การพัฒนาแพลตฟอร์มชุมชนเพื่อเสริมสร้างวัฒนธรรมความปลอดภัยไซเบอร์

นางสาววราพร นิ่มนวล

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568

การพัฒนาแพลตฟอร์มชุมชนเพื่อเสริมสร้างวัฒนธรรมความปลอดภัยไซเบอร์

นางสาววราพร นิ่มนวล

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568

ใบรับรองการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การพัฒนาแพลตฟอร์มชุมชนเพื่อเสริมสร้างวัฒนธรรมความปลอดภัยไซเบอร์

โดย นางสาววราพร นิ่มนวล

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

..... คณบดีบัณฑิตวิทยาลัย / หัวหน้าภาควิชา

(ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี)

คณะกรรมการสอบการค้นคว้าอิสระ

..... ประธานกรรมการ

(รองศาสตราจารย์ ดร.สุมิตรา นวลมีศรี)

..... อาจารย์ที่ปรึกษา

(ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี)

ชื่อ : นางสาววราพร นิ่มนวล
ชื่อการค้นคว้าอิสระ : การพัฒนาแพลตฟอร์มชุมชนเพื่อเสริมสร้างวัฒนธรรมความปลอดภัยไซเบอร์
สาขาวิชา : การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์
ปีการศึกษา : 2568

บทคัดย่อ

การค้นคว้าอิสระนี้มีวัตถุประสงค์เพื่อพัฒนาแพลตฟอร์มชุมชนที่เสริมสร้างวัฒนธรรมความปลอดภัยไซเบอร์ในองค์กร โดยเน้นการมีส่วนร่วมของบุคลากรในการแลกเปลี่ยนข้อมูล ประสบการณ์ และองค์ความรู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ ภายใต้แนวคิดที่ว่าการสร้างวัฒนธรรมความปลอดภัยไซเบอร์ต้องอาศัยความร่วมมือและการสื่อสารที่มีประสิทธิภาพ ไม่ใช่เพียงการพึ่งพามาตรการทางเทคนิคเพียงอย่างเดียว

เครื่องมือหลักในการพัฒนาแพลตฟอร์มคือ Microsoft OneNote ซึ่งเป็นส่วนหนึ่งของชุดซอฟต์แวร์ Microsoft 365 ที่บุคลากรใช้งานอยู่เป็นประจำ โดยแพลตฟอร์มดังกล่าวสามารถสนับสนุนการรวบรวม จัดการ และเผยแพร่เนื้อหาได้หลากหลายรูปแบบ ทั้งยังเชื่อมโยงการทำงานร่วมกับเครื่องมืออื่น ๆ เช่น Microsoft Forms, SharePoint และ Microsoft Teams ได้อย่างมีประสิทธิภาพ

การค้นคว้าอิสระนี้ใช้แนวทางการพัฒนาเชิงทดลอง โดยการออกแบบแพลตฟอร์มเพื่อนำเสนอเนื้อหาเกี่ยวกับข่าวสารไซเบอร์ กรณีศึกษา เทคนิคการป้องกันภัย คำแนะนำจากผู้เชี่ยวชาญและพื้นที่สำหรับแลกเปลี่ยนประสบการณ์ พร้อมกันนี้ยังได้ดำเนินการทดสอบการใช้งานแพลตฟอร์มกับกลุ่มเป้าหมายภายในองค์กร และประเมินผลด้วยแบบสอบถามความพึงพอใจ แบบทดสอบความรู้ และการวิเคราะห์ปริมาณการมีส่วนร่วม

แพลตฟอร์มชุมชนที่สร้างขึ้นนี้ สามารถนำมาใช้เป็นช่องทางการสื่อสารด้านความปลอดภัยไซเบอร์ที่เข้าถึงง่ายและมีประสิทธิภาพ เพื่อเพิ่มความตระหนักรู้และความเข้าใจของบุคลากรเกี่ยวกับภัยคุกคามทางไซเบอร์ และการส่งเสริมให้เกิดพฤติกรรมการใช้งานระบบสารสนเทศอย่างปลอดภัยและยั่งยืนภายในองค์กร

(มีจำนวนทั้งสิ้น 98 หน้า)

คำสำคัญ : แพลตฟอร์มชุมชน ความปลอดภัยไซเบอร์ ฟิชชิ่ง การตอบสนองภัยคุกคาม การตระหนักรู้

_____ อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Miss Waraphon Nimnuan
Independent Study Title : Development of a Community Platform to Foster Cybersecurity Culture
Major Field : Network and Information Security Management
King Mongkut's University of Technology North Bangkok
Independent Study Advisor : Assistant Professor Dr. Nawaporn Wisitpongphan
Academic Year : 2025

ABSTRACT

This independent study aims to develop a community platform that fosters a cybersecurity culture within an organization, emphasizing employee participation in sharing information, experiences, and knowledge related to cyber threats. The study is based on the premise that building a strong cybersecurity culture requires effective collaboration and communication not solely reliance on technical measures.

The core tool used for platform development is Microsoft OneNote, which is a part of the Microsoft 365 suite that is widely used in the organization. OneNote supports the collection, organization, and dissemination of diverse content formats and seamlessly integrates with other tools such as Microsoft Forms, SharePoint, and Microsoft Teams to enhance collaboration and communication.

An experimental development approach was adopted, involving the design and creation of content related to cybersecurity news, case studies, threat prevention techniques, expert recommendations, and a space for knowledge exchange. The platform was tested with a target group of internal personnel and evaluated using satisfaction surveys, knowledge tests, and analysis of participation levels.

The developed community platform not only established an efficient and accessible communication channel for cybersecurity awareness, but also increased employee understanding of cyber threats and promotes secure information system usage behaviors, contributing to a sustainable cybersecurity culture within the organization.

(Total 98 Pages)

Keywords: Community platform, Cybersecurity, Phishing, Threat response, Awareness.

_____ Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงด้วยดี ด้วยความเมตตาและความกรุณาจาก ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์ อาจารย์ที่ปรึกษา ผู้ซึ่งได้ให้คำแนะนำอย่างใกล้ชิด เอาใจใส่ในทุกขั้นตอนด้วยความเสียสละอย่างยิ่งตลอดระยะเวลาการดำเนินงาน ข้าพเจ้าขอกราบขอบพระคุณท่านมา ณ โอกาสนี้ด้วยความเคารพอย่างสูง

นอกจากนี้ ข้าพเจ้าขอแสดงความขอบพระคุณเป็นอย่างยิ่งต่อคณาจารย์ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศทุกท่านที่ได้ถ่ายทอดองค์ความรู้ในหลากหลายสาขา ซึ่งมีส่วนสำคัญต่อการเสริมสร้างองค์ความรู้และเป็นพื้นฐานในการจัดทำการค้นคว้าอิสระฉบับนี้ ตลอดจนคณะกรรมการทุกท่านที่ได้กรุณาให้ข้อเสนอแนะอันเป็นประโยชน์อย่างยิ่งต่อการปรับปรุงและพัฒนาเนื้อหาให้สมบูรณ์ยิ่งขึ้น

ข้าพเจ้าขอขอบพระคุณอย่างยิ่งต่อองค์กรต้นสังกัดที่ได้ให้การสนับสนุนข้อมูล ทรัพยากร ตลอดจนความร่วมมือจากบุคลากรในหน่วยงาน ซึ่งล้วนมีส่วนสำคัญในการผลักดันให้การพัฒนาแพลตฟอร์มชุมชนเพื่อส่งเสริมวัฒนธรรมความปลอดภัยไซเบอร์บรรลุผลตามวัตถุประสงค์ที่ตั้งไว้

สุดท้ายนี้ ข้าพเจ้าขอขอบคุณจากใจต่อครอบครัว เพื่อน ๆ พี่ ๆ น้อง ๆ ทุกท่าน ที่คอยเป็นกำลังใจและอยู่เคียงข้างในทุกช่วงเวลาของการดำเนินงาน จนสามารถผ่านพ้นอุปสรรคต่าง ๆ และทำให้การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี

วราพร นิ่มนวล

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญรูปภาพ

สารบัญภาพ (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศกลายเป็นส่วนสำคัญของการดำเนินงานในทุกองค์กร ความมั่นคงปลอดภัยทางไซเบอร์จึงเป็นประเด็นที่ต้องให้ความสำคัญอย่างยิ่ง รูปแบบภัยคุกคามทางไซเบอร์มีความหลากหลายและพัฒนาซับซ้อนขึ้นอย่างต่อเนื่อง โดยเฉพาะภัยคุกคามที่อาศัยจุดอ่อนของพฤติกรรมผู้ใช้งาน เช่น การหลอกลวงด้วยวิศวกรรมสังคม (Social Engineering) ซึ่งมักยากที่จะรับมือด้วยมาตรการทางเทคนิคเพียงอย่างเดียว [1]

จากรายงานของ Verizon Data Breach Investigations Report ปี 2020 [2] พบว่า การโจมตีทางไซเบอร์จำนวนมากมีต้นเหตุจากการขาดความตระหนักรู้ของบุคลากรภายในองค์กร ซึ่งนำไปสู่การสูญเสียข้อมูล ทรัพย์สิน หรือแม้กระทั่งความน่าเชื่อถือขององค์กร แนวทางหนึ่งที่ได้รับการยอมรับว่าเป็นเครื่องมือสำคัญในการลดความเสี่ยง คือ การส่งเสริม "วัฒนธรรมความปลอดภัยไซเบอร์" ภายในองค์กร (Cybersecurity Culture) ซึ่งมีเป้าหมายเพื่อสร้างความเข้าใจ ความร่วมมือ และพฤติกรรมเชิงบวกในการป้องกันภัยคุกคาม [3]

ด้วยเหตุนี้ แนวคิดในการพัฒนา "แพลตฟอร์มชุมชน (Community Platform)" จึงถูกเสนอขึ้นเพื่อใช้เป็นช่องทางกลางในการสื่อสาร แบ่งปันข้อมูล และสร้างการเรียนรู้ร่วมกันภายในองค์กรเกี่ยวกับภัยคุกคามทางไซเบอร์ โดยมุ่งเน้นให้บุคลากรมีส่วนร่วมในการแลกเปลี่ยนประสบการณ์ ให้คำแนะนำ และเผยแพร่กรณีศึกษาที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ [4]

การเลือกใช้ Microsoft OneNote เป็นแพลตฟอร์มหลักในการพัฒนาแพลตฟอร์มชุมชนครั้งนี้ เนื่องจากองค์กรมีการใช้งานชุดซอฟต์แวร์ Microsoft 365 ในการสื่อสารและปฏิบัติงานในอยู่เป็นประจำ ซึ่งแพลตฟอร์มดังกล่าวมีคุณสมบัติเด่นในด้านการสื่อสาร การทำงานร่วมกัน (Collaboration) การประชุม และการแบ่งปันข้อมูลทรัพยากรภายในองค์กรอย่างมีประสิทธิภาพ อาทิ Microsoft Teams, OneDrive, SharePoint, Microsoft Office Online, Microsoft Forms และ Microsoft Stream เป็นต้น ดังนั้น บุคลากรทุกระดับจึงสามารถเข้าถึงข้อมูลและทำงานร่วมกันได้อย่างสะดวก รวดเร็ว และมีประสิทธิภาพ อีกทั้ง Microsoft OneNote ยังสามารถจัดการข้อมูลได้หลากหลายรูปแบบ ไม่ว่าจะเป็นเอกสาร รูปภาพ วิดีโอ และลิงก์ข้อมูล [5] โดยสามารถเชื่อมโยงการทำงานร่วมกับเครื่องมืออื่น ๆ ในชุดซอฟต์แวร์ Microsoft 365 ได้อย่างราบรื่นและมีประสิทธิผล ส่งผลให้เกิดประสิทธิภาพในการสื่อสารภายในองค์กรได้อย่างสูงสุด

1.2 วัตถุประสงค์

1.2.1 เพื่อพัฒนาแพลตฟอร์มชุมชนด้วย Microsoft OneNote สำหรับรวบรวมและแบ่งปันความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กร

1.2.2 เพื่อส่งเสริมวัฒนธรรมความปลอดภัยไซเบอร์ผ่านการมีส่วนร่วมของบุคลากรในแพลตฟอร์มชุมชน

1.2.3 เพื่อประเมินการนำแพลตฟอร์มชุมชนไปใช้จริงและประสิทธิภาพในการสื่อสารประชาสัมพันธ์ และแลกเปลี่ยนองค์ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ในองค์กร

1.3 ขอบเขตการวิจัย

1.3.1 กลุ่มเป้าหมาย ได้แก่ บุคลากรในองค์กรที่มีการใช้งานระบบสารสนเทศและสื่อสารภายในเป็นประจำ จำนวนไม่น้อยกว่า 52 คน

1.3.2 การวิจัยจะเน้นการพัฒนาและใช้งานแพลตฟอร์มชุมชนบน Microsoft OneNote โดยจัดทำเนื้อหาประกอบด้วย ข่าวสารไซเบอร์ กรณีศึกษา เทคนิคการใช้งานอย่างปลอดภัย คำแนะนำจากผู้เชี่ยวชาญ และพื้นที่แลกเปลี่ยนประสบการณ์

1.3.3 เครื่องมือและวิธีการวิจัย

1.3.3.1 Microsoft OneNote สำหรับการพัฒนาแพลตฟอร์มชุมชน (Community Platform) ในการรวบรวมข้อมูลและเผยแพร่ความรู้เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

1.3.3.2 Microsoft Form สำหรับการพัฒนาแบบทดสอบความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Knowledge Test) และการพัฒนาแบบสอบถามความพึงพอใจของบุคลากรที่เข้ามาใช้งานแพลตฟอร์มชุมชนความปลอดภัยไซเบอร์

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 องค์กรมีช่องทางที่มีประสิทธิภาพในการสื่อสารและส่งเสริมวัฒนธรรมความปลอดภัยไซเบอร์ผ่านการมีส่วนร่วมของบุคลากร

1.4.2 บุคลากรสามารถเข้าถึงข้อมูลและความรู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ได้อย่างสะดวก รวดเร็ว และต่อเนื่อง

1.4.3 ส่งเสริมให้เกิดการเปลี่ยนแปลงเชิงพฤติกรรมของผู้ใช้งานระบบสารสนเทศ และสร้างความยั่งยืนของวัฒนธรรมความปลอดภัยไซเบอร์ในองค์กร

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในการค้นคว้าอิสระครั้งนี้ ผู้วิจัยได้ศึกษาเอกสาร วิชาการ มาตรฐานสากล และงานวิจัยที่เกี่ยวข้อง เพื่อเป็นแนวทางในการพัฒนาแพลตฟอร์มชุมชน (Community Platform) เพื่อเสริมสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ (Cybersecurity Culture) ภายในองค์กร โดยสามารถแบ่งเนื้อหาออกเป็น 5 หัวข้อหลัก ดังนี้

2.1 แนวคิดและทฤษฎีด้านความมั่นคงปลอดภัยไซเบอร์
2.2 แนวคิดวัฒนธรรมความปลอดภัยไซเบอร์ในองค์กร
2.3 วิศวกรรมสังคมและพฤติกรรมผู้ใช้งาน
2.4 แพลตฟอร์มชุมชนกับการเสริมสร้างความรู้และการมีส่วนร่วม
2.5 การใช้ Microsoft OneNote และ Microsoft 365 ในการสนับสนุนการเรียนรู้ร่วมกัน
2.6 งานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎีด้านความมั่นคงปลอดภัยไซเบอร์

ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) หมายถึง แนวทางและมาตรการที่ใช้ในการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ซึ่งรวมถึงการปกป้องข้อมูล ระบบและโครงสร้างพื้นฐานดิจิทัลจากการเข้าถึงโดยไม่ได้รับอนุญาต การโจมตีทางไซเบอร์ และการละเมิดข้อมูล (ISO/IEC 27001 : 2022) โดยมุ่งเน้นไปที่การรักษาความปลอดภัยของข้อมูลและระบบให้มั่นคงและปลอดภัยจากภัยคุกคามทั้งภายในและภายนอกองค์กร

ในยุคดิจิทัลที่องค์กรพึ่งพาเทคโนโลยีสารสนเทศอย่างสูงในการดำเนินงาน ระบบที่ขาดการป้องกันที่เหมาะสมหรือไม่มีมาตรการด้านความมั่นคงปลอดภัย ย่อมตกอยู่ในความเสี่ยงจากภัยคุกคามไซเบอร์ อาทิ มัลแวร์ แรนซัมแวร์ การหลอกลวงแบบฟิชชิง (Phishing) [6] หรือการเข้าถึงข้อมูลโดยมิชอบ ซึ่งอาจนำไปสู่ความเสียหายทั้งในด้านข้อมูล ชื่อเสียงองค์กร และความเสียหายทางเศรษฐกิจ [7]

2.1.1 องค์ประกอบหลักของความมั่นคงปลอดภัยทางไซเบอร์

ความมั่นคงปลอดภัยไซเบอร์สามารถจำแนกองค์ประกอบหลักได้เป็น 3 มิติสำคัญ ได้แก่ เทคโนโลยี กระบวนการ และบุคลากร [8] ซึ่งแต่ละมิติทำงานประสานกันอย่างเป็นระบบ ดังนี้

2.1.1.1 เทคโนโลยี (Technology) เป็นส่วนที่เกี่ยวข้องกับเครื่องมือ ซอฟต์แวร์ และโครงสร้างพื้นฐานที่ใช้เพื่อป้องกัน ควบคุม และตอบสนองต่อภัยคุกคาม [9] ดังนี้

2.1.1.1.1 ไฟร์วอลล์ (Firewall) เป็นระบบหรืออุปกรณ์ที่ใช้ในการควบคุมและกรองการรับส่งข้อมูลระหว่างเครือข่ายภายในองค์กรกับเครือข่ายภายนอก หรือจากแหล่งที่อาจไม่น่าเชื่อถือ โดยทำหน้าที่เป็น “ด่านแรก” ในการตรวจสอบและจำกัดการเข้าถึงระบบสารสนเทศเพื่อป้องกันการบุกรุกหรือการโจมตีจากภายนอก อาทิ การสแกนพอร์ต การเข้าถึงบริการที่ไม่ได้รับอนุญาต หรือการส่งมัลแวร์เข้ามายังระบบ

2.1.1.1.2 โปรแกรมแอนติไวรัสและแอนติมัลแวร์ (Antivirus and Antimalware) เป็นเครื่องมือสำคัญที่ใช้ในการตรวจจับ กักกัน และกำจัดซอฟต์แวร์ที่เป็นอันตราย (Malware) ซึ่งอาจแฝงตัวเข้ามาในระบบสารสนเทศขององค์กร โดยมัลแวร์ที่พบได้บ่อย ได้แก่ ไวรัส (Virus) โทรจัน (Trojan) แรนซัมแวร์ (Ransomware) และสปายแวร์ (Spyware) ซึ่งล้วนเป็นภัยคุกคามที่สามารถส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล ระบบ และการดำเนินงาน

2.1.1.1.3 การเข้ารหัสข้อมูล (Encryption) กระบวนการแปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้โดยบุคคลทั่วไป เว้นแต่จะมี “กุญแจ” หรือรหัสที่ถูกต้องในการถอดรหัส ซึ่งเป็นกลไกสำคัญในการรักษาความลับของข้อมูล (Confidentiality) ตามหลักการความมั่นคงปลอดภัยสารสนเทศ การเข้ารหัสถูกนำมาใช้เพื่อปกป้องข้อมูลสำคัญ เช่น ข้อมูลส่วนบุคคล รหัสผ่าน หรือข้อความในอีเมล เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2.1.1.1.4 ระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection/Prevention Systems : IDS/IPS) เป็นเทคโนโลยีที่ใช้ในการตรวจสอบพฤติกรรมของข้อมูลที่รับส่งภายในเครือข่ายเพื่อตรวจจับกิจกรรมที่ผิดปกติหรืออาจเป็นภัยคุกคาม รวมถึงสามารถดำเนินการตอบสนองโดยอัตโนมัติเพื่อหยุดยั้งการโจมตีที่อาจเกิดขึ้น [10]

ก) ระบบ IDS (Intrusion Detection System) มีหน้าที่ตรวจจับและแจ้งเตือนผู้ดูแลระบบเมื่อพบกิจกรรมต้องสงสัย โดยไม่ดำเนินการตอบโต้โดยตรง

ข) ระบบ IPS (Intrusion Prevention System) นอกจากตรวจจับแล้วยังสามารถดำเนินการตอบสนอง เช่น บล็อกการเชื่อมต่อ หรือปิดพอร์ตที่ถูกใช้โจมตีโดยอัตโนมัติ

2.1.1.1.5 ระบบตรวจสอบและตอบสนองภัยคุกคามที่อุปกรณ์ปลายทาง (Endpoint Detection and Response : EDR) เป็นระบบที่พัฒนาขึ้นเพื่อเพิ่มขีดความสามารถในการตรวจสอบ วิเคราะห์ และตอบสนองต่อภัยคุกคามที่เกิดขึ้นบนอุปกรณ์ปลายทางของผู้ใช้ เช่น โน้ตบุ๊ก คอมพิวเตอร์ตั้งโต๊ะ หรืออุปกรณ์เคลื่อนที่อย่างสมาร์ตโฟน

2.1.1.2 กระบวนการ (Process) คือ ชุดของนโยบาย มาตรการ และขั้นตอนปฏิบัติที่องค์กรกำหนดขึ้นอย่างเป็นระบบ เพื่อควบคุมและจัดการความมั่นคงปลอดภัยของระบบสารสนเทศให้มีประสิทธิภาพ กระบวนการเหล่านี้ครอบคลุมตั้งแต่การประเมินความเสี่ยง การควบคุมการเข้าถึง การรับมือกับเหตุการณ์ด้านความปลอดภัย ไปจนถึงการฟื้นฟูระบบและการตรวจสอบภายใน เพื่อให้มั่นใจว่าทรัพยากรสารสนเทศขององค์กรได้รับการคุ้มครองจากภัยคุกคามทั้งภายในและภายนอกอย่างเหมาะสมและต่อเนื่อง ซึ่งมีตัวอย่างกระบวนการสำคัญ ดังนี้

2.1.1.2.1 การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) เป็นการวางแนวทางและข้อปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร เพื่อสะท้อนถึงความมุ่งมั่นของฝ่ายบริหารในการบริหารจัดการความเสี่ยงด้านสารสนเทศ รวมถึงการสร้างวัฒนธรรมด้านความปลอดภัยในระดับองค์กร

2.1.1.2.2 การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เป็นกระบวนการวางแผนล่วงหน้าเพื่อรับมือกับเหตุการณ์ที่ไม่คาดคิด อาทิ ภัยธรรมชาติ การโจมตีทางไซเบอร์ หรือความล้มเหลวของระบบ โดยมุ่งเน้นให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่องและลดผลกระทบต่อการดำเนินงานให้น้อยที่สุด

2.1.1.2.3 การควบคุมการเข้าถึง (Access Control) เป็นมาตรการในการกำหนดสิทธิ์และบทบาทของผู้ใช้งานในการเข้าถึงข้อมูลหรือระบบ โดยอ้างอิงตามหลัก Need-to-Know และ Least Privilege เพื่อจำกัดความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

2.1.1.2.4 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Management) เป็นกระบวนการตอบสนองต่อเหตุการณ์ที่ส่งผลต่อความมั่นคงปลอดภัยของระบบ โดยเน้นการตรวจสอบ แจ้งเตือน วิเคราะห์ และตอบโต้เพื่อควบคุมความเสียหาย รวมถึงวางแผนป้องกันเหตุการณ์ซ้ำในอนาคต

2.1.1.2.5 การจัดทำแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan : DRP) เป็นแผนที่ระบุขั้นตอนการกู้คืนข้อมูลและระบบให้กลับมาทำงานได้อย่างรวดเร็วหลังเกิดเหตุการณ์ร้ายแรง เช่น ไฟไหม้ น้ำท่วม หรือการโจมตีทางไซเบอร์ เพื่อรักษาความต่อเนื่องของบริการที่สำคัญ

2.1.1.2.6 การตรวจสอบภายใน (Audit) เป็นกระบวนการประเมินและทบทวนมาตรการควบคุมภายใน เพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามนโยบาย กฎหมาย และมาตรฐานที่เกี่ยวข้อง พร้อมทั้งสามารถระบุจุดอ่อนและเสนอแนะแนวทางปรับปรุงได้อย่างเป็นระบบ [11]

2.1.1.3 บุคลากร (People) ถือเป็นองค์ประกอบที่สำคัญที่สุดในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ แม้ว่าจะมีการนำเทคโนโลยีและกระบวนการที่ทันสมัยมาใช้ แต่หากขาดการตระหนักรู้และพฤติกรรมที่ปลอดภัยของบุคลากร ก็ยังคงมีความเสี่ยงสูงต่อการเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งการบริหารจัดการด้านบุคลากรในบริบทของความมั่นคงปลอดภัยสารสนเทศ ควรครอบคลุมทั้งการสร้างความตระหนักรู้ การฝึกอบรมที่เหมาะสม และการปลูกฝังพฤติกรรมที่รับผิดชอบต่อการใช้เทคโนโลยีสารสนเทศ ดังนี้

2.1.1.3.1 การสร้างความตระหนักรู้ (Awareness) เป็นการให้ข้อมูลและปลูกจิตสำนึกแก่บุคลากรในทุกระดับ [12] ให้เข้าใจถึงความเสี่ยงทางไซเบอร์ที่อาจเกิดขึ้นจากพฤติกรรมประจำวัน เช่น การคลิกลิงก์ฟิชชิ่ง การใช้รหัสผ่านที่ไม่ปลอดภัย หรือการใช้อุปกรณ์ส่วนตัวเชื่อมต่อเครือข่ายองค์กรโดยไม่มีมาตรการควบคุม

2.1.1.3.2 การฝึกอบรมและพัฒนา (Training & Education) การจัดฝึกอบรมทั้งในเชิงทฤษฎีและภาคปฏิบัติ เพื่อเพิ่มทักษะในการป้องกันภัยคุกคามไซเบอร์ การตอบสนอง

เหตุการณ์ และการปฏิบัติตามนโยบายองค์กร โดยเนื้อหาควรมีความหลากหลายและเหมาะสมกับบทบาทหน้าที่ของบุคลากร เช่น ฝึกอบรมเฉพาะด้านสำหรับผู้ดูแลระบบหรือผู้บริหารระดับสูง [13]

2.1.1.3.3 การส่งเสริมพฤติกรรมที่ปลอดภัย (Promoting Secure Behavior) เป็นการออกแบบกิจกรรมหรือโครงการเพื่อกระตุ้นให้บุคลากรมีพฤติกรรมที่สอดคล้องกับแนวทางความมั่นคงปลอดภัย เช่น การแข่งขันตอบคำถามความรู้ไซเบอร์ (Cybersecurity Quiz) การจำลองสถานการณ์ฟิชชิ่ง (Phishing Simulation) หรือการจัดทำ Community Platform เพื่อแลกเปลี่ยนความรู้ด้านความปลอดภัยภายในองค์กร [14]

การส่งเสริมให้บุคลากรทุกระดับมีส่วนร่วมในการสร้างวัฒนธรรมความมั่นคงปลอดภัยสารสนเทศอย่างยั่งยืน จึงเป็นกลยุทธ์ที่มีประสิทธิภาพในการลดความเสี่ยงจากภัยคุกคามที่เกิดจาก “จุดอ่อนของมนุษย์” ซึ่งเป็นปัจจัยที่พบมากที่สุดในเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

2.1.2 ประเภทของภัยคุกคามทางไซเบอร์และแนวทางป้องกัน

ภัยคุกคามทางไซเบอร์และการป้องกัน ในการพัฒนาแพลตฟอร์มชุมชนที่เกี่ยวข้องกับการเสริมสร้างวัฒนธรรมความปลอดภัยไซเบอร์นั้น จำเป็นต้องให้ข้อมูลที่ละเอียดและสร้างความตระหนักเกี่ยวกับภัยคุกคามหลักดังต่อไปนี้

2.1.2.1 มัลแวร์ (Malware) หมายถึง ซอฟต์แวร์ที่ถูกออกแบบมาเพื่อสร้างความเสียหายหรือเข้าควบคุมระบบคอมพิวเตอร์ เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) สปายแวร์ (Spyware) และแรนซัมแวร์ (Ransomware) การป้องกันมัลแวร์จำเป็นต้องมีการติดตั้งและอัปเดตโปรแกรมป้องกันไวรัส (Antivirus Software) รวมถึงการฝึกอบรมให้ผู้ใช้งานหลีกเลี่ยงการดาวน์โหลดหรือเปิดไฟล์ที่ไม่น่าเชื่อถือ

2.1.2.2 การโจมตีแบบฟิชชิ่ง (Phishing Attacks) หมายถึง เทคนิคการหลอกลวงที่ผู้โจมตีสร้างอีเมล เว็บไซต์ หรือข้อความปลอมขึ้นมาเพื่อหลอกลวงผู้ใช้ให้เปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลลับขององค์กร การป้องกันต้องอาศัยการให้ความรู้และการอบรมที่ต่อเนื่องเพื่อให้ผู้ใช้สามารถระบุและรับมือกับฟิชชิ่งได้อย่างมีประสิทธิภาพ

2.1.2.3 การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service : DoS/DDoS) หมายถึง การโจมตีที่มีวัตถุประสงค์เพื่อทำให้ระบบไม่สามารถใช้งานได้ โดยการส่งข้อมูลจำนวนมากจนเกินขีดจำกัดของระบบ ทำให้บริการหยุดชะงักหรือไม่สามารถใช้งานได้ การป้องกันการโจมตีลักษณะนี้จำเป็นต้องมีระบบการตรวจสอบเครือข่าย (Network Monitoring) และระบบจัดการการจราจรบนเครือข่าย (Traffic Management)

2.1.3 หลักการพื้นฐานของการรักษาความมั่นคงปลอดภัย (CIA Triad)

ตามมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISO/IEC 27001 : 2022) องค์ประกอบหลักของความมั่นคงปลอดภัยทางไซเบอร์ประกอบด้วย 3 ด้านหลัก ได้แก่

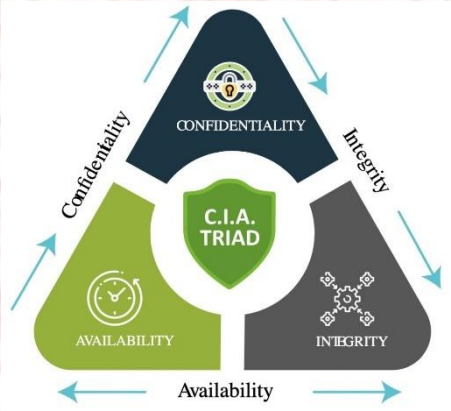
2.1.3.1 ความลับ (Confidentiality) เป็นการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ซึ่งเป็นการรับรองว่าข้อมูลจะถูกเปิดเผยเฉพาะผู้ที่มีสิทธิ์เท่านั้น มาตรการที่ใช้ในการรักษา

ความลับของข้อมูล ได้แก่ การเข้ารหัสข้อมูล (Encryption) การควบคุมการเข้าถึง (Access Control) และการตรวจสอบสิทธิ์ผู้ใช้ (Authentication)

2.1.3.2 ความถูกต้อง (Integrity) เป็นการรักษาความถูกต้องและความน่าเชื่อถือของข้อมูล โดยป้องกันไม่ให้ข้อมูลถูกแก้ไข ดัดแปลง หรือถูกทำลายโดยไม่ได้รับอนุญาต มาตรการสำคัญที่ใช้ได้แก่ การตรวจสอบความถูกต้องของข้อมูล (Data Validation) การสำรองข้อมูล (Backup) และการใช้เทคโนโลยีตรวจจับการเปลี่ยนแปลงของข้อมูล (Hashing & Checksums)

2.1.3.3 ความพร้อมใช้งาน (Availability) เป็นการรับรองว่าระบบและข้อมูลสามารถเข้าถึงได้เมื่อจำเป็น เพื่อให้แน่ใจว่าผู้ใช้สามารถใช้งานข้อมูลและระบบได้ตลอดเวลาโดยไม่มีการหยุดชะงัก มาตรการที่เกี่ยวข้อง ได้แก่ การป้องกันการโจมตีแบบ DDoS (DDoS Protection) การบริหารจัดการความเสี่ยงด้านโครงสร้างพื้นฐาน (Infrastructure Resilience) และการวางแผนกู้คืนระบบ (Disaster Recovery Planning)

องค์ประกอบเหล่านี้ถูกนำมาใช้เป็นกรอบในการกำหนดแนวทางและการดำเนินงานที่เกี่ยวข้องกับการพัฒนาเนื้อหาในแพลตฟอร์มชุมชนที่มุ่งสร้างความรู้และทักษะในการรับมือภัยคุกคามไซเบอร์



ภาพที่ 2-1 องค์ประกอบด้านความมั่นคงปลอดภัยทางไซเบอร์ (CIA Triad)
(ที่มา : https://www.ablenet.co.th/2024/06/06/cia-triad/)

2.1.4 มาตรฐานและแนวทางปฏิบัติด้านความปลอดภัยไซเบอร์ที่เกี่ยวข้อง

มาตรฐานและแนวทางปฏิบัติด้านความปลอดภัยไซเบอร์เป็นสิ่งสำคัญที่ช่วยองค์กรป้องกันภัยคุกคามทางไซเบอร์ ลดความเสี่ยง และปฏิบัติตามข้อกำหนดทางกฎหมาย โดยมีมาตรฐานที่สำคัญหลายฉบับที่ได้รับการยอมรับทั่วโลก ซึ่งครอบคลุมตั้งแต่แนวทางการบริหารความปลอดภัยข้อมูล ไปจนถึงมาตรการทางเทคนิคที่ใช้ป้องกันและตรวจจับภัยคุกคาม ดังนี้

2.1.4.1 มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISO/IEC 27001 : 2022) เป็นมาตรฐานสากลช่วยให้องค์กรสามารถสร้างระบบการจัดการความปลอดภัยของข้อมูลที่เป็นมาตรฐานและมีประสิทธิภาพ ซึ่งครอบคลุมแนวทางด้าน การป้องกันข้อมูล (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมใช้งาน (Availability)

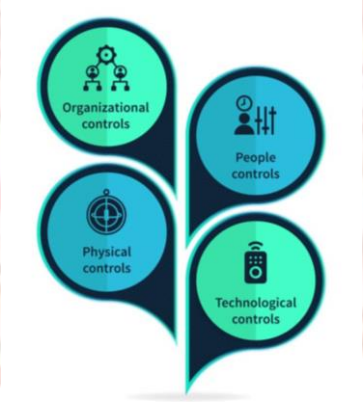
หรือที่เรียกว่า CIA Triad และมีการควบคุมด้านความมั่นคงปลอดภัยของสารสนเทศ (Security Controls) เป็นกลไกสำคัญในการป้องกัน บรรเทา และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยสามารถจำแนกประเภทของการควบคุมออกเป็น 4 ด้านหลัก [14] ดังนี้

2.1.4.1.1 การควบคุมในระดับองค์กร (Organizational Controls) หมายถึง แนวทางและมาตรการด้านการบริหารจัดการภายในองค์กรที่มีจุดประสงค์เพื่อส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยและกำกับดูแลให้สอดคล้องกับนโยบายและเป้าหมายขององค์กร เช่น การจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศ การกำหนดบทบาทและหน้าที่ของผู้มีส่วนเกี่ยวข้อง และการจัดการความเสี่ยงในระดับองค์กร

2.1.4.1.2 การควบคุมด้านบุคลากร (People Controls) เน้นการจัดการความเสี่ยงที่เกี่ยวข้องกับบุคลากรภายในองค์กร โดยครอบคลุมถึงการคัดเลือกบุคลากร การอบรมให้ความรู้และสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ การกำหนดหลักปฏิบัติสำหรับผู้ใช้งาน รวมถึงมาตรการด้านวินัยเมื่อละเมิดนโยบาย

2.1.4.1.3 การควบคุมด้านกายภาพ (Physical Controls) เป็นการควบคุมที่มุ่งเน้นการป้องกันการเข้าถึงทรัพยากรหรือระบบโดยไม่ได้รับอนุญาตในเชิงกายภาพ เช่น การควบคุมการเข้า–ออกอาคารและห้องศูนย์ข้อมูล การใช้ระบบกล้องวงจรปิด (CCTV) ระบบควบคุมประตูด้วยบัตรหรือชีวมาตร และการป้องกันอัคคีภัยหรือเหตุภัยพิบัติที่อาจกระทบต่อระบบสารสนเทศ

2.1.4.1.4 การควบคุมด้านเทคโนโลยี (Technological Controls) หมายถึง การใช้เทคโนโลยีเพื่อเสริมสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ ตัวอย่างของการควบคุมประเภทนี้ ได้แก่ การเข้ารหัสข้อมูล (Encryption) การควบคุมการเข้าถึงด้วยรหัสผ่านหรือระบบยืนยันตัวตนหลายชั้น (Multi-Factor Authentication : MFA) การติดตั้งระบบป้องกันมัลแวร์ และระบบตรวจจับการบุกรุก (Intrusion Detection Systems : IDS)



ภาพที่ 2-2 การควบคุมด้านความมั่นคงปลอดภัยของสารสนเทศ (Security Controls)
(ที่มา : https://www.scrut.io/iso-27001/iso-27001-checklist)

2.1.4.2 กรอบแนวทาง NIST Cybersecurity Framework (NIST CSF) เป็นกรอบแนวทางที่พัฒนาโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) โดยมีวัตถุประสงค์เพื่อใช้เป็นเครื่องมือช่วยให้องค์กร

สามารถบริหารจัดการความเสี่ยงทางไซเบอร์ได้อย่างเป็นระบบและมีประสิทธิภาพ กรอบแนวทางนี้สามารถปรับใช้ได้กับทุกภาคส่วน ทั้งภาครัฐ ภาคเอกชน และองค์กรไม่แสวงหาผลกำไร ซึ่งกรอบ NIST CSF ประกอบด้วย 5 ฟังก์ชันหลัก (Core Functions) ซึ่งครอบคลุมวงจรชีวิตของการจัดการความเสี่ยงไซเบอร์ ดังนี้

2.1.4.2.1 Identify (ระบุ) เป็นการระบุทรัพย์สินดิจิทัลที่ต้องได้รับการปกป้อง พร้อมทั้งวิเคราะห์ความเสี่ยง ช่องโหว่ และผลกระทบที่อาจเกิดขึ้นต่อธุรกิจ เพื่อให้สามารถวางแผนจัดการความมั่นคงปลอดภัยได้อย่างครอบคลุม องค์ประกอบสำคัญของฟังก์ชันนี้ ได้แก่

ก) การจำแนกทรัพย์สินสารสนเทศ (Asset Management)

ข) การวิเคราะห์ความเสี่ยง (Risk Assessment)

ค) การระบุบทบาทและความรับผิดชอบ (Governance)

2.1.4.2.2 Protect (ป้องกัน) เป็นการพัฒนามาตรการควบคุมเพื่อป้องกันไม่ให้ภัยคุกคามสามารถเข้าถึงระบบหรือข้อมูลสำคัญได้ ฟังก์ชันนี้มุ่งเน้นการรักษาความมั่นคงปลอดภัยเชิงรุก เช่น

ก) การควบคุมการเข้าถึงข้อมูล (Access Control)

ข) การให้ความรู้และฝึกอบรมผู้ใช้งาน (Awareness and Training)

ค) การปกป้องข้อมูลด้วยเทคโนโลยีที่เหมาะสม (Data Security)

2.1.4.2.3 Detect (ตรวจจับ) เป็นการจัดตั้งกลไกและระบบที่สามารถตรวจพบเหตุการณ์หรือพฤติกรรมที่ผิดปกติภายในระบบสารสนเทศได้อย่างรวดเร็ว เช่น

ก) ระบบเฝ้าระวังภัยคุกคาม (Anomalies and Events Monitoring)

ข) การตรวจจับการบุกรุก (Intrusion Detection Systems)

ค) การตรวจสอบและรายงานเหตุการณ์ (Security Continuous Monitoring)

2.1.4.2.4 Respond (ตอบสนอง) เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ องค์กรต้องมีแนวทางในการตอบสนองอย่างเป็นระบบ เพื่อจำกัดความเสียหายและป้องกันไม่ให้เหตุการณ์ลุกลาม อาทิ

ก) การวางแผนการตอบสนอง (Response Planning)

ข) การสื่อสารภายในและภายนอกองค์กร (Communication)

ค) การวิเคราะห์สาเหตุและการดำเนินการแก้ไข (Analysis and Mitigation)

2.1.4.2.5 Recover (กู้คืน) เป็นขั้นตอนที่เน้นการฟื้นฟูระบบและบริการให้สามารถกลับมาใช้งานได้อย่างรวดเร็วและมีประสิทธิภาพหลังเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย โดยประกอบด้วย

ก) การวางแผนกู้คืนระบบ (Recovery Planning)

ข) การสนับสนุนจากผู้บริหาร (Improvements and Coordination)

ค) การจัดทำบทเรียนจากเหตุการณ์ (Lessons Learned)

ภาพที่ 2-3 กรอบแนวทาง NIST Cybersecurity Framework (NIST CSF)
(ที่มา : https://www.device42.com/compliance-standards/nist-csf-categories/)

2.1.4.3 การจัดการเหตุการณ์ด้านความปลอดภัยไซเบอร์ (Incident Management Theory) เป็นกระบวนการที่มีความสำคัญอย่างยิ่งในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศภายในองค์กร โดยมีวัตถุประสงค์หลักเพื่อป้องกัน ตรวจจับ ตอบสนอง และกู้คืนจากเหตุการณ์ที่อาจส่งผลกระทบต่อระบบเครือข่าย ข้อมูล และการดำเนินงานขององค์กร ซึ่งมีแนวทางการจัดการเหตุการณ์ที่ได้รับการพัฒนาและยอมรับอย่างกว้างขวางในระดับสากล โดยเฉพาะกรอบแนวทางที่เสนอโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา (National Institute of Standards and Technology : NIST)

วงจรการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (NIST Incident Response Life Cycle) เป็นกรอบการดำเนินงานของ NIST สำหรับการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ได้แบ่งวงจรการจัดการออกเป็น 4 ขั้นตอนหลัก ซึ่งครอบคลุมตั้งแต่การเตรียมความพร้อมไปจนถึงการประเมินผลหลังเหตุการณ์ เพื่อให้การตอบสนองมีความเป็นระบบและสามารถปรับปรุงอย่างต่อเนื่องได้ โดยประกอบด้วย

2.1.4.3.1 Preparation (การเตรียมความพร้อม) เป็นขั้นตอนเริ่มต้นที่องค์กรต้องมีการเตรียมการอย่างรอบด้าน ทั้งในด้านการจัดทำนโยบายและแผนตอบสนองต่อเหตุการณ์ การจัดสรรทรัพยากร การกำหนดบทบาทหน้าที่ของทีมตอบสนองเหตุการณ์ (Incident Response Team) การฝึกอบรมบุคลากร และการจัดหาเครื่องมือหรือระบบที่สามารถตรวจจับภัยคุกคามได้อย่างมีประสิทธิภาพ

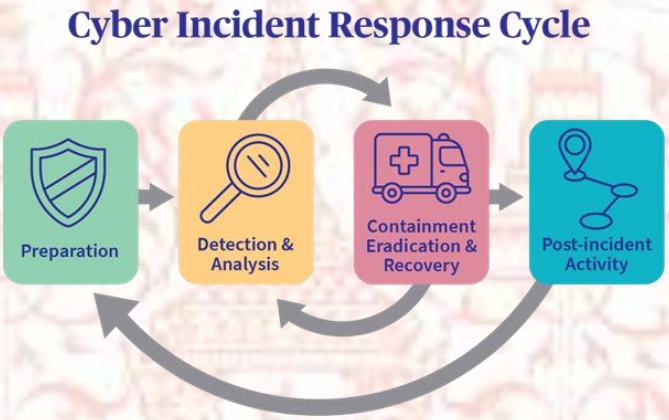
2.1.4.3.2 Detection and Analysis (การตรวจจับและวิเคราะห์) ขั้นตอนนี้มุ่งเน้นการตรวจสอบสัญญาณเตือนของเหตุการณ์ผิดปกติ (Indicators of Compromise) การรวบรวมข้อมูล การวิเคราะห์ลักษณะของเหตุการณ์ และการประเมินความรุนแรง ตลอดจนการระบุขอบเขตของผลกระทบ เพื่อวางแผนการตอบสนองได้อย่างเหมาะสมและทันท่วงที

2.1.4.3.3 Containment, Eradication and Recovery (การจำกัดความเสียหาย การกำจัดภัยคุกคาม และการกู้คืนระบบ) เมื่อมีการระบุเหตุการณ์อย่างชัดเจนแล้ว องค์กรจะต้องดำเนินการควบคุม (Containment) เพื่อจำกัดความเสียหายไม่ให้ลุกลาม จากนั้นดำเนินการกำจัดภัย

คุกคาม (Eradication) เช่น ลบมัลแวร์ ปิดช่องโหว่ และในขั้นสุดท้ายคือการฟื้นฟูระบบ (Recovery) ให้กลับมาใช้งานได้อย่างปลอดภัยและมีเสถียรภาพ

2.1.4.3.4 Post-Incident Activity (การประเมินผลหลังเหตุการณ์) หลังจากเหตุการณ์สิ้นสุดลง องค์กรควรดำเนินการทบทวนการตอบสนองที่เกิดขึ้น วิเคราะห์สาเหตุความผิดพลาด หรือช่องว่างที่อาจเกิดขึ้น พร้อมทั้งบันทึกบทเรียน (Lessons Learned) เพื่อใช้ในการปรับปรุงนโยบาย ขั้นตอน และการฝึกอบรมในอนาคต รวมถึงการยกระดับแผนตอบสนองให้มีประสิทธิภาพมากยิ่งขึ้น

การดำเนินการตามกรอบวงจรของ NIST ดังกล่าว ช่วยให้องค์กรสามารถบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างเป็นระบบ มีประสิทธิภาพ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นในอนาคต



ภาพที่ 2-4 วงจรการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
(ที่มา : https://axaxl.com/fast-fast-forward/articles/the-cyber-incident-response-lifecycle)

