลพัชร พรหมจรรย์

จากการหาค่าดัชนีความสอดคล้อง (IOC) จากผู้ทรงคุณวุฒิจำนวน 5 ท่าน พบว่ามีข้อคำถามจำนวน 4 ข้อคำถามที่มีค่า IOC ต่ำกว่า 0.50 ได้ปรึกษากับอาจารย์ที่ปรึกษาและผู้ทรงคุณวุฒิเป็นที่เรียบร้อยจึงได้ตัดข้อคำถามที่มีค่า IOC ต่ำกว่าเกณฑ์ทิ้งไป แล้วนำแบบสอบถามกระจายไปให้กลุ่มตัวอย่างได้ทำแบบสอบถาม

3.3.3.2 การตรวจสอบค่าความเชื่อมั่น (Reliability) นำแบบสอบถามที่ปรับปรุงแก้ไขแล้ว ทำการทดสอบ (Pre-Test) กับกลุ่มตัวอย่าง จำนวน 30 คน เพื่อทดสอบความเชื่อมั่นของแบบสอบถาม โดยสิ่งที่จะพิจารณาว่าผู้ตอบแบบสอบถามเข้าใจหรือไม่ มีปัญหาการตอบคำถามหรือไม่ และหลังจาก Pre-Test แล้ว พบว่าแบบสอบถามมีความน่าเชื่อถือ (Reliability) จึงนำไปใช้เป็นเครื่องมือในการเก็บรวบรวมข้อมูล การทดสอบหาค่าความเชื่อมั่นของแบบสอบถาม โดยวิธีหาค่าสัมประสิทธิ์อัลฟาของครอนบาช (Cronbach's Alpha Coefficient, 1990) ด้วยโปรแกรม SPSS ดังสมการดังนี้

$$\alpha = \left[\frac{n}{n-1}\right]\left[1 - \frac{\sum S_i^2}{S_t^2}\right]$$

โดย α คือ ค่าความสอดคล้องภายใน
n คือ จำนวนข้อคำถามในแบบสอบถาม
$\sum S_i^2$ คือ ผลร่วมของความแปรปรวนของคะแนนรายข้อ
S_t^2 คือ ความแปรปรวนของคะแนนรวมทั้งฉบับ
ซึ่งค่า α ต้องมีค่ามากกว่า 0.7 ขึ้นไป

จากการตรวจสอบค่าความเชื่อมั่นของแบบสอบถาม ผู้วิจัยแสดงค่าความเชื่อมั่นของแบบสอบถามงานวิจัยนี้ไว้ตามตารางที่ 3.4

ตารางที่ 3.4 แสดงผลค่าความเชื่อมั่นของแบบสอบถาม (Reliability)

ตัวแปร	จำนวนข้อคำถาม	ค่า Cronbach's Alpha
ด้านพฤติกรรมการใช้อินเทอร์เน็ต Internet (INT)	5 ข้อ	0.883
ด้านพฤติกรรมการใช้งานสื่อสังคม Social (SCL)	3 ข้อ	0.916
ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์ On-Line (ONL)	4 ข้อ	0.814
ด้านพฤติกรรมการใช้งานผ่านโปรแกรม Program (PRG)	4 ข้อ	0.885
ด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต Cyber Treat (CST)	4 ข้อ	0.905
ความตระหนักรู้ด้านการใช้คอมพิวเตอร์ Computer (COM)	5 ข้อ	0.860
ความตระหนักรู้ด้านการใช้พาสเวิร์ด Password (PWD)	5 ข้อ	0.887
ความตระหนักรู้ด้านการใช้อีเมล E-mail (EML)	4 ข้อ	0.920

ตารางที่ 3.4 (ต่อ)

ความตระหนักรู้ด้านการเข้าเว็บไซต์ Website (WEB)	4 ข้อ	0.873
ความตระหนักรู้ด้านการใช้ Messaging (MSG)	3 ข้อ	0.886
ความตระหนักรู้เกี่ยวข่าวปลอมในโลกไซเบอร์ Fake News (FAK)	2 ข้อ	0.936
ความตระหนักรู้ด้านการเก็บข้อมูลบนเครื่อง Server Cloud Storage (CLD)	3 ข้อ	0.909
ความตระหนักรู้ด้านเข้าประชุมทางออนไลน์ Conference (CON)	3 ข้อ	0.781
ความตระหนักรู้ในการใช้มือถือ Mobile (MOB)	4 ข้อ	0.873
ความมั่นคงปลอดภัย Security (SEC)	3 ข้อ	0.919
การส่งข้อความซึ่งเต็มไปด้วยความโกรธ Flaming (FLA)	4 ข้อ	0.949
การคุกคามหรือล่วงละเมิด Harassment (HAR)	3 ข้อ	0.963
การปลอมตัว Masquerading แอบอ้าง (MAS)	3 ข้อ	0.958
การเผยแพร่ออกนอกกลุ่ม Outing (OUT)	3 ข้อ	0.934
การกีดกัน Exclusion (EXC)	3 ข้อ	0.852

จากตารางแสดงความเชื่อมั่น (Reliability) พบว่า ด้านพฤติกรรมการใช้อินเทอร์เน็ต Internet (INT) จำนวน 5 ข้อ มีค่า Cronbach’s Alpha 0.883 ด้านพฤติกรรมการใช้งานสื่อสังคม Social (SCL) จำนวน 3 ข้อ มีค่า Cronbach’s Alpha 0.916 ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์ On-Line (ONL) จำนวน 4 ข้อ มีค่า Cronbach’s Alpha 0.814 ด้านพฤติกรรมการใช้งานผ่านโปรแกรม Program (PRG) จำนวน 4 ข้อ มีค่า Cronbach’s Alpha 0.885 ด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต Cyber Treat (CST) จำนวน 4 ข้อ มีค่า Cronbach’s Alpha 0.905 ความตระหนักรู้ด้านการใช้คอมพิวเตอร์ Computer (COM) จำนวน 5 ข้อ มีค่า Cronbach’s Alpha 0.860 ความตระหนักรู้ด้านการใช้พาสเวิร์ด Password (PWD) จำนวน 5 ข้อ มีค่า Cronbach’s Alpha 0.887 ความตระหนักรู้ด้านการใช้อีเมล E-mail (EML) จำนวน 4 ข้อ มีค่า Cronbach’s Alpha 0.920 ความตระหนักรู้ด้านการเข้าเว็บไซต์ Website (WEB) จำนวน 4 ข้อ มีค่า Cronbach’s Alpha 0.873 ความตระหนักรู้ด้านการใช้ Messaging (MSG) จำนวน 3 ข้อ มีค่า Cronbach’s Alpha 0.886 ความตระหนักรู้เกี่ยวข่าวปลอมในโลกไซเบอร์ Fake News (FAK) จำนวน 2 ข้อ มีค่า Cronbach’s Alpha 0.936 ความตระหนักรู้ด้านการเก็บข้อมูลบนเครื่อง Server Cloud Storage (CLD) จำนวน 3 ข้อ มีค่า Cronbach’s Alpha 0.909 ความตระหนักรู้ด้านเข้าประชุมทางออนไลน์ Conference (CON) จำนวน 3 ข้อ มีค่า Cronbach’s Alpha 0.781 ความตระหนักรู้ในการใช้มือถือ Mobile (MOB) จำนวน 4 ข้อ มีค่า Cronbach’s Alpha 0.873 ความมั่นคงปลอดภัย Security (SEC) จำนวน 3 ข้อ มีค่า Cronbach’s Alpha 0.919 การส่งข้อความซึ่งเต็มไปด้วยความโกรธ Flaming (FLA) จำนวน 4 ข้อ มีค่า Cronbach’s Alpha 0.949 การคุกคาม

หรือล่วงละเมิด Harassment (HAR) จำนวน 3 ข้อ มีค่า Cronbach's Alpha 0.963 การปลอมตัว Masquerading แอบอ้าง (MAS) จำนวน 3 ข้อ มีค่า Cronbach's Alpha 0.958 การเผยแพร่ออกนอกกลุ่ม Outing (OUT) จำนวน 3 ข้อ มีค่า Cronbach's Alpha 0.934 การกีดกัน Exclusion (EXC) จำนวน 3 ข้อ มีค่า Cronbach's Alpha 0.852 ซึ่งปัจจัยทุกด้านมีค่ามากกว่า 0.700 จึงสรุปได้ว่าปัจจัยทั้งหมดนี้มีค่าความเชื่อมั่น (Reliability) ตามสถิติ

3.3.4 อุปกรณ์ที่ใช้ในการวิจัย

3.3.4.1 Hardware : Notebook

3.3.4.2 Software : Microsoft Office, Google Forms, Google Spreadsheet, และโปรแกรม SPSS

3.4 การวิเคราะห์ข้อมูล

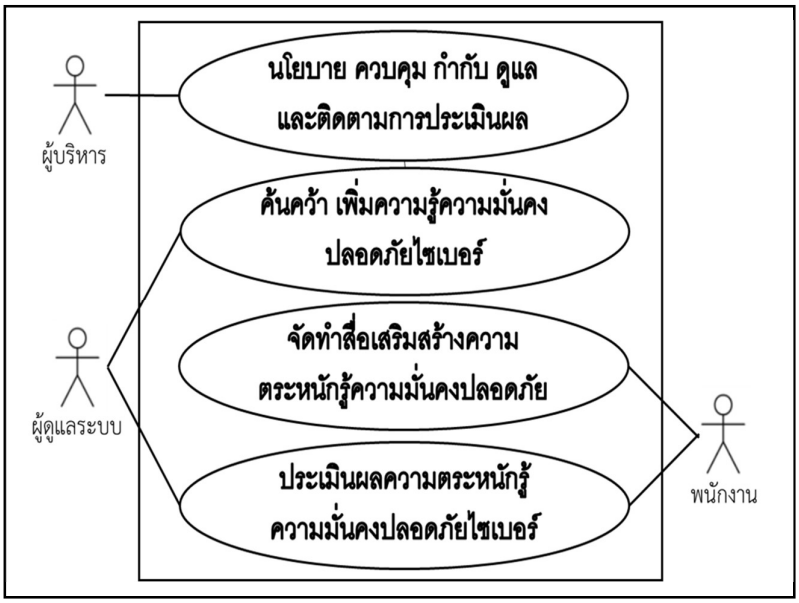
การวิเคราะห์ข้อมูลการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้างจากผู้บริหารระดับสูง ในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด จะใช้การสรุปประเด็นสำคัญจากผู้ให้ข้อมูลที่มีประสบการณ์ในการทำงานด้านเทคโนโลยีดิจิทัลหรือทำงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และนำข้อมูลมาเปรียบเทียบเพื่อหาข้อสรุป

การวิเคราะห์ข้อมูลเชิงปริมาณ เป็นการนำแบบสอบถาม โดยใช้ระบบแบบสอบถามออนไลน์เพื่อตอบคำถามต่าง ๆ ที่ได้กำหนดขึ้น แล้วนำผลมาวิเคราะห์และประมวลผลทางสถิติ ทดสอบหาความสัมพันธ์โดยใช้ Independent Samples T Test / Oneway ANOVA และ Pearson Correlation ด้วยโปรแกรมสำเร็จรูป SPSS และอธิบายค่าของข้อมูลเชิงพรรณนา โดยแจกแจงความถี่ (Frequency) แบบค่าร้อยละ (Percentage) แบบคำนวณค่าเฉลี่ย (Mean) และแบบค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) เพื่อวิเคราะห์หาข้อสรุปต่อไป

3.5 การวิเคราะห์ ออกแบบและพัฒนาแอปพลิเคชัน

การดำเนินการตามวัตถุประสงค์ข้อที่ 3 เพื่อพัฒนาแอปพลิเคชันสำหรับประเมินความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์สำหรับสำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ผู้วิจัยได้ผลจากการสัมภาษณ์เชิงลึกกับผู้บริหารและผู้เชี่ยวชาญด้านระบบสารสนเทศ ระบุให้มีรูปแบบการเรียนรู้ในรูปแบบออนไลน์ โดยให้จัดทำในรูปแบบของ Web Application ติดตั้งใช้งานภายในระบบอินทราเน็ตขององค์กร ซึ่งสอดคล้องกับผลวิจัยของ A. Alarifi, H. Tootell, P. Hyland, (2012) ที่ได้ทำวิจัยเรื่อง "A Study of Information Security Awareness and Practices in Saudi Arabia" ศึกษาเรื่องรูปแบบการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยแก่ประชาชนในประเทศ Saudi Arabia ที่ผลวิจัยพบว่ารูปแบบที่มีประสิทธิภาพสูงที่สุดคือ Web portals ซึ่งเป็นรูปแบบการสร้างความตระหนักรู้ที่เหมาะสมสามารถเข้าใช้งานได้ง่าย ทุกที่ ทุกเวลา และยังสามารถปรับแต่งเนื้อหาให้ทันสมัยได้ง่ายและสะดวกด้วย จึงได้พัฒนาดิจิทัลแพลตฟอร์มเพื่อการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด โดยใช้วงจรการพัฒนาระบบงาน (Software Development Life Cycle : SDLC) ดังนี้

1. การกำหนดปัญหา (Problem Definition) ทำการศึกษาแนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง รวบรวมข้อมูลจากการสัมภาษณ์เชิงลึกกับผู้บริหารและผู้เชี่ยวชาญด้านระบบสารสนเทศของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด และข้อมูลจากแบบสอบถามปลายปิดจากกลุ่มตัวอย่าง ทำให้ทราบถึงพฤติกรรมการใช้งานระบบอินเทอร์เน็ตและกำหนดแนวทางการเสริมสร้างความตระหนักรู้และการพัฒนาแอปพลิเคชันประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด
2. การวิเคราะห์ปัญหา (Analysis) นำข้อมูลที่ได้จากขั้นตอนแรก การกำหนดปัญหามาทำการวิเคราะห์ เพื่อเตรียมความพร้อมในการออกแบบระบบและกำหนดรายละเอียดต่าง ๆ
3. การออกแบบ (Design) ผู้วิจัยได้นำผลจากการวิเคราะห์ มาออกแบบแนวทางการเสริมสร้างความตระหนักรู้และพัฒนาแอปพลิเคชันประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ต่อไป ดังภาพประกอบที่ 3.2



ภาพประกอบที่ 3.2 Use Case Diagram การเสริมสร้างและประเมินผลระดับความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

4. การพัฒนาระบบงาน (Development) หรือการสร้างระบบงานจริง ผู้วิจัยได้จัดทำ Web Application บนดิจิทัลแพลตฟอร์ม AEROTHAI Learning Management System (AEROTHAI LMS) ภายในเครือข่ายอินทราเน็ตของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

5. การทดสอบ (Testing) ทดสอบระบบจะเป็นการตรวจสอบความถูกต้องของระบบงานที่ถูกสร้างขึ้นมาว่าตรงตามกับความต้องการจริง ๆ หรือไม่ ก่อนที่จะทำการเปิดระบบให้ใช้งานจริงต่อไป
6. การติดตั้ง (Implementation) นำแอปพลิเคชันไปใช้งานจริง
7. การบำรุงรักษา (Maintenance) การปรับปรุงแก้ไขแอปพลิเคชันให้เหมาะสมกับการใช้งานตามรอบระยะเวลาทุก 6 เดือน หรือปรับปรุงข้อมูลให้ทันสถานการณ์อย่างสม่ำเสมอ

โดยการทำดิจิทัลแพลตฟอร์มการเสริมสร้างและประเมินผลระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด มีการติดตั้งภายในระบบ Intranet ของบริษัทวิทยุการบินแห่งประเทศไทยจำกัด ด้วยแพลตฟอร์ม Learning Management System (LMS) เป็นแพลตฟอร์มสำหรับการเรียนรู้ออนไลน์ เป็นระบบและบริการการเรียนทางอิเล็กทรอนิกส์ สนับสนุนการเรียนรู้ซึ่งมีเป้าหมายที่จะพัฒนาบุคลากรให้มีประสิทธิภาพในการทำงานเพิ่มมากขึ้น ทุกคนในองค์กรสามารถเข้าถึงคอร์สเรียนต่าง ๆ และนั่งเรียนได้ทุกที่ทุกเวลา

3.6 ระยะเวลาในการดำเนินงาน

ระยะเวลาในการดำเนินงาน ภายใน 1 ปี (กันยายน 2564 - สิงหาคม 2565) มีรายละเอียดดังตารางที่ 3.5

ตารางที่ 3.5 ระยะเวลาในการดำเนินงาน

ขั้นตอนการดำเนินงาน	พ.ศ. 2564				พ.ศ. 2565							
	ก.ย	ต.ค	พ.ย	ธ.ค	ม.ค	ก.พ	มี.ค	เม.ย	พ.ค	มิ.ย	ก.ค	ส.ค
1. กำหนดขอบเขตและวางแผน												
2. ศึกษาทฤษฎีที่เกี่ยวข้องและเครื่องมือที่ใช้												
3. สอบหัวข้อและโครงร่าง												
4. วิเคราะห์และออกแบบระบบ												
5. การพัฒนาและทดสอบระบบ												
6. ทดสอบแก้ไขข้อผิดพลาดการดำเนินงาน												
7. จัดทำรูปเล่มสารนิพนธ์ตามรูปแบบที่บัณฑิตวิทยาลัยกำหนด												
8. นำเสนอผลงานต่อคณะกรรมการ												
9. นำส่งรูปเล่มฉบับสมบูรณ์												

3.7 สรุป

ในบทที่ 3 เป็นการนำเสนอระเบียบวิธีวิจัยเป็นขั้นตอนการวิจัย ประกอบด้วย ประชากรและกลุ่มตัวอย่าง การเก็บรวบรวมข้อมูล เครื่องมือที่ใช้ในการวิจัย การวิเคราะห์ข้อมูล การวิเคราะห์ข้อมูลออกแบบ และพัฒนาแอปพลิเคชัน ระยะเวลาในการดำเนินงาน เพื่อตอบคำถามตามวัตถุประสงค์และสมมติฐานที่ได้กำหนดไว้ ซึ่งผู้วิจัยจะได้นำเสนอผลการวิจัยในบทที่ 4 ต่อไป

