บันทึกข้อความ

ส่วนราชการ กลุ่มสถาปัตยกรรมและภูมิสถาปัตยกรรม สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน โทร. ๑๓๙๕

ที่ กษ ๐๘๐๔.๐๓/ ๑๒๓ **วันที่** ๒๐ สิงหาคม ๒๕๖๘

เรื่อง รายงานผลการการพัฒนาความรู้ผ่านระบบ e-training

เรียน ผส. วพ. ผ่าน ผอ. กสภ.

ตามที่กรมได้กำหนดให้การพัฒนาความรู้ผ่านระบบ e-Training เป็นตัวชี้วัดรายบุคคลด้านการพัฒนาบุคลากร รอบที่ ๒ ปีงบประมาณ ๒๕๖๘ นั้น กระผมได้เข้าร่วมการฝึกอบรมเพื่อพัฒนาความรู้ จำนวน ๒ หลักสูตรคือ ๑) การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ และ ๒) ปัญญาประดิษฐ์เพื่ออนาคตของทุกคน

กระผมขอส่งรายงานผลการพัฒนาความรู้เรื่อง การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ โดยมีรายละเอียดดังนี้

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

คำอธิบายบทเรียน

เรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่างๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

วัตถุประสงค์

หน่วยที่เกี่ยวข้องความสามารถเพิ่มทักษะด้านดิจิทัลของข้าราชการ และบุคลากรภาครัฐเพื่อการปรับเปลี่ยนเป็นรัฐบาลดิจิทัล : CS๑๐๐ CS๒๐๐ CS๓๐๐ CS๔๐๐ CS๕๐๐

ผู้สอน

คุณพลากร ลาภอลงกรณ์

ผู้จัดการส่วนบริการลูกค้า ฝ่ายปฏิบัติการ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) : TDGA

ระยะเวลา : ๐๑:๓๔:๔๓ ชั่วโมง (๘ สื่อการสอน)

เนื้อหา

๑. Cyber security คืออะไร

Cyber security หรือ ความมั่นคงปลอดภัยไซเบอร์ – เป็นการนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้ เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต

ปัจจุบันทั้งภาครัฐและเอกชนเริ่มให้ความสำคัญในเรื่องความมั่นคงปลอดภัยไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบการโจมตีมีความหลากหลายและสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ

กฎหมายและมาตรฐาน ที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

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

๒. ความรู้พื้นฐานของ Cyber security

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์เรียกว่า CIA Triad ประกอบด้วย

C : Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละขุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ เช่น ข้อมูลเงินเดือนพนักงานบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น เบอร์โทรของพนักงานบริษัท จัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้คือ พนักงานบริษัททุกคน เป็นต้น

I : Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิการแก้ไขข้อมูลและการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น บัญชีธนาคาร ข้อมูลในคอมพิวเตอร์ เป็นต้น

A : Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น ข้อมูลบัญชีธนาคาร ข้อมูลในระบบคอมพิวเตอร์ เป็นต้น

๓. รูปแบบภัยคุกคามของ Cyber security

ENISA Threat Landscape ได้ระบุรูปแบบภัยคุกคามไซเบอร์ไว้ดังนี้

: Malware คือซอฟต์แวร์หรือโค้ดประเภทหนึ่ง ที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ จะทำให้สามารถเข้าถึงทรัพยากรของระบบและอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีทำการผลิตออกมา โดย Malware เรียกครอบคลุมถึง ไวรัส (Virus), เวิร์ม (Worms), โทรจัน (Trojans)

: Web-based attacks คือ วิธีโจมตีเหยื่อโดยผ่านทางเว็บไซต์ โดยทำเว็บไซต์หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่โค้ดที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์แล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่มี Malware ติดตั้งไว้ เพื่อให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware เว็บไซต์ที่มักถูก Hack และแก้ไขโค้ด มักเป็นเว็บไซต์ประเภท CMS (Content Management System)

: Phishing คือ วิธีโจมตีเหยื่อโดยผ่านทางช่องทางต่างๆ เช่น e-Mail, SMS, Website หรือช่องทาง Social โดยใช้การหลอกเหยื่อวิธีการต่างๆ ให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการธุรกรรม

: **Web application attacks** คือ วิธีการโจมตีเว็บไซด์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น Code ของเว็บแบบ CMS, Web/Data Server เป็นต้น วิธีการโจมตีนิยมใช้ Cross-Site Scripting, SQL Injection, Path Traversal เป็นต้น สามารถศึกษาวิธีการป้องกันได้จากมาตรฐาน OWASP Top Ten.