2.1.4.4 การบริหารจัดการความเสี่ยงทางไซเบอร์ (Cyber Risk Management) เป็นการบริหารจัดการความเสี่ยงทางไซเบอร์ (Cyber Risk Management) เป็นกระบวนการที่มีบทบาทสำคัญในการวางแผนและดำเนินมาตรการเพื่อป้องกันและลดผลกระทบจากภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นกับระบบสารสนเทศขององค์กร โดยมุ่งเน้นให้เกิดความสมดุลระหว่างระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ กับค่าใช้จ่ายในการดำเนินมาตรการควบคุม ซึ่งแนวทางที่ได้รับความนิยมและเป็นที่ยอมรับอย่างกว้างขวาง คือ กรอบการบริหารความเสี่ยงที่พัฒนาโดย National Institute of Standards and Technology (NIST) ซึ่งช่วยให้องค์กรสามารถประเมิน ควบคุม และติดตามความเสี่ยงได้อย่างเป็นระบบ

โดยกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (NIST Risk Management Framework : RMF) กรอบการบริหารความเสี่ยง RMF ของ NIST ได้รับการออกแบบเพื่อสนับสนุนองค์กรในการบริหารจัดการความเสี่ยงด้านสารสนเทศอย่างครอบคลุม โดยมีขั้นตอนหลัก 7 ขั้นตอน ซึ่งเชื่อมโยงระหว่างการกำหนดบริบท การดำเนินมาตรการควบคุม และการติดตามประเมินผล ดังนี้

2.1.4.4.1 Prepare (เตรียมความพร้อม) เป็นขั้นตอนเริ่มต้นในการกำหนดบริบทขององค์กร ซึ่งรวมถึงการประเมินภารกิจหลัก ทรัพยากรสารสนเทศที่สำคัญ ความต้องการด้านความมั่นคงปลอดภัย และการจัดทำแผนการบริหารความเสี่ยงที่สอดคล้องกับยุทธศาสตร์ขององค์กร

2.1.4.4.2 Categorize (การจำแนกประเภทข้อมูลและระบบ) เป็นการจัดประเภทของข้อมูลและระบบสารสนเทศตามระดับความสำคัญและผลกระทบที่อาจเกิดขึ้นหากเกิดการละเมิดความลับ (Confidentiality) ความถูกต้อง (Integrity) หรือความพร้อมใช้งาน (Availability)

2.1.4.4.3 Select (การเลือกมาตรการควบคุมความเสี่ยง) เป็นการเลือกมาตรการควบคุม (Security Controls) ที่เหมาะสมจากมาตรฐานหรือแนวทางที่กำหนดไว้ เช่น NIST SP 800-53 หรือ ISO/IEC 27001 เพื่อควบคุมความเสี่ยงในระดับที่ยอมรับได้

2.1.4.4.4 Implement (การนำมาตรการไปใช้) เป็นการนำมาตรการควบคุมที่เลือกไว้ไปใช้งานจริงในระบบขององค์กร พร้อมจัดทำเอกสารและบันทึกการดำเนินการเพื่อรองรับการตรวจสอบ

2.1.4.4.5 Assess (การประเมินประสิทธิภาพของมาตรการ) เป็นการตรวจสอบและประเมินผลว่ามาตรการที่ดำเนินการนั้นสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่ โดยอาจใช้วิธีการทดสอบ ตรวจสอบเอกสาร หรือการประเมินจากบุคคลที่สาม

2.1.4.4.6 Authorize (การอนุมัติระบบให้ใช้งาน) ผู้บริหารหรือผู้มีอำนาจจะพิจารณาและอนุมัติให้ระบบสามารถดำเนินงานได้ภายใต้ระดับความเสี่ยงที่ยอมรับได้ พร้อมทั้งจัดทำเอกสารรับรองการอนุมัติ (Authorization Package)

2.1.4.4.7 Monitor (การเฝ้าระวังและปรับปรุง) เป็นขั้นตอนสุดท้ายที่เน้นการติดตาม ตรวจสอบ และปรับปรุงมาตรการควบคุมอย่างต่อเนื่อง เพื่อให้ระบบสามารถตอบสนองต่อภัยคุกคามใหม่ ๆ ที่เกิดขึ้นและรักษาระดับความมั่นคงปลอดภัยอย่างยั่งยืน

ภาพที่ 2-5 NIST Risk Management Framework (7 stages)
(ที่มา : https://anujapawar011.medium.com/what-is-nist-risk-management-framework-e4f8f82b42c5)

2.2 แนวคิดวัฒนธรรมความปลอดภัยไซเบอร์ในองค์กร

ในยุคที่ภัยคุกคามทางไซเบอร์มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว การพึ่งพาเพียงมาตรการด้านเทคโนโลยีอาจไม่เพียงพออีกต่อไป องค์กรจึงจำเป็นต้องสร้าง “วัฒนธรรม

ความปลอดภัยไซเบอร์” (Cybersecurity Culture) ซึ่งเป็นกลไกสำคัญที่ช่วยลดความเสี่ยงจากพฤติกรรมของผู้ใช้งาน และส่งเสริมให้บุคลากรทุกระดับมีส่วนร่วมในการรักษาความมั่นคงปลอดภัยขององค์กร

2.2.1 ความหมายของวัฒนธรรมความปลอดภัยไซเบอร์

วัฒนธรรมความปลอดภัยไซเบอร์ (Cybersecurity Culture) หมายถึง ชุดของค่านิยม ความเชื่อ พฤติกรรม และแนวปฏิบัติที่บุคลากรภายในองค์กรมีร่วมกันเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลและเทคโนโลยีสารสนเทศ โดยวัฒนธรรมดังกล่าวสะท้อนออกมาในการหลีกเลี่ยงพฤติกรรมที่ก่อให้เกิดความเสี่ยง การแจ้งเตือนหรือรายงานเหตุการณ์ที่ผิดปกติ และการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอและต่อเนื่อง

การสร้างวัฒนธรรมความปลอดภัยไซเบอร์ที่ยั่งยืนนั้น ไม่อาจเกิดขึ้นได้จากการบังคับใช้กฎระเบียบหรือมาตรการทางเทคนิคเพียงอย่างเดียว แต่จำเป็นต้องอาศัยกระบวนการปลูกฝังและเสริมสร้างความตระหนักรู้ให้เกิดขึ้นในระยะยาว โดยเฉพาะอย่างยิ่ง บทบาทของผู้นำองค์กรถือเป็นปัจจัยสำคัญในการขับเคลื่อนวัฒนธรรมดังกล่าว ทั้งในแง่ของการเป็นแบบอย่างที่ดี การส่งเสริมค่านิยมด้านความปลอดภัย และการสนับสนุนทรัพยากรที่เพียงพอสำหรับกิจกรรมหรือโครงการที่เกี่ยวข้อง

2.2.2 ปัจจัยที่ส่งผลต่อการสร้างวัฒนธรรมความปลอดภัยไซเบอร์

การเสริมสร้างวัฒนธรรมความปลอดภัยไซเบอร์ที่เข้มแข็งภายในองค์กรจำเป็นต้องอาศัยการประสานกันของปัจจัยหลายประการอย่างเป็นระบบ เพื่อให้เกิดการยอมรับและปฏิบัติตามโดยสมัครใจจากบุคลากรทุกระดับ ทั้งนี้ ปัจจัยสำคัญที่มีผลต่อความสำเร็จของการสร้างวัฒนธรรมความปลอดภัยไซเบอร์ ได้แก่

2.2.2.1 การมีส่วนร่วมของบุคลากรทุกระดับ (Employee Engagement) การที่บุคลากรตระหนักถึงบทบาทของตนในการปกป้องข้อมูลและระบบสารสนเทศขององค์กร ถือเป็นรากฐานสำคัญของวัฒนธรรมความปลอดภัยไซเบอร์ บุคลากรที่มีส่วนร่วมจะแสดงออกโดยการปฏิบัติตามนโยบายความปลอดภัยอย่างจริงจัง หลีกเลี่ยงพฤติกรรมเสี่ยง และมีความพร้อมในการแจ้งเหตุการณ์ที่ผิดปกติเมื่อพบเจอ [14]

2.2.2.2 การสื่อสารภายในที่มีประสิทธิภาพ (Effective Internal Communication) องค์กรควรมีช่องทางและรูปแบบการสื่อสารที่เหมาะสมสำหรับถ่ายทอดข้อมูลเกี่ยวกับภัยคุกคาม แนวปฏิบัติ นโยบาย และเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง โดยเนื้อหาควรเข้าใจง่าย เข้าถึงผู้ปฏิบัติงานทุกระดับ และสามารถกระตุ้นให้เกิดการตื่นตัวและใส่ใจต่อความเสี่ยงที่อาจเกิดขึ้น

2.2.2.3 การฝึกอบรมและสร้างความตระหนักรู้ (Security Awareness & Training) เป็นการจัดอบรมด้านความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอจะช่วยให้บุคลากรสามารถรับมือกับภัยคุกคามที่เปลี่ยนแปลงอยู่เสมอ โดยเฉพาะภัยจากวิศวกรรมสังคม เช่น การโจมตีแบบฟิชชิง การหลอกลวงผ่านสื่อสังคมออนไลน์ หรือการเปิดเผยข้อมูลโดยไม่ตั้งใจ การฝึกอบรมควรปรับให้เหมาะสมกับกลุ่มเป้าหมาย และมีการประเมินผลเพื่อวัดประสิทธิภาพ

2.2.2.4 บทบาทของผู้นำองค์กร (Leadership Commitment) ผู้นำองค์กรมีบทบาทสำคัญในการกำหนดทิศทางและสร้างความตระหนักรู้ในระดับกลยุทธ์ การแสดงออกถึงความมุ่งมั่น เช่น การเป็นแบบอย่างในการปฏิบัติตามนโยบาย การจัดสรรทรัพยากรที่เพียงพอ รวมถึงการสนับสนุนกิจกรรมด้านความมั่นคงปลอดภัย ล้วนเป็นแรงผลักดันที่ช่วยให้บุคลากรเห็นความสำคัญของประเด็นนี้ [15]

2.2.2.5 การส่งเสริมและให้รางวัล (Incentives & Recognition) เป็นการสร้างแรงจูงใจให้บุคลากรแสดงพฤติกรรมที่ส่งเสริมความปลอดภัยไซเบอร์ สามารถดำเนินการผ่านการให้รางวัล การประกาศเกียรติคุณ หรือสิทธิประโยชน์อื่น ๆ แก่ผู้ที่แสดงออกถึงความรับผิดชอบ เช่น การแจ้งเหตุการณ์ที่น่าสงสัย หรือการได้รับคะแนนอบรมความปลอดภัยสูง แนวทางนี้จะช่วยเสริมสร้างแรงจูงใจในเชิงบวกและกระตุ้นการมีส่วนร่วมอย่างต่อเนื่อง

2.2.3 แนวทางการส่งเสริมพฤติกรรมความปลอดภัยทางไซเบอร์

การสร้างพฤติกรรมของบุคลากรที่สอดคล้องกับหลักความมั่นคงปลอดภัยทางไซเบอร์ เป็นองค์ประกอบสำคัญของวัฒนธรรมความปลอดภัยในองค์กร ซึ่งสามารถส่งเสริมได้ผ่านกิจกรรมและกลยุทธ์ที่หลากหลาย โดยมีแนวทางที่นิยมใช้ในองค์กรชั้นนำ ดังต่อไปนี้

2.2.3.1 การใช้เกมเพื่อกระตุ้นการมีส่วนร่วม (Gamification) เป็นการนำหลักการของเกม เช่น ระบบคะแนน ป้ายรางวัล หรือการแข่งขันมาใช้ในการฝึกอบรมความมั่นคงปลอดภัยไซเบอร์ ช่วยเพิ่มแรงจูงใจและความมีส่วนร่วมของบุคลากร โดยเฉพาะในการเรียนรู้เนื้อหาที่เกี่ยวข้องกับนโยบาย ความเสี่ยง และแนวทางปฏิบัติ

2.2.3.2 การจำลองสถานการณ์ฟิชชิง (Phishing Simulation) เป็นการทดสอบพฤติกรรมของบุคลากรโดยการส่งอีเมลฟิชชิงจำลอง เพื่อประเมินความตื่นตัวและความสามารถในการแยกแยะความเสี่ยง พร้อมทั้งให้ข้อมูลย้อนกลับ (Feedback) เพื่อเสริมสร้างความรู้และพัฒนาทักษะการระบุภัยคุกคาม

2.2.3.3 โครงการผู้นำด้านความปลอดภัย (Security Champions Program) เป็นองค์กรสามารถแต่งตั้งบุคลากรในแต่ละหน่วยงานให้ทำหน้าที่เป็น “แชมป์ความปลอดภัย” หรือผู้แทนด้านความมั่นคงปลอดภัย โดยมีบทบาทในการถ่ายทอดแนวปฏิบัติ ส่งเสริมความรู้ และกระตุ้นเพื่อนร่วมงานให้ตระหนักถึงความสำคัญของภัยไซเบอร์

2.2.3.4 การประชาสัมพันธ์อย่างต่อเนื่อง (Ongoing Communication and Campaigns) เป็นการใช้สื่อภายในองค์กร เช่น จดหมายข่าว ป้ายประกาศ วิดีโอสั้น หรืออินทราเน็ต [11] เพื่อเผยแพร่สาระสำคัญเกี่ยวกับความปลอดภัยไซเบอร์อย่างสม่ำเสมอ ช่วยรักษาระดับความตระหนักรู้ และกระตุ้นให้เกิดพฤติกรรมที่สอดคล้องกับนโยบายองค์กร

2.2.3.5 การปลูกฝังแนวคิด Zero Trust (Zero Trust Mindset) เป็นการส่งเสริมแนวคิด “ไม่ไว้ใจโดยอัตโนมัติ” (Never trust, always verify) เป็นแนวทางที่เน้นให้บุคลากรทุกระดับมีความระมัดระวังอยู่เสมอ แม้กับแหล่งที่ดูน่าเชื่อถือ เช่น อีเมลภายในองค์กร หรือลิงก์จากผู้ร่วมงาน เพื่อป้องกันภัยที่แฝงมาอย่างแนบเนียน

2.2.4 ตัวชี้วัดวัฒนธรรมความปลอดภัยไซเบอร์

การประเมินระดับของวัฒนธรรมความปลอดภัยไซเบอร์ภายในองค์กรจำเป็นต้องอาศัยตัวชี้วัดที่สามารถสะท้อนพฤติกรรม การรับรู้ และการมีส่วนร่วมของบุคลากรอย่างรอบด้าน โดยตัวชี้วัดเหล่านี้สามารถแบ่งออกเป็นทั้งเชิงปริมาณและเชิงคุณภาพ เพื่อให้สามารถวิเคราะห์แนวโน้มและปรับปรุงแนวทางการส่งเสริมวัฒนธรรมความปลอดภัยได้อย่างมีประสิทธิภาพ ตัวอย่างตัวชี้วัดที่สำคัญ ได้แก่

2.2.4.1 อัตราการเข้าร่วมอบรมด้านความปลอดภัยไซเบอร์ (% ของบุคลากรที่ผ่านการอบรมตามกำหนดเวลา) จะสะท้อนถึงระดับการมีส่วนร่วมของบุคลากรในการเรียนรู้และพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์ตามแผนที่องค์กรกำหนด

2.2.4.2 ระดับความรู้ความเข้าใจจากแบบทดสอบก่อนและหลังอบรม ช่วยประเมินผลสัมฤทธิ์ของการฝึกอบรมในด้านการถ่ายทอดเนื้อหา ความเข้าใจ และการนำความรู้ไปประยุกต์ใช้

2.2.4.3 จำนวนเหตุการณ์ฟิชชิงที่บุคลากรตอบสนองได้ถูกต้อง (จากการทดสอบจำลอง Phishing Simulation) แสดงให้เห็นถึงความตื่นตัวและทักษะในการรับมือกับภัยคุกคามที่พบได้บ่อยในสภาพแวดล้อมการทำงานจริง

2.2.4.4 จำนวนเหตุการณ์ที่รายงานโดยบุคลากร (Security Incident Reports) สะท้อนถึงความตระหนักรู้และความกล้าในการแจ้งเหตุการณ์ที่น่าสงสัยหรือมีความเสี่ยง โดยไม่กลัวผลกระทบต่อส่วนตน

2.2.4.5 ผลการสำรวจความคิดเห็นเกี่ยวกับวัฒนธรรมความปลอดภัยในองค์กรเป็นเครื่องมือเชิงคุณภาพที่ช่วยวัดการรับรู้ ทัศนคติ และความรู้สึกของบุคลากรเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในภาพรวม

2.2.4.6 ดัชนีการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ (Policy Compliance Rate) ใช้วัดระดับการปฏิบัติตามนโยบายและระเบียบที่เกี่ยวข้อง เช่น การเปลี่ยนรหัสผ่านตามกำหนด การเข้ารหัสข้อมูล หรือการใช้เครื่องมือที่ได้รับอนุมัติ

2.2.4.7 ความถี่ในการจัดกิจกรรมหรือการสื่อสารเรื่องความปลอดภัยภายในองค์กรเป็นดัชนีที่สะท้อนถึงความต่อเนื่องในการส่งเสริมวัฒนธรรมผ่านกิจกรรม เช่น การอบรม การประชาสัมพันธ์ หรือการจัดกิจกรรมรณรงค์ในวันสำคัญ

2.3 วิศวกรรมสังคมและพฤติกรรมผู้ใช้งาน

ในยุคดิจิทัลที่ระบบเทคโนโลยีสารสนเทศมีบทบาทสำคัญต่อการดำเนินงานขององค์กร ภัยคุกคามทางไซเบอร์ไม่ได้อาศัยเพียงกลไกทางเทคนิคในการเจาะระบบเท่านั้น หากแต่ยังอาศัย “จุดอ่อนของมนุษย์” หรือพฤติกรรมของผู้ใช้งานเป็นช่องทางสำคัญในการเข้าถึงข้อมูลหรือระบบภายในองค์กร เทคนิคที่ได้รับความนิยมจากผู้ไม่ประสงค์ดีในลักษณะนี้ คือ วิศวกรรมสังคม (Social Engineering) ซึ่งเป็นการหลอกลวงหรือชักจูงเป้าหมายให้เปิดเผยข้อมูลสำคัญ ดำเนินการบางอย่างที่เป็นประโยชน์ต่อผู้โจมตี หรือเปิดช่องให้ภัยคุกคามเข้าสู่ระบบ โดยอาศัยความไว้ใจ ความเร่งรีบ หรือความไม่รู้ของเหยื่อ มากกว่าการใช้เทคโนโลยีขั้นสูง

2.3.1 รูปแบบของการโจมตีแบบวิศวกรรมสังคม

วิศวกรรมสังคม (Social Engineering) คือเทคนิคที่ผู้ไม่หวังดีใช้หลอกลวงเหยื่อให้เปิดเผยข้อมูลสำคัญหรือดำเนินการบางอย่างโดยอาศัยจิตวิทยาและพฤติกรรมมนุษย์มากกว่าการเจาะระบบทางเทคนิค [1] โดยมีรูปแบบการโจมตีที่หลากหลาย เช่น

2.3.1.1 Phishing การส่งอีเมลหรือข้อความปลอมที่ดูเหมือนมาจากแหล่งที่เชื่อถือได้ เช่น ธนาคาร หน่วยงานภายในองค์กร หรือบริการออนไลน์ เพื่อหลอกลวงให้ผู้ใช้งานเปิดเผยข้อมูลที่สำคัญ เช่น รหัสผ่าน หมายเลขบัตรเครดิต หรือคลิกลิงก์ที่ฝังมัลแวร์ไว้ [16]

2.3.1.2 Pretexting เป็นเทคนิคที่ผู้โจมตีแสดงตนเป็นบุคคลหรือองค์กรที่มีความน่าเชื่อถือ เช่น เจ้าหน้าที่ฝ่าย IT พนักงานธนาคาร หรือบุคลากรหน่วยงานภาครัฐ เพื่อหลอกขอข้อมูลที่เป็นความลับ โดยการสร้างสถานการณ์หรือบริบทปลอมขึ้นมาอย่างแนบเนียน

2.3.1.3 Baiting คือ การล่อลวงผู้ใช้งานด้วยของฟรีหรือสิ่งที่ดึงดูดความสนใจ เช่น USB drive ไฟล์เพลง/วิดีโอ หรือโปรแกรมแคร็ก เมื่อผู้ใช้งานเปิดหรือเชื่อมต่ออุปกรณ์เหล่านั้น มัลแวร์จะถูกติดตั้งในระบบทันทีโดยไม่รู้ตัว

2.3.2 ความเชื่อมโยงระหว่างพฤติกรรมมนุษย์และความเสี่ยงทางไซเบอร์

พฤติกรรมของผู้ใช้งานถือเป็นหนึ่งในจุดอ่อนที่สำคัญที่สุดของระบบความมั่นคงปลอดภัยไซเบอร์ แม้องค์กรจะมีการติดตั้งระบบเทคโนโลยีที่ทันสมัย แต่หากบุคลากรขาดความตระหนักรู้ด้านภัยคุกคาม ก็ยังคงมีความเสี่ยงสูงที่จะตกเป็นเป้าหมายของการโจมตี โดยเฉพาะในรูปแบบของวิศวกรรมสังคม (Social Engineering) เช่น การคลิกลิงก์ฟิชชิง การใช้รหัสผ่านซ้ำในหลายระบบ หรือการละเลยที่จะรายงานเหตุการณ์ที่ผิดปกติ ส่งผลให้ภัยคุกคามสามารถแพร่กระจายได้อย่างรวดเร็วและสร้างความเสียหายร้ายแรงต่อองค์กร

งานวิจัยหลายชิ้นชี้ให้เห็นว่า ความล้มเหลวในการฝึกอบรมบุคลากร และการขาดความเข้าใจด้านจิตวิทยาของมนุษย์ เป็นสาเหตุสำคัญที่ทำให้มาตรการด้านความมั่นคงปลอดภัยไม่ประสบผลสำเร็จ ผู้โจมตีมักใช้กลยุทธ์โน้มน้าว เช่น ความเร่งรีบ อำนาจ หรือความไว้วางใจ เพื่อกระตุ้นให้ผู้ใช้งานตัดสินใจอย่างไม่รอบคอบในสถานการณ์ที่ดูเร่งด่วนหรือกดดัน

เพื่อลดความเสี่ยงจากพฤติกรรมของผู้ใช้งาน แนวทางใหม่ที่มุ่งเน้นการมีส่วนร่วมของบุคลากรได้รับการเสนอแนะ อาทิ การใช้ escape room เพื่อฝึกทักษะด้านความปลอดภัย หรือการประยุกต์ใช้ แนวคิด gamification เช่น การให้คะแนน การแข่งขันตอบคำถาม และการมอบรางวัล เพื่อสร้างแรงจูงใจในการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ แนวทางเหล่านี้ไม่เพียงเพิ่มระดับการมีส่วนร่วม แต่ยังช่วยให้พฤติกรรมที่ปลอดภัยกลายเป็นส่วนหนึ่งของวัฒนธรรมองค์กรได้อย่างยั่งยืน

2.3.3 แนวทางการป้องกันที่ไม่ใช่แค่ด้านเทคนิค

การป้องกันภัยคุกคามจากวิศวกรรมสังคมไม่สามารถพึ่งพาเทคโนโลยีเพียงอย่างเดียวได้ จำเป็นต้องอาศัยมาตรการเชิงพฤติกรรม วัฒนธรรมองค์กร และการมีส่วนร่วมของบุคลากรในทุกระดับ การพัฒนา "ระบบภูมิคุ้มกัน" ทางพฤติกรรมจึงเป็นแนวทางที่ได้รับการเสนอแนะจากงานวิจัยหลายฉบับ โดยมีแนวทางที่สำคัญดังต่อไปนี้

2.3.3.1 การอบรมและทดสอบความตระหนัก (Awareness Training and Assessment) ควรดำเนินการอย่างต่อเนื่องและออกแบบให้สอดคล้องกับบทบาทหน้าที่ของกลุ่มเป้าหมาย เช่น บุคลากรทั่วไป ฝ่ายเทคนิค หรือผู้บริหารระดับสูง โดยเนื้อหาควรครอบคลุมภัยคุกคามที่ทันสมัย วิธีการสังเกตพฤติกรรมต้องสงสัย และวิธีตอบสนองที่เหมาะสม

2.3.3.2 การจำลองสถานการณ์ฟิชชิ่ง (Phishing Simulation) เป็นเทคนิคการทดสอบเชิงปฏิบัติที่ช่วยประเมินระดับความตื่นตัวของบุคลากร โดยใช้ข้อความหรืออีเมลปลอมที่เลียนแบบการโจมตีจริง เพื่อสังเกตพฤติกรรมการคลิก การรายงาน หรือการหลีกเลี่ยง และใช้ผลลัพธ์เป็นแนวทางปรับปรุงการฝึกอบรม

2.3.3.3 การใช้แนวทาง gamification และ escape room เป็นการประยุกต์ใช้หลักการของเกม เช่น ระบบคะแนน การให้รางวัล หรือสถานการณ์จำลองแบบ escape room ช่วยสร้างประสบการณ์การเรียนรู้ที่มีส่วนร่วม สนุก และเสริมสร้างความเข้าใจในภัยคุกคามอย่างลึกซึ้ง โดยเฉพาะในกลุ่มบุคลากรที่มีความหลากหลายทางพื้นฐานด้านเทคนิค

2.3.3.4 การสนับสนุนจากวัฒนธรรมองค์กร (Organizational Culture Support) ความมุ่งมั่นของผู้นำองค์กรเป็นปัจจัยสำคัญในการสร้างวัฒนธรรมที่ส่งเสริมความมั่นคงปลอดภัยไซเบอร์ ผู้นำควรมีบทบาทเชิงรุกในการสื่อสารนโยบาย เป็นแบบอย่างในการปฏิบัติตามแนวทาง และสนับสนุนให้เกิดการรายงานเหตุการณ์โดยไม่ตำหนิหรือเอาผิดบุคลากรที่ประสบเหตุ เพื่อส่งเสริมความกล้าในการเปิดเผยความเสี่ยง

2.4 แพลตฟอร์มชุมชนกับการเสริมสร้างความรู้และการมีส่วนร่วม

การเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ในระดับองค์กร จำเป็นต้องอาศัยแนวทางที่ต่อเนื่อง มีส่วนร่วม และสามารถปรับใช้ได้ในบริบทของการทำงานจริง แทนที่จะพึ่งพาเฉพาะการอบรมแบบทางเดียวหรือมาตรการทางเทคนิคเพียงอย่างเดียวเท่านั้น "แพลตฟอร์มชุมชน" (Community Platform) จึงเป็นกลไกที่มีศักยภาพสูงในการสนับสนุนการเรียนรู้ร่วมกัน การสื่อสารสองทาง และการสร้างการมีส่วนร่วมในวาระความปลอดภัยไซเบอร์ขององค์กร โดยเฉพาะในยุคที่ภัยคุกคามมีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว

2.4.1 ความหมายของแพลตฟอร์มชุมชน

แพลตฟอร์มชุมชนในบริบทของความมั่นคงปลอดภัยไซเบอร์ หมายถึง ระบบหรือเครื่องมือที่ช่วยเอื้ออำนวยให้เกิดการสื่อสาร การแลกเปลี่ยนข้อมูล และการมีปฏิสัมพันธ์ระหว่างบุคลากรในองค์กร ไม่ว่าจะเป็นในรูปแบบทางการ (เช่น Wiki, Knowledge Base) หรือไม่เป็นทางการ (เช่น ฟอรั่มสนทนา กระดานประกาศ หรือกลุ่มสนทนาในแอปพลิเคชันต่าง ๆ) โดยมีเป้าหมายหลักเพื่อเพิ่มการรับรู้ด้านภัยคุกคาม ความเข้าใจในแนวปฏิบัติที่เหมาะสม และส่งเสริมพฤติกรรมที่ปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศ

แพลตฟอร์มเหล่านี้สามารถประยุกต์ใช้ร่วมกับระบบงานประจำ และมีศักยภาพในการเชื่อมโยงกับเครื่องมือสื่อสารภายในอื่น ๆ เช่น Intranet, Microsoft Teams, SharePoint หรือแม้แต่ Social Intranet อย่าง Viva Engage เพื่อสร้างพื้นที่แลกเปลี่ยนเรียนรู้ที่มีชีวิตชีวาและเข้าถึงได้ง่ายในทุกระดับ

2.4.2 บทบาทของแพลตฟอร์มในการสร้างการมีส่วนร่วม การเรียนรู้ร่วมกัน และการสร้างความตระหนักรู้

แพลตฟอร์มชุมชนมีบทบาทสำคัญในการส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กร โดยเป็นเครื่องมือที่ช่วยสนับสนุนการเรียนรู้ร่วมกัน การสื่อสารแบบสองทาง และการสร้างพฤติกรรมที่พึงประสงค์ด้านความปลอดภัยในกลุ่มบุคลากร ซึ่งสามารถจำแนกออกเป็น 3 บทบาทหลัก ดังต่อไปนี้

2.4.2.1 ส่งเสริมการเรียนรู้แบบมีปฏิสัมพันธ์ (Interactive Learning) ซึ่งแพลตฟอร์มชุมชนช่วยเปิดพื้นที่ให้บุคลากรสามารถมีส่วนร่วมในการเรียนรู้ผ่านการตั้งคำถาม การแสดงความเห็น การแบ่งปันประสบการณ์จากสถานการณ์จริง และการเรียนรู้ร่วมกันในรูปแบบที่ยืดหยุ่น ไม่จำกัดด้วยเวลาและสถานที่ ซึ่งสอดคล้องกับหลักการเรียนรู้แบบผู้ใหญ่ (Andragogy) ที่เน้นการเรียนรู้จากประสบการณ์ตรง ส่งผลให้ความรู้ที่ได้รับมีความเชื่อมโยงกับบริบทของการทำงานจริง และสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ

2.4.2.2 กระตุ้นการมีส่วนร่วมของพนักงาน (Employee Engagement) แพลตฟอร์มสามารถกระตุ้นให้พนักงานมีบทบาทมากขึ้นในประเด็นด้านความมั่นคงปลอดภัยไซเบอร์ ไม่ว่าจะเป็นการโพสต์ข้อมูลข่าวสาร แจ้งเตือนภัยคุกคาม การวิเคราะห์เหตุการณ์ที่เกิดขึ้น หรือการนำเสนอแนวทางแก้ไขที่เป็นประโยชน์ต่อองค์กร การมีบทบาทเชิงรุกเหล่านี้ช่วยส่งเสริมให้พนักงานเกิดความรู้สึกเป็นเจ้าของร่วมในวาระความมั่นคงปลอดภัยขององค์กร และช่วยสร้างแรงจูงใจให้เกิดการมีส่วนร่วมในระยะยาว

2.4.2.3 สร้างความตระหนักรู้ต่อเนื่อง (Continuous Awareness) แพลตฟอร์มสามารถทำหน้าที่เป็นสื่อกลางในการเผยแพร่ข้อมูล ข่าวสาร กิจกรรมรณรงค์ หรือเนื้อหาฝึกอบรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอและต่อเนื่อง ไม่จำกัดเฉพาะช่วงเวลาในการอบรมตามตาราง โดยเฉพาะในช่วงที่เกิดเหตุการณ์หรือภัยคุกคามใหม่ ๆ แพลตฟอร์มสามารถอัปเดตข้อมูลเพื่อกระตุ้นการรับรู้และการตอบสนองได้ทันท่วงที ซึ่งจะช่วยสร้างพฤติกรรมที่ปลอดภัยอย่างยั่งยืนในหมู่บุคลากร [16]

2.4.3 ตัวอย่างการใช้งานแพลตฟอร์มในองค์กร

องค์กรชั้นนำในหลากหลายอุตสาหกรรมได้ประยุกต์ใช้แพลตฟอร์มชุมชนในรูปแบบต่าง ๆ เพื่อส่งเสริมการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์และสร้างสภาพแวดล้อมที่เอื้อต่อการมีส่วนร่วมของบุคลากรอย่างต่อเนื่อง ทั้งในระดับปฏิบัติการและระดับนโยบาย โดยมีตัวอย่างการใช้งานที่สามารถจำแนกได้เป็นหมวดหมู่ ดังนี้

2.4.3.1 แพลตฟอร์มชุมชนภายในองค์กร หมายถึง ระบบหรือพื้นที่ออนไลน์ที่พัฒนาขึ้นเพื่อให้บุคลากรสามารถมีส่วนร่วมในการแลกเปลี่ยนความคิดเห็น การตั้งกระทู้ถาม-ตอบ การแบ่งปันประสบการณ์การทำงาน ตลอดจนการแจ้งเตือนภัยคุกคามที่เกี่ยวข้องกับงานด้านความมั่นคงปลอดภัยไซเบอร์ แพลตฟอร์มเหล่านี้มักเชื่อมโยงกับระบบ Intranet หรือระบบสื่อสารภายในที่มีอยู่เดิม เช่น Microsoft Teams, Yammer, หรือ Viva Engage โดยคุณลักษณะสำคัญของแพลตฟอร์มประเภทนี้ ได้แก่

2.4.3.1.1 การสนับสนุนการสนทนาแบบเรียลไทม์และแบบเธรด (threaded discussion)

2.4.3.1.2 การแจ้งเตือนอัตโนมัติเมื่อมีประเด็นใหม่ที่เกี่ยวข้องกับงาน

2.4.3.1.3 การสร้างกลุ่มย่อย (sub-community) เช่น กลุ่มผู้สนใจด้าน phishing กลุ่มวิเคราะห์เหตุการณ์ด้านไซเบอร์ ฯลฯ

2.4.3.1.4 การรวบรวมประเด็นสำคัญที่สามารถย้อนดูหรือค้นหาได้ภายหลัง

การมีแพลตฟอร์มลักษณะนี้ช่วยสร้าง “วัฒนธรรมองค์กรแบบเปิด” ที่ส่งเสริมการเรียนรู้ร่วมกันในหมู่พนักงาน และลดการพึ่งพาการฝึกอบรมแบบทางเดียวเพียงอย่างเดียว

2.4.3.2 ระบบ Wiki หรือคลังข้อมูลความรู้กลาง (Knowledge Base) เป็นอีกหนึ่งรูปแบบของแพลตฟอร์มชุมชนที่เน้นการจัดเก็บเนื้อหาอย่างเป็นระบบ เพื่อให้สามารถค้นหาและเรียกใช้ได้ง่ายในเวลาที่ต้องการ โดยเฉพาะสำหรับข้อมูลที่มีความสำคัญ เช่น แนวทางการปฏิบัติด้านความมั่นคงปลอดภัย (Security Guidelines) แผนตอบสนองเหตุการณ์ (Incident Response Plans) หรือคำถามที่พบบ่อยเกี่ยวกับนโยบายองค์กร โดยมีลักษณะเด่นของระบบนี้ ได้แก่

2.4.3.2.1 เนื้อหาสามารถปรับปรุงได้อย่างต่อเนื่องโดยผู้ใช้งานหรือผู้ดูแลระบบ

2.4.3.2.2 รองรับการเชื่อมโยงภายใน (internal linking) ระหว่างหัวข้อที่เกี่ยวข้อง

2.4.3.2.3 เหมาะสำหรับการเรียนรู้แบบ self-paced โดยไม่จำเป็นต้องมีการโต้ตอบแบบเรียลไทม์

ระบบดังกล่าวถือเป็น “คลังความรู้ขององค์กร” ที่สามารถนำมาใช้เพื่อเสริมสร้างความรู้เชิงลึกให้กับบุคลากรและลดความเสี่ยงจากความเข้าใจผิดด้านนโยบายความปลอดภัย

2.4.3.3 Microsoft OneNote เป็นเครื่องมือที่มีความยืดหยุ่นสูง สามารถประยุกต์ใช้เป็นแพลตฟอร์มชุมชนด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ โดยเฉพาะในกลุ่มงานหรือแผนกที่ต้องการรวบรวมข้อมูลในลักษณะไม่เป็นทางการ เช่น บันทึกเหตุการณ์ความปลอดภัยที่เกิดขึ้นภายในหน่วยงาน หรือแนวทางการป้องกันฟิชชิ่งที่ได้รับการทดลองใช้งานจริง โดยมีคุณสมบัติที่เหมาะกับการใช้งานในบริบทของการสร้างชุมชนความรู้ ได้แก่

2.4.3.3.1 การสร้างโน้ตบุ๊กแยกตามหมวดหมู่ (เช่น ภัยคุกคาม มาตรการตอบสนอง บทเรียนที่ได้รับ)

2.4.3.3.2 รองรับการแทรกเนื้อหาหลายรูปแบบ เช่น ข้อความ รูปภาพ คลิปวิดีโอ เอกสารแนบ ลิงก์

2.4.3.3.3 การใช้งานร่วมกันแบบเรียลไทม์และสามารถกำหนดสิทธิ์การเข้าถึงแต่ละหมวดหมู่ได้

OneNote สามารถผสานรวมกับเครื่องมืออื่นในระบบ Microsoft 365 ได้อย่างมีประสิทธิภาพ และเหมาะสำหรับใช้ทั้งในระดับปัจเจกบุคคล ทีมงาน และหน่วยงานระดับองค์กร

2.4.3.4 แพลตฟอร์มชุมชนที่มีองค์ประกอบของเกม (Gamified Community Platforms) เพื่อเพิ่มแรงจูงใจและความสนุกสนานในการมีส่วนร่วม องค์กรบางแห่งได้นำเทคนิค Gamification มาใช้ภายในแพลตฟอร์มชุมชน โดยออกแบบระบบให้มีองค์ประกอบของเกม เช่น

2.4.3.4.1 การให้ Badge หรือเหรียญรางวัลสำหรับพนักงานที่มีการแชร์ความรู้หรือเข้าร่วมกิจกรรมบ่อยครั้ง

2.4.3.4.2 ระบบ Leaderboard หรือการจัดอันดับผู้ใช้งานที่มีส่วนร่วมสูงสุดประจำเดือน/ไตรมาส

2.4.3.4.3 การออกแบบภารกิจเสมือน (missions) เช่น “ตอบคำถาม 5 ข้อเกี่ยวกับ Phishing ภายในสัปดาห์นี้” หรือ “แบ่งปันบทเรียนจากเหตุการณ์ Security Incident 1 กรณี”

แนวทางนี้ไม่เพียงช่วยเพิ่มความน่าสนใจให้กับการใช้งานแพลตฟอร์ม แต่ยังช่วยกระตุ้นให้บุคลากรมีส่วนร่วมในกระบวนการเรียนรู้อย่างต่อเนื่องในระยะยาว

2.4.4 ข้อพิจารณาในการเลือกใช้แพลตฟอร์มให้เหมาะสม

การเลือกใช้แพลตฟอร์มชุมชนให้เหมาะสมกับบริบทขององค์กรนับเป็นขั้นตอนสำคัญในกระบวนการออกแบบระบบที่มีประสิทธิภาพ โดยเฉพาะอย่างยิ่งในองค์กรที่มีโครงสร้างซับซ้อนหรือมีความแตกต่างด้านความพร้อมทางเทคโนโลยีระหว่างหน่วยงาน การเลือกแพลตฟอร์มอย่างเป็นระบบและมีกลยุทธ์จะส่งผลโดยตรงต่อประสิทธิภาพในการใช้งาน ตลอดจนระดับการมีส่วนร่วมของบุคลากรในระยะยาว ทั้งนี้ องค์กรควรพิจารณาปัจจัยหลักในหลายมิติ ดังต่อไปนี้

2.4.4.1 ลักษณะโครงสร้างองค์กร

โครงสร้างขององค์กรมีอิทธิพลต่อรูปแบบและแนวทางการใช้งานแพลตฟอร์มอย่างมาก หากเป็นองค์กรที่มีลักษณะการบริหารแบบรวมศูนย์ (Centralized) อาจจำเป็นต้องเลือกใช้แพลตฟอร์มที่เน้นการควบคุมเนื้อหาและกำหนดสิทธิ์การเข้าถึงอย่างชัดเจน ขณะที่องค์กรที่มีลักษณะการทำงานแบบกระจาย หรือมีการดำเนินงานในรูปแบบทีมข้ามสายงาน (Cross-functional teams) ควรเลือกแพลตฟอร์มที่สามารถรองรับการทำงานแบบกลุ่มย่อย (Sub-community) และเปิดโอกาสให้แต่ละทีมสามารถบริหารจัดการเนื้อหาได้ด้วยตนเองอย่างอิสระ

2.4.4.2 ระดับความพร้อมด้านดิจิทัลของบุคลากร

แพลตฟอร์มควรได้รับการออกแบบให้สอดคล้องกับระดับทักษะด้านเทคโนโลยีของบุคลากรในองค์กร โดยหากผู้ใช้งานส่วนใหญ่มีความเชี่ยวชาญด้านดิจิทัลในระดับจำกัด ควรเลือกใช้แพลตฟอร์มที่มีอินเทอร์เฟซที่เป็นมิตร ใช้งานง่าย และไม่ซับซ้อน ในทางกลับกัน หากองค์กรมีบุคลากรที่มีความคุ้นเคยกับระบบสารสนเทศและเครื่องมือดิจิทัลอยู่แล้ว อาจสามารถเลือกใช้แพลตฟอร์มที่มีฟีเจอร์ขั้นสูงหรือสามารถปรับแต่งได้มากขึ้น

2.4.4.3 วัตถุประสงค์หลักของการใช้งาน ซึ่งองค์กรควรกำหนดวัตถุประสงค์ของการใช้งานแพลตฟอร์มอย่างชัดเจน เพื่อให้สามารถเลือกแพลตฟอร์มที่ตอบสนองต่อเป้าหมายได้อย่างเหมาะสม เช่น

2.4.4.3.1 การฝึกอบรม (Training) ควรเลือกแพลตฟอร์มที่มีระบบจัดการเนื้อหา (Content Management) รองรับการจัดทำบทเรียน ติดตามผลการเรียนรู้ และวัดผลการฝึกอบรมได้

2.4.4.3.2 การแจ้งเตือนและเผยแพร่ข่าวสาร (Alerts & Communication) ควรมีระบบแจ้งเตือนแบบ Push Notification และฟังก์ชันการจัดการเนื้อหาจากส่วนกลาง เพื่อให้สามารถสื่อสารอย่างรวดเร็วและทั่วถึง

2.4.4.3.3 การสร้างเครือข่ายความรู้ (Knowledge Sharing) ควรมีระบบคลังข้อมูลที่ค้นหาได้ง่าย และรองรับการโต้ตอบ เช่น การแสดงความคิดเห็น การจัดหมวดหมู่เนื้อหา และการจัดอันดับความน่าเชื่อถือของข้อมูล

2.4.4.4 ความสามารถในการเชื่อมต่อกับระบบอื่นในองค์กร

แพลตฟอร์มควรสามารถเชื่อมต่อกับระบบสารสนเทศอื่น ๆ ที่องค์กรใช้อยู่เดิม เช่น Microsoft 365, SharePoint, หรือ Intranet เพื่อสร้างประสบการณ์การใช้งานที่ต่อเนื่อง (Seamless User Experience) ลดภาระการสลับแพลตฟอร์ม และเพิ่มโอกาสในการเข้าถึงเนื้อหาที่เกี่ยวข้องในบริบทของงานประจำ

2.4.4.5 ความมั่นคงปลอดภัยของระบบ

เนื่องจากแพลตฟอร์มชุมชนมักมีการแลกเปลี่ยนข้อมูลที่อาจมีความอ่อนไหว จึงจำเป็นต้องมีมาตรการควบคุมที่รัดกุม เช่น

2.4.4.5.1 การกำหนดสิทธิ์เข้าถึง (Access Control) เพื่อจำกัดการเข้าถึงข้อมูลตามบทบาทหน้าที่

2.4.4.5.2 การเข้ารหัสข้อมูล (Data Encryption) เพื่อปกป้องข้อมูลระหว่างการรับ-ส่ง

2.4.4.5.3 การบันทึกประวัติการใช้งาน (Audit Trail) เพื่อตรวจสอบการเข้าถึงหรือการแก้ไขข้อมูลย้อนหลัง

2.4.4.5.4 การจัดการการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) เพื่อเสริมความมั่นคงในการเข้าสู่ระบบ

การออกแบบและเลือกใช้แพลตฟอร์มชุมชนอย่างเป็นระบบและมีกลยุทธ์ ไม่เพียงช่วยให้เนื้อหาด้านความมั่นคงปลอดภัยสามารถเผยแพร่และเข้าถึงได้ง่ายอย่างเหมาะสมกับแต่ละกลุ่มเป้าหมาย แต่ยังเป็นการสร้างแรงจูงใจในการเรียนรู้ของพนักงาน ลดภาระของฝ่ายสนับสนุนทางเทคนิค และที่สำคัญ คือ สร้างรากฐานของวัฒนธรรมองค์กรที่เข้มแข็งด้านความมั่นคงปลอดภัยในระยะยาว ซึ่งเป็นเป้าหมายหลักของการพัฒนาแพลตฟอร์มชุมชนในบริบทองค์กรยุคดิจิทัล

2.5 การใช้ Microsoft OneNote และ Microsoft 365 ในการสนับสนุนการเรียนรู้ร่วมกัน

ในยุคดิจิทัลที่องค์กรต้องเผชิญกับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและเปลี่ยนแปลงอย่างต่อเนื่อง การสร้าง “ระบบนิเวศแห่งการเรียนรู้ร่วมกัน” (Collaborative Learning Ecosystem) ภายในองค์กรจึงนับเป็นแนวทางสำคัญในการเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์อย่างยั่งยืน โดยเฉพาะเมื่อการพัฒนาองค์ความรู้และพฤติกรรมที่ปลอดภัยของบุคลากรจำเป็นต้อง

อาศัยการมีส่วนร่วมในระดับทีมและองค์กรอย่างเป็นระบบ Microsoft OneNote และชุดเครื่องมือ Microsoft 365 จึงได้รับการยอมรับว่าเป็นโครงสร้างพื้นฐานดิจิทัลที่สามารถสนับสนุนกระบวนการเรียนรู้ร่วมกันดังกล่าวได้อย่างครอบคลุม ทั้งในมิติของการจัดการความรู้ การสื่อสารภายใน และการสร้างการมีส่วนร่วมจากบุคลากรทุกระดับ [17]

2.5.1 คุณสมบัติของ Microsoft OneNote สำหรับการจัดการความรู้

Microsoft OneNote เป็นเครื่องมือบันทึกดิจิทัลที่สามารถประยุกต์ใช้เป็นฐานข้อมูลความรู้ร่วมกัน (Collaborative Knowledge Base) ทั้งในระดับทีมและระดับองค์กร โดยมีคุณลักษณะที่สอดคล้องกับแนวคิดการบริหารจัดการความรู้ (Knowledge Management : KM) และสามารถรองรับการพัฒนาแพลตฟอร์มชุมชนภายในองค์กรได้อย่างมีประสิทธิภาพ ดังนี้

