บันทึกข้อความ

ส่วนราชการ กลุ่มเศรษฐกิจที่ดินทางการเกษตร กองนโยบายและแผนการใช้ที่ดิน โทร. ๒๒๑๗

ที่ กษ ๐๘๓๗.๐๓/๒๕๙ **วันที่** ๑๒ กรกฎาคม ๒๕๖๗

เรื่อง รายงานการพัฒนาความรู้ข้าราชการ จำนวน ๓ เรื่อง

เรียน ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน ผ่านผู้อำนวยการกลุ่มเศรษฐกิจที่ดินทางการเกษตร

ตามที่กรมฯ ได้กำหนดตัวชี้วัดรายบุคคลด้านการพัฒนาบุคลากร การประเมินรอบที่ ๒/๒๕๖๗ (เมษายน ๒๕๖๗ – กันยายน ๒๕๖๗) กำหนดให้ข้าราชการมีการพัฒนาทักษะด้านดิจิทัล ๑ เรื่อง โดยพัฒนาครบถ้วนตามเงื่อนไขของหลักสูตรและพัฒนาความรู้ (เรื่องอื่น ๆ) ๑ เรื่อง รวมทั้งมีการสรุปบทเรียน ๑ เรื่อง ส่งให้ผู้บังคับบัญชาทราบ นั้น

บัดนี้ ข้าพเจ้าได้เข้ารับการฝึกอบรมการเรียนรู้ ๓ หลักสูตร เรียบร้อยแล้ว ประกอบด้วย

๑. หลักสูตร “ความรู้พื้นฐานเพื่อการวิเคราะห์ข้อมูลสำหรับข้าราชการและบุคลากรภาครัฐทุกระดับ” ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

๒. หลักสูตร “การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness” ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

๓. หลักสูตร “กฎหมายพื้นฐานสำหรับข้าราชการ”ของศูนย์พัฒนาการเรียนรู้ทางไกล สถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.

ทั้งนี้ได้จัดทำรายงานสรุปบทเรียน ๒ เรื่อง (รายละเอียดตามเอกสารแนบ)

จึงเรียนมาเพื่อโปรดทราบ และลงนามรายงานสรุปบทเรียน

(นายธนกฤต ผลเกลี้ยง)
เศรษฐกรชำนาญการพิเศษ

เรียน ผอ.กนอ.
เพื่อโปรดพิจารณา ลงนามในรายงาน
พัฒนาความรู้ และแจ้งฝ่ายเลขานุการ
ด้วยครับ

(นายสุภัทรชัย โอฬารกิจกุลชัย)
ผู้อำนวยการกลุ่มเศรษฐกิจที่ดินทางการเกษตร
๑๒ ก.ค. ๖๗

ลงนามแล้ว
- ศก./วภก. รวบรวม

(นายชาคริต อินนะระ)
ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน
๑๒ ก.ค. ๖๗

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร
กองนโยบายและแผนการใช้ที่ดิน กรมพัฒนาที่ดิน

****

ส่วนที่ 1 ข้อมูลทั่วไป

ชื่อ-นามสกุล นายธนกฤต ผลเกลี้ยง
ตำแหน่ง เศรษฐกรชำนาญการพิเศษ **กลุ่ม** เศรษฐกิจที่ดินทางการเกษตร
หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ฯ :
หลักสูตร การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness
สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ :
TDGA E-Learning
หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ฯ :
สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ตั้งแต่วันที่ 15 เดือน พฤษภาคม พ.ศ. 2567 **ถึงวันที่** 27 เดือน พฤษภาคม พ.ศ. 2567
เพื่อ ☑ อบรม ☐ สัมมนา ☐ อื่นๆ ระบุ.....

ส่วนที่ 2 สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

2.1 รายงานสรุปเนื้อหาสาระสำคัญในการอบรม/ สัมมนา/พัฒนาความรู้ฯ

1) Cybersecurity คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ เช่น

- พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

2) พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ : CIA Triad คือ

2.1) การรักษาความลับของข้อมูล (Confidentiality : C) คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ เช่น

- ข้อมูลส่วนเงินเดือนของพนักงานบริษัท จัดเป็น *ความลับสูงสุด* ผู้ที่สามารถเข้าถึงได้ คือ *ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น*
- เบอร์โทรศัพท์ของพนักงาน จัดเป็น *ข้อมูลภายในเท่านั้น* ผู้ที่สามารถเข้าถึงได้ คือ *พนักงานทุกคน*

