บันทึกข้อความ

ส่วนราชการ กลุ่มสถาปัตยกรรมและภูมิสถาปัตยกรรม สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน โทร ๑๓๙๕

ที่ กษ ๐๘๐๔.๐๓/๗๕ **วันที่** ๒๔ กุมภาพันธ์ ๒๕๖๙

เรื่อง รายงานผลการพัฒนาทางไกลด้วยระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์

เรียน ผอ.สวพ. ผ่าน ผอ.กสภ.

ตามแบบกำหนดและประเมินตัวชี้วัดด้านผลสัมฤทธิ์ของประจำปีงบประมาณ พ.ศ. ๒๕๖๙ ของสำนักวิศวกรรมเพื่อการพัฒนาที่ดิน กรมพัฒนาที่ดิน ให้ข้าราชการอบรมศึกษาการพัฒนาความรู้ผ่านระบบ e-learning โดยพัฒนาครบถ้วนตามเงื่อนไขของหลักสูตร อย่างน้อย ๒ เรื่อง และมีการสรุปบทเรียน ๑ เรื่อง ส่งให้ผู้บังคับบัญชา นั้น

ข้าพเจ้า นาย วัชรพล เอี่ยมเพ็ชร์ ตำแหน่ง วิศวกรโยธาปฏิบัติการ สังกัดกลุ่มกลุ่มสถาปัตยกรรมและภูมิสถาปัตยกรรม สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน กรมพัฒนาที่ดิน ได้ผ่านการพัฒนาทางไกลด้วยระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์(LDD e-learning) จำนวน ๒ หลักสูตร ได้แก่

๑. ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Understanding and Using Digital Technology)

๒. การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybercurity Awareness)

จึงขอสรุปบทเรียนที่ได้รับการพัฒนาความรู้ในรอบการประเมินที่ ๑/๒๕๖๙ จำนวน ๑ หลักสูตร ได้แก่ เรื่อง การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybercurity Awareness) รายละเอียดปรากฏตามรายงานสรุปบทเรียน และได้แนบสำเนาใบประกาศนียบัตร จำนวน ๒ หลักสูตร มาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณา

(นายวัชรพล เอี่ยมเพ็ชร์)
วิศวกรโยธาปฏิบัติการ

(นายดนุ เนียมฤทธิ์)
ผู้อำนวยการกลุ่มสถาปัตยกรรมและภูมิสถาปัตยกรรม

คำนำ

การรายงานผลการพัฒนาความรู้ผ่านระบบ e-Learning โดยพัฒนาครบถ้วนตามเงื่อนไขของหลักสูตร เพื่อยกระดับความสำเร็จของการส่งเสริมการพัฒนาความรู้ ครบถ้วนตามงเอนไขของหลักสูตร ตามแบบกำหนดและประเมินตัวชี้วัดด้านความสัมฤทธิ์ของประจำปีงบประมาณ พ.ศ. 2569 ของสำนักวิศวกรรมเพื่อพัฒนาที่ดินกรมพัฒนาที่ดิน กรมพัฒนาที่ดิน ให้ข้าราชการอบรมศึกษา

ข้าพเจ้า นายวัชรพล เอี่ยมเพ็ชร์ ตำแหน่งวิศกรโยธาปฏิบัติการ สังกัด กลุ่มสถาปัตยกรรม สำนักวิศวกรรมเพื่อพัฒนาที่ดิน กรมพัฒนาที่ดิน ได้ผ่านการพัฒนาทางไกลด้วยระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ (LDD e-Learning) ตามหลักสูตรดังกล่าวแล้ว จึงขอส่งรายงานผลการอบรมพัฒนาทางไกลด้วยระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ (LDD e-Learning) เรื่อง การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybercurity Awareness) และมีการสรุปบทเรียนเพื่อรายงานเสนอต่อผู้บังคับบัญชาประกอบการประเมินผลตัวชี้วัด ในลำดับต่อไป

(นายวัชรพล เอี่ยมเพ็ชร์)

วิศวกรโยธาปฏิบัติการ

ชื่อเรื่อง : การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybercurity Awareness)

วัตถุประสงค์

เพื่อเพิ่มทักษะความสามารถด้านดิจิทัลของข้าราชการ และบุคลากรภาครัฐเพื่อการปรับเปลี่ยนเป็นรัฐบาลแบบดิจิทัล