2.5.1.1 การจัดโครงสร้างข้อมูลอย่างเป็นระบบ

OneNote ช่วยให้ผู้ใช้สามารถสร้าง สมุดบันทึก (Notebook) และแบ่งเนื้อหาออกเป็น Section และ Page ได้อย่างชัดเจน ซึ่งเอื้อให้สามารถจัดเก็บข้อมูลในลักษณะหมวดหมู่ เช่น ภัยคุกคามล่าสุด แนวทางรับมือเหตุการณ์ หรือ แนวปฏิบัติด้านความปลอดภัย ได้อย่างเป็นระบบและค้นหาได้สะดวก

2.5.1.2 รองรับเนื้อหาหลากหลายรูปแบบ

ผู้ใช้สามารถแทรกข้อมูลได้หลากหลายประเภท ได้แก่ ข้อความ ลิงก์ รูปภาพ วิดีโอ ไฟล์แนบ หรือเสียงบันทึก ซึ่งช่วยให้การนำเสนอข้อมูลมีความลึกและหลากหลายมิติ รองรับทั้งการเรียนรู้เชิงเทคนิคและการแลกเปลี่ยนประสบการณ์

2.5.1.3 การทำงานร่วมกันแบบเรียลไทม์ (Real-time Collaboration)

OneNote รองรับการใช้งานแบบกลุ่ม โดยผู้ใช้งานหลายคนสามารถเข้าถึง แก้ไข แสดงความคิดเห็น และเพิ่มข้อมูลลงในเนื้อหาเดียวกันได้ในเวลาเดียวกัน พร้อมทั้งมีระบบบันทึกประวัติการเปลี่ยนแปลง (Version History) เพื่อความโปร่งใสในการติดตาม

2.5.1.4 ความยืดหยุ่นในการเข้าถึง

OneNote สามารถเข้าถึงได้จากหลากหลายอุปกรณ์ ไม่ว่าจะเป็นคอมพิวเตอร์ สมาร์ทโฟน หรือแท็บเล็ต ผ่านระบบคลาวด์ของ Microsoft 365 ช่วยให้ผู้ใช้งานสามารถเรียนรู้และใช้งานแพลตฟอร์มได้ทุกที่ทุกเวลา (Anytime, Anywhere)

ด้วยคุณลักษณะข้างต้น Microsoft OneNote จึงเป็นเครื่องมือที่เหมาะสมอย่างยิ่งในการทำหน้าที่เป็น “แพลตฟอร์มชุมชนสำหรับการจัดการความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์” เช่น การจัดเก็บบทเรียนจากเหตุการณ์ (Post-Incident Review) แนวทางปฏิบัติ (Best Practices) หรือข้อมูลอ้างอิงที่ใช้ในการอบรมภายในองค์กรอย่างต่อเนื่อง

2.5.2 การบูรณาการ OneNote กับ Microsoft Teams, Forms และ SharePoint เพื่อสร้างการมีส่วนร่วม

การบูรณาการ Microsoft OneNote เข้ากับเครื่องมืออื่นในชุด Microsoft 365 ถือเป็นกลยุทธ์สำคัญในการส่งเสริมการมีส่วนร่วมของบุคลากร และเสริมสร้างความแข็งแกร่งให้กับโครงสร้างการเรียนรู้ร่วมกันในระดับองค์กร โดยเครื่องมือแต่ละตัวมีบทบาทที่เกื้อหนุนกันและส่งเสริม

กระบวนการเรียนรู้แบบเป็นวงจร (Learning Loop) ซึ่งครอบคลุมการรวบรวมเนื้อหา การแบ่งปัน การประเมินผล และการพัฒนาเนื้อหาอย่างต่อเนื่อง รายละเอียดของการบูรณาการ มีดังนี้

2.5.2.1 Microsoft Teams

Microsoft Teams สามารถบูรณาการกับ OneNote โดยฝังสมุดบันทึกไว้ภายในแต่ละ Channel เพื่อใช้เป็นศูนย์กลางในการจดบันทึกการประชุม การวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Analysis) รวมถึงการจัดเก็บแนวทางปฏิบัติ (Standard Operating Procedures) อย่างเป็นระบบและโปร่งใส นอกจากนี้ยังสามารถใช้เป็นพื้นที่สำหรับถาม-ตอบ (Team-based Q&A) และแลกเปลี่ยนข้อเสนอแนะระหว่างสมาชิกภายในทีม ซึ่งช่วยกระตุ้นให้เกิดการมีส่วนร่วมและการเรียนรู้ร่วมกันในระดับปฏิบัติการ

2.5.2.2 Microsoft Forms

Microsoft Forms ทำหน้าที่เป็นเครื่องมือในการรวบรวมข้อมูล เช่น แบบสอบถามหลังการอบรม ความพึงพอใจของผู้ใช้ หรือการประเมินความเข้าใจในหัวข้อด้านความมั่นคงปลอดภัย ข้อมูลที่ได้สามารถเชื่อมโยงและบันทึกลงใน OneNote เพื่อใช้วิเคราะห์และปรับปรุงแผนการฝึกอบรม หรือเนื้อหาในแพลตฟอร์มชุมชนในลำดับถัดไป ส่งเสริมให้กระบวนการพัฒนาความรู้เป็นไปอย่างมีทิศทางและอิงจากข้อมูลจริง (Data-informed Training Development) [18]

2.5.2.3 Microsoft SharePoint

OneNote สามารถเชื่อมโยงกับ SharePoint เพื่อจัดตั้งเป็นคลังความรู้กลางขององค์กร (Centralized Knowledge Repository) ซึ่งช่วยให้ทุกหน่วยงานสามารถเข้าถึงข้อมูลสำคัญผ่านระบบที่มีความปลอดภัย โดยสามารถกำหนดสิทธิ์การเข้าถึงตามบทบาทหน้าที่ (Role-based Access) ได้อย่างมีประสิทธิภาพ การผนวกนี้ยังช่วยลดความซ้ำซ้อนของข้อมูล เพิ่มความน่าเชื่อถือของแหล่งอ้างอิง และส่งเสริมการจัดการองค์ความรู้ที่มีความต่อเนื่อง

การผสานการทำงานของ OneNote กับ Microsoft Teams, Forms และ SharePoint จึงไม่ได้เป็นเพียงการเชื่อมโยงเครื่องมือในเชิงเทคนิคเท่านั้น แต่ยังเป็นการสร้างโครงสร้างพื้นฐานที่สนับสนุนการเรียนรู้ร่วมกัน การสื่อสารแบบเปิด และการมีส่วนร่วมของบุคลากรอย่างยั่งยืน ส่งผลให้เกิด “วัฏจักรการเรียนรู้” (Learning Cycle) ที่ต่อเนื่อง ตั้งแต่ขั้นตอนการจัดเก็บ ⟶ การแบ่งปัน ⟶ การวิเคราะห์ ⟶ การปรับปรุง ⟶ จนถึงการนำไปใช้จริง ซึ่งเป็นหัวใจสำคัญของการเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยในระดับองค์กร [18]

2.5.3 กรณีศึกษาและงานวิจัยที่เกี่ยวข้องกับการใช้ OneNote เพื่อส่งเสริมความรู้หรือความมั่นคงปลอดภัย

การประยุกต์ใช้ Microsoft OneNote เพื่อส่งเสริมการเรียนรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ได้รับการยืนยันจากงานวิจัยและกรณีศึกษาหลายฉบับ โดยเครื่องมือนี้แสดงให้เห็นถึงศักยภาพในการเพิ่มระดับการมีส่วนร่วมของผู้ใช้งาน (Engagement) ส่งเสริมการจดจำความรู้ (Knowledge Retention) และสนับสนุนการตัดสินใจที่เกี่ยวข้องกับความมั่นคงปลอดภัยภายในองค์กร

ตัวอย่างเช่น งานวิจัยของ Yucel, และคณะ [20] รายงานผลจากการที่องค์กรหนึ่งได้นำ OneNote มาใช้ร่วมกับแพลตฟอร์มชุมชนภายใน เพื่อจัดทำและเผยแพร่บทเรียนจากเหตุการณ์

ด้านไซเบอร์ (Lessons Learned) อย่างต่อเนื่อง ซึ่งสามารถช่วยเพิ่มระดับการมีส่วนร่วมของพนักงานและลดพฤติกรรมที่ละเลยนโยบายด้านความปลอดภัยลงได้มากถึง 35% ภายในระยะเวลาเพียง 6 เดือน

นอกจากนี้ งานของ Warasart และ Piriyasurawong ยังได้ศึกษาการฝึกอบรมด้านไซเบอร์ในรูปแบบ Blended Learning ที่ผสานการใช้ OneNote ร่วมกับ Microsoft Teams และ Forms ผลการศึกษาแสดงให้เห็นว่าผู้เรียนมีอัตราการจดจำเนื้อหาสูงขึ้นกว่า 40% เมื่อเทียบกับกลุ่มที่เข้าร่วมการอบรมแบบดั้งเดิม อีกทั้งยังสามารถตอบสนองต่อสถานการณ์ฟิชชิ่งจำลองได้อย่างถูกต้องมากขึ้น

ขณะที่กรณีศึกษาจากหน่วยงานภาครัฐในสหราชอาณาจักร ได้ประยุกต์ใช้ OneNote ควบคู่กับ SharePoint ในการพัฒนาเป็นศูนย์กลางฐานข้อมูลด้าน Security Policy และ Incident Response Plan สำหรับใช้งานภายในองค์กร ซึ่งช่วยให้เจ้าหน้าที่สามารถเข้าถึงข้อมูลล่าสุดได้ทุกที่ทุกเวลา ลดความล่าช้าในการตัดสินใจ เพิ่มความโปร่งใสในการประสานงาน และสนับสนุนการจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ

กรณีศึกษาทั้งสามนี้สะท้อนให้เห็นว่า Microsoft OneNote มิได้เป็นเพียงเครื่องมือสำหรับจดบันทึกหรือจัดเก็บข้อมูลเท่านั้น หากแต่สามารถพัฒนาให้เป็น “แพลตฟอร์มชุมชน” ที่มีบทบาทสำคัญในการส่งเสริมการเรียนรู้ร่วมกัน การจัดการองค์ความรู้ และการสร้างวัฒนธรรมความมั่นคงปลอดภัยภายในองค์กรได้อย่างยั่งยืนและมีประสิทธิภาพ

2.6 งานวิจัยที่เกี่ยวข้อง

ผู้วิจัยได้ทำการศึกษาค้นคว้าและทบทวนงานวิจัย เพื่อศึกษาแนวคิดและการพัฒนาแพลตฟอร์มชุมชนเพื่อเสริมสร้างวัฒนธรรมความปลอดภัยไซเบอร์ โดยพบว่า

Muronga และคณะ พบว่าการฝึกอบรมมีบทบาทสำคัญในการลดความเสี่ยงที่เกิดจากพฤติกรรมของผู้ใช้ในการเผชิญภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ การฝึกอบรมช่วยให้ผู้ใช้มีความรู้และทักษะในการป้องกันตนเองจากภัยคุกคาม ซึ่งมีความสำคัญต่อการสร้างวัฒนธรรมความปลอดภัยในองค์กร Oroszi และคณะ สนับสนุนการลงทุนในโปรแกรมฝึกอบรมเพื่อเสริมสร้างความตระหนักรู้เป็นวิธีใหม่ในการเสริมสร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์

Warasart และ Piriyasurawong ใช้แพลตฟอร์มออนไลน์ เช่น สื่อสังคมออนไลน์เพื่อเพิ่มความตระหนักรู้และสร้างการมีส่วนร่วมในเรื่องความปลอดภัยไซเบอร์ การวิจัยพบว่าแพลตฟอร์มออนไลน์สามารถเป็นเครื่องมือที่มีประสิทธิภาพในการเผยแพร่ข้อมูลและสนับสนุนด้านความปลอดภัย M. Schiappa และคณะ ใช้แพลตฟอร์มเหล่านี้ช่วยให้ข้อมูลความปลอดภัยกระจายไปยังกลุ่มเป้าหมายได้อย่างรวดเร็วและครอบคลุม

Ioannou และคณะ เน้นถึงความสำคัญของการออกแบบแพลตฟอร์มที่ใช้งานง่ายและส่งเสริมความร่วมมือ การวิจัยนี้ชี้ให้เห็นว่าการออกแบบแพลตฟอร์มที่ดีช่วยให้การแลกเปลี่ยนข้อมูลในองค์กรให้มีความปลอดภัยไซเบอร์เป็นไปอย่างสะดวกและมีประสิทธิภาพ การออกแบบที่ดีช่วยให้ผู้ใช้สามารถเข้าถึงข้อมูลได้ง่ายและร่วมมือกันในการป้องกันภัยคุกคาม

Mansol และคณะ พบว่าการสื่อสารและการฝึกอบรมมีบทบาทสำคัญในการส่งเสริมพฤติกรรมความปลอดภัยในองค์กร การสร้างวัฒนธรรมความปลอดภัยในองค์กรช่วยลดความเสี่ยงจาก

ภัยคุกคามได้อย่างมีประสิทธิภาพ วัฒนธรรมความปลอดภัยช่วยสร้างความตระหนักรู้และความร่วมมือในองค์กร ซึ่งเป็นปัจจัยสำคัญในการป้องกันการโจมตีทางไซเบอร์ Yulianto and Soewito ศึกษาภัยคุกคามจากการโจมตีด้วยแรนซัมแวร์ที่เพิ่มขึ้นในโลกที่เชื่อมต่อถึงกันและดิจิทัลก่อให้เกิดอุปสรรคสำคัญต่อความปลอดภัยทางไซเบอร์ได้เช่นกัน

Roobini และคณะ พบว่าการแบ่งปันข้อมูลภัยคุกคามบนคลาวด์ระหว่างชุมชนหรือองค์กรช่วยลดความเสี่ยงและเพิ่มความสามารถในการป้องกันการโจมตีทางไซเบอร์ ซึ่งการสร้างแพลตฟอร์มการแลกเปลี่ยนข้อมูลช่วยให้ชุมชนสามารถแบ่งปันข้อมูลและความรู้ในการรับมือกับภัยคุกคามได้

Cherqi [18] และคณะ เน้นการใช้ AI, Machine Learning หรือ Open-source Threat Intelligence ในการตรวจจับและแจ้งเตือนภัยคุกคาม เทคโนโลยีอัตโนมัติช่วยเพิ่มประสิทธิภาพในการจัดการชุมชนและลดภาระงานของผู้ดูแลระบบ การใช้เครื่องมือเหล่านี้ช่วยให้การตรวจจับภัยคุกคามเป็นไปอย่างรวดเร็วและแม่นยำ ทำให้สามารถตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพ

Khadka และคณะ ศึกษาหลักการของ persuasion ที่ใช้เป็นกลยุทธ์ทางวิศวกรรมสังคม (Social Engineering) ในการโจมตีแบบฟิชชิ่ง โดยได้ทำการสำรวจแนวทางที่ผู้โจมตีใช้โน้มน้าวเหยื่อผ่านกลวิธีทางจิตวิทยา ซึ่งผลการศึกษานี้ช่วยให้เข้าใจรูปแบบของการชักจูงและสามารถนำไปใช้ในการพัฒนามาตรการตอบสนองหรือการฝึกอบรมเพื่อลดความเสี่ยงจากฟิชชิ่ง

Nasir วิเคราะห์ประสิทธิภาพของโปรแกรมฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ โดยระบุปัจจัยสำคัญที่ส่งผลต่อผลลัพธ์ของการฝึกอบรม เช่น เนื้อหาที่สอดคล้องกับสถานการณ์จริง วิธีการสอนที่ตอบสนองผู้เรียน และการประเมินผลที่ต่อเนื่อง พร้อมนำเสนอแนวทางปฏิบัติที่ดีที่สุดเพื่อการพัฒนาโปรแกรมในอนาคต

Roobini และคณะ เสนอการใช้ระบบ Threat Intelligence แบบ Cloud-Based ที่มุ่งเน้นการแบ่งปันข้อมูลภัยคุกคามระหว่างองค์กรเพื่อการป้องกันร่วมกัน โดยเน้นแนวคิด “ Collective Defence” ซึ่งช่วยให้องค์กรต่าง ๆ สามารถตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบมากขึ้น

Trocoso-Pastoriza และคณะ [19] พัฒนาเฟรมเวิร์กที่ปลอดภัยสำหรับการแบ่งปันข้อมูลภัยคุกคามแบบกระจายตัว (Distributed Threat Intelligence Sharing) ที่รักษาความเป็นส่วนตัวโดยใช้เทคนิค privacy-preserving cryptographic protocols ซึ่งช่วยให้หลายองค์กรสามารถทำงานร่วมกันได้โดยไม่ต้องเปิดเผยข้อมูลที่อ่อนไหว

Yucel และคณะ [20] ศึกษาวิธีการลบข้อมูลสำคัญหรือปรับแต่ง (Redaction and Sanitisation) ข้อมูลก่อนแบ่งปันผ่านแพลตฟอร์ม Threat Intelligence เพื่อหลีกเลี่ยงการรั่วไหลของข้อมูลที่ไม่จำเป็นหรือมีความเป็นส่วนตัวสูง ซึ่งเป็นสิ่งสำคัญในการสร้างความเชื่อมั่นให้กับผู้ใช้แพลตฟอร์มและรักษาความปลอดภัยของข้อมูล

จากการศึกษางานวิจัยที่เกี่ยวข้อง พบว่าแนวทางที่นิยมใช้ในการเสริมสร้างวัฒนธรรมความปลอดภัยไซเบอร์ในองค์กร ได้แก่ การฝึกอบรมและสร้างความตระหนักรู้เพื่อเสริมทักษะผู้ใช้งาน การใช้แพลตฟอร์มออนไลน์ในการเผยแพร่ข้อมูลและสร้างการมีส่วนร่วม รวมถึงการแบ่งปันข้อมูลภัยคุกคามเพื่อการป้องกันร่วมกัน นอกจากนี้ยังมีการนำเทคโนโลยีอัตโนมัติ เช่น AI และ Machine

Learning มาใช้การออกแบบแพลตฟอร์มที่ใช้งานง่ายเพื่อส่งเสริมการเข้าถึง การศึกษาพฤติกรรมผู้ใช้งานเพื่อตอบโต้ภัยวิศวกรรมสังคม และการปกป้องข้อมูลก่อนการแบ่งปัน

งานวิจัยฉบับนี้แตกต่างจากงานที่ผ่านมาด้วยการใช้ Microsoft OneNote เป็นศูนย์กลางของแพลตฟอร์มชุมชน ซึ่งสามารถบูรณาการกับเครื่องมือที่มีอยู่ในองค์กร เช่น Teams และ SharePoint ได้อย่างมีประสิทธิภาพ โดยเน้นการสร้างวัฒนธรรมความปลอดภัยผ่านการมีส่วนร่วมอย่างต่อเนื่อง เช่น การจัดทำบทเรียนจากเหตุการณ์จริง แบบทดสอบ และกระดานแจ้งเตือน แนวทางนี้จึงมุ่งเน้นความยั่งยืนในการเรียนรู้ร่วมกัน มากกว่าการใช้เครื่องมือภายนอกหรือการดำเนินการในระยะสั้น

บทที่ 3
วิธีการดำเนินงานวิจัย

เพื่อให้การพัฒนาแพลตฟอร์มชุมชนด้วย Microsoft OneNote สามารถตอบสนองต่อวัตถุประสงค์ของการวิจัยและส่งเสริมวัฒนธรรมความปลอดภัยไซเบอร์ภายในองค์กรได้อย่างมีประสิทธิภาพ ผู้วิจัยได้กำหนดขั้นตอนการดำเนินงานวิจัยอย่างเป็นระบบ โดยแบ่งออกเป็น 3 ส่วนหลัก ดังนี้

3.1 การออกแบบกรอบการวิจัย

3.2 การกำหนดและคัดเลือกกลุ่มเป้าหมาย

3.3 การพัฒนาและใช้งานแพลตฟอร์มชุมชนภายในองค์กรโดยใช้ Microsoft OneNote

3.4 การพัฒนาแบบทดสอบความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Knowledge Test)

3.5 การพัฒนาแบบสอบถามความพึงพอใจของบุคลากรที่เข้ามาใช้งานแพลตฟอร์มชุมชนความปลอดภัยไซเบอร์

3.6 การประเมินผล

3.1 การออกแบบกรอบการวิจัย

ผู้วิจัยเริ่มต้นด้วยการศึกษาทฤษฎีและแนวคิดที่เกี่ยวข้องกับวัฒนธรรมความปลอดภัยทางไซเบอร์ รวมถึงพฤติกรรมและปัจจัยที่ส่งผลต่อการรับรู้ด้านความปลอดภัยไซเบอร์ของบุคลากร จากนั้นจึงศึกษากรณีตัวอย่างของแพลตฟอร์มชุมชนที่มีเป้าหมายในการให้ความรู้และสร้างความตระหนักด้านความปลอดภัยทางไซเบอร์ โดยมุ่งเน้นให้แพลตฟอร์มชุมชนเป็นแหล่งรวบรวมข้อมูลและแบ่งปันความรู้เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์แก่บุคลากรภายในองค์กร

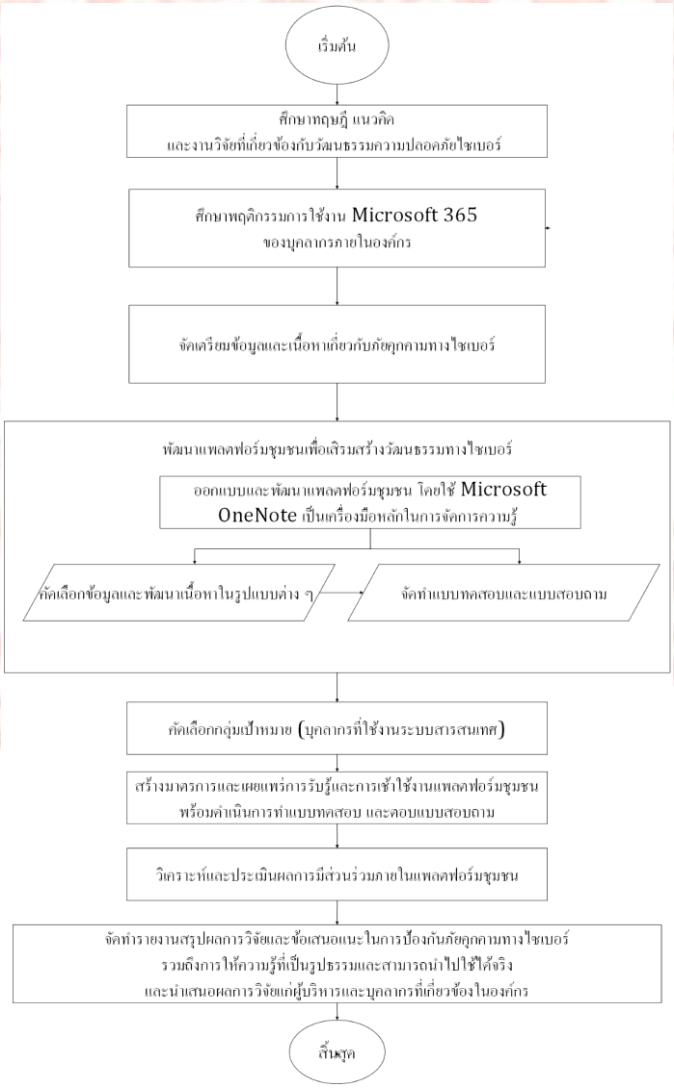
เมื่อเข้าใจแนวคิดพื้นฐานแล้ว ผู้วิจัยดำเนินการออกแบบแพลตฟอร์มชุมชนโดยใช้ Microsoft OneNote เป็นเครื่องมือหลักสำหรับการจัดการเนื้อหาและการมีส่วนร่วมของบุคลากร โดยคำนึงถึงโครงสร้างของแพลตฟอร์ม การจัดหมวดหมู่เนื้อหา กลไกการมีส่วนร่วมและการแลกเปลี่ยนความรู้ของบุคลากร มาตรการรักษาความปลอดภัยของแพลตฟอร์ม และการออกแบบส่วนปฏิสัมพันธ์ให้ใช้งานง่ายและเป็นมิตรกับบุคลากรขององค์กร

หลังจากออกแบบแล้ว ผู้วิจัยพัฒนาแพลตฟอร์มชุมชนโดยใช้ Microsoft OneNote และสร้างเนื้อหาที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ เช่น คู่มือแนะนำการใช้งานแพลตฟอร์ม เนื้อหาความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีป้องกัน บทความและกรณีศึกษาเกี่ยวกับการโจมตีทางไซเบอร์ที่พบในปัจจุบัน ตลอดจนการสื่อสารและการสร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์ผ่านกิจกรรมชุมชน รวมถึงการประเมินความตระหนักรู้ ความเข้าใจ และการตอบสนองภัยคุกคามทางไซเบอร์ของบุคลากร

ภายหลังจากพัฒนาแพลตฟอร์มเบื้องต้นแล้ว ผู้วิจัยจะทำการทดสอบการใช้งานกับกลุ่มเป้าหมาย ซึ่งประกอบด้วยบุคลากรที่มีความหลากหลายทางด้านความรู้ด้านความปลอดภัยไซเบอร์ เพื่อนำข้อมูลที่ได้จากการทดสอบไปปรับปรุงแพลตฟอร์มให้เหมาะสมมากขึ้น โดยมีกระบวนการทดสอบประสบการณ์การใช้งาน (User Experience Testing) การประเมินประสิทธิภาพของแพลตฟอร์ม และการเก็บข้อมูลจากบุคลากรผ่านแบบสอบถาม

สุดท้าย ผู้วิจัยจะทำการวิเคราะห์ข้อมูลที่ได้จากการใช้งานจริง โดยใช้วิธีการวิเคราะห์ข้อมูลเชิงคุณภาพและเชิงปริมาณ เพื่อวัดผลกระทบของแพลตฟอร์มที่มีต่อการเปลี่ยนแปลงพฤติกรรมและการรับรู้ด้านความปลอดภัยไซเบอร์ของบุคลากร พร้อมทั้งให้ข้อเสนอแนะสำหรับการพัฒนาแพลตฟอร์มในอนาคต รวมถึงแนวทางในการส่งเสริมวัฒนธรรมความปลอดภัยทางไซเบอร์ในระดับชุมชนและองค์กรต่อไป

เพื่อให้การวิจัยเป็นไปอย่างมีประสิทธิภาพ สอดคล้องกับขอบเขตและวัตถุประสงค์ ผู้วิจัยจึงได้กำหนดกระบวนการวิจัยแสดงในภาพที่ 3-1



ภาพที่ 3-1 แผนภาพแสดงกระบวนการวิจัย

3.2 การกำหนดและคัดเลือกกลุ่มเป้าหมาย

ผู้วิจัยได้กำหนดกลุ่มเป้าหมายโดยใช้วิธีการเลือกแบบเจาะจง (Purposive Sampling) [21] ซึ่งอาศัยดุลยพินิจในการคัดเลือกกลุ่มเป้าหมายที่มีคุณลักษณะตรงตามวัตถุประสงค์ โดยเน้นผู้ที่มีความเกี่ยวข้องและประสบการณ์ตรงในการใช้งานระบบสารสนเทศภายในองค์กร ซึ่งสามารถให้ข้อมูลที่เป็นประโยชน์ต่อการศึกษาวิจัยได้อย่างมีประสิทธิภาพ ทั้งนี้ ได้กำหนดให้มีตัวแทนจากทุกฝ่ายงาน เพื่อให้ได้ข้อมูลที่สะท้อนมุมมองและพฤติกรรมของผู้ใช้งานระบบสารสนเทศในแต่ละส่วนงานอย่างครอบคลุมและหลากหลาย ดังนั้น กลุ่มเป้าหมายสำหรับทดสอบแพลตฟอร์มนี้ ได้แก่ บุคลากรภายในองค์กรที่มีการใช้งานระบบสารสนเทศและการสื่อสารภายในองค์กรเป็นประจำ จากทั้ง 16 ฝ่ายงาน ซึ่งมีผู้สนใจเข้าร่วม 52 คน จากจำนวนบุคลากรทั้งหมด 109 คน คิดเป็นประมาณร้อยละ 47.71 หรือเกือบครึ่งหนึ่งของจำนวนบุคลากรในองค์กร ซึ่งถือเป็นสัดส่วนที่เหมาะสมในการสะท้อนความคิดเห็นและพฤติกรรมของกลุ่มผู้ใช้งานระบบสารสนเทศในบริบทขององค์กรได้อย่างครอบคลุม

3.3 การพัฒนาและใช้งานแพลตฟอร์มชุมชนภายในองค์กรโดยใช้ Microsoft OneNote

การดำเนินงานในส่วนนี้มุ่งเน้นการพัฒนาและใช้งานแพลตฟอร์มชุมชนภายในองค์กร โดยเลือกใช้ Microsoft OneNote เป็นเครื่องมือหลักในการรวบรวม จัดเก็บ และจัดการเนื้อหาเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ทั้งนี้ เนื่องจาก Microsoft OneNote มีคุณสมบัติที่เหมาะสมกับบริบทของการแบ่งปันความรู้ การทำงานร่วมกัน และการเข้าถึงได้อย่างสะดวกในรูปแบบดิจิทัลภายในองค์กร ซึ่งได้ออกแบบโครงสร้างเนื้อหาหลักในแพลตฟอร์มให้สอดคล้องกับวัตถุประสงค์ของการวิจัย และสนับสนุนการสร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ โดยแบ่งออกเป็นองค์ประกอบสำคัญ 8 ส่วน ดังต่อไปนี้

3.3.1 ส่วนพื้นฐานความปลอดภัยทางไซเบอร์ มีจำนวน 3 หน้า รายละเอียดดังต่อไปนี้

3.3.1.1 หน้าความสำคัญของไซเบอร์

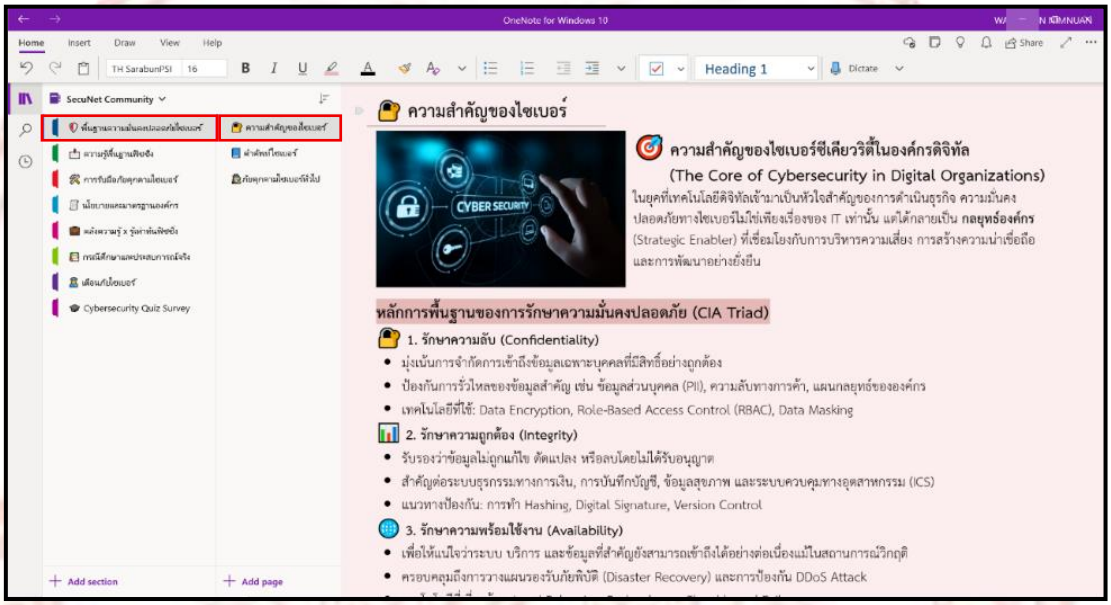
หน้าความสำคัญของไซเบอร์จัดอยู่ในส่วนของ พื้นฐานความปลอดภัยทางไซเบอร์ ซึ่งมีจุดประสงค์เพื่อให้บุคลากรในองค์กรเข้าใจถึงบทบาท ความจำเป็น และประโยชน์ของการมีระบบความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพในโลกยุคดิจิทัล โดยเนื้อหาครอบคลุมหัวข้อหลักที่เชื่อมโยงกับทั้งมิติทางธุรกิจ เทคโนโลยี และการบริหารความเสี่ยง ดังนี้

3.3.1.1.1 ความสำคัญของไซเบอร์ซีเคียวริตี้ในองค์กรดิจิทัล (The Core of Cybersecurity in Digital Organizations) ในยุคที่เทคโนโลยีดิจิทัลเข้ามาเป็นหัวใจสำคัญของการดำเนินธุรกิจ ความมั่นคงปลอดภัยทางไซเบอร์ไม่ใช่เพียงเรื่องของ IT เท่านั้น แต่ได้กลายเป็น กลยุทธ์องค์กร (Strategic Enabler) ที่เชื่อมโยงกับการบริหารความเสี่ยง การสร้างความน่าเชื่อถือ และการพัฒนาอย่างยั่งยืน

3.3.1.1.2 หลักการพื้นฐานของการรักษาความมั่นคงปลอดภัย (CIA Triad)ซึ่งการรักษาความมั่นคงปลอดภัยของสารสนเทศในองค์กรจะพิจารณาตามหลักการ 3 ประการ หรือที่เรียกว่า “CIA Triad” ได้แก่ Confidentiality (การรักษาความลับของข้อมูล) Integrity (ความถูกต้องครบถ้วนของข้อมูล) และ Availability (ความพร้อมใช้งานของข้อมูล)

3.3.1.1.3 เหตุผลที่องค์กรต้องลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ (Why Organizations Must Invest in Cybersecurity) เนื่องจากลดความเสี่ยงทางธุรกิจจากภัยไซเบอร์ สร้างความเชื่อมั่นแก่ผู้มีส่วนได้ส่วนเสีย สอดคล้องกับกฎหมายและมาตรฐานสากล และสนับสนุนการเปลี่ยนผ่านสู่ยุคดิจิทัล (Digital Transformation)

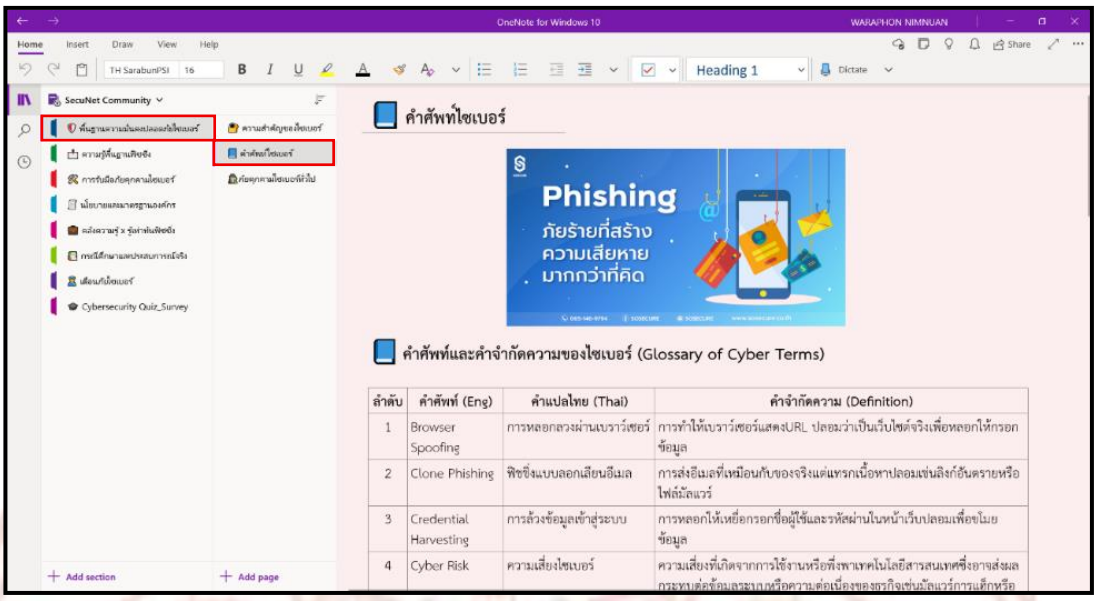
3.3.1.1.4 แนวทางป้องกันความเสี่ยงทางไซเบอร์ ประกอบด้วย ใช้รหัสผ่านที่ปลอดภัยและเปิดใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) หลีกเลี่ยงการคลิกลิงก์หรือเปิดไฟล์แนบจากแหล่งที่ไม่น่าเชื่อถือติดตั้งโปรแกรมป้องกันไวรัส และอัปเดตระบบให้เป็นเวอร์ชันล่าสุด และ สำรองข้อมูล (Backup) เป็นประจำ



ภาพที่ 3-2 หน้าความสำคัญของไซเบอร์

3.3.1.2 หน้าคำศัพท์ไซเบอร์

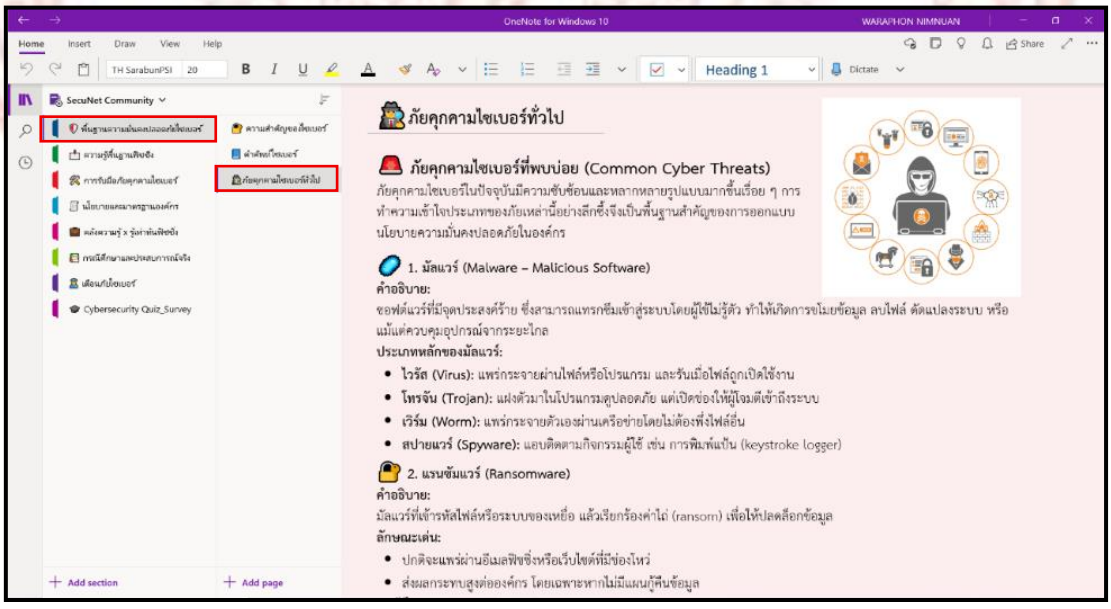
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อส่งเสริมการเรียนรู้และความเข้าใจที่ถูกต้องของบุคลากรในองค์กรเกี่ยวกับคำศัพท์และคำจำกัดความที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ (Glossary of Cyber Terms) โดยมุ่งเน้นให้ผู้ใช้งานสามารถทำความเข้าใจศัพท์เฉพาะทางที่ปรากฏบ่อยในเอกสารเนื้อหา หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวบรวมคำศัพท์สำคัญพร้อมคำแปลภาษาไทยและคำจำกัดความอย่างสังเขป เพื่อให้สามารถนำไปใช้ในการสื่อสาร การเรียนรู้ และการวางมาตรการด้านความปลอดภัยภายในองค์กรได้อย่างมีประสิทธิภาพ ทั้งยังช่วยลดความคลาดเคลื่อนจากความเข้าใจผิดในศัพท์เทคนิค ซึ่งเป็นปัจจัยหนึ่งที่อาจนำไปสู่ความเสี่ยงทางไซเบอร์โดยไม่รู้ตัว



ภาพที่ 3-3 หน้าคำศัพท์ไซเบอร์

3.3.1.3 หน้าภัยคุกคามไซเบอร์ทั่วไป

เนื้อหาในหน้านี้จัดทำขึ้นเพื่อส่งเสริมการเรียนรู้และสร้างความตระหนักรู้ให้แก่บุคลากรในองค์กรเกี่ยวกับลักษณะของภัยคุกคามทางไซเบอร์ที่พบได้บ่อยในสภาพแวดล้อมดิจิทัลยุคปัจจุบัน โดยมีจุดมุ่งหมายเพื่อให้ผู้ใช้งานสามารถเข้าใจประเภทของภัยคุกคามต่าง ๆ ได้อย่างถูกต้อง อันจะนำไปสู่การเตรียมความพร้อมในการป้องกันและรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพ

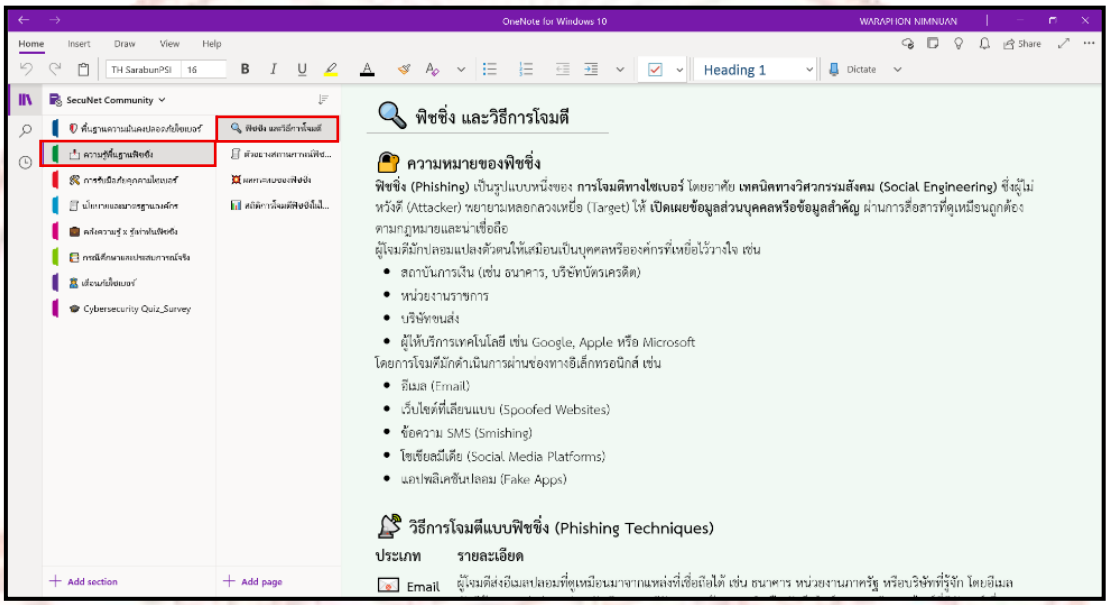


ภาพที่ 3-4 หน้าภัยคุกคามไซเบอร์ทั่วไป

3.3.2 ส่วนความรู้พื้นฐานฟิชชิ่ง มีจำนวน 4 หน้า รายละเอียดดังต่อไปนี้

3.3.2.1 หน้าฟิชชิ่ง และวิธีการโจมตี

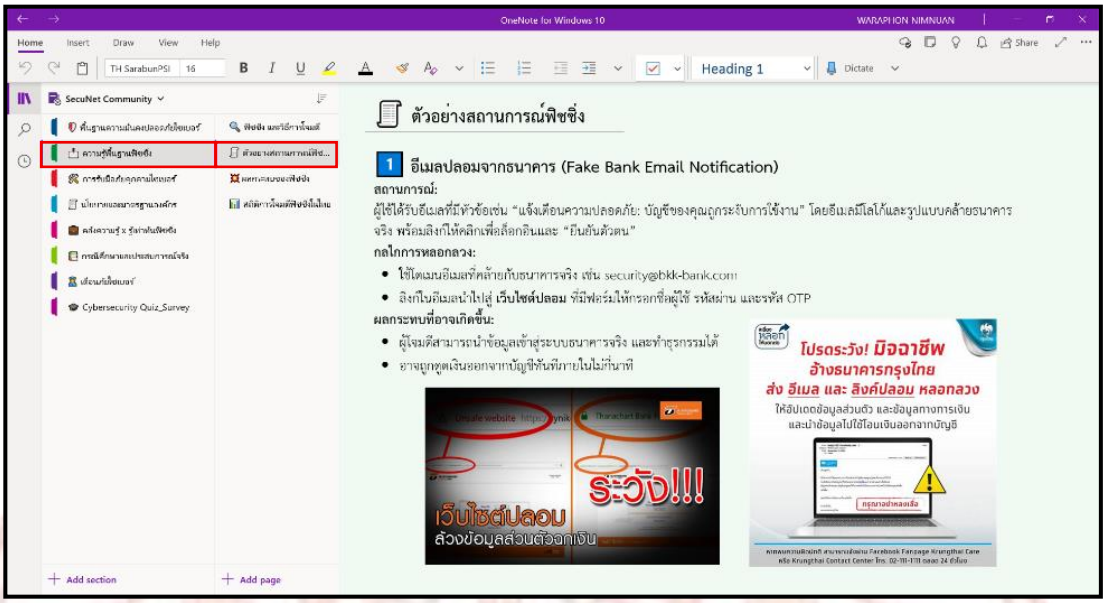
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อให้บุคลากรในองค์กร ตระหนักและเข้าใจถึงความเสี่ยงของการถูกหลอกลวงผ่านสื่ออิเล็กทรอนิกส์ โดยเฉพาะจากเทคนิคที่ใช้หลักการทางวิศวกรรมสังคม (Social Engineering) ซึ่งถือเป็นหนึ่งในภัยคุกคามที่พบบ่อยและมีแนวโน้มเพิ่มขึ้นในหลากหลายช่องทาง โดยเนื้อหาครอบคลุมหัวข้อหลักความหมายของฟิชชิ่ง (Definition of Phishing) ช่องทางที่ใช้ในการโจมตีฟิชชิ่ง (Attack Vectors) และวิธีการโจมตีแบบฟิชชิ่ง (Phishing Techniques)



