

แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๒
รอบการประเมินที่ ๒/ ๒๕๖๙ ตั้งแต่วันที่ ๑ เมษายน – ๓๐ กันยายน ๒๕๖๙
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ชื่อ-นามสกุล นางสาววิลาวัลย์ เรียนเวช ตำแหน่ง นักวิชาการเกษตรชำนาญการ
หน่วยงาน ศูนย์ศึกษาการพัฒนาเขาหินซ้อนอันเนื่องมาจากพระราชดำริ
หัวข้อการพัฒนา การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์
วิธีการพัฒนา การฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์
วันที่พัฒนา ๒๐ สิงหาคม ๒๕๖๙ สถานที่ ศูนย์ศึกษาการพัฒนาเขาหินซ้อนฯ
หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA)
วัตถุประสงค์

เพื่อเป็นการสร้างการเรียนรู้ ด้านความมั่นคงปลอดภัยทางไซเบอร์ (cybersecurity) ระดับต้น (Beginner) จนถึงระดับกลาง (Intermediate) ที่ต้องการดูแลรักษาและการป้องกัน อารมณ์ซึ่ง การรักษา ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความสมบูรณ์พร้อมใช้ (Availability) เพื่อให้ระบบ บริการ ผลิตภัณฑ์ มีความมั่นคงปลอดภัย และสามารถป้องกัน รับมือ ภัยคุกคามที่เกิดจากความ มั่นคงปลอดภัยทางไซเบอร์ หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือโอกาสที่จะทำให้เกิดข้อผิดพลาด การสูญเสีย ที่ จะเกิดขึ้นต่อระบบ บริการ ผลิตภัณฑ์

สรุปสาระสำคัญ

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) คือ การใช้เทคโนโลยี เครื่องมือ และกระบวนการ เพื่อป้องกันข้อมูล ระบบเครือข่าย อุปกรณ์ และโปรแกรมจากภัยคุกคามหรือการเข้าถึงโดยไม่ได้รับอนุญาต รวมถึงการเตรียมพร้อมรับมือและแก้ไขเหตุการณ์ เพื่อลดความเสี่ยงและความเสียหายต่อองค์กร มีกฎหมาย และมาตรฐานที่เกี่ยวข้อง ได้แก่

๑. พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ – กำหนดแนวทางป้องกันและรับมือภัย คุกคามไซเบอร์
๒. พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ – กำหนดความผิดเกี่ยวกับการใช้ หรือเข้าถึงระบบและข้อมูลโดยมิชอบ
๓. พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ – กำหนดหลักเกณฑ์การเก็บ ใช้ เผย และรักษา ความปลอดภัยข้อมูลส่วนบุคคล
๔. ISO/IEC ๒๗๐๐๑ – มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อบริหารความ เสี่ยงและปกป้องข้อมูลอย่างเป็นระบบ

CIA Triad หรือ CIA Model เป็นหลักการพื้นฐานในการรักษาความมั่นคงปลอดภัยของข้อมูล ประกอบด้วย ๓ องค์ประกอบสำคัญ ได้แก่

C – Confidentiality (การรักษาความลับของข้อมูล) มุ่งป้องกันไม่ให้ผู้ที่ไม่สิทธิสามารถเข้าถึงข้อมูล โดยกำหนดสิทธิและระดับการเข้าถึงข้อมูลให้เหมาะสมกับผู้ใช้งานและระดับชั้นความลับของข้อมูล

I – Integrity (การรักษาความถูกต้องครบถ้วนของข้อมูล) มุ่งให้ข้อมูลมีความถูกต้อง ครบถ้วน และไม่ ถูกแก้ไขหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต รวมถึงกำหนดสิทธิในการแก้ไขข้อมูลเฉพาะผู้ที่ได้รับอนุญาต

A – Availability (การรักษาความพร้อมใช้งานของข้อมูล) มุ่งให้ระบบและข้อมูลสามารถเข้าถึงและใช้งานได้อย่างต่อเนื่องเมื่อผู้มีสิทธิต้องการใช้งาน รวมถึงมีการเตรียมระบบสำรองและแนวทางรับมือเมื่อเกิดเหตุขัดข้องหรือภัยคุกคาม

