

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

ชื่อ-นามสกุล นางสาวบุญส่ง สว่างแสง ตำแหน่ง เจ้าพนักงานการเกษตรชำนาญงาน
หน่วยงาน ศูนย์ศึกษาการพัฒนาเขาหินซ้อนอันเนื่องมาจากพระราชดำริ
หัวข้อการพัฒนา การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
วิธีการพัฒนา การฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์
วันที่พัฒนา ๒๖ มิถุนายน ๒๕๖๙ สถานที่ ศูนย์ศึกษาการพัฒนาเขาหินซ้อนฯ
หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA)
วัตถุประสงค์

๑. เพื่อเรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงาน
๒. มีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่างๆ
๓. สามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

สรุปสาระสำคัญ

Cybersecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึง วิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย, โครงสร้างพื้นฐานทางสารสนเทศ, ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญมากยิ่งขึ้นเนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์

๑. Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุด ซึ่งข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่าง เช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุดผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น

- เบอร์โทรของพนักงานในบริษัท จัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

๒. Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลของธนาคารด้านการเงิน ข้อมูลบัญชีธนาคาร และข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๓. Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น ข้อมูลของธนาคารด้านการเงิน ข้อมูลบัญชีธนาคาร และข้อมูลที่อยู่บนระบบคอมพิวเตอร์

รูปแบบภัยคุกคามของ Cybersecurity

๑. Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแพร่ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่ายรวมถึงเซิร์ฟเวอร์ต่างๆ ได้ ทั้งนี้ขึ้นอยู่กับพฤติกรรมแตกต่างกันตามที่ไม่ประสงค์ดีที่ทำการผลิตออกมา ซึ่งเรียกว่า Malware นั้นครอบคลุมถึง Virus, Worms และ Trojans

๒. Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่ เพื่อแก้ไข เว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

๓. Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๔. Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น Code ของเว็บไซต์ เช่น CMS, Web Server หรือ Database Server วิธีการโจมตีที่นิยมใช้ Cross-Site, Scripting, SQL Injection, Path Traversal สามารถศึกษาวิธีการป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP Top Ten

๕. Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับเช่น E-Mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญหรือก่อกวน

๖. DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายโดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกันจุดประสงค์ที่ทำให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้ หรือระบบล่ม

๗. Data breach คือ เกิดการรั่วไหลของข้อมูลที่เกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูล ของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบ ไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ ส่งผลกระทบต่อข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่ในบางกรณีมีการเรียกค่าไถ่ของข้อมูลซึ่งจะสร้างผลกระทบต่อชื่อเสียง และความน่าเชื่อถือขององค์กร

๘. Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่งภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

๙. Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมาย หรือดำเนินการบางอย่างที่ถูก โปรแกรมไว้ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๑๐. Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อกไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์การล็อกไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่าน ที่ใช้ในการปลดล็อกไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง วิธีการป้องกันโดยสำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล โดยควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

๑๑. Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวณผลเพื่อสร้างรายได้กลับไป Hacker

ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

๑. การใช้ Password ในระบบคอมพิวเตอร์ที่ดีและปลอดภัย ควรดำเนินการดังนี้

๑.๑ ควรตั้งให้มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ \$ #) และควรมีความยาวของ Password อย่างน้อย ๘ ตัวอักษร

๑.๒ ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, ๑๒๓๔๕๖, วันเกิด, หมายเลขโทรศัพท์

๑.๓ มีการเปลี่ยน Password อย่างสม่ำเสมอ และไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

๑.๔ ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้

๒. ข้อควรระวัง Fake News หรือ ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่ นั้นดูมีความน่าเชื่อถือ ซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมาก วิธีการสังเกตข่าวปลอม โดยดูว่ามีการพาดหัวข่าว หรือข้อความที่เกินจริง ซึ่งระบุที่มาของข่าวไม่ได้ มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์ และสำนวนการเขียนออกแนวการโฆษณา

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

ได้รับความรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงาน และมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามจากไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่างๆ เพื่อป้องกันความเสียหายภายในองค์กร เนื่องจากการมีระบบคอมพิวเตอร์ในการปฏิบัติงานและเสริมประสิทธิภาพงานให้ได้ดียิ่งขึ้นรวมทั้งสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

การนำองค์ความรู้ไปประยุกต์ใช้

นำความรู้มาถ่ายทอดให้กับเจ้าหน้าที่ภายในองค์กรเกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงาน และการป้องกันความเสียหายที่จะเกิดขึ้นกับองค์กรในระบบการทำงานด้วยคอมพิวเตอร์ ให้เกิดประสิทธิภาพในการทำงานของบุคลากรมากขึ้น

