หลักสูตร
ฝึกอบรมการจัดกิจกรรมการเรียนรู้
ความมั่นคงปลอดภัยไซเบอร์

กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้
กรมส่งเสริมการเรียนรู้
กระทรวงศึกษาธิการ
เอกสารวิชาการ ลำดับที่ 3/2568

READ MORE

CYBER SECURITY
LEARNING ACTIVITIES TRAINING COURSE

หลักสูตร
ฝึกอบรมการจัดกิจกรรมการเรียนรู้ ความมั่นคงปลอดภัยไซเบอร์

กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้

กรมส่งเสริมการเรียนรู้

กระทรวงศึกษาธิการ

เอกสารวิชาการ ลำดับที่ 3/2568

หลักสูตร
ฝึกอบรมการจัดกิจกรรมการเรียนรู้
ความมั่นคงปลอดภัยไซเบอร์

เอกสารวิชาการ ลำดับที่ 3/2568 เผยแพร่ : กันยายน 2568

ที่ปรึกษา :

นายธนากร ดอนเหนือ	อธิบดีกรมส่งเสริมการเรียนรู้
พลอากาศตรี อมร ชมเชย	เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นายชัยพัฒน์ พันธุ์วัฒนสกุล	รองอธิบดีกรมส่งเสริมการเรียนรู้
นางศุทธินี งามเขตต์	อดีตผู้เชี่ยวชาญเฉพาะด้านพัฒนาหลักสูตรการศึกษานอกระบบและการศึกษาตามอัธยาศัย

คณะผู้จัดทำ :

นางสาวเอื้อมพร ศรีภูวงศ์	ผู้อำนวยการกองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้	หัวหน้าคณะทำงาน
นายวรัตม์ ศรีเทพ	นักวิชาการศึกษาชำนาญการ	คณะทำงาน
นางสาวสุจิตตรา เทพเทียน	นักวิชาการศึกษา	คณะทำงาน

กองบรรณาธิการ :

กรมส่งเสริมการเรียนรู้

นางสาวเอื้อมพร ศรีภูวงศ์ นายวรัตม์ ศรีเทพ นางสาวสุพัตรา นันท์แก้ว
นางสาวสุจิตตรา เทพเทียน นางสาวธมลวรรณ วรรณภูงา

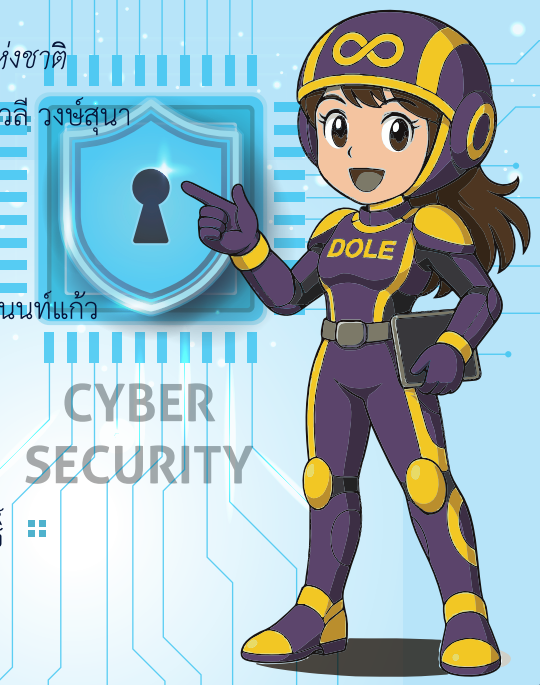
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

พันตรี ปวิช บูรพาชลทิศน์ นายวงศกร นาคนาวา นางสาววัชราวลี วงษ์สุนา
นายจิรายุส ปรีชาเดช พันจ่าอากาศเอกธนรัตน์ วุฒิพรพงษ์

พิสูจน์อักษร :

นางสาวเอื้อมพร ศรีภูวงศ์ นายวรัตม์ ศรีเทพ นางสาวสุพัตรา นันท์แก้ว
นางสาวสุจิตตรา เทพเทียน นางสาวธมลวรรณ วรรณภูงา

ศิลปกรรม ออกแบบปก/รูปเล่ม : นางสาวเอื้อมพร ศรีภูวงศ์



กรมส่งเสริมการเรียนรู้
กระทรวงศึกษาธิการ

คำนำ

กรมส่งเสริมการเรียนรู้ (สกร.) ร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้เล็งเห็นถึงความสำคัญของการเสริมสร้างศักยภาพครู บุคลากรทางการศึกษา และผู้ที่เกี่ยวข้อง ให้มีความรู้ความเข้าใจ และมีทักษะด้านความมั่นคงปลอดภัยไซเบอร์ที่ถูกต้องและทันสมัย อันเป็นรากฐานสำคัญต่อการพัฒนาการเรียนรู้ในยุคดิจิทัลและการสร้างพลเมืองดิจิทัลที่มีคุณภาพ

เอกสารหลักสูตรฝึกอบรมการจัดกิจกรรมการเรียนรู้ความมั่นคงปลอดภัยไซเบอร์ ฉบับนี้ ได้รับความอนุเคราะห์จากผู้ชำนาญการจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มีความเชี่ยวชาญทั้งด้านเนื้อหาและสื่อด้านนี้โดยตรง ผู้เชี่ยวชาญเฉพาะด้านหลักสูตร นักวิชาการ ศึกษานิเทศก์ นักวัดและประเมินผล ตลอดจนผู้ที่เกี่ยวข้อง มาร่วมจัดทำ พิจารณาและตรวจสอบความถูกต้อง เพื่อเป็นแนวทาง ในการพัฒนาศักยภาพครูและบุคลากรทางการศึกษาให้สามารถถ่ายทอดองค์ความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและเหมาะสมกับบริบทของสถานศึกษาและชุมชน โดยมีเนื้อหาครอบคลุมเรื่องพื้นฐานด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์ การป้องกันภัยไซเบอร์ขั้นพื้นฐาน วิถีชีวิตบนโลกดิจิทัล ตลอดจนแนวทางการถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ ทั้งนี้ หลักสูตรได้ออกแบบให้เน้นการปฏิบัติจริง การมีส่วนร่วมและการแลกเปลี่ยนประสบการณ์ เพื่อให้ผู้เข้ารับการอบรมสามารถนำความรู้ไปประยุกต์ใช้ได้อย่างเป็นรูปธรรม เกิดการสร้างภูมิคุ้มกันทางดิจิทัลให้แก่ตนเอง ผู้เรียน และชุมชน ช่วยเสริมสร้างความตระหนักรู้ ทักษะและการมีส่วนร่วมของประชาชนในการใช้ชีวิตบนโลกไซเบอร์อย่างปลอดภัย เป็นการยกระดับคุณภาพการจัดกิจกรรมการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และขยายผลสู่ประชาชนในวงกว้าง

กรมส่งเสริมการเรียนรู้ (สกร.) และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีความมุ่งหวังเป็นอย่างยิ่งว่าหลักสูตรฉบับนี้จะมีส่วนสำคัญในการสนับสนุนการพัฒนาศักยภาพด้านดิจิทัลของครูและบุคลากรทางการศึกษา ตลอดจนส่งเสริมการสร้างสังคมดิจิทัลของประเทศให้มีความมั่นคง ปลอดภัย และยั่งยืนสืบไป

(นายธนากร ดอนเหนือ)
อธิบดีกรมส่งเสริมการเรียนรู้

สารบัญ

คำชี้แจง

เอกสาร หลักสูตรฝึกอบรมการจัดกิจกรรมการเรียนรู้ความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ จัดทำขึ้นเพื่อใช้เป็นแนวทางสำหรับครู บุคลากรทางการศึกษา และผู้เกี่ยวข้อง ในการถ่ายทอดองค์ความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ไปสู่ผู้เรียนและชุมชน โดยมีจุดมุ่งหมายเพื่อพัฒนาศักยภาพและสร้างภูมิคุ้มกันทางดิจิทัลให้แก่ประชาชนทุกกลุ่มวัย เอกสารประกอบด้วยแผนการจัดกิจกรรม เนื้อหาสาระการเรียนรู้ ใบงาน/กิจกรรม และการวัดผล ประเมินผล โดยแบ่งเป็น 4 หน่วยการเรียนรู้ ดังนี้

หน่วยการเรียนรู้ที่ 1 พื้นฐานด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์

หน่วยการเรียนรู้ที่ 2 การป้องกันภัยไซเบอร์ขั้นพื้นฐาน

หน่วยการเรียนรู้ที่ 3 วิถีชีวิตบนโลกดิจิทัล

หน่วยการเรียนรู้ที่ 4 เทคนิคการเผยแพร่และถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ในการนำเอกสารไปใช้ครู บุคลากรทางการศึกษาและผู้ที่เกี่ยวข้อง ควรศึกษารายละเอียดเนื้อหาและการจัดกิจกรรมการเรียนรู้ ให้ชัดเจนเพื่อให้การดำเนินกิจกรรมบรรลุตามวัตถุประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ ให้มีการประเมินผลก่อน และหลังจัดกิจกรรมการเรียนรู้ (Pretest- Posttest) โดยใช้แบบประเมินที่กรมส่งเสริมการเรียนรู้จัดทำขึ้น ระหว่างกิจกรรมการเรียนรู้ควรศึกษาค้นคว้าเพิ่มเติมเพื่อความเข้าใจในเนื้อหาสาระการเรียนรู้ ดำเนินการประเมินผลการเรียนรู้ตามใบงานและกิจกรรมที่กำหนดเพื่อสะท้อนผลการเรียนรู้รายบุคคล รวมถึงการมีส่วนร่วมในการอภิปรายและแลกเปลี่ยนเรียนรู้ เพื่อให้เกิดประสิทธิภาพสูงสุดในการเรียนรู้และสามารถนำความรู้ไปใช้ได้จริง

กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้
กรมส่งเสริมการเรียนรู้

หลักสูตรฝึกอบรมการจัดกิจกรรมการเรียนรู้ความมั่นคงปลอดภัยไซเบอร์

1. ความเป็นมา

ในปัจจุบัน เทคโนโลยีดิจิทัลได้เข้ามามีบทบาทในทุกมิติของการดำรงชีวิตอย่างลึกซึ้งและรวดเร็วครอบคลุมทั้งด้านการศึกษา การทำงาน การเงิน การสื่อสาร หรือการใช้บริการสาธารณะต่าง ๆ ก่อให้เกิดพฤติกรรมการดำรงชีวิตในโลกออนไลน์อย่างแพร่หลายควบคู่กับการเปลี่ยนแปลงของสังคมไทย อย่างไรก็ตาม ความก้าวหน้าดังกล่าวได้นำมาซึ่ง “ความเสี่ยง” และ “ภัยคุกคามทางไซเบอร์” ที่มีแนวโน้มรุนแรงและซับซ้อนมากยิ่งขึ้น ส่งผลกระทบต่อทั้งบุคคล ชุมชน องค์กร และประเทศชาติ อาทิ การโจมตีข้อมูลส่วนบุคคล การหลอกลวงออนไลน์ การปลอมแปลงตัวตน การแพร่กระจายข่าวปลอม และการแทรกแซงระบบสารสนเทศ ซึ่งล้วนแล้วแต่สร้างความเสียหายต่อบุคคล สังคม เศรษฐกิจ และความมั่นคงของประเทศ รัฐบาลจึงกำหนดนโยบายด้านการพัฒนาเศรษฐกิจดิจิทัล ที่มุ่งเน้นการยกระดับทักษะดิจิทัลของประชาชนและการสร้างภูมิคุ้มกันทางไซเบอร์ให้เกิดขึ้นในทุกกลุ่มวัย สอดคล้องกับยุทธศาสตร์ชาติ 20 ปี ที่กำหนดให้ “การเสริมสร้างความมั่นคงปลอดภัยไซเบอร์” และ “การสร้างพลเมืองดิจิทัล” เป็นยุทธศาสตร์หลักในแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 (พ.ศ. 2566 - 2570) ซึ่งเน้นการปรับเปลี่ยนโครงสร้างการเรียนรู้เพื่อให้บุคคลมีสมรรถนะสอดคล้องกับการเปลี่ยนผ่านสู่สังคมเศรษฐกิจดิจิทัล อีกทั้งนโยบายของกระทรวงศึกษาธิการที่ให้ความสำคัญกับ “การพัฒนาครูให้เป็นผู้นำการเปลี่ยนแปลง” และ “การสร้างความปลอดภัยทางเทคโนโลยีให้แก่สถานศึกษาและผู้เรียน” และพระราชบัญญัติส่งเสริมการเรียนรู้ พ.ศ. 2566 โดยเฉพาะ มาตรา 6 (1) (2) ที่ส่งเสริมการเรียนรู้ตลอดชีวิตและการเรียนรู้เพื่อพัฒนาตนเอง และ มาตรา 10 (2) ส่งเสริม สนับสนุน ช่วยเหลือหรือร่วมมือกับภาคีเครือข่ายในการดำเนินการเพื่อจัด ส่งเสริม และสนับสนุนการเรียนรู้

จากบริบทดังกล่าว การส่งเสริม “ความรู้เท่าทันดิจิทัล” และ “ความมั่นคงปลอดภัยไซเบอร์” จึงเป็นวาระสำคัญระดับชาติ ที่ต้องเร่งขับเคลื่อนอย่างเป็นระบบ โดยเฉพาะอย่างยิ่งในภาคการศึกษา ซึ่งครูและบุคลากรทางการศึกษาถือเป็นกลไกสำคัญในการปลูกฝังและถ่ายทอดองค์ความรู้ ทักษะ และจิตสำนึกที่จำเป็นให้แก่ผู้เรียนและประชาชนในทุกช่วงวัย เพื่อสนับสนุนการดำเนินงานตามพันธกิจดังกล่าว กรมส่งเสริมการเรียนรู้ (สกร.) ซึ่งมีภารกิจหลักในการจัด ส่งเสริม และสนับสนุนการเรียนรู้ตลอดชีวิตของประชาชน ได้ร่วมมือกับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานที่ขับเคลื่อนการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ ได้ร่วมกันพัฒนา “หลักสูตรฝึกอบรมการจัดกิจกรรมการเรียนรู้ความมั่นคงปลอดภัยไซเบอร์” ขึ้น เพื่อใช้เป็นแนวทางในการพัฒนาศักยภาพครู และขยายองค์ความรู้สู่ผู้เรียนและชุมชนอย่างต่อเนื่อง อันเป็นกลไกสำคัญในการขับเคลื่อนการเรียนรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ไปสู่พื้นที่ระดับชุมชนผ่านบทบาทของครู สกร. และผู้จัดการเรียนรู้ทั่วประเทศ ซึ่งจะช่วยเสริมสร้างความตระหนักรู้ ทักษะ และการมีส่วนร่วมของประชาชนในการใช้ชีวิตบนโลกไซเบอร์อย่างปลอดภัย มีภูมิคุ้มกัน และเป็นพลเมืองดิจิทัลที่เข้มแข็ง อันจะนำไปสู่การสร้าง “สังคมดิจิทัลที่มั่นคงและยั่งยืน” อย่างแท้จริง

หลักสูตรนี้ได้รับการออกแบบโดยคำนึงถึงความยืดหยุ่นในการนำไปใช้ได้หลากหลายบริบท ไม่ว่าจะเป็นการจัดการเรียนการสอนในชั้นเรียน การอบรมกลุ่มย่อย การจัดกิจกรรมค่าย การประชุมเชิงปฏิบัติการ หรือกิจกรรมพัฒนาคุณภาพผู้เรียน โดยมีเป้าหมายเพื่อเสริมสร้างความรู้ ความเข้าใจ ทักษะ และจิตสำนึกในการใช้เทคโนโลยีดิจิทัลอย่างปลอดภัยและมีความรับผิดชอบ อันจะนำไปสู่การสร้างสังคมดิจิทัลที่มั่นคง ปลอดภัย และยั่งยืนในระยะยาว

2. จุดมุ่งหมาย

1. เพื่อเสริมสร้างความรู้ ความเข้าใจ ด้านความมั่นคงปลอดภัยไซเบอร์
2. เพื่อเสริมสร้างทักษะและนำความรู้ไปปฏิบัติอย่างปลอดภัยจากภัยไซเบอร์
3. เพื่อสร้างความตระหนักรู้และจิตสำนึก ในการใช้เทคโนโลยีดิจิทัลอย่างปลอดภัยและมีความรับผิดชอบ
4. เพื่อถ่ายทอดองค์ความรู้ เผยแพร่ความรู้ รวมทั้งสร้างเครือข่ายการเรียนรู้ ด้านความมั่นคงปลอดภัยไซเบอร์

3. กลุ่มเป้าหมาย

ครู บุคลากรทางการศึกษา และผู้ที่เกี่ยวข้อง

4. ระยะเวลาการอบรม

3 วัน

5. โครงสร้างหลักสูตร

ที่	เรื่อง	จุดประสงค์การเรียนรู้	เนื้อหา	การจัดกระบวนการเรียนรู้	จำนวน	
					ทฤษฎี	ปฏิบัติ
หน่วยการเรียนรู้ที่ 1 พื้นฐานด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์						
1.1	ความรู้พื้นฐานเกี่ยวกับไซเบอร์	เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบายความหมาย และสถานการณ์ของภัยไซเบอร์ได้	ความรู้พื้นฐานเกี่ยวกับไซเบอร์ 1. ความหมายของไซเบอร์ 2. สถานการณ์ของภัยไซเบอร์	• การบรรยาย (Lecture) • การระดมสมอง (Brainstorming) • การประชุมกลุ่มย่อย (Buzz session)	20 นาที	10 นาที
1.2	หลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบายหลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้	หลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 1. Confidentiality (ความลับ) 2. Integrity (ความถูกต้องสมบูรณ์) 3. Availability (ความพร้อมใช้งาน)	• การบรรยาย (Lecture)	20 นาที	10 นาที
1.3	ประเภทภัยคุกคามทางไซเบอร์	เพื่อให้ผู้เข้ารับการอบรมสามารถจำแนกประเภทภัยคุกคามทางไซเบอร์ได้	ประเภทภัยคุกคามทางไซเบอร์ 1. มัลแวร์ (Malware) 2. การโจมตีด้วยการปฏิเสธให้บริการ (DoS/DDoS Attack) 3. ฟิชชิง (Phishing) 4. การโจมตีด้วยการแทรกกลาง (Man-in-the-Middle)	• การบรรยาย (Lecture) • การระดมสมอง (Brainstorming) • การประชุมกลุ่มย่อย (Buzz session)	30 นาที	30 นาที

ที่	เรื่อง	จุดประสงค์การเรียนรู้	เนื้อหา	การจัดกระบวนการเรียนรู้	จำนวน	
					ทฤษฎี	ปฏิบัติ
หน่วยการเรียนรู้ที่ 1 พื้นฐานด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์ (ต่อ)						
1.4	เทคนิคการใช้งานเทคโนโลยีดิจิทัลอย่างปลอดภัย	เพื่อให้ผู้เข้ารับการอบรมสามารถตั้งค่าความปลอดภัยในการใช้งานเทคโนโลยีดิจิทัลได้	เทคนิคการใช้งานเทคโนโลยีดิจิทัลอย่างปลอดภัย 1. การตั้งค่ารหัสผ่าน 2. การยืนยันตัวตน 2 ขั้นตอน (Two-Factor Authentication: 2FA)	• การบรรยาย (Lecture) • การสาธิต (Demonstration) • การฝึกปฏิบัติ (Practice)	30 นาที	30 นาที
หน่วยการเรียนรู้ที่ 2 การป้องกันภัยไซเบอร์ขั้นพื้นฐาน						
2.1	รู้เท่าทันภัยออนไลน์ในชีวิตประจำวัน	เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบาย ความหมาย ประเภทของฟิชชิง (Phishing) ได้ 2. เพื่อให้ผู้เข้ารับการอบรมมีทักษะป้องกันตนเองจากการโจมตีแบบฟิชชิง (Phishing) ได้ 3. เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบาย ความหมาย ลักษณะ และวิธีป้องกันตนเองจากการใช้เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI I) ได้	รู้เท่าทันภัยออนไลน์ในชีวิตประจำวัน 1. รู้ทันกลลวงก่อนตกเป็นเหยื่อฟิชชิง (Phishing) 1.1 ความหมาย และประเภทของฟิชชิง (Phishing) 1.2 วิธีป้องกันตนเองจากการโจมตีแบบฟิชชิง (Phishing) 2. เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) กับภัยคุกคามทางไซเบอร์ 2.1 ความหมาย ลักษณะ ของเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) 2.2 การใช้เทคโนโลยีปัญญาประดิษฐ์ในทางที่ผิดและวิธีป้องกันตนเอง	• การบรรยาย (Lecture) • วิธีการสอนแบบอภิปราย (Discussion Method) • การระดมสมอง (Brainstorming)	40 นาที	30 นาที

ที่	เรื่อง	จุดประสงค์การเรียนรู้	เนื้อหา	การจัดกระบวนการเรียนรู้	จำนวน	
					ทฤษฎี	ปฏิบัติ
หน่วยการเรียนรู้ที่ 2 การป้องกันภัยไซเบอร์ขั้นพื้นฐาน (ต่อ)						
2.2	ร่องรอยดิจิทัล (Digital Footprint)	1. เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบาย ความหมาย และประเภทของร่องรอยดิจิทัลได้ 2. เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบาย วิธีการหลีกเลี่ยงการทิ้งร่องรอยดิจิทัลที่ไม่พึงประสงค์ได้ 3. เพื่อให้ผู้เข้ารับการอบรมสามารถวิเคราะห์ข้อดีและข้อเสียของร่องรอยดิจิทัลได้	ร่องรอยดิจิทัล (Digital Footprint) 1. ความหมายและประเภทของร่องรอยดิจิทัล 2. วิธีการหลีกเลี่ยงการทิ้งร่องรอยดิจิทัล 3. ข้อดีและข้อเสียของร่องรอยดิจิทัล	• การบรรยาย (Lecture) • การระดมสมอง (Brainstorming) • กรณีศึกษา (Case Study) • วิธีการสอนแบบอภิปราย (Discussion Method)	30 นาที	15 นาที
2.3	เทคนิคกลลวงบนโลกไซเบอร์	1. เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบาย เกี่ยวกับเทคนิค กลยุทธ์ ของภัยคุกคามทางไซเบอร์ได้ 2. เพื่อให้ผู้เข้ารับการอบรมสามารถวิเคราะห์ข้อมูลกลลวงบนโลกไซเบอร์ได้ 3. เพื่อให้ผู้เข้ารับการอบรมสามารถรับมือและป้องกันตนเองจากภัยไซเบอร์ได้	เทคนิคกลลวงบนโลกไซเบอร์ 1. เทคนิค กลยุทธ์ ของภัยคุกคามทางไซเบอร์ 2. วิธีการรับมือและป้องกันภัยไซเบอร์ 2.1 หลักการป้องกันพื้นฐาน “ไม่กด ไม่โหลด ไม่ให้ ไม่โอน” 2.2 การตรวจสอบและตั้งสติ	• การบรรยาย (Lecture) • กรณีศึกษา (Case Study) • วิธีการสอนแบบอภิปราย (Discussion Method)	40 นาที	40 นาที

ที่	เรื่อง	จุดประสงค์การเรียนรู้	เนื้อหา	การจัดกระบวนการเรียนรู้	จำนวน	
					ทฤษฎี	ปฏิบัติ
หน่วยการเรียนรู้ที่ 2 การป้องกันภัยไซเบอร์ขั้นพื้นฐาน (ต่อ)						
2.4	ช่องทางการตรวจ-สอบมิจฉาชีพออนไลน์และการแจ้งเหตุ	เพื่อให้ผู้เข้ารับการอบรมสามารถใช้เทคนิคและวิธีการตรวจสอบข้อมูลผู้ติดต่อ และร้านค้าออนไลน์เบื้องต้นได้อย่างปลอดภัย	ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ 1. เทคนิค และวิธีการตรวจสอบข้อมูลผู้ติดต่อทางออนไลน์เบื้องต้น 2. การตรวจสอบร้านค้าอย่างปลอดภัย 3. แนวทางการปฏิบัติเมื่อสงสัยว่าตกเป็นเหยื่อ	• การบรรยาย (Lecture) • วิธีการสอนแบบอภิปราย (Discussion Method)	30 นาที	15 นาที
หน่วยการเรียนรู้ที่ 3 วิถีชีวิตบนโลกดิจิทัล						
3.1	การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)	1. เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบาย ความหมาย ความสำคัญ บอกวิธีการของการเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy) และการมีมารยาทและจริยธรรมบนโลกดิจิทัลได้ 2. เพื่อให้ผู้เข้ารับการอบรมสามารถปฏิบัติตนตามวิธีการเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy) มีมารยาทและจริยธรรมบนโลกดิจิทัลได้อย่างเหมาะสม	การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy) 1. ความหมายและความสำคัญของการเอาใจเขามาใส่ใจเราทางดิจิทัล 2. วิธีการเอาใจเขามาใส่ใจเราทางดิจิทัล 3. มารยาทและจริยธรรมบนโลกดิจิทัล 4. การกลั่นแกล้งบนโลกออนไลน์	• การบรรยาย (Lecture) • วิธีการสอนแบบอภิปราย (Discussion Method) • การฝึกปฏิบัติ (Practice) • กรณีศึกษา (Case Study)	30 นาที	60 นาที

ที่	เรื่อง	จุดประสงค์การเรียนรู้	เนื้อหา	การจัดกระบวนการเรียนรู้	จำนวน	
					ทฤษฎี	ปฏิบัติ
หน่วยการเรียนรู้ที่ 3 วิถีชีวิตบนโลกดิจิทัล (ต่อ)						
3.1 (ต่อ)	การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)	3. เพื่อให้ผู้เข้ารับการอบรมเกิดความตระหนักรู้ถึงปัญหา เห็นใจผู้ตกเป็นเหยื่อการกลั่นแกล้งบนโลกไซเบอร์ และเกิดจิตสำนึกใช้สื่อดิจิทัลอย่างรับผิดชอบ				
3.2	กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล	1. เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบายกฎหมายระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัลที่พบบ่อยและบทลงโทษตามกฎหมาย 2. เพื่อให้ผู้เข้ารับการอบรมสามารถปฏิบัติตนตามกฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัลได้อย่างเหมาะสม 3. เพื่อให้ผู้เข้ารับการอบรมเกิดความตระหนักรู้ถึง สิทธิ หน้าที่ การปฏิบัติตนตามกฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล	กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล 1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 3. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 3.1 ความเป็นส่วนตัวบนโลกออนไลน์ 3.2 ข้อมูลส่วนบุคคล (Personal data) 4. พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568	• การบรรยาย (Lecture) • การฝึกปฏิบัติ (Practice) • วิธีการสอนแบบอภิปราย (Discussion Method)	30 นาที	60 นาที

ที่	เรื่อง	จุดประสงค์การเรียนรู้	เนื้อหา	การจัดกระบวนการเรียนรู้	จำนวน	
					ทฤษฎี	ปฏิบัติ
หน่วยการเรียนรู้ที่ 4 การถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยไซเบอร์						
4.1	การถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยไซเบอร์	เพื่อให้ผู้เข้ารับการอบรมฝึกปฏิบัติการให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์	การฝึกปฏิบัติ/สาธิตการให้ความรู้ เรื่อง พื้นฐานด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์ การป้องกันภัยไซเบอร์ขั้นพื้นฐาน และวิถีชีวิตบนโลกดิจิทัล	• การสาธิต (Demonstration)	-	6
				รวมเวลาการอบรม	**5 ชั่วโมง**	**11 ชั่วโมง**

6. สื่อการเรียนรู้

6.1 ชุดบรรยายของวิทยากร
6.2 ใบความรู้
6.3 สื่อวีดิทัศน์

7. การวัดและประเมินผล

7.1 ทดสอบก่อนเรียน - หลังเรียน
7.2 สังเกต ประเมินการปฏิบัติ และการโต้ตอบระหว่างการเรียน

8. เกณฑ์การจบหลักสูตร

มีระยะเวลาเข้าร่วมกิจกรรมการอบรมไม่น้อยกว่าร้อยละ 80 ของเวลาในการอบรมทั้งหมด

บรรณานุกรม

กรมตำรวจ. (2566). “อินโฟกราฟิก: ศูนย์ AOC 1441 สายด่วนภัยออนไลน์ พร้อมช่วยเหลือตลอด 24 ชั่วโมง โทรทันที เมื่อได้รับความเดือดร้อนจากมิจฉาชีพออนไลน์”. สืบค้นจาก https://www.facebook.com/share/p/17NqoTDdyC/?mibextid=wwXIfr

ผู้จัดการออนไลน์. (2562). “คำล้อเลียนฆ่าคนได้ ‘รัศมี แข’ แชร์ประสบการณ์โดนบูลลี่ ‘ผิวดำ ตัวใหญ่’”. สืบค้นจาก https://mgronline.com/live/detail/9620000104735

ผู้จัดการออนไลน์. (2564, 11 มีนาคม). “หมอแล็บเตือนภัย! หากได้รับข้อความ ‘ได้รับเงินกู้’ อย่ากดอ่านเด็ดขาด”. สืบค้นจาก https://mgronline.com/onlinesection/detail/9640000023607

ผู้จัดการออนไลน์. (2568). “แม่ค้าทุเรียนแจ้งจับ ‘คุณเจมส์’ ลวงส่งภาพลับก่อนข่มขู่เรียกเงิน 5 หมื่น”. สืบค้นจาก https://mgronline.com/crime/detail/9680000062233

ภาพประกอบจาก Freepik Premium. (2568). สืบค้นจาก https://www.freepik.com

มติชนออนไลน์. (2561). “‘บอล หนองขาว’ สำนึกผิด ไลฟ์สดด่าตร. หอบกระเช้าขอโทษ แต่ไม่พ้นโดนไป 2 ข้อหา”. สืบค้นจาก https://www.matichon.co.th/region/news_939275

มติชนออนไลน์. (2564). “ยิปซี-ยิปโซ เปิดใจ สิ่งที่ต้องทนทุกข์นับ 10 ปี จากการถูกเปรียบเทียบจนไม่สนิทใจกัน”. สืบค้นจาก https://www.matichon.co.th/entertainment/news_2711423

สรานนท์ อินทนนท์. (2563). “ทักษะการเอาใจเขามาใส่ใจเราทางดิจิทัล Digital Empathy”. สืบค้นจาก https://cclickthailand.com/fact-sheet-ทักษะการเอาใจเขามาใส่ใจเราทางดิจิทัล

สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2567). “เนื้อหาบทเรียน: หลักสูตรพื้นฐานความมั่นคงปลอดภัยไซเบอร์สำหรับเยาวชนไทย”. สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ.

อมรินทร์ทีวี. (2566, 7 มิถุนายน). “สาวร้องถูกหลอกลงทุน ‘หุ้นจีน’ สูญเงินกว่า 2 ล้าน พบเหยื่ออีกเพียบ”. สืบค้นจาก https://www.amarintv.com/news/crime/506676

Blockdit. (2565, 5 ตุลาคม). “CIA Triad หลักการพื้นฐานด้าน Security ที่ควรต้องรู้”. สืบค้นจาก https://www.blockdit.com/posts/633d4f511c659636156d4dda

DAILYNEWS ONLINE. (2568). “มุก” โดนบูลลี่จากโซเชียลเป็นโรควิตกกังวลเฉียบพลัน เครียดถึงขั้นพบจิตแพทย์. สืบค้นจาก https://www.dailynews.co.th/news/1425884/

EFM Station. (2566). “พลอยชมพู ยอมรับว่าคอมเมนต์คุกคามทางเพศ ทำให้เธอกลัวและไม่อยากแชร์ภาพส่วนตัวบนโซเชียล”. สืบค้นจากhttps://www.facebook.com/efmstation/posts/pfbid02dhswYqBAoxSgzRMJahn8F3DnvSTg2KqTfT6mCb79XCNx9opCBuPPtiRUmAHo2ARHl

Facebook. (2565, 9 ตุลาคม). [ภาพถ่ายเกี่ยวกับภัยออนไลน์]. สืบค้นจาก https://www.facebook.com/photo.php?fbid=481186564420200

KTC. (2565, 21 พฤศจิกายน). “Phishing คืออะไร? วิธีสังเกตและป้องกันภัยไซเบอร์ที่มนุษย์เงินเดือนต้องรู้”. สืบค้นจาก https://www.ktc.co.th/en/article/knowledge/salary-man/phishing

LINE TODAY. (2568). “ทำไม! หลอกซื้อขายออนไลน์ ครองแชมป์แจ้งความออนไลน์มากที่สุด | ชัวร์ก่อนแชร์ in FOCUS”. สืบค้นจาก https://today.line.me/th/v3/article/oq7O6Jp

Pantip.com. (2565, 11 กุมภาพันธ์). “โดนเขาแล้ว email คาดว่ามีปลอมมาจากpostalcare@thailandpost.co.th ไปหายังคุ้กกี้หรืออีเมลส่วนตัวตัวเอง”. สืบค้นจาก https://pantip.com/topic/40510595

Spring News. (2565, 5 ตุลาคม). “ตัวอย่างรหัสผ่านที่ไม่ควรใช้! ‘123456’ ยังติดอันดับโลก แม้รู้ว่าเสี่ยง”. สืบค้นจาก https://www.springnews.co.th/digital-tech/846234

Thai PBS. (2565, 9 ตุลาคม). “รู้ทันกลโกงออนไลน์ : ตัวอย่างข้อความหลอกลวงที่ควรระวัง” [วิดีโอ]. YouTube. สืบค้นจาก https://www.youtube.com/watch?v=ffCL1HsVDb8

Thai PBS. (2565, 9 ตุลาคม). “รู้ทันกลโกงออนไลน์ : วิธีหลอกลวงผ่านข้อความ SMS และลิงก์ปลอม” [วิดีโอ]. YouTube. สืบค้นจาก https://www.youtube.com/watch?v=13YLRAd69mU

Thai PBS. (2568, 18 เมษายน). “แก๊งคอลเซ็นเตอร์อ้าง บ.ขนส่งพัสดุ ส่ง SMS หลอกโอนเงิน 4.5 แสนบาท”. สืบค้นจาก https://www.thaipbs.or.th/news/content/352261

ภาคผนวก

เอกสารประกอบการอบรมตามหลักสูตรฝึกอบรม
การจัดกิจกรรมการเรียนรู้ความมั่นคงปลอดภัยไซเบอร์

ภาคผนวก ก

เอกสารประกอบการอบรมตามหลักสูตรฝึกอบรมการจัดกิจกรรมการเรียนรู้ความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วยแผนการจัดกิจกรรม ของหน่วยการเรียนรู้ 4 หน่วย ดังนี้

หน่วยการเรียนรู้ที่ 1 พื้นฐานด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์

แผนการจัดกิจกรรม

1.1 เรื่อง ความรู้พื้นฐานเกี่ยวกับไซเบอร์

1.2 เรื่อง หลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1.3 เรื่อง ประเภทภัยคุกคามทางไซเบอร์

1.4 เรื่อง เทคนิคการใช้งานเทคโนโลยีดิจิทัลอย่างปลอดภัย

หน่วยการเรียนรู้ที่ 2 การป้องกันภัยไซเบอร์ขั้นพื้นฐาน

แผนการจัดกิจกรรม

2.1 เรื่อง รู้เท่าทันภัยออนไลน์ในชีวิตประจำวัน

2.2 เรื่อง ร่องรอยดิจิทัล (Digital Footprint)

2.3 เรื่อง เทคนิคกลลวงบนโลกไซเบอร์

2.4 เรื่อง ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ

หน่วยการเรียนรู้ที่ 3 วิถีชีวิตบนโลกดิจิทัล

แผนการจัดกิจกรรม

3.1 เรื่อง การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)

3.2 เรื่อง กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล

หน่วยการเรียนรู้ที่ 4 การถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

แผนการจัดกิจกรรม

4.1 เรื่อง การถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

หน่วยการเรียนรู้ที่ 1 พื้นฐานด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์
แผนการจัดกิจกรรม 1.1 เรื่อง ความรู้พื้นฐานเกี่ยวกับไซเบอร์

ระยะเวลา 30 นาที

สาระสำคัญ

โลกไซเบอร์คือสภาพแวดล้อมดิจิทัลที่เชื่อมโยงผู้คน เทคโนโลยี และเครือข่ายเข้าด้วยกัน มีทั้งประโยชน์มหาศาลและความเสี่ยงที่ต้องระมัดระวัง ดังนั้น การมีความรู้พื้นฐานด้านไซเบอร์ จะช่วยให้ผู้เข้ารับการอบรมใช้งานเทคโนโลยีอย่างปลอดภัย มีจริยธรรม และพร้อมรับมือกับภัยคุกคามในยุคดิจิทัล

จุดประสงค์

เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบายความหมาย และสถานการณ์ของภัยไซเบอร์ได้

ขอบข่ายเนื้อหา

1. ความหมายของไซเบอร์
2. สถานการณ์ของภัยไซเบอร์

สื่อการเรียนรู้

1. ใบความรู้ที่ 1.1 เรื่อง ความรู้พื้นฐานเกี่ยวกับไซเบอร์
2. คลิปวิดีโอ เรื่อง ความสำคัญของ Cybersecurity

วัสดุอุปกรณ์

1. เครื่องคอมพิวเตอร์/โน้ตบุ๊ค/แท็บเล็ต/โทรศัพท์มือถือ เชื่อมต่ออินเทอร์เน็ต
2. กระดาษปรู๊ฟ
3. ปากกาเคมี

ขั้นตอนการจัดกิจกรรม

1. วิทยากรให้ผู้เข้ารับการอบรมรับชมคลิปวิดีโอ เรื่อง ความสำคัญของ Cybersecurity

2. วิทยากรให้ผู้เข้ารับการอบรมสะท้อนความรู้สึกและความตระหนักจากการรับชมคลิปวิดีโอในประเด็น “ภัยไซเบอร์ใกล้ตัวเรามากแค่ไหน” พร้อมแสดงความคิดเห็น ตามประสบการณ์และความคิดส่วนบุคคล
3. วิทยากรให้ผู้เข้ารับการอบรมศึกษาใบความรู้ที่ 1.1 เรื่อง ความรู้พื้นฐานเกี่ยวกับไซเบอร์
4. วิทยากรมอบหมายให้ผู้เข้ารับการอบรมทำใบงานที่ 1.1.1 เรื่อง ความหมายของไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์
5. แบ่งกลุ่มผู้เข้ารับการอบรมตามความเหมาะสม และมอบหมายให้ทำใบงานที่ 1.1.2 เรื่อง สถานการณ์ภัยไซเบอร์ทั้ง 6 สถานการณ์ โดยให้ร่วมกันระดมความคิดเห็นและวิเคราะห์สถานการณ์จากคำถาม ดังนี้
   1) พฤติกรรมเสี่ยง ในสถานการณ์นี้ คืออะไร
   2) เราจะป้องกันพฤติกรรมเสี่ยง ได้อย่างไร
   3) หากเหตุเกิดขึ้นกับเรา จะต้องทำอย่างไรต่อไป

   และให้ตัวแทนกลุ่มนำเสนอผลการวิเคราะห์และแนวทางปฏิบัติเกี่ยวกับรับมือสถานการณ์ภัยไซเบอร์
6. วิทยากรและผู้เข้ารับการอบรมสรุปองค์ความรู้ร่วมกัน

การวัดและประเมินผล

1. ใบงาน / ชิ้นงาน / ผลงาน
2. การสังเกต

ใบความรู้ที่ 1.1
เรื่อง ความรู้พื้นฐานเกี่ยวกับไซเบอร์

ปัจจุบันเทคโนโลยีดิจิทัลกลายเป็นส่วนหนึ่งของชีวิตประจำวัน ทั้งการเรียนและการทำงาน ความเสี่ยงจากภัยคุกคามทางไซเบอร์ก็เพิ่มสูงขึ้นตามไปด้วย ไม่ว่าจะเป็น การโจมตีด้วยไวรัสหรือมัลแวร์การหลอกลวงทางออนไลน์ ไปจนถึงการขโมยข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กร สถานการณ์เหล่านี้ไม่ได้เกิดขึ้นเพียงกับหน่วยงานขนาดใหญ่เท่านั้น หากแต่ยังสามารถเกิดได้กับพวกเราทุกคน ดังนั้น เราจึงมีความจำเป็นที่จะต้องเรียนรู้เกี่ยวกับความรู้พื้นฐานเกี่ยวกับไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

ความหมายของไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้ให้คำนิยาม ดังนี้

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“ไซเบอร์” หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

สถานการณ์ของภัยไซเบอร์

ข้อมูลจากสถิติการแจ้งความออนไลน์ในประเทศไทย เมื่อเดือนกรกฎาคม 2568 พบว่า ประชาชนถูกหลอกลวงซื้อขายสินค้าหรือบริการแบบไม่เป็นขบวนการ มีมากเป็นอันดับที่ 1 ภายใต้ความสูญเสียกว่า 150,000,000 บาท นอกจากนี้ยังมีภัยออนไลน์อีกหลายประเภทที่สร้างความสูญเสียต่อประชาชน ซึ่งมีภาพรวมย้อนหลังดังนี้

ที่มา : https://today.line.me/th/v3/article/oq7O6Jp

ใบความรู้ที่ 1.1 (ต่อ)
เรื่อง ความรู้พื้นฐานเกี่ยวกับไซเบอร์

จากภาพ พบว่าจำนวนคดีออนไลน์และความเสียหายที่เกิดขึ้นตั้งแต่วันที่ 1 มีนาคม 2565 ถึงวันที่ 31 กรกฎาคม 2568 สามารถจำแนกโดยเรียงตามความเสียหาย ดังนี้

ที่	ประเภทคดีออนไลน์	จำนวนคดี	ความเสียหาย (บาท)
1	หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์	69,677	31,366,766,461
2	หลอกให้โอนเงินเพื่อทำงาน	120,394	13,954,841,926
3	ข่มขู่ทางโทรศัพท์	63,085	11,018,992,114

ความสูญเสียเหล่านี้ไม่เพียงส่งผลต่อด้านทรัพย์สิน แต่ยังส่งผลต่อความเชื่อมั่นและความปลอดภัยในการใช้เทคโนโลยีอีกด้วย การเข้าใจพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์จึงไม่ใช่ทางเลือกอีกต่อไป แต่เป็นทักษะจำเป็นที่ครูควรมี เพื่อนำไปสร้างภูมิคุ้มกันดิจิทัลให้กับผู้เรียนและชุมชนได้อย่างมั่นใจ

ใบงานที่ 1.1.1
เรื่อง ความหมายของไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์

คำชี้แจง ให้ผู้เข้ารับการอบรมตอบคำถามความรู้พื้นฐานเกี่ยวกับไซเบอร์ ตามความเข้าใจพอสังเขป

1. **อธิบายความหมายของไซเบอร์**

2. **อธิบายความหมายของการรักษาความมั่นคงปลอดภัยไซเบอร์**

3. **บอกเหตุผล “ทำไมถึงรักษาความมั่นคงปลอดภัยไซเบอร์”**

ใบงานที่ 1.1.2
เรื่อง สถานการณ์ภัยไซเบอร์ (1)
“เงินกู้ เงินกลุ้ม”

ที่มา : https://mgronline.com/onlinesection/detail/9640000023607

คำอธิบายสถานการณ์

ป้าน้อยกำลังเดือดร้อนเรื่องเงิน วันหนึ่งได้รับข้อความทางโทรศัพท์แจ้งว่าตนเองได้รับสิทธิ์ให้กู้เงิน 200,000 บาท โดยไม่ต้องส่งเอกสารอะไรเลย ป้าน้อยดีใจจึงกดลิงก์ดังกล่าวทันที หลังจากนั้นไม่นานเงินในบัญชีธนาคารก็หายเกลี้ยงไปจนหมด

วิเคราะห์สถานการณ์จากคำถาม

1. อะไร คือ พฤติกรรมเสี่ยง ?
2. เราจะป้องกันได้อย่างไร ?
3. ถ้าเหตุเกิดขึ้นกับเรา จะต้องทำอย่างไรต่อไป ?

