แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๔
รอบการประเมินที่ ๒ / ๒๕๖๘ ตั้งแต่วันที่ ๑ เมษายน ๒๕๖๘ – ๓๐ กันยายน ๒๕๖๘
ประจำปีงบประมาณ พ.ศ. ๒๕๖๘

ชื่อ-สกุล นางสาวธัญญาภรณ์ สายกระสุน ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ
กลุ่ม/ฝ่าย/สพด. สถานีพัฒนาที่ดินศรีสะเกษ
หัวข้อการพัฒนา หลักสูตร ความมั่นคงปลอดภัยบนอินเตอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล
สถานที่ การฝึกอบรมการเรียนรู้ผ่านสื่อออนไลน์ ระบบ E-Learning ก.พ.
วิทยากร/ผู้ให้ความรู้ อาจารย์ณัฐ พยงค์ศรี ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงดิจิทัลฯ
หน่วยงานที่จัดอบรม สำนักงานคณะกรรมการข้าราชการพลเรือน (สำนักงาน ก.พ.)

วัตถุประสงค์

๑. เพื่อให้สามารถอธิบายสถานการณ์การใช้งานอินเตอร์เน็ตและการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นในยุคดิจิทัล
๒. เพื่อให้สามารถยกตัวอย่างการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวัง เพื่อให้ปลอดภัยจากภัยคุกคาม
๓. เพื่อให้สามารถปฏิบัติตามขั้นตอนการป้องกันตรวจสอบความปลอดภัยด้วยตนเอง

หัวข้อในบทเรียน

แนวโน้มการใช้งานอินเตอร์เน็ตในประเทศไทย สถิติการใช้งานของประเทศไทย ความสัมพันธ์และการกระจายตัวของข้อมูล วิวัฒนาการของเว็บไซต์ รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์ สิ่งที่ต้องพึงระวังในการใช้งานบนอินเทอร์เน็ต พรบ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด การตั้งค่าความปลอดภัยสำหรับ Facebook Gmail LINE รายละเอียดมีดังนี้

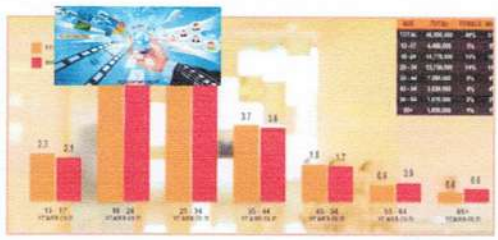
๑. ความหมายความมั่นคงปลอดภัยบนอินเตอร์เน็ต

ความมั่นคงปลอดภัยบนอินเตอร์เน็ต คือ การนำเครื่องมือทางเทคโนโลยีและกระบวนการที่รวมถึงการปฏิบัติที่ถูกต้องในการป้องกันและรับมือการโจมตีเข้ามาที่อุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการถูกเข้าถึงจากบุคคลที่สามที่ไม่ได้รับอนุญาต

๒. การใช้งานอินเตอร์เน็ตของประเทศไทย

๒.๑ แนวโน้มการใช้งานอินเตอร์เน็ตในประเทศไทย ในช่วงปี ๒๐๐๐-๒๐๑๐ ได้เติบโตอย่างรวดเร็วและขยายตัวแบบก้าวกระโดด ปี ๒๐๑๐ จำนวนผู้ใช้งานอินเตอร์เน็ตเพิ่มขึ้นมากกว่า ๙ เท่า และมีผู้สามารถเข้าถึงอินเตอร์เน็ตมากขึ้น เกือบ ๕๐ เปอร์เซ็นต์ของประชากรโลก ทำให้อินเตอร์เน็ตเริ่มมีบทบาทสำคัญในชีวิตประจำวันและเป็นปัจจัยที่ ๕ ในการดำเนินชีวิตของผู้คน เช่น การสื่อสารผ่าน Application LINE, Facebook และอื่น ๆ สามารถช่วยอำนวยความสะดวกในด้านการสื่อสาร การติดต่อธุรกิจ การศึกษา และทางสังคมออนไลน์

