**รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร**
**กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน**

**********

**ส่วนที่ 1 ข้อมูลทั่วไป**

ชื่อ น.ส. อมรรัตน์ นามสกุล สระเพ็ชร
ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ กลุ่ม/ฝ่าย วิเคราะห์สภาพการใช้ที่ดิน

หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ฯ
ความมั่นคงปลอดภัยทางอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล
สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ
E-Learning หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ฯ
สำนักงานคณะกรรมการข้าราชการพลเรือน
ตั้งแต่วันที่ 27 เดือน มิถุนายน พ.ศ. 2563 ถึงวันที่ 25 เดือน กรกฎาคม พ.ศ. 2563
เพื่อ ☑ อบรม ☐ สัมมนา ☐ อื่นๆ ระบุ.....

**ส่วนที่ 2 สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้**

2.1 รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/ สัมมนา/พัฒนาความรู้ฯ

ปัจจุบันระบบอินเทอร์เน็ตมีความสำคัญต่อการดำเนินชีวิต และการปฏิบัติงานราชการเป็นอย่างมาก เนื่องจากเครือข่ายระบบอินเทอร์เน็ตเป็นเครือข่ายที่มีการใช้งานอย่างแพร่หลาย และการเข้าถึงข้อมูลได้สะดวก จึงมีบุคคลใช้เครือข่ายระบบอินเทอร์เน็ตในการกระทำความผิดในรูปแบบต่างๆ

ในประเทศไทยได้มีการออกพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 18 มิถุนายน 2550 และมีผลบังคับใช้ในวันที่ 19 กรกฎาคม 2550 กฎหมายนี้เป็นกฎหมายที่กำหนดฐานความผิดและบทลงโทษสำหรับการกระทำความผิดทางคอมพิวเตอร์ในรูปแบบใหม่ และได้มีการแก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 25 มกราคม 2560

**ภัยคุกคาม (Threat) ของระบบสารสนเทศแบ่งออกได้เป็น 2 ประเภท**

1. ภัยคุกคามทางกายภาพ (Physical threat) คือภัยคุกคามที่เกิดขึ้นกับ Hardware ที่ใช้ในระบบคอมพิวเตอร์ และเครือข่าย เช่น Harddisk เสียหรือทำงานผิดพลาด
2. ภัยคุกคามทางตรรกะ (Logical threat) คือภัยคุกคามที่เกิดกับข้อมูลหรือสารสเทศ โดยขอยกตัวอย่างภัยคุกคามทางตรรกะ ดังต่อไปนี้

2.1 มัลแวร์ (Malware) ย่อมาจากคำว่า Malicious Software ซึ่งหมายถึงโปรแกรมประสงค์ร้ายต่างๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล มัลแวร์ แบ่งออกได้หลากหลายประเภท อาทิเช่น ไวรัส (Virus) หนอนอินเทอร์เน็ต (Worm) ม้าโทรจัน (Trojan Horse) การแอบดักจับข้อมูล (Spyware) ตลอดจนโปรแกรมประเภทขโมยข้อมูล (Cookie) และการฝัง Malicious Mobile Code (MMC) ผ่านทางช่องโหว่ของโปรแกรม Internet Explorer (IE Vulnerability) ที่เกิดขึ้น โดยโปรแกรมจะ

ทำการควบคุมการทำงานโปรแกรม Internet Explorer ให้เป็นไปตามความต้องการของผู้ที่ไม่หวังดี เช่น การแสดงโฆษณาในลักษณะของการ Pop-Up หน้าต่างโฆษณาออกมาเป็นระยะ หรือ แอ็ดแวร์ (Adware) ซึ่งอาจจะเกิดผลกระทบแก่ผู้ใช้งานได้ ถ้ารับโปรแกรมเหล่านี้เข้ามาในเครื่องคอมพิวเตอร์

2.2 การปฏิเสธการให้บริการ (Denial of Service: DoS) เป็นรูปแบบการโจมตีโดยส่งข้อมูลไปยังเครื่องเป้าหมายจำนวนมากๆ ทำให้เครื่องเป้าหมายไม่สามารถทำงานได้ตามปกติ

