แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๒
รอบการประเมินที่ ๒/๒๕๖๗ ตั้งแต่วันที่ ๑ เมษายน – ๓๐ กันยายน ๒๕๖๗
ประจำปีงบประมาณ พ.ศ.๒๕๖๗

ชื่อ-นามสกุล นางสาวชลธิชา เมฆโสภณ **ตำแหน่ง** เจ้าพนักงานธุรการปฏิบัติงาน
หน่วยงาน สถานีพัฒนาที่ดินฉะเชิงเทรา
หัวข้อการพัฒนา ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล
วิธีการพัฒนา OCSC Learning Portal ศูนย์การเรียนรู้ทางสื่ออิเล็กทรอนิกส์แบบบูรณาการ
วันที่พัฒนา ๑๙ สิงหาคม ๒๕๖๗ **สถานที่** ออนไลน์
หน่วยงานที่จัดอบรม สำนักงานคณะกรรมการข้าราชการพลเรือน
วัตถุประสงค์

๑. เพื่อให้สามารถอธิบายสถานการณ์การใช้งานอินเทอร์เน็ตและการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นในยุคดิจิทัล

๒. เพื่อให้สามารถยกตัวอย่างการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวังเพื่อให้ปลอดภัยจากภัยคุกคาม

๓. เพื่อให้สามารถยกตัวอย่างภัยคุกคามต่าง ๆ ได้

๔. เพื่อให้สามารถปฏิบัติตามขั้นตอนการป้องกันตรวจสอบความปลอดภัยด้วยตนเอง

สรุปสาระสำคัญ

การเติบโตของอินเทอร์เน็ตในประเทศไทย มีเปอร์เซ็นต์ค่อนข้างสูงจนกลายเป็นปัจจัยที่ ๕ ของชีวิตประจำวัน สถิติการใช้งานในสังคมไทยที่มีอายุระหว่าง ๒๐ – ๓๐ ปี เป็นกลุ่มเป้าหมายที่ใช้งานอินเทอร์เน็ตค่อนข้างสูง ซึ่งมีความสุ่มเสี่ยงในการเผชิญโลกของอาชญากรรมหรือภัยคุกคามต่าง ๆ บนเครือข่ายอินเทอร์เน็ตค่อนข้างสูง

วิวัฒนาการของเว็บไซต์

ยุค Web ๑.๐ การให้บริการเว็บไซต์ในรูปแบบสื่อสารทางเดียว (One way communication) เป็นยุคที่ผู้พัฒนาเว็บไซต์หรือผู้ดูแลระบบจะเป็นผู้สร้างเนื้อหาเว็บไซต์ แล้วให้ผู้ใช้งานเข้ามาดูเนื้อหาอย่างเดียว

ยุค Web ๒.๐ การใช้งานผ่านเครือข่ายอินเทอร์เน็ตในรูปแบบสื่อสารสองทาง (Two way communication) เป็นยุคที่ให้ผู้ใช้งานสามารถโต้ตอบหรือแสดงความคิดเห็นต่าง ๆ ได้ และในยุค Web ๒.๐ มีการพัฒนาที่เรียกว่า เว็บแพลตฟอร์ม ซึ่งเป็นรูปแบบที่เจ้าของเว็บไซต์ไม่นิยมสร้างเนื้อหา แต่จะเปิดโอกาสให้ผู้ใช้งานเข้ามาสร้างเนื้อหาและเผยแพร่ให้ผู้ใช้งานอื่น ๆ เข้ามารับชมเนื้อหาได้ ทำให้มีการอัพโหลดข้อมูลมหาศาล หรือ Big Data

ยุค Web ๓.๐ เป็นการนำเข้าข้อมูล Big Data มาวิเคราะห์ประมวลผลผ่านแพลตฟอร์มต่าง ๆ

ประเภทของผู้กระทำผิดทางคอมพิวเตอร์

Hacker คือ บุคคลที่มีความสนใจที่จะศึกษาค้นคว้าเกี่ยวกับระบบปฏิบัติการคอมพิวเตอร์ การเจาะระบบต่าง ๆ เมื่อพบวิธีใด ๆ แล้ว ก็จะนำข้อมูลมาเผยแพร่ให้ผู้อื่นทราบ

Cracker คือ บุคคลที่คล้ายกับ Hacker แต่จะนำวิธีที่ตนเองต้นพบมาแสวงหาประโยชน์ต่อตนเอง

Script Kiddy คือ บุคคลที่ได้รับทราบข้อมูลใด ๆ ที่สามารถสร้างความเสียหายกับระบบปฏิบัติการคอมพิวเตอร์แล้ว ก็จะนำข้อมูลนั้นมาทดลองทำตาม