ภาพที่ 3-5 หน้าภัยคุกคามไซเบอร์ทั่วไป

3.3.2.2 หน้าตัวอย่างสถานการณ์ฟิชชิ่ง

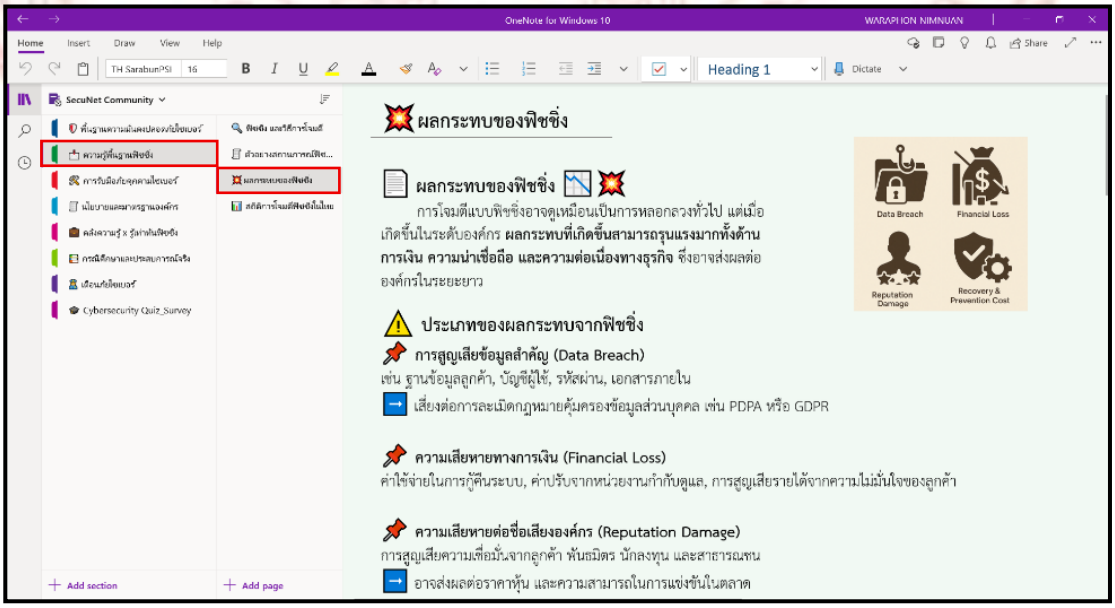
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อให้บุคลากรในองค์กรสามารถเข้าใจลักษณะการโจมตีแบบฟิชชิ่งในบริบทที่เกิดขึ้นจริง โดยแสดงให้เห็นถึงกลยุทธ์ วิธีการหลอกลวง และผลกระทบที่อาจเกิดขึ้น ผ่านกรณีจำลองที่ใกล้เคียงกับเหตุการณ์ที่พบบ่อยในชีวิตประจำวัน ซึ่งเนื้อหาครอบคลุมหัวข้อลักษณะสถานการณ์ฟิชชิ่งที่พบได้บ่อย กลไกการโจมตีและเทคนิคที่ใช้ ผลกระทบที่อาจเกิดขึ้น และจุดสังเกตและแนวทางหลีกเลี่ยง



ภาพที่ 3-6 หน้าตัวอย่างสถานการณ์ฟิชชิ่ง

3.3.2.3 หน้าผลกระทบของฟิชชิ่ง

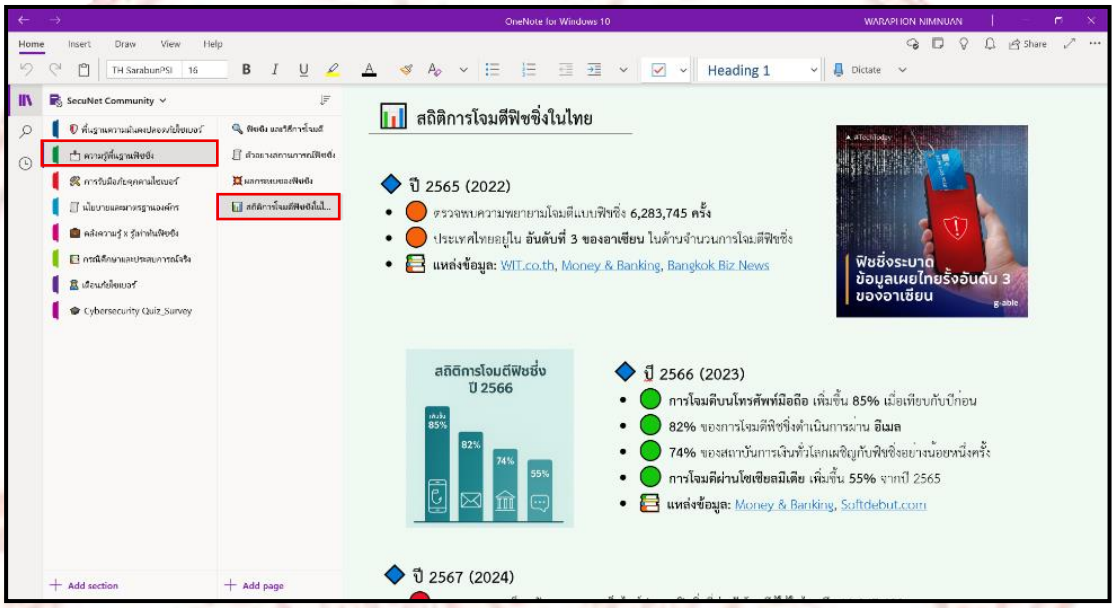
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อให้บุคลากรในองค์กรตระหนักถึงความรุนแรงของการโจมตีแบบฟิชชิ่ง โดยแสดงให้เห็นถึงผลกระทบทั้งในเชิงเทคนิค ธุรกิจ กฎหมาย และภาพลักษณ์ขององค์กร เพื่อเป็นข้อมูลประกอบการกำหนดมาตรการป้องกันและตอบสนองต่อเหตุการณ์อย่างรัดกุม ซึ่งเนื้อหาครอบคลุมหัวข้อภาพรวมของผลกระทบในระดับองค์กร ประเภทของผลกระทบจากฟิชชิ่ง ตัวอย่างผลกระทบเชิงลึก (Deep-Dive Impact Scenarios) และความสัมพันธ์กับกฎหมายและการกำกับดูแล



ภาพที่ 3-7 หน้าผลกระทบของฟิชชิ่ง

3.3.2.4 หน้าสถิติการโจมตีฟิชชิ่งในไทย

เนื้อหาในหน้านี้จัดทำขึ้นเพื่อนำเสนอข้อมูลเชิงปริมาณ เกี่ยวกับแนวโน้มและความถี่ของการโจมตีฟิชชิ่งที่เกิดขึ้นในประเทศไทยในช่วงปี 2565–2567 (2022–2024) โดยข้อมูลที่นำเสนอได้รับการรวบรวมจากแหล่งที่น่าเชื่อถือ เช่น Bangkok Biz News, Money & Banking และ Softdebut.com เพื่อเป็นฐานข้อมูลในการวิเคราะห์ความเสี่ยงและกำหนดมาตรการด้านความมั่นคงปลอดภัยภายในองค์กร ซึ่งเนื้อหาครอบคลุมหัวข้อแนวโน้มจำนวนการโจมตีแยกตามปี ประเภทของช่องทางที่ใช้ในการโจมตี (Channel-based Trends) และการเปลี่ยนแปลงและการเพิ่มขึ้นของความเสี่ยง

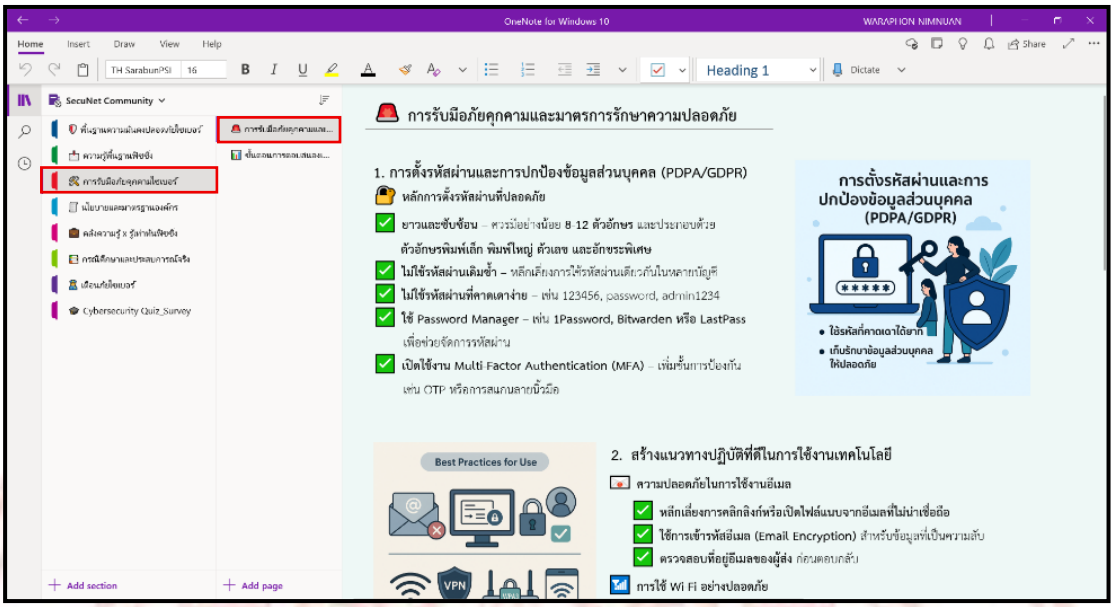


ภาพที่ 3-8 หน้าสถิติการโจมตีฟิชชิ่งในไทย

3.3.3 ส่วนการรับมือภัยคุกคามไซเบอร์ มีจำนวน 2 หน้า รายละเอียดดังต่อไปนี้

3.3.3.1 หน้าการรับมือภัยคุกคามและมาตรการรักษาความปลอดภัย

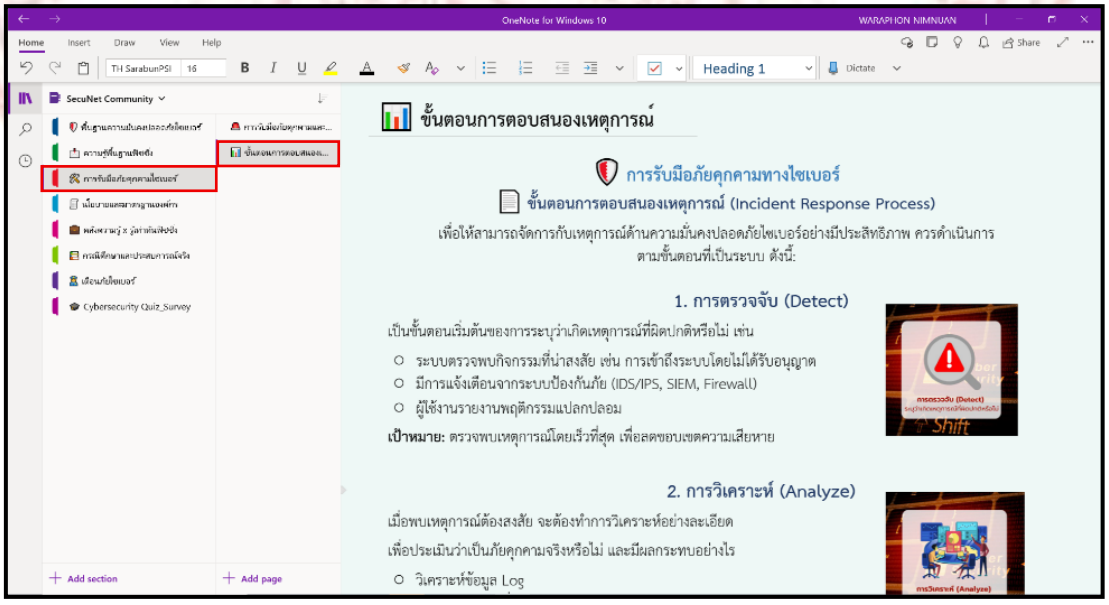
เนื้อหาในหน้านี้จัดทำขึ้นหน้าการรับมือภัยคุกคามและมาตรการรักษาความปลอดภัย เป็นส่วนสำคัญของแพลตฟอร์มที่ให้ความรู้เชิงปฏิบัติเพื่อเสริมสร้างทักษะในการป้องกันภัยคุกคามไซเบอร์ โดยเนื้อหาครอบคลุม แนวทางที่บุคลากรควรปฏิบัติในชีวิตประจำวัน มาตรการทางเทคนิค และการจัดการเหตุการณ์เมื่อพบความผิดปกติในบริบทของการใช้งานภายในองค์กร



ภาพที่ 3-9 หน้าการรับมือภัยคุกคามและมาตรการรักษาความปลอดภัย

3.3.3.2 หน้าขั้นตอนการตอบสนองเหตุการณ์

เนื้อหาในหน้านี้จัดทำขึ้นเพื่อให้บุคลากรในองค์กรเข้าใจกระบวนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ โดยเนื้อหาครอบคลุมตั้งแต่การตรวจจับเบื้องต้นไปจนถึงการกู้คืนระบบและการป้องกันเหตุซ้ำ เพื่อสนับสนุนการจัดการภัยคุกคามอย่างมีประสิทธิภาพ และลดความเสียหายในระดับองค์กร

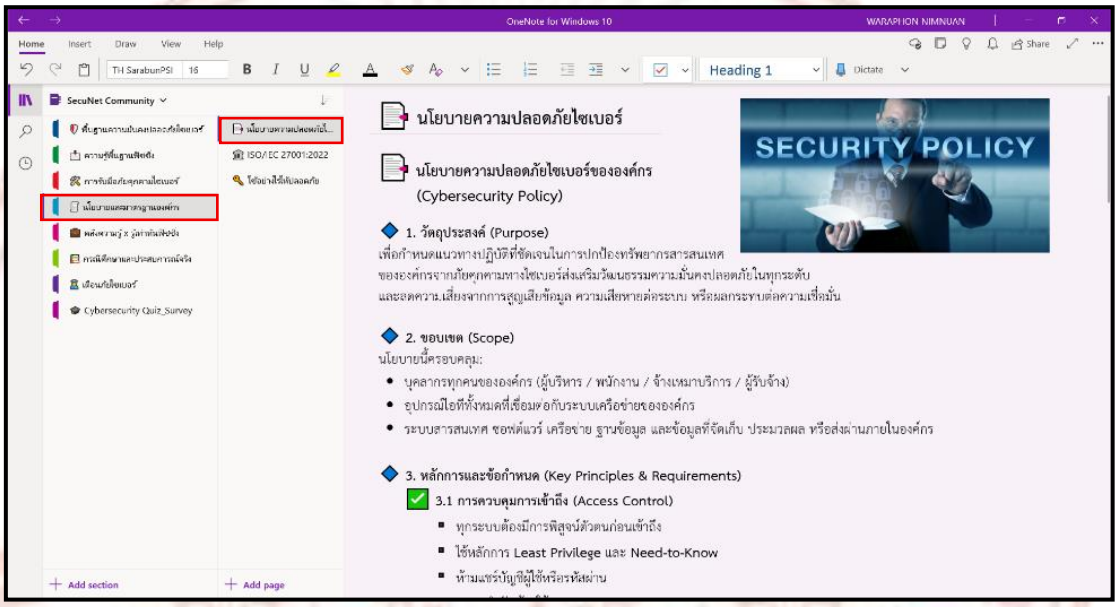


ภาพที่ 3-10 หน้าขั้นตอนการตอบสนองเหตุการณ์

3.3.4 ส่วนนโยบายและมาตรฐานองค์กร มีจำนวน 3 หน้า รายละเอียดดังต่อไปนี้

3.3.4.1 หน้านโยบายความปลอดภัยไซเบอร์

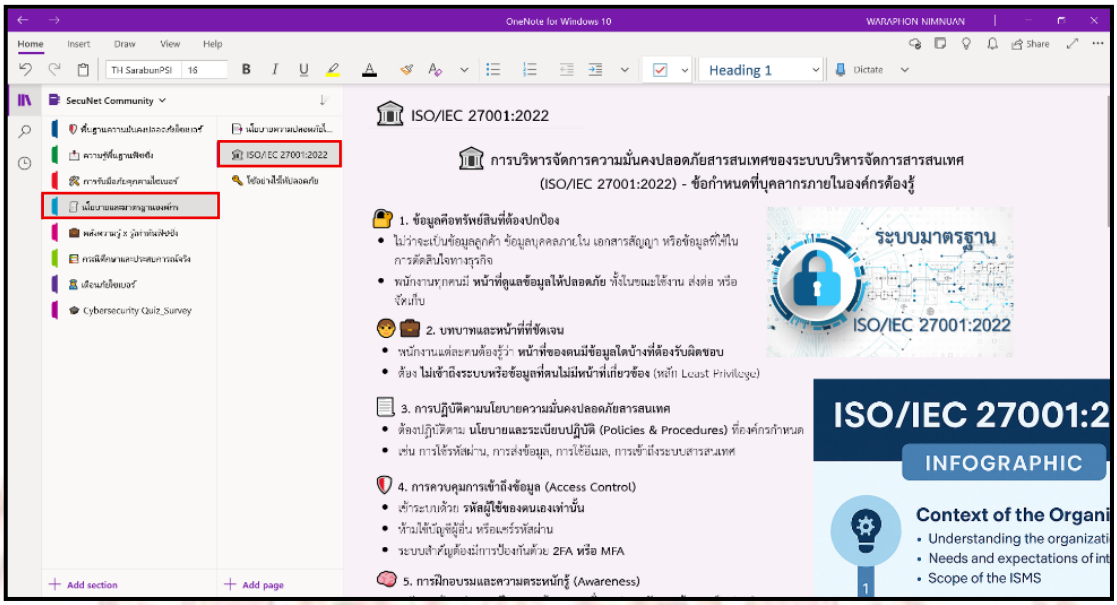
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อแนะนำนโยบายความปลอดภัยไซเบอร์ขององค์กรเป็นแนวทางสำคัญในการกำกับดูแลและควบคุมการใช้งานทรัพยากรสารสนเทศให้ปลอดภัยจากภัยคุกคามไซเบอร์ โดยเนื้อหาครอบคลุมทั้งวัตถุประสงค์ ขอบเขตการบังคับใช้ และ หลักการข้อกำหนดที่สำคัญ ซึ่งสะท้อนถึงแนวทางปฏิบัติที่สอดคล้องกับมาตรฐานความปลอดภัยสากล เช่น ISO/IEC : 27001



ภาพที่ 3-11 หน้านโยบายความปลอดภัยไซเบอร์

3.3.4.2 หน้าการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของระบบบริหารจัดการสารสนเทศ (ISO/IEC 27001:2022)

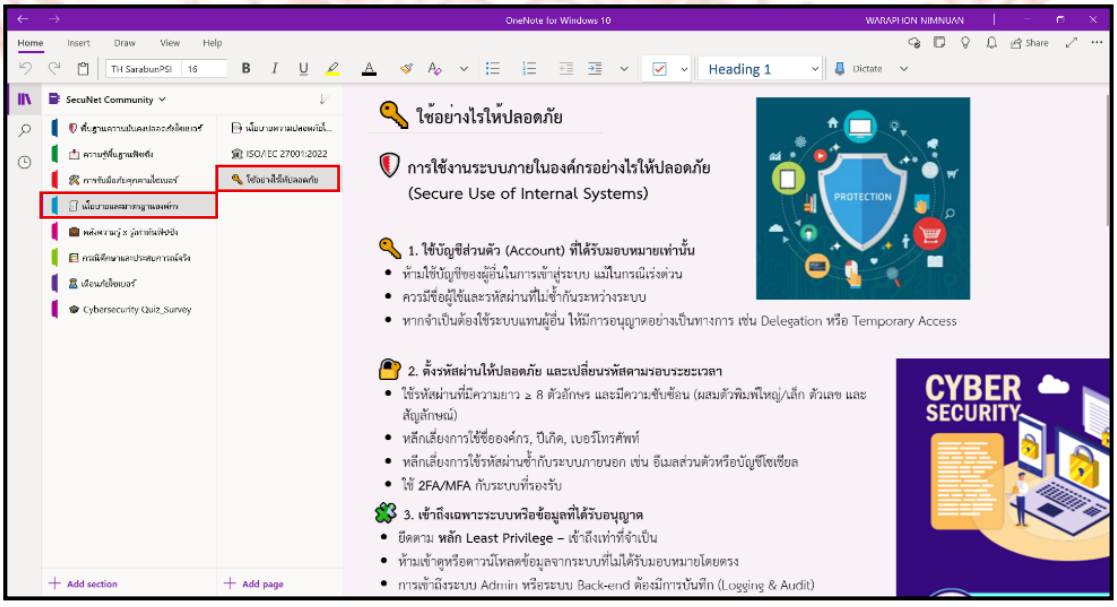
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อให้บุคลากรในองค์กรทุกระดับ “ควรทราบและปฏิบัติตาม” เพื่อให้สอดคล้องกับข้อกำหนดของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ตามมาตรฐาน ISO/IEC 27001 : 2022 โดยเน้นย้ำถึงบทบาท ความรับผิดชอบ และแนวปฏิบัติด้านความมั่นคงปลอดภัยที่จำเป็นต่อการควบคุมความเสี่ยงด้านไซเบอร์ภายในองค์กร



ภาพที่ 3-12 หน้าการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของระบบบริหารจัดการสารสนเทศ (ISO/IEC 27001:2022)

3.3.4.3 หน้าใช้อย่างไรให้ปลอดภัย

เนื้อหาในหน้านี้จัดทำขึ้นเพื่อแนะแนวทางปฏิบัติที่ปลอดภัยในการใช้งานระบบสารสนเทศภายในองค์กร โดยเน้นให้บุคลากรทุกระดับเข้าใจและปฏิบัติตามหลักการด้านความมั่นคงปลอดภัยไซเบอร์ในชีวิตการทำงานประจำวัน โดยครอบคลุมทั้งด้านการใช้งานบัญชี ระบบ อุปกรณ์ ข้อมูล และพฤติกรรมผู้ใช้งาน

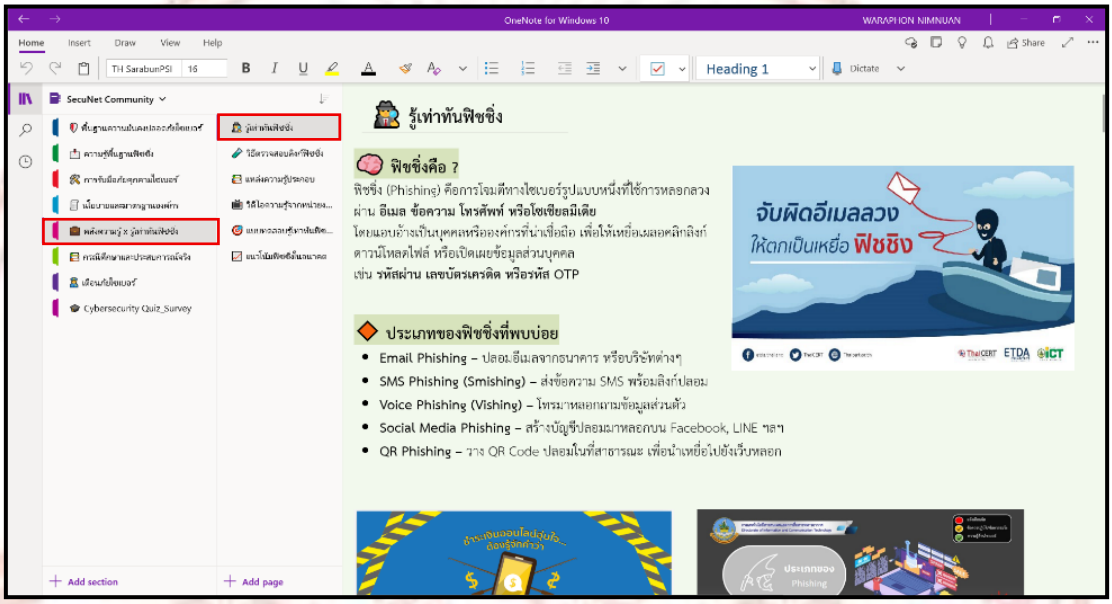


ภาพที่ 3-13 หน้าใช้อย่างไรให้ปลอดภัย

3.3.5 ส่วนคลังความรู้ x รู้เท่าทันฟิชชิ่ง มีจำนวน 6 หน้า รายละเอียดดังต่อไปนี้

3.3.5.1 หน้ารู้เท่าทันฟิชชิ่ง

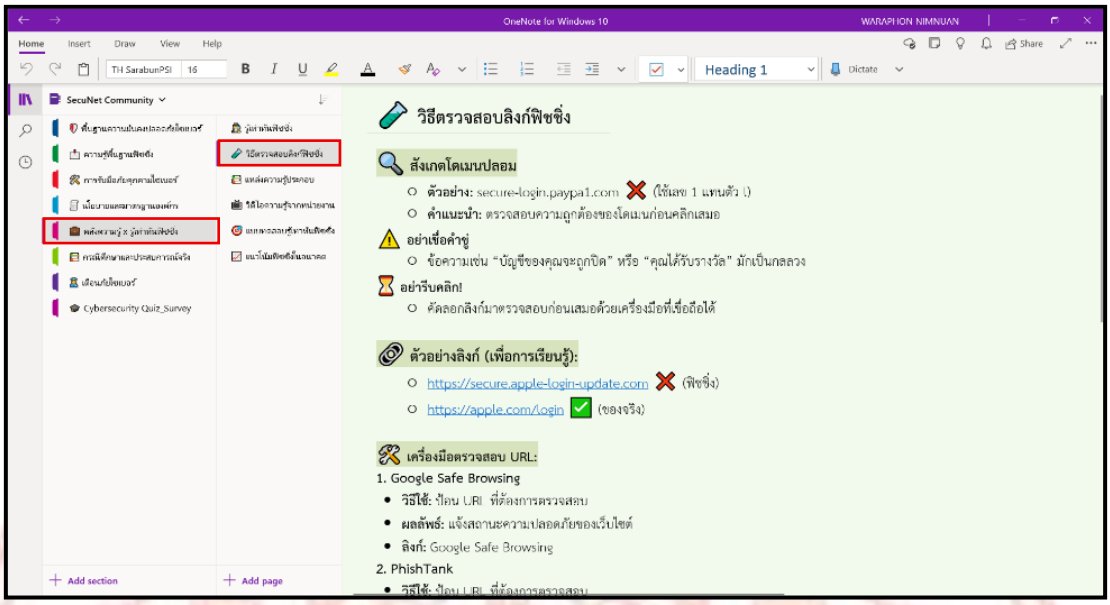
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อเสริมสร้างความเข้าใจพื้นฐานเกี่ยวกับฟิชชิ่ง ซึ่งเป็นหนึ่งในภัยคุกคามทางไซเบอร์ที่พบบ่อยและอาศัยจุดอ่อนด้านพฤติกรรมของผู้ใช้งาน โดยเนื้อหามุ่งเน้นให้บุคลากรสามารถ รู้เท่าทันวิธีการหลอกลวง ระบุประเภทของฟิชชิ่ง และลดความเสี่ยงจากการตกเป็นเหยื่อ



ภาพที่ 3-14 หน้ารู้เท่าทันฟิชชิ่ง

3.3.5.2 หน้าวิธีตรวจสอบลิงก์ฟิชชิ่ง

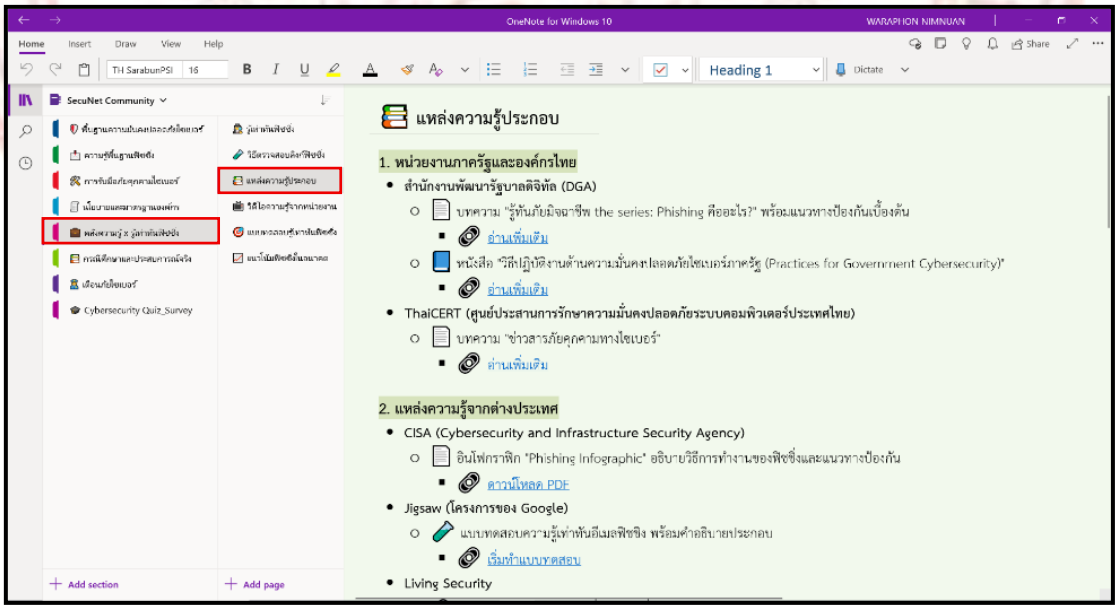
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อให้บุคลากรในองค์กรสามารถเรียนรู้วิธีสังเกตลิงก์ที่เป็นอันตรายและหลีกเลี่ยงการตกเป็นเหยื่อของการโจมตีแบบฟิชชิ่ง โดยเนื้อหาครอบคลุมทั้งตัวอย่างที่ใช้ฝึกวิเคราะห์ หลักการสังเกตโดเมนปลอม และเครื่องมือที่สามารถใช้ตรวจสอบความปลอดภัยของลิงก์



ภาพที่ 3-15 หน้าวิธีตรวจสอบลิงก์ฟิชชิ่ง

3.3.5.3 หน้าแหล่งความรู้ประกอบ

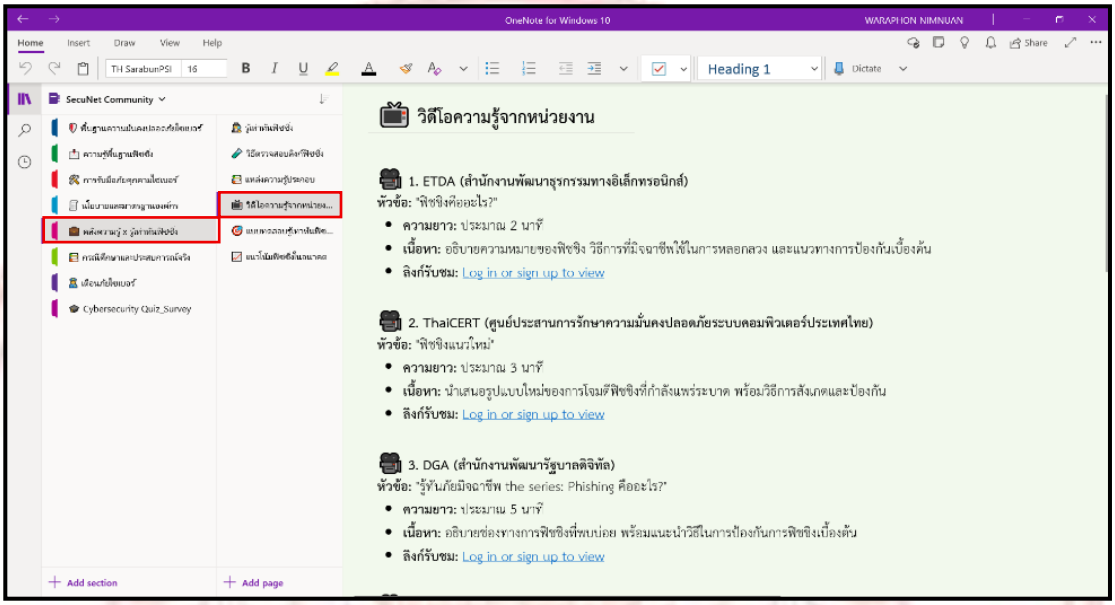
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อรวบรวม บทความ คู่มือ เครื่องมือ และแหล่งฝึกอบรมจากทั้งในประเทศและต่างประเทศ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะประเด็นฟิชชิ่ง (Phishing) และการรับมือกับภัยคุกคามทางไซเบอร์ เพื่อให้บุคลากรสามารถศึกษาเพิ่มเติม ฝึกทักษะ และติดตามสถานการณ์ล่าสุดได้ด้วยตนเอง



ภาพที่ 3-16 หน้าแหล่งความรู้ประกอบ

3.3.5.4 หน้าวิดีโอความรู้จากหน่วยงาน

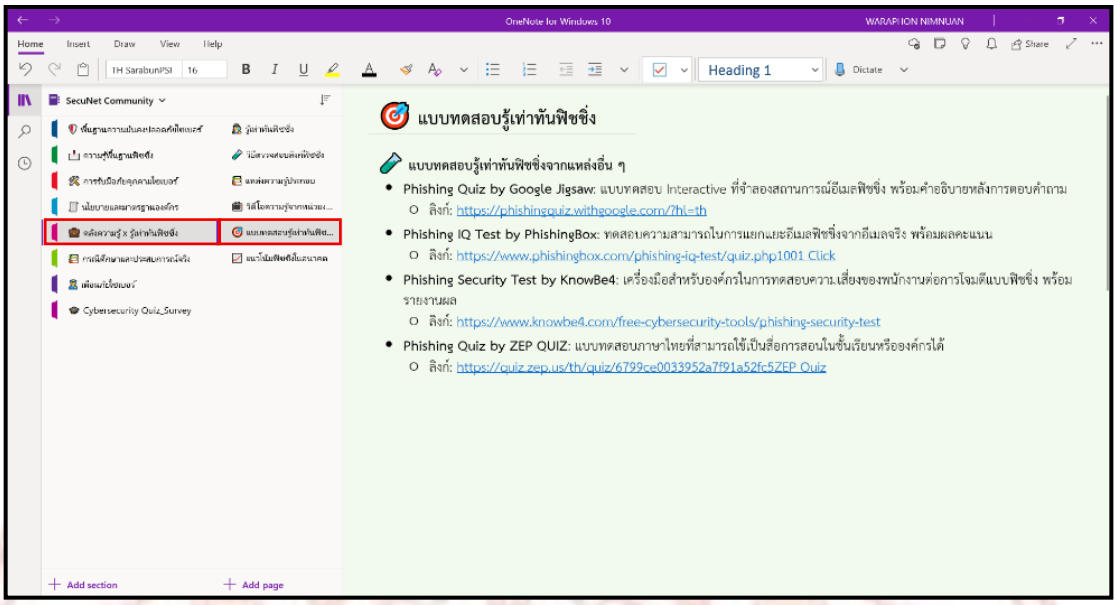
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อเป็นแหล่งรวบรวมสื่อมัลติมีเดียจากองค์กรภาครัฐและภาคเอกชนที่น่าเชื่อถือ ซึ่งจัดทำขึ้นเพื่อ เสริมสร้างความเข้าใจเกี่ยวกับฟิชชิ่งและการป้องกันภัยคุกคามทางไซเบอร์ในรูปแบบที่เข้าถึงง่าย โดยเนื้อหาครอบคลุมทั้งนิยามของฟิชชิ่ง รูปแบบการหลอกลวงที่พบในปัจจุบัน วิธีสังเกต และแนวทางป้องกันเบื้องต้น



ภาพที่ 3-17 หน้าวิดีโอความรู้จากหน่วยงาน

3.3.5.5 หน้าแบบทดสอบรู้เท่าทันฟิชชิ่ง

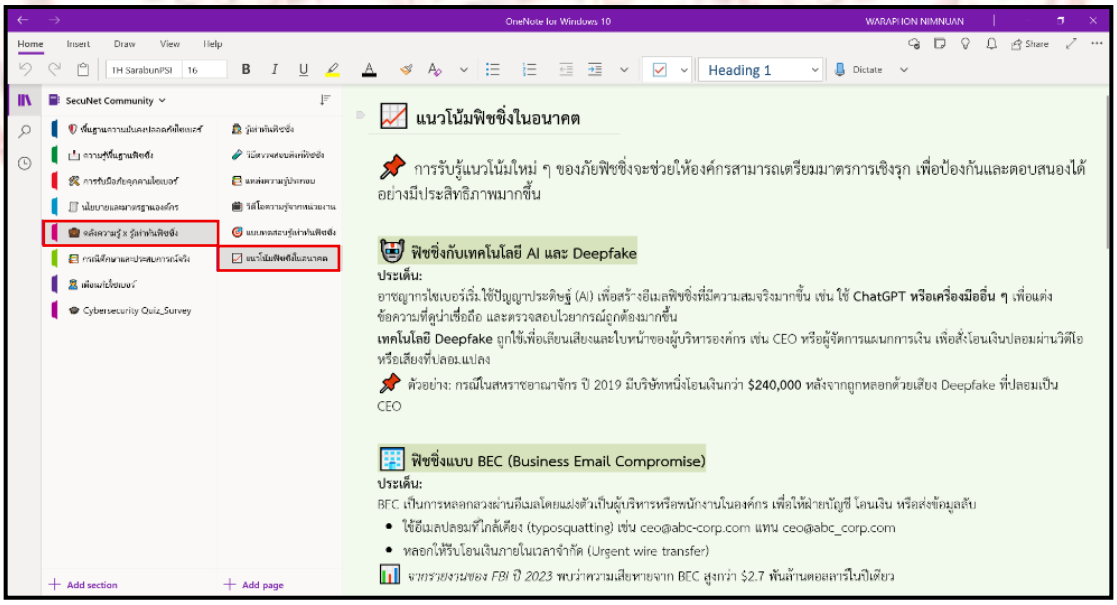
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อเป็นแหล่งรวบรวมแบบทดสอบออนไลน์จากผู้ให้บริการที่เชื่อถือได้ เพื่อช่วยให้บุคลากรในองค์กรสามารถประเมินความรู้ ความเข้าใจ และทักษะในการตรวจจับฟิชชิ่ง ได้ด้วยตนเองผ่านสื่อแบบโต้ตอบ (Interactive) และสถานการณ์จำลอง โดยมุ่งเน้นการเรียนรู้ผ่านประสบการณ์ตรงและคำอธิบายที่เข้าใจง่าย



ภาพที่ 3-18 หน้าแบบทดสอบรู้เท่าทันฟิชชิ่ง

3.3.5.6 หน้าแนวโน้มฟิชชิ่งในอนาคต

เนื้อหาในหน้านี้จัดทำขึ้นเพื่อให้บุคลากรในองค์กรตระหนักถึงแนวโน้มของการโจมตีแบบฟิชชิ่งที่กำลังพัฒนาอย่างรวดเร็ว พร้อมทั้งวิเคราะห์ข้อมูลจากรายงานภัยคุกคาม (Threat Intelligence) ระดับสากล เพื่อให้สามารถเตรียมมาตรการเชิงรุกในการป้องกันและตอบสนองได้อย่างมีประสิทธิภาพ

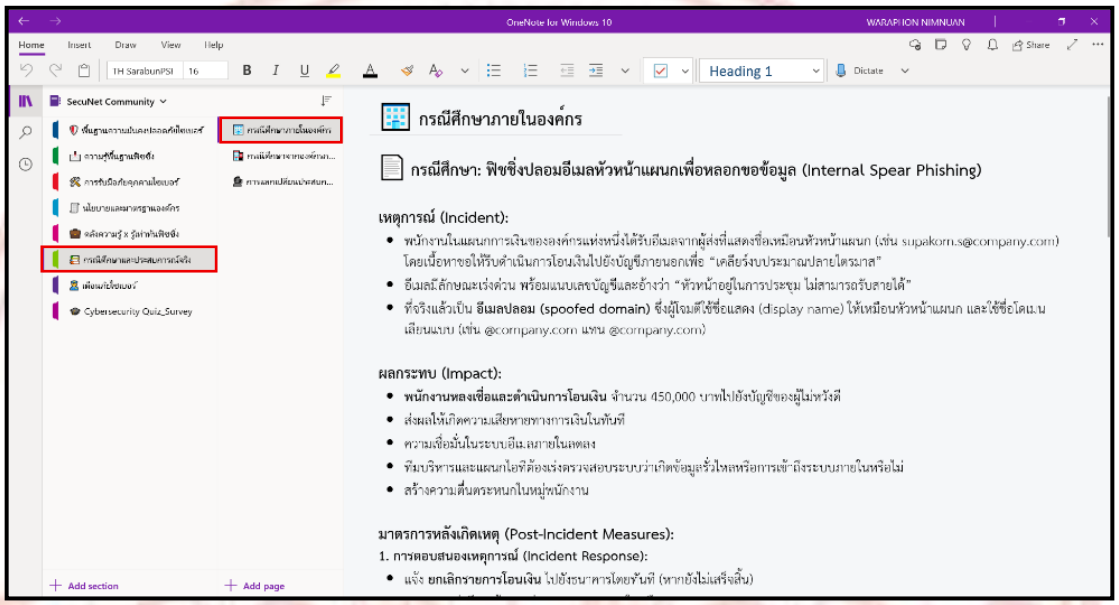


ภาพที่ 3-19 หน้าแนวโน้มฟิชชิ่งในอนาคต

3.3.6 ส่วนกรณีศึกษาและประสบการณ์จริง มีจำนวน 3 หน้า รายละเอียดดังต่อไปนี้

3.3.6.1 หน้ากรณีศึกษาภายในองค์กร

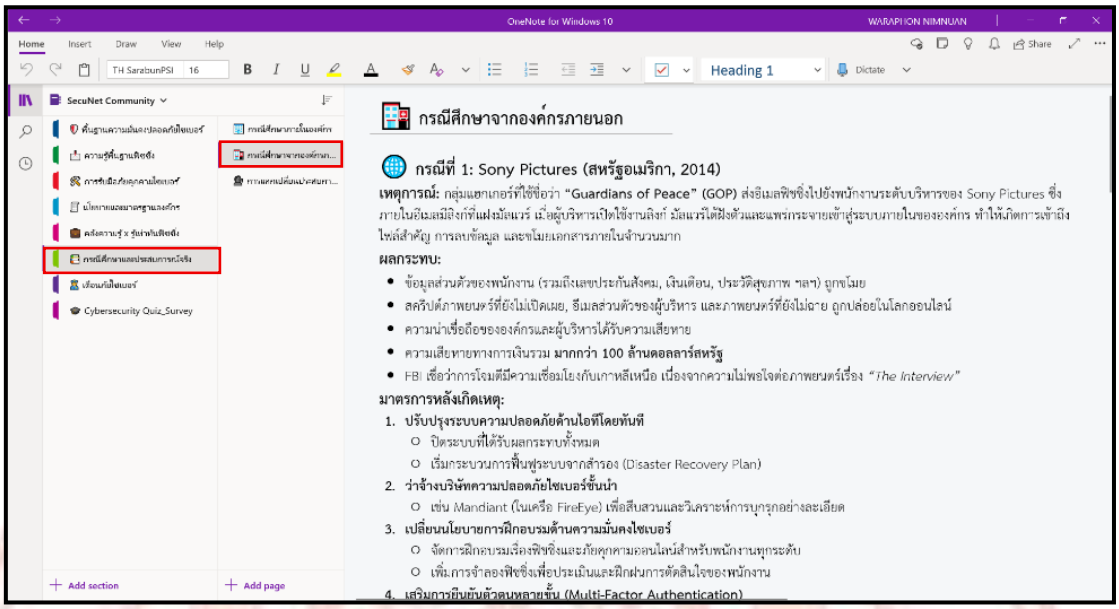
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อถ่ายทอดเหตุการณ์จริงที่เกิดขึ้นภายในองค์กรที่ตกเป็นเหยื่อการโจมตีแบบฟิชชิ่ง เพื่อให้บุคลากรสามารถเรียนรู้จากประสบการณ์โดยตรง เข้าใจวงจรของเหตุการณ์ การตอบสนอง และแนวทางป้องกันไม่ให้เกิดซ้ำ พร้อมชี้ให้เห็นถึงบทบาทสำคัญของ “มนุษย์” ในการเป็นด่านแรกของความมั่นคงปลอดภัย



ภาพที่ 3-20 หน้ากรณีศึกษาภายในองค์กร

3.3.6.2 หน้ากรณีศึกษาจากองค์กรภายนอก

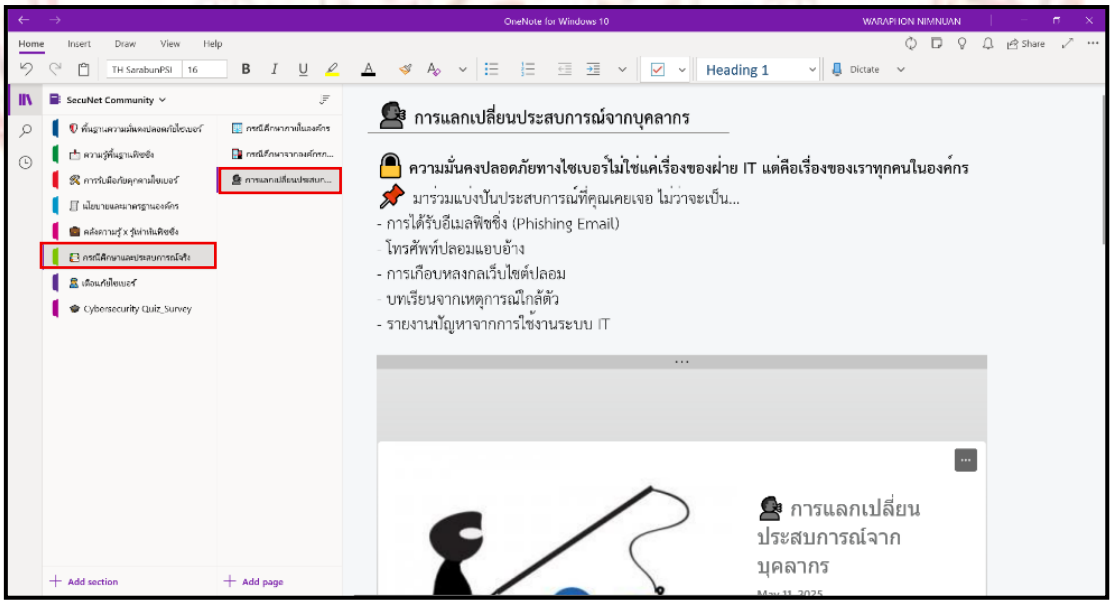
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อเป็นกรณีศึกษาจากองค์กรทั้งในและต่างประเทศที่ประสบกับการโจมตีทางไซเบอร์ โดยเฉพาะฟิชชิ่งและแรนซัมแวร์ เพื่อให้บุคลากรในองค์กรสามารถเรียนรู้จากเหตุการณ์ที่เกิดขึ้นจริง ผลกระทบที่ตามมา และมาตรการรับมือหลังเหตุการณ์ พร้อมวิเคราะห์บทเรียนที่สามารถนำไปประยุกต์ใช้ภายในองค์กรได้