บทนำ

กระบวนการให้ความรู้และฝึกฝนบุคลากรให้เข้าใจถึงความเสี่ยง ภัยคุกคามทางไซเบอร์ และบทบาทของตนเองในการป้องกันข้อมูลสำคัญ โดยเน้นการสร้างพฤติกรรมปลอดภัย เช่น การตั้งรหัสผ่านที่รัดกุม การสังเกตอีเมลหลอกลวง (Phishing) และการใช้งานอินเทอร์เน็ตอย่างปลอดภัย เพื่อเปลี่ยนให้บุคลากรเป็นเกราะป้องกันด่านแรกแทนการเป็นจุดอ่อน

เนื้อหา

1.Cyber security คืออะไร

Cyber security หรือ ความมั่นคงปลอดภัยไซเบอร์ เป็นการนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้ เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึง จากบุคคลที่สามโดยไม่ได้รับอนุญาต

ปัจจุบันทั้งภาครัฐและเอกชนเริ่มให้ความสำคัญในเรื่องความมันคงปลอดภัยไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบการโจมตีมีความหลากหลายและ สร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ

2.ความรู้พื้นฐานของ Cyber security

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์เรียกว่า CIA Triad ประกอบด้วย

C : Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลสามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ เช่น ข้อมูลเงินเดือนพนักงานบริษัทจัดเป็นความลับสูงสุด ผู้สามารถเข้าถึงได้คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น เบอร์โทรของพนักงานบริษัท จัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้คือ พนักงานบริษัททุกคน เป็นต้น

I : Integriry หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิการแก้ไขข้อมูลและการรักษา
ความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น บัญชีธนาคาร ข้อมูลในคอมพิวเตอร์ เป็นต้น

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

3. 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 หรือช่องทางSocial โดยใช้การหลอกเหยื่อวิธีการต่างๆ ให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Passwordหรือข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการธุรกรรม

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

Spam คือ วิธีการที่ผู้ส่งหรือผู้ไม่ประสงค์ดี ทำการส่งข้อมูล ข้อความ หรือโฆษณาต่างๆ ผ่านช่องทาง ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญหรือก่อกวนต่างๆ ไปยังผู้รับ เช่น e Mail, SMS, website หรือช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้รับอนุญาตไปยังผู้รับ

DDoS (Distributed Daniel of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลา เดียวกัน จุดประสงค์เพื่อให้เว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

Data Breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของแอปพลิเคชั่น หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชั่นไม่ทราบ ซึ่งผู้โจมดีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ ผลกระทบคือ ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่ โดนเรียกค่าไถ่ สร้างผลกระทบต่อชื่อเสียงและความ น่าเชื่อถือขององค์กร

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

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี โดยท่าการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือ ดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ส่วนมากเครื่องที่ติด Botnets จะไม่ทราบ เพราะ Botnets จะไม่ทำงาน ตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

Ransomware คือ Malware ประเภทหนึ่ง เมื่อถูกติดตั้งในเครื่องคอมพิวเตอร์แล้ว จะทำการล็อก เพลโดยวีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ท่าให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้โดยมีจุดประสงค์เพื่อเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคให้ไฟล์ในเครื่องให้กลับมาใช้งานได้อีกครั้ง วิธีการ ป้องกัน ให้สำรองข้อมูลเป็นประจำ โดยแยกเก็บไฟล์สำรองข้อมูล ติดตั้ง Anti-Malware และมีการ Update อย่างสม้าเสมอ ควรตระหนักทุกครั้งก่อนเปิดไฟล์ต่างๆ ที่ได้รับมา

Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Crypto Currency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ ของเหยื่อประมวลผลเพื่อสร้างรายได้ส่งกลับไปหา Hacker

ประโยชน์ที่ได้รับ

ได้เข้าใจถึงภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ ที่เกิดขึ้นในปัจจุบันและช่วยสร้างจิตสำนึกและความระมัดระวังในการใช้งานเทคโนโลยีดิจิทัล ทั้งในระดับบุคคลและระดับองค์กร เพื่อลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ที่มักเกิดจากความประมาทหรือความไม่รู้ของมนุษย์ (Human Error)

แนวคิดการนำไปใช้ปรับใช้ในการพัฒนาตนเองและหน่วยงาน

ความปลอดภัยทางไซเบอร์ เริ่มมีความสำคัญมากยิ่งขึ้นต่อการทำงานภายในองค์กร และการใช้ชีวิตของบุคลากรภาครัฐ โดยทั้งสองส่วนนี้ ถ้าได้เพิ่มประสิทธิภาพในการป้องกันภัยคุกคามไซเบอร์ จะเป็นการลดความเสียหายด้านเวลาและทรัพยากรต่างๆ อันส่งผลต่อประสิทธิภาพและประสิทธิผลในการปฏิบัติงานราชการ