ใบงานที่ 1.1.2
เรื่อง สถานการณ์ภัยไซเบอร์ (2)
“รหัส (ไม่) ลับ”

ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

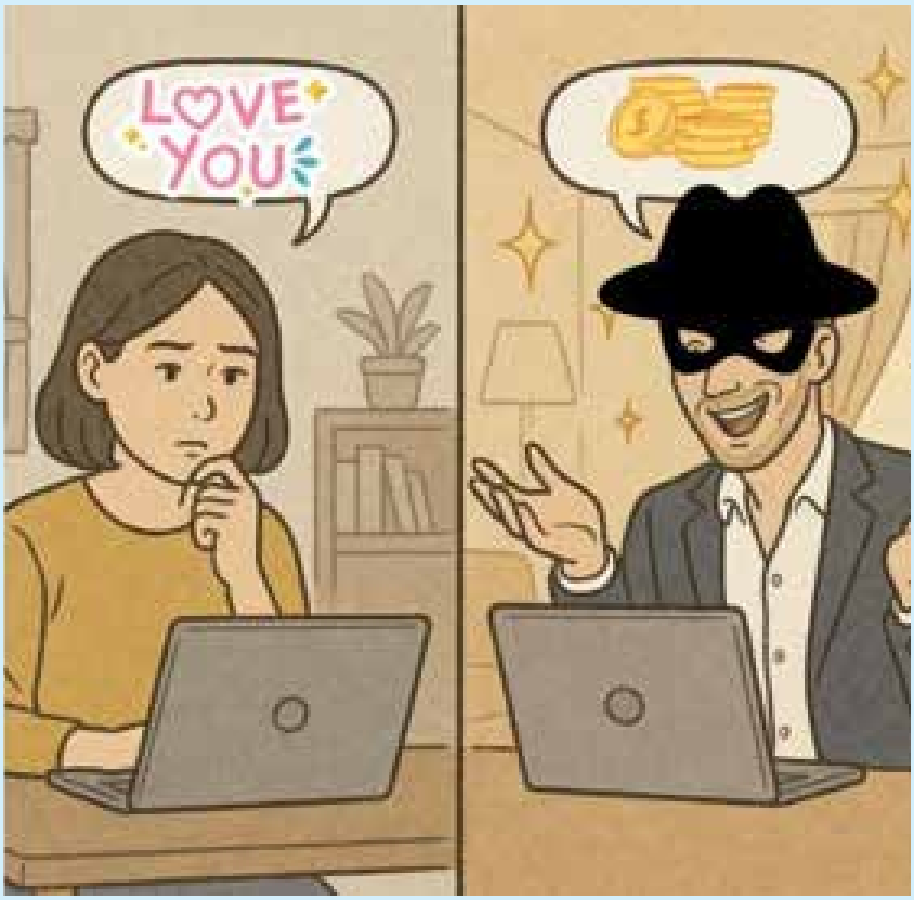
คำอธิบายสถานการณ์

นายธงชัย ตั้งรหัสเฟซบุ๊กว่า “12345678” จนวันหนึ่งพบว่าตนเองไม่สามารถเข้าเฟซบุ๊กได้ และเฟซบุ๊กของตนเองถูกบุคคลอื่นปลอมเป็นตนเองไปยืมเงินคนรู้จัก ซ้ำร้ายยังมีคนหลงเชื่อโอนเงินให้หลายรายอีกด้วย

วิเคราะห์สถานการณ์จากคำถาม

1. อะไร คือ พฤติกรรมเสี่ยง ?
2. เราจะป้องกันได้อย่างไร ?
3. ถ้าเหตุเกิดขึ้นกับเรา จะต้องทำอย่างไรต่อไป ?

ใบงานที่ 1.1.2
เรื่อง สถานการณ์ภัยไซเบอร์ (3)
“ลัก ลวง”



ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

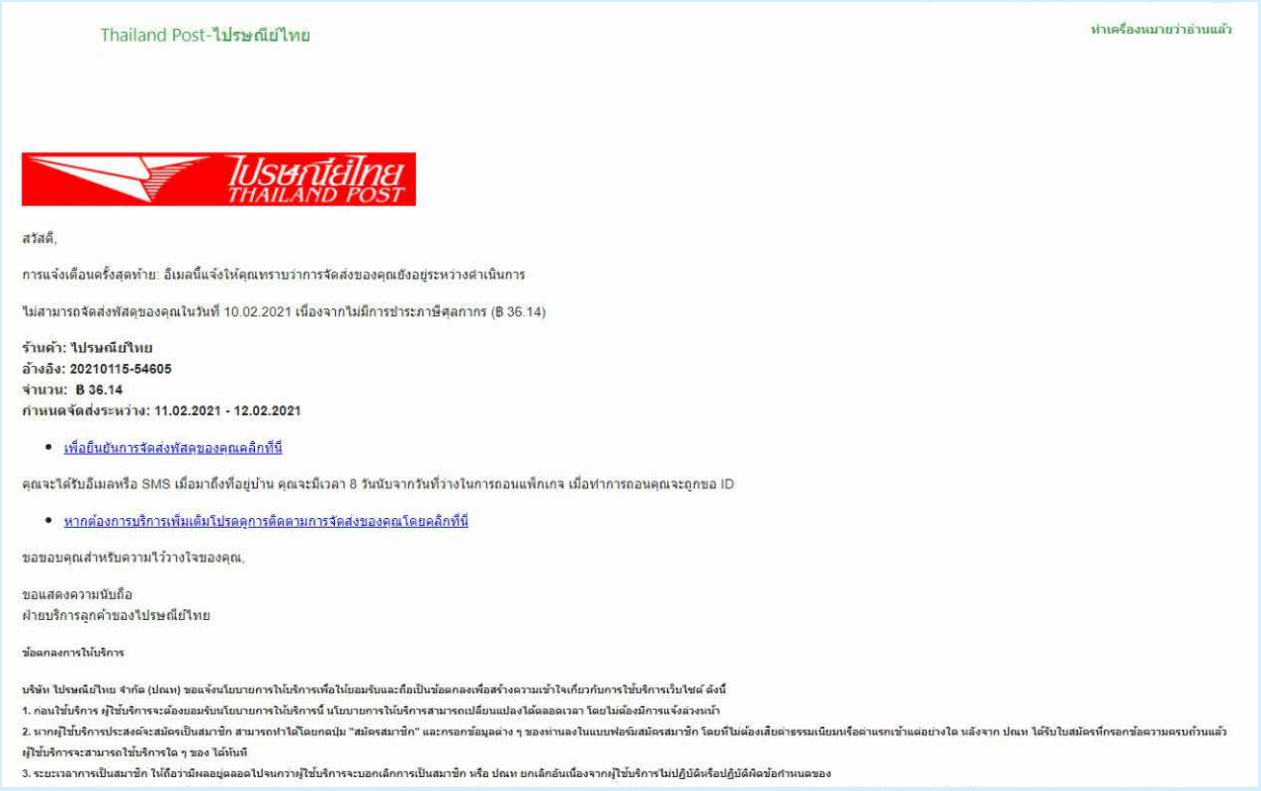
คำอธิบายสถานการณ์

สมใจรู้จักกับเดวิดผ่านทางแอปพลิเคชันหาคู่ออนไลน์ สมใจคุยกับเดวิดมาได้ประมาณหนึ่งสัปดาห์ เดวิดบอกว่ารักมาก อยากบินมาหาที่ประเทศไทย และจะแต่งงานด้วย สมใจจึงตัดสินใจโอนเงินให้เดวิดให้เป็นค่าใช้จ่าย เมื่อเดวิดได้รับเงินแล้ว สมใจก็ไม่สามารถติดต่อเดวิดได้อีกเลย

วิเคราะห์สถานการณ์จากคำถาม

1. อะไร คือ พฤติกรรมเสี่ยง ?
2. เราจะป้องกันได้อย่างไร ?
3. ถ้าเหตุเกิดขึ้นกับเรา จะต้องทำอย่างไรต่อไป ?

ใบงานที่ 1.1.2
เรื่อง สถานการณ์ภัยไซเบอร์ (4)
“ส่งด่วนจากต่างแดน”



Thailand Post-ไปรษณีย์ไทย

ทำเครื่องหมายว่าอ่านแล้ว

ไปรษณีย์ไทย THAILAND POST

สวัสดี,

การแจ้งเตือนครั้งสุดท้าย: อีเมลนี้แจ้งให้คุณทราบว่าการจัดส่งของคุณยังอยู่ระหว่างดำเนินการ

ไม่สามารถจัดส่งพัสดุของคุณในวันที่ 10.02.2021 เนื่องจากไม่มีการชำระภาษีศุลกากร (B 36.14)

ร้านค้า: ไปรษณีย์ไทย
อ้างอิง: 20210115-54605
จำนวน: B 36.14
กำหนดจัดส่งระหว่าง: 11.02.2021 - 12.02.2021

- เพื่อยืนยันการจัดส่งพัสดุของคุณคลิกที่นี่

คุณจะได้รับอีเมลหรือ SMS เมื่อมาถึงที่อยู่บ้าน คุณจะมีเวลา 8 วันนับจากวันที่ว่างในการถอนแพ็กเกจ เมื่อทำการถอนคุณจะถูกขอ ID

- หากต้องการบริการเพิ่มเติมโปรดดูการติดตามการจัดส่งของคุณโดยคลิกที่นี่

ขอขอบคุณสำหรับความไว้วางใจของคุณ,

ขอแสดงความนับถือ
ฝ่ายบริการลูกค้าของไปรษณีย์ไทย

ข้อตกลงการให้บริการ

บริษัท ไปรษณีย์ไทย จำกัด (ปณท) ขอแจ้งนโยบายการให้บริการเพื่อให้ยอมรับและถือเป็นข้อตกลงเพื่อสร้างความเข้าใจเกี่ยวกับการใช้บริการเว็บไซต์ ดังนี้
1. ก่อนใช้บริการ ผู้ใช้บริการจะต้องยอมรับนโยบายการให้บริการนี้ นโยบายการให้บริการสามารถเปลี่ยนแปลงได้ตลอดเวลา โดยไม่ต้องมีการแจ้งล่วงหน้า
2. หากผู้ใช้บริการประสงค์จะสมัครเป็นสมาชิก สามารถทำได้โดยกดปุ่ม "สมัครสมาชิก" และกรอกข้อมูลต่าง ๆ ของท่านลงในแบบฟอร์มสมัครสมาชิก โดยที่ไม่ต้องเสียค่าธรรมเนียมแรกเข้าแต่อย่างใด หลังจาก ปณท ได้รับใบสมัครที่กรอกข้อความครบถ้วนแล้ว ผู้ใช้บริการจะสามารถใช้บริการใด ๆ ของ ได้ทันที
3. ระยะเวลาการเป็นสมาชิก ให้ถือว่ามีผลอยู่ตลอดไปจนกว่าผู้ใช้บริการจะขอเลิกการเป็นสมาชิก หรือ ปณท ยกเลิกอันเนื่องจากผู้ใช้บริการไม่ปฏิบัติหรือปฏิบัติผิดข้อกำหนดของ

ที่มา : https://pantip.com/topic/40510595/%7Broom_url%7D

คำอธิบายสถานการณ์

ณเดชน์ได้รับอีเมลจากไปรษณีย์ไทยแจ้งว่ามีพัสดุจากต่างประเทศค้างส่งอยู่ที่ที่ทำการไปรษณีย์ ต้องเสียค่าธรรมเนียมและภาษีก่อน จึงจะจัดส่งได้ ณเดชน์จึงคิดว่าตนเองคงจะได้รับของใช้แพง ๆ จากต่างประเทศโดยที่ตนเองไม่ได้สั่งซื้อ จึงเข้าไปกรอกรายละเอียดข้อมูลบัตรเครดิต หลังจากนั้น บัตรเครดิตของณเดชน์ก็ถูกตัดเงินไปเป็นจำนวนมาก จนตนเองต้องตกเป็นหนี้ธนาคาร

วิเคราะห์สถานการณ์จากคำถาม

1. อะไร คือ พฤติกรรมเสี่ยง ?
2. เราจะป้องกันได้อย่างไร ?
3. ถ้าเหตุเกิดขึ้นกับเรา จะต้องทำอย่างไรต่อไป ?

ใบงานที่ 1.1.2
เรื่อง สถานการณ์ภัยไซเบอร์ (5)
“เกมกล คนเครื่องแบบ”

ที่มา : https://www.amarintv.com/news/crime/506676

คำอธิบายสถานการณ์

อรุณีได้รับโทรศัพท์จากตำรวจนายหนึ่ง แจ้งว่าอรุณีมีส่วนพัวพันกับอาชญากรรมข้ามชาติ จำเป็นต้องโอนเงินเข้ามาให้ตำรวจอายัดตรวจสอบ จึงจะพ้นความผิด อรุณีจึงรีบโอนเงินให้จนหมดบัญชี เพราะความเกรงกลัวจะถูกติดคุก แต่หลังจากนั้นอรุณีก็ไม่สามารถติดต่อตำรวจได้อีกเลย และเงินก็ไม่ได้รับคืนกลับมา

วิเคราะห์สถานการณ์จากคำถาม

1. อะไร คือ พฤติกรรมเสี่ยง ?
2. เราจะป้องกันได้อย่างไร ?
3. ถ้าเหตุเกิดขึ้นกับเรา จะต้องทำอย่างไรต่อไป ?

ใบงานที่ 1.1.2
เรื่อง สถานการณ์ภัยไซเบอร์ (6)
“ยินดีด้วย คุณคือผู้โชค(ไม่)ดี”

ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

คำอธิบายสถานการณ์

มานะได้รับข้อความทางโทรศัพท์ระบุว่า “ยินดีด้วย ! คุณเป็นผู้โชคดี ได้รับเงินเยียวยาจากรัฐบาล จำนวน 20,000 บาท โปรดกรอกรายละเอียดที่ www.rataban999.com” ด้วยความดีใจและอยากได้เงินเยียวยา จึงกดลิงก์และกรอกรายละเอียดส่วนตัวไป หลังจากนั้นเงินในบัญชีของมานะ ถูกถอนออกไปจนหมดสิ้น

วิเคราะห์สถานการณ์จากคำถาม

1. อะไร คือ พฤติกรรมเสี่ยง ?
2. เราจะป้องกันได้อย่างไร ?
3. ถ้าเหตุเกิดขึ้นกับเรา จะต้องทำอย่างไรต่อไป ?

แนวคำตอบใบงานที่ 1.1.1
เรื่อง ความหมายของไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์

1. อธิบายความหมายของไซเบอร์

ไซเบอร์ หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต โครงข่าย โทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

2. อธิบายความหมายของการรักษาความมั่นคงปลอดภัยไซเบอร์

การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือ และลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อย ภายในประเทศ

3. บอกเหตุผล “ทำไมต้องรักษาความมั่นคงปลอดภัยไซเบอร์”

1. เพื่อรักษาความลับของข้อมูล ป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์เข้าถึงข้อมูลสำคัญ เช่น ข้อมูลส่วนบุคคล ข้อมูลทางธุรกิจ ข้อมูลขององค์กร

2. เพื่อรักษาความถูกต้องและความสมบูรณ์ของข้อมูล ทำให้มั่นใจ ถูกต้องและความสมบูรณ์ของข้อมูลว่าข้อมูลไม่ถูกแก้ไข ดัดแปลง หรือลบโดยไม่ได้รับอนุญาต ข้อมูลจึงยังคงเชื่อถือได้

3. เพื่อให้ข้อมูลและระบบพร้อมใช้งานเสมอ ป้องกันไม่ให้ระบบล่มหรือไม่สามารถเข้าถึงได้ เช่น การโจมตีทางไซเบอร์ ความขัดข้องอื่น ๆ ที่ทำให้ผู้ใช้ไม่สามารถใช้งานได้

แนวคำตอบใบงานที่ 1.1.2
เรื่อง สถานการณ์ภัยไซเบอร์ (1)
“เงินกู้ เงินกลุ้ม”

กรณีของป้าน้อยเป็นตัวอย่างของมิจฉาชีพหลอกให้กดลิงก์ผ่าน SMS ปลอม ซึ่งเป็นภัยที่กำลังระบาดมาก โดยอาศัยความเดือดร้อนทางการเงินของเหยื่อเป็นช่องทางในการล่อลวง

อะไร คือ พฤติกรรมเสี่ยง ?

1. เชื่อในข้อความปล่อยกู้ที่ง่ายและรวดเร็วเกินจริง เช่น “กู้ได้ทันที ไม่ต้องใช้เอกสาร ไม่เช็คเครดิต” ซึ่งเป็นเงื่อนไขที่ผิดปกติสำหรับสถาบันการเงินที่ถูกกฎหมาย
2. กดลิงก์จากข้อความโดยไม่ตรวจสอบความน่าเชื่อถือของผู้ส่ง มิจฉาชีพมักใช้ลิงก์ที่ดูคล้ายของจริง แต่เป็นเว็บไซต์ปลอมที่ดึงข้อมูลส่วนตัวหรือฝังมัลแวร์
3. ให้ข้อมูลสำคัญในเว็บไซต์หรือแอปพลิเคชันปลอม เช่น เลขบัญชี เลขบัตรประชาชน รหัสผ่าน

เราจะป้องกันได้อย่างไร ?

1. อย่าเชื่อข้อเสนอ “กู้เงินง่าย” โดยไม่มีหลักประกันหรือไม่ตรวจสอบธนาคารจริง ทั้งนี้ แหล่งเงินกู้ถูกกฎหมายจะมีการตรวจสอบประวัติเครดิต เอกสารแสดงรายได้ ฯลฯ
2. ไม่กดลิงก์จาก SMS หรือแอปพลิเคชันที่ไม่รู้จัก
3. รู้ทันกลโกงมิจฉาชีพที่มักหลอกให้ดาวน์โหลดแอปพลิเคชันที่ฝังมัลแวร์ หรือส่ง OTP เพื่อเจาะข้อมูลบัญชี
4. หากไม่มั่นใจ ควรปรึกษาครอบครัวหรือผู้มีความรู้ก่อนทำธุรกรรมทางการเงินใด ๆ

ถ้าเหตุเกิดขึ้นกับเรา จะต้องทำอย่างไรต่อไป ?

1. รีบติดต่อธนาคารทันที เพื่ออายัดบัญชีธนาคาร
2. รวบรวมหลักฐาน เช่น ข้อความที่ได้รับ ลิงก์เว็บไซต์ที่เข้าไป สลิปการหักเงิน บันทึกหน้าจอ และแจ้งความกับตำรวจ
3. เฝ้าติดตามธุรกรรมทางการเงินของตนเองอย่างใกล้ชิด เพื่อตรวจสอบว่ามีรายการผิดปกติอื่น ๆ หรือไม่

แนวคำตอบใบงานที่ 1.1.2
เรื่อง สถานการณ์ภัยไซเบอร์ (2)
“รหัส (ไม่) ลับ”

กรณีของนายธงชัยเป็นตัวอย่างของการตั้งรหัสผ่านไม่ปลอดภัย จนทำให้บัญชีเฟซบุ๊กถูกแฮ็ก และถูกนำไปใช้ในทางที่ผิด โดยการหลอกยืมเงินจากเพื่อน ซึ่งเป็นภัยที่เกิดขึ้นบ่อยมากในโลกออนไลน์

อะไร คือ พฤติกรรมเสี่ยง ?

1. ตั้งรหัสผ่านง่ายเกินไป คือ “12345678” ซึ่งเป็นรหัสผ่านยอดนิยมที่ถูกใช้บ่อยและเดาง่าย
2. ไม่มีการเปิดการยืนยันตัวตนแบบ 2 ขั้นตอน (Two-Factor Authentication) ทำให้เมื่อแฮ็กเกอร์เข้าถึงรหัสผ่าน ก็สามารถเข้าใช้งานบัญชีได้ทันที
3. ผู้เสียหายอาจใช้รหัสผ่านเดียวกันกับหลายบัญชี

เราจะป้องกันได้อย่างไร ?

1. ตั้งรหัสผ่านให้รัดกุมและปลอดภัย อย่างน้อย 12 ตัวอักษร ประกอบด้วย ตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ - เล็ก ตัวเลขและสัญลักษณ์พิเศษ หลีกเลี่ยงการใช้ชื่อเล่น วันเกิด หรือเลขเรียงกัน เช่น 123456
2. เปิดการยืนยันตัวตนแบบ 2 ขั้นตอน (Two-Factor Authentication) ใช้ร่วมกับเบอร์โทรศัพท์ หรือแอปพลิเคชัน เช่น Google Authenticator
3. เปลี่ยนรหัสผ่านเป็นประจำ และไม่ใช้รหัสเดียวกันในหลายบัญชี
4. ระวังการเข้าสู่ระบบผ่าน Wi-Fi สาธารณะ หรือเครื่องคอมพิวเตอร์ที่ไม่ใช่ของตนเอง

ถ้าเหตุเกิดขึ้นกับเรา จะต้องทำอย่างไรต่อไป ?

1. รีบแจ้งเฟซบุ๊กว่าบัญชีถูกแฮ็ก
2. แจ้งเพื่อนหรือคนรู้จักทันทีว่าเฟซบุ๊กถูกแฮ็ก และห้ามโอนเงินหรือให้ข้อมูลกับคนที่แอบอ้าง
3. เปลี่ยนรหัสผ่านทุกบัญชีที่ใช้รหัสเดียวกับบัญชีที่ถูกแฮ็ก
4. แจ้งความหากมีการนำบัญชีไปหลอกยืมเงินผู้อื่น โดยเฉพาะหากมีคนรู้จักโอนเงินไปให้คนร้าย
5. เก็บหลักฐานทุกอย่าง เช่น ข้อความที่คนร้ายใช้คุยกับเพื่อน บัญชีที่ให้โอนเงิน

แนวคำตอบใบงานที่ 1.1.2
เรื่อง สถานการณ์ภัยไซเบอร์ (3)
“ลัก ลวง”

กรณีของสมใจเป็นตัวอย่างของการหลอกลวงในรูปแบบความรักออนไลน์ ซึ่งเป็นภัยทางไซเบอร์ที่มิจฉาชีพมักใช้ “ความรัก” เป็นเครื่องมือเพื่อหลอกให้เหยื่อโอนเงิน

อะไร คือ พฤติกรรมเสี่ยง ?

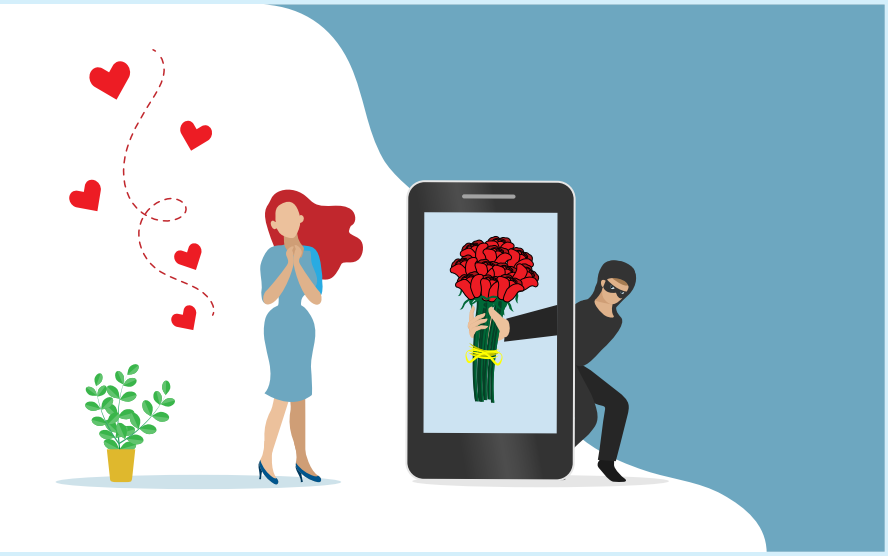
1. เชื่อใจคนแปลกหน้าในโลกออนไลน์เร็วเกินไป เพิ่งรู้จักกันเพียงหนึ่งสัปดาห์ แต่เชื่อว่าฝ่ายตรงข้าม “รักจริง” และ “จะมาแต่งงาน”
2. โอนเงินให้กับบุคคลที่ไม่เคยพบหน้าจริง ๆ โดยอ้างว่าเป็นค่าใช้จ่ายเดินทาง เอกสาร หรือภาษี
3. ขาดความระมัดระวังในการประเมินสถานการณ์ เชื่อคำพูดหวานซึ้งเพื่อหว่านล้อมหรือคำสัญญาเกินจริงโดยไม่ตั้งคำถาม

เราจะป้องกันได้อย่างไร ?

1. ตั้งสติ และระวังคนที่ “รักเร็วเกินไป” หรือให้สัญญาเกินจริง เช่น บอกจะแต่งงาน ซื้อบ้าน หรือย้ายมาอยู่ด้วยทั้งที่เพิ่งรู้จักกันไม่กี่วัน
2. อย่าโอนเงินหรือส่งข้อมูลส่วนตัวให้กับคนที่ไม่เคยพบตัวจริง แม้จะคุยกันนานแค่ไหนก็ตาม
3. ตรวจสอบตัวตนของอีกฝ่าย เช่น ขอวิดีโอคอล ค้นหารูปภาพเพื่อดูว่าเป็นรูปภาพแอบอ้างหรือไม่
4. ระวังประวัติปลอม ซึ่งมักใช้รูปคนต่างชาติ หน้าตาดี ฐานะดี เช่น ทหาร หมอ วิศวกร นักธุรกิจ
5. ปรึกษาครอบครัวหรือเพื่อนก่อนตัดสินใจโอนเงินให้ใคร

ถ้าเหตุเกิดขึ้นกับเรา จะต้องทำอย่างไรต่อไป ?

1. รวบรวมหลักฐานทั้งหมด เช่น ข้อความสนทนา รูปภาพ สลิปการโอนเงิน เบอร์บัญชีปลายทาง อีเมล ชื่อผู้ใช้ในแอปพลิเคชัน
2. แจ้งความกับตำรวจ



แนวคำตอบใบงานที่ 1.1.2
เรื่อง สถานการณ์ภัยไซเบอร์ (4)
“ส่งด่วนจากต่างแดน”

กรณีของณเดชน์เป็นตัวอย่างของ “อีเมลหลอกลวง” เมื่อผู้ใช้งานคลิกเข้าสู่ระบบ อาชญากรที่สร้างเว็บไซต์ปลอมเหล่านั้นก็จะล้วงข้อมูลส่วนบุคคลของผู้ใช้งานไปทันที ไม่ว่าจะเป็นหมายเลขบัตรเครดิต เลขบัตรประจำตัวประชาชน ตลอดจนรหัสผ่านในการเข้าสู่บัญชีต่าง ๆ

อะไร คือ พฤติกรรมเสี่ยง ?

1. หลงเชื่ออีเมลหลอกลวง ไม่ตรวจสอบความน่าเชื่อถือของอีเมล เช่น ชื่อผู้ส่ง ชื่ออีเมล หรือข้อความที่ใช้หลอกล่อ
2. ให้ข้อมูลส่วนตัวและข้อมูลทางการเงินโดยไม่ตรวจสอบให้แน่ชัด
3. เชื่อว่าได้รับของจากต่างประเทศโดยที่ตนเองไม่ได้สั่งซื้อ

เราจะป้องกันได้อย่างไร ?

1. อย่าหลงเชื่อข้อความที่แจ้งว่ามีของรอจัดส่งโดยไม่ได้สั่งซื้อ
2. ของจากต่างประเทศจะไม่มีทางมาถึงหากเราไม่เคยสั่ง หรือถ้ามีจริง ควรตรวจสอบกับผู้ส่งหรือบริษัทขนส่งโดยตรงเท่านั้น
3. อย่าให้ข้อมูลส่วนตัวหรือบัตรเครดิตผ่านลิงก์ในอีเมล
4. ใช้วิธีเข้าผ่านเว็บไซต์หลักด้วยตนเอง เช่น พิมพ์ URL ด้วยตนเอง
5. ตรวจสอบความถูกต้องของอีเมลผู้ส่ง ของจริงจะเป็นทางการตามชื่อบริษัท

ถ้าเหตุเกิดขึ้นกับเรา จะต้องทำอย่างไรต่อไป ?

1. รีบติดต่อธนาคารทันที เพื่อแจ้งอายัดบัตรเครดิตหรือบัตรเดบิตที่ถูกหลอกให้กรอกข้อมูล และขอระงับการทำรายการที่ยังไม่เรียบร้อย
2. รวบรวมหลักฐาน เช่น อีเมลที่ได้รับ ลิงก์เว็บไซต์ที่เข้าไป สลิปการหักเงิน บันทึกหน้าจอ และแจ้งความกับตำรวจ
3. เฝ้าติดตามธุรกรรมทางการเงินของตนเองอย่างใกล้ชิด เพื่อตรวจสอบว่ามีรายการผิดปกติอื่น ๆ หรือไม่

แนวคำตอบใบงานที่ 1.1.2
เรื่อง สถานการณ์ภัยไซเบอร์ (5)
“เกมกล คนเครื่องแบบ”

กรณีของอรุณีเป็นตัวอย่างของ “แก๊งคอลเซ็นเตอร์หลอกโอนเงิน” ซึ่งเป็นอาชญากรรมที่พบบ่อยมากในปัจจุบัน โดยเฉพาะในกลุ่มผู้สูงอายุ หรือผู้ที่มีความเชื่อและความกลัวต่อเจ้าหน้าที่รัฐ ซึ่งอาจปลอมตัวมาในลักษณะต่าง ๆ เช่น เจ้าหน้าที่ตำรวจ ทหาร เจ้าหน้าที่สรรพากร เจ้าพนักงานที่ดิน

อะไร คือ พฤติกรรมเสี่ยง ?

1. เชื่อว่าคนโทรมาเป็นเจ้าหน้าที่ตำรวจจริงโดยไม่มีการตรวจสอบ
2. ตกใจและกลัวจนขาดสติไตร่ตรอง
3. โอนเงินให้บุคคลที่ไม่รู้จักโดยไม่มีหลักฐานหรือขั้นตอนที่ถูกต้อง

เราจะป้องกันได้อย่างไร ?

1. ตั้งสติ ไม่ตกใจ ไม่ทำตามคำสั่งใครทางโทรศัพท์
2. ตรวจสอบก่อนทุกครั้ง เช่น เดินทางไปพบตำรวจตัวจริงที่สถานีตำรวจใกล้บ้าน
3. อย่าให้ข้อมูลส่วนตัวทางโทรศัพท์
4. ตระหนักไว้ว่าหากเราไม่เคยทำความผิด เราก็จะไม่มีความผิดใด ๆ

ถ้าเหตุเกิดขึ้นกับเรา จะต้องทำอย่างไรต่อไป ?

1. รีบติดต่อธนาคารทันที เพื่อแจ้งอายัดบัตรเครดิตหรือบัตรเดบิตที่ถูกหลอกให้กรอกข้อมูลและขอระงับการทำรายการที่ยังไม่เรียบร้อย
2. รวบรวมหลักฐาน เช่น เบอร์โทรศัพท์ ชื่อบัญชี และแจ้งความกับตำรวจ
3. เฝ้าติดตามธุรกรรมทางการเงินของตนเองอย่างใกล้ชิด เพื่อตรวจสอบว่ามีรายการผิดปกติอื่น ๆ หรือไม่

แนวคำตอบใบงานที่ 1.1.2
เรื่อง สถานการณ์ภัยไซเบอร์ (6)
“ยินดีด้วย คุณคือผู้โชค(ไม่)ดี”

กรณีของมานะเป็นตัวอย่างของการหลอกลวงผ่าน SMS หรือเว็บไซต์ปลอม ที่แอบอ้างว่า เป็นหน่วยงานของรัฐ เพื่อดึงดูดให้กรอกข้อมูลส่วนตัว แล้วนำข้อมูลไปใช้ถอนเงินหรือทำธุรกรรมโดยไม่ได้รับอนุญาต

อะไร คือ พฤติกรรมเสี่ยง ?

1. หลงเชื่อข้อความ SMS ที่ระบุว่า “ได้รับเงินเยียวยา” โดยไม่ตรวจสอบความถูกต้อง เนื้อหาลวง มักจงใจใช้คำว่า “รัฐบาล” “เยียวยา” “ด่วน” เพื่อกระตุ้นอารมณ์
2. กดลิงก์ที่แนบมากับข้อความโดยไม่พิจารณา โดยเว็บไซต์ปลอมมักใช้ชื่อใกล้เคียงกับของจริง
3. กรอกข้อมูลส่วนตัวในเว็บไซต์ที่ไม่น่าเชื่อถือ เช่น ชื่อ - นามสกุล เลขบัตรประชาชน เลขบัญชี PIN รหัส OTP

เราจะป้องกันได้อย่างไร ?

1. อย่ากดลิงก์ที่มากับ SMS หรือข้อความแปลก ๆ โดยเฉพาะถ้าอ้างว่าได้รับสิทธิ์พิเศษ เงินเยียวยา เงินรางวัล ฯลฯ
2. ตรวจสอบเว็บไซต์ก่อนเข้าใช้งาน ซึ่งเว็บไซต์ของรัฐโดยปกติจะต้องลงท้ายด้วย “.go.th” (บางหน่วยงานอาจเป็นรูปแบบอื่น ต้องตรวจสอบทุกครั้ง)
3. ไม่กรอกข้อมูลส่วนตัวในเว็บไซต์ที่ไม่มั่นใจ เช่น รหัส ATM เลขหลังบัตรเครดิต
4. ติดตามข่าวสารจากแหล่งทางการ เช่น หน่วยงานของรัฐโดยตรง

ถ้าเหตุเกิดขึ้นกับเรา จะต้องทำอย่างไรต่อไป ?