ภาพที่ 3-21 หน้ากรณีศึกษาจากองค์กรภายนอก

3.3.6.3 หน้าการแลกเปลี่ยนประสบการณ์จากบุคลากร

เนื้อหาในหน้านี้จัดทำขึ้นเพื่อมุ่งเน้นการเปิดพื้นที่ให้บุคลากรภายในองค์กรได้ แลกเปลี่ยนประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตนเคยเผชิญ ไม่ว่าจะเป็นเหตุการณ์จริงหรือเหตุการณ์เฉียดใกล้ โดยมีวัตถุประสงค์เพื่อ เสริมสร้างความตระหนักรู้ เรียนรู้ร่วมกัน และสร้างวัฒนธรรมการระวังภัยไซเบอร์แบบมีส่วนร่วม

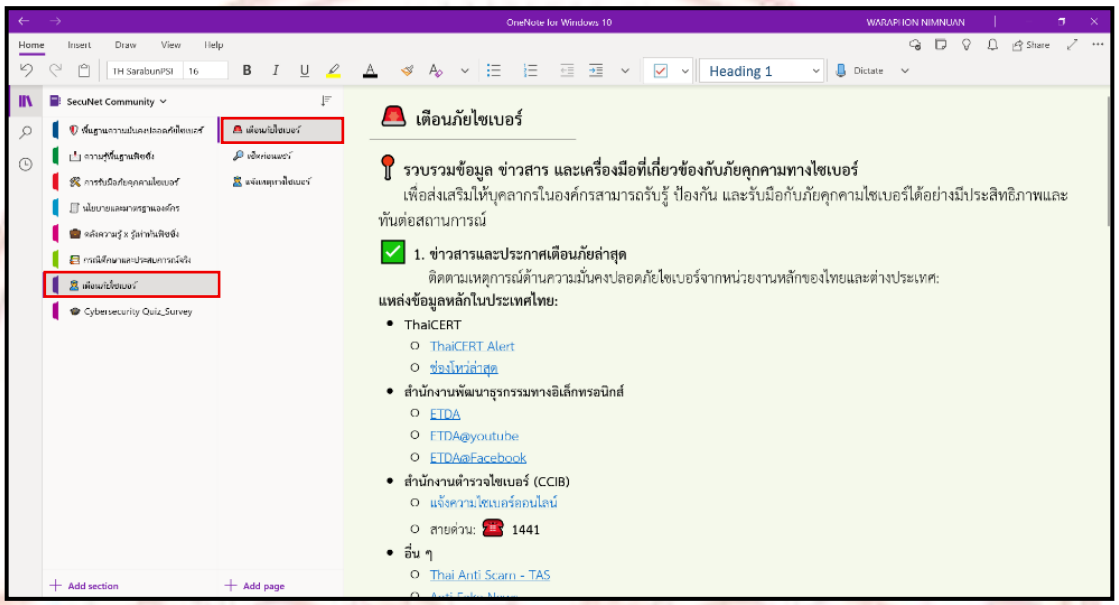


ภาพที่ 3-22 หน้าการแลกเปลี่ยนประสบการณ์จากบุคลากร

3.3.7 ส่วนเตือนภัยไซเบอร์ มีจำนวน 3 หน้า รายละเอียดดังต่อไปนี้

3.3.7.1 หน้าเตือนภัยไซเบอร์

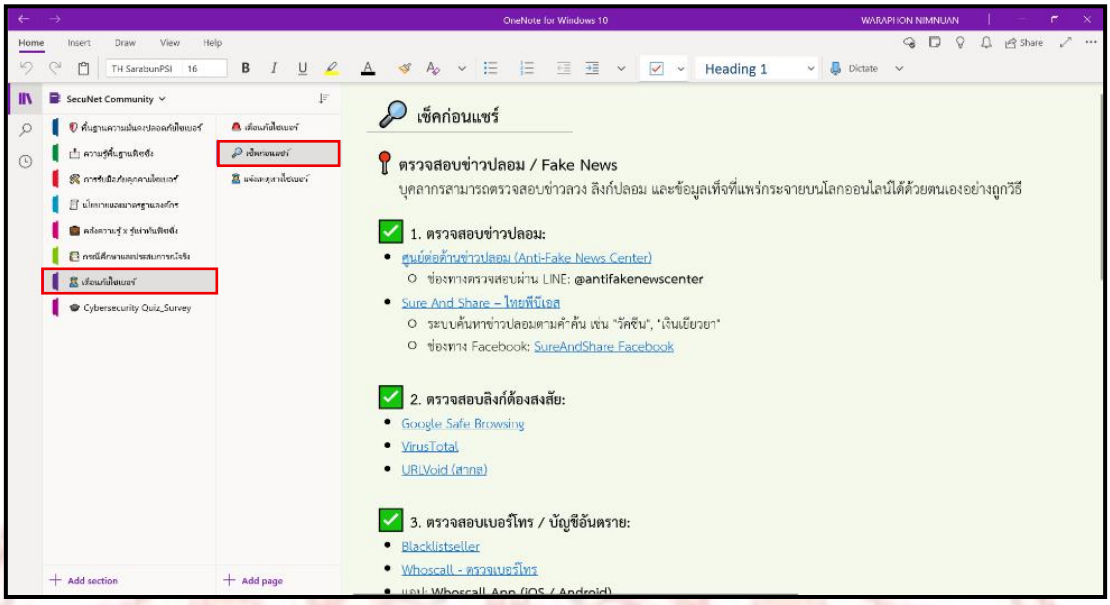
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อรวบรวมข่าวสารและเครื่องมือที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์จากแหล่งที่เชื่อถือได้ ทั้งในประเทศและต่างประเทศ โดยมีจุดมุ่งหมายเพื่อให้บุคลากรในองค์กร สามารถรับรู้สถานการณ์ด้านความมั่นคงไซเบอร์ได้อย่างทันท่วงที พร้อมทั้งเข้าใจแนวทางการป้องกันอย่างถูกต้องและนำไปใช้ได้จริง



ภาพที่ 3-23 หน้าเตือนภัยไซเบอร์

3.3.7.2 หน้าเช็คก่อนแชร์

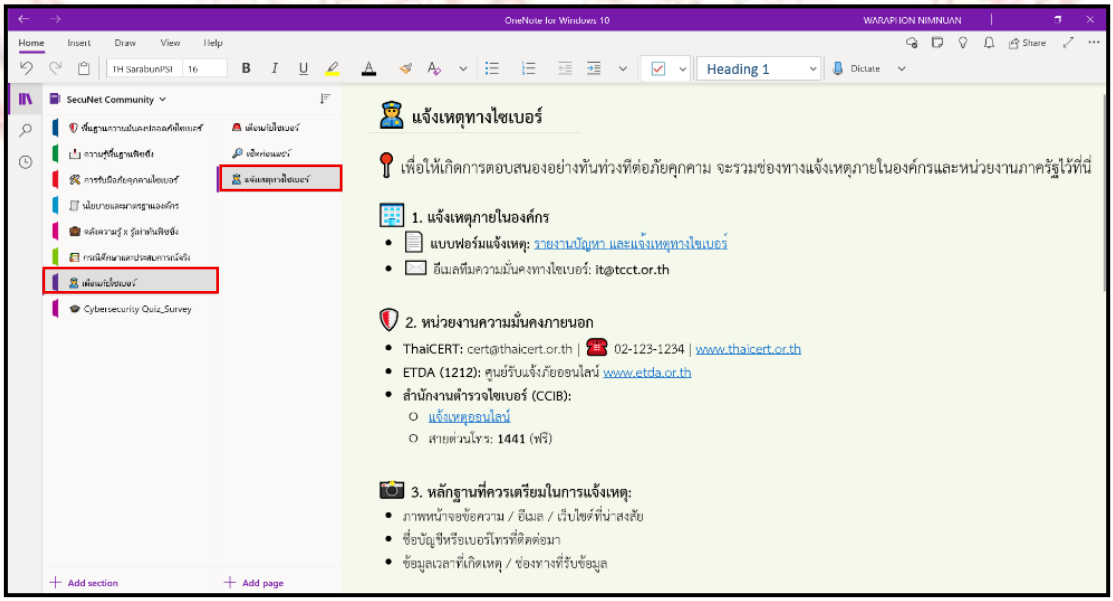
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อให้บุคลากรในองค์กรมีทักษะในการตรวจสอบข่าวปลอม ลิงก์อันตราย และข้อมูลที่อาจทำให้เกิดความเข้าใจผิดก่อนส่งต่อ โดยเน้นการใช้งานเครื่องมือที่น่าเชื่อถือและเข้าถึงง่าย พร้อมแนะนำวิธีการปฏิบัติอย่างเป็นระบบ



ภาพที่ 3-24 หน้าเช็คก่อนแชร์

3.3.7.3 หน้าแจ้งเหตุทางไซเบอร์

เนื้อหาในหน้านี้จัดทำขึ้นเพื่ออำนวยความสะดวกในการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งภายในและภายนอกองค์กร โดยรวบรวมช่องทางติดต่อ เครื่องมือ และแนวทางการจัดเตรียมหลักฐาน เพื่อให้การตอบสนองเป็นไปอย่างรวดเร็ว มีประสิทธิภาพ และสามารถติดตามต่อได้

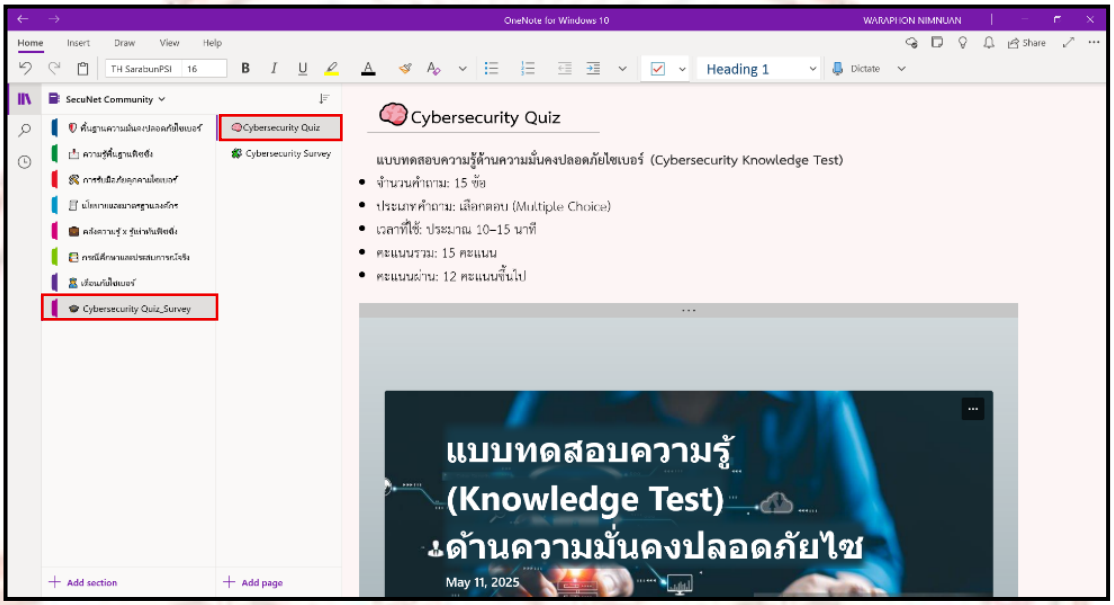


ภาพที่ 3-25 หน้าแจ้งเหตุทางไซเบอร์

3.3.8 ส่วน Cybersecurity Quiz_Survey มีจำนวน 2 หน้า รายละเอียดดังต่อไปนี้

3.3.8.1 หน้า Cybersecurity Quiz

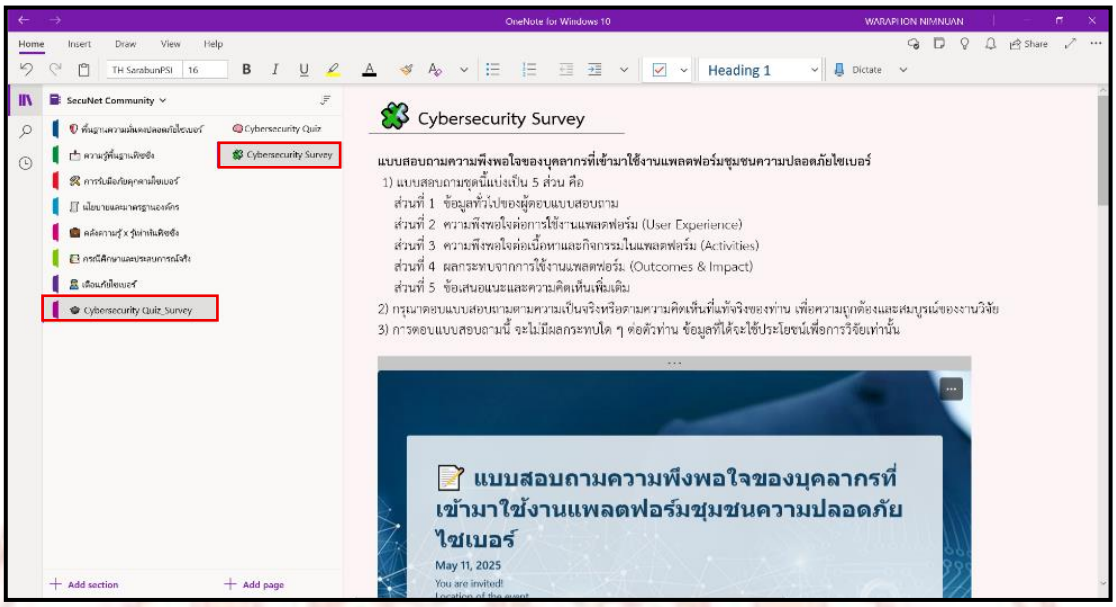
เนื้อหาในหน้านี้จัดทำขึ้นเพื่อประเมินความเข้าใจพื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ของบุคลากรในองค์กร โดยอ้างอิงจากการเรียนรู้ผ่านแพลตฟอร์มชุมชน ซึ่งนำเสนอเนื้อหาในรูปแบบที่ส่งเสริมการมีส่วนร่วม ความเข้าใจเชิงบริบท และการเรียนรู้จากสถานการณ์จริง โดยผลการประเมินสามารถนำไปใช้วิเคราะห์ระดับความเข้าใจของบุคลากรแต่ละกลุ่ม และใช้เป็นข้อมูลประกอบการวางแผนพัฒนาหลักสูตรหรือกิจกรรมฝึกอบรมในอนาคตได้อย่างเหมาะสม



ภาพที่ 3-26 หน้า Cybersecurity Quiz

3.3.8.2 หน้า Cybersecurity Survey

แบบสอบถามชุดนี้มีวัตถุประสงค์เพื่อประเมินความคิดเห็นและความพึงพอใจของบุคลากรในองค์กรที่ได้เข้าร่วมเรียนรู้ผ่านแพลตฟอร์มชุมชนความมั่นคงปลอดภัยไซเบอร์ โดยมุ่งเน้นการเรียนรู้ที่มีส่วนร่วม สอดคล้องกับบริบทการทำงานจริง และสร้างความตระหนักรู้ต่อภัยคุกคามในโลกดิจิทัล โดยข้อมูลจากแบบสอบถามนี้จะถูกนำไปใช้ในการปรับปรุงเนื้อหา รูปแบบการนำเสนอ และกิจกรรมในแพลตฟอร์ม ให้มีความเหมาะสม ทันสมัย และตอบโจทย์การเปลี่ยนแปลงของภัยคุกคามไซเบอร์ในอนาคตได้อย่างมีประสิทธิภาพ



ภาพที่ 3-27 หน้า Cybersecurity Survey

3.4 การพัฒนาแบบทดสอบความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Knowledge Test)

แบบทดสอบความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ใช้ในงานวิจัยนี้ จัดทำขึ้นภายใต้กรอบของการวิจัยเรื่อง “การพัฒนาแพลตฟอร์มชุมชนเพื่อเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ในองค์กร” โดยมีวัตถุประสงค์หลักเพื่อวัดระดับความรู้ ความเข้าใจ และการเรียนรู้ของบุคลากรที่ได้มีส่วนร่วมในการใช้งานแพลตฟอร์ม ซึ่งครอบคลุมการเรียนรู้ผ่านสื่อ เนื้อหา กิจกรรม และปฏิสัมพันธ์ภายในแพลตฟอร์ม Microsoft OneNote ที่ใช้เป็นศูนย์กลางของการแลกเปลี่ยนองค์ความรู้และการเสริมสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กร ซึ่งการดำเนินงานวิจัยในส่วนนี้ประกอบด้วยขั้นตอนสำคัญ ดังนี้

3.4.1 การออกแบบแบบทดสอบความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Knowledge Test)

การออกแบบและพัฒนาแบบทดสอบโดยยึดหลักการวิจัยเชิงเนื้อหา (Content-based Design) ซึ่งอ้างอิงจากการทบทวนแนวคิด ทฤษฎี และกรอบเนื้อหาที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ โดยเฉพาะประเด็นที่ถูกนำเสนอภายในแพลตฟอร์มชุมชน เช่น แนวคิดพื้นฐานด้านไซเบอร์ซีเคียวริตี้ (Cybersecurity Essentials), การโจมตีแบบฟิชชิ่งและการหลอกลวงทางสื่อดิจิทัล (Phishing & Social Engineering), การจัดการภัยคุกคามและเหตุการณ์ (Threat Management & Incident Response), การใช้เทคโนโลยีสารสนเทศอย่างปลอดภัยในองค์กร (Safe Use of Technology at Work) และกฎหมายหรือมาตรฐานที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และมาตรฐาน ISO/IEC 27001:2022

แบบทดสอบถูกออกแบบเป็นข้อสอบแบบปรนัย (Multiple Choice Questions : MCQ) จำนวน 15 ข้อ แบ่งเป็น 3 ระดับความยาก ได้แก่ ระดับง่าย (Basic), ระดับปานกลาง (Intermediate) และระดับยาก (Advanced) อย่างละ 5 ข้อ เพื่อให้สามารถประเมินความรู้ของผู้ตอบในด้านระดับ

การรับรู้ ความเข้าใจ และการคิดวิเคราะห์ในบริบทองค์กร โดยในแต่ละข้อจะมีคำอธิบายประกอบคำตอบ (Answer Explanation) เพื่อส่งเสริมการเรียนรู้แบบย้อนกลับ (Reflective Learning) หลังจากการทำแบบทดสอบ

ผู้วิจัยได้นำแบบร่างเข้าสู่กระบวนการตรวจสอบความตรงตามเนื้อหา (Content Validity) โดยขอคำแนะนำจากอาจารย์ที่ปรึกษา เพื่อพิจารณาความชัดเจนของถ้อยคำ ความเหมาะสมของระดับภาษา ความครอบคลุมของเนื้อหาในแต่ละหัวข้อ ระดับความยากที่เหมาะสม และความถูกต้องของตัวเลือกและคำอธิบายเฉลย จากนั้นผู้วิจัยได้นำข้อเสนอแนะที่ได้รับไปปรับปรุงให้สมบูรณ์ก่อนนำไปใช้งานจริง

3.4.2 โครงสร้างแบบทดสอบความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Knowledge Test)

แบบทดสอบฉบับสมบูรณ์ประกอบด้วย 2 ส่วนหลัก ได้แก่

3.4.2.1 ส่วนที่ 1 : ข้อมูลทั่วไปของผู้ทดสอบ

ในส่วนนี้จะใช้เก็บข้อมูลทั่วไปของผู้ทดสอบ ได้แก่ ชื่อ–นามสกุล และฝ่ายงานที่สังกัด เพื่อใช้ในการจำแนกกลุ่มข้อมูลตามบริบทหน่วยงานในการวิเคราะห์ผล โดยข้อมูลที่เก็บรวบรวมจะใช้เพื่อวัตถุประสงค์ทางวิชาการเท่านั้นภายใต้หลักจริยธรรมการวิจัยในมนุษย์อย่างเคร่งครัด

3.4.2.2 ส่วนที่ 2 : แบบทดสอบความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Knowledge Test)

ในส่วนนี้ใช้เพื่อชี้แจงวัตถุประสงค์ของแบบทดสอบ แนวทางการทำแบบทดสอบ ระยะเวลาในการทำ และเกณฑ์การให้คะแนน เพื่อสร้างความเข้าใจที่ตรงกันก่อนการเริ่มต้นประเมินผล รวมทั้งประกอบด้วยข้อคำถามจำนวน 15 ข้อ แบ่งออกเป็น 3 กลุ่มตามระดับความยาก ดังนี้

3.4.2.2.1 ระดับพื้นฐาน (Basic : ข้อ 1–5) ประเมินความรู้ทั่วไป เช่น คำศัพท์พื้นฐาน ความหมายของมัลแวร์ การใช้รหัสผ่านอย่างปลอดภัย และการสังเกตความผิดปกติในเว็บไซต์หรืออีเมล

3.4.2.2.2 ระดับปานกลาง (Intermediate : ข้อ 6–10) ประเมินความเข้าใจในสถานการณ์จำลอง การเลือกแนวทางที่เหมาะสม เช่น การแยกแยะฟิชชิ่งอีเมล หรือการป้องกันข้อมูลส่วนบุคคล

3.4.2.2.3 ระดับยาก (Advanced : ข้อ 11–15) ประเมินการคิดวิเคราะห์และการประยุกต์ใช้ เช่น การตอบสนองต่อเหตุการณ์ผิดปกติ การอ้างอิงมาตรฐาน ISO/IEC : 27001/2022 หรือ PDPA

ทุกข้อคำถามมีตัวเลือก 4 ตัวเลือก และมีเพียงคำตอบเดียวที่ถูกต้อง โดยหลังจากส่งคำตอบผู้ตอบจะได้รับคำอธิบายเฉลยเพื่อเสริมความเข้าใจ ซึ่งช่วยส่งเสริมการเรียนรู้ภายหลังการประเมิน

3.4.3 การจัดเก็บข้อมูลและจริยธรรมในการวิจัย

แบบทดสอบถูกจัดทำในรูปแบบออนไลน์ผ่านแพลตฟอร์ม Microsoft Forms และเผยแพร่ผ่านลิงก์ https://forms.office.com/r/JE7dkmSDkc ให้กับกลุ่มตัวอย่างที่เคยใช้งานแพลตฟอร์มชุมชน โดยมีการแจ้งให้ผู้เข้าร่วมทราบล่วงหน้าเกี่ยวกับวัตถุประสงค์ของแบบทดสอบ สิทธิใน

การปฏิเสธเข้าร่วม ความเป็นส่วนตัวของคำตอบ และการใช้ข้อมูลเพื่อวัตถุประสงค์ทางวิชาการเท่านั้น

ผลลัพธ์จากแบบทดสอบจะถูกรวบรวมโดยไม่ระบุตัวตน และนำไปวิเคราะห์ร่วมกับข้อมูลจากแบบสอบถามความพึงพอใจ เพื่อศึกษาความสัมพันธ์ระหว่างระดับความรู้ ความพึงพอใจในการใช้งานแพลตฟอร์ม และพฤติกรรมการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากร ทั้งนี้ การดำเนินการทั้งหมดอยู่ภายใต้หลักจริยธรรมการวิจัยในมนุษย์อย่างเคร่งครัด

3.5 การพัฒนาแบบสอบถามความพึงพอใจของบุคลากรที่เข้ามาใช้งานแพลตฟอร์มชุมชนความปลอดภัยไซเบอร์

เครื่องมือที่ใช้ในการวิจัยครั้งนี้ คือ แบบสอบถามความพึงพอใจของบุคลากรที่เข้ามาใช้งานแพลตฟอร์มชุมชนความปลอดภัยไซเบอร์ ซึ่งจัดทำขึ้นภายใต้กรอบของการวิจัยเรื่อง “การพัฒนาแพลตฟอร์มชุมชนเพื่อเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ในองค์กร” โดยมีวัตถุประสงค์เพื่อประเมินระดับความพึงพอใจของผู้ใช้งาน และศึกษาผลกระทบจากการใช้งานแพลตฟอร์มต่อพฤติกรรม ทัศนคติ และความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของบุคลากรภายในองค์กร ซึ่งการดำเนินงานวิจัยในส่วนนี้ประกอบด้วยขั้นตอนสำคัญ ดังนี้

3.5.1 การออกแบบแบบสอบถามความพึงพอใจของบุคลากรที่เข้ามาใช้งานแพลตฟอร์มชุมชนความปลอดภัยไซเบอร์

การออกแบบและพัฒนาแบบสอบถามโดยอิงจากการทบทวนแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับการประเมินประสบการณ์ของผู้ใช้งานแพลตฟอร์มดิจิทัล (User Experience Assessment) การมีส่วนร่วมในชุมชนออนไลน์เพื่อการเรียนรู้และแลกเปลี่ยนความคิดเห็น (Online Community Engagement) และการส่งเสริมพฤติกรรมที่ปลอดภัยทางไซเบอร์ (Cybersecurity Behavior) โดยเฉพาะในบริบทของการใช้แพลตฟอร์มภายในองค์กร ทั้งนี้เพื่อให้ได้เครื่องมือที่สามารถประเมินได้อย่างครอบคลุมถึงประสิทธิภาพของแพลตฟอร์มชุมชนที่พัฒนาขึ้นโดยใช้ Microsoft OneNote ว่ามีส่วนช่วยในการส่งเสริมความรู้ ความตระหนักรู้ และพฤติกรรมของบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ได้จริงหรือไม่

แบบสอบถามร่างแรกได้ถูกนำเข้าสู่กระบวนการตรวจสอบความเที่ยงตรงด้านเนื้อหา (Content Validity) โดยการขอความเห็นจากอาจารย์ที่ปรึกษา เพื่อประเมินความชัดเจนของถ้อยคำและภาษาที่ใช้ ความครอบคลุมของเนื้อหาแต่ละหัวข้อ ความเหมาะสมของโครงสร้างแบบสอบถาม และความสามารถในการวัดผลตามวัตถุประสงค์ของการวิจัย

จากการพิจารณาดังกล่าว ผู้วิจัยได้นำข้อเสนอแนะที่ได้รับมาปรับปรุงแบบสอบถามให้เหมาะสมทั้งในด้านเนื้อหา รูปแบบ และภาษา โดยเน้นให้สามารถสะท้อนบริบทการใช้งานแพลตฟอร์มชุมชนที่พัฒนาขึ้นอย่างแท้จริง และสุดท้ายได้จัดทำแบบสอบถามฉบับสมบูรณ์สำหรับนำไปใช้ในการเก็บรวบรวมข้อมูลภาคสนามจากกลุ่มเป้าหมายในองค์กร

3.5.2 โครงสร้างแบบสอบถามความพึงพอใจของบุคลากรที่เข้ามาใช้งานแพลตฟอร์มชุมชนความปลอดภัยไซเบอร์

แบบสอบถามฉบับสมบูรณ์ประกอบด้วย 5 ส่วนหลัก โดยแต่ละส่วนมีวัตถุประสงค์และรูปแบบคำถามที่แตกต่างกัน เพื่อให้สามารถเก็บข้อมูลได้อย่างรอบด้าน ครอบคลุมทั้งมิติด้านข้อมูลพื้นฐาน ความพึงพอใจ การมีส่วนร่วม และผลกระทบที่เกิดขึ้นจากการใช้งานแพลตฟอร์มชุมชนความมั่นคงปลอดภัยทางไซเบอร์ รายละเอียดของแต่ละส่วนมีดังนี้

3.5.2.1 ส่วนที่ 1 : ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

วัตถุประสงค์ของส่วนนี้คือเพื่อใช้ในการจำแนกกลุ่มผู้ใช้งานในเชิงบริบท โดยไม่มีการระบุตัวตนเพื่อรักษาความเป็นส่วนตัวของผู้ตอบแบบสอบถาม ข้อมูลที่เก็บรวบรวมประกอบด้วย หน่วยงานที่สังกัด ทั้งนี้ เพื่อวิเคราะห์แนวโน้มและความแตกต่างของความคิดเห็นในแต่ละกลุ่ม คำถามในส่วนนี้ใช้รูปแบบเลือกตอบ (Checklist)

3.5.2.2 ส่วนที่ 2 : ความพึงพอใจต่อการใช้งานแพลตฟอร์ม (User Experience)

ส่วนนี้มีวัตถุประสงค์เพื่อประเมินประสบการณ์ของผู้ใช้งานที่มีต่อการใช้งานแพลตฟอร์ม Microsoft OneNote ในมิติด้านเทคนิค การออกแบบ และความสะดวกในการเข้าถึง โดยประเมินหัวข้อ เช่น ความง่ายในการใช้งาน (Ease of Use) การออกแบบส่วนติดต่อผู้ใช้งาน (Interface Design) ความเร็วในการเข้าถึงข้อมูล ความชัดเจนของการจัดวางเนื้อหา และความเสถียรของระบบ เพื่อสะท้อนคุณภาพของแพลตฟอร์มในฐานะเครื่องมือสนับสนุนการเรียนรู้ คำถามใช้มาตราส่วนประมาณค่า 5 ระดับ (Likert Scale)

3.5.2.3 ส่วนที่ 3 : ความพึงพอใจต่อเนื้อหาและกิจกรรมในแพลตฟอร์ม (Content and Activities)

วัตถุประสงค์ของส่วนนี้คือเพื่อประเมินความเหมาะสม ความน่าสนใจ และคุณภาพของเนื้อหาและกิจกรรมที่จัดอยู่ในแพลตฟอร์ม ซึ่งอาจรวมถึงข่าวสารด้านความปลอดภัยไซเบอร์ บทความกรณีศึกษา เทคนิคการใช้งาน Microsoft 365 อย่างปลอดภัย และกิจกรรมแลกเปลี่ยนความคิดเห็น ผู้ตอบแบบสอบถามจะประเมินความสอดคล้องของเนื้อหากับภัยคุกคามที่เกิดขึ้นจริง ความเข้าใจง่าย และศักยภาพของกิจกรรมในการส่งเสริมการมีส่วนร่วม คำถามในส่วนนี้ใช้มาตราส่วนประมาณค่า 5 ระดับ

3.5.2.4 ส่วนที่ 4 : ผลกระทบจากการใช้งานแพลตฟอร์ม (Outcomes and Impact)

ส่วนนี้มีเป้าหมายเพื่อวัดผลที่เกิดขึ้นกับผู้ใช้งานภายหลังการมีส่วนร่วมกับแพลตฟอร์ม โดยครอบคลุมทั้งในด้านการเรียนรู้ การเปลี่ยนแปลงพฤติกรรม และความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ตัวอย่างของพฤติกรรมที่พิจารณา ได้แก่ การระมัดระวังในการคลิกลิงก์ การใช้รหัสผ่านอย่างปลอดภัย การตรวจสอบอีเมลต้องสงสัย และการเฝ้าระวังภัยคุกคามในชีวิตประจำวัน คำถามในส่วนนี้ใช้มาตราส่วนประมาณค่า 5 ระดับ พร้อมช่องให้ผู้ตอบระบุความคิดเห็นเพิ่มเติมในเชิงคุณภาพ

3.5.2.5 ส่วนที่ 5 : ข้อเสนอแนะและความคิดเห็นเพิ่มเติม (Suggestions and Open Comments)

ในส่วนสุดท้ายนี้ ผู้วิจัยเปิดโอกาสให้ผู้ใช้งานสามารถแสดงความคิดเห็นเกี่ยวกับแพลตฟอร์มชุมชนได้อย่างอิสระ ทั้งในด้านจุดแข็ง จุดที่ควรปรับปรุง รวมถึงข้อเสนอแนะเกี่ยวกับเนื้อหา กิจกรรม หรือฟีเจอร์ที่ต้องการเพิ่มเติมในอนาคต เพื่อใช้เป็นแนวทางในการพัฒนาแพลตฟอร์มให้มี

ประสิทธิภาพมากยิ่งขึ้นและตอบสนองต่อความต้องการของผู้ใช้งานได้อย่างตรงจุด คำถามในส่วนนี้ประกอบด้วยคำถามปลายเปิดเพื่อให้ผู้ตอบสามารถให้ข้อมูลเชิงคุณภาพที่สะท้อนมุมมองส่วนบุคคล ซึ่งอาจไม่สามารถวัดได้จากคำถามแบบปิดในส่วนอื่น ๆ ของแบบสอบถาม

3.6 การประเมินผล

เพื่อให้สามารถวัดผลสัมฤทธิ์ของการพัฒนาแพลตฟอร์มชุมชนด้วย Microsoft OneNote ในการส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ภายในองค์กรได้อย่างเป็นรูปธรรม ผู้วิจัยได้ออกแบบกระบวนการประเมินผลอย่างเป็นระบบใน 2 ส่วน ได้แก่

3.6.1 การประเมินความพึงพอใจของผู้ใช้งาน

ผู้วิจัยใช้แบบสอบถามความพึงพอใจเป็นเครื่องมือหลักในการประเมินประสบการณ์ของบุคลากรที่ใช้งานแพลตฟอร์ม Microsoft OneNote ซึ่งได้รับการออกแบบอย่างครอบคลุมทั้งในเชิงโครงสร้าง การใช้งาน และผลกระทบจากการมีส่วนร่วม โดยมุ่งเน้นการวัดทั้งเชิงปริมาณและคุณภาพ เพื่อนำผลลัพธ์ไปปรับปรุงการพัฒนาแพลตฟอร์มในรอบถัดไป โดยแบบสอบถามครอบคลุม 5 ด้าน ดังนี้

3.6.1.1 ข้อมูลพื้นฐานของผู้ใช้งาน เช่น หน่วยงานที่สังกัด เพื่อนำไปจำแนกกลุ่มผู้ใช้งานในเชิงบริบท และวิเคราะห์แนวโน้มการใช้งานในกลุ่มต่าง ๆ อย่างมีประสิทธิภาพ

3.6.1.2 ความพึงพอใจต่อการใช้งานแพลตฟอร์ม (User Experience) ประเมินความง่ายในการเข้าถึงแพลตฟอร์ม ความสอดคล้องของโครงสร้างการจัดวางเนื้อหา ความชัดเจนของอินเทอร์เฟซ การแสดงผลผ่านอุปกรณ์ต่าง ๆ และความเสถียรของระบบ ซึ่งสะท้อนถึงคุณภาพของ Microsoft OneNote ในฐานะแพลตฟอร์มการเรียนรู้ร่วมสมัยภายในองค์กร

3.6.1.3 ความพึงพอใจต่อเนื้อหาและกิจกรรมในแพลตฟอร์ม (Content and Activities) ประเมินความเหมาะสมของหัวข้อ ความทันสมัยของเนื้อหา การเข้าใจง่าย และความน่าสนใจของกิจกรรม เช่น การแลกเปลี่ยนประสบการณ์ กรณีศึกษา แบบทดสอบ และสื่อมัลติมีเดีย ทั้งนี้เพื่อสะท้อนระดับการมีส่วนร่วมของผู้ใช้งานและศักยภาพของแพลตฟอร์มในการสร้างความตระหนักรู้ในระยะยาว

3.6.1.4 ผลกระทบจากการใช้งานแพลตฟอร์ม (Outcomes and Impact) วิเคราะห์การเปลี่ยนแปลงในด้านพฤติกรรม ความคิด ทัศนคติ และการนำแนวทางความมั่นคงปลอดภัยไปใช้จริง เช่น ความรอบคอบในการใช้งานอีเมล การป้องกันข้อมูลส่วนบุคคล และการตอบสนองต่อเหตุการณ์ผิดปกติ

3.3.1.5 ข้อเสนอแนะเพิ่มเติม (Suggestions and Open Comments) เปิดพื้นที่ให้ผู้ใช้งานแสดงความคิดเห็นอย่างอิสระ ทั้งจุดเด่น จุดที่ควรปรับปรุง และข้อเสนอแนะเกี่ยวกับฟังก์ชันหรือหัวข้อใหม่ ๆ ที่ควรมีในแพลตฟอร์ม ซึ่งจะเป็นแนวทางสำคัญในการพัฒนารอบถัดไปให้ตอบโจทย์ความต้องการผู้ใช้งานได้ตรงจุดยิ่งขึ้น

ข้อมูลทั้งหมดจากแบบสอบถามจะนำมาวิเคราะห์เพื่อสรุปผลในเชิงปริมาณและคุณภาพ พร้อมทั้งนำไปเปรียบเทียบกับผลการเรียนรู้และระดับการมีส่วนร่วม เพื่อใช้ในการวางแนวทางพัฒนาต่อเนื่องอย่างเป็นระบบ

3.6.2 การประเมินผลการเรียนรู้จากแบบทดสอบความรู้

การประเมินผลสัมฤทธิ์ทางการเรียนรู้ดำเนินการผ่าน แบบทดสอบความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ที่ผู้วิจัยออกแบบขึ้นโดยเฉพาะ เพื่อวัดระดับความรู้ ความเข้าใจ และการวิเคราะห์เชิงสถานการณ์ของผู้ใช้งานหลังจากได้เรียนรู้ผ่านแพลตฟอร์ม Microsoft OneNote โดยแบบทดสอบมีจำนวน 15 ข้อ แบ่งตามระดับความยากดังนี้

3.6.2.1 ระดับพื้นฐาน (Basic: ข้อ 1–5) เน้นการวัดความเข้าใจทั่วไป เช่น คำศัพท์พื้นฐานด้านไซเบอร์ซีเคียวริตี้ ความหมายของมัลแวร์ การเลือกใช้รหัสผ่านที่ปลอดภัย และการแยกแยะพฤติกรรมเสี่ยงเบื้องต้น

3.6.2.2 ระดับปานกลาง (Intermediate: ข้อ 6–10) วัดความสามารถในการวิเคราะห์สถานการณ์สมมุติ เช่น การตรวจจับฟิชชิ่งอีเมล การตอบสนองเมื่อพบการหลอกลวงทางออนไลน์ และแนวทางการจัดการภัยคุกคามระดับองค์กร

3.6.2.3 ระดับสูง (Advanced: ข้อ 11–15): มุ่งเน้นการประเมินทักษะคิดวิเคราะห์และการประยุกต์ใช้ความรู้ เช่น การเลือกมาตรการตามข้อกำหนด PDPA หรือ ISO/IEC 27001:2022 การวางแนวทางตอบสนองเหตุการณ์ และการประเมินผลกระทบจากภัยไซเบอร์ในระดับนโยบาย

แบบทดสอบถูกจัดทำในรูปแบบ ข้อสอบปรนัย (Multiple Choice Questions) พร้อมคำอธิบายประกอบคำตอบ (Answer Explanation) เพื่อส่งเสริมการเรียนรู้ย้อนกลับ (Reflective Learning) โดยผู้ใช้งานสามารถเรียนรู้จากเฉลยที่อธิบายเหตุผลเบื้องหลังคำตอบที่ถูกต้อง ซึ่งจะช่วยกระตุ้นให้เกิดการทบทวนและเสริมสร้างความเข้าใจเชิงลึกมากยิ่งขึ้น

ผลคะแนนจากแบบทดสอบจะถูกนำไปวิเคราะห์เชิงเปรียบเทียบร่วมกับข้อมูลจากแบบสอบถามความพึงพอใจ เพื่อวิเคราะห์ความสัมพันธ์ระหว่าง “ระดับความรู้ที่ได้รับ” และ “ประสบการณ์การใช้งาน” ซึ่งจะเป็นข้อมูลเชิงประจักษ์สำคัญสำหรับการออกแบบหลักสูตรอบรม กิจกรรมส่งเสริมความรู้ และกลยุทธ์การสร้างวัฒนธรรมความมั่นคงปลอดภัยในองค์กรอย่างยั่งยืน

บทที่ 4
ผลการดำเนินการวิจัย

ในการค้นคว้าอิสระครั้งนี้ มีวัตถุประสงค์เพื่อพัฒนาแพลตฟอร์มชุมชนโดยใช้ Microsoft OneNote เป็นเครื่องมือหลักในการส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กร โดยมุ่งเน้นการสร้างสภาพแวดล้อมแห่งการเรียนรู้ร่วมกันผ่านเนื้อหาที่หลากหลาย กิจกรรมที่ออกแบบให้ผู้ใช้งานมีส่วนร่วมอย่างต่อเนื่อง และการบูรณาการกับเครื่องมือในชุด Microsoft 365 เพื่อให้บุคลากรสามารถเข้าถึงข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์ได้อย่างสะดวก รวดเร็ว และต่อเนื่อง

ผู้วิจัยได้ดำเนินการศึกษาพฤติกรรมการใช้งาน Microsoft 365 ของบุคลากรภายในองค์กรทั้งหมด เพื่อวิเคราะห์แนวโน้มการใช้งานเครื่องมือดิจิทัลที่เกี่ยวข้อง และประเมินผลการใช้งานแพลตฟอร์มชุมชนในมิติต่าง ๆ ได้แก่ ระดับความพึงพอใจต่อการใช้งาน การพัฒนาด้านความรู้และทัศนคติ การมีส่วนร่วมในกิจกรรมของแพลตฟอร์ม รวมถึงผลกระทบที่เกิดขึ้นต่อพฤติกรรมด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในภาพรวม โดยผลการวิเคราะห์ข้อมูลและประเมินผลการดำเนินงาน มีรายละเอียดดังต่อไปนี้

4.1 ภาพรวมการดำเนินการทดลองใช้งานแพลตฟอร์ม
4.2 พฤติกรรมการใช้งาน Microsoft 365 ของบุคลากรภายในองค์กร
4.3 การประชาสัมพันธ์เพื่อกระตุ้นการใช้งานแพลตฟอร์ม และช่องทางการสื่อสารภายในองค์กร
4.4 ผลการประเมินความรู้จากแบบทดสอบ
4.5 ผลการประเมินความพึงพอใจของผู้ใช้งาน
4.6 สรุปผลเบื้องต้นจากการใช้งานแพลตฟอร์ม

4.1 ภาพรวมการดำเนินการทดลองใช้งานแพลตฟอร์ม

ผู้วิจัยได้ดำเนินการพัฒนาแพลตฟอร์มชุมชนเพื่อส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กร โดยใช้ Microsoft OneNote เป็นเครื่องมือหลักในการจัดการเนื้อหาและเชื่อมโยงการเรียนรู้ร่วมกันภายในองค์กร แพลตฟอร์มดังกล่าวถูกออกแบบให้มีการจัดหมวดหมู่เนื้อหาอย่างเป็นระบบ ครอบคลุมหัวข้อสำคัญด้านความมั่นคงปลอดภัยไซเบอร์จำนวน 8 ส่วน ได้แก่

4.1.1 ความรู้เบื้องต้นด้านความมั่นคงปลอดภัยไซเบอร์
4.1.2 การโจมตีแบบฟิชชิ่งและการหลอกลวงทางสื่ออิเล็กทรอนิกส์
4.1.3 การตอบสนองต่อเหตุการณ์ไซเบอร์
4.1.4 แนวทางการใช้งานเทคโนโลยีสารสนเทศอย่างปลอดภัย
4.1.5 นโยบายและมาตรฐานที่เกี่ยวข้อง
4.1.6 กรณีศึกษาจากเหตุการณ์จริง
4.1.7 การแจ้งเตือนและบทวิเคราะห์ภัยคุกคาม
4.1.8 แบบทดสอบความรู้และแบบประเมินตนเอง

นอกจากการจัดทำเนื้อหาความรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบแล้ว ผู้วิจัยยังได้บูรณาการแพลตฟอร์มชุมชน Microsoft OneNote เข้ากับเครื่องมืออื่นภายใต้ชุด Microsoft 365 เพื่อเพิ่มประสิทธิภาพในการเรียนรู้และการสื่อสารภายในองค์กร โดยมีการเชื่อมโยงกับ Microsoft Forms สำหรับใช้เป็นเครื่องมือในการสร้างแบบทดสอบ และแบบสอบถาม ซึ่งครอบคลุมทั้งการประเมินความเข้าใจในเนื้อหาหลังการเรียนรู้ และการวัดความพึงพอใจของผู้ใช้งานแพลตฟอร์ม เพื่อให้สามารถติดตามผลการดำเนินงานและนำข้อมูลไปปรับปรุงกิจกรรมให้สอดคล้องกับความต้องการของบุคลากรได้อย่างต่อเนื่อง

นอกจากนี้ ยังได้ใช้ Microsoft Teams และ Microsoft Outlook เป็นช่องทางสำคัญในการสื่อสารภายในองค์กร โดยเฉพาะการเผยแพร่ข่าวสารด้านภัยคุกคามไซเบอร์ที่เกิดขึ้นล่าสุด หรือสถานการณ์ตัวอย่างที่เกี่ยวข้องกับพฤติกรรมเสี่ยง เพื่อกระตุ้นให้บุคลากรติดตามและเข้าศึกษาข้อมูลเพิ่มเติมผ่านแพลตฟอร์ม OneNote ได้สะดวกและทันเวลา ทั้งนี้ รูปแบบการส่งสารได้รับการออกแบบให้น่าสนใจ เช่น การใช้ข้อความเชิงกระตุ้น ความสั้นกระชับ และมีการแนบลิงก์เข้าสู่หัวข้อที่เกี่ยวข้องในแพลตฟอร์มโดยตรง ช่วยให้การเข้าถึงข้อมูลเป็นไปอย่างมีประสิทธิภาพ และส่งเสริมการเรียนรู้แบบบูรณาการในชีวิตประจำวันของผู้ใช้งาน

