

สรุปบทเรียน

การอบรมผ่านหลักสูตรออนไลน์ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA)

หลักสูตร Digital Literacy : ความฉลาดทางดิจิทัล (Digital Intelligence)

นายอภิชัย กะตะศิลา

นักวิชาการเกษตรปฏิบัติการ

สถานีพัฒนาที่ดินนครราชสีมา สำนักงานพัฒนาที่ดินเขต 3

1. Digital Identity อัตลักษณ์ดิจิทัล

1.1. โลกดิจิทัล (Digital World)

โลกดิจิทัล คือ โลกเสมือนที่ถูกสร้างขึ้นคู่ขนานกับโลกความจริง เป็นเครื่องมือทรัพยากรกิจกรรมที่มีกิจกรรมคล้ายกับโลกความจริง พื้นที่ในโลกดิจิทัลถูกสร้างขึ้นจากอุปกรณ์อิเล็กทรอนิกส์ที่สามารถกำหนดพื้นที่กิจกรรมต่างๆได้เหมือนกับโลกความเป็นจริง ใช้เป็นพื้นที่พูดคุยแลกเปลี่ยนประสบการณ์ สามารถใช้ Social Media ได้ สร้างพื้นที่ในการซื้อขายสินค้าและธุรกรรมทางการเงิน ร้านค้าออนไลน์ หรือธนาคารออนไลน์ กิจกรรมในพื้นที่โลกดิจิทัลนั้นจะมีเฉพาะสมาชิกหรือผู้คนพลเมืองดิจิทัลเท่านั้น

โลกดิจิทัล สามารถค้นหาและเข้าถึงสื่อที่ต้องการได้ง่าย เช่น เข้าถึงได้ด้วยอุปกรณ์พกพาได้ทุกที่ทุกเวลา สามารถพูดคุย ติดต่อกับผู้คนที่ไม่ค่อยได้พบกันได้ง่าย สามารถเผยแพร่สื่อ เนื้อหา และบอกประสบการณ์ผ่านช่องทางออนไลน์ได้อย่างสะดวก แต่มีข้อจำกัดคือไม่สามารถให้คำปรึกษา สร้างแรงบันดาลใจได้อย่างลึกซึ้งได้เท่าโลกของความเป็นจริง ไม่สามารถเข้าร่วมกิจกรรมที่ต้องมีการปฏิบัติจริงร่วมกันได้ในบางกิจกรรม ไม่สามารถทำธุรกรรมบางประเภทได้

มารยาทในโลกของดิจิทัล ใส่ใจและให้เกียรติไม่ต่างจากโลกความจริง แบ่งปันสิ่งดีๆและสร้างสรรค์ ตรวจสอบการส่งข้อมูลให้ตรงกับกลุ่ม ปฏิบัติตามกฎหมายออนไลน์ ไม่แสดงความเห็นด้วยถ้อยคำที่รุนแรง ไม่แสดงอารมณ์ขันที่หมิ่นเหม่เสียดสี ไม่ส่งต่อข้อมูลที่ไม่แน่ใจว่าเป็นความจริง ไม่ใช่ไซเบอร์ลอร์ดในการให้ร้ายผู้อื่น

จริยธรรมของพลเมืองในโลกดิจิทัล ให้เกียรติและเคารพความคิดเห็นและสิทธิของผู้อื่น หลีกเลี่ยงการระราน ช่มชู้ หรือหยอกล้อให้เกิดพ้อตี ขออนุญาตเมื่อนำข้อมูลผู้อื่นไปใช้ ไตร่ตรองก่อนแชร์หรือโพสต์ข้อมูล ไม่ควรแชร์หรือโพสต์ข้อมูลส่วนบุคคลมากเกินไป ระวังตระวังในการแชร์หรือโพสต์ข้อมูล และระวังการใช้ความเป็นผู้อาวุโสในการสนทนา

1.2. อัตลักษณ์ดิจิทัล (Digital Identity)

อัตลักษณ์ดิจิทัล (Digital Identity) คือชุดข้อมูลรูปแบบอิเล็กทรอนิกส์ที่ใช้ระบุตัวตนบุคคล องค์กร หรืออุปกรณ์บนโลกออนไลน์ ประกอบด้วยชื่อ ข้อมูลส่วนบุคคล พฤติกรรม และข้อมูลชีวมาตร เช่น ลายนิ้วมือ การสแกนใบหน้า เพื่อใช้ยืนยันตัวตนในการทำธุรกรรม เข้าสู่ระบบ หรือเข้าถึงบริการดิจิทัลต่างๆ อย่างปลอดภัย

อัตลักษณ์ดิจิทัลที่เป็นข้อมูลเดียวกับโลกความจริง ประกอบด้วย ชื่อ-นามสกุล รูปภาพประจำตัว วันเดือนปีเกิด เลขประจำตัวประชาชน หมายเลขบัตรเครดิต

