การอบรมหลักสูตร e-Learning ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
หลักสูตร TDGA e-Learning จำนวน ๑ เรื่อง ดังนี้

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

หลักสูตรนี้เป็นการเรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

๑.๑ วัตถุประสงค์

๑.๑.๑ เพื่อสร้างความตระหนักรู้ (To Raise Awareness)
๑.๑.๒ เพื่อปกป้องทรัพย์สินดิจิทัล (To Protect Digital Assets)
๑.๑.๓ เพื่อสร้างระบบป้องกันที่ยั่งยืน (To Establish Defensive Habits)
๑.๑.๔ เพื่อรักษาความต่อเนื่องของชีวิตและธุรกิจ (To Ensure Continuity)
๑.๑.๕ เพื่อให้ผู้เรียนมีทักษะการเรียนรู้ตลอดชีวิต

๑.๒ สรุปบทเรียน

๑) Cybersecurity คืออะไร

Cybersecurity หรือ **ความมั่นคงปลอดภัยทางไซเบอร์** คือ การฝึกฝนและชุดของเครื่องมือที่ใช้เพื่อปกป้องระบบ เครือข่าย อุปกรณ์ และข้อมูลจากการโจมตีทางดิจิทัล (Cyberattacks) โดยมีเป้าหมายหลักคือการรักษาความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล

ในยุคปัจจุบันที่ทุกอย่างเชื่อมต่อกับอินเทอร์เน็ต Cybersecurity ไม่ใช่เรื่องไกลตัว แต่เป็นเกราะป้องกันที่ช่วยไม่ให้ข้อมูลส่วนตัวหรือความลับทางธุรกิจถูกขโมยไป

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

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

๒) ความรู้พื้นฐานของ Cybersecurity

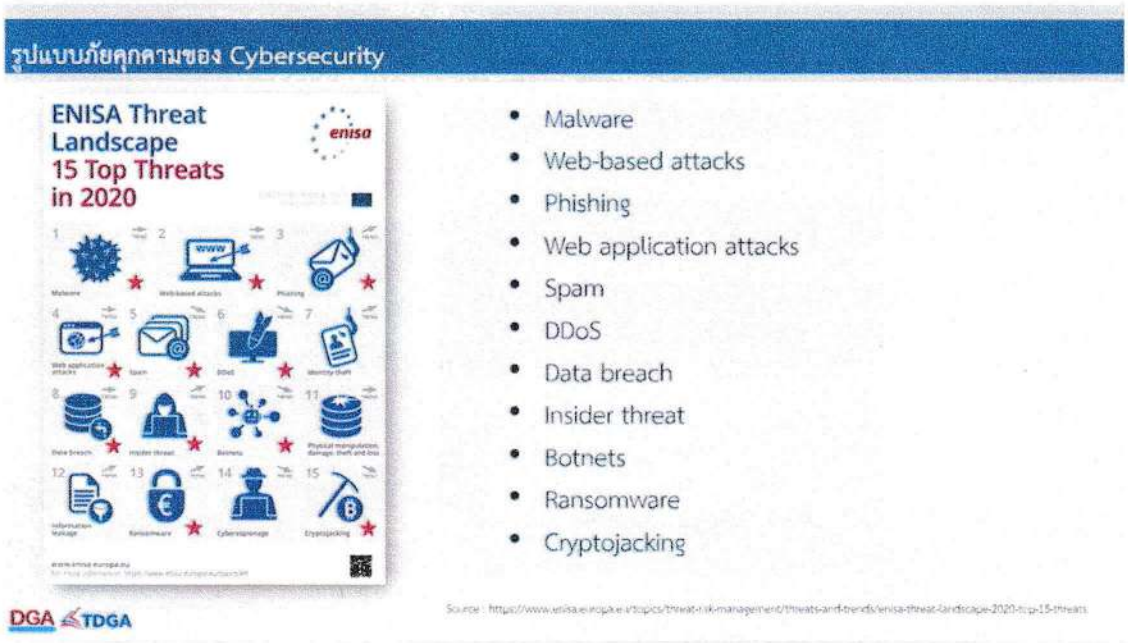
สำหรับพื้นฐานของ Cybersecurity นั้น ไม่ได้มีแค่เรื่องการตั้งรหัสผ่าน แต่เป็นระบบนิเวศขนาดใหญ่ที่ผสมผสานระหว่าง เทคโนโลยี (Technology), กระบวนการ (Process) และ คน (People) เข้าด้วยกัน

1. เสาหลัก 3 ประการ (The CIA Triad)

นี่คือเข็มทิศของนักความปลอดภัยไซเบอร์ทุกคน หากส่วนใดส่วนหนึ่งขาดไป ระบบจะถือว่าไม่ปลอดภัยทันที

- **Confidentiality (การรักษาความลับ):** ข้อมูลต้องถูกเห็นโดยผู้ที่มีสิทธิ์เท่านั้น (เช่น การทำ Encryption หรือการใส่รหัสไฟล์)
- **Integrity (ความถูกต้องของข้อมูล):** ข้อมูลต้องไม่ถูกแก้ไขระหว่างทาง หรือถ้าถูกแก้ ต้องตรวจสอบได้ (เช่น การใช้ Digital Signature)
- **Availability (ความพร้อมใช้งาน):** ระบบต้องใช้งานได้ตลอดเวลาที่ต้องการ (เช่น การป้องกันการโดนยิงเว็บหรือ DDoS)