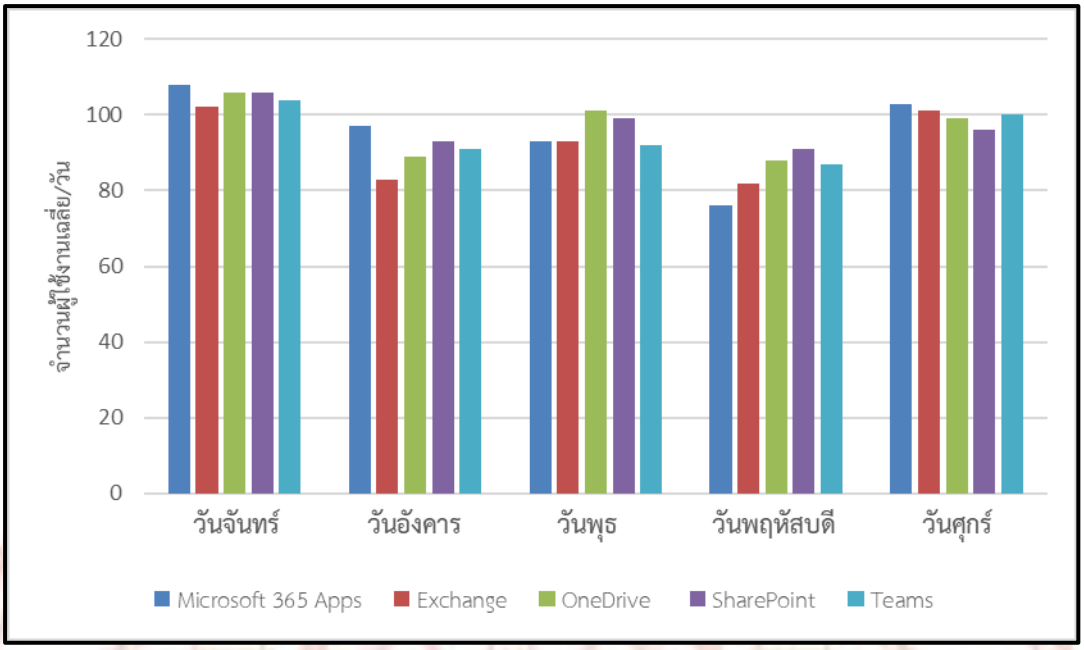
จากการออกแบบแพลตฟอร์มในลักษณะเชิงบูรณาการดังกล่าว ผู้วิจัยมีเป้าหมายให้แพลตฟอร์มชุมชนนี้ทำหน้าที่เป็น “ศูนย์กลางการเรียนรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์” ภายในองค์กร โดยมุ่งเน้นการตอบสนองต่อรูปแบบการเรียนรู้ของบุคลากรในยุคดิจิทัลที่เปลี่ยนแปลงอย่างรวดเร็ว ทั้งในด้านความสะดวกในการเข้าถึงเนื้อหา และการเรียนรู้ด้วยตนเอง แพลตฟอร์มได้รับการออกแบบให้สามารถส่งเสริมการเรียนรู้ที่ต่อเนื่อง ไม่จำกัดเวลาและสถานที่ ตลอดจนสนับสนุนการมีส่วนร่วมของบุคลากรอย่างแท้จริง ผ่านกิจกรรมเชิงโต้ตอบ การแลกเปลี่ยนประสบการณ์ และกระบวนการประเมินผลอย่างสม่ำเสมอ ซึ่งทั้งหมดนี้ล้วนมีส่วนสำคัญในการหล่อหลอมและเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ในระดับองค์กรได้อย่างยั่งยืน

4.2 พฤติกรรมการใช้งาน Microsoft 365 ของบุคลากรภายในองค์กร

4.2.1 ภาพรวมการใช้งาน Microsoft 365 ของบุคลากรภายในองค์กร

จากการเก็บรวบรวมและวิเคราะห์ข้อมูลพฤติกรรมการใช้งาน Microsoft 365 ของบุคลากรภายในองค์กร ดังแสดงในภาพที่ 4-1 พบว่าบุคลากรมีการใช้งานเครื่องมือต่าง ๆ อย่างหลากหลาย และสอดคล้องกับลักษณะงานและความต้องการเฉพาะด้านของแต่ละฝ่ายงาน โดยเครื่องมือหลักที่มีการใช้งานอย่างต่อเนื่อง ได้แก่ Microsoft Exchange และ Microsoft Teams ซึ่งใช้สำหรับการสื่อสารอย่างเป็นทางการและไม่เป็นทางการ ทั้งในรูปแบบของอีเมล การประชุมออนไลน์ และการสนทนาในทีมงาน

ทั้งนี้ ภาพรวมการใช้งานในช่วง 1 สัปดาห์ พบว่า Microsoft 365 Apps มีจำนวนผู้ใช้งานเฉลี่ยสูงที่สุด รองลงมาได้แก่ Microsoft Exchange, Teams, OneDrive และ SharePoint ซึ่งมีการใช้งานอย่างสม่ำเสมอในทุกวันทำการ โดยสะท้อนให้เห็นถึงบทบาทสำคัญของเครื่องมือเหล่านี้ในการสนับสนุนกระบวนการทำงาน การจัดเก็บและแบ่งปันข้อมูล รวมถึงการสื่อสารภายในองค์กรอย่างมีประสิทธิภาพ



ภาพที่ 4-1 ภาพรวมสถิติการใช้งาน Microsoft 365 ของบุคลากรภายในองค์กร

นอกจากนี้ เครื่องมือที่สนับสนุนการจัดเก็บและบริหารจัดการเอกสาร เช่น Microsoft OneDrive และ SharePoint ก็ได้รับความนิยมในกลุ่มผู้ใช้งานที่ต้องจัดการเอกสารเป็นประจำ เนื่องจากสามารถแบ่งปันไฟล์ระหว่างฝ่ายงานและควบคุมสิทธิ์การเข้าถึงได้อย่างมีประสิทธิภาพ

สำหรับ Microsoft OneNote ซึ่งเป็นเครื่องมือหลักที่ใช้ในการพัฒนาแพลตฟอร์มชุมชน เพื่อเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ พบว่ามีแนวโน้มการเข้าถึงและใช้งานเพิ่มขึ้นอย่างเห็นได้ชัด โดยเฉพาะในช่วงที่มีการรณรงค์ประชาสัมพันธ์และจัดกิจกรรมเชิงมีส่วนร่วมในแพลตฟอร์ม ทั้งนี้ แม้จะไม่มีรายงานการใช้งานแบบแยกเฉพาะจากระบบ Microsoft Admin Center แต่จากการติดตามผลผ่านแบบสอบถาม การตอบสนองของผู้ใช้งาน และบันทึกกิจกรรมในระบบ พบว่าบุคลากรให้ความสนใจและเข้าถึงเนื้อหาในแพลตฟอร์มเพิ่มมากขึ้น ซึ่งสะท้อนให้เห็นถึงศักยภาพของเครื่องมือดังกล่าวในการเป็นช่องทางการเรียนรู้ และส่งเสริมความตระหนักรู้ในประเด็นด้านความมั่นคงปลอดภัยขององค์กรได้อย่างมีประสิทธิผล

ภาพรวมนี้แสดงให้เห็นว่าการนำชุดเครื่องมือ Microsoft 365 มาใช้ภายในองค์กรไม่เพียงแต่ช่วยสนับสนุนการทำงานและการสื่อสารประจำวันเท่านั้น แต่ยังสามารถต่อยอดสู่การพัฒนาแนวทางการเรียนรู้และสร้างการมีส่วนร่วมที่ยั่งยืนในระดับองค์กรได้อีกด้วย

4.2.2 การใช้งาน Exchange ของบุคลากรภายในองค์กร

บุคลากรในองค์กรใช้งาน Exchange เป็นเครื่องมือหลักสำหรับการรับส่งอีเมลภายในและภายนอกองค์กร รวมถึงการจัดการปฏิทิน นัดหมาย และประชุมออนไลน์ผ่านฟีเจอร์ที่เชื่อมต่อกับ Teams และ Zoom ซึ่ง Exchange ยังถูกใช้ในการจัดหมวดหมู่อีเมลที่สำคัญ การตั้งค่าแจ้งเตือน และการทำงานร่วมกับกล่องจดหมายของแผนกต่าง ๆ พบว่าผู้บริหารระดับต้นถึงกลางมีแนวโน้มใช้งาน Exchange อย่างสม่ำเสมอในการติดตามงานและติดต่อประสานงาน

4.2.3 การใช้งาน Microsoft OneDrive ของบุคลากรภายในองค์กร

บุคลากรภายในองค์กรมีการใช้งาน OneDrive เพื่อจัดเก็บและสำรองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการทำงาน โดยนิยมใช้ในการบันทึกไฟล์เอกสารที่ต้องมีการปรับปรุงบ่อย เช่น รายงานการประชุม แผนงาน หรือเอกสารอ้างอิง ทั้งยังใช้ร่วมกับการแชร์ไฟล์ให้เพื่อนร่วมทีมในลักษณะเฉพาะรายบุคคล โดยพบว่ามีแนวโน้มการใช้งานสูงในกลุ่มฝ่ายสนับสนุนและงานเอกสารที่ต้องการความสะดวกรวดเร็วในการเข้าถึงไฟล์จากหลายอุปกรณ์

4.2.4 การใช้งาน Microsoft SharePoint ของบุคลากรภายในองค์กร

การใช้งาน SharePoint ภายในองค์กรส่วนใหญ่เน้นไปที่การเป็นศูนย์กลางจัดเก็บเอกสารที่เกี่ยวข้องกับแต่ละฝ่ายงาน เช่น คำสั่งภายใน นโยบายองค์กร หรือคู่มือปฏิบัติงาน โดยบุคลากรสามารถเข้าถึงไฟล์ต่าง ๆ ได้ตามสิทธิ์ที่กำหนดไว้ ช่วยเพิ่มความเป็นระบบในการจัดเก็บข้อมูล และลดความซ้ำซ้อนของไฟล์ที่เผยแพร่ผ่านหลายช่องทาง โดยกลุ่มที่ใช้งานเป็นประจำ ได้แก่ เจ้าหน้าที่ธุรการและฝ่ายบริหารงานทั่วไป

4.2.5 การใช้งาน Microsoft Teams ของบุคลากรภายในองค์กร

Microsoft Teams เป็นแพลตฟอร์มหลักในการสื่อสารแบบเรียลไทม์ขององค์กร ทั้งในรูปแบบแชท การประชุมทางวิดีโอ การแชร์หน้าจอ และการสร้างทีมย่อยสำหรับการทำงานเป็นกลุ่ม พบว่ามีการใช้งาน Microsoft Teams อย่างแพร่หลายในกลุ่มงานโครงการและฝ่ายบริหารที่ต้องการความคล่องตัวในการสื่อสารแบบทันที นอกจากนี้ยังนิยมใช้ในการจัดประชุมออนไลน์และบันทึกการประชุมควบคู่กับ OneNote

4.2.6 การใช้งาน Microsoft OneNote ภายใต้ Microsoft 365 Apps

เนื่องจากในหน้ารายงานการใช้งาน Microsoft 365 ขององค์กร ยังไม่มีการแสดงผลการใช้งานของ Microsoft OneNote แยกออกมาอย่างชัดเจน ผู้วิจัยจึงขออธิบายการใช้งาน Microsoft OneNote ในฐานะที่เป็นหนึ่งในแอปพลิเคชันหลักภายใต้ชุด Microsoft 365 Apps ที่ได้รับการติดตั้งและใช้งานร่วมกับแอปอื่น ๆ เช่น Exchange, Teams, Word, Excel และ PowerPoint

Microsoft OneNote ทำหน้าที่เป็นแพลตฟอร์มสำหรับการจดบันทึกและจัดการความรู้แบบดิจิทัล โดยได้รับการบูรณาการอย่างแน่นแฟ้นกับแอปพลิเคชันอื่นในชุด Microsoft 365 เช่น Exchange ใช้แนบโน้ตประกอบการประชุมหรือติดตามงานจากอีเมล, Teams ใช้แชร์โน้ตภายในช่องทางสนทนาหรือกลุ่มการทำงาน, Forms เชื่อมโยงแบบประเมินหรือแบบทดสอบเข้าในโน้ตแต่ละหัวข้อ และ Word, Excel แนบเอกสารประกอบเพื่ออ้างอิงร่วมกับบันทึกในแต่ละหน้า

จากการใช้งานจริงภายในองค์กร พบว่าการใช้ Microsoft OneNote เพื่อพัฒนาแพลตฟอร์มชุมชนด้านความมั่นคงปลอดภัยทางไซเบอร์นั้น ช่วยเสริมการเรียนรู้ การมีส่วนร่วม และการสื่อสารอย่างต่อเนื่องของบุคลากร โดยไม่จำเป็นต้องพึ่งแพลตฟอร์มภายนอกเพิ่มเติม ทั้งยังสอดรับกับแนวทางการใช้งานเครื่องมือในชุด Microsoft 365 ที่องค์กรมีอยู่แล้ว

ดังนั้น แม้ Microsoft OneNote จะไม่มีรายงานการใช้งานเฉพาะเจาะจงแยกออกมาในระบบรายงานของผู้ดูแล Microsoft 365 แต่ก็ถือว่าเป็นหนึ่งในแอปที่มีบทบาทสำคัญในการเสริมสร้างกระบวนการเรียนรู้ และการแลกเปลี่ยนข้อมูลภายในองค์กรในลักษณะบูรณาการกับแอปอื่นในชุดเดียวกัน

4.3 การประชาสัมพันธ์เพื่อกระตุ้นการใช้งานแพลตฟอร์ม และช่องทางการสื่อสารภายในองค์กร

ในการพัฒนาแพลตฟอร์มชุมชนความมั่นคงปลอดภัยไซเบอร์บน Microsoft OneNote ให้ประสบความสำเร็จตามวัตถุประสงค์ของการค้นคว้าอิสระ ไม่เพียงแต่ต้องคำนึงถึงโครงสร้างเนื้อหาและเครื่องมือเทคโนโลยีที่ใช้ แต่ยังต้องให้ความสำคัญกับกระบวนการประชาสัมพันธ์และการสร้างการรับรู้ (Awareness Building) อย่างเป็นระบบ เพื่อให้บุคลากรภายในองค์กรเกิดความสนใจ เข้าถึง และมีส่วนร่วมกับแพลตฟอร์มอย่างต่อเนื่อง

ผู้วิจัยจึงได้ออกแบบและดำเนินการประชาสัมพันธ์แพลตฟอร์มผ่านหลากหลายช่องทางการสื่อสารภายในองค์กร โดยยึดแนวคิด “การสื่อสารแบบบูรณาการ” (Integrated Communication) ซึ่งครอบคลุมทั้งช่องทางทางการ (Formal Channels) และช่องทางไม่เป็นทางการ (Informal Channels) เพื่อตอบสนองพฤติกรรมการรับสารของบุคลากรในแต่ละระดับ ดังรายละเอียดต่อไปนี้

4.3.1 หนังสือเวียนภายในองค์กร

ได้จัดทำหนังสือเวียนในรูปแบบราชการ เพื่อแจ้งข่าวสารเกี่ยวกับช่องทางการเข้าใช้งานแพลตฟอร์มชุมชนความมั่นคงปลอดภัยไซเบอร์อย่างเป็นทางการแก่ฝ่ายงานและผู้บริหารระดับต้น พร้อมทั้งประชาสัมพันธ์การใช้งานแพลตฟอร์มดังกล่าว ซึ่งประกอบด้วยแบบทดสอบความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Knowledge Test) และกิจกรรมอื่น ๆ ที่ส่งเสริมการเรียนรู้ ทั้งนี้ ขอความร่วมมือจากบุคลากรที่ใช้งานแพลตฟอร์มดังกล่าวในการตอบแบบสอบถามความพึงพอใจ เพื่อใช้เป็นข้อมูลประกอบการพัฒนาและปรับปรุงแพลตฟอร์มให้มีประสิทธิภาพยิ่งขึ้น

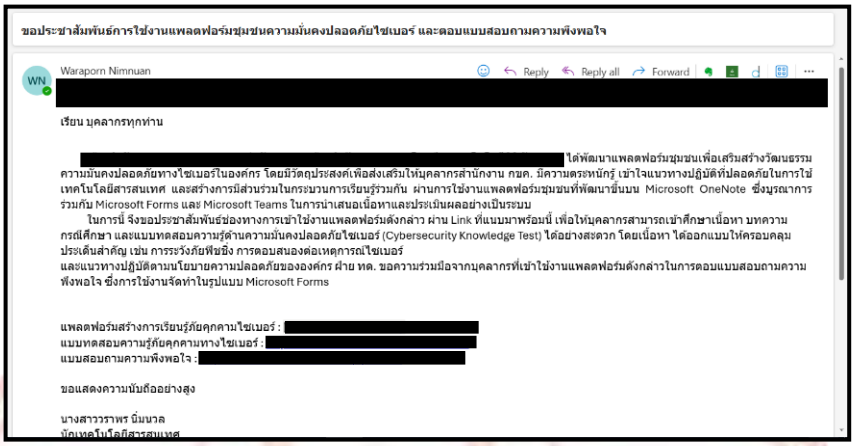
นอกจากนี้ หนังสือเวียนยังทำหน้าที่เป็นเครื่องมือสำคัญในการสร้างการรับรู้เชิงนโยบาย (Policy Awareness) และกระตุ้นการสนับสนุนจากผู้บริหารระดับต้น ซึ่งมีบทบาทในการขับเคลื่อนการใช้งานของบุคลากรในหน่วยงานภายใต้ความรับผิดชอบ อันเป็นปัจจัยสำคัญต่อความต่อเนื่องและความยั่งยืนของการใช้แพลตฟอร์มภายในองค์กร

4.3.2 Microsoft Teams

Microsoft Teams ถูกนำมาใช้เป็นช่องทางหลักในการเผยแพร่ข้อมูล ข่าวสาร และกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับแพลตฟอร์ม โดยอาศัยกลุ่มหรือช่องทางการสื่อสารภายในที่บุคลากรใช้งานอยู่แล้วในชีวิตประจำวัน การออกแบบเนื้อหาเน้นความกระชับ ดึงดูดความสนใจ และการใช้สื่อผสม เช่น อินโฟกราฟิก วิดีโอ และภาพเหตุการณ์จำลอง เพื่อกระตุ้นให้ผู้รับสารคลิกเข้าสู่แพลตฟอร์ม OneNote และเรียนรู้เพิ่มเติม

4.3.3 จดหมายข่าวอิเล็กทรอนิกส์ (Email Bulletin)

ผู้วิจัยได้จัดส่งจดหมายข่าวอิเล็กทรอนิกส์ (Email Bulletin) เป็นประจำในลักษณะรายสัปดาห์หรือรายเดือน โดยเนื้อหาประกอบด้วยการสรุปสถานการณ์ภัยคุกคามไซเบอร์ที่เกิดขึ้นจริง ทั้งในภาคธุรกิจ หน่วยงานภาครัฐ และจากแหล่งข่าวสาธารณะ พร้อมแนบลิงก์เข้าสู่บทเรียนหรือเนื้อหาที่เกี่ยวข้องภายในแพลตฟอร์ม OneNote เพื่อสร้างบริบทของการเรียนรู้ที่ผู้ใช้งานสามารถเชื่อมโยงกับประสบการณ์จริงได้



ภาพที่ 4-2 จดหมายข่าวอิเล็กทรอนิกส์ (Email Bulletin)

4.3.4 Intranet Banner

มีการจัดวางแบนเนอร์ประชาสัมพันธ์ชื่อว่า “Cyber Security Knowledge Hub” ในตำแหน่งที่มองเห็นได้ชัดเจนบนหน้าแรกของระบบอินทราเน็ตขององค์กร เช่น บริเวณหน้าเข้าสู่ระบบการลงเวลาทำงาน หรือเมนูหลักของระบบสารสนเทศภายใน แบนเนอร์ได้รับการออกแบบให้โดดเด่นด้วยการใช้ภาพเคลื่อนไหว ข้อความกระตุ้นความสนใจ และปุ่มคลิกเพื่อเข้าสู่แพลตฟอร์มโดยตรง เพื่ออำนวยความสะดวกและลดขั้นตอนการเข้าถึงข้อมูล

4.3.5 โปสเตอร์ประชาสัมพันธ์ QR Code

มีการจัดทำโปสเตอร์ประชาสัมพันธ์ QR Code สำหรับเชื่อมต่อเข้าสู่แพลตฟอร์ม OneNote ได้โดยตรง ติดตั้งในพื้นที่ที่มีการใช้งานจริงภายในสำนักงาน เช่น บริเวณจุดสแกนบัตร ห้องประชุม โถงลิฟต์ และบอร์ดประชาสัมพันธ์ตามชั้นต่าง ๆ ภายในอาคาร โดยออกแบบข้อความให้มีความกระชับ ชัดเจน และมีเนื้อหาที่กระตุ้นแรงจูงใจ เช่น การเชิญชวนเข้าร่วมกิจกรรม การเรียนรู้จากเหตุการณ์จริง หรือการสะสมคะแนนจากการทำแบบทดสอบ เพื่อเพิ่มความน่าสนใจและการมีส่วนร่วม

ภาพที่ 4-3 โปสเตอร์ประชาสัมพันธ์ QR Code

4.4 ผลการประเมินความรู้จากแบบทดสอบ

4.4.1 วัตถุประสงค์ของการประเมินความรู้จากแบบทดสอบ

การประเมินความรู้ผ่านแบบทดสอบมีวัตถุประสงค์เพื่อวัดผลการเรียนรู้ของบุคลากรภายในองค์กร หลังจากที่ได้เข้าเข้าใช้งานแพลตฟอร์มชุมชนความมั่นคงปลอดภัยไซเบอร์ที่พัฒนาขึ้นบน Microsoft OneNote โดยมุ่งเน้นให้สามารถตรวจสอบระดับความเข้าใจในหัวข้อสำคัญด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งในเชิงทฤษฎีและการประยุกต์ใช้จริงในบริบทการทำงานขององค์กร

กลุ่มเป้าหมายสำหรับการทดสอบความรู้ผ่านแพลตฟอร์มชุมชนนี้ ได้แก่ บุคลากรภายในองค์กรที่มีการใช้งานระบบสารสนเทศและการสื่อสารภายในองค์กรเป็นประจำ จำนวนทั้งสิ้น 16 ฝ่ายงาน โดยมีผู้สนใจเข้าร่วมทำแบบทดสอบความรู้ จำนวน 52 คน จากบุคลากรทั้งหมด 109 คน คิดเป็นประมาณร้อยละ 47.71 หรือเกือบครึ่งหนึ่งของจำนวนบุคลากรในองค์กร ซึ่งถือเป็นสัดส่วนที่เหมาะสมและสามารถสะท้อนความคิดเห็นและพฤติกรรมของกลุ่มผู้ใช้งานระบบสารสนเทศในบริบทขององค์กรได้อย่างครอบคลุม

ในการกำหนดกลุ่มเป้าหมาย ผู้วิจัยใช้วิธีการเลือกแบบเจาะจง (Purposive Sampling) [22] ซึ่งอาศัยดุลยพินิจของผู้วิจัยในการคัดเลือกกลุ่มเป้าหมายที่มีคุณลักษณะตรงตามวัตถุประสงค์ของการวิจัย โดยเน้นผู้ที่มีความเกี่ยวข้องและประสบการณ์ตรงในการใช้งานระบบสารสนเทศภายในองค์กร ทั้งนี้ ได้มีการคัดเลือกตัวแทนจากทุกฝ่ายงานเพื่อให้ข้อมูลที่ได้รับสามารถสะท้อนมุมมองและพฤติกรรมการใช้งานระบบสารสนเทศในแต่ละส่วนงานได้อย่างครอบคลุมและหลากหลาย

แบบทดสอบถูกออกแบบภายใต้แนวคิดการประเมินผลหลังการเรียนรู้ (Post-Learning Assessment) และสอดคล้องกับกรอบเนื้อหาที่ปรากฏในแพลตฟอร์ม โดยมีการจัดทำเป็นแบบปรนัย จำนวน 15 ข้อ เพื่อประเมินความรู้ในประเด็นที่ครอบคลุม ดังนี้

4.4.1.1 พื้นฐานความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Basics) ที่อธิบายหลักการเบื้องต้นของความมั่นคงปลอดภัยไซเบอร์ ได้แก่ หลักการ CIA Triad (Confidentiality, Integrity, Availability) และแนวคิดเรื่องภัยคุกคาม ความเสี่ยง และมาตรการป้องกันในระดับพื้นฐาน

4.4.1.2 การโจมตีแบบฟิชชิ่ง (Phishing Attacks) โดยเน้นการประเมินความสามารถในการแยกแยะประเภทของฟิชชิ่ง เช่น Email Phishing, Spear Phishing และ Smishing รวมถึงพฤติกรรมที่มีความเสี่ยงต่อการตกเป็นเหยื่อ

4.4.1.3 พฤติกรรมเสี่ยงในที่ทำงาน (Unsafe Practices at Work) โดยเน้นการวิเคราะห์สถานการณ์จำลองที่อาจก่อให้เกิดช่องโหว่ เช่น การตั้งรหัสผ่านไม่ปลอดภัย การคลิกลิงก์น่าสงสัย หรือการเปิดเผยข้อมูลบนโซเชียลมีเดียโดยไม่ตรวจสอบแหล่งที่มา

4.4.1.4 แนวทางป้องกันภัยไซเบอร์เบื้องต้น (Basic Cyber Hygiene) ตรวจสอบความรู้เกี่ยวกับมาตรการพื้นฐานที่บุคลากรสามารถนำไปปรับใช้ได้ทันที เช่น การใช้ Two-Factor Authentication (2FA), การอัปเดตซอฟต์แวร์ การใช้เครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) และการแจ้งเหตุผ่าน ThaiCERT

4.4.1.5 มาตรฐานและกฎหมายที่เกี่ยวข้อง (Cybersecurity Law & Standard) วัดความเข้าใจต่อกฎหมายสำคัญ เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

พระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2550 รวมถึงมาตรฐาน ISO/IEC 27001:2022 และแนวทางการนำไปประยุกต์ใช้ในระดับองค์กร

ผลการประเมินจะนำไปวิเคราะห์ระดับความสำเร็จของแพลตฟอร์มในการถ่ายทอดองค์ความรู้และใช้เป็นข้อมูลประกอบในการปรับปรุงเนื้อหา กิจกรรม และวิธีการเรียนรู้ในอนาคต เพื่อให้สอดคล้องกับระดับความรู้พื้นฐานของบุคลากร และตอบสนองต่อบริบทการใช้งานจริงขององค์กรได้ดียิ่งขึ้น

4.4.2 ลักษณะของแบบทดสอบ

แบบทดสอบที่ใช้ในการประเมินผลการเรียนรู้ของบุคลากรหลังจากการเข้าใช้งานแพลตฟอร์มชุมชนความมั่นคงปลอดภัยไซเบอร์บน Microsoft OneNote ได้รับการออกแบบโดยอิงจากโครงสร้างเนื้อหาภายในแพลตฟอร์ม โดยครอบคลุมหัวข้อด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริบทขององค์กรจริง โดยมีลักษณะของแบบทดสอบ ดังนี้

4.4.2.1 จำนวนข้อทั้งหมด : 15 ข้อ

4.4.2.2 ประเภทของข้อคำถาม : ปรนัยแบบเลือกตอบ (Multiple Choice) โดยมีคำตอบให้เลือก 4 ตัวเลือก และมีคำตอบที่ถูกต้องเพียงข้อเดียวในแต่ละคำถาม

4.4.2.3 คะแนนเต็ม : 15 คะแนน (ข้อละ 1 คะแนน)

4.4.2.4 รูปแบบการจัดสอบ : ดำเนินการผ่านระบบออนไลน์โดยใช้เครื่องมือ Microsoft Forms ซึ่งเป็นส่วนหนึ่งของชุดโปรแกรม Microsoft 365 ทำให้สามารถจัดเก็บข้อมูลวิเคราะห์ผล และระบุความเชื่อมโยงกับบัญชีผู้ใช้ในระบบองค์กรได้อย่างสะดวกและปลอดภัย

4.4.2.5 จำนวนผู้ทำแบบทดสอบ : 52 คน โดยเป็นกลุ่มบุคลากรจากฝ่ายงานในองค์กรซึ่งได้รับเชิญให้เข้าร่วมกิจกรรมภายใต้แพลตฟอร์มที่พัฒนาขึ้น

การออกแบบข้อสอบมุ่งเน้นการวัดผลตามจุดมุ่งหมายเชิงพฤติกรรม (Learning Objectives) ของแต่ละหัวข้อในแพลตฟอร์มชุมชน โดยเฉพาะอย่างยิ่งในระดับการประเมินความเข้าใจเชิงการประยุกต์ใช้ (Applied Knowledge) ผ่านสถานการณ์จำลอง ที่ใกล้เคียงกับความเป็นจริงในองค์กร เช่น การระบุพฤติกรรมเสี่ยง การรับมือกับอีเมลฟิชชิ่ง การตั้งรหัสผ่านที่ปลอดภัย และการเลือกใช้มาตรการด้านความปลอดภัยอย่างเหมาะสม

ทั้งนี้ แบบทดสอบยังได้รับการกลั่นกรองและตรวจสอบจากอาจารย์ที่ปรึกษา เพื่อให้แน่ใจว่าเนื้อหาในแต่ละข้อมีความถูกต้อง ชัดเจน และมีความเที่ยงตรงในการวัดผลการเรียนรู้ตามเป้าหมายของการประเมิน

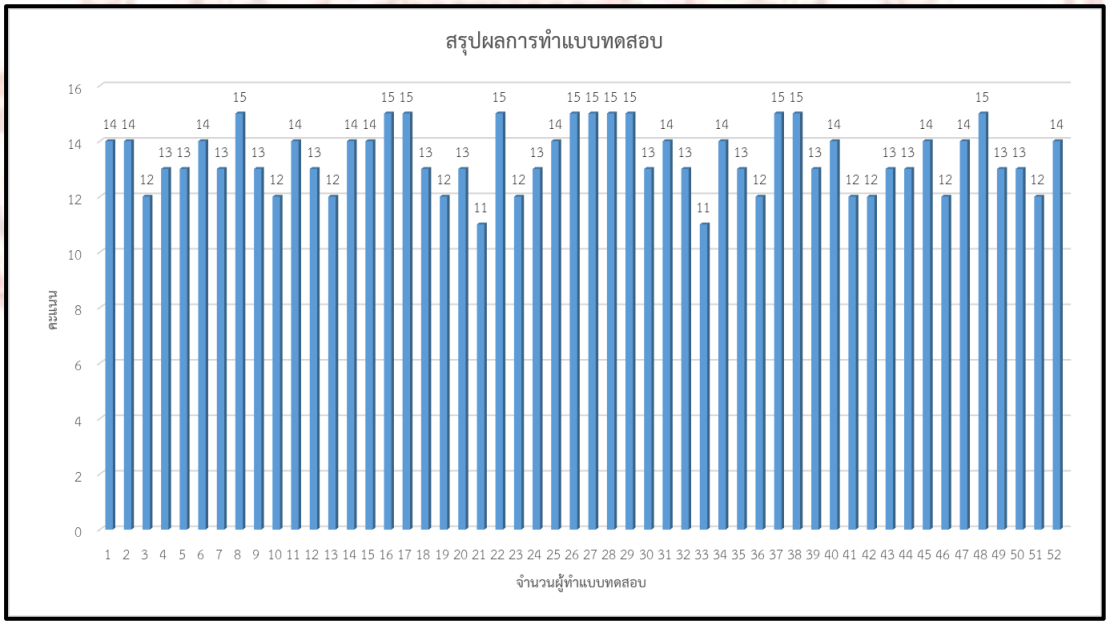
4.4.3 สรุปผลการประเมินความรู้จากแบบทดสอบ

จากผลการประเมินแบบทดสอบความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ที่จัดขึ้นภายหลังการเข้าใช้งานแพลตฟอร์ม พบว่ากลุ่มเป้าหมาย จำนวน 52 คน มีแนวโน้มผลคะแนนอยู่ในระดับค่อนข้างดี โดยมีรายละเอียดค่าทางสถิติที่สำคัญ ดังนี้

ตารางที่ 4-1 สรุปผลการประเมินความรู้จากแบบทดสอบ

รายละเอียด		สรุปผล
Mean	(ค่าเฉลี่ย) x = AVERAGE	13.40
Median	(ค่ามัธยฐาน) = MEDIAN	13
Max	(ค่ามากที่สุด) = MAX	15
Min	(ค่าน้อยที่สุด) = MIN	11
S.D.	(ส่วนเบี่ยงเบนมาตรฐาน) = STDEV	1.14

ค่าเฉลี่ยและมัธยฐานของคะแนนสอบอยู่ในระดับสูงเมื่อเทียบกับคะแนนเต็ม (15 คะแนน) โดยมีค่าเฉลี่ยอยู่ที่ 13.40 คะแนน และมัธยฐานอยู่ที่ 13 คะแนน แสดงให้เห็นถึงผลสัมฤทธิ์ของการเรียนรู้ที่มีประสิทธิภาพภายหลังการเข้าใช้งานแพลตฟอร์มชุมชนความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ เมื่อพิจารณาจากเกณฑ์ผ่านที่กำหนดไว้ที่ 12 คะแนนขึ้นไป (คิดเป็น 80% ของคะแนนเต็ม) พบว่ามีผู้ทำแบบทดสอบ จำนวน 50 คนจาก 52 คน (คิดเป็นร้อยละ 96.15) ที่ผ่านเกณฑ์ดังกล่าว สะท้อนให้เห็นว่าแพลตฟอร์มสามารถถ่ายทอดองค์ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ให้กับบุคลากรภายในองค์กรได้อย่างมีประสิทธิภาพ



ภาพที่ 4-4 สรุปผลการทำแบบทดสอบ

4.4.4 การวิเคราะห์การกระจายความถี่ของผลคะแนนแบบทดสอบ

การวิเคราะห์การกระจายตัวของคะแนนแบบทดสอบช่วยให้เห็นภาพรวมของลักษณะการเรียนรู้ของกลุ่มเป้าหมายได้อย่างเป็นระบบ โดยสามารถสรุปผลการแจกแจงความถี่ของคะแนนได้ดังตารางต่อไปนี้

ตารางที่ 4-2 การกระจายความถี่ของผลคะแนนแบบทดสอบ

คะแนน	จำนวน	ร้อยละ
11	2 คน	3.85
12	10 คน	19.23
13	16 คน	30.77
14	13 คน	25.00
15	11 คน	21.15

จากตารางแสดงให้เห็นว่ากลุ่มคะแนนที่มีความถี่สูงสุด คือ 13 คะแนน ซึ่งมีจำนวนผู้ได้คะแนนสูงถึง 16 คน หรือคิดเป็นร้อยละ 30.77 ของผู้ทำแบบทดสอบทั้งหมด รองลงมาคือกลุ่มที่ได้ 14 คะแนน (ร้อยละ 25) และ 15 คะแนน (ร้อยละ 21.15) ตามลำดับ ทั้งนี้ คะแนนในช่วง 13 - 15 คะแนน ถือเป็นระดับคะแนนสูง โดยคิดเป็นสัดส่วนรวมกันร้อยละ 77 ของกลุ่มเป้าหมายทั้งหมด ซึ่งสะท้อนถึงแนวโน้มของการเรียนรู้ที่มีประสิทธิภาพ

นอกจากนี้ เมื่อพิจารณาจากเกณฑ์ผ่านขั้นต่ำที่กำหนดไว้ที่ 12 คะแนนขึ้นไป (ร้อยละ 80 ของคะแนนเต็ม) พบว่ามีผู้ทำแบบทดสอบ 50 คนจาก 52 คน (คิดเป็นร้อยละ 96.15) ที่ผ่านเกณฑ์ดังกล่าว แสดงให้เห็นว่าเนื้อหาในแพลตฟอร์มชุมชนมีความเหมาะสมต่อการเรียนรู้ และสามารถเสริมสร้างความรู้ความเข้าใจในหัวข้อด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

ผลการวิเคราะห์การกระจายความถี่ของคะแนนแบบทดสอบดังกล่าว ยังชี้ให้เห็นว่าไม่มีผู้ทำแบบทดสอบใดได้คะแนนในระดับต่ำอย่างชัดเจน (เช่น ต่ำกว่า 10 คะแนน หรือร้อยละ 60 ของคะแนนเต็ม) ซึ่งเป็นข้อบ่งชี้ว่าผู้ทำแบบทดสอบมีความรู้พื้นฐานเพียงพอ และสามารถเข้าใจเนื้อหาผ่านการเรียนรู้จากแพลตฟอร์มชุมชนได้ ทั้งในด้านทฤษฎีและสถานการณ์จำลองในบริบทการทำงานจริง

4.4.5 การอภิปรายผลการประเมินระดับความรู้

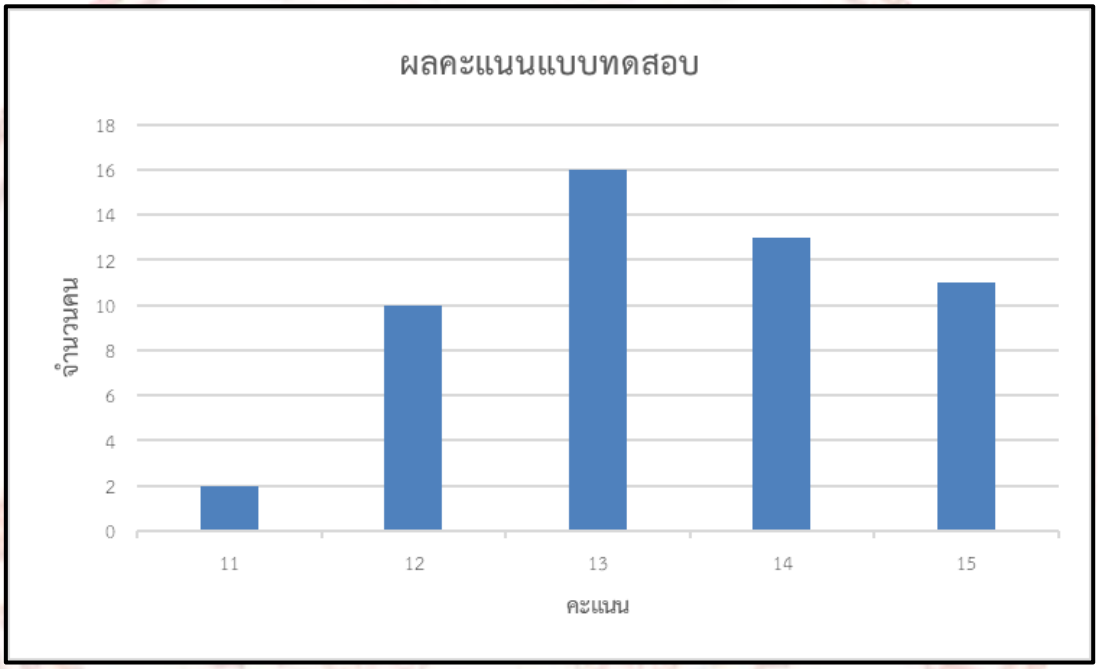
ผลการประเมินแบบทดสอบแสดงให้เห็นว่าบุคลากรภายในองค์กรมีระดับความรู้และความเข้าใจในประเด็นด้านความมั่นคงปลอดภัยทางไซเบอร์ใน**ระดับดีถึงดีมาก** โดยมีการกระจายของคะแนนแบบทดสอบในลักษณะที่กระจุกตัวอยู่ใกล้เคียงกับค่าเฉลี่ยและมัธยฐานของคะแนนทั้งหมด ซึ่งบ่งชี้ว่าผู้ทำแบบทดสอบส่วนใหญ่มีความเข้าใจในสาระสำคัญของเนื้อหา และสามารถถ่ายทอดความรู้ไปสู่การรับรู้และพฤติกรรมที่เหมาะสมได้อย่างมีประสิทธิภาพ

นอกจากนี้ เมื่อพิจารณาจากเกณฑ์ผ่านที่กำหนดไว้ที่ 12 คะแนน (คิดเป็นร้อยละ 80 ของคะแนนเต็ม) พบว่ามีผู้ทำแบบทดสอบผ่านเกณฑ์ ถึงร้อยละ 96.15 ของผู้ทำแบบทดสอบทั้งหมด สะท้อนให้เห็นว่าบุคลากรสามารถบรรลุจุดประสงค์เชิงพฤติกรรมตามที่แพลตฟอร์มได้ออกแบบไว้ ทั้งนี้ ยังไม่พบบุคลากรรายใดที่มีคะแนนต่ำในระดับวิกฤต ซึ่งเป็นข้อบ่งชี้ถึงความเหมาะสมของโครงสร้างเนื้อหา ระดับความยากของแบบทดสอบ และกลยุทธ์การเรียนรู้ที่ใช้ภายในแพลตฟอร์ม

ข้อสอบที่ใช้ในการประเมินถูกออกแบบให้มุ่งเน้นการประยุกต์ใช้ความรู้ในบริบทจริง โดยเน้นคำถามที่สอดคล้องกับสถานการณ์ที่อาจพบเจอในสภาพแวดล้อมขององค์กร เช่น การจำแนกอีเมลฟิชชิ่ง การวิเคราะห์พฤติกรรมเสี่ยงในการใช้เทคโนโลยีสารสนเทศ และการเลือกใช้มาตรการป้องกันเบื้องต้นที่เหมาะสม

ผลลัพธ์จากแบบทดสอบจึงสามารถนำมาใช้เป็นดัชนีชี้วัดเบื้องต้นของประสิทธิผลการเรียนรู้ผ่านแพลตฟอร์มชุมชน และเป็นข้อมูลสำคัญในการประเมินผลกระทบในระดับองค์รวมของการพัฒนาแพลตฟอร์มชุมชน โดยเฉพาะในด้านการส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ การเปลี่ยนแปลงพฤติกรรม และการสร้างการมีส่วนร่วมของบุคลากรอย่างต่อเนื่อง

นอกจากนี้ ผลการวิเคราะห์เชิงอธิบายยังช่วยให้ผู้วิจัยสามารถกำหนดแนวทางในการปรับปรุงและพัฒนาเนื้อหา กิจกรรม และรูปแบบการเรียนรู้ในอนาคตให้สอดคล้องกับระดับความเข้าใจของบุคลากร และตอบสนองต่อความต้องการที่ลึกซึ้งมากยิ่งขึ้น เช่น การพัฒนาแบบทดสอบระดับสูงที่เน้นการตัดสินใจในเหตุการณ์ซับซ้อน หรือการใช้สถานการณ์จำลองแบบ Interactive Simulation



ภาพที่ 4-5 การกระจายความถี่ของผลคะแนนแบบทดสอบ

4.5 ผลการประเมินความพึงพอใจของผู้ใช้งาน

การประเมินผลในส่วนนี้มีวัตถุประสงค์เพื่อวัดระดับความพึงพอใจของบุคลากรภายในองค์กรที่ได้เข้ามาใช้งานแพลตฟอร์มชุมชนความมั่นคงปลอดภัยไซเบอร์ ซึ่งพัฒนาขึ้นบนซอฟต์แวร์ Microsoft OneNote โดยมีเป้าหมายเพื่อส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ในรูปแบบของการเรียนรู้ร่วมกันภายในองค์กร ผ่านการมีส่วนร่วมของผู้ใช้งานจากหลากหลายหน่วยงาน

แบบสอบถามที่ใช้ในการประเมินถูกออกแบบให้ครอบคลุมทั้งในมิติของการใช้งาน การเรียนรู้ และผลกระทบต่อพฤติกรรม โดยแบ่งออกเป็น 5 ส่วน ได้แก่

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ส่วนที่ 2 ความพึงพอใจต่อการใช้งานแพลตฟอร์ม (User Experience)

ส่วนที่ 3 ความพึงพอใจต่อเนื้อหาและกิจกรรมในแพลตฟอร์ม (Activities)

ส่วนที่ 4 ผลกระทบจากการใช้งานแพลตฟอร์ม (Outcomes & Impact)

ส่วนที่ 5 ข้อเสนอแนะและความคิดเห็นเพิ่มเติม

โดยผลการประเมินนำเสนอในรูปแบบของจำนวน และร้อยละ เพื่อสะท้อนระดับความพึงพอใจในแต่ละด้าน พร้อมการวิเคราะห์เชิงพรรณนาเพื่อเสริมความเข้าใจในภาพรวมของการใช้งานแพลตฟอร์ม

ทั้งนี้ ข้อมูลที่ได้รับจะถูกนำมาใช้เพื่อวัตถุประสงค์ทางวิชาการเท่านั้น โดยไม่มีการเปิดเผยชื่อหรือข้อมูลส่วนบุคคลใด ๆ ที่สามารถระบุตัวตนของผู้ตอบแบบสอบถามได้ เพื่อรักษาความลับและจริยธรรมในการค้นคว้าอิสระตามหลักวิชาการ

4.5.1 ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

จากบุคลากรทั้งหมดขององค์กรจำนวน 109 คน มีผู้เข้าร่วมตอบแบบสอบถามความพึงพอใจต่อการใช้งานแพลตฟอร์มชุมชนความมั่นคงปลอดภัยไซเบอร์จำนวน 52 คน คิดเป็น ร้อยละ 47.71 ของจำนวนบุคลากรทั้งหมด โดยผู้ตอบแบบสอบถามดังกล่าวมาจากฝ่ายงานภายในองค์กรจำนวน 16 ฝ่ายงาน ครอบคลุมทุกฝ่ายงาน ซึ่งสะท้อนให้เห็นถึงความหลากหลายและเป็นตัวแทนที่เหมาะสมของกลุ่มเป้าหมายที่มีประสบการณ์ตรงในการใช้งานแพลตฟอร์ม

การมีส่วนร่วมจากทุกฝ่ายงานส่งผลให้ข้อมูลที่ได้รับจากการประเมินมีความครอบคลุมและสามารถสะท้อนบริบทของการใช้งานจริงในระดับฝ่ายงานได้อย่างหลากหลาย ทั้งนี้ ข้อมูลทั้งหมดที่ได้รับจะถูกนำมาใช้เพื่อวัตถุประสงค์ทางวิชาการ โดยไม่มีการเปิดเผยชื่อหรือข้อมูลส่วนบุคคลใด ๆ ที่สามารถระบุตัวตนได้ เพื่อรักษาความลับและจริยธรรมในการค้นคว้าอิสระ

ตารางที่ 4-3 จำนวนและร้อยละของบุคลากรแต่ละฝ่ายงานที่ร่วมตอบแบบสอบถามความพึงพอใจ

ลำดับ	ฝ่ายงาน	จำนวน (n=52)	ร้อยละ
1	ฝ่ายอำนวยการกลาง	10	19.23
2	ฝ่ายการคลัง	3	5.77
3	ฝ่ายทรัพยากรบุคคล	3	5.77
4	ฝ่ายยุทธศาสตร์องค์กร	4	7.69
5	ฝ่ายเทคโนโลยีดิจิทัล	2	3.85
6	ฝ่ายกิจการต่างประเทศ	3	5.77
7	ฝ่ายส่งเสริมการแข่งขันทางการค้า	2	3.85
8	สถาบันการแข่งขันทางการค้า	2	3.85
9	ฝ่ายกำกับดูแลการรวมธุรกิจ	3	5.77
10	ฝ่ายโครงสร้างตลาดและระบบธุรกิจ	2	3.85
11	ฝ่ายวิจัยเศรษฐกิจและการแข่งขัน	2	3.85
12	ฝ่ายแสวงหาข้อเท็จจริง	3	5.77
13	ฝ่ายสอบสวน	5	9.62
14	ฝ่ายกฎหมายและพัฒนาการบังคับใช้กฎหมาย	2	3.85
15	ฝ่ายบริหารงานคดี	4	7.69
16	ฝ่ายตรวจสอบภายใน	2	3.85

