

Digital Literacy : ความฉลาดทางดิจิทัล (Digital Intelligence)

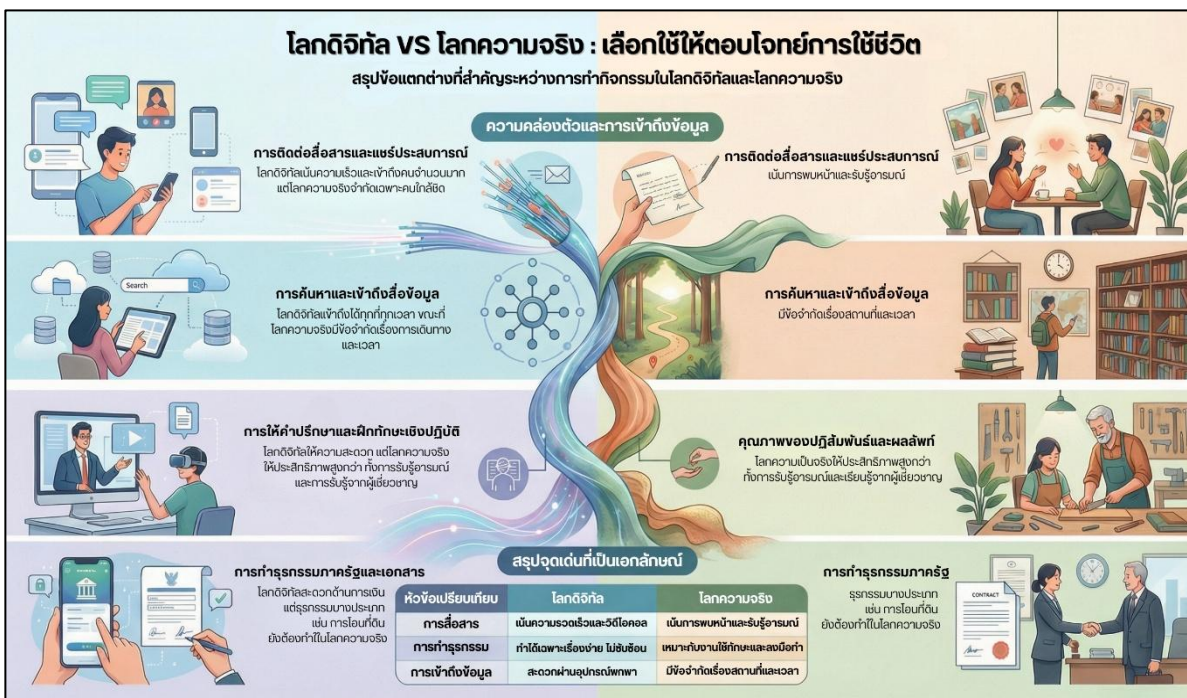
โดย นางสาวเพ็ญภา ศีลาคำ
นักวิชาการแผนกที่ภาพถ่ายปฏิบัติการ

วัตถุประสงค์

1. เพื่อให้มีความรู้ความเข้าใจเกี่ยวกับองค์ประกอบและการปฏิบัติตนในโลกดิจิทัลอย่างถูกต้อง
2. เพื่อสร้างทักษะการปกป้องข้อมูลส่วนบุคคลและการจัดการความปลอดภัยทางไซเบอร์

สรุปเนื้อหา

โลกดิจิทัล (Digital World) หมายถึง โลกเสมือนที่ถูกสร้างขึ้นควบคู่กับโลกแห่งความเป็นจริง โดยมีองค์ประกอบทั้งพื้นที่ ผู้คน และทรัพยากรที่สามารถจำลองกิจกรรมต่าง ๆ ได้ผ่านอุปกรณ์อิเล็กทรอนิกส์ และเครือข่ายอินเทอร์เน็ต โลกดิจิทัลจึงเป็นพื้นที่สำคัญที่ผู้คนสามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และดำเนินกิจกรรมต่าง ๆ ได้อย่างไร้ข้อจำกัดด้านเวลาและสถานที่ สามารถพิจารณาข้อแตกต่างระหว่างโลกแห่งความเป็นจริงและโลกดิจิทัลได้ดัง ภาพที่ ๑



