

สรุปบทเรียนที่ได้รับจากการพัฒนาความรู้
ผ่านระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ TDGA e - Learning
หลักสูตร ความฉลาดทางดิจิทัล (Digital Intelligence)

สรุปบทเรียน

๑. บทนำ (Introduction)

ความฉลาดทางด้านดิจิทัล เป็นความสามารถในการใช้เทคโนโลยีทางด้านดิจิทัลและข้อมูลในการตัดสินใจ และการแก้ปัญหา โดยใช้ความรู้และทักษะทางด้านเทคโนโลยีในการวิเคราะห์ข้อมูลและการประมวลผลข้อมูลที่มาของความฉลาดทางด้านดิจิทัลเป็นผลการศึกษาและพัฒนาตัวเอง (DQ Institute) หน่วยงานที่เกิดจากความร่วมมือของภาครัฐและเอกชนทั่วโลก ร่วมกันประสานงานร่วมมือกับ (World Economic Forum) ที่มุ่งให้เด็ก ๆ ทุกคนในประเทศ ได้รับการศึกษาทางด้านทักษะพลเมืองดิจิทัลที่มีคุณภาพ และใช้ชีวิตบนโลกออนไลน์อย่างปลอดภัย

๒. อัตลักษณ์ดิจิทัล (Digital Identity)

๒.๑ โลกดิจิทัล

โลกดิจิทัลเสมือนที่ถูกสร้างขึ้นคู่ขนานกับโลกความจริง เป็นเครื่องมือทรัพยากรกิจกรรมคล้ายกับโลกความจริง พื้นที่ในโลกดิจิทัลถูกสร้างขึ้นจากอุปกรณ์อิเล็กทรอนิกส์ที่สามารถสร้างกำหนดพื้นที่ในกิจกรรมต่างๆ ได้เสมือนกับโลกความเป็นจริง สามารถใช้โซเชียลมีเดียได้ เป็นพื้นที่ในการพูดคุยแลกเปลี่ยนประสบการณ์ พื้นที่ในการซื้อ - ขายสินค้า ทำธุรกรรม ใช้เฉพาะสมาชิกที่เป็นผู้คน หรือพลเมืองดิจิทัลเท่านั้น

๓. การใช้เทคโนโลยีดิจิทัลอย่างเหมาะสม (Digital Use)

๓.๑ การใช้เทคโนโลยีอย่างสมดุล

การใช้เทคโนโลยีอย่างสมดุล การใช้หน้าจอจะมีผลต่อร่างกายและการใช้ชีวิต ได้แก่ ปวดหลัง หรือปวดคอ เสียสายตา นิ้วล็อกและเกิดความเครียด หลักเกณฑ์ในการจัดการสมดุลให้กับเวลาหน้าจอ ในโลกความเป็นจริงให้คนเป็นเบอร์หนึ่งเสมอ มีเป้าหมายทุกครั้งที่ใช้งานดิจิทัล ใช้ร่างกายให้เป็นมาตรฐาน เตรียมใจให้พร้อมเมื่อเวลาเจอหน้าจอ

การเอาใจเขามาใส่ใจเราทางดิจิทัล สิ่งที่เราควรทำ แสดงความคิดเห็นอย่างจริงจัง ตรงไปตรงมา เช่น เป็นกำลังใจให้นะ มีอะไรให้ช่วยบอกนะสู้ๆ นะ ส่งสติ๊กเกอร์ห่วงใย ตระหนักรู้อยู่เสมอว่าไม่เพียงแค่ว่าเราเป็นผู้สื่อสารกับคนนั้นเท่านั้นแต่ยังมีอีกหลายคนเป็นเพื่อนเรา ระมัดระวังก่อนที่จะแสดงความคิดเห็นอะไรลงไป เพราะอาจจะกลายเป็นดราม่าได้ และสิ่งที่ไม่ควรทำ แสดงความเห็นหยอกล้อกัน ให้ความรู้สึกสนุกสนานในโลกดิจิทัลแตกต่างกันออกไปการโพสต์แสดงความคิดเห็นอาจจะไปจี้ปมในใจเนื่องจากอาจจะตีความหมายในการสื่อสารผิดได้

๔. การจัดการความปลอดภัยในโลกดิจิทัล (Digital Security)

๔.๑ การล่วงละเมิดทางไซเบอร์ คือ การแสดงพฤติกรรมที่เป็นอันตราย สร้างความรำคาญหรือสร้างความเสียหายให้กับผู้อื่น ทางด้านความรู้สึกอาจจะลุกลามไปยังทรัพย์สินหรือการล่วงละเมิดในชีวิตจริงในการใช้โซเชียลมีเดีย เกมส์ เครือข่ายออนไลน์ต่างๆ ได้แก่

๑) การกระรานทางไซเบอร์ (Cyberbullying) การกลั่นแกล้ง การให้ร้าย การด่าว่า การข่มเหง หรือการรังแกผู้อื่นในโลกดิจิทัล เช่น โซเชียลมีเดียต่างๆ