แนวคิดเพื่อการพัฒนาสำนักวิศวกรรมเพื่อการพัฒนาที่ดิน ดังนี้

1. ควรมีการถ่ายทอดความรู้ ความปลอดภัยทางไซเบอร์ที่อัพเดทเป็นปัจจุบันอย่างสม่ำเสมอ เพื่อให้บุคลากรทุกคน ได้เรียนรู้ถึงภัยคุมคามไซเบอร์รูปแบบใหม่ๆ

2.ควรจัดทาระบบตรวจสอบการ Hack หรือการั่วไหล/การเปลี่ยนแปลงข้อมูลของสวพ.จากผู้ไม่ประสงค์ดี อย่างสม่ำเสมอ โดยระบบนี้จะเป็นประโยชน์ต่อหน่วยงานและต่อการให้บริการแก่ประชาชนได้มากยิ่งขึ้น

3.คารจัดทำระบบสนับสนุนให้มีการเปลี่ยน Password ของบุคลากรในหน่วยงาน เพื่อความปลอดภัยของ ไซเบอร์ อยู่เป็นระยะ

DGA
DIGITAL GOVERNMENT DEVELOPMENT AGENCY

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

วัชรพล เอี่ยมเพ็ชร์

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 22 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-22T21:57:14.767+07:00
fe35e779

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

วัชรพล เอี่ยมเพ็ชร์

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ

(Understanding and Using Digital Technology)

จำนวนชั่วโมงการเรียนรู้ 2:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 22 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

e558fe24

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (dga)
Date: 2026-02-22T19:22:32.174+07:00

บันทึกข้อความ

ส่วนราชการ กลุ่มพัฒนาโครงสร้างพื้นฐานที่ ๑ สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน โทร.๑๒๘๓

ที่ กษ ๐๘๐๔.๐๖/ ๘๙ **วันที่** ๒๐ กุมภาพันธ์ ๒๕๖๙

เรื่อง รายงานผลการเรียนรู้จากการพัฒนาผ่านระบบออนไลน์ (TDGA E-learning) ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy

เรียน ผอ. สวพ. ผ่าน ผอ.กพฐ.๑

ตามที่ ข้าพเจ้าได้เข้าอบรมการพัฒนาผ่านระบบออนไลน์ (TDGA E-learning) ของกรมพัฒนาที่ดิน ตามตัวชี้วัดความสำเร็จของการพัฒนาความรู้ของบุคลากรในหน่วยงาน ข้าพเจ้าได้ผ่านการอบรมหลักสูตรดังนี้

๑. หลักสูตร การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

๒. หลักสูตร Digital intelligence : ความฉลาดทางดิจิทัล

รายละเอียดตามเอกสารแนบท้าย

จึงเรียนมาเพื่อโปรดพิจารณา

(นายฐากูร สาธุพันธ์)
วิศวกรโยธาปฏิบัติการ

(นายชัยวัฒน์ จะวิเสน)
ผู้อำนวยการกลุ่มพัฒนาโครงสร้างพื้นฐานที่ ๑

สรุปผลการเรียนรู้

๑.หัวข้อการพัฒนาความรู้

เรื่อง การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

๒.เนื้อหาโดยสังเขป

หลักสูตรการสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) ของ Thailand Digital Government Academy (TDGA) มีเนื้อหามุ่งเน้นการเสริมสร้างความรู้พื้นฐาน ความเข้าใจ และทักษะที่จำเป็นต่อการปฏิบัติงานในยุคดิจิทัล โดยเฉพาะอย่างยิ่งในบริบทของหน่วยงานภาครัฐที่มีการจัดเก็บและใช้ประโยชน์จากข้อมูลจำนวนมาก