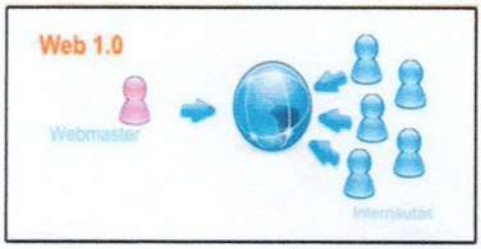
๒.๒ สถิติการใช้งานของประเทศไทย กลุ่มอายุ ๒๐-๓๐ ปี มีอัตราการใช้งานอินเตอร์เน็ตสูง ประมาณ ๖๐-๗๐ เปอร์เซ็นต์ นอกจากนี้ กลุ่มผู้สูงอายุหรือผู้ที่เริ่มใช้งานอินเตอร์เน็ตในวัยเกษียณ ซึ่งอัตราการใช้ Social Media เพิ่มมากขึ้น จึงมีความเสี่ยงต่อการพบเจอกับภัยคุกคามทางอินเตอร์เน็ตได้ทุกที่ทุกเวลา



๓. รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์

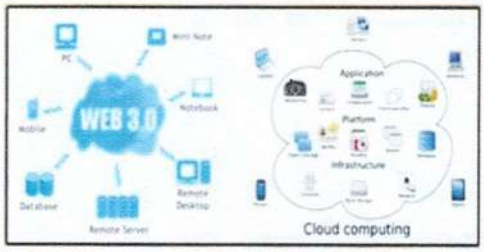
๓.๑ ความเป็นมาของอินเตอร์เน็ต

Internet การสื่อสารแบบดิจิทัลและเว็บไซต์เข้ามามีบทบาทกับการใช้ชีวิตอย่างมาก มี ๔ ยุค ดังนี้



๑) ยุค Web 1.0 เป็นยุคเริ่มต้น ที่การให้บริการเว็บไซต์ในรูปแบบการสื่อสารทางเดียว(One Way Communication) คือ เว็บไซต์ที่สร้างขึ้นมาเพื่อให้ผู้พัฒนาหรือผู้สร้างติดต่อสื่อสารกับบุคคลอื่นอย่างเดียว ผู้ที่เข้าถึงเว็บไซต์สามารถเข้าชม รับทราบเนื้อหาอย่างเดียวเท่านั้น ไม่มีการตอบโต้กับผู้ที่เข้าร่วมชมข้อมูลบนเว็บไซต์

๒) ยุค Web 2.0 เป็นยุคที่เว็บไซต์มีการพัฒนาเป็นการใช้งานผ่านเครือข่ายอินเตอร์เน็ตในรูปแบบสองทาง (Two Way Communication) คือ เว็บไซต์ที่เปิดโอกาสให้กับผู้ใช้งานสามารถโต้ตอบ สนทนากับบุคคลอื่นได้ เช่น เว็บบอร์ด เว็บแพลตฟอร์ม (Facebook, Youtube, Wikipedia)



๓) ยุค Web 3.0 เป็นยุคที่แพลตฟอร์มเริ่มมีข้อมูลจำนวนมากมาย สามารถนำข้อมูลจำนวนมาวิเคราะห์และแนะนำให้กับผู้ใช้งานเว็บไซต์ได้ มีความสามารถในการอ่าน เขียน ตอบโต้ข้อมูลได้ในรูปแบบที่มีความอัจฉริยะมากขึ้น ด้วยการเชื่อมโยงข้อมูลแบบ Decentralized หรือไร้ศูนย์กลาง เช่น Application ที่มีการใช้งานแบบ Blockchain

๔) ยุค Web 4.0 เป็นยุคที่เทคโนโลยีเชื่อมโยงโลกออนไลน์เข้ากับโลกความจริงผ่านระบบอัจฉริยะ เช่น Artificial Intelligence (AI) และ Internet of Things (IoT) ทำให้เว็บไซต์สามารถเข้าใจและตอบสนองต่อความต้องการของผู้ใช้ได้อย่างอัตโนมัติ