อัตลักษณ์ดิจิทัลที่เกิดจากกิจกรรมบนโลกดิจิทัล ได้แก่ บัญชีและรหัสผ่าน สถานที่ที่เช็คอิน พฤติกรรม และประวัติการใช้งาน การค้นหาข้อมูล การกดถูกใจ เนื้อหา ข้อความ กลุ่มหรือสังคม เพื่อหรือบุคคลหรือองค์กร บนโลกดิจิทัล

ผลที่เกิดจากการสร้างอัตลักษณ์ดิจิทัล สามารถแสดงได้ทั้งทางบวกและทางลบ ผลทางบวก ได้แก่

ผู้คนที่จดจำเราในทางที่ดี สร้างความสัมพันธ์ที่ดีกับคนรอบตัว เปิดโอกาสมากมาย อยู่ในสังคมดิจิทัลที่น่าอยู่ และผลทางลบ ได้แก่ ผู้คนที่จดจำในทางไม่ดี ความสัมพันธ์ไม่ดี ถูกระรานในโลกดิจิทัล(ผู้คนมุ่งร้าย) ถูกโจรกรรมทางดิจิทัล เสียโอกาสในหน้าที่การงาน และส่งผลต่อสภาพจิตใจ



การสร้างอัตลักษณ์ดิจิทัลที่ดี ประกอบด้วย

- ตระหนักอยู่เสมอว่าทุกอย่างที่เราแชร์หรือเผยแพร่ในโลกดิจิทัลจะอยู่ในนั้นตลอดไป
- คิดก่อนโพสต์และแชร์
- ใจเย็นให้มากที่สุดในโลกดิจิทัล
- เลิกคิดว่านี่คือโลกจำลอง
- ทุกอย่างในโลกออนไลน์มีเจ้าของ
- อย่งให้ผู้อื่นรู้ข้อมูลของเรามากเกินไป
- ปกป้องรหัสผ่านและเปลี่ยนบ่อยๆ
- ตรวจสอบตัวตนของเราบนโลกดิจิทัลอยู่เสมอ

แนวทางปฏิบัติที่ดีในการสร้างอัตลักษณ์ดิจิทัลกับตัวตนที่แท้จริง

- ควรใช้ ชื่อ-นามสกุล ที่ไม่ทำให้ผู้อื่นเสียหาย และไม่ควรรู้ชื่อผู้อื่น
- ไม่ใช่ภาพของผู้อื่นมาเป็นรูปภาพประจำตัวหรือละเมิดทำให้ผู้อื่นเสียหาย
- ตั้งค่าความเป็นส่วนตัวและไม่เปิดเผยข้อมูลที่ไม่ควรเผยแพร่
- ตรวจสอบประวัติการใช้งานบนอินเทอร์เน็ต หากประวัติเสียหายให้ทำการลบ
- ตรวจสอบเนื้อหา ข้อความ รูปภาพที่เราได้เผยแพร่ในโลกดิจิทัล
- ตรวจสอบการใช้เครื่องมือเช็คอินบนเฟซบุ๊ก หากพบว่าไม่เหมาะสมให้ลบ
- ตรวจสอบกลุ่มที่เข้าร่วม หากมีเนื้อหาไม่เหมาะสมให้กดออกจากกลุ่ม
- ตรวจสอบบุคคลที่รับเป็นเพื่อน หากพบว่าไม่เหมาะสมให้ลบ
- ตรวจสอบการแสดงความคิดเห็น หากไม่เหมาะสมให้ลบ

1.3. ความเป็นส่วนตัวในโลกดิจิทัล (Digital Privacy)

ความเป็นส่วนตัวในโลกดิจิทัล (Digital Privacy) คือ สิทธิ์ในการควบคุมการจัดเก็บ การใช้ และการแบ่งปันข้อมูลส่วนบุคคลบนโลกออนไลน์ เช่น ข้อมูลประจำตัว ประวัติการใช้งาน หรือตำแหน่งที่ตั้ง เป็นการป้องกันข้อมูลสำคัญไม่ให้ตกไปอยู่ในมือผู้ไม่หวังดีหรือถูกนำไปหาผลประโยชน์โดยไม่ได้รับอนุญาต โดยมี

ความสำคัญอย่างยิ่งต่อความปลอดภัยส่วนบุคคลและการลดความเสี่ยงจากการถูกโจรกรรมข้อมูล

ข้อมูลส่วนตัวในโลกดิจิทัลแบ่งความสำคัญของความเป็นส่วนตัว ดังนี้ 1. ข้อมูลส่วนบุคคลที่สามารถเผยแพร่ได้ไม่เป็นอันตราย ได้แก่ ชื่อจริง ชื่อเล่น อายุ เพศ พี่น้อง อาหารที่ชอบ หนังสือเรื่องโปรด สัตว์เลี้ยง และ 2. ข้อมูลส่วนบุคคลที่ไม่ควรเปิดเผยเป็นสาธารณะเนื่องจากความปลอดภัยทั้งตัวตนบนโลกดิจิทัลและชีวิตจริง เช่น เลขบัตรประชาชน เลขบัญชีธนาคาร ที่อยู่บ้าน วันเกิด หมายเลขโทรศัพท์