บทที่ 4

ผลการวิจัย

งานวิจัยเรื่อง“การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด” การวิจัยนี้ มุ่งเน้นศึกษา วิเคราะห์ ระดับความตระหนักรู้และความเข้าใจของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด เกี่ยวกับด้านความเสี่ยงต่อภัยคุกคามทางไซเบอร์หรือไม่อย่างไร เป็นงานวิจัยแบบผสมผสาน (Mixed Method) คือเป็นการวิจัยเชิงคุณภาพ (Qualitative Research) และการวิจัยเชิงปริมาณ (Quantitative Research โดยการจัดทำแบบสัมภาษณ์เชิงลึกกับกับผู้ทรงคุณวุฒิที่เป็นผู้บริหารและผู้รับผิดชอบงานด้านไซเบอร์ และทำแบบสอบถามแบบปลายปิด (Close-end Questionnaire) และ เก็บรวบรวมข้อมูลจากบุคลากรกลุ่มตัวอย่างในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด เป็นผู้ตอบคำถามเอง (Self-Administered) และทำการวิเคราะห์ข้อมูลและพัฒนาระบบแอปพลิเคชันสำหรับการเสริมสร้างและประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ โดยใช้วงจรการพัฒนาระบบงาน (Software Development Life Cycle : SDLC) นำข้อมูลทั้งหมดมาทำการศึกษาวิเคราะห์ ตามวัตถุประสงค์ของการวิจัย คือ 1) เพื่อศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ 2) เพื่อพัฒนาแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์ 3) เพื่อจัดทำแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ซึ่ง ผู้วิจัยได้แบ่งขั้นตอนในการนำเสนอผลการวิเคราะห์ข้อมูลออกเป็นดังนี้

4.1 ผลการวิจัยเพื่อตอบวัตถุประสงค์ข้อที่ 1

4.2 ผลการวิจัยเพื่อตอบวัตถุประสงค์ข้อที่ 2

4.3 ผลการวิจัยเพื่อตอบวัตถุประสงค์ข้อที่ 3

4.4 สรุป

4.1 ผลการวิจัยเพื่อตอบวัตถุประสงค์ข้อที่ 1

เพื่อศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

4.1.1 ผลการวิเคราะห์เนื้อหาจากการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้าง

ผู้วิจัยได้ศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ด้วยการเก็บรวบรวมข้อมูลด้วยการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้างจากผู้บริหารระดับสูง ในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ได้แสดงไว้ในตารางที่ 4.1

ตารางที่ 4.1 ผลการวิเคราะห์เนื้อหาจากการสัมภาษณ์แบบเชิงลึก

ข้อคำถามสัมภาษณ์	ข้อมูลสัมภาษณ์
ความเสี่ยงด้านไซเบอร์ในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด	1. เป็นความเสี่ยงที่ต้องพึงระวังเป็นอย่างสูง 2. มีความเสี่ยงด้านภัยคุกคามจากคนในองค์กรที่ได้รับอนุญาตในการเข้าถึงข้อมูลที่เป็นความลับ 3. การนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กรในช่วงการระบาดของไวรัส COVID-19 ส่งผลให้องค์กรต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มากขึ้น
ภัยคุกคามทางไซเบอร์ที่มีในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด	1. ระบบคอมพิวเตอร์ที่ให้บริการส่วนใหญ่จะเป็นระบบปิด แต่ก็อาจมีการทะลุทะลวงเข้าไปยังเครือข่ายหลักของวิทยุการบินได้ 2. พนักงานยังขาดความเข้าใจในภัยคุกคามทางไซเบอร์และการระวังป้องกัน 3. กฎหมายยังไม่ครอบคลุมและไม่ทันสมัยเพียงพอ 4. ควรจัดทำนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ 5. ประเด็นที่น่าเป็นห่วง คือ Hacking at home จากการใช้อุปกรณ์ที่เชื่อมต่อกับอินเทอร์เน็ตเพื่อทำงานของแต่ละคน 6. ในองค์กรถือว่ามีความพร้อมในเชิงป้องกัน แต่ต้องระมัดระวัง Insider threat คือภัยที่เกิดจากภายในบุคลากร
บุคลากรมีความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์มากน้อยแค่ไหน อย่างไร	1. ปัจจุบันบุคลากรวิทยุการบินฯ มีความตระหนักรู้และเข้าใจเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์มากขึ้น เพราะมีการเข้ารับการอบรมเนื้อหาเกี่ยวกับ Digital Literacy 2. ผู้ใช้บริการยังขาดความเข้าใจ 3. บริษัทฯ ยังไม่ได้ประเมินความรู้ความตระหนักรู้ของพนักงานในภาพรวม

ตารางที่ 4.1 (ต่อ)

บุคลากรรู้เท่าทัน สามารถปกป้องตนเองและหน่วยงานไม่ให้ตกเป็นเหยื่อภัยทางไซเบอร์ ได้หรือไม่	1. บุคลากรส่วนใหญ่ประมาณ 70% มีความรู้ในระดับสูงพอประมาณ และมีการ Warning จากผู้เกี่ยวข้องด้านไซเบอร์อย่างสม่ำเสมอ สามารถรู้เท่าทันและป้องกันตนเองและหน่วยงานได้
แนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ควรเป็นอย่างไร	1. ควรใช้วิธีการเรียนรู้แบบออนไลน์และวิธีการเรียนโดยใช้วีดิทัศน์ผสมผสานกัน
เนื้อหาของการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ควรเป็นอย่างไร	ผู้บริหารระดับสูงส่วนใหญ่เรียงลำดับเรื่องที่สำคัญ ดังนี้ 1. ด้านการจัดการข้อมูลส่วนตัว 2. ด้านการจัดการรหัสผ่าน 3. ด้านการใช้งานอินเทอร์เน็ต 4. ด้านการใช้งานโซเชียลมีเดีย 5. ด้านการใช้อีเมล 6. ซอฟต์แวร์ประสงค์ร้าย 7. ซอฟต์แวร์เรียกค่าไถ่ 8. การหลอกลวงทางอินเทอร์เน็ตหรือฟิชชิง และ 9. เงินตราเข้ารหัสลับหรือคริปโทเคอร์เรนซี
ปัจจัยความสำเร็จต่อการการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ควรมีอะไรบ้าง	1. วัฒนธรรมด้านการเรียนรู้ทางดิจิทัล 2. การตระหนักถึงความเสี่ยงที่จะมาทางเครือข่ายคอมพิวเตอร์ 3. ฝ่ายบริหารและฝ่าย IT ต้องคอยควบคุมการใช้เทคโนโลยีดิจิทัล 4. ควรพิจารณาตามกรอบดัชนีตัวชี้วัดตาม ITU 5. การบริหารจัดการให้เป็นระบบ มีการจำลอง สถานการณ์ใหม่ ๆ 6. การมีระบบสื่อสารในสังคมกลุ่มย่อยในระดับหน่วยงาน 7. การสื่อสารประชาสัมพันธ์ให้พนักงานรับรู้ต้องรวดเร็ว 8. การประเมินติดตามผลอย่างสม่ำเสมอ

จากตารางที่ 4.1 ผลการวิเคราะห์เนื้อหาจากการสัมภาษณ์แบบเชิงลึก พบว่า ความเสี่ยงด้านไซเบอร์ในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด การนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กรในช่วงการระบาดของไวรัส COVID-19 ส่งผลให้บริษัทวิทยุการบินฯ ต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มากขึ้น การที่พนักงานยังขาดความเข้าใจในภัยคุกคามทางไซเบอร์และการระวังป้องกัน เป็นประเด็นที่น่าห่วงจากการ Hacking at home จากการใช้อุปกรณ์ที่เชื่อมต่อกับอินเทอร์เน็ตเพื่อทำงานของแต่ละคน คือ ภัยคุกคามทางไซเบอร์ที่มีในบริษัทวิทยุการบินฯ ซึ่งบริษัทวิทยุการบินฯ ถือว่ามีความพร้อมในเชิงป้องกัน แต่คงต้องระมัดระวัง Insider threat คือภัยที่เกิดจากภายในบุคลากรภายในบริษัทวิทยุการบินฯ ปัจจุบันบุคลากรวิทยุการบินฯ มีความตระหนักรู้และเข้าใจเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์มากขึ้น แต่ยังไม่ได้ประเมินความรู้ความตระหนักรู้ของพนักงาน บุคลากรส่วนใหญ่ประมาณ 70% มีความรู้ในระดับสูงพอประมาณและมีการ Warning จากผู้เกี่ยวข้องด้านไซเบอร์อย่างสม่ำเสมอ สามารถรู้เท่าทันและป้องกันตนเองและหน่วยงานได้ มีการระบุการสร้างเสริมความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ด้วยวิธีการเรียนรู้แบบออนไลน์และวิธีการเรียนโดยใช้วีดิทัศน์ผสมผสานกัน

4.1.2 ผลการวัดระดับความตระหนักรู้ก่อนการสร้างความตระหนักรู้

ผู้วิจัยได้ใช้แบบสอบถามชุดที่ 1 ซึ่งประกอบด้วยตัวแปร 14 ตัว ดังนี้ 1) พฤติกรรมการใช้อินเทอร์เน็ต 2) พฤติกรรมการใช้งานสื่อสังคม 3) พฤติกรรมการเข้าถึงสื่อออนไลน์ 4) พฤติกรรมการใช้งานผ่านโปรแกรม 5) พฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต 6) ความตระหนักรู้ด้านการใช้คอมพิวเตอร์ 7) ความตระหนักรู้ด้านการใช้พาสเวิร์ด 8) ความตระหนักรู้ด้านการใช้อีเมล 9) ความตระหนักรู้ด้านการเข้าเว็บไซต์ 10) ความตระหนักรู้ด้านการใช้ Messaging 11) ความตระหนักรู้เกี่ยวข่าวปลอมในโลกไซเบอร์ 12) ความตระหนักรู้ด้านการเก็บข้อมูลบนเครื่อง Server 13) ความตระหนักรู้ด้านเข้าประชุมทางออนไลน์ และ 14) ความตระหนักรู้ในการใช้มือถือ เพื่อทำการเก็บรวบรวมข้อมูลระดับพฤติกรรมและระดับความตระหนักรู้ ตามวัตถุประสงค์ ข้อที่ 1 “เพื่อศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์” และเพื่อยืนยันสมมติฐาน ข้อที่ 1 “พฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อยู่ในระดับมาก” จากการเก็บรวบรวมข้อมูลจากบุคลากรกลุ่มตัวอย่างในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด จำนวน 55 คน เป็นผู้ตอบคำถามเอง (Self-Administered) ได้ผลดังนี้

4.1.2.1 ข้อมูลทั่วไปบุคลากรของกลุ่มตัวอย่าง ประกอบด้วย เพศ อายุ ระดับการศึกษาสูงสุด สายงานที่ปฏิบัติ อายุงาน และระยะเวลาโดยฉลี่ยที่ใช้งานคอมพิวเตอร์ ในแต่ละวันของเวลาทำงาน แสดงผลไว้ในตารางที่ 4.2

ตารางที่ 4.2 แสดงผลข้อมูลทั่วไปของกลุ่มตัวอย่าง

เพศ	**จำนวน (คน)**	**ร้อยละ**
ชาย	37	67.3
หญิง	18	32.7
รวม	**55**	**100.0**

อายุ	**จำนวน (คน)**	**ร้อยละ**
ต่ำกว่า 30 ปี	3	5.5
30 – 40 ปี	8	14.5
41 – 50 ปี	13	23.6
51 – 60 ปี	31	56.4
61 ปีขึ้นไป	0	0.0
รวม	**55**	**100**

ตารางที่ 4.2 (ต่อ)

ระดับการศึกษาสูงสุด	จำนวน (คน)	ร้อยละ
ต่ำกว่าปริญญาตรี	1	1.8
ปริญญาตรี	26	47.3
ปริญญาโท	27	49.1
ปริญญาเอก	1	1.8
รวม	**55**	**100**

สายงานที่ปฏิบัติงาน	จำนวน (คน)	ร้อยละ
ด้านปฏิบัติการ	14	25.5
ด้านวิศวกรรม	32	58.2
ด้านธุรการ	5	9.1
ด้านอื่น ๆ	4	7.3
รวม	**55**	**100**

อายุงาน	จำนวน (คน)	ร้อยละ
ไม่เกิน 5 ปี	3	5.5
6 – 10 ปี	4	7.3
11 – 15 ปี	10	18.2
16 ปีขึ้นไป	38	69.1
รวม	**55**	**100**

ระยะเวลาโดยฉลี่ยที่ใช้งานในแต่ละวัน	จำนวน (คน)	ร้อยละ
น้อยกว่า 1 ชั่วโมงต่อวัน	3	5.4
1 – 3 ชั่วโมงต่อวัน	15	27.3
4 – 6 ชั่วโมงต่อวัน	20	36.4
มากกว่า 6 ชั่วโมงต่อวัน	17	30.9
รวม	**55**	**100**

จากตารางที่ 4.2 พบว่ากลุ่มตัวอย่าง ส่วนมากเป็นเพศชาย จำนวน 37 คน คิดเป็นร้อยละ 67.3 และเป็นเพศหญิง จำนวน 18 คน คิดเป็นร้อยละ 32.7 ตามลำดับ

กลุ่มตัวอย่าง ส่วนมากมีอายุ 51 – 60 ปี จำนวน 31 คน คิดเป็นร้อยละ 56.4 อายุ 41 – 50 ปี จำนวน 13 คน คิดเป็นร้อยละ 23.6 อายุ 30 – 40 ปี จำนวน 8 คน คิดเป็นร้อยละ 14.5 อายุต่ำกว่า 30 ปี จำนวน 3 คน คิดเป็นร้อยละ 5.5 และอายุ 61 ปีขึ้นไป ไม่มีผู้ตอบแบบสอบถาม ตามลำดับ

กลุ่มตัวอย่าง ส่วนมากมีระดับการศึกษา ปริญญาโท จำนวน 27 คน คิดเป็นร้อยละ 49.1 ปริญญาตรี จำนวน 26 คน คิดเป็นร้อยละ 47.3 ต่ำกว่าปริญญาตรี จำนวน 1 คน คิดเป็นร้อยละ 1.8 และปริญญาเอก จำนวน 1 คน คิดเป็นร้อยละ 1.8 ตามลำดับ

กลุ่มตัวอย่าง ส่วนมากปฏิบัติงานด้านวิศวกรรม จำนวน 32 คน คิดเป็นร้อยละ 58.2 ปฏิบัติงานด้านปฏิบัติการ จำนวน 14 คน คิดเป็นร้อยละ 25.2 ปฏิบัติงานด้านธุรการ จำนวน 5 คน คิดเป็นร้อยละ 9.1 และปฏิบัติงานด้านอื่น ๆ จำนวน 4 คน คิดเป็นร้อยละ 7.3 ตามลำดับ

กลุ่มตัวอย่าง ส่วนมากมีอายุงาน 16 ปีขึ้นไป จำนวน 38 คน คิดเป็นร้อยละ 69.1 อายุงาน 11-15 ปี จำนวน 10 คน คิดเป็นร้อยละ 18.2 อายุงาน 6-10 ปี จำนวน 4 คน คิดเป็นร้อยละ 7.3 และอายุงานไม่เกิน 5 ปี จำนวน 3 คน คิดเป็นร้อยละ 5.5 ตามลำดับ

กลุ่มตัวอย่าง ส่วนมากใช้งานคอมพิวเตอร์ ในแต่ละวันของเวลาทำงาน มีระยะเวลาโดยฉลี่ย 4-6 ชั่วโมงต่อวัน จำนวน 20 คน คิดเป็นร้อยละ 36.4 มีระยะเวลาโดยฉลี่ย มากกว่า 6 ชั่วโมงต่อวัน จำนวน 17 คน คิดเป็นร้อยละ 30.9 มีระยะเวลาโดยฉลี่ย 1-3 ชั่วโมงต่อวัน จำนวน 15 คน คิดเป็นร้อยละ 27.3 และมีระยะเวลาโดยฉลี่ย น้อยกว่า 1 ชั่วโมงต่อวัน จำนวน 3 คน คิดเป็นร้อยละ 5.4 ตามลำดับ

4.1.2.2 พฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง ประกอบด้วย ด้านพฤติกรรมการใช้อินเทอร์เน็ต ด้านพฤติกรรมการใช้งานสื่อสังคม ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์ ด้านพฤติกรรมการใช้งานผ่านโปรแกรมด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต แสดงผลไว้ในตารางที่ 4.3

ตารางที่ 4.3 แสดงผลระดับพฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง

รายการประเมิน	$\overline{X}$	S.D.	แปลผล
1. การใช้อินเทอร์เน็ต	4.20	0.57	มาก
2. การใช้งานสื่อสังคม	4.49	0.39	มากที่สุด
3. การเข้าถึงสื่อออนไลน์	3.93	0.29	มาก
4. การใช้งานผ่านโปรแกรม	4.03	0.45	มาก
5. การป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต	4.25	0.37	มากที่สุด
ค่าเฉลี่ยโดยรวม	**4.18**	**0.41**	**มาก**

จากตารางที่ 4.3 พบว่ากลุ่มตัวอย่าง มีผลการประเมินระดับพฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่างมีค่าอยู่ในระดับมาก ($\overline{X}$ = 4.18)

4.1.2.3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง ประกอบด้วย ความตระหนักรู้ด้านการใช้คอมพิวเตอร์ (Computer) ความตระหนักรู้ด้านการใช้พาสเวิร์ด (Password) ความตระหนักรู้ด้าน

การใช้อีเมล (E-mail) ความตระหนักรู้ด้านการเข้าเว็บไซต์ (Website) ความตระหนักรู้ด้านการใช้ Messaging ความตระหนักรู้เกี่ยวข่าวปลอมในโลกไซเบอร์ (Fake News) ความตระหนักรู้ด้านการเก็บข้อมูลบนเครื่อง Server (Cloud Storage) ความตระหนักรู้ด้านเข้าประชุมทางออนไลน์ (Conference) ความตระหนักรู้ในการใช้มือถือ (Mobile) แสดงผลไว้ในตารางที่ 4.4

ตารางที่ 4.4 แสดงผลระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง

รายการประเมิน	$\overline{X}$	S.D.	แปลผล
1. ด้านการใช้คอมพิวเตอร์ (Computer)	4.41	0.57	มากที่สุด
2. ด้านการใช้พาสเวิร์ด (Password)	4.07	0.39	มาก
3. ด้านการใช้อีเมล (E-mail)	4.20	0.29	มาก
4. ด้านการเข้าเว็บไซต์ (Website)	4.03	0.45	มาก
5. ด้านการใช้ (Messaging)	4.31	0.37	มากที่สุด
6. เกี่ยวข่าวปลอมในโลกไซเบอร์ (Fake News)	4.09	0.48	มาก
7. ด้านการเก็บข้อมูลบนเครื่อง Server (Cloud Storage)	4.17	0.51	มาก
8. ด้านเข้าประชุมทางออนไลน์ (Conference)	4.25	0.52	มากที่สุด
9. การใช้มือถือ (Mobile)	4.25	0.49	มากที่สุด
ค่าเฉลี่ยโดยรวม	**4.20**	**0.45**	**มาก**