๓.๒ ลักษณะการกระทำความผิดทางคอมพิวเตอร์

ประเภทของผู้กระทำความผิด สามารถแบ่งได้หลายประเภท ดังนี้

๑. Hacker คือ บุคคลที่มีความสนใจที่จะศึกษาค้นคว้าเกี่ยวกับระบบปฏิบัติการคอมพิวเตอร์การเจาะระบบต่าง ๆ เมื่อพบวิธีใด ๆ แล้วก็นำข้อมูลมาเผยแพร่ให้ผู้อื่นทราบ

๒. Cracker คือ บุคคลที่คล้ายกับ Hacker แต่จะนำวิธีที่ตนเองค้นพบมาแสวงหาประโยชน์ต่อตนเอง นำมาใช้โจมตีทำให้เกิดความเสียหายในระบบคอมพิวเตอร์

๓. Script Kiddy คือ บุคคลที่ได้รับทราบข้อมูลที่สามารถสร้างความเสียหายกับคอมพิวเตอร์แล้วก็นำข้อมูลนั้นมาทำตาม ทำให้เกิดความเสียหายกับเว็บไซต์หรือผู้ใช้บริการบนอินเตอร์เน็ต

๔. Spy คือ บุคคลที่นำข้อมูลแอบเข้ามาในระบบคอมพิวเตอร์เพื่อสืบข้อมูลต่าง ๆ มักโจมตีในลักษณะการโจรกรรมข้อมูล

๕. Employee คือ บุคคลที่นำข้อมูลลสำคัญขององค์กรไปเผยแพร่โดยไม่เจตนา ทำให้ผู้ที่ได้ข้อมูลสามารถโจมตีระบบขององค์กรได้ เป็นปัจจัยหนึ่งที่ต้องระมัดระวัง

๖. Terrorist คือ บุคคลที่ประสงค์ไม่ดี ก่อความไม่สงบในระบบคอมพิวเตอร์ ซึ่งมีความชำนาญในการเจาะระบบ มักโจมตีระบบเพื่อหาประโยชน์ทางการเงินหรือทำลายข้อมูลเพื่อจุดประสงค์ที่เกี่ยวข้องกับการก่อการร้าย

๓.๓ รูปแบบการกระทำความผิดทางคอมพิวเตอร์

๑. Social Engineering เป็นปฏิบัติการทางจิตวิทยา หลอกล่อให้เหยื่อติดกับโดยไม่ต้องอาศัยความชำนาญเกี่ยวกับคอมพิวเตอร์

๒. Password Guessing เป็นการเดา Password เพื่อเข้าสู่ระบบ

๓. Denial of Service (DOS) เป็นการโจมตีลักษณะหนึ่งที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบและการร้องขอในคราวละมาก ๆ เพื่อที่จะทำให้ระบบหยุดให้บริการ

๔. Decryption เป็นการถอดข้อมูลที่มีการเข้ารหัสอยู่

๕. Birthday Attacks เป็นการสุ่มคีย์ขึ้นมาและอาจจะตรงกับคีย์ที่เราเข้ารหัสไว้

๖. Man in the middle Attacks เป็นการพยายามที่จะทำตัวเป็นคนกลางเพื่อดักเปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว

๔. สิ่งที่ต้องพึงระวังในการใช้งานบนอินเตอร์เน็ต

การใช้งานอินเตอร์เน็ตมีความสะดวกและเป็นประโยชน์หลาย ๆ ด้าน แต่มีความเสี่ยงในการเผชิญกับการโจมตีหรือภัยคุกคามจากการกระทำความผิดทางคอมพิวเตอร์ ดังนี้