การจัดการข้อมูลส่วนตัว 1. ไม่เปิดเผยหรือเผยแพร่ข้อมูลที่ไม่ควรเปิดเผย 2. หลีกเลี่ยงการตั้งโปรไฟล์ในโซเชียลมีเดียให้เป็นสาธารณะ 3. จัดการอุปกรณ์ให้ปลอดภัยและรัดเข็มขัด 4. ให้ความสนใจกับเงื่อนไขและข้อตกลงในการใช้โปรแกรม 5. ตั้งรหัสผ่านให้มีความปลอดภัย

กฎหมายที่เกี่ยวข้อง

- PDPA คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยระบุให้องค์กรหรือหน่วยงานเก็บข้อมูลส่วนบุคคลของประชาชน ไม่ว่าจะ เป็นบริษัทเอกชนหรือหน่วยงานภาครัฐ ต้องไม่นำข้อมูลส่วนตัวของเราไปใช้ โดยที่เราไม่ยินยอม กฎหมายยังคุ้มครองไปถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) เช่น เชื้อชาติ เผ่าพันธุ์ ความเชื่อ ศาสนา ความเห็นทางการเมือง พฤติกรรมทางเพศ และอื่นๆทั้งหมด บทลงโทษสำหรับผู้ละเมิดสิทธิและความเป็นส่วนตัวตามกฎหมาย PDPA ประกอบด้วย โทษทางอาญา จำคุกไม่เกิน 1 ปี และ/หรือปรับสูงสุด 1 ล้านบาท โทษทางแพ่ง จ่ายสินไหมไม่เกิน 2 เท่าของสินไหมที่แท้จริง โทษทางปกครอง ปรับไม่เกิน 5 ล้านบาท

- พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี 2550 และ 2560 ประกอบด้วย 1. ผู้ใดแก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหาย (มาตรา 9-10) จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ 2. ส่งข้อมูลหรืออีเมลก่อความรำคาญผู้อื่นหรือส่งอีเมลสแปม (มาตรา 11) โทษจำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ 3. นำข้อมูลที่ผิด พ.ร.บ. เข้าสู่ระบบคอมพิวเตอร์ (มาตรา 14) จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 6 แสนบาท หรือทั้งจำทั้งปรับ

การป้องกันการถูกคุกคามความเป็นส่วนตัวในโลกดิจิทัล

- สร้างรหัสผ่านที่รัดกุม
- อัปเดตระบบของคุณอยู่ตลอด
- ตั้งค่าความปลอดภัยบนอุปกรณ์
- ป้องกันอุปกรณ์ด้วยซอฟต์แวร์ป้องกันไวรัส
- สำรองไฟล์และข้อมูลของคุณไปยังคลาวด์หรือบนฮาร์ดไดรฟ์ภายนอก



2. Digital Use การใช้เทคโนโลยีอย่างเหมาะสม

2.1. การใช้เทคโนโลยีอย่างสมดุล

หลักเกณฑ์ในการจัดการสมดุลให้กับเวลาหน้าจอ 1.ในโลกความเป็นจริงให้คนเป็นเบอร์หนึ่งเสมอ 2.มีเป้าหมายทุกครั้งที่ใช้งานดิจิทัล 3.ใช้ร่างกายให้เป็นมาตรฐานวัด 4.เตรียมใจให้พร้อมเมื่อเวลาเจอหน้าจอ

แนะนำเครื่องมือสำหรับใช้ในการบริหารการใช้งานหน้าจอ ระบบ Android แนะนำให้ติดตั้งแอปพลิเคชัน Digital Wellbeing เพื่อใช้งานตรวจสอบเวลาการใช้งานหน้าจอ และระบบ IOS สามารถเข้าไปดูได้ที่ การตั้งค่า > เวลาหน้าจอ จะสามารถตรวจสอบการใช้งานหน้าจอได้เลย



สัญญาณบอกเขตการเสพติดเนื้อหา 1.เข้าไปอ่าน ดู กดไลค์ กดหัวใจหลายๆ ครั้ง ในหนึ่งวันหรือเกือบทุกชั่วโมง 2.หากวันไหนไม่ได้เข้าไปอ่าน กดไลค์ กดหัวใจ หัวใจจะรู้สึกว่ายังขาดอะไรไปสักอย่าง 3.ทุกครั้งที่ว่างหรือมีเรื่องราวในวันนั้นแวบขึ้นมาในความคิดแบบไม่ตั้งใจ การเสพติดเนื้อหาหรือเสพติดอินเทอร์เน็ตจะมีผลต่อสุขภาพจิต คือ เกิดภาวะซึมเศร้า เสี่ยงต่ออาการวิตกกังวล ขาดความยับยั้งชั่งใจ รู้สึกต่อต้านสังคม