จากตารางที่ 4.4 พบว่ากลุ่มตัวอย่าง มีผลการการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง มีค่าอยู่ในระดับมาก ($\overline{X}$ = 4.20)

4.2 ผลการวิจัยเพื่อตอบวัตถุประสงค์ข้อที่ 2

เพื่อพัฒนาแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์

ผลจากการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้างจากผู้บริหารระดับสูง ในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด และจากการเก็บรวบรวมข้อมูลจากบุคลากรกลุ่มตัวอย่างในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด จำนวน 55 คน พบว่า แนวทางการเสริมสร้างความตระหนักรู้ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์ ที่เหมาะสมกับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด มากที่สุดคือวิธีการเรียนรู้แบบออนไลน์และวิธีการเรียนโดยใช้วีดิทัศน์ผสมผสานกัน ผู้วิจัยจึงได้เสนอแนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ในรูปแบบของ Web Application ที่ติดตั้งบนแพลตฟอร์ม AEROTHAI Learning Management System (LMS) ซึ่งได้ให้ผู้เชี่ยวชาญด้านระบบสารสนเทศของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด และ

ผู้ทรงคุณวุฒิ จำนวน 8 ท่าน ประเมินความเหมาะสมของแนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด แสดงได้ดังตารางที่ 4.5

ตารางที่ 4.5 ผลการประเมินความเหมาะสมแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

รายการประเมิน	$\overline{X}$	S.D.	แปลผล
ความเหมาะสมของแนวทางการเสริมสร้างความตระหนักรู้	4.88	0.34	มากที่สุด
ค่าเฉลี่ยโดยรวม	**4.88**	**0.34**	**มากที่สุด**

จากตารางที่ 4.5 ผลการประเมินความเหมาะสมแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด พบว่า แนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์ ที่ผู้วิจัยได้จัดทำขึ้นมีความเหมาะสมอยู่ในระดับมาก ($\overline{X}$ = 4.88)

4.3 ผลการวิจัยเพื่อตอบวัตถุประสงค์ข้อที่ 3

เพื่อจัดทำแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

4.3.1 ผลการวิเคราะห์ ออกแบบและพัฒนาแอปพลิเคชัน

ผู้วิจัยได้นำผลจากการสัมภาษณ์เชิงลึกและผลข้อมูลจากการเก็บรวบรวมแบบสอบถามชุดที่ 1 มาวิเคราะห์ ออกแบบ และพัฒนาระบบแอปพลิเคชันสำหรับการเสริมสร้างและประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ได้ผลการวิจัยจากการสัมภาษณ์เชิงลึกให้จัดทำแนวทางการเรียนรู้ในรูปแบบออนล์และวีดิทัศน์ผสมผสานกัน ซึ่งเป็นไปตามวัตถุประสค์ข้อที่ 2 ของการวิจัย “เพื่อพัฒนาแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์” นำมาใช้วงจรการพัฒนาระบบงาน (Software Development Life Cycle : SDLC) ทำให้ได้มาซึ่งดิจิทัลแพลตฟอร์มในรูปแบบของ Web Application สำหรับการเสริมสร้างและประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด และทำการการติดตั้งภายในระบบเครือข่าย Intranet ของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ด้วยแพลตฟอร์ม AEROTHAI Learning Management System (AEROTHAI LMS) เป็นแพลตฟอร์มสำหรับการเรียนรู้ออนไลน์ เป็นระบบและบริการการเรียนทางอิเล็กทรอนิกส์ สนับสนุนการเรียนรู้ซึ่งมีเป้าหมายที่จะพัฒนาบุคลากรให้มีประสิทธิภาพในการทำงานเพิ่มมากขึ้น ทุกคนในองค์กรสามารถเข้าถึงคอร์สเรียนต่าง ๆ และนั่งเรียนได้ทุกที่ทุกเวลา เป็นไปตามวัตถุประสงค์ข้อที่ 3 ของการวิจัย “เพื่อจัดทำ

แอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด” ดังภาพประกอบที่ 4.1

ภาพประกอบที่ 4.1 แสดงแพลตฟอร์ม AEROTHAI Learning Management System (AEROTHAI LMS) สำหรับการเรียนรู้ออนไลน์

4.3.2 ผลการประเมินการยอมรับแอปพลิเคชันการประเมินระดับความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

จากการนำแอปพลิเคชันการประเมินระดับความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ให้ผู้เชี่ยวชาญด้านระบบสารสนเทศของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด และผู้ทรงคุณวุฒิ จำนวน 8 ท่าน ประเมินการยอมรับแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด แสดงได้ดังตารางที่ 4.6

ตารางที่ 4.6 ผลการประเมินการยอมรับแอปพลิเคชันการประเมินระดับความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

รายการประเมิน	$\bar{X}$	S.D.	แปลผล
การยอมรับแอปพลิเคชันการประเมินระดับความตระหนักรู้	4.88	0.34	มากที่สุด
ค่าเฉลี่ยโดยรวม	**4.88**	**0.34**	**มากที่สุด**

จากตารางที่ 4.6 ผลการประเมินการยอมรับแอปพลิเคชันการประเมินระดับความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด พบว่า แอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด มีค่าการยอมรับอยู่ในระดับมาก ($\overline{X}$ = 4.88)

4.3.3 ผลการวัดระดับความตระหนักรู้หลังจากสร้างความตระหนักรู้

ผู้วิจัยใช้แบบสอบถามชุดที่ 2 ซึ่งได้เพิ่มตัวแปรโดยที่อิงตัวแปรจากชุดที่ 1 ซึ่งมี 14 ตัวแปร ผู้วิจัยได้เพิ่มตัวแปรที่เกี่ยวข้องกับระดับความตระหนักรู้อีก 6 ตัวแปร ที่จะทำการวัดระดับความตระหนักรู้หลังจากสร้างความตระหนักรู้ด้วยแพลตฟอร์ม AEROTHAI Learning Management System แล้วนั้น รวมแล้วเป็น 20 ตัวแปร ประกอบด้วย 1) ด้านพฤติกรรมการใช้อินเทอร์เน็ต 2) ด้านพฤติกรรมการใช้งานสื่อสังคม 3) ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์ 4)ด้านพฤติกรรมการใช้งานผ่านโปรแกรม 5) ด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต 6) ความตระหนักรู้ด้านการใช้คอมพิวเตอร์ 7) ความตระหนักรู้ด้านการใช้พาสเวิร์ด 8) ความตระหนักรู้ด้านการใช้อีเมล 9) ความตระหนักรู้ด้านการเข้าเว็บไซต์ 10) ความตระหนักรู้ด้านการใช้ Messaging 11) ความตระหนักรู้เกี่ยวข่าวปลอมในโลกไซเบอร์ 12) ความตระหนักรู้ด้านการเก็บข้อมูลบนเครื่อง Server 13) ความตระหนักรู้ด้านเข้าประชุมทางออนไลน์ 14)ความตระหนักรู้ในการใช้มือถือ 15)ความมั่นคงปลอดภัย 16) การส่งข้อความซึ่งเต็มไปด้วยความโกรธ 17) การคุกคามหรือล่วงละเมิด 18) การปลอมตัวหรือแอบอ้าง 19) การเผยแพร่ออกนอกกลุ่ม และ 20) การกีดกัน ซึ่งหลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ผ่านทางระบบ AEROTHAI Learning Management System (AEROTHAI LMS) สำหรับการเรียนรู้ออนไลน์เรียบร้อยแล้ว จากบุคลากรกลุ่มตัวอย่างในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด จำนวน 99 คน เป็นผู้ตอบคำถามเอง (Self-Administered) ได้ผลการวิจัยดังนี้

4.3.3.1 ข้อมูลทั่วไปบุคลากรของกลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย เพศ อายุ ระดับการศึกษาสูงสุด สายงานที่ปฏิบัติ อายุงาน และระยะเวลาโดยฉลี่ยที่ใช้งานคอมพิวเตอร์ ในแต่ละวันของเวลาทำงาน แสดงผลไว้ในตารางที่ 4.5

ตารางที่ 4.7 แสดงผลข้อมูลทั่วไปของกลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

เพศ	**จำนวน (คน)**	**ร้อยละ**
ชาย	54	54.5
หญิง	45	45.5
รวม	**99**	**100.0**

ตารางที่ 4.7 (ต่อ)

อายุ	จำนวน (คน)	ร้อยละ
ต่ำกว่า 30 ปี	5	5.1
30 – 40 ปี	11	11.1
41 – 50 ปี	33	33.1
51 – 60 ปี	49	49.5
61 ปีขึ้นไป	1	1.0
รวม	**99**	**100**

ระดับการศึกษาสูงสุด	จำนวน (คน)	ร้อยละ
ต่ำกว่าปริญญาตรี	2	2.0
ปริญญาตรี	49	49.5
ปริญญาโท	47	47.5
ปริญญาเอก	1	1.0
รวม	**99**	**100**

สายงานที่ปฏิบัติงาน	จำนวน (คน)	ร้อยละ
ด้านปฏิบัติการ	22	22.2
ด้านวิศวกรรม	43	43.4
ด้านธุรการ	18	18.2
ด้านอื่น ๆ	16	16.2
รวม	**99**	**100**

อายุงาน	จำนวน (คน)	ร้อยละ
ไม่เกิน 5 ปี	5	5.1
6 – 10 ปี	10	10.1
11 – 15 ปี	10	10.1
16 ปีขึ้นไป	74	74.7
รวม	**99**	**100**

ตารางที่ 4.7 (ต่อ)

ระยะเวลาโดยฉลี่ยที่ใช้งานในแต่ละวัน	จำนวน (คน)	ร้อยละ
น้อยกว่า 1 ชั่วโมงต่อวัน	2	2.0
1 – 3 ชั่วโมงต่อวัน	26	26.3
4 – 6 ชั่วโมงต่อวัน	44	44.4
มากกว่า 6 ชั่วโมงต่อวัน	27	27.3
รวม	**99**	**100**

จากตารางที่ 4.7 พบว่ากลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ส่วนมากเป็นเพศชาย จำนวน 54 คน คิดเป็นร้อยละ 54.5 และเป็นเพศหญิง จำนวน 45 คน คิดเป็นร้อยละ 45.5 ตามลำดับ

กลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ส่วนมากมีอายุ 51 – 60 ปี จำนวน 49 คน คิดเป็นร้อยละ 49.5 อายุ 41 – 50 ปี จำนวน 33 คน คิดเป็นร้อยละ 33.3 อายุ 30 – 40 ปี จำนวน 11 คน คิดเป็นร้อยละ 11.1 อายุต่ำกว่า 30 ปี จำนวน 5 คน คิดเป็นร้อยละ 5.1 และอายุ 61 ปีขึ้นไป จำนวน 1 คน คิดเป็นร้อยละ 1.0 ตามลำดับ

กลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ส่วนมากมีระดับการศึกษา ปริญญาตรี จำนวน 49 คน คิดเป็นร้อยละ 49.5 ปริญญาโท จำนวน 47 คน คิดเป็นร้อยละ 47.5 ต่ำกว่าปริญญาตรี จำนวน 2 คน คิดเป็นร้อยละ 2.0 และปริญญาเอก จำนวน 1 คน คิดเป็นร้อยละ 1.0 ตามลำดับ

กลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ส่วนมากปฏิบัติงานด้านวิศวกรรม จำนวน 43 คน คิดเป็นร้อยละ 43.4 ปฏิบัติงานด้านปฏิบัติการ จำนวน 22 คน คิดเป็นร้อยละ 22.2 ปฏิบัติงานด้านธุรการ จำนวน 18 คน คิดเป็นร้อยละ 18.2 และปฏิบัติงานด้านอื่น ๆ จำนวน 16 คน คิดเป็นร้อยละ 16.2 ตามลำดับ

กลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ส่วนมากมีอายุงาน 16 ปีขึ้นไป จำนวน 74 คน คิดเป็นร้อยละ 74.7 อายุงาน 11-15 ปี จำนวน 10 คน คิดเป็นร้อยละ 10.1 อายุงาน 6-10 ปี จำนวน 10 คน คิดเป็นร้อยละ 10.1 และอายุงานไม่เกิน 5 ปี จำนวน 5 คน คิดเป็นร้อยละ 5.1 ตามลำดับ

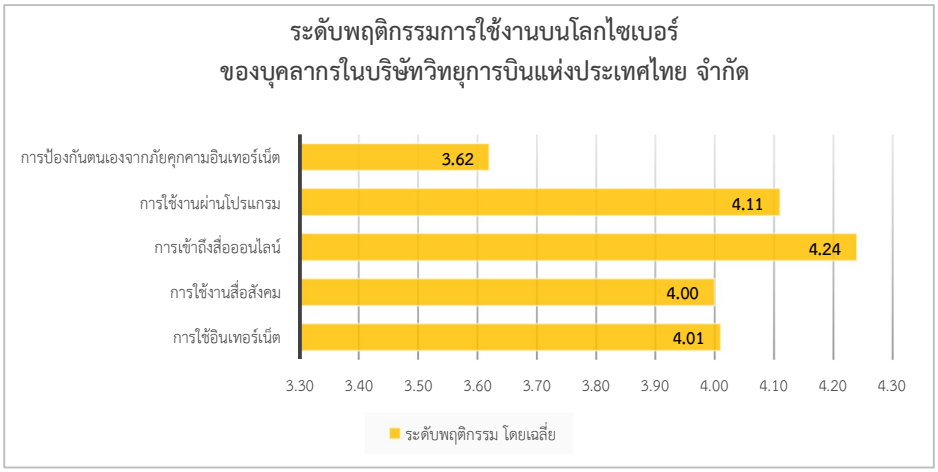
กลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ส่วนมากใช้งานคอมพิวเตอร์ ในแต่ละวันของเวลาทำงานมีระยะเวลาโดยฉลี่ย 4-6 ชั่วโมงต่อวัน จำนวน 44 คน คิดเป็นร้อยละ 44.4 มีระยะเวลาโดยฉลี่ย มากกว่า 6 ชั่วโมงต่อวัน จำนวน 27 คน คิดเป็นร้อยละ 27.3 มีระยะเวลาโดยฉลี่ย 1-3 ชั่วโมงต่อวัน จำนวน 26 คน คิดเป็นร้อยละ 26.3 และมีระยะเวลาโดยฉลี่ย น้อยกว่า 1 ชั่วโมงต่อวัน จำนวน 2 คน คิดเป็นร้อยละ 2.0 ตามลำดับ

4.3.3.2 พฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย ด้านพฤติกรรมการใช้อินเทอร์เน็ต ด้านพฤติกรรมการใช้งานสื่อสังคม

ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์ ด้านพฤติกรรมการใช้งานผ่านโปรแกรมด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต แสดงผลไว้ในตารางที่ 4.8

ตารางที่ 4.8 แสดงผลระดับพฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

รายการประเมิน	$\overline{X}$	S.D.	แปลผล
1. การใช้อินเทอร์เน็ต	4.01	0.23	มาก
2. การใช้งานสื่อสังคม	4.00	0.06	มาก
3. การเข้าถึงสื่อออนไลน์	4.24	0.10	มากที่สุด
4. การใช้งานผ่านโปรแกรม	4.11	0.13	มาก
5. การป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต	3.62	0.10	มาก
ค่าเฉลี่ยโดยรวม	**4.00**	**0.06**	**มาก**



ภาพประกอบที่ 4.2 แสดงผลระดับพฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

จากตารางที่ 4.8 และภาพประกอบที่ 4.2 แสดงให้เห็นว่าระดับพฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ส่วนมากสรุประดับพฤติกรรมรวม อยู่ในระดับมาก โดยมีระดับพฤติกรรมด้านการเข้าถึงสื่อออนไลน์ ในระดับมากที่สุด ($\overline{X}$ = 4.24) ระดับพฤติกรรมด้านการใช้งานผ่านโปรแกรม ในระดับมาก ($\overline{X}$ = 4.11) ระดับพฤติกรรมด้านการใช้อินเทอร์เน็ต ในระดับมาก ($\overline{X}$ = 4.01) ระดับพฤติกรรมด้านการใช้งานสื่อสังคม ในระดับมาก ($\overline{X}$ =

4.00) และระดับพฤติกรรมด้านการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต ในระดับมาก ($\overline{X}$ = 3.62) ตามลำดับ

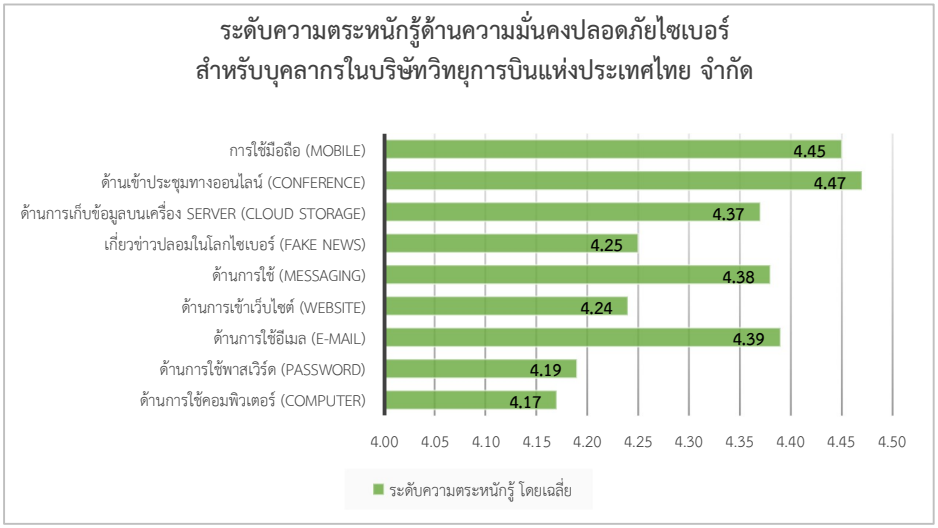
4.3.3.3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย ความตระหนักรู้ด้านการใช้คอมพิวเตอร์ (Computer) ความตระหนักรู้ด้านการใช้พาสเวิร์ด (Password) ความตระหนักรู้ด้านการใช้อีเมล (E-mail) ความตระหนักรู้ด้านการเข้าเว็บไซต์ (Website) ความตระหนักรู้ด้านการใช้ Messaging ความตระหนักรู้เกี่ยวข่าวปลอมในโลกไซเบอร์ (Fake News) ความตระหนักรู้ด้านการเก็บข้อมูลบนเครื่อง Server (Cloud Storage) ความตระหนักรู้ด้านเข้าประชุมทางออนไลน์ (Conference) ความตระหนักรู้ในการใช้มือถือ (Mobile) แสดงผลไว้ในตารางที่ 4.9

