# การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness

โดย นางสาวปนัสยา พวงสมบัติ
เจ้าพนักงานธุรการปฏิบัติงาน

**วัตถุประสงค์**

๑. เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
๒. เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆ และแนวทางป้องกันแก้ไข
๓. เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

**เนื้อหา**

**Cybersecurity คืออะไร**

Cybersecurity หรือความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี กระบวนการ และวิธีปฏิบัติที่ออกแบบเพื่อป้องกันและรับมือการโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานระบบสารสนเทศ หรือโปรแกรมที่อาจจะเกิดความเสียหาย จากการเข้าถึงของผู้ที่ไม่ได้รับอนุญาต

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ได้แก่

๑. พระราชบัญญัติการรักษาความมั่นคงความปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๒. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐
๓. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
๔. มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

**ความรู้พื้นฐานของ Cybersecurity**

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ หรือ CIA Triad ประกอบด้วย

C = Confidentiality หรือการรักษาความลับของข้อมูล คือการที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับชั้นของความลับที่กำหนดไว้

I = Integrity หรือการรักษาความถูกต้องของข้อมูล คือการระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างสม่ำเสมอ

A = Availability หรือความพร้อมใช้งานของข้อมูล คือการที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา มีความต่อเนื่องในการให้บริการข้อมูล

**รูปแบบภัยคุกคามของ Cybersecurity** มีทั้งหมด ๑๑ รูปแบบ

๑. Malware หรือซอฟต์แวร์ หรือ Code ประเภทหนึ่งเมื่อถูกติดตั้ง หรือเปิดระบบคอมพิวเตอร์จะทำให้มัลแวร์เข้าถึงทรัพยากรของระบบคอมพิวเตอร์ ทำให้ส่งผลกระทบต่อคอมพิวเตอร์ มัลแวร์นั้นจะครอบคลุมอยู่ด้วยกันทั้งหมด ๓ ประเภท

๑) ไวรัส (Virus)
๒) เวิร์ม (Worms)
๓) โทรจิน (Trojans)

๒. Web-Based attacks คือ การโจมตีผ่านทางเว็บไซต์โดยการแฮ็ก หรือทำให้เว็บไซต์มีช่องโหว่ เมื่อกดเข้าไปแล้วจะทำให้คอมพิวเตอร์ติดมัลแวร์ เว็บไซต์ส่วนใหญ่ที่จะโดนแฮ็คหรือแก้โค้ดเป็นเว็บไซต์ประเภท CMS หรือ Content Management System

๓. Phishing คือ การโจมตีผ่านช่องทาง email, SMS, website และ social หลอกล่อ โดยทำให้หลงเชื่อและให้ข้อมูลส่วนบุคคลเช่น username หรือ password

๔. Web application attacks คือ การโจมตีโดยอาศัยช่องโหว่ต่าง ๆ เช่น Code ของเว็บไซต์ เซิร์ฟเวอร์ หรือ Database Server

๕. Spam คือ การโจมตีผ่านการส่งข้อมูลข้อความโฆษณาต่าง ๆ ไปทาง email, SMS, website และ social เป็นจำนวนมากเพื่อสร้างความรำคาญหรือก่อกวนแก่ผู้ที่ได้รับ

๖. DDos คือ การโจมตีระบบเว็บไซต์ ระบบการให้บริการ และระบบเครือข่าย เพื่อทำให้ระบบล่ม ใช้งานไม่ได้

๗. Data breach คือ การโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ แอพพลิเคชั่น และระบบบริการต่าง ๆ โดยเจ้าของข้อมูลไม่ทราบหรือไม่รู้ตัว เพื่อนำไปขายหรือเรียกค่าไถ่ ทำให้เกิดผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

๘. Insider threat คือ ภัยที่เกิดจากบุคลากรภายในองค์กร อาจจะเกิดโดยที่ตั้งใจหรือไม่ได้ตั้งใจ โดยผ่านทางเว็บไซต์ที่ใช้งานโดยปกติของบุคลากร สาเหตุที่เกิดส่วนใหญ่เนื่องจากระบบภายในองค์กรอาจมีการป้องกันระบบเครือข่ายคอมพิวเตอร์ต่ำ

๙. Botnets หรือ Robot network คือ โปรแกรมที่ถูกเขียนขึ้นโดยอาจแอบแฝงมาพร้อมกับโปรแกรมในคอมพิวเตอร์และอุปกรณ์ต่าง ๆ โปรแกรมไม่ได้ทำงานตลอดเวลาแต่จะทำงานก็ต่อเมื่อถูกเรียกใช้จากผู้ที่เขียนโปรแกรม