4.5.2 ส่วนที่ 2 ความพึงพอใจต่อการใช้งานแพลตฟอร์ม (User Experience)

การประเมินความพึงพอใจต่อการใช้งานแพลตฟอร์มมุ่งเน้นไปที่ประสบการณ์ของผู้ใช้งานในการเข้าถึงและใช้งานแพลตฟอร์มชุมชนความมั่นคงปลอดภัยไซเบอร์ โดยประเมินผ่าน 4 ประเด็นหลัก ได้แก่ แพลตฟอร์มใช้งานง่าย ไม่ซับซ้อน การเข้าถึงเนื้อหาทำได้สะดวก รวดเร็ว ความเร็วและความเสถียรเพียงพอต่อการใช้งาน และการจัดหมวดหมู่และการนำทางเนื้อหาชัดเจน

จากผลการประเมินพบว่า ผู้ตอบแบบสอบถามส่วนใหญ่มีความพึงพอใจในระดับ “มาก” และ “มากที่สุด” ในทุกหัวข้อ โดยเฉพาะหัวข้อ “แพลตฟอร์มใช้งานง่าย ไม่ซับซ้อน” ที่มีผู้ตอบในระดับ “มาก” และ “มากที่สุด” รวมกันถึงร้อยละ 76.92 และหัวข้อ “การเข้าถึงเนื้อหาทำได้สะดวก รวดเร็ว” ที่รวมแล้วคิดเป็นร้อยละ 78.84

นอกจากนี้ ไม่พบผู้ตอบแบบสอบถามที่ประเมินความพึงพอใจในระดับ “น้อย” หรือ “น้อยที่สุด” ในทุกหัวข้อของการประเมิน สะท้อนถึงความสามารถของแพลตฟอร์มในการออกแบบให้รองรับประสบการณ์ผู้ใช้งานได้อย่างเหมาะสม ทั้งในด้านการเข้าถึง ความเสถียร และการใช้งานโดยรวม

ผลการประเมินในส่วนนี้จึงแสดงให้เห็นว่าแพลตฟอร์มมีศักยภาพในการใช้งานจริง และสามารถสนับสนุนการเรียนรู้ในบริบทขององค์กรได้อย่างมีประสิทธิภาพ

ตารางที่ 4-4 ความพึงพอใจต่อการใช้งานแพลตฟอร์ม (User Experience) (n=52)

หัวข้อ	ความพึงพอใจ	จำนวน	ร้อยละ
แพลตฟอร์มใช้งานง่าย ไม่ซับซ้อน	มากที่สุด	8	15.38
	มาก	32	61.54
	ปานกลาง	12	23.08
	น้อย	0	0
	น้อยที่สุด	0	0
การเข้าถึงเนื้อหาทำได้สะดวก รวดเร็ว	มากที่สุด	7	13.46
	มาก	34	65.38
	ปานกลาง	11	21.15
	น้อย	0	0
	น้อยที่สุด	0	0
ความเร็วและความเสถียรเพียงพอต่อการใช้งาน	มากที่สุด	9	17.31
	มาก	29	55.77
	ปานกลาง	14	26.92
	น้อย	0	0
	น้อยที่สุด	0	0
การจัดหมวดหมู่และการนำทางเนื้อหาชัดเจน	มากที่สุด	11	21.15
	มาก	26	50.00

ตารางที่ 4-4 (ต่อ)

หัวข้อ	ความพึงพอใจ	จำนวน	ร้อยละ
	ปานกลาง	15	28.85
	น้อย	0	0
	น้อยที่สุด	0	0

4.5.3 ส่วนที่ 3 ความพึงพอใจต่อเนื้อหาและกิจกรรมในแพลตฟอร์ม (Activities)

การประเมินความพึงพอใจในด้านเนื้อหาและกิจกรรมภายในแพลตฟอร์มชุมชนความมั่นคงปลอดภัยไซเบอร์มีเป้าหมายเพื่อวัดความเหมาะสม ความหลากหลาย และความสอดคล้องของเนื้อหากับบริบทความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงการสร้างแรงจูงใจในการเรียนรู้ผ่านกิจกรรมที่ออกแบบไว้ในแพลตฟอร์ม

ผลการประเมินพบว่า ผู้ตอบแบบสอบถามส่วนใหญ่มีความพึงพอใจในระดับ “มาก” และ “มากที่สุด” ในทุกหัวข้อ โดยเฉพาะในหัวข้อ “กิจกรรม เช่น แบบฝึกหัด / Quiz / แชร์ความรู้ สร้างความสนใจ” มีผู้ตอบในระดับ “มาก” และ “มากที่สุด” รวมกันถึง ร้อยละ 76.92 แสดงให้เห็นว่ากิจกรรมที่จัดทำในแพลตฟอร์มสามารถสร้างความน่าสนใจและกระตุ้นการมีส่วนร่วมของผู้ใช้งานได้อย่างมีประสิทธิภาพ

ขณะเดียวกันเนื้อหาเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในภาพรวม ได้รับการประเมินว่ามีประโยชน์ ครอบคลุมหัวข้อสำคัญ และมีความทันสมัย สอดคล้องกับสถานการณ์ภัยคุกคามที่เกิดขึ้นจริง โดยไม่มีผู้ตอบประเมินในระดับ “น้อย” หรือ “น้อยที่สุด”

ข้อมูลจากผลการประเมินดังกล่าวสะท้อนว่าแพลตฟอร์มสามารถจัดเตรียมเนื้อหาและกิจกรรมได้อย่างเหมาะสมกับความต้องการของบุคลากร และสอดคล้องกับแนวโน้มภัยไซเบอร์ที่องค์กร

ตารางที่ 4-5 ความพึงพอใจต่อเนื้อหาและกิจกรรมในแพลตฟอร์ม (Activities) (n=52)

หัวข้อ	ความพึงพอใจ	จำนวน	ร้อยละ
เนื้อหาเกี่ยวกับความปลอดภัยไซเบอร์มีประโยชน์ต่อการทำงานจริง	มากที่สุด	9	17.31
	มาก	27	51.92
	ปานกลาง	16	30.77
	น้อย	0	0
	น้อยที่สุด	0	0
กิจกรรม เช่น แบบฝึกหัด / Quiz / แชร์ความรู้ สร้างความสนใจ	มากที่สุด	8	15.38
	มาก	32	61.54
	ปานกลาง	12	23.08
	น้อย	0	0
	น้อยที่สุด	0	0

ตารางที่ 4-5 (ต่อ)

หัวข้อ	ความพึงพอใจ	จำนวน	ร้อยละ
เนื้อหาครอบคลุมหัวข้อสำคัญด้านความมั่นคงปลอดภัยไซเบอร์	มากที่สุด	10	19.23
	มาก	28	53.85
	ปานกลาง	14	26.92
	น้อย	0	0
	น้อยที่สุด	0	0
เนื้อหาทันสมัย สอดคล้องกับสถานการณ์และภัยคุกคามที่เกิดขึ้นจริง	มากที่สุด	10	19.23
	มาก	29	55.77
	ปานกลาง	13	25.00
	น้อย	0	0
	น้อยที่สุด	0	0

4.5.4 ส่วนที่ 4 ผลกระทบจากการใช้งานแพลตฟอร์ม (Outcomes & Impact)

การประเมินผลในส่วนนี้มุ่งเน้นไปที่การพิจารณาผลลัพธ์ที่เกิดขึ้นกับผู้ใช้งานหลังจากเข้าร่วมใช้งานแพลตฟอร์มชุมชนความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะในด้านความรู้ ทัศนคติ และพฤติกรรมที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ในบริบทขององค์กร

จากผลการประเมิน พบว่าผู้ใช้งานส่วนใหญ่มีความรู้และทักษะเพิ่มขึ้นจากการเรียนรู้ผ่านแพลตฟอร์ม โดยในหัวข้อ “ท่านมีความรู้ด้านความปลอดภัยไซเบอร์เพิ่มขึ้นจากการใช้งานแพลตฟอร์ม” มีผู้ตอบในระดับ “มากที่สุด” และ “มาก” รวมกันถึง ร้อยละ 80.77

นอกจากนี้ ผู้ใช้งานยังสามารถนำความรู้ที่ได้รับไปประยุกต์ใช้จริงในงาน เช่น การปรับพฤติกรรมการใช้งานระบบ IT ให้ปลอดภัยยิ่งขึ้น และการรู้เท่าทันภัยไซเบอร์จากการมีส่วนร่วมในแพลตฟอร์มชุมชน โดยไม่มีผู้ประเมินอยู่ในระดับ “น้อย” หรือ “น้อยที่สุด”

ผลลัพธ์ที่ได้สะท้อนว่าแพลตฟอร์มไม่เพียงแต่ให้ข้อมูลความรู้เชิงทฤษฎีเท่านั้น แต่ยังสามารถส่งผลต่อการเปลี่ยนแปลงพฤติกรรมของผู้ใช้งานได้ในทางปฏิบัติ ซึ่งเป็นเป้าหมายสำคัญของการส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ในองค์กร

ตารางที่ 4-6 ผลกระทบจากการใช้งานแพลตฟอร์ม (Outcomes & Impact) (n=52)

หัวข้อ	ความพึงพอใจ	จำนวน	ร้อยละ
ท่านมีความรู้ด้านความปลอดภัยไซเบอร์เพิ่มขึ้นจากการใช้งานแพลตฟอร์ม	มากที่สุด	11	21.15
	มาก	31	59.62
	ปานกลาง	10	19.23
	น้อย	0	0
	น้อยที่สุด	0	0

ตารางที่ 4-6 (ต่อ)

หัวข้อ	ความพึงพอใจ	จำนวน	ร้อยละ
ท่านสามารถนำความรู้ไปปรับปรุงพฤติกรรมการใช้งานระบบ IT ให้มีความปลอดภัยมากยิ่งขึ้น	มากที่สุด	10	19.23
	มาก	30	57.69
	ปานกลาง	12	23.08
	น้อย	0	0
	น้อยที่สุด	0	0
ท่านสามารถนำความรู้จากแพลตฟอร์มไปประยุกต์ใช้ในงานจริง	มากที่สุด	9	17.31
	มาก	28	53.85
	ปานกลาง	15	28.85
	น้อย	0	0
	น้อยที่สุด	0	0
การเข้าร่วมในชุมชนช่วยให้รู้ทันภัยไซเบอร์ได้มากขึ้น	มากที่สุด	9	17.31
	มาก	28	53.85
	ปานกลาง	15	28.85
	น้อย	0	0
	น้อยที่สุด	0	0

4.5.5 ส่วนที่ 5 ข้อเสนอแนะและความคิดเห็นเพิ่มเติม

แบบสอบถามในส่วนนี้เปิดโอกาสให้ผู้ใช้งานสามารถแสดงความคิดเห็นและข้อเสนอแนะเพิ่มเติมเกี่ยวกับแพลตฟอร์มชุมชนความมั่นคงปลอดภัยไซเบอร์ ทั้งในด้านเนื้อหา กิจกรรม ฟีเจอร์ และการนำเสนอ เพื่อให้สะท้อนถึงความรู้สึกของผู้ใช้งานต่อการเรียนรู้ผ่านแพลตฟอร์มอย่างอิสระ

จากการรวบรวมความคิดเห็นของผู้ตอบแบบสอบถาม พบว่าข้อเสนอแนะสามารถจำแนกได้เป็น 3 หมวดหลัก ได้แก่

4.5.5.1 จุดเด่นของแพลตฟอร์มที่ท่านชื่นชอบ

4.5.5.1.1 มีภัยไซเบอร์ในแบบต่าง ๆ ให้เรียนรู้ เข้าใจง่าย

4.5.5.1.2 เนื้อหาย่อยมาให้แล้ว ไม่ต้องอ่านเยอะ

4.5.5.1.3 ครอบคลุมดี เป็นศูนย์รวมที่ดีของความรู้ด้านไซเบอร์

4.5.5.1.4 มีนโยบายสั้น ๆ ไม่ต้องอ่านเล่มจริง กำลังดี

สรุป : ผู้ใช้งานส่วนใหญ่มองว่าแพลตฟอร์มมีจุดแข็งในด้านความเข้าใจง่าย การจัดการเนื้อหาอย่างกระชับ และมีลักษณะเป็นศูนย์กลางของความรู้ที่เข้าถึงได้สะดวก

4.5.5.2 ข้อเสนอแนะเพื่อพัฒนาแพลตฟอร์ม / เนื้อหา / กิจกรรม

4.5.5.2.1 ควรเพิ่มเนื้อหาเกี่ยวกับภัยคุกคามใหม่ ๆ อย่างต่อเนื่อง

4.5.5.2.2 ควรเพิ่มแบบทดสอบให้มากขึ้น และมีหลายระดับความยากง่าย

4.5.5.2.3 อยากให้มีข้อมูลอัปเดตเรื่อย ๆ โดยเฉพาะภัยไซเบอร์จากแอปพลิเคชันหรือช่องทางใหม่

สรุป : ข้อเสนอส่วนใหญ่เน้นที่ความต่อเนื่องของการอัปเดตเนื้อหา การเพิ่มความหลากหลายของแบบทดสอบ และการสร้างแรงจูงใจผ่านกิจกรรมที่มีลักษณะโต้ตอบ

4.5.5.3 เนื้อหา หรือฟีเจอร์ที่ท่านอยากให้เพิ่มเติมในอนาคต

4.5.5.3.1 ต้องการแบบทดสอบที่แตกต่าง เช่น Crossword, Matching, Drag & Drop

4.5.5.3.2 อยากให้รวมเนื้อหาไว้ที่เดียว โหลดหรือค้นหาได้ง่าย

4.5.5.3.3 ควรมีส่วนที่ให้ผู้ใช้งานแชร์ประสบการณ์การเผชิญภัยไซเบอร์จริง

สรุป : ผู้ใช้งานแสดงความสนใจในเรื่องของการเข้าถึงเนื้อหาได้สะดวก และรูปแบบการเรียนรู้ที่หลากหลาย รวมถึงการมีปฏิสัมพันธ์ร่วมกับชุมชนผู้ใช้งานคนอื่น ๆ

บทสรุป : ความคิดเห็นและข้อเสนอแนะที่ได้รับจากผู้ใช้งาน ถือเป็นข้อมูลสำคัญในการพัฒนาแพลตฟอร์มให้มีประสิทธิภาพยิ่งขึ้นในอนาคต โดยเฉพาะการเสริมสร้างการมีส่วนร่วม การปรับปรุงเนื้อหาให้ทันสมัย และการออกแบบกิจกรรมให้ดึงดูดและตอบโจทย์ผู้ใช้งานในหลากหลายบริบทขององค์กร

4.6 สรุปผลเบื้องต้นจากการใช้งานแพลตฟอร์ม

จากการดำเนินการทดลองใช้งานแพลตฟอร์มชุมชนความมั่นคงปลอดภัยไซเบอร์ที่พัฒนาขึ้นบน Microsoft OneNote พบว่า แพลตฟอร์มสามารถตอบสนองต่อวัตถุประสงค์หลักของการค้นคว้าอิสระได้อย่างชัดเจน โดยเฉพาะใน 3 ด้านสำคัญ ได้แก่ (1) การส่งเสริมการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในลักษณะที่เป็นมิตรและเข้าถึงง่าย (2) การกระตุ้นให้เกิดการเปลี่ยนแปลงพฤติกรรมในการใช้งานเทคโนโลยีสารสนเทศให้มีความระมัดระวังและปลอดภัยมากขึ้น และ (3) การสร้างพื้นที่กลางสำหรับการแลกเปลี่ยนประสบการณ์ ความรู้ และความคิดเห็นเกี่ยวกับประเด็นด้านความมั่นคงปลอดภัยทางไซเบอร์ระหว่างบุคลากรในองค์กร ซึ่งสอดคล้องกับแนวคิดเรื่อง “ชุมชนแห่งการเรียนรู้” (Community of Practice) ที่เน้นการเรียนรู้ร่วมกันผ่านการปฏิบัติจริงและการมีส่วนร่วม

การวิเคราะห์ผลการใช้งานในเบื้องต้นชี้ให้เห็นว่า บุคลากรมีระดับความเข้าใจในประเด็นภัยคุกคามทางไซเบอร์ เช่น การฟิชชิ่ง มัลแวร์ และการใช้เทคโนโลยีอย่างไม่ปลอดภัย เพิ่มขึ้นอย่างมีนัยสำคัญหลังจากเข้าร่วมเรียนรู้ผ่านแพลตฟอร์ม โดยมีผลการประเมินจากแบบทดสอบวัดความเข้าใจหลังการใช้งาน รวมถึงข้อมูลเชิงปริมาณจากแบบสอบถามที่แสดงถึงการเปลี่ยนแปลงพฤติกรรมการใช้งานจริงในทิศทางที่ดีขึ้น

ทั้งนี้ ปัจจัยสำคัญที่ส่งผลต่อประสิทธิภาพของการเรียนรู้บนแพลตฟอร์ม ได้แก่ การออกแบบเนื้อหาที่มีความหลากหลายทั้งในรูปแบบข้อความ กราฟิก คลิปวิดีโอ และแบบทดสอบออนไลน์ ซึ่งครอบคลุมสถานการณ์จริงในบริบทขององค์กร เช่น กรณีการโจมตีแบบฟิชชิ่งผ่านอีเมลภายในการใช้ USB drive ที่ไม่ปลอดภัย หรือการแชร์รหัสผ่านระหว่างบุคลากร โดยการเรียนรู้

ผ่านสถานการณ์เหล่านี้สามารถเชื่อมโยงกับประสบการณ์ของผู้ใช้งานได้อย่างเป็นระบบ ช่วยให้การรับรู้ไม่จำกัดเพียงในเชิงทฤษฎี แต่เกิดความเข้าใจในระดับปฏิบัติ (practical understanding)

นอกจากนี้ ยังพบว่า บุคลากรส่วนใหญ่มีพฤติกรรมการใช้งาน Microsoft 365 เป็นประจำ โดยเฉพาะ OneNote ซึ่งถือเป็นเครื่องมือที่ได้รับการยอมรับในด้านความสะดวก ความคล่องตัว และความสามารถในการจัดการความรู้ (Knowledge Management) ภายในองค์กร คุณลักษณะเด่นของ OneNote เช่น การเข้าถึงจากอุปกรณ์ที่หลากหลาย การแชร์เนื้อหาแบบเรียลไทม์ และการผสานรวมกับแอปพลิเคชันอื่นในระบบ Microsoft 365 (เช่น Teams, Outlook, Forms) ทำให้การพัฒนาแพลตฟอร์มชุมชนบน OneNote สามารถตอบสนองต่อพฤติกรรมการทำงานของผู้ใช้งานจริงได้อย่างเหมาะสม ทั้งในมิติของการสื่อสารภายใน การเรียนรู้ร่วมกัน และการเก็บรักษาองค์ความรู้เชิงโครงสร้าง

กล่าวโดยสรุป แพลตฟอร์มชุมชนความมั่นคงปลอดภัยทางไซเบอร์ที่พัฒนาขึ้น ไม่เพียงแต่เป็นเครื่องมือเพื่อเสริมสร้างวัฒนธรรมด้านความปลอดภัยในระดับเบื้องต้น หากแต่ยังมีศักยภาพในการขยายผลและต่อยอดเป็นส่วนหนึ่งของกลยุทธ์การบริหารจัดการความรู้ด้านความมั่นคงปลอดภัยในระดับองค์กรอย่างยั่งยืน โดยสามารถทำหน้าที่เป็นฐานข้อมูลกลาง (Knowledge Hub) สำหรับการรวบรวม ประมวลผล และเผยแพร่ความรู้ด้านภัยคุกคามทางไซเบอร์ และแนวทางการป้องกันที่เหมาะสมกับบริบทขององค์กร อันจะเป็นรากฐานสำคัญในการพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ที่ยั่งยืนและยืดหยุ่นต่อการเปลี่ยนแปลงในอนาคต

บทที่ 5
สรุปผล อภิปรายผล และข้อเสนอแนะ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อพัฒนาแพลตฟอร์มชุมชนโดยใช้ Microsoft OneNote เป็นเครื่องมือหลักในการเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กร โดยมุ่งเน้นให้บุคลากรสามารถเข้าถึงองค์ความรู้ด้านไซเบอร์ได้อย่างสะดวก เรียนรู้จากสถานการณ์จริง และแลกเปลี่ยนประสบการณ์ร่วมกันในรูปแบบของชุมชนออนไลน์ ซึ่งในการดำเนินการวิจัยได้มีการออกแบบและจัดทำเนื้อหาภายในแพลตฟอร์มให้ครอบคลุมหัวข้อสำคัญ เช่น ความรู้พื้นฐานด้านความมั่นคงปลอดภัย ฟิชชิ่ง กรณีศึกษา การแจ้งเตือนภัย และกิจกรรมแบบทดสอบ โดยทดลองใช้งานจริงกับกลุ่มเป้าหมายจำนวน 52 คนจากทุกฝ่ายงานในองค์กร ผลการวิเคราะห์ข้อมูลจากแบบสอบถาม ความพึงพอใจ และผลการเรียนรู้พบว่า แพลตฟอร์มชุมชนที่พัฒนาขึ้นสามารถส่งเสริมทั้งความรู้ ทัศนคติ และพฤติกรรมของผู้ใช้งานได้อย่างมีนัยสำคัญ อีกทั้งยังช่วยกระตุ้นการมีส่วนร่วมภายในองค์กรในประเด็นด้านความปลอดภัยไซเบอร์ได้อย่างเป็นรูปธรรม พบข้อสรุปและข้อเสนอแนะ ดังนี้

5.1 สรุปผลการวิจัย

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อพัฒนาแพลตฟอร์มชุมชนโดยใช้ Microsoft OneNote เป็นเครื่องมือหลักในการเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กร โดยเน้นให้บุคลากรสามารถเข้าถึงองค์ความรู้ด้านไซเบอร์ได้อย่างสะดวก เรียนรู้จากสถานการณ์จริง และแลกเปลี่ยนประสบการณ์ร่วมกันในรูปแบบของชุมชนออนไลน์

ผลการดำเนินงานพบว่า แพลตฟอร์มชุมชนที่พัฒนาขึ้นสามารถตอบสนองต่อวัตถุประสงค์ของการวิจัยได้อย่างครบถ้วน ทั้งในด้านเนื้อหาที่หลากหลาย ครอบคลุมหัวข้อสำคัญด้านความมั่นคงปลอดภัยไซเบอร์ เช่น ฟิชชิ่ง การแจ้งเตือนภัย และกรณีศึกษา ตลอดจนสามารถบูรณาการการใช้งานร่วมกับ Microsoft Forms และ Microsoft Teams เพื่อสนับสนุนการมีส่วนร่วมของผู้ใช้งานได้อย่างมีประสิทธิภาพ

จากผลการประเมิน พบว่าผู้ใช้งานมีความพึงพอใจต่อแพลตฟอร์มในระดับมาก และมีผลสัมฤทธิ์ทางการเรียนรู้สูง โดยเฉพาะในด้านความเข้าใจภัยคุกคามไซเบอร์ ทัศนคติที่ดีขึ้นต่อการป้องกันความเสี่ยง และพฤติกรรมที่แสดงถึงความตระหนักรู้ด้านความปลอดภัยมากยิ่งขึ้น ซึ่งแสดงให้เห็นว่าแพลตฟอร์มชุมชนดังกล่าวมีศักยภาพในการเป็นกลไกสำคัญในการส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างยั่งยืน

5.2 อภิปรายผล

ผลการวิจัยสอดคล้องกับแนวคิดของ Warasart และ Piriyasurawong [9] ที่ชี้ให้เห็นว่าชุมชนแห่งการเรียนรู้ที่มีลักษณะเชิงกิจกรรมหรือเกม (Gamified Learning Communities) สามารถเพิ่มแรงจูงใจและการมีส่วนร่วมของผู้เรียนได้อย่างมีนัยสำคัญ

การสร้างพื้นที่การเรียนรู้ที่เปิดกว้างผ่าน OneNote และการแลกเปลี่ยนความรู้ใน Microsoft Teams ยังสนับสนุนแนวคิดของ Yucel et al. [21] ที่กล่าวถึงความสำคัญของ “Community-driven Threat Awareness” ในฐานะรากฐานของวัฒนธรรมความมั่นคงปลอดภัยที่ยั่งยืนภายในองค์กร

นอกจากนี้ การใช้แบบทดสอบที่มีคำอธิบายเสริมและกิจกรรมที่ผู้ใช้งานสามารถสะท้อนความคิดด้วยตนเอง ถือเป็นการส่งเสริมการเรียนรู้แบบ Active Learning และ Reflective Learning ซึ่งช่วยให้บุคลากรสามารถประเมินตนเอง ปรับเปลี่ยนพฤติกรรม และเรียนรู้ได้ต่อเนื่องโดยไม่ต้องพึ่งการอบรมแบบดั้งเดิมเพียงอย่างเดียว

ข้อเสนอแนะในการพัฒนาต่อยอดแพลตฟอร์มของกลุ่มตัวอย่างที่เข้าร่วมตอบแบบสอบถามสะท้อนให้เห็นระดับความเข้าใจและความสนใจในการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กร ดังนั้น ในอนาคตองค์กรจะต้องมอบหมายทีมงานสำหรับปรับปรุงเนื้อหาด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นปัจจุบัน และสร้างกิจกรรมดึงดูดให้บุคลากรเข้ามาเรียนรู้อย่างต่อเนื่องต่อไป

5.3 ข้อเสนอแนะ

เพื่อยกระดับผลสัมฤทธิ์ของแพลตฟอร์มชุมชนและขยายผลในระดับองค์กร ผู้วิจัยมีข้อเสนอแนะเชิงปฏิบัติ ดังนี้

5.3.1 ขยายการใช้งานแพลตฟอร์ม ไปยังทุกหน่วยงานขององค์กร พร้อมจัดอบรมเบื้องต้นเพื่อแนะนำแนวทางการใช้งาน และปลูกฝังแนวคิดด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างทั่วถึง

5.3.2 แต่งตั้ง “Cybersecurity Champion” ในแต่ละฝ่ายงาน เพื่อเป็นผู้ประสานงาน ส่งเสริมกิจกรรม แลกเปลี่ยนแนวปฏิบัติที่ดี และกระตุ้นให้เกิดการมีส่วนร่วมภายในชุมชน

5.3.3 ปรับปรุงและอัปเดตเนื้อหาอย่างต่อเนื่อง โดยเฉพาะประเด็นภัยคุกคามใหม่ ๆ เช่น ฟิชชิ่งที่ใช้ AI, Deepfake, การโจมตีผ่านแอปปลอม และ BEC (Business Email Compromise)

5.3.4 เพิ่มสื่อและกิจกรรมแบบมีปฏิสัมพันธ์ เช่น วิดีโอประกอบ หรือการตั้งคำถามผ่าน Teams เพื่อสร้างแรงจูงใจและพัฒนาการเรียนรู้แบบมีส่วนร่วม

5.3.5 บูรณาการแพลตฟอร์มเข้ากับแผนพัฒนาทรัพยากรบุคคล โดยใช้เป็นเกณฑ์หนึ่งในการประเมินพฤติกรรมการใช้เทคโนโลยีอย่างปลอดภัยในระดับรายบุคคลหรือฝ่ายงาน

บรรณานุกรม

2. Salama, R., Al-Turjman, F., Bhatla, S., and Yadav, S. P. “Social Engineering Attack Types and Prevention Techniques – A Survey.” Proceedings of the 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN). IEEE. (2023): 817–820.
3. Divakarla, U., and Chandrasekaran, K. “Predicting Phishing Emails and Websites to Fight Cybersecurity Threats Using Machine Learning Algorithms.” Proceedings of the 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON). IEEE. (2023): 1–10.
4. Falkevych, V., and Lisnyak, A. “Internal and External Threats in Cyber Security and Methods for Their Prevention.” Proceedings of the 2023 13th International Conference on Advanced Computer Information Technologies (ACIT). IEEE. (2023): 414–419.
5. Yucel, C., Chalkias, I., Mallis, D., Cetinkaya, D., Henriksen-Bulmer, J., and Cooper, A. “Data Sanitisation and Redaction for Cyber Threat Intelligence Sharing Platforms.” Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE. (2021): 343–347.
6. Tosh, D., Sengupta, S., Kamhoua, C., Kwiat, K., and Martin, A. “An Evolutionary Game-Theoretic Framework for Cyber-Threat Information Sharing.” Proceedings of the 2015 IEEE International Conference on Communications (ICC). IEEE. (2015): 7341–7346.
7. Gupta, S., Singhal, A., and Kapoor, A. “A Literature Survey on Social Engineering Attacks: Phishing Attack.” Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA). IEEE. (2016): 537–540.
8. Khadka, K., Ullah, A. B., Ma, W., and Marroquin, E. M. “A Survey on the Principles of Persuasion as a Social Engineering Strategy in Phishing.” arXiv preprint arXiv:2412.18488. (2024). [Online]. Available: https://arxiv.org/abs/2412.18488., Accessed 10 May. 2025.
9. Warasart, M., and Piriyasurawong, P. “Synthesis of Gamified Social Collaboration via Mesh Community of Practice to Enhance Cybersecurity Awareness.”

Proceedings of the 2022 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON). IEEE. (2022): 359–363.

10. Mansol, N. H., Mohd Alwi, N. H., and Ismail, W. "Managing Organizational Culture Requirement for Business Continuity Management (BCM) Implementation Using Goal-Question-Metric (GQM) Approach." Proceedings of the 2015 IEEE Conference on Open Systems (ICOS). IEEE. (2015): 85–90.
11. Yulianto, S., and Soewito, B. "Ransomware Resilience: Investigating Organizational Security Culture and Its Impact on Cybersecurity Practices Against Ransomware Threats." Proceedings of the 2023 International Conference on Informatics Engineering, Science & Technology (INCITEST). IEEE. (2023): 1–7.
12. Roobini, M. S., Chowdary, M. B., Srinivas, Y., Jayanthi, S., and Srividhya, E. "Cloud Based Threat Intelligence Sharing for Collective Defence." Proceedings of the 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM). IEEE. (2024): 1–6.
13. Muronga, K., Herselman, M., Botha, A., and Da Veiga, A. "An Analysis of Assessment Approaches and Maturity Scales Used for Evaluation of Information Security and Cybersecurity User Awareness and Training Programs: A Scoping Review." Proceedings of the 2019 Conference on Next Generation Computing Applications (NextComp). IEEE. (2019): 1–6.
14. Oroszi, E. D. "Security Awareness Escape Room – A Possible New Method in Improving Security Awareness of Users." Proceedings of the 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). IEEE. (2019): 1–4.
15. Ioannou, M., Stavrou, E., and Bada, M. "Cybersecurity Culture in Computer Security Incident Response Teams: Investigating Difficulties in Communication and Coordination." Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE. (2019): 1–4.

16. Nasir, S. “Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions.” Proceedings of the Cyber Secure Nigeria Conference, Abuja, Nigeria. CSEAN. (2023): 151–160. [Online]. Available: https://cybersecurenigeria.org/wp-content/uploads/2023/08/Paper-18-CSEAN-SMART-Conference-Proceedings-2023.pdf., Accessed 10 May. 2025.
17. Abdullah, A. S., and Mohd, M. “Spear Phishing Simulation in Critical Sector: Telecommunication and Defense Sub-sector.” Proceedings of the 2019 International Conference on Cybersecurity (ICoCSec). IEEE. (2019): 26–31.
18. Schiappa, M., Chantry, G., and Garibay, I. “Cyber Security in a Complex Community: A Social Media Analysis on Common Vulnerabilities and Exposures.” Proceedings of the 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS). IEEE. (2019): 13–20.
19. Cherqi, O., Moukafih, Y., Ghogho, M., and Benbrahim, H. “Enhancing Cyber Threat Identification in Open-Source Intelligence Feeds Through an Improved Semi-Supervised Generative Adversarial Learning Approach with Contrastive Learning.” IEEE Access. IEEE. Vol. 11 (2023): 84440–84452.
20. Trocoso-Pastoriza, J. R., Mermoud, A., Bouyé, R., Marino, F., Bossuat, J.-P., Lenders, V., and Hubaux, J.-P. “Orchestrating Collaborative Cybersecurity: A Secure Framework for Distributed Privacy-Preserving Threat Intelligence Sharing.” arXiv preprint arXiv:2209.02676. (2022). [Online]. Available: https://arxiv.org/abs/2209.02676., Accessed 10 May. 2025.
21. Yucel, C., Chalkias, I., Mallis, D., Cetinkaya, D., Henriksen-Bulmer, J., and Cooper, A. “Data Sanitisation and Redaction for Cyber Threat Intelligence Sharing Platforms.” Proceedings of the 2021 International Conference on Cybersecurity and Protection of Digital Services (Cyber Security). IEEE. (2021): 1–6.

This is Mendeley biography

ภาคผนวก ก

การออกแบบคำถาม และคำตอบของแบบทดสอบความรู้ (Knowledge Test)
ด้านความมั่นคงปลอดภัยไซเบอร์

แบบทดสอบความรู้ (Knowledge Test) ด้านความมั่นคงปลอดภัยไซเบอร์

ข้อที่ 1: ข้อใด ***ไม่ใช่*** หนึ่งในหลัก 3 ประการของไซเบอร์ซีเคียวริตี้ (CIA Triad) ?

A) Confidentiality

B) **Accessibility**

C) Integrity

D) Availability

เหตุผล:

☒ A คือ 3 หลักการสำคัญ: ความลับ (Confidentiality)

☑ **B Accessibility ไม่ใช่หนึ่งในองค์ประกอบของ CIA Triad**

☒ C คือ 3 หลักการสำคัญ: ความถูกต้อง (Integrity)

☒ D คือ 3 หลักการสำคัญ: ความพร้อมใช้งาน (Availability)

ข้อที่ 2: การป้องกันไม่ให้ข้อมูลลูกค้าถูกเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาตเกี่ยวข้องกับหลักการใดของไซเบอร์ซีเคียวริตี้ ?

A) Integrity

B) **Confidentiality**

C) Availability

D) Accountability

เหตุผล:

☒ A เกี่ยวกับการไม่เปลี่ยนแปลงข้อมูล

☑ **B ความลับ (Confidentiality) เน้นการป้องกันไม่ให้ข้อมูลรั่วไหล**

☒ C เกี่ยวกับการเข้าถึงระบบได้ตามเวลา

☒ D ไม่ใช่หลักใน CIA Triad แต่เกี่ยวข้องกับการตรวจสอบย้อนกลับ

ข้อที่ 3: ข้อใดต่อไปนี้เป็นตัวอย่างของ “ภัยคุกคามจากภายใน” (Insider Threat) ?

A) พนักงานดาวน์โหลดมัลแวร์จากเว็บไซต์ต้องสงสัยโดยไม่ได้ตั้งใจ

B) ผู้ใช้งาน Wi-Fi สาธารณะโดนดักข้อมูลจากแฮกเกอร์

C) ผู้ใช้ถูกโทรหลอกให้เปิดเผยรหัส OTP

D) ผู้โจมตีใช้ Botnet เพื่อโจมตีเซิร์ฟเวอร์องค์กร

เหตุผล:

☑ **A ภัยคุกคามจากภายในเกิดจาก “บุคคลภายในองค์กร” ที่มีสิทธิ์เข้าถึงระบบ เช่น พนักงานที่เผลอติดตั้งมัลแวร์**

☒ B เป็น MitM Attack (Man-in-the-Middle Attack) หรือการโจมตีแบบดักกลางทาง

☒ C เป็น Vishing (Voice Phishing) หรือผู้ไม่หวังดีใช้โทรศัพท์หรือข้อความเสียง

☒ D เป็น DDoS Attack (Distributed Denial of Service) หรือการโจมตีทางไซเบอร์ที่ส่งคำขอจำนวนมหาศาลพร้อมกันจากหลายเครื่องไปยังเซิร์ฟเวอร์หรือระบบของเป้าหมาย

ข้อที่ 4: ข้อใดเป็นการกระทำที่เสี่ยงต่อการตกเป็นเหยื่อฟิชชิ่ง ?

A) ตรวจสอบ URL ก่อนคลิกทุกครั้ง

B) **คลิกลิงก์จากอีเมลที่ไม่ได้ร้องขอทันที**

C) ใช้บริการ VirusTotal เพื่อตรวจสอบลิงก์

D) สงสัยอีเมลที่ใช้ชื่อโดเมนแปลก เช่น @micros0ft.com

เหตุผล:

☒ A เป็นเทคนิคช่วยลดความเสี่ยงต่อการตกเป็นเหยื่อฟิชชิ่ง

☑ **B คือพฤติกรรมที่ควรหลีกเลี่ยงโดยตรง**

☒ C เป็นเทคนิคช่วยลดความเสี่ยงต่อการตกเป็นเหยื่อฟิชชิ่ง

☒ D เป็นเทคนิคช่วยลดความเสี่ยงต่อการตกเป็นเหยื่อฟิชชิ่ง

ข้อที่ 5: ข้อใดคือหลักการตั้งรหัสผ่านที่ปลอดภัยตามแนวทางที่แนะนำขององค์กร ?

A) ใช้ชื่อเล่นและวันเกิดผสมกัน

B) ใช้รหัสผ่านสั้น ๆ แต่จำง่าย เช่น 123456

C) **ตั้งรหัสผ่านอย่างน้อย 8-12 ตัวอักษร พร้อมอักขระพิเศษ ตัวเลข และตัวพิมพ์ใหญ่**

D) ใช้รหัสผ่านเดียวกันกับทุกระบบ เพื่อให้ง่ายต่อการจดจำ

เหตุผล:

☒ A ใช้ข้อมูลที่คาดเดาได้ง่าย

☒ B ใช้ข้อมูลที่คาดเดาได้ง่าย

☑ **C เป็นไปตามแนวทางที่แนะนำ: ความยาว ≥ 8-12 ตัวอักษร และประกอบด้วยหลากหลายรูปแบบ**

☒ D เสี่ยงหากรหัสผ่านรั่วเพียงระบบเดียว

ข้อที่ 6: ข้อใดคือลักษณะสำคัญของ Email Phishing ?

A) การส่งข้อความ SMS เพื่อให้ผู้ใช้คลิกลิงก์

B) การสร้างเว็บไซต์ปลอมที่มีโลโก้เหมือนของจริง

C) **การส่งอีเมลปลอมที่ดูเหมือนมาจากหน่วยงานที่น่าเชื่อถือ**

D) การใช้บัญชี Facebook ปลอมเพื่อหลอกลวงเหยื่อ

เหตุผล:

☒ A เป็นลักษณะของ Smishing (SMS+Phishing) หรือผู้ไม่หวังดีใช้ ข้อความ SMS เป็นช่องทางในการหลอกลวงเหยื่อให้เปิดเผยข้อมูลสำคัญ

☒ B เป็นลักษณะของ Website Spoofing หรือการปลอมแปลงเว็บไซต์

☑ **C Email Phishing คือการส่งอีเมลที่ปลอมแปลงว่าเป็นหน่วยงานจริง เช่น ธนาคาร หรือองค์กรรัฐ พร้อมข้อความเร่งด่วน เช่น “บัญชีมีปัญหา” เพื่อหลอกให้คลิกลิงก์ปลอม**

☒ D เป็นลักษณะของ Social Media Phishing หรือการโจมตีแบบฟิชชิ่งที่เกิดผ่านช่องทางโซเชียลมีเดีย

ข้อที่ 7: ข้อใดต่อไปนี้ ***อธิบายลักษณะของ Spear Phishing*** ได้ถูกต้องที่สุด ?

A) การโจมตีแบบสุ่มผ่านอีเมลถึงคนจำนวนมาก

B) การโจมตีผ่านเบราว์เซอร์โดยหลอกว่าเป็นเว็บจริง

C) **การโจมตีแบบเจาะจงเป้าหมาย โดยใช้ข้อมูลเฉพาะของเหยื่อ**

D) การส่ง SMS ปลอมเพื่อหลอกให้คลิกลิงก์

เหตุผล:

☒ A เป็น Email Phishing แบบทั่วไป

☒ B เป็นลักษณะของ Browser Spoofing

☑ **C คือคำจำกัดความตรงของ Spear Phishing**

☒ D เป็นลักษณะของ Smishing

ข้อที่ 8: หากคุณได้รับอีเมลแจ้งเตือนว่า “บัญชีของคุณถูกล็อก” ควรทำอย่างไรเป็นอันดับแรก ?

A) คลิกลิงก์ในอีเมลเพื่อปลดล็อกทันที

B) ตอบกลับอีเมลเพื่อขอข้อมูลเพิ่มเติม

C) **ตรวจสอบกับเว็บไซต์จริงโดยไม่คลิกจากอีเมล**

D) ส่งอีเมลต่อให้เพื่อนเพื่อขอคำปรึกษา

เหตุผล:

☒ A เสี่ยงต่อการตกเป็นเหยื่อฟิชชิ่ง

☒ B เสี่ยงต่อการตกเป็นเหยื่อฟิชชิ่ง

☑ **C เป็นวิธีปลอดภัยที่สุด เพราะหลีกเลี่ยงการคลิกลิงก์หรือเปิดไฟล์แนบจากอีเมล**

☒ D อาจทำให้การแพร่กระจายของฟิชชิ่งขยายวงกว้าง

ข้อที่ 9: เหตุใดควร **"เช็กก่อนแชร์"** ข้อมูลบนโซเชียลมีเดีย ?

A) เพื่อให้ข้อมูลดูน่าเชื่อถือมากขึ้น

B) เพื่อเลี่ยงความผิดกฎหมายเรื่องลิขสิทธิ์

C) เพื่อให้เพื่อนในโซเชียลมีเดียรู้ว่าเราอัปเดตข่าวสารตลอด

D) **เพื่อป้องกันการเผยแพร่ข่าวปลอมและลดโอกาสฟิชชิ่ง**

เหตุผล:

☒ A เป็นเพียงผลทางภาพลักษณ์

☒ B เกี่ยวกับลิขสิทธิ์

☒ C เน้นเรื่องภาพลักษณ์ ไม่ใช่ความปลอดภัย

☑ **D คือเหตุผลหลักของแนวคิด “เช็กก่อนแชร์” เพื่อลดความเสี่ยงข่าวปลอมและลิงก์ฟิชชิ่ง**

ข้อที่ 10: เครื่องมือใดที่ใช้สำหรับตรวจสอบความปลอดภัยของเว็บไซต์ต้องสงสัย ?

A) Google Maps

B) **URLVoid**

C) Canva

D) ShareX

เหตุผล:

☒ A ใช้สำหรับแผนที่

☑ **B เป็นเครื่องมือวิเคราะห์โดเมนและความน่าเชื่อถือของ URL**

☒ C เป็นแพลตฟอร์มออกแบบ

☒ D ใช้สำหรับจับภาพหน้าจอ

ข้อที่ 11: เมื่อพบเหตุการณ์น่าสงสัย เช่น ฟิชชิ่ง ควรดำเนินการอย่างไรเป็นอันดับแรก ?

A) ตอบกลับเพื่อสอบถามความชัดเจน

B) ส่งต่อให้เพื่อนช่วยตรวจสอบ

C) คลิกที่ลิงก์เพื่อดูว่าเกิดอะไรขึ้น

D) **เก็บหลักฐาน และแจ้งผู้ดูแลระบบ (ฝ่าย IT) หรือ ThaiCERT**

เหตุผล:

☒ A เสี่ยงต่อการขยายผลการโจมตีหรือถูกหลอกซ้ำ

☒ B เสี่ยงต่อการขยายผลการโจมตีหรือถูกหลอกซ้ำ

☒ C เสี่ยงต่อการขยายผลการโจมตีหรือถูกหลอกซ้ำ

☑ **D เป็นแนวทางปฏิบัติที่ถูกต้อง: ไม่ตอบ ไม่คลิก แจ้งทันที**

ข้อที่ 12: จากสถิติในปี 2566 วิธีการโจมตีฟิชชิ่งใดถูกใช้มากที่สุด ?

A) ผ่าน SMS

B) ผ่านโฆษณาบนเว็บไซต์

C) **ผ่านอีเมล**

D) ผ่านการโทรศัพท์หลอกลวง

เหตุผล:

☒ A มีการเพิ่มขึ้นของ Smishing แต่ไม่สูงเท่าผ่านอีเมล

☒ B ไม่ปรากฏในสถิติที่อ้างอิง

☑ **C ระบุชัดว่า 82% ของการโจมตีเกิดผ่านอีเมล**

☒ D ไม่ปรากฏในสถิติที่อ้างอิง

ข้อที่ 13: จากกรณีศึกษา Sony Pictures การป้องกันฟิชชิ่งที่มีประสิทธิภาพควรเน้นมาตรการใด ?

A) ห้ามส่งอีเมลภายในองค์กร

B) **ใช้การยืนยันตัวตนแบบ 2 ขั้นตอน Two-Factor Authentication (2FA), ระบบตรวจจับปลายทาง และฝึกอบรมพนักงาน**

C) ลบไฟล์แนบทั้งหมดโดยอัตโนมัติ

D) ใช้รหัสผ่านเดียวกันเพื่อความสะดวกในการควบคุม

เหตุผล:

☒ A เป็นไปไม่ได้ในทางปฏิบัติ

☑ **B เป็นมาตรการป้องกันเชิงรุกตามบทเรียนจากกรณี Sony Pictures**

☒ C ไม่สามารถใช้กับอีเมลงานทั้งหมด

☒ D ขัดกับหลักความปลอดภัยด้านรหัสผ่าน

ข้อที่ 14: ในเชิงกลยุทธ์ องค์กรควรมีเครื่องมือใดเพื่อป้องกันและตรวจจับการโจมตีฟิชชิ่ง ?