ตารางที่ 4.9 แสดงผลระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่างหลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

รายการประเมิน	$\overline{X}$	S.D.	แปลผล
1. ด้านการใช้คอมพิวเตอร์ (Computer)	4.17	0.10	มาก
2. ด้านการใช้พาสเวิร์ด (Password)	4.19	0.23	มาก
3. ด้านการใช้อีเมล (E-mail)	4.39	0.06	มากที่สุด
4. ด้านการเข้าเว็บไซต์ (Website)	4.24	0.09	มากที่สุด
5. ด้านการใช้ (Messaging)	4.38	0.08	มากที่สุด
6. เกี่ยวข่าวปลอมในโลกไซเบอร์ (Fake News)	4.25	0.02	มากที่สุด
7. ด้านการเก็บข้อมูลบนเครื่อง Server (Cloud Storage)	4.37	0.03	มากที่สุด
8. ด้านเข้าประชุมทางออนไลน์ (Conference)	4.47	0.03	มากที่สุด
9. การใช้มือถือ (Mobile)	4.45	0.04	มากที่สุด
ค่าเฉลี่ยโดยรวม	**4.32**	**0.07**	**มากที่สุด**

จากตารางที่ 4.9 ผลวิจัยพบว่าระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ส่วนมากสรุประดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ รวม อยู่ในระดับมากที่สุด โดยมีระดับความตระหนักรู้ด้านเข้าประชุมทางออนไลน์ (Conference) มีค่าอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.47) ระดับความตระหนักรู้ด้านการใช้มือถือ (Mobile) มีค่าอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.45) ระดับความตระหนักรู้ด้านการใช้อีเมล (E-mail) มีค่าอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.39) ระดับความตระหนักรู้ด้านการใช้ (Messaging) มีค่าอยู่ในระดับมาก

ที่สุด ($\overline{X}$ = 4.38) ระดับความตระหนักรู้ด้านการเก็บข้อมูลบนเครื่อง Server (Cloud Storage) มีค่าอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.37) ระดับความตระหนักรู้ด้านเกี่ยวข่าวปลอมในโลกไซเบอร์ (Fake News) มีค่าอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.25) ระดับความตระหนักรู้ด้านการเข้าเว็บไซต์ (Website) มีค่าอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.24) ระดับความตระหนักรู้ด้านการใช้พาสเวิร์ด (Password) มีค่าอยู่ในระดับมาก ($\overline{X}$ = 4.19) และระดับความตระหนักรู้ด้านการใช้คอมพิวเตอร์ (Computer) มีค่าอยู่ในระดับมาก ($\overline{X}$ = 4.17) ตามลำดับ ดังภาพประกอบที่ 4.3



ภาพประกอบที่ 4.3 แสดงผลระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่างหลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

4.3.3.4 ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย ความมั่นคงปลอดภัย (Security) การส่งข้อความซึ่งเต็มไปด้วยความโกรธ (Flaming) การคุกคามหรือล่วงละเมิด (Harassment) การปลอมตัว (Masquerading) แอบอ้าง การเผยแพร่ออกนอกกลุ่ม (Outing) การกีดกัน (Exclusion) แสดงผลไว้ในตารางที่ 4.10

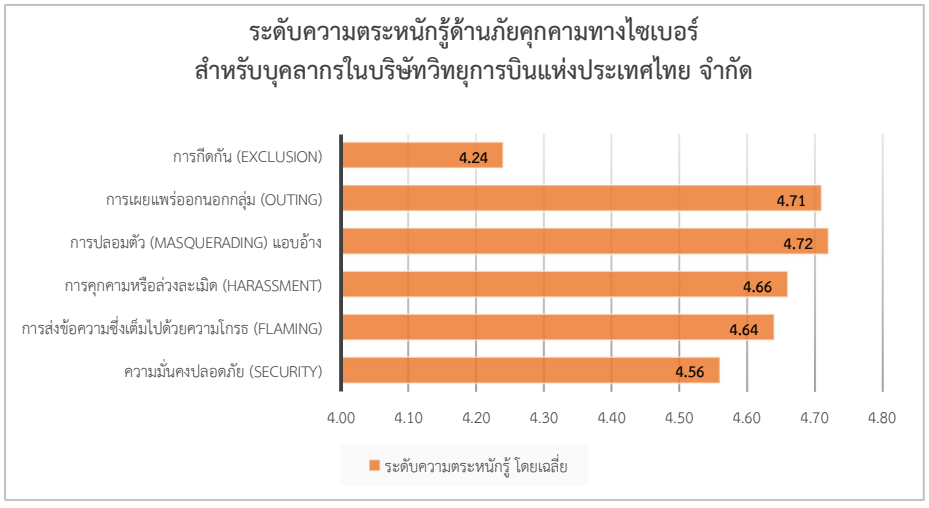
ตารางที่ 4.10 แสดงผลระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่างหลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

รายการประเมิน	$\overline{X}$	S.D.	แปลผล
1. ด้านความมั่นคงปลอดภัย (Security)	4.56	0.13	มากที่สุด
2. ด้านการส่งข้อความซึ่งเต็มไปด้วยความโกรธ (Flaming)	4.64	0.05	มากที่สุด

ตารางที่ 4.10 (ต่อ)

3. ด้านการคุกคามหรือล่วงละเมิด (Harassment)	4.66	0.03	มากที่สุด
4. ด้านการปลอมตัว (Masquerading) แอบอ้าง	4.72	0.02	มากที่สุด
5. ด้านการเผยแพร่ออกนอกกลุ่ม (Outing)	4.71	0.03	มากที่สุด
6. ด้านการกีดกัน (Exclusion)	4.24	0.12	มากที่สุด
ค่าเฉลี่ยโดยรวม	**4.59**	**0.05**	**มากที่สุด**

จากตารางที่ 4.10 ผลวิจัยพบว่าระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง หลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ส่วนมากสรุประดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์อยู่ในระดับมากที่สุด โดยมีระดับความตระหนักรู้ด้านการปลอมตัว (Masquerading) แอบอ้าง มีค่าอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.72) ระดับความตระหนักรู้ด้านการเผยแพร่ออกนอกกลุ่ม (Outing) มีค่าอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.71) ระดับความตระหนักรู้ด้านการคุกคามหรือล่วงละเมิด (Harassment) มีค่าอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.66) ระดับความตระหนักรู้ด้านการส่งข้อความซึ่งเต็มไปด้วยความโกรธ (Flaming) มีค่าอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.64) ระดับความตระหนักรู้ด้านความมั่นคงปลอดภัย (Security) มีค่าอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.56) และระดับความตระหนักรู้ด้านการกีดกัน (Exclusion) มีค่าอยู่ในระดับมากที่สุด ($\overline{X}$ = 4.24) ตามลำดับ ดังภาพประกอบที่ 4.4



ภาพประกอบที่ 4.4 แสดงผลระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่างหลังจากได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

4.4 สรุป

บทที่ 4 นี้ ผู้วิจัยได้นำเสนอผลการวิจัยเพื่อตอบวัตถุประสงค์ทั้ง 3 ข้อ ซึ่งประกอบด้วย 1) เพื่อศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ขอบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ 2) เพื่อพัฒนาแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์ 3) เพื่อจัดทำแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ซึ่งผู้วิจัยได้สรุปผลการวิจัยและอภิปรายผล นำเสนอในบทที่ 5 ต่อไป

บทที่ 5

สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

จากการวิจัยเรื่อง“การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด” มีวัตถุประสงค์เพื่อศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อพัฒนาแนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และจัดทำแอปพลิเคชันประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด โดยสามารถสรุปผลการวิจัยได้ดังนี้

1. สรุปผลการวิจัย
2. อภิปรายผล
3. ปัญหา อุปสรรคและข้อจำกัดของการวิจัย
4. ข้อเสนอแนะ

5.1 สรุปผลการวิจัย

การวิจัยเรื่อง“การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด” มีวัตถุประสงค์การวิจัยดังนี้

1. เพื่อศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
2. เพื่อพัฒนาแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่ยงและภัยคุกคามจากการใช้งานบนโลกไซเบอร์
3. เพื่อจัดทำแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

การวิจัยนี้เป็นงานวิจัยแบบผสมผสาน (Mixed Method) คือเป็นการวิจัยเชิงคุณภาพ (Qualitative Research) และการวิจัยเชิงปริมาณ (Quantitative Research) เพื่อนำข้อมูลทั้งสองส่วนมาทำการศึกษา วิเคราะห์ ตามวัตถุประสงค์ของการวิจัย ได้ผลการวิจัยเชิงคุณภาพ (Qualitative Research) มีดังนี้

ผลการวิจัยเชิงคุณภาพ (Qualitative Research) จากการสัมภาษณ์เชิงลึกด้วยแบบสัมภาษณ์แบบกึ่งโครงสร้างพบว่า สภาพปัญหาการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ มีการกำหนดกลยุทธ์ด้านภัยคุกคามทางไซเบอร์ ผู้บังคับบัญชาให้ความสำคัญกับนโยบายด้านความมั่นคงปลอดภัยไซเบอร์

มีการระบุภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อการปฏิบัติงานโดยตรง มีการประเมินความเสี่ยงด้านภัยคุกคามทางไซเบอร์ โดยมีการระบุการสร้างเสริมความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ด้วยวิธีการเรียนรู้แบบออนไลน์และวิธีการเรียนโดยใช้วีดิทัศน์ผสมผสานกัน

ผลการวิจัยเชิงปริมาณ (Quantitative Research) จากการเก็บรวบรวมข้อมูลจากบุคลากรกลุ่มตัวอย่างในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ด้วยแบบสอบถามแบบปลายปิด (Close-end Questionnaire) โดยออกแบบคำถามออกเป็นส่วน 3 ส่วน ส่วนที่ 1 ข้อมูลทั่วไปบุคลากรของกลุ่มตัวอย่าง ส่วนที่ 2 พฤติกรรมการใช้งานระบบอินเทอร์เน็ต จำนวน 5 ด้าน ส่วนที่ 3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ จำนวน 9 ด้าน ได้ผลการวิจัยเชิงปริมาณ (Quantitative Research) ดังนี้

ส่วนที่ 1 ข้อมูลทั่วไปบุคลากรผู้เข้ารับการประเมิน ผลวิจัยพบว่าส่วนใหญ่เป็นเพศชายมากกว่าเพศหญิง มีอายุส่วนใหญ่อยู่ที่ 51 – 60 ปี ระดับการศึกษาสูงสุดอยู่ที่ปริญญาโท สายการปฏิบัติงานเป็นสายงานวิศวกรรม ปฏิบัติงานมากกว่า 16 ปีขึ้นไป ใช้ระยะเวลาโดยเฉลี่ยในการใช้งานคอมพิวเตอร์ในแต่ละวันของเวลาทำงาน อยู่ที่ 4 – 6 ชั่วโมงต่อวัน

ส่วนที่ 2 พฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ จำนวน 5 ด้าน ผลวิจัยพบว่า ระดับพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยรวมพฤติกรรมทั้ง 5 ด้าน อยู่ใน ระดับมาก

ส่วนที่ 3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด จำนวน 9 ด้าน ผลวิจัยพบว่า ระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด โดยรวมความตระหนักรู้ทั้ง 9 ด้าน อยู่ใน ระดับมาก

ผลข้อมูลจากการสัมภาษณ์เชิงลึกและผลจากการเก็บรวบรวมข้อมูลด้วยแบบสอบถามชุดที่ 1 ผู้วิจัยได้นำข้อมูลมาวิเคราะห์ ออกแบบ และพัฒนาสร้างแอปพลิเคชันสำหรับการเสริมสร้างและประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ในรูปแบบ Web Application และทำการการติดตั้งภายในระบบเครือข่าย Intranet ของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ด้วยแพลตฟอร์ม AEROTHAI Learning Management System (AEROTHAI LMS) และเปิดระบบให้บุคลากรเข้าร่วมการเสริมสร้างและประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ได้ผลข้อมูลจากการประเมินระดับความตระหนักรู้หลังจากที่บุคลากรได้รับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ แบ่งเป็น 3 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลทั่วไปบุคลากรผู้เข้ารับการประเมิน ผลวิจัยพบว่า ส่วนใหญ่เป็นเพศชายมากกว่าเพศหญิง มีระดับอายุส่วนใหญ่อยู่ที่ระดับอายุ 51 – 60 ปี รองลงไปเป็นระดับอายุ 41 – 50 ปี ระดับอายุ 30 – 40 ปี ระดับอายุต่ำกว่า 30 ปี และระดับอายุ 61 ปีขึ้นไปตามลำดับ ระดับการศึกษาสูงสุดส่วนใหญ่อยู่ที่ระดับปริญญาตรี รองลงไปเป็นระดับปริญญาโท ระดับต่ำกว่าปริญญาตรี และระดับปริญญาเอกตามลำดับ สายการปฏิบัติงานส่วนใหญ่เป็นสายงานวิศวกรรม รองลงไปเป็นสายงานปฏิบัติการ สายงานธุรการ และสายงานอื่น ๆ ตามลำดับ อายุงานส่วนใหญ่ปฏิบัติงานมากกว่า 16 ปีขึ้นไป รองลงไปเป็นระดับปฏิบัติงานมา 11 – 15 ปี มีจำนวนเท่ากันกับ ระดับปฏิบัติงานมา 6 –

10 ปี และระดับปฏิบัติงานมาไม่เกิน 5 ปี ตามลำดับ การใช้ระยะเวลาโดยเฉลี่ยในการใช้งานคอมพิวเตอร์ในแต่ละวันของเวลาทำงาน ส่วนใหญ่อยู่ที่ระดับ 4 – 6 ชั่วโมงต่อวัน รองลงไปเป็นระดับมากกว่า 6 ชั่วโมงต่อวัน ระดับ 1 – 3 ชั่วโมงต่อวัน และน้อยกว่า 1 ชั่วโมงต่อวัน

ส่วนที่ 2 พฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ผลวิจัยพบว่า ระดับพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ มีความปลอดภัยอยู่ใน ระดับมาก เมื่อพิจารณาจากปัจจัยย่อยต่าง ๆ เรียงลำดับค่าเฉลี่ยจากมากไปหาน้อยพบว่า พฤติกรรมด้านการเข้าถึงสื่อออนไลน์มีพฤติกรรมปลอดภัยในระดับมากที่สุด พฤติกรรมด้านการใช้งานผ่านโปรแกรมมีพฤติกรรมปลอดภัยในระดับมาก พฤติกรรมด้านการใช้อินเทอร์เน็ตมีพฤติกรรมปลอดภัยในระดับมาก พฤติกรรมด้านการใช้งานสื่อสังคมมีพฤติกรรมปลอดภัยในระดับมาก และ พฤติกรรมด้านการป้องกันตนเองจากภัยคุกคามอินทอร์เน็ตมีพฤติกรรมปลอดภัยในระดับมาก โดยรวมพฤติกรรมมีความปลอดภัยอยู่ในระดับ มาก

ส่วนที่ 3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ผลวิจัยพบว่า ระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด มีความตระหนักรู้อยู่ใน ระดับมากที่สุด เมื่อพิจารณาจากปัจจัยย่อยต่าง ๆ เรียงลำดับค่าเฉลี่ยจากมากไปหาน้อยพบว่า ความตระหนักรู้ด้านเข้าประชุมทางออนไลน์ (Conference) อยู่ในระดับมากที่สุด ความตระหนักรู้ในการใช้มือถือ (Mobile) อยู่ในระดับมากที่สุด ความตระหนักรู้ด้านการใช้อีเมล (E-mail) อยู่ในระดับมากที่สุด ความตระหนักรู้ด้านการใช้ (Messaging) อยู่ในระดับมากที่สุด ความตระหนักรู้ด้านการเก็บข้อมูลบนเครื่อง Server (Cloud Storage) อยู่ในระดับมากที่สุด ความตระหนักรู้เกี่ยวข่าวปลอมในโลกไซเบอร์ (Fake News) อยู่ในระดับมากที่สุด ความตระหนักรู้ด้านการเข้าเว็บไซต์ (Website) อยู่ในระดับมากที่สุด ความตระหนักรู้ด้านการใช้พาสเวิร์ด (Password) อยู่ในระดับมาก ความตระหนักรู้ด้านการใช้คอมพิวเตอร์ (Computer) อยู่ในระดับมาก โดยรวมความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ อยู่ในระดับความตระหนักรู้ มากที่สุด

ส่วนที่ 4 ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ผลวิจัยพบว่า ระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด มีความตระหนักรู้อยู่ใน ระดับมากที่สุด เมื่อพิจารณาจากปัจจัยย่อยต่าง ๆ เรียงลำดับค่าเฉลี่ยจากมากไปหาน้อยพบว่า ความตระหนักรู้ด้านการปลอมตัว (Masquerading) แอบอ้าง อยู่ในระดับมากที่สุด ความตระหนักรู้ด้านการเผยแพร่ออกนอกกลุ่ม (Outing) อยู่ในระดับมากที่สุด ความตระหนักรู้ด้านการคุกคามหรือล่วงละเมิด (Harassment) อยู่ในระดับมากที่สุด ความตระหนักรู้ด้านการส่งข้อความซึ่งเต็มไปด้วยความโกรธ (Flaming) อยู่ในระดับมากที่สุด ความตระหนักรู้ด้านความมั่นคงปลอดภัย (Security) อยู่ในระดับมากที่สุด ความตระหนักรู้ด้านการกีดกัน (Exclusion) อยู่ในระดับมากที่สุด โดยรวมความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์อยู่ในระดับความตระหนักรู้ มากที่สุด