รูปแบบภัยคุกคามทางไซเบอร์ ภัยคุกคามทางไซเบอร์มีหลายรูปแบบและมีวิธีการโจมตีที่แตกต่างกัน ผู้ใช้งานควรรู้จักลักษณะภัยคุกคาม เพื่อป้องกันและรับมือได้อย่างเหมาะสม โดยรูปแบบที่พบบ่อย ได้แก่

๑. Malware (มัลแวร์) ซอฟต์แวร์หรือชุดคำสั่งที่ใช้ทำลายระบบ ขโมยข้อมูล หรือเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

๒. Web-based Attacks (การโจมตีผ่านเว็บไซต์) การโจมตีผ่านเว็บไซต์ เช่น การเจาะระบบเว็บไซต์ที่มีช่องโหว่และแทรกชุดคำสั่งที่เป็นอันตราย เมื่อผู้ใช้งานเข้าชมเว็บไซต์ดังกล่าว อาจถูกเปลี่ยนเส้นทางไปยังเว็บไซต์ที่มี Malware หรือถูกหลอกให้ดาวน์โหลดไฟล์อันตราย

๓. Phishing (ฟิชซิง) การหลอกผ่านอีเมล SMS เว็บไซต์ หรือสื่อสังคมออนไลน์ เพื่อขโมยรหัสผ่าน ข้อมูลส่วนบุคคล หรือข้อมูลสำคัญ

๔. Web Application Attacks (การโจมตีเว็บแอปพลิเคชัน) การใช้ช่องโหว่ของเว็บไซต์หรือเว็บแอปพลิเคชันเพื่อเข้าถึงหรือแก้ไขข้อมูล หรือทำให้ระบบผิดปกติ

๕. Spam (สแปม) การส่งข้อความหรืออีเมลจำนวนมากโดยไม่ได้รับอนุญาต ซึ่งอาจใช้เผยแพร่ Malware หรือหลอกลวง

๖. DDoS (Distributed Denial of Service) การส่งข้อมูลหรือคำขอจำนวนมากจากหลายอุปกรณ์ไปยังระบบเป้าหมาย จนระบบทำงานหนักและไม่สามารถให้บริการได้

๗. Data Breach (การรั่วไหลของข้อมูล) การเข้าถึง เปิดเผย หรือขโมยข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๘. Insider Threat ภัยจากบุคคลภายในองค์กร ทั้งจากความตั้งใจหรือความผิดพลาด เช่น เปิดเผยข้อมูลหรือใช้รหัสผ่านไม่ปลอดภัย

๙. Botnet (เครือข่ายคอมพิวเตอร์ที่ถูกควบคุม) เครือข่ายอุปกรณ์ที่ถูกติด Malware และผู้โจมตีสามารถควบคุมจากระยะไกลโดยเจ้าของไม่รู้ตัว

๑๐. Ransomware (แรนซัมแวร์) มัลแวร์ประเภทหนึ่งที่ใช้รหัสหรือล็อกไฟล์ในคอมพิวเตอร์ ทำให้ไม่สามารถเปิดหรือใช้งานข้อมูลได้ตามปกติ จากนั้นผู้โจมตีมักเรียก ransom เพื่อแลกกับการปลดล็อกหรือคืนข้อมูล

๑๑. Cryptojacking การแอบใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นเพื่อขุด Cryptocurrency ทำให้เครื่องช้าลง ใช้พลังงานมากขึ้น และอาจทำให้อุปกรณ์เสื่อมสภาพเร็วขึ้น

ความตระหนักรู้ด้าน Cyber security ในชีวิตประจำวัน

Computer สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

๑. ควรมีการแยก user ใช้งานกันของแต่ละบุคคล
๒. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
๓. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
๔. มีการอัปเดต Patch ระบบปฏิบัติการ (OS)
๕. มีการ Update Version ของโปรแกรมบนเครื่อง
๖. ไม่ควรจด password และติด password ไว้ที่หน้าจอ
๗. มีการใช้ password ที่มีความซับซ้อนและไม่ควรบอก password แก่ผู้อื่น

