สรุปการพัฒนาความรู้

เรื่อง

ความมั่นคงปลอดภัยบนอินเทอร์เน็ต และการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

ผู้บรรยาย อาจารย์ณัฐ พยงค์ศรี
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงดิจิทัลฯ

จัดโดย สำนักงาน ก.พ.

ความมั่นคงปลอดภัยบนอินเทอร์เน็ต

ความมั่นคงปลอดภัยบนอินเทอร์เน็ต คือ การนำเครื่องมือทางเทคโนโลยีและกระบวนการที่รวมถึงการปฏิบัติที่ถูกต้องในการป้องกันและรับมือการโจมตีเข้ามาที่อุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการถูกเข้าถึงจากบุคคลที่สามที่ไม่ได้รับอนุญาต

การใช้งานอินเทอร์เน็ตในประเทศไทย

ประเทศไทย มีอัตราการใช้งานอินเทอร์เน็ตเพิ่มขึ้นสูงอย่างต่อเนื่อง และยังมีอัตราการใช้ Social Media เพิ่มมากขึ้นด้วย อุปกรณ์ที่นิยมในการใช้อินเทอร์เน็ตส่วนใหญ่เป็นโทรศัพท์มือถือ มากกว่าคอมพิวเตอร์ จึงมีความเสี่ยงต่อการพบเจอกับภัยคุกคามทางอินเทอร์เน็ตได้ทุกที่ ทุกเวลา

จากผลการสำรวจ พบว่า
ผู้ตอบแบบสำรวจ มีการใช้อินเทอร์เน็ต
โดยเฉลี่ยต่อวัน อยู่ที่
10 ชั่วโมง 36 นาที

วันทำงาน/วันเรียนหนังสือ
10 ชั่วโมง 55 นาที

วันหยุด
9 ชั่วโมง 49 นาที

ภัยคุกคามทางอินเทอร์เน็ต

ภัยคุกคามทางอินเทอร์เน็ต คือ การกระทำหรือการดำเนินการใดๆ ผ่านระบบสารสนเทศ หรือระบบเครือข่าย ที่จะก่อให้เกิดผลเสียต่อระบบข้อมูลเครือข่าย และระบบข้อมูลภายใน

รูปแบบของภัยคุกคามทางอินเทอร์เน็ต

Hacker คือ บุคคลที่มีความสนใจที่จะศึกษาค้นคว้าเกี่ยวกับระบบปฏิบัติการคอมพิวเตอร์การเจาะระบบต่าง ๆ เมื่อพบวิธีใด ๆ แล้ว ก็จะนำข้อมูลมาเผยแพร่ให้ผู้อื่นทราบ

Cracker คือ บุคคลที่คล้ายกับ Hacker แต่จะนำวิธีที่ตนเองค้นพบมาแสวงหาประโยชน์ต่อตนเอง

Script Kiddy คือ บุคคลที่ได้รับทราบข้อมูลที่สามารถสร้างความเสียหายกับระบบคอมพิวเตอร์แล้ว ก็จะนำข้อมูลนั้นมาทำตาม

Spy คือ บุคคลที่แอบเข้ามาในระบบคอมพิวเตอร์เพื่อสืบข้อมูลต่างๆ

Employee คือ บุคคลที่นำข้อมูลสำคัญขององค์กรไปเผยแพร่โดยไม่เจตนา ทำให้ผู้ที่ได้ข้อมูลสามารถโจมตีระบบขององค์กรได้

Terrorist คือ บุคคลที่ประสงค์ไม่ดี ก่อความไม่สงบในระบบคอมพิวเตอร์

การป้องกันภัยคุกคามทางอินเทอร์เน็ต

- เปิดใช้งานคอมพิวเตอร์เมื่อใดให้มีสติก่อนเสมอ
- ตั้งรหัสผ่านผสมตัวอักษรเพื่อไม่ให้คาดเดาได้ง่าย
- สังเกตว่ามีโปรแกรมที่แปลกปลอมแสดงขึ้นมาพร้อมการเปิดเครื่องหรือไม่
- อัปเดตระบบปฏิบัติการและซอฟต์แวร์อยู่เสมอ
- เว็บไซต์ให้บริการธุรกรรมอิเล็กทรอนิกส์ต้องมีการสร้างรหัสการเข้าข้อมูล และใบรับรองทางอิเล็กทรอนิกส์
- ไม่ควรเปิดเผยข้อมูลส่วนตัวลงบนเว็บไซต์หากจำเป็นให้สังเกตเนื้อหาว่าในเว็บไซต์นั้นน่าเชื่อถือหรือไม่
- ไม่ควรเข้าเว็บไซต์ที่เสี่ยง เช่น เว็บการพนัน เว็บลามก
- ศึกษาข้อกฎหมายเกี่ยวกับการใช้งานอินเทอร์เน็ต