๑. การโจมตีผ่านเครือข่ายอินเตอร์เน็ต การโจมตีระบบที่สำคัญ เช่น ระบบการคมนาคม ระบบการเงินหรือสาธารณูปโภคพื้นฐาน เช่น ไฟฟ้าและประปาถูกทำลายหรือหยุดทำงานโดยการโจมตี เช่น DDoS (Distributed Denial of Service) ทำให้ไม่สามารถใช้งานระบบได้ตามปกติ ส่งผลกระทบต่อการดำเนินชีวิตประจำวัน

๒. การเจาะรหัสผ่านหรือระบบผ่านช่องโหว่ ช่องโหว่ของระบบปฏิบัติการหรือเครือข่ายที่ยังไม่ได้รับการอัพเดทหรือแพตช์สามารถถูกโจมตีและทำให้ข้อมูลถูกขโมยหรือระบบล้มเหลว

๓. การโจมตีด้วย Malware and Virus Treat เช่น ไฟล์/ภาพที่ส่งผ่านสื่อสังคมออนไลน์

๔. การโจมตีรูปแบบ Zombie Attack การใช้คอมพิวเตอร์ที่ถูกควบคุมจากผู้โจมตีเพื่อส่งคำขอหรือคำสั่งไปยังระบบอื่น ๆ โดยที่เจ้าของคอมพิวเตอร์ไม่รู้ตัว

๕. กลลวงทางสังคม Social Engineering การหลอกลวงที่เกิดจากการปลอมตัว เช่น การปลอมตัวเป็นผู้หญิงหรือบุคคลที่มีความน่าเชื่อถือ เพื่อให้เหยื่อหลงเชื่อและเปิดเผยข้อมูลสำคัญ

๖. Phishing การสร้างเว็บไซต์ปลอมที่มีลักษณะเหมือนเว็บไซต์จริง เพื่อหลอกลวงผู้ใช้ให้กรอกข้อมูลส่วนตัว เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลบัตรเครดิต

๗. การละเมิดข้อมูลส่วนบุคคล การเปิดเผยข้อมูลส่วนตัว เช่น การแชร์สถานที่ผ่านโซเชียลมีเดีย อาจทำให้โจรทราบและเข้ามาก่อเหตุได้หรือใช้บริการต่างๆ ที่อาจเก็บข้อมูลเกี่ยวกับการเดินทาง

๕. พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐) ได้ถูกบังคับใช้เพื่อป้องกันและควบคุมการกระทำผิดที่เกี่ยวข้องกับการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศ โดยในมาตราที่ ๓ จะมีการกำหนดคำศัพท์ที่เกี่ยวข้องดังนี้

- ระบบคอมพิวเตอร์ หมายถึง ระบบที่มีการจัดเก็บข้อมูล การประมวลผล หรือการเชื่อมต่อเครือข่ายข้อมูล
- ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูลที่ถูกจัดเก็บในรูปแบบดิจิทัล และสามารถส่งผ่านเครือข่ายคอมพิวเตอร์
- ข้อมูลจราจรทางคอมพิวเตอร์ หมายถึง ข้อมูลที่เกี่ยวข้องกับการส่งและรับข้อมูลในระบบคอมพิวเตอร์ เช่น ข้อมูลการเชื่อมต่อระหว่างผู้ใช้และเว็บไซต์ หรือข้อมูลที่เกี่ยวข้องกับการใช้บริการอินเทอร์เน็ต
- ผู้ให้บริการ หมายถึง บุคคลหรือองค์กรที่ให้บริการการเข้าถึงระบบคอมพิวเตอร์หรือการเชื่อมต่ออินเทอร์เน็ต
- ผู้ใช้บริการ หมายถึง บุคคลที่ใช้บริการคอมพิวเตอร์หรือบริการอินเทอร์เน็ตต่างๆ ในการสื่อสารหรือเข้าถึงข้อมูล

