

แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๒
รอบการประเมินที่ ๒/๒๕๖๙ ตั้งแต่วันที่ ๑ เมษายน ๒๕๖๙ – ๓๐ กันยายน ๒๕๖๙
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ชื่อ - นามสกุล นายเจษฎาพงษ์ นะตาปา ตำแหน่ง เจ้าพนักงานการเกษตรปฏิบัติงาน
หน่วยงาน สถานีพัฒนาที่ดินฉะเชิงเทรา
หัวข้อการพัฒนา ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Understanding and using digital technology)
วิธีการพัฒนา ผ่านการอบรมทางออนไลน์
วันที่พัฒนา ๑๙ สิงหาคม ๒๕๖๙ สถานที่ สถานีพัฒนาที่ดินฉะเชิงเทรา
หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

วัตถุประสงค์

มีความรู้ ความเข้าใจความรู้ด้านสารสนเทศ สื่อ และเทคโนโลยี ตามแนวทางการเรียนรู้ในศตวรรษที่ ๒๑ รู้เท่าทันสื่อดิจิทัล คิด วิเคราะห์ แยกแยะ สื่อดิจิทัลเพื่อเลือกใช้งานได้อย่างเหมาะสม มีความเข้าใจและปฏิบัติงานด้านดิจิทัลได้อย่างถูกต้องและปลอดภัย ตลอดจนตระหนักถึงภัยคุกคามทางดิจิทัลและสามารถตรวจสอบการทำงานตามหลักปฏิบัติงานที่ดีได้ในเบื้องต้น มีความเข้าใจในการใช้เทคโนโลยีดิจิทัลเพื่อทำงานผลิต ชุดข้อมูลสำหรับการบริการสาธารณะ และมีความรู้ในการใช้สื่อดิจิทัลเพื่อการทำงานได้อย่างมีประสิทธิภาพ

สรุปสาระสำคัญ

๑. จริยธรรมการใช้เทคโนโลยีสารสนเทศ

จริยธรรม (ethics) หมายถึง หลักศีลธรรมจรรยาที่กำหนดขึ้นเพื่อใช้เป็นแนวทางปฏิบัติหรือควบคุมการใช้ระบบคอมพิวเตอร์และสารสนเทศ เป็นหลักของความถูกต้องและความผิดที่บุคคลใช้เป็นแนวทางในการ ปฏิบัติกล่าวถึงใน ๔ ประเด็น ในลักษณะตัวย่อว่า PAPA

- ๑) ความเป็นส่วนตัว (Privacy) สิทธิในการควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น
- ๒) ความถูกต้อง (Accuracy) ขึ้นอยู่กับความถูกต้องในการบันทึกข้อมูล ต้องมีผู้รับผิดชอบในเรื่องความ ถูกต้อง การตรวจสอบความถูกต้องก่อนการบันทึก เช่น ถ้าให้ลูกค้าป้อนข้อมูลเอง ต้องให้สิทธิในการเข้าไป ตรวจสอบความถูกต้องด้วยตนเอง ข้อมูลต้องมีความทันสมัยอยู่เสมอ
- ๓) ความเป็นเจ้าของ (Property) กรรมสิทธิในการถือครองทรัพย์สิน โดยทรัพย์สินแบ่งเป็น
 - จับต้องได้ เช่น คอมพิวเตอร์ รถยนต์
 - จับต้องไม่ได้แต่บันทึกลงในสื่อต่าง ๆ ได้

ทรัพย์สินทางปัญญา (บทเพลง โปรแกรมคอมพิวเตอร์) ได้รับความคุ้มครองสิทธิภายใต้กฎหมาย ความลับทางการค้า (สูตร กรรมวิธีการผลิต รูปแบบสินค้า)
ลิขสิทธิ์สิทธิในการกระทำใดๆ เกี่ยวกับงานเขียน ดนตรี ศิลปะ คุ้มครองในเรื่องการคัดลอกผลงาน หรือทำซ้ำ โดยคุ้มครอง ๕๐ ปีหลังจากได้แสดงผลงานครั้งแรก

สิทธิบัตร หนังสือที่คุ้มครองเกี่ยวกับสิ่งประดิษฐ์หรือออกแบบผลิตภัณฑ์ มีอายุ ๒๐ ปี นับตั้งแต่วันที่ขอรับสิทธิ

๔) การเข้าถึงข้อมูล (Data accessibility) กำหนดสิทธิตามระดับผู้ใช้งาน ป้องกันการเข้าไปดำเนินการต่างๆ กับข้อมูลของผู้ที่ไม่เกี่ยวข้องต้องมีการออกแบบระบบรักษาความปลอดภัยในการเข้าถึงข้อมูลของผู้ใช้

๒. การเข้าถึงสื่อดิจิทัล

แบนด์วิดท์ (Bandwidth) หมายถึง อัตราการส่งข้อมูลผ่านตัวกลางไปยังอีกสถานที่หนึ่ง ซึ่งตัวกลางนั้น เป็นสายทองแดงหรือสายใยแก้วนำแสง ก็จะมีผลให้อัตราการส่งข้อมูลไปยังสถานที่หนึ่งที่แตกต่างกัน มีหน่วยเป็น บิตต่อวินาที bps (bit per second) กิโลบิตต่อวินาที (Kbps) และเมกะบิตต่อวินาที (Mbps)

ประเภทของการเข้าถึงอินเทอร์เน็ต มี ๒ ประเภท ดังนี้

๑) การเชื่อมต่ออินเทอร์เน็ตแบบใช้สาย (Wire Internet)

- Modem Dial
- Lease Line
- ADSL
- LAN
- Fiber Optic

๒) การเชื่อมต่ออินเทอร์เน็ตแบบไร้สาย (Wireless Internet)

- Wi-Fi
- Mobile Phone
- บลูทูธ
- GPS
- Cloud
- IoT (Internet Optic)
- Big Data

๓. ความเข้าใจและการสื่อสารยุคดิจิทัล (Digital Literacy Curriculum)

ข้อเท็จจริง (Fact) ข้อความแห่งเหตุการณ์ที่เป็นมาหรือเป็นอยู่ตามจริง ข้อความหรือเหตุการณ์ที่จะต้อง วินิจฉัยว่าเท็จหรือจริง ข้อเท็จจริง นั้นต้องสามารถพิสูจน์สนับสนุนยืนยันได้

ข้อคิดเห็น (Opinion) ความเห็น ความรู้สึกนึกคิดของผู้ส่งสารที่สอดแทรกอยู่ในเนื้อหา อาจกล่าวได้ว่า ข้อคิดเห็น นั้นไม่สามารถสนับสนุนยืนยันได้

ลักษณะข้อเท็จจริง (Fact)	ลักษณะข้อเท็จจริง (Opinion)
๑. มีความเป็นไปได้	๑. เป็นข้อความที่แสดงความรู้สึก
๒. มีความสมจริง	๒. เป็นข้อความที่แสดงความคิดคะเน
๓. มีหลักฐานเชื่อถือได้	๓. เป็นข้อความที่แสดงการเปรียบเทียบ
๔. มีความสมเหตุสมผล อุปมาอุปมัย	๔. เป็นข้อความที่เป็นข้อเสนอแนะ หรือเป็น ความคิดเห็นของผู้พูดเอง

ที่มา: ราชบัณฑิตยสถาน พ.ศ. ๒๕๒๕ (ราชบัณฑิตยสถาน ๒๕๒๕ : ๑๓๓)

๔. ความปลอดภัยยุคดิจิทัล

ความเป็นส่วนตัว รอยเท้าดิจิทัล Digital Footprint คือ ข้อเขียน รูปภาพ สิ่งต่าง ๆ ที่เราเขียนหรือลงไว้ใน Social Media ทั้งหลาย ไม่ว่าจะเป็น Facebook Twitter Instagram Social Cam หรือช่องทางไหนก็ตาม

ความมั่นคงปลอดภัย ได้แก่การตั้งรหัสผ่าน การพิสูจน์ตัวตน การกำหนดสิทธิ์ การเข้ารหัสข้อมูล HTTPS ย่อมาจาก Hypertext Transfer Protocol Secure หรือ Hypertext Transfer Protocol Over SSL (Secure Socket Layer) การทำงานเหมือนกับ HTTP ธรรมดาแต่ทำอยู่บน SSL เพื่อให้เกิดความปลอดภัยในการส่งข้อมูลมากยิ่งขึ้น มีรูปแบบดังนี้

- การใช้งาน URL จะเข้าต้นด้วย https// ตามด้วยชื่อของเว็บไซต์
- ทำงานที่พอร์ต (port) ๔๔๓ (มาตรฐาน)
- ส่งข้อมูลเป็นแบบ Cipher text คือ มีการเข้ารหัสข้อมูลในระหว่างการส่ง (Encryption) สามารถถูกจับได้ แต่อ่านข้อมูลนั้นไม่รู้เรื่อง
- มีการทำ Authentication เพื่อตรวจสอบยืนยันระบุตัวตน

WPA๒ คือ เทคโนโลยีการรักษาความปลอดภัยที่ปกป้องเครือข่าย WI-FI ของคุณโดยการเข้ารหัส การจราจรบนเครือข่าย นอกจากนี้ ยังทำให้ผู้ใช้ที่ไม่ได้รับอนุญาตเข้าถึงเครือข่ายได้ยากขึ้น

ภัยจากสาธารณะ

มัลแวร์ (malware - malicious software) คือ โปรแกรมที่ถูกสร้างขึ้นมาเพื่อประสงค์ร้ายต่อเครื่อง คอมพิวเตอร์และเพื่อมาล้วงข้อมูลสำคัญไปจากผู้ใช้งานคอมพิวเตอร์

WannaCry ไวรัสเรียกค่าไถ่ที่ระบาดไปทั่วโลก โดยวันแรกที่ระบาด มีเครื่องคอมพิวเตอร์ติดถึง ๒๓๐,๐๐๐ กว่าเครื่องใน ๑๕๐ ประเทศ ควรปรับปรุงและอัปเดต windows และ software อยู่เสมอ การหลอกลวง (Scam) เล่ห์อุบาย แผนการร้าย คำนี้อาศัยอยู่ในวงการออนไลน์ จะใช้เรียกพฤติกรรมที่มีเจตนาหลอกลวง ให้เสียทรัพย์สิน ให้เสียข้อมูล ตัวอย่าง การหลอกลวงทางอินเทอร์เน็ต เช่น Email Scams Phishing Scam เป็นต้น

การโจมตีแบบวิศวกรรมสังคม (Social Engineering)

Phishing คือ คำที่ใช้เรียกเทคนิคการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น ในบทความนี้จะเน้นในเรื่องของ Phishing ที่มี จุดมุ่งหมายเพื่อหลอกลวงทางการเงิน เนื่องจากจะทำให้ผู้อ่านมองเห็น

การหลอกลวงออนไลน์ (Fraud) มีฉาชีพติดต่อเหยื่อ สร้างความน่าเชื่อถือ หว่านล้อมให้โอนเงิน ไม่ส่ง สินค้าหรือส่งสินค้าปลอม ปิดช่องทางการสื่อสาร เปลี่ยนชื่อ เริ่มวงจรใหม่

ความปลอดภัยยุคดิจิทัล

Mobile Security and Privacy ติดตั้งโปรแกรมป้องกันไวรัสบนมือถือ ติดตั้งเฉพาะโปรแกรมที่น่าเชื่อถือ ปิดการใช้งาน WIFI และ Bluetooth เมื่อไม่ได้ใช้งาน ปรับปรุงระบบปฏิบัติการให้ทันสมัยอยู่เสมอ สำรองข้อมูลที่ สำคัญ ตั้งค่าให้มือถือลบข้อมูลอัตโนมัติเพื่อสูญหาย

พฤติกรรมเสี่ยง เมื่อใช้อุปกรณ์ในที่สาธารณะ เชื่อมกับไวไฟที่ไม่ได้เข้ารหัส ไม่ระวังว่ามีผู้อื่นแอบฟังบทสนทนาอยู่ ไม่ระวังผู้อื่นแอบหน้าจอลบข้อมูลส่วนตัว

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

ได้รับความรู้ ความเข้าใจความรู้ด้านสารสนเทศ สื่อ และเทคโนโลยี รู้เท่าทันสื่อดิจิทัลวิเคราะห์ แยกแยะ สื่อดิจิทัล เพื่อเลือกใช้ทำงานได้อย่างเหมาะสม ตระหนักถึงภัยคุกคามทางดิจิทัลเพื่อการทำงาน ได้อย่างมีประสิทธิภาพ

(ลงชื่อ)



(นายเจษฎาพงษ์ นตะปา)

ตำแหน่ง เจ้าพนักงานการเกษตรปฏิบัติงาน

(ลงชื่อ)



(นายบุญสม พรหมสุวรรณ)

ตำแหน่ง ผู้อำนวยการสถานีพัฒนาที่ดินฉะเชิงเทรา

ความเข้าใจและใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Understanding and using digital technology)

1. จริยธรรมการใช้เทคโนโลยีสารสนเทศ (PAPA)



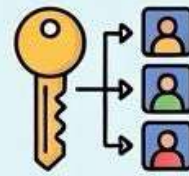
ความเป็นส่วนตัว
สิทธิควบคุมข้อมูล
ของตนเอง



ความถูกต้อง
บันทึกข้อมูลให้
ถูกต้องและทันสมัย



ความเป็นเจ้าของ
ทรัพย์สินทางปัญญา
ลิขสิทธิ์ สิทธิบัตร



การเข้าถึงข้อมูล
กำหนดสิทธิตาม
ระดับผู้ใช้งาน

2. การเข้าถึงสื่อดิจิทัล (Internet Access)

แบบใช้สาย



ADSL



LAN



Fiber Optic

bps, Kbps, Mbps

แบบไร้สาย



Wi-Fi



Mobile
Phone



Bluetooth



GPS



Cloud



IoT



Big Data

3. ความเข้าใจและการสื่อสารยุคดิจิทัล (Digital Literacy: Fact vs Opinion)

ลักษณะข้อเท็จจริง (Fact)

- มีความเป็นไปไม่ได้
- มีความสมบูรณ์
- มีหลักฐานเชื่อถือได้
- มีความสมเหตุสมผล อุปมาอุปไมย



ลักษณะข้อคิดเห็น (Opinion)

- แสดงความรู้สึก
- แสดงความคาดคะเน
- แสดงการเปรียบเทียบ
- เป็นข้อเสนอแนะหรือความคิดเห็น



4. ความปลอดภัยยุคดิจิทัล (Digital Security & Safety)



รอยเท้าดิจิทัล (Digital Footprint)

ข้อมูลที่เราลงไว้บนสื่อออนไลน์



HTTPS & พอร์ต 443

Hypertext Transfer Protocol
Secure, Secured Network

- เข้ารหัสข้อมูล



มัลแวร์ & Phishing

WannaCry, Scam,
โจมตีแบบวิศวกรรมสังคม



ความปลอดภัยบนมือถือ (Mobile Security)

- ติดตั้งโปรแกรมป้องกัน
- อัปเดตระบบ
- เสี่ยง WIFI สาธารณะไม่เข้ารหัส

ประโยชน์ที่ได้รับ

- จากการเพิ่มให้ความรู้, วิเคราะห์ข้อมูลสื่อสารได้อย่างรวดเร็ว, เลือกใช้เทคโนโลยีได้อย่างเหมาะสม
- ตระหนักต่อภัยคุกคามและความปลอดภัยดิจิทัล และกฎหมายด้านเทคโนโลยีดิจิทัล