บันทึกข้อความ

ส่วนราชการ กลุ่มวิเคราะห์สภาพการใช้ที่ดิน กองนโยบายและแผนการใช้ที่ดิน โทร. ๒๑๘๙

ที่ กษ ๐๘๓๗.๐๒/๔๓๘ **วันที่** ๒๔ พฤษภาคม ๒๕๖๗

เรื่อง ขอส่งสรุปรายงานการฝึกอบรมพร้อมใบประกาศ

เรียน ผอ.กลุ่มวิเคราะห์สภาพการใช้ที่ดิน

ตามที่ข้าพเจ้า นางสาวภาวดี สิทธิ์ประเสริฐ นักวิชาการเกษตรชำนาญการ กลุ่มวิเคราะห์สภาพการใช้ที่ดิน กองนโยบายและแผนการใช้ที่ดิน ได้เข้ารับการฝึกอบรมผ่านระบบการเรียนออนไลน์ (TDGA e-learning) ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) จำนวน ๒ หลักสูตร นั้น

ในการนี้ ได้ดำเนินการจัดทำรายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้ กองนโยบายและแผนการใช้ที่ดิน จำนวน ๑ เรื่อง คือ การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ CyberSecurity Awareness เรียบร้อยแล้ว จึงขอส่งสรุปรายงานการฝึกอบรมพร้อมใบประกาศตามเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ และแจ้ง ผอ.กนผ. ลงนามในหนังสือ

ภาวดี สิทธิ์ประเสริฐ

(นางสาวภาวดี สิทธิ์ประเสริฐ)
นักวิชาการเกษตรชำนาญการ

เรียน ผอ.กนผ.

เพื่อโปรดทราบ และลงนามในเอกสารที่แนบ

(นางสาวอมรรัตน์ สระเพ็ชร)
นักวิชาการเกษตรชำนาญการพิเศษ
ผู้อำนวยการกลุ่มวิเคราะห์สภาพการใช้ที่ดิน

ลงนามแล้ว
- ศก. / วภก. รวบรวม

(นายชาคริต อินนะระ)
ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน
๒๔ พ.ค. ๒๕๖๗

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร
กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

****

ส่วนที่ ๑ ข้อมูลทั่วไป

ชื่อ นางสาวภาวดี นามสกุล สิทธิ์ประเสริฐ
ตำแหน่ง นักวิชาการเกษตรชำนาญการ กลุ่ม/ฝ่าย กลุ่มวิเคราะห์สภาพการใช้ที่ดิน
หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ฯ
การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ CyberSecurity Awareness
สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ
ระบบการเรียนออนไลน์ (TDGA e-learning)
หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ ฯ
สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ตั้งแต่วันที่ ๑๓ เดือน พฤษภาคม พ.ศ. ๒๕๖๗ ถึงวันที่ ๑๓ เดือน พฤษภาคม พ.ศ. ๒๕๖๗
เพื่อ ☑ อบรม ☐ สัมมนา ☐ อื่นๆ ระบุ

ส่วนที่ ๒ สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

๒.๑ รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/สัมมนา/พัฒนาความรู้ฯ

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ CyberSecurity Awareness

CyberSecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการ รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือ จากการถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต

ปัจจุบันหน่วยงานภาครัฐและภาคเอกชน ได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

- พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐
- พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

ความรู้พื้นฐานของ CyberSecurity

หลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ มีด้วยกัน ๓ ด้าน ซึ่งเรียกกันว่า “CIA Triad” หรือ “สามเหลี่ยม CIA” ประกอบด้วย

๑. Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

• ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุดผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น

• เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

๒. Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูลและการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

• ข้อมูลของธนาคารด้านการเงิน

• ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๓. Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

• ข้อมูลของธนาคารด้านการเงิน

• ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

รูปแบบภัยคุกคามของ CyberSecurity ตัวอย่างภัยคุกคาม เช่น

๑. Malware คือ ซอฟต์แวร์ หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่ เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง ไวรัส (Virus), เวิร์ม (Worms), และโทรจัน (Trojans)

๒. Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware ซึ่งเว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

๓. Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๔. Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น

• Code ของเว็บไซต์เช่น CMS

• Web Serverหรือ Database Serve

๕. Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Socialโดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน

๖. DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้ หรือระบบล่ม

๗. Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของ Application หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการ Application หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ ส่งผลกระทบ คือ

• ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่

• ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล

• สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

๘. Insider threat คือ ภัยที่เกิดจากบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรง เนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

วิธีการป้องกัน ทำได้โดย นำหลักการ Zero Trust มาใช้งานภายในองค์กร

๙. Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมาย หรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๑๐. Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์ เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน ทำได้โดย

• สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล

• ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

• ก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิด

๑๑. Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Computer สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย มีดังนี้

๑. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล

๒. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

๓. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๖. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

๗. มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

Password การใช้ Password ที่ดี คือ

๑. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #)

๒. มีความยาวของ Password อย่างน้อย ๘ตัวอักษร

๓. ควรหลีกเลี่ยงการใช้ Common password หรือ Default passwordหรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, ๑๒๓๔๕๖, วันเกิด, หมายเลขโทรศัพท์

๔. มีการเปลี่ยน Password อย่างสม่ำเสมอ

๕. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้

๖. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

๗. ไม่ควรบอก Password แก่ผู้อื่น

๘. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, ๑๒๓๔๕๖, วันเกิด, หมายเลขโทรศัพท์

๙. Password ควรมีความยาว อย่างน้อย ๘ ตัวอักษร

E-mail สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจ

๓. ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค

๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านทางช่องทางอื่น ๆ

๕. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๖. ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค

๗. ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค

Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Socialต่าง ๆ

๒. ไม่ควรทำการบันทึก Password ต่าง ๆ บน Browser

๓. เว็บไซต์สาหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น

๔. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefoxเป็นต้น

๕. ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ

๖. ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browserในโหมด Safe Web Browsing

๗. ควรติดตั้ง Anti-Malware และ Update อย่างสม่ำเสมอ

๘. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น

๙. กรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing

Messaginge LINE สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรบันทึก Password ไว้ที่โปรแกรม

๒. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง

๓. มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่าง ๆ ที่ได้รับมา

๔. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

๕. ไม่ควรแชร์ข้อมูลหรือข่าวสารต่าง ๆ โดยไม่ทราบที่มาของข้อมูล

๖. เข้าใช้งานโดย QR

๗. ห้ามบันทึกรหัสผ่านไว้

Fake News หรือ ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือ ซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตข่าวปลอม

๑. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ

๒. ระบุที่มาของข่าวไม่ได้

๓. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์

๔. สำนวนการเขียนออกแนวการโฆษณา

LINE Official Account

บัญชี Line เพื่อธุรกิจ มี ๓ ประเภท โดยสามารถดูได้จากสีที่แตกต่างของโล่ ดังนี้

๑. บัญชีทั่วไป บัญชีโล่สีเทาที่ผู้ใช้งาน LINE Official Account จะได้รับเมื่อเริ่มต้นใช้งาน ซึ่งสามารถอัพเกรดบัญชี เป็นบัญชีรับรองหรือบัญชี พรีเมียม ในภายหลังได้

๒. บัญชีรับรอง บัญชีโล่สีน้ำเงิน ที่ช่วยให้ลูกค้าค้นหาธุรกิจได้ง่ายขึ้นทั้งบน LINE และ Search engine ต่าง ๆ โดยมีค่าใช้จ่ายในการดำเนินการ ๘๘๘ บาท ตลอดอายุการใช้งาน

๓. บัญชี พรีเมียม บัญชีโล่สีเขียว ที่เหมาะกับธุรกิจขนาดใหญ่หรือองค์กรที่ต้องการสร้างฐานผู้ติดตามเป็นหลักล้าน สามารถค้นหาได้ง่าย และใช้งาน สปอนเซอร์ สติกเกอร์ และจะต้องมีค่าใช้จ่ายขั้นต่ำที่กำหนด

Conference สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ใช้สถานที่เหมาะสมกับการ Conference

๒. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง

๓. แชร์เอกสารต่าง ๆ อย่างระมัดระวัง

๔. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน

๕. มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

๖. ควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

Cloud Storage สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. แยก User ในการใช้งานของแต่ละบุคคล

๒. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จาเป็นเท่านั้น

๓. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจาเป็น

๔. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

๖. มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

Free WIFI สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน

๒. หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

Mobile สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์

๒. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา

๓. กำหนด Application permission ให้เหมาะสม

๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

Internet Connection สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน

๒. เปลี่ยน SSID และรหัสผ่านของ WIFIที่กำหนดมาจากผู้ให้บริการ

๓. กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น

IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่าง ๆ หรือ Application ต่าง ๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่ายเปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย เช่น

