สรุปความรู้จากการอบรมหลักสูตร
การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

นางนิภารัตน์ ตระกูลพงษ์
ตำแหน่ง นักวิชาการเกษตรชำนาญการ
สถานีพัฒนาที่ดินสุรินทร์ สำนักงานพัฒนาที่ดินเขต ๓

ส่วนที่ ๑ สรุปรายละเอียดเนื้อหาของหลักสูตร

สรุปหลักสูตร การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

Cybersecurity Awareness คือการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์เกี่ยวกับภัยคุกคามทางไซเบอร์ ความเสี่ยง และแนวทางปฏิบัติที่ดีที่สุดในการปกป้องข้อมูลส่วนบุคคลและองค์กร ซึ่งการตระหนักรู้ด้านความปลอดภัยทางไซเบอร์ Cybersecurity Awareness หรือ Security Awareness เปรียบเสมือนเกราะป้องกันที่ช่วยให้องค์กรสามารถป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้ทั้งในปัจจุบันและในอนาคต

Cybersecurity หรือ ความมั่งคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

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

รูปแบบของภัยคุกคาม Cybersecurity

Cybersecurity ได้แก่ Malware, Web-based attacks, Phishing, Web application attacks, Spam, DDoS, Data breach, Insider threat, Botnets, Ransomware, Cryptojaking

- Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีวัตถุประสงค์เพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ เมื่อถูกติดตั้งจะเข้าถึงทรัพยากรระบบคอมพิวเตอร์และอาจแชร์ข้อมูลไปยังเครื่องอื่นๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆ ชื่อเรียก Malware รวมถึง ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojans)
- Web-based attacks คือ วิธีการโจมตีผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขโดยการใส่ code เมื่อเหยื่อเข้าเว็บฯ ทำให้คอมพิวเตอร์เหยื่อติด Malware
- Phishing การหลอกล่อเหยื่อให้ข้อมูลส่วนตัว เช่น Username Password
- Web application attacks โจมตีเว็บฯ เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น web Server
- Spam การส่งข้อมูล ข้อความ โฆษณาต่างๆ ผ่านช่องทางต่างๆ เช่น E-mail Web-side จำนวนมาก เพื่อสร้างความรำคาญหรือก่อกวน
- DDoS การโจมตีเป้าหมายที่เป็นเว็บฯ ระบบการให้บริการ หรือระบบเครือข่าย เพื่อทำให้ไม่สามารถใช้งานหรือระบบล่อ

- Data breach เกิดการรั่วไหลของข้อมูลโดยที่เจ้าของข้อมูลไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่
- Insider threat ภัยจากคนในองค์กรจากความตั้งใจ และไม่ตั้งใจ
- Botnets โปรแกรมที่เขียนขึ้นเพื่อโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ จากผู้ผลิต
- Ransomware เมื่อถูกติดตั้งจะล็อคไฟล์โดยวิธีการเข้ารหัสทำให้ไม่สามารถเปิดใช้งานได้ จุดประสงค์เพื่อเรียกค่าไถ่รหัสผ่าน
- Cryptojacking Hacker เข้าเครื่องคอมพิวเตอร์เหยื่อโดยวิธีการต่างๆ และทำการติดตั้งโปรมแกรมเพื่อขุดเหรียญ Cryptocurrency

การตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

๑. คอมพิวเตอร์ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ

๑.๑ ควรแยก User ใช้งานของแต่ละคน

๑.๒ ควร logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

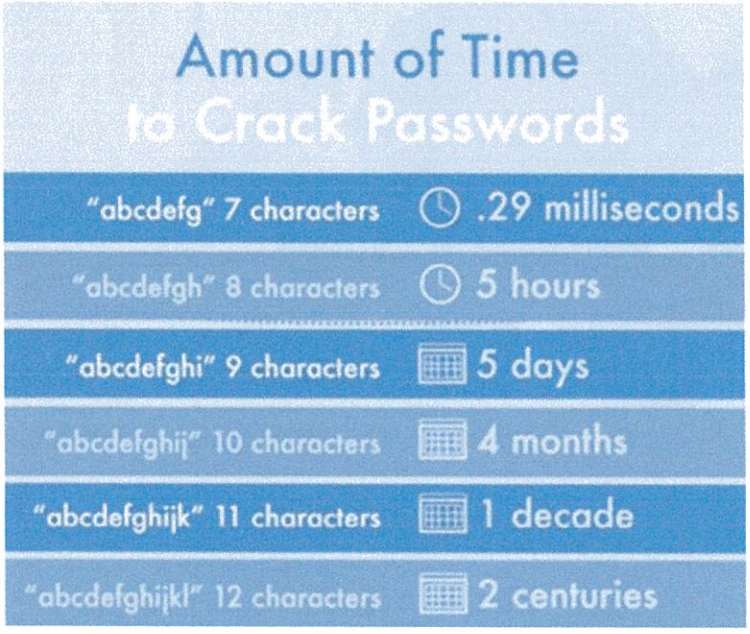
๑.๓ ควรติดตั้ง Anti-Malware และ Update สม่ำเสมอ