1. รีบติดต่อธนาคารทันที เพื่อแจ้งอายัดบัตรเครดิตหรือบัตรเดบิตที่ถูกหลอกให้กรอกข้อมูล และขอระงับการทำรายการที่ยังไม่เรียบร้อย
2. รวบรวมหลักฐาน เช่น อีเมลที่ได้รับ ลิงก์เว็บไซต์ที่เข้าไป สลิปการหักเงิน บันทึกหน้าจอ และแจ้งความกับตำรวจ

หน่วยการเรียนรู้ที่ 1 พื้นฐานด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์
แผนการจัดกิจกรรม 1.2 เรื่อง หลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ระยะเวลา 30 นาที

สาระสำคัญ

การรักษาความมั่นคงปลอดภัยไซเบอร์ มีองค์ประกอบหลักการพื้นฐาน 3 ประการ (CIA Triad) คือ 1) Confidentiality (ความลับ) 2) Integrity (ความถูกต้องสมบูรณ์) และ 3) Availability (ความพร้อมใช้งาน) ร่วมกับมาตรการสนับสนุนอื่น ๆ เพื่อให้การใช้งานข้อมูลและระบบดิจิทัลมีความปลอดภัย น่าเชื่อถือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

จุดประสงค์

เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบายหลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้

ขอบข่ายเนื้อหา

1. Confidentiality (ความลับ)
2. Integrity (ความถูกต้องสมบูรณ์)
3. Availability (ความพร้อมใช้งาน)

สื่อการเรียนรู้

1. PowerPoint บรรยายให้ความรู้ เรื่อง หลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

https://shorturl.asia/LDm8w

2. ใบความรู้ที่ 1.2 เรื่อง หลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

วัสดุอุปกรณ์

เครื่องคอมพิวเตอร์/โน้ตบุ๊ค/แท็บเล็ต/โทรศัพท์มือถือ เชื่อมต่ออินเทอร์เน็ต

ขั้นตอนการจัดกิจกรรม

1. วิทยากรสอบถามชวนคุยเกี่ยวกับเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์
2. วิทยากรบรรยายให้ความรู้ เรื่อง หลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยอธิบายหลักการพื้นฐาน ได้แก่ Confidentiality (ความลับ) Integrity (ความถูกต้องสมบูรณ์) และ Availability (ความพร้อมใช้งาน) พร้อมทั้งยกตัวอย่างสถานการณ์ภัยไซเบอร์ที่เกี่ยวข้องในแต่ละหลักการ
3. วิทยากรตั้งคำถามเพื่อกระตุ้นการวิเคราะห์หลักการพื้นฐานที่เกี่ยวข้องกับสถานการณ์ภัยไซเบอร์ ยกตัวอย่างคำถาม ดังนี้

- กรณีระบบของหน่วยงานหนึ่งถูกโจมตีด้วยระบบ DDoS ถือเป็นรูปแบบพื้นฐานการโจมตีแบบใด
- กรณีนาย A ส่งไฟล์เก็บไว้ที่เซิร์ฟเวอร์ และนาย B ได้ดักจับหรือเปลี่ยนแปลงไฟล์ของนาย A ก่อนถูกจัดเก็บไว้ในเซิร์ฟเวอร์ ถือเป็นรูปแบบพื้นฐานการโจมตีแบบใด

4. วิทยากรให้ผู้เข้ารับการอบรมศึกษาใบความรู้ที่ 1.2 เรื่อง หลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
5. วิทยากรมอบหมายให้ผู้เข้ารับการอบรมทำใบงานที่ 1.2 เรื่อง หลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
6. วิทยากรสรุปองค์ความรู้เกี่ยวกับหลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การวัดและประเมินผล

1. ใบงาน
2. การสังเกต

ใบความรู้ที่ 1.2
เรื่อง หลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ในปัจจุบัน ความมั่นคงปลอดภัยไซเบอร์เป็นเรื่องสำคัญต่อประชาชนเป็นอย่างมาก เนื่องจากข้อมูลส่วนตัวหรือข้อมูลของหน่วยงานถือเป็นสิ่งมีค่าและต้องได้รับการคุ้มครอง โดยองค์ประกอบด้านความมั่นคงปลอดภัยไซเบอร์มีองค์ประกอบหลักการพื้นฐาน 3 ประการ คือ Confidentiality (ความลับ) Integrity (ความถูกต้องสมบูรณ์) และ Availability (ความพร้อมใช้งาน) หรือเรียกย่อว่า “CIA Triad” ซึ่งถือเป็นหลักการพื้นฐานของความมั่นคงปลอดภัยไซเบอร์ ที่ทุกคนควรเรียนรู้ เพราะมีความสำคัญ คือ เป็นแนวคิดหลักในการรักษาความปลอดภัยของข้อมูล ที่จะช่วยให้ประชาชนเห็นความสำคัญของข้อมูลที่ตนมี และมีความระมัดระวังในการเปิดเผยหรือส่งต่อข้อมูลมากขึ้น หรือในส่วนขององค์กรหน่วยงานก็สามารถนำหลักการดังกล่าวมาปรับใช้ในการรักษาข้อมูลหน่วยงาน ข้อมูลพนักงาน และข้อมูลทางธุรกิจ โดยองค์ประกอบหลักการพื้นฐานของความมั่นคงปลอดภัยไซเบอร์ 3 ประการ มีรายละเอียด ดังนี้

1. Confidentiality (ความลับ)

มุ่งเน้นที่การควบคุมการเข้าถึงระบบหรือข้อมูล เพื่อรักษาความลับ ให้เป็นไปตามชั้นความลับของระบบหรือข้อมูลนั้น ๆ ซึ่งจะต้องควบคุมว่าระบบหรือข้อมูลนี้ “ใครสามารถเข้าถึงหรืออ่านได้” “ใครสามารถเพิ่ม แก้ไข หรือลบได้” เช่น คอมพิวเตอร์ส่วนตัวของเรา ควรจะเป็นเราเท่านั้นที่จะสามารถเข้าไปใช้งานได้ หรือสามารถที่จะอ่านข้อมูลภายในเครื่องได้

2. Integrity (ความถูกต้องสมบูรณ์)

มุ่งเน้นที่ความถูกต้องสมบูรณ์ของข้อมูลในระบบ ซึ่งต้องคงอยู่ในสภาพเดิมตั้งแต่เริ่มทำการเก็บข้อมูล ระหว่างการส่งข้อมูล กระทั่งข้อมูลมาถึงปลายทาง โดยข้อมูลจะต้องไม่ถูกเปลี่ยนแปลงแก้ไขหรือทำลายระหว่างการส่งข้อมูล

3. Availability (ความพร้อมใช้งาน)

มุ่งเน้นที่ความพร้อมใช้งานของระบบหรือข้อมูล โดยระบบหรือข้อมูลจะต้องใช้งานได้ทุกเมื่อที่ต้องการหรือตามเวลาที่กำหนดไว้ ซึ่งหากสามารถรักษาไว้ซึ่งความลับและความถูกต้องสมบูรณ์ได้แล้ว แต่ไม่มีความพร้อมใช้งานถือว่ายังไม่สอดคล้องตามคุณสมบัติของความมั่นคงปลอดภัยทางไซเบอร์ เช่น ไฟล์เอกสารนำเสนอประมูลถูกเก็บไว้ในตู้เซฟอย่างดีเรียบร้อย แต่เมื่อถึงเวลาที่จำเป็นต้องใช้ ไม่สามารถเปิดตู้เซฟได้ก็อาจทำให้ส่งผลกระทบต่อธุรกิจได้

ที่มา : https://www.blockdit.com/posts/633d4f511c659636156d4dda

ใบงานที่ 1.2
เรื่อง หลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

คำชี้แจง ให้ผู้เข้ารับการอบรมตอบคำถามต่อไปนี้ พร้อมอธิบายเหตุผลประกอบ

1. หากระบบเก็บข้อมูลลูกค้าออนไลน์ถูกโจมตีจนทำให้แฮ็กเกอร์สามารถเข้าถึงและคัดลอกข้อมูลส่วนตัวของลูกค้าทั้งหมดออกไปได้ โดยที่ข้อมูลในระบบยังคงอยู่เหมือนเดิมและสามารถ ใช้งานได้ปกติ เหตุการณ์นี้กระทบต่อหลักการใดของหลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มากที่สุด เพราะเหตุใด

2. ในระหว่างการส่งข้อมูลคำสั่งซื้อจากลูกค้าไปยังเซิร์ฟเวอร์ขององค์กร มีผู้ไม่ประสงค์ดี ดักจับข้อมูล และเปลี่ยนแปลงจำนวนสินค้าในคำสั่งซื้อนั้นก่อนที่ข้อมูลจะไปถึงเซิร์ฟเวอร์ เหตุการณ์นี้กระทบต่อหลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มากที่สุด เพราะเหตุใด

3. หากระบบเก็บข้อมูลลูกค้าขององค์กรล่ม ไม่สามารถเข้าถึงข้อมูลใด ๆ ได้เลยเป็นเวลาหลายชั่วโมง เนื่องจากเซิร์ฟเวอร์ขัดข้อง แม้จะไม่มีการโจรกรรมหรือเปลี่ยนแปลงข้อมูลใด ๆ เหตุการณ์นี้กระทบต่อหลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มากที่สุด เพราะเหตุใด

แนวคำตอบใบงานที่ 1.2
เรื่อง หลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1. หากระบบเก็บข้อมูลลูกค้าออนไลน์ถูกโจมตีจนทำให้แฮ็กเกอร์สามารถเข้าถึงและคัดลอกข้อมูลส่วนตัวของลูกค้าทั้งหมดออกไปได้ โดยที่ข้อมูลในระบบยังคงอยู่เหมือนเดิมและสามารถใช้งานได้ปกติ เหตุการณ์นี้กระทบต่อหลักการใดของหลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มากที่สุด เพราะเหตุใด

จากเหตุการณ์ข้อที่ 1 กระทบต่อ Confidentiality (ความลับ) มากที่สุด เพราะข้อมูลส่วนตัวของลูกค้าซึ่งควรจะเป็นความลับได้ถูกเปิดเผยและเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต (แฮ็กเกอร์) แม้ข้อมูลจะยังคงอยู่ในระบบและใช้งานได้ก็ตาม

2. ในระหว่างการส่งข้อมูลคำสั่งซื้อจากลูกค้าไปยังเซิร์ฟเวอร์ขององค์กร มีผู้ไม่ประสงค์ดีดักจับข้อมูลและเปลี่ยนแปลงจำนวนสินค้าในคำสั่งซื้อนั้นก่อนที่ข้อมูลจะไปถึงเซิร์ฟเวอร์ เหตุการณ์นี้กระทบต่อหลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มากที่สุด เพราะเหตุใด

จากเหตุการณ์ข้อที่ 2 กระทบต่อ Integrity (ความถูกต้องสมบูรณ์) มากที่สุด เพราะข้อมูลคำสั่งซื้อได้ถูกเปลี่ยนแปลงแก้ไขระหว่างการส่งข้อมูลทำให้ข้อมูลไม่ถูกต้องและไม่ตรงกับต้นฉบับที่ลูกค้าระบุไว้

3. หากระบบเก็บข้อมูลลูกค้าขององค์กรล่ม ไม่สามารถเข้าถึงข้อมูลใด ๆ ได้เลยเป็นเวลาหลายชั่วโมงเนื่องจากเซิร์ฟเวอร์ขัดข้อง แม้จะไม่มีการโจรกรรมหรือเปลี่ยนแปลงข้อมูลใด ๆ เหตุการณ์นี้กระทบต่อหลักการพื้นฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มากที่สุด เพราะเหตุใด

จากเหตุการณ์ข้อที่ 3 กระทบต่อ Availability (ความพร้อมใช้งาน) มากที่สุด เพราะผู้ใช้งาน (ทั้งลูกค้าและพนักงาน) ไม่สามารถเข้าถึงและใช้งานระบบหรือข้อมูลได้ตามปกติ ซึ่งส่งผลกระทบต่อการดำเนินงานขององค์กรอย่างรุนแรง

หน่วยการเรียนรู้ที่ 1 พื้นฐานด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์
แผนการจัดกิจกรรม 1.3 เรื่อง ประเภทภัยคุกคามทางไซเบอร์

ระยะเวลา 1 ชั่วโมง

สาระสำคัญ

ภัยคุกคามทางไซเบอร์มีหลายประเภท ทั้งด้านซอฟต์แวร์ เครือข่าย ข้อมูลส่วนบุคคล และพฤติกรรมของผู้ใช้งาน ซึ่งส่งผลกระทบต่อความปลอดภัย ความเชื่อมั่น และการใช้เทคโนโลยีดิจิทัล ดังนั้นผู้ใช้ทุกคนจึงควรตระหนักรู้และเรียนรู้วิธีป้องกันตนเองจากภัยคุกคามเหล่านี้

จุดประสงค์

เพื่อให้ผู้เข้ารับการอบรมสามารถจำแนกประเภทภัยคุกคามทางไซเบอร์ได้

ขอบข่ายเนื้อหา

1. มัลแวร์ (Malware)
2. การโจมตีด้วยการปฏิเสธให้บริการ (DoS/DDoS Attack)
3. ฟิชชิง (Phishing)
4. การโจมตีด้วยการแทรกกลาง (Man-in-the-Middle)

สื่อการเรียนรู้

1. ใบความรู้ที่ 1.3 เรื่อง ประเภทภัยคุกคามทางไซเบอร์
2. คลิปวิดีโอ เรื่อง รูปแบบภัยคุกคามทางไซเบอร์

https://dg.th/31usi4c0pn

วัสดุอุปกรณ์

1. เครื่องคอมพิวเตอร์/โน้ตบุ๊ค/แท็บเล็ต/โทรศัพท์มือถือ เชื่อมต่ออินเทอร์เน็ต
2. กระดาษปรู๊ฟ
3. ปากกาเคมี

ขั้นตอนการจัดกิจกรรม

1. วิทยากรให้ผู้เข้ารับการอบรมรับชมคลิปวิดีโอ เรื่อง รูปแบบภัยคุกคามทางไซเบอร์

https://dg.th/31usi4c0pn

2. วิทยากรให้ผู้เข้ารับการอบรมสะท้อนความรู้สึกและความตระหนักจากการรับชมคลิปวิดีโอ ในประเด็นรูปแบบภัยคุกคามทางไซเบอร์ ตามความคิดส่วนบุคคล
3. วิทยากรให้ผู้เข้ารับการอบรมศึกษาใบความรู้ที่ 1.3 เรื่อง ประเภทภัยคุกคามทางไซเบอร์
4. วิทยากรแบ่งกลุ่มผู้เข้ารับการอบรมตามความเหมาะสม โดยให้ร่วมกันระดมความคิดเห็น และวิเคราะห์ตามใบงานที่ 1.3 เรื่อง ประเภทภัยคุกคามทางไซเบอร์
5. วิทยากรเลือกกลุ่มออกมานำเสนอผลการวิเคราะห์ประเภทภัยคุกคามทางไซเบอร์ กลุ่มละไม่เกิน 5 นาที
6. วิทยากรสรุปองค์ความรู้เกี่ยวกับประเภทภัยคุกคามทางไซเบอร์

การวัดและประเมินผล

1. ใบงาน / ชิ้นงาน / ผลงาน
2. การสังเกต

ใบความรู้ที่ 1.3
เรื่อง ประเภทภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์เป็นหนึ่งในความเสี่ยงสำคัญที่ส่งผลกระทบต่อข้อมูล ระบบ และความมั่นคงขององค์กร หรือบุคคลในยุคดิจิทัล การเข้าใจประเภทของภัยคุกคามเหล่านี้เป็นพื้นฐานสำคัญในการวางแผนป้องกันและรับมืออย่างมีประสิทธิภาพ ภัยคุกคามทางไซเบอร์มีหลายประเภท ซึ่งแต่ละประเภทมีลักษณะและผลกระทบที่แตกต่างกัน จำเป็นต้องมีการเฝ้าระวังและเสริมสร้างความรู้ด้านไซเบอร์อย่างต่อเนื่องเพื่อรับมือกับภัยเหล่านี้ได้ทันเหตุการณ์

ภัยคุกคามทางไซเบอร์ จำแนกเป็น 4 ประเภท ได้แก่

1. มัลแวร์ (Malware)

มัลแวร์ คือ โปรแกรมที่เป็นอันตรายถูกทำขึ้นมาเพื่อมุ่งร้ายต่อข้อมูลในระบบ ทำให้เครื่องคอมพิวเตอร์ทำงานผิดไปจากเดิม รวมถึงการขโมยข้อมูลส่วนบุคคลของผู้ใช้งานและการลบข้อมูล ซึ่งมัลแวร์มีหลากหลายรูปแบบ ดังนี้

1.1 โทรจัน (Trojan) เป็นโปรแกรมที่แปลกปลอมเข้ามาในเครื่อง ซึ่งมักจะดาวน์โหลดโปรแกรมหรือซอฟต์แวร์ตัวอื่นติดมาด้วย เมื่อติดตั้งลงเครื่องเสร็จสิ้น โทรจันจะทำการขโมยหรือลบข้อมูลออกจากเครื่อง และบางครั้งอาจเป็นเหตุให้เครื่องนั้นทำงานช้าลงหรือหยุดชะงัก

1.2 แบ็คดอร์ (Backdoor) เป็นโปรแกรมที่ผู้โจมตีได้ติดตั้งไว้บนเครื่องเหยื่อ ที่จะอนุญาตให้ผู้โจมตีเข้าถึงเครื่องเวลาใดก็ได้ เป้าหมายของแบ็คดอร์ คือ การลบหลักฐานการเข้าถึงเครื่องออกจากบันทึกกิจกรรม (log) ของเครื่อง แบ็คดอร์จะมีประสิทธิภาพเมื่อสามารถเข้ามาในเครื่องได้อีกครั้ง จะเกิดบันทึกกิจกรรมภายในระบบน้อยลงหรือบางครั้งอาจไม่เกิดบันทึกกิจกรรมเลยก็เป็นได้ ทำให้เหยื่อไม่อาจรู้ได้เลยว่าเครื่องนั้นถูกฝังแบ็คดอร์ หรือถูกโจมตีไปเป็นที่เรียบร้อยแล้ว

1.3 ไวรัส (Virus) และ เวิร์ม (Worms) มีความคล้ายคลึงกัน เนื่องจากมีจุดประสงค์เพื่อให้ระบบติดไวรัสมัลแวร์ต่าง ๆ และเป็นหนึ่งในวิธีการสร้างช่องให้ผู้โจมตีสามารถเข้าถึงเครื่องได้ง่าย ไวรัสและเวิร์มหลายตัวมีการนำโทรจันและแบ็คดอร์ผูกไปด้วย เพื่อฝังทางเข้าไว้ให้กับผู้โจมตีแล้ว จึงแพร่กระจายต่อไป

ไวรัสและเวิร์มมีความแตกต่างกัน คือ ไวรัสจะติดกับตัวติดตั้งโปรแกรมหรือไฟล์ที่สามารถทำงานได้ ซึ่งเมื่อมีการเรียกใช้โปรแกรมที่มีไวรัสอยู่ ไวรัสก็จะกระจายตัวเอง โดยการฝังตัวเองเข้าไปอยู่ในโปรแกรมต่าง ๆ เช่น เกม อีเมล รหัสไฟล์ ในขณะที่เวิร์มจะกระจายด้วยตัวเองได้โดยไม่จำเป็นต้องมีพาหะ จะสามารถกระจายตัวจากระบบสู่ระบบแบบอัตโนมัติด้วยตนเอง

1.4 แรนซัมแวร์ (Ransomware) เป็นมัลแวร์ที่เข้าทำการใส่รหัสหรือควบคุมไฟล์นั้น เช่น ไฟล์เอกสาร รูปภาพ วิดีโอ โดยเจ้าของไฟล์จะไม่สามารถเปิดไฟล์ได้เลย เว้นแต่ต้องทำการจ่ายเงิน เพื่อเอารหัสมาเปิดกู้คืนข้อมูล มัลแวร์ประเภทนี้จึงเป็นที่รู้จักในชื่อ “มัลแวร์เรียกค่าไถ่”

1.5 แอดแวร์ (Adware) เป็นมัลแวร์โฆษณาสินค้า ที่มักจะขึ้นมารบกวนผู้ใช้งานคอมพิวเตอร์หรืออุปกรณ์ เพื่อต้องการให้มีการซื้อสินค้านั้น ๆ

ใบความรู้ที่ 1.3 (ต่อ)
เรื่อง ประเภทภัยคุกคามทางไซเบอร์

1.6 สปายแวร์ (Spyware) เป็นมัลแวร์สายลับที่จะดึงข้อมูลต่าง ๆ ที่อยู่ในคอมพิวเตอร์ ส่งไปยังบุคคลภายนอกหรือแฮ็กเกอร์

1.7 รูทคิท (Rootkit) เป็นมัลแวร์ที่สามารถควบคุมหรือเข้าใช้เครื่องที่ถูกติดตั้งได้จากระยะไกล พร้อมสามารถหลบซ่อนการมีอยู่ของตัวเอง ทำให้ยากต่อการลบหรือตรวจสอบ

1.8 บ็อตเน็ต (Botnet) เป็นมัลแวร์ที่แฮ็กเกอร์ส่งเข้าควบคุมอุปกรณ์ เพื่อให้ทำงานใดงานหนึ่งจากคำสั่งของแฮ็กเกอร์

2. การโจมตีด้วยการปฏิเสธให้บริการ (DoS/DDoS Attack)

การโจมตีด้วยการปฏิเสธให้บริการ คือ การโจมตีที่ผู้ไม่หวังดีส่งคำขอเข้าถึงเว็บไซต์หรือข้อมูลจำนวนมากในเวลาเดียวกัน เพื่อมุ่งหวังให้ระบบไม่สามารถให้บริการได้ แต่ในบางกรณีจะมีการโจมตีแบบ DDoS ที่รุนแรง ซึ่งเป็นการโจมตีเซิร์ฟเวอร์ที่กระจายตัวมาจากอุปกรณ์และอินเทอร์เน็ตจำนวนมากในเวลาเดียวกัน แต่บางครั้งที่เว็บไซต์หรือระบบใด ๆ ไม่สามารถใช้บริการได้ อาจจะเป็นเพราะมีผู้ใช้บริการในเวลาเดียวกันจำนวนมาก ทำให้ระบบไม่พร้อมใช้งาน เช่น วันนี้เปิดรับสมัครสอบวันแรก มีผู้สนใจสมัครจำนวนมากเข้ามาพร้อมกัน ทำให้ระบบสูญเสียการให้บริการ (ระบบล่ม)

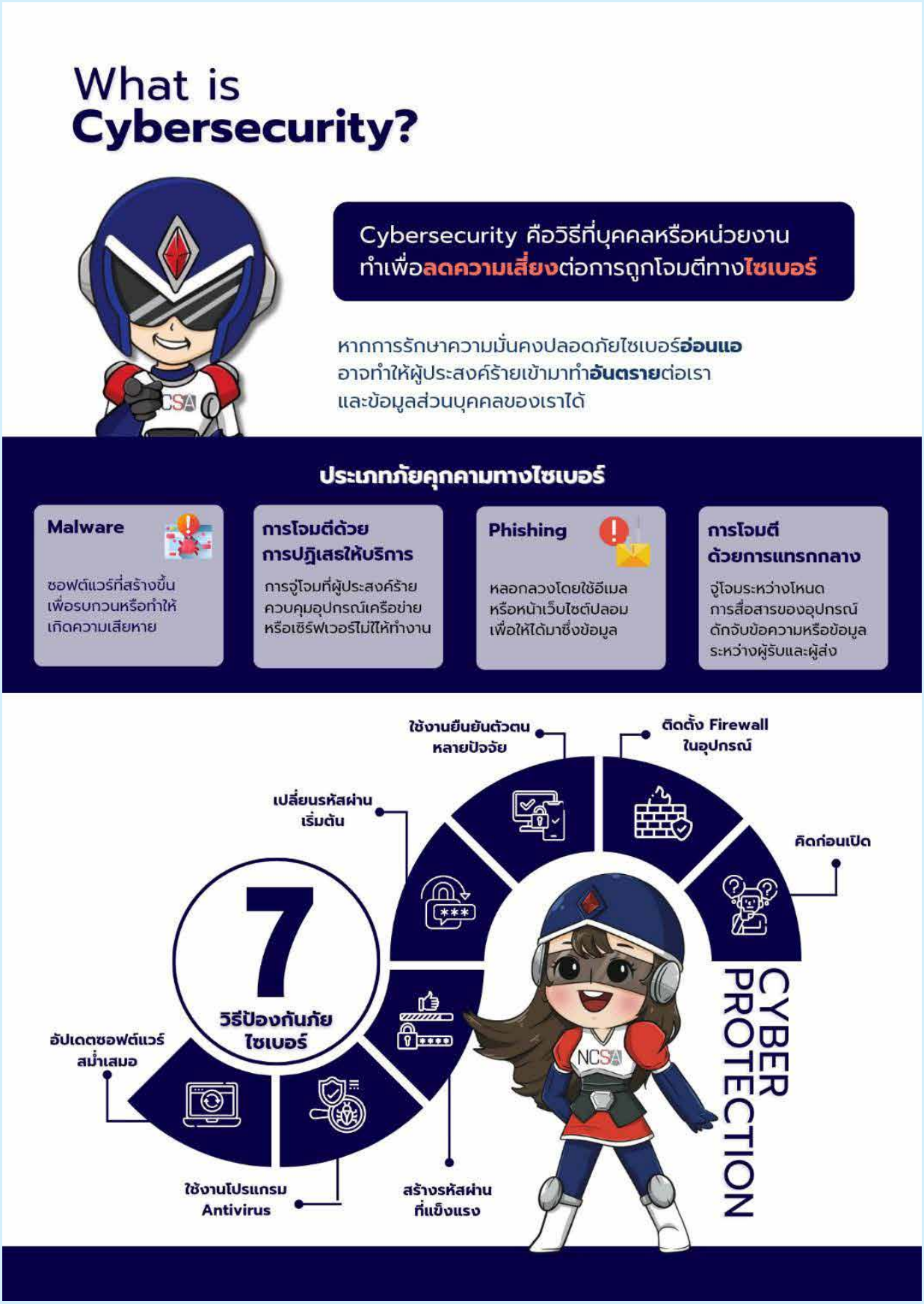
3. ฟิชชิ่ง (Phishing)

ฟิชชิ่ง คือ การโจมตีโดยพยายามหลอกลวงให้บุคคลหลงเชื่อทำตามคำสั่งด้วยการปลอมแปลงหรือปลอมตัวให้น่าเชื่อถือ เช่น ปลอมตัว ปลอมอีเมล ปลอมเว็บไซต์ โดยให้เหยื่อทำการเปิดเผยข้อมูลส่วนบุคคล เช่น หมายเลขบัตรเครดิต ข้อมูลธนาคาร รหัสผ่าน เพื่อการขโมยเงินหรือข้อมูลประจำตัวต่อไป

4. การโจมตีด้วยการแทรกกลาง (Man-in-the-Middle)

การโจมตีด้วยการแทรกกลาง คือ การที่ผู้ไม่ประสงค์ดีแทรกตนเองไปอยู่ตรงกลางระหว่างการสื่อสารของอุปกรณ์คอมพิวเตอร์หรือบุคคล แล้วทำหน้าที่เป็นเสมือนตัวกลางในการรับส่งข้อมูล โดยที่ผู้ใช้งานจะไม่สามารถทราบได้ว่ามีผู้ไม่ประสงค์ดีเป็นผู้รับและส่งสารต่อกับคู่สนทนาของตนอยู่ ทำให้ผู้ไม่ประสงค์ดีสามารถใช้รูปแบบการโจมตีในลักษณะนี้เพื่อดักรับหรือเปลี่ยนแปลงข้อมูลที่ทั้งสองฝั่งสื่อสารกัน การโจมตีในรูปแบบนี้ถูกนำมาประยุกต์ใช้กับการโจมตีระบบเครือข่ายไร้สาย ทำให้ผู้ไม่ประสงค์ดีสามารถแทรกแซงการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ และอุปกรณ์ Wireless Access Point เพื่อเข้าถึง ปลอมแปลง หรือแก้ไขข้อมูลระหว่างการสื่อสารของทั้งสองฝ่าย

ใบความรู้ที่ 1.3 (ต่อ)
เรื่อง ประเภทภัยคุกคามทางไซเบอร์



ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ใบงานที่ 1.3
เรื่อง ประเภทภัยคุกคามทางไซเบอร์

คำชี้แจง ให้ผู้เข้ารับการอบรมร่วมกันระดมความคิดเห็น วิเคราะห์ประเภทภัยคุกคามทางไซเบอร์ และนำเสนอผลการวิเคราะห์

1. ประเภทภัยคุกคามทางไซเบอร์

ประเภทภัยคุกคาม	ลักษณะการโจมตี	เป้าหมายหลักของการโจมตี	ตัวอย่าง
1. มัลแวร์ (Malware)			
2. การโจมตีด้วยการปฏิเสธให้บริการ (DoS/DDoS Attack)			
3. ฟิชชิง (Phishing)			
4. การโจมตีด้วยการแทรกกลาง (Man-in-the-Middle)			

2. อธิบายความแตกต่างระหว่าง Virus และ Worm พอสังเขป

.....

.....

.....

.....

.....

แนวคำตอบใบงานที่ 1.3
เรื่อง ประเภทภัยคุกคามทางไซเบอร์

1. ประเภทภัยคุกคามทางไซเบอร์

ประเภทภัยคุกคาม	ลักษณะการโจมตี	เป้าหมายหลักของการโจมตี	ตัวอย่าง
1. มัลแวร์ (Malware)	โปรแกรมอันตรายที่มุ่งร้ายต่อข้อมูลในระบบ ทำให้คอมพิวเตอร์ทำงานผิดปกติ หรือขโมย/ลบข้อมูล	ขโมยข้อมูล ทำลายข้อมูล ควบคุมเครื่องของเหยื่อ	โทรจัน แบ็คดอร์ ไวรัส เวิร์ม
2. การโจมตีด้วยการปฏิเสธให้บริการ (DoS/DDoS Attack)	ผู้ไม่หวังดีส่งคำขอเข้าถึงข้อมูลหรือเว็บไซต์จำนวนมากในเวลาเดียวกัน	ทำให้ระบบไม่สามารถให้บริการได้ และเกิดภาวะระบบล่ม	การส่งคำขอเข้าเว็บไซต์พร้อมกันจำนวนมากเพื่อโจมตี
3. ฟิชชิง (Phishing)	หลอกล่อให้เหยื่อเชื่อว่าแหล่งที่มานั้นน่าเชื่อถือ เพื่อให้เหยื่อเปิดเผยข้อมูลส่วนบุคคลที่สำคัญ	ขโมยข้อมูลส่วนบุคคล ข้อมูลบัตรเครดิต รหัสผ่าน และข้อมูลธนาคาร	เว็บไซต์ปลอมที่ทำเลียนแบบเว็บไซต์จริงเพื่อหลอกให้กรอกข้อมูล
4. การโจมตีด้วยการแทรกกลาง (Man-in-the-Middle)	การที่ผู้ไม่ประสงค์ดีแทรกตัวอยู่ระหว่างการสื่อสารของอุปกรณ์คอมพิวเตอร์ 2 ฝ่าย	ดักรับ ขโมย หรือเปลี่ยนแปลงข้อมูลที่ส่งผ่านระหว่างกัน	การแทรกแซงการเชื่อมต่อ เช่น ผ่านเครือข่าย Wi-Fi ที่ไม่ปลอดภัย ผู้โจมตีสามารถดักข้อมูลบัญชีธนาคารหรือรหัสผ่านที่ส่งผ่านเครือข่าย สาธารณะได้

2. อธิบายความแตกต่างระหว่าง Virus และ Worm พอสังเขป

virus จะติดกับตัวติดตั้งโปรแกรมหรือไฟล์ ที่สามารถทำงานได้ ซึ่งเมื่อมีการเรียกใช้โปรแกรมที่มี Virus อยู่ Virus ก็จะกระจายตัวเอง โดยการฝังตัวเองเข้าไปอยู่ในโปรแกรมต่าง ๆ เช่น เกม อีเมล visual basic script และไฟล์แฟลช ในขณะที่ Worm จะกระจายด้วยตัวเองได้ ซึ่งไม่จำเป็นต้องมีพาหะ จะกระจายตัวจากระบบสู่ระบบแบบอัตโนมัติด้วยตนเอง

โดยสรุป Virus จะต้องอาศัย “พาหะ” หรือไฟล์ที่สามารถทำงานได้ เช่น เกม อีเมล ในการกระจายตัว โดยจะกระจายเมื่อมีการเรียกใช้งานไฟล์นั้น ๆ ในขณะที่ Worm สามารถกระจายตัวเองจากระบบสู่ระบบได้โดยอัตโนมัติ ซึ่งไม่จำเป็นต้องมีพาหะในการแพร่กระจาย

หน่วยการเรียนรู้ที่ 1 พื้นฐานด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์
แผนการจัดกิจกรรม 1.4 เรื่อง เทคนิคการใช้งานเทคโนโลยีดิจิทัลอย่างปลอดภัย

ระยะเวลา 1 ชั่วโมง

สาระสำคัญ

การใช้งานเทคโนโลยีดิจิทัลอย่างปลอดภัยต้องอาศัยการป้องกันทางเทคนิค ได้แก่ การตั้งค่ารหัสผ่าน การอัปเดตซอฟต์แวร์ การใช้โปรแกรมรักษาความปลอดภัย และการมีวินัยส่วนบุคคล เช่น ระวังการเปิดเผยข้อมูล รู้เท่าทันสื่อ และสำรองข้อมูล เพื่อให้ผู้ใช้สามารถใช้เทคโนโลยีได้อย่างมั่นใจ ลดความเสี่ยง และรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

จุดประสงค์

เพื่อให้ผู้เข้ารับการอบรมสามารถตั้งค่าความปลอดภัยในการใช้งานเทคโนโลยีดิจิทัลได้

ขอบข่ายเนื้อหา

1. การตั้งค่ารหัสผ่าน
2. การยืนยันตัวตน 2 ขั้นตอน (Two-Factor Authentication: 2FA)

สื่อการเรียนรู้

1. PowerPoint บรรยายให้ความรู้ เรื่อง การตั้งค่ารหัสผ่าน

https://shorturl.asia/pWhgi

2. PowerPoint บรรยายให้ความรู้ เรื่อง การยืนยันตัวตน 2 ขั้นตอน (Two-Factor Authentication: 2FA)

https://shorturl.asia/6r3zm

3. ใบความรู้ที่ 1.4.1 เรื่อง การตั้งค่ารหัสผ่าน
4. ใบความรู้ที่ 1.4.2 เรื่อง การยืนยันตัวตน 2 ขั้นตอน (Two-Factor Authentication: 2FA)
5. คลิปวิดีโอ เรื่อง ความปลอดภัยเริ่มต้นที่รหัสผ่าน

https://dg.th/9hiecwd2az

6. คลิปวิดีโอ เรื่อง OTP และ 2FA รหัสผ่าน x2 (คูณสอง) ที่ปลอดภัยแห่งยุค

วัสดุอุปกรณ์

เครื่องคอมพิวเตอร์/โน้ตบุ๊ค/แท็บเล็ต/โทรศัพท์มือถือ เชื่อมต่ออินเทอร์เน็ต

ขั้นตอนการจัดกิจกรรม

1. วิทยากรชวนคิดในประเด็นเกี่ยวกับ “การใช้งานเทคโนโลยีดิจิทัลอย่างปลอดภัย”
2. วิทยากรบรรยายให้ความรู้ เรื่อง การตั้งค่ารหัสผ่าน และให้ผู้เข้ารับการอบรมรับชมคลิปวิดีโอ เรื่อง ความปลอดภัยเริ่มต้นที่รหัสผ่าน

3. วิทยากรให้ผู้เข้ารับการอบรมศึกษาใบความรู้ที่ 1.4.1 เรื่อง การตั้งค่ารหัสผ่าน
4. วิทยากรมอบหมายให้ผู้เข้ารับการอบรมทำใบงานที่ 1.4 เรื่อง การประเมินความปลอดภัยของรหัสผ่าน และฝึกปฏิบัติการตั้งค่ารหัสผ่านด้วยตนเอง
5. วิทยากรให้ให้ผู้เข้ารับการอบรมรับชมคลิปวิดีโอ เรื่อง OTP และ 2FA รหัสผ่าน x2 (คูณสอง) ที่ปลอดภัยแห่งยุค

6. วิทยากรให้ผู้เข้ารับการอบรมศึกษาใบความรู้ที่ 1.4.2 เรื่อง การยืนยันตัวตน 2 ขั้นตอน (Two-Factor Authentication: 2FA)
7. วิทยากรอธิบายหลักการและสาธิตวิธีการยืนยันตัวตน 2 ขั้นตอน (Two-Factor Authentication: 2FA)
8. วิทยากรและผู้เข้ารับการอบรมร่วมกันสรุปองค์ความรู้เกี่ยวกับการตั้งค่าความปลอดภัยในการใช้งานเทคโนโลยีดิจิทัล

การวัดและประเมินผล

1. ใบงาน
2. การสังเกต

ใบความรู้ที่ 1.4.1

เรื่อง การตั้งค่ารหัสผ่าน

รหัสผ่านเป็นส่วนหนึ่งที่มีความสำคัญในการรักษาความปลอดภัยของบัญชีผู้ใช้งานหรือในระบบที่ต้องการความปลอดภัย ซึ่งรหัสผ่านถือเป็นสิ่งที่ใช้สำหรับยืนยันความถูกต้องของตัวบุคคลนั้น ๆ การใช้งานรหัสผ่านจึงช่วยป้องกันความปลอดภัยจากการเข้าถึงข้อมูลโดยมิชอบนั้นได้ หากผู้ใช้งานไม่ให้ความสำคัญในการตั้งค่ารหัสผ่าน ก็จะทำให้ผู้ไม่หวังดีสามารถคาดเดารหัสผ่านและเข้าถึงข้อมูลของได้อย่างง่าย ข้อมูลจาก SPRiNG TECH โดยสำนักข่าว Spring News เมื่อปี 2567 ได้นำเสนอตัวอย่างรหัสผ่านที่ห้ามนำมาใช้เด็ดขาด เนื่องจากง่ายต่อการคาดเดา ดังนี้

อันดับ	ตัวอย่างรหัสผ่านที่คาดเดาง่าย	จำนวนการใช้งาน
1	123456	4,524,867
2	Admin	4,008,850
3	12345678	1,371,152
4	123456789	1,213,047
5	1234	969,811
6	12345	728,414
7	password	710,321

ที่มา: https://www.springnews.co.th/digital-tech/846234

วิธีการตั้งรหัสผ่านที่ปลอดภัย ดังนี้

1. รหัสผ่านต้องประกอบไปด้วย ตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลขที่สลับลำดับกัน และผสมอักขระพิเศษลงไปด้วย เช่น @ ? ! # (ยิ่งหลากหลาย ยิ่งถอดรหัสได้ยากขึ้น)

2. ควรตั้งรหัสผ่านให้มีความยาวอย่างน้อย 12 - 14 ตัวอักษร

3. ไม่ควรตั้งรหัสผ่านเป็นข้อมูลส่วนตัว เช่น ตั้งรหัสผ่านโดยใช้ชื่อ เบอร์โทร และข้อมูลส่วนบุคคล

4. การตั้งรหัสผ่านเป็นคำไม่มีความหมาย มีความปลอดภัยกว่าการตั้งรหัสเป็นคำที่มีความหมาย เช่น do&12sS@d2

5. รหัสผ่านควรมีการเปลี่ยนอย่างน้อย 1 ครั้ง ภายใน 2 - 3 เดือน

6. หลีกเลี่ยงการตั้งรหัสผ่านหลาย ๆ บัญชีเป็นรหัสผ่านเดียวกัน เพื่อเป็นการลดความเสี่ยงที่จะโดนเจาะเข้าบัญชีอื่น ๆ

