การประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ กรณีศึกษาคลินิกเอกชน

นายอโนชา คุ้มแพทย์

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568

การประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ กรณีศึกษาคลินิกเอกชน

นายอโนชา คุ้มแพทย์

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568

ใบรับรองการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ กรณีศึกษาคลินิกเอกชน

โดย นายอโนชา คุ้มแพทย์

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

คณบดีคณะเทคโนโลยีสารสนเทศ
และนวัตกรรมดิจิทัล

.....

(ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี)

คณะกรรมการสอบการค้นคว้าอิสระ

..... ประธานกรรมการ

(รองศาสตราจารย์ ดร.สุมิตรา นวลมีศรี)

..... อาจารย์ที่ปรึกษา

(ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์)

ชื่อ : นายอโนชา คุ้มแพทย์
ชื่อการค้นคว้าอิสระ : การประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ กรณีศึกษาคลินิกเอกชน
สาขาวิชา : การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์
ปีการศึกษา : 2568

บทคัดย่อ

การค้นคว้าอิสระครั้งนี้มีวัตถุประสงค์เพื่อ (1) ประเมินระดับความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ในคลินิกเอกชน และ (2) พัฒนาและนำสื่อการเรียนรู้ออนไลน์มาใช้เพื่อเสริมสร้างความรู้และการป้องกันภัยคุกคามทางไซเบอร์ กลุ่มตัวอย่างคือบุคลากรของคลินิกจำนวน 80 คน ที่ได้จากการสุ่มแบบง่ายตามสูตรของยามาเน่ เครื่องมือวิจัยประกอบด้วยแบบทดสอบก่อนและหลังเรียน คะแนนเต็ม 25 คะแนน โดยมีเกณฑ์การแปลผล 3 ระดับ คือ น้อย (0–12 คะแนน) ปานกลาง (13–17 คะแนน) และมาก (18–25 คะแนน) เครื่องมือได้รับการตรวจสอบความตรงเชิงเนื้อหาโดยผู้เชี่ยวชาญ 3 ท่าน ซึ่งทุกข้อมีค่า IOC มากกว่า 0.5 ข้อมูลที่ได้ถูกวิเคราะห์ด้วยสถิติเชิงพรรณนา และทดสอบสมมติฐานด้วยสถิติแบบ Paired Samples t-test

ผลการวิจัยพบว่า ก่อนการอบรม บุคลากรส่วนใหญ่มีระดับความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์อยู่ในระดับต่ำ โดยมีคะแนนเฉลี่ย 9.20 คะแนน หลังเข้าร่วมกิจกรรมการเรียนรู้ผ่านสื่อออนไลน์แบบโต้ตอบด้วยโปรแกรม Genially คะแนนเฉลี่ยเพิ่มขึ้นเป็น 20.30 คะแนน เพิ่มขึ้น 11.10 คะแนน (ร้อยละ 44.4) สัดส่วนของผู้ที่มีความรู้ระดับสูงเพิ่มจากร้อยละ 2.50 เป็นร้อยละ 82.50 โดยไม่มีผู้ใดอยู่ในระดับต่ำอีกต่อไป ผลการทดสอบทางสถิติแบบ Paired Samples t-test พบว่าความแตกต่างของคะแนนก่อนและหลังการอบรมมีนัยสำคัญทางสถิติที่ระดับ .05 แสดงให้เห็นว่าสื่อการเรียนรู้ออนไลน์มีประสิทธิผลในการเสริมสร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรได้อย่างชัดเจน

สรุปผลและข้อเสนอแนะ ผลการศึกษานี้ยืนยันว่าการใช้สื่อการเรียนรู้ออนไลน์แบบโต้ตอบ เช่น Genially มีศักยภาพในการส่งเสริมการเรียนรู้เชิงรุกและช่วยเพิ่มพฤติกรรมด้านความปลอดภัยทางไซเบอร์ได้อย่างเป็นรูปธรรม หน่วยงานด้านสาธารณสุขและองค์กรที่ใช้ระบบคลาวด์ สามารถ

ประยุกต์แนวทางนี้ในการอบรมบุคลากร เพื่อสร้างวัฒนธรรมความปลอดภัย ลดความเสี่ยงจากภัยไซเบอร์ และยกระดับการคุ้มครองข้อมูลส่วนบุคคลของผู้ป่วยที่มีความอ่อนไหวในระยะยาว

(มีจำนวนทั้งสิ้น 64 หน้า)

คำสำคัญ : ความตระหนักรู้, ความมั่นคงปลอดภัยไซเบอร์, ภัยคุกคาม

_____ อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Mr. Anocha Khumphaet

Independent Study Title : An Assessment of Cybersecurity Awareness among Personnel Working on Cloud-Based Systems: A Case Study of a Private Clinic

Major Field : Network and Information Security Management
King Mongkut's University of Technology North Bangkok

Independent Study Advisor : Assistant Professor Dr. Pongsarun Boonyopakorn

Academic Year : 2025

ABSTRACT

This independent study aimed to (1) assess the level of cybersecurity awareness among personnel using cloud-based systems in a private clinic and (2) develop and implement online learning media to enhance knowledge and prevention of cyber threats. The sample comprised 80 clinic staff selected through simple random sampling based on Yamane's formula. Research instruments included pre- and post-tests of 25 points each, with three levels of interpretation: low (0–12), moderate (13–17), and high (18–25). The instruments were validated by three experts, with all items achieving an IOC above 0.5. Data were analyzed using descriptive statistics and a paired samples t-test to evaluate differences between pre- and post-test scores.

The results indicated that prior to the training, most participants had low cybersecurity awareness, with an average score of 9.20. After completing the Genially-based online learning program, the mean score increased to 20.30—an improvement of 11.10 points (44.4%). The proportion of participants with high-level knowledge rose sharply from 2.50% to 82.50%, while none remained in the low category. A paired samples t-test confirmed that this difference was statistically significant ($p < .05$), demonstrating the effectiveness of the online learning media in enhancing cybersecurity awareness.

In conclusion, the findings affirm that the use of interactive online learning tools, such as Genially, can foster active learning and tangibly improve cybersecurity-related behaviors. Healthcare organizations and other cloud-based institutions can apply this approach to staff training programs to cultivate a culture of security, reduce exposure to cyber threats, and strengthen patient data protection in the long term.

(Total 64 Pages)

Keywords: Awareness, Cybersecurity, Threats

_____ Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระเรื่อง "การประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ กรณีศึกษาคลินิกเอกชน" ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดีด้วยความร่วมมือและความช่วยเหลืออันดียิ่งจากหลายฝ่าย ผู้วิจัยขอกราบขอบพระคุณทุกท่านมา ณ โอกาสนี้เป็นอย่างสูง โดยเฉพาะอย่างยิ่ง ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์ และ ดร.ธนวรรธน์ โยชะนัง อาจารย์ที่ปรึกษาการค้นคว้าอิสระ ที่ได้กรุณาเสียสละเวลาอันมีค่าในการให้ความรู้ คำปรึกษา คำแนะนำ รวมถึงการตรวจสอบและแก้ไขความถูกต้องของงานวิจัยด้วยความเอาใจใส่และเมตตาอย่างยิ่งตลอดมา

นอกจากนี้ ผู้วิจัยขอขอบพระคุณ คณาจารย์ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศทุกท่าน ที่ได้ถ่ายทอดความรู้ซึ่งเป็นรากฐานสำคัญในการจัดทำการค้นคว้าอิสระนี้ ตลอดจนขอขอบพระคุณ คณะผู้บริหารคลินิก ที่ได้กรุณาอนุญาตให้เข้าดำเนินการวิจัย อำนวยความสะดวกในการทำแบบทดสอบและการเข้าร่วมการอบรมของบุคลากร และขอขอบพระคุณ คณะกรรมการผู้ทรงคุณวุฒิทั้ง 3 ท่าน ที่กรุณาสละเวลาดำเนินการตรวจสอบและให้คำแนะนำอันเป็นประโยชน์ต่อการพัฒนาแบบสอบถาม ซึ่งเป็นเครื่องมือสำคัญในการวิจัยฉบับนี้

ท้ายที่สุดนี้ ผู้วิจัยขอขอบคุณ ครอบครัว เพื่อน ๆ และพี่น้อง ในภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ ที่คอยให้กำลังใจและสนับสนุนเสมอมา จนการค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงไปด้วยดี คุณค่าและประโยชน์อันพึงมีจากงานวิจัยฉบับนี้ ผู้วิจัยขอมอบแด่ความกรุณาของทุกท่านที่ได้ให้การสนับสนุนตลอดมา

อโนชา คุ้มแพทย์

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูปภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในยุคดิจิทัลปัจจุบัน เทคโนโลยีสารสนเทศได้กลายเป็นกลไกสำคัญในการขับเคลื่อนการดำเนินงานขององค์กรทุกภาคส่วน โดยเฉพาะการประยุกต์ใช้ ระบบคลาวด์ (Cloud Computing) ที่ได้รับความนิยมอย่างแพร่หลาย อย่างไรก็ดี การนำระบบคลาวด์มาใช้ในองค์กรย่อมนำมาซึ่งประเด็นด้าน ความมั่นคงปลอดภัยสารสนเทศ ที่ทวีความซับซ้อนขึ้น โดยเฉพาะความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและการโจมตีทางไซเบอร์ ประเด็นนี้ยิ่งมีความสำคัญอย่างยิ่งใน ภาคส่วนสุขภาพ ซึ่งมีการจัดเก็บและประมวลผล ข้อมูลสุขภาพของผู้ป่วย ซึ่งเป็นข้อมูลที่มีความละเอียดอ่อนและอ่อนไหวสูง การขาดมาตรการรักษาความปลอดภัยที่เหมาะสมจึงก่อให้เกิดผลกระทบทั้งในเชิงกฎหมาย จริยธรรม และชื่อเสียงขององค์กร การเสริมสร้าง ความตระหนักรู้ด้านความปลอดภัยไซเบอร์ ของบุคลากรจึงเป็นหัวใจสำคัญที่ช่วยลดความเสี่ยงและเพิ่มประสิทธิภาพในการป้องกันภัยคุกคามได้อย่างยั่งยืน

บุคลากร เป็นตัวแปรที่สำคัญที่สุดในการรักษาความปลอดภัยทางไซเบอร์ เนื่องจากข้อมูลทางสถิติในปี 2025 ชี้ให้เห็นว่าแม้ระบบจะมีมาตรการทางเทคนิคที่เข้มแข็งเพียงใด หากบุคลากรขาดความตระหนักรู้ ย่อมเพิ่มความเสี่ยงต่อความล้มเหลวของระบบได้อย่างรวดเร็ว โดยรายงานล่าสุดยืนยันว่า 60% ถึง 95% ของเหตุการณ์ความปลอดภัยทางไซเบอร์เกี่ยวข้องกับ องค์ประกอบด้านมนุษย์ (Human Element) หรือความผิดพลาด (Errors) [26] และ Phishing ยังคงเป็นช่องทางหลักในการเข้าถึงระบบ (16%) [27] ซึ่งตอกย้ำถึงความจำเป็นเร่งด่วนที่หน่วยงานด้านสุขภาพต้องมีแนวทางปฏิบัติที่เข้มงวดในการป้องกันภัยคุกคามเหล่านี้

ดังนั้น เมื่อพิจารณาบริบทของ คลินิกเอกชน ที่ต้องจัดการกับข้อมูลสุขภาพที่มีความอ่อนไหวไม่ต่างกัน แม้จะมีขนาดองค์กรที่เล็กกว่าโรงพยาบาล การนำระบบคลาวด์มาใช้เพื่อจัดเก็บและบริหารจัดการข้อมูลผู้ป่วย จึงต้องอาศัยความรอบคอบและมาตรการความปลอดภัยที่ครอบคลุมทั้งด้านเทคนิคและด้านบุคลากร การค้นคว้าอิสระ เรื่อง "การประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ในคลินิกเอกชน" จึงมีความสำคัญเชิงวิชาการและเชิงปฏิบัติอย่างยิ่ง เนื่องจากการประเมินนี้เป็นการเติมเต็มช่องว่างขององค์ความรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ในบริบทขององค์กรด้านสุขภาพที่มีขนาดเล็กและใช้ระบบคลาวด์เป็นหลัก โดยผลการวิจัยจะสามารถนำไปประยุกต์ใช้ในการกำหนดมาตรการอบรม พัฒนา และกำกับดูแลระบบสารสนเทศทางการแพทย์ให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นต่อไป

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อประเมินระดับความตระหนักรู้ เกี่ยวกับภัยคุกคามและอาชญากรรมทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ของคลินิก ก่อนและหลัง ใช้งานสื่อการเรียนรู้ที่ผู้วิจัยจัดทำขึ้น

1.2.2 เพื่อจัดทำและพัฒนาสื่อการเรียนรู้ เรื่องภัยคุกคามและอาชญากรรมไซเบอร์และวิธีบรรเทาภัยคุกคามแต่ละประเภท เพื่อใช้ในการยกระดับความตระหนักรู้ของบุคลากร

1.3 ขอบเขตงานวิจัย

1.3.1 ขอบเขตด้านเนื้อหา

งานวิจัยมุ่งเน้นการยกระดับ “ความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์” ของบุคลากรที่ทำงานบนระบบคลาวด์ของคลินิกเอกชน ผ่านสื่อการเรียนรู้ออนไลน์ (Genially-based) ครอบคลุมสาระ 4 ด้าน: (1) ความหมายและความสำคัญของความมั่นคงปลอดภัยไซเบอร์ (2) ประเภทของมัลแวร์ (3) ประเภทของการโจมตีทางไซเบอร์ และ (4) การปฏิบัติปลอดภัยในชีวิตประจำวัน

1.3.2 ขอบเขตด้านประชากร

ขอบเขตด้านประชากร จะแบ่งเป็น 2 กลุ่ม

1.3.2.1 กลุ่มประชากรและกลุ่มตัวอย่างหลักในการวิจัย (Intervention Group)

- ประชากร (Population) บุคลากรผู้ปฏิบัติงานบนระบบคลาวด์ของคลินิกทั้งหมด จำนวน 99 คน ซึ่งเป็นกลุ่มเป้าหมายหลักในการเข้าร่วมโปรแกรมการสร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์
- กำหนดขนาดกลุ่มตัวอย่างโดยใช้สูตรการคำนวณขนาดกลุ่มตัวอย่างของยามาเน่ (Yamane, 1967) ซึ่งเป็นวิธีที่เหมาะสมสำหรับการสุ่มตัวอย่างเชิงความน่าจะเป็น โดยกำหนดความคลาดเคลื่อนที่ยอมรับได้ (Maximum Error/Precision, e) ไม่เกิน 5% (0.05) (ซึ่งจากการคำนวณได้ขนาดกลุ่มตัวอย่างเท่ากับ 79.36 คน) ผู้วิจัยจึงกำหนดขนาดกลุ่มตัวอย่างไว้ที่ 80 คน เพื่อให้การดำเนินการสุ่มตัวอย่างและรวบรวมข้อมูลมีความเหมาะสมและสอดคล้องกับข้อกำหนดทางสถิติ
- กลุ่มตัวอย่าง (Sample) บุคลากรผู้ปฏิบัติงานบนระบบคลาวด์ของคลินิก จำนวน 80 คน
- ใช้วิธี การสุ่มตัวอย่างอย่างง่าย (Simple Random Sampling) ดำเนินการโดยการจัดทำบัญชีรายชื่อประชากรบุคลากรผู้ปฏิบัติงานบนระบบคลาวด์ทั้งหมด จากนั้นจึงทำการสุ่มเลือกบุคลากรให้ได้ครบตามจำนวน เพื่อให้กลุ่มตัวอย่างที่ได้เป็นตัวแทนของประชากรและสอดคล้องกับข้อกำหนดทางสถิติของการวิเคราะห์เชิงปริมาณ (Quantitative Analysis)

1.3.2.2 กลุ่มผู้เชี่ยวชาญสำหรับการตรวจสอบเครื่องมือจำนวน 3 ท่าน

1.3.3 ขอบเขตด้านระยะเวลา

ระยะเวลาในการวิจัยจากการศึกษา วิเคราะห์ ออกแบบและสรุป ระยะเวลา 1 ภาคการศึกษา ตั้งแต่เดือนกรกฎาคม - พฤศจิกายน2568

1.3.4 ขอบเขตด้านเครื่องมือ

1.3.4.1 เครื่องมือทำแบบสอบถามGoogle Form

1.3.4.2 เครื่องมือที่ใช้ทดสอบความเที่ยง,สัมประสิทธิ์,อำนาจตรงของเนื้อหาแบบสอบถามได้แก่ IOC (Index of Item – Objective Congruence)

1.3.4.3 Genially สำหรับสร้างสื่อการเรียนรู้ออนไลน์

1.3.4.4 เครื่องมือที่ใช้ในการวิเคราะห์เปรียบเทียบสรุปผลการวิจัยได้แก่ Excel

1.4 ประโยชน์ของการวิจัย

1.4.1 ทราบถึงระดับความตระหนักรู้ต่อภัยคุกคามไซเบอร์ของบุคลากรในคลินิก เพื่อจะได้นำผลการค้นคว้าอิสระมาเป็นแนวทางในการพัฒนาทักษะของบุคลากรต่อไป

1.4.2 คลินิกได้สื่อการเรียนรู้ส่งเสริมความตระหนักรู้ด้านภัยคุกคามไซเบอร์ที่เหมาะสมกับระดับความตระหนักรู้ของคลินิก

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

การค้นคว้าอิสระนี้จัดทำเพื่อการประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ กรณีศึกษาคลินิกเอกชนแห่งหนึ่ง ทางผู้จัดทำได้ดำเนินการทบทวนแนวคิดทฤษฎี และงานวิจัยที่เกี่ยวข้อง เพื่อนำมาใช้ในการดำเนินการค้นคว้าอิสระและสร้างกรอบแนวคิดสำหรับค้นคว้าอิสระดังนี้

2.1 แนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์
2.2 แนวคิดความมั่นคงปลอดภัยทางไซเบอร์
2.3 แนวคิดเกี่ยวกับความตระหนักรู้ (Awareness)
2.4 สื่อการเรียนการสอน
2.5 ระบบคลาวด์คอมพิวติ้ง (Cloud Computing)
2.6 กรอบแนวคิดในการวิจัย (Conceptual Framework)
2.7 งานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดเกี่ยวกับภัยคุกคามทางไซเบอร์

2.1.1 ภัยคุกคามทางไซเบอร์ (Cyber Threats) หมายถึง ความเสี่ยงหรือการกระทำใด ๆ ที่มีศักยภาพในการทำลายหรือเข้าถึงข้อมูลและระบบสารสนเทศโดยมิชอบ ซึ่งอาจส่งผลกระทบต่อความมั่นคงขององค์กรและความเป็นส่วนตัวของบุคคล [6] การทำความเข้าใจภัยคุกคามในมิติที่กว้างกว่าการโจมตีทางเทคนิคจึงเป็นสิ่งสำคัญ โดยสามารถจำแนกมิติหลักของภัยคุกคามตามแหล่งที่มาและเป้าหมายได้ดังนี้

2.1.1.1 ภัยคุกคามจากมัลแวร์ (Malware Threats) และช่องโหว่ทางเทคนิค

ภัยประเภทนี้เป็นภัยคุกคามทางเทคนิคที่เกี่ยวข้องกับซอฟต์แวร์ที่ถูกออกแบบมาเพื่อสร้างความเสียหายหรือรบกวนการทำงานของระบบ เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) แรนซัมแวร์ (Ransomware) และ สปายแวร์ (Spyware) ซึ่งเป็นสาเหตุหลักของการสูญเสียข้อมูลและทรัพย์สินทางดิจิทัล [2] นอกจากนี้ยังรวมถึงภัยจาก ช่องโหว่ซอฟต์แวร์และแอปพลิเคชัน (Application Vulnerability) ซึ่งผู้โจมตีสามารถใช้เจาะระบบปฏิบัติการหรือแอปพลิเคชันที่บุคลากรใช้งานได้

2.1.1.2 ภัยคุกคามจากวิศวกรรมสังคม (Social Engineering)

เป็นการโจมตีที่อาศัย ช่องโหว่ด้านพฤติกรรม และความไม่ตระหนักรู้ของบุคลากร มากกว่าการเจาะระบบทางเทคนิค โดยผู้ไม่หวังดีจะหลอกลวงหรือชักจูงให้บุคลากรเปิดเผยข้อมูลสำคัญ การโจมตีที่พบบ่อยและมีความเสี่ยงสูงในปัจจุบัน ได้แก่ ฟิชชิง (Phishing) ซึ่งเป็นการส่งอีเมลปลอมหรือเว็บไซต์ปลอม และ การโจมตีด้วยรหัสผ่าน (Password Attack) ผ่านการเดารหัสผ่านหรือใช้เครื่องมืออัตโนมัติ การสร้างความตระหนักรู้และการฝึกอบรมจึงเป็นมาตรการป้องกันที่มีประสิทธิภาพที่สุดสำหรับภัยในกลุ่มนี้ [2]

2.1.1.3 ภัยคุกคามที่เกี่ยวข้องกับระบบคลาวด์และข้อมูล

เนื่องจากระบบคลาวด์เป็นโครงสร้างพื้นฐานที่สำคัญต่อองค์กร การโจมตีจึงมุ่งเน้นไปที่การละเมิดหลักการรักษาความมั่นคงปลอดภัยพื้นฐานอันได้แก่ ความลับ (Confidentiality) ความถูกต้อง (Integrity) และ ความพร้อมใช้ (Availability) (CIA Triad) ภัยที่พบบ่อยในสภาพแวดล้อมคลาวด์ ได้แก่ การกำหนดสิทธิ์ผู้ใช้งานที่ไม่เหมาะสม (Misconfiguration), การใช้รหัสผ่านที่ไม่รัดกุม การรั่วไหลของข้อมูล (Data Breach) และการละเมิดความเป็นส่วนตัวของผู้ใช้ ซึ่งมีผลกระทบโดยตรงต่อการปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) โดยเฉพาะอย่างยิ่งข้อมูลด้านสุขภาพที่มีความอ่อนไหวสูง

2.1.1.4 ภัยคุกคามจากบุคลากรภายใน (Insider Threats) และเครือข่าย

ภัยประเภทนี้เกิดจากบุคลากรที่มีสิทธิ์เข้าถึงข้อมูลอยู่แล้ว ซึ่งอาจทำได้ทั้งโดย ตั้งใจ (เช่น การนำข้อมูลไปขายหรือทำลายระบบ) หรือ ไม่ตั้งใจ เช่น การคลิกลิงก์อันตรายจากอีเมลที่ไม่น่าเชื่อถือ หรือการใช้อุปกรณ์ส่วนตัวที่ไม่มีความปลอดภัย นอกจากนี้ยังรวมถึง การโจมตีเครือข่าย (Network Attack) เช่น การดักจับข้อมูล (Man-in-the-Middle) ซึ่งทั้งหมดนี้สะท้อนความจำเป็นในการเสริมสร้างความตระหนักรู้และพฤติกรรมที่เหมาะสมต่อการใช้งานระบบสารสนเทศในระดับองค์กร [3]

2.1.2 ประเภทของภัยคุกคามทางไซเบอร์

การโจมตีทางไซเบอร์ถูกแบ่งตามกลไกและเป้าหมายของการโจมตี ซึ่งบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ในคลินิกควรตระหนักถึงประเภทต่อไปนี้

2.1.2.1 มัลแวร์ (Malware): หมายถึงซอฟต์แวร์ประสงค์ร้ายที่ถูกออกแบบมาเพื่อแทรกซึมระบบ ทำลาย แก้ไข หรือขโมยข้อมูล เช่น ไวรัส โทรจัน และแรนซัมแวร์ ซึ่งเป็นภัยคุกคามที่พบบ่อยในสถานพยาบาล เนื่องจากระบบคลินิกมักเชื่อมต่อกับอุปกรณ์จำนวนมากและใช้เครือข่ายร่วมกัน หากเกิดการติดมัลแวร์ อาจทำให้ระบบเวชระเบียนไม่สามารถเข้าถึงได้ ส่งผลต่อการให้บริการทางการแพทย์

2.1.2.2 ฟิชชิงและสแกม (Phishing and Scam): เป็นรูปแบบหลักของวิศวกรรมสังคม โดยเป็นการหลอกลวงผู้ใช้ผ่านช่องทางดิจิทัล เช่น อีเมล เว็บไซต์ปลอม หรือข้อความสั้น เพื่อให้เหยื่อเปิดเผยข้อมูลส่วนตัว เช่น รหัสผ่าน หรือข้อมูลบัตรเครดิต [2]

2.1.2.3 การโจมตีด้วยรหัสผ่าน (Password Attack): ความพยายามในการเข้าถึงระบบโดยการเดารหัสผ่าน หรือใช้เครื่องมืออัตโนมัติเพื่อถอดรหัส [4] ซึ่งเน้นย้ำถึงความจำเป็นของการใช้รหัสผ่านที่รัดกุมและการพิสูจน์ตัวตนหลายชั้น

2.1.2.4 การโจมตีเครือข่าย (Network Attack): การโจมตีที่มุ่งเป้าไปที่โครงสร้างพื้นฐานของเครือข่าย เช่น การดักจับข้อมูล (Man-in-the-Middle) หรือการโจมตีเพื่อปฏิเสธการให้บริการ (DoS/DDoS)

2.1.2.5 ภัยคุกคามต่อข้อมูลส่วนบุคคล (Data Breach): การเข้าถึงหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ซึ่งก่อให้เกิดความเสียหายทางกฎหมายและจริยธรรมต่อคลินิกที่ต้องปฏิบัติตาม PDPA [5]

2.2 แนวคิดความมั่นคงปลอดภัยทางไซเบอร์

2.2.1 ความหมายของความมั่นคงปลอดภัยทางไซเบอร์

ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) หมายถึง การปกป้องระบบสารสนเทศ เครือข่ายคอมพิวเตอร์ อุปกรณ์ดิจิทัล และข้อมูลจากภัยคุกคามที่เกิดจากผู้ไม่หวังดี การโจมตี หรือความล้มเหลวของระบบ หลัก CIA Triad เป็นกรอบแนวคิดพื้นฐานในการรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งประกอบด้วยสามองค์ประกอบหลัก ได้แก่ Confidentiality (ความลับ/การรักษาความลับ), Integrity (ความถูกต้อง/ความสมบูรณ์) และ Availability (ความพร้อมใช้งาน) แนวคิดนี้ถูกยอมรับอย่างกว้างขวางทั้งในระดับองค์กรและมาตรฐานสากล เช่น ISO/IEC 27001 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 [6]

2.2.1.1 Confidentiality หมายถึงการปกป้องข้อมูลจากการเข้าถึงโดยผู้ไม่ได้รับอนุญาต โดยใช้เทคนิค เช่น การเข้ารหัสข้อมูล การควบคุมสิทธิ์การเข้าถึง และการใช้รหัสผ่านที่ซับซ้อน เพื่อรักษาความลับของข้อมูลสำคัญ เช่น ข้อมูลผู้ป่วยและข้อมูลธุรกรรมทางการเงิน การสร้างความตระหนักรู้ของบุคลากรในการรักษาความลับถือเป็นสิ่งสำคัญต่อการลดความเสี่ยงด้านภัยคุกคามไซเบอร์ [7], [5]