5.2 อภิปรายผล

จากการดำเนินการวิจัยตามวัตถุประสงค์ข้อที่ 1 เพื่อศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ทำให้ทราบว่าสภาพปัญหาการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ได้มีการกำหนดกลยุทธ์ด้านภัยคุกคามทางไซเบอร์แล้ว ผู้บังคับบัญชาให้ความสำคัญกับนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ มีการระบุภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อการปฏิบัติงานโดยตรง มีการประเมินความเสี่ยงด้านภัยคุกคามทางไซเบอร์ โดยมีการระบุการสร้างเสริมความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ด้วยวิธีการเรียนรู้แบบออนไลน์และวิธีการเรียนโดยใช้วีดิทัศน์ผสมผสานกัน อันเป็นแนวทางสำหรับการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ตามวัตถุประสงค์ของการวิจัยข้อที่ 2 และมีผลสอดคล้องกับงานวิจัยของ A. Alarifi, H. Tootell, P. Hyland, (2012) ศึกษาเรื่องรูปแบบการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยแก่ประชาชนในประเทศ Saudi Arabia ที่ผลวิจัยพบว่ารูปแบบที่มีประสิทธิภาพสูงที่สุดคือ Web portals และต่ำที่สุดคือ Seminars

ผลการวิจัยผลตามวัตถุประสงค์ของการศึกษาวิจัยข้อที่ 1 ได้จากข้อมูลการสัมภาษณ์เชิงลึกที่กล่าวถึงการที่ต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มากขึ้น และจากการแก็บรวบรวมข้อมูลระดับพฤติกรรมรวมถึงระดับความตระหนักรู้ก่อนการสร้างความตระหนักรู้ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ได้ผลการประเมินสรุประดับพฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ของกลุ่มตัวอย่าง เท่ากับ 4.18 อยู่ในระดับมากตรงตามสมมติฐานการวิจัย ข้อที่ 1 พฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อยู่ในระดับมาก และการดำเนินการตามวัตถุประสงค์ข้อที่ 3 เพื่อพัฒนาแอปพลิเคชันสำหรับประเมินความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์สำหรับสำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ผู้วิจัยได้พัฒนาดิจิทัลแพลตฟอร์มเพื่อการเสริมสร้างและประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ในรูปแบบของ Web Application โดยใช้วงจรการพัฒนาระบบงาน (Software Development Life Cycle : SDLC) และติดตั้งภายในระบบเครือข่าย Intranet ของบริษัทวิทยุการบินแห่งประเทศไทยจำกัด ด้วยแพลตฟอร์ม AEROTHAI Learning Management System (LMS) เป็นแพลตฟอร์มสำหรับการเรียนรู้ออนไลน์ เป็นระบบและบริการการเรียนทางอิเล็กทรอนิกส์ สนับสนุนการเรียนรู้ซึ่งมีเป้าหมายที่จะพัฒนาบุคลากรให้มีประสิทธิภาพในการทำงานเพิ่มมากขึ้น ทุกคนในองค์กรสามารถเข้าถึงคอร์สเรียนต่าง ๆ และนั่งเรียนได้ทุกที่ทุกเวลา หลังจากการบุคลากรได้รับการเสริมสร้างความตระหนักรู้แล้วได้ผลการประเมินสรุประดับพฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด โดยรวม เท่ากับ 4.00 อยู่ในระดับมาก ผลระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด โดยรวม เท่ากับ 4.32 อยู่ในระดับมากที่สุด และผลระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด โดยรวม เท่ากับ 4.59 อยู่ในระดับมากที่สุด

ตามสมมติฐานการวิจัย ข้อที่ 2 แนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ผู้วิจัยได้เสนอผลรูปแนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ในรูปแบบ Web Application ที่ติดตั้งบนแพลตฟอร์ม AEROTHAI Learning Management System (LMS) และผลหลังการเสริมสร้างความตระหนักรู้ให้กับผู้บริหารระดับสูง ผู้เชี่ยวชาญด้านระบบสารสนเทศของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด และผู้ทรงคุณวุฒิ จำนวน 8 ท่าน ประเมินความเหมาะสมของแนวทางการเสริมสร้างความตระหนักรู้และการยอมรับแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด พบว่าแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด มีความเหมาะสมอยู่ในระดับมาก ($\overline{X}$ = 4.88) และสมมติฐานการวิจัย ข้อที่ 3 แอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด มีค่าการยอมรับอยู่ใน ระดับมาก ($\overline{X}$ = 4.88)

ผู้วิจัยได้ทำการตรวจสอบปัจจัยข้อมูลทั่วไปทางด้านประชากรของกลุ่มตัวอย่างมีผลต่อระดับความตระหนักรู้อย่างไร พบว่าบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ว่ามีผลต่อระดับการประเมินความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์หรือไม่ พบว่าข้อมูลทั่วไปของบุคลากรบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ไม่มีผลต่อระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เนื่องด้วยบริษัทวิทยุการบินแห่งประเทศไทย จำกัด มีนโยบายการสรรหาและคัดเลือกบุคลากร มุ่งเน้นให้การสรรหา การคัดเลือก การบรรจุแต่งตั้ง บุคลากรทั้งภายนอกและภายในองค์กรมีกระบวนการและแนวทางที่เป็นระบบ โปร่งใส และเป็นธรรม สอดคล้องกับแผนอัตรากำลัง การจัดการเส้นทางอาชีพ และการสืบทอดตำแหน่ง สำหรับบุคลากรของบริษัทวิทยุการบินฯ ที่ได้รับการคัดเลือกบรรจุเข้ามาเป็นพนักงานของบริษัทวิทยุการบินฯ ต้องมีคุณสมบัติของผู้สมัครครบถ้วน เช่น จบการศึกษาอยู่ในระดับปริญญาตรีขึ้นไป หลังจากที่ได้รับการคัดเลือกบรรจุแล้วบริษัทวิทยุการบินฯ ยังได้ส่งเสริมในการฝึกอบรมเรียนรู้ในด้านต่าง ๆ ที่เป็นความสามารถของตำแหน่งงานนั้น และบุคลากรส่วนใหญ่ทำงานอยู่ในสายงานวิศวกรรมและสายงานปฏิบัติการ ซึ่งจะเป็นผู้ใช้งานระบบสารสนเทศเป็นประจำและมีการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับบุคลากรตั้งแต่แรกเข้าและมีการแจ้งเตือนอยู่เสมอ ดังนั้น ปัจจัยด้านข้อมูลทั่วไปด้านประชากรจึงไม่มีผลต่อการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางด้านไซเบอร์

ซึ่งสอดคล้องกับงานวิจัยที่เกี่ยวข้องได้มีการนำปัจจัยข้อมูลทั่วไปทางด้านประชากรมาทำการวิจัย อาทิ สุธาเทพ รุณเรศ (2561) วิจัยเรื่อง “ปัจจัยที่มีผลต่อการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร” ผลการวิจัยพบว่า ปัจจัยทางด้านลักษณะทางประชากรด้านอายุ ระดับการศึกษาสูงสุด และรายได้ส่วนตัวต่อเดือน มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต แต่ปัจจัยทางด้านลักษณะทางประชากรด้านเพศ ไม่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี (2565) วิจัยเรื่อง “ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร” ผลการวิจัยพบว่า ปัจจัยด้านบุคคลพบว่าบุคลากรในบริษัทเอกชนแห่งนี้ที่มี เพศ

อายุ และประสบการณ์การทำงาน (อายุงาน) ที่ต่างกันมีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่ไม่แตกต่างกัน และในส่วนบุคลากรที่มีระดับการศึกษาสูงสุด แผนกที่สังกัด และประสบการณ์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่ต่างกัน มีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่แตกต่างกันอย่างมีนัยสำคัญทางสถิต

5.3 ปัญหา อุปสรรคและข้อจำกัดของการวิจัย

การวิจัยเรื่อง “การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด” ผู้วิจัยได้พบปัญหา อุปสรรคและข้อจำกัดของการวิจัยดังนี้

1. การวิจัยในครั้งนี้มีข้อจำกัดด้านระยะเวลาในการค้นคว้า ทบทวน วรรณกรรม ซึ่งอาจทำให้การศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ แนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด หาข้อมูลเชิงลึกได้อย่างไม่เพียงพอตามที่ผู้วิจัยได้ทำการศึกษามาและอาจทำให้การวิเคราะห์ประเด็นต่าง ๆ ไม่สามารถครอบคลุมถึงส่วนที่สำคัญ

2. สถานการณ์โรคระบาด COVID-19 ส่งผลให้การสัมภาษณ์เชิงลึกมีอุปสรรคในด้านการสื่อสาร เช่น การนัดหมายคลาดเคลื่อนจากการประชุม ทำงานออนไลน์ ระบบการสื่อสารที่ไม่เสถียร

5.4 ข้อเสนอแนะ

งานวิจัยนี้ได้วิธีการเรียนรู้แบบออนไลน์และวิธีการเรียนโดยใช้วีดิทัศน์ผสมผสานกันอันเป็นแนวทางการเสริมสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ความเหมาะสมต่อการใช้งานกับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่เหมาะสม หากแต่ควรทำการปรับปรุงเนื้อหาให้เป็นปัจจุบันอยู่เสมอ ทั้งนี้เพราะภัยคุกคามทางไซเบอร์และเทคโนโลยีมีการเปลี่ยนแปลงอยู่ตลอดเวลา และสามารถต่อยอดได้โดยทำตรวจสอบจุดประสงค์การใช้งานและสื่อที่ใช้สร้างเนื้อหาแนวทางปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งทำการประเมินและนำผลมาพัฒนาบุคลากรต่อไป

รูปแบบการเรียนรู้เพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ยังมีรูปแบบอื่นอีกที่น่าสนใจ เช่น การเรียนรู้ในรูปแบบของการจำลองสถานการณ์ รูปแบบการเรียนรู้ในรูปแบบการจำลองเกม สามารถนำไปเป็นรูปแบบของงานวิจัยต่อไปได้ในครั้งต่อไป

บรรณานุกรม

กระทรวงคมนาคม. (2562). **แผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ กระทรวงคมนาคม พ.ศ. 2562 – 2566**. หน้า 5-6 กระทรวงคมนาคม.

กริน ธัญญวิกรม และ ธีระ กุลสวัสดิ์. (2564). **การจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ กรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย**. (วิทยานิพนธ์ ปริญญามหาบัณฑิต). มหาวิทยาลัยบูรพา.

กรุงเทพธุรกิจ.(2564). **เปลี่ยน สูงวัย เท่าทันสื่อดิจิทัล ไม่หลง Fake News ยุคโควิด** สืบค้นเมื่อ ธันวาคม 2564 จากเว็บไซต์ https://www.bangkokbiznews.com/social/958666.

สำนักงานสถิติแห่งชาติ. (2564). **สรุปผลที่สำคัญ สำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารใน ครัวเรือน พ.ศ. 2563.** กรุงเทพฯ: สำนักงานสถิติแห่งชาติ.

คณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท วิทยุการบินแห่งประเทศไทย จำกัด. (2564). **แผนปฏิบัติการดิจิทัล บริษัทวิทยุการบินแห่งประเทศไทย จำกัด พ.ศ. 2565-2569.** กรุงเทพมหานคร: บริษัทวิทยุการบินแห่งประเทศไทย จำกัด. สืบค้นจาก https://www.aerothai.co.th/home.

จิตสุภา ฤทธิผลิน. (2564). **กลยุทธ์การคืนสภาพได้ทางไซเบอร์:แนวทางสำคัญในการดำเนินงาขององค์กรในยุคดิจิทัล.** NBTC Journal. สำนักเทคโนโลยีสารสนเทศ. สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ.

ชนินทร เฉลิมทรัพย์, นาวาอากาศเอก. (2561). **แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ.** เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2561.

ฐานเศรษฐกิจดิจิทัล. (15 ธันวาคม 2564). **โควิด-19 ดันคนไทยใช้เน็ต ทุบสถิติวันละ 12 ชั่วโมง Gen Z ใช้เน็ตสูงสุดปีแรก.** สืบค้นเมื่อวันที่ 5 มกราคม 2565 จากเว็บไซต์ บริษัท ฐานเศรษฐกิจ มัลติมีเดีย จำกัด. https://www.thansettakij.com/tech/506786.

ณัฐดนัย เนียมทอง.(2561). **คลังความรู้ SciMath: ความเข้าใจดิจิทัลกับผู้สูงอายุ**. สืบค้นเมื่อวันที่ 24 ธันวาคม 2564 จากเว็บไซต์ https://www. scimath. org/ article-technology/item/7943-2018-03-20-04-39-55

ณรงค์เวตย์ เรืองจวง, นาวาอากาศเอก. (2560). **แนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ.** เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2560.

บทความ IT Security. (14 สิงหาคม 2563). **7 วิธีเพิ่มความปลอดภัย ตัวตนออนไลน์ ไม่ให้หลุดเป็นสาธารณะ.** สืบค้นเมื่อวันที่ 5 มกราคม 2565 จากเว็บไซต์ บริษัทโทรคมนาคมแห่งชาติ จำกัด (มหาชน). https://www.cyfence.com/article/7-way-to-secure-your-online-identity/.

พงษ์ชัย เฉลิมกลิ่น. (2551). **ความตระหนักรู้ของพนักงานนิคมอุตสาหกรรมเกตเวย์ซิตี้ต่อลักษณะปัญหาสิ่งแวดล้อม.** ภาคนิพนธ์ ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาการจัดการสิ่งแวดล้อม สถาบันบัณฑิตพัฒนบริหารศาสตร์.

บรรณานุกรม (ต่อ)

พงษ์ศักดิ์ ผกามาศ. (2553). **ระบบไอซีทีและการจัดการยุคใหม่ (พิมพ์ครั้งที่ 1).** กรุงเทพมหานคร: บริษัท วิตตี้ กรุ๊ป จำกัด.

พงษ์ศักดิ์ ผกามาศ. (2562). **การจัดการระบบไอซีทีเชิงกลยุทธ์แบบบูรณาการ : กลยุทธ์การพัฒนาองค์กร สู่ความเป็นเลิศในยุคดิจิทัล.** มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์.

เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี. (2565). **ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร.** มหาวิทยาลัยธุรกิจบัณฑิตย์.

ราชบัณฑิตยสถาน. (2562). **พจนานุกรมศัพท์คอมพิวเตอร์และเทคโนโลยีสารสนเทศ.** กรุงเทพฯ : สำนักงานราชบัณฑิตยสภา.

ราชิต อรุณรังสี, พลตรี. (2561). **ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้.** เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2561.

ฤทัยชนนี สิทธิชัย และ ธันยากร ตุดเกื้อ. (2560). **พฤติกรรมการรังแกบนโลกไซเบอร์ของเยาวชนในสามจังหวัดชายแดนใต้**. มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตปัตตานี.

วิทยา จุลวัฒนานนท์. (2563). **การต่อต้านภัยคุกคามทางไซเบอร์ต่อการให้บริการการเดินอากาศของประเทศไทย.** วิทยาลัยการทัพอากาศ. กรมยุทธศึกษาทหารอากาศ.

ศุภวิชญ์ สาตราวาหะ, กีรติสรรพ์ ผลละออ, วิชากร ต่ายทอง. (2560). **การวิเคราะห์พฤติกรรมป้องกันภัยคุกคามทางโทรศัพท์มือถือของคนไทยด้วยโปรแกรม RapidMiner.** เอกสารวิจัย วิทยาศาสตรบัณฑิต สาขาวิชาคอมพิวเตอร์ โรงเรียนนายเรืออากาศนวมินทกษัตริยาธิราช.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2564)**. CS101 ความมั่นคงปลอดภัยไซเบอร์เบื้องต้น**. สืบค้นเมื่อวันที่ 22 ธันวาคม 2564 จากเว็บไซต์ https://www.etda.or.th/th/Useful-Resource/Knowledge-Sharing/Articles/Cybersecurity-101.aspx

สำนักงานส่งเสริมเศรษฐกิจดิจิทัล. (2021). **Digital Literacy กับสังคมผู้สูงอายุ**. สืบค้นเมื่อวันที่ 24 ธันวาคม 2564 จากเว็บไซต์ https://www.depa.or.th/th/article-view/digital-literacy

สุธาเทพ รุณเรศ. (2561). **ปัจจัยที่มีผลต่อการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร.** มหาวิทยาลัยธรรมศาสตร์. สืบค้นจาก http://ethesisarchive.library.tu.ac.th/thesis/2018/TU_2018_5923036155_7 502_9460.pdf.

สุรชัย ฉัตรเฉลิมพันธุ์ และ เทอดพงษ์ แดงสี. (2563). **การเสริมสร้างความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในองค์กร: กรณีการจำลองการโจมตีด้วยฟิชชิ่ง**. กรุงเทพมหานคร. มหาวิทยาลัยธนบุรี.

บรรณานุกรม (ต่อ)

สุรพงศ์ ทรัพยาคม และ อรรถพล ป้อมสถิต. (2563). **การวิเคราะห์การรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562.** ปทุมธานี. มหาวิทยาลัยรังสิต.

A. Alarifi, H. Tootell, P. Hyland (2012). **A Study of Information Security Awareness and Practices in Saudi Arabia.** The 2nd International Conference on Communications and Information Technology (ICCIT): Digital Information Management, Hammamet.

Fillgoods. (26 ธันวาคม 2564). **เจาะพฤติกรรมผู้บริโภคในไทย ปี 2562 คนไทยมีการใช้อินเทอร์เน็ตทำกิจกรรมออนไลน์ที่เปลี่ยนไปอย่างไร.** สืบค้นเมื่อวันที่ 5 มกราคม 2565 จากเว็บไซต์ บริษัท ฟิลกู้ด เทคโนโลยี จำกัด. https://www.fillgoods.co/online-biz/shop-orders-thai-user-behavior- internet-activities/.

International Telecommunication Union. **Global Cybersecurity Index 2017.** Switzerland. Retrieved from www.itu.int.

IT Pro team. (24 January 2020). **Our 5-minute guide to security awareness training**. จากเว็บไซต์ ITPro. https://www.itpro.co.uk/security/33974/our-5-minute-guide-to- security-awareness-training.

Khera, V. (24 March 2021). **Red Team VS Blue Team.** Retrieved from Linkedin. https://www.linkedin.com/pulse/red-teamvs-blue-dr-varin-khera/?trackingId=yUCDstClsMUBW29dovQTWg%3D%3D.

Michael Hanna. (2020).**Exploring Cybersecurity A Exploring Cybersecurity Awareness and T eness and Training Straining Strategies T ategies To Protect Information Systems and Data** (Ph.D.Thesis). Walden University.