ภาพที่ ๑ ข้อแตกต่างที่สำคัญระหว่างโลกดิจิทัลและโลกความจริง

ที่มา : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

อัตลักษณ์ดิจิทัล (Digital Identity) หมายถึง ข้อมูลที่ใช้ระบุและสะท้อนตัวตนของคุณในโลกออนไลน์ ซึ่งช่วยให้สามารถเข้าถึงบริการต่าง ๆ ได้อย่างสะดวกและปลอดภัย อีกทั้งยังสะท้อนความสัมพันธ์ ปฏิสัมพันธ์ และภาพลักษณ์ที่บุคคลสื่อสารออกไปสู่สังคมดิจิทัล การสร้างอัตลักษณ์ดิจิทัลที่ดีจึงเป็นสิ่งสำคัญ เนื่องจากส่งผลต่อความน่าเชื่อถือและภาพลักษณ์ในระยะยาว

ความเป็นส่วนตัวในโลกดิจิทัล (Digital Privacy) หมายถึง สิทธิของคุณในการควบคุมและบริหารจัดการข้อมูลส่วนบุคคล รวมถึงกิจกรรมต่าง ๆ ที่เกิดขึ้นบนเครือข่ายอินเทอร์เน็ต เพื่อป้องกันไม่ให้ข้อมูลสำคัญถูกนำไปใช้โดยไม่ได้รับอนุญาต ข้อมูลส่วนบุคคลสามารถแบ่งออกเป็น ๒ ประเภท ได้แก่

๑. Personal Information ข้อมูลที่สามารถเปิดเผยได้ เช่น ชื่อ อายุ และความสนใจ เป็นต้น

๒. Private Information ข้อมูลที่ไม่ควรเปิดเผย เช่น เลขบัตรประชาชน เลขบัญชีธนาคาร ที่อยู่ และหมายเลขโทรศัพท์ เป็นต้น

การคุ้มครองข้อมูลส่วนบุคคลเกี่ยวข้องกับกฎหมายสำคัญ เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

การใช้เทคโนโลยีอย่างเหมาะสม (Digital Use) หมายถึง การกำกับควบคุมการใช้งานเทคโนโลยีให้อยู่ในระดับที่สมดุล เพื่อลดผลกระทบต่อสุขภาพและคุณภาพชีวิต โดยครอบคลุมการบริหารเวลา การเลือกรับสื่อ และการรักษาความสัมพันธ์ทางสังคม ทักษะดังกล่าวช่วยส่งเสริมให้เกิดการใช้เทคโนโลยีอย่างมีสติ และเกิดประโยชน์สูงสุด

การจัดการความปลอดภัยในโลกดิจิทัล (Digital Security) เป็นสิ่งสำคัญที่ช่วยป้องกันความเสียหายต่อข้อมูลและระบบเครือข่าย โดยครอบคลุมทั้งการป้องกันการล่อลวงละเมิดทางไซเบอร์ เช่น การกลั่นแกล้ง หรือคุกคามออนไลน์ และการป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดจากการตั้งรหัสผ่านที่ไม่รัดกุม หรือความประมาทในการใช้งาน โดยการจัดการความปลอดภัยในโลกดิจิทัล ประกอบด้วย

๑. การล่อลวงละเมิดทางไซเบอร์ (Cyber Abuse) คือ การแสดงพฤติกรรมที่เป็นอันตราย สร้างความรำคาญ หรือสร้างความเสียหายให้กับผู้อื่นบนเครือข่ายออนไลน์ต่าง ๆ ดังภาพที่ ๒



ภาพที่ ๒ การล่อลวงละเมิดทางไซเบอร์ (Cyber Abuse)

ที่มา : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

๒. ภัยคุกคามทางไซเบอร์ (Cyber Threat) คือ การกระทำหรือการดำเนินการใด ๆ ผ่านการใช้ระบบสารสนเทศหรือเครือข่ายที่ก่อให้เกิดผลเสียต่อระบบข้อมูลเครือข่ายหรือข้อมูลภายใน สาเหตุของภัยคุกคามทางไซเบอร์ ได้แก่ การตั้งพาสเวิร์ดที่ง่ายเกินไป โปรแกรมรักษาความปลอดภัยไม่ทำงาน และความประมาท ภัยคุกคามทางไซเบอร์แบ่งออกเป็น ๖ ประเภท ดังภาพที่ ๓

รู้เท่าทันภัยคุกคามทางไซเบอร์ (Understanding Cyber Threats)

ภัยคุกคามผ่านการสื่อสารและอีเมล (Communication & Email Threats)

อีเมลอันตราย (Dangerous Email)

อีเมลมุ่งเน้นการบุกรุกบัญชี เพื่อขโมยข้อมูลส่วนบุคคล หรือทรัพย์สิน

สแปม (Spam)

ข้อความที่ส่งโดยไม่ได้รับอนุญาต สร้างความรำคาญ และปฏิเสธการรับได้ยาก

ฟิชชิ่ง (Phishing)

