รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร
กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

****

ส่วนที่ 1 ข้อมูลทั่วไป

ชื่อ-นามสกุล นางสาวกาญจนา วงค์กาด
ตำแหน่ง เศรษฐกรปฏิบัติการ **กลุ่ม** เศรษฐกิจที่ดินทางการเกษตร

หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ฯ :
ความมั่นคงปลอดภัยบนอินเตอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ :
ระบบอิเล็กทรอนิกส์ (HRD: e – Learning)

หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ฯ :
สำนักงานคณะกรรมการข้าราชการพลเรือน

ตั้งแต่วันที่ 17 เดือน มิถุนายน พ.ศ. 2564 **ถึงวันที่** 23 เดือน มิถุนายน พ.ศ. 2564
เพื่อ ☑ อบรม ☐ สัมมนา ☐ อื่นๆ ระบุ

ส่วนที่ 2 สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

2.1 รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/ สัมมนา/พัฒนาความรู้ฯ

อินเตอร์เน็ตมีบทบาทสำคัญในการดำเนินชีวิต เป็นปัจจัยที่ 5 และมีแนวโน้มการใช้งานเพิ่มขึ้นอย่างต่อเนื่อง จึงทำให้การใช้อินเตอร์เน็ต หรือสื่อสังคมออนไลน์ มีภัยคุกคาม อาชญากร ปรับตัวเพิ่มขึ้นตามไปด้วย ทำให้เราต้องมีความรู้เรื่องภัยคุกคามบนอินเตอร์เน็ต วิธีการป้องกัน และกฎหมายที่เกี่ยวข้องในการใช้งานอินเตอร์เน็ต

ยุคของอินเตอร์เน็ต แบ่งออกเป็น 4 ยุค

1) การให้บริการเว็บไซต์ในรูปแบบการสื่อสารทางเดียว (Web 1.0) ที่ไม่สามารถโต้ตอบได้ เช่น การส่ง E-mail

2) การใช้งานผ่านเครือข่ายอินเตอร์เน็ตในรูปแบบสองทาง (Web 2.0) ที่สามารถโต้ตอบ แสดงความคิดเห็นได้ เช่น Platform, Social Media

3) การใช้งานอินเตอร์เน็ตในช่วงรอยต่อระหว่าง Web 2.0 และ Web 3.0 ที่นำข้อมูล Big Data มาวิเคราะห์ข้อมูลให้ตรงกับความต้องการของมนุษย์มากขึ้น มีการเชื่อมโยงข้อมูลที่หลากหลาย

4) การใช้งานอินเตอร์เน็ต Web 4.0 ที่เว็บไซต์สามารถเรียนรู้พฤติกรรมของมนุษย์ สามารถให้คำแนะนำ ชักจูงให้คล้อยตามได้ สามารถรับรู้อารมณ์ ความรู้สึกในช่วงสนทนาได้

ประเภทของผู้กระทำความผิด

- Hacker คนที่มีความสนใจเกี่ยวกับระบบบริการคอมพิวเตอร์ และมีการแชร์ข้อมูลกัน
- Cracker คนที่มีความสามารถนำความรู้มาโจมตี ทำให้เกิดความเสียหายในระบบคอมพิวเตอร์
- Script kiddy คนที่มีความอยากรู้ อยากลอง ซึ่งบางครั้งอาจทำให้เกิดความเสียหายในระบบคอมพิวเตอร์
- Spy คนที่นำความลับ ข้อมูล ไปเผยแพร่แก่บุคคลภายนอกโดยไม่ได้รับอนุญาต
- Employee คนในองค์กร ที่สามารถเข้าสู่ระบบคอมพิวเตอร์ได้ บางครั้งอาจไม่ปฏิบัติตามระบบรักษาความปลอดภัยขององค์กร
- Terrorist กลุ่มก่อการร้าย มีจุดมุ่งหมายชัดเจนที่จะก่อความไม่สงบบนเครือข่ายอินเตอร์เน็ต

รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์

- Social Engineering เป็นปฏิบัติการทางจิตวิทยา หลอกล่อให้เหยื่อติดกับโดดไม่ต้องอาศัยความชำนาญเกี่ยวกับคอมพิวเตอร์

- Password Guessing การเดา Password เพื่อเข้าสู่ระบบ

- Denial of Service (DOS) การโจมตีลักษณะหนึ่งที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบและการร้องขอในคราวละมาก ๆ เพื่อที่จะให้ระบบหยุดการให้บริการ