7. ไม่ควรเลือกการจดจำรหัสผ่านอัตโนมัติในเบราว์เซอร์ เมื่อสร้างรหัสผ่านที่ปลอดภัยแล้ว สิ่งที่ควรทำเพิ่มเติมดังนี้

7.1 ควรเปิดใช้งานการยืนยันตัวตน 2 ขั้นตอน (Two-Factor Authentication: 2FA) เพื่อยืนยันตัวตนเข้าระบบแบบสองชั้น

7.2 ไม่ใช้รหัสผ่านซ้ำ ๆ กันในแต่ละเว็บไซต์ ซึ่งดูเหมือนจะไม่มีผลกระทบอะไร แต่การใช้รหัสผ่านซ้ำกันในแต่ละเว็บไซต์ส่งผลร้ายแรงกว่าที่คิด เพราะไม่ใช่ทุกเว็บไซต์จะดูแลรหัสผ่านของเราได้อย่างปลอดภัย อาจเกิดเหตุการณ์รหัสผ่านรั่วไหล หรือโดนขโมยข้อมูล จนทำให้แฮกเกอร์นำรหัสผ่านชุดเดียวกันมาเข้าระบบในเว็บอื่น ๆ ได้

7.3 เลือกใช้โปรแกรมช่วยเก็บรหัสผ่าน (Password Manager) ที่น่าเชื่อถือในการบันทึกรหัสผ่าน

ใบความรู้ที่ 1.4.2
เรื่อง การยืนยันตัวตน 2 ขั้นตอน
(Two-Factor Authentication: 2FA)

การยืนยันตัวตน 2 ขั้นตอน เป็นวิธีการยืนยันตัวตนที่ได้รับความนิยมและเป็นที่แพร่หลายมากที่สุด ประกอบไปด้วยการใช้งานรหัสผ่านร่วมกับการยืนยันตัวตน เช่น การส่งรหัสผ่านครั้งเดียว (OTP) ผ่าน SMS หรืออีเมล เพื่อช่วยให้มั่นใจว่า ผู้ที่ลงชื่อเข้าใช้นั้นเป็นตัวตนจริง ต่อให้ผู้อื่นรู้รหัสผ่าน แต่ไม่สามารถยืนยันตัวตนในขั้นตอนที่ 2 ได้ก็ไม่สามารถเข้าถึงได้ แต่การยืนยันตัวตน 2 ขั้นตอน มีจุดอ่อน คือ ถ้าใช้รหัสผ่านอีเมลเดียวกันก็ไม่สามารถป้องกันได้ อย่างไรก็ตามควรเปิดการยืนยันตัวตน 2 ขั้นตอนกับทุกบริการเพื่อความปลอดภัย

วิธีการยืนยันตัวตน 2 ขั้นตอน มีรูปแบบ ดังนี้

1. การเก็บรักษารหัสผ่านด้วยโปรแกรมช่วยเก็บรหัสผ่าน (Password Manager)

โปรแกรมช่วยเก็บรหัสผ่านเป็นเสมือนพวงกุญแจที่เก็บกุญแจหลาย ๆ ดอกเข้าด้วยกัน กุญแจแต่ละดอกคือ รหัสผ่าน จากที่ทราบกันแล้วว่ารหัสผ่านที่ดี คือ รหัสผ่านที่ไม่ซ้ำกัน แต่หากให้จดจำรหัสผ่านสำหรับทุกบริการก็คงไม่สะดวก โปรแกรมเก็บรหัสผ่านจึงเข้ามาจัดการส่วนนี้ ซึ่งโปรแกรมเหล่านี้จะสร้างรหัสผ่าน ที่ประกอบขึ้นจากตัวอักษรและตัวเลขที่มีความยาวเหมาะสม ยากต่อการคาดเดา และเก็บรักษาไว้อย่างปลอดภัย ระบบปฏิบัติการรุ่นใหม่ ๆ หรือเว็บเบราว์เซอร์ปัจจุบันมักจะมีโปรแกรมช่วยเก็บรหัสผ่านติดตั้งมาให้ เช่น iCloud Keychain บน mac OS และ iOS หรืออาจใช้โปรแกรมจากผู้พัฒนาบุคคลที่สาม (Third Party) เช่น One Password

2. การยืนยันตนโดยไม่ใช้รหัสผ่าน (Password Less)

เป็นวิธีการยืนยันตัวตนที่หลายเว็บไซต์นำมาใช้งานเมื่อรหัสผ่านไม่ปลอดภัย และผู้ให้บริการเว็บไซต์ต้องแสดงความรับผิดชอบหากรหัสผ่านหลุดออกไป วิธีแก้ปัญหาคือให้ยืนยันตัวตนผ่านลิงก์ที่ถูกส่งไปทางอีเมล หรือ SMS หรือใช้รหัสผ่านครั้งเดียว เท่านั้น

3. การใช้ซอฟต์แวร์หรือฮาร์ดแวร์ช่วยยืนยันตัวตน (Authenticator)

การใช้แอปพลิเคชันช่วยยืนยันตัวตน โดย Google Authenticator ที่เปรียบเสมือนเป็นการยืนยันตัวตน 2 ขั้นตอน มีข้อดีตรงที่ไม่จำเป็นต้องใช้อีเมลหรือเบอร์โทรศัพท์ แต่ระบบลงชื่อเข้าใช้ต้องรองรับด้วยเช่นกัน ซึ่งจะทำให้มั่นใจได้ว่าเป็นผู้ที่ยืนยันตัวตนจริง ๆ เพราะต้องใช้โทรศัพท์เท่านั้น

4. เทคโนโลยีไบโอเมตริกซ์ (Biometric)

เป็นเทคโนโลยีที่ปกติมักจะฝังเข้ามาในฮาร์ดแวร์โทรศัพท์มือถือหรือคอมพิวเตอร์ เช่น Touch ID Face ID บนคอมพิวเตอร์แมคหรือไอโฟน ซึ่งจะทำงานร่วมกับซอฟต์แวร์ช่วยยืนยันตัวตน หรือโปรแกรมช่วยเก็บรหัสผ่าน

ใบงานที่ 1.4
เรื่อง การประเมินความปลอดภัยของรหัสผ่าน

คำชี้แจง ให้ผู้เข้ารับการอบรมวิเคราะห์รหัสผ่าน ฝึกการตั้งรหัสผ่านใหม่และประเมินความปลอดภัย

ให้ทำเครื่องหมาย ✓ ลงในช่อง ☐ ที่คิดว่ามีคุณลักษณะตรงกับรหัสผ่าน R@inB0w$Tr33!

☐ 1.1 มีความยาวอย่างน้อย 12 ตัวอักษร

☐ 1.2 มีตัวพิมพ์ใหญ่และพิมพ์เล็ก

☐ 1.3 มีตัวเลขและสัญลักษณ์

☐ 1.4 ไม่ใช้คำศัพท์ทั่วไปหรือข้อมูลส่วนตัว

☐ 1.5 นำรหัสผ่านนี้ไปใช้ซ้ำในหลายบัญชี

2. ตั้งรหัสผ่านใหม่ แล้วประเมินความปลอดภัยด้วยตนเอง

2.1 รหัสผ่านที่ตั้ง

.....

.....

.....

2.2 จุดแข็งของรหัสผ่าน

.....

.....

.....

2.3 จุดอ่อนของรหัสผ่าน (ถ้ามี)

.....

.....

.....

2.4 หากมีจุดอ่อน มีแนวทางปรับปรุงอย่างไร

.....

.....

.....

แนวคำตอบใบงานที่ 1.4
เรื่อง การประเมินความปลอดภัยของรหัสผ่าน

ให้ทำเครื่องหมาย ✓ ลงในช่อง ☐ ที่คิดว่ามีคุณลักษณะตรงกับรหัสผ่าน R@inB0w$Tr33!

☑ 1.1 มีความยาวอย่างน้อย 12 ตัวอักษร

☑ 1.2 มีตัวพิมพ์ใหญ่และพิมพ์เล็ก

☑ 1.3 มีตัวเลขและสัญลักษณ์

☑ 1.4 ไม่ใช้คำศัพท์ทั่วไปหรือข้อมูลส่วนตัว

☐ 1.5 นำรหัสผ่านนี้ไปใช้ซ้ำในหลายบัญชี

2. ตั้งรหัสผ่านใหม่ แล้วประเมินความปลอดภัยด้วยตนเอง

2.1 รหัสผ่านที่ตั้ง

R@inB0w$Tr33!

2.2 จุดแข็งของรหัสผ่าน

มีความยาวมากกว่า 12 ตัวอักษร มีอักษรภาษาอังกฤษพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และสัญลักษณ์

2.3 จุดอ่อนของรหัสผ่าน (ถ้ามี)

อาจจำยาก

2.4 หากมีจุดอ่อน มีแนวทางปรับปรุงอย่างไร

ใช้ Password Manager เพื่อช่วยจัดการและจำรหัสผ่าน

หน่วยการเรียนรู้ที่ 2 การป้องกันภัยไซเบอร์ขั้นพื้นฐาน
แผนการจัดกิจกรรม 2.1 เรื่อง รู้เท่าทันภัยออนไลน์ในชีวิตประจำวัน

ระยะเวลา 1 ชั่วโมง 10 นาที

สาระสำคัญ

ความหมาย และประเภทของฟิชชิง (Phishing) เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) วิธีป้องกันตนเองจากการโจมตีแบบฟิชชิง และเทคโนโลยีปัญญาประดิษฐ์ รวมถึงภัยคุกคามทางไซเบอร์

จุดประสงค์

1. เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบาย ความหมาย ประเภทของฟิชชิง (Phishing) ได้
2. เพื่อให้ผู้เข้ารับการอบรมมีทักษะป้องกันตนเองจากการโจมตีแบบฟิชชิง (Phishing) ได้
3. เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบาย ความหมาย ลักษณะ และวิธีป้องกันตนเองจากการใช้เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ได้

ขอบข่ายเนื้อหา

1. รู้ทันกลลวงก่อนตกเป็นเหยื่อฟิชชิง (Phishing)
2. เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) กับภัยคุกคามทางไซเบอร์

สื่อการเรียนรู้

1. ใบความรู้ที่ 2.1.1 เรื่อง รู้ทันกลลวงก่อนตกเป็นเหยื่อฟิชชิง (Phishing)
2. ใบความรู้ที่ 2.1.2 เรื่อง เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) และภัยคุกคาทางไซเบอร์
3. คลิปวิดีโอ เรื่อง Phishing คืออะไร ? โดนหลอกขโมยข้อมูลแบบนี้ได้ไง!

4. คลิปวิดีโอ เรื่อง AI กับความปลอดภัยทางไซเบอร์

5. คลิปวิดีโอ เรื่อง เธอเป็นใครกันแน่ (AI DEEPFAKE)

วัสดุอุปกรณ์

1. เครื่องคอมพิวเตอร์/โน้ตบุ๊ค/แท็บเล็ต/โทรศัพท์มือถือ เชื่อมต่ออินเทอร์เน็ต
2. กระดาษปรู๊ฟ
3. ปากกาเคมี

ขั้นตอนการจัดกิจกรรม

1. วิทยากรชวนคุยในประเด็น ภัยคุกคามทางไซเบอร์ใกล้ตัวเรามากขึ้น วิธีการที่มิจฉาชีพใช้เพื่อหลอกลวงให้เหยื่อเปิดเผยข้อมูลส่วนตัว
2. วิทยากรให้ผู้เข้ารับการอบรมเรียนรู้จากสื่อคลิปวิดีโอ เรื่อง Phishing คืออะไร ? โดนหลอกขโมยข้อมูลแบบนี้ได้ไง!

พร้อมทั้งศึกษาใบความรู้ที่ 2.1.1 และทำใบงานที่ 2.1 เรื่อง รู้ทันกลลวงก่อนตกเป็นเหยื่อฟิชชิง (Phishing)

3. วิทยากรเลือกผู้เข้ารับการอบรมนำเสนอใบงาน 5 - 10 คน (สามารถปรับเปลี่ยนได้ตามความเหมาะสม) แล้วให้ผู้เข้ารับการอบรมแลกเปลี่ยนเรียนรู้
4. วิทยากรให้ผู้เข้ารับการอบรมเรียนรู้จากสื่อคลิปวิดีโอ เรื่อง AI กับความปลอดภัยทางไซเบอร์

เรื่อง เธอเป็นใครกันแน่ (AI DEEPFAKE)

และศึกษาใบความรู้ที่ 2.1.2 เรื่อง เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence : AI) และภัยคุกคามทางไซเบอร์

5. วิทยากรและผู้เข้ารับการอบรมสรุปองค์ความรู้ร่วมกัน

การวัดและประเมินผล

1. ใบงาน
2. การสังเกต

ใบความรู้ที่ 2.1.1
เรื่อง รู้ทันกลลวงก่อนตกเป็นเหยื่อฟิชชิง (Phishing)

ความหมายและประเภทของฟิชชิง (Phishing)

ฟิชชิง (Phishing) คือ รูปแบบการโจมตีทางไซเบอร์ที่พบในชีวิตประจำวันได้บ่อยและสามารถส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบ โดยอาศัยหลักการด้านวิศวกรรมสังคม (Social Engineering) หรือการใช้จิตวิทยาหลอกลวง เพื่อให้เหยื่อหลงเชื่อและเปิดเผยข้อมูลสำคัญด้วยตนเอง โดยฟิชชิง (Phishing) แบ่งเป็น 9 ประเภท ดังนี้

1. ฟิชชิงอีเมล (Email Phishing) เป็นรูปแบบพื้นฐานที่สุดและแพร่หลายที่สุด ผู้โจมตีจะส่งอีเมลไปยังเป้าหมายจำนวนมากแบบไม่เจาะจง (หว่าน) โดยแอบอ้างเป็นองค์กรที่น่าเชื่อถือ เช่น ธนาคาร บริษัทขนส่ง หรือผู้ให้บริการโซเชียลมีเดีย เพื่อหลอกให้เหยื่อคลิกลิงก์ที่เป็นอันตรายหรือดาวน์โหลดไฟล์แนบที่มีมัลแวร์ซ่อนอยู่ ตัวอย่างเนื้อหาอีเมล เช่น ขอให้ผู้รับคลิกลิงก์เพื่อยืนยันรายละเอียดบัญชี โดยลิงก์จะนำผู้รับไปยังเว็บไซต์ปลอมที่รวบรวมข้อมูลการเข้าสู่ระบบ

2. ฟิชชิงเจาะจง (Spear Phishing) เป็นการโจมตีที่มุ่งเป้าแบบเฉพาะเจาะจง ไปยังบุคคลหรือองค์กรที่กำหนดไว้ล่วงหน้า ผู้โจมตีจะรวบรวมข้อมูลของเป้าหมาย เช่น จากโซเชียลมีเดีย เพื่อสร้างอีเมลหรือข้อความที่มีความน่าเชื่อถือสูง ทำให้เหยื่อหลงเชื่อได้ง่ายกว่าฟิชชิงทั่วไป

3. ฟิชชิงปลาใหญ่ (Whaling Phishing) เป็นรูปแบบหนึ่งของสเปียร์ฟิชชิงที่มุ่งเป้าไปที่ บุคคลระดับสูงในองค์กร ซึ่งเปรียบเสมือน “ปลาใหญ่” (Whales) เช่น กรรมการบริษัท ผู้บริหารฝ่ายการเงิน หรือผู้บริหารอื่น ๆ เนื่องจากบุคคลเหล่านี้มีสิทธิ์เข้าถึงข้อมูลสำคัญและมีอำนาจในการตัดสินใจที่ส่งผลกระทบต่อองค์กรได้

4. ฟิชชิงเสียง (Vishing Phishing) เป็นการฟิชชิงผ่านการใช้เสียง โดยผู้โจมตีจะใช้การโทรศัพท์เพื่อหลอกลวงเหยื่อ หรือที่รู้จักกันในชื่อ “แก๊งคอลเซ็นเตอร์” โดยมักอ้างตัวเป็นเจ้าหน้าที่จากหน่วยงานภาครัฐหรือสถาบันการเงิน เพื่อข่มขู่หรือสร้างความน่าเชื่อถือให้เหยื่อยอมให้ข้อมูลส่วนตัว

5. ฟิชชิงข้อความ (Smishing Phishing) เป็นการฟิชชิงผ่านข้อความ SMS โดยผู้โจมตีจะส่งข้อความที่มีลิงก์อันตรายมายังโทรศัพท์มือถือของเหยื่อ เช่น อ้างว่าเหยื่อได้รับรางวัล มีพัสดุที่ต้องยืนยัน มีธุรกรรมที่น่าสงสัยและต้องการการตรวจสอบ และยังเกี่ยวข้องกับการใช้ประโยชน์จากความนิยมของช่องทางสื่อสังคมสาธารณะ รวมถึงการสร้างบัญชีสนับสนุนลูกค้าปลอมเพื่อหลอกล่อให้บุคคลให้ข้อมูลที่ละเอียดอ่อนอีกด้วย เช่น ข้อความที่อ้างว่ามาจากบริษัทจัดส่งพัสดุที่ถูกต้องตามกฎหมาย ขอให้ผู้รับคลิกลิงก์เพื่อติดตามพัสดุแล้วจึงหลอกให้ใส่ข้อมูลส่วนตัว

6. ฟิชชิงปลอมตัว (Angler Phishing) เป็นการโจมตีที่เกิดขึ้นบนโซเชียลมีเดีย ผู้โจมตีจะสร้างบัญชีปลอมที่เลียนแบบฝ่ายบริการลูกค้าของบริษัทต่าง ๆ จากนั้นจะคอยจับตาดูโพสต์ที่ผู้ใช้แสดงความไม่พอใจในบริการ และจะเข้าไปตอบกลับโดยสวมรอยเป็นเจ้าหน้าที่ เพื่อหลอกขอข้อมูลส่วนตัวจากเหยื่อ เช่น ในบัญชี เฟซบุ๊ก ได้โพสต์โวยวายเกี่ยวกับการฝากเงินล่าช้าหรือบริการธนาคารที่ไม่ดี และโพสต์นั้นมีชื่อธนาคารอยู่ ผู้ไม่หวังดีจะใช้ข้อมูลนี้เพื่อแสร้งทำเป็นว่ามาจากธนาคาร แล้วติดต่อข้อมูลส่วนตัวเพื่อที่จะแก้ปัญหานั้นให้

ใบความรู้ที่ 2.1.1 (ต่อ)
เรื่อง รู้ทันกลลวงก่อนตกเป็นเหยื่อฟิชชิง (Phishing)

7. ฟิชชิงผู้บริหารปลอม (CEO Fraud Phishing) เป็นการโจมตีที่ผู้ไม่ประสงค์ดี สวมรอยเป็นผู้บริหารระดับสูง เช่น กรรมการบริษัท จากนั้น ส่งอีเมลไปยังพนักงานภายในองค์กร (โดยเฉพาะฝ่ายการเงินหรือบัญชี) เพื่อสั่งการให้โอนเงินหรือเปิดเผยข้อมูลลับของบริษัทอย่างเร่งด่วน

8. ฟิชชิงค้นหาปลอม (Search Engine Phishing) ผู้โจมตีจะสร้างเว็บไซต์ปลอมที่เลียนแบบเว็บไซต์ของบริการยอดนิยม จากนั้นใช้เทคนิคการปรับแต่งเพื่อทำให้ติดอันดับบนเครื่องมือค้นหา เมื่อผู้ใช้คำค้นหาที่เกี่ยวข้องและคลิกเข้าไปยังเว็บไซต์ปลอม ก็จะถูกหลอกให้กรอกข้อมูลส่วนตัวโดยไม่รู้ตัว

9. ฟิชชิงคิวอาร์โคด (Quishing) เป็นการหลอกลวงโดยใช้การปลอมคิวอาร์โคด (QR Code) ให้เหยื่อสแกนโคดที่สร้างมาเพื่อขโมยข้อมูลส่วนตัว ข้อมูลทางการเงิน สามารถตกเป็นเหยื่อได้ง่ายผ่านโคดที่ปรากฏบนแผ่นพับ โปสเตอร์ อีเมล สื่อสังคมสาธารณะ หรือใบเสร็จรับเงินปลอม

วิธีป้องกันตนเองจากการโจมตีแบบฟิชชิ่ง

ด้วยการหลอกลวงแบบฟิชชิงมีความซับซ้อนจากอดีตมากขึ้น และก่อให้เกิดภัยคุกคามที่สำคัญต่อตัวบุคคลเองและองค์กร ซึ่งการป้องกันตัวเองจากการโจมตีแบบฟิชชิง (Phishing) จะต้องอาศัยความตระหนักรู้ การเฝ้าระวังและมาตรการเชิงรุกที่ผสมผสานกัน โดยวิธีป้องกัน ดังนี้

1. ไม่คลิกลิงก์หรือดาวน์โหลดไฟล์แนบจากผู้ส่งที่ไม่รู้จัก โดยเฉพาะอย่างยิ่งอีเมลที่กระตุ้นให้คลิกลิงก์หรือให้ข้อมูลที่ละเอียดอ่อน ดังนั้น จึงควรตรวจสอบตัวตนของผู้ส่งโดยการตรวจสอบที่อยู่อีเมล

2. อัปเดตซอฟต์แวร์ให้อยู่ในเวอร์ชันล่าสุดเป็นประจำและเปิดใช้งานการอัปเดตอัตโนมัติเพื่อให้แน่ใจว่าระบบปฏิบัติการ โปรแกรมป้องกันไวรัส รวมถึงเบราว์เซอร์ได้รับการติดตั้งแพตช์รักษาความปลอดภัยล่าสุด โดยการติดตั้งตัวป้องกันไวรัสและมัลแวร์เพื่อตรวจจับและบล็อกการโจมตี

3. ตรวจสอบที่อยู่ของอีเมลที่ได้รับว่าถูกต้องหรือไม่ ส่งมาจากบริษัทหรือหน่วยงานที่น่าเชื่อถือหรือไม่ รวมไปถึงตัวสะกดต่าง ๆ ซึ่งมักจะมีการปลอมเล็กน้อยเพื่อให้ดูเหมือนจริง

ใบความรู้ที่ 2.1.1 (ต่อ)
เรื่อง รู้ทันกลลวงก่อนตกเป็นเหยื่อฟิชชิง (Phishing)

PHISHING

เป็นคำพ้องเสียง
ที่มาจากคำว่า Fishing
เปรียบเทียบได้ง่ายๆเหยื่อล่อ
ที่ใช้ในการตกปลานั้น
คือ กลวิธีของมิจฉาชีพ
โดยมักจะเป็นข้อความ
หรือการโทรมาหลอกลวง
ทำให้หลงเชื่อจนตกเป็นเหยื่อ

เทคนิคป้องกัน (Defensive Techniques)

ติดตั้งระบบหรือใช้บริการ **Email Security** และ **Email Sandboxing สำหรับตรวจจับและป้องกันอีเมล** Phishing ตรวจสอบและวิเคราะห์ทราฟฟิกเว็บแบบเรียลไทม์ เพื่อป้องกันผู้ใช้เผลอคลิกลิงก์ Phishing ที่แนบมากับอีเมล ศึกษาหาความรู้เกี่ยวกับ Phishing

สิ่งที่ไม่ควรโพสต์บนโซเชียล

วันเกิด ที่อยู่ บัตรประชาชน หรือ **เอกสารและข้อมูลสำคัญ**ต่างๆ เนื่องจากอาจจะถูกคาดเดารหัสผ่านได้ง่าย เบอร์โทรศัพท์ เนื่องจากอาจถูกปลอมตัวโทรไปหลอกถามข้อมูลสำคัญได้

สนทนา

คุยกับบุคคล
ที่มีความเชี่ยวชาญ
หรือเคยมีประสบการณ์
ในการรับมือกับ Phishing
เพื่อที่อนาคตจะสามารถ
รับมือกับเหตุการณ์
ที่จะเกิดขึ้นได้

ฝึกซ้อม

ฝึกซ้อมรับมือกับ
Phishing เพื่อเพิ่ม
ประสบการณ์
และพร้อมรับมือ
เมื่อเกิดเหตุการณ์จริง

ใกล้ตัว

พยายามทำให้ประเด็น
ด้านความมั่นคงปลอดภัย
เป็นเรื่องใกล้ตัว
เช่น เชื่อมโยงกับการเล่น
อินเทอร์เน็ตประจำวัน

ความตระหนัก

เปลี่ยนรูปแบบ
ในการสร้างความตระหนัก
ไปเรื่อยๆ เช่น ส่งอีเมล
เปิดวิดีโอ เพื่อลด
ความซ้ำซากจำเจ

ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ใบความรู้ที่ 2.1.2
เรื่อง เทคโนโลยีปัญญาประดิษฐ์
(Artificial Intelligence: AI) และภัยคุกคามทางไซเบอร์

ความหมายลักษณะของเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence : AI)

ลักษณะของเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence : AI) คือ การพัฒนาระบบคอมพิวเตอร์ที่สามารถเลียนแบบกระบวนการคิดและการตัดสินใจของมนุษย์ โดยระบบปัญญาประดิษฐ์สามารถประมวลผลข้อมูลจำนวนมาก วิเคราะห์ข้อมูลเหล่านั้น และทำการตัดสินใจหรือการกระทำที่มีความคล้ายคลึงกับมนุษย์ได้ ปัจจุบันเทคโนโลยีปัญญาประดิษฐ์เข้ามามีบทบาทในชีวิตประจำวันของมนุษย์เป็นอย่างมาก โดยเฉพาะอย่างยิ่งปัญญาประดิษฐ์สร้างสรรค์ (Generative AI) เช่น การสร้างสรรค์ภาพ วิดีโอ รวมถึงสนับสนุนการดำเนินงานของมนุษย์ในมิติต่าง ๆ ได้อย่างรวดเร็วและง่ายดายมากยิ่งขึ้น ในขณะเดียวกันการใช้เทคโนโลยีปัญญาประดิษฐ์ในทางที่ผิด ก็สามารถนำมาซึ่งภัยคุกคามทางไซเบอร์ได้เช่นกัน ยกตัวอย่าง การจำลองเสียง ภาพใบหน้าเป็นบุคคลสำคัญ บุคคลในครอบครัวหรือเพื่อน เพื่อหลอกลวงให้เหยื่อหลงเชื่อและส่งข้อมูลสำคัญรวมถึงการโอนเงินให้กับผู้ไม่หวังดี ด้วยเทคนิคปัญญาประดิษฐ์หลอกลวงขั้นสูง (AI Deepfake)

ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

แนวทางป้องกันตนเองจากภัยคุกคามที่เกิดจากปัญญาประดิษฐ์

1. ตรวจสอบแหล่งที่มา ว่ามาจากหน่วยงานที่น่าเชื่อถือหรือองค์กรภาครัฐหรือไม่ ตรวจสอบข้อมูลจากหลาย ๆ แหล่งว่าตรงกันหรือไม่ หากไม่สามารถตรวจสอบแหล่งที่มาได้อย่างแน่ชัด ไม่ควรหลงเชื่อหรือปฏิบัติตามสิ่งที่ได้รับชมรับฟัง

2. สังเกตความผิดปกติ ตรวจสอบลักษณะความปกติของเนื้อหาหรือองค์ประกอบในเนื้อหา เช่น ลักษณะของร่างกาย จำนวนนิ้วเกินมาหรือไม่ มีรอยยิ้มที่ผิดปกติหรือไม่ ความเร็วและการใช้น้ำเสียงในการพูด และการมีอารมณ์ร่วมกับเนื้อหา

3. เครื่องมือช่วยตรวจสอบ ใช้เครื่องมือดิจิทัลช่วยตรวจสอบความน่าเชื่อถือและเปรียบเทียบข้อมูลกับแหล่งที่มาต่าง ๆ เช่น ข้อความหรือภาพที่รับชมอยู่ไปค้นหาในเครื่องมือค้นหา (Google) การรับชมเนื้อหารายการที่ตีแผ่ความจริงหรือชวนเปรียบเทียบข่าวปลอม เช่น รายการชัวร์ก่อนแชร์ โดย อสมท.

ใบงานที่ 2.1
เรื่อง รู้ทันกลลวงก่อนตกเป็นเหยื่อฟิชชิง (Phishing)

คำชี้แจง ให้อ่านสถานการณ์ต่อไปนี้ แล้วระบุว่าเป็นการโจมตีแบบฟิชชิง (Phishing) ประเภทใด พร้อมอธิบายเหตุผล และเสนอแนวทางป้องกันตนเองจากสถานการณ์นั้น

สถานการณ์	ประเภทของฟิชชิง (Phishing)	เหตุผล	แนวทางป้องกัน
1. คุณได้รับอีเมลจากธนาคารให้คลิกลิงก์เพื่อยืนยันบัญชี			
2. มีคนโทรมาบอกว่าเป็นเจ้าหน้าที่รัฐ ขอข้อมูลบัตรประชาชนเพื่อยืนยันตัวตน			
3. คุณโพสต์บ่นเรื่องบริการบน Facebook แล้วมีบัญชีแปลก ๆ ทักมาขอข้อมูลเพื่อช่วยเหลือ			
4. มีเว็บไซต์แปลก ๆ โผล่ขึ้นมาเป็นอันดับแรกเมื่อคุณค้นหาคำว่า “สมัครบัตรเครดิต”			

แนวคำตอบใบงานที่ 2.1
เรื่อง รู้ทันกลลวงก่อนตกเป็นเหยื่อฟิชชิง (Phishing)

สถานการณ์	ประเภทของฟิชชิง (Phishing)	เหตุผล	แนวทางป้องกัน
1. คุณได้รับอีเมลจากธนาคารให้คลิกลิงก์เพื่อยืนยันบัญชี	Email Phishing	ใช้ชื่อธนาคารเพื่อหลอกให้คลิกลิงก์ปลอม	ตรวจสอบ URLก่อนคลิก, ติดต่อธนาคารโดยตรง
2. มีคนโทรมาบอกว่าเป็นเจ้าหน้าที่รัฐ ขอข้อมูลบัตรประชาชนเพื่อยืนยันตัวตน	Vishing (Voice Phishing)	ใช้เสียงและความเร่งด่วนเพื่อหลอกให้เปิดเผยข้อมูล	อย่าให้ข้อมูลส่วนตัวทางโทรศัพท์, ตรวจสอบหมายเลขโทรศัพท์
3. คุณโพสต์บ่นเรื่องบริการบน Facebook แล้วมีบัญชีแปลก ๆ ทักมาขอข้อมูลเพื่อช่วยเหลือ	Angler Phishing	แอบอ้างเป็นฝ่ายบริการเพื่อหลอกขอข้อมูล	ตรวจสอบโปรไฟล์, อย่าให้ข้อมูลส่วนตัวในแชท
4. มีเว็บไซต์แปลก ๆ โผล่ขึ้นมาเป็นอันดับแรกเมื่อคุณค้นหาคำว่า “สมัครบัตรเครดิต”	Search Engine Phishing	ใช้ SEO หลอกให้เข้าเว็บปลอม	ตรวจสอบ URL, ใช้เว็บไซต์ทางการเท่านั้น

หน่วยการเรียนรู้ที่ 2 การป้องกันภัยไซเบอร์ขั้นพื้นฐาน
แผนการจัดกิจกรรม 2.2 เรื่อง ร่องรอยดิจิทัล (Digital Footprint)

ระยะเวลา 45 นาที

สาระสำคัญ

เสริมสร้างความเข้าใจเกี่ยวกับข้อมูลและพฤติกรรมที่เกิดขึ้นบนโลกออนไลน์ ซึ่งสามารถทิ้งร่องรอยไว้ทั้งแบบตั้งใจและแบบอัตโนมัติ โดยร่องรอยเหล่านี้ส่งผลทั้งด้านบวกและด้านลบต่อผู้ใช้ เช่น การปรับเนื้อหาให้เหมาะสม หรือสร้างความเสี่ยงด้านความเป็นส่วนตัว ผู้เข้ารับการอบรมจะสามารถจำแนกร่องรอยเป็นประเภท Active และ Passive พร้อมทั้งเรียนรู้วิธีหลีกเลี่ยงร่องรอยที่ไม่พึงประสงค์ เช่น การตั้งค่าความเป็นส่วนตัว หรือใช้โหมดไม่ระบุตัวตน ตลอดจนวิเคราะห์ข้อดีและข้อเสียของร่องรอยดิจิทัลเพื่อสร้างความตระหนักรู้ในการใช้เทคโนโลยีอย่างปลอดภัย มีความรับผิดชอบและเป็นพลเมืองดิจิทัลที่มีภูมิคุ้มกันในการดำเนินชีวิตบนโลกออนไลน์

จุดประสงค์

1. เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบายความหมาย และประเภทของร่องรอยดิจิทัลได้
2. เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบายวิธีการหลีกเลี่ยงการทิ้งร่องรอยดิจิทัลที่ไม่พึงประสงค์ได้
3. เพื่อให้ผู้เข้ารับการอบรมสามารถวิเคราะห์ข้อดีและข้อเสียของร่องรอยดิจิทัลได้

ขอบข่ายเนื้อหา

ร่องรอยดิจิทัล (Digital Footprint)

สื่อการเรียนรู้

1. ใบความรู้ที่ 2.2 เรื่อง ร่องรอยดิจิทัล (Digital Footprint)
2. คลิปวิดีโอ เรื่อง ข่าวอาสาสมัครดิจิทัล Digital Footprint คืออะไร

วัสดุอุปกรณ์

1. เครื่องคอมพิวเตอร์/โน้ตบุ๊ค/แท็บเล็ต/โทรศัพท์มือถือ เชื่อมต่ออินเทอร์เน็ต
2. กระดาษปรู๊ฟ
3. ปากกาเคมี

ขั้นตอนการจัดกิจกรรม

1. วิทยากรชวนคุยในประเด็น การโพสต์ข้อความ แชร์รูปภาพ หรือการกดไลก์ในโซเชียลมีเดีย เป็นการทิ้งข้อมูลของเราไว้บนโลกออนไลน์ ซึ่งสามารถตามร่องรอยได้
2. วิทยากรให้ผู้เข้ารับการอบรมศึกษาใบความรู้ที่ 2.2 เรื่อง ร่องรอยดิจิทัล (Digital Footprint)
3. วิทยากรให้ผู้เข้ารับการอบรมเรียนรู้จากสื่อคลิปวิดีโอ เรื่อง ข่าวอาสาสมัครดิจิทัล Digital Footprint คืออะไร

และให้ผู้เข้ารับการอบรมแลกเปลี่ยนประสบการณ์การทิ้งร่องรอยดิจิทัลที่ส่งผลกระทบต่อตนเอง

4. แบ่งกลุ่มผู้เข้ารับการอบรมตามความเหมาะสม โดยให้ร่วมกันระดมความคิดเห็นและวิเคราะห์ตามใบงานที่ 2.2 เรื่อง ร่องรอยดิจิทัล (Digital Footprint)
5. วิทยากรและผู้เข้ารับการอบรมสรุปองค์ความรู้ร่วมกัน

การวัดและประเมินผล

1. ใบงาน / ชิ้นงาน / ผลงาน
2. การสังเกต

ใบความรู้ที่ 2.2
เรื่อง ร่องรอยดิจิทัล (Digital Footprint)

ปัจจุบันการใช้งานเทคโนโลยีดิจิทัลผ่านระบบออนไลน์ จะทิ้งประวัติ หลักฐานหรือข้อมูลต่าง ๆ ไว้เบื้องหลัง เรียกว่า ร่องรอยดิจิทัล (Digital Footprint) การทำความเข้าใจและบริหารจัดการร่องรอยเหล่านี้ จึงเป็นทักษะพื้นฐานที่สำคัญอย่างยิ่งต่อความมั่นคงปลอดภัยและความเป็นส่วนตัว ซึ่งมีความจำเป็นต้องเรียนรู้ เพราะทุกการใช้สื่อออนไลน์อาจมีการทิ้งข้อมูลที่ส่งผลต่อความปลอดภัยและภาพลักษณ์ มีความเสี่ยงที่จะถูกละเมิดความเป็นส่วนตัวหรือถูกนำข้อมูลไปใช้ในทางที่ผิด การเข้าใจและจัดการร่องรอยดิจิทัลอย่างเหมาะสม จึงสำคัญต่อการปกป้องตนเอง สร้างความน่าเชื่อถือ และเป็นพื้นฐานของการเป็นพลเมืองดิจิทัลที่รับผิดชอบ

ความหมายและประเภทของร่องรอยดิจิทัล (Digital Footprint)

ร่องรอยดิจิทัล คือ ชุดข้อมูลที่เกิดจากการกระทำทั้งหมดของผู้ใช้งานบนโลกอินเทอร์เน็ต ตั้งแต่ การเข้าชมเว็บไซต์ การส่งอีเมล การใช้งานสื่อสังคมสาธารณะ เช่น การโพสต์ การแสดงความคิดเห็น การกดไลก์ การแชร์ ไปจนถึงข้อมูลที่ระบบรวบรวมโดยอัตโนมัติ ข้อมูลเหล่านี้สามารถถูกบันทึก จัดเก็บ และสืบค้นได้จากบุคคลอื่น ซึ่งอาจนำไปสู่ความเสี่ยงด้านความเป็นส่วนตัวและความปลอดภัยได้

ร่องรอยดิจิทัลสามารถแบ่งเป็น 2 ประเภทหลัก ดังนี้

1. ร่องรอยดิจิทัลแบบมิได้เจตนา (Passive Digital Footprint) คือ ร่องรอยที่เกิดจากการรวบรวมข้อมูลโดยที่ผู้ใช้อาจไม่รู้ตัวหรือไม่ได้ตั้งใจทิ้งไว้ ส่วนใหญ่มักเป็นข้อมูลที่ถูกสร้างขึ้นเมื่อผู้ใช้เข้าใช้งานบริการหรือเว็บไซต์ต่าง ๆ เช่น รหัสประจำคอมพิวเตอร์ ประวัติการค้นหา ข้อมูลตำแหน่ง

2. ร่องรอยดิจิทัลแบบเจตนา (Active Digital Footprint) คือ ร่องรอยที่เกิดจากการกระทำโดยเจตนาของผู้ใช้งาน ที่ผู้ใช้จงใจแบ่งปันข้อมูลเกี่ยวกับตนเองสู่สาธารณะ เช่น การโพสต์ข้อความ รูปภาพ หรือวิดีโอลงบนโซเชียลมีเดีย การส่งอีเมลหรือข้อความสนทนา การเขียนบล็อกหรือแสดงความคิดเห็นในเว็บบอร์ด และการกรอกข้อมูลในแบบฟอร์มออนไลน์

วิธีป้องกันการทิ้งร่องรอยดิจิทัล

การบริหารจัดการเพื่อลดความเสี่ยงและควบคุมร่องรอยดิจิทัลได้อย่างมีประสิทธิภาพ โดยมีแนวปฏิบัติดังนี้

1. ร่องรอยดิจิทัลแบบมิได้เจตนา

1.1 คิดก่อนโพสต์ ข้อมูลที่โพสต์หรือแสดงความคิดเห็น จะคงอยู่บนโลกออนไลน์อย่างถาวร แม้จะลบไปแล้วก็ตาม ควรหลีกเลี่ยงการเผยแพร่ข้อมูลที่อ่อนไหว เช่น ข้อมูลทางการเงิน ที่อยู่ หรือข้อมูลแสดงทรัพย์สินส่วนตัวที่อาจล่อเป้าหมายต่อผู้ไม่ประสงค์ดี