เนื้อหาเริ่มจากการอธิบายภาพรวมสถานการณ์ภัยคุกคามทางไซเบอร์ในปัจจุบัน ทั้งในระดับประเทศและระดับองค์กร เช่น การโจมตีด้วยมัลแวร์ (Malware) การเรียกค่าไถ่ข้อมูล (Ransomware) การหลอกลวงผ่านอีเมลหรือข้อความ (Phishing) รวมถึงเทคนิค Social Engineering ซึ่งมุ่งโจมตีที่พฤติกรรมและความผิดพลาดของผู้ใช้งาน มากกว่าการเจาะระบบโดยตรง ทั้งนี้ได้เน้นให้เห็นว่าบุคลากรทุกระดับมีบทบาทสำคัญในการป้องกันภัยไซเบอร์ และความประมาทเพียงเล็กน้อยอาจก่อให้เกิดความเสียหายต่อข้อมูลและภาพลักษณ์ขององค์กรได้

หลักสูตรยังให้ความรู้เกี่ยวกับหลักการพื้นฐานของความมั่นคงปลอดภัยสารสนเทศ ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งานของข้อมูล (Availability) หรือที่เรียกว่า CIA Triad พร้อมทั้งอธิบายแนวทางปฏิบัติที่เหมาะสม เช่น การตั้งรหัสผ่านที่รัดกุม การใช้ระบบยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) การสำรองข้อมูลอย่างสม่ำเสมอ และการระมัดระวังในการเปิดไฟล์หรือคลิกลิงก์จากแหล่งที่ไม่น่าเชื่อถือ

ในส่วนของ AI Basics ได้อธิบายแนวคิดพื้นฐานเกี่ยวกับปัญญาประดิษฐ์ (Artificial Intelligence: AI) กลไกการทำงานโดยสังเขป และตัวอย่างการประยุกต์ใช้ AI ในภาครัฐ เช่น การวิเคราะห์ข้อมูลจำนวนมาก การให้บริการตอบคำถามอัตโนมัติ และการสนับสนุนการตัดสินใจเชิงนโยบาย นอกจากนี้ยังกล่าวถึงความเสี่ยงที่เกี่ยวข้องกับการใช้งาน AI อาทิ การนำข้อมูลสำคัญหรือข้อมูลส่วนบุคคลไปป้อนในระบบโดยไม่เหมาะสม ความเสี่ยงด้านข้อมูลรั่วไหล (Data Leakage) ปัญหา Deepfake และการบิดเบือนข้อมูล รวมถึงข้อควรคำนึงด้านจริยธรรม ความโปร่งใส และความรับผิดชอบในการใช้ AI

นอกจากนี้ยังมีการนำเสนอกรณีศึกษาจากเหตุการณ์จริง เพื่อให้ผู้เข้าอบรมเห็นภาพผลกระทบที่เกิดขึ้นจากการละเลยมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ ตลอดจนแนวทางการรับมือและการฟื้นฟูระบบเมื่อเกิดเหตุการณ์ไม่พึงประสงค์ โดยเน้นการสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับการป้องกันเชิงรุก การรายงานเหตุการณ์ผิดปกติอย่างทันท่วงที และการพัฒนาความรู้ของบุคลากรอย่างต่อเนื่อง

โดยสรุป เนื้อหาของหลักสูตรมุ่งสร้างความตระหนักรู้ เสริมสร้างทักษะพื้นฐาน และปลูกฝังพฤติกรรมการใช้งานเทคโนโลยีอย่างปลอดภัย ควบคู่กับการใช้ AI อย่างมีความรับผิดชอบ เพื่อสนับสนุนการพัฒนาองค์กรภาครัฐสู่การเป็นหน่วยงานดิจิทัลที่มั่นคง ปลอดภัย และสร้างความเชื่อมั่นให้แก่ประชาชนผู้รับบริการอย่างยั่งยืน

๓.ประโยชน์ที่ได้รับ

๑. มีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามไซเบอร์ในรูปแบบต่าง ๆ

๒. สามารถปฏิบัติตนได้อย่างถูกต้องเพื่อลดความเสี่ยงด้านความปลอดภัยสารสนเทศ

๓. มีความเข้าใจพื้นฐานเกี่ยวกับ AI และการใช้งานอย่างปลอดภัย

๔. ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลประชาชน

๕. เสริมสร้างทักษะดิจิทัลที่จำเป็นต่อการพัฒนารัฐบาลดิจิทัล

๖. สนับสนุนการทำงานของหน่วยงานให้สอดคล้องกับนโยบาย Digital Government

๔.แนวคิดในการนำไปใช้ในการพัฒนางานของตนเองและหน่วยงาน

๑ การยกระดับมาตรการคุ้มครองข้อมูลประชาชน

- กำหนดแนวปฏิบัติในการจัดเก็บและใช้ข้อมูลเกษตรกรและผู้รับบริการอย่างปลอดภัย
- ควบคุมสิทธิ์การเข้าถึงข้อมูลตามหน้าที่ความรับผิดชอบ
- ลดความเสี่ยงจากการรั่วไหลของข้อมูลส่วนบุคคล

