

สรุปบทเรียนการพัฒนาความรู้

หลักสูตร

"Digital Literacy: ความฉลาดทางดิจิทัล (Digital Intelligence)"

ชื่อ-สกุล (ภาษาไทย) นางสาวทิพานันท์ อุปนิสากร ตำแหน่ง นักวิทยาศาสตร์ปฏิบัติการ

สังกัด กลุ่มวิจัยเคมีดิน สำนักวิทยาศาสตร์เพื่อการพัฒนาที่ดิน

วันที่อบรม 31 สิงหาคม 2569

วัตถุประสงค์

- เพื่อให้ผู้เรียนเข้าใจความหมาย ตระหนักรู้ถึงความสำคัญ และมีทักษะในการใช้งานอินเทอร์เน็ตและเทคโนโลยีดิจิทัลอย่างเหมาะสม
- เพื่อให้ผู้เรียนมีความรู้เท่าทันภัยคุกคามไซเบอร์ รู้วิธีการปกป้องข้อมูลส่วนบุคคล และสามารถนำเทคโนโลยีดิจิทัลมาประยุกต์ใช้เพื่อยกระดับคุณภาพชีวิตและการทำงานได้อย่างปลอดภัย

สรุปบทเรียน

1. ความเข้าใจเกี่ยวกับโลกดิจิทัล (Digital Realm & Reality)

โลกดิจิทัล คือ สภาพแวดล้อมเสมือนจริงที่เกิดจากการเชื่อมต่อของเทคโนโลยีสารสนเทศเครือข่ายอินเทอร์เน็ต และอุปกรณ์อิเล็กทรอนิกส์ เพื่อช่วยอำนวยความสะดวกในการสืบค้นข้อมูล การติดต่อสื่อสาร การเผยแพร่เนื้อหา และการรับบริการต่าง ๆ ได้อย่างรวดเร็ว อย่างไรก็ตาม โลกดิจิทัลและโลกความจริงมีคุณลักษณะที่แตกต่างกันอย่างชัดเจน ดังนี้

มิติการเปรียบเทียบ	โลกดิจิทัล (Digital World)	โลกความจริง (Real World)
การสืบค้นและเข้าถึงสารสนเทศ	สะดวกรวดเร็วผ่านอุปกรณ์พกพา เข้าถึงข้อมูลได้ตลอด 24 ชั่วโมง ไร้ข้อจำกัดด้านเวลาและสถานที่	มีข้อจำกัดทางกายภาพ ต้องเดินทางไปยังสถานที่จัดเก็บ เช่น ห้องสมุดหรือคลังเอกสาร หรือรอคอยสื่อสิ่งพิมพ์
การสื่อสารและการถ่ายทอดความรู้สึก	อาศัยการพิมพ์ข้อความหรือสื่อดิจิทัลเป็นหลัก การส่งผ่านอารมณ์ความรู้สึกและความเข้าใจเชิงลึกทำได้จำกัด	สื่อสารแบบเห็นหน้า สังเกตส่ายตา น้ำเสียง และภาษากายได้ สร้างความเข้าใจและอารมณ์ร่วมได้ดีกว่า
การปฏิบัติกิจกรรมและกระบวนการ	รองรับกิจกรรมจำลองหรือขั้นตอนที่ไม่ซับซ้อน เหมาะกับการส่งผ่านข้อมูล และเอกสารอิเล็กทรอนิกส์	มีความสมบูรณ์สูงสำหรับงานที่ต้องลงมือปฏิบัติจริง ใช้ทักษะความเชี่ยวชาญ และการประสานงานเชิงกายภาพ

2. อัตลักษณ์และการคุ้มครองความเป็นส่วนตัวดิจิทัล (Digital Identity & Privacy)

อัตลักษณ์ดิจิทัล (Digital Identity) คือภาพลักษณ์และตัวตนทางออนไลน์ที่เกิดจากรอยการเผยแพร่ข้อมูล การลงทะเบียน หรือกิจกรรมต่าง ๆ บนเครือข่ายอินเทอร์เน็ต ซึ่งส่งผลต่อการรับรู้ของผู้อื่นในสังคมออนไลน์