๑๐. Ransomware คือ มันแวร์ที่ถูกติดตั้งลงในเครื่องแล้วจะทำการล็อกไฟล์ โดยจะเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่องคอมพิวเตอร์ จุดประสงค์ส่วนใหญ่เพื่อทำการเรียกค่าไถ่รหัสผ่าน

๑๑. Crytojacking คือ การแฮ็กเกอร์ เข้าเครื่องคอมพิวเตอร์แอบติดตั้งโปรแกรม เพื่อขุดเหรียญโดยอาศัย CPU หรือGPU เพื่อสร้างรายได้กลับไปยังแฮกเกอร์

**ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน แบ่งเป็นสองวัน คือวันทำงานและวันพักผ่อน**

วันทำงานประกอบไปด้วย

๑. คอมพิวเตอร์

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ ควรมีการแยก user การใช้งานของแต่ละคน และควรล็อกเอาท์เมื่อไม่ได้อยู่หน้าเครื่องคอม ติดตั้งแอนติมัลแวร์และมีการอัพเดทแพท และเวอร์ชั่นอย่างสม่ำเสมอ ไม่ควรจดพาสเวิร์ดและติดพาสเวิร์ดไว้ที่หน้าจอไม่ควรบอกพาสเวิร์ดผู้อื่นมีการใช้พาสเวิร์ดที่ดี

พาสเวิร์ดที่ดี คือ ต้องมีความซับซ้อน เช่น มีตัวอักษรเล็ก-ใหญ่ ตัวเลข หรืออักขระพิเศษ มีความยาวอย่างน้อย ๘ ตัวอักษร ไม่ควรใช้พาสเวิร์ดที่สามารถคาดเดาได้ง่าย เช่น วันเกิดหรือเบอร์โทรศัพท์ ควรเปลี่ยนพาสเวิร์ดอย่างสม่ำเสมอ ไม่ควรใช้พาสเวิร์ดซ้ำกันในแต่ละระบบ

๒. อีเมล

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ ไม่เปิดอีเมล เปิดไฟล์หรือคลิกลิงค์ ที่น่าสงสัยหรือผู้ส่งที่ไม่ชัดเจน เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านช่องทางอื่น ๆ เพิ่มเติม

๓. Website

สิ่งที่ควรปฏิบัติปฏิบัติเพื่อความปลอดภัย คือ ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่ชัดเจน ไม่ควรบันทึกรหัสผ่านต่าง ๆ บนเว็บไซต์ สำหรับทำธุรกรรมที่สำคัญจะต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น ใช้เบราว์เซอร์ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome เป็นต้น ควรมีการอัพเดทเวอร์ชั่นของเบราเซอร์ ถ้าเกิดว่าไม่ได้ใช้เครื่องคอมพิวเตอร์ส่วนตัวควรใช้เบราเซอร์ในโหมด Save web browser ควรติดตั้งแอนตี้มัลแวร์ และอัพเดทอย่างสม่ำเสมอ

๔. Messaging

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ ไม่ควรบันทึก password ไว้ที่โปรแกรม กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ควรบันทึกไฟล์ต่างๆไว้บนเครื่อง มีความตระหนักก่อนเปิดลิงค์หรือไฟล์ต่าง ๆ ที่ได้รับมา ไม่ควรแชร์ข้อมูลข่าวสารต่าง ๆ โดยไม่ทราบที่มาของข้อมูล และมีการอัพเดทเวอร์ชั่นของโปรแกรมสม่ำเสมอ

๕. conference

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ การใช้สถานที่ให้เหมาะกับการ conference การประชุมควรมีแต่ผู้ที่เกี่ยวข้องเข้าร่วม และแชร์เอกสารต่าง ๆ อย่างระมัดระวัง ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน มีการอัพเดทเวอร์ชั่นของโปรแกรม conference อย่างสม่ำเสมอ และควรให้มีการขออนุญาตผู้เข้าร่วมประชุมก่อนที่จะบันทึกภาพและเสียงในที่ประชุม

๖. Cloud Storage

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ แยก user ในการใช้งานของแต่ละบุคคล และควรกำหนดผู้เข้าถึงไฟล์เท่าที่จำเป็นเท่านั้น ควรปิดการเข้าถึงหรือปิดการแชร์ไฟล์เมื่อไม่จำเป็น ควรติดตั้งแอนติมัลแวร์ มีการอัพเดทเวอร์ชั่นอย่างสม่ำเสมอ