Spy คือ บุคคลที่แอบเข้ามาในระบบปฏิบัติการคอมพิวเตอร์เพื่อสอบข้อมูลต่าง ๆ

Employee คือ บุคคลที่นำข้อมูลสำคัญขององค์กรไปเผยแพร่โดยไม่ได้เจตนาทำให้ผู้ได้รับข้อมูลสามารถโจมตีระบบขององค์กรตนเองได้

Terrorist คือ บุคคลที่มีความประสงค์ในการก่อความไม่สงบในระบบคอมพิวเตอร์

ประเภทของภัยคุกคามทางไซเบอร์

Malicious Software หรือที่รู้จักกันว่า มัลแวร์ (Malware) เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายคอมพิวเตอร์เครือข่าย

Dos Attack (denial-of-service attack) หรือ distributed denial-pf-service (DDoS) attack การโจมตีโดยปฏิเสธการให้บริการ เป็นความพยายามทำให้เครื่องหรือทรัพยากรเครือข่ายสำหรับผู้ใช้ที่เป็นเป้าหมายเข้าใช้บริการไม่ได้ เช่น การที่มีผู้ไม่ประสงค์ดีทำการโจมตีเว็บไซต์ของหน่วยงานราชการ โดยเสมือนมีผู้เข้าใช้งานเว็บไซต์นั้นจำนวนมาก จนทำให้ระบบไม่สามารถใช้งานหรือให้บริการได้

Plishing คือกลลวงที่แยบยลทางอินเทอร์เน็ตที่มาในรูปแบบของการปลอมแปลงอีเมล์ หรือข้อความที่สร้างขึ้นเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลส่วนตัว ข้อมูลทางด้านการเงิน โดยแอบอ้างว่ามาจากองค์กรต่าง ๆ โดยส่งข้อมูลมาเพื่อหลอกให้ผู้ใช้งานทำการอัพเดทข้อมูล ติดตั้งระบบ หรือยืนยันข้อมูลบัญชีผู้ใช้งาน หากไม่ตอบกลับอีเมล์ อาจทำให้ผลเสียตามมา เช่น การสร้างเว็บไซต์เลียนแบบธนาคารเพื่อหลอกให้ผู้ใช้งานกรอกรหัสผ่าน

แนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ตเพื่อการรักษาความมั่นคงปลอดภัย

๑. เพิ่มความระวังในการใช้อินเทอร์เน็ต เพื่อไม่ให้เกิดการติดซอฟต์แวร์ที่เป็นอันตราย (Malware)หลีกเลี่ยงการเข้าเว็บไซต์ผิดกฎหมายหรือที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นที่ไม่รู้จักกันมาก่อน ไม่ควรเปิดไฟล์แนบหรือโปรแกรมต่างๆ ผ่านทางสังคมออนไลน์ (Social Media)

๒. ในการใช้บริการอินเทอร์เน็ต ไม่ควรตั้งรหัสผ่านเหมือนกันทุกระบบ หรือตั้งรหัสที่ง่ายต่อการเดา เช่น วันเดือนปีเกิดตัวเลขที่เรียงกัน ตัวพยัญชนะเรียงกัน เป็นต้น เพราะหากโดนแฮกเกอร์เจาะระบบสำเร็จแล้วระบบอื่นๆ ก็อาจถูกเจาะระบบด้วย

๓. ควรติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

ข้อแนะนำในการรักษาความปลอดภัยบนโลกไซเบอร์ในการใช้งานอินเทอร์เน็ตและการปฏิบัติตน

๑. ไม่ตั้งรหัสผ่านที่ง่ายเกินไป รหัสผ่านเป็นกุญแจที่ใช้ในการเข้าถึงข้อมูลและเอกสารของเรา อาชญากรจะใช้วิธีการต่าง ๆ ในการเข้ารหัสให้ได้ เพื่อไม่ให้บุคคลเหล่านี้เข้าถึงข้อมูลได้ง่าย ควรตั้งรหัสที่ซับซ้อน

ประกอบไปด้วยตัวอักษร ตัวพิมพ์ใหญ่และเล็ก ตัวเลข และสัญลักษณ์พิเศษเพื่อให้ยากต่อการคาดเดา และรหัสผ่านควรมีตั้งแต่ ๘ ตัวขึ้นไป และไม่ควรทำการบันทึกรหัสผ่านไว้ในอุปกรณ์ดิจิทัลหรือคอมพิวเตอร์สำนักงาน

๒. ใส่ใจกับการตั้งค่าความเป็นส่วนตัว แอปพลิเคชัน ส่วนใหญ่จะมีตัวเลือกในการตั้งค่าความเป็นส่วนตัวให้แก่ผู้ใช้งานระบบ เพื่อที่จะสามารถตัดสินใจได้ว่าข้อมูลไหนที่สามารถแบ่งปันข้อมูลได้ ข้อมูลไหนควรปิดเป็นความลับ ทางที่ดีควรเลือกตั้งค่าความเป็นส่วนตัวให้มากที่สุด ระมัดระวังในการเปิดเผยชื่อ เบอร์โทรศัพท์ ช่องทางการติดต่อ อีเมล์และที่อยู่ส่วนตัว และปฏิเสธแอปที่พยายามจะเข้าถึงกล้องถ่ายรูปของเรา