2.2.1.2 Integrity คือการรักษาความถูกต้องและสมบูรณ์ของข้อมูล ไม่ให้ถูกแก้ไขดัดแปลง หรือสูญหายโดยไม่ได้รับอนุญาต การประเมินความสมบูรณ์ของข้อมูลสามารถทำได้ด้วยเทคนิค เช่น การใช้ค่า Hash, Digital Signature, Checksums และระบบบันทึกเหตุการณ์ เพื่อให้มั่นใจว่าข้อมูลยังคงเชื่อถือได้ งานวิจัยพบว่าการพัฒนาความตระหนักรู้ในการปฏิบัติด้านการเขียนโปรแกรมและการจัดการข้อมูลมีผลต่อความสมบูรณ์ของข้อมูลอย่างมีนัยสำคัญ [4], [2]

2.2.1.3 Availability เป็นการรับประกันว่าข้อมูลและระบบสารสนเทศพร้อมให้บริการแก่ผู้ใช้งานที่ได้รับอนุญาตเมื่อจำเป็น การออกแบบระบบให้มีความพร้อมใช้งานสูงมักใช้การสำรองข้อมูล ระบบคลาวด์ การป้องกัน DDoS และการบำรุงรักษาฮาร์ดแวร์อย่างสม่ำเสมอ นอกจากนี้ การสร้างความตระหนักรู้ของบุคลากรในองค์กรเกี่ยวกับการป้องกันและตอบสนองต่อภัยคุกคามสามารถเพิ่มความพร้อมใช้งานของระบบได้อย่างมีประสิทธิภาพ [8]

ดังนั้น หลัก CIA Triad เป็นรากฐานสำคัญของความมั่นคงปลอดภัยไซเบอร์ที่ช่วยให้องค์กรสามารถป้องกันภัยคุกคาม รักษาความถูกต้องของข้อมูล และทำให้ระบบพร้อมใช้งานได้อย่างต่อเนื่อง การประยุกต์ใช้ต้องอาศัยทั้งเทคโนโลยี กระบวนการ และการสร้างความตระหนักรู้ในบุคลากร เพื่อให้สามารถตอบสนองต่อภัยคุกคามที่ซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็วในยุคดิจิทัล

2.2.2 ความมั่นคงปลอดภัยทางไซเบอร์ครอบคลุมทั้งด้านเทคโนโลยี นโยบาย และพฤติกรรมของผู้ใช้งาน โดยประกอบด้วยหลายแนวคิดสำคัญ ได้แก่

2.2.2.1 การป้องกัน (Prevention) การวางมาตรการเพื่อป้องกันภัยคุกคามไม่ให้เกิดขึ้น เช่น การตั้งค่าระบบเครือข่ายให้ปลอดภัย การติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ และการใช้รหัสผ่านที่มีความซับซ้อน โรงพยาบาลพุทธโสธร เป็นตัวอย่างของการฝึกอบรมบุคลากรให้ระมัดระวังภัยคุกคามทางไซเบอร์ เช่น การเปิดไฟล์แนบอีเมลที่ไม่ทราบแหล่งที่มา [7]

2.2.2.2 การตรวจจับ (Detection) การเฝ้าระวังระบบเพื่อตรวจสอบพฤติกรรมหรือเหตุการณ์ที่อาจเป็นภัยคุกคาม เช่น การใช้ระบบ IDS/IPS (Intrusion Detection/Prevention

System) การวิเคราะห์ Log และการตรวจสอบความผิดปกติของการเข้าถึงข้อมูล บริษัทวิทยุการบินแห่งประเทศไทย จำกัด มีการติดตั้งระบบเฝ้าระวังเครือข่ายเพื่อแจ้งเตือนการเข้าถึงระบบที่ผิดปกติทันที [9]

2.2.2.3 การตอบสนอง (Response) การดำเนินการเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย เช่น การกู้คืนระบบที่ถูกโจมตี การแจ้งเตือนบุคลากร และการปิดช่องโหว่ [10] ระบุว่าการตอบสนองอย่างรวดเร็วเป็นสิ่งสำคัญในการลดผลกระทบต่อระบบสารสนเทศองค์กร

2.2.2.4 การฟื้นฟู (Recovery) การทำให้ระบบกลับมาทำงานได้ตามปกติหลังจากเกิดเหตุการณ์ภัยคุกคาม รวมถึงการวิเคราะห์สาเหตุและปรับปรุงมาตรการป้องกันในอนาคต โรงพยาบาลสระบุรี ได้พัฒนาระบบสำรองข้อมูลและแนวทางฟื้นฟูระบบสารสนเทศ เพื่อให้บริการผู้ป่วยไม่สะดุดแม้เกิดการโจมตีทางไซเบอร์ [11]

2.2.3 ในระดับองค์กร แนวคิดความมั่นคงปลอดภัยทางไซเบอร์ต้องบูรณาการทั้ง People, Process, Technology ได้แก่

2.2.3.1 People (บุคลากร) การสร้างความตระหนักรู้และฝึกอบรมพนักงานให้สามารถระบุภัยคุกคาม เช่น ฟิชชิง การโจมตีรหัสผ่าน และมัลแวร์ ตลอดจนการใช้งานระบบอย่างปลอดภัย เช่น การใช้ VPN หรือระบบยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) [7], [3]

2.2.3.2 Process (กระบวนการ) การกำหนดนโยบาย มาตรการ และแนวปฏิบัติ เช่น การควบคุมการเข้าถึงข้อมูล การสำรองข้อมูล และการรายงานเหตุการณ์ทางไซเบอร์ โรงพยาบาลและหน่วยงานรัฐหลายแห่งได้จัดทำแนวทางปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น การจำกัดสิทธิ์การเข้าถึงข้อมูลผู้ป่วยตามบทบาทหน้าที่ [5]

2.2.3.3 Technology (เทคโนโลยี) การใช้เครื่องมือและเทคโนโลยีเพื่อป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคาม เช่น Firewall, Antivirus, ระบบเฝ้าระวังเครือข่าย และระบบเข้ารหัสข้อมูล [7]

การบริหารความเสี่ยงด้านไซเบอร์ (Cyber Risk Management) เป็นองค์ประกอบสำคัญในการวางแผนมาตรการป้องกันและรับมือ โดยเน้นการประเมินความเสี่ยง การจัดลำดับความสำคัญ และการปรับมาตรการให้เหมาะสมกับระดับความเสี่ยงขององค์กร องค์กรเอกชนในกรุงเทพฯ ที่ทำการสำรวจพบว่าการสร้างความตระหนักรู้ด้านภัยคุกคามและการฝึกอบรมพนักงานช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์ได้อย่างชัดเจน [12]

นอกจากนี้ ในยุคดิจิทัลและ AI การโจมตีรหัสผ่านหรือระบบ IoT สามารถเกิดขึ้นได้รวดเร็วและซับซ้อน จึงจำเป็นต้องพัฒนากลยุทธ์การรักษาความมั่นคงปลอดภัยแบบองค์รวม การสร้างวัฒนธรรมความปลอดภัย (Security Culture) และการปรับปรุงมาตรการอย่างต่อเนื่องเป็นสิ่งจำเป็นสำหรับองค์กรทุกประเภท [13]

จึงสรุปได้ว่า แนวคิดความมั่นคงปลอดภัยทางไซเบอร์ประกอบด้วยการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูระบบ โดยบูรณาการทั้งบุคลากร กระบวนการ และเทคโนโลยี พร้อมทั้งใช้หลักการบริหารความเสี่ยงในการตัดสินใจ เพื่อสร้างระบบสารสนเทศและเครือข่ายที่มั่นคง ปลอดภัย และสามารถรองรับภัยคุกคามในยุคดิจิทัลได้อย่างมีประสิทธิภาพ ตัวอย่างจากโรงพยาบาลและองค์กรไทยช่วยยืนยันความสำคัญของการสร้างความตระหนักรู้และการปฏิบัติตามมาตรการอย่างจริงจัง

2.3 ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)หมายถึงระดับความรู้ ความเข้าใจ และการรับรู้ของบุคลากรเกี่ยวกับภัยคุกคามไซเบอร์ ตลอดจนความสามารถในการปฏิบัติตามมาตรการรักษาความปลอดภัยอย่างเหมาะสม การสร้างความตระหนักรู้ดังกล่าวมีบทบาทสำคัญต่อการป้องกันความเสี่ยงด้านข้อมูลและระบบสารสนเทศขององค์กร โดยเฉพาะในองค์กรที่มีการใช้งาน ระบบคลาวด์ ซึ่งข้อมูลผู้ป่วยและข้อมูลสำคัญขององค์กรถูกเก็บและประมวลผลผ่านเครือข่ายอินเทอร์เน็ต [7], [3]

2.3.1 แนวคิดความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สามารถวิเคราะห์ผ่าน โมเดล Knowledge–Attitude–Behavior (KAB) ซึ่งแบ่งออกเป็นสามองค์ประกอบหลักดังนี้:

2.3.1.1 ความรู้ (Knowledge):บุคลากรต้องมีความเข้าใจเกี่ยวกับภัยคุกคามไซเบอร์ เช่น ฟิชชิง มัลแวร์ การโจมตีด้วยรหัสผ่าน และช่องโหว่ของระบบคลาวด์ รวมถึงมาตรการป้องกัน เช่น การใช้รหัสผ่านที่รัดกุม การเข้ารหัสข้อมูล และการสำรองข้อมูล [2], [4]

2.3.1.2 ทัศนคติ (Attitude):การตระหนักรู้ของบุคลากรไม่ได้หมายถึงเพียงการมีความรู้ แต่รวมถึง ทัศนคติที่รับผิดชอบ และการให้ความสำคัญกับความปลอดภัยของข้อมูล การยอมรับนโยบายและมาตรการด้านความมั่นคงปลอดภัย การเข้าใจผลกระทบของการละเมิดข้อมูล และความเต็มใจในการปฏิบัติตามแนวทางปฏิบัติที่เหมาะสม [3]

2.3.1.3 พฤติกรรม (Behavior):พฤติกรรมของบุคลากรเป็นตัวชี้วัดผลการประเมินความตระหนักรู้ เช่น การตั้งรหัสผ่านที่ซับซ้อน การตรวจสอบอีเมลและไฟล์ที่เข้ามา การปฏิบัติตามนโยบายการเข้าถึงข้อมูลบนระบบคลาวด์ การจัดเก็บและใช้ข้อมูลอย่างปลอดภัย ตลอดจนการรายงานเหตุการณ์ผิดปกติหรือภัยคุกคามทันที [5], [12]

ความมั่นคงปลอดภัยทางไซเบอร์ถือเป็นประเด็นสำคัญในยุคดิจิทัล เนื่องจากภัยคุกคามทางไซเบอร์สามารถส่งผลกระทบต่อความลับของข้อมูล ความถูกต้องของระบบ และความพร้อมใช้งานของบริการ การบริหารความมั่นคงปลอดภัยไซเบอร์จึงต้องอาศัย กรอบกฎหมายและมาตรฐานสากล เพื่อสร้างแนวทางปฏิบัติที่เป็นระบบและลดความเสี่ยงที่อาจเกิดขึ้นต่อองค์กรทั้งภาครัฐและเอกชน กฎหมายความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย ที่สำคัญ ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งกำหนดให้หน่วยงานภาครัฐและเอกชนต้องจัดทำมาตรการป้องกันการโจมตีทางไซเบอร์ และต้องรายงานภัยคุกคามต่อหน่วยงานกำกับดูแลอย่างสม่ำเสมอ [6] นอกจากนี้ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566 [10] ยังช่วยเสริมความชัดเจนในกระบวนการจัดการและการตอบสนองต่อเหตุการณ์ภัยคุกคาม และแนวทางดังกล่าวยังสอดคล้องกับการกำกับดูแลการรับมือภัยคุกคามในระดับองค์กร [14] นอกจากกฎหมายไทยแล้ว มาตรฐานสากล ก็มีบทบาทสำคัญในการกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ เช่น ISO/IEC 27001 ซึ่งเน้นระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ และ ISO/IEC 27005 สำหรับการบริหารความเสี่ยงด้านไซเบอร์ มาตรฐานเหล่านี้ช่วยให้องค์กรสามารถวางนโยบาย การควบคุม และการประเมินความเสี่ยงได้อย่างเป็นระบบ นอกจากนี้ การปฏิบัติตามมาตรฐานสากลยังช่วยสร้างความน่าเชื่อถือ ป้องกันการละเมิดข้อมูลส่วนบุคคล และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ [6]

งานวิจัยหลายชิ้นชี้ให้เห็นว่า ความตระหนักรู้ของบุคลากร เป็นปัจจัยสำคัญในการประยุกต์ใช้กฎหมายและมาตรฐานไซเบอร์อย่างมีประสิทธิภาพ การฝึกอบรมบุคลากรสาธารณสุขหรือบุคลากรองค์กรปกครองส่วนท้องถิ่นช่วยลดความเสี่ยงจากภัยคุกคาม การโจมตีทางดิจิทัล และการรั่วไหลของข้อมูล [7], [2] นอกจากนี้ การบูรณาการแนวทาง Corporate Governance กับมาตรการความมั่นคงปลอดภัยไซเบอร์ช่วยให้องค์กรประเมินความเสี่ยงและติดตามมาตรการป้องกันภัยคุกคามได้อย่างต่อเนื่อง [14]

โดยสรุป การประยุกต์ใช้ กฎหมายและมาตรฐานความมั่นคงปลอดภัยไซเบอร์ ร่วมกับการสร้างความตระหนักรู้และการฝึกอบรมบุคลากร เป็นกลยุทธ์สำคัญที่ช่วยให้องค์กรสามารถป้องกันความเสียหายจากภัยคุกคามไซเบอร์ได้อย่างเป็นระบบ ยั่งยืน และตอบสนองต่อภัยคุกคามดิจิทัลในยุคเทคโนโลยีสูงได้อย่างมีประสิทธิภาพ

2.4 สื่อการเรียนการสอน

2.4.1 ความหมายและความสำคัญของสื่อการเรียนการสอน

สื่อการเรียนการสอนหมายถึง เครื่องมือ วัสดุ อุปกรณ์ หรือระบบที่ใช้ในการถ่ายทอดสาระความรู้จากผู้สอนไปยังผู้เรียน เพื่อช่วยให้ผู้เรียนเกิดความเข้าใจและสามารถพัฒนาทักษะตามเป้าหมายที่ตั้งไว้ สื่อการสอนมีบทบาทสำคัญในการสร้างประสบการณ์ตรง ลดข้อจำกัดด้านเวลาและสถานที่ และช่วยให้การเรียนรู้มีประสิทธิภาพมากยิ่งขึ้น [15]

ในยุคดิจิทัล สื่อการเรียนการสอนได้เปลี่ยนแปลงจากสื่อสิ่งพิมพ์ดั้งเดิมไปสู่สื่อมัลติมีเดีย เช่น วิดีโอ อินโฟกราฟิก เว็บไซต์ แอปพลิเคชัน และสื่อแบบโต้ตอบ (Interactive Media) เช่น Genially ที่ช่วยสร้างการมีส่วนร่วมของผู้เรียนอย่างกระตือรือร้น [16]

2.4.2 ทฤษฎีการเรียนรู้ที่เกี่ยวข้องกับสื่อการสอน

สื่อการสอนสัมพันธ์กับทฤษฎีการเรียนรู้หลากหลายสำนัก ได้แก่

2.4.2.1 แนวคิดการออกแบบการสอนของ Gagné (2005) [17] เน้นกระบวนการเรียนรู้ที่เป็นระบบและเชื่อมโยงระหว่างวัตถุประสงค์ เนื้อหา และกิจกรรมการเรียนรู้ โดย ทฤษฎี 9 ขั้นของกาเย่ ครอบคลุม (1) การดึงดูดความสนใจ (2) การแจ้งวัตถุประสงค์ (3) การกระตุ้นความรู้เดิม (4) การเสนอเนื้อหาใหม่ (5) การให้คำแนะนำแก่การเรียนรู้ (6) การกระตุ้นการแสดงพฤติกรรมการเรียนรู้ (7) การให้ข้อมูลย้อนกลับ (8) การประเมินผลการเรียนรู้ และ (9) การส่งเสริมการคงอยู่และการถ่ายโอนความรู้ไปใช้ สื่อที่ออกแบบดีจะช่วยให้กิจกรรมทั้งเก้าขั้นเกิดขึ้นอย่างเป็นลำดับ ส่งเสริมความเข้าใจเชิงลึกและผลสัมฤทธิ์ทางการเรียนรู้ของผู้เรียน

2.4.2.2 ทฤษฎีการเรียนรู้จากสื่อหลายมิติ [18] อธิบายว่าผู้เรียนจะเข้าใจได้ดีกว่าเมื่อใช้ทั้งข้อความและภาพในการเรียนรู้ การออกแบบสื่อจึงควรหลีกเลี่ยงการนำเสนอข้อมูลที่ซับซ้อนเกินไป และเลือกใช้สื่อที่สอดคล้องกับการประมวลผลของสมอง

2.4.2.3 การออกแบบการสอนอย่างเป็นระบบ [19] เน้นการวิเคราะห์ผู้เรียน วัตถุประสงค์การเรียนรู้ เนื้อหา และการประเมินผล เพื่อเลือกสื่อที่เหมาะสม สะท้อนว่าสื่อไม่ได้เป็นเพียงตัวกลาง แต่เป็นส่วนหนึ่งของระบบการเรียนรู้ที่ต้องออกแบบอย่างรอบคอบ

2.4.3 การพัฒนาสื่อการเรียนการสอนในยุคดิจิทัล

การพัฒนาสื่อการเรียนการสอนในยุคดิจิทัล (Digital Era) เป็นกระบวนการที่เน้นการใช้เทคโนโลยีดิจิทัลมาสนับสนุนการเรียนรู้ โดยไม่เพียงทำหน้าที่เป็น “เครื่องมือถ่ายทอดความรู้” แต่ยังสร้างปฏิสัมพันธ์ (Interactivity) และประสบการณ์การเรียนรู้ (Learning Experience) ที่สอดคล้องกับบริบทของผู้เรียนในศตวรรษที่ 21 ซึ่งมีลักษณะสำคัญคือ การเข้าถึงข้อมูลได้ทุกที่ทุกเวลา การเรียนรู้แบบยืดหยุ่น และการใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือสำคัญ

2.4.3.1 กระบวนการพัฒนาสื่อดิจิทัล

การพัฒนาสื่อการเรียนการสอนยุคดิจิทัลต้องมีการออกแบบที่เป็นระบบ สามารถประยุกต์จากโมเดล ADDIE หรือ Dick & Carey (2015) [19] ได้ โดยสรุปกระบวนการได้ดังนี้

1) การวิเคราะห์ (Analysis)
   - 1.1 ศึกษาลักษณะผู้เรียน (อายุ ความรู้เดิม ความสนใจ)
   - 1.2 กำหนดวัตถุประสงค์การเรียนรู้
   - 1.3 วิเคราะห์บริบทและข้อจำกัดของการใช้สื่อ (เช่น อุปกรณ์ อินเทอร์เน็ต)
2) การออกแบบ (Design)
   - 2.1 วางโครงสร้างบทเรียน (Learning Structure)
   - 2.2 เลือกรูปแบบสื่อ (e-Learning, วิดีโอ, อินโฟกราฟิก, เกมการศึกษา ฯลฯ)
   - 2.3 กำหนดปฏิสัมพันธ์ (Interaction) เช่น แบบทดสอบออนไลน์ ฟอรัม หรือ AR/VR
3) การพัฒนา (Development)
   - 3.1 ใช้เครื่องมือดิจิทัล เช่น Adobe Captivate, Articulate Storyline, Canva, Genially, หรือแพลตฟอร์ม LMS
   - 3.2 ผลิตสื่อในรูปแบบดิจิทัล เช่น วิดีโอแอนิเมชัน อินโฟกราฟิก โมดูลออนไลน์
4) การนำไปใช้ (Implementation)
   - 4.1 ใช้ในชั้นเรียนจริง หรือผ่าน LMS/Platform (เช่น Google Classroom, Moodle, Microsoft Teams)
   - 4.2 มีการอบรมครูและผู้เรียนให้เข้าใจวิธีใช้
5) การประเมินผล (Evaluation)
   - 5.1 ประเมินผลการเรียนรู้ของผู้เรียน (ผลสัมฤทธิ์ทางการเรียน ทักษะที่พัฒนา)
   - 5.2 ประเมินคุณภาพสื่อ (ความน่าสนใจ ความเหมาะสม ความถูกต้องของเนื้อหา)
   - 5.3 นำข้อเสนอแนะมาปรับปรุงสื่อ

2.5 ระบบคลาวด์คอมพิวติ้ง (Cloud Computing)

2.5.1 รูปแบบการให้บริการที่เปิดโอกาสให้ผู้ใช้งานสามารถเข้าถึงทรัพยากรด้านคอมพิวเตอร์ (เช่น เซิร์ฟเวอร์, พื้นที่จัดเก็บข้อมูล, แอปพลิเคชัน หรือบริการ) ผ่านเครือข่ายอินเทอร์เน็ตได้ทุกที่ทุกเวลาตามความต้องการ โดยไม่จำเป็นต้องลงทุนและดูแลโครงสร้างพื้นฐานด้วยตนเอง [20] การวิจัยนี้

เน้นบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ ดังนั้นจึงจำเป็นต้องทำความเข้าใจรูปแบบการให้บริการหลัก 3 รูปแบบ

2.5.1.1 โครงสร้างพื้นฐานในฐานะบริการ (Infrastructure as a Service: IaaS): ผู้ให้บริการดูแลฮาร์ดแวร์ ผู้ใช้ดูแลระบบปฏิบัติการและข้อมูล

2.5.1.2 แพลตฟอร์มในฐานะบริการ (Platform as a Service: PaaS): ผู้ให้บริการดูแลทั้งฮาร์ดแวร์และระบบปฏิบัติการ ผู้ใช้ดูแลเฉพาะแอปพลิเคชันและข้อมูล

2.5.1.3 ซอฟต์แวร์ในฐานะบริการ (Software as a Service: SaaS): ผู้ให้บริการดูแลทั้งหมด ผู้ใช้เข้าถึงและใช้งานซอฟต์แวร์ผ่านเว็บเบราว์เซอร์เท่านั้น ซึ่งเป็นรูปแบบที่ พบบ่อยที่สุดในคลินิก สำหรับการจัดการข้อมูลผู้ป่วยและระบบบริหารจัดการต่างๆ [21]

ตารางที่ 2-1 แสดงความแตกต่างของรูปแบบการให้บริการคลาวด์หลัก 3 รูปแบบ (IaaS, PaaS, SaaS)

ส่วนประกอบของระบบ	On-Premises (ระบบภายใน)	IaaS	PaaS	SaaS
การจัดการข้อมูล	ผู้ใช้รับผิดชอบ (You Manage)	ผู้ใช้รับผิดชอบ	ผู้ใช้รับผิดชอบ	ผู้ให้บริการรับผิดชอบ (Provider Manages)
แอปพลิเคชัน	ผู้ใช้รับผิดชอบ	ผู้ใช้รับผิดชอบ	ผู้ใช้รับผิดชอบ	ผู้ให้บริการรับผิดชอบ
ระบบปฏิบัติการ (OS)	ผู้ใช้รับผิดชอบ	ผู้ใช้รับผิดชอบ	ผู้ให้บริการรับผิดชอบ	ผู้ให้บริการรับผิดชอบ
เครือข่าย/เซิร์ฟเวอร์	ผู้ใช้รับผิดชอบ	ผู้ให้บริการรับผิดชอบ	ผู้ให้บริการรับผิดชอบ	ผู้ให้บริการรับผิดชอบ

ตารางที่ 2-1 แสดงความแตกต่างของรูปแบบการให้บริการคลาวด์หลัก 3 รูปแบบ (IaaS, PaaS, SaaS) โดยเน้นไปที่การแบ่งขอบเขตความรับผิดชอบระหว่าง ผู้ให้บริการคลาวด์ (Cloud Provider) และ ผู้ใช้งาน (คลินิก) ซึ่งมีความสำคัญต่อการกำหนดมาตรการด้านความตระหนักรู้

2.5.2 ความท้าทายด้านความมั่นคงปลอดภัยและความรับผิดชอบร่วมกัน

การใช้งานระบบคลาวด์ทำให้ความรับผิดชอบด้านความปลอดภัยเปลี่ยนแปลงไปจากระบบภายในองค์กรเดิม ซึ่งความเข้าใจผิดในเรื่องนี้ถือเป็นช่องโหว่สำคัญที่สุด การรักษาความมั่นคงปลอดภัยบนคลาวด์ถูกกำหนดด้วยแนวคิด แบบจำลองความรับผิดชอบร่วมกัน (Shared Responsibility Model) ดังนี้

2.5.2.1 ความรับผิดชอบของผู้ให้บริการคลาวด์: รับผิดชอบความปลอดภัย ของระบบคลาวด์ (Security of the Cloud) เช่น การรักษาความปลอดภัยของศูนย์ข้อมูลและโครงสร้างพื้นฐาน

2.5.2.2 ความรับผิดชอบของผู้ใช้งาน (User's Responsibility): รับผิดชอบความปลอดภัย ภายในระบบคลาวด์ (Security in the Cloud) ขอบเขตความรับผิดชอบนี้จะขยายตาม

รูปแบบการให้บริการ (เช่น IaaS ผู้ใช้รับผิดชอบมากที่สุด, SaaS ผู้ใช้รับผิดชอบน้อยที่สุด) แต่โดยทั่วไปแล้ว ความรับผิดชอบที่ผู้ใช้งานต้องจัดการเองเสมอคือ

- การจัดการข้อมูล (Data Management)
- การจัดการสิทธิ์การเข้าถึง (Identity and Access Management: IAM)
- สิทธิ์ผู้ใช้งาน และการใช้ Multi-Factor Authentication
- ความปลอดภัยของผู้ใช้งานเอง (User Security)

การที่บุคลากรขาดความตระหนักรู้และความเข้าใจที่ถูกต้องในขอบเขตความรับผิดชอบของตนเองในการจัดการ ความปลอดภัยภายในคลาวด์ จึงเป็นช่องโหว่ที่ใหญ่ที่สุด [22] งานวิจัยนี้จึงมุ่งเน้นไปที่การประเมินและยกระดับความตระหนักรู้ในส่วนที่บุคลากรต้องรับผิดชอบโดยตรง เพื่อลดความเสี่ยงจากการรั่วไหลของข้อมูลสุขภาพตามหลักการ Shared Responsibility Model