๒ การประยุกต์ใช้ AI เพื่อเพิ่มประสิทธิภาพการให้บริการ

- พัฒนาระบบตอบคำถามอัตโนมัติ (Chatbot) ให้ข้อมูลเบื้องต้นเกี่ยวกับบริการด้านการพัฒนาที่ดิน
- ใช้ AI วิเคราะห์ข้อมูลเชิงพื้นที่ (Spatial Data) เพื่อสนับสนุนการวางแผนงานวิศวกรรม
- ปรับปรุงกระบวนการให้บริการออนไลน์ให้รวดเร็วและแม่นยำยิ่งขึ้น

๓ การสร้างวัฒนธรรมองค์กรด้านความมั่นคงปลอดภัยไซเบอร์

- ถ่ายทอดความรู้ให้บุคลากรในหน่วยงาน
- จัดทำคู่มือแนวปฏิบัติด้าน Cybersecurity
- ส่งเสริมการเฝ้าระวังและรายงานเหตุการณ์ผิดปกติ

๔ การพัฒนาองค์กรสู่การเป็นหน่วยงานดิจิทัลที่มั่นคง

- บูรณาการเทคโนโลยีดิจิทัลควบคู่กับมาตรการรักษาความปลอดภัย
- สร้างความเชื่อมั่นแก่ประชาชนว่าหน่วยงานมีมาตรฐานด้านความปลอดภัยข้อมูล
- สนับสนุนการให้บริการประชาชนแบบ Citizen-Centric ที่ปลอดภัย โปร่งใส และตรวจสอบได้

๕.ใบประกาศนียบัตร

มีใบประกาศนียบัตรผลการฝึกอบรม เรื่อง การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (ตามเอกสารแนบท้าย)

สรุปผลการเรียนรู้

๑.หัวข้อการพัฒนาความรู้

เรื่อง Digital intelligence : ความฉลาดทางดิจิทัล

๒.เนื้อหาโดยสังเขป

หลักสูตร Digital Intelligence : ความฉลาดทางดิจิทัล ของ TDGA มุ่งเน้นการเสริมสร้างความรู้ความเข้าใจ และทักษะที่จำเป็นสำหรับบุคลากรภาครัฐในการปฏิบัติงานในยุคดิจิทัล โดยเนื้อหาครอบคลุมทั้งมิติด้านเทคโนโลยี ความปลอดภัย กฎหมาย และจริยธรรม เพื่อให้สามารถใช้เครื่องมือดิจิทัลได้อย่างมีประสิทธิภาพและรับผิดชอบ สาระสำคัญประกอบด้วย

๒.๑ แนวคิดและกรอบความเข้าใจเรื่อง Digital Intelligence (DQ) อธิบายความหมายของความฉลาดทางดิจิทัลในฐานะ "ทักษะชีวิตดิจิทัล" (Digital Life Skills) ที่บุคลากรภาครัฐต้องมี เพื่อให้สามารถทำงานในสภาพแวดล้อมที่ขับเคลื่อนด้วยข้อมูลและเทคโนโลยีได้อย่างเหมาะสม โดยเชื่อมโยงกับบริบทของรัฐบาลดิจิทัล (Digital Government) ที่เน้นความโปร่งใส ตรวจสอบได้ และยึดประชาชนเป็นศูนย์กลาง (Citizen-Centric)

๒.๒ การรู้เท่าทันสื่อและข้อมูล (Digital & Media Literacy) มุ่งพัฒนาทักษะการวิเคราะห์ ประเมิน และคัดกรองข้อมูลข่าวสารในโลกออนไลน์ โดยครอบคลุมถึง

- การตรวจสอบความน่าเชื่อถือของแหล่งข้อมูล
- การแยกแยะข่าวจริง–ข่าวปลอม (Fake News)
- การทำความเข้าใจอคติของข้อมูล (Bias)
- การใช้ข้อมูลอย่างถูกต้องตามหลักวิชาการและจริยธรรม

เนื้อหาส่วนนี้ช่วยให้บุคลากรสามารถตัดสินใจบนพื้นฐานของข้อมูลที่ถูกต้อง ลดความเสี่ยงจากการสื่อสารข้อมูลผิดพลาด ซึ่งอาจส่งผลกระทบต่อภาพลักษณ์ของหน่วยงานภาครัฐ