๑.๔ มีการ Update Patch ของระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๑.๕ มีการ Update Version ของโปรแกรม อย่างสม่ำเสมอ

๑.๖ ไม่ควรจด Password ไว้ที่หน้าจอและไม่ควรบอกกับคนอื่น

*** Password ควรมีความยาวอย่างน้อย ๘ ตัวอักษร



๒. E-mail

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๒.๑ ไม่เปิด E-mail ที่น่าสงสัย

๒.๒ ไม่เปิดแนบไฟล์จาก E-mail ที่น่าสงสัย

๒.๓ ไม่คลิก Link ใน E-mail โดยไม่มีการเช็ค

๒.๔ การทำธุรกรรมต่างๆ ควรมีการเช็คผ่านช่องทางอื่นๆ เพิ่มเติม

๓. Webside

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๓.๑ ไม่เข้าเว็บฯ ที่ได้รับจากช่องทางที่ไม่แน่ชัด

๓.๒ ไม่ควรบันทึก Password บน Browser

๓.๓ เว็บฯ ธุรกรรมการเงินต้องมี SSL ผ่าน HTTPS เท่านั้น

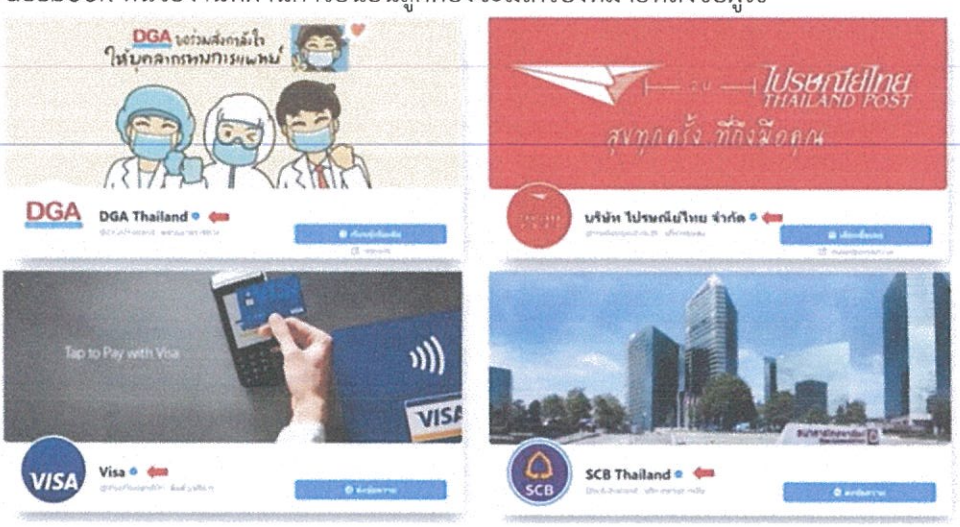
๓.๔ ใช้ Browser ที่ผู้ใช้งานนิยมใช้ เช่น Google Chrome Mozilla Firefox

๓.๕ มีการ Update Version Browser สม่ำเสมอ

๓.๖ ในกรณีคอมพิวเตอร์ไม่ใช่เครื่องส่วนตัวควรใช้ Browser Safe Web Browsing

๓.๗ ติดตั้ง Anti-Virus และ Update สม่ำเสมอ

*** Facebook หน่วยงานที่ผ่านการยืนยันถูกต้องจะมีเครื่องหมายหลังชื่อผู้ใช้



๔. Messaging

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย / Line

๔.๑ ไม่ควรบันทึก Password ไว้ที่โปรแกรม

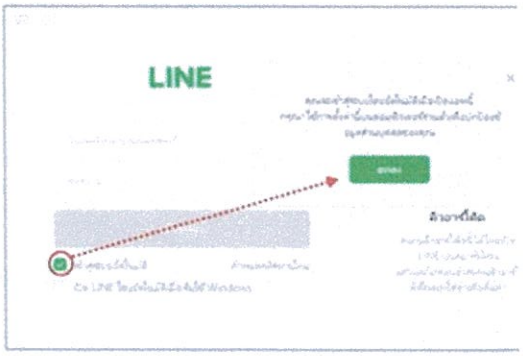
๔.๒ กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ควรบันทึกไฟล์ต่างๆไว้บนเครื่อง