Password การใช้ Password ที่ดี คือ

๑. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ
๒. มีความยาวของ Password อย่างน้อย ๔ ตัวอักษร
๓. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่าย
๔. มีการเปลี่ยน Password อย่างสม่ำเสมอ
๕. ใช้ MultiFactor Authentication ในกรณีที่สามารถใช้งานได้
๖. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
๗. ไม่ควรบอก Password แก่ผู้อื่น

E-mail สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
๓. ไม่คลิกลิงก์ใน E-mail โดยไม่มีการตรวจเช็ค
๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ

Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง social ต่างๆ
๒. ไม่ควรทำการบันทึก Password ต่างๆบน Browser
๓. เว็บไซต์สำหรับการทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS
๔. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งานเช่น google chrome mozilla firefox เป็นต้น
๕. ควรมีการอัปเดตเวอร์ชันของ Browser อย่างสม่ำเสมอ
๖. ในกรณีที่เครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน browser ในโหมด safe web browsing
๗. ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ

Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรบันทึก password ไว้ที่โปรแกรม
๒. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
๓. มีความระมัดระวังก่อนเปิดลิงค์หรือไฟล์ต่างๆที่ได้รับมา
๔. มีการอัปเดตเวอร์ชันของโปรแกรมอย่างสม่ำเสมอ

แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับตนเอง

๑. ตรวจสอบข้อมูลก่อนแชร์ เพื่อป้องกันการเผยแพร่ข่าวสารหรือข้อมูลที่ไม่เป็นความจริง
๒. ติดตามข่าวสารด้านความปลอดภัยไซเบอร์ เพื่อรู้เท่าทันภัยคุกคามรูปแบบใหม่
๓. ใช้อินเทอร์เน็ตอย่างระมัดระวัง หลีกเลี่ยงเว็บไซต์ที่น่าเชื่อถือหรือไม่เหมาะสม
๔. ไม่เปิดไฟล์หรือลิงก์ที่ไม่ทราบแหล่งที่มา โดยเฉพาะจากบุคคลหรืออีเมลที่ไม่รู้จัก
๕. ใช้รหัสผ่านที่แตกต่างกันในแต่ละระบบ และหลีกเลี่ยงการใช้รหัสผ่านเดียวกันทุกบัญชี

ประโยชน์ที่ได้จากพัฒนาความรู้

๑. มีความรู้และความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ สามารถรู้เท่าทันรูปแบบการโจมตีและความเสี่ยงที่อาจเกิดขึ้น
๒. สามารถป้องกันตนเองและข้อมูลสำคัญได้อย่างเหมาะสม เช่น การตั้งรหัสผ่านที่ปลอดภัย และการหลีกเลี่ยงลิงก์หรือไฟล์ที่น่าสงสัย

๓. เพิ่มความระมัดระวังในการใช้งานเทคโนโลยีและอินเทอร์เน็ต ลดโอกาสในการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์

๔. สามารถนำความรู้ไปประยุกต์ใช้ในการปฏิบัติงาน และช่วยสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์ภายในองค์กร

การนำองค์ความรู้ไปประยุกต์ใช้

๑. ปกป้องกันข้อมูลของหน่วยงาน โดยจัดเก็บและส่งต่อข้อมูลอย่างเหมาะสม ไม่เปิดเผยข้อมูลสำคัญแก่ผู้ที่ไม่มีความรู้

๒. เพิ่มความระมัดระวังในการใช้งานอีเมลและอินเทอร์เน็ต ตรวจสอบผู้ส่ง ลิงก์ และไฟล์แนบก่อนเปิดหรือดาวน์โหลด เพื่อป้องกัน Phishing และ Malware