๒) การรังควานทางไซเบอร์ (Online Harassment) การล่วงละเมิดทางไซเบอร์ที่ร้ายแรงกว่าพัฒนาจากการระรานทางไซเบอร์ โดยการส่งข้อความหรือคอมเมนต์ทำร้ายจิตใจ

๓) การสะกดรอยตามไซเบอร์ (Cyberstalking) การติดต่อหรือส่งข้อความมาซ้ำๆ อย่างต่อเนื่องจากบุคคลที่เราไม่ต้องการ เกิดจากแรงจูงใจต่างๆ มากมาย เช่น อารมณ์ ความรู้สึก

๔) การแกล้งหรือการก่อกวน (Trolling) คือการจงใจโพสต์ หรือคอมเมนต์ข้อความที่ยั่ว ทำให้เสียอารมณ์ ตกใจ ทะเลาะกับคนอื่น การแกล้งมีหลายรูปแบบแต่มักเป็นประเด็นขัดแย้ง

๔.๒ สาเหตุของการล่วงละเมิดทางไซเบอร์

๑) ต้องการก่อกวนโดยไม่มีสาเหตุ หรือเรียกว่านักเลงคีย์บอร์ด

๒) ต้องการแกล้งกันเล็กๆ น้อยๆ

๓) แกล้งกันจนขัดแย้งบานปลาย กลายเป็นเรื่องใหญ่ หรือจากความขัดแย้งรุนแรงแต่แรกแล้วใช้พื้นที่ในโลกออนไลน์โจมตีอีกฝ่าย

๔) ต้องการรังควานผู้ที่เป็นเป้าหมายหรือผู้ขัดแย้งอยู่

๕) ต้องการรังควานผู้ที่เป็นเป้าหมาย

๖) ต้องการข่มขู่หรือสร้างความหวาดกลัว ให้กับผู้ที่เป็นเป้าหมายหรือผู้ที่ขัดแย้งกันอย่างรุนแรง

๗) ติดตามไปประสังค์ร้ายในชีวิตจริง

๔.๓ สาเหตุของภัยคุกคามทางไซเบอร์

๑) การตั้งพาสเวิร์ดที่ง่ายเกินไป มีคนใช้รหัสผ่าน “๑๒๓๔๕๖” นับล้านบัญชีเนื่องจากจำง่าย และยังใช้รหัสผ่านเดียวกันในหลายเว็บไซต์ เปิดโอกาสให้ผู้ประสังค์ร้ายเข้าถึงข้อมูลได้

๒) โปรแกรมรักษาความปลอดภัยไม่ทำงาน อุปกรณ์มีโปรแกรมรักษาความปลอดภัยแต่ในบางครั้งอาจจะไม่ทำงาน หรือทำงานไม่เต็มที่เนื่องจากติดลิขสิทธิ์ หรือขาดการอัปเดต

๓) ความประมาท ผู้ประสังค์ร้ายในโลกดิจิทัลมักจะจ้องเล่นงาน โจมตีช่องโหว่ ผู้ที่ไม่ระมัดระวังหรือประมาท เกิดจากการกดรับไฟล์หรือลิงค์จากผู้อื่น

๔.๔ ผลกระทบของภัยคุกคามทางไซเบอร์

๑) ตัวบุคคล ผู้ประสังค์ร้ายสามารถคุกคามเพื่อนำข้อมูลส่วนบุคคลไปใช้แอบอ้าง เพื่อผลประโยชน์ทางทรัพย์สิน และสัมพันธ์ได้

๒) อุปกรณ์และระบบต่างๆ ผู้ประสังค์ร้ายสามารถโจมตีให้อุปกรณ์ และระบบไม่สามารถใช้งานได้เพื่อเรียกเก็บเงินค่าไถ่เพื่อให้ใช้อุปกรณ์ได้ดังเดิม

๔.๕ คำแนะนำในการท่องโลกดิจิทัล

๑) ตรวจสอบก่อนรับคำขอเป็นเพื่อน โดยเฉพาะคนที่รู้จักในชีวิตจริง

๒) บล็อกคนที่เคยติดต่อ ด้วยข้อความในแง่ลบหรือไม่ปลอดภัย

๓) คิดให้รอบคอบ เกี่ยวกับการแชร์ลิงก์ไปยังเว็บไซต์หรือโซเชียลมีเดียต่างๆ

๔) คิดก่อนอัปโหลดและแชร์รูปภาพ ควรคิดและระวังก่อนโพสต์รูป ทั้งรูปส่วนตัวและรูปครอบครัว

๕) คำนึงถึงสิ่งที่เขียนถึงผู้อื่น เราไม่มีทางรู้ว่าใครจะอ่านความคิดเห็นเหล่านี้และพวกเขาจะตีความอย่างไร

๖) ให้เพื่อนออนไลน์อยู่แค่บนโลกออนไลน์ อย่าตกลงที่จะพบคนที่รู้จักบนโลกออนไลน์เพียงลำพัง พาเพื่อนหรือครอบครัวไปด้วย