2.1 ความเป็นส่วนตัวในโลกดิจิทัล

2.2.1 ข้อมูลส่วนตัวที่เปิดเผยได้โดยพลอดภัย: ข้อมูลที่ไม่ก่อให้เกิดความเสียหาย เช่น ชื่อ-นามสกุล เพศ อายุ งานอดิเรก หรือความสนใจทั่วไป

2.2.2 ข้อมูลที่ต้องปกปิดเป็นความลับ: หมายเลขบัตรประจำตัวประชาชน เลขที่บัญชีธนาคาร/บัตรเครดิต เบอร์โทรศัพท์ส่วนตัว ที่อยู่พักอาศัยและวันเดือนปีเกิด

2.2.3 มาตรการป้องกันความปลอดภัยเชิงปฏิบัติ: หลีกเลี่ยงการตั้งค่าบัญชีโซเชียลมีเดียเป็นสาธารณะ กำหนดรหัสผ่านที่ซับซ้อนและเปลี่ยนตามรอบระยะเวลา ตั้งค่าระบบกู้คืนบัญชี อัปเดตระบบปฏิบัติการอุปกรณ์ให้ทันสมัย และตรวจสอบเงื่อนไขสิทธิการเข้าถึงข้อมูลของแอปพลิเคชันก่อนกดยินยอมทุกครั้ง

2.3 กรอบกฎหมายที่เกี่ยวข้องและบทลงโทษ

2.3.1 พ.ร.บ. คຸ້ມครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA): กำกับดูแลไม่ให้หน่วยงานหรือองค์กรนำข้อมูลส่วนบุคคลไปใช้หรือเผยแพร่โดยไม่ได้รับความยินยอมและให้การคุ้มครองเข้มงวดแก่ ข้อมูลอ่อนไหว (Sensitive Data) เช่น เชื้อชาติ ศาสนา ความคิดเห็นทางการเมือง พฤติกรรมทางเพศ และประวัติอาชญากรรม

- 1) โทษทางอาญา: จำคุกไม่เกิน 1 ปี และ/หรือปรับสูงสุดไม่เกิน 1 ล้านบาท
- 2) โทษทางแพ่ง: จ่ายค่าสินไหมทดแทนจริง และค่าสินไหมเพื่อการลงโทษสูงสุด 2 เท่า
- 3) โทษทางปกครอง: ปรับสูงสุดไม่เกิน 5 ล้านบาท

2.3.2 พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับปี 2550 และ 2560): กำหนดความผิดและบทลงโทษเกี่ยวกับการใช้งานระบบและข้อมูลคอมพิวเตอร์โดยมิชอบ

- 1) มาตรา 9-10 แก้ไข ดัดแปลง ทำลายข้อมูลผู้อื่นโดยมิชอบ โทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ
- 2) มาตรา 11 ส่งข้อมูลหรืออีเมลสแปมก่อความรำคาญผู้อื่น โทษจำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 40,000 บาท หรือทั้งจำทั้งปรับ
- 3) มาตรา 14 นำข้อมูลเท็จหรือข้อมูลอันเป็นภัยเข้าสู่ระบบคอมพิวเตอร์ โทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 600,000 บาท หรือทั้งจำทั้งปรับ

3. การใช้เทคโนโลยีอย่างเหมาะสมและมีจริยธรรม (Digital Use & Empathy)

3.1 การใช้เทคโนโลยีอย่างสมดุล (Balanced Use of Technology): การใช้อุปกรณ์ดิจิทัลยาวนานเกินไป ส่งผลเสียต่อสุขภาพ เช่น ปัญหาสายตาจากแสงสะท้อนหรือตัวหนังสือขนาดเล็กเกินไป และอาการปวดกล้ามเนื้อคอ บ่า ไหล่ (Office Syndrome) จากการนั่งผิดท่า จึงต้องบริหารเวลาพักสายตาและปรับเปลี่ยนอิริยาบถอย่างสม่ำเสมอ

3.2 แนวทางที่ควรปฏิบัติ (Digital Empathy): สื่อสารด้วยความจริงใจ ให้เกียรติผู้อื่น มีสติและพิจารณาญาณในการไตร่ตรองข้อมูลก่อนโพสต์หรือตอบโต้

3.3 แนวทางที่ควรงดเว้น: การพิมพ์ข้อความหยอกล้อที่สุ่มเสี่ยงต่อการเข้าใจผิด การโพสต์ไว้อย่างตอว่า ตำหนิ หรือการนินทาให้ร้ายผู้อื่น