2.2. การเอาใจเขามาใส่ใจเราทางดิจิทัล (Digital Empathy)

กรณีที่ 1 คนใกล้ชิดสนิทสนม โพสต์ข้อความ สิ้นหวังหมดกำลังใจ ในการทำงาน ควรแสดงความเห็นอย่างจริงใจ ตรงไปตรงมา เช่น เป็นกำลังใจให้นะ มีอะไรให้ช่วยบอกนะ สู้ๆ ส่งสติ๊กเกอร์ห่วงใย และตระหนักอยู่เสมอว่าไม่เพียงแค่ว่าเราเป็นผู้สื่อสารกับคนนั้นเท่านั้น แต่ยังมีอีกหลายคนเป็นเพื่อนเขา ระวังระวังก่อนที่จะแสดงความคิดเห็นอะไรลงไปเพราะอาจจะกลายเป็นดราม่าได้ ไม่ควรแสดงความเห็นหยอกล้อให้ความรู้สึกสับสน ในโลกดิจิทัลแตกต่างกันออกไป การโพสต์แสดงความคิดเห็นอาจจะไปจี้ปมในใจเนื่องจากอาจจะตีความหมายในการสื่อสารผิดได้

กรณีที่ 2 เราเห็นเพื่อนของเพื่อนกดโกรธได้ภาพงานแต่งงานของเรา ควรนิ่งเฉย เข้าใจว่าเป็นการกดผิด หากคิดถึงตัวเราเอง เราอาจจะกดภาพแสดงความรู้สึกในโพสต์ ดังนั้นควรมีวิจารณญาณในการตีความ และไม่ควรวัยวายต่อว่าตำหนิต่างต่อหน้าและในโพสต์หรือคอมเมนต์หรือไปนินทาลับหลัง

กรณีที่ 3 เมื่อเราเห็นเพื่อนสนิทของเราโพสต์ข้อความว่า ตกงาน ไม่มีงานทำ อยู่ในภาวะเศรษฐกิจตกต่ำ ควรโพสต์หรือคอมเมนต์ให้กำลังใจ พร้อมสนับสนุนให้คำแนะนำในช่องทางส่วนตัว ยิ่งในโลกดิจิทัลเป็นพื้นที่สาธารณะเราควรระวังการตอบโต้หรือแสดงความคิดเห็น ไม่ควร comment สั่งสอนในเชิงลดทอนกำลังใจหรือซ้ำเติม

ข้อระวังเนื้อหาในการโพสต์ 1.เนื้อหาหรือรูปภาพที่เป็นลิขสิทธิ์ของผู้อื่น 2.เนื้อหาหรือรูปภาพที่อาจ

ทำให้เกิดความขัดแย้งด้านความเชื่อและศาสนา 3.เนื้อหาหรือรูปภาพที่แสดงความรุนแรงและการทารุณ 4. เนื้อหาหรือรูปภาพแอบถ่ายหรือภาพบุคคลอื่นที่ไม่ได้รับอนุญาต

การใช้เทคโนโลยีในการตอบโต้ แสดงความเห็น หรือมีปฏิสัมพันธ์ในการติดตามเนื้อหาทางด้านดิจิทัล มีผลกระทบต่อสุขภาพจิตของตัวเราเองและผู้อื่น ดังนั้น เราควรใช้ข้อความสื่อสารในเชิงบวก ไม่ทำให้ผู้อื่นเกิดความเสียหายหรือกระทบจิตใจ เมื่อโพสต์ comment เผยแพร่สื่อเนื้อหาใดๆ ต้องไตร่ตรองอย่างน้อย 3 ครั้ง ให้ตั้งคำถามเสมอกับการสื่อสารเนื้อหาในการเผยแพร่ว่าเมื่อผู้อื่นเห็นหรือได้อ่านจะรู้สึกอย่างไร

3. Digital Security การจัดการความปลอดภัยในโลกดิจิทัล

การล่วงละเมิดทางไซเบอร์ คือ การแสดงพฤติกรรมที่เป็นอันตราย สร้างความรำคาญ หรือสร้างความเสียหายให้กับผู้อื่นบนเครือข่ายออนไลน์ต่างๆ ประกอบด้วย การระรานทางไซเบอร์ การรังควานทางไซเบอร์ การสะกดรอยตามทางไซเบอร์ และการก่อกวน