๗) ระวังเรื่องเพศสัมพันธ์ทางออนไลน์ ระวังการส่งหรือได้รับข้อความบรรยายในเรื่องเช็กส์

๘) ปกป้องตัวตนของเรา เลือกชื่อผู้ใช้ที่ไม่ใช่ของจริงและรูปโปรไฟล์ที่ไม่แสดงข้อมูลส่วนบุคคลใดๆ

๙) นึกถึงความเป็นส่วนตัว หลีกเลี่ยงการแบ่งปันข้อมูลส่วนบุคคลทางออนไลน์ที่อาจนำไปใช้ในทางที่ผิดโดยบุคคลอื่นในชีวิตจริง

๔.๖ รูปแบบภัยคุกคามทางไซเบอร์

๑) อีเมลอันตราย อีเมลที่เหมือนมาจากเกม หรืออื่นๆ หากกดรับบัญชีจะถูกบุกรุก เพื่อให้ได้ข้อมูลส่วนบุคคลหรือเสียทรัพย์

๒) สแปม (Spam) อีเมลที่มีข้อความที่ส่งให้ผู้รับโดยไม่ได้รับอนุญาตและไม่เปิดโอกาสให้ปฏิเสธข้อความ ซึ่งก่อให้เกิดความรำคาญ

๓) ฟิชซิง (Phishing) การหลอกลวงให้เหยื่อคลิกลิงก์ หรือให้เหยื่อกรอกข้อมูลส่วนตัว คำว่า ฟิชซิงคล้ายการ ตกปลาเพื่อล่อเหยื่อ

๔) มัลแวร์ (Malware) โปรแกรมที่สร้างความเสียหายต่ออุปกรณ์ไอที ตั้งแต่การเข้าควบคุมระบบคอมพิวเตอร์ เปลี่ยนรหัสผ่าน

๕) ภัยจากการชอปปิงออนไลน์ รูปแบบนี้ทำให้นักต้มตุ๋นมีช่องทางมากขึ้นในการหลอกให้เราจ่ายเงิน

๖) ภัยจากการไม่สำรองข้อมูล การจัดเก็บข้อมูลทั้งหมดไว้บนคอมพิวเตอร์มีความเสี่ยงที่จะสูญหายได้

๕. การรู้เท่าทันดิจิทัล (Digital Literacy)

๕.๑ การใช้งานสื่อสารสนเทศ

๑) แหล่งที่เผยแพร่ข้อมูล การสร้างหรือผลิตข้อมูลโดยเจ้าของแหล่งข้อมูล และการสร้างหรือผลิตข้อมูลโดยชุมชนผู้ใช้งาน

๒) แบ่งตามสิทธิการเข้าถึงข้อมูล ได้แก่ แหล่งข้อมูลที่เข้าถึงโดยเสรี และแหล่งข้อมูลที่จำกัดการเข้าถึง

๓) แบ่งตามประเภทของข้อมูล ได้แก่ แหล่งข้อมูลเพื่อการศึกษาเรียนรู้ แหล่งข้อมูลด้านสุขภาพ แหล่งข้อมูลด้านธุรกรรมและการเงิน

๔) แหล่งข้อมูลด้านเศรษฐศาสตร์และธุรกิจ

๖. การสื่อสารดิจิทัล (Digital Communication)

๖.๑ ร่องรอยดิจิทัล หากเปรียบเทียบกับความเป็นจริงแล้ว เมื่อเราเดินผ่านจะเกิดรอยเท้า หรือการขีดเขียนผนังจะเกิดร่องรอยขีดเขียนทิ้งไว้ หรือเดินผ่านใครสักคนก็อาจจดจำเราได้ เมื่อต้องการให้ติดตามตัวเราก็ต้องอาศัยร่องรอยเหล่านั้นติดตามตัวเราไปในโลกของดิจิทัล ร่องรอยดิจิทัล คือข้อมูลพฤติกรรมการใช้งานในโลกดิจิทัลของเรา ซึ่งระบบจะบันทึกไว้ทั้งหมด ร่องรอยดิจิทัลเกิดขึ้นจากการใช้งานโลก

๖.๒ การมีปฏิสัมพันธ์และการสร้างความร่วมมือ การสื่อสารและการมีปฏิสัมพันธ์ทางดิจิทัล เราสามารถทำได้ดังนี้ โทรไปหา โทรผ่านไลน์ โทรวีดีโอคอล แชทหรือโพสต์ และคอมเมนต์ต่างๆ การใช้งานทางด้านดิจิทัลเพื่อการสื่อสารและการสร้างความร่วมมือ

ประกาศนียบัตร

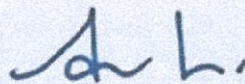
ให้ไว้เพื่อแสดงว่า

คุณ นาทอนงค์ ไสกาพิมพ์

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
Digital Literacy: ความฉลาดทางดิจิทัล (Digital Intelligence)

รวมระยะเวลาทั้งสิ้น 1:32 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 6 มิถุนายน 2568



(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