<u>วันพักผ่อนประกอบไปด้วย</u>

๑. คอมพิวเตอร์ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ควรมีการแยก User การใช้งานของแต่ละบุคคล ควรล็อกเอาท์เมื่อไม่อยู่หน้าจอ ติดตั้งแอนติมัลแวร์ และอัพเดทเวอร์ชั่นอยู่สม่ำเสมอ ไม่ควรจดพาสเวิร์ดหรือติดพาสเวิร์ดไว้ที่จอ มีการใช้พาสเวิร์ดที่ดีและไม่บอกพาสเวิร์ดแก่ผู้อื่น

๒. Free Wi-Fi สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือไม่ควรใช้งาน Wi-Fi ที่เปิดให้บริการแบบไม่มีรหัสผ่าน หลีกเลี่ยงการใช้งาน Wi-Fi ที่ไม่รู้จักที่ใช้บริการ

๓. Mobile สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ ให้เปิดใช้งาน Pin /Password, Face scan, หรือ Fingerprint เข้าใช้งานอุปกรณ์ ไม่ติดตั้งแอพพลิเคชั่นที่น่าสงสัยไม่รู้แหล่งที่มา มีการอัพเดทเวอร์ชั่นของโปรแกรมอยู่แบบเสมอ

๔. Internet Connection สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ เปลี่ยน default password ของ Router ที่มาจากโรงงานเปลี่ยน SSID และรหัสผ่านของ Wi-Fi ที่กำหนดมาจากผู้ให้บริการและกำหนดผู้ที่สามารถเข้าใช้งานอินเตอร์เน็ตเท่าที่จำเป็น

๕. IOT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อเครือข่ายอินเทอร์เน็ต เพื่อใช้งานกับระบบต่าง ๆ หรือแอพพลิเคชั่นต่าง ๆ เช่น หลอดไฟ พัดลม หรือเครื่องกรองอากาศ จะต้องมีความปลอดภัยทางด้านเครือข่ายเปรียบได้กับเป็นคอมพิวเตอร์ขนาดเล็กที่ใช้ควบคุมอุปกรณ์อิเล็กทรอนิกส์

**การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน**

สามารถนำความรู้ความรู้ความเข้าใจในการจัดเก็บข้อมูลและลำดับการใช้ข้อมูลมาประยุกต์ใช้ในการปฏิบัติงานเพื่อให้ข้อมูลถูกเก็บเป็นสัดส่วนและสามารถเข้าถึงได้ตามความสำคัญของข้อมูลนั้น ๆ เพื่อป้องกันการเข้าถึงข้อมูลของไวรัส หรือมัลแวร์ที่อาจจะเข้าแอบแฝงมากับเครื่องคอมพิวเตอร์ เพื่อความปลอดภัยของข้อมูลในการปฏิบัติงาน

**ประโยชน์ที่ได้รับ**

**- ต่อตนเอง**

๑. ได้รับความรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ และข้อควรระวังเบื้องต้นในการใช้โปรแกรมต่างๆ

๒. ได้รับความรู้เกี่ยวกับมัลแวร์ และการป้องกันคอมพิวเตอร์เบื้องต้น

**- ต่อองค์กร** สามารถนำความรู้ความเข้าใจเกี่ยวกับมัลแวร์ต่าง ๆ การป้องกัน และแก้ไขคอมพิวเตอร์เบื้องต้น เพื่อให้ไม่ถูกโจมตีทางคอมพิวเตอร์

**- ต่อสาธารณะ** สามารถนำความรู้ความเข้าใจที่ได้รับไปเผยแพร่ หรืออธิบาย หรือทำความเข้าใจเกี่ยวกับภัยที่แอบแฝงมาจากการใช้คอมพิวเตอร์ และวิธีการป้องกัน หรือข้อควรระวังที่สามารถใช้คอมพิวเตอร์และอินเตอร์เน็ตได้อย่างปลอดภัย

**แหล่งที่มา**

**หลักสูตร :** การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness

**บรรยายโดย :** คุณพลากร ลาภอลงกรณ์ ผู้จัดการส่วนบริการลูกค้า ฝ่ายปฏิบัติการ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

**สถาบัน/หน่วยงาน/ระบบ :** สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

**รูปแบบหลักสูตร :** TDGA E-Learning

**ช่วงเวลาการฝึกอบรม :** สิงหาคม ๒๕๖๗