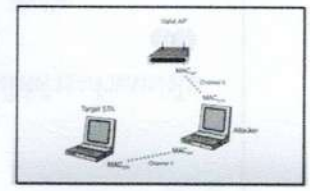
พระราชบัญญัตินี้มีจุดประสงค์เพื่อคุ้มครองการใช้งานอินเทอร์เน็ตในประเทศไทย และการป้องกันการกระทำความผิดที่เกิดจากการใช้เทคโนโลยีที่อาจสร้างความเสียหายต่อระบบและผู้ใช้ โดยมีการกำหนดบทลงโทษที่เหมาะสมเพื่อยับยั้งการกระทำความผิดที่เกี่ยวข้องกับการใช้คอมพิวเตอร์ มีดังนี้

ข้อห้าม ☒	โทษ ☒
มาตรา ๕ การกระทำความผิดเกี่ยวกับการเข้าถึงข้อมูลโดยมิชอบ	
➢ ห้ามมิให้ผู้ใดเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือเจาะระบบโดยมิชอบ ซึ่งจะมีการลงโทษทั้งทางอาญาและทางแพ่ง	➢ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตอาจทำให้ถูกลงโทษจำคุกและ/หรือปรับ หากเป็นการเข้าถึงข้อมูลเพื่อก่อความเสียหายหรือเผยแพร่ข้อมูลที่ผิดกฎหมาย จะมีโทษที่รุนแรงขึ้น
มาตรา ๖ การกระทำความผิดเกี่ยวกับการทำลายหรือเปลี่ยนแปลงข้อมูล	
➢ ห้ามมิให้มีการทำลาย แก้ไข ลบหรือทำให้ข้อมูล คอมพิวเตอร์เสียหายโดยมิชอบ	➢ หากการกระทำดังกล่าวทำให้เกิดความเสียหายแก่ผู้อื่นหรือระบบคอมพิวเตอร์ จะมีโทษจำคุกและ/หรือปรับ ถ้าผู้กระทำมีเจตนากระทำการดังกล่าวเพื่อการขโมยข้อมูลหรือเผยแพร่ข้อมูลที่เป็นอันตรายจะถูกลงโทษหนักขึ้น
มาตรา ๗ การกระทำความผิดเกี่ยวกับการคุกคามและการแอบอ้าง	
➢ ห้ามมิให้มีการคุกคามหรือแอบอ้างเป็นบุคคลอื่นโดยใช้ข้อมูลหรือคอมพิวเตอร์ในการหลอกลวงหรือก่อให้เกิดความเสียหาย เช่น การใช้ข้อมูลส่วนบุคคลของผู้อื่นเพื่อแอบอ้างหรือหลอกลวง	➢ ผู้กระทำความผิดในลักษณะนี้จะถูกลงโทษตามความร้ายแรงของการกระทำ ทั้งจำคุกและ/หรือปรับ
มาตรา ๘-๒๖ การกระทำความผิดในด้านการกระจายข้อมูลที่ผิดกฎหมาย	
➢ ห้ามมิให้ผู้ใดกระจายข้อมูลที่ผิดกฎหมายผ่านระบบคอมพิวเตอร์ โดยเฉพาะข้อมูลที่มีเนื้อหาหมิ่นประมาท ข่มขู่ คุกคาม หรือข้อมูลที่เป็นอันตราย	➢ ผู้กระทำความผิดในกรณีดังกล่าวจะถูกลงโทษทั้งจำคุกและ/หรือปรับ โดยความร้ายแรงของโทษจะขึ้นอยู่กับผลกระทบที่เกิดขึ้นจากการกระทำ