1.2 จำกัดการเข้าถึงข้อมูล ตรวจสอบเลือกรับเป็นเพื่อน เลือกโพสต์ให้เฉพาะบุคคลที่รู้จักและไว้ใจในโซเชียลมีเดียเห็นได้เท่านั้น เพื่อป้องกันไม่ให้ข้อมูลส่วนตัวรั่วไหลไปสู่มิจฉาชีพ

ใบความรู้ที่ 2.2 (ต่อ)
เรื่อง ร่องรอยดิจิทัล (Digital Footprint)

2. ร่องรอยดิจิทัลแบบเจตนา

2.1 หลีกเลี่ยงเว็บไซต์ที่ไม่น่าเชื่อถือ ระมัดระวังการคลิกลิงก์หรือเข้าชมเว็บไซต์ที่ไม่มีการเข้ารหัส (ไม่ใช่ HTTPS) หรือเว็บไซต์ที่มีการให้ระบุข้อมูลส่วนบุคคลมากเกินความจำเป็น

2.2 ปิดการเชื่อมต่อเมื่อไม่ใช้งาน ปิดการเชื่อมต่อเทคโนโลยีไร้สายส่วนบุคคล (Bluetooth Technology) และการเชื่อมต่อเครือข่ายแบบไร้สาย (Wi-Fi) เมื่อไม่ได้ใช้งาน เพื่อลดการถูกติดตามหรือการโจมตีจากอุปกรณ์ใกล้เคียง

2.3 หลีกเลี่ยงการทำธุรกรรมผ่านเครือข่ายแบบไร้สาย (Wi-Fi) สาธารณะ

2.4 ยกเลิกบัญชีที่ไม่ได้ใช้งาน ปิดหรือยกเลิกการเป็นสมาชิกในบริการหรืออีเมลที่มิได้ใช้งานแล้ว เพื่อลดจำนวนข้อมูลของเราที่ถูกจัดเก็บอยู่ในระบบต่าง ๆ

ข้อดีและข้อเสียของร่องรอยดิจิทัล

1. ข้อดีของร่องรอยดิจิทัล

1.1 ช่วยให้ค้นหาข้อมูลและติดต่อสื่อสารได้สะดวก ร่องรอยดิจิทัลช่วยให้ค้นหาข้อมูลต่าง ๆ บนโลกออนไลน์ได้ง่ายและรวดเร็ว โดยไม่ต้องเสียเวลาค้นหาด้วยตัวเอง ข้อมูลส่วนตัวที่เคยกรอกไว้บนเว็บไซต์ต่าง ๆ เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ จะถูกบันทึกไว้ ทำให้สามารถกรอกข้อมูลต่าง ๆ ได้สะดวกโดยไม่ต้องพิมพ์ใหม่ ช่วยให้ติดต่อสื่อสารกับเพื่อน ครอบครัว และคนรู้จักได้ง่ายขึ้น โดยไม่ต้องพึ่งพาโทรศัพท์หรืออีเมล

1.2 ช่วยให้ธุรกิจเข้าถึงลูกค้าได้ง่ายขึ้น ธุรกิจสามารถวิเคราะห์พฤติกรรมของลูกค้าผ่านร่องรอยดิจิทัล เพื่อนำมาปรับใช้ได้หลายวัตถุประสงค์ เช่น เพื่อนำมาพัฒนาสินค้าและบริการให้ตรงกับความต้องการของร่องรอยดิจิทัลเพื่อโฆษณาสินค้าและบริการให้ตรงกลุ่มเป้าหมาย และเพื่อสร้างความสัมพันธ์กับลูกค้าผ่านโซเชียลมีเดียและสร้างฐานลูกค้า

1.3 ช่วยให้สามารถเรียนรู้สิ่งใหม่ ๆ ได้อย่างสะดวก มีแหล่งข้อมูลออนไลน์มากมาย เช่น บทความ วิดีโอ และเว็บไซต์ ที่สามารถช่วยให้เรียนรู้สิ่งใหม่ ๆ ได้ โซเชียลมีเดียและกลุ่มออนไลน์ต่าง ๆ ช่วยให้สามารถแลกเปลี่ยนเรียนรู้กับผู้คนที่มีความสนใจคล้ายกัน

1.4 ช่วยให้สามารถหางานและโอกาสทางธุรกิจได้ บริษัทต่าง ๆ มักใช้โซเชียลมีเดียเพื่อค้นหาผู้สมัครงาน ร่องรอยดิจิทัลสามารถช่วยให้สร้างประวัติย่อส่วนบุคคลออนไลน์ และแสดงผลงานให้บริษัทต่าง ๆ ได้เห็น นอกจากนี้ โซเชียลมีเดียและเว็บไซต์ต่าง ๆ ยังช่วยสามารถหาโอกาสทางธุรกิจ เช่น หาคู่ค้า หาลูกค้า หานักลงทุน

ใบความรู้ที่ 2.2 (ต่อ)
เรื่อง ร่องรอยดิจิทัล (Digital Footprint)

2. ข้อเสียของร่องรอยดิจิทัล

2.1 ข้อมูลส่วนตัวอาจถูกเปิดเผย ข้อมูลส่วนตัว เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ ข้อมูลทางการเงิน รูปภาพ ซึ่งอาจถูกเปิดเผยโดยไม่ได้ตั้งใจ ผ่านโพสต์บนโซเชียลมีเดีย เว็บไซต์ หรือแอปพลิเคชันต่าง ๆ ข้อมูลนี้อาจถูกนำไปใช้โดยบุคคลอื่นโดยไม่ได้รับอนุญาต

2.2 ถูกมิจฉาชีพนำข้อมูลไปใช้ในทางที่ผิด ข้อมูลส่วนตัวอาจถูกนำไปใช้เพื่อการหลอกลวง ขโมยเงิน หรือปลอมแปลงตัวตน มิจฉาชีพอาจใช้ข้อมูลส่วนตัวเพื่อสร้างบัญชีปลอม ติดต่อเพื่อนหรือครอบครัว อาจเกิดความเสียหายทางการเงิน สูญเสียชื่อเสียง หรือถูกดำเนินคดี

2.3 ถูกติดตามพฤติกรรมและความสนใจ บริษัทต่าง ๆ สามารถติดตามพฤติกรรมการใช้งานออนไลน์ผ่านคุกกี้ (Cookies) และเทคโนโลยีอื่น ๆ ข้อมูลนี้ถูกนำไปใช้เพื่อวิเคราะห์พฤติกรรม แสดงโฆษณาที่ตรงใจ อาจสูญเสียความเป็นส่วนตัว และถูกจำกัดเสรีภาพในการเลือกข้อมูล

2.4 ถูกกลั่นแกล้งหรือคุกคามออนไลน์ ข้อมูลส่วนตัวที่เปิดเผยบนโลกออนไลน์ อาจถูกนำไปใช้เพื่อการกลั่นแกล้ง คุกคาม หรือสร้างความเสียหาย อาจเกิดผลกระทบทางจิตใจ สูญเสียความมั่นใจ และกลัวการใช้ชีวิตออนไลน์

ใบความรู้ที่ 2.2 (ต่อ)
เรื่อง ร่องรอยดิจิทัล (Digital Footprint)

Digital Footprint

คือ **ร่องรอย**ดิจิทัลที่เกิดขึ้นจากการใช้งาน**บนอินเทอร์เน็ต** และเทคโนโลยีดิจิทัล ไม่ว่าจะเป็นการโพสต์ข้อความ การแชร์รูปภาพ การกดไลค์ หรือการค้นหาข้อมูล บนแพลตฟอร์มต่าง ๆ

Digital Footprint มี 2 ประเภท

Passive Digital Footprint

ร่องรอยดิจิทัลที่ผู้ใช้ไม่ได้ตั้งใจสร้างขึ้น โดยทิ้งไว้บนอินเทอร์เน็ตโดยไม่รู้ตัว

VS

Active Digital Footprint

ร่องรอยดิจิทัลที่ผู้ใช้เจตนาสร้างขึ้น ซึ่งเป็นข้อมูลดิจิทัลที่เปิดเผยโดยตั้งใจ

ข้อดีของ Digital Footprint

สร้างภาพลักษณ์ที่ดีให้กับองค์กร

เพิ่มโอกาสในการเข้าถึงกลุ่มเป้าหมายใหม่ ๆ

ช่วยในการตัดสินใจและวางแผนทางการตลาด

เรียนรู้จากพฤติกรรมในอดีต

ข้อเสียของ Digital Footprint

ขาดความเป็นส่วนตัว

เกิดการโจมตีบนโลกออนไลน์

ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ใบงานที่ 2.2
เรื่อง ร่องรอยดิจิทัล (Digital Footprint)

คำชี้แจง ให้อ่านสถานการณ์และตอบคำถาม

สถานการณ์ที่ 1 น้อยโพสต์รูปบัตรประชาชนลงบน เฟซบุ๊ก เพื่อยืนยันกับเพื่อนว่าตัวเองอายุ 18 ปี จริง

ที่มา : https://www.shutterstock.com/th/search/thai-id-card?

คำถาม

1. การกระทำนี้จะสร้างร่องรอยดิจิทัลแบบใด ?

2. มีความเสี่ยงอะไรบ้างจากการโพสต์นี้ ?

3. หากคุณเป็นเพื่อนของน้อย คุณจะแนะนำอย่างไร ?

ใบงานที่ 2.2 (ต่อ)
เรื่อง ร่องรอยดิจิทัล (Digital Footprint)

สถานการณ์ที่ 2 จอห์นสมัครเรียนออนไลน์และกรอกข้อมูลที่อยู่เบอร์โทรศัพท์ และรหัสผ่านซ้ำกับที่ใช้ในโซเชียลมีเดีย

ที่มา : https://www.lexis-translations.com/en/website-translations/

คำถาม

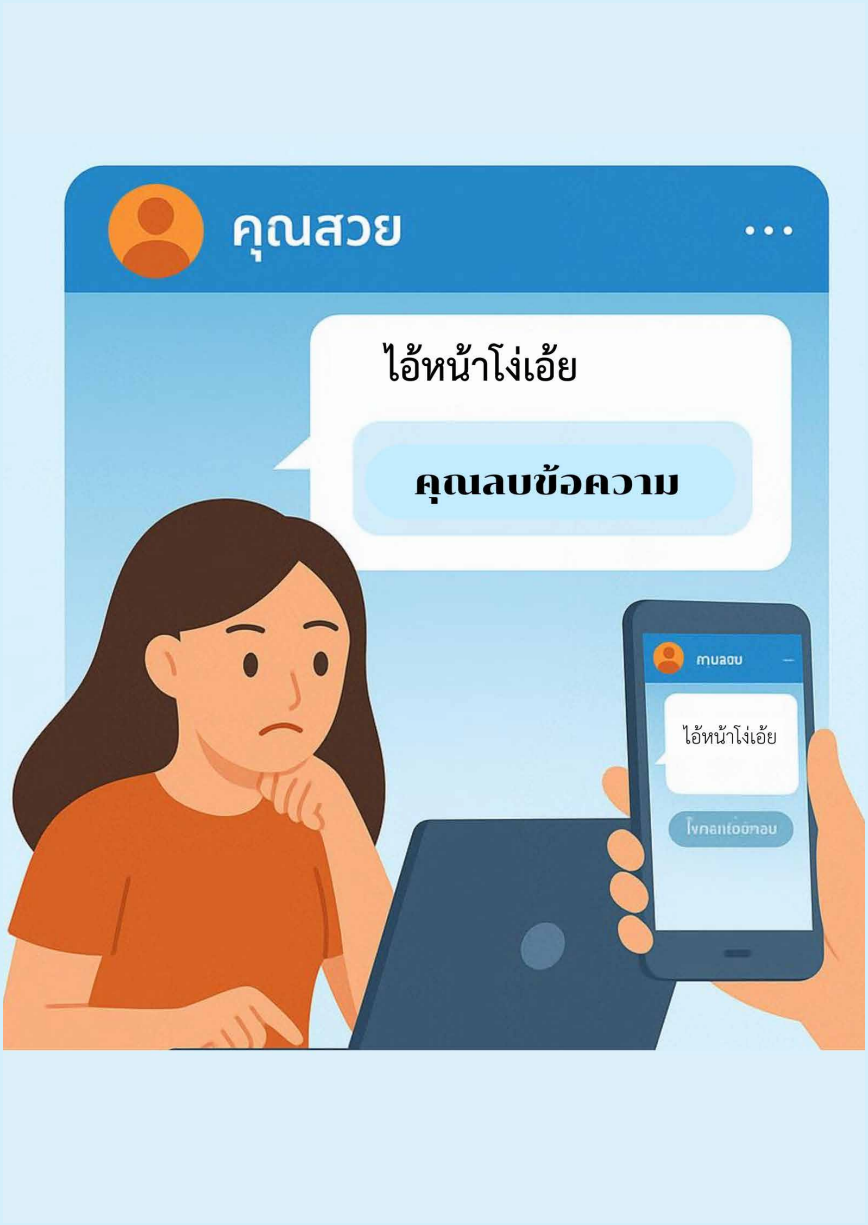
1. พฤติกรรมนี้เสี่ยงต่ออะไร ?

2. ควรแก้ไขหรือป้องกันอย่างไร ?

3. ถ้าข้อมูลรั่วไหลจะเกิดผลกระทบอะไรบ้าง ?

ใบงานที่ 2.2 (ต่อ)
เรื่อง ร่องรอยดิจิทัล (Digital Footprint)

สถานการณ์ที่ 3 คุณสวยคอมเมนต์ด่าผู้อื่นด้วยถ้อยคำรุนแรงในโซเชียลมีเดีย โดยคิดว่าไม่มีใครรู้ว่าคุณสวยด่าใคร



ที่มา : กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้

คำถาม

1. พฤติกรรมนี้เสี่ยงต่ออะไร ?

2. ควรแก้ไขหรือป้องกันอย่างไร ?

3. ถ้าข้อมูลรั่วไหลจะเกิดผลกระทบอะไรบ้าง ?

แนวคำตอบใบงานที่ 2.2
เรื่อง ร่องรอยดิจิทัล (Digital Footprint)

สถานการณ์ที่ 1 น้อยโพสต์รูปบัตรประชาชนลงบน เฟซบุ๊ก เพื่อยืนยันกับเพื่อนว่าตัวเองอายุ 18 ปี จริง

1. ร่องรอยดิจิทัลแบบ Active (เกิดจากการโพสต์เอง) เสี่ยงต่อการถูกขโมย
2. ข้อมูลส่วนตัว เช่น เลขบัตรประชาชน นำไปทำธุรกรรมผิดกฎหมาย
3. ควรแนะนำไม่ให้โพสต์ข้อมูลสำคัญ ควรใช้วิธีอื่น เช่น ยืนยันตัวตนกับเพื่อนด้วยบัตรจริงแบบส่วนตัว

สถานการณ์ที่ 2 จอห์นสมัครเรียนออนไลน์และกรอกข้อมูลที่อยู่เบอร์โทรศัพท์ และรหัสผ่านซ้ำกับที่ใช้ในโซเชียลมีเดีย

1. เสี่ยงต่อการถูกแฮ็กบัญชีโซเชียลมีเดีย หรือการรั่วไหลข้อมูล
2. ควรตั้งรหัสผ่านที่แตกต่างกัน และเปิดใช้การยืนยันตัวตน 2 ขั้นตอน (Two-Factor Authentication: 2FA)
3. ถ้าข้อมูลรั่วไหล อาจถูกโจรกรรมบัญชีโซเชียลมีเดีย ถูกหลอกลวง หรือโดนขโมยข้อมูลทางการเงิน

สถานการณ์ที่ 3 คุณสวยคอมเมนต์ด่าผู้อื่นด้วยถ้อยคำรุนแรงในโซเชียลมีเดีย โดยคิดว่าไม่มีใครรู้ว่าคุณสวยด่าใคร

1. ทิ้งร่องรอยดิจิทัลเชิงลบ ที่อาจถูกบันทึกหรือแคปหน้าจอไว้ได้
2. หากถูกฟ้องร้อง อาจมีผลทางกฎหมาย เช่น หมิ่นประมาท หรือถูกแบนจากแพลตฟอร์ม
3. ควรใช้สื่อออนไลน์อย่างสุภาพ เคารพผู้อื่น เพราะทุกอย่างบนโลกออนไลน์ติดตามย้อนกลับได้

หน่วยการเรียนรู้ที่ 2 การป้องกันภัยไซเบอร์ขั้นพื้นฐาน
แผนการจัดกิจกรรม 2.3 เรื่อง เทคนิคกลลวงบนโลกไซเบอร์

ระยะเวลา 1 ชั่วโมง 20 นาที

สาระสำคัญ

สร้างความเข้าใจเกี่ยวกับรูปแบบ กลยุทธ์ และเทคนิคที่มิจฉาชีพใช้ในการก่อภัยคุกคามทางไซเบอร์ โดยเฉพาะการหลอกลวงผ่านพฤติกรรมในชีวิตประจำวัน เช่น การแอบอ้างตัวตน การสร้างความเร่งด่วน และการใช้ช่องทางออนไลน์ในการหลอกให้เปิดเผยข้อมูลหรือโอนเงิน ผู้เข้ารับการอบรมจะได้เรียนรู้จากกรณีศึกษาที่เกิดขึ้นจริง เพื่อวิเคราะห์พฤติกรรมเสี่ยง วิธีหลอกลวง และผลกระทบต่อบุคคลในสังคม พร้อมทั้งฝึกวิธีการป้องกัน เช่น การตั้งสติ ตรวจสอบข้อมูลก่อนดำเนินการ รวมถึงการใช้หลัก “ไม่กด ไม่โหลด ไม่ให้ ไม่โอน” เป็นแนวทางพื้นฐานในการลดความเสี่ยง นำไปสู่การใช้เทคโนโลยีดิจิทัลอย่างปลอดภัย

จุดประสงค์

1. เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบายเกี่ยวกับเทคนิค กลยุทธ์ ของภัยคุกคามทางไซเบอร์ได้
2. เพื่อให้ผู้เข้ารับการอบรมสามารถวิเคราะห์ข้อมูลกลลวงบนโลกไซเบอร์ได้
3. เพื่อให้ผู้เข้ารับการอบรมสามารถรับมือและป้องกันตนเองจากภัยไซเบอร์ได้

ขอบข่ายเนื้อหา

1. เทคนิค กลยุทธ์ ของภัยคุกคามทางไซเบอร์
2. วิธีการรับมือและป้องกันภัยไซเบอร์
   - หลักการป้องกันพื้นฐาน “ไม่กด ไม่โหลด ไม่ให้ ไม่โอน”
   - การตรวจสอบและตั้งสติ

สื่อการเรียนรู้

1. ใบความรู้ที่ 2.3 เรื่อง เทคนิคกลลวงบนโลกไซเบอร์
2. คลิปวิดีโอ เรื่อง ชัวร์ก่อนแชร์ FACT CHECK EXPERT: ประเภทของการหลอกลวงออนไลน์ (Scams)

https://dg.th/s3oavek6md

วัสดุอุปกรณ์

1. เครื่องคอมพิวเตอร์/โน้ตบุ๊ค/แท็บเล็ต/โทรศัพท์มือถือ เชื่อมต่ออินเทอร์เน็ต
2. กระดาษปรู๊ฟ
3. ปากกาเคมี

ขั้นตอนการจัดกิจกรรม

1. วิทยากรชวนคุยในประเด็น กลลวงบนโลกไซเบอร์ เทคนิค กลยุทธ์ที่มิจฉาชีพเลือกใช้ในการหลอกลวงที่เกิดขึ้นในสังคม การรับมือและวิธีการป้องกัน
2. วิทยากรให้ผู้เข้ารับการอบรมเรียนรู้จากสื่อคลิปวิดีโอ เรื่อง ชัวร์ก่อนแชร์ FACT CHECK EXPERT: ประเภทของการหลอกลวงออนไลน์ (Scams)

https://dg.th/s3oavek6md

3. วิทยากรให้ผู้เข้ารับการอบรมศึกษาใบความรู้ที่ 2.3 เรื่อง เทคนิคกลลวงบนโลกไซเบอร์ และสะท้อนประสบการณ์ที่เคยพบเจอมิจฉาชีพหลอกลวง
4. แบ่งกลุ่มผู้เข้ารับการอบรมตามความเหมาะสม และทำใบงานที่ 2.3 เรื่อง วิเคราะห์กลลวงบนโลกไซเบอร์
5. วิทยากรและผู้เข้ารับการอบรมสรุปองค์ความรู้ร่วมกัน

การวัดและประเมินผล

1. ใบงาน / ชิ้นงาน / ผลงาน
2. การสังเกต

ใบความรู้ที่ 2.3
เรื่อง เทคนิคกลลวงบนโลกไซเบอร์

เทคนิค กลยุทธ์ ของภัยคุกคามทางไซเบอร์

การหลอกลวงทางออนไลน์ คือ การหลอกลวงทางอินเทอร์เน็ตมีจุดประสงค์เพื่อหลอกล่อบุคคลอื่นให้เปิดเผยข้อมูลส่วนตัว ข้อมูลทางการเงิน หรือข้อมูลละเอียดอ่อนอื่น ๆ หรือขโมยเงินของบุคคลนั้นโดยตรง ซึ่งการหลอกลวงทางออนไลน์มีได้หลายรูปแบบ ตั้งแต่ข้อความฟิชชิ่งและตลาดออนไลน์ปลอมไปจนถึงโปรไฟล์หาคู่ปลอมที่ซับซ้อน และข้อตกลงการลงทุนที่ดูดีเกินจริง สิ่งที่การหลอกลวงทางออนไลน์มักมีเหมือนกันคือการใช้กลวิธีทางวิศวกรรมสังคมเพื่อหลอกลวง ชักจูง และเอาเปรียบเหยื่อ

รายงานของ Federal Trade Commission ประจำปี 2023 ซึ่งเป็นหน่วยงานคุ้มครองผู้บริโภคของสหรัฐอเมริกา ระบุว่านับตั้งแต่ปี 2021 เป็นต้นมา หนึ่งในสี่ของผู้ที่รายงานว่า ถูกหลอกลวงเอาเงิน กล่าวว่าการหลอกลวงเริ่มต้นจากโซเชียลมีเดีย อย่างไรก็ตาม มิจฉาชีพสามารถใช้แพลตฟอร์มดิจิทัลเกือบทุกแพลตฟอร์ม ทั้งอีเมล ข้อความ และเว็บไซต์ เพื่อดำเนินแผนการชั่วร้ายของตน

ในการก่ออาชญากรรมไซเบอร์ มิจฉาชีพไม่ได้พึ่งพาแต่ช่องโหว่ทางเทคนิคที่ซับซ้อนเท่านั้น แต่ยังใช้ “วิศวกรรมสังคม” (Social Engineering) เป็นกลยุทธ์หลักในการหลอกลวงและชักจูงเหยื่อให้ตกหลุมพรางได้อย่างแนบเนียน การประยุกต์ใช้เทคนิคเหล่านี้ในรูปแบบที่ซับซ้อนและเป็นอันตรายอย่างยิ่ง โดยมีรายละเอียดของกลยุทธ์ที่มิจฉาชีพนำมาใช้ ดังนี้

1. การสร้างเรื่องราวสมมติ (Pretexting) มิจฉาชีพสร้างสถานการณ์หรือเรื่องราวเท็จที่ดูน่าเชื่อถือและเกี่ยวข้องกับผู้เสียหายอย่างยิ่ง เช่น การกล่าวถึงสิทธิ์เงินบำเหน็จยังชีพ หรือการอ้างอิงหน่วยงานต้นสังกัดเดิม รวมถึงการเสนอ “ทุนการศึกษา” หรือ “โอกาสในการทำงาน” เพื่อลดความระแวงและสร้างความไว้วางใจ

2. การหลอกลวงแบบฟิชชิง (Phishing) หลังจากสร้างความน่าเชื่อถือ มิจฉาชีพจะส่งลิงก์อันตรายผ่านแพลตฟอร์ม LINE SMS หรืออีเมล เพื่อหลอกให้ผู้เสียหายคลิกและดาวน์โหลดแอปพลิเคชันปลอม ซึ่งเป็นประตูสู่การเข้าควบคุมอุปกรณ์ ยกตัวอย่างเช่น แอปพลิเคชัน Digital Pension หรือ ลิงก์สำหรับตรวจสอบพัสดุ

3. มัลแวร์ (Malware) แอปพลิเคชันปลอมที่ถูกส่งมาให้ติดตั้งนั้น แท้จริงแล้วคือ มัลแวร์ประเภทควบคุมจากระยะไกล เมื่อติดตั้งแล้ว จะทำให้มิจฉาชีพสามารถควบคุมโทรศัพท์มือถือของผู้เสียหายจากระยะไกลได้อย่างสมบูรณ์ รวมถึงการมองเห็นหน้าจอ การเข้าถึงแอปพลิเคชัน และข้อมูลภายในเครื่อง

ใบความรู้ที่ 2.3 (ต่อ)
เรื่อง เทคนิคกลลวงบนโลกไซเบอร์

4. การแอบอ้างตัวตน (Impersonation) มิจฉาชีพสร้างโปรไฟล์ปลอมที่น่าเชื่อถือ หรือแอบอ้างเป็นบุคคล/หน่วยงานที่เกี่ยวข้องกับการให้ทุนการศึกษาหรือการจัดหางาน ทำให้เหยื่อเข้าใจผิดว่ากำลังติดต่อกับผู้มีอำนาจหรือผู้เชี่ยวชาญจริง

5. การแสวงหาประโยชน์จากความไว้วางใจและความเปราะบาง (Exploiting Trust and Vulnerability) มิจฉาชีพใช้ประโยชน์จากความหวัง ความใฝ่ฝัน หรือความเปราะบางทางอารมณ์ของเยาวชน เพื่อหลอกล่อให้ทำตามคำสั่งที่ไม่สมเหตุสมผล

6. การข่มขู่เรียกค่าไถ่ (Coercion/Extortion) หลังจากที่มิจฉาชีพได้คลิปวิดีโอหรือข้อมูลที่ละเอียดอ่อนของเหยื่อแล้ว มิจฉาชีพจะเปลี่ยนท่าทีทันที โดยใช้คลิปเหล่านั้นเป็นเครื่องมือในการข่มขู่ว่าจะเผยแพร่สู่สาธารณะ

7. การหลบเลี่ยงการตรวจสอบ มิจฉาชีพจะใช้กลยุทธ์ต่าง ๆ เพื่อให้การทุจริตเป็นไปอย่างรวดเร็วและยากต่อการตรวจจับ เช่น การแบ่งวงเงินในการโอนเงินออกเป็นหลายครั้ง แต่ละครั้งไม่เกินวงเงินที่ต้องมีการสแกนใบหน้าเพื่อหลีกเลี่ยงระบบยืนยันตัวตนที่เข้มงวด

8. การใช้บัญชีม้า เงินที่ถูกโอนออกจากบัญชีผู้เสียหายจะถูกส่งไปยังบัญชีม้าที่มิจฉาชีพเตรียมไว้ ทำให้การติดตามเงินคืนเป็นไปได้ยากและซับซ้อน ทั้งนี้ สำหรับผู้ที่เปิดบัญชีม้าจะมีโทษตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 คือ จำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 300,000 บาท หรือทั้งจำ ทั้งปรับ

9. การแจ้งความล่วงหน้า (Pre-emptive reporting) เป็นการสร้างความสับสนหรือถ่วงเวลาการดำเนินการของเจ้าหน้าที่เมื่อผู้เสียหายตัวจริงพยายามแจ้งความผ่านศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ โทร 1441 เช่น ผู้ก่อเหตุมีการแจ้งความออนไลน์ไว้ล่วงหน้าถึง 13 ครั้ง

วิธีการรับมือและป้องกันภัยไซเบอร์

ในปัจจุบัน ภัยคุกคามทางไซเบอร์ได้พัฒนาสู่ความซับซ้อนที่อาศัยทั้งช่องโหว่ทางเทคนิคและช่องโหว่ทางจิตวิทยา การทำความเข้าใจกลวิธีของมิจฉาชีพ โดยเฉพาะการใช้เทคนิควิศวกรรมสังคมที่แนบเนียนจึงเป็นรากฐานสำคัญในการสร้างภูมิคุ้มกันให้แก่ประชาชนทุกท่าน การเสริมสร้างความรู้ความเข้าใจ การสร้างวินัยในการตรวจสอบข้อมูล และการมีสติในการรับมือกับสถานการณ์ฉุกเฉิน จะช่วยลดโอกาสในการตกเป็นเหยื่อ และสร้างสังคมดิจิทัลที่ปลอดภัยอย่างยั่งยืน

ดังนั้น เพื่อป้องกันตนเองและบุคคลใกล้ชิดจากภัยคุกคามในลักษณะดังกล่าว ประชาชนควรยึดหลักปฏิบัติและแนวทาง ดังนี้

ใบความรู้ที่ 2.3 (ต่อ)
เรื่อง เทคนิคกลลวงบนโลกไซเบอร์

1. หลักการป้องกันพื้นฐาน “ไม่กด ไม่โหลด ไม่ให้ ไม่โอน”

1.1 ไม่กดลิงก์ ห้ามคลิกลิงก์ที่น่าสงสัยที่ส่งมาทาง SMS, LINE, อีเมล หรือช่องทางอื่น ๆ โดยเด็ดขาด ไม่ว่าข้อความนั้นจะดูน่าเชื่อถือเพียงใดก็ตาม

1.2 ไม่โหลดแอปพลิเคชันที่ไม่ใช่จากแหล่งที่เชื่อถือได้ ควรดาวน์โหลดแอปพลิเคชันจาก Google Play Store (สำหรับ Android) หรือ App Store (สำหรับ iOS) เท่านั้น และควรตรวจสอบชื่อผู้พัฒนาแอปพลิเคชันให้ถูกต้อง จำไว้ว่าหน่วยงานราชการหรือธนาคารไม่มีนโยบายให้ติดตั้งแอปพลิเคชันเพื่อทำธุรกรรมหรือขอควบคุมโทรศัพท์มือถือของคุณ

1.3 ไม่ให้ข้อมูลส่วนบุคคล อย่าเปิดเผยข้อมูลส่วนตัว เช่น เลขบัตรประชาชน เลขบัญชีธนาคาร รหัสผ่าน หรือรหัส OTP (One Time Password) ให้กับใครทางโทรศัพท์หรือช่องทางออนไลน์ หากไม่แน่ใจในตัวตนของผู้ติดต่อ

1.4 ไม่โอนเงิน อย่าโอนเงินตามคำบอกของคนแปลกหน้า หรือเมื่อถูกข่มขู่ สร้างความกลัว หรือ อ้างสิทธิประโยชน์ที่เกินจริง

2. การตรวจสอบและตั้งสติ

2.1 “เอ๊ะไว้ก่อน” เมื่อมีผู้ติดต่อมาและแจ้งข้อมูลที่เกี่ยวข้องกับเงิน สิทธิประโยชน์ หรือข้อมูลส่วนตัว ให้ตั้งข้อสงสัยและระมัดระวังเป็นอันดับแรก

2.2 หน่วงเวลาไว้ก่อน หากถูกเร่งรัดให้ดำเนินการใด ๆ ให้แจ้งว่าจะขอตรวจสอบข้อมูลก่อน ไม่รีบร้อนปฏิบัติตามคำสั่ง

2.3 สอบถามและปรึกษา ติดต่อสอบถามหน่วยงานที่ถูกอ้างถึงโดยตรงจากเบอร์โทรศัพท์ที่เป็นทางการ (ค้นหาจากเว็บไซต์ทางการเท่านั้น) หรือปรึกษาคนในครอบครัว หรือบุคคลที่ไว้ใจ เพื่อช่วยตรวจสอบและวิเคราะห์ข้อมูล

ใบงานที่ 2.3
เรื่อง วิเคราะห์กลลวงบนโลกไซเบอร์

คำชี้แจง อ่านกรณีศึกษาต่อไปนี้ แล้วระบุว่าเป็นการใช้ “เทคนิคกลลวง” แบบใด

กรณีศึกษาที่ 1 มิจฉาชีพหลอกผู้สูงอายุ วัย 70 ปี สูญเงินกว่า 70,000 บาท ด้วยกลโกง “บำเหน็จยังชีพ” ผ่านแอปพลิเคชันปลอม

เมื่อเดือนสิงหาคม 2567 ที่ผ่านมา อดีตข้าราชการหญิงวัย 70 ปี ในจังหวัดลพบุรี ตกเป็นเหยื่อของมิจฉาชีพ สูญเงินไปกว่า 72,221 บาท โดยเริ่มจากการถูกโทรศัพท์อ้างตัวเป็นเจ้าหน้าที่จากหน่วยงานต้นสังกัดเดิมแจ้งเรื่องสิทธิ์ “บำเหน็จยังชีพ” และหลอกให้แอดไลน์เพื่อรับแบบฟอร์ม หลังจากนั้นได้ส่งลิงก์ “APPLICATION DIGITAL PENSION” ปลอม เพื่อให้ติดตั้งแอปพลิเคชัน ผู้เสียหายหลงเชื่อเพราะมีข้อมูลส่วนตัวบางส่วนตรงกับความเป็นจริง ทันทีที่ติดตั้งแอปพลิเคชันปลอม ทำให้มิจฉาชีพได้ใช้โปรแกรมควบคุมโทรศัพท์มือถือของผู้เสียหายจากระยะไกล สามารถเข้าถึงแอปพลิเคชันธนาคาร และโอนเงินออกจากบัญชีธนาคารอย่างรวดเร็ว โดยทำธุรกรรมต่อเนื่อง 2 ครั้ง เพื่อหลีกเลี่ยงการสแกนใบหน้า แม้ธนาคารจะโทรแจ้งความผิดปกติ และผู้เสียหายจะพยายามอายัดบัญชี แต่เงินก็ถูกโอนออกไปหมดแล้วภายในเวลาไม่ถึง 1 นาที เหตุการณ์นี้ ย้ำเตือนถึงอันตรายจากกลโกง วิศวกรรมสังคม ที่ใช้ข้อมูลส่วนบุคคลและการควบคุมระยะไกล (REMOTE ACCESS) เพื่อทุจริตทางการเงิน

ที่มา : Thai PBS. สถานีประชาชน. (2568, กรกฎาคม 02) มิจฉาชีพหลอกผู้สูงอายุ ติดตั้งแอปฯ ควบคุมเครื่อง – โอนเงินหมดบัญชี. https://www.youtube.com/watch?v=ffCL1HsVDb8&list=LL&index=1

กรณีศึกษาที่ 2 กลโกง “พัสดุมีปัญหา” หลอกติดตั้งแอปพลิเคชัน ดูดเงินจากบัญชี กว่า 450,000 บาท

วันที่ 18 พฤษภาคม 2568 อุทาหรณ์เตือนใจนักช็อปออนไลน์ เมื่อนางสาววรรณ (นามสมมติ) วัย 47 ปี ต้องสูญเงินกว่า 450,000 บาท ภายในเวลาไม่ถึง 1 ชั่วโมง หลังตกเป็นเหยื่อกลโกง “พัสดุมีปัญหา” ของมิจฉาชีพ เรื่องราวเริ่มต้นขึ้นเมื่อเธอได้รับ SMS ปริศนา อ้างว่า “ขนส่งไม่สามารถจัดส่งพัสดุของคุณได้” พร้อมแนบลิงก์ปลอมไปยังแอปพลิเคชัน LINE ด้วยความกังวลว่าพัสดุที่สั่งไว้จะมีปัญหาจริง เธอจึงกดลิงก์นั้น และนั่นคือจุดเริ่มต้นที่มิจฉาชีพซึ่งแอบอ้างเป็นฝ่ายบริการลูกค้าบริษัทขนส่งเข้ามาหลอกลวง มิจฉาชีพใช้กลวิธีจูงใจ โดยเสนอว่าจะคืนเงินประกันสินค้าให้ 2,000 บาท ก่อนจะส่งลิงก์อันตรายอีกครั้ง เพื่อเชื่อมต่อแอปพลิเคชันธนาคาร จากนั้นก็ออกคำสั่งให้ผู้เสียหายตั้งค่าโทรศัพท์และทำตามขั้นตอนอย่างเร่งรีบ ซึ่งเป็นกลวิธีในการเข้าควบคุมโทรศัพท์จากระยะไกล เพียงไม่ถึง 1 ชั่วโมง เงินในบัญชีของ นางสาววรรณ ก็ถูกโอนออกไป 2 ครั้ง รวม 450,000 บาท แม้จะรีบแจ้งสายด่วนตำรวจไซเบอร์ 1441 ทันที ก็ไม่ทันการณ์ เหตุการณ์นี้ยังคงเป็นปริศนาว่ามิจฉาชีพทราบข้อมูลการสั่งซื้อสินค้าได้อย่างไร และบริษัทครีมทาหน้าก็ปฏิเสธการมีส่วนเกี่ยวข้องใด ๆ กับการหลอกลวงครั้งนี้

ที่มา : Thai PBS. (2568, พฤษภาคม 18) แก๊งคอลเซนเตอร์ อ้าง บ.ขนส่งพัสดุ ส่งSMS หลอกโอนเงิน 4.5 แสนบาท. https://www.thaipbs.or.th/news/content/352261

ใบงานที่ 2.3 (ต่อ)
เรื่อง วิเคราะห์กลลวงบนโลกไซเบอร์

กรณีศึกษาที่ 3 กลโกงมิจฉาชีพอ้างให้ “ทุนการศึกษา” หลอกถ่ายคลิปโป๊เรียกค่าไถ่

วันที่ 7 กรกฎาคม 2568 กลโกงของมิจฉาชีพยังคงปรับเปลี่ยนรูปแบบอย่างต่อเนื่อง ล่าสุดพบรูปแบบใหม่ที่พุ่งเป้าไปที่กลุ่มนักเรียนและเยาวชน ด้วยกลอุบายการอ้างว่าจะมอบ “ทุนการศึกษา” หรือ “โอกาสในการทำงาน” เพื่อหลอกล่อให้เหยื่อถ่ายคลิปวิดีโออนาจารหรือคลิปถอดเสื้อผ้า จากนั้น ใช้คลิปดังกล่าวเป็นเครื่องมือในการแบล็กเมลเรียกค่าไถ่ หากไม่ยอมจ่ายเงินก็จะนำคลิปไปเผยแพร่ พฤติการณ์ของมิจฉาชีพเริ่มต้นด้วยการใช้เทคนิควิศวกรรมสังคม โดยแอบอ้างเป็นบุคคลหรือหน่วยงานที่น่าเชื่อถือ ผ่านช่องทางออนไลน์ต่าง ๆ เช่น LINE Messenger Facebook Instagram TikTok หรือ อีเมล เมื่อสามารถสร้างความไว้วางใจได้ในระดับหนึ่ง มิจฉาชีพจะหลอกเหยื่อว่าจำเป็นต้องมีการ “ทดสอบ” หรือ “ยืนยันตัวตน” ด้วยการถ่ายคลิปวิดีโอที่มีลักษณะสุ่มเสี่ยง เช่น ถอดเสื้อ ถอดกางเกง หรือทำท่าทางอนาจาร โดยอ้างว่า จะนำไปใช้ในการพิจารณารับทุน หรือเพื่อทดสอบความกล้า ความเหมาะสมกับตำแหน่งงานหลังจากได้ชมคลิปวิดีโอ มิจฉาชีพจะเปิดเผยธาตุแท้ทันที โดยใช้คลิปนั้นเป็นเครื่องมือในการข่มขู่เรียกค่าไถ่ หากเหยื่อไม่ยอมจ่ายเงิน มิจฉาชีพจะขู่ว่าจะนำคลิปไปเผยแพร่ในสื่อสังคมออนไลน์ ส่งให้เพื่อน ผู้ปกครอง หรือโรงเรียนของเหยื่อ การกระทำนี้ไม่เพียงสร้างความเสียหายทางการเงิน แต่ยังส่งผลกระทบอย่างร้ายแรงต่อสุขภาพจิตและชื่อเสียงของนักเรียนและเยาวชนที่ตกเป็นเหยื่ออีกด้วย