แนวทางการถ่ายทอดองค์ความรู้สู่เกษตรกร

โดยจัดอบรมให้กับเกษตรกรที่เป็นแกนนำทางด้านการเกษตร เพื่อให้ทราบเรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามจากไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่างๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน นำไปปรับใช้ในชีวิตประจำวันและภาคเกษตรต่อไป

(ลงนาม) นพธ สุวาทิต
(นางสาวบุญส่ง สุวาทิต)
เจ้าพนักงานการเกษตรชำนาญงาน

(ลงนาม) 
(นายอนุรักษ์ บัวคลี่คลาย)
ผู้อำนวยการศูนย์ศึกษาการพัฒนาเขาหินซ้อน
อันเนื่องมาจากพระราชดำริ

การสร้างความรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

Cybersecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์

คือการนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกต้องแบบไว้เพื่อป้องกันและรับมือที่อาจถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจเกิดความเสียหายจากการที่เข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐและภาคเอกชนให้ความสำคัญในเรื่องมากยิ่งขึ้นเนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้นรวมถึงรูปแบบของการโจมตีทางมีหลากหลายมากยิ่งขึ้น ทำให้เกิดความเสียหายในองค์กรเพิ่มมากขึ้น



พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์

การรักษาความลับของข้อมูล (Confidentiality) คือ เป็นการที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้เช่นข้อมูลส่วนเงินเดือนของพนักงานเป็นความลับสูงสุดหรือเบอร์โทรของพนักงานในบริษัท

การรักษาความถูกต้องของข้อมูล (Integrity) คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลของธนาคารด้านการเงิน ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่ระบบคอมพิวเตอร์

ความพร้อมใช้งานของข้อมูล (Availability) คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น ข้อมูลบัญชีธนาคารข้อมูลที่อยู่ระบบคอมพิวเตอร์

รูปแบบภัยคุกคามของ Cybersecurity

Malware

Malware คือ ซอฟต์แวร์ หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมา เพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ เมื่อติดตั้งหรือเปิดในระบบคอมพิวเตอร์ จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแพร่ข้อมูล ไปยังคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่ายรวมถึงเซิร์ฟเวอร์ต่างๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ไม่ประสงค์ ที่ทำการผลิตออกมารวมถึง Virus Worms และ Trojans

Botnets

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมาย หรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์)

Insider threat

Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติ เช่น คอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน ซึ่ง Insider threat เป็นภัยที่มีความรุนแรงภายในองค์กร ถ้ามีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่ายและผลลัพธ์ของภัยนี้มีความรุนแรง

Phishing

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

Data breach

Data breach คือ เกิดการรั่วไหลของข้อมูลที่เกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลเว็บไซต์, ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

Web-based attacks

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้วจะนำเหยื่อไปที่เป็นเป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

DDoS

DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบให้บริการ โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมาก ยิ่งมาที่เป้าหมายเดียวภายในเวลาเดียวกันจุดประสงค์ที่กระทำเพื่อให้เว็บไซต์ระบบ การให้บริการหรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล้ม

Web application attacks

Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น Code ของเว็บไซต์ เช่น CMS, Web Server หรือ Database Server

Ransomware

Ransomware คือ Malware ประเภทหนึ่งที่มีจุดประสงค์ที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่าน

Cryptojacking

Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และ แอปทำการติดตั้งโปรแกรมที่ใช้ เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปให้ Hacker

Spam

Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ ที่ทำการส่งข้อมูล, ข้อความ, หรือ โฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อความเสียหาย

การระวัง

Fake News หรือ ข่าวปลอมเป็นภัยคุกคามใกล้ตัวที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวปลอมที่นำมาเผยแพร่ในสื่อความน่าเชื่อถือ ซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ มีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็ว วิธีการสังเกตข่าวปลอม โดยดูว่ามีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าเชื่อถือในการรับรู้ที่มาของข่าวไม่ได้ ซึ่งมักจะไม่มีระบุวันที่ และเวลาที่เกิดเหตุการณ์ และส่วนการเขียนออกแนวการโฆษณา

ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

การใช้ Password ในระบบคอมพิวเตอร์ที่มั่นคงปลอดภัย ควรดำเนินการดังนี้

1. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (@ \$ #) และความยาวของ Password อย่างน้อย 8 ตัวอักษร
2. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, 123456, วันเกิด, หมายเลขโทรศัพท์ และควรมีการเปลี่ยน Password อยู่เสมอ
3. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
4. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ และไม่ควรบอก Password แก่ผู้อื่น



จัดทำโดยนางสาวบุญส่ง สว่างแสง
ศูนย์ศึกษาการพัฒนาเขาหินซ้อนอันเนื่องมาจากพระราชดำริ
สำนักงานพัฒนาที่ดินเขต 2