๖. ตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์

๖.๑ การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด บางกรณีอาจไม่ผิดกฎหมายตาม พ.ร.บ. คอมพิวเตอร์ แต่เป็นพฤติกรรมที่ไม่เหมาะสมต่อสังคมในแง่ของคุณธรรมและจริยธรรม เช่น การใช้โปรแกรมโกงในการเล่นเกมส์ เป็นการใช้ซอฟต์แวร์ที่ช่วยโกงในการเล่นเกมส์เพื่อให้ได้ผลลัพธ์ที่ไม่สมจริง ซึ่งแม้ไม่ผิดกฎหมายโดยตรง แต่เป็นการละเมิดกฎของผู้พัฒนาเกม และส่งผลเสียต่อประสบการณ์ของผู้เล่นคนอื่นๆ การเสพสารเสพติดผ่านโซเชียลมีเดีย เป็นแพลตฟอร์มที่สามารถเผยแพร่ข้อมูลที่ไม่เหมาะสมได้ เช่น การแสดงภาพหรือการเชิญชวนใช้สารเสพติด ซึ่งอาจทำให้เกิดการเลียนแบบจากผู้ใช้คนอื่น การแชร์ข้อมูลโดยขาดความยั้งคิด ผู้ใช้งานมักแชร์ข้อมูลหรือโพสต์ต่างๆ โดยไม่พิจารณาผลกระทบต่อผู้อื่น หรือไม่สนใจว่าเป็นข้อมูลเท็จหรือไม่ เหตุการณ์นี้อาจส่งผลให้เกิดความเข้าใจผิด หรือสร้างปัญหาตามมา การทำร้ายร่างกายผ่านโซเชียล การใช้โซเชียลมีเดียเพื่อแสดงหรือเผยแพร่ความรุนแรง อาจส่งผลให้เกิดความรุนแรงในชีวิตจริง เช่น การข่มขู่หรือการกระทำรุนแรงต่อบุคคลอื่น

๖.๒ ตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์



➢การเข้าใช้งาน Free Wi-Fi ปลอม เพื่อดักจับข้อมูลส่วนบุคคล การตั้งค่า Wi-Fi ปลอมที่มีชื่อคล้ายกับเครือข่ายW-Fi ที่ผู้ใช้เชื่อว่าเป็นเครือข่ายฟรี เช่น WF-Fi ในสถานที่สาธารณะ เพื่อดักจับข้อมูลส่วนตัวของผู้ใช้ เช่น ข้อมูลบัญชีผู้ใช้งาน การล็อกอิน หรือข้อมูลบัตรเครดิต

➢Euro Grabber คือ มัลแวร์ที่สร้างขึ้นเพื่อดักจับข้อมูลการทำธุรกรรมทางการเงินบนอุปกรณ์เคลื่อนที่หรือคอมพิวเตอร์ ซึ่งโดยปกติจะทำผ่านแอปพลิเคชั่นปลอมที่เหมือนกับแอปพลิเคชั่นธนาคาร เพื่อขโมยข้อมูลการเข้าใช้งานและข้อมูลส่วนตัวของผู้ใช้

➢Web Defacement คือ การที่แฮกเกอร์เจาะเข้ามาในเว็บไซต์และทำการเปลี่ยนแปลงข้อมลบนหน้าเว็บโซต์ เช่น การเปลี่ยนเนื้อหาหรือการแสดงข้อความที่ไม่เหมาะสม เป็นการโชว์ความสามารถหรืออำนาจในการเข้าถึงระบบ

➢ไวรัสเรียกค่าไถ่ (Ransomware) เช่น CryptoLocker ซึ่งเป็นไวรัสที่เข้ารหัสข้อมูลของผู้ใช้แล้วเรียกค่าไถ่เพื่อให้ผู้ใช้สามารถเข้าถึงข้อมูลนั้นได้อีกครั้ง โดยไม่มีการรับประกันว่าจะได้ข้อมูลคืนหลังจากการจ่ายเงิน

➢Hot Hot ตัวอย่างของการหลอกลวงทางออนไลน์ เช่น

๑) บราวเซอร์ติดมัลแวร์ มัลแวร์ที่แอบสวมรอยเป็นเว็บไซต์ เช่น Facebook โดยหลอกให้ผู้ใช้ติดตั้งโปรแกรมที่เปลี่ยนสีของหน้าเว็บไซต์ แต่เบื้องหลังจะนำบัญชี Facebook ของผู้ใช้ไปโพสต์หรือคอมเม้นต์ในเว็บไซต์ต่างๆ เพื่อหลอกให้เพื่อนๆ ดาวน์โหลดมัลแวร์ต่อ