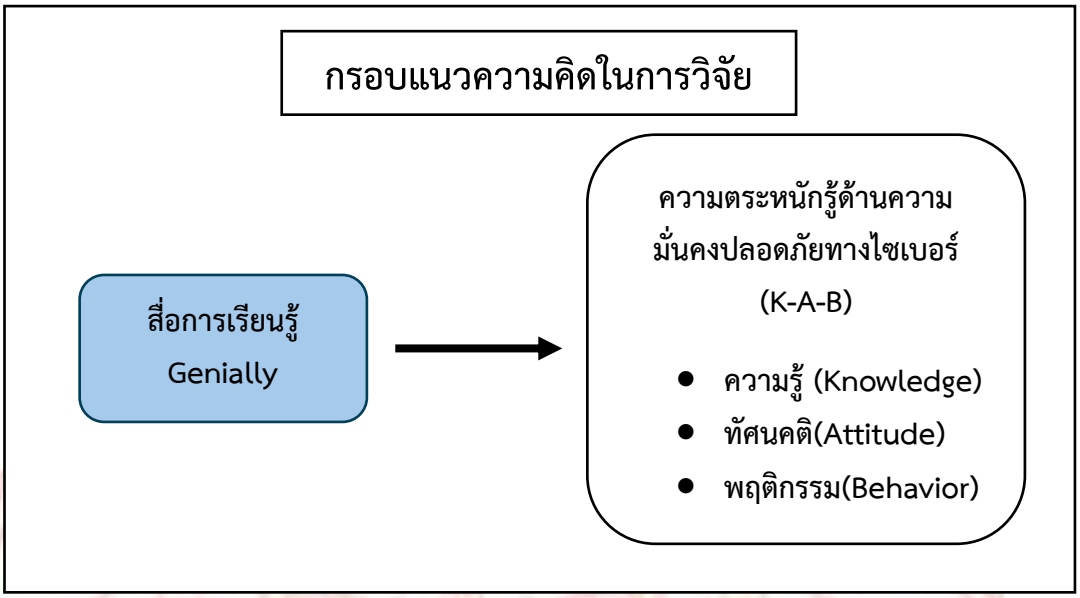
2.6 กรอบแนวคิดในการวิจัย (Conceptual Framework)

การวิจัยนี้มุ่งเน้นศึกษาผลของ สื่อการเรียนรู้แบบออนไลน์ที่สร้างด้วย Genially (ตัวแปรอิสระ) ต่อ ระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ (ตัวแปรตาม) โดยใช้กรอบแนวคิดตามโมเดล K–A–B (Knowledge–Attitude–Behavior) ซึ่งประกอบด้วย 3 มิติ ได้แก่

2.6.1 ความรู้ (Knowledge) — ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ เช่น ฟิชชิง มัลแวร์ การใช้รหัสผ่านที่ปลอดภัย และแนวทางการรักษาความปลอดภัยข้อมูลบนระบบคลาวด์

2.6.2 ทัศนคติ (Attitude) — การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยข้อมูล และความตั้งใจที่จะปฏิบัติตามมาตรการความปลอดภัย

2.6.3 พฤติกรรม (Behavior) — การนำความรู้ไปใช้จริง เช่น การตั้งรหัสผ่านที่รัดกุม การตรวจสอบอีเมลต้องสงสัย และการใช้ระบบคลาวด์อย่างปลอดภัย



ภาพที่ 2-1 กรอบแนวความคิดในการวิจัย

2.7 งานวิจัยที่เกี่ยวข้อง

การทบทวนงานวิจัยที่เกี่ยวข้องมีความสำคัญต่อการกำหนดกรอบแนวคิดและการระบุตำแหน่งของงานวิจัย (Research Gap) เพื่อให้เห็นถึงความแตกต่างและความต่อเนื่องจากองค์ความรู้ที่มีอยู่เดิม งานวิจัยที่เกี่ยวข้องในครั้งนี้แบ่งออกเป็น 2 ประเภท ได้แก่ งานวิจัยเชิงปริมาณ (Quantitative Research) และงานวิจัยเชิงคุณภาพหรือเชิงพัฒนา (Qualitative / Developmental Research) โดยมุ่งเน้นงานที่เกี่ยวข้องกับระบบคลาวด์ (Cloud Computing), ระบบสาธารณสุข (Healthcare) และสื่อดิจิทัลเชิงโต้ตอบ (Interactive Learning Media) เช่น Genially หรือสื่อออนไลน์รูปแบบอื่น

2.7.1 งานวิจัยเชิงปริมาณ (Quantitative Research)

พันธนนท์ [4] ศึกษาระดับความตระหนักรู้เกี่ยวกับภัยคุกคามไซเบอร์ของบุคลากรที่ปฏิบัติงานบนเครือข่ายในองค์กรปกครองส่วนท้องถิ่น โดยใช้แบบสอบถามเป็นเครื่องมือวัดผล พบว่ากลุ่มตัวอย่างส่วนใหญ่มีระดับความตระหนักรู้ในระดับ “ปานกลาง” (ค่าเฉลี่ย = 3.42, SD = 0.65) ปัจจัยที่มีอิทธิพลคือประสบการณ์และการเข้ารับการอบรม ผลการศึกษาชี้ให้เห็นว่า “การอบรมด้านความมั่นคงปลอดภัย” เป็นตัวแปรสำคัญที่ส่งผลต่อพฤติกรรมการใช้งานอย่างปลอดภัย

วิไล ฤทธิเดช [7] ศึกษาความรู้ ความตระหนัก และพฤติกรรมของบุคลากรสาธารณสุขที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของสารสนเทศในโรงพยาบาล พบว่า บุคลากรมีระดับความรู้ในเกณฑ์ “ปานกลาง” และความตระหนักรู้ในระดับ “สูง” แต่พฤติกรรมการรักษาความปลอดภัยยังมีข้อบกพร่อง งานวิจัยนี้สอดคล้องกับโมเดล K–A–B (Knowledge–Attitude–Behavior) ซึ่งเป็นกรอบแนวคิดหลักที่ใช้ในการศึกษาครั้งนี้

วรรษา เปาอินทร์ [5] ทำการพัฒนาแนวทางการจัดการความมั่นคงปลอดภัยของข้อมูลสุขภาพ (Health Data Security) โดยอ้างอิงมาตรฐานสากล เช่น ISO/IEC 27001 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ผลการวิจัยพบว่าแนวทางที่พัฒนาขึ้นมีความเหมาะสมในระดับสูง ครอบคลุมทั้งมาตรการเชิงเทคนิค องค์กร และกฎหมาย

สุภาพร พันธ์ยา และคณะ [24] ศึกษาการตระหนักรู้ของผู้ใช้งานอินเทอร์เน็ตต่อภัยคุกคามจากการคาดเดารหัสผ่าน (Password Attack) โดยใช้การวิจัยเชิงทดลอง (Experimental Research) พบว่าหลังจากได้รับการอบรมและให้ความรู้เกี่ยวกับการตั้งรหัสผ่านที่ปลอดภัย ระดับการตระหนักรู้ของกลุ่มตัวอย่างเพิ่มขึ้นอย่างมีนัยสำคัญทางสถิติ จากการสังเคราะห์จะเห็นได้ว่างานวิจัยเชิงปริมาณส่วนใหญ่ให้ความสำคัญกับการวัดระดับความรู้ ความตระหนัก และพฤติกรรมของบุคลากรก่อนและหลังการอบรม รวมถึงการทดสอบผลสัมฤทธิ์ของสื่อหรือการฝึกอบรม ซึ่งสอดคล้องกับรูปแบบการศึกษาครั้งนี้ที่ใช้สื่อการเรียนรู้แบบโต้ตอบ Genially เพื่อเปรียบเทียบคะแนนก่อนและหลังเรียน

2.7.2 งานวิจัยเชิงคุณภาพและเชิงพัฒนา (Qualitative / Developmental Research)

วันทนีย์ ชัยนาจิตร [23] ศึกษาการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยดิจิทัลของอาสาสมัครสาธารณสุขประจำหมู่บ้าน (อสม.) โดยใช้กิจกรรมเชิงปฏิบัติการ (Workshop) และการสัมภาษณ์สะท้อนผล พบว่าหลังเข้าร่วมกิจกรรม ระดับความตระหนักรู้เพิ่มขึ้นเฉลี่ยร้อยละ 20 และผู้เข้าร่วมสามารถระบุภัยคุกคามดิจิทัลได้ถูกต้องมากขึ้น

วรรษา เปาอินทร์ [5] ใช้วิธีการวิจัยเชิงพัฒนา (Developmental Research) เพื่อสร้างแนวทางการคุ้มครองข้อมูลสุขภาพในโรงพยาบาล โดยเก็บข้อมูลจากการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญและการตรวจสอบความเหมาะสมของแบบจำลอง ผลการวิจัยเสนอแนวทาง 3 ด้าน ได้แก่ มาตรการทางเทคนิค มาตรการทางองค์กร และมาตรการทางกฎหมาย ซึ่งได้รับการประเมินว่ามีความเหมาะสมสูง

DeCarlo [25] ศึกษาการใช้ Gamification เพื่อพัฒนาเครื่องมือเรียนรู้ด้านการป้องกันภัยคุกคามไซเบอร์ โดยเน้นการรับมือกับ Phishing ผ่านสื่อเกมแบบโต้ตอบ ผลการวิจัยพบว่าสื่อดังกล่าวช่วยเพิ่มแรงจูงใจในการเรียนรู้และลดพฤติกรรมเสี่ยงได้อย่างมีประสิทธิภาพ งานวิจัยนี้แสดงให้เห็นถึงความสำคัญของสื่อการเรียนรู้แบบโต้ตอบ (Interactive Learning Media) ซึ่งมีลักษณะใกล้เคียงกับสื่อ Genially ที่ใช้ในการศึกษาครั้งนี้

2.7.3 งานวิจัยที่เกี่ยวข้องกับระบบคลาวด์ (Cloud), ระบบสุขภาพ (Healthcare) และสื่อดิจิทัลเชิงโต้ตอบ (Interactive Learning Media)

งานวิจัยด้านระบบคลาวด์มีบทบาทสำคัญในการกำหนดแนวทางด้านความมั่นคงปลอดภัยสารสนเทศในยุคดิจิทัล โดย Mell และ Grance (2011) [20] ได้ให้คำจำกัดความ “ระบบคลาวด์คอมพิวติ้ง” ว่าเป็นรูปแบบของการให้บริการทรัพยากรคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ต ซึ่งมีคุณสมบัติสำคัญ 5 ประการ ได้แก่ การให้บริการตามความต้องการ การเข้าถึงได้ผ่านเครือข่าย การรวมทรัพยากร ความยืดหยุ่น และการวัดผลการใช้งาน

Hashizume และคณะ (2013) [21] ได้ทำการวิเคราะห์ประเด็นด้านความมั่นคงปลอดภัยของระบบคลาวด์ในมิติต่าง ๆ เช่น ความเป็นส่วนตัว การควบคุมสิทธิ์เข้าถึง การพิสูจน์ตัวตน และการป้องกันข้อมูลสูญหาย ผลการวิเคราะห์พบว่าปัญหาส่วนใหญ่เกิดจากการขาดมาตรการควบคุมที่ชัดเจนในชั้นการให้บริการ

วรรษา เปาอินทร์ (2565) [5] ได้ทำการพัฒนาแนวทางปฏิบัติเพื่อพัฒนาความมั่นคงปลอดภัยและความเป็นส่วนตัวของข้อมูลสุขภาพในโรงพยาบาล โดยนำมาตรฐาน PDPA และแนวคิด Cloud Security มาประยุกต์ใช้กับระบบฐานข้อมูลผู้ป่วย ซึ่งสะท้อนถึงการบูรณาการระหว่างระบบคลาวด์กับความมั่นคงปลอดภัยทางสุขภาพ

จากการทบทวนงานวิจัยที่เกี่ยวข้องทั้งในและต่างประเทศ พบว่ามีประเด็นร่วมกันอยู่หลายประการ กล่าวคือ งานวิจัยส่วนใหญ่ให้ความสำคัญกับการประเมิน ระดับความรู้ ความตระหนัก และพฤติกรรมด้านความปลอดภัยทางไซเบอร์ (K–A–B Model) โดยใช้แบบสอบถามหรือสื่ออบรมออนไลน์เป็นเครื่องมือหลัก เช่น งานของ พันธนนท์ (2566) [4] และ วิไล ฤทธิเดช (2565) [7] ที่พบว่าการอบรมสามารถเพิ่มระดับความตระหนักรู้ได้อย่างมีนัยสำคัญทางสถิติ รวมถึงงานของ DeCarlo (2020) [25] ที่ใช้แนวคิด Gamification เพื่อสร้างแรงจูงใจในการเรียนรู้และลดพฤติกรรมเสี่ยงจากฟิชชิง (Phishing) ได้อย่างมีประสิทธิภาพ

ขณะเดียวกัน งานของ วรรษา เปาอินทร์ (2565) [5] และ Hashizume et al. (2013) [21] ได้เน้นประเด็นด้าน ความมั่นคงปลอดภัยข้อมูลสุขภาพ (Health Data Security) และ ความปลอดภัยของระบบคลาวด์ (Cloud Security) ซึ่งเป็นบริบทสำคัญขององค์กรสาธารณสุขในยุคดิจิทัล โดยเน้นการประยุกต์ใช้มาตรฐานสากล เช่น ISO/IEC 27001 และ PDPA ในการพัฒนาแนวทางการคุ้มครองข้อมูล

อย่างไรก็ตาม งานวิจัยที่กล่าวมาข้างต้นส่วนใหญ่ ยังมุ่งเน้นเฉพาะการให้ความรู้หรือการอบรมทั่วไป โดยไม่ได้ออกแบบสื่อการเรียนรู้เชิงโต้ตอบเฉพาะสำหรับบุคลากรสาธารณสุขในระบบคลาวด์ ซึ่งมีความเสี่ยงเฉพาะด้านข้อมูลผู้ป่วยที่ต้องคุ้มครองตามกฎหมาย PDPA

ดังนั้น งานวิจัยฉบับนี้จึงมี ลักษณะต่อยอด (Extension) จากงานวิจัยก่อนหน้าใน 3 มิติหลัก ได้แก่

- ด้านเครื่องมือ (Tool Innovation) พัฒนา สื่อการเรียนรู้แบบโต้ตอบด้วยแพลตฟอร์ม Genially ที่ผสมผสานภาพ เสียง และสถานการณ์จำลอง เพื่อเพิ่มการมีส่วนร่วมและความเข้าใจเชิงลึก
- ด้านวิธีวิจัย (Methodology) ใช้การออกแบบการวิจัยแบบ Pre–Post Experimental Design เพื่อวัดการเปลี่ยนแปลงจริงของคะแนนก่อนและหลังเรียน พร้อมทดสอบสมมติฐานด้วย Paired Samples t-test
- ด้านบริบทการประยุกต์ (Contextual Application) มุ่งเน้นกลุ่มเป้าหมายบุคลากรคลินิกเอกชนที่ปฏิบัติงานบนระบบคลาวด์ ซึ่งจากการทบทวนเอกสารที่เข้าถึงได้พบว่ายังมีหลักฐานเชิงประจักษ์ในบริบทนี้จำกัด จึงมีความจำเป็นต้องพัฒนาและประเมินสื่อการเรียนรู้แบบโต้ตอบให้เหมาะสมกับสภาพแวดล้อมดังกล่าว

การศึกษาครั้งนี้จึงเป็นการนำแนวคิด K–A–B Model มาบูรณาการเข้ากับเทคโนโลยีการเรียนรู้สมัยใหม่ เพื่อสร้างแนวทางใหม่ในการยกระดับความตระหนักรู้และพฤติกรรมความปลอดภัยทางไซเบอร์อย่างมีประสิทธิผลในภาคสาธารณสุขยุคดิจิทัล

บทที่ 3
วิธีการดำเนินการวิจัย

การศึกษาครั้งนี้เป็นการวิจัยเชิงปริมาณ (Quantitative Research) โดยใช้รูปแบบการวิจัยเชิงสำรวจ (Survey Research) มีวัตถุประสงค์เพื่อประเมินระดับความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ กรณีศึกษาคลินิกเอกชน

โดยผู้จัดทำได้ดำเนินการศึกษาค้นคว้าอิสระตามขั้นตอน ดังนี้

3.1 กระบวนการดำเนินการวิจัย

3.2 การกำหนดกลุ่มประชากรกลุ่มตัวอย่าง

3.3 การจัดทำเครื่องมือที่ใช้ในการวิจัย

3.4 จัดทำสื่อการเรียนรู้ออนไลน์

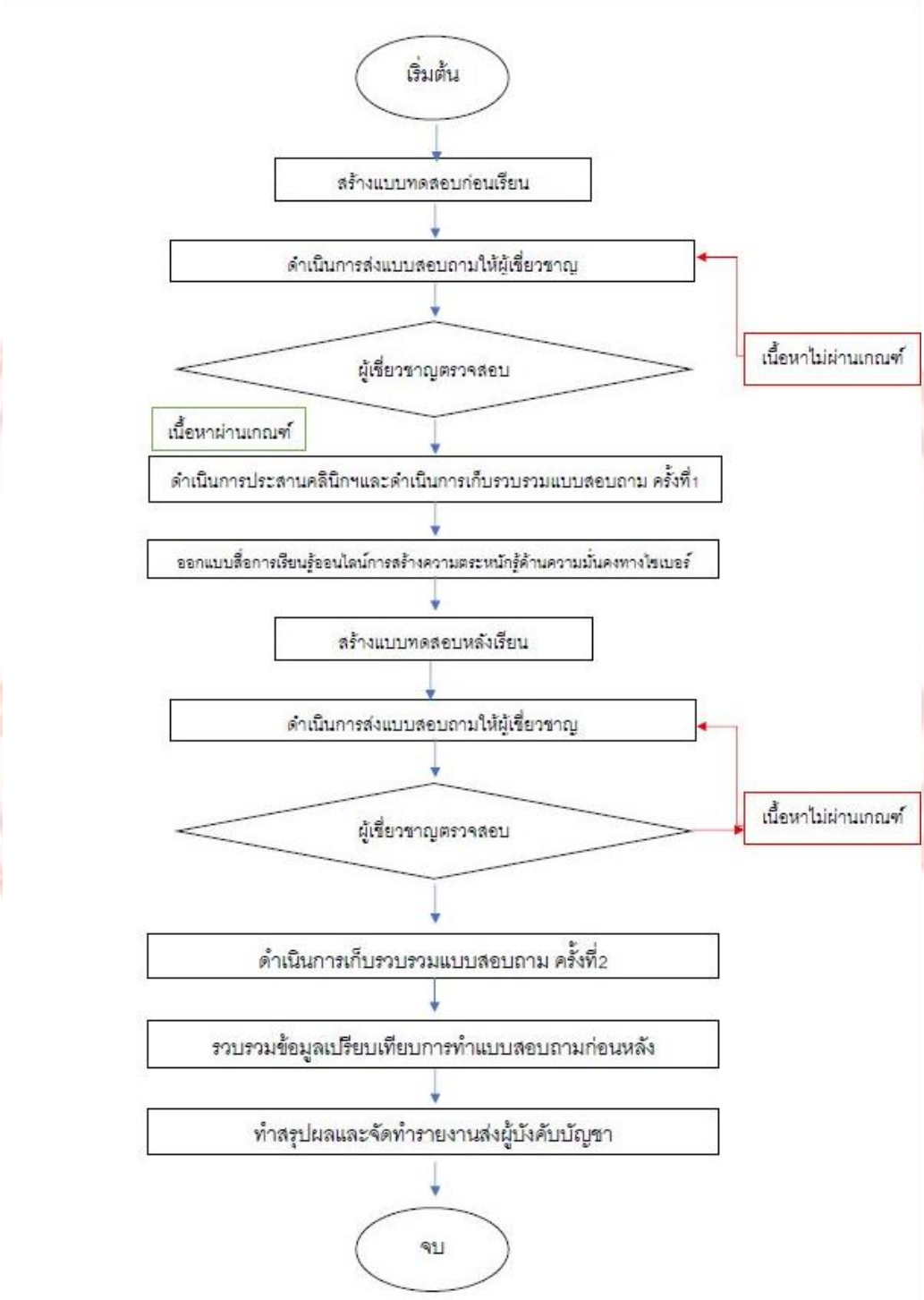
3.5 การเก็บและรวบรวมข้อมูล

3.6 การวิเคราะห์ข้อมูล

3.1 กระบวนการดำเนินการวิจัย

กระบวนการวิจัยในการศึกษาครั้งนี้ประกอบด้วยขั้นตอนที่เป็นลำดับอย่างเป็นระบบ ดังแสดงในภาพที่ 3-1 โดยเริ่มจากการสร้างแบบทดสอบก่อนเรียนเพื่อใช้เป็นเครื่องมือในการประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ จากนั้นดำเนินการส่งแบบทดสอบให้ผู้เชี่ยวชาญจำนวน 3 ท่านตรวจสอบความสอดคล้องของข้อคำถามกับวัตถุประสงค์ของการวัดตามดัชนีความสอดคล้องของข้อคำถาม (Index of Item-Objective Congruence: IOC) โดยกำหนดเกณฑ์การยอมรับไว้ที่ค่า IOC ≥ 0.50 หากรายการใดไม่ผ่านเกณฑ์จะดำเนินการปรับปรุงแก้ไขก่อนนำไปใช้จริง เมื่อเครื่องมือผ่านการตรวจสอบแล้ว ผู้วิจัยได้ประสานงานกับคลินิกเอกชนที่เป็นกรณีศึกษาเพื่อเก็บข้อมูลแบบทดสอบก่อนเรียนครั้งที่ 1 จากบุคลากรกลุ่มตัวอย่าง เพื่อนำผลคะแนนที่ได้มาวิเคราะห์เป็นค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน เพื่อสะท้อนระดับความรู้พื้นฐานเบื้องต้น จากนั้นผู้วิจัยได้ออกแบบและพัฒนาสื่อการเรียนรู้ออนไลน์ว่าด้วยการสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ และจัดให้บุคลากรกลุ่มตัวอย่างได้ใช้งานสื่อดังกล่าว ภายหลังการเรียนรู้ ผู้วิจัยสร้างแบบทดสอบหลังเรียนและดำเนินการให้ผู้เชี่ยวชาญตรวจสอบความเหมาะสมเช่นเดียวกับแบบทดสอบก่อนเรียน เมื่อผ่านการตรวจสอบแล้ว จึงดำเนินการทดสอบครั้งที่ 2 (หลังเรียน) จากนั้นนำผลการทำแบบทดสอบก่อนและหลังเรียนมาวิเคราะห์เปรียบเทียบความแตกต่างของคะแนนด้วยสถิติ Paired Samples t-test เพื่อประเมินประสิทธิภาพของสื่อการเรียนรู้ที่ใช้ สุดท้าย ผู้วิจัยได้รวบรวม วิเคราะห์ และสรุปผลการวิจัย พร้อมจัดทำรายงานเพื่อนำเสนอแก่ผู้บังคับบัญชาต่อไป

ภาพรวมกระบวนการดำเนินการวิจัย (Process Diagram)



ภาพที่3-1 ขั้นตอนกระบวนการดำเนินงาน (Process Diagram)

3.2 การกำหนดประชากรกลุ่มตัวอย่าง

3.2.1 ประชากรที่ใช้ในการวิจัยในครังนี้ ประชากรกลุ่มตัวอย่างที่ใช้ในการศึกษา คือบุคคลากรของคลินิกฯ จำนวน 100 คน

3.2.2 การกำหนดขนากลุ่มตัวอย่าง

ขนาดตัวอย่างในการค้นคว้าครั้งนี้ ผู้ศึกษาได้กำหนดขนาดของกลุ่มตัวอย่างจามสูตรของทาโร ยามาเน่ (Taro Yamane ,1967) โดยกำหนดความคลาดเคลื่อนไม่เกิน 5% ดังนั้นขนาดของกลุ่มตัวอย่างจะคำนวณดังสมการที่ 3-1

$$n = N / (1 + N e^2) \qquad (3\text{-}1)$$

เมื่อ N = ขนาดของประชากร

n = ขนาดของกลุ่มตัวอย่าง

e = ค่าความคลาดเคลื่อนของกลุ่มตัวอย่างกำหนดให้เท่ากับ 0.05

แทนค่าในสูตร

ค่า: $N = 99, e = 0.05 \Rightarrow n = 99 / (1 + 99(0.05)^2) \approx 79.36 \Rightarrow$ ปัดเป็น 80 คน

จากการคำนวณข้างต้นพบว่า ขนาดกลุ่มตัวอย่างที่เหมาะสมคือ 80 คน ซึ่งเพียงพอสำหรับการวิจัยเชิงปริมาณในระดับความเชื่อมั่น 95%.