A) ระบบจัดการข้อมูลเหตุการณ์ด้านความปลอดภัย (SIEM) + ระบบรักษาความปลอดภัยของอีเมล (Email Security) + ระบบป้องกันการรั่วไหลของข้อมูลสำคัญ (DLP)

B) ระบบหรืออุปกรณ์ที่ทำหน้าที่กรองและควบคุมการรับส่งข้อมูลระหว่างเครือข่ายภายใน (Firewall) เพียงอย่างเดียว

C) ช่องทางการเชื่อมต่อที่ปลอดภัย (Virtual Private Network: VPN) สำหรับทุกพนักงาน

D) ปรับให้ทุกคนใช้ระบบอีเมลหลักจาก Microsoft Outlook (ซึ่งเป็นส่วนหนึ่งของ Microsoft 365) ไปใช้ Gmail (ซึ่งเป็นส่วนหนึ่งของ Google Workspace)

เหตุผล:

☑ **A การป้องกันฟิชชิ่งระดับองค์กรต้องอาศัยเครื่องมือหลายชั้น เช่น SIEM (วิเคราะห์ log), Email Security (สแกนอีเมล), และ DLP (ป้องกันข้อมูลรั่ว)**

☒ B Firewall ไม่สามารถตรวจจับอีเมลฟิชชิ่ง

☒ C VPN ช่วยเข้ารหัสการเชื่อมต่อ ไม่ป้องกันฟิชชิ่งโดยตรง

☒ D เปลี่ยนระบบอีเมลไม่ใช่การป้องกันเชิงกลยุทธ์

ข้อที่ 15: นโยบายความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร สอดคล้องกับกฎหมายหรือมาตรฐานใดต่อไปนี้มากที่สุด ?

A) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และมาตรฐานสากลด้านบริหารจัดการความมั่นคงปลอดภัยของข้อมูล (ISO/IEC 27001:2022)

B) พระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2550 เท่านั้น

C) พระราชบัญญัติทรัพย์สินทางปัญญา

D) พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540

เหตุผล:

☑ **A เป็นกฎหมายและมาตรฐานที่เกี่ยวข้องโดยตรงกับการจัดการความมั่นคงปลอดภัยของข้อมูลและการคุ้มครองข้อมูลส่วนบุคคลในองค์กร**

☒ B แม้เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แต่ไม่ใช่กรอบนโยบายด้านความมั่นคงปลอดภัยข้อมูลโดยตรง

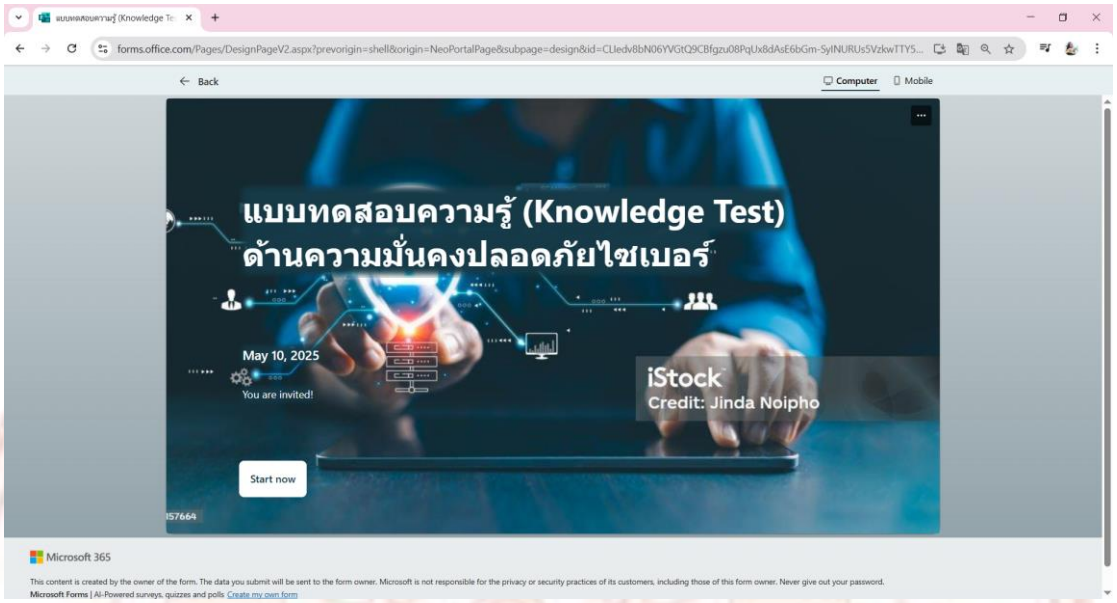
☒ C มุ่งเน้นทรัพย์สินทางปัญญา ไม่ครอบคลุมการกำหนดนโยบายความมั่นคงปลอดภัยของข้อมูลในองค์กร

☒ D มุ่งเน้นการเปิดเผยข้อมูลของหน่วยงานรัฐ ไม่ใช่การกำหนดมาตรการด้านไซเบอร์ซีเคียวริตี้ในองค์กร

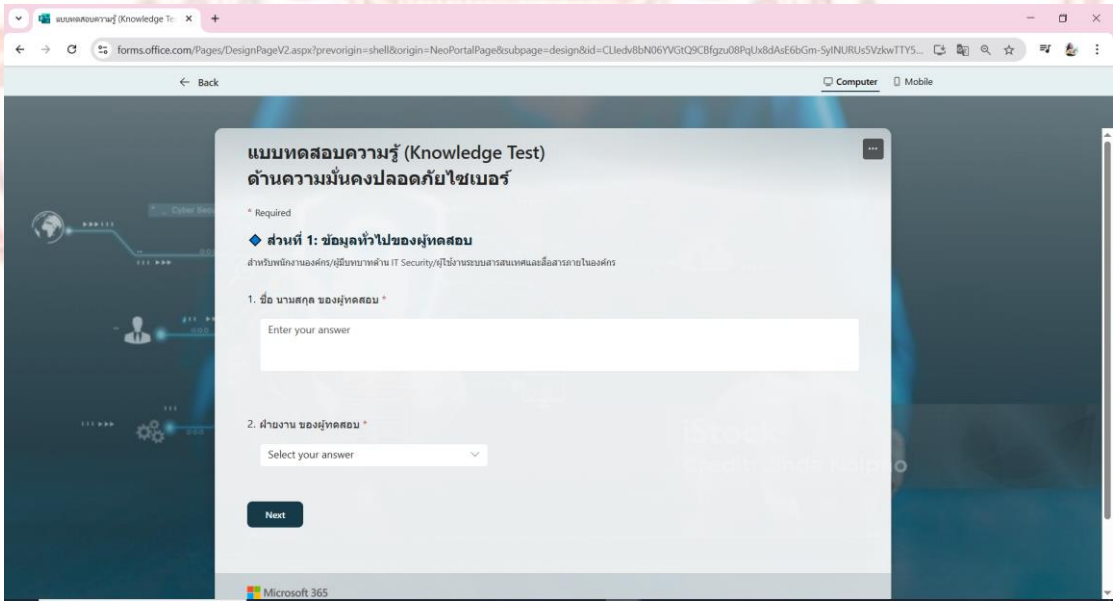
ภาคผนวก ข

แบบฟอร์มทดสอบความรู้ (Knowledge Test) ด้านความมั่นคงปลอดภัยไซเบอร์

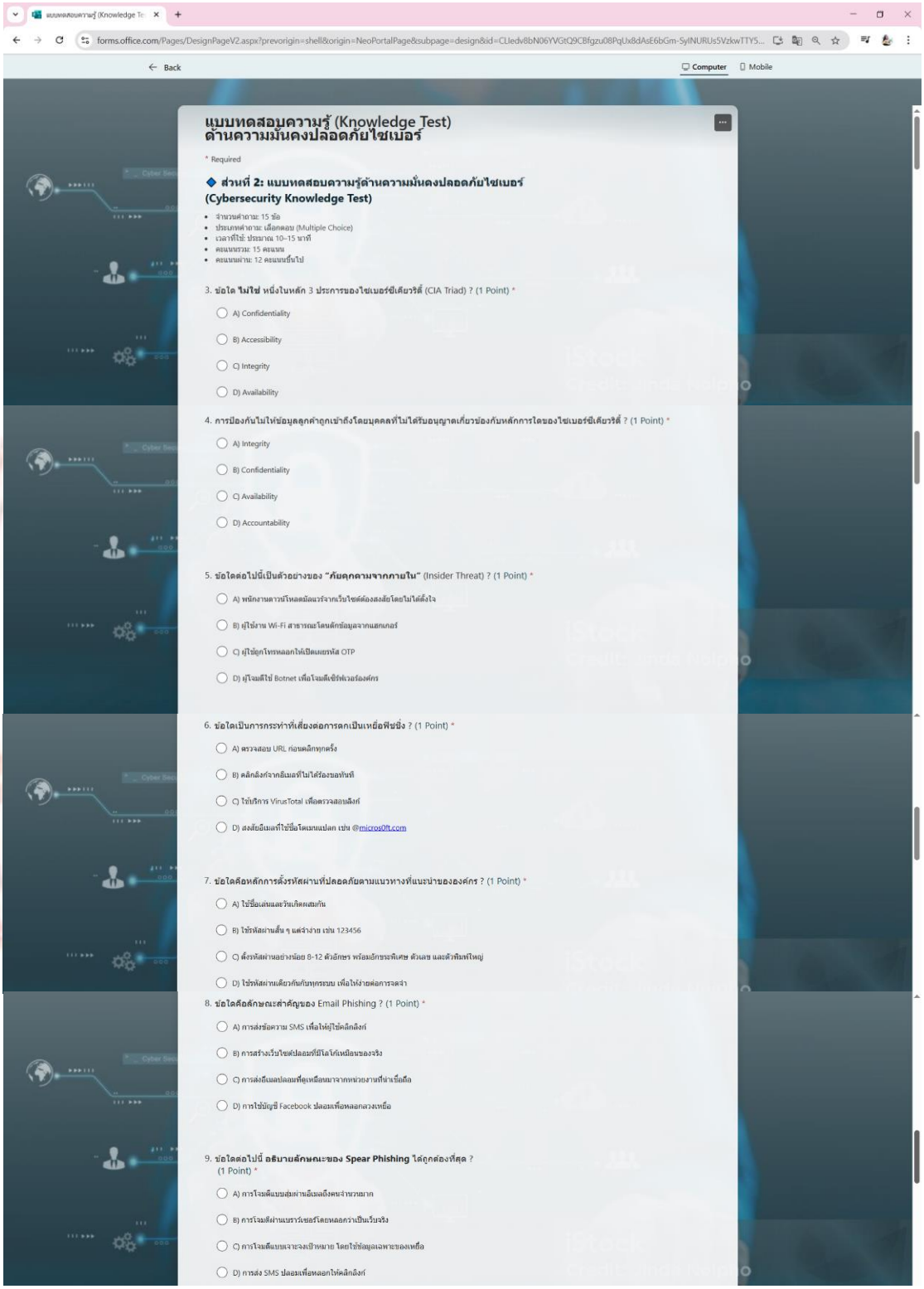
แบบฟอร์มทดสอบความรู้ (Knowledge Test) ด้านความมั่นคงปลอดภัยไซเบอร์



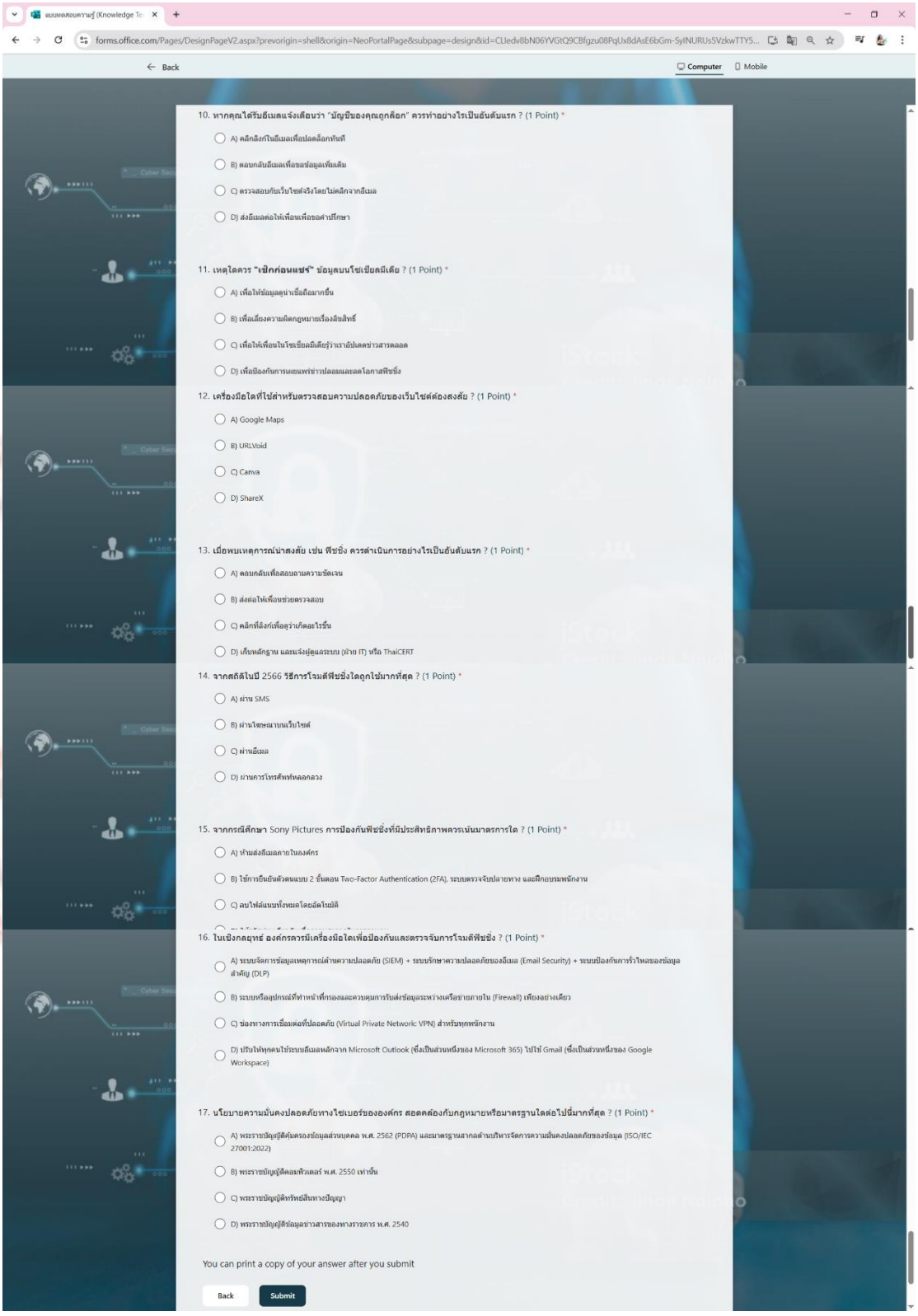
ภาพที่ ข-1 หน้าแรกของแบบฟอร์มทดสอบความรู้ (Knowledge Test) ด้านความมั่นคงปลอดภัยไซเบอร์



ภาพที่ ข-2 ส่วนที่ 1 ข้อมูลทั่วไปของผู้ทดสอบ



ภาพที่ ข-3 ส่วนที่ 2 แบบฟอร์มทดสอบความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Knowledge Test)



ภาพที่ ข-4 ส่วนที่ 2 แบบฟอร์มทดสอบความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Knowledge Test) (ต่อ)

ภาคผนวก ค

การออกแบบคำถามของแบบสอบถามความพึงพอใจของบุคลากรที่เข้ามาใช้งานแพลตฟอร์มชุมชนความปลอดภัยไซเบอร์

แบบสอบถามความพึงพอใจของบุคลากรที่เข้ามาใช้งานแพลตฟอร์มชุมชนความปลอดภัยไซเบอร์

1) แบบสอบถามชุดนี้แบ่งเป็น 5 ส่วน คือ
   ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม
   ส่วนที่ 2 ความพึงพอใจต่อการใช้งานแพลตฟอร์ม (User Experience)
   ส่วนที่ 3 ความพึงพอใจต่อเนื้อหาและกิจกรรมในแพลตฟอร์ม (Activities)
   ส่วนที่ 4 ผลกระทบจากการใช้งานแพลตฟอร์ม (Outcomes & Impact)
   ส่วนที่ 5 ข้อเสนอแนะและความคิดเห็นเพิ่มเติม
2) กรุณาตอบแบบสอบถามตามความเป็นจริงหรือตามความคิดเห็นที่แท้จริงของท่าน เพื่อความถูกต้องและสมบูรณ์ของงานวิจัย
3) การตอบแบบสอบถามนี้ จะไม่มีผลกระทบใด ๆ ต่อตัวท่าน ข้อมูลที่ได้จะใช้ประโยชน์เพื่อการวิจัยเท่านั้น

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

วัตถุประสงค์ : เพื่อใช้จำแนกกลุ่มผู้ใช้งานและวิเคราะห์ข้อมูลตามบริบทโดยไม่ระบุตัวตน

1) ท่านสังกัดหน่วยงาน/ฝ่ายใด

ส่วนที่ 2 ความพึงพอใจต่อการใช้งานแพลตฟอร์ม (User Experience)

คำชี้แจง: โปรดประเมินระดับความพึงพอใจตามหัวข้อลงใน ◯ ที่ตรงกับความคิดเห็นของท่านมากที่สุด

1) ประเมินด้านการออกแบบ ประสบการณ์ผู้ใช้งาน และประสิทธิภาพของแพลตฟอร์ม

หัวข้อ	น้อยมาก	น้อย	ปานกลาง	มาก	มากที่สุด
แพลตฟอร์มใช้งานง่าย ไม่ซับซ้อน	◯	◯	◯	◯	◯
การเข้าถึงเนื้อหาทำได้สะดวก รวดเร็ว	◯	◯	◯	◯	◯
ความเร็วและความเสถียรเพียงพอต่อการใช้งาน	◯	◯	◯	◯	◯
การจัดหมวดหมู่และการนำทางเนื้อหาชัดเจน	◯	◯	◯	◯	◯

ส่วนที่ 3: ความพึงพอใจต่อเนื้อหาและกิจกรรมในแพลตฟอร์ม (Activities)

คำชี้แจง: โปรดประเมินระดับความพึงพอใจตามหัวข้อลงใน ◯ ที่ตรงกับความคิดเห็นของท่านมากที่สุด

2) ประเมินเนื้อหา กิจกรรมการมีส่วนร่วม และความเหมาะสมของการเรียนรู้ในแพลตฟอร์ม

หัวข้อ	น้อยมาก	น้อย	ปานกลาง	มาก	มากที่สุด
เนื้อหาเกี่ยวกับความปลอดภัยไซเบอร์มีประโยชน์ต่อการทำงานจริง	◯	◯	◯	◯	◯
กิจกรรม เช่น แบบฝึกหัด / Quiz /	◯	◯	◯	◯	◯

หัวข้อ	น้อยมาก	น้อย	ปานกลาง	มาก	มากที่สุด
แชร์ความรู้ สร้างความสนใจ					
เนื้อหาครอบคลุมหัวข้อสำคัญด้านความมั่นคงปลอดภัยไซเบอร์	◯	◯	◯	◯	◯
เนื้อหาทันสมัย สอดคล้องกับสถานการณ์และภัยคุกคามที่เกิดขึ้นจริง	◯	◯	◯	◯	◯

ส่วนที่ 4: ผลกระทบจากการใช้งานแพลตฟอร์ม (Outcomes & Impact)

คำชี้แจง: โปรดประเมินระดับความพึงพอใจตามหัวข้อลงใน ◯ ที่ตรงกับความคิดเห็นของท่านมากที่สุด

3) ความเปลี่ยนแปลงด้านความรู้ ทัศนคติ และพฤติกรรมของผู้ใช้งาน

หัวข้อ	น้อยมาก	น้อย	ปานกลาง	มาก	มากที่สุด
ท่านมีความรู้ด้านความปลอดภัยไซเบอร์เพิ่มขึ้นจากการใช้งานแพลตฟอร์ม	◯	◯	◯	◯	◯
ท่านสามารถนำความรู้ไปปรับปรุงพฤติกรรมการใช้งานระบบ IT ให้มีความปลอดภัยมากยิ่งขึ้น	◯	◯	◯	◯	◯
ท่านสามารถนำความรู้จากแพลตฟอร์มไปประยุกต์ใช้ในงานจริง	◯	◯	◯	◯	◯
การเข้าร่วมในชุมชนช่วยให้รู้ทันภัยไซเบอร์ได้มากขึ้น	◯	◯	◯	◯	◯

ส่วนที่ 5: ข้อเสนอแนะและความคิดเห็นเพิ่มเติม

วัตถุประสงค์: เพื่อเปิดโอกาสให้ผู้ใช้งานแสดงมุมมองเพิ่มเติม และพัฒนาแพลตฟอร์มให้ดียิ่งขึ้น

4) จุดเด่นของแพลตฟอร์มที่ท่านชื่นชอบ

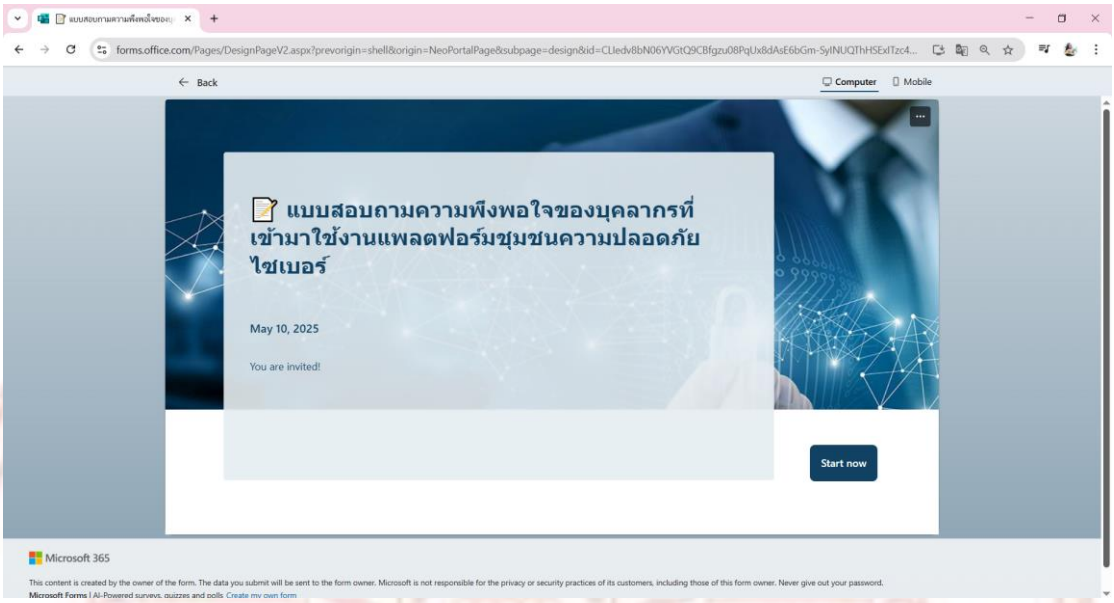
5) ข้อเสนอแนะเพื่อพัฒนาแพลตฟอร์ม / เนื้อหา / กิจกรรม

6) เนื้อหา หรือฟีเจอร์ที่ท่านอยากให้เพิ่มเติมในอนาคต

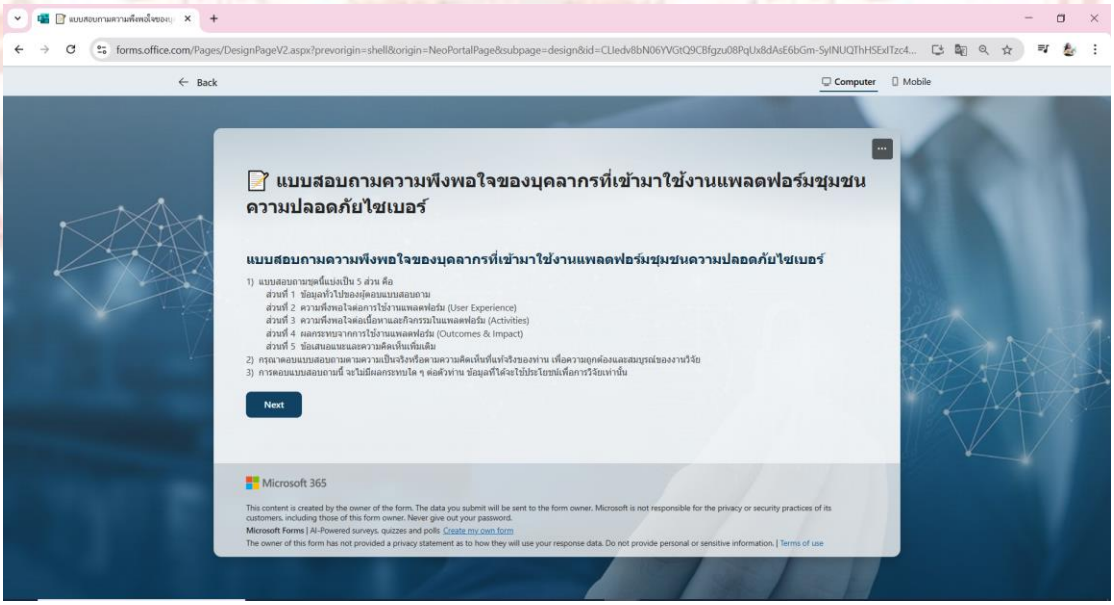
ภาคผนวก ง

แบบฟอร์มสอบถามความพึงพอใจของบุคลากรที่เข้ามาใช้งานแพลตฟอร์มชุมชนความปลอดภัยไซเบอร์

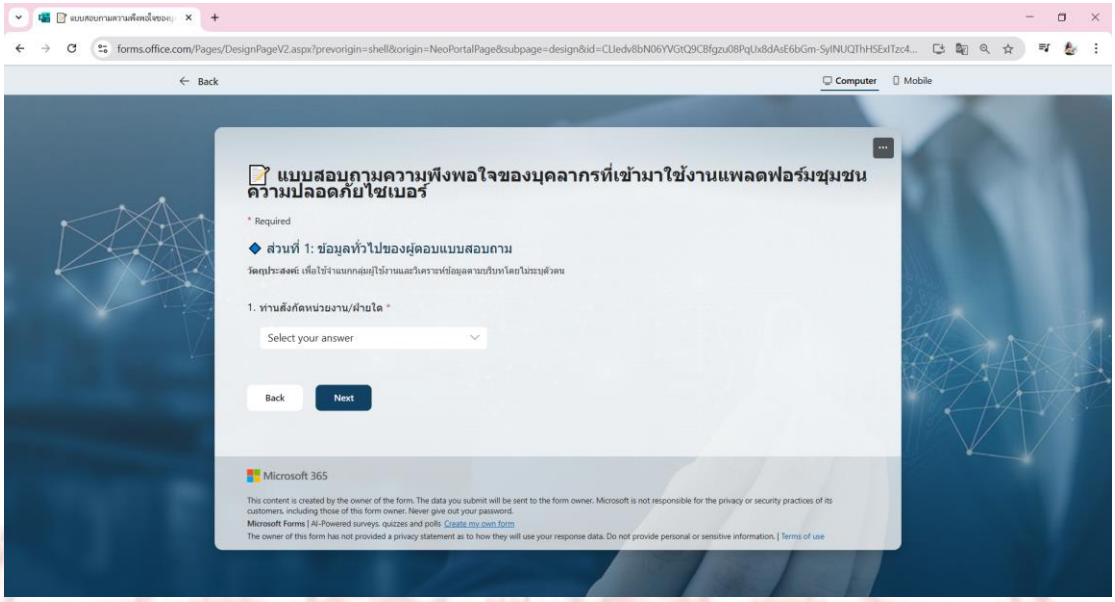
แบบฟอร์มสอบถามความพึงพอใจของบุคลากรที่เข้ามาใช้งานแพลตฟอร์มชุมชนความปลอดภัยไซเบอร์



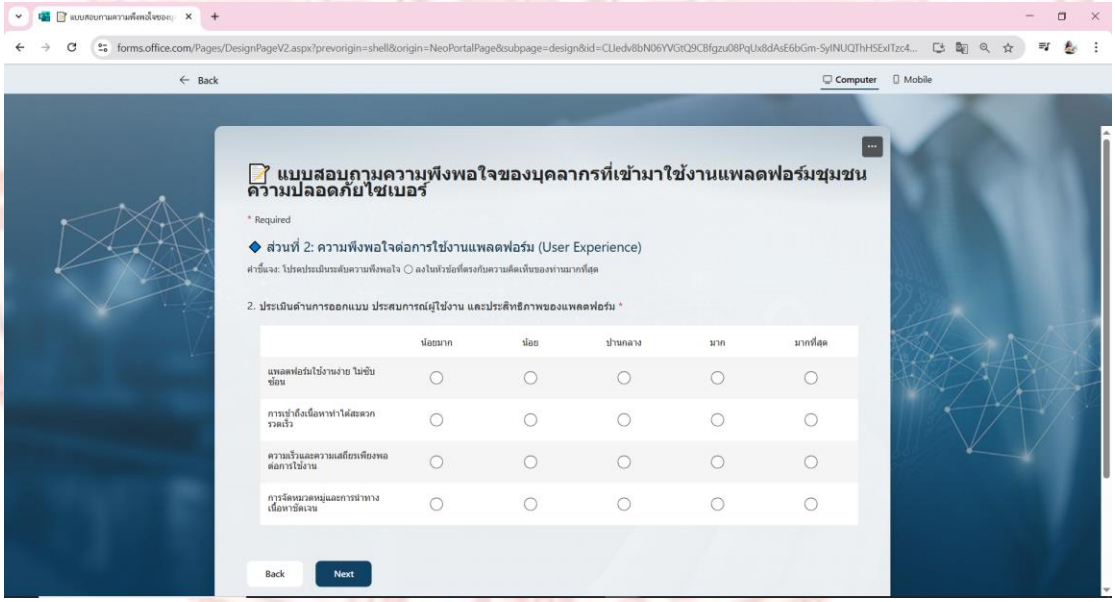
ภาพที่ ง-1 หน้าแรกของแบบฟอร์มสอบถามความพึงพอใจของบุคลากรที่เข้ามาใช้งานแพลตฟอร์มชุมชนความปลอดภัยไซเบอร์



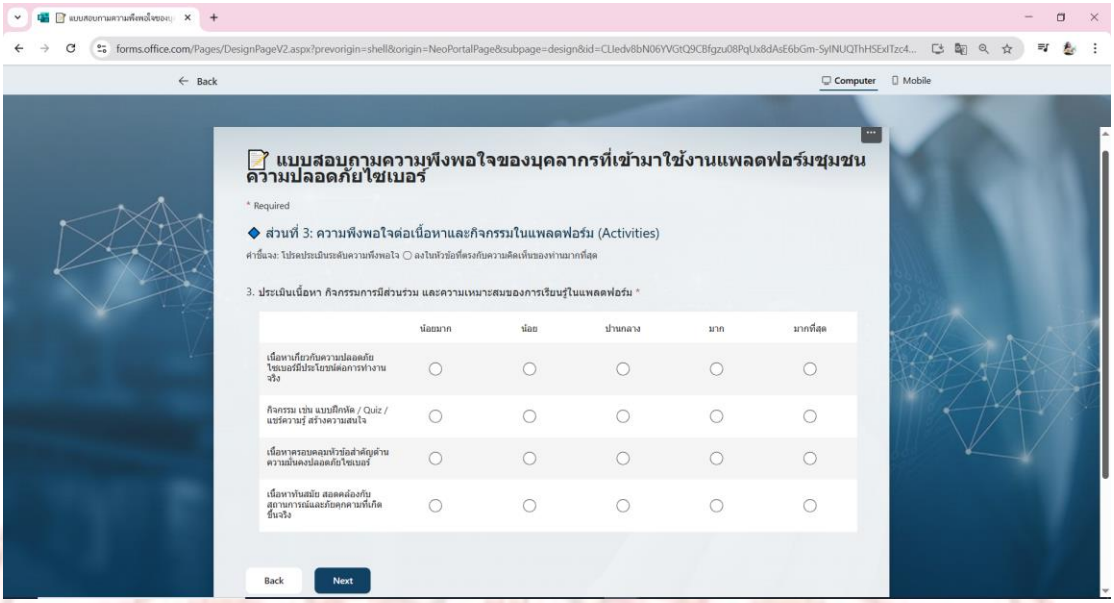
ภาพที่ ง-2 หน้าคำชี้แจงของแบบฟอร์มสอบถามความพึงพอใจของบุคลากรที่เข้ามาใช้งานแพลตฟอร์มชุมชนความปลอดภัยไซเบอร์



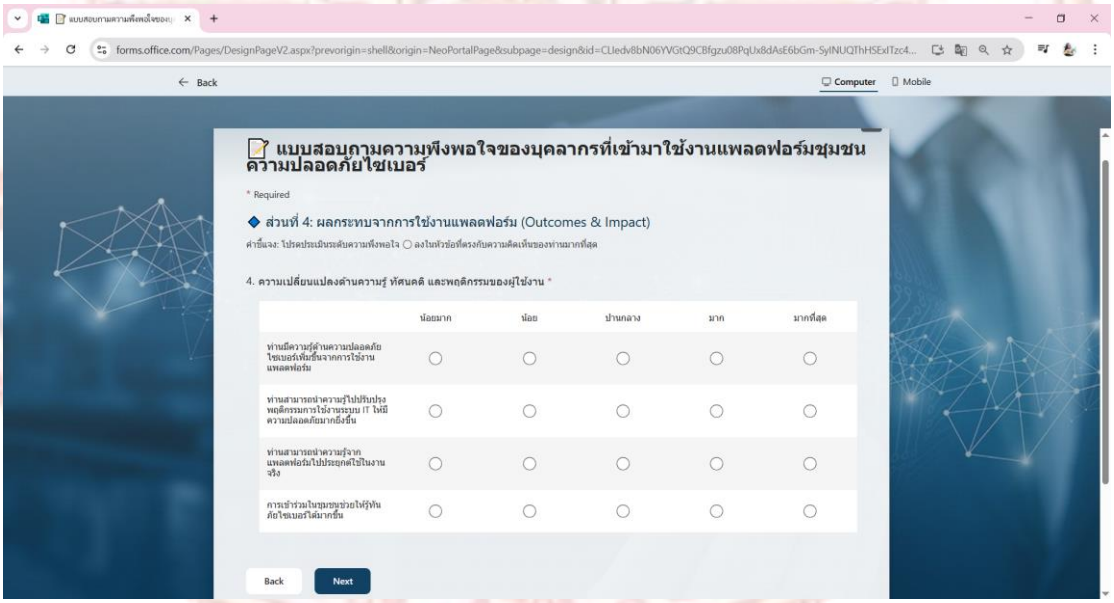
ภาพที่ ง-3 ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม



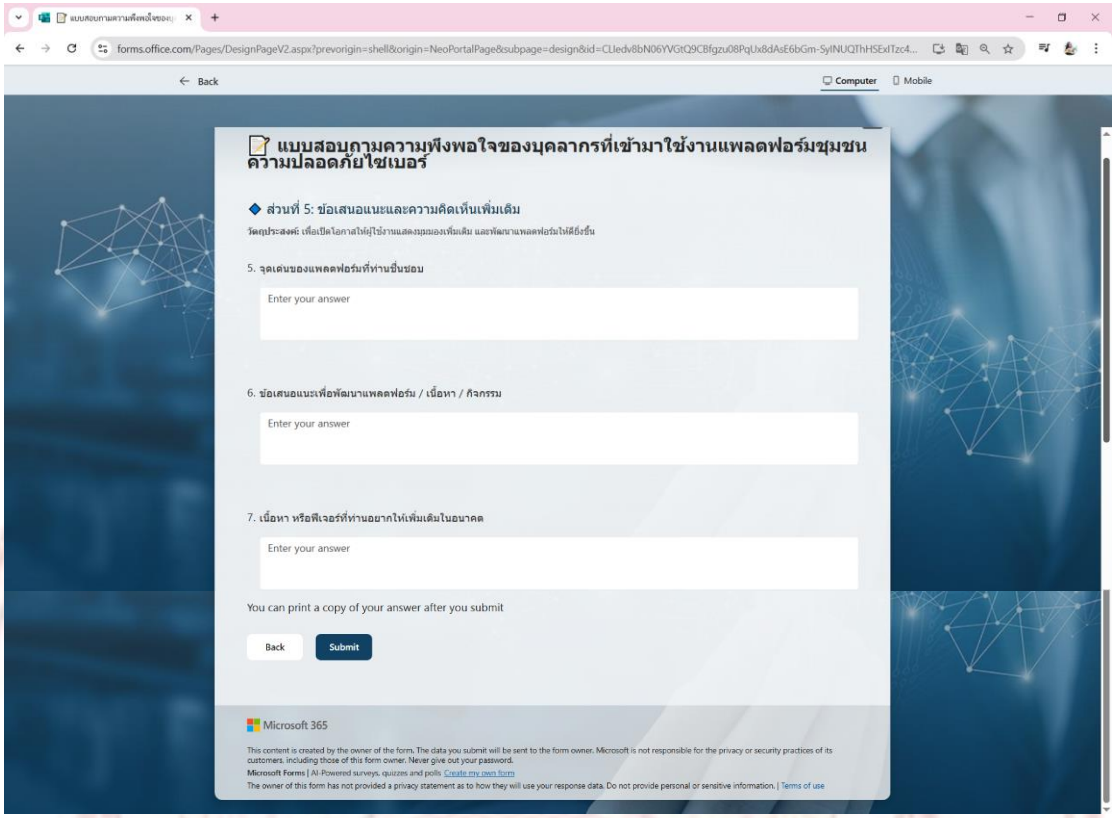
ภาพที่ ง-4 ส่วนที่ 2 ความพึงพอใจต่อการใช้งานแพลตฟอร์ม (User Experience)



ภาพที่ ง-5 ส่วนที่ 3 ความพึงพอใจต่อเนื้อหาและกิจกรรมในแพลตฟอร์ม (Activities)



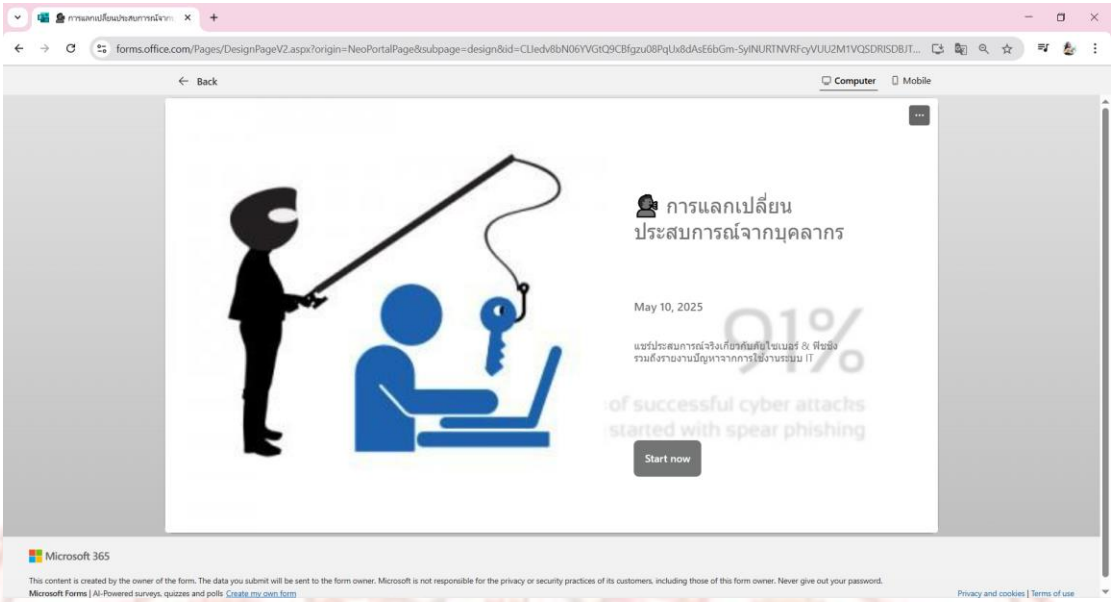
ภาพที่ ง-6 ส่วนที่ 4 ผลกระทบจากการใช้งานแพลตฟอร์ม (Outcomes & Impact)



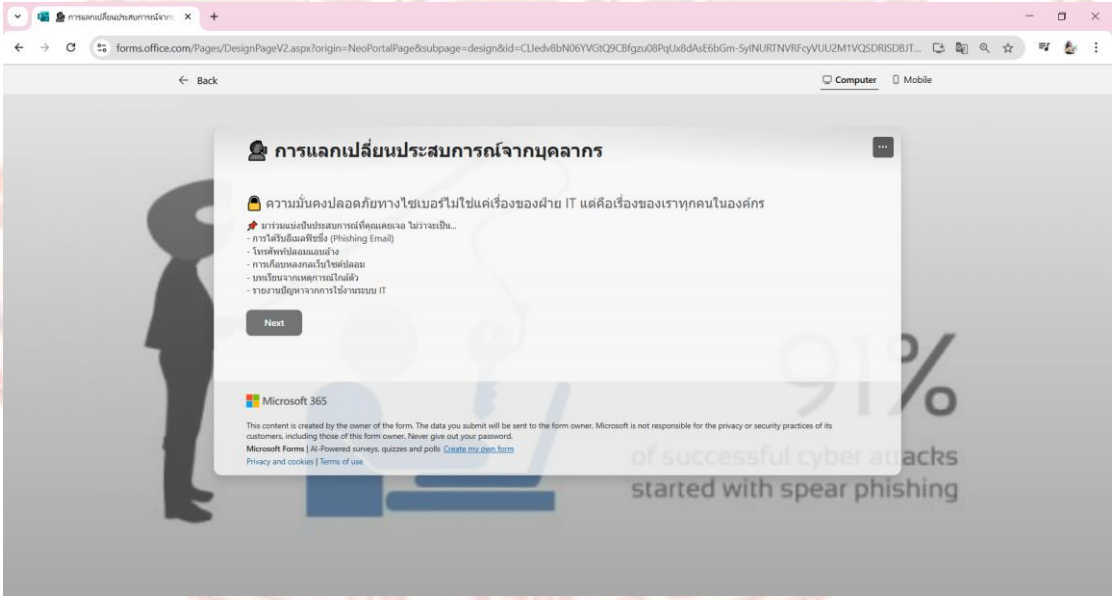
ภาพที่ ง-7 ส่วนที่ 5 ข้อเสนอแนะและความคิดเห็นเพิ่มเติม

ภาคผนวก ช

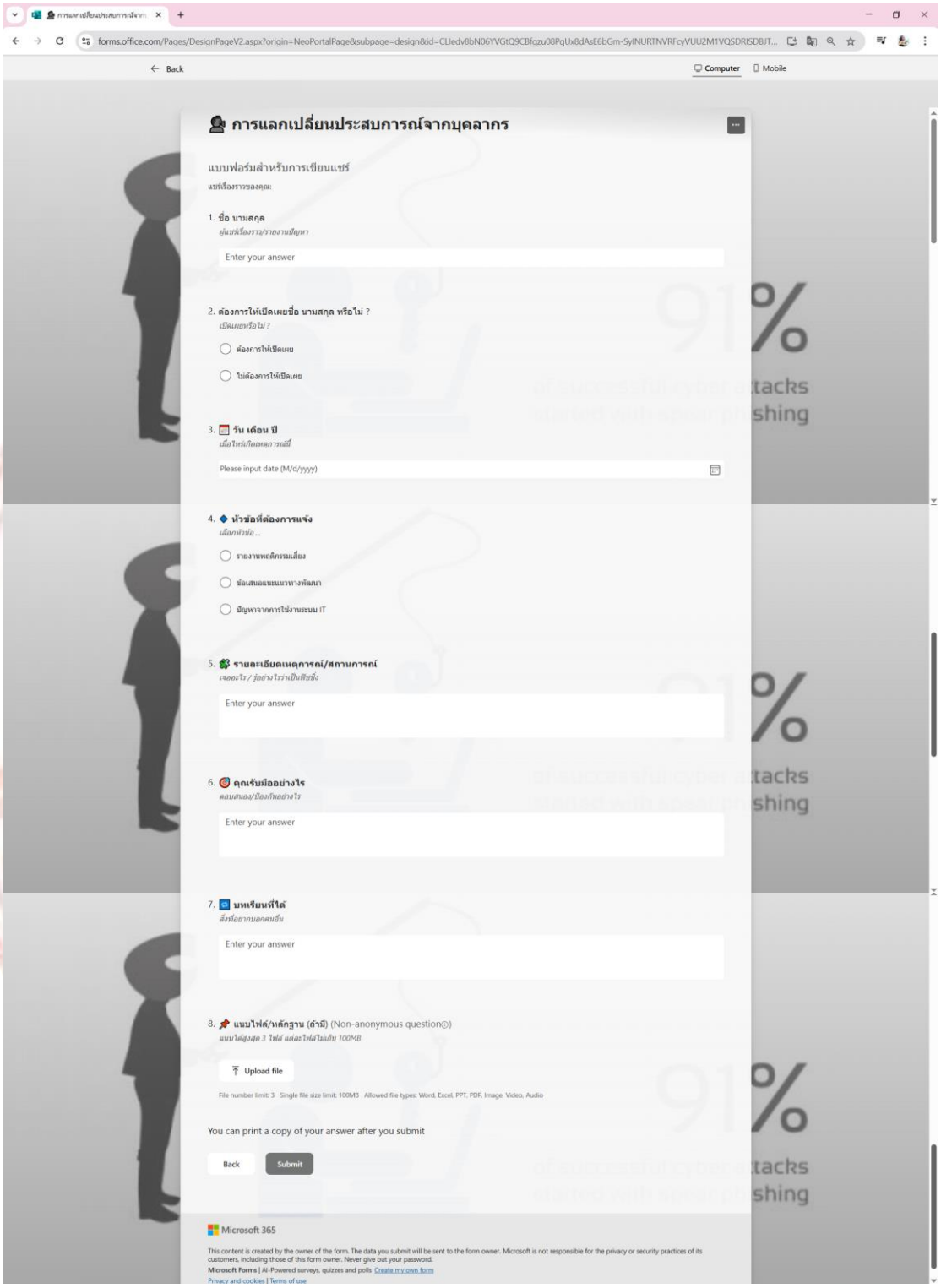
แบบฟอร์มการแลกเปลี่ยนประสบการณ์จากบุคลากร



ภาพที่ ช-1 หน้าแรกของแบบฟอร์มการแลกเปลี่ยนประสบการณ์จากบุคลากร



ภาพที่ ช-2 หน้าคำชี้แจงของแบบฟอร์มการแลกเปลี่ยนประสบการณ์จากบุคลากร



ภาพที่ ช-3 แบบฟอร์มการแลกเปลี่ยนประสบการณ์จากบุคลากร

ประวัติผู้เขียน

ชื่อ นางสาววราพร นิ่มนวล

ชื่อการค้นคว้าอิสระ การพัฒนาแพลตฟอร์มชุมชนเพื่อเสริมสร้างวัฒนธรรมความปลอดภัยไซเบอร์

สาขาวิชา การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

ประวัติ สำเร็จการศึกษาระดับปริญญาตรี สาขาการจัดการเทคโนโลยีการผลิตและสารสนเทศ วิทยาลัยเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