ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ

(Understanding and using digital technology)

นางสาวกานต์มณี จันทร์ขาว นักวิชาการเกษตรชำนาญการ กองเทคโนโลยีชีวภาพทางดิน

ที่มา: หลักสูตร ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Understanding and using digital technology) ผ่านระบบออนไลน์ TDGA โดย คณาจารย์จากสาขาวิชาเทคโนโลยีการจัดการระบบสารสนเทศ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล วันที่ 20 กุมภาพันธ์ 2569

เนื้อหาวิชาเรียนรู้เกี่ยวกับสิทธิ เสรีภาพ และความรับผิดชอบเมื่อใช้สิทธิบนสื่อสาธารณะยุคดิจิทัล เพื่อความเข้าใจการสื่อสารผ่านทางสื่อ และเครื่องมือทางดิจิทัลในแง่มุมต่างๆ มีความเข้าใจ ความมั่นคง ความเป็นส่วนตัวในการใช้อุปกรณ์อิเล็กทรอนิกส์ในยุคดิจิทัล รวมถึงภัยในรูปแบบต่างๆ ทั้งในแง่วิธีการที่ได้รับการคุกคามผลกระทบที่เกิดขึ้น การป้องกัน การลดความเสี่ยง ตลอดจนมีความเข้าใจสารสนเทศและสื่อในยุคดิจิทัลเพื่อที่สามารถระบุข้อมูลที่ต้องการหาข้อมูลนั้น ประเมินประโยชน์ ความเกี่ยวข้อง ความถูกต้อง ความน่าเชื่อถือของข้อมูลนั้นจากแหล่งต่างๆ ได้

1. จริยธรรมการใช้เทคโนโลยีสารสนเทศ

จริยธรรมในการใช้งานคอมพิวเตอร์ จริยธรรมเกี่ยวกับการใช้เทคโนโลยีคอมพิวเตอร์และสารสนเทศ จะกล่าวถึงใน 4 ประเด็น ในลักษณะตัวย่อว่า PAPA

1.1 ความเป็นส่วนตัว (Privacy) หมายถึง สิทธิในการควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น โดยมีตัวอย่างการละเมิดความเป็นส่วนตัว ดังนี้

1.1.1 การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เช่น การเข้าไปอ่าน e-mail ของผู้อื่น หรือใช้คอมพิวเตอร์ตรวจจับการทำงานของพนักงาน

1.1.2 การนำข้อมูลไปใช้ในเชิงธุรกิจ ได้แก่ การรวบรวมข้อมูลส่วนบุคคลสร้างเป็นฐานข้อมูลแล้วเอาไปขาย หรือการทำธุรกิจผ่านเว็บไซต์เพื่อรวบรวมข้อมูลไปขาย (เช่น บริษัท doubleclick และ enage)

1.1.3 การรบกวนด้วยข้อมูลขยะ เช่น การใช้โปรแกรม sniffer วิเคราะห์การใช้ internet เพื่อติดตามผู้ใช้และส่ง e-mail ขายสินค้า ทำให้เกิดอีเมลขยะ (junk mail) ที่ผู้รับไม่ต้องการ หรือที่เรียกว่า สแปม (Spam)

1.2 ความถูกต้อง (Accuracy) ความถูกต้องแม่นยำของข้อมูลและสารสนเทศ

ความถูกต้องของสารสนเทศขึ้นอยู่กับ ความถูกต้องในการบันทึกข้อมูล ต้องมีผู้รับผิดชอบ ในเรื่องความถูกต้องของข้อมูลชัดเจน ต้องมีการตรวจสอบความถูกต้องก่อนการบันทึกข้อมูลทุกครั้ง การให้สิทธิเจ้าของข้อมูล เช่น หากให้ลูกค้าป้อนข้อมูลเอง ต้องให้สิทธิลูกค้าในการเข้าไปตรวจสอบความถูกต้องด้วยตนเองได้ข้อมูลต้องมีความทันสมัยอยู่เสมอ

1.3 ความเป็นเจ้าของ (Property) กรรมสิทธิ์และสิทธิในทรัพย์สินทางปัญญา ได้แก่ ทรัพย์สินที่จับต้องได้ เช่น คอมพิวเตอร์ รถยนต์ ทรัพย์สินทางปัญญา (จับต้องไม่ได้) เช่น บทเพลง โปรแกรมคอมพิวเตอร์