3.3 การสร้างเครื่องมือที่ใช้ในวิจัย

3.3.1 ขั้นตอนในการสร้างเครื่องมือที่ใช้ในการค้นคว้าอิสระในงานวิจัยในครั้งนี้ ใช้วิธีการทำแบบทดสอบ ซึ่งในการออกแบบชุดคำถาถามในครั้งนี้นั้น ทางผู้วิจัยได้ทำการสร้างขึ้นเอง และได้กำหนดลักษณะของเครื่องมือในการวิจัย ดังนี้

ตอนที่ 1 ลักษณะทางประชากร เกี่ยวกับปัจจัยส่วนบุคคล จำนวน 5 ข้อ ได้แก่ เพศ อายุ ระดับการศึกษา ระดับตำแหน่ง และระยะเวลาการทำงานที่เกี่ยวข้องกับระบบคอมพิวเตอร์

ตอนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ จำนวน 25 ข้อ ประกอบด้วย 4 หัวข้อ ได้แก่

1.ความหมายและความสำคัญของ Cyber Security

2.ประเภทของมัลแวร์

3.ประเภทการโจมตีทางไซเบอร์

4.ความตระหนักรู้ด้าน Cyber Security ในชีวิตประจำวัน

3.3.2 สร้างชุดคำถามเพื่อศึกษาความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ จำนวน 25 ข้อ โดยข้อที่ถูกต้องจะได้ 1 คะแนน ผู้วิจัยได้กำหนดเกณฑ์การแปลผลคะแนนแบบทดสอบความรู้ ซึ่งมีคะแนนเต็ม 25 คะแนน โดยอ้างอิงหลักการทางการศึกษาและทฤษฎีการเรียนรู้ (Bloom, 1956) พร้อมใช้เกณฑ์ร้อยละของคะแนนที่ได้รับ เพื่อนำมาใช้จำแนกระดับความรู้ของผู้ตอบแบบสอบถาม ดังนี้

ค่าเฉลี่ยคะแนน	การแปลผล
0–12 คะแนน (ต่ำกว่า 50%)	ระดับความรู้น้อย
13–17 คะแนน (50–69%)	ระดับความรู้ปานกลาง
18–25 คะแนน (70% ขึ้นไป)	ระดับความรู้มาก

3.3.3 ผู้เชี่ยวชาญประเมินความสอดคล้องของแบบสอบถาม ตรวจสอบคุณภาพของเครื่องมือโดยผู้เชี่ยวชาญ จำนวน 3 ท่าน ทำการประเมินวามสอดคล้องของข้อคำถามในเครื่องมือ โดยมีหลักให้คะแนนดังนี้

คะแนน	แปลผล
+1	เมื่อข้อคำถามสอดคล้องกับวัตถุประสงค์
0	เมื่อไม่แน่ใจข้อคำถามสอดคล้องกับวัตถุประสงค์
-1	เมื่อข้อคำถามไม่สอดคล้องกับวัตถุประสงค์

นำผลประเมินจากผู้เชี่ยวชาญาคำนวณหาค่าดัชนีความสอดคล้อง (IOC : Index of Item – Objective Congruence) โดยเลือกข้อคำถามที่มีค่า IOC มากกว่า 0.5 จากผู้เชี่ยวชาญ จำนวน 3 ท่าน จากนั้นนำผลวิเคราะห์ความสอดคล้อง ข้อคิดเห็น และนำคำแนะนำต่างๆ มาปรับปรุงแก้ไข

3.4 การเก็บรวบรวมข้อมูล

การวิจัยครั้งนี้ได้เก็บรวบรวมข้อมูลที่ได้จากทำแบบทดสอบจากชุดคำถาม ก่อนและหลัง ดูสื่อการเรียนรู้ออนไลน์ เพื่อยกระดับตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ ตามวัตถุประสงค์ ขั้นตอนการดำเนินการดังนี้

3.4.1 ผู้วิจัยได้ดำเนินการประสานงานกับคลินิกฯ และนำแบบทดสอบที่ได้รับการปรับปรุงตามข้อเสนอแนะของผู้เชี่ยวชาญ มอบให้ผู้ประสานงานของคลินิกฯ พร้อมทั้งชี้แจงวัตถุประสงค์ของการวิจัยเป็นลายลักษณ์อักษรไว้อย่างชัดเจน การเก็บรวบรวมข้อมูลเริ่มดำเนินการตั้งแต่เดือนสิงหาคม ถึงเดือนกันยายน พ.ศ. 2568

3.4.2 ผู้วิจัยได้นำแบบทดสอบก่อนเรียน (Pre-test) ที่จัดทำในรูปแบบแบบทดสอบออนไลน์ผ่าน Google Form ให้บุคลากรของคลินิกฯ ทำก่อนดูสื่อการเรียนรู้ออนไลน์เรื่องการสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ ทั้งนี้ แบบสอบถามครั้งที่ 1 มีวัตถุประสงค์เพื่อเก็บรวบรวมข้อมูลผลคะแนนความรู้และความตระหนักรู้เบื้องต้นของบุคลากร ก่อนการเข้ารับชมสื่อการเรียนรู้ดังกล่าว

3.4.3 ผู้วิจัยได้จัดให้บุคลากรของคลินิกได้ดูสื่อการเรียนรู้ออนไลน์ว่าด้วยการสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ โดยสื่อการเรียนรู้ดังกล่าวนำเสนอความรู้เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ครอบคลุมเนื้อหาสำคัญ 4 หัวข้อ ได้แก่ 1) ความหมายและความสำคัญของ Cyber Security 2) ประเภทของมัลแวร์ 3) ประเภทของการโจมตีทางไซเบอร์ และ 4) ความตระหนักรู้ด้าน Cyber Security ในชีวิตประจำวัน ทั้งนี้ หลังจากที่บุคลากรได้เข้ารับชมสื่อการเรียนรู้เรียบร้อยแล้ว ผู้วิจัยทำการออกแบบแบบทดสอบหลังเรียน จากนั้นส่งแบบทดสอบให้ผู้เชี่ยวชาญตรวจสอบความ

ถูกต้อง ผู้วิจัยได้ดำเนินการให้ทำแบบทดสอบหลังเรียน (Post-test) โดยจัดทำในรูปแบบแบบทดสอบออนไลน์ผ่าน Google Form เช่นเดียวกับครั้งแรก แบบสอบถามครั้งที่ 2 นี้มีวัตถุประสงค์เพื่อประเมินผลสัมฤทธิ์ทางการเรียนรู้และตรวจสอบการเปลี่ยนแปลงด้านความรู้ ความเข้าใจ รวมถึงระดับความตระหนักรู้ของบุคลากรเกี่ยวกับความมั่นคงทางไซเบอร์หลังการดูสื่อการเรียนรู้

3.5 การวิเคราะห์ข้อมูล

ผู้วิจัยได้ทำการวิเคราะห์ข้อมูลตามแนวทางสถิติเชิงพรรณนา (Descriptive Statistics) เพื่ออธิบายลักษณะทางประชากร และข้อมูลทั่วไปของกลุ่มตัวอย่างที่เข้าร่วมการศึกษา โดยใช้การคำนวณค่าสถิติ ได้แก่ ค่าสัดส่วนร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน ค่าสูงสุด ค่าต่ำสุด และร้อยละของค่าเฉลี่ย ข้อมูลเชิงอนุมานวิเคราะห์ด้วยสถิติ t-test แบบกลุ่มตัวอย่างสัมพันธ์ (Paired Samples t-test) เพื่อเปรียบเทียบคะแนนก่อน–หลังเรียน และรายงานขนาดอิทธิพล (Effect Size) ประเภท Cohen's dz สำหรับการทดสอบแบบจับคู่ โดยคำนวณจากสูตร $dz = t/\sqrt{n}$ เพื่อแปลความหมายความแรงของผลตามเกณฑ์มาตรฐาน นอกจากนี้ ผู้วิจัยได้ใช้ Google Forms เป็นเครื่องมือในการเก็บรวบรวมข้อมูล และนำข้อมูลที่ได้มาวิเคราะห์เพื่อหาค่าสถิติภาพรวม โดยคำนึงถึงเหตุผลทางวิชาการเป็นหลัก และมิได้นำข้อมูลหรือรายละเอียดส่วนบุคคลของผู้เข้าร่วมการศึกษา

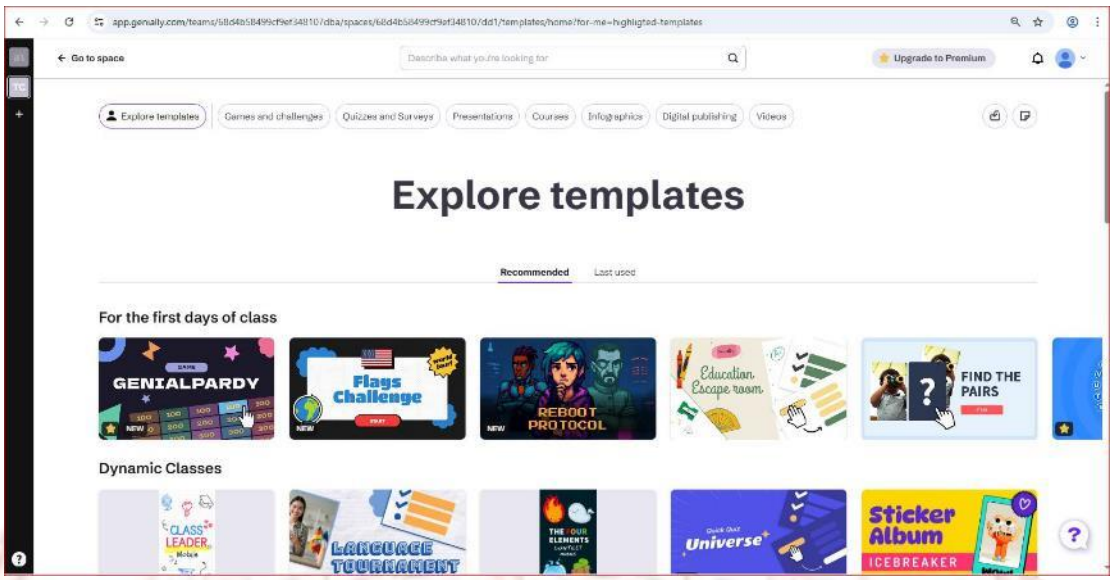
3.6 การจัดทำสื่อออนไลน์

การวิจัยครั้งนี้ได้ใช้เครื่องมือ Genially ซึ่งเป็นโปรแกรมสำเร็จรูปสำหรับการสร้างสื่อการเรียนรู้ออนไลน์แบบเชิงโต้ตอบ (Interactive) ผู้วิจัยได้นำโปรแกรมดังกล่าวมาพัฒนาเป็นสื่อการเรียนรู้เพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมีขั้นตอนการดำเนินงานดังนี้

3.6.1 การวิเคราะห์ผลการทดสอบก่อนเรียน (Pretest Analysis) ผู้วิจัยทำการเก็บข้อมูลคะแนนก่อนเรียนของกลุ่มตัวอย่าง และวิเคราะห์ผลเพื่อสะท้อนระดับความรู้พื้นฐานในด้านความมั่นคงปลอดภัยทางไซเบอร์ ผลการวิเคราะห์ดังกล่าวถูกนำมาใช้เป็นข้อมูลตั้งต้นในการออกแบบและจัดทำสื่อการเรียนรู้ให้เหมาะสมกับผู้เรียน

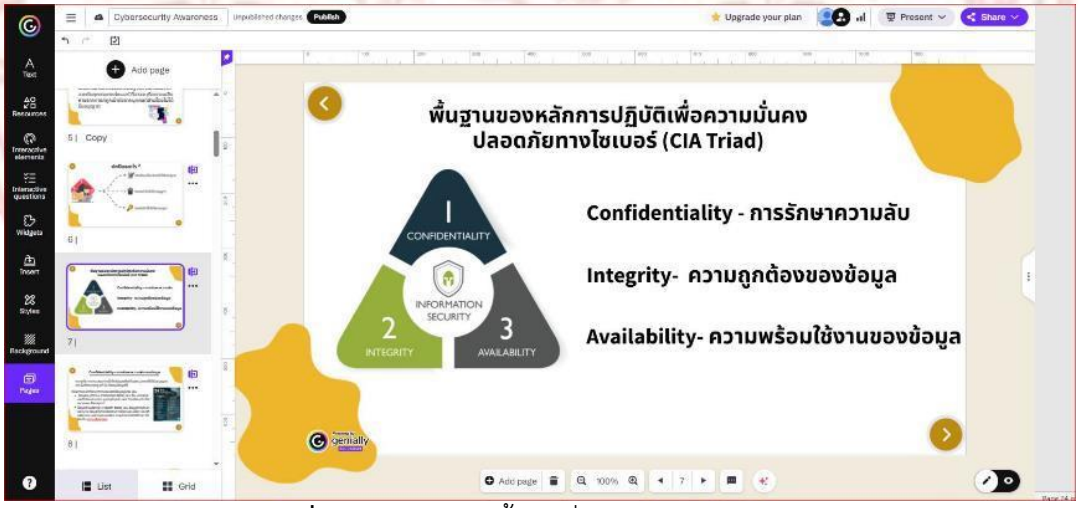
3.6.2 ในการออกแบบสื่อการเรียนรู้ ผู้วิจัยอ้างอิงแนวคิดของ Gagné (2005) [17] ซึ่งประกอบด้วยขั้นตอนสำคัญ เช่น การสร้างแรงจูงใจให้ผู้เรียน การนำเสนอเนื้อหาอย่างเป็นลำดับ การสร้างโอกาสในการโต้ตอบกับสื่อ และการทบทวนเพื่อเสริมความจำระยะยาว โดยโครงสร้างเนื้อหาถูกจัดเรียงให้ไล่ระดับจากบทนำ แนวคิดพื้นฐาน ตัวอย่างภัยคุกคามที่พบบ่อย วิธีป้องกัน ไปจนถึงแนวทางปฏิบัติจริงที่สามารถประยุกต์ใช้ในงานประจำ

3.6.3 ผู้วิจัยเลือกใช้เทมเพลตสำเร็จรูปที่ Genially จัดเตรียมไว้ โดยพิจารณาให้สอดคล้องกับเนื้อหา วัตถุประสงค์การเรียนรู้ และลักษณะผู้เรียน เทมเพลตที่เลือกช่วยให้การนำเสนอมีรูปแบบที่เป็นระบบ ชัดเจน และสามารถปรับแต่งเพิ่มเติมได้ตามความเหมาะสม ซึ่งส่งผลให้สื่อมีความเป็นมืออาชีพและดึงดูดความสนใจของผู้เรียนมากขึ้น ดังภาพที่ 3-2



ภาพที่ 3-2 รูปแบบของสื่อการเรียนรู้ (Templates)

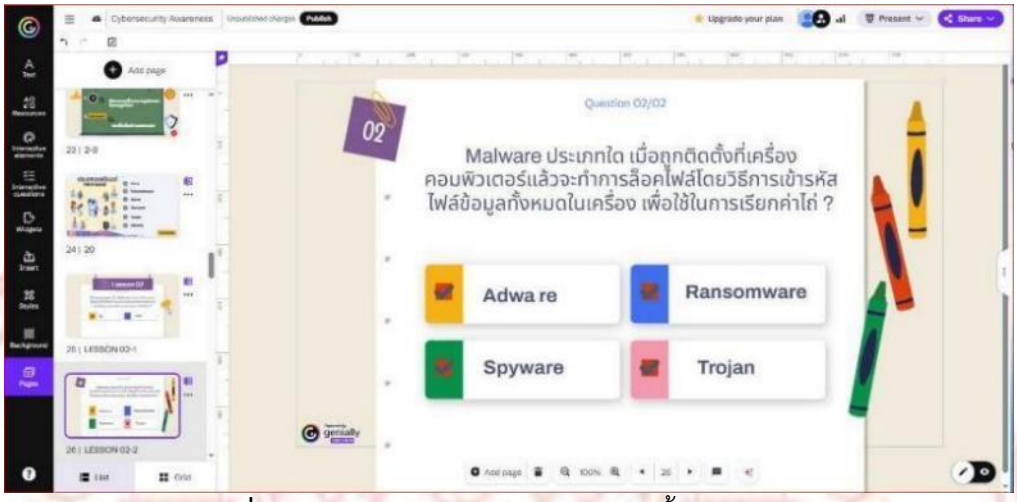
3.6.4 ผู้วิจัยนำเนื้อหาที่ได้จากการวิเคราะห์มาออกแบบเป็นสื่อการเรียนรู้ โดยจัดเรียงข้อความ รูปภาพ วิดีโอ และสื่อประกอบอื่น ๆ ลงในพื้นที่การนำเสนออย่างมีลำดับขั้นตอน เน้นความชัดเจน กระชับ และเชื่อมโยงกับวัตถุประสงค์การเรียนรู้ เพื่อให้ผู้เรียนสามารถทำความเข้าใจได้ง่าย และเกิดการเรียนรู้ที่ต่อเนื่อง นอกจากนี้ยังมีการเลือกใช้โทนสี ตัวอักษร และองค์ประกอบกราฟิกที่เหมาะสม เพื่อเพิ่มความสวยงามและความน่าสนใจของสื่อ ดังภาพที่ 3-3



ภาพที่ 3-3 การแทรกเนื้อหาที่ต้องการลงบนเทมเพลต

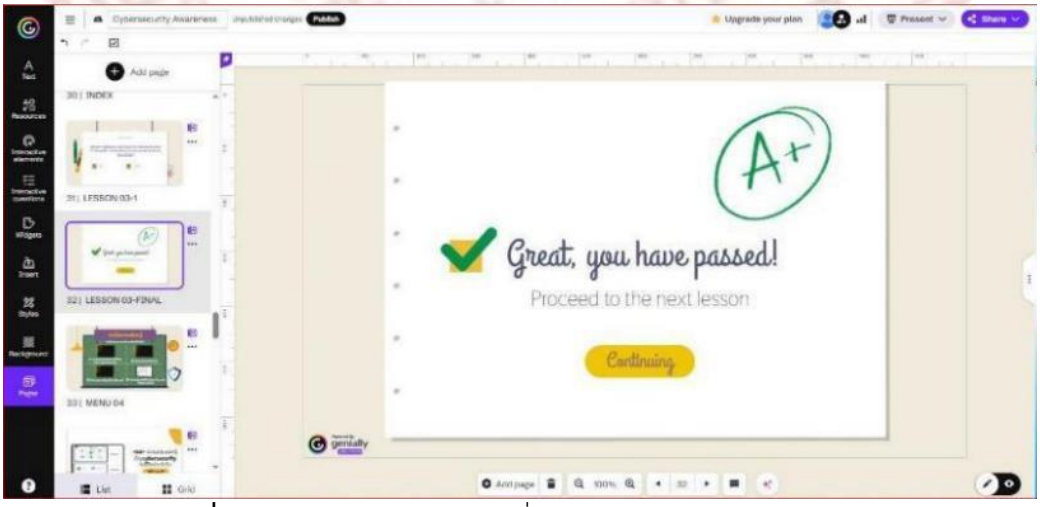
3.6.5 การปรับแต่งองค์ประกอบเชิงโต้ตอบ (Interactive Customization) เพื่อกระตุ้นการมีส่วนร่วมของผู้เรียน ผู้วิจัยได้เพิ่มฟังก์ชันเชิงโต้ตอบ เช่น การใส่ข้อคำถามเพื่อวัดความเข้าใจเบื้องต้นเกี่ยวกับเนื้อหาที่แสดงให้ผู้เรียนเห็น การสร้างปุ่มกดเพื่อนำทางไปยังเนื้อหาส่วนต่าง ๆ การเชื่อมโยงลิงก์ไปยังสื่อหรือแหล่งข้อมูลเพิ่มเติม และการใช้แอนิเมชันเพื่อช่วยอธิบายเนื้อหาที่ซับซ้อน ทั้งนี้ การ

ออกแบบองค์ประกอบเชิงโต้ตอบยังช่วยให้ผู้เรียนสามารถมีปฏิสัมพันธ์กับสื่อได้มากขึ้น ลดความจำเจจากการเรียนรู้แบบอ่านหรือฟังเพียงอย่างเดียว และเสริมสร้างประสบการณ์การเรียนรู้ที่มีความหมายและจดจำได้ง่าย ดังภาพที่ 3-4

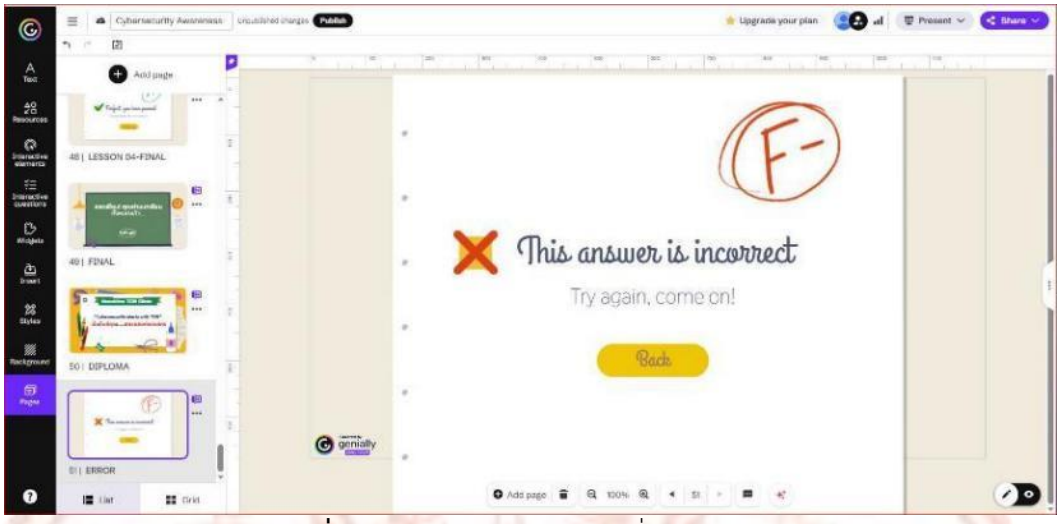


ภาพที่ 3-4 การใส่ข้อคำถามแทรกระหว่างเนื้อหาแต่ละส่วน

เมื่อผู้เรียนตอบคำถามได้ถูกต้อง ระบบจะอนุญาตให้เข้าสู่บทเรียนในลำดับถัดไป ซึ่งช่วยเสริมสร้างแรงจูงใจและความมั่นใจในการเรียนรู้ อย่างไรก็ตาม หากผู้เรียนตอบคำถามไม่ถูกต้อง ระบบจะถูกออกแบบให้ย้อนกลับไปยังหน้าที่มีเนื้อหาที่เกี่ยวข้องกับคำถามดังกล่าว เพื่อให้ผู้เรียนได้มีโอกาสทบทวน ทำความเข้าใจ และเรียนรู้ซ้ำในส่วนที่ยังมีข้อบกพร่อง กระบวนการดังกล่าวถือเป็นการส่งเสริมการเรียนรู้แบบมีปฏิสัมพันธ์ (Interactive Learning) และช่วยให้ผู้เรียนสามารถเรียนรู้ด้วยตนเอง (Self-directed Learning) ได้อย่างมีประสิทธิภาพ อีกทั้งยังทำให้ผู้เรียนเกิดการเรียนรู้อย่างต่อเนื่อง ไม่เพียงแต่จดจำคำตอบที่ถูกต้อง แต่ยังเข้าใจเนื้อหาที่อยู่เบื้องหลังคำตอบนั้นอย่างถ่องแท้ ตัวอย่างการทำงานของระบบแสดงไว้ในภาพที่ 3-5 และ 3-6



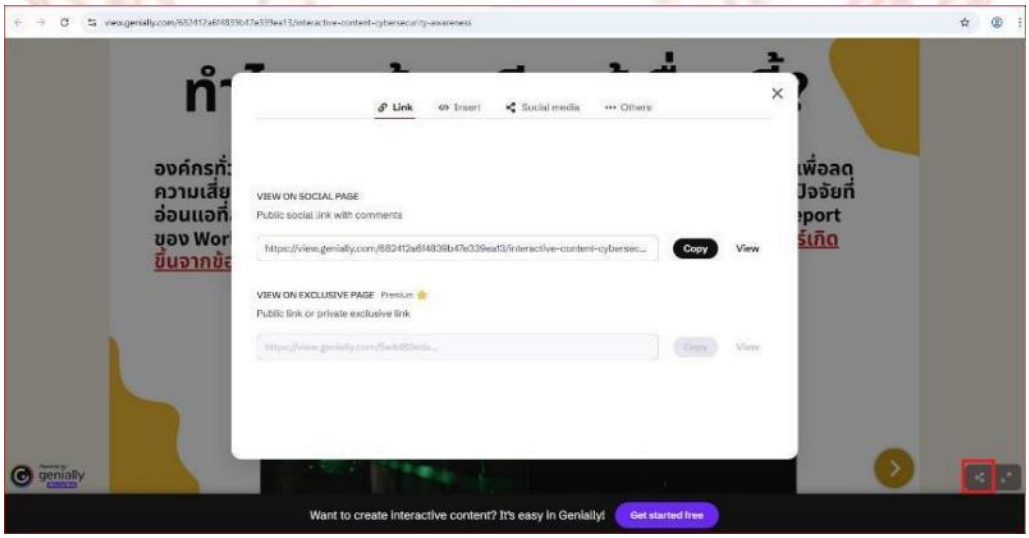
ภาพที่ 3-5 แสดงการตอบคำถามที่ถูกต้องและอนุญาตให้ไปยังหน้าถัดไปได้



ภาพที่ 3-6 แสดงการตอบคำถามที่ผิดและให้ย้อนกลับ

3.6.6 การตรวจสอบความถูกต้องและความเหมาะสมของสื่อ (Content Review) ผู้วิจัยทำการตรวจสอบความถูกต้องของเนื้อหา รูปแบบการนำเสนอ และการทำงานขององค์ประกอบเชิงโต้ตอบ เพื่อให้สื่อมีความสมบูรณ์และใช้งานได้อย่างราบรื่น สามารถกดปุ่ม Present ที่มุมขวาบนของหน้าจอ เพื่อทำการตรวจสอบความถูกต้อง ความสมบูรณ์ และการแสดงผลของสื่อก่อนนำไปใช้จริงได้

3.6.7 การเผยแพร่และนำไปใช้ (Implementation and Publishing) เมื่อสื่อการเรียนรู้มีความสมบูรณ์ หากต้องการเผยแพร่สื่อการเรียนรู้ ผู้ใช้งานสามารถเลือกการกระจายสื่อได้โดยกดที่ไอคอนสามจุด บริเวณข้างปุ่ม Present ซึ่งระบบจะแสดงตัวเลือกสำหรับการเผยแพร่หลายรูปแบบ เช่น การสร้างลิงก์สำหรับเข้าถึง การส่งผ่านอีเมล หรือผ่านเครือข่ายสังคมออนไลน์ รวมถึงการเชื่อมต่อกับแพลตฟอร์มการเรียนรู้ เช่น Google Classroom เพื่อให้ผู้เรียนสามารถเข้าถึงสื่อได้สะดวก เพื่อให้กลุ่มตัวอย่างเข้าศึกษา และใช้เป็นเครื่องมือในการจัดกิจกรรมการเรียนรู้ก่อนการทดสอบหลังเรียน (Posttest) ดังแสดงในภาพที่ 3-7



ภาพที่ 3-7 แสดงถึงวิธีการส่งสื่อการเรียนรู้ออนไลน์ไปให้ผู้เรียน

บทที่ 4
ผลการวิจัย

ผู้วิจัยได้นำแบบทดสอบก่อนเรียนไปใช้เพื่อประเมินระดับความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ของบุคลากรในคลินิก จากนั้นดำเนินการจัดกิจกรรมเสริมสร้างความตระหนักรู้โดยใช้สื่อการเรียนรู้ออนไลน์กับกลุ่มบุคลากร เพื่อนำข้อมูลที่ได้มาวิเคราะห์และเปรียบเทียบผลลัพธ์ด้านความตระหนักรู้ของบุคลากรในคลินิก โดยผลการวิจัยปรากฏตามขั้นตอนการดำเนินงานดังต่อไปนี้

4.1 ผลการดำเนินการจัดทำหนังสือขอความอนุเคราะห์และหนังสือแต่งตั้งผู้เชี่ยวชาญ

4.2 ผลการดำเนินการสร้างเนื้อหาแบบทดสอบก่อนเรียน

4.3 ผลการดำเนินการตรวจสอบเนื้อหาแบบทดสอบก่อนเรียนโดยผู้เชี่ยวชาญ

4.4 ผลลัพธ์จากการดำเนินการทดสอบก่อนเรียนด้วยชุดแบบทดสอบก่อนเรียน

4.5 ผลลัพธ์จากการสร้างสื่อการเรียนรู้ออนไลน์

4.6 ผลลัพธ์จากการเปรียบเทียบคะแนนการทดสอบก่อนเรียนและหลังเรียน

4.1 ผลการดำเนินการจัดทำหนังสือขอความอนุเคราะห์และหนังสือแต่งตั้งผู้เชี่ยวชาญ

ผู้วิจัยได้ดำเนินการจัดทำหนังสือขอความอนุเคราะห์ถึงคลินิก เพื่อขออนุญาตดำเนินการวิจัยและเก็บรวบรวมข้อมูลจากบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ โดยระบุขั้นตอนในการเก็บข้อมูลอย่างชัดเจน ทั้งนี้ เพื่อให้การดำเนินงานเป็นไปอย่างถูกต้องตามหลักจริยธรรมการวิจัยและได้รับอนุญาตจากผู้บริหารคลินิกอย่างเป็นทางการ ดังแสดงใน ภาคผนวก ข