2.3 ฟิชชิ่ง (Phishing) เป็นการหลอกลวง โดยสร้าง e-mail หรือหน้า website ปลอมเพื่อให้ผู้ใช้งานเกิดความสับสน และทำธุรกรรม รวมถึงกรอกรายละเอียดข้อมูลส่วนบุคคลบนหน้า website หรือ e-mail ปลอมดังกล่าว ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลส่วนตัวของบุคคลนั้นๆ ได้ และทำการคัดลอกนำไปปลอมแปลงเพื่อประกอบธุรกรรมต่างๆ แทนผู้เป็นเจ้าของข้อมูลตัวจริงได้

2.4 Man-in-the-Middle (MitM) เป็นการโจมตีโดยดักรับข้อมูลจากระบบเครือข่าย ทำหน้าที่เป็นตัวแทนในการดักรับหรือเปลี่ยนแปลงข้อมูลระหว่างคู่สนทนา

2.5 Website Defacement คือการโจมตีเพื่อเปลี่ยนแปลงข้อมูลที่เผยแพร่หน้า website

**แนวทางการป้องกันภัยคุกคามทางอินเทอร์เน็ต**

1. ทำการสำรองข้อมูลอย่างสม่ำเสมอ
2. อัพเดทโปรแกรมป้องกันไวรัส และระบบปฏิบัติการอย่างสม่ำเสมอ
3. กำหนด password ที่ยากต่อการคาดเดา ทำการเปลี่ยน password เป็นระยะ และไม่ควรตั้งเป็น password เดียวกันทุกระบบ
4. ควรทำธุรกรรมทางการเงินผ่านเครือข่ายอินเทอร์เน็ตอย่างระมัดระวัง
5. ไม่ลง Software มากเกินความจำเป็น
6. ไม่ควรเข้าหรือ download ข้อมูลจาก website ที่ไม่น่าเชื่อถือ
7. ไม่ควรเปิดเผยข้อมูลส่วนตัวผ่าน Social network
8. ศึกษากฎหมายเกี่ยวกับการใช้อินเตอร์เน็ต
9. เก็บหลักฐานการจราจรของข้อมูลไว้ในระบบไม่น้อยกว่า 90 วัน

2.2 ประสบการณ์/ประโยชน์ที่ได้รับ /การประยุกต์ใช้กับหน่วยงาน

☑ต่อตนเอง

1. ช่วยเพิ่มศักยภาพในการใช้งานเครือข่ายอินเทอร์เน็ต
2. สามารถป้องกันภัยจากการใช้งานเครือข่ายอินเทอร์เน็ตได้เบื้องต้น

☑ต่อหน่วยงาน / การนำมาประยุกต์ใช้กับหน่วยงาน

สามารถความรู้ที่ได้มาเผยแพร่แก่บุคคลากรของกลุ่มให้มีความระมัดระวังในการใช้งานเครือข่ายอินเทอร์เน็ต

2.3 ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้ฯ

ไม่มี

2.4 ข้อคิดเห็นและข้อเสนอแนะ

1. ควรมีการจัดตั้งงบประมาณเพื่อจัดซื้อ Software และ Hardware ในการป้องกันภัยจากอินเตอร์เน็ต
2. ควรมีการจัดตั้งงบประมาณเพื่อจัดซื้อ Hardware หรือเช่าระบบ Cloud ในการสำรองข้อมูล

ลงชื่อ.....

(น.ส. อมรรัตน์ สระเพ็ชร)

ตำแหน่ง นักวิชาการเกษตรชำนาญการพิเศษ

ผู้รายงาน

วันที่ 29 เดือน กรกฎาคม พ.ศ. 2563

**ส่วนที่ 3 ความเห็นของผู้บังคับบัญชา**

(/) ทราบ

ลงชื่อ.....

(นายสมศักดิ์ สุขจันทร์)

ตำแหน่ง ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

วันที่ 31 เดือน ก.ค. พ.ศ. 2563