๒.๓ ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Awareness) ให้ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่พบบ่อย เช่น ฟิชชิ่ง (Phishing), มัลแวร์ (Malware), แรนซัมแวร์ (Ransomware) และการโจมตีทางวิศวกรรมสังคม (Social Engineering) พร้อมแนวทางป้องกันเบื้องต้น ได้แก่

- การตั้งรหัสผ่านที่รัดกุมและไม่ใช้ซ้ำ
- การยืนยันตัวตนหลายขั้นตอน (Multi-Factor Authentication: MFA)
- การระมัดระวังการเปิดไฟล์แนบหรือคลิกลิงก์จากแหล่งที่ไม่รู้จัก
- การอัปเดตระบบและโปรแกรมอย่างสม่ำเสมอ

เนื้อหานี้ช่วยลดความเสี่ยงต่อการรั่วไหลของข้อมูลราชการ และเสริมสร้างความมั่นคงปลอดภัยในระดับองค์กร

๒.๔ การคุ้มครองข้อมูลส่วนบุคคลและการบริหารจัดการข้อมูล (Data Privacy & Data Governance) เน้นความสำคัญของการจัดเก็บ ใช้ และเปิดเผยข้อมูลอย่างเหมาะสม โดยสอดคล้องกับกฎหมายและระเบียบที่เกี่ยวข้อง เช่น หลักการคุ้มครองข้อมูลส่วนบุคคล การกำหนดสิทธิ์การเข้าถึงข้อมูล (Access Control) และการจัดหมวดหมู่ข้อมูล (Data Classification)
บุคลากรจะได้เรียนรู้บทบาทหน้าที่ของตนในการรักษาความลับของข้อมูลประชาชน รวมถึงแนวปฏิบัติเมื่อเกิดเหตุข้อมูลรั่วไหล (Data Breach)

๒.๕ จริยธรรมดิจิทัล (Digital Ethics) และความรับผิดชอบต่อสังคมมุ่งสร้างจิตสำนึกในการใช้เทคโนโลยีอย่างมีความรับผิดชอบ เคารพสิทธิผู้อื่น และไม่ละเมิดกฎหมาย เช่น

- การใช้สื่อสังคมออนไลน์อย่างเหมาะสมในฐานะข้าราชการ
- การไม่เผยแพร่ข้อมูลที่สร้างความแตกแยกหรือเข้าใจผิด
- การรักษาภาพลักษณ์และความน่าเชื่อถือของหน่วยงาน

๒.๖ ทักษะการทำงานและการสื่อสารในสภาพแวดล้อมดิจิทัล

ส่งเสริมการใช้เครื่องมือดิจิทัลเพื่อเพิ่มประสิทธิภาพการทำงาน เช่น ระบบประชุมออนไลน์ ระบบจัดการเอกสารอิเล็กทรอนิกส์ (e-Document) และแพลตฟอร์มทำงานร่วมกัน (Collaboration Tools) โดยเน้น

- การจัดเก็บข้อมูลอย่างเป็นระบบ
- การแบ่งปันข้อมูลอย่างปลอดภัย
- การทำงานเป็นทีมในรูปแบบ Hybrid หรือ Remote

๓.ประโยชน์ที่ได้รับ

๑ มีความเข้าใจเกี่ยวกับแนวคิด Digital Intelligence และสามารถประเมินพฤติกรรมการใช้เทคโนโลยีของตนเองได้

๒ ตระหนักถึงความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และสามารถป้องกันตนเองจากภัยคุกคามเบื้องต้น

๓ มีความรู้ในการจัดการข้อมูลและรักษาความลับของทางราชการอย่างถูกต้อง

๔ เสริมสร้างจริยธรรมในการใช้สื่อดิจิทัล ลดความเสี่ยงต่อการละเมิดสิทธิหรือกฎหมาย

๕ พัฒนาทักษะการทำงานร่วมกันผ่านระบบดิจิทัล เพิ่มประสิทธิภาพการปฏิบัติงาน

๔.แนวคิดในการนำไปใช้ในการพัฒนางานของตนเองและหน่วยงาน

ระดับบุคคล

- ปรับพฤติกรรมการใช้งานอีเมลและระบบสารสนเทศให้ปลอดภัยมากขึ้น
- ตรวจสอบข้อมูลก่อนเผยแพร่หรือส่งต่อ
- ใช้เครื่องมือดิจิทัลในการจัดเก็บเอกสารและข้อมูลอย่างเป็นระบบ
- ปฏิบัติตามแนวทางด้านความปลอดภัยสารสนเทศของหน่วยงานอย่างเคร่งครัด