นอกจากนี้ ผู้วิจัยยังได้จัดทำหนังสือแต่งตั้งผู้เชี่ยวชาญจำนวน 3 ท่าน เพื่อให้มีส่วนร่วมในการประเมินความเหมาะสมของเครื่องมือวิจัย ทั้งในด้านเนื้อหา (Content Validity) และความสอดคล้องกับวัตถุประสงค์การวิจัย ผลการแต่งตั้งและรายชื่อผู้เชี่ยวชาญได้แนบไว้ใน ภาคผนวก ค เพื่อแสดงกระบวนการดำเนินงานและหลักฐานการตรวจสอบความเที่ยงตรงของเครื่องมืออย่างครบถ้วน

4.2 ผลการดำเนินการสร้างเนื้อหาแบบทดสอบก่อนเรียน

ผู้วิจัยได้ดำเนินการพัฒนาแบบทดสอบก่อนเรียน เรื่องความรู้เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ครอบคลุมประเด็นสำคัญจำนวน 4 ด้าน ได้แก่ 1) ความหมายและความสำคัญของความมั่นคงปลอดภัยทางไซเบอร์ 2) ประเภทของมัลแวร์ 3) ประเภทของการโจมตีทางไซเบอร์ และ 4) ความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในชีวิตประจำวัน แบบทดสอบดังกล่าวมีจำนวนทั้งหมด 25 ข้อ อยู่ในรูปแบบปรนัยหลายตัวเลือก (Multiple Choice) โดยมีวัตถุประสงค์เพื่อใช้ประเมินความรู้ก่อนการเรียนรู้ด้วยสื่อการเรียนรู้ออนไลน์ ตลอดจนใช้เป็นข้อมูลคะแนนพื้นฐาน (Baseline) สำหรับการวิเคราะห์เปรียบเทียบผลการเรียนรู้ในขั้นตอนต่อไป

4.3 ผลการดำเนินการตรวจสอบเนื้อหาแบบทดสอบก่อนเรียนโดยผู้เชี่ยวชาญ

ผู้วิจัยได้ดำเนินการส่งแบบทดสอบก่อนเรียนให้ผู้เชี่ยวชาญจำนวน 3 ท่าน ทำการตรวจสอบความถูกต้องของเนื้อหาและให้ข้อเสนอแนะในการปรับปรุงแก้ไข ทั้งนี้ การตรวจสอบคุณภาพของเครื่องมือวิจัยได้ใช้วิธีการหาค่าดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ของการวิจัย

(Index of Item-Objective Congruence: IOC) ผู้เชี่ยวชาญได้ประเมินข้อคำถามจำนวน 25 ข้อ ผลการตรวจสอบพบว่าค่าดัชนีความสอดคล้อง ของข้อคำถามทุกข้อมีค่าตั้งแต่ 0.67 ถึง 1.00 ซึ่งสูงกว่าเกณฑ์ที่กำหนดไว้ (≥ 0.50)แสดงให้เห็นว่าแบบทดสอบมีความเที่ยงตรงเชิงเนื้อหาในระดับที่เหมาะสม สามารถนำไปใช้ในการเก็บรวบรวมข้อมูลได้อย่างถูกต้องและเชื่อถือได้ ดังแสดงใน ตารางที่ 4-1

ตารางที่ 4-1 ค่าความสอดคล้อง (IOC)ของแบบทดสอบ

ข้อ	ผู้เชี่ยวชาญคนที่ 1	ผู้เชี่ยวชาญคนที่ 2	ผู้เชี่ยวชาญคนที่ 3	ผลรวมของคะแนนΣR	ค่าเฉลี่ย IOC	แปลผล
1	+1	+1	+1	3	1.00	ใช้ได้
2	+1	+1	+1	3	1.00	ใช้ได้
3	+1	+1	+1	3	1.00	ใช้ได้
4	+1	+1	+1	3	1.00	ใช้ได้
5	+1	0	+1	2	0.67	ใช้ได้
6	+1	+1	+1	3	1.00	ใช้ได้
7	+1	+1	+1	3	1.00	ใช้ได้
8	+1	+1	+1	3	1.00	ใช้ได้
9	+1	+1	0	2	0.67	ใช้ได้
10	0	+1	+1	2	0.67	ใช้ได้
11	+1	+1	+1	3	1.00	ใช้ได้
12	+1	+1	+1	3	1.00	ใช้ได้
13	+1	+1	+1	3	1.00	ใช้ได้
14	+1	0	+1	2	0.67	ใช้ได้
15	+1	+1	+1	3	1.00	ใช้ได้
16	0	+1	+1	2	0.67	ใช้ได้
17	+1	+1	+1	3	1.00	ใช้ได้
18	+1	+1	+1	3	1.00	ใช้ได้
19	+1	+1	+1	3	1.00	ใช้ได้
20	+1	+1	0	2	0.67	ใช้ได้
21	+1	+1	+1	3	1.00	ใช้ได้
22	+1	+1	+1	3	1.00	ใช้ได้
23	+1	+1	+1	3	1.00	ใช้ได้
24	+1	+1	+1	3	1.00	ใช้ได้
25	+1	+1	+1	3	1.00	ใช้ได้

4.4 ผลลัพธ์จากการดำเนินการทดสอบก่อนเรียนด้วยชุดแบบทดสอบก่อนเรียน

การวิเคราะห์ข้อมูลในบทนี้ มีวัตถุประสงค์เพื่อนำเสนอผลการวิเคราะห์ลักษณะทางประชากรของผู้ตอบแบบสอบถาม และผลการประเมินความตระหนักรู้ของผู้เข้าร่วมโครงการ โดยแบ่งการนำเสนอออกเป็น 2 ส่วน ดังนี้

4.4.1 ผลการวิเคราะห์ข้อมูลพื้นฐานด้านลักษณะทางประชากร

จากข้อมูลในตาราง 4-2 พบว่ากลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิง จำนวน 60 คน คิดเป็นร้อยละ 75.00 ขณะที่เพศชายมีจำนวน 20 คน คิดเป็นร้อยละ 25.00 กลุ่มตัวอย่างส่วนใหญ่มีอายุระหว่าง 21–30 ปี จำนวน 40 คน (ร้อยละ 50.00) รองลงมาคือช่วง 31–40 ปี จำนวน 25 คน (ร้อยละ 31.25) สำหรับระดับการศึกษา พบว่าส่วนใหญ่มีระดับปริญญาตรี จำนวน 39 คน (ร้อยละ 48.75) รองลงมาคือระดับต่ำกว่าปริญญาตรี จำนวน 35 คน (ร้อยละ 43.75) และสูงกว่าปริญญาตรี จำนวน 6 คน (ร้อยละ 7.50) ส่วนระดับตำแหน่งงาน กลุ่มตัวอย่างส่วนใหญ่เป็นพนักงานปฏิบัติงาน จำนวน 57 คน (ร้อยละ 71.25) รองลงมาคือหัวหน้าแผนก/หัวหน้าหน่วย จำนวน 12 คน (ร้อยละ 15.00) และระดับผู้จัดการ/รองผู้อำนวยการมีจำนวนไม่มาก สำหรับระยะเวลาการทำงานที่เกี่ยวข้องกับระบบคอมพิวเตอร์ พบว่าส่วนใหญ่มีประสบการณ์ 1–5 ปี จำนวน 34 คน (ร้อยละ 42.50) รองลงมาคือประสบการณ์น้อยกว่า 1 ปี จำนวน 19 คน (ร้อยละ 23.75) และ 6–10 ปี จำนวน 16 คน (ร้อยละ 20.00) ข้อมูลลักษณะทางประชากรดังกล่าวช่วยให้ผู้วิจัยสามารถวิเคราะห์ความสัมพันธ์ระหว่างเพศ อายุ ระดับการศึกษา ตำแหน่งงาน และประสบการณ์การทำงานกับผลการทดสอบก่อนเรียน-หลังเรียนได้อย่างเป็นระบบ

ตารางที่ 4-2 ลักษณะทางประชากรของกลุ่มตัวอย่าง

ลักษณะประชากร	รายการ	จำนวนคน (N)	ร้อยละ (%)
เพศ	หญิง	60	75
	ชาย	20	25
	รวม	80	100
อายุ	ต่ำกว่า 21 ปี	3	3.75
	21–30 ปี	40	50
	31–40 ปี	25	31.25
	41–50 ปี	9	11.25
	51 ปีขึ้นไป	3	3.75
	รวม	80	100
ระดับการศึกษา	ต่ำกว่าปริญญาตรี	35	43.75

ตารางที่ 4-2 (ต่อ)

ลักษณะประชากร	รายการ	จำนวนคน (N)	ร้อยละ (%)
	ปริญญาตรี	39	48.75
	สูงกว่าปริญญาตรี	6	7.5
	รวม	80	100
ระดับตำแหน่ง	รองผู้อำนวยการ/ผู้ช่วยผู้อำนวยการ	3	3.75
	ผู้จัดการฝ่าย/ผู้ช่วยผู้จัดการฝ่าย	8	10
	หัวหน้าแผนก/หัวหน้าหน่วย	12	15
	พนักงานปฏิบัติงาน	57	71.25
	รวม	80	100
ระยะเวลาการทำงาน (ปี)	น้อยกว่า 1	19	23.75
	1–5	34	42.5
	6–10	16	20
	11–15	4	5
	มากกว่า 15	7	8.75
	รวม	80	100

4.4.2 ผลการวิเคราะห์ระดับความตระหนักรู้ของผู้ตอบแบบสอบถาม

ผู้วิจัยได้นำแบบทดสอบก่อนเรียนไปทดลองกับกลุ่มบุคลากรของคลินิก เพื่อเก็บข้อมูลเบื้องต้นเกี่ยวกับระดับความรู้และความเข้าใจของผู้เข้าร่วม โดยใช้กลุ่มประชากรตามขอบเขตของงานวิจัย จำนวนทั้งสิ้น 80 คน แบบทดสอบก่อนเรียนจัดทำในรูปแบบออนไลน์ผ่าน Google Form เพื่ออำนวยความสะดวกในการเข้าถึงและลดข้อจำกัดด้านเวลาและสถานที่ ผลลัพธ์จากการทดสอบก่อนเรียนถูกนำมาประมวลผลทางสถิติ โดยคำนวณค่าเฉลี่ย (Mean) ค่ามัธยฐาน (Median) ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) ค่าสัมประสิทธิ์ความแปรผัน (Coefficient of Variation: C.V.) และรวมถึงการจัดกลุ่มคะแนนตามระดับความรู้ของผู้เข้าร่วมตามเกณฑ์ที่กำหนด ดังนี้

- 0–12 คะแนน (ต่ำกว่า 50%) จัดอยู่ในระดับความรู้น้อย
- 13–17 คะแนน (50–69%) จัดอยู่ในระดับความรู้ปานกลาง
- 18–25 คะแนน (70% ขึ้นไป) จัดอยู่ในระดับความรู้มาก

ตารางที่ 4-3 ประมวลผลทางสถิติ

ค่าสถิติ (Statistic)	ผลลัพธ์ (Value)	หมายเหตุ
จำนวนบุคลากรที่นำมาประมวลผล (N)	80	
ค่าเฉลี่ย (Mean)	9.25	จากคะแนนเต็ม 25
ค่ามัธยฐาน (Median)	9	
ส่วนเบี่ยงเบนมาตรฐาน (S.D.)	3.309	ค่า S.D. ดิบ
S.D. แบบ normalized (0–1)	0.132	คำนวณจาก S.D. ÷ 25 (จำนวนข้อคำถาม)
ค่าสัมประสิทธิ์ความแปรผัน (Coefficient of Variation: C.V.)	0.358	คำนวณจาก S.D. ÷ $\bar{x}$

จากตารางที่ 4-3 แสดงผลการวิเคราะห์สถิติเชิงพรรณนาเกี่ยวกับคะแนนแบบทดสอบก่อนเรียนของบุคลากรจำนวน 80 คน พบว่าค่าเฉลี่ยของคะแนนเท่ากับ 9.25 คะแนน จากคะแนนเต็ม 25 คะแนน แสดงว่าผู้ตอบแบบทดสอบมีคะแนนเฉลี่ยอยู่ในระดับค่อนข้างต่ำเมื่อเทียบกับคะแนนเต็ม

ค่ามัธยฐานเท่ากับ 9 คะแนน ซึ่งใกล้เคียงกับค่าเฉลี่ย สะท้อนให้เห็นว่าการกระจายตัวของคะแนนอยู่ในลักษณะสมมาตรพอสมควร

ส่วนเบี่ยงเบนมาตรฐาน (S.D.) มีค่าเท่ากับ 3.309 ซึ่งเป็นค่า S.D. ดิบที่สะท้อนให้เห็นถึงความแตกต่างของคะแนนระหว่างบุคคลในระดับปานกลาง กล่าวคือ คะแนนของผู้ตอบส่วนใหญ่ยังมีความแตกต่างกันบ้าง แต่ไม่ได้กระจายมากจนเกินไป

เมื่อคำนวณค่า S.D. แบบ normalized (S.D. ÷ คะแนนเต็ม) ได้ค่าเท่ากับ 0.132 หรือร้อยละ 13.2% ของคะแนนเต็ม 25 คะแนน หมายความว่าคะแนนของกลุ่มตัวอย่างมีการกระจายตัวอยู่ประมาณร้อยละ 13 ของช่วงคะแนนทั้งหมด ซึ่งอยู่ในระดับต่ำ–ปานกลาง และสามารถแปลได้ว่าคะแนนโดยรวมค่อนข้างรวมกลุ่มกันในช่วงคะแนนต่ำถึงปานกลาง

นอกจากนี้ เมื่อนำค่า S.D. มาเปรียบเทียบกับค่าเฉลี่ยเพื่อคำนวณหาค่าสัมประสิทธิ์ความแปรผัน (Coefficient of Variation: C.V.) ซึ่งเป็นตัวชี้วัดระดับความกระจายตัวของข้อมูลในหน่วยมาตรฐานเดียวกัน (คำนวณโดยสูตร C.V. = S.D. ÷ $\bar{x}$) พบว่ามีค่าเท่ากับ 0.358 หรือคิดเป็น 35.8% ซึ่งจัดอยู่ในเกณฑ์ “ค่อนข้างสูง” หมายความว่าความแปรปรวนของคะแนนมีค่อนข้างมาก แสดงให้เห็นว่าระดับความรู้ของบุคลากรในช่วงก่อนการอบรมยังมีความแตกต่างกันอยู่พอสมควร บางส่วนมีพื้นฐานความรู้ด้านความปลอดภัยทางไซเบอร์มากกว่าเพื่อนร่วมงาน ขณะที่บางส่วนยังขาดความเข้าใจในประเด็นสำคัญ ซึ่งเป็นสิ่งที่สะท้อนถึงความจำเป็นในการพัฒนาศักยภาพผ่านสื่อการเรียนรู้ออนไลน์ที่ออกแบบไว้ในงานวิจัยนี้

ผลการกระจายตัวของคะแนนดังกล่าวสะท้อนให้เห็นถึงลักษณะความแตกต่างของพื้นฐานความรู้ของบุคลากรในคลินิกอย่างชัดเจน กลุ่มตัวอย่างไม่ได้มีความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์ในระดับเดียวกัน บางรายมีความรู้พื้นฐานอยู่แล้วในระดับหนึ่ง แต่อีกหลายรายมีความรู้ในระดับต่ำ ส่งผลให้จำเป็นต้องมีการออกแบบสื่อการเรียนรู้ที่สามารถตอบสนองผู้เรียนที่มีพื้นฐานต่างกันได้

ตารางที่ 4-4 กลุ่มคะแนนตามระดับความรู้ก่อนเรียน

เกณฑ์คะแนน	เกณฑ์ร้อยละ (คะแนนเต็ม 25)	ระดับความรู้	จำนวนคน	ร้อยละ (%)
0–12 คะแนน	ต่ำกว่า 50%	น้อย	54	67.50%
13–17 คะแนน	50–69%	ปานกลาง	24	30.00%
18–25 คะแนน	70% ขึ้นไป	มาก	2	2.50%
รวม			80	100.00%

จากตารางที่ 4-4 แสดงผลการจำแนกกลุ่มคะแนนของบุคลากรตามระดับความรู้ก่อนเรียน พบว่า บุคลากรส่วนใหญ่มีระดับความรู้ อยู่ในระดับ “น้อย” จำนวน 54 คน คิดเป็นร้อยละ 67.50 รองลงมาคือระดับ “ปานกลาง” จำนวน 24 คน คิดเป็นร้อยละ 30.00 และมีเพียง 2 คน (ร้อยละ 2.50) ที่มีระดับความรู้ “มาก” ก่อนการเรียนรู้ ผลดังกล่าวแสดงให้เห็นว่า โดยภาพรวมบุคลากรส่วนใหญ่ยังมีความรู้ด้านความปลอดภัยทางไซเบอร์ในระดับต่ำ ซึ่งสะท้อนให้เห็นถึงความจำเป็นในการจัดกิจกรรมการเรียนรู้หรือการอบรมเพิ่มเติม เพื่อยกระดับความเข้าใจและความตระหนักรู้ของบุคลากรเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ตารางที่ 4-5 กลุ่มคะแนนตามระดับความรู้ก่อนเรียน จำแนกตามระดับความตระหนักรู้แต่ละด้าน

ด้าน	น้อย (%)	ปานกลาง (%)	มาก (%)
ด้านที่ 1: ความหมายและความสำคัญของความมั่นคงปลอดภัยไซเบอร์ (5 ข้อ)	65.00%	32.50%	2.50%
ด้านที่ 2: ประเภทของมัลแวร์ (5 ข้อ)	70.00%	27.50%	2.50%
ด้านที่ 3: ประเภทของการโจมตีทางไซเบอร์ (6 ข้อ)	80.00%	18.75%	1.25%
ด้านที่ 4: ความมั่นคงปลอดภัยในชีวิตประจำวัน (9 ข้อ)	55.00%	40.00%	5.00%
ค่าเฉลี่ย 4 ด้าน	67.50%	29.69%	2.81%

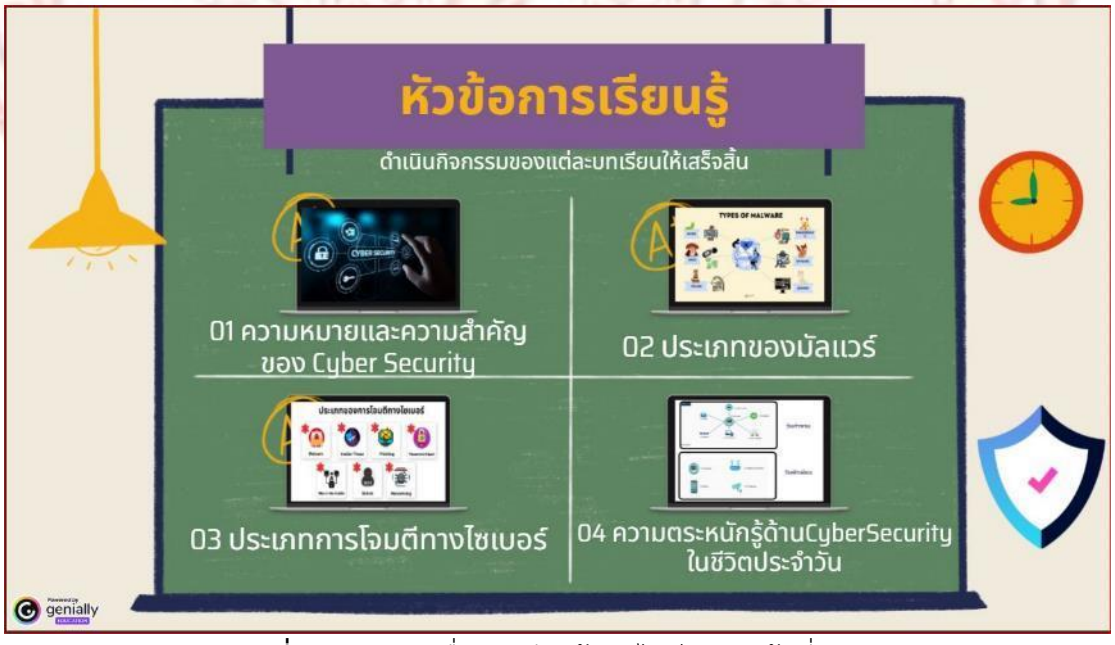
จากตารางที่ 4-5 แสดงผลการจำแนกกลุ่มคะแนนก่อนเรียนของบุคลากร จำแนกตามระดับความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ในแต่ละด้าน พบว่า โดยภาพรวมบุคลากรส่วนใหญ่มีระดับความรู้ อยู่ในระดับ “น้อย” เฉลี่ยร้อยละ 67.50 ขณะที่ระดับ “ปานกลาง” มีร้อยละ 29.69 และระดับ “มาก” มีเพียงร้อยละ 2.81 แสดงให้เห็นว่าก่อนการอบรม บุคลากรส่วนใหญ่ยังมีความรู้พื้นฐานด้านความปลอดภัยทางไซเบอร์อยู่ในระดับต่ำ

เมื่อพิจารณาเป็นรายด้าน พบว่า ด้านที่ 3 เรื่องประเภทของการโจมตีทางไซเบอร์ มีสัดส่วนของผู้ที่มีความรู้ระดับ “น้อย” สูงที่สุด คือร้อยละ 80.00 รองลงมาคือ ด้านที่ 2 ประเภทของมัลแวร์ ร้อยละ 70.00 และ ด้านที่ 1 ความหมายและความสำคัญของความมั่นคงปลอดภัยไซเบอร์ ร้อยละ 65.00 ในขณะที่ ด้านที่ 4 ความมั่นคงปลอดภัยในชีวิตประจำวัน มีสัดส่วนของผู้ที่มีความรู้ระดับ “น้อย” ต่ำที่สุด คือร้อยละ 55.00 และเป็นด้านเดียวที่มีผู้ตอบในระดับ “มาก” สูงกว่าด้านอื่น (ร้อยละ 5.00)

ผลการวิเคราะห์นี้สะท้อนอย่างชัดเจนว่า ก่อนการเข้าร่วมกิจกรรมการเรียนรู้ บุคลากรยังขาดความเข้าใจเชิงลึกเกี่ยวกับภัยคุกคามทางไซเบอร์ โดยเฉพาะในประเด็นทางเทคนิค (เช่น ประเภทการโจมตีและมัลแวร์) ส่วนความรู้ด้านการใช้งานในชีวิตประจำวันที่ค่อนข้างสูงกว่าด้านอื่น อาจเป็นผลมาจากความคุ้นเคยในการใช้งานเทคโนโลยีในชีวิตประจำวัน ผลลัพธ์นี้จึงช่วยตอกย้ำถึงความจำเป็นและความสำคัญของการจัดกิจกรรมการเรียนรู้ในครั้งนี้ เพื่อยกระดับความรู้และสร้างความตระหนักรู้ให้แก่บุคลากรอย่างเป็นระบบ

4.5 ผลลัพธ์จากการสร้างสื่อการเรียนรู้ออนไลน์

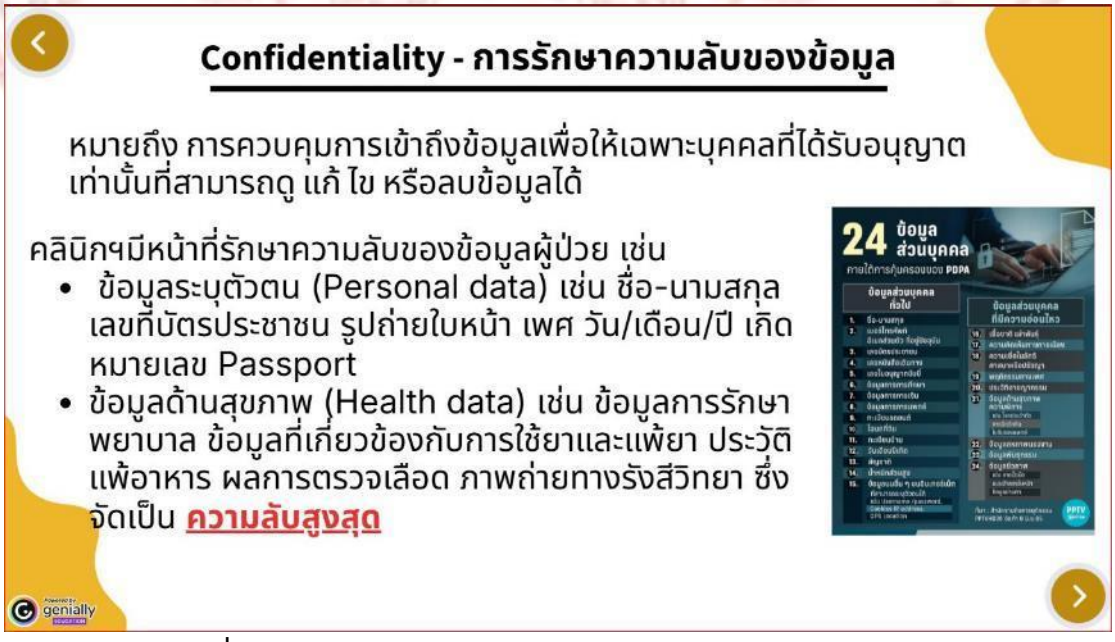
จากการพัฒนาสื่อการเรียนรู้ออนไลน์เรื่อง Cybersecurity Awareness โดยใช้แพลตฟอร์ม Genially พบว่าสื่อที่สร้างขึ้นมีโครงสร้างประกอบด้วย 4 บทเรียนหลัก ได้แก่ (1) ความหมายและความสำคัญของความมั่นคงปลอดภัยไซเบอร์ (2) ประเภทของมัลแวร์ (3) ประเภทของการโจมตีทางไซเบอร์ และ (4) ความตระหนักรู้ในชีวิตประจำวัน โดยแต่ละบทเรียนถูกออกแบบให้มีการนำเสนอในรูปแบบสื่ออินเทอร์แอคทีฟที่ผสมผสานข้อความ ภาพประกอบ กราฟิก และกิจกรรมแบบทดสอบท้ายบท เพื่อสร้างปฏิสัมพันธ์ระหว่างผู้เรียนกับเนื้อหา โดยมีตัวอย่างสื่อการเรียนรู้ดังภาพที่ 4-1