๒) การหลอกลวงผ่านแอปพลิเคชั่น Line การแฮกบัญชี Line ของผู้ใช้แล้วส่งข้อความหลอกลวงไปยังสมาชิกในรายชื่อ เพื่อขอให้ซื้อสินค้าหรือบริการที่ไม่มีอยู่จริง

๗. การตั้งค่าความปลอดภัยสำหรับ Facebook Gmail LINE

๗.๑ ข้อคิดเตือนใจในการใช้งานอินเทอร์เน็ต

- อย่าติดตั้งโปรแกรมโดยไม่อ่านรายละเอียด อ่านคำแนะนำและเงื่อนไขก่อนการติดตั้งทุกครั้ง
- ระมัดระวังหากเข้าใช้อินเทอร์เน็ตฟรี อาจเสี่ยงต่อการถูกตักจับข้อมูล
- อย่าติดตั้งแอนตี้ไวรัสปลอม เลือกใช้โปรแกรมจากแหล่งที่เชื่อได้
- ห้ามคลิกลิงก์แปลก ๆ หรือเปิดไฟล์แบโดยไม่ตรวจสอบ มีความเสี่ยงที่ลิงก์เหล่านั้นจะนำไปสู่มัลแวร์
- อย่ากดจดจำรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ โดยเฉพาะเครื่องสาธารณะ อาจเสี่ยงต่อการถูกขโมยข้อมูล
- ปิดใช้งานฟังก์ชัน autorun ใน removable drive เพื่อป้องกันการติดเชื้อจากไวรัส
- Login เป็น administrator ใช้สิทธิ์นี้ในกรณีที่จำเป็น เพื่อป้องกันความเสี่ยงจากการเข้าถึงข้อมูลที่สำคัญ
- Update windows และ antivirus เป็นประจำ เพื่อรักษาความปลอดภัยในระบบ

๗.๒ วิธีป้องกันความปลอดภัยและตรวจสอบความปลอดภัยด้วยตนเอง

การปฏิบัติตามข้อแนะนำดังตารางนี้จะช่วยเพิ่มความปลอดภัยในการใช้งานออนไลน์และป้องกันการละเมิดความเป็นส่วนตัวจากการแฮกข้อมูลหรือการโจมตีทางไซเบอร์ต่างๆ ได้อย่างมีประสิทธิภาพ

การป้องกันความปลอดภัย		
Facebook	Gmail	Line
➢ ตั้งรหัสผ่านให้เป็นมาตรฐาน ใช้รหัสที่ไม่สามารถเดาได้ง่าย เช่น การใช้ตัวเลขและอักษรผสมกัน ➢ใช้ ๒-factor authentication เพิ่มความปลอดภัยในการเข้าใช้งาน Facebook ด้วยการยืนยันตัวตนจากอุปกรณ์อื่น ➢ ตั้งค่า login alert รับการแจ้งเตือนหากผู้อื่นพยายามเข้าใช้งานบัญชีของเรา logout หลังการใช้งาน โดยเฉพาะหากใช้งานผ่านเครื่องคอมพิวเตอร์สาธารณะ	➢การแสกนไวรัส ตรวจสอบคอมพิวเตอร์ด้วยโปรแกรมแอนตี้ไวรัสเป็นประจำ ➢ตรวจสอบ security checkup ของ account ทำการตรวจสอบการตั้งค่าความปลอดภัยในบัญชี ➢ตรวจสอบ privacy checkup ของ account ควบคุมข้อมูลส่วนบุคคลและการแชร์ข้อมูล ➢การตั้งค่าการกู้คืนบัญชี ในกรณีที่ลืมรหัสผ่านหรือบัญชีถูกแฮก ➢ ลงทะเบียนการเข้าใช้งานแบบ ๒ ขั้นตอน เพิ่มความปลอดภัยในการเข้าสู่ระบบ Gmail ➢ไม่ควรใช้รหัสผ่านเดียวกันกับเว็บไซต์อื่น ควรตั้งรหัสผ่านที่แตกต่างกันเพื่อความปลอดภัย ➢logout หลังการใช้งาน และทำการเคลียร์ browsing data เสมอ	➢ ปิด Line ID สำหรับการค้นหา ป้องกันไม่ให้คนที่ไม่รู้จักสามารถค้นหาคุณได้ ➢ ตั้งค่าการแชทจากคนที่ไม่ใช่เพื่อน จำกัดการรับข้อความจากบุคคลที่ไม่ใช่เพื่อนใน Line ➢การบล็อกคนที่ไม่ต้องการจะคุยด้วย ป้องกันไม่ให้บุคคลเหล่านั้นส่งข้อความหาคุณ ➢ตั้งค่าการเพิ่มเพื่อนจากหมายเลขโทรศัพท์ ควบคุมว่าผู้ใดสามารถเพิ่มเราเป็นเพื่อนได้ ➢ ตั้งค่าความเป็นส่วนตัวในการโพสต์ใน Timeline: ควบคุมว่าใครสามารถเห็นโพสต์ของเรา

การนำความรู้จากบทเรียนไปใช้ประโยชน์

จากการพัฒนาความรู้ผ่านระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ LDD e-Training หลักสูตร “ความมั่นคงปลอดภัยบนอินเตอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล” ได้เสริมสร้างความรู้ ความเข้าใจเกี่ยวกับภัยคุกคามทางอินเตอร์เน็ต และมีความรู้ในการรับมือ วิธีป้องกันภัยคุกคามทางอินเตอร์เน็ตได้อย่างถูกต้อง สามารถนำไปประยุกต์ใช้การปฏิบัติในปัจจุบัน เนื่องจากการทำงานต้องอาศัยเทคโนโลยีดิจิทัลใช้อินเตอร์เน็ตในการสืบค้นข้อมูล จึงต้องระมัดระวังในการใช้อินเตอร์เน็ตให้เกิดความมั่นคงปลอดภัยต่อตนเองและหน่วยงาน และสามารถนำความรู้ที่ได้จากการศึกษาหลักสูตรดังกล่าวไปให้คำแนะนำแก่ผู้รับบริการได้เบื้องต้น

ธัญญาภรณ์ สายกระสุน

(นางสาวธัญญาภรณ์ สายกระสุน)
นักวิชาการเกษตรปฏิบัติการ
ผู้สรุปรายงานพัฒนาความรู้
วันที่ ๒๖ กรกฎาคม ๒๕๖๘

(นายสาคร เหมือนตา)
ผู้อำนวยการสถานีพัฒนาที่ดินศรีสะเกษ
ผู้ตรวจรายงานพัฒนาความรู้
วันที่ กรกฎาคม ๒๕๖๘

กรมพัฒนาที่ดิน

ขอมอบประกาศนียบัตรฉบับนี้ไว้เพื่อแสดงว่า

นางสาวธัญญาภรณ์ สายกระสุน

ได้ผ่านการฝึกอบรมการเรียนรู้ผ่านสื่อออนไลน์ ระบบ LDD e-Training

หลักสูตร "แนวทางปฏิบัติด้านการจัดซื้อจัดจ้าง "

รุ่นที่ 2/2568 : เมษายน 2568 - กันยายน 2568

(ดร.ทวีศักดิ์ ธนเดโชพล)

อธิบดีกรมพัฒนาที่ดิน

สำนักงาน ก.พ.
Office of the Civil Service Commission

สำนักงานคณะกรรมการข้าราชการพลเรือน

ขอมอบประกาศนียบัตรฉบับนี้ให้เพื่อแสดงว่า

นางสาวธัญญาภรณ์ สายกระสุน

ได้ผ่านการพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์

วิชา ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตน สำหรับข้าราชการยุคดิจิทัล

(รวมระยะเวลาทั้งสิ้น 4 ชั่วโมง)

ให้ไว้ ณ วันที่ 17 พฤษภาคม พ.ศ. 2568

(นายปิยวัฒน์ ศิวรักษ์)
เลขาธิการคณะกรรมการข้าราชการพลเรือน