ที่มา : Ch7HDNews. ประเด็นเด็ด 7 สี (2568, กรกฎาคม 7) เอาความฝันมาหากิน ! มิจฉาชีพหลอก นักศึกษาได้ทุนเรียนต่อนอกhttps://www.youtube.com/watch?v=13YLRAd69mU

ใบงานที่ 2.3 (ต่อ)
เรื่อง วิเคราะห์กลลวงบนโลกไซเบอร์

กรณีศึกษา	เทคนิคกลลวงที่ใช้	วิธีป้องกันที่ควรทำ
กรณีศึกษาที่ 1 มิจฉาชีพหลอกผู้สูงอายุ วัย 70 ปี สูญเงินกว่า 70,000 บาท ด้วยกลโกง “บำเหน็จยังชีพ” ผ่านแอปพลิเคชันปลอม		
กรณีศึกษาที่ 2 กลโกง “พัสดุมีปัญหา” หลอกติดตั้งแอปพลิเคชัน ดูดเงินจากบัญชีกว่า 450,000 บาท		
กรณีศึกษาที่ 3 กลโกงมิจฉาชีพอ้าง “ให้ทุนการศึกษา” หลอกถ่ายคลิปโป๊เรียกค่าไถ่		

แนวคำตอบใบงานที่ 2.3
เรื่อง วิเคราะห์กลลวงบนโลกไซเบอร์

กรณีศึกษา	เทคนิคกลลวงที่ใช้	วิธีป้องกันที่ควรทำ
กรณีศึกษาที่ 1 มิจฉาชีพหลอกผู้สูงอายุ วัย 70 ปี สูญเงินกว่า 70,000 บาท ด้วยกลโกง “บำเหน็จยังชีพ” ผ่านแอปพลิเคชันปลอม	- การสร้างเรื่องราวสมมติ - การหลอกลวงแบบฟิชชิ่ง - มัลแวร์ - การหลบเลี่ยงการตรวจสอบ - การใช้บัญชีม้า	**ไม่โหลด** ตรวจสอบข้อมูลก่อน ดำเนินการแจ้งสายด่วน ตำรวจไซเบอร์ 1441
กรณีศึกษาที่ 2 กลโกง “พัสดุมีปัญหา” หลอกติดตั้งแอปพลิเคชัน ดูดเงินจากบัญชีกว่า 450,000 บาท	- การหลอกลวงแบบฟิชชิ่ง - มัลแวร์ - การหลบเลี่ยงการตรวจสอบ - การใช้บัญชีม้า	**ไม่กด** ตรวจสอบข้อมูลก่อน ดำเนินการแจ้งสายด่วน ตำรวจไซเบอร์ 1441
กรณีศึกษาที่ 3 กลโกงมิจฉาชีพอ้าง “ให้ทุนการศึกษา” หลอกถ่ายคลิปโป๊เรียกค่าไถ่	- การสร้างเรื่องราวสมมติ - การแอบอ้างตัวตน - การข่มขู่เรียกค่าไถ่ - การแจ้งความล่วงหน้า	**ไม่ให้** ตรวจสอบข้อมูลก่อน ดำเนินการแจ้งสายด่วน ตำรวจไซเบอร์ 1441

หน่วยการเรียนรู้ที่ 2 การป้องกันภัยไซเบอร์ขั้นพื้นฐาน
แผนการจัดกิจกรรม 2.4 เรื่อง ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ

ระยะเวลา 45 นาที

สาระสำคัญ

ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ เทคนิคและวิธีการตรวจสอบข้อมูลผู้ติดต่อทางออนไลน์เบื้องต้น การตรวจสอบร้านค้าอย่างปลอดภัย และแนวทางการปฏิบัติเมื่อสงสัยว่าตกเป็นเหยื่อ

จุดประสงค์

เพื่อให้ผู้เข้ารับการอบรมสามารถใช้เทคนิคและวิธีการตรวจสอบข้อมูลผู้ติดต่อ และร้านค้าออนไลน์เบื้องต้นได้อย่างปลอดภัย

ขอบข่ายเนื้อหา

1. เทคนิค และวิธีการตรวจสอบข้อมูลผู้ติดต่อทางออนไลน์เบื้องต้น
2. การตรวจสอบร้านค้าอย่างปลอดภัย
3. แนวทางการปฏิบัติเมื่อสงสัยว่าตกเป็นเหยื่อ

สื่อการเรียนรู้

1. ใบความรู้ที่ 2.4 เรื่อง ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ
2. คลิปวิดีโอ เรื่อง ถูกหลอก โดนโกงออนไลน์ อย่าตกใจ โทรหา AOC 1441

วัสดุอุปกรณ์

1. เครื่องคอมพิวเตอร์/โน้ตบุ๊ค/แท็บเล็ต/โทรศัพท์มือถือ เชื่อมต่ออินเทอร์เน็ต
2. กระดาษปรู๊ฟ
3. ปากกาเคมี

ขั้นตอนการจัดกิจกรรม

1. วิทยากรชวนคุยในประเด็น เมื่อพบเจอสถานการณ์ถูกมิจฉาชีพหลอกลวงควรทำอย่างไร
2. วิทยากรให้ผู้เข้ารับการอบรมเรียนรู้จากสื่อคลิปวิดีโอ เรื่อง ถูกหลอก โดนโกงออนไลน์ อย่าตกใจ โทรหา AOC 1441

https://dg.th/rh9bdiu6lx

และศึกษาใบความรู้ที่ 2.4 เรื่อง ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ

3. วิทยากรมอบหมายให้ผู้เข้ารับการอบรมทำใบงานที่ 2.4 เรื่อง ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ
4. วิทยากรเลือกผู้เข้ารับการอบรมนำเสนอใบงาน 5 - 10 คน (สามารถปรับเปลี่ยนได้ตามความเหมาะสม) แล้วให้ผู้เข้ารับการอบรมแลกเปลี่ยนเรียนรู้
5. วิทยากรและผู้เข้ารับการอบรมสรุปองค์ความรู้ร่วมกัน

การวัดและประเมินผล

1. ใบงาน
2. การสังเกต

ใบความรู้ที่ 2.4
เรื่อง ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ

เทคนิคและวิธีการตรวจสอบข้อมูลผู้ติดต่อทางออนไลน์เบื้องต้น

การตรวจสอบข้อมูลเบื้องต้นและการยืนยันตัวตนของผู้ติดต่อทางออนไลน์เป็นสิ่งสำคัญที่ช่วยป้องกันการถูกหลอกลวงและรักษาความปลอดภัยในโลกไซเบอร์ โดยมีเทคนิคและวิธีการตรวจสอบข้อมูล ดังนี้

1. ตรวจสอบข้อมูลประวัติและรูปภาพ ตรวจสอบว่าชื่อและรูปภาพในประวัติดูเหมือนถูกต้องและไม่ใช่ข้อมูลที่ถูกสร้างขึ้นหรือขโมยมาจากแหล่งอื่นและประวัติการใช้งาน ดูประวัติการโพสต์ หรือกิจกรรมอื่น ๆ ของผู้ติดต่อว่ามีความสอดคล้องกันหรือไม่

2. การตรวจสอบด้วยการค้นหาข้อมูล ค้นหาชื่อและรูปภาพในอินเทอร์เน็ต ใช้เครื่องมือค้นหารูปภาพ เช่น Google Image เพื่อดูว่ารูปภาพในโปรไฟล์นั้นถูกใช้ในที่อื่น ๆ หรือไม่ รวมถึงค้นหาประวัติออนไลน์ใช้ชื่อและข้อมูลอื่น ๆ ของผู้ติดต่อในการค้นหาเพิ่มเติมในอินเทอร์เน็ต เพื่อตรวจสอบว่าเขาเป็นใครและมีประวัติอย่างไร

3. สอบถามข้อมูลเพิ่มเติม ถามคำถามเฉพาะเจาะจง สอบถามข้อมูลที่ผู้ติดต่อควรจะรู้ หากผู้ติดต่อมีปฏิกิริยาตอบสนองที่แปลกประหลาดหรือลังเลใจ นั่นอาจเป็นสัญญาณที่ควรระวัง และตรวจสอบกับแหล่งข้อมูลที่เชื่อถือได้ หากผู้ติดต่ออ้างว่าเป็นตัวแทนจากองค์กรหรือบริษัท ลองติดต่อองค์กรโดยตรง เพื่อยืนยันข้อมูล

4. ใช้เทคโนโลยีเพื่อช่วยตรวจสอบ การตรวจสอบด้วย 2 ขั้นตอน (Two-Factor Authentication: 2FA) หากเป็นการยืนยันตัวตนในการเข้าถึงบัญชี ควรใช้ระบบการยืนยันตัวตนแบบ 2 ขั้นตอน และโปรแกรมป้องกันการหลอกลวง (Anti-phishing tools) ใช้เครื่องมือป้องกันการหลอกลวงที่ติดตั้งในเบราว์เซอร์หรืออุปกรณ์ เพื่อช่วยตรวจสอบความถูกต้องของลิงก์และอีเมลที่ได้รับ

5. รักษาความเป็นส่วนตัวและไม่เปิดเผยข้อมูลสำคัญ หลีกเลี่ยงการเปิดเผยข้อมูลส่วนบุคคล อย่าเปิดเผยข้อมูลส่วนตัว เช่น รหัสผ่าน หรือข้อมูลทางการเงินให้กับใครที่คุณไม่แน่ใจ และไม่คลิกลิงก์ที่น่าสงสัย รวมถึงระวังการคลิกลิงก์ในอีเมลหรือข้อความที่ไม่ได้ร้องขอ โดยเฉพาะหากมาจากแหล่งที่ไม่คุ้นเคย

6. การใช้วิจารณญาณและการระมัดระวัง อย่ารีบร้อนในการตัดสินใจหากผู้ติดต่อพยายามกดดันให้คุณทำอะไรอย่างรวดเร็ว เช่น ให้ข้อมูลส่วนตัวหรือโอนเงิน ให้ชะลอการตัดสินใจและตรวจสอบข้อมูลเพิ่มเติมก่อน การใช้เทคนิคและวิธีการเหล่านี้สามารถช่วยเพิ่มความปลอดภัยในการติดต่อสื่อสารและยืนยันตัวตนทางออนไลน์ได้อย่างมีประสิทธิภาพ

ใบความรู้ที่ 2.4 (ต่อ)
เรื่อง ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ

การตรวจสอบร้านค้าอย่างปลอดภัย

การซื้อสินค้าออนไลน์มีความสะดวกสบาย แต่ก็มาพร้อมกับความเสี่ยง จากสถิติการแจ้งความออนไลน์เมื่อเดือนมิถุนายน 2568 รายงานว่า “ภัยการหลอกลวงซื้อขายสินค้าหรือบริการแบบไม่เป็นกระบวนการ” เป็นประเภทคดีออนไลน์ที่มีจำนวนมากเป็นอันดับที่ 1 ดังนั้น ความระมัดระวังในการซื้อสินค้าออนไลน์ และการตรวจสอบร้านค้าอย่างปลอดภัยจึงเป็นสิ่งสำคัญ คำแนะนำที่ควรปฏิบัติ มีดังนี้

1. เลือกซื้อกับร้านค้าที่มีที่อยู่และข้อมูลผู้ขายที่ชัดเจน สิ่งหนึ่งที่สำคัญในการเลือกซื้อสินค้าและบริการออนไลน์คือความน่าเชื่อถือของร้าน ซึ่งหากร้านใดที่ไม่มีที่อยู่ของร้านที่ชัดเจน หรือไม่สามารถระบุตัวตนและติดต่อผู้ขายได้ ก็เป็นไปได้ว่าอาจเป็นการหลอกลวง

2. ดูประวัติการซื้อหรือคะแนนจากผู้ซื้อ ประวัติการซื้อสินค้าก็เป็นส่วนหนึ่งในการนำมาพิจารณาว่าร้านค้าดังกล่าวเข้าข่ายหลอกลวงหรือเอารัดเอาเปรียบลูกค้าหรือไม่ ซึ่งหากมีลูกค้าเข้ามาแสดงความคิดเห็นด้านลบอาจต้องดูข้อมูลสินค้าให้ชัดเจนมากขึ้น หรือหาร้านอื่นมาเปรียบเทียบข้อมูล

3. ขอดูรูปถ่ายจริง การขอดูภาพเพิ่มเติมเป็นสิทธิ์ของลูกค้า ซึ่งหากผู้ขายไม่ยินยอมให้ดูรูปภาพเพิ่มเติมหรือไม่ให้ดูรายละเอียดเชิงลึก อาจสันนิษฐานได้ว่าสินค้าอาจมีตำหนิ หรือไม่ตรงกับข้อมูลที่แสดงบนหน้าเว็บไซต์

4. วิธีการส่งและวันที่จะได้รับของ นอกจากข้อมูลของสินค้าแล้ว การจัดส่งก็เป็นส่วนสำคัญในการเลือกซื้อสินค้าออนไลน์ ซึ่งบางครั้งการจัดส่งไม่ได้มาตรฐานจะทำให้สินค้าชำรุดหรือสูญหายได้

5. ขอหลักฐานการส่งสินค้า เมื่อชำระเงินเรียบร้อยแล้วควรติดตามการจัดส่งจากผู้ซื้อ หรือขอดูหลักฐานการส่งสินค้า เพื่อยืนยันว่าผู้ขายได้จัดส่งสินค้าให้

6. บันทึกการสนทนาการซื้อขายไว้เป็นหลักฐาน หากเกิดปัญหาการบันทึกข้อมูลการสนทนาสามารถใช้เป็นหลักฐานในการเอาผิดกับร้านค้าที่หลอกลวงหรือเอาเปรียบได้ ซึ่งสำคัญมากในการติดตามตัวผู้ขายมารับโทษหรือคืนเงินค่าสินค้า

7. บันทึกภาพเพจร้าน ภาพหน้าร้านออนไลน์ หรือภาพการโพสต์ขายสินค้า นอกจากการบันทึกการสนทนาแล้ว การบันทึกภาพเพจร้าน ภาพหน้าร้านออนไลน์ หรือภาพการโพสต์ขายสินค้าก็สามารถใช้เป็นหลักฐานเอาผิดกับผู้ขายได้ ซึ่งบางครั้งหลังการกระทำความผิดผู้ขายอาจลบข้อมูล ข้อมูลนี้จึงเป็นข้อมูลสำคัญในการเอาผิดกับผู้ขาย

8. แจ้งความกับตำรวจหากถูกฉ้อโกงหรือเอารัดเอาเปรียบจากผู้ขาย ในขั้นตอนนี้จะเป็นขั้นตอนที่สำคัญในการเอาผิดกับผู้ขายที่หลอกลวง โดยใช้หลักฐานที่กล่าวมาในข้างต้นประกอบเป็นคำร้องในการแจ้งความเอาผิดกับผู้กระทำความผิด

ใบความรู้ที่ 2.4 (ต่อ)
เรื่อง ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ

แนวทางการปฏิบัติเมื่อสงสัยว่าตกเป็นเหยื่อ

1. รีบตัดการเชื่อมต่อทันที เมื่อสงสัยว่าถูกควบคุมโทรศัพท์ ให้ปิดอินเทอร์เน็ต (ปิด Wi-Fi และ Mobile Data) หรือปิดเครื่องโทรศัพท์ทันที เพื่อตัดการเชื่อมต่อกับมิจฉาชีพ (กรณีถูกหลอกติดตั้งมัลแวร์)

2. ติดต่อธนาคารทันที โทรแจ้งธนาคารเจ้าของบัญชีทุกแห่งที่เกี่ยวข้อง เพื่อขออายัดบัญชีและระงับการทำธุรกรรม (กรณีเกี่ยวข้องกับการโอนเงิน)

3. รวบรวมหลักฐาน เก็บภาพหน้าจอการสนทนา เบอร์โทรศัพท์ ลิงก์ที่ได้รับ หรือข้อมูลอื่น ๆ ที่เกี่ยวข้องไว้ให้ได้มากที่สุด โดยเฉพาะอย่างยิ่ง หลักฐานการข่มขู่หรือการขอข้อมูล/คลิปส่วนตัว

4. แจ้งความออนไลน์หรือที่สถานีตำรวจ

4.1 ติดต่อ ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ โทร 1441 ซึ่งจะช่วยดำเนินการอายัดบัญชีเบื้องต้นและประสานงานกับหน่วยงานที่เกี่ยวข้องภายใน 72 ชั่วโมง เพื่อให้สามารถไปแจ้งความที่สถานีตำรวจในท้องที่เพื่อดำเนินคดีต่อไป

4.2 เข้าแจ้งความผ่าน www.thaipoliceonline.com

4.3 ข้อสำคัญ หากมิจฉาชีพแจ้งความไว้ล่วงหน้า เช่น กรณี 1441 ซ้ำซ้อน ให้แจ้งเจ้าหน้าที่ตำรวจ ณ สถานีตำรวจ ที่ไปแจ้งความ เพื่อให้เจ้าหน้าที่ตรวจสอบและดำเนินการแก้ไขความผิดพลาดในระบบ

5. นำโทรศัพท์ส่งตรวจสอบ หากเป็นไปได้ ควรส่งโทรศัพท์มือถือที่ถูกควบคุมให้ผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ตรวจสอบ เพื่อเก็บพยานหลักฐานทางดิจิทัลและทำการ Factory Reset (คืนค่าโรงงาน) เพื่อล้างมัลแวร์ทั้งหมด

6. แจ้งผู้ให้บริการเครือข่ายโทรศัพท์ แจ้งปัญหาที่เกิดขึ้นกับผู้ให้บริการเครือข่าย เพื่อขอคำแนะนำเพิ่มเติม

ใบความรู้ที่ 2.4 (ต่อ)
เรื่อง ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ

ที่มา : https://www.facebook.com/photo.php?fbid=481186564420200&id=100075865826566&set=a.179615524577307

ที่มา : https://www.ktc.co.th/en/article/knowledge/salary-man/phishing

ใบงานที่ 2.4
เรื่อง ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ

คำชี้แจง ให้ผู้เข้ารับการอบรมตอบคำถาม ตามความเข้าใจพอสังเขป

1. จงอธิบายเทคนิคและวิธีการตรวจสอบผู้ติดต่อทางออนไลน์ตามหัวข้อที่กำหนด

1.1 การตรวจสอบข้อมูลโปรไฟล์

1.2 การตรวจสอบด้วยการค้นหาข้อมูล

1.3 การใช้วิจารณญาณ

2. ให้ระบุสิ่งที่ควรปฏิบัติในการซื้อสินค้าออนไลน์อย่างปลอดภัยอย่างน้อย 4 ข้อ

2.1

2.2

2.3

2.4

ใบงานที่ 2.4 (ต่อ)
เรื่อง ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ

3. จงเรียงลำดับขั้นตอนการปฏิบัติเมื่อสงสัยว่าตกเป็นเหยื่อมิจฉาชีพออนไลน์

3.1

3.2

3.3

3.4

3.5

4. สรุปความรู้และใจความสำคัญของเรื่อง “ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ” มาพอสังเขป

แนวคำตอบใบงานที่ 2.4
เรื่อง ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ

1. จงอธิบายเทคนิคและวิธีการตรวจสอบผู้ติดต่อทางออนไลน์ตามหัวข้อที่กำหนด

1.1 การตรวจสอบข้อมูลโปรไฟล์
- 1) ตรวจสอบชื่อและรูปภาพว่าดูถูกต้องและไม่ใช่ข้อมูลที่ถูกปลอมแปลง
- 2) ดูประวัติการโพสต์และกิจกรรมต่าง ๆ ว่ามีความสอดคล้องกันหรือไม่

1.2 การตรวจสอบด้วยการค้นหาข้อมูล
- 1) ค้นหาชื่อและรูปภาพในอินเทอร์เน็ต เช่น Google Image เพื่อดูว่าถูกนำไปใช้ในที่อื่นหรือไม่
- 2) ค้นหาประวัติออนไลน์เพิ่มเติมเพื่อตรวจสอบว่าผู้ติดต่อเป็นใครและมีประวัติอย่างไร

1.3 การใช้วิจารณญาณ
- 1) อย่ารีบร้อนในการตัดสินใจ โดยเฉพาะเมื่อถูกกดดันให้โอนเงินหรือให้ข้อมูลส่วนตัวอย่างเร่งด่วน
- 2) ชะลอการตัดสินใจและตรวจสอบข้อมูลเพิ่มเติมให้แน่ใจก่อนเสมอ

2. ให้ระบุสิ่งที่ควรปฏิบัติในการซื้อสินค้าออนไลน์อย่างปลอดภัยอย่างน้อย 4 ข้อ

2.1 เลือกร้านค้าที่มีที่อยู่และข้อมูลผู้ขายที่ชัดเจน
2.2 ตรวจสอบประวัติการซื้อหรือคะแนนจากผู้ซื้อคนอื่น ๆ
2.3 ขอดูรูปถ่ายสินค้าจริงเพิ่มเติม หากผู้ขายไม่ยินยอมอาจสันนิษฐานได้ว่าสินค้ามีตำหนิหรือไม่ตรงปก
2.4 บันทึกการสนทนาและภาพเพจร้านค้าไว้เป็นหลักฐานเผื่อเกิดปัญหา

3. จงเรียงลำดับขั้นตอนการปฏิบัติเมื่อสงสัยว่าตกเป็นเหยื่อมิจฉาชีพออนไลน์

3.1 รีบตัดการเชื่อมต่ออินเทอร์เน็ต หรือปิดเครื่องโทรศัพท์ทันที
3.2 ติดต่อธนาคารเจ้าของบัญชีทุกแห่งเพื่อขออายัดบัญชี
3.3 รวบรวมหลักฐานต่าง ๆ ให้ได้มากที่สุด เช่น ภาพหน้าจอการสนทนา หรือเบอร์โทรศัพท์
3.4 ติดต่อสายด่วน 1441 เพื่อแจ้งความออนไลน์หรือไปสถานีตำรวจในพื้นที่
3.5 นำโทรศัพท์ส่งตรวจสอบโดยผู้เชี่ยวชาญเพื่อเก็บหลักฐานและทำการคืนค่าโรงงาน
3.6 แจ้งผู้ให้บริการเครือข่ายโทรศัพท์เพื่อขอคำแนะนำเพิ่มเติม

4. สรุปความรู้และใจความสำคัญของเรื่อง “ช่องทางการตรวจสอบมิจฉาชีพออนไลน์และการแจ้งเหตุ” มาพอสังเขป

“อยู่ในดุลพินิจ”

หน่วยการเรียนรู้ที่ 3 วิถีชีวิตบนโลกดิจิทัล
แผนการจัดกิจกรรม 3.1 เรื่อง การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)

ระยะเวลา 1 ชั่วโมง 30 นาที

สาระสำคัญ

การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy) และการมีมารยาทและจริยธรรมบนโลกดิจิทัล หมายถึง ความตระหนักรู้ถึงปัญหา เห็นใจผู้ตกเป็นเหยื่อการกลั่นแกล้งบนโลกไซเบอร์ และเกิดจิตสำนึกในการใช้สื่อดิจิทัลอย่างรับผิดชอบ

จุดประสงค์

1. เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบาย ความหมาย ความสำคัญ บอกวิธีการของการเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy) และการมีมารยาทและจริยธรรมบนโลกดิจิทัลได้
2. เพื่อให้ผู้เข้ารับการอบรมสามารถปฏิบัติตนตามวิธีการเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy) มีมารยาทและจริยธรรมบนโลกดิจิทัลได้อย่างเหมาะสม
3. เพื่อให้ผู้เข้ารับการอบรมเกิดความตระหนักรู้ถึงปัญหา เห็นใจผู้ตกเป็นเหยื่อการกลั่นแกล้งบนโลกไซเบอร์ และเกิดจิตสำนึกใช้สื่อดิจิทัลอย่างรับผิดชอบ

ขอบข่ายเนื้อหา

1. ความหมายและความสำคัญของการเอาใจเขามาใส่ใจเราทางดิจิทัล
2. วิธีการเอาใจเขามาใส่ใจเราทางดิจิทัล
3. มารยาทและจริยธรรมบนโลกดิจิทัล
4. การกลั่นแกล้งบนโลกออนไลน์

สื่อการเรียนรู้

1. PowerPoint บรรยาย เรื่อง การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)

https://shorturl.at/VzaGq

2. ใบความรู้ที่ 3.1 เรื่อง การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)
3. สื่อคลิปวิดีโอ เรื่อง การระรานทางไซเบอร์ Cyberbullying

https://dg.th/30t6i2aol5

วัสดุอุปกรณ์

1. เครื่องคอมพิวเตอร์/โน้ตบุ๊ค/แท็บเล็ต/โทรศัพท์มือถือ เชื่อมต่ออินเทอร์เน็ต
2. กระดานไวท์บอร์ด
3. กระดาษปรู๊ฟ
4. ปากกาเคมี

ขั้นตอนการจัดกิจกรรม

1. วิทยากรบรรยาย เรื่อง การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy) พร้อมทั้งให้ผู้เข้ารับการอบรมศึกษาเนื้อหาจากใบความรู้ที่ 3.1 เรื่อง การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)
2. ผู้เข้ารับการอบรมเรียนรู้จากสื่อคลิปวิดีโอ เรื่อง การระรานทางไซเบอร์ Cyberbullying แล้วร่วมกันสรุปและแลกเปลี่ยนเรียนรู้

3. กิจกรรม ใบงานที่ 3.1 วิเคราะห์กรณีตัวอย่าง ฝึกทักษะ “เข้าใจตัวเรา เข้าใจผู้อื่น”
   3.1 แบ่งกลุ่มผู้เข้ารับการอบรมเป็นกลุ่มย่อย จำนวน 6 กลุ่ม (สามารถเปลี่ยนแปลงได้ตามความเหมาะสม)
   3.2 ให้แต่ละกลุ่มจับฉลาก กรณีตัวอย่าง เพื่อวิเคราะห์สถานการณ์ และสรุปเป็นแผนผังความคิดเขียนลงในกระดาษปรู๊ฟ ตามประเด็น ดังนี้
   1) ถ้าเหตุการณ์นี้เกิดขึ้นกับเรา หรือคนในครอบครัวของเรา เราจะรู้สึกอย่างไร ?
   2) หากเราเป็นเหยื่อ เราจะจัดการความรู้สึกและแก้ไขปัญหาของเราอย่างไร ?
   3) เราจะปฏิบัติตัวเพื่อลดปัญหาได้อย่างไร ?

   ตามกรณีตัวอย่างต่อไปนี้
   1) กรณีตัวอย่าง “คำล้อเลียนฆ่าคนได้” รัศมีแข แชร์ประสบการณ์โดนบูลลี่ “ผิวดำ ตัวใหญ่”
   2) กรณีตัวอย่าง “มุก วรนิษฐ์ ดาราดัง โดนบูลลี่จากโซเชียลจนเป็นโรควิตกกังวลเฉียบพลันเครียดถึงขั้นพบจิตแพทย์”
   3) กรณีตัวอย่าง “พลอยชมพู เล่าเหตุการณ์” ถูกนำภาพไปตัดต่อและเผยแพร่จนมีผลกระทบทางจิตใจ
   4) กรณีตัวอย่าง “ยิปซี ยิปโซ เปิดใจต้องทนทุกข์นับ 10 ปี” จากการเปรียบเทียบบนโลกออนไลน์จนไม่สนิทใจต่อกัน
   5) กรณีตัวอย่าง แม่ค้าทุเรียนแจ้งจับ “คุณเจมส์” ลวงส่งภาพลับก่อนข่มขู่เรียกเงิน 50,000 บาท
   6) กรณีตัวอย่าง รู้สำนึกผิดแต่สายไป “บอล หนองขาว” สำนึกผิดไลฟ์สดด่าตำรวจ
4. จากสถานการณ์ดังกล่าวให้แต่ละกลุ่มนำเสนอ แลกเปลี่ยนเรียนรู้ และร่วมกันสรุป วิทยากรอธิบายเพิ่มเติม

การวัดและประเมินผล

1. ใบงาน / ชิ้นงาน / ผลงาน
2. การสังเกต

ใบความรู้ที่ 3.1
เรื่อง การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)

การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)

1. ความหมายและความสำคัญของการเอาใจเขามาใส่ใจเราทางดิจิทัล

การเอาใจเขามาใส่ใจเราทางดิจิทัล หมายถึง ความสามารถในการเข้าใจความรู้สึก เห็นอกเห็นใจ และให้ความเคารพต่อผู้อื่นในโลกออนไลน์ ทั้งผ่านข้อความ การสนทนา และการกระทำบนสื่อดิจิทัล

ความสำคัญของการเอาใจเขามาใส่ใจเรา (Digital Empathy) ในเด็กและวัยรุ่นส่วนใหญ่มักไม่ให้ความสำคัญในการเอาใจเขามาใส่ใจเรา เพราะเป็นช่วงวัยที่ยังขาดทักษะในการสื่อสาร มีวุฒิภาวะไม่เพียงพอ และมีความคึกคะนอง จึงอาจแสดงความคิดเห็นที่ไม่เหมาะสมต่อผู้อื่น แต่วัยผู้ใหญ่ก็สามารถพบได้เช่นกัน หากบุคคลนั้นขาดวิจารณญาณและความยั้งคิด ซึ่งการขาดการเอาใจเขามาใส่ใจเราอาจนำไปสู่ปัญหาต่าง ๆ เช่น การเผยแพร่ข้อมูลเท็จและข่าวปลอม การโพสต์ข้อมูลเสียดสี หรือล้อเลียนผู้อื่น การสร้างข้อมูลที่ทำให้เข้าใจผิดโดยเชื่อมโยงเรื่องราวที่ไม่เกี่ยวข้องกัน การแอบอ้างชื่อบุคคลหรือองค์กรเพื่อดัดแปลงข้อมูล ตัดต่อ และเปลี่ยนแปลงข้อเท็จจริง ทำให้เกิดความสับสนและเข้าใจผิด การกลั่นแกล้งในโลกออนไลน์ (Cyberbullying) โดยการใช้คำหยาบคายคุกคาม ข่มขู่ ดูหมิ่นผู้อื่น การกระตุ้นให้เกิดความเกลียด การใช้ความรุนแรง หรือทำผิดกฎหมาย การเหยียดเชื้อชาติ เพศ และสีผิว การใช้ข้อความ รูปภาพ หรือวิดีโอประจานให้อับอาย การแอบอ้างตัวตนของผู้อื่นและสร้างบัญชีปลอม การล่อลวงและการเกาะติดชีวิตออนไลน์ของผู้อื่น (Cyber Stalking) บางครั้งการกระทำเหล่านี้อาจเกิดขึ้นโดยที่ไม่เจตนา เช่น การพิมพ์บ่นส่วนตัว แต่เป็นข้อความที่ส่งเสริมให้เกิดความขัดแย้ง การพูดซ้ำเรื่องที่จะทำให้เกิดประเด็น หรือแม้แต่การแชร์ข้อความที่มีความรุนแรง ซึ่งอาจทำให้เกิดผลกระทบต่อสภาพจิตใจและร่างกายของคนใดคนหนึ่ง เช่น การเห็นคุณค่าในตัวเองลดลง ซึมเศร้า วิตกกังวล การเรียนและการทำงานแย่ลง หรืออาจส่งผลกระทบต่อสังคมในวงกว้าง

2. วิธีการเอาใจเขามาใส่ใจเราทางดิจิทัล

ความเห็นอกเห็นใจเป็นทักษะที่ฝึกฝนได้ โดยปฏิบัติต่อผู้อื่นเหมือนที่ต้องการให้ผู้อื่นปฏิบัติต่อตนเอง นึกไว้เสมอว่าไม่มีใครชอบให้คนอื่นทำไม่ดีกับตนเอง จึงต้องทำดีต่อผู้อื่นด้วย ซึ่งวิธีการสร้างการเอาใจเขามาใส่ใจเราทางดิจิทัล สามารถทำได้หลายวิธี ดังนี้

2.1 เคารพความเป็นส่วนตัวของผู้อื่น ไม่โพสต์หรือแท็กรูปของผู้อื่นก่อนได้รับการอนุญาต โดยเฉพาะภาพที่อาจทำให้ผู้อื่นได้รับความอับอาย

2.2 ไม่บุกรุกหรือเข้าถึงข้อมูลส่วนบุคคลของผู้อื่นโดยไม่ได้รับอนุญาต

2.3 ไม่ส่งข้อความไร้สาระหรือไม่เกี่ยวข้องกับเนื้อหาในช่องทางสาธารณะที่รบกวนผู้ใช้งานคนอื่น

2.4 ไม่ใช้ภาษาหยาบคาย ข่มขู่หรือคุกคามผู้อื่น ไม่ส่งข้อความหรือภาพลามกอนาจารให้ผู้อื่น

2.5 ไม่สร้างข้อมูลเท็จ ควรตรวจสอบความถูกต้องของข้อมูลที่ได้รับก่อนเสมอ และไม่ส่งต่อข้อมูลที่ไม่ทราบที่มาชัดเจน

ใบความรู้ที่ 3.1 (ต่อ)
เรื่อง การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)

2.6 อ่านทบทวนหลาย ๆ รอบก่อนกดโพสต์ และระมัดระวังการโพสต์รหัสผ่าน ข้อความ รูปภาพ หรือวิดีโอส่วนตัวลงในสื่อโซเชียล เพราะแม้จะลบทิ้งแล้ว แต่เมื่อเผยแพร่สู่สาธารณะแล้วอาจมีคนบันทึก (Save) ข้อมูลเก็บไว้ และอาจทำให้เกิดปัญหาตามมาในอนาคต

2.7 การกระทำบางอย่างด้วยความไม่ตั้งใจหรือรู้เท่าไม่ถึงการณ์ ได้แก่ การล็อกอินบัญชีของเพื่อนเพื่อโพสต์ข้อความหรือรูปภาพกลั่นแกล้ง การตัดต่อภาพแล้วนำไปโพสต์ให้เสียหาย ถือเป็นการเผยแพร่ข้อมูลที่เป็นเท็จ ซึ่งมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

2.8 ยอมรับและเคารพความแตกต่างทางความคิดเห็น เพศ และเชื้อชาติ โลกออนไลน์เป็นสถานที่รวมผู้คนมากมายจากทั่วโลก แต่ละคนมีลักษณะภายนอกและมุมมองความคิดที่ต่างกัน ควรให้เกียรติ และรับฟังความคิดเห็นของผู้อื่น

2.9 สอนให้เด็กเรียนรู้และเข้าใจความรู้สึกของผู้อื่น ซึ่งจะช่วยให้เข้าใจความรู้สึกของคนอื่น ทั้งในชีวิตจริงและในโลกออนไลน์ได้ดีขึ้น

2.10 ไม่ตอบโต้การกลั่นแกล้งหรือระรานกลับด้วยวิธีการเดียวกัน เพราะจะยิ่งเพิ่มความรุนแรงของเหตุการณ์มากยิ่งขึ้น ควรใช้การปิดกั้น (Block) แทน เพื่อไม่ให้ผู้ที่ระรานสามารถติดต่อ โพสต์ หรือกลั่นแกล้งได้

2.11 เมื่อถูกกลั่นแกล้งในโลกออนไลน์ ควรบอกบุคคลที่ไว้ใจเพื่อขอความช่วยเหลือ ในกรณีถูกข่มขู่คุกคาม หรือแอบอ้างตัวตน ให้เก็บรวบรวมข้อมูลของผู้กระทำและเหตุการณ์ เพื่อแจ้งความดำเนินคดี

ใบความรู้ที่ 3.1 (ต่อ)
เรื่อง การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)

จะเห็นได้ว่า Digital Empathy ไม่ใช่แค่การ “เข้าใจผู้อื่น” แต่ยังเป็นการ “แสดงออกอย่างเหมาะสม” ผ่านการสื่อสารในสื่อออนไลน์ เป็นทักษะสำคัญของพลเมืองดิจิทัลในศตวรรษที่ 21

Checklist Digital Empathy

ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ใบความรู้ที่ 3.1 (ต่อ)
เรื่อง การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)

3. มารยาทและจริยธรรมบนโลกดิจิทัล

3.1 **มารยาทดิจิทัล (Digital Etiquette)** หมายถึง พฤติกรรมที่เหมาะสม สุภาพ และให้เกียรติผู้อื่น เมื่อใช้งานเทคโนโลยีดิจิทัล เช่น การพิมพ์คุย การแสดงความคิดเห็น หรือการประชุมออนไลน์

3.2 **จริยธรรมดิจิทัล (Digital Ethics)** หมายถึง หลักคุณธรรมและความถูกต้องในการใช้เทคโนโลยีสารสนเทศ ไม่เอาเปรียบผู้อื่น ไม่เผยแพร่ข้อมูลที่ก่อให้เกิดความเสื่อมเสียต่อผู้อื่น และเคารพสิทธิของผู้ใช้งานทุกคนในโลกออนไลน์

ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ใบความรู้ที่ 3.1 (ต่อ)
เรื่อง การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)

4. การกลั่นแกล้งบนโลกออนไลน์ (Cyberbullying)

โลกในศตวรรษที่ 21 เป็นสังคมไร้พรมแดน ทั้งในแง่ของพื้นที่และเวลาที่อาศัยเทคโนโลยีผ่านช่องทางออนไลน์ ทำให้สามารถเข้าถึงข้อมูลข่าวสารและวัฒนธรรมที่แตกต่างกันของแต่ละมุมโลกได้อย่างง่ายดาย แต่ความง่ายดายเหล่านี้ได้นำมาซึ่งปัญหาที่เรียกกันทั่วไปว่าการกลั่นแกล้งบนโลกออนไลน์ ซึ่งมีการละเมิดสิทธิส่วนบุคคลในหลายรูปแบบที่แตกต่างกันออกไป

4.1 การกลั่นแกล้งบนโลกออนไลน์ คือ การกลั่นแกล้งกันโดยอาศัยเทคโนโลยีดิจิทัล ซึ่งอาจจะเกิดขึ้นได้บนโซเชียลมีเดีย แอปแชท เกมออนไลน์ และข้อความทางโทรศัพท์มือถือ เป็นพฤติกรรมที่เกิดขึ้นซ้ำ ๆ โดยมีจุดมุ่งหมายเพื่อสร้างรอยแผล ความโกรธ หรือความอับอาย ต่อผู้ที่เป็นเป้าหมาย