๓. ใส่ใจรอยเท้าดิจิทัล เพราะสิ่งที่ใช้โพสในโลกออนไลน์แล้ว สิ่งนั้นจะคงอยู่ตลอดไป แม้ว่าโพสต้นทางจะถูกลบไปแล้ว แต่คนอื่น ๆ ก็สามารถตามร่องรอยของเราได้ เมื่อคิดที่จะทำการโพสหรือเปิดเผยข้อมูลสู่สาธารณะหรือเฉพาะกลุ่มเพื่อนก็ตาม ควรโพสต์เฉพาะเรื่องที่ดี ๆ หรือเป็นเรื่องในแง่บวก ไม่พาดพิงถึงบุคคลอื่น ไม่วิพากษ์วิจารณ์ผู้อื่น ไม่ทำผิดกฎหมายของพรบ.คอมพิวเตอร์ และระมัดระวังในการเปิดเผยข้อมูลส่วนตัวให้มากที่สุด

๔. การติดตั้งโปรแกรมรักษาความปลอดภัยให้กับอุปกรณ์ทุกตัว รวมถึงโทรศัพท์ด้วย เพื่อที่จะปกป้องอุปกรณ์จากภัยคุกคามในโลกไซเบอร์

๕. รองข้อมูลไว้เสมอ การสำรองข้อมูลเป็นเรื่องที่สำคัญ เพื่อป้องกันการถูกเรียกค่าไถ่จากข้อมูล

๖. ติดตั้งเครื่องมือติดตามอุปกรณ์หรือล็อคหน้าจอ ในกรณีที่ทำหายเพื่อป้องกันไม่ให้ผู้ที่เอาไปเข้าถึงข้อมูลได้

๗. ระมัดระวังในการใช้บลูทูธ ควรปิดโหมดบลูทูธไว้เสมอเมื่อไม่ได้ใช้งาน

๘. อัพเดทระบบปฏิบัติการอยู่เสมอ ทั้งระบบปฏิบัติการดิจิทัล โปรแกรมและแอปพลิเคชันที่ติดตั้งในเครื่องมือ

๙. ระมัดระวังในการใช้ Wi-Fi อุปกรณ์ Wi-Fi ที่ใช้ควรมีความปลอดภัยควรตั้งรหัสผ่านไว้ตลอดเวลา และไม่ใช้ Wi-Fi สาธารณะ เมื่อต้องเปิดเผยข้อมูลส่วนตัว หรือการทำธุรกรรมต่าง ๆ

๑๐. ลบข้อมูลหรือโปรแกรมที่ไม่ได้ใช้งานแล้ว หากว่ามีโปรแกรมหรือแอปที่ไม่ได้ใช้งานหลายเดือนและควรเอาออก หรือข้อมูลที่ไม่ได้ใช้แล้วควรเอาออก หรือแยกไว้ในฮาร์ดไดร์ฟต่างหาก หรือเก็บไว้ในลักษณะออฟไลน์

๑๑. ระมัดระวังการหลอกให้กรอกข้อมูล (Plishing) ควรสังเกต URL ของเว็บไซต์ให้ชัดเจนและอย่ากดลิงก์ที่เปิดไฟล์แนบเข้ามา และระมัดระวังการล้วงข้อมูลของคอลเซ็นเตอร์

๑๒. ใช้สื่อสังคมออนไลน์อย่างระมัดระวัง ไม่ควรรับคนที่ไม่รู้จักเป็นเพื่อน หลีกเลี่ยงการแชทกับคนแปลกหน้า ไม่เปิดเผยข้อมูลส่วนตัวสู่สาธารณะ ลบบัญชีสังคมออนไลน์ที่ไม่ได้ใช้แล้ว

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

๑. สามารถอธิบายสถานการณ์การใช้งานอินเทอร์เน็ตและการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นในยุคดิจิทัล

๒. สามารถปฏิบัติตามขั้นตอนการป้องกันตรวจสอบความปลอดภัยด้วยตนเอง

๓. สามารถระวังไม่ให้ตนเองกระทำความผิดทางคอมพิวเตอร์ และพึงระวังการใช้งานบนอินเทอร์เน็ต

๔. สามารถนำความรู้มาประยุกต์ใช้ในการปฏิบัติงานได้อย่างปลอดภัย ไม่เกิดอันตรายต่อเทคโนโลยีดิจิทัลของหน่วยงาน

(นางสาวชลธิชา เผ่าโสภณ)
เจ้าพนักงานธุรการปฏิบัติงาน

(นายบุญสม พรหมสุวรรณ์)
ผู้อำนวยการสถานีพัฒนาที่ดินฉะเชิงเทรา