ภาพที่ 4-1 ตัวอย่างสื่อการเรียนรู้ออนไลน์ตามหัวข้อที่กำหนด

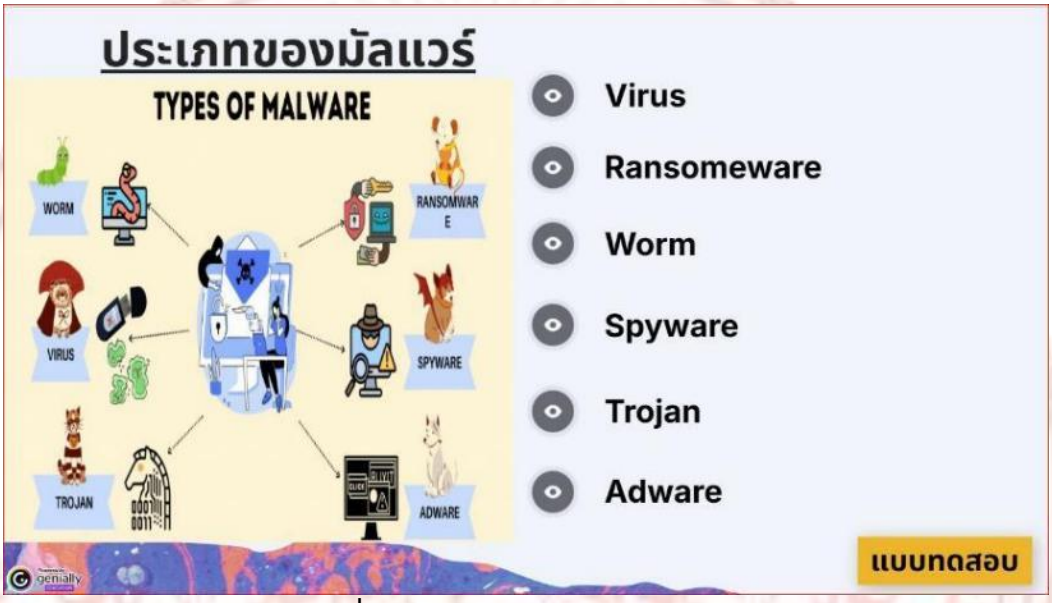
แสดงผลการสร้างสื่อการเรียนรู้ออนไลน์ ด้านที่ 1 “ความหมายและความสำคัญของความมั่นคงปลอดภัยไซเบอร์” โดยอธิบายตามหลัก CIA Triad ได้แก่ การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วนของข้อมูล (Integrity) และความพร้อมใช้งาน (Availability) ในบริบทของคลินิก เช่น การไม่เปิดเผยข้อมูลผู้ป่วยให้บุคคลภายนอก การตรวจสอบความถูกต้องของข้อมูลก่อนบันทึกในระบบ และการดูแลให้ระบบเวชระเบียนออนไลน์พร้อมใช้งานอยู่เสมอ เพื่อให้ผู้เรียนเข้าใจและเห็นภาพการประยุกต์ใช้จริงในงานประจำวัน ดังภาพที่ 4-2 และ ภาพที่ 4-3

ภาพที่ 4-2 ตัวอย่างความหมายและความสำคัญของ Cyber Security(1)



ภาพที่ 4-3 ตัวอย่างความหมายและความสำคัญของ Cyber Security(2)

แสดงผลการสร้างสื่อการเรียนรู้ออนไลน์ ด้านที่ 2 “ประเภทของมัลแวร์” เพื่อให้ผู้เรียนเข้าใจภัยคุกคามจากซอฟต์แวร์อันตราย เช่น ไวรัส โทรจัน และแรนซัมแวร์ โดยมีการอธิบายรายละเอียดของมัลแวร์แต่ละประเภท ได้แก่ มัลแวร์คืออะไร ทำงานอย่างไร ผลกระทบที่อาจเกิดขึ้น วิธีป้องกัน และ สิ่งแรกที่ควรปฏิบัติเมื่อพบเจอ เพื่อให้ผู้เรียนเห็นภาพการทำงานจริงในคลินิก เช่น การหลีกเลี่ยงการเปิดไฟล์แนบที่ไม่รู้แหล่งที่มา การอัปเดตโปรแกรมป้องกันไวรัส และการแจ้งฝ่ายไอทีทันทีเมื่อพบความผิดปกติในระบบ ดังภาพที่ 4-4 และ ภาพที่ 4-5



ภาพที่ 4-4 ตัวอย่างประเภทของมัลแวร์(1)

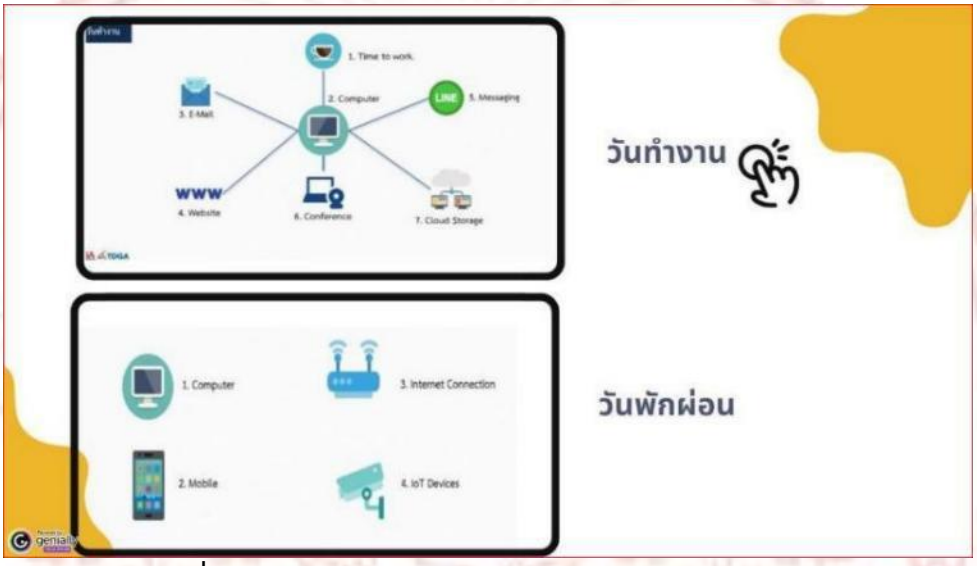
ภาพที่ 4-5 ตัวอย่างประเภทของมัลแวร์(2)

แสดงผลการสร้างสื่อการเรียนรู้ออนไลน์ ด้านที่ 3 “ประเภทของการโจมตีทางไซเบอร์” เพื่อให้ผู้เรียนเข้าใจรูปแบบการโจมตีที่พบได้บ่อยในองค์กร เช่น Insider Threat, Phishing, Password Attack และ Man-in-the-Middle โดยเน้นให้ผู้เรียนเห็นภาพการทำงานจริง เช่น การ แสดงรายละเอียดของการโจมตีแบบ Password Attack โดยอธิบายวิธีการโจมตีแบบ Brute Force เพื่อเจาะระบบพร้อมเสนอแนวทางการป้องกัน เช่น การตั้งรหัสผ่านที่ซับซ้อน ประกอบด้วยตัวอักษร ตัวเลข และสัญลักษณ์ รวมถึงการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ เพื่อให้ผู้เรียนเข้าใจแนวทางการปฏิบัติที่นำไปใช้ได้จริงในการ เพื่อสร้างความตระหนักรู้ว่าการโจมตีทางไซเบอร์สามารถเกิดขึ้นได้จากทั้งภายนอกและภายในองค์กร ดังภาพที่ 4-6 และ ภาพที่ 4-7

ภาพที่ 4-6 ตัวอย่างบทเรียนประเภทภัยคุกคามไซเบอร์(1)

ภาพที่ 4-7 ตัวอย่างบทเรียนประเภทภัยคุกคามไซเบอร์(2)

แสดงผลการสร้างสื่อการเรียนรู้ออนไลน์ ด้านที่ 4 “ความตระหนักรู้ในชีวิตประจำวัน” โดยยกตัวอย่างพฤติกรรมการใช้งานเทคโนโลยีทั้งในวันทำงานและวันพักผ่อน เพื่อให้ผู้เรียนเห็นภาพการปฏิบัติจริงในชีวิตประจำวัน เช่น การใช้งานโทรศัพท์มือถือ และการเชื่อมต่ออุปกรณ์ IoT อย่างปลอดภัย แสดงเนื้อหาความรู้เกี่ยวกับการใช้งานเว็บไซต์อย่างปลอดภัย โดยอธิบายแนวทางการปฏิบัติที่ถูกต้อง เช่น ไม่เข้าสู่เว็บไซต์ที่ไม่น่าเชื่อถือ ตรวจสอบสัญลักษณ์ SSL/HTTPS ก่อนทำธุรกรรม เพื่อให้ผู้เรียนตระหนักถึงการป้องกันความเสี่ยงจากการใช้งานอินเทอร์เน็ตในชีวิตจริง ทั้งในช่วงเวลาทำงานและเวลาส่วนตัว ดังภาพที่ 4-8 และ ภาพที่ 4-9



ภาพที่ 4-8 ตัวอย่างบทเรียนความตระหนักรู้ในชีวิตประจำวัน(1)

ภาพที่ 4-9 ตัวอย่างบทเรียนความตระหนักรู้ในชีวิตประจำวัน(2)

4.6 ผลลัพธ์จากการเปรียบเทียบคะแนนการทดสอบก่อนเรียนและหลังเรียน

จากการดำเนินการเสร็จสิ้นเป็นที่เรียบร้อย ผู้วิจัยได้ดำเนินการเก็บรวบรวมข้อมูลคะแนนการทดสอบความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ทั้ง ก่อนเรียน และ หลังเรียน จากกลุ่มประชากรตามขอบเขตการวิจัย คือ บุคลากรที่ปฏิบัติงานบนระบบคลาวด์ของคลินิก จำนวน 80 คน แสดงผลการวิเคราะห์ค่าสถิติเชิงพรรณนาของคะแนนทดสอบความรู้ก่อนเรียน (Pre-test) และหลังเรียน (Post-test) ของกลุ่มตัวอย่างจำนวน 80 คน ซึ่งประกอบด้วย จำนวน (N) ค่าเฉลี่ย (Mean) ค่ามัธยฐาน (Median) และส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation)

ตารางที่ 4-6 ค่าสถิติเชิงพรรณนาของคะแนนทดสอบก่อนเรียน หลังเรียน และผลต่างของคะแนน

ค่าสถิติ (Statistic)	คะแนนก่อนเรียน	คะแนนหลังเรียน	ผลต่าง
จำนวนบุคลากร (N)	80	80	80
ค่าเฉลี่ย (Mean)	9.25	19.75	10.5
ค่ามัธยฐาน (Median)	9	20	11
ส่วนเบี่ยงเบนมาตรฐาน (S.D.)	3.31	2.8	4.46
S.D. แบบ normalized (0–1)	0.132	0.112	
ค่าสัมประสิทธิ์ความแปรผัน (Coefficient of Variation: C.V.)	0.358	0.142	

จากตารางที่ 4-6 ผลการวิเคราะห์ข้อมูลของกลุ่มตัวอย่างจำนวน 80 คน พบว่า ก่อนการเข้าร่วมกิจกรรม กลุ่มตัวอย่างมีคะแนนทดสอบโดยเฉลี่ยอยู่ที่ 9.25 คะแนน (S.D. = 3.31) โดยมีค่ามัธยฐานของคะแนนอยู่ที่ 9.00 คะแนน แสดงให้เห็นว่าระดับคะแนนของผู้ตอบส่วนใหญ่กระจุกตัวอยู่บริเวณช่วงคะแนนต่ำ และค่าส่วนเบี่ยงเบนมาตรฐานที่ค่อนข้างสูงสะท้อนให้เห็นว่าระดับความรู้พื้นฐานเดิมของกลุ่มตัวอย่างมีความแตกต่างกันพอสมควร

ภายหลังการเข้าร่วมกิจกรรม พบว่าคะแนนทดสอบของกลุ่มตัวอย่างเพิ่มสูงขึ้นอย่างชัดเจน โดยมีค่าเฉลี่ยเท่ากับ 19.75 คะแนน (S.D. = 2.80) และมีค่ามัธยฐานอยู่ที่ 20.00 คะแนน ซึ่งสูงกว่าก่อนเรียนอย่างมาก การที่ค่าส่วนเบี่ยงเบนมาตรฐานลดลงจาก 3.31 เหลือ 2.80 แสดงให้เห็นว่าคะแนนของกลุ่มตัวอย่างหลังการเรียนรู้มีความกระจายตัวลดลง สะท้อนถึงความสม่ำเสมอของผลสัมฤทธิ์ทางการเรียนที่ดีขึ้นอย่างเห็นได้ชัด

เมื่อนำค่า S.D. มาคำนวณในรูปแบบ normalized (S.D. ÷ คะแนนเต็ม 25) พบว่า S.D. แบบ normalized ลดลงจาก 0.132 ก่อนเรียน เหลือเพียง 0.112 หลังเรียน หมายความว่าการกระจายของคะแนนเมื่อเทียบกับคะแนนเต็มมีแนวโน้มลดลง และคะแนนส่วนใหญ่รวมกลุ่มอยู่ในช่วงคะแนนสูงมากขึ้น ซึ่งสะท้อนถึงประสิทธิภาพของสื่อการเรียนรู้ที่ช่วยลดช่องว่างระหว่างผู้เรียนแต่ละคนได้ดี

นอกจากนี้ ค่าสัมประสิทธิ์ความแปรผัน (Coefficient of Variation: C.V.) ซึ่งใช้วัดระดับความสม่ำเสมอของคะแนน พบว่า ก่อนเรียนมีค่าเท่ากับ 0.358 (35.8%) และหลังเรียนลดลงเหลือ 0.142 (14.2%) แสดงให้เห็นว่าคะแนนหลังเรียนมีความสม่ำเสมอมากขึ้นอย่างชัดเจน หมายความว่าผู้เข้าร่วมมีความเข้าใจในเนื้อหาความปลอดภัยทางไซเบอร์ในระดับที่ใกล้เคียงกันมากขึ้น ซึ่งบ่งชี้ว่าสื่อ

การเรียนรู้ออนไลน์ที่ใช้ในการวิจัยมีประสิทธิภาพทั้งในด้านการเพิ่มพูนความรู้และลดความแตกต่างระหว่างผู้เรียนได้อย่างมีนัยสำคัญเชิงทิศทาง

ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation: S.D.) เท่ากับ 4.46 ที่ปรากฏในตารางผลการวิเคราะห์นั้น ไม่ได้มาจากการลบค่าความเบี่ยงเบนมาตรฐานของคะแนนก่อนเรียนและหลังเรียนโดยตรง แต่เป็น ค่า S.D. ของผลต่างคะแนน (Standard Deviation of the Difference Scores) ซึ่งคำนวณจากผลต่างระหว่างคะแนนก่อนและหลังเรียนของผู้เข้าร่วมแต่ละคน (จำนวน 80 คน) ค่า S.D. ของผลต่างคะแนนที่ได้เท่ากับ 4.46 หมายความว่า ผลต่างคะแนนของผู้เข้าร่วมมีการกระจายตัวเฉลี่ยประมาณ ±4.46 คะแนน สะท้อนถึงความหลากหลายของระดับการพัฒนาในแต่ละบุคคลหลังจากเข้าร่วมการเรียนรู้ด้วยสื่อออนไลน์ ค่าดังกล่าวถูกนำมาใช้ในการคำนวณ สถิติ t-test แบบกลุ่มสัมพันธ์ (Paired Samples t-test) ซึ่งใช้สำหรับเปรียบเทียบคะแนนก่อนและหลังเรียนของกลุ่มตัวอย่าง “กลุ่มเดียวกัน” โดยพิจารณาจากผลต่างคะแนนของแต่ละคน ไม่ใช่การเปรียบเทียบระหว่างสองกลุ่มอิสระ ในขั้นตอนการคำนวณ ค่าเฉลี่ยของผลต่างคะแนน (Mean Difference) เท่ากับ 10.50 คะแนน เมื่อนำค่าเฉลี่ยผลต่างนี้ไปหารด้วยค่า S.D. ของผลต่าง (4.46) หารด้วยรากที่สองของขนาดตัวอย่าง (√80)

ผลการวิเคราะห์ข้อมูลด้วยสถิติ t-test แบบกลุ่มสัมพันธ์ (Paired Samples t-test) เพื่อเปรียบเทียบคะแนนก่อนและหลังเรียน มีรายละเอียดดังตารางต่อไปนี้

ตารางที่ 4-7 ผลการทดสอบค่าทีแบบกลุ่มสัมพันธ์ (Paired Samples t-test) เพื่อเปรียบเทียบคะแนนก่อนเรียนและหลังเรียน (N = 80)

ค่าเฉลี่ยก่อนเรียน	ส่วนเบี่ยงเบนมาตรฐานก่อนเรียน	ค่าเฉลี่ยหลังเรียน	ส่วนเบี่ยงเบนมาตรฐานหลังเรียน	ผลต่างเฉลี่ย	t	df	p	ขนาดอิทธิพล (Cohen’s d_z)
9.25	3.309	19.75	2.804	10.50	21.040	79	< .001**	2.35

**ระดับนัยสำคัญทางสถิติที่ .001*

จากตารางที่ 4-7 ผลการทดสอบทางสถิติแบบ Paired Samples t-test พบว่าค่าเฉลี่ยคะแนนหลังเรียน ($\bar{X}$ = 19.75, S.D. = 2.804) สูงกว่าค่าเฉลี่ยก่อนเรียน ($\bar{X}$ = 9.25, S.D. = 3.309) อย่างมีนัยสำคัญทางสถิติที่ระดับ .001 (t = 21.040, df = 79, p < .001**) แสดงว่าหลังการเข้าร่วมกิจกรรมการเรียนรู้ผ่านสื่อออนไลน์ด้วยเครื่องมือ Genially บุคลากรมีระดับความรู้ด้านความปลอดภัยทางไซเบอร์เพิ่มขึ้นอย่างมีนัยสำคัญ

นอกจากนี้ เมื่อพิจารณาขนาดอิทธิพล (Effect Size) ด้วยสถิติ Cohen’s d_z = 2.35 พบว่าอยู่ในระดับ “สูงมาก” (Very Large Effect) ตามเกณฑ์ของ Cohen (1988) ซึ่งกำหนดว่า d = 0.2 หมายถึงขนาดอิทธิพลเล็ก (Small), d = 0.5 ขนาดปานกลาง (Medium) และ d = 0.8 ขนาดใหญ่ (Large) ดังนั้นค่า d_z = 2.35 จึงสะท้อนให้เห็นว่าสื่อการเรียนรู้ที่พัฒนาขึ้นมีผลต่อการเพิ่มพูนความรู้ของผู้เรียนอย่างมีประสิทธิภาพและมีอิทธิพลสูงมาก

ผลการวิเคราะห์ดังกล่าวยังสอดคล้องกับค่าความแปรปรวน (C.V.) ที่ลดลงอย่างเด่นชัดจาก 0.358 เหลือ 0.142 หลังการอบรม ซึ่งแสดงถึงความสม่ำเสมอของคะแนนหลังเรียนมากกว่าก่อนเรียน กล่าวคือ ผู้เข้าอบรมส่วนใหญ่สามารถเข้าใจเนื้อหาได้ใกล้เคียงกันและมีความรู้ในทิศทางเดียวกันมากขึ้น

โดยสรุป ผลการทดสอบทางสถิติ Paired Samples t-test ยืนยันอย่างชัดเจนว่า การใช้สื่อการเรียนรู้ออนไลน์ด้วยแพลตฟอร์ม Genially มีประสิทธิผลสูงในการส่งเสริมความรู้ ความเข้าใจ และความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรในคลินิกเอกชนได้อย่างเป็นรูปธรรม

การวิจัยนี้ได้วิเคราะห์การเปลี่ยนแปลงระดับความรู้ของบุคลากรจำนวน 80 คน จากการใช้สื่อการเรียนรู้ออนไลน์ โดยจำแนกกลุ่มตัวอย่างตามเกณฑ์คะแนนทดสอบ (คะแนนเต็ม 25 คะแนน) ออกเป็น 3 ระดับ ได้แก่ ระดับความรู้มาก (18–25 คะแนน) ปานกลาง (13–17 คะแนน) และน้อย (0–12 คะแนน) ซึ่งผลการเปรียบเทียบระดับความรู้ในช่วงก่อนและหลังเรียน ปรากฏดังตารางที่ 4-8

ตารางที่ 4-8 ตารางเปรียบเทียบการจัดกลุ่มคะแนนตามระดับความรู้ (ก่อนและหลังเรียน)

ระดับความรู้	ก่อนเรียน (คน)	ก่อนเรียน (%)	หลังเรียน (คน)	หลังเรียน (%)	เปลี่ยนแปลง (ร้อยละ ±)
น้อย	54	67.50	0	0.00	-67.50
ปานกลาง	24	30.00	14	17.50	-12.50
มาก	2	2.50	66	82.50	+80.00
รวม	80	100.00	80	100.00	—

จากตารางที่ 4-8 แสดงผลการเปรียบเทียบระดับความรู้ของบุคลากรก่อนและหลังการเข้าร่วมกิจกรรมการเรียนรู้ พบว่าก่อนการเรียนรู้ บุคลากรส่วนใหญ่มีความรู้ในระดับ “น้อย” จำนวน 54 คน คิดเป็นร้อยละ 67.50 รองลงมาคือระดับ “ปานกลาง” จำนวน 24 คน (ร้อยละ 30.00) และมีเพียง 2 คน (ร้อยละ 2.50) ที่มีความรู้ในระดับ “มาก” ผลดังกล่าวสะท้อนว่าบุคลากรส่วนใหญ่ยังมีพื้นฐานความรู้ด้านความปลอดภัยทางไซเบอร์ในระดับต่ำก่อนการเรียนรู้ หลังจากการเข้าร่วมกิจกรรมสื่อการเรียนรู้ออนไลน์ พบการเปลี่ยนแปลงในทางที่ดีขึ้นอย่างชัดเจน โดยไม่พบผู้ที่มีความรู้ระดับ “น้อย” อีกต่อไป (ร้อยละ 0.00) กลุ่มผู้มีความรู้ระดับ “ปานกลาง” ลดลงเหลือเพียง ร้อยละ 17.50 ในขณะที่กลุ่มผู้มีความรู้ระดับ “มาก” เพิ่มขึ้นอย่างเด่นชัดเป็น ร้อยละ 82.50 ซึ่งแสดงให้เห็นถึงผลลัพธ์ของการเรียนรู้ที่มีประสิทธิภาพ ผลการเปลี่ยนแปลงดังกล่าวสอดคล้องกับผลการทดสอบทางสถิติที่ได้รายงานไว้ก่อนหน้านี้ ซึ่งยืนยันว่าคะแนนหลังเรียนสูงกว่าก่อนเรียนอย่างมีนัยสำคัญทางสถิติ

การเปลี่ยนแปลงดังกล่าวสะท้อนให้เห็นว่าสื่อการเรียนรู้ออนไลน์มีความเหมาะสมกับบริบทของกลุ่มตัวอย่าง เนื่องจากเนื้อหามีการนำเสนอผ่านตัวอย่างสถานการณ์จริงในงานประจำของคลินิก ทำให้ผู้เรียนสามารถเชื่อมโยงความรู้กับพฤติกรรมการปฏิบัติงานได้โดยตรง เช่น การป้องกันการเปิดอีเมลที่มีความเสี่ยง การตั้งรหัสผ่านที่ปลอดภัย และการดูแลการเข้าถึงข้อมูลผู้ป่วยบนระบบคลาวด์ ส่งผลให้เกิดการพัฒนาความรู้และความตระหนักรู้ในระดับที่สูงขึ้นอย่างมีนัยสำคัญ

ตารางที่ 4-9 ตารางเปรียบเทียบการจัดกลุ่มคะแนนแต่ละด้าน (ก่อนและหลังเรียน)

ด้าน	ก่อนอบรม			หลังอบรม		
	น้อย	ปานกลาง	มาก	น้อย	ปานกลาง	มาก
ด้านที่ 1 ความหมายและความสำคัญของความมั่นคงปลอดภัยไซเบอร์	65.00%	32.50%	2.50%	6.00%	29.00%	65.00%
ด้านที่ 2 ประเภทของมัลแวร์	70.00%	27.50%	2.50%	11.00%	31.00%	58.00%
ด้านที่ 3 ประเภทของการโจมตีทางไซเบอร์	80.00%	18.75%	1.25%	12.00%	30.00%	58.00%
ด้านที่ 4 ความมั่นคงปลอดภัยในชีวิตประจำวัน	55.00%	40.00%	5.00%	5.00%	27.00%	68.00%
เฉลี่ย 4 ด้าน	**67.50%**	**29.69%**	**2.81%**	**8.50%**	**29.25%**	**62.25%**

จากจากตารางที่ 4-9 พบว่า หลังการอบรม บุคลากรมีระดับความรู้เพิ่มขึ้นในทุกด้านอย่างชัดเจน โดยเฉพาะ ด้านที่ 4 (ความมั่นคงปลอดภัยในชีวิตประจำวัน) ซึ่งเกี่ยวข้องกับพฤติกรรมการใช้งานเทคโนโลยีในชีวิตจริง มีสัดส่วนของผู้ตอบที่อยู่ในระดับความรู้ “มาก” สูงที่สุดคือ ร้อยละ 68 แสดงให้เห็นว่าผู้เข้าอบรมสามารถนำความรู้จากสื่อการเรียนรู้ไปปรับใช้ในการปฏิบัติงานและชีวิตประจำวันได้อย่างมีประสิทธิภาพ และเกิดการตระหนักรู้ถึงความสำคัญของพฤติกรรมปลอดภัยในโลกดิจิทัลมากยิ่งขึ้น ด้านที่ 1 (ความหมายและความสำคัญของความมั่นคงปลอดภัยไซเบอร์) มีผู้ตอบในระดับ “มาก” รองลงมา คือ ร้อยละ 65 สะท้อนให้เห็นว่าผู้เข้าอบรมเข้าใจแนวคิดพื้นฐานและหลักการสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้ดีขึ้น ซึ่งเป็นรากฐานสำคัญที่ส่งผลต่อการพัฒนาความเข้าใจในด้านอื่น ๆ ที่ซับซ้อนกว่า สำหรับ ด้านที่ 2 (ประเภทของมัลแวร์) และ ด้านที่ 3 (ประเภทของการโจมตีทางไซเบอร์) มีสัดส่วนผู้ตอบระดับ “มาก” เท่ากันที่ ร้อยละ 58 แม้จะมีค่าน้อยกว่าด้านอื่น แต่ยังคงแสดงให้เห็นแนวโน้มการพัฒนาเชิงบวก โดยเฉพาะในประเด็นทางเทคนิคที่มักเข้าใจยากสำหรับบุคลากรทั่วไป ซึ่งสะท้อนว่าการเรียนรู้ผ่านสื่อออนไลน์ช่วยให้บุคลากรสามารถทำความเข้าใจภัยคุกคามไซเบอร์รูปแบบต่าง ๆ ได้ในระดับที่เพียงพอต่อการป้องกันตนเองในเบื้องต้น

โดยภาพรวม เมื่อพิจารณาทั้ง 4 ด้าน พบว่า บุคลากรมีระดับความรู้ “มาก” เพิ่มขึ้นอย่างมีนัยสำคัญ และระดับ “น้อย” ลดลงอย่างเห็นได้ชัด ทั้งนี้แนวโน้มของผลรายด้านมีความสอดคล้องกับผลโดยรวม กล่าวคือ หลังการอบรม บุคลากรส่วนใหญ่สามารถเข้าใจทั้งแนวคิดพื้นฐาน ภัยคุกคาม