๑. ควรใช้ Application โดยตรงจากผู้ผลิตสินค้า และควรมีการ Update Application อย่างสม่ำเสมอ

๒. ควรมีการเปลี่ยน Password เช่น กล้องวงจรปิด เมื่อเชื่อมต่อกับ internet ควรมีการเปลี่ยนแปลง Password ที่ได้มาจากโรงงาน เป็นต้น

๒.๒ ประสบการณ์/ประโยชน์ที่ได้รับการประยุกต์ใช้กับหน่วยงาน

☑ ต่อตนเอง

๑. ทำให้มีความรู้ ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในปัจจุบัน

๒. ทำให้มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ประเภทต่างๆ และแนวทางป้องกันแก้ไข

๓. สามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

☑ ต่อหน่วยงาน/การนำมาประยุกต์ใช้กับหน่วยงาน

๑. ช่วยระวังปัญหาที่เกี่ยวข้องกับความปลอดภัยของข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับของหน่วยงานได้ในระดับหนึ่ง

๒. ช่วยลดค่าใช้จ่ายในการแก้ไขปัญหาการโจมตีทางไซเบอร์ให้กับหน่วยงาน

๓. ช่วยป้องกันความเสียหายที่เกิดขึ้นกับหน่วยจากการถูกคุกคามทางไซเบอร์ได้ในระดับหนึ่ง

๒.๓ ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้

การเข้าเรียน TDGA e-learning มีปัญหาเกี่ยวกับการเข้าสู่ระบบ แต่สามารถแก้ไขได้ วิดีโอไม่สามารถเล่นได้อย่างต่อเนื่อง ถ้าความแรงของ Internet ไม่เพียงพอ

๒.๔ ข้อคิดเห็นและข้อเสนอแนะ

ปัจจุบันหน่วยงานเปลี่ยนผ่านเข้าสู่องค์กรดิจิทัล บุคลากรจึงต้องเตรียมความพร้อมเข้าสู่การทำงานแบบองค์กรดิจิทัล ควรมีการเข้าอบรมหลักสูตรที่มีความเกี่ยวข้องกับการพัฒนาทักษะด้านดิจิทัล เพื่อให้การปฏิบัติงานมีประสิทธิภาพ และหลักสูตรการพัฒนาทักษะด้านดิจิทัลควรมีอย่างต่อเนื่อง และควรมีหลักสูตรที่เกี่ยวกับการทำงานด้านดิจิทัลของหน่วยงาน เพื่อให้ความรู้ที่ได้สามารถใช้ปฏิบัติงานได้จริงต่อไป

ลงชื่อ ภาวดี สิทธิ์ประเสริฐ

(นางสาวภาวดี สิทธิ์ประเสริฐ)

ตำแหน่ง นักวิชาการเกษตรชำนาญการ

ผู้รายงาน

วันที่ ๒๔ เดือน พฤษภาคม พ.ศ. ๒๕๖๗

( ) ทราบ

ลงชื่อ .....

(นายชาคริต อินนะระ)

ตำแหน่ง ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน

วันที่ ๒๔ เดือน พ. ค. พ.ศ. ๖๗

DGA
DIGITAL GOVERNMENT DEVELOPMENT AGENCY

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

ภาวดี สิทธิ์ประเสริฐ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

Cybersecurity Awareness

รวมระยะเวลาทั้งสิ้น 1 : 30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 14 พ.ค. 2567

(นายชรินทร์ ธีรฐิตยางกูร)

ผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

61615d39

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล(องค์การมหาชน) (สพร.)
Digital Government Development Agency (Public Organization) (DGA)
Date: 2024-05-14T01:09:01.681+07:00

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

ภาวดี สิทธิ์ประเสริฐ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Digital Literacy

รวมระยะเวลาทั้งสิ้น 0 : 30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 14 พ.ค. 2567

(นายชรินทร์ ธีรฐิตยางกูร)

ผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

2349e6c9

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล(องค์การมหาชน) (สพร.)
Digital Government Development Agency (Public Organization) (DGA)
Date: 2024-05-14T01:09:01.704+07:00