2.2) การรักษาความถูกต้องของข้อมูล (Integrity : I) คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลบัญชีธนาคารด้านการเงิน
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

ส่วนที่ 2 (ต่อ)

2.3) ความพร้อมใช้งานของข้อมูล (Availability : A) คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น ข้อมูลในบัญชี สามารถเรียกดูได้ตลอดเวลา

3) รูปแบบภัยคุกคามของ Cybersecurity

3.1) Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อ Malware นั้นครอบคลุมถึง ไวรัส (Virus)}, เวิร์ม (Worms), โทรจัน (Trojans)

3.2) Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ Code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

3.3) Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็ปไซต์ หรือช่องทาง Social โดยวิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและใช้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

3.4) Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น Code ของเว็ปไซต์ เช่น CMS, Web Server หรือ Database Server วิธีการโจมตีที่นิยมใช้ คือ Cross-Site Scripting, SQL Injection, Path Traversal

3.5) Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็ปไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน

3.6) DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็ปไซต์, ระบบการให้บริการ หรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีเป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็ปไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

3.7) Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็ปไซต์, ข้อมูลของแอปพลิเคชั่น หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของข้อมูลนั้น ๆ

ผลกระทบ คือ (1) ข้อมูลสำคัญส่วนตัว หรือองค์กรโดนนำไปเผยแพร่

(2) บางกรณีมีการเรียกค่าไถ่ของข้อมูล

(3) สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

3.8) Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

วิธีการป้องกัน นำหลักการ Zero Trust มาใช้งานภายในองค์กร

ส่วนที่ 2 (ต่อ)

3.9) Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรองรับคำสั่งให้ทำการโจมตีเป้าหมาย หรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

3.10) Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ที่จุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

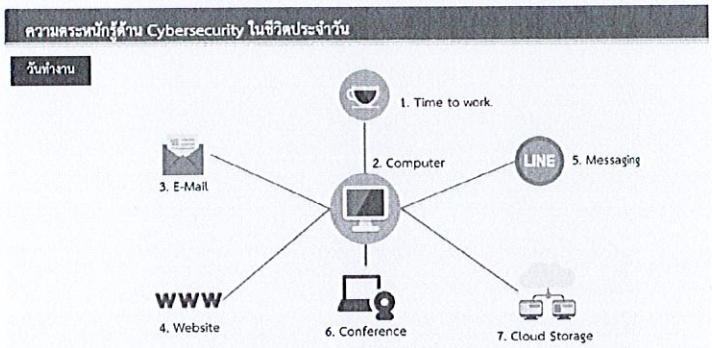
วิธีการป้องกัน (1) สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล

(2) ควรติดตั้ง Anti-Malware และมีการ Update อย่างสม่ำเสมอ

(3) ก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการปิด

3.11) Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวณผลเพื่อสร้างรายได้กลับไปที่ Hacker

4) ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน (วันทำงาน)



4.1) Computer สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

(1) ควรมีการแยก User ใช้งานกันของแต่ละบุคคล

(2) ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

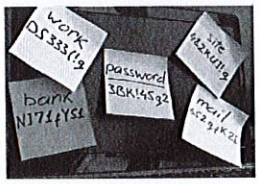
(3) ควรติดตั้ง Anti-Malware และมีการ Update อย่างสม่ำเสมอ เพราะไวรัสมีตัวใหม่มาอยู่เรื่อย ๆ

(4) มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

(5) มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

(6) ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

(7) มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น



การใช้ Password ที่ดี คือ 1) มีความซับซ้อน เช่น มีทั้งตัวอักษรเล็ก ใหญ่ ตัวเลข และอักขระพิเศษ 2) มีความยาวของ Password อย่างน้อย 8 ตัวอักษร 3) ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น 123456 วันเกิด หมายเลขโทรศัพท์ 4) มีการเปลี่ยนแปลง Password อย่างสม่ำเสมอ 5) ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้ 6) ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ 7)ไม่ควรบอก Password แก่ผู้อื่น

ส่วนที่ 2 (ต่อ)