QuickServ. (2020). **ข้อแนะนำสำหรับ Security Awareness Training.** จากเว็บไซต์ บริษัท ควิกเซิร์ฟ โปรไวเดอร์ จำกัด. https://www.quickserv.co.th/cloud/knowledge-base/solutions/ข้อแนะนำสำหรับ-Security-Awareness-Training/.

National Institute of Standards and Technology. (2018). **Framework for Improving Critical Infrastructure Cybersecurity.** National Institute of Standards and Technology, (pp 5-27).

Tero Haukilehto. (2019). **Improving Cyber Security awareness**. JAMK University of Applied Sciences.

Thamonton Jang .(2020). **ผลสำรวจพบผู้สูงวัย 44.72% ใช้ไลน์เป็นโซเชียลมีเดียหลัก ช่วงโควิด-19**. สืบค้นเมื่อวันที่ 24 ธันวาคม 2564 จากเว็บไซต์ https://www.bltbangkok.com/news/25662.

บรรณานุกรม (ต่อ)

Thanakorn Mehinkong.(2015). **Cybersecurity Knowledge Architecture for Supporting the Adaptive Intrusion Detection Systems Using Association Rules**. The Journal of KMUTNB., Vol. 25.

Therdpong Daengsi et al., (2021). **Cybersecurity Awareness Enhancement: A Study of the Efects of Age and Gender of Thai Employees Associated with Phishing Attacks.** Retrieved from Springer Nature. https://link.springer.com/article/10.1007/s10639-021-10806-7.

ภาคผนวก

ภาคผนวก ก
แบบสอบถาม

แบบสอบถาม

เรื่อง

การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากร ในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

คำชี้แจง

การวิจัยนี้ มุ่งเน้นศึกษา วิเคราะห์ ระดับความตระหนักรู้และความเข้าใจของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด เกี่ยวกับความเสี่ยงและภัยคุกคามทางไซเบอร์ เพื่อนำมาวิเคราะห์ และนำไปสู่การกำหนดแนวทางการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

แบบสอบถามฉบับนี้ แบ่งเป็น 4 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลทั่วไปบุคลากรของกลุ่มตัวอย่าง

ส่วนที่ 2 พฤติกรรมการใช้งานระบบอินเทอร์เน็ต

ส่วนที่ 3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ 4 ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์

ผู้วิจัย ขอความกรุณาท่านได้ตอบแบบสอบถามตามความเป็นจริงในปัจจุบัน เพื่อให้ได้ข้อมูลที่แท้จริงและสมบูรณ์มากที่สุด ซึ่งการศึกษาวิจัยครั้งนี้จะสรุปออกมาในภาพรวม จะไม่มีผลกระทบต่อท่านและองค์กรแต่อย่างใด

ขอขอบพระคุณเป็นอย่างยิ่ง

นายสุทธิพันธุ์ ชวลิตเลขา

นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

มหาวิทยาลัยศรีปทุม

ส่วนที่ 1 ข้อมูลทั่วไปบุคลากรของกลุ่มตัวอย่าง

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงใน ☐ หน้าข้อความ ตามสภาพความเป็นจริง

1. เพศ

☐ ชาย ☐ หญิง

2. อายุ

☐ ต่ำกว่า 30 ปี ☐ 30-40 ปี
☐ 41-50 ปี ☐ 51-60 ปี
☐ 61 ปีขึ้นไป

3. ระดับการศึกษาสูงสุด

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี
☐ ปริญญาโท ☐ ปริญญาเอก

4. สายงานที่ปฏิบัติ

☐ ด้านปฏิบัติการ ☐ ด้านวิศวกรรม
☐ ด้านธุรการ ☐ ด้านอื่น ๆ

5. ท่านได้ปฏิบัติงานในหน่วยงานแห่งนี้มานานเท่าใด

☐ ไม่เกิน 5 ปี ☐ 6 – 10 ปี
☐ 11 – 15 ปี ☐ 16 ปีขึ้นไป

6. ท่านได้ใช้เวลาโดยเฉลี่ยอยู่กับคอมพิวเตอร์นานเท่าใด ในแต่ละวันของเวลาทำงาน

☐ น้อยกว่า 1 ชั่วโมงต่อวัน ☐ 1 - 3 ชั่วโมงต่อวัน
☐ 4 – 6 ชั่วโมงต่อวัน ☐ มากกว่า 6 ชั่วโมงต่อวัน

ส่วนที่ 2 พฤติกรรมการใช้งานระบบอินเทอร์เน็ต

คำชี้แจง โปรดพิจารณาข้อคำถามต่อไปนี้แล้วทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับความจริง ความคิดเห็นหรือความรู้สึกของท่านมากที่สุดเพียงช่องเดียว แบ่งระดับคำตอบเป็น 5 ระดับ ดังนี้

5 หมายถึง เป็นจริงหรือเห็นด้วยมากที่สุด

4 หมายถึง เป็นจริงหรือเห็นด้วยมาก

3 หมายถึง เป็นจริงหรือเห็นด้วยปานกลาง

2 หมายถึง เป็นจริงหรือเห็นด้วยน้อย

1 หมายถึง ไม่เป็นจริงหรือเห็นด้วยน้อยที่สุด

ผู้วิจัยขอขอบพระคุณอย่างสูงในความร่วมมือด้วยดีของท่านมา ณ โอกาสนี้

ข้อ	พฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด	ระดับความความคิดเห็น				
		5	4	3	2	1
ด้านพฤติกรรมการใช้อินเทอร์เน็ต						
1	การใช้อีเมลตนเองในการสมัครบัญชีออนไลน์					
2	การตั้งค่าบัญชีให้เป็นส่วนตัว					
3	การกรอกข้อมูลส่วนตัวตามอีเมลที่ส่งมา					
4	การดาวน์โหลดไฟล์โดยไม่ทราบแหล่งที่มาออนไลน์					
5	การเข้าเว็บไซต์ที่ไม่เหมาะสม					
ด้านพฤติกรรมการใช้งานสื่อสังคม						
1	การเผยแพร่ข้อความ รูปภาพ วีดิทัศน์ ลงในสื่อสาธารณะ					
2	อนุญาตให้บุคคลที่ไม่รู้จักเข้าถึงการใช้งานบน Social Media ของตนเอง					
3	ไม่จำกัดการเข้าถึงข้อมูลส่วนตัวในบัญชี Social Media					
ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์						
1	การเข้าถึงสื่อออนไลน์ที่ไม่รู้จักมาก่อน					
2	การเข้าถึงสื่อที่มีโฆษณาเชิญชวนไปยังเว็บไซต์อื่น					
3	การเข้าถึงสื่อออนไลน์ที่ไม่ได้รับการคัดกรอง					
4	การเข้าสื่อออนไลน์ที่ให้เปิดเผยข้อมูลส่วนตัวมากเกินไป					
ด้านพฤติกรรมการใช้งานผ่านโปรแกรม						
1	การใช้งานผ่านโปรแกรมที่ไม่มีลิขสิทธิ์					

ข้อ	พฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด	ระดับความความคิดเห็น				
		5	4	3	2	1
ด้านพฤติกรรมการใช้งานผ่านโปรแกรม						
2	การโหลดโปรแกรมที่ไม่มีลิขสิทธิ์จากแหล่งต่าง ๆ					
3	การติดตั้งโปรแกรมต่าง ๆ จากบุคคลอื่น					
4	การติดตั้งโปรแกรมโดยไม่ศึกษารายละเอียด					
ด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต						
1	มีโปรแกรมป้องกัน Spyware					
2	การเปิดการใช้งานโปรแกรม Firewall					
3	มีการสำรอง (Backup) ข้อมูลเป็นประจำ					
4	มีโปรแกรมสำหรับลบไฟล์แบบถาวร (Files Shredder)					

ส่วนที่ 3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

ข้อ	ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด	ระดับความตระหนักรู้				
		5	4	3	2	1
ความตระหนักรู้ด้านการใช้คอมพิวเตอร์ (Computer)						
1	มีการแยก User ใช้งานกันของแต่ละบุคคล					
2	Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์					
3	ติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ					
4	มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ					
5	มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ					
ความตระหนักรู้ด้านการใช้พาสเวิร์ด (Password)						
1	พาสเวิร์ดมีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #) และมีความยาวของ Password อย่างน้อย 8 ตัวอักษร					

ข้อ	ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด	ระดับความตระหนักรู้				
		5	4	3	2	1
ความตระหนักรู้ด้านการใช้พาสเวิร์ด (Password)						
2	มีการหลีกเลี่ยงใช้ Common Password หรือ Default Password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น password, 123456, วันเกิด, หมายเลขโทรศัพท์					
3	มีการเปลี่ยน Password อย่างสม่ำเสมอ ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้					
4	ไม่ใช้ Password ซ้ำกันในแต่ละระบบ รวมทั้งไม่ควรบอก Password แก่ผู้อื่น					
5	ไม่จด Password และติด Password ไว้ที่หน้าจอ					
ความตระหนักรู้ด้านการใช้อีเมล (E-mail)						
1	ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน					
2	ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน					
3	ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจสอบ					
4	เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการตรวจสอบผ่านทางช่องทางอื่น ๆ เพิ่มเติม					
ความตระหนักรู้ด้านการเข้าเว็บไซต์ (Website)						
1	ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ					
2	ไม่ทำการบันทึก Password ต่าง ๆ บน Browser เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือหากมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS และการใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox					
3	มีการ Update Version ของ Browser อย่างสม่ำเสมอ					
4	มีการใช้งาน Browser ในโหมด Safe Web Browsing รวมทั้งได้ติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ					
ความตระหนักรู้ด้านการใช้ Messaging						
1	ไม่บันทึก Password ไว้ที่โปรแกรม					

ข้อ	ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัททวิทยุการบินแห่งประเทศไทย จำกัด	ระดับความตระหนักรู้				
		5	4	3	2	1
ความตระหนักรู้ด้านการใช้ Messaging						
2	กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง					
3	มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่าง ๆ ที่ได้รับมา					
ความตระหนักรู้เกี่ยวข่าวปลอมในโลกไซเบอร์ (Fake News)						
1	ไม่อ่านข่าวที่ไม่ได้ระบุที่มาของข่าวไม่ได้					
2	ไม่อ่านข่าวที่ไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์					
ความตระหนักรู้ด้านการเก็บข้อมูลบนเครื่อง Server (Cloud Storage)						
1	ควรแยก User ในการใช้งานของแต่ละบุคคล					
2	ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็น และปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น					
3	ควรติดตั้ง Anti-Malware และ Update อย่างสม่ำเสมอ และควรมีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ					
ความตระหนักรู้ด้านเข้าประชุมทางออนไลน์ (Conference)						
1	การใช้สถานที่เหมาะสมกับการประชุม (Conference)					
2	การประชุม (Conference) ควรมีแต่ผู้ที่เกี่ยวข้อง					
3	ควรมีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ และควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม					
ความตระหนักรู้ในการใช้มือถือ (Mobile)						
1	ควรเปิดการใช้งาน PIN / Password, Face Scan หรือ Fingerprint					
2	การเข้าใช้งานอุปกรณ์ ไม่ติดตั้ง Application ที่น่าสงสัย หรือไม่รู้แหล่งที่มา					
3	การกำหนด Application permission ให้เหมาะสม					
4	ควรมีการ Update Patch ระบบปฏิบัติการ (OS) และมีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ					

ส่วนที่ 4 ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

ข้อ	ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด	ระดับความตระหนักรู้				
		5	4	3	2	1
ความมั่นคงปลอดภัย (Security)						
1	ควรมีการติดตั้งโปรแกรมป้องกัน Malware ในคอมพิวเตอร์ส่วนตัว					
2	ควรมีการป้องกันและตรวจสอบแหล่งที่มาของข้อมูลก่อนการกรอกข้อมูลส่วนตัว หรือคลิก Link ต่าง ๆ					
3	ควรหาทางวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กรจะถูกลักลอบเจาะเข้าสู่ระบบเพื่อแสวงประโยชน์					
การส่งข้อความซึ่งเต็มไปด้วยความโกรธ (Flaming)						
1	ไม่ควรกล่าวถึงหรือกล่าวหาผู้อื่นในทางเสียหายหรือทำให้ได้รับความอับอายในสื่อสังคมออนไลน์					
2	ไม่ควรใช้ข้อความหรือถ้อยคำที่หยาบคายในสื่อสังคมออนไลน์					
3	ไม่ควรล้อเลียนพฤติกรรม รูปร่างหน้าตาของผู้อื่นในสื่อสังคมออนไลน์					
4	ไม่ยั่วยุหรือปะทะคารมให้เกิดความเสียหายแก่ตนเองและผู้อื่นบนโลกออนไลน์					
การคุกคามหรือล่วงละเมิด (Harassment)						
1	ไม่ควรเผยแพร่ข่าวลือในด้านลบหรือข่าวเท็จของผู้อื่นผ่านทางสื่อสังคมออนไลน์					
2	ไม่ควรข่มขู่หรือใส่ร้ายผู้อื่นให้บุคคลที่สามเกลียดชังกันผ่านทางสื่อสังคมออนไลน์					
3	ไม่ควรนำภาพหรือคลิปวิดีโอของผู้อื่นที่จะก่อให้เกิดเสื่อมเสียไปเผยแพร่ผ่านทางสื่อสังคมออนไลน์					
การปลอมตัว (Masquerading) แอบอ้าง						
1	ไม่ควรมีการปลอมแปลงชื่อหรือภาพของผู้อื่นเพื่อให้ร้ายบุคคลที่สามผ่านทางสื่อสังคมออนไลน์					

ข้อ	ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด	ระดับความตระหนักรู้				
		5	4	3	2	1
การปลอมตัว (Masquerading) แอบอ้าง						
2	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นในการสนทนาผ่านทางสื่อสังคมออนไลน์					
3	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อผลประโยชน์ให้ตนเองผ่านทางสื่อสังคมออนไลน์					
การเผยแพร่ออกนอกกลุ่ม (Outing)						
1	ไม่ควรนำชื่อบุพการีหรือญาติพี่น้องของผู้อื่นไปเปิดเผยผ่านทางสื่อสังคมออนไลน์โดยไม่ได้รับอนุญาต					
2	ไม่ควรนำที่อยู่หรือข้อมูลส่วนตัวของผู้อื่นไปเผยแพร่ผ่านทางสื่อสังคมออนไลน์โดยไม่ได้รับอนุญาต					
3	ไม่ควรนำเบอร์โทรศัพท์และข้อมูลการทำงานของผู้อื่นไปเผยแพร่ผ่านทางสื่อสังคมออนไลน์โดยไม่ได้รับอนุญาต					
การกีดกัน (Exclusion)						
1	ไม่ควรปิดกั้นหรือบล็อกข้อความสนทนาของบุคคลที่ไม่ชอบในกลุ่มสนทนาทางสื่อสังคมออนไลน์					
2	ไม่ควรกดดันหรือลบรายชื่อบุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางสื่อสังคมออนไลน์					
3	ไม่สร้างกลุ่มเฉพาะออกมาโจมตีบุคคลที่ไม่ชอบทางสื่อสังคมออนไลน์					

ขอขอบพระคุณที่ท่านได้กรุณาเสียสละเวลาในการตอบแบบสอบถาม

ภาคผนวก ข
แบบตรวจสอบคุณภาพเครื่องมืองานวิจัย

แบบสอบถามการวิจัย
แบบตรวจสอบคุณภาพเครื่องมืองานวิจัย

เรื่อง การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากร ในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

คำชี้แจง : การวิจัยนี้ มุ่งเน้นศึกษา วิเคราะห์ ระดับความตระหนักรู้และความเข้าใจของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด เกี่ยวกับความเสี่ยงและภัยคุกคามทางไซเบอร์ เพื่อนำมาวิเคราะห์ และนำไปสู่การกำหนดแนวทางการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

แบบสอบถามฉบับนี้ แบ่งเป็น 4 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลทั่วไปบุคลากรของกลุ่มตัวอย่าง

ส่วนที่ 2 พฤติกรรมการใช้งานระบบอินเทอร์เน็ต

ส่วนที่ 3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ 4 ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์

<u>คำชี้แจง</u> : ให้ท่านพิจารณาว่า ข้อคำถามแต่ละข้อต่อไปนี้ มีความสอดคล้องกับวัตถุประสงค์ในการวัดหรือไม่ โดยให้ท่านทำเครื่องหมาย / ลงในช่องว่างหลังข้อคำถามแต่ละข้อ โดยมีเกณฑ์ในการพิจารณา ดังนี้

1 หมายถึง ท่านเห็นว่าข้อความนั้นมีความสอดคล้องกับวัตถุประสงค์

0 หมายถึง ท่านไม่แน่ใจว่าข้อคำถามนั้นมีความสอดคล้องกับวัตถุประสงค์หรือไม่

-1 หมายถึง ท่านเห็นว่าข้อความนั้นไม่สอดคล้องกับวัตถุประสงค์

ลงนามชื่อผู้เชี่ยวชาญ .....

(.....)