สาเหตุการล่วงละเมิดทางไซเบอร์ คือ ต้องการก่อกวนโดยไม่มีสาเหตุหรือเรียกว่านักเลงคีย์บอร์ด ต้องการแกล้งกันเล็กน้อยๆ หรือแกล้งกันจนขัดแย้งบานปลายกลายเป็นเรื่องใหญ่ หรือจากความขัดแย้งรุนแรงแต่แรกแล้วใช้พื้นที่ในโลกออนไลน์โจมตีอีกฝ่าย ต้องการรังควานผู้ที่เป่าหมายหรือผู้ขัดแย้งกันอยู่ ต้องการข่มขู่หรือสร้างความหวาดกลัวให้กับผู้ที่เป่าหมายหรือผู้ที่ขัดแย้งกันอย่างรุนแรง หรือกระทั่งติดตามไปประสังคร้ายในชีวิต

ภัยคุกคามทางไซเบอร์ (Cyber Threat) สาเหตุของภัยคุกคามทางไซเบอร์ ประกอบด้วย การตั้งพาสเวิร์ดที่ง่ายเกินไป โปรแกรมรักษาความปลอดภัยไม่ทำงาน และความประมาท

ผลกระทบของภัยคุกคามทางไซเบอร์ มี 2 ส่วนประกอบด้วย ผลกระทบต่อตัวบุคคล ผู้ประสังคร้ายสามารถคุกคามเพื่อนำข้อมูลส่วนบุคคลไปใช้แอบอ้างเพื่อผลประโยชน์ทางทรัพย์สินและความสัมพันธ์ได้ และผลกระทบต่ออุปกรณ์และระบบต่างๆ ผู้ประสังคร้ายสามารถโจมตีให้อุปกรณ์และระบบไม่สามารถใช้งานได้เพื่อเรียกเก็บเงินค่าไถ่เพื่อให้ใช้อุปกรณ์ได้ดังเดิม

รูปแบบภัยคุกคามทางไซเบอร์

- อีเมลอันตราย คือ อีเมลที่เหมือนมาจากเกมหรืออื่นๆ หากกดรับบัญชีจะถูกบุกรุกเพื่อให้ได้ข้อมูลส่วนบุคคลหรือเสียหาย
- สปแอม (Spam) คือ อีเมลที่มีข้อความที่ส่งให้ผู้รับโดยไม่ได้รับอนุญาตและไม่เปิดโอกาสให้ปฏิเสธข้อความซึ่งก่อให้เกิดความรำคาญ
- ฟิชชิ่ง (Phishing) คือ การหลอกลวงให้เหยื่อคลิก หรือให้เหยื่อกรอกข้อมูลส่วนตัว คำว่า ฟิชชิ่ง คล้ายการตกปลาเพื่อล่อเหยื่อ
- มัลแวร์ (Malware) คือ โปรแกรมที่สร้างความเสียหายต่ออุปกรณ์ไอที ตั้งแต่การเข้าควบคุมระบบคอมพิวเตอร์ ตลอดจนการเปลี่ยนรหัสผ่าน
- ภัยจากการช้อปปิ้งออนไลน์ รูปแบบนี้ทำให้นักต้มตุ๋นมีช่องทางมากขึ้นในการหลอกให้เราจ่ายเงิน
- ภัยจากการไม่สำรองข้อมูล การจัดเก็บข้อมูลทั้งหมดไว้บนคอมพิวเตอร์ มีความเสี่ยงที่จะสูญหายได้

4. Media and Information Use การใช้งานสื่อสารสนเทศ

4.1. การใช้งานสื่อสารสนเทศ

รูปแบบของแหล่งข้อมูลดิจิทัล แบ่งได้ดังนี้ 1.แหล่งที่เผยแพร่ข้อมูล ได้แก่ การสร้างหรือผลิตข้อมูล

โดยเจ้าของแหล่งข้อมูล และการสร้างหรือผลิตข้อมูลโดยชุมชนผู้ใช้งาน 2.แบ่งตามสิทธิการเข้าถึงข้อมูล ได้แก่ แหล่งข้อมูลที่เข้าถึงได้โดยเสรี และแหล่งข้อมูลที่จำกัดการเข้าถึง และ 3.แบ่งตามประเภทของข้อมูล ได้แก่ แหล่งข้อมูลเพื่อการศึกษาเรียนรู้ แหล่งข้อมูลเพื่อความบันเทิง แหล่งข้อมูลด้านสุขภาพ แหล่งข้อมูลด้าน ธุรกิจและการเงิน และแหล่งข้อมูลด้านเศรษฐศาสตร์และธุรกิจ