4.2) E-mail สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

(1) ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

(2) ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

(3) ไม่คลิก Link ใน E-mail โดยไม่มีการตรวจเช็ค

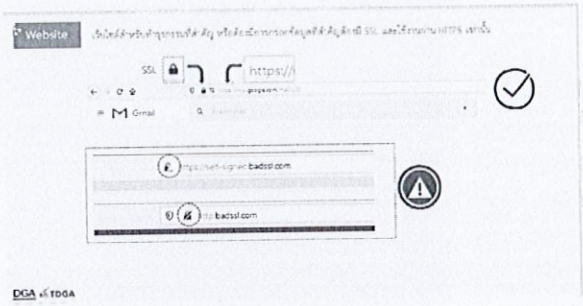
(4) เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านทางช่องทางอื่น ๆเพิ่มเติม

4.3) Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

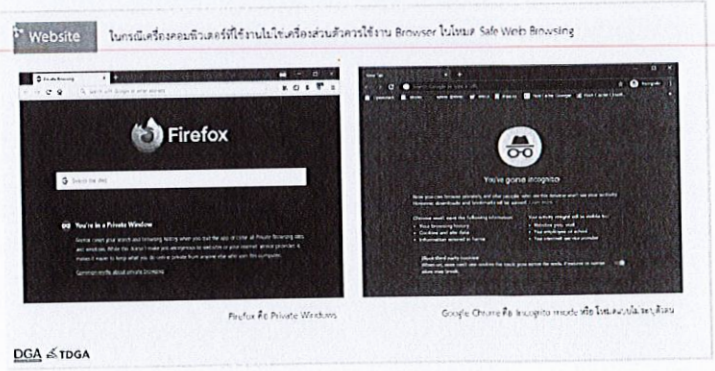
(1) ไม่เข้าเว็ปไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ

(2) ไม่ควรทำการบันทึก Password ต่าง ๆ บน Browser

(3) เว็ปไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น



(4) ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น



ส่วนที่ 2 (ต่อ)

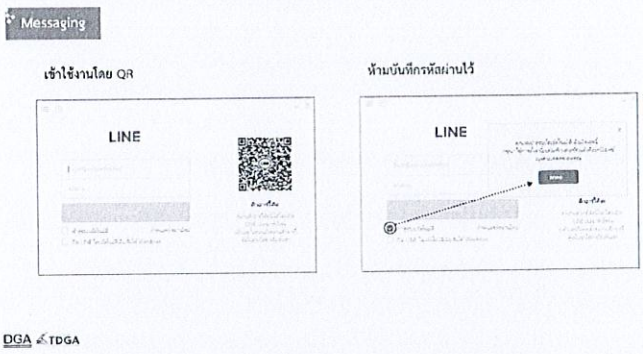
(5) ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ

(6) ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing

(7) ควรติดตั้ง Anti-Malware และ Update อย่างสม่ำเสมอ

4.4) Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

(1) ไม่ควรบันทึก Password ไว้ที่โปรแกรม



(2) กรณีไม่ใช่คอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง

(3) มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่าง ๆ ที่ได้รับมา

(4) มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

Fake News หรือข่าวปลอม เป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากขึ้น

วิธีการสังเกตข่าวปลอม 1) มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ 2) ระบุที่มาของข่าวไม่ได้ 3) มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์ 4) สำนวนการเขียนออกแนวโฆษณา

4.5) Conference สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

(1) ใช้สถานที่เหมาะสมกับการ Conference

(2) ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง

(3) แชร์เอกสารต่าง ๆ อย่างระมัดระวัง

(4) ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน

(5) มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

ส่วนที่ 2 (ต่อ)

4.6) Cloud Storage สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

(1) แยก User ในการใช้งานของแต่ละบุคคล

(2) ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น

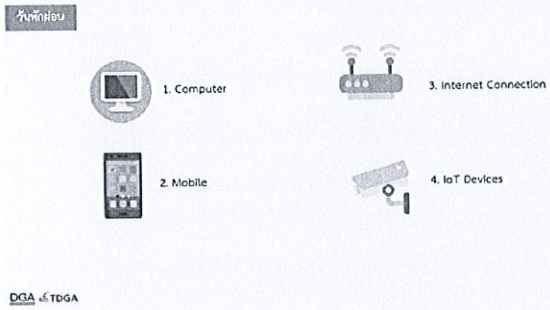
(3) ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น

(4) ควรติดตั้ง Anti-Malware และ Update อย่างสม่ำเสมอ

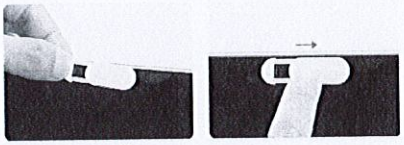
(5) มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