ส่วนที่ 2 พฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้ทรงคุณวุฒิคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

ข้อ	พฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด								
ด้านพฤติกรรมการใช้อินเทอร์เน็ต									
1	การใช้อีเมลตนเองในการสมัครบัญชีออนไลน์	1	1	1	1	0	0.8	ใช้ได้	
2	การตั้งค่าบัญชีให้เป็นส่วนตัว	1	1	1	1	1	1	ใช้ได้	
3	การกรอกข้อมูลส่วนตัวตามอีเมลที่ส่งมา	1	1	1	1	1	1	ใช้ได้	
4	การดาวน์โหลดไฟล์โดยไม่ทราบแหล่งที่มาออนไลน์	1	0	1	1	1	0.8	ใช้ได้	
5	การเข้าเว็บไซต์ที่ไม่เหมาะสม	1	0	1	1	1	0.8	ใช้ได้	
ด้านพฤติกรรมการใช้งานสื่อสังคม									
6	การเผยแพร่ข้อความ รูปภาพ วีดิทัศน์ ลงในสื่อสาธารณะ	1	1	-1	1	1	0.6	ใช้ได้	
7	อนุญาตให้บุคคลที่ไม่รู้จักเข้าถึงการใช้งานบน Social Media ของตนเอง	1	1	1	1	1	1	ใช้ได้	
8	ไม่จำกัดการเข้าถึงข้อมูลส่วนตัวในบัญชี Social Media	1	1	1	1	1	1	ใช้ได้	
ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์									
9	การเข้าถึงสื่อออนไลน์ที่ไม่รู้จักมาก่อน	1	0	1	1	1	0.8	ใช้ได้	
10	การเข้าถึงสื่อที่มีโฆษณาเชิญชวนไปยังเว็บไซต์อื่น	1	0	1	1	1	0.8	ใช้ได้	
11	การเข้าถึงสื่อออนไลน์ที่ไม่ได้รับการคัดกรอง	1	0	1	1	1	0.8	ใช้ได้	

ส่วนที่ 2 (ต่อ) พฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้ทรงคุณวุฒิคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

ข้อ	พฤติกรรมการใช้งานระบบอินเทอร์เน็ตของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด								
<u>ด้านพฤติกรรมการเข้าถึงสื่อออนไลน์</u>									
12	การเข้าสื่อออนไลน์ที่ให้เปิดเผยข้อมูลส่วนตัวมากเกินไป	1	1	1	1	1	1	ใช้ได้	
<u>ด้านพฤติกรรมการใช้งานผ่านโปรแกรม</u>									
13	การใช้งานผ่านโปรแกรมที่ไม่มีลิขสิทธิ์	1	0	1	1	1	0.8	ใช้ได้	
14	การโหลดโปรแกรมที่ไม่มีลิขสิทธิ์จากแหล่งต่าง ๆ	1	0	1	1	1	0.8	ใช้ได้	
15	การติดตั้งโปรแกรมต่าง ๆ จากบุคคลอื่น	1	1	1	1	0	0.8	ใช้ได้	
16	การติดตั้งโปรแกรมโดยไม่ศึกษารายละเอียด	1	0	1	1	1	0.8	ใช้ได้	
<u>ด้านพฤติกรรมการป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต</u>									
17	มีโปรแกรมป้องกัน Spyware	1	0	0	1	1	0.6	ใช้ได้	
18	การเปิดการใช้งานโปรแกรม Firewall	1	0	1	1	1	0.8	ใช้ได้	
19	มีการสำรอง (Backup) ข้อมูลเป็นประจำ	1	0	1	1	1	0.8	ใช้ได้	
20	มีโปรแกรมสำหรับลบไฟล์แบบถาวร (Files Shredder)	1	0	1	1	0	0.6	ใช้ได้	

ส่วนที่ 3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทยจำกัด

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้ทรงคุณวุฒิคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

ข้อ	ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด								
ความตระหนักรู้ด้านการใช้คอมพิวเตอร์ (Computer)									
21	มีการแยก User ใช้งานกันของแต่ละบุคคล	1	1	1	1	1	1	ใช้ได้	
22	Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์	1	1	1	1	1	1	ใช้ได้	
23	ติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ	1	0	1	1	1	0.8	ใช้ได้	
24	มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ	1	0	1	1	1	0.8	ใช้ได้	
25	มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ	1	0	1	1	1	0.8	ใช้ได้	
ความตระหนักรู้ด้านการใช้พาสเวิร์ด (Password)									
26	พาสเวิร์ดมีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #) และมีความยาวของ Password อย่างน้อย 8 ตัวอักษร	1	1	1	1	1	1	ใช้ได้	

ส่วนที่ 3 (ต่อ) ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้ทรงคุณวุฒิคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			
ข้อ	**ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด**							
<u>ความตระหนักรู้ด้านการใช้พาสเวิร์ด (Password)</u>								
27	มีการหลีกเลี่ยงใช้ Common Password หรือ Default Password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น password, 123456, วันเกิด, หมายเลขโทรศัพท์	1	1	1	1	1	1	ใช้ได้	
28	มีการเปลี่ยน Password อย่างสม่ำเสมอ ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้	1	1	1	1	1	1	ใช้ได้	
29	ไม่ใช้ Password ซ้ำกันในแต่ละระบบ รวมทั้งไม่ควรบอก Password แก่ผู้อื่น	1	1	1	1	1	1	ใช้ได้	
30	ไม่จด Password และติด Password ไว้ที่หน้าจอ	1	1	1	1	1	1	ใช้ได้	
<u>ความตระหนักรู้ด้านการใช้อีเมล (E-mail)</u>								
31	ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน	1	1	1	1	1	1	ใช้ได้	
32	ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน	1	1	1	1	1	1	ใช้ได้	
33	ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจสอบ	1	1	1	1	1	1	ใช้ได้	

ส่วนที่ 3 (ต่อ) ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม		ประมาณค่าความคิดเห็นผู้ทรงคุณวุฒิคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
		1	2	3	4	5			
ข้อ	**ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด**								
<u>ความตระหนักรู้ด้านการใช้อีเมล (E-mail)</u>									
34	เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการตรวจสอบผ่านทางช่องทางอื่น ๆ เพิ่มเติม	1	1	1	1	0	0.8	ใช้ได้	
<u>ความตระหนักรู้ด้านการเข้าเว็บไซต์ (Website)</u>									
35	ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ	1	0	1	1	1	0.8	ใช้ได้	
36	ไม่ทำการบันทึก Password ต่าง ๆ บน Browser เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือหากมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS และการใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox	1	1	1	1	1	1	ใช้ได้	
37	มีการ Update Version ของ Browser อย่างสม่ำเสมอ	1	0	1	1	1	0.8	ใช้ได้	
38	มีการใช้งาน Browser ในโหมด Safe Web Browsing รวมทั้งได้ติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ	1	1	1	1	0	0.8	ใช้ได้	

ส่วนที่ 3 (ต่อ) ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้ทรงคุณวุฒิคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

ข้อ	ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด								
ความตระหนักรู้ด้านการใช้ (Messaging)									
39	ไม่บันทึก Password ไว้ที่โปรแกรม	1	1	1	1	1	1	ใช้ได้	
40	กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง	1	1	1	1	1	1	ใช้ได้	
41	มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่าง ๆ ที่ได้รับมา	1	0	1	1	1	0.8	ใช้ได้	
42	มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ และไม่ควรแชร์ข้อมูลหรือข่าวสารต่าง ๆ โดยไม่ทราบที่มาของข้อมูล	1	0	-1	1	1	0.4	ปรับปรุง/ตัดทิ้ง	
ความตระหนักรู้เกี่ยวข่าวปลอมในโลกไซเบอร์ (Fake News)									
43	ไม่ดูข่าวที่มีการพาดหัวข่าวหรือข้อความที่เกินจริง	1	0	1	-1	1	0.4	ปรับปรุง/ตัดทิ้ง	
44	ไม่อ่านข่าวที่ไม่ได้ระบุที่มาของข่าวไม่ได้	1	0	1	1	0	0.6	ใช้ได้	
45	ไม่อ่านข่าวที่ไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์	1	0	1	1	0	0.6	ใช้ได้	
46	ไม่อ่านข่าวที่ใช้สำนวนการเขียนออกแนวการโฆษณา	1	0	0	1	0	0.4	ปรับปรุง/ตัดทิ้ง	

ส่วนที่ 3 (ต่อ) ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้ทรงคุณวุฒิคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

ข้อ	**ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด**								
<u>ความตระหนักรู้ด้านการเก็บข้อมูลบนเครื่อง Server (Cloud Storage)</u>									
47	ควรแยก User ในการใช้งานของแต่ละบุคคล	1	1	1	1	1	1	ใช้ได้	
48	ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็น และปิดการเข้าถึงไฟล์หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น	1	1	1	1	1	1	ใช้ได้	
49	ควรติดตั้ง Anti-Malware และ Update อย่างสม่ำเสมอ และควรมีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ	1	0	1	1	1	0.8	ใช้ได้	
<u>ความตระหนักรู้ด้านเข้าประชุมทางออนไลน์ (Conference)</u>									
50	การใช้สถานที่เหมาะสมกับการประชุม (Conference)	1	0	1	1	1	0.8	ใช้ได้	
51	การประชุม (Conference) ควรมีแต่ผู้ที่เกี่ยวข้อง	1	0	1	1	1	0.8	ใช้ได้	
52	การแชร์เอกสารต่าง ๆ อย่างระมัดระวัง และควรใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน	1	0	-1	1	1	0.4	ปรับปรุง/ตัดทิ้ง	

ส่วนที่ 3 (ต่อ) ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้ทรงคุณวุฒิคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

ข้อ	ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด								
<u>ความตระหนักรู้ด้านเข้าประชุมทางออนไลน์ (Conference)</u>									
53	ควรมีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ และควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม	1	1	1	1	1	1	ใช้ได้	
<u>ความตระหนักรู้ในการใช้มือถือ (Mobile)</u>									
54	ควรเปิดการใช้งาน PIN / Password, Face Scan หรือ Fingerprint	1	1	1	1	1	1	ใช้ได้	
55	การเข้าใช้งานอุปกรณ์ ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา	1	0	1	1	1	0.8	ใช้ได้	
56	การกำหนด Application permission ให้เหมาะสม	1	0	1	1	1	0.8	ใช้ได้	
57	ควรมีการ Update Patch ระบบปฏิบัติการ (OS) และมีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ	1	0	1	1	1	0.8	ใช้ได้	

ส่วนที่ 4 ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้ทรงคุณวุฒิคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

ข้อ	ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด								
ความมั่นคงปลอดภัย (Security)									
58	ควรมีการติดตั้งโปรแกรมป้องกัน Malware ในคอมพิวเตอร์ส่วนตัว	1	1	1	1	1	1	ใช้ได้	
59	ควรมีการป้องกันและตรวจสอบแหล่งที่มาของข้อมูลก่อนการกรอกข้อมูลส่วนตัวหรือคลิก Link ต่าง ๆ	1	1	1	1	1	1	ใช้ได้	
60	ควรหาทางวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กรจะถูกลักลอบเจาะเข้าสู่ระบบเพื่อแสวงประโยชน์	1	1	1	1	1	1	ใช้ได้	
การส่งข้อความซึ่งเต็มไปด้วยความโกรธ (Flaming)									
61	ไม่ควรกล่าวถึงหรือกล่าวหาผู้อื่นในทางเสียหายหรือทำให้ได้รับความอับอายในสื่อสังคมออนไลน์	1	1	1	1	1	1	ใช้ได้	
62	ไม่ควรใช้ข้อความหรือถ้อยคำที่หยาบคายในสื่อสังคมออนไลน์	1	1	1	1	1	1	ใช้ได้	
63	ไม่ควรล้อเลียนพฤติกรรมรูปร่างหน้าตาของผู้อื่นในสื่อสังคมออนไลน์	1	1	1	1	1	1	ใช้ได้	
64	ไม่ยั่วยุหรือปะทะคารมให้เกิดความเสียหายแก่ตนเองและผู้อื่นบนโลกออนไลน์	1	1	1	1	1	1	ใช้ได้	

ส่วนที่ 4 (ต่อ) ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้ทรงคุณวุฒิคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

ข้อ	ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด								
การคุกคามหรือล่วงละเมิด (Harassment)									
65	ไม่ควรเผยแพร่ข่าวลือในด้านลบหรือข่าวเท็จของผู้อื่นผ่านทางสื่อสังคมออนไลน์	1	1	1	1	1	1	ใช้ได้	
66	ไม่ควรข่มขู่หรือใส่ร้ายผู้อื่นให้บุคคลที่สามเกลียดชังกันผ่านทางสื่อสังคมออนไลน์	1	1	1	1	1	1	ใช้ได้	
67	ไม่ควรนำภาพหรือคลิปวิดีโอของผู้อื่นที่จะก่อให้เกิดเสื่อมเสียไปเผยแพร่ผ่านทางสื่อสังคมออนไลน์	1	1	1	1	1	1	ใช้ได้	
การปลอมตัว (Masquerading) แอบอ้าง									
68	ไม่ควรมีการปลอมแปลงชื่อหรือภาพของผู้อื่นเพื่อให้ร้ายบุคคลที่สามผ่านทางสื่อสังคมออนไลน์	1	1	1	1	1	1	ใช้ได้	
69	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นในการสนทนาผ่านทางสื่อสังคมออนไลน์	1	1	1	1	1	1	ใช้ได้	
70	ไม่ควรมีการแอบอ้างชื่อหรือภาพของผู้อื่นเพื่อผลประโยชน์ให้ตนเองผ่านทางสื่อสังคมออนไลน์	1	1	1	1	1	1	ใช้ได้	

ส่วนที่ 4 (ต่อ) ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

คำชี้แจง โปรดทำเครื่องหมาย 1 หรือ 0 หรือ -1 ตามความคิดเห็นของท่านลงในช่องว่างหลังข้อคำถามแต่ละข้อ

ข้อคำถาม	ประมาณค่าความคิดเห็นผู้ทรงคุณวุฒิคนที่					ค่า IOC	การแปลผล	ข้อเสนอแนะเพิ่มเติม
	1	2	3	4	5			

ข้อ	ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด								
การเผยแพร่ออกนอกกลุ่ม (Outing)									
71	ไม่ควรนำชื่อบุพการีหรือญาติพี่น้องของผู้อื่นไปเปิดเผยผ่านทางสื่อสังคมออนไลน์โดยไม่ได้รับอนุญาต	1	1	1	1	1	1	ใช้ได้	
72	ไม่ควรนำที่อยู่หรือข้อมูลส่วนตัวของผู้อื่นไปเผยแพร่ผ่านทางสื่อสังคมออนไลน์โดยไม่ได้รับอนุญาต	1	1	1	1	1	1	ใช้ได้	
73	ไม่ควรนำเบอร์โทรศัพท์และข้อมูลการทำงานของผู้อื่นไปเผยแพร่ผ่านทางสื่อสังคมออนไลน์โดยไม่ได้รับอนุญาต	1	1	1	1	1	1	ใช้ได้	
การกีดกัน (Exclusion)									
74	ไม่ควรปิดกั้นหรือบล็อกข้อความสนทนาของบุคคลที่ไม่ชอบในกลุ่มสนทนาทางสื่อสังคมออนไลน์	1	0	1	1	1	0.8	ใช้ได้	
75	ไม่ควรกดดันหรือลบรายชื่อบุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางสื่อสังคมออนไลน์	1	1	1	1	1	1	ใช้ได้	
76	ไม่สร้างกลุ่มเฉพาะออกมาโจมตีบุคคลที่ไม่ชอบทางสื่อสังคมออนไลน์	1	1	1	1	1	1	ใช้ได้	

ภาคผนวก ค

แบบประเมินแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

แบบประเมินแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

คำชี้แจง : แบบประเมินนี้ได้จัดทำขึ้นเพื่อสอบถามความคิดเห็นของผู้บริหารและผู้ทรงคุณวุฒิทางด้านเทคโนโลยีดิจิทัล เกี่ยวกับ**ความเหมาะสมของแนวทางการเสริมสร้างความตระหนักรู้และการยอมรับแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด** ซึ่งเป็นส่วนหนึ่งของการวิจัยในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

ผู้วิจัยจึงใคร่ขอความร่วมมือให้ท่านผู้บริหารและผู้ทรงคุณวุฒิตอบแบบสอบถามทุกข้อด้วยตัวของท่านเอง โดยให้ข้อมูล หรือแสดงความคิดเห็นที่ตรงกับความเป็นจริง ความรู้สึก หรือความคิดเห็นของท่านมากที่สุด ข้อมูลที่ได้จะนำไปใช้ประกอบการศึกษาและจะใช้เพื่อประโยชน์ทางวิชาการเท่านั้น ผู้วิจัยขอรับรองว่าจะไม่มีผลกระทบหรือก่อให้เกิดความเสียหายต่อตัวท่านแต่ประการใด ข้อคำถามในแบบสอบถาม แบ่งออกเป็น 2 ส่วน คือ

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบประเมิน

ส่วนที่ 2 ระดับความคิดเห็นโดยรวมของผู้ทรงคุณวุฒิที่มีต่อแนวทางการเสริมสร้างความตระหนักรู้และแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ผู้วิจัย ขอขอบพระคุณอย่างสูงในความร่วมมือด้วยดีของท่านมา ณ โอกาสนี้

นายสุทธิพันธุ์ ชวลิตเลขา โทรศัพท์ 06-3542-9291 E-Mail : Jackie.Angelo@hotmail.com

นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

มหาวิทยาลัยศรีปทุม

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบประเมิน

1.ชื่อ-สกุล.....

2. ตำแหน่งงานของท่าน (โปรดระบุ) .....

.....

3. ระยะเวลาของประสบการณ์ที่ท่านได้ทำงานด้านเทคโนโลยีดิจิทัล

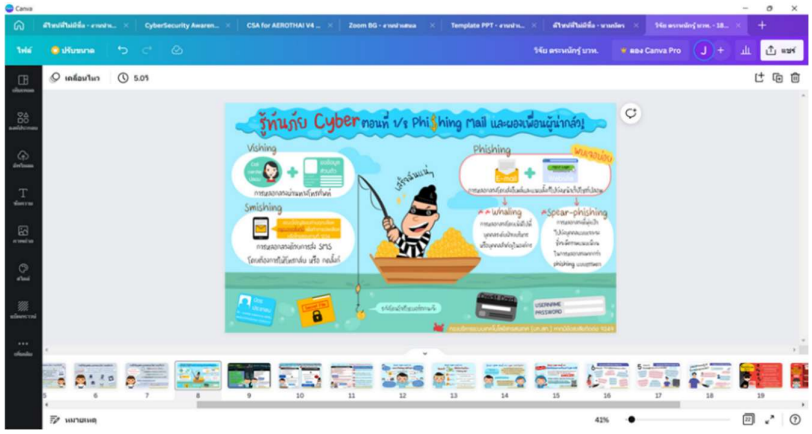
☐ น้อยกว่า 1 ปี ☐ 1-3 ปี

☐ 3-5 ปี ☐ มากกว่า 5 ปี

ส่วนที่ 2 ระดับความคิดเห็นโดยรวมของผู้ทรงคุณวุฒิที่มีต่อแอปพลิเคชันการประเมินระดับตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

<u>คำชี้แจง</u>

จากผลการวิเคราะห์ข้อมูลจากการสัมภาษณ์เชิงลึกกับผู้บริหารและผู้เชี่ยวชาญด้านระบบสารสนเทศของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ได้แนวทางการเสริมสร้างความตระหนักรู้ควรใช้วิธีการเรียนรู้แบบออนไลน์และวิธีกสรเรียนโดยใช้วีดิทัศน์ผสมผสานกัน ซึ่งผู้วิจัยได้จัดทำหลักสูตรการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และจัดทำสื่อด้วยโปรแกรม Microsoft PowerPoint และ โปรแกรม Canva for Windows เพื่อการเรียนรู้ในรูปแบบออนไลน์ผ่าน Web Application บนดิจิทัลแพลตฟอร์ม AEROTHAI Learning Management System (AEROTHAI LMS) ภายในเครือข่ายอินทราเน็ตของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด เป็นแพลตฟอร์มสำหรับการเรียนรู้ออนไลน์ เป็นระบบและบริการการเรียนทางอิเล็กทรอนิกส์ สนับสนุนการเรียนรู้ซึ่งมีเป้าหมายที่จะพัฒนาบุคลากรให้มีประสิทธิภาพในการทำงานเพิ่มมากขึ้น ทุกคนในองค์กรสามารถเข้าถึงคอร์สเรียนต่าง ๆ และนั่งเรียนได้ทุกที่ทุกเวลา ดังภาพประกอบต่อไปนี้



ภาพประกอบที่ 1 แสดงการจัดทำ Info Graphics ตามเนื้อหาหลักสูตร

ภาพประกอบที่ 2 แสดงการจัดทำสื่อการสร้างความตระหนักรู้สำหรับการเรียนรู้ในรูปแบบออนไลน์

ภาพประกอบที่ 3 แสดงการติดตั้งใช้งานบนดิจิทัลแพลตฟอร์ม AEROTHAI Learning Management System

1. “แนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด” ตาม**ภาพประกอบที่ 1 - 3 มีความเหมาะสม อยู่ในระดับใด (☐ 5 ----- ☐ 4----- ☐ 3---- ☐ 2 -----☐ 1)** หรือควรต้องทำการปรับปรุงอย่างไร เพราะเหตุใด

.....