และแนวทางการป้องกันตนเองในชีวิตประจำวันได้ดียิ่งขึ้น แสดงให้เห็นถึง ประสิทธิผลของสื่อการเรียนรู้ออนไลน์ที่พัฒนาขึ้น ว่าสามารถส่งเสริมทั้งความรู้ ความเข้าใจ และการนำไปใช้จริงในบริบทการทำงานบนระบบคลาวด์ของคลินิกได้อย่างเป็นรูปธรรม

ผลลัพธ์รายด้านที่สอดคล้องกันดังกล่าว แสดงให้เห็นว่าการเรียนรู้ออนไลน์มีบทบาทสำคัญในการเสริมสร้างความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์อย่างรอบด้าน โดยผู้เข้าอบรมสามารถพัฒนาความรู้ได้ทั้งในเชิงแนวคิดพื้นฐานและเชิงปฏิบัติจริงที่เกี่ยวข้องกับการใช้งานเทคโนโลยีในชีวิตประจำวัน ตลอดจนการระมัดระวังต่อภัยคุกคามไซเบอร์ในรูปแบบต่าง ๆ การเปลี่ยนแปลงที่เกิดขึ้นไม่เพียงเป็นการเพิ่มขึ้นของระดับคะแนนเท่านั้น แต่ยังสะท้อนถึงความตระหนักรู้ที่เพิ่มขึ้นต่อความเสี่ยงและความสำคัญในการปกป้องข้อมูลส่วนบุคคลและข้อมูลผู้ป่วยของคลินิก ซึ่งเป็นข้อมูลที่มีความละเอียดอ่อนและต้องการมาตรการรักษาความปลอดภัยที่เหมาะสม สื่อการเรียนรู้ที่นำมาใช้จึงมีส่วนช่วยกระตุ้นให้บุคลากรเกิดความเข้าใจและความพร้อมต่อการปฏิบัติตามแนวทางความปลอดภัยไซเบอร์ในบริบทของการทำงานบนระบบคลาวด์ได้อย่างมีประสิทธิภาพ

บทที่ 5
สรุป อภิปรายผล และข้อเสนอแนะ

จากการศึกษางานวิจัยเรื่องการประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ในคลินิกเอกชนแห่งหนึ่ง โดยใช้แบบทดสอบก่อนและหลังเรียนเพื่อวัดผล จากการวิเคราะห์เปรียบเทียบผลลัพธ์ของค่าคะแนน สามารถสรุปผลการดำเนินงานออกเป็น 3 ส่วน

5.1 สรุปผลการวิจัย

5.2 อภิปรายผลการวิจัย

5.3 ข้อเสนอแนะ

5.1 สรุปผลการวิจัย

5.1.1 สรุปผลโดยรวม

ผลการวิจัยโดยรวมแสดงให้เห็นว่า สื่อการเรียนรู้ออนไลน์มีประสิทธิภาพสูงมากในการยกระดับความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรในคลินิกเอกชนแห่งหนึ่ง โดยก่อนการอบรม ค่าเฉลี่ยคะแนนความตระหนักรู้อยู่ในระดับต่ำเพียง 9.25 คะแนน และบุคลากรส่วนใหญ่จัดอยู่ในระดับ ความรู้น้อย (81.25%) ขณะที่ภายหลังการเข้าร่วมกิจกรรมการเรียนรู้ผ่านสื่อออนไลน์แบบโต้ตอบ (Interactive Learning) ค่าเฉลี่ยคะแนนเพิ่มสูงขึ้นเป็น 19.75 คะแนน ซึ่งเป็นผลต่างที่เพิ่มขึ้นถึง 10.50 คะแนน และส่งผลให้บุคลากรส่วนใหญ่อยู่ในระดับ ความรู้มาก (81.25%) โดยมีบุคลากรที่อยู่ในระดับความรู้น้อยเพียง 2.50% เท่านั้น

เมื่อพิจารณาการกระจายตัวของคะแนน (Data Dispersion) พบว่าหลังการเรียนรู้ คะแนนมีความสม่ำเสมอมากขึ้นอย่างเด่นชัด โดยค่าความเบี่ยงเบนมาตรฐาน (S.D.) ลดลงจาก 3.31 เป็น 2.80 สะท้อนว่าผู้เรียนมีระดับคะแนนใกล้เคียงกันมากขึ้น และเมื่อแปลงค่า S.D. ให้อยู่ในรูปแบบมาตรฐาน (S.D. แบบ normalized = S.D. ÷ คะแนนเต็ม 25) พบว่าค่าลดลงจาก 0.132 ก่อนเรียน เหลือเพียง 0.112 หลังเรียน หรือคิดเป็นการลดลงเชิงสัดส่วนของการกระจายคะแนนประมาณ 2% ของคะแนนเต็ม ผลดังกล่าวชี้ให้เห็นว่าความแตกต่างระหว่างผู้เรียนลดลงทั้งในเชิงค่าจริงและเชิงสัดส่วนของคะแนนเต็ม ซึ่งเป็นตัวบ่งชี้ถึงความเข้าใจที่ใกล้เคียงกันและการเรียนรู้ที่มีประสิทธิภาพในกลุ่มตัวอย่าง

ขณะเดียวกัน ค่าสัมประสิทธิ์ความแปรผัน (Coefficient of Variation: C.V.) ซึ่งใช้เปรียบเทียบระดับการกระจายสัมพัทธ์ของคะแนน พบว่าลดลงอย่างชัดเจนจาก 0.358 (35.8%) ก่อนเรียน เหลือเพียง 0.142 (14.2%) หลังเรียน แสดงว่าผลสัมฤทธิ์ทางการเรียนของผู้เข้าร่วมมีความสม่ำเสมอมากขึ้น โดยผู้เรียนส่วนใหญ่เข้าใจเนื้อหาในทิศทางเดียวกันมากกว่าเดิม

ผลการทดสอบทางสถิติแบบ Paired Samples t-test ยืนยันแนวโน้มดังกล่าว โดยพบว่าค่าเฉลี่ยคะแนนหลังเรียนสูงกว่าก่อนเรียนอย่างมีนัยสำคัญทางสถิติที่ระดับ .001 ($t = 21.040$, $df = 79$, $p < .001$**) และมีขนาดอิทธิพล (Cohen's $d_z = 2.35$) ซึ่งอยู่ในระดับ "สูงมาก" (Very Large Effect) ตามเกณฑ์ของ Cohen (1988) แสดงให้เห็นว่าสื่อการเรียนรู้ที่พัฒนาขึ้นมีผลต่อการพัฒนาความรู้ของบุคลากรอย่างมีประสิทธิภาพและชัดเจนในเชิงผลลัพธ์

โดยสรุป สื่อการเรียนรู้ออนไลน์ที่พัฒนาด้วยแพลตฟอร์ม Genially สามารถส่งเสริมให้บุคลากรมีผลสัมฤทธิ์ทางการเรียนรู้และความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์เพิ่มขึ้นอย่างมีนัยสำคัญ ทั้งในเชิงปริมาณ (ค่าเฉลี่ยคะแนนเพิ่มขึ้น) และเชิงคุณภาพ (ค่าการกระจายของคะแนนลดลง — ทั้ง S.D. ดิบ, S.D. แบบ normalized, และ C.V.) ซึ่งสะท้อนถึงประสิทธิภาพของสื่อที่ออกแบบให้มี การมีส่วนร่วม (Engagement), การโต้ตอบ (Interactivity) และ สถานการณ์จำลอง (Simulation) ที่ใกล้เคียงกับสภาพการทำงานจริง ทำให้ผู้เรียนสามารถนำความรู้ไปปรับใช้ในบริบทจริงได้อย่างมีประสิทธิผลและยั่งยืน

5.1.2 สรุปข้อมูลพื้นฐานของผู้ตอบแบบสอบถาม

จากการรวบรวมข้อมูลของกลุ่มตัวอย่างจำนวน 80 คน พบว่าผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง (75.00%) ซึ่งมีสัดส่วนสูงกว่าเพศชายอย่างชัดเจน และอยู่ในช่วงอายุ 21–30 ปี (50.00%) ซึ่งเป็นกลุ่มวัยทำงานตอนต้นที่มีความคุ้นเคยกับเทคโนโลยีดิจิทัล แต่ก็มีแนวโน้มที่จะเผชิญความเสี่ยงสูงกว่าในการรับมือภัยคุกคามรูปแบบใหม่

ในด้านตำแหน่งงาน พบว่าผู้เข้าร่วมส่วนใหญ่อยู่ในตำแหน่ง พนักงานปฏิบัติงาน (71.25%) ซึ่งเป็นกลุ่มที่ใช้ระบบคลาวด์โดยตรงในงานประจำวัน การที่กลุ่มตัวอย่างหลักเป็นผู้ใช้งานระดับปฏิบัติการ (Frontline Users) ทำให้ผลการวิจัยมีความสำคัญอย่างยิ่ง เนื่องจากเป็นการประเมินความตระหนักรู้ของบุคลากรที่มีบทบาทโดยตรงในการปกป้องข้อมูลขององค์กร

เมื่อพิจารณาการเปรียบเทียบตามตัวแปรทางประชากร เช่น เพศ อายุ และตำแหน่งงาน พบว่าไม่มีความแตกต่างอย่างมีนัยสำคัญทางสถิติ ซึ่งแสดงว่าสื่อการเรียนรู้ออนไลน์ที่พัฒนาขึ้นมีประสิทธิภาพเท่าเทียมกันในทุกกลุ่มผู้เรียน และสามารถเข้าถึงบุคลากรได้อย่างทั่วถึง

5.2 อภิปรายผลการวิจัย

ผลการวิจัยแสดงให้เห็นว่าคะแนนความตระหนักรู้เพิ่มขึ้นอย่างมีนัยสำคัญทางสถิติหลังการอบรม (จากค่าเฉลี่ย 9.20 เป็น 20.30; ผลต่างเฉลี่ย 11.10 คะแนน; $t(79)=18.51$, $p<.001$; ขนาดอำนาจอธิบาย Cohen's $d_z=2.07$) ซึ่งตีความได้ว่าโปรแกรมการเรียนรู้ที่พัฒนาด้วยสื่อออนไลน์มี ผลกระทบระดับสูงมาก ตามเกณฑ์ของ Cohen [28] เมื่อพิจารณาการกระจายระดับความรู้ พบว่าสัดส่วนผู้ที่อยู่ในระดับ “มาก” เพิ่มขึ้นอย่างเด่นชัด ขณะที่ระดับ “น้อย” ลดลงเป็นศูนย์ สะท้อนถึงการยกระดับสมรรถนะเชิงการรับรู้ของบุคลากรอย่างกว้างขวาง

ผลลัพธ์ดังกล่าวสอดคล้องกับกรอบ KAB Model ที่ชี้ว่า “ความรู้ (Knowledge)” ที่เพิ่มขึ้นจะส่งผลต่อ “ทัศนคติ (Attitude)” และนำไปสู่ “พฤติกรรม (Behavior)” ที่ปลอดภัยมากขึ้นเมื่อเผชิญความเสี่ยงไซเบอร์ ทั้งนี้ แม้งานวิจัยครั้งนี้จะวัดผลเป็นคะแนนความรู้เป็นหลัก แต่การออกแบบกิจกรรมแบบโต้ตอบ (interactive) ที่จำลองสถานการณ์ภัยคุกคามและให้ป้อนกลับทันที ย่อมเอื้อต่อการก่อตัวของทัศนคติและการลงมือปฏิบัติที่ถูกต้องตามลำดับขั้นของ KAB กล่าวคือ เมื่อบุคลากรเข้าใจภัยคุกคาม (Know) เกิดความตระหนักและความรู้สึกอยากป้องกัน (Feel) จึงแสดงพฤติกรรมที่ปลอดภัยมากขึ้น (Do) [30], [31]

กลไกที่ทำให้สื่อออนไลน์มีประสิทธิภาพ อธิบายได้จาก (1) ความเป็นสื่อโต้ตอบ ของ Genially ที่เปิดโอกาสให้ผู้เรียนทดลอง-ผิด-ถูกและได้รับ feedback ทันที ช่วยเสริมการประมวลผลเชิงลึกตาม

หลัก multimedia learning ของ Mayer [18] และสอดคล้องกับหลักการออกแบบการสอนของ Gagné [17] (2) ความสอดคล้องกับบริบทงานจริงบนระบบคลาวด์ของคลินิก เนื้อหาและตัวอย่างใช้กรณีที่บุคลากรพบในงานจริง เช่น การจัดการเวชระเบียน การควบคุมการเข้าถึง และการป้องกันฟิชชิง จึงเอื้อต่อ transfer ไปสู่พฤติกรรมการทำงาน (3) การยึดมาตรฐานและข้อกำกับร่วมสมัย (เช่น นิยามและความเสี่ยงบนคลาวด์ [20], [21]) ทำให้ผู้เรียนเห็นภาพของมาตรการปฏิบัติที่สอดคล้องทั้งเชิงเทคนิคและเชิงนโยบายในสถานบริการสุขภาพ [5]

เมื่อเปรียบเทียบกับงานวิจัยที่เกี่ยวข้อง (ข้อ 2.7) ผลการเพิ่มขึ้นของคะแนนหลังการฝึกอบรมสอดคล้อง กับงานของ พันธนนท์ [4] ที่รายงานผลสัมฤทธิ์หลังอบรมสูงขึ้นอย่างมีนัยสำคัญ และ สอดรับ กับข้อค้นพบของ วิไล ฤทธิเดช [7] ที่ระบุว่าบุคลากรสาธารณสุขต้องการการอบรมอย่างต่อเนื่องเพื่อปิดช่องว่างทักษะพื้นฐาน ด้านประสิทธิภาพของสื่อที่มีปฏิสัมพันธ์ ผลของเรายัง เป็นไปในทิศทางเดียวกัน กับ DeCarlo [25] ที่พบว่า gamified/interactive learning ช่วยเพิ่มแรงจูงใจและการนำความรู้ไปใช้จริงได้ดีกว่าวิธีบรรยาย ทั้งนี้ ผลของเราขยายความรู้เดิมโดยนำสื่อโต้ตอบไปผูกกับ บริบทคลินิกบนระบบคลาวด์ ซึ่งยังมีหลักฐานเชิงประจักษ์จำกัดเมื่อเทียบกับบริบทอื่น ๆ [5], [20], [21]

ผลการวิเคราะห์รายด้านยืนยันแนวโน้มหลังอบรมชัดเจนว่า ความรู้เพิ่มขึ้นทุกด้าน โดยเฉพาะด้านที่ 4 (ชีวิตประจำวัน) ซึ่งเชื่อมกับพฤติกรรมจริง มีผู้ตอบระดับ “มาก” สูงสุด ร้อยละ 68 สะท้อนการนำความรู้ไปใช้ได้จริง รองลงมาคือ ด้านที่ 1 (ความหมายและความสำคัญ) ร้อยละ 65 แสดงถึงความเข้าใจพื้นฐานที่มั่นคง ส่วน ด้านที่ 2 (มัลแวร์) และ ด้านที่ 3 (การโจมตี) อยู่ที่ ร้อยละ 58 แม้ซับซ้อนกว่าแต่ยังเพิ่มขึ้นอย่างมีนัยสำคัญ โดยสรุป ผลรายด้านสอดคล้องกับภาพรวม คือ กลุ่ม “มาก” เพิ่มขึ้นและ “น้อย” ลดลงอย่างเด่นชัด สะท้อน ประสิทธิผลของสื่อการเรียนรู้ออนไลน์ ในการยกระดับความรู้และเอื้อต่อการประยุกต์ใช้เชิงพฤติกรรมในงานจริง

5.3 ข้อเสนอแนะ

5.3.1 ข้อเสนอแนะในการนำผลวิจัยไปใช้ (Practical Recommendations)

5.3.1.1 บรรจุหลักสูตรในการปฐมนิเทศและการอบรมประจำปี ควรนำชุดความรู้ที่ใช้ในการอบรมนี้ไปพัฒนาเป็น หลักสูตรภาคบังคับ สำหรับบุคลากรใหม่ และจัดให้มีการ ทบทวนความรู้อย่างต่อเนื่องทุก 6 ถึง 12 เดือน เพื่อให้ความตระหนักรู้ไม่ลดลงตามกาลเวลา เนื่องจากภัยคุกคามทางไซเบอร์มีการเปลี่ยนแปลงอยู่ตลอดเวลา

5.3.1.2 เชื่อมโยงผลการอบรมกับนโยบายองค์กร ควรนำความรู้ที่เพิ่มขึ้นไปปรับใช้ในการกำหนด นโยบายและแนวปฏิบัติที่เป็นรูปธรรม โดยเฉพาะอย่างยิ่งการใช้รหัสผ่านที่รัดกุม การรายงานเหตุการณ์ที่น่าสงสัยทันที และขั้นตอนการจัดการข้อมูลส่วนบุคคลบนระบบคลาวด์ เพื่อให้ความตระหนักรู้ถูกแปลงไปสู่การปฏิบัติงานจริงอย่างเป็นระบบ

5.3.1.3 ใช้คะแนนเฉลี่ยหลังเรียนเป็นตัวชี้วัด คลินิกควรใช้ค่าเฉลี่ยคะแนนหลังเรียน 19.75 (หรือร้อยละ 81.25 ของผู้มีความรู้มาก) เป็น เกณฑ์มาตรฐาน (Baseline Score) สำหรับการประเมินประสิทธิภาพความตระหนักรู้ของบุคลากรในรอบปีถัดไป

5.3.1.4 บูรณาการสื่อเข้ากับระบบงาน ควรนำสื่อการเรียนรู้ออนไลน์ที่พัฒนาด้วย Genially ไปบูรณาการเข้ากับ แพลตฟอร์มการเรียนรู้ (LMS) หรือระบบ On-boarding ของคลินิก

เพื่อให้บุคลากรเข้าถึงสื่อได้ง่ายและสามารถเรียนรู้ได้ด้วยตนเองตามความสะดวก (Self-paced Learning)

5.3.2 ข้อเสนอแนะสำหรับการวิจัยในอนาคต (Future Research Recommendations)

5.3.2.1 การขยายขอบเขตเนื้อหาของสื่อการเรียนรู้ จากผลการวิจัยที่ชี้ชัดว่าสื่อการเรียนรู้แบบโต้ตอบมีประสิทธิภาพสูง งานวิจัยในอนาคตจึงควร พัฒนาสื่อการเรียนรู้ให้ครอบคลุมหัวข้อสำคัญอื่นๆ ที่เกี่ยวข้องกับบริบทของคลินิกโดยตรง โดยเฉพาะเนื้อหาที่เกี่ยวข้องกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อให้บุคลากรไม่เพียงตระหนักถึงภัยคุกคาม แต่ยังเข้าใจถึงหน้าที่และความรับผิดชอบตามกฎหมายในการจัดการข้อมูลคนไข้

5.3.2.2 วิจัยเชิงพฤติกรรมเพื่อวัดผลในระยะยาว ควรมีการวิจัยติดตามผลเพื่อประเมินความยั่งยืนของความตระหนักรู้ และที่สำคัญคือการเปลี่ยนแปลงของ พฤติกรรมการใช้งานจริง (Behavior) ของบุคลากรในระยะ 3-6 เดือน ถึง 1 ปี หลังสิ้นสุดการอบรม. วิธีการที่มีประสิทธิภาพคือการใช้เครื่องมือจำลองสถานการณ์การโจมตี เช่น การทำ Phishing Simulation เพื่อเก็บข้อมูลเชิงประจักษ์ และยืนยันว่าความรู้ที่เพิ่มขึ้นได้นำไปสู่พฤติกรรมการป้องกันภัยที่ยั่งยืนจริง

5.3.2.3 วิจัยเชิงคุณภาพเพื่อหาปัจจัยเชิงลึก ควรศึกษาปัจจัยเชิงลึก เช่น วัฒนธรรมองค์กร, แรงจูงใจส่วนบุคคล, หรือรูปแบบการเรียนรู้ ที่มีอิทธิพลต่อการนำความรู้ไปใช้จริง เพื่อนำผลมาปรับปรุงการออกแบบสื่อการเรียนรู้ให้มีประสิทธิภาพสูงสุดในบริบทขององค์กรขนาดเล็กและภาคบริการสุขภาพ

5.3.2.4 การวิจัยต่อยอดเพื่อทดสอบตัวแบบทางทฤษฎี ควรมีการวิจัยต่อยอดเพื่อ ทดสอบตัวแบบ (Model) ที่เชื่อมโยงประสิทธิผลของสื่อการเรียนรู้กับการนำไปใช้จริง โดยใช้ทฤษฎีความปลอดภัยไซเบอร์ (เช่น Protection Motivation Theory - PMT) หรือกรอบแนวคิดด้านความปลอดภัย (เช่น NIST Cybersecurity Framework) เป็นกรอบในการวิเคราะห์ เพื่อเพิ่มความลึกซึ้งทางทฤษฎีให้กับผลการวิจัย

5.3.2.5 การวิจัยเชิงเปรียบเทียบเพื่อประเมินการประยุกต์ใช้ในวงกว้าง ควรมีการวิจัยแบบ เปรียบเทียบ (Comparative Study) โดยนำสื่อนี้ไปทดลองใช้กับบุคลากรในองค์กรสุขภาพอื่นที่มีขนาดใหญ่กว่า หรือมีการใช้งานระบบคลาวด์ที่ซับซ้อนกว่า เพื่อประเมินความสามารถในการนำไปปรับใช้ในภาพรวม (Generalizability) ของสื่อการเรียนรู้ที่พัฒนาขึ้น

บรรณานุกรม

1. This is Mend Symantec, a Division of Broadcom. (2021). The Ransomware Threat in 2021: Evolution of a Crisis. White Paper.

2. ณัฐ กุลกฤษฎา. (2566). การส่งเสริมความตระหนักรู้การเขียนโปรแกรมที่มีความมั่นคงปลอดภัยผ่านสื่อออนไลน์. กรุงเทพมหานคร: มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.

3. อนาวิล แก้วสะอาด, รัฐวี อุตกฤษฎ์. (2564). แนวทางบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร. กรุงเทพมหานคร: มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.

4. พันธนนท์ สกุลชินสีห์. (2566). การประเมินความตระหนักรู้ถึงภัยคุกคามไซเบอร์ของบุคลากรผู้ปฏิบัติงานระบบเครือข่ายอินเทอร์เน็ตขององค์การบริหารส่วนตำบล. กรุงเทพมหานคร: มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.

5. วรรษา เปาอินทร์. (2565). การพัฒนาแนวทางปฏิบัติเพื่อพัฒนาความมั่นคงปลอดภัยและความเป็นส่วนตัวของข้อมูลสุขภาพ. วารสารสมาคมเวชสารสนเทศไทย, 1(1), 1–13.

6. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2562). พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. กรุงเทพมหานคร : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

7. วิไล ฤทธิเดช. (2565). ความรู้ ความตระหนักและพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรสาธารณสุขในประเทศไทย: กรณีศึกษาโรงพยาบาลพุทธโธร. กรุงเทพมหานคร: มหาวิทยาลัยศิลปากร.

8. ปริญญา หอมอเนก, ACIS Research LAB. (2557). บทวิเคราะห์กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก. National Defense Studies Institute Journal.

9. สุทธิพันธุ์ ชวลิตเลขา. (2564). การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรในบริษัทวิทยุการบินแห่งประเทศไทย จำกัด. กรุงเทพมหานคร: มหาวิทยาลัยศรีปทุม.

10. คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์. (2566). หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566. ราชกิจจานุเบกษา, 140(พิเศษ 107), 39.

11. สมศิริ พันธุ์ศักดิ์ศิริ, เสาวนีย์ สมันต์ตรีพร. (2566). ประสิทธิผลของการจัดการความปลอดภัยระบบสารสนเทศ โรงพยาบาลสระบุรี. วารสารสหวิทยาการมนุษยศาสตร์และสังคมศาสตร์, 6(2), 1047–1065.

12. เมธาพร ธรรมศิริ, ศิรภัสสศ์ วงศ์ทองดี. (2565). ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร. Research and Management Journal.

13. วิลาส วิถีไพร. (2561). การพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง. กรุงเทพมหานคร: มหาวิทยาลัยศรีปทุม.

14. ชรินทิพย์ ปั้นสุวรรณ, สุมนทิพย์ จิตสว่าง. (2566). แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล. วารสารออนไลน์.

15. Twinkl Blog. (2568). ทำความรู้จักกับสื่อการสอน. สืบค้นเมื่อ 25 กรกฎาคม 2568, จาก https://www.twinkl.co.th/blog/teaching-resources

16. ARITC Online. (2566). เครื่องมือแบบ Interactive Genially. YouTube. สืบค้นเมื่อ 30 กรกฎาคม 2568, จาก https://www.youtube.com/watch?v=jGOEZGj_NWw

17. Gagné, R. M., Wager, W. W., Golas, K. C., & Keller, J. M. (2005). Principles of instructional design. 5th ed. Wadsworth/Thomson Learning.

18. Mayer, R. E. (2009). Multimedia learning. 2nd ed. Cambridge: Cambridge University Press.

19. Dick, W., Carey, L., & Carey, J. O. (2015). The systematic design of instruction. 8th ed. Pearson.

20. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. Gaithersburg (MD): National Institute of Standards and Technology, United States Department of Commerce.

21. Hashizume, K., Rosado, D., Fernández, M., & Diaz, F. (2013). An analysis of security issues for cloud computing. Journal of Network and Computer Applications, 40(1), 164–185.

22. Andress, J. (2019). Foundations of Information Security: A Straightforward Introduction. No Starch Press.

23. วันทนีย์ ชัยนาจิตร. (2567). การยกระดับความตระหนักรู้ด้านการใช้ดิจิทัลเพื่อความมั่นคงปลอดภัยในอาสาสมัครสาธารณสุขประจำหมู่บ้าน. กรุงเทพมหานคร: มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.

24. สุภาพร พันธ์ยา, คริชณะ ฉิมมณีราชศักดิ์, สมยานนทนากุล. (2566). การตระหนักรู้เท่าทันภัยคุกคามจากการใช้อินเทอร์เน็ต: กรณีจำลองการโจมตีด้วยการคาดเดารหัสผ่าน. ปทุมธานี: มหาวิทยาลัยรังสิต.

25. DeCarlo, S. M. (2020). Measuring the Application of Knowledge Gained from the Gamification of Cybersecurity Training in Healthcare. Robert Morris University.

26. Verizon. (2025). 2025 Data Breach Investigations Report (DBIR). สืบค้นเมื่อ 30 กันยายน 2568, จาก https://www.verizon.com/business/resources/reports/dbir/

27. IBM Security. (2025). Cost of a Data Breach Report 2025. สืบค้นเมื่อ 30 กันยายน 2568, จาก https://www.ibm.com/security/data-breach.

28. Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.). Lawrence Erlbaum. Eley biography

29. Yamane, T. (1967). Statistics: An introductory analysis (2nd ed.). Harper & Row.

ภาคผนวก

ภาคผนวก ก
แบบทดสอบการประเมินความตระหนักรู้

แบบสอบถามประเมินความตระหนักรู้

เรื่อง การประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์

แบบสอบถามชุดนี้จัดทำขึ้นโดยมีวัตถุประสงค์ ประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ ของบุคลากรของคลินิกเ
สาขาการแพทย์แผนจีนหัวเฉียว ซึ่งเป็นส่วนหนึ่งของวิชา การค้นคว้าอิสระ รหัสวิชา 070315002 หลักสูตรวิทยาศาสตร์มหาบัณฑิต คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล สาขาวิชา การบริหารเครือข่าย และความมั่นคงปลอดภัยสารสนเทศ ทางผู้วิจัยใคร่ขอความร่วมมือจากผู้ตอบแบบสอบถาม ในการให้ข้อมูลที่ตรงกับสภาพความเป็นจริงมากที่สุด โดยที่ข้อมูล ทั้งหมดของท่านจะถูกเก็บเป็นความลับ และใช้เพื่อประโยชน์ทางการศึกษาเท่านั้น
แบบสอบถามประกอบด้วย 2 ส่วน รวมทั้งสิ้น 30 ข้อ
ส่วนที่ 1 ข้อมูลส่วนบุคคล ลักษณะทางประชากร จำนวน 5 ข้อ
ส่วนที่ 2 ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ จำนวน 25 ข้อ ประกอบไปด้วย 4 หัวข้อ ได้แก่
1.ความหมายและความสำคัญของ Cyber Security = 5 ข้อ
2.ประเภทของมัลแวร์ = 5 ข้อ
3.ประเภทการโจมตีทางไซเบอร์ = 6 ข้อ
4.ความตระหนักรู้ด้านCyberSecurity ในชีวิตประจำวัน = 9 ข้อ

จะรบกวนเวลาของท่านประมาณ 20นาที ขอขอบพระคุณทุกท่านที่กรุณาสละเวลาในการตอบแบบสอบถาม มา ณ โอกาสนี้

นักศึกษาปริญญาโท คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล สาขาวิชา การบริหารเครือข่าย และความมั่นคงปลอดภัยสารสนเทศ

กรุณากรอก ชื่อ-สกุล *

Your answer

รหัสพนักงาน *

Your answer

ส่วนที่ 2 แบบทดสอบความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ จำนวน 25 ข้อ

ประกอบไปด้วย 4 หัวข้อ ได้แก่
01 Cyber security คืออะไร
02 ประเภทของมัลแวร์
03 ประเภทการโจมตีทางไซเบอร์
04 ความตระหนักรู้ด้านCyberSecurity ในชีวิตประจำวัน

1. ข้อใดคือวัตถุประสงค์หลักของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ครอบคลุมมากที่สุด ซึ่งสะท้อนถึงหลักการพื้นฐานของ 'CIA Triad'? *

- a. การป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต และการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- b.การปกป้องข้อมูลจากการถูกแก้ไข และการทำให้ระบบสารสนเทศทำงานได้ตลอดเวลา
- c.การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลและระบบ
- d.การยืนยันตัวตนของผู้ใช้งาน (Authentication) การห้ามปฏิเสธความรับผิด (Non-repudiation) และการปฏิบัติตามนโยบายองค์กร

2. การรักษาความมั่นคงปลอดภัยสารสนเทศในคลินิกฯเป็นหน้าที่ใคร? *

- a.ผู้บริหารระดับสูง
- b.เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ (IT)
- c.เจ้าหน้าที่ทุกคนที่มีสิทธิ์เข้าถึงข้อมูล
- d.เจ้าหน้าที่เวร์เวชระเบียน

3.การที่บุคคลไม่ได้รับอนุญาตทำการเปลี่ยนแปลง แก้ไข หรือลบข้อมูลผู้ป่วยในระบบสารสนเทศทางการแพทย์ ถือเป็นการละเมิดหลักการความมั่นคงปลอดภัยไซเบอร์ข้อใด *

- a. การรักษาความลับ Confidentiality
- b.การรักษาความครบถ้วนสมบูรณ์ Integrity
- c. ความถูกต้องแท้จริง Authenticity
- d.การห้ามปฏิเสธความรับผิด Non-repudiation

4. การเข้าไปดูข้อมูลประวัติส่วนตัวของ ผู้ป่วยแล้วเอาไปบอกต่อกับบุคคลอื่น ถือว่าผิดหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ข้อใด? *

- a. การห้ามปฏิเสธความรับผิด Non-repudiation
- b.การรักษาความลับ Confidentiality
- c. การรักษาความครบถ้วนสมบูรณ์ Integrity
- d.การรักษาความพร้อมใช้งาน Availability

5. สถานการณ์ใดต่อไปนี้ที่แสดงถึงการละเมิดหลักการความพร้อมใช้งานของระบบ (Availability) มากที่สุด? *

- a.ข้อมูลส่วนตัวของลูกค้าถูกเปิดเผยสู่สาธารณะโดยไม่ได้รับอนุญาต
- b.พนักงานปฏิเสธว่าไม่ได้เป็นคนส่งข้อมูลสำคัญออกจากบริษัท แม้จะมีบันทึกการกระทำไว้
- c.ผู้ไม่หวังดีแอบแก้ไขข้อมูลราคาในเว็บไซต์ขายของออนไลน์
- d.ระบบ HIS ล่มไม่สามารถให้บริการได้

6. มัลแวร์ประเภทใดที่มีวัตถุประสงค์หลักในการแอบสอดแนมกิจกรรมของผู้ใช้งานและเก็บข้อมูลที่ละเอียดอ่อน เช่น การพิมพ์บนแป้นพิมพ์, พฤติกรรมการเข้าชมเว็บไซต์, หรือข้อมูลส่วนบุคคล โดยที่ผู้ใช้งานไม่รู้ตัว? *

- a. Keylogger
- b. Spyware
- c. Adware
- d. Worm

7. คุณกำลังใช้งานคอมพิวเตอร์ที่ใช้ในการให้บริการผู้ป่วยในคลินิกฯ และทันใดนั้นหน้าจอคอมพิวเตอร์ก็แสดงข้อความแจ้งเตือน ดังรูปภาพ สิ่งแรกที่คุณควรดำเนินการเพื่อลดความเสียหายให้เหลือน้อยที่สุดคือข้อใด? *

- ○ a.กดปุ่มกากบาทเพื่อปิดหน้าต่างแจ้งเตือนและปิดเครื่องคอมพิวเตอร์ทันที
- ○ b.สำรองข้อมูลส่วนตัวของผู้ป่วยไว้ใน External Hard Disk โดยเร็วที่สุด
- ○ c.แจ้งฝ่ายเทคโนโลยีสารสนเทศ (IT) หรือผู้ที่รับผิดชอบทันที พร้อมทั้งหยุดการใช้งานคอมพิวเตอร์เครื่องนั้น
- ○ d.ถอดสาย LAN หรือปิดการเชื่อมต่อ Wi-Fi ทันที เพื่อตัดการแพร่กระจายของมัลแวร์

8. ข้อใดไม่ใช่ลักษณะของมัลแวร์ประเภท Trojan Horse? *

- ○ a.สามารถสร้างช่องทางลับ (Backdoor) เพื่อให้ผู้ไม่หวังดีเข้าถึงระบบได้
- ○ b.ปลอมตัวเป็นโปรแกรมที่มีประโยชน์
- ○ c.ต้องอาศัยการกระทำของผู้ใช้ในการติดตั้ง
- ○ d.สามารถแพร่กระจายตัวเองไปยังระบบอื่นได้โดยอัตโนมัติ

9. ข้อใดต่อไปนี้อธิบายความแตกต่างระหว่างWormและVirus ไม่ถูกต้อง? *

- a.Wormมีความสามารถในการแพร่กระจายได้อย่างรวดเร็วกว่าVirus
- b.Virusสามารถจำลองตัวเองได้โดยอาศัยโฮสต์แอปพลิเคชัน
- c.Worm สามารถจำลองตัวเองได้โดยอาศัยโฮสต์แอปพลิเคชัน
- d. Virus ถูกกำจัดออกจากระบบคอมพิวเตอร์ได้ยากกว่าWorm

10.มัลแวร์ประเภทใดที่มักจะปลอมตัวเป็นโปรแกรมที่ดูมีประโยชน์หรือน่าสนใจเพื่อหลอกให้ * ผู้ใช้ติดตั้ง?

- a.Ransomware
- b.Trojan
- c.Adware
- d. Spyware

11.ข้อใดไม่ใช่ประเภทภัยคุกคามทางไซเบอร์? *

- a.Man in the middle
- b.Botnet
- c.Insider Threat
- d.Cloud Computing

12.ในสถานการณ์ที่ต้องเผชิญกับอีเมลที่มีความน่าสงสัย พฤติกรรมการตอบสนองของ * บุคคลใดที่ถือว่ามีความเสี่ยงสูงสุดที่จะเปิดช่องทางให้เกิดการโจมตีจากผู้ไม่ประสงค์ดี?

- a.นายเอ คลิกดาวน์โหลดและเปิดไฟล์แนบชื่อ "ใบแจ้งหนี้.zip" ที่ได้รับจากอีเมลที่ไม่รู้จัก
- b.นายบี ตรวจสอบที่อยู่อีเมลผู้ส่ง (Sender's Email Address) อย่างละเอียดก่อนเปิดอีเมล
- c.นายซี โทรศัพท์สอบถามผู้ส่งต้นทางเพื่อยืนยันความถูกต้องของอีเมลก่อนที่จะดำเนินการใดๆ
- d.นายดี แจ้งให้ฝ่ายไอทีทราบทันทีเกี่ยวกับอีเมลที่น่าสงสัยนั้น

13. การโจมตีประเภทใดที่ Botnet มักถูกใช้มากที่สุด? *

- a.DDoS (Distributed Denial of Service) Attack
- b.Cross-Site Scripting (XSS)
- c.Password Attack
- d.Man-in-the-Middle Attack

14. การโจมตี (phishing) เป็นวิธีการที่ผู้โจมตีใช้เพื่อจุดประสงค์หลักในการบรรลุเป้าหมายใด? *

- a.การติดตั้งมัลแวร์เรียกค่าไถ่ (Ransomware) ลงบนคอมพิวเตอร์ของเหยื่อ
- b.การขัดขวางการทำงานของเว็บไซต์หรือบริการออนไลน์
- c.การเข้าถึงข้อมูลส่วนตัวและข้อมูลที่ละเอียดอ่อนของเหยื่อ
- d.การสแกนหาช่องโหว่ (Vulnerabilities) ในระบบเครือข่ายขององค์กร

15.ในการป้องกันการโจมตีแบบ **Phishing** ที่มีประสิทธิภาพมากที่สุดสำหรับผู้ใช้งานทั่วไป ควรให้ความสำคัญกับมาตรการใดเป็นอันดับแรก? *

- a.การตรวจสอบที่อยู่อีเมลผู้ส่งและไม่คลิกลิงก์หรือไฟล์แนบจากแหล่งที่ไม่น่าเชื่อถือ
- b.การใช้รหัสผ่านแบบ Multi-Factor Authentication (MFA) สำหรับทุกบัญชี
- c.การบล็อกอีเมลทั้งหมดที่มาจากที่อยู่ต่างประเทศที่ไม่คุ้นเคย
- d.ทั้งหมดที่กล่าวมา

16. ในการติดตั้งและใช้งาน Mobile Application ข้อใดคือแนวทางปฏิบัติที่ถูกต้องที่สุดเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัย? *

- a.อนุญาตให้แอปพลิเคชันเข้าถึงข้อมูลทุกอย่างที่ร้องขอทันที เพื่อให้ใช้งานได้ง่ายและไม่มีข้อผิดพลาด
- b.ปฏิเสธการให้สิทธิ์เข้าถึงทั้งหมดทันทีที่แอปพลิเคชันร้องขอ
- c.ให้สิทธิ์เข้าถึงเฉพาะข้อมูลและฟังก์ชันที่จำเป็นสำหรับการทำงานของแอปพลิเคชันนั้นๆ เท่านั้น
- d.ดาวน์โหลดและติดตั้งแอปพลิเคชันจากเว็บไซต์ทั่วไปที่ไม่ได้มาจาก App Store หรือ Play Store

17. ในบริบทของการรักษาความปลอดภัยข้อมูลผู้ป่วยในระบบสารสนเทศของคลินิก การกระทำใดของผู้ใช้งานมีความเสี่ยงสูงสุดที่จะเปิดช่องทางให้ผู้ไม่หวังดีสามารถเจาะระบบและเข้าถึงข้อมูลที่ละเอียดอ่อนได้? *

- a.การเชื่อมต่อ USB drive ที่ไม่ทราบที่มาเข้ากับคอมพิวเตอร์ที่ใช้ในคลินิกฯ
- b.การใช้อีเมลส่วนตัว (เช่น Gmail) ในการรับ-ส่งข้อมูลที่ต้องใช้ในคลินิก และเปิดไฟล์แนบที่ไม่รู้จักที่ได้รับจากอีเมลดังกล่าว
- c.การเข้าสู่ระบบด้วยรหัสผ่านที่ตั้งไว้ตามข้อมูลส่วนตัว เช่น 'ชื่อ+วันเกิด' และใช้รหัสนี้กับทุกบัญชีที่เกี่ยวข้องกับการทำงาน
- d.การตั้งค่า Antivirus เป็นโหมด 'ปิด' ชั่วคราว เพื่อติดตั้งโปรแกรมที่ดาวน์โหลดมาจากเว็บไซต์ที่ไม่ใช่ทางการ

18. คุณได้รับอีเมลที่อ้างว่ามาจาก 'Google' แจ้งว่ามีกิจกรรมน่าสงสัยในบัญชีของคุณและขอให้คุณคลิกที่ลิงก์เพื่อยืนยันตัวตน คุณควรทำอย่างไร? *

- a.คลิกที่ลิงก์ทันทีและกรอกข้อมูลส่วนตัวเพื่อยืนยันตัวตนให้เสร็จสิ้น
- b.ส่งต่ออีเมลนี้ให้เพื่อนหรือคนในครอบครัวเพื่อขอความช่วยเหลือในการตรวจสอบ
- c.ลบอีเมลนั้นทิ้งทันทีเพราะคิดว่าเป็นอีเมลขยะ
- d.ปิดอีเมลนั้นและเข้าไปที่เว็บไซต์ Google โดยตรง จากนั้นตรวจสอบการแจ้งเตือนในบัญชีของคุณ

19. ข้อใดคือความแตกต่างที่สำคัญระหว่าง Cloud Computing และ Cloud Storage? *

- a.Cloud Computing คือภาพรวมของการให้บริการด้านไอที ส่วน Cloud Storage เป็นแค่ส่วนหนึ่งของการจัดเก็บข้อมูล
- b. Cloud Computing เน้นการใช้งานซอฟต์แวร์ ส่วน Cloud Storage เน้นการสำรองข้อมูล
- c. ภัยคุกคามทางไซเบอร์ที่เกิดจากบุคคลภายในองค์กร
- d. Cloud Storage เป็นบริการที่จัดการโดยผู้ใช้ทั้งหมด ส่วน Cloud Computing จัดการโดยผู้ให้บริการ

20. ข้อใดคือลักษณะของรหัสผ่านที่ปลอดภัยที่สุด? *

- a.สั้นและง่ายต่อการจดจำ
- b.ใช้รหัสผ่านเดียวสำหรับทุกบัญชี
- c.มีตัวอักษรพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลข และสัญลักษณ์ผสมกัน
- d.เปลี่ยนรหัสผ่านทุกๆ 1 เดือน

21. ข้อใดไม่จัดเป็นการลงลายมือชื่ออิเล็กทรอนิกส์ e-Signature? *

- a.การใช้ Username และ Password
- b.การเสียบบัตรและใส่รหัส
- c.การถ่ายภาพเอกสารที่ลงลายมือชื่อแล้วส่งให้ผู้อื่น
- d.การกด I Accept หรือ ฉันยอมรับ

22. พิจารณาการทำธุรกรรมออนไลน์ที่สำคัญ เช่น การเข้าสู่ระบบอินเทอร์เน็ตแบงก์กิ้งหรือการซื้อของออนไลน์ เว็บไซต์ที่น่าเชื่อถือควรใช้งานบนโปรโตคอลใดเพื่อรับประกันความสมบูรณ์และความลับของข้อมูลที่ส่งผ่าน *

- a.HTTPS
- b.HTTP
- c.HTML
- d.HDLC

23. ข้อใดหมายถึง Cloud Computing *

- a.ระบบประมวลผลโดยใช้การสื่อสารทางไกล
- b.ระบบประมวลโดยใช้ทรัพยากรสารสนเทศร่วมกัน
- c.ระบบประมวลแบบใช้ Internet
- d..ระบบประมวลโดยใช้ทรัพยากรสารสนเทศและการสื่อสารร่วมกันโดยผ่านระบบInternet

24.หลักการ **3-2-1 Backup** ซึ่งเป็นแนวทางปฏิบัติที่ดีที่สุดในการสำรองข้อมูลเพื่อรับมือกับภัยพิบัติหรือข้อมูลสูญหาย มีองค์ประกอบเชิงกลยุทธ์ที่สำคัญและต้องปฏิบัติอย่างเคร่งครัดอย่างไร? *

- a.สำเนาข้อมูล 2 ชุด โดยแบ่งเป็น 1 รูปแบบสื่อบันทึกที่แตกต่างกัน และ เก็บสำเนา 3 ชุดไว้นอกสถานที่
- b.สำเนาข้อมูล 1 ชุด โดยเก็บไว้ใน 3 รูปแบบสื่อบันทึกที่แตกต่างกัน และ สำเนา 2 ชุด เก็บไว้นอกสถานที่
- c.สำเนาข้อมูล 3 ชุด โดยแบ่งเป็น 2 รูปแบบสื่อบันทึกที่แตกต่างกัน และ เก็บสำเนา 1 ชุดไว้นอกสถานที่
- d.ไม่มีข้อถูก

25. คุณกำลังเข้าใช้บริการ Wi-Fi สาธารณะที่ร้านกาแฟ เพื่อการสั่งของออนไลน์ การกระทำใดต่อไปนี้เป็นแนวทางที่ปลอดภัยที่สุดตามหลักการรักษาความปลอดภัยทางไซเบอร์? *

- a.เชื่อมต่อโดยตรงกับเครือข่าย Wi-Fi ที่ไม่มีการตั้งรหัสผ่าน เพื่อความสะดวกและรวดเร็ว
- b.เข้าใช้งานแอปพลิเคชันธนาคารและทำธุรกรรมทางการเงินที่สำคัญทันที
- c.ใช้ Wi-Fi จากแหล่งที่เชื่อถือได้ที่ใช้ชื่อว่า True Wi-Fi, AIS Wi-Fi, Dtac Wi-Fi
- d.ปิดการแชร์ไฟล์และปิดการเชื่อมต่ออัตโนมัติของ Wi-Fi ก่อนการใช้งาน

ภาคผนวก ข
หนังสือขอความอนุเคราะห์ในการเก็บรวบรวมแบบทดสอบ

ที่ อว ๗๑๐๗/ ๔๒๔

คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กทม. ๑๐๘๐๐

๗ สิงหาคม ๒๕๖๘

เรื่อง ขอความอนุเคราะห์เก็บรวบรวมข้อมูลเพื่อประกอบการทำการค้นคว้าอิสระ

เรียน ผู้อำนวยการคลินิก

เนื่องด้วย นายอโนชา คุ้มแพทย์ รหัสประจำตัว ๖๕-๐๗๐๑๑๘-๕๘๒๔-๕ นักศึกษาระดับบัณฑิตศึกษา ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กำลังดำเนินการจัดทำการค้นคว้าอิสระ เรื่อง "การประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ กรณีศึกษาคลินิกเอกชนแห่งหนึ่ง" โดยมี ผู้ช่วยศาตราจารย์ ดร. พงศ์ศรัณย์ บุญโญปกรณ์ เป็นอาจารย์ที่ปรึกษาหลักการค้นคว้าอิสระ ในการนี้ นักศึกษาประสงค์ขอความอนุเคราะห์ในการประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ของคลินิก เพื่อใช้ประกอบการทำการค้นคว้าอิสระต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ จักขอบพระคุณยิ่ง

มอบหมายให้ นายอโนชา คุ้มแพทย์
☐ ศึกษาข้อมูล
☑ ดำเนินการ
☐ สรุปและเสนอรายงานเพื่อกลุ่มบัติ

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ตั้งวรรณวิทย์)
รองคณบดีฝ่ายวิชาการและวิจัย
ปฏิบัติการแทนคณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

(นายอรัญ เยียมสุริย์)
ผู้อำนวยการ

ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
โทร. ๐ ๒๕๕๕ ๒๗๑๗
โทรสาร ๐ ๒๕๘๗ ๕๘๘๐
www.itd.kmutnb.ac.th

(นายสมชาย จิรพินิจวงศ์)
รองผู้อำนวยการด้านการแพทย์

เอกสารเปิดประโยชน์ให้คลินิก เรื่องระบบคอม. ที่ใช้ คอมฯ และฝ่าย IT ร่วมวางแผนในการบริหารจัดการ คอม. ได้ (Year plan)

ภาคผนวก ค
หนังสือขอความอนุเคราะห์ผู้เชี่ยวชาญในการตรวจแบบทดสอบ

ที่ อว ๗๑๐๗/๕๒๒

คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กทม. ๑๐๘๐๐

๗ สิงหาคม ๒๕๖๘

เรื่อง ขอความอนุเคราะห์เป็นผู้เชี่ยวชาญในการประเมินคุณภาพเพื่อประกอบการทำการค้นคว้าอิสระ

เรียน นายเจษฎาแจ่มประวิทย์ ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ คลินิก

เนื่องด้วย นายอโนชา คุ้มแพทย์ รหัสประจำตัว ๖๕-๐๗๐๓๑๘-๕๘๒๔-๕ นักศึกษาระดับบัณฑิตศึกษา ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กำลังดำเนินการจัดทำการค้นคว้าอิสระ เรื่อง "การประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ กรณีศึกษาคลินิกเอกชนแห่งหนึ่ง" โดยมี ผู้ช่วยศาตราจารย์ ดร. พงศ์ศรัณย์ บุญโญปกรณ์ เป็นอาจารย์ที่ปรึกษาหลักการค้นคว้าอิสระ ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์จากท่านเพื่อโปรดพิจารณาเอกสาร สำหรับประกอบการทำการค้นคว้าอิสระดังกล่าว

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ จักขอบพระคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ตั้งวรรณวิทย์)
รองคณบดีฝ่ายวิชาการและวิจัย
ปฏิบัติการแทนคณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
โทร. ๐ ๒๕๕๕ ๒๗๑๗
โทรสาร ๐ ๒๕๘๗ ๕๘๘๐
www.itd.kmutnb.ac.th

ที่ อว ๗๑๐๗/๔๒๓

คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กทม. ๑๐๘๐๐

๗ สิงหาคม ๒๕๖๘

เรื่อง ขอความอนุเคราะห์เป็นผู้เชี่ยวชาญในการประเมินคุณภาพเพื่อประกอบการทำการค้นคว้าอิสระ

เรียน นายธนวิทย์ บุญเกิด ผู้อำนวยการฝ่ายระบบคุณภาพและความปลอดภัยอาชีวอนามัย และ ผู้จัดการแผนกเทคโนโลยีสารสนเทศ บริษัท ฟินเทคนิค จำกัด

เนื่องด้วย นายอโนชา คุ้มแพทย์ รหัสประจำตัว ๖๕-๐๗๐๓๑๘-๕๘๒๔-๕ นักศึกษาระดับบัณฑิตศึกษา ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กำลังดำเนินการจัดทำการค้นคว้าอิสระ เรื่อง "การประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ กรณีศึกษาคลินิกเอกชนแห่งหนึ่ง" โดยมี ผู้ช่วยศาตราจารย์ ดร. พงศ์ศรัณย์ บุญโญปกรณ์ เป็นอาจารย์ที่ปรึกษาหลักการค้นคว้าอิสระ ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์จากท่านเพื่อโปรดพิจารณาเอกสาร สำหรับประกอบการทำการค้นคว้าอิสระดังกล่าว

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ จักขอบพระคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ตั้งวรรณวิทย์)
รองคณบดีฝ่ายวิชาการและวิจัย
ปฏิบัติการแทนคณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
โทร. ๐ ๒๕๕๕ ๒๗๑๗
โทรสาร ๐ ๒๕๘๗ ๕๘๘๐
www.itd.kmutnb.ac.th

ที่ อว ๗๑๐๗/๔๒๘

คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
๑๕๑๘ ถนนประชาราษฎร์ ๑ แขวงวงศ์สว่าง
เขตบางซื่อ กทม. ๑๐๘๐๐

๗ สิงหาคม ๒๕๖๘

เรื่อง ขอความอนุเคราะห์เป็นผู้เชี่ยวชาญในการประเมินคุณภาพเพื่อประกอบการทำการค้นคว้าอิสระ

เรียน นางสาววรรณภา สอนจันทร์ นักวิชาการคอมพิวเตอร์ชำนาญการ กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม กรมสนับสนุนบริการสุขภาพ

เนื่องด้วย นายอโนชา คุ้มแพทย์ รหัสประจำตัว ๖๕-๐๗๐๓๑๘-๕๘๒๔-๕ นักศึกษาระดับบัณฑิตศึกษา ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กำลังดำเนินการจัดทำการค้นคว้าอิสระ เรื่อง "การประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ กรณีศึกษาคลินิกเอกชนแห่งหนึ่ง" โดยมี ผู้ช่วยศาตราจารย์ ดร. พงศ์ศรัณย์ บุญโญปกรณ์ เป็นอาจารย์ที่ปรึกษาหลักการค้นคว้าอิสระ ในการนี้ นักศึกษามีความประสงค์ขอความอนุเคราะห์จากท่านเพื่อโปรดพิจารณาเอกสาร สำหรับประกอบการทำการค้นคว้าอิสระดังกล่าว

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ จักขอบพระคุณยิ่ง

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ตั้งวรรณวิทย์)
รองคณบดีฝ่ายวิชาการและวิจัย
ปฏิบัติการแทนคณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

ภาควิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
โทร. ๐ ๒๕๕๕ ๒๗๑๗
โทรสาร ๐ ๒๕๘๗ ๕๘๘๐
www.itd.kmutnb.ac.th

ประวัติผู้เขียน

ชื่อ	นายอโนชา คุ้มแพทย์
ชื่อการค้นคว้าอิสระ	การประเมินความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่ปฏิบัติงานบนระบบคลาวด์ กรณีศึกษาคลินิกเอกชน
สาขาวิชา	การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
ประวัติ	
วัน เดือน ปี เกิด	05 ตุลาคม 2529
ประวัติการศึกษา	
ปริญญาตรี	สาขาเทคโนโลยีสารสนเทศและการสื่อสาร คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยหอการค้าไทย