- Decryption ถอดข้อมูลที่มีการเข้ารหัสอยู่

- Birthday Attacks สุ่มคีย์ขึ้นมาและอาจจะตรงกับคีย์ที่เราเข้ารหัสไว้

- Man in the middle Attacks การพยายามที่จะทำตัวเป็นคนกลางเพื่อคอยดักเปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (แก้ไขเพิ่มเติม พ.ศ. 2560) ตัวอย่างเช่น

- มาตรา 1 พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2551”

- มาตรา 2 พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับตั้งแต่ประกาศในราชกิจจานุเบกษา เป็นต้นไป

- มาตรา 3

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

ตัวอย่างภัยคุกคามบนอินเตอร์เน็ต

<u>Hacking Wi-Fi User</u>

- เหยื่อมักเข้าสู่ระบบอินเตอร์เน็ตไร้สานสาธารณะ ที่ให้บริการฟรีไม่ต้องลงทะเบียนโดยขาดความรอบคอบ

- ผู้ไม่ประสงค์ดีจะทำการปลอมแปลงชื่อตัวกระจายสัญญาณ และเหยื่อมักคุ้นเคยกับชื่อดังกล่างและทำการเชื่อมต่อเข้าสู่ระบบ

- ผู้ไม่ประสงค์ดีทำการปล่อยสัญญาณอินเตอร์เน็ตให้ใช้บริการฟรี

<u>ไวรัสเรียกค่าไถ่</u>

ไวรัส CryptOlOcker เรียกค่าไถ่ที่กำลังระบาดในไทย ด้วยการเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ที่ซับซ้อนกว่าแต่ก่อน ทำให้มีการเรียกเก็บเงินหลักหมื่นขึ้นไป และยิ่งนานการเรียกค่าไถ่จะมีราคาสูงขึ้น ซึ่งไม่มีการรับประกันว่าเมื่อจ่ายเงินแล้วจะได้ไฟล์คืน จึงมีวิธีการป้องกันอย่างง่ายดังนี้

1) ขอให้ระมัดระวังจากการรับอีเมล์แปลก ๆ ที่มีไฟล์แนบ

2) การเข้าเว็บไซต์ให้อ่านให้ละเอียดหากเข้าแล้วมีการทำการโหลดไฟล์ ขอให้ลบอย่าเปิดไฟล์เด็ดขาด

3) ลง Antivirus ที่มีการ Update

4) สำรองข้อมูลเป็นประจำ และอย่าเสียบอุปกรณ์สำรองข้อมูลค้างเพราะมันสามารถลามถึงกันได้

การเก็บพยานหลักฐานเมื่อข้อมูลถูกคุกคามบนอินเตอร์เน็ต

พยายามเก็บ E-mail ที่ส่งมา โดยเก็บทั้งตัว E-mail และตัว E-mail Header การเก็บควรเก็บหลาย ๆ รูปแบบ แต่ต้องมีเวลาที่ได้รับหรือส่งอีเมล์ที่ชัดเจน เช่น

- Screen Capture + PDF
- Screen Capture + ถ่ายรูปด้วยกล้องมือถือ

การตั้งค่าความปลอดภัยสำหรับ Facebook

การตั้งรหัสผ่าน มีกฎในการตั้ง ดังนี้

1) ไม่ควรตั้งเป็นหมายเลขโทรศัพท์
2) ไม่ควรตั้งเป็นวัดเกิดตัวเองหรือคนใกล้ชิด
3) ไม่ควรตั้งชื่อตัวเอง ชื่อเล่น ชื่อ User
4) ไม่ควรเป็นชุดตัวเลข หรืออักษรที่เดาได้ง่าย

การ Login เข้าสู่ระบบอย่างปลอดภัย

ควรแจ้งเตือนผ่านระบบ โดยการส่งข้อความ Alerts ทาง Facebook, Messenger และ E-mail มีวิธีเปิดใช้งานโดยเลือก Setting → Security And Login → Setting Up Extra Security → Get alerts about unrecognized logins → Get notifications → เลือกช่องทางที่ต้องการให้แจ้งเตือน → Save Changes

การตั้งค่าความปลอดภัยสำหรับ G-mail

- การตรวจหาไวรัส หรือมัลแวร์ โดยการสแกนเครื่องคอมพิวเตอร์เป็นประจำด้วยโปรแกรมป้องกันไวรัส เช่น McAfee, Norton, BullGuard
- การตรวจสอบความปลอดภัยของบัญชี สามารถทำได้โดยเลือก My Account → Sign-in & security → Get started เพื่อตรวจสอบความปลอดภัยของบัญชี
- การกู้คืนบัญชี สามารถทำได้โดยให้ระบบส่ง Code ไปยังเบอร์โทรศัพท์, G-mail อื่น
- การลงทะเบียนยืนยัน 2 ขั้นตอน การลงชื่อเข้าใช้ด้วยรหัสผ่าน และ Code ที่ระบบจะส่งให้ทางโทรศัพท์ โดยเลือก 2-Step Verification
- ไม่ควรใช้รหัสผ่าน G-mail ร่วมกับเว็บไซต์อื่นเป็นอันขาด ไม่จดรหัสผ่านใส่กระดาษ ไม่บอกรหัสผ่านให้ผู้อื่น
- จำเป็นต้อง Logout หลังใช้งานอยู่เสมอ และล้างแคชและคุกกี้ อยู่เสมอบนเครื่องคอมพิวเตอร์