๓. รักษาความปลอดภัยของบัญชีผู้ใช้งาน ใช้รหัสผ่านที่มีความปลอดภัยและแตกต่างกันในแต่ละระบบ รวมถึงเปิดใช้การยืนยันตัวตนหลายขั้นตอนเมื่อมี

๔. ตรวจสอบข้อมูลก่อนนำไปใช้หรือเผยแพร่ โดยเฉพาะข้อมูลจากสื่อออนไลน์ เพื่อลดการเผยแพร่ข้อมูลที่ไม่ถูกต้องหรือเป็นเท็จ

๕. นำความรู้ไปถ่ายทอดให้เพื่อนร่วมงาน เพื่อสร้างความตระหนักและลดความเสี่ยงจากภัยไซเบอร์ภายในหน่วยงาน

๖. สามารถรับมือเมื่อเกิดเหตุผิดปกติ เช่น พบอีเมลต้องสงสัย ไฟล์แปลกปลอม หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยรีบแจ้งผู้รับผิดชอบด้านระบบสารสนเทศของหน่วยงานทันที

แนวทางการถ่ายทอดองค์ความรู้สู่ผู้เกี่ยวข้อง

๑. สร้างความรู้และความตระหนัก ให้เกษตรกรรู้จักภัยไซเบอร์ที่พบบ่อย เช่น ลิงก์ปลอม SMS หลอกลวง และการขอรหัส OTP

๒. ฝึกทักษะการป้องกันตนเอง โดยใช้หลัก “หยุด-คิด-เช็ค” ตรวจสอบข้อมูล ลิงก์ และแหล่งที่มา ก่อนคลิกหรือแชร์ พร้อมแนะนำการตั้งรหัสผ่านที่ปลอดภัย

๓. ถ่ายทอดผ่านสื่อและกิจกรรมที่เข้าใจง่าย เช่น การสาธิตสถานการณ์จริง อินโฟกราฟิก คลิปสั้น และการอบรมกลุ่มเกษตรกร เพื่อให้สามารถนำความรู้ไปใช้ในชีวิตประจำวันได้จริง

(ลงนาม).....

(นางสาววิลาวัลย์ เรียนเวช)

นักวิชาการเกษตรชำนาญการ

(ลงนาม).....

(นายอนุรักษ บัวคลีคลาย)

ผู้อำนวยการศูนย์ศึกษาการพัฒนาเขาหินซ้อน

อันเนื่องมาจากพระราชดำริ

การสร้างความรู้ความมั่นคงทางไซเบอร์



ข้อมูลการพัฒนา

- ประจำปีงบประมาณ : พ.ศ. 2569
- ชื่อ-นามสกุล : นางสาววิลาวัลย์ เรือนเวช
- ตำแหน่ง : นักวิชาการเกษตรชำนาญการ
- กลุ่ม/ฝ่าย/สพด. : ศูนย์ศึกษาการพัฒนาเขาหินซ้อน อันเนื่องมาจากพระราชดำริ
- หัวข้อการพัฒนา : การสร้างความรู้ความมั่นคงทางไซเบอร์
- วิธีการพัฒนา : อบรมออนไลน์
- วันที่ : 20 สิงหาคม 2569
- สถานที่ : ศูนย์ศึกษาการพัฒนาเขาหินซ้อน อันเนื่องมาจากพระราชดำริ
- หน่วยงานที่จัดอบรม : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA)

วัตถุประสงค์ของการเรียน

เพื่อเป็นการสร้างการเรียนรู้ ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ระดับต้น (Beginner) จนถึงระดับกลาง (Intermediate) ที่ต้องการดูแลรักษา และการป้องกัน อำรงไว้ซึ่ง การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความสมบูรณ์พร้อมใช้ (Availability) เพื่อให้ระบบบริการ ผลิตภัณฑ์ มีความมั่นคงปลอดภัย และสามารถป้องกัน รับมือ ภัยคุกคามที่เกิดจากความมั่นคงปลอดภัยทางไซเบอร์ หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือโอกาสที่จะทำให้เกิดข้อผิดพลาด การสูญเสีย ที่จะเกิดขึ้น ต่อระบบ บริการ ผลิตภัณฑ์