4.2 รูปแบบการกลั่นแกล้งบนโลกออนไลน์ที่มักพบบ่อย

1) การทำให้อับอาย สร้างความเสียหายต่อผู้ถูกกระทำ โดยส่วนใหญ่มักจะเป็นการแกล้งที่มีจุดประสงค์เพื่อสร้างความอับอาย และความเสียหายต่อบุคคลอื่นโดยเจตนา ใช้ถ้อยคำในเชิงลบ ไม่ว่าจะเป็นการด่าทอ ล้อเลียน ใส่ร้าย ขู่ทำร้าย พูดจาส่อเสียด เหยียดเพศสภาพและความเป็นชาติพันธุ์ผ่านช่องทางการสนทนาหรือบางทีโพสต์อย่างโจ่งแจ้งประจานบนสื่อสังคมสาธารณะให้ผู้ถูกกระทำได้รับความอับอายหรือใช้ถ้อยคำโจมตีให้เกิดความเสียหาย

2) การประจาน ไม่ว่าจะเป็นคลิปอนาจาร หรือคลิปที่ผู้ถูกกระทำโดนถูกรุมทำร้าย รุมแกล้ง แล้วนำคลิปไปโพสต์บนโซเชียลมีเดีย เพื่อก่อให้เกิดการแสดงความคิดเห็นที่เสียหายต่อผู้ถูกกระทำ และเผยแพร่ความรุนแรง

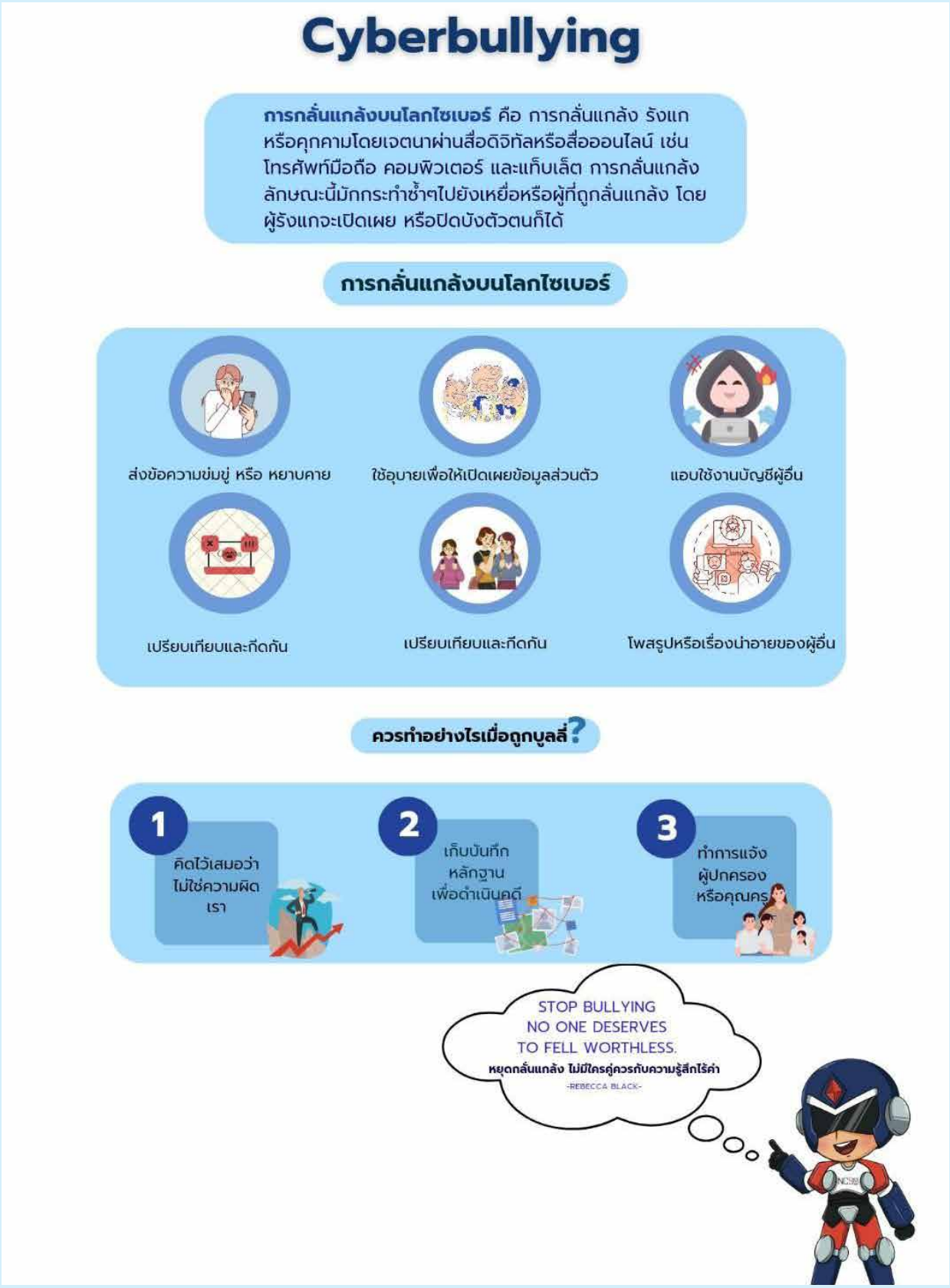
3) การแอบอ้างตัวตนของผู้อื่น การที่ให้ผู้อื่นล่วงรู้ถึงรหัสผ่านแอปพลิเคชันหลักที่ใช้ประจำหรือสื่อสังคมสาธารณะ การทำธุรกรรมในพื้นที่ออนไลน์ ต้องมีความระมัดระวังอย่างยิ่ง เพราะมีหลายกรณีที่รหัสผ่านหลุดเปิดเผยให้ผู้อื่นล่วงรู้โดยไม่เจตนา โดยการให้เพื่อนหรือคนไม่สนิทเป็นผู้สมัครแอปพลิเคชันให้ เช่น LINE Messenger Facebook และ Instagram ซึ่งอาจตกเป็นเหยื่อโดนรังแกด้วยการถูกสวมรอยใช้ Facebook ของตัวเอง

4) การแบล็กเมล์ (Blackmail) คือ การขู่เข็ญเอาเงิน รีดเอาทรัพย์ ขู่เข็ญเอาเงิน โดยผู้ไม่หวังดีมีเจตนากลั่นแกล้งทำให้เสียหายโดยอ้างว่าจะเปิดเผยความลับ ภาพลับ หรือข้อมูลส่วนตัว ให้บุคคลอื่นได้รับรู้

5) การหลอกลวง เป็นข่าวที่ถูกพูดถึงบ่อย ๆ ผู้มีชื่อเสียงหลายคนตกเป็นเหยื่อของกลุ่มมิจฉาชีพหลอกลวงให้ผู้คนหลงเชื่อ โดยสวมรอยเป็นบุคคลที่เป็นที่รู้จักในวงกว้าง และเป็นที่นับถืออย่างกว้างขวาง เพื่อให้ผู้เสียหายโอนเงินไปให้ด้วยวิธีการต่าง ๆ หรือการทำให้บุคคลเป้าหมายชื่นชมในภาพลักษณ์จนมีการนัดเจอเพื่อทำมิดีมิร้าย หลอกให้มีเพศสัมพันธ์ หรือทำอนาจาร

6) การสร้างข่าวปลอม เป็นการกระทำที่พบเห็นบ่อยครั้ง ซึ่งส่วนใหญ่มักจะเป็นกระทำเพื่อผลประโยชน์อย่างใดอย่างหนึ่งและมักจะทำในรูปแบบโจมตีฝ่ายตรงข้าม

ใบความรู้ที่ 3.1 (ต่อ)
เรื่อง การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)



ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ใบงานที่ 3.1
วิเคราะห์กรณีตัวอย่าง ฝึกทักษะ “เข้าใจตัวเรา เข้าใจผู้อื่น”

คำชี้แจง แบ่งกลุ่มผู้เข้ารับการอบรม เป็นกลุ่มย่อย จำนวน 6 กลุ่ม (สามารถเปลี่ยนแปลงได้ตามความเหมาะสม) และให้แต่ละกลุ่มจับฉลาก กรณีตัวอย่าง เพื่อวิเคราะห์สถานการณ์ และสรุปเป็นแผนผังความคิด เขียนลงในกระดาษปรู๊ฟ ตามประเด็น ดังนี้

1. ถ้าเหตุการณ์นี้เกิดขึ้นกับเรา หรือคนในครอบครัวของเรา เราจะรู้สึกอย่างไร ?
2. หากเราเป็นเหยื่อ เราจะจัดการความรู้สึกและแก้ไขปัญหาของเราอย่างไร ?
3. เราจะปฏิบัติตัวเพื่อลดปัญหาได้อย่างไร ?

ใบงานที่ 3.1 (ต่อ)
วิเคราะห์กรณีตัวอย่าง ฝึกทักษะ “เข้าใจตัวเรา เข้าใจผู้อื่น”

กลุ่มที่ 1 กรณีตัวอย่าง

“คำล้อเลียนฆ่าคนได้”รัศมี แข แชร์ประสบการณ์โดนบูลลี่ “ผิวดำ ตัวใหญ่”

ที่มา: https://mgronline.com/live/detail/9620000104735

ที่ผ่านมารัศมีแขเล่าว่า มีน้อง ๆ อินบ็อกซ์เข้ามาปรึกษาปัญหาในชีวิตประจำวันบ่อยครั้ง โดยเฉพาะกับการถูกล้อเลียนเรื่องสีผิว ซึ่งเจ้าตัวได้ให้คำแนะนำว่าชีวิตแต่ละคนต่างต้องมีเรื่องที่ยากลำบากกว่าจะผ่านมาถึงวันนี้ได้ อีกทั้งยังสะท้อนปัญหาการบูลลี่ในสังคมไทยขณะนี้ด้วยว่าถึงขั้นวิกฤติที่สุดของที่สุด เป็นการไม่มีขอบเขต ทุกคนเอาแต่สนุก เห็นคนที่อ่อนแอกว่าและทำร้ายเขา มันไม่โอเคเลย หรือบางคนที่พลาดแล้วไปทำร้าย ไปล้อเลียนเขา เขาเดินเอามีดมาแทงคุณ มีการเสียชีวิตเกิดขึ้น ถามว่ามันคุ้มไหมกับสิ่งที่ได้ทั้งสองแบบเลยไม่มีผลไหนที่คุ้ม

ฉะนั้น สังคมเราตอนนี้โดยเฉพาะในโซเชียล มันเกินเหตุไปแล้ว ความคิดเห็นส่วนตัวคือความคิดเห็นที่อยู่กับตัวเอง ไม่ได้เผยแพร่ เราแสดงความคิดเห็นได้ แต่ต้องใช้คำพูดที่ไม่ทำให้อีกฝ่ายรู้สึกกระทบกระทั่ง หรือพูดคุยด้วยเหตุผล ไม่ใช่ใช้คำพูดรุนแรง

ใบงานที่ 3.1 (ต่อ)
วิเคราะห์กรณีตัวอย่าง ฝึกทักษะ “เข้าใจตัวเรา เข้าใจผู้อื่น”

กลุ่มที่ 2 กรณีตัวอย่าง

“มุก วรนิษฐ์ ดาราดัง โดนบูลลี่จากโซเชียลจนเป็นโรควิตกกังวลเฉียบพลันเครียดถึงขั้นพบจิตแพทย์”

ที่มา: https://www.dailynews.co.th/news/1425884/

เราก็ยังเป็นมือใหม่ คำคอมเมนต์ต่าง ๆ นานา ยังไม่ค่อยคุ้น ไม่เคยเจอ บางทีเวลาเราโดนว่า ก็จะคิดว่าทำไมเขาต้องทำแบบนี้กับเรา ตอนเด็ก ๆ ก็เหมือนป่วยเลย เพราะโดนแรงคอมเมนต์แล้วไม่เข้าใจ โดนลามไปเรื่องส่วนตัว ไม่สวยอะไรแบบนี้ เป็นอาชีพที่หลาย ๆ คน สามารถเข้ามาคอมเมนต์ทำร้ายจิตใจหรือทำให้มีความสุขก็ทำได้ง่าย กว่าจะผ่านมาได้ เรายังรับมือไม่ทัน ช่วงนั้นมุกก็อยู่แต่ในบ้านไม่กินข้าว กินอะไรไม่ลง แล้วไม่อยากดูโซเชียลด้วย แล้วมุกก็อาจเป็นยุคแรก ๆ ที่โดนเรื่องโซเชียล บางทีเราก็ไม่แข็งแรงพอที่จะกล้าออกมาพูดอะไรด้วยซ้ำ มุกต้องพบจิตแพทย์ด้วยนะคะ บ้านมุกจะเป็นอะไรที่เครียดนิด ๆ หน่อย ๆ ก็จะหาจิตแพทย์กัน เพื่อให้เรายังมีความสุขแบบทุกวันนี้

ใบงานที่ 3.1 (ต่อ)
วิเคราะห์กรณีตัวอย่าง ฝึกทักษะ “เข้าใจตัวเรา เข้าใจผู้อื่น”

กลุ่มที่ 3 กรณีตัวอย่าง

“พลอยชมพู เล่าเหตุการณ์ ถูกนำภาพไปตัดต่อและเผยแพร่จนมีผลกระทบทางจิตใจ”

ที่มา: https://www.facebook.com/share/p/1BcCoydZwq/
ภาพ: https://www.thepeople.co/read/42241

พลอยชมพู เล่าว่า เหตุการณ์ลักษณะนี้ไม่ได้เพิ่งเริ่มต้นตอนโต หรือเมื่อมีการแต่งตัวที่ดูเป็นผู้ใหญ่มากขึ้นเท่านั้น แต่กลับเกิดขึ้นตั้งแต่ตอนที่เธอยังเป็นเด็ก โดยครั้งหนึ่งเธอเคยถูกนำภาพไปตัดต่อเป็นลักษณะภาพแอบถ่าย ในตอนนั้นแม้จะสามารถพิสูจน์ได้ว่าไม่ใช่ร่างกายของตัวเอง แต่ข่าวและภาพเหล่านั้นก็ทิ้งบาดแผลทางจิตใจไว้กับเธอไม่น้อยเลย

“จริง ๆ ภัยที่ถูกคุกคามหนูเจอมาตั้งแต่เด็กแล้วค่ะ ตอนนั้นเคยมีคนเอารูปไปตัดต่อเป็นภาพเหมือนแอบถ่าย ตอนนั้นตกใจมาก รู้สึกหลอนว่าโดนแอบถ่ายหรือเปล่า พอพิสูจน์ได้ว่าไม่ใช่ก็สบายใจขึ้น แต่มันก็มีผลกระทบทางจิตใจ ทำให้ไม่กล้าแต่งตัว ไม่กล้าลงภาพส่วนตัว แม้เราจะไม่ได้ทำอะไรผิดเลยก็ตาม”

พลอยชมพู ยังบอกอีกด้วยว่า ความรู้สึกเหล่านี้ค่อย ๆ บั่นทอนความมั่นใจ ทำให้เธอไม่อยากโพสต์ภาพหรือแบ่งปันช่วงชีวิตส่วนตัวบนโลกโซเชียลอีกต่อไปแล้ว แต่เมื่อได้ใช้เวลาเยียวยา พักผ่อน และปรับความคิด เธอเริ่มกลับมาดีขึ้นทีละน้อย

เธอฝากข้อคิดสำคัญถึงผู้คนในโลกออนไลน์ โดยขอให้ทุกคนตระหนักและเคารพในพื้นที่ส่วนตัวของผู้อื่นมากขึ้นเพราะคำพูดหรือคอมเมนต์เพียงไม่กี่คำ อาจกลายเป็นรอยแผลลึกที่ไม่อาจมองเห็นได้จากภายนอก และมันส่งผลกระทบต่อชีวิตคนคนหนึ่งได้จริง ๆ

ใบงานที่ 3.1 (ต่อ)
วิเคราะห์กรณีตัวอย่าง ฝึกทักษะ “เข้าใจตัวเรา เข้าใจผู้อื่น”

กลุ่มที่ 4 กรณีตัวอย่าง

“ยิปซี ยิปโซ เปิดใจต้องทนทุกข์นับ 10 ปี
จากการเปรียบเทียบบนโลกออนไลน์ จนไม่สนิทใจต่อกัน”

ที่มา: https://www.matichon.co.th/entertainment/news_2711423/

ทั้งคู่ก็ยอมรับว่าจริง ๆ แล้วเธอทั้ง 2 คน ก็ถูกเปรียบเทียบกันมาตั้งแต่เด็ก ด้วยความที่พี่สาวเป็นคนป๊อป ขณะที่น้องเป็นเด็กอ้วน ๆ ใส่แว่น แต่ตอนนั้นเราก็ไม่เข้าใจ เราก็ใช้ชีวิตสงบสุขมาเรื่อย ๆ โดยยิปโซเล่าว่า ยิปซีเป็นสาวสวยแก๊งนางฟ้าของโรงเรียน ส่วนตนนั้นเป็นที่รู้จักในนาม ‘น้องสาวพี่ยิปซี’ แล้วเวลาเขามองเราจะถอนหายใจ และพูดว่าทำไมไม่สวยเหมือนพี่สาว ตอนนั้นเสียใจมาก เวลาที่โดนเปรียบเทียบคู่พี่น้อง หรือเพื่อน มันมีความรู้สึกนะ เอาให้ได้แบบพี่สิ เก่งแบบพี่นะ

ยิปซี จึงเสริมต่อว่า ประโยคพวกนี้นะ มันสำคัญมาก มันมีผลต่อคาแรกเตอร์ของเด็กว่าสิ่งที่เขาเป็นอยู่ มันยังไม่โอเค เขาจะต้องเป็นอีกแบบหนึ่งเพื่อให้ได้รับการยอมรับ ด้านยิปโซก็ว่า ทุกการแข่งขันมีผู้แพ้ผู้ชนะเสมอ พอมีผู้ชนะ ผู้ชนะก็จะเริ่มหวงแหนชัยชนะ อยากชนะต่อไปเรื่อย ๆ ผู้แพ้ก็รู้สึกแย่ไปเรื่อย ๆ

คอมเมนต์แบบนี้มีผลกระทบต่อชีวิตมาก ๆ แต่กว่าจะแยกแยะได้ มันผ่านความเจ็บปวดและเชื่อว่าหลายคนยังไม่หลุดยังเจ็บปวด คนสองคนไม่จำเป็นจะต้องแข่งขัน เรามีดีในแต่ละคน

ใบงานที่ 3.1 (ต่อ)
วิเคราะห์กรณีตัวอย่าง ฝึกทักษะ “เข้าใจตัวเรา เข้าใจผู้อื่น”

กลุ่มที่ 5 กรณีตัวอย่าง

แม่ค้าทุเรียนแจ้งจับ “คุณเจมส์”
ลวงส่งภาพลับก่อนข่มขู่เรียกเงิน 50,000 บาท

ที่มา: https://mgronline.com/crime/detail/9680000062233/

แม่ค้าทุเรียนแจ้งความถูกหนุ่มแชทหลอกขอดูภาพลับ ก่อนข่มขู่เรียกเงิน 50,000 บาท อ้างภรรยาจับได้ ขู่ฟ้องชู้ วันนี้ (2 กรกฎาคม 2567) น.ส.หยก (นามสมมุติ) อายุ 36 ปี แม่ค้าทุเรียน พร้อมด้วย นายณธัชพงศ์ บุญเกิด หรือ “ทนายกบ” เดินทางเข้าแจ้งความกับตำรวจ สภ.เมืองนนทบุรี หลังถูกชายคนหนึ่งรู้จักผ่านเฟซบุ๊ก ใช้ชื่อว่า “คุณเจมส์” แชทพูดคุยในลักษณะลามก หลอกขอดูภาพลับ ก่อนนำภาพดังกล่าวมาข่มขู่เรียกเงินจำนวน 50,000 บาท อ้างว่าภรรยาของฝ่ายชายเห็นข้อความ และจะดำเนินคดีในข้อหาชู้สาวหากไม่ยอมจ่ายเงิน

ใบงานที่ 3.1 (ต่อ)
วิเคราะห์กรณีตัวอย่าง ฝึกทักษะ “เข้าใจตัวเรา เข้าใจผู้อื่น”

กลุ่มที่ 6 กรณีตัวอย่าง

รู้สำนึกผิดแต่สายไป “บอล หนองขาว” สำนึกผิดไลฟ์สดด่าตำรวจ

ที่มา: https://www.matichon.co.th/region/news_939275/

“บอล หนองขาว” ควงแฟนสาวหอบกระเช้าขอโทษตำรวจ แต่ไม่พ้นถูกดำเนินคดี 2 ข้อหา จากกรณีที่ “บอล หนองขาว” อายุ 31 ปี ชาว ต.หนองขาว อ.ท่าม่วง จ.กาญจนบุรี ใช้โทรศัพท์มือถือไลฟ์สด ด่าทอเจ้าหน้าที่ตำรวจ สภ.หนองขาว ด้วยถ้อยคำที่หยาบคาย และ นายบอล ยังสั่งให้แฟนสาวแชร์คลิปขณะไลฟ์สดออกไปสู่สาธารณะด้วย โดยก่อนหน้านี้ นายบอล ได้ก่อเหตุทำร้ายแม่และยายของตนเอง และเจ้าหน้าที่ตำรวจได้เข้าระงับเหตุ ซึ่งเหตุการณ์ดังกล่าวนั้นเกิดขึ้นเมื่อวันที่ 20 เมษายน 2567 ที่ผ่านมา ต่อมาเจ้าหน้าที่ตำรวจ สภ.หนองขาว ได้นำคลิปดังกล่าวมาเป็นหลักฐาน พร้อมกับแจ้งความดำเนินคดี นายบอล ในข้อหาดูหมิ่นเจ้าพนักงานขณะปฏิบัติหน้าที่และหมิ่นประมาทด้วยการโฆษณา จากนั้นเจ้าหน้าที่ได้ออกหมายเรียกให้มาพบเจ้าหน้าที่เพื่อรับทราบกล่าวหา

หน่วยการเรียนรู้ที่ 3 วิถีชีวิตบนโลกดิจิทัล
แผนการจัดกิจกรรม 3.2 เรื่อง กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล

ระยะเวลา 1 ชั่วโมง 30 นาที

สาระสำคัญ

กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัลในประเทศไทย มีหลายฉบับที่ถูกบัญญัติขึ้นเพื่อรองรับการเปลี่ยนแปลงของโลกยุคดิจิทัล ทั้งในด้านการใช้เทคโนโลยี ความปลอดภัยทางไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และการป้องกันอาชญากรรมออนไลน์ ซึ่งกฎหมายที่สำคัญและเกี่ยวข้องมี 4 ฉบับ ได้แก่ 1) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ 2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560 กำหนดลักษณะความผิด เช่น การเข้าถึงหรือแก้ไขข้อมูลโดยมิชอบ การเผยแพร่ข้อมูลเท็จ และบทลงโทษแก่ผู้กระทำผิด รวมถึงหน้าที่ของผู้ให้บริการอินเทอร์เน็ต 3) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ที่มุ่งคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลโดยการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลต้องได้รับความยินยอม หากฝ่าฝืนจะมีโทษทางกฎหมาย และ 4) พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 เป็นกฎหมายที่ออกมาเพื่อรับมือกับภัยออนไลน์ที่เพิ่มขึ้นอย่างรวดเร็ว โดยเฉพาะการหลอกลวงผ่านโทรศัพท์และอินเทอร์เน็ต ซึ่งสร้างความเสียหายแก่ประชาชนจำนวนมาก

จุดประสงค์

1. เพื่อให้ผู้เข้ารับการอบรมสามารถอธิบายกฎหมาย ระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล ที่พบบ่อยและบทลงโทษตามกฎหมาย
2. เพื่อให้ผู้เข้ารับการอบรมสามารถปฏิบัติตนตามกฎหมาย และระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัลได้อย่างเหมาะสม
3. เพื่อให้ผู้เข้ารับการอบรมเกิดความตระหนักรู้ถึง สิทธิ หน้าที่ การปฏิบัติตนตามกฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล

ขอบข่ายเนื้อหา

1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
3. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
4. พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568

สื่อการเรียนรู้

1. PowerPoint บรรยาย เรื่อง กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล

https://shorturl.at/3E8YN

2. ใบความรู้ที่ 3.2 เรื่อง กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล
3. สื่อคลิปวิดีโอ เรื่อง กฎหมายที่เกี่ยวข้องกับ Cybersecurity

https://dg.th/akrzb1t405

4. ใบงานที่ 3.2.1 เรื่อง ประเภทของข้อมูลส่วนบุคคล
5. ใบงานที่ 3.2.2 เรื่อง สถานการณ์จำลอง “ควรกระทำอย่างไรให้ถูกต้อง”

วัสดุอุปกรณ์

เครื่องคอมพิวเตอร์/โน้ตบุ๊ค/แท็บเล็ต/โทรศัพท์มือถือ เชื่อมต่ออินเทอร์เน็ต

ขั้นตอนการจัดกิจกรรม

1. วิทยากรตั้งคำถามว่า “ตัวเรามีข้อมูลอะไรบ้าง ? ” และให้ผู้เข้ารับการอบรมแลกเปลี่ยนเรียนรู้ร่วมกัน
2. วิทยากรบรรยาย เรื่อง กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล พร้อมทั้งให้ผู้เข้ารับการอบรมศึกษาเนื้อหาจากใบความรู้ที่ 3.2 เรื่อง กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล
3. วิทยากรให้ผู้เข้ารับการอบรมเรียนรู้จากสื่อคลิปวิดีโอ เรื่อง กฎหมายที่เกี่ยวข้องกับ Cybersecurity แล้วร่วมกันสรุปและแลกเปลี่ยนเรียนรู้

https://dg.th/akrzb1t405

4. กิจกรรมฝึกทักษะรายบุคคล ให้ผู้เข้ารับการอบรมทำการวิเคราะห์ข้อมูลและสถานการณ์จำลองตามใบงานที่ 3.2.1 เรื่อง ประเภทของข้อมูลส่วนบุคคล และใบงานที่ 3.2.2 สถานการณ์จำลอง “ควรกระทำอย่างไรให้ถูกต้อง”
5. วิทยากรเลือกนำเสนอใบงานละ 5 - 7 คน (สามารถปรับเปลี่ยนได้ตามความเหมาะสม) แล้วให้ผู้เข้ารับการอบรมแลกเปลี่ยนเรียนรู้ และวิทยากรอธิบายเพิ่มเติม

การวัดและประเมินผล

1. ใบงาน
2. การสังเกต

ใบความรู้ที่ 3.2
เรื่อง กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล

กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล

ในยุคดิจิทัลที่เทคโนโลยีเข้ามามีบทบาทในชีวิตประจำวันมากขึ้น อาชญากรรมทางเทคโนโลยีทวีความรุนแรงและซับซ้อนมากขึ้นตามไปด้วย ส่งผลให้ภาครัฐจำเป็นต้องมีมาตรการทางกฎหมายที่เข้มงวดและทันสมัย กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัลในประเทศไทย มีหลายฉบับที่ถูกบัญญัติขึ้นเพื่อรองรับการเปลี่ยนแปลงของโลกยุคดิจิทัล ทั้งในด้านการใช้เทคโนโลยี ความปลอดภัยทางไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และการป้องกันอาชญากรรมออนไลน์ ซึ่งกฎหมายที่สำคัญและเกี่ยวข้องมี 4 ฉบับ ดังนี้

ที่มา : กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ส่งผลให้เกิดคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยมีสาระสำคัญดังนี้

1. วัตถุประสงค์หลัก

1.1 เพื่อกำหนดมาตรการการป้องกันและรับมือภัยคุกคามทางไซเบอร์ที่อาจกระทบต่อโครงสร้างพื้นฐานและความมั่นคงของประเทศ

1.2 สร้างระบบการประสานงานระหว่างหน่วยงานรัฐและเอกชนในการรับมือกับภัยไซเบอร์

1.3 กำหนดมาตรการและแผนปฏิบัติการด้านความมั่นคงไซเบอร์อย่างเป็นระบบ

2. หน้าที่และอำนาจ

2.1 เสนอและกำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติ

2.2 ประสานงานกับหน่วยงานต่าง ๆ เพื่อป้องกันและลดความเสี่ยงจากภัยไซเบอร์

2.3 กำหนดมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

2.4 มีอำนาจในการสั่งการและดำเนินการในกรณีเกิดภัยคุกคามทางไซเบอร์ระดับร้ายแรงหรือวิกฤติ

ใบความรู้ที่ 3.2 (ต่อ)
เรื่อง กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (ฉบับที่ 2)

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือที่เรียกสั้น ๆ ว่า พ.ร.บ. คอมพิวเตอร์ เป็นกฎหมายหลักที่ใช้กำกับดูแลการกระทำบนโลกออนไลน์ แม้จะเป็นเรื่องเข้าใจยาก และต้องอาศัยการตีความทางกฎหมาย แต่เป็นสิ่งจำเป็นที่ทุกคนจะต้องศึกษาทำความเข้าใจ เพื่อป้องกันไม่ให้ตนเองกระทำผิดโดยรู้เท่าไม่ถึงการณ์ การอ้างว่าไม่รู้กฎหมายไม่ทำให้พ้นความผิด หรือได้รับการละเว้นโทษ ซึ่งพอสรุปได้ ดังนี้

1. วัตถุประสงค์หลัก

1.1 ป้องกันการใช้คอมพิวเตอร์ในทางที่ผิด เช่น การแฮ็กข้อมูล การเผยแพร่ข้อมูลเท็จ หรือเนื้อหาลามก
1.2 คุ้มครองผู้ใช้งานคอมพิวเตอร์และอินเทอร์เน็ตจากการถูกละเมิดสิทธิ
1.3 สร้างความรับผิดชอบในการใช้งานเทคโนโลยีดิจิทัล

2. ตัวอย่างพฤติกรรมที่มักทำผิดกฎหมาย

2.1 การส่งอีเมลหรือข้อความโฆษณาขายสินค้าไปให้คนจำนวนมาก ๆ เช่น การฝากร้านขายของในอินสตาแกรม การส่งข้อความลูกโซ่ เช่น ให้อ่านคำสวดอธิษฐานตามนี้ดัง ๆ 10 รอบแล้วแชร์ไปให้เพื่อนอีก 10 คน แล้วคุณจะโชคดี การกระทำเช่นนี้ก่อความเดือดร้อนรำคาญให้ประชาชนและทำให้เกิดเนื้อหาขยะที่ไม่เป็นประโยชน์มากมายบนเครือข่าย

2.2 การโพสต์ด้วยความคึกคะนองหรือสร้างความตระหนกตกใจ เช่น ตนเป็นคนวางระเบิดหน้าห้างสรรพสินค้า ปล่อยข่าวดาวหางกำลังจะพุ่งชนโลก เขื่อนกำลังจะแตก หุ้นตัวนั้นจะขึ้นตัวนี้จะลงให้รีบวางแผนทำกำไร โรงไฟฟ้าปิดซ่อมบำรุงจะทำให้ไฟดับทั้งเมือง ใช้สบู่เหลวทำให้ตายเร็วกว่าสบู่ก้อน ฯลฯ ถ้าไม่เป็นความจริงอาจเข้าข่ายการส่งข้อมูลข่าวสารปลอม หรือบิดเบือนข้อมูลเท็จ ที่ทำให้เกิดความตื่นตระหนก เสียหาย กระทบต่อความปลอดภัยของประชาชนความมั่นคงทางเศรษฐกิจ โครงสร้างพื้นฐาน ความมั่นคงของประเทศ หรือการโพสต์ข้อมูลที่มีลักษณะลามกอนาจารที่ประชาชนทั่วไปเข้าถึงได้

2.3 การตัดต่อ แต่งเติม หรือดัดแปลงภาพ ที่ทำให้คนอื่นเสียหาย อับอาย ถูกดูถูกดูหมิ่น ถูกเกลียดชัง แม้การกระทำดังกล่าว กระทำกับคนที่เสียชีวิตไปแล้ว แต่บิดา มารดา คู่สมรส หรือบุตรของผู้เสียชีวิตก็สามารถร้องทุกข์แทนได้

2.4 การกระทำด้วยเหตุจูงใจเดียวอาจกระทำความผิดหลายกฎหมายหลายมาตราได้ เช่น เพื่อนโกรธกันด้วยเรื่องส่วนตัว จึงแอบเจาะเข้าระบบคอมพิวเตอร์และอีเมลของเพื่อน ลบข้อมูลที่สำคัญ ไปหลายอย่าง ทั้งยังส่งอีเมลในนามของเพื่อนไปหาเจ้านาย โดยแนบภาพตัดต่อของเจ้านายให้ดูตลกขบขัน พูดถึงเจ้านายในทางเสียหาย ปล่อยข่าวว่าเจ้านายคนนี้ทุจริตทำให้บริษัทล้มละลาย จะต้องเลิกจ้างพนักงานหลายพันคน กรณีนี้มีการกระทำความผิดหลายมาตรา ก็จะมีโทษเพิ่มขึ้นตามมาตรานั้น ๆ ดังนั้นก่อนจะโพสต์หรือส่งต่อข้อมูลใด ๆ ให้ไตร่ตรองอย่างรอบคอบ รวมทั้งการแชร์ข้อมูลของคนอื่นก็ควรตรวจสอบให้แน่ใจว่าเป็นความจริง ไม่ส่งผลกระทบ หรือไม่ไปละเมิดสิทธิคนอื่น ทำให้ผู้อื่นเกิดความเสียหาย จึงควรงดโพสต์หรือส่งต่อข้อมูลนั้น ๆ

ดังนั้น ก่อนจะแสดงความเห็นหรือส่งต่อข้อมูลใด ๆ ให้ไตร่ตรองอย่างรอบคอบ รวมทั้งการแชร์ข้อมูลจากคนอื่นควรตรวจสอบให้แน่ใจว่าเป็นความจริง ไม่ส่งผลกระทบ หรือไม่ไปละเมิดสิทธิคนอื่น ทำให้ผู้อื่นเกิดความเสียหาย

ใบความรู้ที่ 3.2 (ต่อ)
เรื่อง กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือที่เรียกกันว่า “PDPA” เป็นกฎหมายที่มีเป้าหมายเพื่อคุ้มครองสิทธิของบุคคลในการควบคุมข้อมูลส่วนบุคคลของตนเอง ทั้งนี้ ความเป็นส่วนตัวในโลกดิจิทัล คือ สิทธิการปกป้องข้อมูลความเป็นส่วนตัวในโลกออนไลน์ของผู้ใช้งานที่บุคคลหรือหน่วยงานอื่นจะนำไปจัดเก็บ นำไปใช้ประโยชน์หรือนำข้อมูลนั้นไปเผยแพร่ ซึ่งส่วนหนึ่งของข้อมูลส่วนตัวได้ถูกจัดเก็บไว้ โดยผู้ให้บริการโทรศัพท์ ผู้ให้บริการอินเทอร์เน็ต และผู้ให้บริการสื่อสังคมออนไลน์ (ผู้ควบคุมข้อมูลส่วนบุคคล) เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ

1. วัตถุประสงค์หลัก

1.1 ป้องกันการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคล
1.2 กำหนดมาตรฐานการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอย่างเหมาะสม
1.3 กำหนดความรับผิดชอบขององค์กรในการจัดเก็บข้อมูลส่วนบุคคล

2. ข้อมูลส่วนบุคคล แบ่งออกเป็น 2 ประเภท ได้แก่

2.1 ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ เช่น

1) ชื่อ-นามสกุล หรือชื่อเล่น
2) เลขประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่น ๆ ที่มีข้อมูลส่วนบุคคลที่กล่าวมา ย่อมสามารถใช้ระบุตัวบุคคลได้ จึงถือเป็นข้อมูลส่วนบุคคล)
3) ที่อยู่ อีเมล เลขโทรศัพท์
4) ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น รหัสประจำคอมพิวเตอร์
5) ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์ โฉนดที่ดิน
6) ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด สัญชาติ น้ำหนัก ส่วนสูง ข้อมูลตำแหน่งที่อยู่ ข้อมูลการศึกษา ข้อมูลทางการเงิน ข้อมูลการจ้างงาน
7) ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง
8) ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล
9) ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

ใบความรู้ที่ 3.2 (ต่อ)
เรื่อง กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล

2.2 ข้อมูลส่วนบุคคลที่อ่อนไหว หมายถึง ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ ตัวอย่าง ข้อมูลส่วนบุคคลที่ข้อมูลอ่อนไหว ประกอบด้วย

1) เชื้อชาติ
2) เผ่าพันธุ์
3) ความคิดเห็นทางการเมือง
4) ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
5) พฤติกรรมทางเพศ
6) ประวัติอาชญากรรม
7) ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
8) ข้อมูลสหภาพแรงงาน
9) ข้อมูลพันธุกรรม
10) ข้อมูลชีวภาพ
11) ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า ลายนิ้วมือ ฟิล์มเอกซเรย์ ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง
12) ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

3. หลักการสำคัญ

3.1 ต้องแจ้งวัตถุประสงค์ก่อนเก็บข้อมูล
3.2 ต้องขอความยินยอมอย่างชัดเจน
3.3 เจ้าของข้อมูลมีสิทธิในการเข้าถึง แก้ไข ลบ หรือคัดค้านการใช้ข้อมูลของตน
3.4 ต้องมีมาตรการรักษาความปลอดภัยของข้อมูล
3.5 หากเกิดการละเมิด ต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ภายใน 72 ชั่วโมง

4. ข้อยกเว้น

4.1 ใช้ข้อมูลเพื่อกิจกรรมส่วนตัวหรือครอบครัว
4.2 หน่วยงานรัฐที่เกี่ยวข้องกับความมั่นคง
4.3 การใช้ข้อมูลเพื่อสื่อมวลชน ศิลปกรรม หรือวรรณกรรมตามจริยธรรม

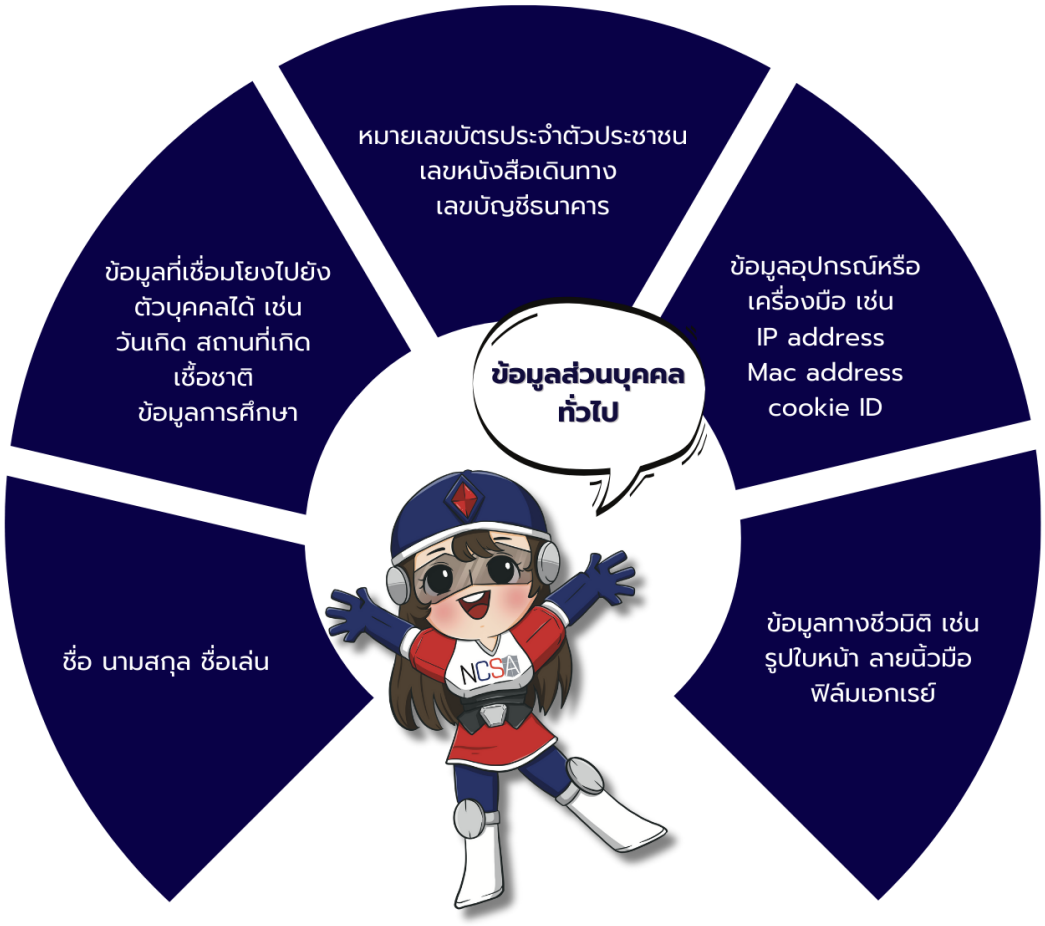
5. บทลงโทษ

5.1 ทางแพ่ง: ชดใช้ค่าสินไหมทดแทน
5.2 ทางอาญา: จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ
5.3 ทางปกครอง: ปรับสูงสุดไม่เกิน 5,000,000 บาท

