สรุปบทเรียนที่ได้รับจากการพัฒนาความรู้
ฝึกอบรมผ่านการพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์
สำนักงานคณะกรรมการข้าราชการพลเรือน

ชื่อ-สกุล นายกฤษดา ศรีทับทิม
กลุ่ม/ฝ่าย สถานีพัฒนาที่ดินสุรินทร์ สำนักงานพัฒนาที่ดินเขต ๓
หลักสูตร ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ
เป้าหมายการเรียนรู้

1. มีความรู้ ความเข้าใจในด้านสารสนเทศ สื่อ และเทคโนโลยี ตามแนวทางการเรียนรู้ในศตวรรษที่ 21

2. รู้ทันสื่อดิจิทัล เพื่อสามารถคิดวิเคราะห์ แยกแยะ สื่อดิจิทัลเพื่อเลือกใช้ทำงานได้อย่างเหมาะสม

3. มีการใช้เทคโนโลยีดิจิทัลและสื่อดิจิทัล เพื่อทำงานได้อย่างถูกต้องและปลอดภัย ตลอดจนตระหนักถึงภัย คุกคามทางดิจิทัลและสามารถตรวจสอบการทำงานตามหลักปฏิบัติงานที่ดีได้ในเบื้องต้น

4. มีความเข้าใจในการใช้เทคโนโลยีดิจิทัล เพื่อทำงานผลิตชุดข้อมูลสำหรับการบริการสาธารณะ และมีความรู้ ในการใช้สื่อดิจิทัลเพื่อการทำงานได้อย่างมีประสิทธิภาพ

๑. จริยธรรมการใช้เทคโนโลยีสารสนเทศ

๑.๑ ความเป็นส่วนตัว

- สิทธิในการควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น
- การละเมิดความเป็นส่วนตัว

๑.๒ ความถูกต้อง

- ความต้องขึ้นอยู่กับความถูกต้องในการบันทึกข้อมูล
- ต้องมีผู้รับผิดชอบในเรื่องความถูกต้อง

๑.๓ ความเป็นเจ้าของ

๑.๓.๑ กรรมสิทธิ์ในการถือครองทรัพย์สิน โดยทรัพย์สินแบ่งเป็น

-จับต้องได้ คอมพิวเตอร์ รถยนต์

-จับต้องไม่ได้แต่บันทึกลงในสื่อต่างๆ ได้ (ทรัพย์สินทางปัญญา) บทเพลง โปรแกรมคอมพิวเตอร์

๑.๓.๒ ได้รับความคุ้มครองสิทธิภายใต้กฎหมาย

-ความลับทางการค้า เกี่ยวกับสูตร กรรมวิธีการผลิต รูปแบบสินค้า

-ลิขสิทธิ์ สิทธิในการกระทำใดๆ เกี่ยวกับ งานเขียน ดนตรี ศิลปะ โดยคุ้มครอง ๕๐ ปี หลังจากได้แสดงผลงานครั้งแรก

-สิทธิบัตร หนังสือที่คุ้มครองเกี่ยวกับสิ่งประดิษฐ์ หรือออกแบบผลิตภัณฑ์ มีอายุ ๒๐ ปี นับตั้งแต่วันที่ขอรับสิทธิ

๑.๓.๓ ความเป็นเจ้าของ

-สิทธิการเป็นเจ้าของ หมายถึง กรรมสิทธิ์ในการถือครองทรัพย์สิน ที่จับต้องได้ หรืออาจเป็นทรัพย์สินทางปัญญา

-ความเป็นเจ้าของด้านเทคโนโลยีสารสนเทศ มักจะหมายถึงลิขสิทธิ์ซอฟต์แวร์

ประเภทซอฟต์แวร์

-software license หมายถึง ผู้ใช้ต้องซื้อสิทธิ์มา จึงจะมีสิทธิ์ใช้ได้

-software หมายถึง ผู้ใช้สามารถทดลองใช้ก่อนที่จะซื้อ

-freeware หมายถึง ใช้งานได้ฟรี และเผยแพร่ให้ผู้อื่นได้

๑.๓.๔ การเข้าถึงข้อมูล

-กำหนดสิทธิตามระดับผู้ใช้งาน

-ป้องกันการเข้าไปดำเนินการต่างๆ กับข้อมูลของผู้ที่ไม่เกี่ยวข้อง

-ต้องมีการออกแบบระบบรักษาความปลอดภัยในการเข้าถึงข้อมูลของผู้ใช้

๒. การเข้าถึงสื่อดิจิทัล

สื่อดิจิทัล หมายถึง สื่อที่นำเอาข้อความ กราฟิก ภาพเคลื่อนไหว เสียง มาจัดรูปแบบ โดยอาศัยเทคโนโลยีความเจริญก้าวหน้าทางด้านคอมพิวเตอร์ และการสื่อสารมาประยุกต์ใช้ ทำให้ลดค่าใช้จ่ายและระยะเวลา

ประเภทของการเข้าถึงอินเตอร์เน็ต

- การเชื่อมต่ออินเตอร์เน็ตแบบใช้สาย(Wire Internet)
  - -Modem Dial
  - -Lease Line
  - -ADSL
  - -LAN
  - -Fiber Optic
- การเชื่อมต่ออินเตอร์เน็ตแบบไร้สาย(Wireless Internet)
  - -Wi-Fi
  - -Mobile Phone

๓. ความเข้าใจและกากรสื่อสารยุคดิจิทัล

ผู้รับสารและผู้ส่งสารต้องตระหนักถึงสารที่ได้รับ ๒ ส่วน

-ข้อเท็จจริง หมายถึง ข้อมูลที่สามารถพิสูจน์หรือยืนยันได้

-ข้อคิดเห็น หมายถึง ข้อมูลที่ไม่สามารถพิสูจน์หรือยืนยันได้

ลักษณะของข้อเท็จจริง

-มีความเป็นไปได้

-มีความสมจริง

-มีหลักฐานเชื่อถือได้

-มีความสมเหตุสมผล

ลักษณะของข้อคิดเห็น

-เป็นข้อความที่แสดงความรู้สึก

-เป็นข้อความที่แสดงความคาดคะเน

-เป็นข้อความที่แสดงการเปรียบเทียบอุปมาอุปมัย

-เป็นข้อความที่เป็นข้อเสนอแนะหรือเป็นความคิดเห็นของผู้พูดเอง

เล่นSocial Network ให้ปลอดภัย"รู้"ไว้เลี่ยงอันตราย

๑. คิดให้รอบคอบสักนิดก่อนโพสต์ เพราะมันเปิดเผยและทุกคนเข้าถึงได้ง่าย

๒. ระมัดระวังในการคลิกลิงก์ที่มากับการแชร์ เพราะอาจนำไปสู่ไวรัสหรือช่องทางขโมยข้อมูล

๓. เข้าโซเชียลเน็ตเวิร์ก พิมพ์ URL โดยตรง เลี่ยงคลิกลิงก์ เพราะอาจเป็น URL ปลอม

๔. รอบคอบก่อนตอบรับเป็นเพื่อน คัดกรองคนที่จะขอเป็นเพื่อนโดยเข้าไปดูโปรไฟล์ก่อนทุกครั้ง

๕. ตั้งค่าความเป็นส่วนตัว หลีกเลี่ยงตั้งค่าแบบสาธารณะและอนุญาตให้เพื่อนเท่านั้นที่เห็นกิจกรรมของเราได้

๖. ไม่แสดงข้อมูลส่วนตัวที่เป็นความลับ เช่น บัตรประชาชน บัตรเคดิต

๗. เปิดใช้งาน Do Not Track ป้องกันการติดตามและเก็บข้อมูลจากผู้ให้บริการโซเชียลเน็ตเวิร์ก รวมถึงผู้ไม่หวังดีที่เข้ามาขโมยข้อมูล

๘. ใช้วิจารณญาณในการับข่าวสาร อย่าปักใจเชื่อทันที อาจมีการสร้างกระแส สวมรอย

๙. ควบคุมการใช้งานของบุตรหลาน

๑๐. ตระหนักว่าเป็นสังคมเสรี

๔. ความปลอดภัยยุคดิจิทัล

ความปลอดภัยยุคดิจิทัล ความเป็นส่วนตัว (Privacy) ส่วนสำคัญคือ รอยเท้าดิจิทัล (Digital Footprint) โดยข้อมูลต่างๆ เช่น ข้อความ รูปภาพ สิ่งต่าง ๆ และลงไว้ใน Social Media Facebook, Twitter, Instagram, Social Cam หรือ ช่องทางไหนก็ตาม ซึ่งอันตรายของการทิ้ง Digital Footprint ข้อมูลมีโอกาสโดนทำสำเนาไปนับไม่ถ้วน และอยู่ใน มือผู้ไม่หวังดี ทำให้เสียภาพพจน์ และภาพลักษณ์โดยไม่อาจแก้ไขได้ ความมั่นคงปลอดภัย (Security) ดังนี้

๑) การกำหนดรหัสผ่าน รหัสผ่านที่ไม่ควรตั้ง

-ใช้รหัสเดียวกันหมด รู้รหัสเดียวสามารถเข้าถึงได้หมด

-ไม่มีการเปลี่ยนรหัสผ่าน

-คาดเดาง่าย เช่น 1234567

-ประกอบด้วยข้อมูลบุคคล เช่น วันเกิด เบอร์โทร

-ใช้ตัวพิมพ์ทั้งหมด ไม่มีตัวเลขหรือตัวอักษรผสม รวมทั้งสัญลักษณ์ต่าง ๆ ประกอบกัน

๒. รหัสผ่านที่ดี

-ใช้รหัสผ่านที่ยาว (อย่างน้อย ๘ ตัว)

-ใช้ตัวอักษรตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก ตัวเลข

-ใช้คำมีความหมาย เช่น ชื่อเล่น love happy

-ใช้ตัวอักษรที่แตกต่างกันอย่างน้อย 4 ตัว (อย่าใช้ ตัวอักษรซ้ำกัน) ใช้ตัวเลขและตัวอักษรแบบสุ่ม

๒) การพิสูจน์ตัวตน การพิสูจน์ตัวบุคคลโดยใช้ ๒ ปัจจัย (Two-Factor Authentication) คือ การใช้ปัจจัยที่สอง ร่วมกับการล็อกอินด้วยรหัสผ่านตามปกติ ซึ่งหลังจากการล็อกอินด้วยรหัสผ่านแล้ว ระบบจะถาม รหัสยืนยันจากอุปกรณ์อื่น เช่น โทรศัพท์มือถือ หรือ Token เพื่อความปลอดภัยมากขึ้น อาทิ Google 2 Factor Authentication เป็นต้น 3) การกำหนดสิทธิ์ (Authorization) หลักการสิทธิน้อยที่สุด Principle of Least Privilege สามารถใช้ปรับปรุงความปลอดภัยของระบบคอมพิวเตอร์ เป็นเรื่องพื้นฐานแต่สำคัญมากที่มักถูกถูกมองข้าม หลักการนี้ คือผู้ใช้ จะต้องมีระดับต่ำที่สุดของสิทธิตามความต้องการเพื่อกระทำงานตามที่มอบหมาย

๓) การเข้ารหัสข้อมูล HTTPS ย่อมาจาก Hypertext Transfer Protocol Secure หรือ Hypertext Transfer Protocol Over SSL (Secure Socket Layer) เป็นการทำงานเหมือนกับ HTTP ธรรมดาแต่ทำอยู่บน SSL เพื่อให้ เกิดความปลอดภัยในการส่งข้อมูลมากยิ่งขึ้น มีรูปแบบดังนี้ - การใช้งาน URL จะเข้าต้นด้วย http:// ตามด้วยชื่อของเว็บไซต์ - ทำงานที่พอร์ต (port) 443 (มาตรฐาน) - ส่งข้อมูลเป็นแบบ Cipher text คือ มีการเข้ารหัสข้อมูลในระหว่างการส่ง (Encryption) สามารถถูกดักจับได้ แต่อ่านข้อมูลนั้นไม่รู้เรื่อง - มีการทำ Authentication เพื่อตรวจสอบยืนยันระบุตัวตน WPA2 คือ เทคโนโลยีการรักษาความปลอดภัยที่ปกป้องเครือข่าย Wi-Fi ของคุณโดยการ เข้ารหัสการจราจรบนครือข่าย นอกจากนี้ ยังทำให้ผู้เข้าที่ได้รับอนุญาตเข้าถึงหรือข่ายได้ยากขึ้น

๔) มัลแวร์ (malware - malicious software) คือ โปรแกรมที่ถูกสร้างขึ้นมาเพื่อประสงค์ร้ายต่อ เครื่องคอมพิวเตอร์และเพื่อมาล้วงข้อมูลสำคัญไปจากผู้ใช้งานคอมพิวเตอร์ เช่น WannaCry ไวรัสเรียกค่าไถที่ ระบาดไปทั่วโลก โดยวันแรกที่ระบาด มีเครื่องคอมพิวเตอร์ติดถึง 230,000 กว่าเครื่องใน 150 ประเทศ

๕) การหลอกลวง (Scam) เล่ห์อุบาย แผนการร้าย คำนี้ หากอยู่ในวงการออนไลน์ จะใช้เรียกพฤติกรรมที่มีเจตนาหลอกลวง ให้เสียทรัพย์ ให้เสียข้อมูล การหลอกลวงทางอินเทอร์เน็ต เช่น Email Scams Phishing Scam เป็นต้น โดยการใช้การโจมตีแบบวิศวกรรมสังคม (Social Engineering) จาก

ความไม่รู้เท่าทัน ของผู้ใช้งาน โดยใช้อีเมล์หรือหน้าเว็บไซต์ปลอม เพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคล อื่น ๆ เพื่อนำข้อมูลที่ ได้ไปใช้ในการเข้าถึงระบบ หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น นอกจากนี้ การหลอกลวงออนไลน์ (Fraud) มิจฉาชีพติดต่อเหยื่อสร้างความน่าเชื่อถือ หว่านล้อมให้โอนเงิน ไม่ส่ง สินค้าหรือส่งสินค้าปลอม ปิดช่องทางการสื่อสาร เปลี่ยนชื่อเริ่มวงจรใหม่ ข้อควรระวังเมื่อซื้อสินค้าออนไลน์

(๑) ตรวจสอบความน่าเชื่อถือของร้านค้าเสมอ

(๒) ซื้อสินค้าที่จ่ายผ่านบัตรเครดิต ผ่านระบบที่ น่าเชื่อถือ อาทิ Verified toy VISA และ Master Card Secure Code เป็นต้น

(๓) เช็คยอดหนี้ในบัตรเครดิตอย่างละเอียด

(๔) ไม่ส่งข้อมูลส่วนตัวหรือข้อมูลรหัสผ่าน

(๕) ระวังเมื่อพบร้านที่ขายสินค้าถูกมาก ๆ เมื่อเทียบกับร้าน

๖) ความเป็นส่วนตัวและความปลอดภัยบนมือถือ (Mobile Security and Privacy) สร้างความปลอดภัยดังนี้

(๑) ติดตั้งโปรแกรมป้องกันไวรัสบนมือถือ

(๒) ติดตั้งเฉพาะโปรแกรมที่น่าเชื่อถือ

(๓) ปิดการใช้งาน WIFI และ Bluetooth เมื่อไม่ได้ใช้งาน

(๔) ปรับปรุงระบบปฏิบัติการให้ทันสมัยอยู่เสมอ

(๕) สำรองข้อมูลที่สำคัญ

(๖) ตั้งค่าให้มือถือพบข้อมูลอัตโนมัติเพื่อสูญหาย

พฤติกรรมเสี่ยง เมื่อใช้อุปกรณ์ในที่สาธารณะ (1) เชื่อมกับไวไฟที่ไม่ได้เข้ารหัส (2) ไม่ระวังว่ามีผู้อื่นแอบฟังบทสนทนาอยู่ (3) ไม่ระวังผู้อื่นแอบหน้าจอ (4) ไม่ระวังรอบตัว

(นายกฤษดา ศรีทับทิม)
นักวิชาการเกษตรชำนาญการ