ลักษณะของข้อมูลที่มีคุณภาพ ประกอบด้วย 1.เป็นข้อมูลที่ทันสมัย คือ ข้อมูลต้องเป็นปัจจุบันหรือ อัปเดต วันที่เผยแพร่หากนานแล้วต้องพิจารณา ลิงก์เว็บยังสามารถเปิดได้ แผนภูมิและกราฟมีวันที่รวบรวม 2. เป็นข้อมูลที่ตอบโจทย์ คือ มีเนื้อหาเกี่ยวข้องกับเรื่องที่เราต้องการ มีวัตถุประสงค์ของเนื้อหาตรงตามความ ต้องการ นำเสนอเนื้อหาสำหรับกลุ่มเป้าหมายที่ตรงกับตัวเรา 3.ข้อมูลเที่ยงตรงแม่นยำ คือ เนื้อหาใช้ภาษา ถูกต้องตามหลักไวยากรณ์ ข้อมูลถูกต้องและสามารถตรวจสอบได้ มีอ้างอิงแหล่งที่มาของข้อมูล การนำเสนอ ข้อมูลดูมีความเป็นมืออาชีพ 4.ผู้เขียนเชื่อถือได้ คือ มีการระบุผู้เขียนชัดเจน มีรายละเอียดเกี่ยวกับผู้เขียน ผู้เขียนมีความเชี่ยวชาญ ประสบการณ์ คุณวุฒิเหมาะสมกับเนื้อหา

การสืบค้นข้อมูลจากสื่อดิจิทัล ประกอบด้วย การใช้คำค้นหาหรือคีย์เวิร์ด กำหนดคำหรือประโยค คำค้น การเลือกใช้เครื่องมือค้นหาให้เหมาะสม และการใช้ Advanced Search ในการช่วยค้นหาบน Google แนะนำเครื่องมือในการสืบค้นข้อมูล



แนะนำเครื่องมือในการเก็บรวบรวมข้อมูล



4.2. ผู้จัดทำสื่อและสารสนเทศ

ประเภทของเนื้อหาสื่อดิจิทัล ประกอบด้วย 1.เนื้อหาดิจิทัลเกี่ยวกับสุขภาพอนามัย เป็นเนื้อหาเกี่ยวกับการดูแลสุขภาพ สาเหตุการเกิดโรคต่างๆ วิธีการป้องกันการเกิดโรคร้าย จัดทำขึ้นโดยหน่วยงานทางสุขภาพ 2.เนื้อหาดิจิทัลเกี่ยวกับข้อมูลภาครัฐ เป็นการให้บริการข้อมูลต่างๆ ของภาครัฐ สิทธิและหน้าที่ของประชาชนในเรื่องต่างๆ กฎหมาย ระเบียบ เป็นต้น 3.เนื้อหาดิจิทัลเพื่อความบันเทิง ตอบสนองความต้องการความบันเทิง เช่น ภาพยนตร์ นิยาย จัดทำขึ้นโดยบริษัทหรือผู้ประกอบการด้านบันเทิง 4.เนื้อหาดิจิทัลด้านการตลาด เพื่อซื้อขายหรือสร้างแรงจูงใจ ให้เกิดการซื้อสินค้าหรือบริการ ผลิตโดยบริษัทหรือห้างร้านที่ทำธุรกิจ 5.เนื้อหาที่ใช้สำหรับการศึกษาและเรียนรู้ ทั้งการศึกษาที่อยู่ในระบบและการศึกษาเรียนรู้ตามอัธยาศัย จัดทำขึ้นโดยสถาบันการศึกษาหรือผู้เชี่ยวชาญ 6.เนื้อหาดิจิทัลด้านข่าวสาร รายงานความเคลื่อนไหวที่เกิดขึ้นในสังคม อาจจะเป็นด้านธุรกิจ ด้านการศึกษา หรือเหตุการณ์ทั่วไป

ประเภทของสื่อดิจิทัล ประกอบด้วย 1.รูปภาพดิจิทัล สร้างขึ้นเพื่อบันทึกเรื่องราว อาจเป็นภาพถ่ายหรือภาพสแกน 2.ข้อความดิจิทัล สร้างขึ้นเพื่อบอกเล่าเหตุการณ์ ผลิตโดยโปรแกรมคอมพิวเตอร์ 3.เสียง สร้างขึ้นสำหรับการบรรยาย โดยใช้อุปกรณ์บันทึกเสียงหรือโปรแกรมคอมพิวเตอร์ 4.วิดีโอ เป็นการผสมของเสียงและภาพ สร้างด้วยโทรศัพท์หรือกล้องวิดีโอ 5.กราฟิก Digital สร้างขึ้นแทนการสื่อความหมาย สร้างด้วยโปรแกรมคอมพิวเตอร์

หลักการสร้างเนื้อหาให้ถูกกฎหมายและมีจริยธรรม เป็นเรื่องของลิขสิทธิ์ กับ Creative Commons โดยลิขสิทธิ์ ห้ามทุกคน ห้ามทุกอย่าง เป็นกรอบแนวคิดของสมัยเดิมก่อนเกิดเทคโนโลยีสารสนเทศ และแลกเปลี่ยนข้อมูลผ่านอินเทอร์เน็ต ส่วน Creative Commons เสนอทางเลือกให้เจ้าของลิขสิทธิ์สามารถแบ่งปันข้อมูลได้ เลือกสงวนสิทธิ์ตามที่ต้องการได้ ตรงใจ ตรงไลฟ์สไตล์

