การพัฒนาทางไกลด้วยระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ (TDGA E-Training)
สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness

รอบ ๑/๒๕๖๖ ตุลาคม ๒๕๖๕-มีนาคม ๒๕๖๖
นายประมุข ถิ่นใหญ่ ตำแหน่งนักสำรวจดินชำนาญการพิเศษ
กลุ่มวางแผนการใช้ที่ดิน สำนักงานพัฒนาที่ดินเขต ๑๑

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

เป็นการเรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

วัตถุประสงค์

๑. เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
๒. เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆ และแนวทางป้องกันแก้ไข
๓. เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

๑. Cybersecurity คืออะไร
๒. รูปแบบภัยคุกคามของ Cybersecurity
๓. ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

Cybersecurity คืออะไร

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑

รูปแบบภัยคุกคามของ Cybersecurity

ตัวอย่างรูปแบบภัยคุกคาม เช่น Malware, Web-based attacks, Phishing, Web application attacks, Span, DDoS, Data breach, Insider threat, Botnets, Ransomware, Cryptojacking

Malware คือ ซอฟต์แวร์หรือCode ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นในเครือข่ายรวมถึงเซิร์ฟเวอร์ต่างๆได้ โดยพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง ไวรัส (Virus) เวิร์ม (Worms) โทรจัน (Trojans)

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้วจะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malwaer ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

Web application attacks คือ วิธีโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น Code ของเว็บไซต์ เช่น CMS Web Server หรือ Database Server

Span คือ วิธีการที่ผู้ส่งหรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความ หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail SMS เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญหรือก่อกวน

DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ ระบบการให้บริการหรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์ ระบบการให้บริการหรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่หรือการโจมตีเพื่อขโมยข้อมูลเว็บไซต์ ข้อมูลของแอปพลิเคชันหรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชันหรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัทหรือสมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่ายและผลลัพธ์ของภัยนี้มีความรุนแรง

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์

Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง สามารถป้องกัน โดนการสำรองข้อมูลเป็นประจำ ทำการแยกเก็บไฟล์สำรองข้อมูล ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมาควรมีความตระหนักก่อนที่จะทำการเปิด

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

ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

Computer ควรแยก User ใช้งานกันของแต่ละบุคคล, Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์, ติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ, มีการ Update Patch ระบบปฏิบัติการ OS อย่างสม่ำเสมอ, มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ และไม่ควรจด Password

Password ที่ดี คือ ต้องมีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ # ฿) มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, ๑๒๓๔๕๖, วันเกิด, หมายเลขโทรศัพท์ เป็นต้น ควรมีการเปลี่ยน Password อย่างสม่ำเสมอ ใช้ Multi Authentication ในกรณีที่สามารถใช้งานได้ ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

E-mail ไม่เปิด E-mail และไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน ไม่คลิก Link ใน E-mail โดยไม่มีการตรวจเช็ค และเรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆเพิ่มเติม

Website ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ ไม่ควรทำการบันทึก Password ต่างๆ บน Browser ควรใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งานเท่านั้น เช่น Google Chrome, Mozilla Firefox เป็นต้น Update Version ของ Browser อย่างสม่ำเสมอ ติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ ในกรณีทำงานที่ไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing และเว็บไซต์สำหรับทำธุรกรรมที่สำคัญหรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น

Messaging ไม่ควรบันทึก Password ไว้ที่โปรแกรม มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล ไม่ควรบันทึกไฟล์ต่างๆไว้บนเครื่องที่ไม่ใช่เครื่องส่วนตัว Update Version ของโปรแกรมอย่างสม่ำเสมอ

Fake News หรือข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีน่ากลัวอย่างมาก เนื่องจากข่าวปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือ ซึ่งทำให้ผู้รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น สังเกตจาก ระบุที่มาของข่าวไม่ได้ มีการพาดหัวข่าวหรือข้อความที่เกินจริงเพื่อสร้างความน่าสนใจ มักไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์ สำนวนการเขียนออกแนวการโฆษณา

Conference ใช้สถานที่เหมาะสมกับการ Conference การประชุมควรมีแต่ผู้ที่เกี่ยวข้อง แชร์เอกสารต่างๆอย่างระมัดระวัง ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

Cloud Storage ควรแยก User ในการใช้งานของแต่ละบุคคล ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น ปิดการเข้าถึงไฟล์หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น ควรมีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น ติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ Update Version ของโปรแกรมอย่างสม่ำเสมอ

Mobile เปิดการใช้งาน PIN/Password Face scan หรือ Fingerprint ในการใช้งานอุปกรณ์ ไม่ติดตั้ง Application ที่ไม่รู้แหล่งที่มา มีการ update Patch ระบบปฏิบัติการ OS อย่างสม่ำเสมอ และ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

ประมุข ถิ่นใหญ่

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

Cybersecurity Awareness

รวมระยะเวลาทั้งสิ้น 1 : 30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 22 ก.พ. 2566

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

f7aaa721

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล(องค์การมหาชน) (สพร.)
Digital Government Development Agency (Public Organization) (DGA)
Date: 2023-02-22T18:17:05.284+07:00