

ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Understanding and using digital technology)

โดย นางสาวบุษบา ฐิณ้อม
ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ
หน่วยงาน กลุ่มวิชาการฯ สำนักงานพัฒนาที่ดินเขต ๑๐

วัตถุประสงค์

๑. มีความรู้ ความเข้าใจความรู้ด้านสารสนเทศ สื่อ และเทคโนโลยี ตามแนวทางการเรียนรู้ในศตวรรษที่ ๒๑
๒. รู้เท่าทันสื่อดิจิทัล คิด วิเคราะห์ แยกแยะ สื่อดิจิทัลเพื่อเลือกใช้งานได้อย่างเหมาะสม
๓. มีความเข้าใจและปฏิบัติงานด้านดิจิทัลได้อย่างถูกต้องและปลอดภัย ตลอดจนตระหนักถึงภัยคุกคามทางดิจิทัลและสามารถตรวจสอบการทำงานตามหลักปฏิบัติงานที่ดีได้ในเบื้องต้น
๔. มีความเข้าใจในการใช้เทคโนโลยีดิจิทัล เพื่อทำงานผลิตชุดข้อมูลสำหรับการบริการสาธารณะ และมีความรู้ในการใช้สื่อดิจิทัลเพื่อการทำงานได้อย่างมีประสิทธิภาพ

สรุปรายละเอียดเนื้อหาของหลักสูตร

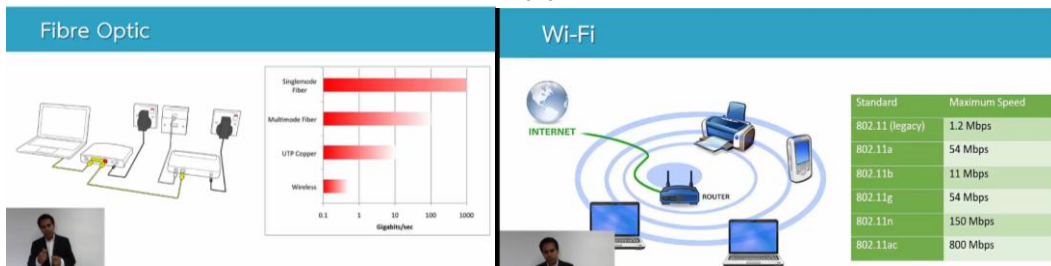
๑. จริยธรรมการใช้เทคโนโลยีสารสนเทศ

- ความหมายของจริยธรรม: หลักศีลธรรมจรรยาและหลักความถูกต้องที่ประชาชนตกลงร่วมกัน เพื่อใช้เป็นแนวทางปฏิบัติและควบคุมการใช้คอมพิวเตอร์/สารสนเทศ
- จริยธรรมในการใช้งานคอมพิวเตอร์ (หลัก PAPA):
 ๑. Privacy (ความเป็นส่วนตัว): สิทธิในการควบคุมข้อมูลของตนเอง ปัญหาที่พบคือ การอ่านอีเมลผู้อื่น, สปแอม (Spam) จากโปรแกรม Sniffer, และการแอบนำข้อมูลไปขาย
 ๒. Accuracy (ความถูกต้อง): ข้อมูลต้องได้รับการตรวจสอบและแก้ไขให้ถูกต้องและทันสมัยอยู่เสมอ
 ๓. Property (ความเป็นเจ้าของ/ทรัพย์สินทางปัญญา):
 - ซอฟต์แวร์: แบ่งเป็น *Software License* (ต้องซื้อสิทธิ), *Shareware* (ทดลองใช้ก่อนซื้อ), และ *Freeware* (ใช้และแจกจ่ายฟรี)
 - ความคุ้มครองตามกฎหมาย: สิทธิบัตร/อนุสิทธิบัตร (คุ้มครองการประดิษฐ์ ๒๐/๑๐ ปี), ลิขสิทธิ์ (คุ้มครองผลงาน ๕๐ ปีหลังเสียชีวิตหรือแรกสร้าง), ความลับทางการค้า, เครื่องหมายการค้า, และสิ่งบ่งชี้ทางภูมิศาสตร์
 ๔. Data Accessibility (การเข้าถึงข้อมูล): กำหนดสิทธิตามระดับผู้ใช้งานและจัดทำระบบรักษาความปลอดภัย ป้องกันผู้ไม่เกี่ยวข้องเข้าถึงข้อมูล
- บัญญัติ ๑๐ ประการของการใช้อินเทอร์เน็ต: เน้นการไม่ทำร้าย ไม่ส่อดนมั ไม่โจรกรรม ไม่สร้างหลักฐานเท็จ ไม่ละเมิดลิขสิทธิ์ และเคารพกฎระเบียบสังคม
- พ.ร.บ. ลิขสิทธิ์:
 - งานที่คุ้มครอง: วรรณกรรม, นาฏกรรม, ศิลปกรรม, ดนตรี, โสตทัศนวัสดุ, ภาพยนตร์, สิ่งบันทึกเสียง, งานแพร่เสียงแพร่ภาพ
 - สิ่งที่ไม่คุ้มครอง: ความคิด, ทฤษฎี, ข่าวสารข้อเท็จจริงประจำวัน, กฎหมาย, ประกาศทางราชการ

- **สิทธิเจ้าของลิขสิทธิ์:** สิทธิทางเศรษฐกิจ (ทำซ้ำ ดัดแปลง เผยแพร่ ให้เช่า) และสิทธิทางศีลธรรม (ห้ามบิดเบือนทำลายชื่อเสียง)
- **บทลงโทษ:** ปรับ ๑๐,๐๐๐ – ๑๐๐,๐๐๐ บาท (หากทำเพื่อการค้า จำคุก ๓ เดือน – ๒ ปี หรือปรับ ๕๐,๐๐๐ – ๔๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ)
- **ข้อยกเว้นการละเมิด:** ทำเพื่อการศึกษา/วิจัย, ใช้ส่วนตัว, ตีพิมพ์/รายงานข่าวโดยให้เครดิต, การใช้งานในห้องสมุด (ต้องไม่ขัดต่อผลประโยชน์และสิทธิอันชอบธรรมของเจ้าของลิขสิทธิ์)

๒. การเข้าถึงสื่อดิจิทัล

- **สื่อดิจิทัล:** สื่อที่รวมข้อความ ภาพ เสียง โดยอาศัยเทคโนโลยีคอมพิวเตอร์และการสื่อสาร
- **วิถีชีวิตดิจิทัล (Digital Lifestyle):** สื่อปัจจุบันมีความรวดเร็ว ประหยัด ไร้ขีดจำกัดด้านพื้นที่และเวลา มีปฏิสัมพันธ์สองทาง และเปิดให้มือสมัครเล่นนำเสนอสื่อได้
- **การเชื่อมต่ออินเทอร์เน็ต:**
 - แบบใช้สาย (Wire): Dial-up, Leased Line, ADSL, LAN, Fiber Optic
 - แบบไร้สาย (Wireless): Wi-Fi, สัญญาณโทรศัพท์มือถือ (๓G, ๔G, LTE)



- **เทคนิคการค้นหาข้อมูล (Search Engine):**
 - ตัดคำที่ไม่ต้องการ (-), ค้นหาสิ ("..."), ใช้คำเชื่อม (OR), ค้นหาเฉพาะเว็บไซต์ (site:) หรือประเภทไฟล์ (filetype:)
 - ค้นหาโดยเว้นคำไว้ (*), ค้นหาภาพ (images.google.com), แปลงหน่วย/ค่าเงิน, ค้นหาตำแหน่ง (Google Maps)

๓. ความเข้าใจและการสื่อสารยุคดิจิทัล

- **การเลือกรูปแบบการสื่อสารให้เหมาะสม:**
 - Synchronous (ประสานเวลา) vs Asynchronous (ไม่ประสานเวลา)
 - การสื่อสารแบบตัวต่อตัว vs แบบกลุ่ม
 - การสื่อสารแบบเป็นทางการ vs ไม่เป็นทางการ
 - พิจารณาตามความสำคัญ ความเร่งด่วน และความจำเป็นในการบันทึกไว้อ้างอิง



๔. ความปลอดภัยยุคดิจิทัล

- **Digital Footprint (รอยเท้าดิจิทัล):** ร่องรอยข้อมูลส่วนตัว พฤติกรรม รูปภาพ หรือความสัมพันธ์ที่ทิ้งไว้บน Social Media ซึ่งเสี่ยงต่อการถูกคัดลอก เสียภาพลักษณ์ หรือตกอยู่ในมือผู้ไม่หวังดี
- **ความปลอดภัยของรหัสผ่าน:**
 - **ข้อห้าม:** อย่าใช้รหัสเดียวกันทุกบริการ, อย่าใช้ข้อมูลส่วนตัว (วันเกิด/เบอร์โทร/คำง่ายๆ), ควรอัปเดตรหัสผ่านเสมอ
 - **รหัสผ่านที่ดี:** ยาวอย่างน้อย ๘ ตัวอักษร มีตัวพิมพ์ใหญ่-เล็ก ตัวเลข และสัญลักษณ์ผสมกัน
- **การรักษาความปลอดภัยระบบ:**
 - **Two-Factor Authentication (๒FA):** ยืนยันตัวตน ๒ ขั้นตอน (ใช้รหัสผ่าน + รหัสจากอุปกรณ์อื่น)
 - **Principle of Least Privilege:** ให้สิทธิการเข้าถึงระบบแก่ผู้ใช้เท่าที่จำเป็นต่อการทำงานเท่านั้น
 - **HTTPS:** การส่งข้อมูลแบบเข้ารหัส (Cipher Text) ผ่าน SSL บนพอร์ต ๔๔๓ เพื่อป้องกันการแอบดักข้อมูล
 - **WPA๒:** เทคโนโลยีเข้ารหัสความปลอดภัยสำหรับเครือข่าย Wi-Fi
- **ภัยคุกคามและการหลอกลวง:**
 - **Malware:** โปรแกรมประสงค์ร้ายที่คอยดักจับหรือล้วงข้อมูล



- **Phishing & Social Engineering:** เทคนิคหลอกลวงด้วยอีเมลหรือเว็บปลอมเพื่อขโมยข้อมูลส่วนตัว/การเงิน



- **ข้อควรระวังการช้อปปิ้งออนไลน์:** ตรวจสอบความน่าเชื่อถือของร้านค้า, ชำระผ่านระบบที่ปลอดภัย (Verified by VISA ฯลฯ), ระวังร้านที่ขายถูกผิดปกติ
- **ความปลอดภัยบนอุปกรณ์เคลื่อนที่ (Mobile Security):** ติดตั้งโปรแกรมสแกนไวรัส, อัปเดต OS เสมอ, ปิด Wi-Fi/Bluetooth เมื่อไม่ใช้, ตั้งลบข้อมูลอัตโนมัติหากเครื่องหาย และระมัดระวังการใช้งานในที่สาธารณะ

ประโยชน์ที่ได้รับจากการฝึกอบรม

๑. ต่ตนเอง เสริมสร้างความปลอดภัยส่วนบุคคล: เข้าใจการสร้างรหัสผ่านที่ปลอดภัย (Strong Password) และการเปิดใช้งานระบบยืนยันตัวตน ๒ ขั้นตอน (2FA) ทำให้ลดเสี่ยงจากการถูกแฮกบัญชี และตระหนักรู้เรื่อง Digital Footprint: ระวังการโพสต์ข้อมูลส่วนตัวบนโซเชียลมีเดีย ช่วยป้องกันการสูญเสียภาพลักษณ์และอันตรายจากผู้ไม่หวังดีและการหลอกลวงออนไลน์ (Scam) และนำความรู้ไปพัฒนาทักษะดิจิทัล: ค้นหาข้อมูลได้อย่างรวดเร็วและแม่นยำด้วยเทคนิค Search Engine ขั้นสูง ตลอดจนเลือกช่องทางการสื่อสารได้เหมาะสมตามสถานการณ์

๒. ต่องค์กร ยกระดับความปลอดภัยข้อมูลขององค์กร: เจ้าหน้าที่มีความเข้าใจในหลักการจำกัดสิทธิเข้าถึงข้อมูล (Principle of Least Privilege) และการใช้โปรโตคอลปลอดภัย (เช่น HTTPS / WPA๒) ลดความเสี่ยงข้อมูลรั่วไหล และลดความเสี่ยงทางกฎหมาย: องค์กรปฏิบัติตาม พ.ร.บ. ลิขสิทธิ์ และกฎหมายทรัพย์สินทางปัญญาอย่างถูกต้อง ป้องกันปัญหาการฟ้องร้องและโทษปรับ ทำให้สร้างวัฒนธรรมองค์กรที่ดี: เกิดสภาพแวดล้อมการทำงานที่เคารพสิทธิ ความเป็นส่วนตัว และมีจริยธรรมในการใช้เทคโนโลยีร่วมกัน

๓. ต่สาธารณะ ลดปัญหาการละเมิดลิขสิทธิ์: ร่วมสร้างสังคมที่เคารพผลงาน ทรัพย์สินทางปัญญา และสิทธิของผู้อื่น (ตามหลัก “ขออนุญาต - ให้เครดิต - ห้ามดัดแปลง”) และสร้างสังคมไซเบอร์ที่ปลอดภัย: การสร้างพลเมืองดิจิทัล (Digital Citizen) ที่มีจริยธรรม ช่วยลดอาชญากรรมทางเทคโนโลยีและการหลอกลวงในสังคมโดยรวม

การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน

นำไปใช้ในการจัดการและปกป้องข้อมูลโดยใช้รหัสผ่านที่รัดกุม มีตรวจสอบสิทธิการเข้าถึงไฟล์งาน และฐานข้อมูล โดยให้สิทธิ์เฉพาะผู้ที่เกี่ยวข้องเท่านั้น (Least Privilege) และหลีกเลี่ยงการเชื่อมต่อ Wi-Fi สาธารณะที่ไม่ปลอดภัยในการทำงาน หรือส่งข้อมูลสำคัญผ่านทางช่องทางที่ไม่เข้ารหัส (เลือกใช้ HTTPS) ปฏิบัติตามกฎหมายและจริยธรรมโดยตรวจสอบประเภทลิขสิทธิ์ของซอฟต์แวร์ รูปภาพ ข้อความ หรือสื่อก่อนนำมาใช้งานขององค์กร โดยเลือกใช้ Freeware หรือสื่อที่อนุญาตถูกต้อง และให้เครดิตอ้างอิงทุกครั้งและไม่คัดลอก ทำซ้ำ หรือดัดแปลงผลงานของผู้อื่นเพื่อการค้าโดยไม่ได้รับอนุญาต

แหล่งที่มา

หลักสูตร : ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ

วิทยากร/ผู้ให้ความรู้ : ๑. ดร.ปรัชญ์ สง่างาม
๒. ผู้ช่วยศาสตราจารย์ ดร.ทวีศักดิ์ สมานชื่น
๓. ผู้ช่วยศาสตราจารย์ ดร.โชติศรีรัต ธรรมบุษดี
๔. อาจารย์มนัสศิริ จันสุทธิราษฎร์

หน่วยงานที่จัดอบรม : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล

รูปแบบหลักสูตร : e-Learning

ช่วงเวลาการฝึกอบรม : สิงหาคม ๒๕๖๔