PDPA
ข้อมูลส่วนบุคคล คืออะไร

พระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562

ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม



สิทธิของเจ้าของข้อมูล

1. ข้อมูลที่ให้เพื่อประโยชน์ของตัวเรา
2. ต้องมั่นใจว่าข้อมูลที่ให้ไปมีกระบวนการจัดการที่ดี ปลอดภัย ไม่รั่วไหล
3. เราเป็นเจ้าของข้อมูลเสมอ
4. สามารถเพิกถอนความยินยอมในการให้ข้อมูลได้ตลอดเวลา

ที่มา : สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ใบความรู้ที่ 3.2 (ต่อ)
เรื่อง กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568

1. พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

มีผลบังคับใช้ตั้งแต่วันที่ 17 มีนาคม 2566 มีเจตนารมณ์เพื่อให้หน่วยงานและธนาคารทุกแห่งร่วมกันกำหนดมาตรการดูแลประชาชนจากมิจฉาชีพหลอกโอนเงิน และรับมือกับการหลบเลี่ยงการตรวจสอบธุรกรรมของมิจฉาชีพผ่าน “บัญชีม้า”

1.1 บัญชีม้า คือ บัญชีเงินฝากธนาคารที่เปิดขึ้นโดยบุคคลหนึ่งแต่ถูกนำไปใช้ โดยบุคคลอื่น โดยเฉพาะมิจฉาชีพที่นำมาใช้เป็นช่องทางในการรับเงินและถ่ายโอนเงินที่ได้มาจากการกระทำ ความผิดเพื่อป้องกันไม่ให้มีพยานหลักฐานเชื่อมโยงมาถึงตัวได้

1.2 มาตรการสำคัญ

1) สถาบันการเงินสามารถระงับธุรกรรมต้องสงสัยได้ทันทีเป็นการชั่วคราว (ระงับได้ไม่เกิน 3 วัน)

2) ประชาชนสามารถแจ้งเหตุผ่านระบบอิเล็กทรอนิกส์ และธนาคารต้องดำเนินการระงับธุรกรรมทันที

3) การเปิดเผยข้อมูลส่วนบุคคลเพื่อป้องกันอาชญากรรม ไม่อยู่ภายใต้ข้อมูลส่วนบุคคล (PDPA) แต่ห้ามเปิดเผยให้บุคคลที่ไม่เกี่ยวข้อง

4) ผู้เปิดบัญชีหรือหมายเลขโทรศัพท์ให้ผู้อื่นใช้ (บัญชีม้าและซิมม้า) โดยรู้ว่าจะนำไปใช้ในการกระทำผิด มีโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ

5) ผู้จัดหา ซื้อขาย หรือโฆษณาบัญชีหรือหมายเลขโทรศัพท์เพื่อใช้ในการกระทำผิดมีโทษจำคุก 2 - 5 ปี หรือปรับ 200,000 - 500,000 บาท หรือทั้งจำทั้งปรับ

2. พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568

เพื่อให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ผู้ให้บริการโทรศัพท์มือถือ เครือข่ายโทรศัพท์ และสถาบันการเงินมีส่วนรับผิดชอบในความเสียหายที่เกิดขึ้นกับผู้เสียหาย และให้คณะกรรมการธุรกรรมตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน สามารถพิจารณาคืนเงินแก่ผู้เสียหายได้ โดยไม่ต้องรอให้มีการยื่นฟ้องคดีต่อศาลจนมีคำสั่งถึงที่สุดก่อน นอกจากนี้ ยังมุ่งหวังให้กฎหมายฉบับนี้เป็นเครื่องมือสำคัญในการปราบปรามแก๊งคอลเซ็นเตอร์ รวมถึงอาชญากรรมออนไลน์ต่าง ๆ โดยมีสาระสำคัญ ดังนี้

2.1 แก้ไขเพิ่มเติมบทนิยามเพื่อให้เกิดความครอบคลุมมากขึ้น ได้แก่ **“ผู้ประกอบธุรกิจ”** หมายถึง ผู้ประกอบธุรกิจตามกฎหมายว่าด้วยระบบการชำระเงินและผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ตามกฎหมายว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัล **“กระเป๋าสินทรัพย์ดิจิทัล (Digital Wallet)”** หมายถึง ระบบที่ใช้ในการจัดเก็บสินทรัพย์ดิจิทัล **“บัญชีเงินอิเล็กทรอนิกส์”** หมายความรวมถึงบัญชีสินทรัพย์ดิจิทัล

ใบความรู้ที่ 3.2 (ต่อ)
เรื่อง กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล

2.2 ผู้ให้บริการเครือข่ายโทรศัพท์มือถือ – สถาบันการเงิน – โซเชียลมีเดีย ต้องรับผิดร่วม หากมีความเสียหาย เกิดจากการหลอกลวงทางไซเบอร์ แล้วพบว่าให้บริการเครือข่ายโทรศัพท์มือถือ ธนาคาร หรือแพลตฟอร์มออนไลน์ ไม่ได้ปฏิบัติตามมาตรฐานที่หน่วยงานรัฐกำหนดไว้ ต้องร่วมชดใช้ความเสียหายด้วย

2.3 หน่วยงานใหญ่ กำหนดมาตรฐานหรือมาตรการป้องกันอาชญากรรมทางเทคโนโลยี ได้แก่ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) และคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.) เป็นผู้กำหนด “มาตรการป้องกัน” ที่แต่ละภาคส่วนต้องปฏิบัติตาม เพื่อให้ทุกระบบมีมาตรฐานเดียวกัน และสามารถเชื่อมต่อป้องกันภัยไซเบอร์ได้อย่างเป็นรูปธรรม

2.4 คัดกรอง SMS ต้องเริ่มทันที ข้อความ SMS ที่ดูเหมือนไม่มีพิษภัย กลับกลายเป็นกับดักของมิจฉาชีพ และเป็นช่องทางของมิจฉาชีพ ที่จะเข้าถึงข้อมูลในโทรศัพท์เสียหาย หลอกติดตั้งแอปพลิเคชัน สามารถควบคุมโทรศัพท์ของผู้เสียหาย สามารถโอนเงินจากบัญชีผู้เสียหาย ที่เรียกกันว่า “แอปดูดเงิน” กฎหมายฉบับนี้จึงกำหนดให้ผู้ให้บริการเครือข่ายโทรศัพท์และโทรคมนาคมต้องมีระบบ คัดกรองข้อความที่เสี่ยง เช่น SMS ปลอมหลอกกดลิงก์ โอนเงิน หรือแจ้งเตือนปลอม ไม่ใช่แค่ดูแลสัญญาณโทรศัพท์ แต่ต้องดูแลความปลอดภัยของเนื้อหาด้วย

2.5 พบเบอร์ทำผิด = ระงับบริการได้ทันที สำนักงานตำรวจแห่งชาติ สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) กรมสอบสวนคดีพิเศษ (DSI) และศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) พบพยานหลักฐานชัดเจนว่า เบอร์โทรศัพท์ใช้กระทำความผิด เช่น ส่งข้อความหลอกลวง โทรหลอกโอนเงิน หรือเปิดบัญชีปลอม สามารถแจ้ง คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) เพื่อระงับเบอร์นั้นได้ทันที โดยไม่ต้องรอคำสั่งศาล เพราะความเร็วในการสกัดกั้นอาจเป็นจุดเปลี่ยนของการหยุดยั้งการหลอกลวง

2.6 ยกเลิกระงับบริการ ต้องผ่านความเห็นชอบร่วม หากเจ้าของเบอร์โทรศัพท์หรือบัญชีธนาคารที่ถูกระงับยืนยันว่าตนเองไม่ได้ทำผิด การคืนสิทธิให้ใช้งานได้อีกครั้งจะไม่เกิดขึ้นทันที ต้องผ่านความเห็นชอบร่วมกันของ 5 หน่วยงาน ได้แก่ 1) สำนักงานตำรวจแห่งชาติ 2) กรมสอบสวนคดีพิเศษ (DSI) 3) สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) 4) ศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) และ 5) คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) เพื่อให้มั่นใจว่าไม่มีการใช้ช่องว่างในทางที่ผิดอีก

ใบความรู้ที่ 3.2 (ต่อ)
เรื่อง กฎหมายและระเบียบที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล

2.7 ยกระดับ “ศปอท.” คุมเกมไซเบอร์ระดับชาติ ศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) เป็นกลไกใหม่ ในสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีหน้าที่เชิงรุก ในการสกัดภัยไซเบอร์ตั้งแต่ต้นทาง เช่น รับแจ้งเหตุจากผู้เสียหาย ระงับธุรกรรมต้องสงสัยในบัญชีเงินฝากหรือบัญชีอิเล็กทรอนิกส์ เผยแพร่รายชื่อบัญชีต้องสงสัย กระเป๋าสินทรัพย์ดิจิทัล แจ้งข้อมูลเบอร์โทรและ SMS ที่เกี่ยวข้องกับอาชญากรรม โดยคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ดำเนินการ หน่วยงานนี้จึงเป็นเส้นเลือดใหญ่ที่ทำให้มาตรการทั้งหมดขับเคลื่อนได้จริง

2.8 ลงทะเบียนเบอร์มั่ว = มีโทษจริง หากผู้ขายหรือผู้ลงทะเบียนรู้ (หรือควรรู้) ว่าเบอร์โทรศัพท์นั้นจะถูกใช้ทำความผิด มีโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ นับเป็นบทลงโทษที่จริงจังเพื่อปราบปรามบัญชีม้า และเบอร์ผีที่เป็นจุดเริ่มของการฉ้อโกงออนไลน์ให้หมดไป

ที่มา : กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้

ใบงานที่ 3.2.1
เรื่อง ประเภทของข้อมูลส่วนบุคคล

คำชี้แจง ให้ผู้เข้ารับการอบรมศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้วเขียนรายละเอียดที่เกี่ยวข้องกับข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่อ่อนไหว

ข้อมูลส่วนบุคคลทั่วไป

ข้อมูลส่วนบุคคลทั่วไปที่อ่อนไหว

หมายเหตุ: สำหรับแปะโพสต์อิทแยกประเภท

ใบงานที่ 3.2.2
เรื่อง สถานการณ์จำลอง “ควรกระทำอย่างไรให้ถูกต้อง”

คำชี้แจง ให้ผู้เข้ารับการอบรมวิเคราะห์สถานการณ์จำลองตามที่กำหนด และตอบคำถาม

สถานการณ์จำลองที่ 1

คำอธิบายสถานการณ์

เอและบีไปทำบัตรประชาชนที่ที่ว่าการอำเภอพร้อมกัน จึงได้ถ่ายรูปบัตรประชาชนของตนเองเอาไว้และโพสต์ลงเฟซบุ๊กเอาไว้เป็นที่ระลึก

การกระทำของเอและบีถูกต้องหรือไม่ ?

จากสถานการณ์ การกระทำของเอและบีถูกต้องหรือไม่ เพราะอะไร ก่อให้เกิดผลเสียอย่างไร และควรปฏิบัติอย่างไรให้ถูกต้องเหมาะสม จงอธิบาย

สถานการณ์จำลองที่ 2

คำอธิบายสถานการณ์

น้องกระรอกไปร้องคาราโอเกะกับเพื่อน ๆ โดยทางร้านตั้งเงื่อนไขว่าหากแสดงบัตรประชาชน พร้อมยินยอมให้ทางร้านถ่ายรูปเก็บเอาไว้ จะได้ต่อเวลาพิเศษ 30 นาที น้องซีจึงยินยอมให้ทางร้านถ่ายรูปบัตรประชาชน เพราะต้องการเวลาพิเศษเพิ่มเติม

การกระทำของน้องกระรอกถูกต้องหรือไม่ ?

จากสถานการณ์ การกระทำของกระรอกถูกต้องหรือไม่ เพราะอะไร ก่อให้เกิดผลเสียอย่างไร และควรปฏิบัติอย่างไรให้ถูกต้องเหมาะสม จงอธิบาย

ใบงานที่ 3.2.2 (ต่อ)
เรื่อง สถานการณ์จำลอง “ควรกระทำอย่างไรให้ถูกต้อง”

คำชี้แจง ให้ผู้เข้ารับการอบรมวิเคราะห์สถานการณ์จำลองตามที่กำหนด และตอบคำถาม

สถานการณ์จำลองที่ 3

คำอธิบายสถานการณ์

พี่สมพงษ์เป็นผู้จัดการฝ่ายรับสมัครงานของบริษัทแห่งหนึ่ง วันหนึ่งได้สัมภาษณ์งานน้องมะลิผู้สมัครงาน หลังจากคุยเรื่องหน้าที่การทำงานแล้ว จึงได้สอบถามถึงความคิดเห็นทางการเมือง ความเชื่อทางศาสนา และรสนิยมทางเพศ เพราะหวังว่าจะได้ข้อมูลเพิ่มเติมมากขึ้น

การกระทำของพี่สมพงษ์ถูกต้องหรือไม่ ?

จากสถานการณ์ การกระทำของสมพงษ์ถูกต้องหรือไม่ เพราะอะไร ก่อให้เกิดผลเสียอย่างไร และควรปฏิบัติอย่างไรให้ถูกต้องเหมาะสม จงอธิบาย

สถานการณ์จำลองที่ 4

คำอธิบายสถานการณ์

กุ๊กไก่ได้มีโอกาสเดินทางไปเที่ยวต่างประเทศเป็นครั้งแรก จึงอยากโพสต์รูปอวดเพื่อน ๆ จึงถ่ายรูปหน้าข้อมูลหนังสือเดินทางของตนเอง เพื่อเป็นการยืนยันให้เพื่อน ๆ เชื่อว่าตนเองกำลังจะเดินทางไปต่างประเทศจริง ๆ

การกระทำของนางสาวกุ๊กไก่ถูกต้องหรือไม่ ?

จากสถานการณ์ การกระทำของกุ๊กไก่ถูกต้องหรือไม่ เพราะอะไร ก่อให้เกิดผลเสียอย่างไร และควรปฏิบัติอย่างไรให้ถูกต้องเหมาะสม จงอธิบาย

ใบงานที่ 3.2.2 (ต่อ)
เรื่อง สถานการณ์จำลอง “ควรกระทำอย่างไรให้ถูกต้อง”

คำชี้แจง ให้ผู้เข้ารับการอบรมวิเคราะห์สถานการณ์จำลองตามที่กำหนด และตอบคำถาม

สถานการณ์จำลองที่ 5

คำอธิบายสถานการณ์

หมอสมชายต้องการข้อมูลทางการแพทย์ของนายวิชัยซึ่งกำลังป่วยหนัก นายวรศักดิ์ซึ่งเป็นบุตรชายเห็นว่าข้อมูลทางการแพทย์ของพ่อเป็นข้อมูลจำเป็นต่อการรักษา จึงให้ข้อมูลดังกล่าวแก่นายแพทย์สมชายไป

การกระทำของนายวรศักดิ์ถูกต้องหรือไม่ ?

จากสถานการณ์ การกระทำของนายวรศักดิ์ถูกต้องหรือไม่ เพราะอะไร ก่อให้เกิดผลเสียอย่างไร และควรปฏิบัติอย่างไรให้ถูกต้องเหมาะสม จงอธิบาย

สถานการณ์จำลองที่ 6

คำอธิบายสถานการณ์

นายกเกรียงไกรเป็นนายกเทศมนตรีตำบลแห่งหนึ่ง วันหนึ่งได้รับการติดต่อจากบริษัทเงินกู้เศรษฐีไทย ว่าอยากได้ข้อมูลส่วนตัวของประชาชนในพื้นที่ตำบล เพื่อประชาสัมพันธ์โครงการเงินกู้ดอกเบี้ยต่ำ นายเกรียงไกรเห็นว่าประชาชนน่าจะได้ประโยชน์ จึงให้ข้อมูลส่วนตัวของประชาชนแก่บริษัทเงินกู้เศรษฐีไทยไปทั้งหมด

การกระทำของนายกเกรียงไกรถูกต้องหรือไม่ ?

จากสถานการณ์ การกระทำของนายกเกรียงไกรถูกต้องหรือไม่ เพราะอะไร ก่อให้เกิดผลเสียอย่างไร และควรปฏิบัติอย่างไรให้ถูกต้องเหมาะสม จงอธิบาย

แนวคำตอบใบงานที่ 3.2.1
เรื่อง ประเภทของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลทั่วไป

ข้อมูลส่วนบุคคล คือ ข้อมูลใด ๆ ที่สามารถระบุตัวบุคคลนั้นได้ (ระบุไปถึงเจ้าของข้อมูล) ไม่ว่าจะเป็นทางตรงหรือทางอ้อมก็ตาม แต่จะไม่รวมไปถึงข้อมูลของผู้ที่เสียชีวิตแล้ว หรือ ข้อมูลของนิติบุคคล เช่น บริษัท มูลนิธิ สมาคม องค์กร ตัวอย่าง เช่น

1) ชื่อ-นามสกุล หรือชื่อเล่น
2) เลขประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่น ๆ ที่มีข้อมูลส่วนบุคคลที่กล่าวมาย่อมสามารถใช้ระบุตัวบุคคลได้ จึงถือเป็นข้อมูลส่วนบุคคล)
3) ที่อยู่ อีเมล เลขโทรศัพท์
4) ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น รหัสประจำคอมพิวเตอร์
5) ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์ โฉนดที่ดิน
6) ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด สัญชาติ น้ำหนัก ส่วนสูงข้อมูลตำแหน่งที่อยู่ ข้อมูลการศึกษา ข้อมูลทางการเงิน ข้อมูลการจ้างงาน
7) ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง
8) ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น Log File
9) ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต

ข้อมูลส่วนบุคคลทั่วไปที่อ่อนไหว

ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) คือ ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ ตัวอย่าง ข้อมูลส่วนบุคคลที่ข้อมูลอ่อนไหว มีอะไรบ้าง

1) เชื้อชาติ
2) เผ่าพันธุ์
3) ความคิดเห็นทางการเมือง
4) ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
5) พฤติกรรมทางเพศ
6) ประวัติอาชญากรรม
7) ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
8) ข้อมูลสหภาพแรงงาน
9) ข้อมูลพันธุกรรม

แนวคำตอบใบงานที่ 3.2.2
เรื่อง สถานการณ์จำลอง “ควรกระทำอย่างไรให้ถูกต้อง”

สถานการณ์จำลอง 1

ไม่ถูกต้อง ซึ่งไม่มีความผิดทางกฎหมาย แต่เนื่องจากหน้าบัตรประชาชนประกอบด้วยข้อมูลส่วนบุคคลที่สำคัญมากมาย เช่น เลขบัตรประชาชน ชื่อ-นามสกุล วันเดือนปีเกิด ซึ่งข้อมูลทั้งหมดอาจถูกลักลอบนำไปใช้ได้อย่างกว้างขวาง และเป็นผลเสียต่อเจ้าของบัตรประชาชนอย่างยิ่ง

สถานการณ์จำลอง 2

ไม่ถูกต้อง เพราะเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล และการยินยอมดังกล่าวอาจไม่เป็นไปโดยสมัครใจอย่างแท้จริง อีกทั้งการเก็บข้อมูลจากทางร้านนั้นไม่มีเหตุผลอันสมควร และอาจขัดต่อกฎหมายคุ้มครองข้อมูลส่วนบุคคล

สถานการณ์จำลอง 3

ไม่ถูกต้อง เนื่องจากข้อมูลดังกล่าวถือเป็นข้อมูลส่วนบุคคลที่อ่อนไหว มีความสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงไม่ควรถามคำถามเช่นนี้กับผู้อื่น และผู้ถูกถามก็ไม่จำเป็นต้องตอบ ซึ่งอาจขัดต่อกฎหมายคุ้มครองข้อมูลส่วนบุคคล

สถานการณ์จำลอง 4

ไม่ถูกต้อง เนื่องจากหน้าข้อมูลหนังสือเดินทางประกอบด้วยข้อมูลส่วนบุคคลที่สำคัญมากมาย เช่น เลขบัตรประชาชน ชื่อ-นามสกุล วันเดือนปีเกิด ซึ่งข้อมูลทั้งหมดอาจถูกลักลอบนำไปใช้เกี่ยวกับอาชญากรรมข้ามชาติได้ และอาจขัดต่อกฎหมายคุ้มครองข้อมูลส่วนบุคคล

สถานการณ์จำลอง 5

ถูกต้อง ถึงแม้ว่าข้อมูลทางการแพทย์จะเป็นข้อมูลส่วนบุคคล แต่หากมีจุดประสงค์เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล สามารถเปิดเผยได้โดยไม่ต้องขอความยินยอม (กฎหมายมีข้อยกเว้นให้บางประการ)

สถานการณ์จำลอง 6

ไม่ถูกต้อง เนื่องจากห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และยังเป็นการนำข้อมูลส่วนบุคคลที่ตนเองเก็บไว้ไปใช้ผิดวัตถุประสงค์อีกด้วย ซึ่งอาจขัดต่อกฎหมายคุ้มครองข้อมูลส่วนบุคคล

หน่วยการเรียนรู้ที่ 4 การถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยไซเบอร์
แผนการจัดกิจกรรม 4.1 เรื่องการถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ระยะเวลา 6 ชั่วโมง

สาระสำคัญ

การฝึกปฏิบัติ/สาธิตการให้ความรู้ เรื่อง พื้นฐานด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์ การป้องกันภัยไซเบอร์ขั้นพื้นฐาน และวิถีชีวิตบนโลกดิจิทัล

จุดประสงค์

เพื่อให้ผู้เข้ารับการอบรมฝึกปฏิบัติ การให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ขอบข่ายเนื้อหา

การฝึกปฏิบัติ/สาธิตการให้ความรู้ตามหน่วยการเรียนรู้ จำนวน 3 เรื่อง คือ
หน่วยการเรียนรู้ที่ 1 เรื่อง พื้นฐานด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์
หน่วยการเรียนรู้ที่ 2 เรื่อง การป้องกันภัยไซเบอร์ขั้นพื้นฐาน
หน่วยการเรียนรู้ที่ 3 เรื่อง วิถีชีวิตบนโลกดิจิทัล

สื่อการเรียนรู้

ตามเล่มเอกสารหลักสูตรฝึกอบรมการจัดกิจกรรมการเรียนรู้ความมั่นคงปลอดภัยไซเบอร์ฉบับนี้

วัสดุอุปกรณ์

ตามรายละเอียดแผนการจัดกิจกรรมของแต่ละหน่วยการเรียนรู้

ขั้นตอนการจัดกิจกรรม

1. ชี้แจงการถ่ายทอดความรู้ด้านความมั่นคงปลอดภัยไซเบอร์
2. แบ่งกลุ่มผู้เข้ารับการอบรม กลุ่มละ 10 – 12 คน
3. แต่ละกลุ่มแบ่งเนื้อหาให้สมาชิกในกลุ่มเลือกคนละ 1 เรื่อง
4. สมาชิกแต่ละคนวางแผนการเป็นวิทยากร
5. สาธิตการให้ความรู้ในเรื่องที่รับผิดชอบ สมาชิกในกลุ่มที่เหลือ ทำหน้าที่เป็นผู้เข้ารับการอบรม (ผลัดกันเป็นวิทยากร ผลัดกันเป็นผู้เข้ารับการอบรม)
6. วิทยากรประจำกลุ่ม ประเมินการสาธิตการเป็นวิทยากรรายบุคคล

การวัดและประเมินผล

แบบประเมินการสาธิตการให้ความรู้

ภาคผนวก ข

การประเมินผลโดยการสาธิตการให้ความรู้

1. แบบประเมินผลการสาธิตการให้ความรู้

1.1 ชื่อผู้รับการประเมิน: .....

ประเด็นการประเมิน	ดีมาก (3 คะแนน)	ดี (2 คะแนน)	พอใช้ (1 คะแนน)
1. ความถูกต้องของเนื้อหา	☐	☐	☐
2. ความชัดเจนในการถ่ายทอด	☐	☐	☐
3. การเลือกใช้สื่อ/เทคโนโลยี	☐	☐	☐
4. การสร้างการมีส่วนร่วม	☐	☐	☐
5. เวลาในการนำเสนอเหมาะสม	☐	☐	☐
6. มีการสร้างบรรยากาศการเรียนรู้	☐	☐	☐

1.2 จุดเด่น

.....

.....

.....

1.3 จุดด้อย

.....

.....

.....

1.4 ข้อเสนอแนะเพิ่มเติม

.....

.....

.....

ลงชื่อ.....ผู้ประเมิน

(.....)

2. เกณฑ์การประเมินการสาธิตการให้ความรู้

2.1 เกณฑ์การประเมิน

ประเด็นการประเมิน	ระดับคุณภาพ		
	ดีมาก	ดี	พอใช้
1. ความถูกต้องของเนื้อหา	เนื้อหาถูกต้องครบถ้วน ชัดเจน และมีการเพิ่มเติมข้อมูลเสริมที่เป็นประโยชน์	เนื้อหาถูกต้อง ครบถ้วนในประเด็นสำคัญ	เนื้อหามีบางส่วนคลาดเคลื่อนหรือไม่ครบถ้วน
2. ความชัดเจนในการถ่ายทอด	ถ่ายทอดได้ชัดเจน สื่อสารเข้าใจง่าย และมีการยกตัวอย่างประกอบที่ทำให้เข้าใจลึกซึ้ง	ถ่ายทอดได้ชัดเจนเข้าใจง่ายในระดับหนึ่ง	ถ่ายทอดเนื้อหาบางช่วงไม่ชัดเจน ทำให้ผู้ฟังสับสน
3. การเลือกใช้สื่อ/เทคโนโลยี	ใช้สื่อตรงตามเนื้อหาประเด็นหรือหัวข้อที่สอน เหมาะสมมีเทคนิคช่วยส่งเสริมการเรียนรู้ หรือใช้สื่ออื่นเสริม	ใช้สื่อตรงตามเนื้อหาประเด็นหรือหัวข้อที่สอน เหมาะสมแต่ขาดเทคนิคช่วยส่งเสริมการเรียนรู้	ใช้สื่อไม่ตรงประเด็นหรือหัวข้อที่สอนหรือใช้แต่ขาดเทคนิคช่วยส่งเสริมการเรียนรู้
4. การสร้างการมีส่วนร่วม	เปิดโอกาสให้ผู้ฟังมีส่วนร่วมอย่างต่อเนื่องและสร้างบรรยากาศที่กระตือรือร้น	เปิดโอกาสให้ผู้ฟังมีส่วนร่วมพอสมควร	เปิดโอกาสให้ผู้ฟังมีส่วนร่วมน้อย
5. เวลาในการนำเสนอเหมาะสม	ใช้เวลาเหมาะสม บริหารเวลาได้ดีและไม่ทำให้ผู้ฟังรู้สึกยืดเยื้อหรือตัดจบเร็วเกินไป	ใช้เวลาเหมาะสมตามที่กำหนด	ใช้เวลาไม่เหมาะสมล่าช้าหรือเร่งรีบเกินไป
6. การสร้างบรรยากาศการเรียนรู้	บรรยากาศเป็นกันเอง กระตุ้นให้เกิดการเรียนรู้และความสนใจตลอดการนำเสนอ	บรรยากาศเอื้อต่อการเรียนรู้ในระดับที่เหมาะสม	บรรยากาศไม่เอื้อต่อการเรียนรู้มากนัก

2.2 เกณฑ์การตัดสิน ได้ระดับคุณภาพดีขึ้นไปถือว่าผ่าน

2.3 เกณฑ์การตัดสินคุณภาพ

ช่วงคะแนน	ระดับคุณภาพ
6 - 10 คะแนน	พอใช้
11 - 14 คะแนน	ดี
15 - 18 คะแนน	ดีมาก

ภาคผนวก ค

การประเมินโดยการสังเกตพฤติกรรมการเรียนรู้ผู้เข้ารับการอบรม

1. แบบสังเกตพฤติกรรมการเรียนรู้ผู้เข้ารับการอบรม

เรื่อง.....

ชื่อ - สกุล	ประเด็นการประเมิน															คะแนน	ระดับคุณภาพ
	1. มีความรับผิดชอบต่องานที่ได้รับมอบหมาย			2. การสื่อสารแลกเปลี่ยนเรียนรู้อย่างสร้างสรรค์			3. นำเสนอแนวคิดหรือแนวทางการนำความรู้ไปประยุกต์ใช้			4. การให้ความร่วมมือและการมีส่วนร่วมในกิจกรรมการเรียนรู้			5. ความตั้งใจในการเรียนรู้				
	3	2	1	3	2	1	3	2	1	3	2	1	3	2	1		

ลงชื่อ.....ผู้ประเมิน

(.....)

2. เกณฑ์การประเมินพฤติกรรมการเรียนรู้ผู้เข้ารับการอบรม

เรื่อง.....

2.1 เกณฑ์การประเมิน

ประเด็นการประเมิน	ดีมาก (3 คะแนน)	ดี (2 คะแนน)	พอใช้ (1 คะแนน)
1. มีความรับผิดชอบต่องานที่ได้รับมอบหมาย	ผลการปฏิบัติงานมีความครบถ้วนเป็นแบบอย่างได้	ผลการปฏิบัติงานมีความครบถ้วน ถูกต้อง	ผลการปฏิบัติงานยังไม่ครบถ้วนสมบูรณ์บางส่วน
2. การสื่อสารแลกเปลี่ยนเรียนรู้อย่างสร้างสรรค์	ถ่ายทอดความรู้/แสดงความคิดได้ชัดเจนโดยใช้ภาษาและท่าทีเหมาะสม เป็นต้นแบบและรับฟังความคิดเห็นผู้อื่น	ถ่ายทอดความรู้/แสดงความคิดได้ชัดเจนโดยใช้ภาษาและท่าทีเหมาะสม และรับฟังความคิดเห็นผู้อื่น	ถ่ายทอดความรู้/แสดงความคิดได้ชัดเจนโดยใช้ภาษาและท่าทีเหมาะสมเป็นบางครั้ง
3. นำเสนอแนวคิดหรือแนวทางการนำความรู้ไปประยุกต์ใช้	นำเสนอแนวคิดหรือแนวทางการนำความรู้ไปประยุกต์ใช้ได้อย่างเหมาะสม และนำไปใช้เป็นตัวอย่างได้	นำเสนอแนวคิดหรือแนวทางการนำความรู้ไปประยุกต์ใช้ได้อย่างเหมาะสม และเป็นไปได้	นำเสนอแนวคิดหรือแนวทางการนำความรู้ไปประยุกต์ใช้ได้บางส่วน
4. การให้ความร่วมมือและการมีส่วนร่วมในกิจกรรมการเรียนรู้	ให้ความร่วมมือและมีส่วนร่วมทุกกิจกรรม ด้วยความกระตือรือร้น	ให้ความร่วมมือและมีส่วนร่วมทุกกิจกรรม	ให้ความร่วมมือ และมีส่วนร่วมบางกิจกรรม
5. ความตั้งใจในการเรียนรู้	ตั้งใจเรียนรู้อย่างสม่ำเสมอ มีสมาธิตลอดเวลา	ตั้งใจเรียนรู้เป็นส่วนใหญ่ มีสมาธิพอสมควร	ไม่ค่อยตั้งใจเรียนรู้ บ่อยครั้งที่ขาดสมาธิ

2.2 เกณฑ์การตัดสิน ได้ระดับคุณภาพดีขึ้นไปถือว่าผ่าน

2.3 เกณฑ์การตัดสินคุณภาพ

ช่วงคะแนน	ระดับคุณภาพ
5 - 8 คะแนน	พอใช้
9 - 12 คะแนน	ดี
13 - 15 คะแนน	ดีมาก

ภาคผนวก ง

ตารางแสดงรายการคลิปวิดีโอประกอบ
หลักสูตรฝึกอบรมการจัดกิจกรรมการเรียนรู้ความมั่นคงปลอดภัยไซเบอร์

รายละเอียดดัง QR Code และ Short link ที่แนบ

https://shorturl.asia/pqY5m

ภาคผนวก จ

รายนามคณะผู้จัดทำ

ที่ปรึกษา

นายธนากร ดอนเหนือ	อธิบดีกรมส่งเสริมการเรียนรู้
พลอากาศตรี อมร ชมเชย	เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นายชัยพัฒน์ พันธุ์วัฒนสกุล	รองอธิบดีกรมส่งเสริมการเรียนรู้
นางศุทธินี งามเขตต์	อดีตผู้เชี่ยวชาญเฉพาะด้านพัฒนาหลักสูตร

ผู้รับผิดชอบโครงการ

นางสาวเอื้อมพร ศรีภูวงศ์	หัวหน้าและเลขานุการโครงการ
นายวรัตม์ ศรีเทพ	คณะทำงานและผู้ช่วยเลขานุการ
นางสาวสุจิตตรา เทพเทียน	คณะทำงานและผู้ช่วยเลขานุการ

คณะทำงาน

นางสาวเอื้อมพร ศรีภูวงศ์	ผู้อำนวยการกองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้
พันตรี ปวิช บูรพาชลทิศน์	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นายวงศกร นาคนาวา	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นางสาววัชราวลี วงษ์สุนา	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นายจิรายุส ปรีชาเดช	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
พันจ่าอากาศเอกธนรัตน์ วุฒิพรพงษ์	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นางวิบูลผล พร้อมมูล	ผู้อำนวยการสำนักงาน สกร.ประจำจังหวัดชลบุรี
นางอัญชลี ปสันตา	รองผู้อำนวยการสำนักงาน สกร.ประจำกรุงเทพมหานคร
นางสาวจิราภรณ์ ตันติถาวร	ผู้อำนวยการ สกร.ระดับเขตธนบุรี กรุงเทพมหานคร
นางสาวไพจิตร คงแก้ว	ผู้อำนวยการ สกร.ระดับอำเภอเมืองสมุทรสาคร จังหวัดสมุทรสาคร
นายสุรเชษฐ์ สุนทรากร	ผู้อำนวยการ สกร.ระดับอำเภอเมืองภูเก็ต จังหวัดภูเก็ต
นางสาวนุรัต วรกฎ	ผู้อำนวยการ สกร.ระดับอำเภอบ้านฝาง จังหวัดขอนแก่น
นางสาวอรทัย ปานขาว	ครูชำนาญการพิเศษ สกร.ระดับอำเภอเมืองระยอง จังหวัดระยอง
นางธัญรัศม์ มิ่งไชยอนันต์	ครูชำนาญการพิเศษ สกร.ระดับอำเภอสว่างวีระวงศ์ จังหวัดอุบลราชธานี
นางสาวสมร จันทร์หา	ครูชำนาญการพิเศษ สกร.ระดับเขตมีนบุรี กรุงเทพมหานคร
นางสาวเยาวภา บุญญาธิการ	ครูชำนาญการพิเศษ สกร.ระดับเขตห้วยขวาง กรุงเทพมหานคร
นางสาวปริญญารัตน์ ม้าทอง	ครูชำนาญการ สกร.ระดับเขตสายไหม กรุงเทพมหานคร

คณะทำงาน (ต่อ)

นายณัฐวัฒน์ หงษ์จุ้ย	ครู สกร.ระดับอำเภอทุ่งช้าง จังหวัดน่าน
นายณัฐพล วรมิตรปุญวงศ์	ครู สกร.ระดับอำเภอป่าบอน จังหวัดพัทลุง
นางสาวพจมาน จงไกรจักร์	ครู สกร.ระดับอำเภองาว จังหวัดลำปาง
นางสาวบีบีฮวา สะมัท	ครู สกร.ระดับอำเภอเมืองนครปฐม จังหวัดนครปฐม
นางสาวณภษร ศรีบุณยะแก้ว	ครู สกร.ระดับอำเภอเมืองชลบุรี จังหวัดชลบุรี
นางสาวณัฐฐิญา ทองศิริอุบล	ครู สกร.ระดับอำเภอศรีบุญเรือง จังหวัดหนองบัวลำภู
นายเดชดนัย มิฟองฟู	ครูศูนย์การเรียนรู้ สกร.ระดับอำเภอแม่ระมาด จังหวัดตาก
นางสาวพรรณทิพย์ สว่างศรี	ครูศูนย์การเรียนรู้ สกร.ระดับอำเภอเดิมบางนางบวช จังหวัดสุพรรณบุรี
นางสาวตรีรยา ศรีศักดา	ครูศูนย์การเรียนรู้ สกร.ระดับอำเภอเดิมบางนางบวช จังหวัดสุพรรณบุรี
นายธวัช ทองหล่อ	ครูศูนย์การเรียนรู้ สกร.ระดับอำเภอเมืองนครปฐม จังหวัดนครปฐม
นางสาวชนัญชิดา สยานันท์	นักวิชาการศึกษาชำนาญการพิเศษ กองมาตรฐานและส่งเสริมการเรียนรู้เพื่อคุณวุฒิ
นายวรัตม์ ศรีเทพ	นักวิชาการศึกษาชำนาญการ กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้
นางสาวสุพัตรา นนท์แก้ว	นักวิชาการศึกษาปฏิบัติการ กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้
นางสาวธมลวรรณ วรรณภูงา	นักวิชาการศึกษา กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้
นางสาวสุจิตตรา เทพเทียน	นักวิชาการศึกษา กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้
นางสาวปัทมา สนั่นโสตร	นักวิชาการศึกษา กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้
นางสาวปรียาวดี คำวัน	นักวิชาการศึกษา กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้

คลิปวิดีโอประกอบหลักสูตรฯ

CYBER SECURITY

LEARNING ACTIVITIES TRAINING COURSE

กรมส่งเสริมการเรียนรู้
กระทรวงศึกษาธิการ

กลุ่มพัฒนาทักษะการเรียนรู้
กองส่งเสริมและพัฒนานวัตกรรมการเรียนรู้

www.korpor.dole.go.th