สรุปสาระสำคัญ

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) คือ การใช้เทคโนโลยี เครื่องมือ และกระบวนการต่าง ๆ เพื่อป้องกันข้อมูล ระบบเครือข่าย อุปกรณ์ และโปรแกรมขององค์กรจากการเข้าถึงหรือโจมตีโดยไม่ได้รับอนุญาต รวมถึงการเตรียมความพร้อมในการรับมือและแก้ไขปัญหาก็อาจเกิดขึ้น ปัจจุบันหน่วยงานภาครัฐและภาคเอกชนให้ความสำคัญกับความมั่นคงปลอดภัยไซเบอร์มากขึ้น เนื่องจากภัยคุกคามทางไซเบอร์มีรูปแบบที่หลากหลายและซับซ้อนมากขึ้น ซึ่งอาจส่งผลกระทบต่อข้อมูล ระบบงาน และการดำเนินงานขององค์กร ดังนั้น การมีมาตรการป้องกันและรับมือที่เหมาะสมจึงเป็นสิ่งสำคัญในการลดความเสี่ยงและความเสียหายที่จะเกิดขึ้น



กฎหมายและมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ต้องเป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง เพื่อป้องกันข้อมูล ระบบสารสนเทศ และการดำเนินงานขององค์กร

1

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดแนวทางและมาตรการในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

2

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ กำหนดความผิดและบทลงโทษเกี่ยวกับการใช้หรือเข้าถึงระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์โดยมิชอบ

3

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดหลักเกณฑ์ในการเก็บรวบรวม ใช้ เปิดเผย และดูแลรักษาข้อมูลส่วนบุคคลให้มีความปลอดภัย

4

มาตรฐาน ISO/IEC 27001

เป็นมาตรฐานสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System: ISMS) เพื่อช่วยให้องค์กรสามารถบริหารจัดการความเสี่ยงและปกป้องข้อมูลได้อย่างเป็นระบบ



CIA Triad หรือ CIA Model เป็นหลักการพื้นฐานในการรักษาความมั่นคงปลอดภัยของข้อมูล ประกอบด้วย 3 องค์ประกอบสำคัญ



C - Confidentiality (การรักษาความลับของข้อมูล)

มุ่งป้องกันไม่ให้ผู้ที่ไม่พึงประสงค์สามารถเข้าถึงข้อมูล โดยกำหนดสิทธิและระดับการเข้าถึงข้อมูลให้เหมาะสมกับผู้ใช้งานและระดับชั้นความลับของข้อมูล



I - Integrity (การรักษาความถูกต้องครบถ้วนของข้อมูล)

มุ่งให้ข้อมูลมีความถูกต้อง ครบถ้วน และไม่ถูกแก้ไขหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต รวมถึงกำหนดสิทธิในการแก้ไขข้อมูลเฉพาะผู้ที่ได้รับอนุญาต



A - Availability (การรักษาความพร้อมใช้งานของข้อมูล)

มุ่งให้ระบบและข้อมูลสามารถเข้าถึงและใช้งานได้อย่างต่อเนื่องเมื่อผู้มีส่วนเกี่ยวข้องต้องการใช้งาน รวมถึงมีการเตรียมระบบสำรองและแผนการรับมือเมื่อเกิดเหตุขัดข้องหรือภัยคุกคาม

รูปแบบภัยคุกคามทางไซเบอร์ (ที่พบบ่อย)

1



Malware (มัลแวร์)

ซอฟต์แวร์หรือชุดคำสั่งที่ถูกสร้างขึ้นโดยมีจุดประสงค์เพื่อสร้างความเสียหาย ขโมยข้อมูล หรือเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต เมื่อถูกติดตั้งในอุปกรณ์แล้ว อาจสามารถเข้าถึงทรัพยากรของเครื่อง เช่น ต่อเนื่องกับอุปกรณ์อื่นในเครือข่าย หรือส่งข้อมูลไปยังเซิร์ฟเวอร์ของมัลแวร์ได้

2



Web-based Attacks (การโจมตีผ่านเว็บไซต์)

การโจมตีโดยใช้เว็บไซต์เป็นช่องทาง เช่น การเจาะระบบเว็บไซต์ที่มีช่องโหว่ และแทรกชุดคำสั่งที่เป็นอันตราย เมื่อผู้ใช้งานเข้าเว็บไซต์ดังกล่าว อาจถูกเปลี่ยนเส้นทางไปยังเว็บไซต์ที่มี Malware หรือถูกหลอกให้ดาวน์โหลดไฟล์อันตราย

3



Phishing (ฟิชชิง)

การหลอกลวงผ่านช่องทางต่าง ๆ เช่น อีเมล SMS เว็บไซต์ หรือสื่อสังคมออนไลน์ โดยสร้างข้อความหรือเว็บไซต์ปลอมให้ผู้ใช้หลงเชื่อ เพื่อหลอกให้ผู้ใช้งานเปิดเผยข้อมูลสำคัญ เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคล ซึ่งอาจถูกนำไปใช้ในการเข้าถึงระบบหรือทำธุรกรรมโดยไม่ได้รับอนุญาต

4



Web Application Attacks (การโจมตีเว็บแอปพลิเคชัน)

การโจมตีที่มุ่งเป้าไปยังช่องโหว่ของเว็บแอปพลิเคชัน เช่น การแทรกคำสั่ง SQL การโจมตีแบบ Cross-Site Scripting (XSS) หรือการ bypass การยืนยันตัวตน ส่งผลให้ผู้ใช้สามารถเข้าถึงข้อมูล แก้ไขข้อมูล หรือควบคุมระบบได้

มาตรการป้องกันภัยคุกคามทางไซเบอร์

1

ใช้รหัสผ่านที่แข็งแกร่งและเปลี่ยนรหัสผ่านสม่ำเสมอ

ตั้งรหัสผ่านที่มีความซับซ้อน และเปลี่ยนรหัสผ่านอย่างน้อยทุก 6 เดือน



2

ไม่เปิดเผยข้อมูลสำคัญ

หลีกเลี่ยงการให้ข้อมูลสำคัญ เช่น รหัสผ่าน ข้อมูลส่วนบุคคล หรือข้อมูลทางการเงิน แก่บุคคลหรือเว็บไซต์ที่น่าเชื่อถือ



3

อัปเดตซอฟต์แวร์และระบบอย่างสม่ำเสมอ

อัปเดตระบบปฏิบัติการและซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุด เพื่อลดช่องโหว่ที่อาจถูกโจมตี



4

ตรวจสอบความน่าเชื่อถือของอีเมลและเว็บไซต์

ไม่คลิกลิงก์หรือดาวน์โหลดไฟล์จากแหล่งที่น่าเชื่อถือ และตรวจสอบ URL ให้ถูกต้องก่อนใช้งาน



5

สำรองข้อมูลอย่างสม่ำเสมอ

สำรองข้อมูลสำคัญไว้ในสื่อที่ปลอดภัย และทดสอบการกู้คืนข้อมูลเป็นประจำ



6

ใช้โปรแกรมป้องกันไวรัสและไฟร์วอลล์

ติดตั้งและอัปเดตโปรแกรมป้องกันไวรัส และเปิดใช้งานไฟร์วอลล์ เพื่อป้องกันการโจมตีจากภายนอก



7

สร้างความตระหนักรู้และฝึกอบรมบุคลากร

ให้ความรู้และฝึกอบรมอย่างต่อเนื่อง เพื่อให้บุคลากรสามารถป้องกันภัยคุกคามทางไซเบอร์ได้อย่างถูกต้อง



ความมั่นคงปลอดภัยทางไซเบอร์ เริ่มต้นที่ "ความตระหนักรู้" ของทุกคน ร่วมกันป้องกันข้อมูล องค์กร และประเทศ ให้ปลอดภัยในยุคดิจิทัล