.....

.....

2. “แอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด” ตาม**ภาพประกอบที่ 1 - 3 มีระดับการยอมรับ อยู่ในระดับใด (☐ 5 ----- ☐ 4----- ☐ 3---- ☐ 2 -----☐1)** เพราะเหตุใด

.....

.....

.....

4. ข้อเสนอแนะอื่น ๆ ต่อสิ่งที่ควรปรับปรุงใน **“แอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด”** ควรมีอะไรบ้าง

.....

.....

.....

ภาคผนวก ง

การประชุมวิชาการระดับชาติและนานาชาติ ประจำปี 2565

วันศุกร์ที่ 1 กรกฎาคม 2565 ณ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี
SRIPATUM UNIVERSITY AT CHONBURI

ที่ มศป.ชบ 0521.2 / ว 1262

มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี
79 ถนนบางนา-ตราด ตำบลคลองตำหรุ
อำเภอเมือง จังหวัดชลบุรี 20000

21 มิถุนายน 2565

เรื่อง ตอบรับการนำเสนอผลงานทางวิชาการ

เรียน นายสุทธิพันธุ์ ชาลิตเลขา

ตามที่ท่านส่งผลงานทางวิชาการเพื่อนำเสนอในประชุมวิชาการระดับชาติ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี ประจำปี 2565 เรื่อง งานวิจัยและนวัตกรรมเพื่อการขับเคลื่อนยุคเศรษฐกิจดิจิทัล วันศุกร์ที่ 1 กรกฎาคม 2565 แบบออนไลน์ ความละเอียดทราบแล้วนั้น

มหาวิทยาลัยฯ ขอแจ้งให้ทราบว่าผลงานทางวิชาการของท่าน ผ่านการประเมินจากผู้ทรงคุณวุฒิ และให้นำเสนอในการประชุมดังกล่าว ท่านสามารถตรวจสอบวัน และเวลาการนำเสนอได้ที่ https://www.chonburi.spu.ac.th/spuccon2022/ ตั้งแต่วันจันทร์ที่ 27 มิถุนายน 2565 เป็นต้นไป

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

(รองศาสตราจารย์กาญจนา มณีแสง)
รองอธิการบดีฝ่ายวิจัยและแผน ปฏิบัติหน้าที่แทน
รองอธิการบดี วิทยาเขตชลบุรี

สำนักงานวิจัยและพัฒนานวัตกรรม
โทรศัพท์ 0-3814-6123 ต่อ 2506, 2507
โทรสาร 0-3814-6011 (บริการวันอาทิตย์-จันทร์)
e-mail : research@chonburi.spu.ac.th

มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

ขอมอบเกียรติบัตรนี้ไว้เพื่อแสดงว่า

สุทธิพันธุ์ ชวลิตเลขา

ได้นำเสนอผลงานวิชาการภาคบรรยาย

เรื่อง การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบิน

แห่งประเทศไทย จำกัด

ในการประชุมวิชาการระดับชาติและนานาชาติ ประจำปี 2565 (2022 **SPUC National and International Conference**)

เรื่อง งานวิจัยและนวัตกรรมเพื่อการขับเคลื่อนยุคเศรษฐกิจดิจิทัล

(Research and Innovation to forward the digital economy era)

วันศุกร์ที่ 1 กรกฎาคม 2565

ณ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

(ดร.บุษบา ชัยจินดา)

รองอธิการบดี วิทยาเขตชลบุรี

ภาคผนวก จ
โครงการเปิดบ้านสานฝัน ปีที่ 6

การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

STRENGTHENING CYBERSECURITY AWARENESS FOR PERSONNEL IN AERONAUTICAL RADIO OF THAILAND CO., LTD.

SPU SRIPATUM UNIVERSITY

คณะเทคโนโลยีสารสนเทศ School of Information Technology Sripatum University


นายสุทธิพันธุ์ ชวลิตเลขา
ผู้วิจัย


ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง
อาจารย์ที่ปรึกษา


ดร.สุรชัย ทองแก้ว
อาจารย์ที่ปรึกษา

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาสภาพปัญหา พฤติกรรมการใช้งานบนโลกไซเบอร์ พัฒนาแนวทางการเสริมสร้างและจัดทำแอปพลิเคชันการประเมินระดับความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด กลุ่มตัวอย่างคือบุคลากรในบริษัทวิทยุการบินฯ จำนวน 99 คน เครื่องมือที่ใช้ในการวิจัย ได้แก่ แบบสัมภาษณ์แบบกึ่งโครงสร้างและแบบสอบถามปลายปิด ผลวิจัยพบว่า ผู้บังคับบัญชาของบริษัทวิทยุการบินฯ ให้ความสำคัญกับนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ มีการระบุภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อการปฏิบัติงานโดยตรง ภาพรวมความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับมากที่สุด ในส่วนการพัฒนาแนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ พบว่าบุคลากรในบริษัทวิทยุการบินฯ มีต้องการสร้างความตระหนักรู้ด้วยวิธีการเรียนรู้แบบออนไลน์และวิดีทัศน์ผสมผสานกัน

ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันภัยคุกคามด้านไซเบอร์จะยังคงเป็นภัยคุกคามที่มีแนวโน้มเพิ่มขึ้นแล้วยังมีการใช้เทคโนโลยีที่มีวิวัฒนาการสูงขึ้น บริษัทวิทยุการบินแห่งประเทศไทย จำกัด ตระหนักถึงความมั่นคงปลอดภัยของโลกไซเบอร์เป็นปัจจัยสำคัญที่จะสร้างความเชื่อมั่นให้กับผู้ใช้บริการ กอปรกับมีการกำหนดวิสัยทัศน์ดิจิทัล "ให้เป็นองค์กรดิจิทัลที่ให้บริการการเดินอากาศด้วยคุณภาพสูงสุดอย่างยั่งยืน" (คณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทวิทยุการบินแห่งประเทศไทย จำกัด, 2564) ผู้วิจัยจึงศึกษาการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด และนำผลวิจัยไปนำเสนอแนวทางพัฒนาการเสริมสร้างความตระหนักรู้และจัดทำแอปพลิเคชันสำหรับประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาสภาพปัญหาและพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ที่มีความเสี่งด้านความมั่นคงปลอดภัยไซเบอร์
2. เพื่อพัฒนาแนวทางการเสริมสร้างความตระหนักรู้แก่บุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ถึงความเสี่งและภัยคุกคามจากการใช้งานบนโลกไซเบอร์
3. เพื่อจัดทำแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

ประโยชน์ของงานวิจัย

1. สามารถลดความเสี่งและความเสียหายจากการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด ในด้านความมั่นคงปลอดภัยไซเบอร์
2. การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด จากการใช้งานบนโลกไซเบอร์ เป็นประโยชน์ต่อบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด และสามารถให้ความรู้ต่อบุคคลใกล้ตัวได้
3. สามารถใช้เป็นต้นแบบวิธีการประเมินความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ได้

ขอบเขตของการวิจัย

งานวิจัยนี้ เป็นการศึกษาพฤติกรรม และความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อวิเคราะห์และพัฒนาแนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และพัฒนาแอพพลิเคชั่นสำหรับประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

วิธีดำเนินการวิจัย

1. ศึกษาและรวบรวมข้อมูล ทฤษฎีที่เกี่ยวข้อง
2. สัมภาษณ์เชิงลึกแบบกึ่งโครงสร้างกับผู้บริหารเพื่อทราบถึงปัญหาและแนวทางการเสริมสร้างความตระหนักรู้
3. ใช้แบบสอบถามปลายปิดเพื่อวิเคราะห์พฤติกรรม
4. วิเคราะห์ ออกแบบและพัฒนาแอปพลิเคชันการเสริมสร้างและประเมินความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์
5. ติดตั้งแอปพลิเคชันบนแพลตฟอร์ม AEROTHAI Learning Management System ระบบการเรียนรู้ออนไลน์ภายในองค์กร
6. เสริมสร้างและประเมินระดับความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

การวิเคราะห์ ออกแบบ และพัฒนาแอปพลิเคชัน

ผู้วิจัยได้ทำการวิเคราะห์ระบบเชิงวัตถุ แล้วพัฒนาแอปพลิเคชันโดยใช้วงจรการพัฒนาระบบงาน (System Development Life Cycle : SDLC)

Use Case Diagram

ผลการวิจัย

ผลการประเมินพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

จากการสำรวจระดับพฤติกรรมการใช้งานบนโลกไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำนวน 99 คน ซึ่งพบว่า มีความเสี่งด้านความมั่นคงปลอดภัยไซเบอร์ อยู่ในระดับมาก สามารถแสดงได้ดังตารางที่ 1

ตารางที่ 1 ผลการประเมินพฤติกรรมการใช้งานบนโลกไซเบอร์

รายการประเมิน	$\bar{X}$	S.D.	ระดับพฤติกรรมการใช้งานบนโลกไซเบอร์
1. การใช้อินเทอร์เน็ต	4.01	0.23	มาก
2. การใช้งานสื่อสังคม	4.00	0.06	มาก
3. การเข้าซื้อสื่อออนไลน์	4.24	0.10	มากที่สุด
4. การใช้งานผ่านโปรแกรม	4.11	0.13	มาก
5. การป้องกันตนเองจากภัยคุกคามอินเทอร์เน็ต	3.62	0.10	มาก
สรุประดับพฤติกรรม	4.00	0.06	มาก

ผลการประเมินระดับความตระหนักรู้ถึงความมั่นคงปลอดภัยและภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

จากการสำรวจระดับความตระหนักรู้ทางไซเบอร์ของบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำนวน 99 คน สามารถแสดงได้ดังตารางที่ 2 และ 3

ตารางที่ 2 ผลการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

รายการประเมิน	$\bar{X}$	S.D.	ระดับความตระหนักรู้
1. ด้านการใช้คอมพิวเตอร์	4.17	0.10	มาก
2. ด้านการใช้พาสเวิร์ด	4.19	0.23	มาก
3. ด้านการใช้อีเมล	4.39	0.06	มากที่สุด
4. ด้านการเข้าเว็บไซต์	4.24	0.09	มากที่สุด
5. ด้านการใช้ Messaging	4.38	0.08	มากที่สุด
6. เกี่ยวข้องกับคอมโนโลยีไซเบอร์	4.25	0.02	มากที่สุด
7. ด้านการเก็บข้อมูลบนเครื่อง Server	4.37	0.03	มากที่สุด
8. ด้านเข้าประชุมทางออนไลน์	4.47	0.03	มากที่สุด
9. ด้านการใช้มือถือ	4.45	0.04	มากที่สุด
สรุประดับความตระหนักรู้	4.32	0.07	มากที่สุด

ตารางที่ 3 ผลการประเมินระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์

รายการประเมิน	$\bar{X}$	S.D.	ระดับความตระหนักรู้
1. ด้านความมั่นคงปลอดภัย (Security)	4.56	0.13	มากที่สุด
2. ด้านการส่งข้อความเชิงเดือดด้วยความโกรธ (Flaming)	4.64	0.05	มากที่สุด
3. ด้านการคุกคามหรือล่วงละเมิด (Harassment)	4.66	0.03	มากที่สุด
4. ด้านการปลอมตัว (Masquerading) แอบอ้าง	4.72	0.02	มากที่สุด
5. ด้านการเผยแพร่ออกนอกกลุ่ม (Outing)	4.71	0.03	มากที่สุด
6. ด้านการกีดกัน (Exclusion)	4.24	0.12	มากที่สุด
สรุประดับความตระหนักรู้	4.59	0.05	มากที่สุด

ผลการจัดทำแอปพลิเคชันการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด

โดยการทำลิงค์ดิจิทัลแพลตฟอร์มการเสริมสร้างและประเมินระดับความตระหนักรู้ ด้วยแพลตฟอร์ม Learning Management System (LMS) เป็นระบบการเรียนรู้ออนไลน์ภายในองค์กร

สรุปผลการวิจัย

สรุปผลการวิเคราะห์ข้อมูลจากการวิจัยเชิงคุณภาพและการวิจัยเชิงปริมาณได้ผลวิจัยดังนี้ มีการระบุให้มีการเสริมสร้างความตระหนักรู้ด้วยวิธีการเรียนรู้ออนไลน์ซึ่งผู้วิจัยได้ออกแบบพัฒนาระบบและติดตั้งแอปพลิเคชันใช้งานบนแพลตฟอร์ม AEROTHAI Learning Management System ภายในองค์กร ซึ่งสามารถสร้างความตระหนักรู้ได้ผลลัพธ์ตามวัตถุประสงค์ของการวิจัย โดยมีระดับพฤติกรรมการใช้งานบนโลกไซเบอร์ โดยรวมอยู่ในระดับ มาก ระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ โดยรวมอยู่ในระดับ มากที่สุด และด้านภัยคุกคามทางไซเบอร์ โดยรวมอยู่ในระดับ มากที่สุด

เอกสารอ้างอิง

คณะอนุกรรมการเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท วิทยุการบินแห่งประเทศไทย จำกัด. (2564). นโยบายดิจิทัล. กรุงเทพฯ : บริษัทวิทยุการบินแห่งประเทศไทย จำกัด.

สุธาเทพ รุณเรส. (2561). ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร. การค้นคว้าอิสระหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชานโยบายและการบริหารเทคโนโลยีสารสนเทศ วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์.

Tero Haukilehto. (2019). Improving Cyber Security awareness. J AMK University

คณะเทคโนโลยีสารสนเทศ
School of Information Technology
Sripatum University

คณะเทคโนโลยีสารสนเทศ

มหาวิทยาลัยศรีปทุม

ขอมอบเกียรติบัตรฉบับนี้เพื่อแสดงว่า

นาย สุทธิพันธุ์ ชวลิตเลขา

ได้เข้าร่วมนำเสนอผลงานทางวิชาการในโครงการเปิดบ้านสานฝัน ปีที่ 6
หัวข้อเรื่อง "การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์
สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด"

วันอาทิตย์ที่ 10 กรกฎาคม 2565

(ผู้ช่วยศาสตราจารย์ ดร.ธนา สุขวารี)
คณบดีคณะเทคโนโลยีสารสนเทศ

ประวัติผู้วิจัย

ชื่อ-สกุล นายสุทธิพันธุ์ ชวลิตเลขา

วันเดือนปี เกิด 25 สิงหาคม 2510

ที่อยู่ปัจจุบัน 51/61 ถนนเพชรเกษม ตำบลหัวหิน อำเภอหัวหิน
จังหวัดประจวบคีรีขันธ์ 77110

วุฒิการศึกษา พ.ศ. 2565 วิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
พ.ศ. 2541 คณะครุศาสตร์อุตสาหกรรม
สาขาวิชา วิศวกรรมอิเล็กทรอนิกส์-โทรคมนาคม
มหาวิทยาลัยเทคโนโลยีราชมงคลเทคนิคกรุงเทพ

ประสบการณ์ทำงาน พ.ศ. 2558 - ปัจจุบัน
วิศวกรบริหารระบบจราจรทางอากาศ (ภูมิภาค) ศูนย์ควบคุมการบินหัวหิน
บริษัทวิทยุการบินแห่งประเทศไทย จำกัด
พ.ศ. 2556 – 2558
วิศวกรบริหารระบบ ศูนย์ควบคุมการบินหัวหิน
บริษัทวิทยุการบินแห่งประเทศไทย จำกัด
พ.ศ. 2553 – 2556
วิศวกรระบบอาวุโส ศูนย์ควบคุมการบินหัวหิน
บริษัทวิทยุการบินแห่งประเทศไทย จำกัด

พ.ศ. 2546 – 2553
วิศวกรระบบอาวุโส ฝ่ายบริหารส่วนภูมิภาค 1
บริษัทวิทยุการบินแห่งประเทศไทย จำกัด
พ.ศ. 2539 – 2546
วิศวกรระบบอาวุโส กองวิศวกรรมระบบติดตามอากาศยาน
บริษัทวิทยุการบินแห่งประเทศไทย จำกัด
พ.ศ. 2537 – 2539
วิศวกรระบบเรดาร์ กองช่างระบบเรดาร์
บริษัทวิทยุการบินแห่งประเทศไทย จำกัด
พ.ศ. 2535 – 2537
ช่างระบบ 1 กองช่างระบบเรดาร์
บริษัทวิทยุการบินแห่งประเทศไทย จำกัด
พ.ศ. 2532 – 2535
ช่างซ่อมบำรุง 1 กองช่างระบบเรดาร์
บริษัทวิทยุการบินแห่งประเทศไทย จำกัด

สถานที่ทำงานปัจจุบัน ศูนย์ควบคุมการบินหัวหิน บริษัทวิทยุการบินแห่งประเทศไทย จำกัด

ผลงานวิชาการที่ได้รับการตีพิมพ์

[1] สุทธิพันธุ์ ชวลิตเลขา, ประสงค์ ปราณีตพลกรัง และสุรชัย ทองแก้ว **“การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด”** การประชุมวิชาการระดับชาติและนานาชาติ ประจำปี 2565 เรื่อง งานวิจัยและนวัตกรรมเพื่อการขับเคลื่อนเศรษฐกิจยุคดิจิทัล, 1 กรกฎาคม 2565 ณ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี