สรุปสิ่งที่ได้รับจากการอบรม/พัฒนาความรู้/ประโยชน์ที่ได้รับจากการอบรม
ผ่านสื่ออิเล็กทรอนิกส์ TDGA e-training

ส่วนที่ ๑ ข้อมูลทั่วไป

ชื่อ นายนิพนธ์ นามสกุล ตรีระแสง

ตำแหน่ง เจ้าพนักงานการเกษตรอาวุโส สังกัด ศูนย์ปฏิบัติการพัฒนาที่ดินโครงการหลวง สำนักงานพัฒนาที่ดินเขต ๖

หลักสูตร/หัวข้อเรื่องอบรม

๑. การออกแบบบริการดิจิทัลภาครัฐ (Government Digital Service Design)

วันที่ ๒๐ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙ ถึงวันที่ ๒๑ กุมภาพันธ์ พ.ศ. ๒๕๖๙

☑ อบรม ☐ สัมมนา ☐ อื่นๆ ระบุ.....

๒. ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Understanding and Using Digital Technology)

วันที่ ๒๑ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙ ถึงวันที่ ๒๒ กุมภาพันธ์ พ.ศ. ๒๕๖๙

☑ อบรม ☐ สัมมนา ☐ อื่นๆ ระบุ.....

ส่วนที่ ๒ สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

หลักสูตรที่สรุป

ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Understanding and Using Digital Technology)

วัตถุประสงค์หลักสูตร

๑. มีความรู้ความเข้าใจด้านสารสนเทศ สื่อ และเทคโนโลยี ตามแนวทางการเรียนรู้ในศตวรรษที่ ๒๑ รู้เท่าทันสื่อดิจิทัล คิด วิเคราะห์ แยกแยะ สื่อดิจิทัลเพื่อเลือกใช้ทำงานได้อย่างเหมาะสม

๒. มีความเข้าใจและปฏิบัติงานด้านดิจิทัลได้อย่างถูกต้องและปลอดภัย ตลอดจนตระหนักถึงภัยคุกคามทางดิจิทัลและสามารถตรวจสอบการทำงานตามหลักปฏิบัติงานที่ดีได้ในเบื้องต้น

๓. มีความเข้าใจในการใช้เทคโนโลยีดิจิทัล เพื่อทำงานผลิตชุดข้อมูลสำหรับการบริการสาธารณะ และมีความรู้ในการใช้สื่อดิจิทัลเพื่อการทำงานได้อย่างมีประสิทธิภาพ

ความหมายของจริยธรรม

๑. หลักศีลธรรมจรรยาที่กำหนดขึ้นเพื่อใช้เป็นแนวทางปฏิบัติหรือควบคุมการใช้ระบบคอมพิวเตอร์และสารสนเทศ

๒. หลักของความถูกต้องและความผิดที่บุคคลใช้เป็นแนวทางในการปฏิบัติ

๓. สรุป เป็นหลักเกณฑ์ที่ประชาชนตกลงร่วมกันเพื่อใช้เป็นแนวทางในการปฏิบัติร่วมกันในสังคม

จริยธรรมในการใช้งานคอมพิวเตอร์ จะกล่าวถึง ๔ ประเด็น ดังนี้

๑. ความเป็นส่วนตัว (Privacy)

๒. ความถูกต้อง (Accuracy)

๓. ความเป็นเจ้าของ (Property)

๔. การเข้าถึงข้อมูล (Data accessibility)

บัญญัติ ๑๐ ประการ ของการใช้อินเตอร์เน็ต

๑. ต้องไม่ใช้คอมพิวเตอร์ทำร้ายหรือละเมิดผู้อื่น

๒. ต้องไม่รบกวนการทำงานของผู้อื่น

๓. ต้องไม่สอดแนม แก้ไข หรือเปิดดูแฟ้มข้อมูลของผู้อื่น

๔. ต้องไม่ใช้คอมพิวเตอร์เพื่อการโจรกรรมข้อมูลข่าวสาร

๕. ต้องไม่ใช้คอมพิวเตอร์สร้างหลักฐานที่เป็นเท็จ

๖. ต้องไม่คัดลอกโปรแกรมของผู้อื่นที่มีลิขสิทธิ์

๗. ต้องไม่ละเมิดการใช้ทรัพยากรคอมพิวเตอร์โดยที่ตนเองไม่มีสิทธิ์

๘. ต้องไม่นำเอาผลงานของผู้อื่นมาเป็นของตน

๙. ต้องคำนึงถึงสิ่งที่จะเกิดขึ้นกับสังคมที่เกิดจากการกระทำของท่าน

๑๐. ต้องใช้คอมพิวเตอร์โดยเคารพกฎระเบียบ กติกา และมีมารยาท

จำไว้ ๓ ข้อ "พ.ร.บ. ลิขสิทธิ์" หลัก ๓ ประการของการไม่ละเมิดกฎหมายลิขสิทธิ์ คือ

๑) ขออนุญาต

๒) ให้เครดิต

๓) ห้ามดัดแปลง

งานที่กฎหมายลิขสิทธิ์ให้ความคุ้มครอง งานสร้างสรรค์ประเภทวรรณกรรมและศิลปกรรม ๙ ประเภท

๑) วรรณกรรม

๒) นาฏกรรม

๓) ศิลปกรรม

๔) ดนตรีกรรม

๕) โสตทัศนวัสดุ

๖) ภาพยนตร์และเสียงประกอบของภาพยนตร์

๗) สิ่งบันทึกเสียง

๘) งานแพร่เสียงแพร่ภาพ

๙) งานอื่นใดในแผนกวรรณคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะ

สิ่งที่ไม่ถือเป็นงานอันมีลิขสิทธิ์ ได้แก่

๑. ความคิด ขั้นตอน กรรมวิธี ระบบ วิธีใช้หรือวิธีทำงาน แนวความคิด หลักการ การค้นพบ หรือทฤษฎีทางวิทยาศาสตร์หรือคณิตศาสตร์

๒. ข่าวประจำวันและข้อเท็จจริงต่างๆ ที่มีลักษณะเป็นเพียงข่าวสารไม่ใช่ลักษณะของงานริเริ่มสร้างสรรค์ในแผนกวรรณคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะ

๓. รัฐธรรมนูญและกฎหมาย

๔. ระเบียบ ข้อบังคับ ประกาศ คำสั่ง คำชี้แจง และหนังสือโต้ตอบของกระทรวง ทบวง กรม หรือหน่วยงานของรัฐหรือของท้องถิ่น

๕. คำพิพากษา คำสั่ง คำวินิจฉัยและรายงานของทางราชการ

๖. คำแปลและการรวบรวมสิ่งต่างๆ ข้างต้น ที่กระทรวง ทบวง กรม หรือหน่วยงานอื่นใดของรัฐหรือของท้องถิ่นจัดทำขึ้น

๗. ตัวอย่างของสิ่งที่ไม่ถือเป็นงานลิขสิทธิ์ เช่น รายชื่อของผู้ใช้โทรศัพท์ (จาก ก-ฮ) ในสมุดโทรศัพท์ ชื่อทั่วไป ชื่อเรื่อง วลีสั้นๆ คำขวัญ เป็นต้น

สิทธิของเจ้าของลิขสิทธิ์ แบ่งเป็นสิทธิหลัก ๒ ประการ คือ

๑) สิทธิทางเศรษฐกิจ

๒) สิทธิทางศีลธรรม

หลักการพิจารณาในการใช้งานลิขสิทธิ์ ได้แก่

๑) ต้องไม่ขัดต่อการแสวงหาประโยชน์จากงานอันมีลิขสิทธิ์

๒) ต้องไม่กระทบกระเทือนถึงสิทธิอันชอบด้วยกฎหมายของเจ้าของลิขสิทธิ์เกินสมควร

สื่อดิจิทัล หมายถึง สื่อที่นำเอาข้อความ กราฟิก ภาพเคลื่อนไหว เสียง มาจัดรูปแบบ โดยอาศัยเทคโนโลยีความเจริญก้าวหน้าทางด้านคอมพิวเตอร์ และการสื่อสารมาประยุกต์ใช้ ทำให้ลดค่าใช้จ่ายและระยะเวลา

ประเภทของสื่อดิจิทัล

๑) ภาพดิจิทัล

๒) เสียงดิจิทัล

๓) วิดีโอดิจิทัล

๔) ทีวีดิจิทัล

๕) อินเทอร์เน็ตดิจิทัล

แบนด์วิดท์ (Bandwidth) หมายถึง อัตราการส่งข้อมูลผ่านตัวกลางไปยังอีกสถานที่หนึ่ง ซึ่งตัวกลางนั้นจะเป็นสายทองแดงหรือสายใยแก้วนำแสง ก็จะมีผลให้อัตราการส่งข้อมูลไปยังสถานที่หนึ่งที่แตกต่างกัน ซึ่งแบนด์วิดท์นั้น จะมีหน่วยเป็นบิตต่อวินาที bps (bit per second) กิโลบิตต่อวินาที (Kbps) และ เมกะบิตต่อวินาที (Mbps)

ประเภทของการเข้าถึงอินเทอร์เน็ต

การเชื่อมต่ออินเทอร์เน็ตแบบใช้สาย (Wire Internet) ได้แก่

๑) Modem Dial

๒) Lease Line

๓) ADSL

๔) LAN

๕) Fiber Optic

การเชื่อมต่ออินเทอร์เน็ตแบบไร้สาย (Wireless Internet) ได้แก่

๑) Wi-Fi

๒) Mobile Phone

ลักษณะพิเศษของ Big Data

๑) Volume คือข้อมูลมหาศาลขนาดใหญ่ มีจำนวนมากเกินกว่าระบบฐาน ข้อมูลแบบเดิม ๆ สามารถที่จะจัดการได้

๒) Velocity ข้อมูลที่ต้องวิเคราะห์เข้าสู่ระบบฐานข้อมูลอย่างรวดเร็ว โดยให้ความสำคัญกับข้อมูลที่เป็น Real-time

๓) Variety ข้อมูลที่มีความหลากหลายทั้งที่เป็นแบบโครงสร้างหรือรูปแบบที่ไม่แน่นอน

ลักษณะข้อเท็จจริง (Fact)

๑) มีความเป็นไปได้

๒) มีความสมจริง

๓) มีหลักฐานเชื่อถือได้

๔) มีความสมเหตุสมผล

ลักษณะข้อคิดเห็น (Opinion)

๑) เป็นข้อความที่แสดงความรู้สึก

๒) เป็นข้อความที่แสดงความคาดคะเน

๓) เป็นข้อความที่แสดงการเปรียบเทียบอุปมาอุปมัย

๔) เป็นข้อความที่เป็นข้อเสนอแนะหรือเป็นความคิดเห็นของผู้พูดเอง

การเล่น Social Network ให้ปลอดภัย

๑) คิดให้รอบคอบ

๒) ระมัดระวัง

๓) พิมพ์ URL โดยตรง

๔) รอบคอบ

๕) ตั้งค่า

๖) ไม่แสดงข้อมูล

๗) Do Not Track

๘) ใช้วิจารณญาณ

๙) ควบคุมการใช้งาน

๑๐) สังคมเสรี

ความปลอดภัยยุคดิจิทัล

ความเป็นส่วนตัว

๑) รอยเท้าดิจิทัล (Digital Footprint) คือ ข้อเขียน รูปภาพ สิ่งต่างๆ ที่เราเขียนหรือลงไว้ใน Social Media ทั้งหลาย ไม่ว่าจะเป็น Facebook, Twitter, Instagram, Social Cam หรือช่องทางไหนก็ตาม

ข้อมูลพื้นฐานของ Digital Footprint

๑) ภาพหรือข้อมูลส่วนตัว เช่น หมายเลขโทรศัพท์ ที่อยู่ หมายเลขบัตรประชาชน

๒) การดำเนินชีวิต และการเป็นอยู่ของเรา

๓) ภาพกับเพื่อน กลุ่มต่างๆ

๔) ความสัมพันธ์กับคนต่างๆ ยกตัวอย่าง เช่น เพื่อนใน Facebook (เพื่อนร่วมงาน เจ้านาย)

ความมั่นคงปลอดภัย

๑) การพิสูจน์ตัวตน

๒) การกำหนดสิทธิ์

๓) การเข้ารหัสข้อมูล

๔) มัลแวร์

๕) การหลอกลวง

๖) ภัยจากสาธารณะ

อันตรายของการทิ้ง Digital Footprint

๑) ทดสอบค้นหาชื่อตัวเอง

๒) ข้อมูลมีโอกาสโดนทำสำเนา

๓) อยู่ในมือผู้ไม่หวังดี

๔) เสียภาพพจน์ และภาพลักษณ์ โดยไม่อาจแก้ไขได้

รหัสผ่านที่ไม่ควรตั้ง

๑) ใช้รหัสเดียวกันหมด รู้รหัสเดียวสามารถเข้าถึงได้หมด

๒) ไม่มีการเปลี่ยนรหัสผ่าน

๓) คาดเดาง่าย เช่น ๑๒๓๔๕๖๗

๔) ประกอบด้วยข้อมูลบุคคล เช่น วันเกิด เบอร์โทร ๕) ใช้คำมีความหมาย เช่น ชื่อเล่น love happy

๖) ใช้ตัวพิมพ์ทั้งหมด ไม่มีตัวเลขหรือตัวอักษรผสม

รหัสผ่านที่ดี

๑) ใช้รหัสผ่านที่ยาว (อย่างน้อย ๘ ตัว)

๒) ใช้ตัวอักษรตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก ตัวเลข รวมทั้งสัญลักษณ์ต่างๆ ประกอบกัน

๓) ใช้สัญลักษณ์อย่างน้อยหนึ่งตัวในตำแหน่งที่ ๒-๖

๔) ใช้ตัวอักษรที่แตกต่างกันอย่างน้อย ๔ ตัว (อย่าใช้ตัวอักษรซ้ำกัน) ใช้ตัวเลขและตัวอักษรแบบสุ่ม

การพิสูจน์ตัวตนโดยใช้ ๒ ปัจจัย (Two-Factor Authentication) คือการใช้ปัจจัยที่สอง ร่วมกับการล็อกอินด้วยรหัสผ่านตามปกติ ซึ่งหลังจากการล็อกอินด้วยรหัสผ่านแล้วระบบจะถามรหัสยืนยันจากอุปกรณ์อื่น เช่น โทรศัพท์มือถือ หรือ Token เพื่อความปลอดภัยมากขึ้น อาทิ Google ๒ Factor Authentication เป็นต้น

การกำหนดสิทธิ์ (Authorization) หลักการสิทธิน้อยที่สุด Principle of Least Privilege สามารถใช้ปรับปรุงความปลอดภัยของระบบคอมพิวเตอร์ นี่เป็นเรื่องพื้นฐานแต่สำคัญมากที่มักถูกมองข้าม หลักการนี้คือ ผู้ใช้จะต้องมีระดับต่ำที่สุดของสิทธิตามความต้องการเพื่อกระทำงานตามที่มอบหมาย

การเข้ารหัสข้อมูล HTTPS ย่อมาจาก Hypertext Transfer Protocol Secure หรือ Hypertext Transfer Protocol Over SSL(Secure Socket Layer) เป็นการทำงานเหมือนกับ HTTP ธรรมดาแต่ทำอยู่บน SSL เพื่อให้เกิดความปลอดภัยในการส่งข้อมูลมากยิ่งขึ้น มีรูปแบบดังนี้

- การใช้งาน URL จะขึ้นต้นด้วย https:// ตามด้วยชื่อของเว็ปไซต์
- ทำงานที่พอร์ต(port) ๔๔๓ (มาตรฐาน)