: **Spam** คือ วิธีการที่ผู้ส่งหรือผู้ไม่ประสงค์ดี ทำการส่งข้อมูล ข้อความ หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น e-Mail, SMS, Website หรือช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญหรือก่อกวน

: **DDoS (Distributed Daniel of Service)** คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซด์ ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์เพื่อให้เว็บไซด์ ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

: **Data Breach** คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซด์ ข้อมูลของแอปพลิเคชั่น หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชั่นไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ ผลกระทบคือข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่ โดนเรียกค่าไถ่ สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

: **Insider treat** คือ ภัยที่เกิดจากบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ทโฟน เป็นต้น จัดเป็นภัยที่มีความรุนแรง เนื่องจากองค์กรอาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย การป้องกันควรนำหลักการ Zero Trust มาใช้งานภายในองค์กร

: **Botnets** หรือ **Robot Network** คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี โดยทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ส่วนมากเครื่องที่ติด Botnets จะไม่ทราบ เพราะ Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

: **Ransomware** คือ Malware ประเภทหนึ่ง เมื่อถูกติดตั้งในเครื่องคอมพิวเตอร์แล้ว จะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ โดยมีจุดประสงค์เพื่อเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคให้ไฟล์ในเครื่องให้กลับมาใช้งานได้อีกครั้ง วิธีการป้องกัน ให้สำรองข้อมูลเป็นประจำ โดยแยกเก็บไฟล์สำรองข้อมูล ติดตั้ง Anti-Malware และมีการ Update อย่างสม่ำเสมอ ควรตระหนักทุกครั้งก่อนเปิดไฟล์ต่างๆ ที่ได้รับมา

: **Cryptojacking** คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Crypto Currency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้ส่งกลับไปหา Hacker

๔. ความตระหนักรู้ด้าน Cyber security ในชีวิตประจำวัน (วันทำงานและวันพักผ่อน)

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

: Office Computer - ควรแยก User ใช้งานของแต่ละบุคคล
- ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
- ควรติดตั้ง Anti-Malware และมีการ Update อย่างสม่ำเสมอ
- ควร Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- ควร Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
- ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
- มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

: Password
- มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #)
- มีความยาวของ Password ไม่น้อยกว่า ๘ ตัวอักษร
- ควรหลีกเลี่ยงการใช้ Common Password หรือ Default Password หรือ สิ่งที่คาดเดาได้ง่าย เช่น password, ๑๒๓๔๕๖, วันเกิด หรือหมายเลขโทรศัพท์ เป็นต้น
- เปลี่ยน Password อย่างสม่ำเสมอ
- ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
- ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
- ไม่ควรบอก Password แก่ผู้อื่น

: e-Mail
- ไม่เปิด e-Mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน (เอาเม้าส์ไปชี้ที่ชื่อผู้ส่งเพื่อตรวจสอบ)
- ไม่เปิดไฟล์แนบจาก e-Mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
- ไม่คลิก Link ใน e-Mail โดยไม่มีการตรวจเช็ค (เอาเม้าส์ไปชี้ที่ Link เพื่อตรวจสอบ)
- ก่อนทำธุรกรรมที่สำคัญต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

ถ้าพบว่า Mail ที่ส่งมา เป็น Spam Mail สามารถแจ้ง Spam Report ใน Browser ได้ และถ้าพบว่าเป็น Phishing ก็สามารถแจ้ง Phishing Report ใน Browser ได้เช่นกัน

: Website
- ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ
- ไม่ควรบันทึก Password ต่างๆ บน Browser
- เว็บไซต์สำหรับทำธุรกรรมสำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL : Secure Sockets Layer (อยู่ในรูปกุญแจปิด ถ้าอยู่ในรูปอื่นให้หลีกเลี่ยงการเข้าใช้) และใช้งานผ่าน HTTPS : Hypertext Transfer Protocol & SSL/TLS (HTTPS://) เท่านั้น
- ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้ เช่น Google, Chrome, Mozilla, Firefox เป็นต้น
- ควร Update Version ของ Browser อย่างสม่ำเสมอ
- หากเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing ใน Firefox จะเรียก Private Window หรือ Chrome จะเรียก Google Safe Browsing
- ควรติดตั้ง Anti-Malware และมีการ Update อย่างสม่ำเสมอ

Facebook จะแสดงเครื่องหมายยืนยันความถูกต้องเป็นรูปวงกลมเครื่องหมายถูกสีฟ้าหลังชื่อของ Facebook Account นั้น

Line จะแสดงเครื่องหมายยืนยันความถูกต้องเป็นรูปโล่ดาวหลังชื่อของ Line Official Account นั้น:

: Messaging
- ไม่ควรบันทึก Password ไว้ที่โปรแกรม
- หากเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
- มีความตระหนักก่อนเปิด Link หรือไฟล์ต่างๆ ที่ได้รับมา
- ควร Update Version ของโปรแกรมอย่างสม่ำเสมอ
- ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล
- โปรแกรม Line ไม่ควรบันทึกรหัสผ่านไว้ ควรเข้าใช้งานด้วย QR Code

: Fake News หรือ ข่าวปลอมเป็นภัยคุมคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวมาก เนื่องจากข่าวสารปลอมที่เผยแพร่นั้นมีความน่าเชื่อถือ ทำให้ผู้รับข่าวสารหลงเชื่อ สามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ โดยมักเผยแพร่ผ่านช่องทางออนไลน์ เช่น Line, Facebook เป็นต้น ทำให้การกระจายข่าวรวดเร็วมาก

วิธีการสังเกตข่าวปลอม

๑. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ
๒. ระบุที่มาของข่าวไม่ได้
๓. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
๔. สำนวนการเขียนออกแนวการโฆษณา

ข่าวปลอมเหล่านี้ สามารถตรวจสอบความถูกต้องผ่าน**ศูนย์ต่อต้านข่าวปลอม ประเทศไทย**

: Conference
- ใช้สถานที่เหมาะสมกับการ Conference
- ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
- ควรแชร์เอกสารต่างๆ อย่างระมัดระวัง
- ควรใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
- ควร Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ
- ควรขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนการบันทึกภาพและเสียงในการประชุม

: Cloud Storage - ควรแยก User ใช้งานของแต่ละบุคคล
- ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
- ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
- ควรติดตั้ง Anti-Malware และมีการ Update อย่างสม่ำเสมอ
- ควร Update Version ของโปรแกรมอย่างสม่ำเสมอ
- มีการติดตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

: Home Computer - ควรติดตั้ง Webcam Cover ใช้ปิดกล้องเพื่อป้องกันการแอบส่องดูความเป็นส่วนตัว
- ควรติดตั้งวัสดุปิดลำโพงที่เครื่องคอมพิวเตอร์ เพื่อป้องกันการฟังความเป็นส่วนตัว
- ควรแยก User ใช้งานของแต่ละบุคคล
- ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
- ควรติดตั้ง Anti-Malware และมีการ Update อย่างสม่ำเสมอ

- ควร Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- ควร Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
- ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
- มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

: Free WIFI
- ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
- หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

: Mobile
- เปิดการใช้งาน PIN/Password, Face Scan หรือ Finger Scan ในการเข้าใช้งานอุปกรณ์
- ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
- กำหนด Application Permission ให้เหมาะสม โดยตรวจสอบโปรแกรมที่ขอใช้งาน Microphone, Camera หรือ download files without notification เป็นต้น
- ควร Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- ควร Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
- ตระหนักรู้ SMS หลอกลวงที่ส่งมาให้คลิก Link หรือติดต่อตามข้อมูลที่ให้มาใน SMS

: Internet Connection
- เปลี่ยน Default Password ของ Router ที่ผู้ผลิตติดตั้งมาจากโรงงาน
- เปลี่ยน SSID (Service Set Identifier) และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ ควรตั้ง Password ของ Home WIFI ที่ยากต่อการ Hack
- ไม่ควรอนุญาตให้บุคคลภายนอกเข้าใช้งาน Home WIFI
- กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น

: IoT Device คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเตอร์เน็ต เพื่อใช้ในการทำงานร่วมกับระบบต่างๆ หรือแอปพลิเคชั่นต่างๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ กล้องวงจรปิด, ตู้เย็น, เครื่องซักผ้า-อบผ้า เป็นต้น ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

- ควรหลีกเลี่ยงการใช้ Default Password ที่ผู้ผลิตติดตั้งมา เพราะถูก Hack ได้ง่าย

สุดท้ายแล้วผู้ใช้งานทุกคน ควรหา**จุดสมดุลของความสะดวกสบายในการใช้งานไซเบอร์กับความปลอดภัยทางไซเบอร์** อย่างเหมาะสม

<u>ประโยชน์ที่ได้รับจากการอบรม</u>

ได้ความรู้และความเข้าใจถึงความสำคัญของความปลอดภัยทางไซเบอร์ รูปแบบต่างๆ ของภัยคุมคามไซเบอร์ สิ่งที่ควรปฏิบัติสำหรับการป้องกันภัยคุกคามไซเบอร์ในชีวิตประจำวันต่างๆ รวมถึงข้อแนะนำและข้อสังเกตต่างๆ เพื่อให้การเข้าใช้งานไซเบอร์มีความปลอดภัยเพิ่มมากขึ้น

<u>แนวคิดในการนำไปใช้พัฒนางานของตนเองและหน่วยงาน</u>

ความปลอดภัยทางไซเบอร์ เริ่มมีความสำคัญมากยิ่งขึ้นต่อการทำงานภายในองค์กร และการใช้ชีวิตของบุคลากรภาครัฐ โดยทั้งสองส่วนนี้ ถ้าได้เพิ่มประสิทธิภาพในการป้องกันภัยคุกคามไซเบอร์ จะเป็นการลดความเสียหายด้านเวลาและทรัพยากรต่างๆ อันส่งผลต่อประสิทธิภาพและประสิทธิผลในการปฏิบัติงานราชการ

แนวคิดเพื่อการพัฒนาสำนักวิศวกรรมเพื่อการพัฒนาที่ดิน ดังนี้

๑. ควรมีการถ่ายทอดความรู้ ความปลอดภัยทางไซเบอร์ที่อัพเดทเป็นปัจจุบันอย่างสม่ำเสมอ เพื่อให้บุคลากรทุกคน ได้เรียนรู้ถึงภัยคุมคามไซเบอร์รูปแบบใหม่ๆ

๒. ควรจัดทำระบบตรวจสอบการ Hack หรือการรั่วไหล/การเปลี่ยนแปลงข้อมูลของ สวพ. จากผู้ไม่ประสงค์ดี อย่างสม่ำเสมอ โดยระบบนี้จะเป็นประโยชน์ต่อหน่วยงานและต่อการให้บริการแก่ประชาชนได้มากยิ่งขึ้น

๓. ควรจัดทำระบบสนับสนุนให้มีการเปลี่ยน Password ของบุคลากรในหน่วยงาน เพื่อความปลอดภัยไซเบอร์ อยู่เป็นระยะ

พร้อมนี้กระผมได้แนบประกาศนียบัตรการฝึกอบรมหัวข้อที่ ๑, ๒ จำนวน ๒ แผ่น

จึงเรียนมาเพื่อโปรดทราบ และนำเรียน ผส. วพ. พิจารณาคัดกรองในระดับหน่วยงานเพื่อใช้ในการรวบรวมขึ้นบนเว็บไซต์ของหน่วยงาน ตามตัวชี้วัดรายบุคคลรอบที่ ๒ ปีงบประมาณ ๒๕๖๘ ต่อไป

(นายไชยยุทธ ลียะวณิช)
สถาปนิกชำนาญการ

(นายดนุ เนียมฤทธิ์)
ผู้อำนวยการกลุ่มสถาปัตยกรรมและภูมิสถาปัตยกรรม

(นายธนากร นาเชียงใต้)
ผู้อำนวยการสำนักวิศวกรรมเพื่อการพัฒนาที่ดิน

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ ไชยยุทธ ลียะวณิช

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 18 สิงหาคม 2568

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2025-08-18T20:04:23.720+07:00

c372b3f6

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ ไชยยุทธ ลียะวณิช

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

AI for Everyone : ปัญญาประดิษฐ์เพื่ออนาคตของทุกคน

จำนวนชั่วโมงการเรียนรู้ 2:00 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 18 สิงหาคม 2568

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Digitally signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2025-08-18T20:10:36.821+07:00

6b72e5bd