การตั้งค่าความปลอดภัยสำหรับ Line

- หากบัญชีถูกขโมยสามารถเข้าไปกรอกแบบฟอร์มใน Link https://contact-cc.line.me/detailld/11242 เพื่อแจ้งให้ทีมงาน Line ทราบและลบบัญชี เพื่อป้องกันผู้ไม่หวังดี
- หากไม่ต้องการให้ Line ID ค้นหาได้ มีวิธีการปิดโดยเลือก Setting → Allow Others to Add by ID ให้เป็น off
- วิธีการป้องกันการแชตจากบุคคลไม่พึงประสงค์ (วิธีการปฏิเสธข้อความจากคนที่ไม่ใช่เพื่อน) มีวิธีการโดยเลือก Setting → Fillter Messages ให้เป็น on
- การบล็อกคนที่เราไม่ต้องการจะคุยด้วย มีวิธีการโดยเลือก รายชื่อเพื่อนที่ต้องการบล็อก → ... → Block
- ไม่ต้องการให้คนอื่นสามารถเพิ่มเราเป็นเพื่อนโดยใช้หมายเลขโทรศัพท์ มีวิธีการโดยเลือก Setting → แถบ Privacy → Allow Others to Add ให้เป็น off
- การโพสต์ข้อความบน Timeline แบบเฉพาะเจาะจง มีวิธีการคือ เลือกโพสต์แบบไหน แชร์แบบไหน เช่น Public, My LINE Friend, Only Me

ข้อเตือนใจในการใช้งานอินเตอร์เน็ต

1) ไม่ติดตั้งโปรแกรมโดยไม่อ่านรายละเอียด
2) ไม่เล่นอินเตอร์เน็ตไร้สายฟรี (ของฟรีไม่มีในโลก)
3) ไม่ติดตั้งโปรแกรม Antivirus ปลอม
4) ไม่คลิกลิงค์หรือเปิดไฟล์แนบที่มากับอีเมล์โดยไม่ตรวจสอบ
5) ไม่จดจำรหัสผ่านไว้บนเครื่อง
6) ไม่เปิดใช้งานฟังก์ชัน Autorun ใน Removeable drive
7) ไม่ Login เป็น Administrator
8) ไม่ปิด Windows Update
9) อัพเดตโปรแกรม Antivirus เสมอ

2.2 ประสบการณ์/ประโยชน์ที่ได้รับ/การประยุกต์ใช้กับหน่วยงาน

☑ **ต่อตนเองเพื่อเพิ่มพูนความรู้**

- ได้รับความรู้ ความเข้าใจ เกี่ยวกับสถานการณ์การใช้อินเตอร์เน็ต สิ่งที่ต้องระวังในการใช้งานคอมพิวเตอร์ วิธีการป้องกันและตรวจสอบความปลอดภัยบนอินเตอร์เน็ต รวมไปถึงการปฏิบัติตนในยุคดิจิทัล

☑ **ต่อหน่วยงาน/การนำมาประยุกต์ใช้กับหน่วยงาน**

- สามารถนำมาปรับใช้ในการทำงาน โดยเฉพาะการเข้าใช้ระบบคอมพิวเตอร์ อินเตอร์เน็ต ในการทำงานให้มีความปลอดภัย

2.3 ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้ฯ

-

2.4 ข้อคิดเห็นและข้อเสนอแนะ

-

ลงชื่อ.....กาญจนา วงค์กาด.....
(นางสาวกาญจนา วงค์กาด)
ตำแหน่ง เศรษฐกรปฏิบัติการ
ผู้รายงาน
วันที่ 5 เดือน กรกฎาคม พ.ศ. 2564

ส่วนที่ 3 ความเห็นของผู้บังคับบัญชา

(✓) ทราบ

.....

.....

.....

ลงชื่อ.....
(นายสมศักดิ์ สุขจันทร์)
ตำแหน่ง.....ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน.....
วันที่.....๑๓.....เดือน.....ก.ค.....พ.ศ. .....๖๔.....