การใช้อนบายหลอกล่อให้เหยื่อคลิกลิงก์ หรือกรอกข้อมูลส่วนตัวที่สำคัญ

ภัยจากระบบและพฤติกรรมการใช้งาน (System & Behavioral Threats)

มัลแวร์ (Malware)

โปรแกรมประสงค์ร้ายที่สร้างความเสียหายหรือเข้าควบคุมระบบคอมพิวเตอร์

ภัยจากการช้อปปิ้งออนไลน์ (Online Shopping Risks)

การสร้างกลโกงเพื่อหลอกให้ผู้ใช้โอนเงินหรือชำระเงินในช่องทางที่ไม่ปลอดภัย

ภัยจากการไม่สำรองข้อมูล (Data Backup Risks)

ความเสี่ยงที่จะสูญเสียข้อมูลทั้งหมด หากเก็บไว้ในคอมพิวเตอร์เพียงเครื่องเดียว

ภาพที่ ๓ ภัยคุกคามทางไซเบอร์ (Cyber Threat)

ที่มา : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

การรู้เท่าทันดิจิทัล (Digital Literacy) หมายถึง ทักษะที่ช่วยให้บุคคลสามารถใช้เทคโนโลยีได้อย่างมีประสิทธิภาพ ปลอดภัย และมีความรับผิดชอบ รวมถึงสามารถวิเคราะห์ ประเมิน และสร้างเนื้อหาได้อย่างเหมาะสม โดยแหล่งข้อมูลดิจิทัล สามารถแบ่งออกเป็น ๓ รูปแบบ ดังนี้

๑. แบ่งตามแหล่งที่เผยแพร่ข้อมูล ได้แก่ การสร้างหรือผลิตข้อมูลโดยเจ้าของแหล่งข้อมูล หรือชุมชนผู้ใช้งาน

๒. แบ่งตามสิทธิการเข้าถึงข้อมูล ได้แก่ การเข้าถึงได้อย่างเสรี และการจำกัดการเข้าถึง

๓. แบ่งตามประเภทของข้อมูล ได้แก่ แหล่งข้อมูลเพื่อการศึกษาเรียนรู้ เพื่อความบันเทิง ด้านสุขภาพ ด้านธุรกรรม และด้านเศรษฐศาสตร์

โดยข้อมูลที่มีคุณภาพควรมีความทันสมัย ถูกต้อง มีแหล่งอ้างอิง และระบุผู้เขียนอย่างชัดเจน สำหรับเนื้อหาดิจิทัลมีหลายประเภท เช่น ด้านสุขภาพ ภาครัฐ ความบันเทิง การตลาด การศึกษา และข่าวสาร ซึ่งถูกนำเสนอผ่านสื่อดิจิทัลในรูปแบบต่าง ๆ ได้แก่ ข้อความ รูปภาพ เสียง วิดีโอ และกราฟิก

ร่องรอยดิจิทัล (Digital Footprint) หมายถึง ข้อมูลที่เกิดจากการใช้งานอินเทอร์เน็ตและเทคโนโลยี ซึ่งสะท้อนพฤติกรรม ความสนใจ และตัวตนของบุคคล ร่องรอยดิจิทัลอาจเป็นทั้งเชิงบวก เช่น การสื่อสารอย่างสุภาพและสร้างสรรค์ หรือเชิงลบ เช่น การแสดงความคิดเห็นที่ไม่เหมาะสม โดยมีวิธีในการรับมือกับความเสียหายจากร่องรอยดิจิทัล ได้ดังภาพที่ ๔ ซึ่งแบ่งออกเป็น ๒ ประเภท ดังนี้

๑. ร่องรอยที่ตั้งใจสร้าง (Active Digital Footprints) ข้อมูลที่เราตั้งใจเปิดเผยหรือบันทึกในโลกออนไลน์ด้วยตัวเอง โดยที่เรารับรู้และเจตนาให้ข้อมูลนั้นปรากฏอยู่ เช่น การสื่อสาร ข้อมูลส่วนตัว การระบุตำแหน่ง และการแสดงออกบนโซเชียลมีเดีย เป็นต้น

๒. ร่องรอยที่ไม่ตั้งใจสร้าง (Passive Digital Footprints) ข้อมูลที่ถูกบันทึกไว้โดยอัตโนมัติจากการใช้งานอินเทอร์เน็ต โดยที่ผู้ใช้อาจไม่ได้สังเกตหรือตั้งใจจะทิ้งร่องรอยนั้นไว้ เช่น หมายเลขไอพี (IP Address) ที่ระบุตัวตนของเครื่องคอมพิวเตอร์ หรือมีชื่อ ประวัติการใช้งาน พฤติกรรมการบริโภค และการติดตามตำแหน่งแบบเรียลไทม์