5. Digital Communication ด้านการสื่อสารดิจิทัล

5.1. ร่องรอยดิจิทัล (Digital Footprint)

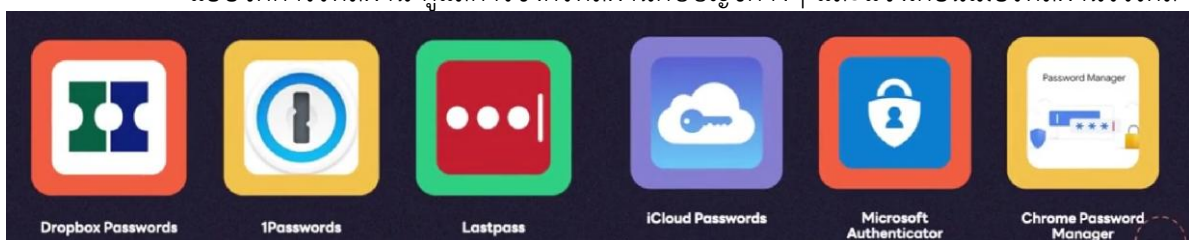
ร่องรอยทางดิจิทัล (Digital Footprint) คือ ข้อมูลกิจกรรมที่ทิ้งไว้จากการใช้งานอินเทอร์เน็ต ทั้งที่ตั้งใจโพสต์/แชร์ (Active) เช่น โซเชียลมีเดีย คอมเมนต์ และที่ไม่ตั้งใจ (Passive) เช่น คุกกี้ ประวัติค้นหา ETDA ซึ่งเปรียบเสมือนรอยเท้าที่คงอยู่ถาวรยากจะลบเลือน บ่งบอกตัวตน ความสนใจ และอาจถูกมิฉาชีพหรือนายจ้างนำไปใช้ตรวจสอบได้

ร่องรอยดิจิทัลเชิงบวก ได้แก่ โพสต์อย่างสร้างสรรค์ เป็นกลาง และชื่นชมด้วยความจริงใจ แสดงความคิดเห็นในโพสต์ หรือแชตด้วยข้อความที่สุภาพ ค้นหาข้อมูลที่เป็นประโยชน์และสร้างสรรค์

ร่องรอยดิจิทัลเชิงลบ ได้แก่ โพสต์พาดพิงถึงผู้อื่นในทางที่ไม่ดี เสียดสี หรือไม่ระวัง แสดงความคิดเห็นในโพสต์ของผู้อื่นด้วยข้อความไม่สุภาพ ค้นหาข้อมูลที่ไม่เป็นประโยชน์หรือไม่สร้างสรรค์

แนะนำเครื่องมือช่วยจัดการร่องรอยดิจิทัล

- แอปจัดการรหัสผ่าน ดูแลการซิงค์รหัสผ่านกับบัญชีต่างๆ และแจ้งเตือนเมื่อรหัสผ่านรั่วไหล



- แอปหรือเว็บไซต์ช่วยป้องกันการติดตาม จะช่วยป้องกันการติดตามและบันทึกการใช้งานต่างๆ ป้องกันไม่ให้ข้อมูลรั่วไหล



- เครื่องมือค้นหาแบบส่วนตัว จะช่วยให้เราค้นหาสิ่งที่ต้องการแบบไม่เปิดเผยตัวตนได้



วิธีการรับมือกับความเสียหายจากรอยเท้าดิจิทัล แบ่งเป็น 4 กรณี ดังนี้

- กรณี ถูกทำให้เสียชื่อเสียงจากโพสต์หรือคอมเมนต์ ให้ลบหรือแก้ไข โพสต์หรือคอมเมนต์ที่เป็นปัญหา ขอโทษผู้อื่นที่ได้รับผลกระทบอย่างจริงจัง สร้างร่องรอยใหม่ที่เหมาะสม
- กรณี ถูกละเมิดข้อมูลส่วนตัว ให้กด Report และเปลี่ยน password แจ้งเจ้าหน้าที่ให้ทราบและช่วยกด Report
- กรณี สูญเสียทรัพย์สินจากการถูกขโมยข้อมูล รวบรวมหลักฐานต่างๆ แจ้งความและลงบันทึกประจำวันกับตำรวจ โทรสายด่วน occ 1212
- กรณี ถูกตามจากโฆษณาที่แชร์หรือรูปที่ถูกแท็ก ให้เช็คอินได้ถ้าไม่ใช่สถานที่ส่วนตัว ปิดการแสดงโฆษณา ตั้งค่าการมองเห็นแค่เฉพาะเพื่อน

5.2. การมีปฏิสัมพันธ์และการสร้างความร่วมมือ (Interaction and Collaboration)