3.4 ประเภทเนื้อหาที่ต้องระมัดระวัง: ผลงานที่มีลิขสิทธิ์ ประเด็นความขัดแย้งทางศาสนา และความเชื่อ ภาพความรุนแรงหรือทารุณกรรม ภาพแอบถ่าย และข้อมูลส่วนบุคคลที่ไม่อนุญาตให้เผยแพร่

4. การจัดการความปลอดภัยและภัยคุกคามทางไซเบอร์ (Digital Security)

การล่วงละเมิดทางไซเบอร์ (Cyber Abuse) คือ พฤติกรรมที่เป็นอันตราย สร้างความรำคาญ หรือก่อความเสียหายแก่ผู้อื่นทางออนไลน์ แบ่งเป็น 4 รูปแบบหลัก

4.1 การกระรานทางไซเบอร์ (Cyberbullying): การกลั่นแกล้ง ให้อาย ด่าว่า ข่มเหง หรือรังแกผู้อื่นผ่านโซเชียลมีเดีย

4.2 การรังควานทางไซเบอร์ (Cyber Harassment): การละเมิดที่รุนแรงกว่าการกระราน โดยส่งข้อความหรือคอมเมนต์ทำร้ายจิตใจอย่างต่อเนื่อง

4.3 การสะกดรอยตามทางไซเบอร์ (Cyber Stalking): การติดตาม เฝ้ามอง หรือส่งข้อความก่อกวนซ้ำ ๆ จากบุคคลที่ไม่ต้องการ

4.4 การก่อกวน (Trolling): การเจตนาโพสต์ข้อความยั่วยุ บั่นป่วน เพื่อให้ผู้อื่นเกิดโทสะ ตกใจ หรือขัดแย้งกัน

5. อื่นๆ

5.1 ความเสี่ยง: โดยสาเหตุแห่งความเสี่ยงนั้นเกิดจากการตั้งรหัสผ่านง่ายเกินไป อุปกรณ์ไม่มีซอฟต์แวร์ป้องกันภัยคุกคาม หรือความประมาทในการกดลิงก์แปลกปลอม

5.2 ผลกระทบและช่องทางช่วยเหลือ: กระทบต่อบุคคล (ถูกขโมยอัตลักษณ์หรือนำข้อมูลไปแอบอ้าง) และกระทบต่ออุปกรณ์ (ถูกมัลแวร์โจมตีหรือเรียกค่าไถ่ Ransomware)

5.3 ภัยคุกคาม: ได้แก่ อีเมลอันตราย สแปม ฟิชซิง มัลแวร์ ภัยจากการซื้อสินค้าออนไลน์ และภัยจากการไม่สำรองข้อมูล ทั้งนี้สามารถตรวจสอบและแจ้งเหตุภัยคุกคามได้ผ่าน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) และศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ

ประโยชน์ที่ได้รับต่อตนเอง

1. ได้รับความรู้ ความเข้าใจ และสามารถนำไปปรับใช้ในด้านจริยธรรมการใช้คอมพิวเตอร์
2. ได้รับความรู้และสามารถนำไปปฏิบัติงานด้านดิจิทัลและสามารถตรวจสอบการทำงานตามการปฏิบัติงานเบื้องต้นได้อย่างถูกต้อง ปลอดภัย

ประโยชน์ที่ได้รับต่อหน่วยงาน

1. รู้เท่าทัน และเสริมสร้างความปลอดภัยทางไซเบอร์ขององค์กร โดยลดความเสี่ยงจากการถูกโจมตีข้อมูล หรือภัยคุกคามทางดิจิทัล เนื่องจากบุคลากรมีความรู้เท่าทันการหลอกลวง และรู้วิธีป้องกันระบบตามหลักปฏิบัติที่ถูกต้อง

2. ลดความเสี่ยงทางกฎหมายและจริยธรรม โดยการดำเนินงานของหน่วยงานจะเป็นไปอย่างถูกต้องตามหลักจริยธรรมคอมพิวเตอร์และกฎหมายลิขสิทธิ์ ช่วยป้องกันปัญหาการละเมิดทรัพย์สินทางปัญญาของผู้อื่นในการผลิตผลงาน