1.3.1 การคุ้มครองตามกฎหมาย ประกอบด้วย

1) ความลับทางการค้า เกี่ยวกับสูตร กรรมวิธีการผลิต หรือรูปแบบสินค้า

2) ลิขสิทธิ์ คุ้มครองงานเขียน ดนตรี ศิลปะ ป้องกันการคัดลอก/ทำซ้ำ มีอายุคุ้มครอง 50 ปี หลังการแสดงผลงานครั้งแรก

3) สิทธิบัตร คุ้มครองสิ่งประดิษฐ์หรือการออกแบบผลิตภัณฑ์ มีอายุคุ้มครอง 20 ปี นับจากวันที่ขอรับสิทธิ

1.3.2 ประเภทของซอฟต์แวร์ และสิทธิในการใช้งาน

1) Software license ผู้ใช้ต้องซื้อสิทธิ์มาก่อนจึงจะมีสิทธิ์ใช้งานได้

2) Shareware ผู้ใช้สามารถทดลองใช้งานได้ก่อนที่จะตัดสินใจซื้อ

3) Freeware สามารถใช้งานได้ฟรีและเผยแพร่ให้ผู้อื่นได้

1.4 การเข้าถึงข้อมูล (Data accessibility) สิทธิและขอบเขตในการเข้าถึงข้อมูลสารสนเทศ เน้นเรื่องความปลอดภัยและสิทธิในการเข้าถึงข้อมูล

1.4.1 มีการกำหนดสิทธิตามระดับผู้ใช้งาน

1.4.2 ป้องกันการเข้าถึงข้อมูลของผู้ที่ไม่เกี่ยวข้อง

1.4.3 ต้องมีการออกแบบระบบรักษาความปลอดภัย ในการเข้าถึงข้อมูลของผู้ใช้

2. การเข้าถึงสื่อดิจิทัล

2.1 อินเทอร์เน็ต (Internet): ย่อมาจาก Inter Connection network หมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายคอมพิวเตอร์ทั่วโลกเข้าไว้ด้วยกัน เพื่อให้เกิดการสื่อสาร และการแลกเปลี่ยนข้อมูลโดยประโยชน์ของ Internet มีดังนี้

2.1.1 การสื่อสาร เช่น e-mail, chat และ telephone

2.1.2 การแลกเปลี่ยนข้อมูล เช่น ส่งไฟล์ต่างๆ webboard

2.1.3 เครื่องมือทางธุรกิจ เช่น เว็บไซต์บริษัท ระบบธุรกรรมทางอิเล็กทรอนิกส์

2.1.4 การสืบค้นข้อมูล เช่น google, bing, aol และ yahoo

2.1.5 ความบันเทิง เช่น youtube และ sanook

2.2 Cloud คือ บริการที่เราสามารถใช้งานทรัพยากรคอมพิวเตอร์ (เช่น พื้นที่เก็บข้อมูล หน่วยประมวลผล หรือซอฟต์แวร์) ผ่านอินเทอร์เน็ต โดยที่เราไม่ต้องมีเครื่องเซิร์ฟเวอร์ตั้งอยู่ที่บ้านหรือที่ทำงานเอง ข้อมูลจะถูกเก็บไว้ที่เครื่องคอมพิวเตอร์ของผู้ให้บริการ (เช่น Google, Microsoft หรือ Amazon) และเราสามารถเข้าถึงข้อมูลเหล่านั้นได้จากทุกที่ทุกเวลาเพียงแค่มีอินเทอร์เน็ต

2.3 Big Data คือ ข้อมูลที่มีปริมาณมหาศาล มีความซับซ้อน และเพิ่มขึ้นอย่างรวดเร็ว หรือผลผลิตจากการที่ผู้คนใช้งานอินเทอร์เน็ตเพื่อสื่อสาร ค้นหาข้อมูล และบันทึกกิจกรรมต่างๆ จนเกิดเป็นฐานข้อมูลขนาดใหญ่ โดยปกติ Big Data จะประกอบด้วยหลัก 5Vs ดังนี้:

2.3.1 Volume (ปริมาณ) ข้อมูลมีจำนวนมหาศาลมาก (เช่น ข้อมูลการแชท หรือ e-mail ของคนทั้งโลก)

2.3.2 Velocity (ความเร็ว) ข้อมูลเกิดขึ้นและเปลี่ยนแปลงตลอดเวลาแบบ Real-time

2.3.3 Variety (ความหลากหลาย) มีทั้งข้อความ รูปภาพ วิดีโอ หรือไฟล์เสียง

2.3.4 Veracity (ความแม่นยำ) ข้อมูลมีความน่าเชื่อถือและถูกต้อง

2.3.5 Value (คุณค่า) สามารถนำข้อมูลมาวิเคราะห์เพื่อสร้างประโยชน์ทางธุรกิจได้

3. ความเข้าใจและการสื่อสารยุคดิจิทัล

การเข้าใจและการสื่อสารในยุคดิจิทัลไม่ใช่แค่เรื่องของการใช้แอปพลิเคชันเก่งขึ้น มันคือการปรับเปลี่ยนกระบวนทัศน์ (Paradigm Shift) ในการรับส่งข้อมูลที่มีความเร็วสูงและซับซ้อนกว่ายุคก่อนเป็นอย่างมาก โดยแบ่งประเด็นสำคัญออกเป็น 3 ด้านหลัก ดังนี้

3.1 ความเข้าใจในยุคดิจิทัล (Digital Literacy & Understanding) ในยุคที่ข้อมูลท่วมท้น (Information Overload) ความเข้าใจไม่ได้วัดกันที่ว่าเรารู้เยอะแค่ไหน แต่วัดที่ความสามารถในการคัดกรองข้อมูลต่างๆ

3.1.1 Critical Thinking การมีวิจารณญาณแยกแยะระหว่าง Fact (ข้อเท็จจริง) และ Fake News (ข่าวปลอม)

3.1.2 Data Synthesis ความสามารถในการนำข้อมูลจากหลายแหล่ง (Multi-platform) มาประมวลผลเป็นองค์ความรู้เดียว

3.1.3 Digital Empathy: ความเข้าใจในบริบทของผู้อื่นผ่านหน้าจอ ซึ่งมักขาดน้ำเสียงและภาษากาย ทำให้เกิดการตีความผิดได้ง่าย

3.2 ลักษณะเฉพาะของการสื่อสารยุคใหม่ (Nature of Digital Communication)
การสื่อสารเปลี่ยนจาก หนึ่งไปยังกลุ่ม (One-to-Many) เป็น ทุกคนถึงทุกคน (Many-to-Many) โดยมีลักษณะเด่นคือ

3.2.1 Real-time & Instant ความคาดหวังต่อการตอบกลับที่รวดเร็ว (Instant Gratification)

3.2.2 Two-way Interaction ผู้รับสารไม่ใช่แค่คนฟัง แต่เป็นผู้สร้างเนื้อหา (Content Creator) และผู้โต้ตอบได้ในทันที

3.2.3 Visual Dominance การใช้ภาพ (Infographic) วิดีโอสั้น (TikTok/Reels) และ Emoji เพื่อสื่อสารอารมณ์แทนตัวอักษร

3.3 ความท้าทายที่ต้องระวัง แม้จะสะดวกสบาย แต่การสื่อสารยุคนี้มีกับดักที่ควรระวัง

ประเด็น	ผลกระทบ	วิธีรับมือ
Echo Chamber	จะเห็นแต่ความเห็นที่เหมือนกับเรา	เปิดรับแหล่งข่าวที่หลากหลาย
Digital Footprint	สิ่งที่โพสต์จะคงอยู่ตลอดไป	คิดก่อนคลิก (Pause before post)
Context Collapse	ข้อมูลถูกนำไปใช้ผิดบริบท	สื่อสารให้ชัดเจนและระบุที่มา

4. ความปลอดภัยยุคดิจิทัล

4.1 Digital Footprint คือ ข้อเขียน รูปภาพ หรือสิ่งต่างๆ ที่เราเขียนหรือลงไว้ใน Social Media ทั้งหลาย เช่น Facebook, Twitter, Instagram, Social Cam และ TikTok หรือช่องทางอื่นๆ ข้อมูลพื้นฐานของ Digital Footprint ได้แก่

4.1.1 ภาพหรือข้อมูลส่วนตัว เช่น หมายเลขโทรศัพท์ ที่อยู่ หมายเลขบัตรประชาชน

4.1.2 การดำเนินชีวิต และ การเป็นอยู่ของเรา

4.1.3 ภาพกับเพื่อน กลุ่มต่าง ๆ

4.2.4 ความสัมพันธ์กับคนต่างๆ ยกตัวอย่างเช่น เพื่อนใน Facebook (เพื่อนร่วมงาน และเจ้านาย)

4.2 ปัจจัยที่กระทำก่อให้เกิด Digital Footprint

4.2.1 ไม่เห็นเป็นอะไร Facebook และ Instagram เป็นพื้นที่ส่วนตัว

4.2.2 ไม่ใช่คนดัง ไม่ใช่ดารา ไม่มีใครสนใจหรอก

4.2.3 แค่อยากระบายอะไรบ้าง

ความเข้าใจผิดที่คิดว่าโซเชียลมีเดียเป็น พื้นที่ส่วนตัว นั้นมักจะนำไปสู่ปัญหาในภายหลัง เพราะข้อมูลที่ถูกโพสต์ลงไปแล้วมักจะคงอยู่ตลอดไปและเข้าถึงได้โดยผู้อื่น

4.3 อันตรายของการสร้าง Digital Footprint

4.3.1 ทดสอบค้นหาชื่อตัวเอง

4.3.2 ข้อมูลมีโอกาสโดนทำสำเนาไปนับไม่ถ้วน

4.3.3 อยู่ในมือผู้ไม่หวังดี

4.3.4 เสียภาพพจน์ และภาพลักษณ์ โดยไม่อาจแก้ไขได้

4.4 คำแนะนำในการตั้งรหัสผ่านให้ปลอดภัย

4.4.1 สิ่งที่ไม่ควรนำมาตั้งเป็นรหัสผ่านจากข้อมูลพื้นฐานของ Digital Footprint ควรหลีกเลี่ยงการใช้ข้อมูลเหล่านี้เพราะผู้ไม่หวังดีสามารถหาได้ง่าย ได้แก่

1) ข้อมูลส่วนตัว เช่น หมายเลขโทรศัพท์ วันเดือนปีเกิด หรือที่อยู่

2) หมายเลขระบุตัวตน เช่น หมายเลขบัตรประชาชน

3) ชื่อบุคคลใกล้ชิด เช่น ชื่อเพื่อนใน Facebook ชื่อเพื่อนร่วมงาน หรือชื่อเจ้านาย

4.4.2 หลักการตั้งรหัสผ่านที่แข็งแรง (Strong Password) รหัสผ่านที่ดีควรป้องกันไม่ให้ข้อมูลของคุณถูกทำสำเนาหรือนำไปใช้ในทางที่ผิดจนเสียภาพลักษณ์

1) ความยาว: ควรมีความยาวอย่างน้อย 12 ตัวอักษรขึ้นไป

2) ความหลากหลาย ผสมผสานระหว่าง อักษรตัวพิมพ์ใหญ่ (A-Z) ตัวพิมพ์เล็ก (a-z) ตัวเลข (0-9) และสัญลักษณ์พิเศษ (เช่น @, #, $, %)

3) ไม่ใช้ซ้ำหลีกเลี่ยงการใช้รหัสผ่านเดียวกันในทุกบัญชี เพราะหากหลุดไปเพียงครั้งเดียว ข้อมูลทั้งหมดจะตกอยู่ในอันตรายทันที

4.4.3 การเพิ่มชั้นความปลอดภัย (2FA) นอกจากการตั้งรหัสผ่านแล้ว ควรเปิดใช้งาน การยืนยันตัวตนแบบสองชั้น (Two-Factor Authentication) เพื่อป้องกันกรณีที่รหัสผ่านหลุดไปอยู่ในมือผู้ไม่หวังดี ซึ่งจะช่วยลดโอกาสที่ภาพลักษณ์ของคุณจะเสียหายโดยไม่อาจแก้ไขได้

4.5 การหลอกลวงออนไลน์ (Fraud) และข้อควรระวังเมื่อซื้อสินค้า

4.5.1 ตรวจสอบความน่าเชื่อถือ ควรตรวจสอบร้านค้าเสมอก่อนตัดสินใจซื้อ

4.5.2 ใช้ระบบชำระเงินที่มั่นใจได้ เลือกซื้อสินค้าที่จ่ายผ่านบัตรเครดิตผ่านระบบที่น่าเชื่อถือ เช่น Verified by VISA หรือ MasterCard SecureCode

4.5.3 ตรวจสอบยอดการใช้จ่าย เช็กยอดหนี้ในบัตรเครดิตอย่างละเอียดสม่ำเสมอ

4.5.4 การป้องกันข้อมูลส่วนบุคคล ไม่ส่งข้อมูลส่วนตัวหรือข้อมูลรหัสผ่าน ให้กับผู้อื่น

4.5.5 สังเกตราคาสินค้า ระวังเมื่อพบร้านที่ขายสินค้าถูกผิดปกติเมื่อเทียบกับร้านอื่น