10 ข้อ รอบรู้

ป้องกันภัยจากโซเชียลมีเดีย

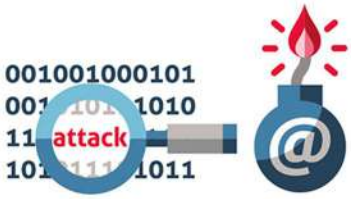
- คิดให้รอบคอบ
- ไม่แสดงข้อมูล
- ระมัดระวัง
- Do Not Track
- พิมพ์ URL โดยตรง
- ใช้วิจารณญาณ
- รอบคอบ
- ควบคุมการใช้งาน
- ตั้งค่า
- สังคมเสรี

ข้อควรเลี่ยง

เพื่อลดความเสี่ยงในการกระทำความผิดโดยรู้เท่าไม่ถึงการ
พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ 2560

นำภาพตัดต่อ ดัดแปลง เข้าสู่ระบบคอมพิวเตอร์

โดยมีเจตนาทำให้ผู้อื่นเสียชื่อเสียง ได้รับความอับอาย



ปลอมแปลง ทำลาย แก้ไข

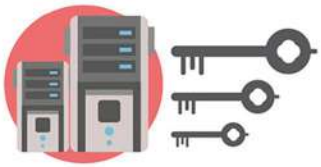
ข้อมูลคอมพิวเตอร์ของผู้อื่น
โดยเจ้าของไม่อนุญาต

ขัดขวาง รบกวน

การทำงานของระบบคอมพิวเตอร์ของผู้อื่น
ทำให้ไม่สามารถทำงานได้ตามปกติ

แอบดักรับข้อมูลของผู้อื่น

ระหว่างการส่งข้อมูลในระบบคอมพิวเตอร์



Hack ระบบคอมพิวเตอร์

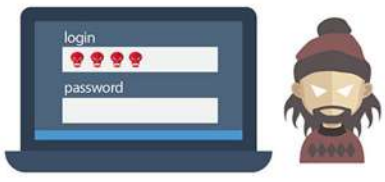
ที่มีมาตรการป้องกัน
เช่น ปลอมแปลง password เพื่อเข้าใช้งาน

เข้าดูหรือขโมย

ข้อมูลในระบบคอมพิวเตอร์ของผู้อื่น

จำหน่ายหรือเผยแพร่โปรแกรม

สำหรับใช้กระทำความผิด



ใช้ Username/password

ที่ไม่ใช่ของตนเอง

เผยแพร่ภาพ ข้อมูลใด ๆ

ที่หมิ่นสถาบันเบื้องสูง

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

ทำให้มีความเข้าใจ ในเรื่องภัยคุกคามทางอินเทอร์เน็ต และ
มีความรู้ในการรับมือ รวมถึงวิธีป้องกันภัยคุกคามทางอินเทอร์เน็ต
ได้อย่างถูกต้อง สามารถนำมาประยุกต์ใช้ในการปฏิบัติงาน
เนื่องจากปัจจุบันการทำงานต้องอาศัยเทคโนโลยีดิจิทัล
ใช้อินเทอร์เน็ตในการค้นหาข้อมูล จึงต้องมีการระมัดระวัง
ในการใช้อินเทอร์เน็ตให้เกิดความมั่นคงปลอดภัย
เพื่อเป็นการป้องกันภัยให้กับทั้งตนเองและหน่วยงาน

สรุปความรู้โดย

นางสาวฐานิตา กุญแจทอง
เจ้าหน้าที่ระบบงานคอมพิวเตอร์
กลุ่มทะเบียนประวัติและบำเหน็จความชอบ
กองการเจ้าหน้าที่
สิงหาคม 2567