วิธีรับมือกับความเสียหายจากร่องรอยดิจิทัล



ภาพที่ ๔ วิธีรับมือกับร่องรอยดิจิทัล (Digital Footprint)

ที่มา : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

การปรับตัวในยุคดิจิทัล (Digital Disruption) คือ การเปลี่ยนแปลงครั้งใหญ่จากเทคโนโลยีที่เข้ามาเข้ามามีผลต่อธุรกิจเดิมให้ใช้ไม่ได้ผลอีกต่อไป กลายเป็นทั้งแรงกดดันให้ต้องปรับตัวและเป็นโอกาสทองในการสร้างความได้เปรียบผ่านนวัตกรรมที่ล้ำสมัยกว่าเดิม หัวใจสำคัญ คือการตอบสนองความคาดหวังของลูกค้าที่สูงขึ้นด้วยความรวดเร็วและช่องทางออนไลน์ที่ครอบคลุม หากธุรกิจใดนำเทคโนโลยีมาประยุกต์ใช้ได้อย่างมีประสิทธิภาพ จะสามารถก้าวขึ้นเป็นผู้นำตลาดได้อย่างก้าวกระโดด

การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน

ความฉลาดทางดิจิทัลเป็นทักษะพื้นฐานที่จำเป็นในการใช้เทคโนโลยีอย่างมีประสิทธิภาพและปลอดภัย โดยครอบคลุมตั้งแต่การสร้างอัตลักษณ์ดิจิทัลที่ดีเพื่อความน่าเชื่อถือ การตระหนักถึงความเป็นส่วนตัว โดยแยกแยะข้อมูลที่เปิดเผยได้และข้อมูลส่วนตัวที่ไม่ควรเปิดเผย ไปจนถึงการรู้เท่าทันภัยคุกคามและการล่วงละเมิดทางไซเบอร์ในรูปแบบต่างๆ รวมถึงลดความเสี่ยงด้านความปลอดภัยทางไซเบอร์ในการทำงานได้อย่างมีประสิทธิภาพ

ประโยชน์ต่อตนเอง

๑. มีความรู้และทักษะในการใช้เทคโนโลยีดิจิทัลได้อย่างถูกต้องและปลอดภัย
๒. สามารถปกป้องข้อมูลส่วนบุคคลและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
๓. เพิ่มประสิทธิภาพในการทำงานและการใช้ชีวิตประจำวัน
๔. มีความตระหนักรู้และรับผิดชอบต่อการใช้สื่อและเทคโนโลยีดิจิทัลมากขึ้น

ประโยชน์ต่อองค์กร

๑. ช่วยให้องค์กรใช้เทคโนโลยีดิจิทัลได้อย่างถูกต้องและปลอดภัย
๒. ลดความเสี่ยงจากการรั่วไหลของข้อมูลและภัยคุกคามทางไซเบอร์
๓. เพิ่มประสิทธิภาพและความรวดเร็วในการปฏิบัติงาน เสริมสร้างความน่าเชื่อถือและภาพลักษณ์ที่ดีขององค์กร
๔. ส่งเสริมการปฏิบัติงานอย่างมีความรับผิดชอบ เป็นระบบ สนับสนุนการปฏิบัติตามนโยบายและมาตรฐานด้านความปลอดภัยข้อมูล

ประโยชน์ต่อสาธารณะ

๑. ทำให้ประชาชนได้รับบริการที่ปลอดภัยและเชื่อถือได้มากขึ้น
๒. ลดความเสี่ยงจากการรั่วไหลของข้อมูลส่วนบุคคล
๓. ส่งเสริมการใช้เทคโนโลยีดิจิทัลอย่างรู้เท่าทันและปลอดภัย
๔. เพิ่มความโปร่งใสและยกระดับคุณภาพการให้บริการสาธารณะ

แหล่งที่มา

หลักสูตร : Digital Literacy : ความฉลาดทางดิจิทัล Digital Intelligence

บรรยายโดย : อาจารย์สุมนต์ จิตรพัฒนพร หัวหน้ากลุ่มงานวิชาการคอมพิวเตอร์
มหาวิทยาลัยราชภัฏนครสวรรค์

สถาบัน: สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัลสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

รูปแบบหลักสูตร : การเรียนออนไลน์ (TDGA e-learning)

ช่วงเวลาการฝึกอบรม : กุมภาพันธ์ ๒๕๖๙