๔.๓ มีความตระหนักก่อนเปิด Link ที่ได้รับมา

๔.๔ มีการ Update Version สม่ำเสมอ

เข้าใช้งานโดย QR

ห้ามบันทึกรหัสผ่านไว้



๕. Fake News คือข่าวปลอมเป็นภัยคุกคามที่มีความน่ากลัวอย่างมากเนื่องจากมีการนำเสนอที่ดูมีความน่าเชื่อถือทำให้เกิดการหลงเชื่อ วิธีสังเกตข่าวปลอม จะมีการพาดหัวข่าวที่เกินจริง ระบุแหล่งข่าวไม่ได้ ระบุวันที่และเหตุการณ์ไม่ได้ และสำนวนการเขียนจะเป็นแนวการโฆษณา

๖. Conference การประชุมทางไกลผู้ที่เข้าประชุมควรมีแต่ผู้ที่เกี่ยวข้อง การแชร์เอกสารมีความระมัดระวัง ใช้โปรแกรมปกติทั่วไป และมีการ Update โปรแกรมอย่างสม่ำเสมอ

๗. Cloud Storage คือ การนำข้อมูลไปจัดเก็บไว้บนเซิร์ฟเวอร์ของผู้ให้บริการ ที่เรียกว่า Host จุดเด่นสำคัญของ Cloud Storage คือการที่เราทำการจัดเก็บข้อมูลไว้เช่นเดียวกับที่เก็บในฮาร์ดไดรฟ์ , , SSD หรือ Storage ส่วนตัวอื่นๆ แต่สามารถเรียกใช้ หรือเข้าถึงข้อมูลต่างๆ ได้ง่ายดายผ่านเครือข่ายอินเตอร์เน็ต สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ควรแยก User ในการใช้งานแต่ละคน และกำหนดผู้เข้าถึงข้อมูลที่จำเป็นเท่านั้น มีการติดตั้ง Anti-Malware และ Update สม่ำเสมอ มีการตั้ง Password ที่ดี และไม่บอกคนอื่น

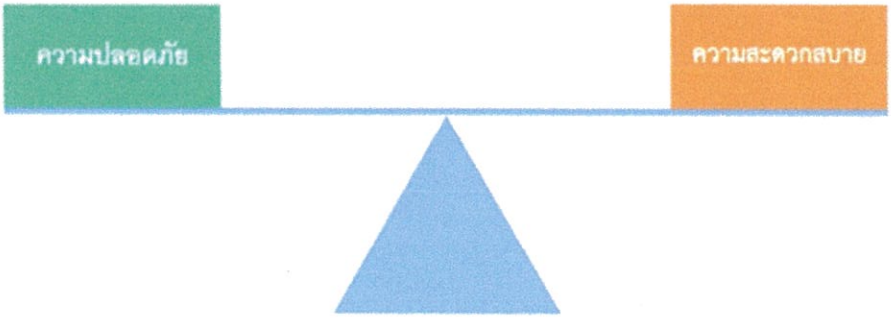
๘. Free WiFi สิ่งควรปฏิบัติ ไม่ควรใช้งาน Wifi ที่เปิดใช้บริการแบบไม่มีรหัสผ่าน หรือไม่รู้ที่มาในการให้บริการ

๙. Mobile โทรศัพท์มือถือ สิ่งที่ควรปฏิบัติ เปิดใช้งาน PIN/Password, Face scan Fingerprint ในการใช้งานอุปกรณ์ ไม่ติดตั้ง Application ที่น่าสงสัย และกำหนด Application permission ให้เหมาะสม มีการ Update Path ระบบปฏิบัติการ (OS) และ Update Version โปรแกรมอย่างสม่ำเสมอ ** ระวังอย่าหลงเชื่อ SMS หลอกลวง

๑๐. Internet Connection สิ่งที่ควรปฏิบัติคือ ควรเปลี่ยน Default Password ที่มาจากโรงงาน เปลี่ยน SSID และรหัสผ่านของ Wifi ที่กำหนดมาจากผู้ให้บริการ กำหนดที่สามารถใช้งานเท่าที่จำเป็น

๑๑. IoT Device คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเตอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่างๆหรือ Application ต่างๆ เช่น หลอดไฟ พัดลม

สรุป การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ คือ ความสมดุลระหว่างความปลอดภัยกับความสะดวกสบาย



ส่วนที่ ๒ ประโยชน์ที่ได้รับจากการอบรม

มีความตระหนักรู้ด้านความมั่นคงทางไซเบอร์เกี่ยวกับภัยคุกคามทางไซเบอร์ ความเสี่ยง และแนวทางปฏิบัติที่ดีที่สุดในการปกป้องข้อมูลส่วนบุคคลและองค์กร

ส่วนที่ ๓ การนำไปใช้ประโยชน์

๑. สามารถสังเกต ระมัดระวัง และป้องกันอันตรายที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

๒. การลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์

๓. เพิ่มประสิทธิภาพการทำงาน ก่อให้เกิดประสิทธิภาพ ในการจัดการข้อมูลขององค์กร

DGA
DIGITAL GOVERNMENT DEVELOPMENT AGENCY

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ นิภารัตน์ ตระกูลพงษ์

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 18 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

23492172

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-18T21:15:05.191+07:00