การใช้งานเทคโนโลยีดิจิทัลเพื่อสื่อสารและสร้างความร่วมมือ ทำได้ด้วยวิธีการดังนี้

- การสื่อสารระหว่างบุคคล เป็นการใช้อุปกรณ์ดิจิทัลสื่อสาร เช่น โทรศัพท์ พิมพ์ข้อความคอล หรือ video call ในห้องสนทนาการ
- การสื่อสารระหว่างกลุ่มคน เฉพาะกลุ่มแบบไม่เป็นสาธารณะ เป็นการตั้งกลุ่มเพื่อการสื่อสาร เช่น กลุ่ม Facebook ที่เป็นกลุ่มปิด หรือกลุ่มสนทนาใน Social Media
- การสื่อสารระหว่างกลุ่มคน แบบเป็นสาธารณะ เป็นการโพสต์แบบเป็นสาธารณะ โพสต์บนหน้า Facebook ส่วนตัวแล้วเปิดเป็นสาธารณะ ตั้งกลุ่ม Facebook แบบสาธารณะ ตั้งกลุ่มใน LINE แบบเปิด

6. Digital Disruption การปรับตัวในยุคดิจิทัล

แนวทางการปรับตัวของบุคลากรในยุคดิจิทัล ประกอบด้วย มุ่งเน้นการพัฒนาทักษะ (Upskill/Reskill) ให้เท่าทันเทคโนโลยีใหม่ พัฒนาทักษะการเก็บข้อมูล การใช้อุปกรณ์ดิจิทัลในการเก็บรวบรวมและจัดการข้อมูล และการเพิ่มเป้าหมายและขีดความสามารถของตัวเอง

แนวทางการปรับตัวของบุคลากรในสถานที่ทำงานใหม่ ประกอบด้วย เปิดโอกาสให้ตัวเองได้เรียนรู้

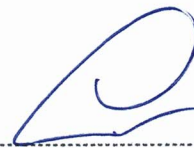
และเป็นส่วนหนึ่งขององค์กร เป็นผู้มีความรับผิดชอบเดียวกันกับองค์กร รู้จักปรับตัวให้เข้ากับเพื่อนร่วมงาน เรียนรู้ เพื่อนร่วมงานที่มีวัยต่างกัน และมีกระบวนการทำงานของเราที่ชัดเจน

การเป็นผู้นำที่ดีในองค์กรในยุคดิจิทัล ต้องผสมผสานความเข้าใจด้านเทคโนโลยี (Digital Literacy) เข้ากับความฉลาดทางอารมณ์ (EQ) เพื่อนำองค์กรผ่านการเปลี่ยนแปลง (Change Management) โดยเน้น การตัดสินใจด้วยข้อมูล (Data-driven) เปิดใจรับฟัง ปรับตัวไว และสร้างวัฒนธรรมการทำงานร่วมกันแบบทีม เพื่อสร้างนวัตกรรมและประสิทธิภาพสูงสุด

การบริหารองค์กรในยุคดิจิทัล องค์กรควรมีเป้าหมาย วิสัยทัศน์ที่ชัดเจน และมีข้อมูลที่จำเป็นทั้งใน ด้านการนำไปสู่เป้าหมาย และมีความเท่าทันการเปลี่ยนแปลงในยุคดิจิทัล การปรับเปลี่ยนกระบวนการทำงาน และวัฒนธรรมองค์กรโดยใช้เทคโนโลยี (Digital Transformation) มาช่วยเพิ่มประสิทธิภาพ ความคล่องตัว และสร้างนวัตกรรมใหม่ๆ เพื่อตอบสนองต่อความต้องการของลูกค้าและสภาพแวดล้อมที่เปลี่ยนแปลงอย่างรวดเร็ว โดยครอบคลุมทั้งการใช้ข้อมูลสารสนเทศ การปรับปรุงขั้นตอนการทำงาน ส่งเสริมการเรียนรู้และการ พัฒนาทักษะบุคลากรที่สามารถเรียนรู้ได้ตลอดชีวิต

การทำงานร่วมกันในสังคมและวัฒนธรรมดิจิทัล ประกอบด้วย การเตรียมพร้อมบุคลากรรับ Digital Refinement ปรับความคิดให้มีความพร้อมที่จะเรียนรู้และยอมรับเทคโนโลยีใหม่ๆ และทดลองปฏิบัติไป พร้อมกับการทำงาน และส่งเสริมการเรียนรู้และฝึกอบรมอยู่เสมอ

ลงชื่อ



(นายอภิชัย กะตะศิลา)

นักวิชาการเกษตรปฏิบัติการ

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ อภิชัย กะตะศิลา

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Digital Literacy : ความฉลาดทางดิจิทัล

(Digital Intelligence)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 14 กุมภาพันธ์ 2569



(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล



e888e7b1