- ส่งข้อมูลเป็นแบบ Cipher text คือ มีการเข้ารหัสข้อมูลในระหว่างการส่ง (Encryption) สามารถถูกดักจับได้ แต่อ่านข้อมูลนั้นไม่รู้เรื่อง

- มีการทำ Authentication เพื่อตรวจสอบยืนยันระบุตัวตน

การเข้ารหัสข้อมูล WPA๒ คือ เทคโนโลยีการรักษาความปลอดภัยที่ปกป้องเครือข่าย Wi-Fi ของคุณ โดยการเข้ารหัสการจราจรบนเครือข่าย นอกจากนี้ยังทำให้ผู้ใช้ที่ไม่ได้รับอนุญาตเข้าถึงเครือข่ายได้ยากขึ้น

มัลแวร์ (malware-malicious software) คือ โปรแกรมที่ถูกสร้างขึ้นมาเพื่อประสงค์ร้ายต่อเครื่องคอมพิวเตอร์และเพื่อมาล้วงข้อมูลสำคัญไปจากผู้ใช้งานคอมพิวเตอร์

WannaCry ไวรัสเรียกค่าไถ่ที่ระบาดไปทั่วโลก โดยวันแรกที่ระบาด มีเครื่องคอมพิวเตอร์ติดถึง ๒๓๐,๐๐๐ กว่าเครื่องใน ๑๕๐ ประเทศ

การหลอกลวง (Scam) เล่ห์อุบาย แผนการร้าย คำนี้หากอยู่ในวงการออนไลน์ จะใช้เรียกพฤติกรรมที่มีเจตนาหลอกลวง ให้เสียทรัพย์ ให้เสียข้อมูล ตัวอย่าง การหลอกลวงทางอินเทอร์เน็ต เช่น Email Scam Phishing Scam เป็นต้น

การโจมตีแบบวิศวกรรมสังคม (Social Engineering) Phishing คือคำที่ใช้เรียกเทคนิคการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่นๆ เพื่อนำเข้าข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่นๆ เช่น ด้านการเงิน เป็นต้น

การหลอกลวงออนไลน์ (Fraud) มิจฉาชีพติดต่อเหยื่อ สร้างความน่าเชื่อถือ หว่านล้อมให้โอนเงินไม่ส่งสินค้าหรือส่งสินค้าปลอม ปิดช่องทางการสื่อสาร เปลี่ยนชื่อ เริ่มวงจรใหม่

Mobile Security and Privacy

๑) ติดตั้งโปรแกรมป้องกันไวรัสบนมือถือ

๒) ติดตั้งเฉพาะโปรแกรมที่น่าเชื่อถือ

๓) ปิดการใช้งาน WIFI และ Bluetooth เมื่อไม่ได้ใช้งาน

๔) ปรับปรุงระบบปฏิบัติการให้ทันสมัยอยู่เสมอ

๕) สำรองข้อมูลที่สำคัญ ๖) ตั้งค่าให้มือถือลบข้อมูลอัตโนมัติเมื่อสูญหาย

พฤติกรรมเสี่ยงเมื่อใช้อุปกรณ์ในที่สาธารณะ

๑) เชื่อมกับไวไฟที่ไม่ได้เข้ารหัส

๒) ไม่ระวังว่ามีผู้อื่นแอบฟังบทสนทนาอยู่

๓) ไม่ระวังผู้อื่นแอบดูหน้าจอ

๔) ไม่ระวังรอบตัว

ประโยชน์ที่คาดว่าจะได้รับ

ผู้เรียนมีความรู้ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Understanding and Using Digital Technology) ได้อย่างครบถ้วน ถูกต้อง เหมาะสม และสามารถนำความรู้ที่ได้รับไปปรับใช้และถ่ายทอดได้อย่างมีประสิทธิภาพและเกิดประสิทธิผลในการปฏิบัติงานที่เกี่ยวข้องต่อไป