ระดับหน่วยงาน

- ส่งเสริมวัฒนธรรมองค์กรด้านความปลอดภัยไซเบอร์
- จัดกิจกรรมอบรมหรือถ่ายทอดความรู้ด้าน Digital Intelligence อย่างต่อเนื่อง
- พัฒนาแนวปฏิบัติ (Guideline) ด้านการใช้สื่อสังคมออนไลน์และการคุ้มครองข้อมูล
- สนับสนุนการใช้ระบบดิจิทัลเพื่อเพิ่มประสิทธิภาพการให้บริการประชาชน

๕.ใบประกาศนียบัตร

มีใบประกาศนียบัตรผลการฝึกอบรม เรื่อง Digital intelligence : ความฉลาดทางดิจิทัล (ตามเอกสารแนบท้าย)

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ ฐากูร สาธุพันธ์

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 12 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (dpas.)
Date: 2026-02-12T12:00:59.863+07:00
2dd4bf94

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ ฐากูร สาธุพันธ์

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Digital Literacy : ความฉลาดทางดิจิทัล

(Digital Intelligence)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 11 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-11T15:48:50.595+07:00

8b247fe5

บันทึกข้อความ

ส่วนราชการ กลุ่มพัฒนาโครงสร้างพื้นฐานที่ ๔ สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน โทร. ๑๒๘๓ ต่อ ๑๐๖

ที่ กษ ๐๘๐๔.๐๙/๕๗ **วันที่** ๒๓ กุมภาพันธ์ ๒๕๖๙

เรื่อง ขอส่งรายงานผลการพัฒนาความรู้ผ่านสื่ออิเล็กทรอนิกส์ รอบการประเมินที่ ๑/๒๕๖๙

เรียน ผอ.สวพ. ผ่าน ผอ.กพฐ.๔

ตามแบบกำหนดการและประเมินตัวชี้วัดเพื่อประกอบการพิจารณาเลื่อนเงินเดือนระดับกอง/ สำนัก ด้านผลสัมฤทธิ์ของงานรอบการประเมินที่ ๑ และ ๒ ประจำปีงบประมาณ พ.ศ.๒๕๖๙ ซึ่งตัวชี้วัดระดับความสำเร็จของการส่งเสริมการพัฒนาความรู้ของบุคลากรในหน่วยงาน ในรอบการประเมินที่ ๑/๒๕๖๙ ของ สำนักวิศวกรรมเพื่อการพัฒนาที่ดิน กรมพัฒนาที่ดิน กำหนดให้ข้าราชการมีการพัฒนาความรู้ครบถ้วนตามเงื่อนไขของหลักสูตร ๒ เรื่อง และมีการสรุปบทเรียน ๑ ส่งให้ผู้บังคับบัญชาทราบ นั้น

ข้าพเจ้า นายพงศกร สุวรรณวิโก ตำแหน่ง วิศวกรโยธาปฏิบัติการ ได้ผ่านการพัฒนาความรู้ของบุคลากรด้วยระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ รวมทั้งหมดจำนวน ๒ หลักสูตร ได้แก่

๑. การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
๒. ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Understanding and Using Digital Technology)

ครบถ้วนตามเงื่อนไขของหลักสูตรการพัฒนาความรู้ของบุคลากรด้วนระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ โดยพัฒนาครบถ้วนตามเงื่อนไขของหลักสูตร ทั้งมีการสรุปบทเรียน ๑ เรื่อง คือเรื่องการสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) เป็นที่เรียบร้อยแล้ว รายละเอียดปรากฏตามรายงาน สรุปบทเรียน และประกาศนียบัตร จำนวน ๒ แผ่น ที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณา

(นายพงศกร สุวรรณวิโก)
วิศวกรโยธาปฏิบัติการ

(นายวีระพงษ์ พิกุลประยงค์)
ผู้อำนวยการกลุ่มโครงสร้างพื้นฐานที่ ๔

สรุปรายงานการพัฒนาความรู้

1. **หัวข้อการพัฒนาความรู้**

เรื่อง การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

2.. **เนื้อหาโดยสังเขป**

Cybersecurity หรือ **ความมั่นคงปลอดภัยไซเบอร์** คือ การนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการ
ที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต โดยในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ (CIA Triad) ประกอบด้วย