(6) มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

5) ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน (วันพักผ่อน)



5.1) Computer การติดตั้ง webcam cover ปกป้องเว็บแคมของคุณเมื่อไม่ได้ใช้งานและป้องกันไม่ให้แฮกเกอร์เว็บแอบดู



สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

(1) ควรมีการแยก User ใช้งานกันของแต่ละบุคคล

(2) ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

(3) ควรติดตั้ง Anti-Malware และมีการ Update อย่างสม่ำเสมอ เพราะไวรัสมีตัวใหม่มาอยู่เรื่อย ๆ

(4) มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

(5) มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

(6) ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

(7) มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

5.2) Free WIFI สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

(1) ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน

(2) หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

5.3) Mobile สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

(1) เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการใช้งานอุปกรณ์

(2) ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา

(3) กำหนด Application permission ให้เหมาะสม

(4) มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

(5) มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

ส่วนที่ 2 (ต่อ)

5.4) Internet Connection สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

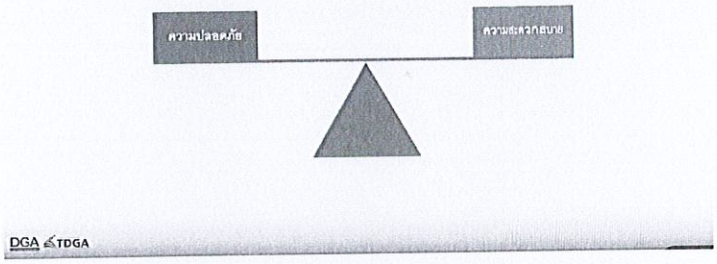
(1) เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน

(2) เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ใช้บริการ

(3) กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น

5.5) IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่าง ๆ หรือแอปพลิเคชั่นต่าง ๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

สรุปการสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์



2.2 ประสบการณ์/ประโยชน์ที่ได้รับ /การประยุกต์ใช้กับหน่วยงาน

☑ต่อตนเองเพื่อเพิ่มพูนความรู้

☑ต่อหน่วยงาน / การนำมาประยุกต์ใช้กับหน่วยงาน
เพื่อนำสิ่งที่ได้รับอบรมมาช่วยสนับสนุนการทำงานของตนเองในพื้นที่

2.3 ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้ฯ

-

2.4 ข้อคิดเห็นและข้อเสนอแนะ

1) การสร้างความตระหนักรู้ทางด้านไซเบอร์ให้กับพนักงานทุกคน ทำแล้วจะส่งผลดีอย่างไรต่อองค์กร

2) การสร้างการตระหนักรู้ด้านความมั่นคงปลอดภัยในการใช้ทรัพยากรสารสนเทศภายในองค์กร ช่วยให้องค์กรมีความพร้อมและสามารถปรับตัวให้เข้ากับการเปลี่ยนแปลง ทั้งยังลดโอกาสที่จะถูกโจมตีทางไซเบอร์ในรูปแบบต่างๆ ได้มากขึ้น

3) การฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความปลอดภัยจะช่วยลดโอกาสที่เจ้าหน้าที่จะตกเป็นเหยื่อของการโจมตีทางไซเบอร์ (Cyberattack)

ส่วนที่ 2 (ต่อ)

ลงชื่อ.....
(นายธนกฤต ผลเกลี้ยง)
ตำแหน่ง เศรษฐกรชำนาญการพิเศษ
ผู้รายงาน
วันที่ 12 เดือน กรกฎาคม พ.ศ. 2567

ส่วนที่ 3 ความเห็นของผู้บังคับบัญชา

(✓) ทราบ

.....

.....

.....

ลงชื่อ.....
(นายชาคริต อินนะระ)
ตำแหน่ง ผู้อำนวยการกองนโยบายและแผนการใช้ที่ดิน
วันที่ ๑๒ เดือน ก.ค. พ.ศ. ๖๗

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

ธนกฤต ผลเกลี้ยง

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์
Cybersecurity Awareness

รวมระยะเวลาทั้งสิ้น 1 : 30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 27 พ.ค. 2567

(นายชรินทร์ ธีรฐิตยางกูร)

ผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

9c137b63

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล(องค์การมหาชน) (สพร.)
Digital Government Development Agency (Public Organization) (DGA)
Date: 2024-05-27T07:00:00.696+07:00