2. ประเภทของภัยคุกคาม (Common Threats)



- **Malware (ซอฟต์แวร์ประสงค์ร้าย):** Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงเฮิร์ฟเวอร์ต่างๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง ไวรัส(Virus), เวิร์ม (Worms), โทรจัน(Trojans)
- **Web-based attacks** คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware
- **Phishing** คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม
- **Web application attacks** คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น
    - Code ของเว็บไซต์ เช่น CMS
    - Web Server หรือ Database Server
    - วิธีการโจมตีที่นิยมใช้
    - Cross-Site Scripting
    - SQL Injection
    - Path Traversal
- **Spam** คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับเช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน
- **DDos (Distributed Denial of Service)** คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม
- **Data breach** คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ
    - ผลกระทบ
    - ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
    - ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
    - สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

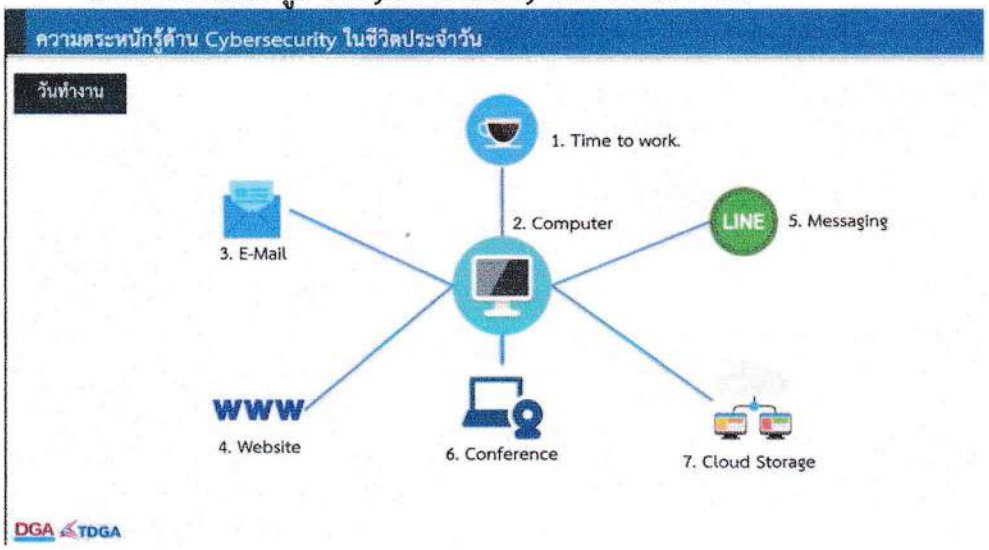
- **Insider threat** คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง
- **Botnets หรือ Robot Network** คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)
- **Ransomware** คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่าน ที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง วิธีการป้องกัน
    - สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล
    - ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
    - ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิด

- **Cryptojacking** คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวณผลเพื่อสร้างรายได้กลับไปที่ Hacker

DGA TDGA

Source : https://www.dga.or.th/document-sharing/infographic/36181/

๓.ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน



- Computer
  - สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

    ๑. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล

    ๒. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์ควรติดตั้ง 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 (! @ S #)
    ๒. มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร
    ๓. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, ๑๒๓๔๕๖, วันเกิด, หมายเลขโทรศัพท์
    ๔. มีการเปลี่ยน Password อย่างสม่ำเสมอ
    ๕. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
    ๖. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
    ๗. ไม่ควรบอก Password แก่ผู้อื่น

- E-mail
  - สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย
    ๑. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
    ๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
    ๓.ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค
    ๔.เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

- Website

- สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย
  ๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ
  ๒. ไม่ควรทำการบันทึก Password ต่างๆ บน Browser
  ๓.เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
  ๔.ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น
  ๕. ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ
  ๖. ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing
  ๗. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

- **Messaging**
  - สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย
    ๑.ไม่ควรบันทึก Password ไว้ที่โปรแกรม
    ๒.กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
    ๓. มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา
    ๔. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

- **Fake News**

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

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

- Line Official Account

- Conference
  - สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

    ๑.ใช้สถานที่เหมาะสมกับการ Conference

    ๒.ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง

    ๓.แชร์เอกสารต่างๆ อย่างระมัดระวัง

    ๔. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน

    ๕. มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

- Cloud Storage
  - สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

    ๑. แยก User ในการใช้งานของแต่ละบุคคล

    ๒. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น

    ๓. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น

    ๔. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

    ๕. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ
  - ๖. มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

ลงนาม.....

(นางสาววาทินี ขัดทองงาม)

เจ้าพนักงานการเกษตรปฏิบัติงาน

ลงนาม.....

(นายไลซันต์ ตั้งภูมิ)

ตำแหน่ง ผู้อำนวยการสถานีพัฒนาที่ดินชัยภูมิ

รับรองผลการพัฒนาความรู้

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ วาทินี ขัดทองงาม

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 23 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

448b3041

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
Date: 2026-03-04T15:04:02.065+07:00