1. **Confidentiality หรือ การรักษาความลับของข้อมูล** คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้คือ พนักงานบริษัททุกคน

2. **Integrity หรือ การรักษาความถูกต้องของข้อมูล** คือ การที่ระบุสิทธิของการแก้ไขข้อมูลและการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

3. **Availability หรือ ความพร้อมใช้งานของข้อมูล** คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

รูปแบบภัยคุกคามของ Cybersecurity

1. Malware คือ โปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมา เพื่อทำอันตรายกับข้อมูลในระบบ เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ ขโมยหรือทำลายข้อมูลหรืออาจจะเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องของเราได้ เช่น Virus (ไวรัส) Worm (เวิร์ม) และ Trojan (โทรจัน)

2. Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

3. Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

4. Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น Code ของเว็บไซต์เช่น CMS และ Web Server หรือ Database Server โดยวิธีการโจมตีที่นิยมใช้ ได้แก่ Cross-Site Scripting , SQL Injection และ Path Traversal

5. Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญ หรือก่อกวน

6. DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้ หรือระบบล่ม

7. Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ ผลกระทบต่อข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่ ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล และสร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

8. Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

9. Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

10. Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่ง

จุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

11. Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

1. Computer สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ ควรมีการแยก User ใช้งานกันของแต่ละบุคคล ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์ ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ มีการใช้ Password ที่ดี และไม่ควรบอก Password แก่ผู้อื่น

2. Password โดยการใช้ Password ที่ดี คือ มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #) มีความยาวของ Password อย่างน้อย 8 ตัวอักษร ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น password, 123456, วันเกิด, หมายเลขโทรศัพท์ มีการเปลี่ยน Password อย่างสม่ำเสมอ ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้ ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ และไม่ควรบอก Password แก่ผู้อื่น

3. E-mail สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค และเรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

4. Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ ไม่ควรทำการบันทึก Password ต่างๆ บน Browser เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัว ควรใช้งาน Browser ในโหมด Safe Web Browsing ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

5. Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ ไม่ควรบันทึก Password ไว้ที่โปรแกรม กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ และไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

6. Conference สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ ใช้สถานที่เหมาะสมกับการ Conference ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง มีการแชร์เอกสารต่างๆ อย่างระมัดระวัง ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน และมีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

7. Cloud Storage สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ แยก User ในการใช้งานของแต่ละบุคคล ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

2. **ประโยชน์ที่ได้รับ**

ทำให้เข้าใจถึงหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ และสามารถนำความรู้ไปใช้ในการปฏิบัติเพื่อความปลอดภัยในการใช้อุปกรณ์เครือข่าย ระบบและโปรแกรมต่างๆ เป็นการเฝ้าระวังและป้องกันคอมพิวเตอร์ เครือข่าย ซอฟต์แวร์แอปพลิเคชัน ระบบที่สำคัญ และข้อมูลให้ปลอดภัยจากภัยคุกคามทางดิจิทัลที่อาจเกิดขึ้นได้ทั้งในการทำงานและการใช้ในชีวิตประจำวัน

3. **แนวคิดในการนำไปใช้ในการพัฒนางานของตนเองและหน่วยงาน**

1. การจัดการข้อมูลของตนเอง เช่น การใช้ Passphrase (วลีรหัสผ่าน) ที่ยาวและจำง่ายแต่เดายาก และการแยกบัญชีส่วนตัวออกจากบัญชีทำงานอย่างชัดเจน
2. ฝึกนิสัยการตรวจสอบลิงก์หรือไฟล์แนบทุกครั้ง แม้จะส่งมาจากคนที่รู้จัก โดยเช็กอีเมลผู้ส่ง (Sender Address) หรือสอบถามกลับผ่านช่องทางอื่นหากดูผิดปกติ
3. พัฒนาทักษะการคัดแยกประเภทข้อมูล (Data Classification) ว่าข้อมูลใดเป็นความลับ ข้อมูลใดเปิดเผยได้ และจัดเก็บ/ส่งต่ออย่างถูกวิธี (เช่น การใส่รหัสผ่านไฟล์ก่อนส่ง)

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ พงศกร สุวรรณวิโก

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 5 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ พงศกร สุวรรณวิโก

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ

(Understanding and Using Digital Technology)

จำนวนชั่วโมงการเรียนรู้ 2:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 5 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล