

ความฉลาดทางดิจิทัล (Digital Intelligence)

โดย นายเนติพงศ์ ศรีสว่าง
นักวิชาการแผนกภาพถ่ายปฏิบัติการ

วัตถุประสงค์

๑. เพื่อให้เข้าใจความหมาย ตระหนักรู้ถึงความสำคัญ และมีทักษะในการใช้งานอินเทอร์เน็ตและเทคโนโลยีดิจิทัลอย่างเหมาะสม

๒. เพื่อให้มีความรู้เท่าทันภัยคุกคามไซเบอร์ รู้วิธีการปกป้องข้อมูลส่วนบุคคล และสามารถนำเทคโนโลยีดิจิทัลมาประยุกต์ใช้เพื่อยกระดับคุณภาพชีวิตและการทำงานได้อย่างปลอดภัย

สรุปเนื้อหา

หลักสูตรนี้เป็นการประยุกต์ใช้กรอบมาตรฐานสากล DQ (Digital Intelligence Quotient) หรือ ความฉลาดทางดิจิทัล คือ กรอบแนวคิดที่ครอบคลุมความสามารถทางด้านเทคนิค ความรู้ ความเข้าใจ และความคิดทางสังคม ที่มีพื้นฐานอยู่ในค่านิยมทางศีลธรรม ซึ่งเป็นทักษะที่ช่วยให้บุคคลสามารถเผชิญหน้าและรับมือกับความท้าทายทางด้านดิจิทัลได้อย่างมีประสิทธิภาพ โดยกรอบแนวคิดนี้เป็นผลการศึกษาและพัฒนาโดย DQ Institute ร่วมกับ World Economic Forum เน้นในการพัฒนาครบทั้งมิติ "ความรู้ ทักษะ และทัศนคติ" เพื่อเตรียมความพร้อมก้าวเป็นพลเมืองดิจิทัลคุณภาพ ที่ทำงานได้อย่างมีประสิทธิภาพและใช้ชีวิตในโลกออนไลน์ได้อย่างปลอดภัย โดยมีโครงสร้างและองค์ประกอบหลัก ดังนี้

๑. อัตลักษณ์และโลกดิจิทัล (Digital Identity & Digital World)

๑.๑ อัตลักษณ์ดิจิทัล คือ ตัวตนที่เกิดจากข้อมูลที่ถูกเผยแพร่ออนไลน์ (ชื่อ รูปภาพ เบอร์โทรศัพท์ การกดถูกใจ) ซึ่งส่งผลทั้งเชิงบวก (โอกาสที่ดี ความสัมพันธ์ที่ดี) และเชิงลบ (การถูกคุกคาม)

๑.๒ โลกดิจิทัล คือ สังคมคู่ขนานที่เชื่อมโยงผู้คนเข้าด้วยกันผ่านอุปกรณ์และเทคโนโลยี ช่วยให้การค้นหาข้อมูล การสื่อสาร และการทำธุรกรรมภาครัฐหรือเอกชน เช่น การโอนที่ดินหรือการทำใบขับขี่ สามารถทำได้อย่างรวดเร็วทุกที่ทุกเวลา อย่างไรก็ตาม ผู้เรียนต้องใช้งานด้วยความระมัดระวัง มีมารยาท และเคารพผู้อื่น เช่นเดียวกับการปฏิบัติตนในโลกความเป็นจริง

ในการจัดการอัตลักษณ์ดิจิทัล เป็นการสร้างตัวตนบนโลกออนไลน์อย่างเหมาะสม จึงควรคิดก่อนโพสต์ทุกครั้งเนื่องจากข้อความและข้อมูลจะคงอยู่ถาวร ควรใช้ชื่อและรูปถ่ายจริง ไม่แอบอ้างเป็นผู้อื่น ต้องตั้งค่าความเป็นส่วนตัวอย่างรัดกุมโดยไม่เปิดเผยข้อมูลส่วนตัวที่สำคัญ เช่น เลขบัตรประชาชน หรือเลขบัญชีธนาคาร พร้อมทั้งหมั่นตรวจสอบกลุ่มที่เข้าร่วม และประวัติการใช้งานของตนเองอย่างสม่ำเสมอ

๒. การจัดการความปลอดภัยในโลกดิจิทัล (Digital Security)

คือ การปกป้องระบบคอมพิวเตอร์ อุปกรณ์ เครือข่าย และการถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การโจรกรรม หรือการโจมตีทางไซเบอร์ ผ่านการปฏิบัติตามนโยบาย กระบวนการ และการใช้เครื่องมืออย่างเหมาะสม มีรายละเอียดดังนี้

๒.๑ สาเหตุและช่องโหว่ความเสี่ยงทางไซเบอร์ เกิดจากการใช้รหัสผ่านที่คาดเดาง่าย การไม่อัปเดตระบบรักษาความปลอดภัย การหลอกล่อให้คลิกลิงก์ปลอม (Phishing) อีเมลขยะ (Spam) การติดไวรัสคอมพิวเตอร์ (Malware) รวมถึงภัยหลอกลวงจากการซื้อสินค้าออนไลน์

๒.๒ รูปแบบภัยคุกคามทางไซเบอร์ เกิดจาก การส่งข้อความก่อกวน (Online Harassment) การสะกดรอยตามออนไลน์ (Cyberstalking) การกลั่นแกล้งบนโลกดิจิทัล (Cyberbullying) และการโพสต์ข้อความยั่วเย้าเพื่อสร้างความขัดแย้ง (Trolling)

๒.๓ วิธีป้องกันและรับมือ ระวังการรับเพื่อน บล็อกบุคคลที่คุกคาม เปลี่ยนรหัสผ่านให้ซับซ้อนขึ้น ทำการสำรองข้อมูลสำคัญไว้บนคลาวด์ (Google Drive, iCloud, Dropbox, OneDrive) หากประสบภัยคุกคามสามารถแจ้งเหตุได้ที่ศูนย์รับแจ้งความออนไลน์ (Thai Police Online) หรือสายด่วน ETDA



ภาพที่ ๑ สถิติความเสียหายสะสมของศูนย์รับแจ้งความออนไลน์ (Thai Police Online)
(ที่มา : ภาพประกอบโดยศูนย์รับแจ้งความออนไลน์ (Thai Police Online) ณ วันที่ ๓ กันยายน ๒๕๖๙
<https://thaipoliceonline.go.th>)

๓. การรู้เท่าทันสื่อและการจัดทำสารสนเทศ (Media and Information Literacy/Create)

คือ การสืบค้นข้อมูลผ่านเครื่องมืออย่าง Google Search หรือ YouTube พร้อมทั้งประเมินความถูกต้อง ความน่าเชื่อถือ และคัดกรองข้อมูลที่ทันสมัยตรงตามวัตถุประสงค์ ตลอดจนการประยุกต์ใช้แอปพลิเคชัน อย่าง LINE, Facebook, Microsoft OneNote หรือ Google Keep เพื่อบันทึกและจัดการสารสนเทศ อย่างมีประสิทธิภาพ ก่อนนำมาใช้งาน

๔. การจัดทำสื่อและสารสนเทศ (Media and Information Creation)

คือ กระบวนการนำข้อมูลผ่านการประเมินและประมวลผล มาสรุป เรียบเรียงใหม่ เป็นสื่อรูปแบบต่าง ๆ เช่น ข้อความ รูปภาพ อินโฟกราฟิก หรือวิดีโอ โดยใช้เครื่องมือดิจิทัลอย่างเหมาะสม มีความรับผิดชอบ และเคารพลิขสิทธิ์ ทั้งนี้ ควรไตร่ตรองเนื้อหาก่อนโพสต์ คำนึงถึงความรู้สึกของผู้อ่าน สื่อสารเชิงบวก และไม่ละเมิดสิทธิผู้อื่น (เช่น ไม่นำภาพหรือข้อมูลส่วนตัวของผู้อื่นมาเผยแพร่โดยไม่ได้รับอนุญาต)

๕. จริยธรรมและกฎหมายที่เกี่ยวข้อง (Ethics & Laws)

คือ การเข้าใจและปฏิบัติตามหลักจริยธรรม บรรทัดฐานทางสังคม และข้อบังคับทางกฎหมาย ในการใช้งานดิจิทัล เพื่อให้สามารถปกป้องตนเองและเคารพสิทธิของผู้อื่นได้อย่างถูกต้อง โดยการสื่อสารด้วยความสุภาพ ไม่ให้เกียรติผู้อื่น ไม่ใช่ถ้อยคำรุนแรง บูลลี่ หรือสร้างความเกลียดชัง (Hate Speech) ไม่คัดลอก ดัดแปลง หรือนำผลงานของผู้อื่น (รูปภาพ บทความ วิดีโอ) ไปใช้โดยไม่ได้รับอนุญาต และต้องอ้างอิงแหล่งที่มา ทุกครั้ง และต้องไตร่ตรองความถูกต้องและผลกระทบก่อนที่จะกระทำการโพสต์หรือแชร์ข้อมูล

ดังนั้น การใช้งานดิจิทัลไม่ได้มีเพียงเรื่องของมารยาทหรือจริยธรรมเท่านั้น แต่ยังมีขอบเขตทางกฎหมายที่ต้องปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันตนเองจากการกระทำผิดโดยไม่ตั้งใจ และร่วมสร้างบรรทัดฐานสังคมออนไลน์ที่ปลอดภัย หากมีการละเมิดนอกจากจะสร้างผลกระทบต่จริยธรรม ซึ่งทำให้เกิดความขัดแย้ง และการเสื่อมเสียชื่อเสียงแล้ว ยังมีบทลงโทษทางกฎหมายที่เกี่ยวข้อง ได้แก่

- พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act, PDPA) ห้ามนำข้อมูลส่วนตัวผู้อื่นไปใช้โดยไม่ยินยอม บทลงโทษมีทั้งทางอาญา จำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิน ๑ ล้านบาท ทางแพ่งจ่ายสินไหมไม่เกิน ๒ เท่า และทางปกครอง ปรับไม่เกิน ๕ ล้านบาท

- พ.ร.บ. คอมพิวเตอร์ การโพสต์ข้อมูลเท็จ ข้อมูลหลอกลวง หรือเนื้อหาที่สร้างความเสียหายต่อความมั่นคง มีโทษจำคุกไม่เกิน ๕ ปี หรือปรับไม่เกิน ๑ ล้านบาท รวมถึงสร้างผลกระทบต่จริยธรรม ทำให้เกิดความขัดแย้งและเสื่อมเสียชื่อเสียงในสังคม

การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน

- ในฐานะปฏิบัติงานสามารถดูแลความปลอดภัยของข้อมูลและอุปกรณ์ได้ เริ่มจากการตั้งรหัสผ่านที่รัดกุม คาดเดายาก และอัปเดตระบบความปลอดภัยอย่างสม่ำเสมอเพื่อป้องกันการโจมตีทางไซเบอร์ ควบคุมไปกับการสื่อสารอย่างสร้างสรรค์ โดยนำเสนอการทำงานเชิงบวก หลีกเลี่ยงการใช้ถ้อยคำรุนแรง การละเมิดสิทธิ หรือการกลั่นแกล้งผู้อื่นทางออนไลน์ ต้องประเมินคุณภาพของข้อมูลก่อนนำมาอ้างอิง โดยตรวจสอบทั้งความถูกต้อง ความน่าเชื่อถือ และความทันสมัย รวมถึงต้องตรวจสอบข้อมูลให้ชัวร์ก่อนแชร์ ไม่ส่งต่อเนื้อหาเท็จหรือสิ่งที่ก่อให้เกิดความเสียหายต่อหน่วยงาน เพื่อป้องกันการกระทำผิดตาม พ.ร.บ. คอมพิวเตอร์

ประโยชน์ที่ได้รับ

- ต่อตนเอง การตั้งรหัสผ่านที่รัดกุมและไม่ใช้ข้อมูลส่วนตัวที่คาดเดายาก ช่วยลดเสี่ยงจากการถูกโจรกรรมข้อมูล มัลแวร์ และภัยมิจฉาชีพ การสร้างอัตลักษณ์ดิจิทัลเชิงบวกช่วยสร้างความประทับใจที่ดี ช่วยกระชับความสัมพันธ์กับคนรอบข้าง รู้จักวิธีป้องกันตนเองด้วยการไม่ตอบโต้ บล็อก และรายงานผู้ก่อวนเพื่อลดความเครียดและผลกระทบทางจิตใจ

- ต่อองค์กร การปฏิบัติตามกฎหมาย PDPA ช่วยปกป้องข้อมูลของผู้รับบริการไม่ให้รั่วไหล ดัดแปลง หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งนอกจากจะช่วยให้งานขององค์กรราบรื่นและแม่นยำแล้ว ยังช่วยดูแลรักษาความปลอดภัยของอุปกรณ์ ผ่านการอัปเดตโปรแกรมอย่างสม่ำเสมอเพื่อปิดช่องโหว่ ป้องกันการโจมตีจากผู้ไม่หวังดี ตลอดจนลดความเสี่ยงจากการถูกเรียกค่าไถ่หรือการสูญเสียข้อมูลสำคัญของหน่วยงาน

- ต่อสาธารณะ การมีมารยาทในการสื่อสาร พูดคุยกันในเชิงบวก แสดงความเห็นอกเห็นใจ ไม่ใช่ถ้อยคำ
 หยาบคาย ไม่สร้างความเกลียดชัง และเคารพความคิดเห็นที่แตกต่าง ช่วยลดการละเมิดสิทธิและการระราน
 ทางไซเบอร์ลงได้ นอกจากนี้ ยังช่วยลดความขัดแย้งและความตึงเครียดในสังคมได้ด้วยการเช็คความถูกต้อง
 และแหล่งที่มาของข้อมูลก่อนแชร์ทุกครั้ง เพื่อป้องกันการส่งต่อข่าวเท็จและไม่สร้างความเสียหายในวงกว้าง

แหล่งที่มา

หลักสูตร : Digital Literacy

บรรยายโดย : นายสมนธ์ จิรพัฒน์พร

สถาบัน/หน่วยงาน/ระบบ : TDGA

รูปแบบหลักสูตร : การเรียนรู้ออนไลน์ TDGA e-Learning

ช่วงเวลาการฝึกอบรม : สิงหาคม ๒๕๖๙