



คู่มือการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(AWARENESS CYBER SECURITY)



สารบัญ

หน้า

บทนำ ๑

ความมุ่งหมาย..... ๑

วัตถุประสงค์..... ๑

ขอบเขตในการการบริหารจัดการระบบบริการสารสนเทศให้มีความพร้อมใช้ตามมาตรฐาน..... ๒

รูปแบบภัยคุกคามและผลกระทบทางไซเบอร์..... ๒

การรักษาความปลอดภัยไซเบอร์..... ๙

ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน..... ๙

๑. บทนำ

ภัยคุกคามทางไซเบอร์มีปริมาณและความซับซ้อนเพิ่มมากขึ้น การใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือขาดความเข้าใจ อาจตกเป็นเหยื่อหรือเครื่องมือของผู้ไม่ประสงค์ดีในการปฏิบัติการที่ไม่พึงประสงค์ ซึ่งอาจก่อให้เกิดความเสียหายแก่ผู้ที่ตกเป็นเหยื่อหรือองค์กร รวมถึงอาจส่งผลกระทบต่อความมั่นคงของชาติได้

ตามนโยบายเร่งด่วนของรัฐมนตรีว่าการกระทรวงกลาโหม ประจำปีงบประมาณ พ.ศ.๒๕๖๕ (๑ ต.ค.๖๔ – ๓๐ ก.ย.๖๕) ข้อ ๒.๕ เร่งพัฒนาขีดความสามารถการปฏิบัติการด้านไซเบอร์ ทั้งในด้านกำลังพล เครื่องมือ องค์ความรู้และระบบบริหารจัดการ ด้วยการบูรณาการความร่วมมือกับทุกภาคส่วนทั้งภายในและต่างประเทศ เพื่อให้สามารถรองรับภัยคุกคามด้านไซเบอร์ ที่มีผลกระทบต่อความมั่นคงของชาติอย่างต่อเนื่องตลอดจนให้การสนับสนุนการดำเนินงานด้านไซเบอร์ระดับประเทศได้อย่างมีประสิทธิภาพ

โดยมีความสอดคล้องกับ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ หมวด ๓ การรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรา ๔๒ (๗) การสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนพัฒนาการด้านไซเบอร์เพื่อความมั่นคง ระยะที่ ๒ (พ.ศ.๒๕๖๖ – ๒๕๗๐) กห.

๒. ความมุ่งหมาย

การดำเนินการจัดทำคู่มือการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีความมุ่งหมายเพื่อให้ข้าราชการ นขต.สป. และข้าราชการภายในหน่วย มีความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศและพัฒนาบุคลากรให้มีความตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ และรู้เท่าทันภัยคุกคามต่างๆที่เกิดขึ้นให้สามารถใช้งานระบบเครือข่ายในองค์กรได้อย่างเต็มประสิทธิภาพ

๓. วัตถุประสงค์

๓.๑ เพื่อเสริมสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

๓.๒ เพื่อให้เกิดความตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ และรู้เท่าทันภัยคุกคามต่างๆ ที่เกิดขึ้น

๓.๓ เพื่อให้สามารถนำความรู้ที่ได้รับไปประยุกต์ใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ

๔. ขอบเขตในการบริหารจัดการระบบบริการสารสนเทศให้มีความพร้อมใช้ตามมาตรฐาน

ปัจจุบัน กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม เป็นหน่วยงานที่มีภารกิจให้บริการ ด้านเทคโนโลยีสารสนเทศ การสื่อสาร ด้านอวกาศเพื่อความมั่นคง และด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ แก่หน่วยงานขึ้นตรงสำนักงานปลัดกระทรวงกลาโหม โดยงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีศูนย์ไซเบอร์ เป็นหน่วยรับผิดชอบ เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ที่ให้บริการแก่หน่วยงานขึ้นตรงสำนักงานปลัดกระทรวงกลาโหม จึงได้มีการจัดทำคู่มือการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นมา

๕. หัวข้อการบรรยายแบ่งเป็นการบรรยายเป็น 3 หัวข้อ ดังนี้

๕.๑ รูปแบบภัยคุกคามและผลกระทบทางไซเบอร์

๕.๑.๑ **มัลแวร์ (Malware)** คือ ซอฟต์แวร์ หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อทำให้ส่งผลกระทบต่อระบบคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์โดยตรง เมื่อถูกติดตั้งหรือถูกเรียกใช้งาน ซึ่ง Malware จะสามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย โดยสามารถกระจายตัวออกไปในเครือข่ายเพื่อติดเครื่องอื่น ๆ รวมถึงเซิฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ผลิตหรือผู้ไม่ประสงค์ดีทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง ไวรัส (Virus), เวิร์ม (Worms) หรือโทรจัน (Trojans) สามารถเกิดขึ้นตลอดเวลา โดยมีการนำ Code มาแก้ไขและผลิตออกมาเรื่อย ๆ ซึ่งมีจุดประสงค์ที่แตกต่างกันออกไปตามความต้องการของผู้ที่ผลิต

๕.๑.๒ **Web-based attacks** คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ Hacker จัดทำเว็บไซต์ปลอมขึ้นมา หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยใส่ Code ที่ทำงานเมื่อเหยื่อเข้าเว็บไซต์ดังกล่าวแล้วจะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware และเกิดกระบวนการต่อไปตามที่ Hacker ต้องการเพิ่มเติม ในส่วนของเว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System) ที่ใช้งานอย่างแพร่หลาย เช่น Wordpress หรือ Joomla ที่มีช่องโหว่หรือขาดการอัปเดต ซึ่งถือว่าเป็นอันตรายในระดับหนึ่งทั้งในส่วนของผู้ใช้งานและผู้ให้บริการเว็บไซต์ด้วย

๕.๑.๓ **Phishing** คือ วิธีการโจมตีเหยื่อผ่านช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social เช่น Facebook หรือ Line โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือข้อมูลสำคัญอื่น ๆ ยกตัวอย่างให้เห็นภาพมากขึ้นเช่น เราอาจจะได้รับ SMS จากธนาคารแจ้งเตือนว่ารหัสต่าง ๆ ที่อยู่กับธนาคารของ ๆ ของคุณ หมดอายุต้องทำอย่างไรบ้าง ได้รับอีเมล์ที่มาจากธนาคารให้คลิกลิงก์แล้วเข้าไปกรอกข้อมูลส่วนบุคคล หรือเพื่อใส่ Username Password อันนี้คือส่วนของภัยคุกคามด้าน Phishing ซึ่ง Phishing เป็นคำพ้องเสียงว่าจากคำว่า Fishing หรือตกปลา คือทำอย่างไรก็ได้เพื่อหลอกล่อเหยื่อให้เหยื่อติดกับและให้ข้อมูลต่าง ๆ กลับมาที่ Hacker เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรมต่อไป

๕.๑.๔ **Web application attacks** คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ ที่อยู่บนตัวเว็บไซต์เอง ส่วนใหญ่มักจะเกิดใน code ของพวกเว็บไซต์ CMS ตามที่เล่าไปก่อนหน้า ช่องโหว่ที่เกิดใน CMS พวก Wordpress Joomla หรืออะไรก็ตาม ซึ่งส่วนใหญ่จะขาดการอัปเดทเวอร์ชั่น คือติดตั้งครั้งแรกเสร็จเรียบร้อยแล้วก็ไม่มีการอัปเดท Patch ซึ่งก็จะมีช่องโหว่ในแต่ละเวอร์ชั่น ที่ทางผู้ผลิต CMS ก็จะมีการอัปเดตเวอร์ชันออกมาอยู่โดยตลอดอยู่แล้ว แต่ในส่วนของผู้ดูแลอาจจะขาดการอัปเดทเพื่อปิดช่องโหว่ที่เกิดขึ้น ก็จะถูกโจมตีเข้ามาได้ หรือถูก Hack หรือถูกเปลี่ยนหน้าเว็บไซต์ได้ ถัดมาคือส่วนของ Web Server หรือ Database Server ที่เราตั้งขึ้นมา หรือที่เราดูแล เหมือนกันครับ ขาดการอัปเดท Patch หรือขาดการอัปเดทเวอร์ชัน อันนี้สำคัญครับส่วนวิธีการโจมตีที่นิยมใช้ ในการโจมตีก็จะมีพวก Cross-Site Scripting, SQL Injection เป็นการแทรก Code ต่าง ๆ เข้าไปผ่านช่องโหว่ของเว็บไซต์ หรือแม้แต่ Path Traversal ซึ่งเป็นการสุ่มเข้าไปที่ Path ดูว่า Path ต่าง ๆ ที่อยู่ในเว็บไซต์เราอันไหนที่มีข้อมูลสำคัญอยู่บ้างโดยการสุ่ม Path ไปเรื่อย ๆ ถ้าเราไม่ได้ปิดช่องโหว่ตรงนี้ก็อาจจะโดน Hack เข้ามาได้

ขอแนะนำเพิ่มเติมในส่วนของวิธีการป้องกัน สามารถศึกษาวิธีการป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP Top Ten โดย Search เข้าไปใน google เลย ซึ่งจะมีวิธีการป้องกัน เช่น Cross-Site Scripting ต้องแก้ไขอย่างไร มีวิธีการอย่างไรบ้าง SQL Injection ต้องแก้ไขอย่างไร Path Traversal ต้องแก้ไขอย่างไร ซึ่งจริง ๆ แล้วมีส่วนของวิธีการโจมตีมากกว่านี้ อันนี้เป็นตัวอย่างที่ส่วนใหญ่มักจะเกิดกับตัวเว็บไซต์

๕.๑.๕ **Spam** คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล หรือยัดเยียดข้อมูลผ่านช่องทางที่เป็นข้อความ หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญ หรือก่อกวน ในส่วนนี้เมื่อก่อน Spam จะเกิดขึ้นในอีเมล์เป็นหลัก แต่ในปัจจุบัน Spam เริ่มมาที่ SMS มากขึ้น หลาย ๆ ท่านอาจจะเคยได้รับข้อความให้เข้าเว็บไซต์ต่าง ๆ หรือเว็บไซต์พนัน ก็ Spam ผ่านทาง SMS กันแล้วในปัจจุบัน

๕.๑.๖ **DDoS** (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องที่เป็นต้นทางการโจมตีจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์เพื่อทำให้เว็บไซต์, ระบบการให้บริการ เว็บไซต์ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม ในต่างประเทศเองก็มีหลายเคสเหมือนกันที่เกิดขึ้นจากการโจมตี DDoS และในไทยเองก็มีเหมือนกันที่อาจจะเคยเห็นตามข่าว ที่นัดเข้าเว็บไซต์พร้อมกันในเวลานี้ เพื่อไม่ให้เว็บไซต์นั้นให้บริการได้ข้อแนะนำเพิ่มเติมไม่ควรเข้าร่วมกิจกรรมนัดเข้าเว็บไซต์พร้อมกัน เพราะอาจตกเป็นหนึ่งในผู้กระทำความผิดตาม พ.ร.บ.คอมพิวเตอร์ ได้

๕.๑.๗ **Data breach** คือ การรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลเว็บไซต์, ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชันหรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของข้อมูลชุดนั้น ๆ เพื่อไม่ให้เผยแพร่ข้อมูลชุดนั้น ข้อมูลในนั้นอาจจะเป็น username password email หรือข้อมูลที่เป็นความลับต่าง ๆ ขององค์กรผลกระทบ อย่างเช่นถ้าเป็นข้อมูลส่วนบุคคลที่เป็นความลับของเรา ถูกนำไปเผยแพร่ เราก็อาจจะรู้สึกไม่ปลอดภัยที่ข้อมูลของเราอยู่บนโลกอินเทอร์เน็ต หรืออาจสร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร อย่างเช่นเคสล่าสุด ข้อมูลคนไข้ของกระทรวงสาธารณะสุขที่หลุดออกไป หรือข้อมูลนักท่องเที่ยวที่เข้ามาในประเทศไทยที่หลุดออกไป โดยมากภัยคุกคามที่เป็น Data breach นั้นเกิดจากระบบที่ขาดการอัปเดทหรือขาดการดูแลที่ดี ตรงนี้จะต้องฝากถึงผู้ดูแลระบบต่าง ๆ ให้ดูแลระบบให้ดี

๕.๑.๘ **Insider threat** คือ ภัยที่เกิดจากบุคลากรภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน อาจจะมีช่องโหว่หรืออะไรก็ตามที่อาจจะทำให้ข้อมูลจากภายในองค์กรหลุดออกไป หรือโดน Hack ผ่านเครื่องคอมพิวเตอร์ของคนภายในองค์กร ซึ่ง Insider threat ถือเป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรงวิธีการป้องกันนำหลักการ Zero Trust มาใช้งานภายในองค์กร หลักการของ Zero trust อธิบายสั้น ๆ คือ ทุกครั้งที่มีการเข้าใช้งาน

ระบบอะไรก็ตาม เราไม่เชื่อว่าเครื่องคอมพิวเตอร์ หรืออุปกรณ์นั้น ๆ ปลอดภัย แม้จะเป็นเครื่องภายในองค์กร หรือเป็นใครก็ตาม เราต้องผ่านการยืนยันตัวตนตลอดเวลา การจะนำ Zero trust มาใช้ในองค์กรอาจจะต้องไปศึกษาเพิ่มเติม แต่ควรที่จะนำมาใช้ เพราะปัจจุบัน Insider threat เริ่มมีผลกระทบที่รุนแรงมากยิ่งขึ้น

๕.๑.๙ **Botnets หรือ Robot Network** คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องเหยื่อที่ถูก Botnets แฝงตัวอยู่จะไม่ทราบว่าติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกใช้จากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๕.๑.๑๐ **Ransomware** คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ทั้งโดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware จะทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกันสำรองข้อมูลเป็นประจำ เช่นทุกวัน ทุกสัปดาห์ หรือทุกเดือน โดยทำการแยกเก็บไฟล์สำรองข้อมูล ไม่ใช่ว่าสำรองข้อมูลจาก Desktop ไว้ที่ Drive D แบบนี้ไม่ได้เพราะถ้าหากติด Ransomware ขึ้นมา ไฟล์ทั้งหมดในเครื่องก็จะถูกเข้ารหัสควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ หรือบางครั้งติดตั้ง Anti-Virus ไว้ในเครื่องแล้วแต่ไม่มีการอัปเดตเลย หรือก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิดคิดก่อนที่จะเปิดไฟล์เช่น เราได้รับไฟล์นี้จากคนที่เรารู้จักหรือไม่

๕.๑.๑๑ **Cryptojacking** คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker ต้องย้อนกลับไปทำความเข้าใจถึง Cryptocurrency ก่อน Cryptocurrency คือเหรียญดิจิทัล ซึ่งเหรียญดิจิทัลเหล่านี้จะมีการประมวลผลตลอดเวลา ซึ่งจำเป็นต้องใช้ในส่วนของ CPU หรือ GPU (การ์ดจอ) บนเครื่องคอมพิวเตอร์ในการประมวลผล และหลังจากประมวลผลเรียบร้อยก็จะส่งกลับไปที่ส่วนกลางของเหรียญดิจิทัลนั้น ๆ เพื่อที่จะได้รับค่าตอบแทนในการประมวลผล ซึ่ง Cryptojacking นั้น คือการที่ Hacker Hack เข้ามาที่เครื่องเรา มาใช้ทรัพยากรของเครื่องเราทำการแอบขุด เพื่อให้ Hacker เหล่านั้นได้รับค่าตอบแทนกลับไป โดยเครื่องที่ติด Cryptojacking นั้นจะสังเกตได้จากการทำงานของ CPU กับ GPU จะมีการทำงานอย่างมากโดยที่เรายังไม่ทันได้ใช้งานอะไรเลย สามารถตรวจสอบได้จาก Task Manager หรือ Activity Monitor



โดยผลกระทบจากภัยคุกคามต่าง ๆ ที่ได้กล่าวมาอาจส่งผลกระทบต่อด้านต่าง ๆ ได้ ดังนี้

ด้านการเมือง



ผลกระทบทางการเมือง

- นักการเมืองใช้เป็นเครื่องมือในการสื่อสารด้านนโยบาย หาเสียงเลือกตั้ง และให้บริการประชาชน
- ประชาชนหรือผู้ชุมนุมใช้เรียกร้องความต้องการกับรัฐบาล
- การเมืองระหว่างประเทศ ใช้เพื่อการฑูต การปฏิบัติการข่าวสาร สงครามไซเบอร์ และเพื่อต่อรองผลประโยชน์ระหว่างประเทศ

ด้านเศรษฐกิจ



ผลกระทบทางเศรษฐกิจ

- การใช้เงินในรูปแบบดิจิทัลทดแทนเงินสด (Cryptocurrency) และการใช้สกุลเงินดิจิทัลที่ออกโดยธนาคารกลาง (CBDC)
- การเกิดธุรกรรมผ่านรายการบัญชีแบบสาธารณะที่ไม่ผ่านตัวกลาง (Blockchain)
- ธนาคารและสถาบันการเงินถูกบังคับให้ปรับตัวก่อนที่จะถูกทำให้หายไป (Finance Disrupt)

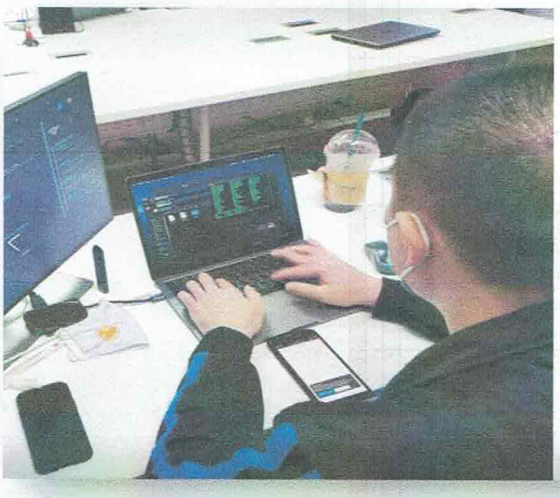
ด้านสังคม



ผลกระทบทางสังคม

- การเกิดสื่อสังคมออนไลน์ (Social Media) เป็นช่องทางและตัวตนเสมือนบนโลกดิจิทัลในการติดต่อระหว่างกัน
- อาชญากรรมทางคอมพิวเตอร์(Cybercrime) ในการฉ้อโกงและหลอกลวงบนโลกดิจิทัล
- ข่าวปลอม (Fake news) การให้ข้อมูลที่ผิดจากความเป็นจริง ก่อให้เกิดความเข้าใจผิดและอาจเกิดความจลาจล

ด้านเทคโนโลยี



ผลกระทบทางเทคโนโลยี

- การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) เพื่อป้องกันระบบและข้อมูลให้มีความปลอดภัย
- ระบบ Big Data ที่มีการใช้ปริมาณข้อมูลที่มหาศาลจัดเก็บและวิเคราะห์
  เพื่อนำไปช่วยมนุษย์ในการตัดสินใจ
- ระบบ AI และ Machine Learning เพื่อช่วยในการประเมินผลอัตโนมัติ
- ระบบ Quantum Computer โดยใช้อะตอมเพื่อประมวลผลให้เร็วมากขึ้น

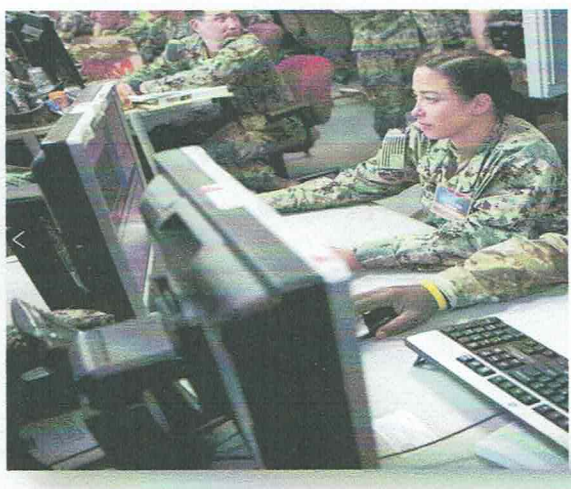
ด้านกฎหมาย



ผลกระทบ ทางกฎหมาย

- เกิดข้อตกลงด้านไซเบอร์ระหว่างประเทศ (Tallinn manual)
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2540
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

ด้านทหาร



ผลกระทบ ทางทหาร

- พื้นที่ไซเบอร์ ถือเป็นพื้นที่ปฏิบัติการทางทหาร (ด้านที่ 5)
- การจัดตั้งกองบัญชาการทางไซเบอร์เพื่อเตรียมกำลังและใช้กำลังทางไซเบอร์ขึ้นทั่วโลก
- ขีดความสามารถคือ การโจรกรรมและวินาศกรรม
- การก่อการร้ายทางไซเบอร์ โจมตีโครงสร้างพื้นฐานสำคัญของประเทศ

๕.๒ การรักษาความปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการ ที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือต่อการโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากขึ้น รวมถึงรูปแบบของการโจมตีทางไซเบอร์ที่มีความหลากหลายมากขึ้น และสร้างความเสียหายให้กับหน่วยงานมากขึ้นเรื่อย ๆ



๕.๓ ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

Computer

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย



1. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
2. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
4. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
7. มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

E-mail

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย



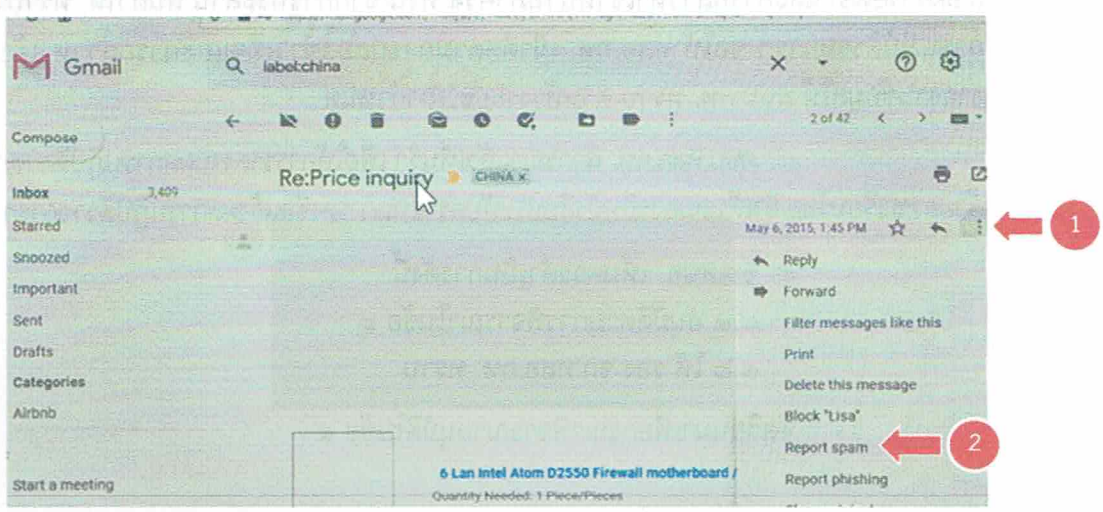
1. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
2. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
3. ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค
4. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม



E-mail ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

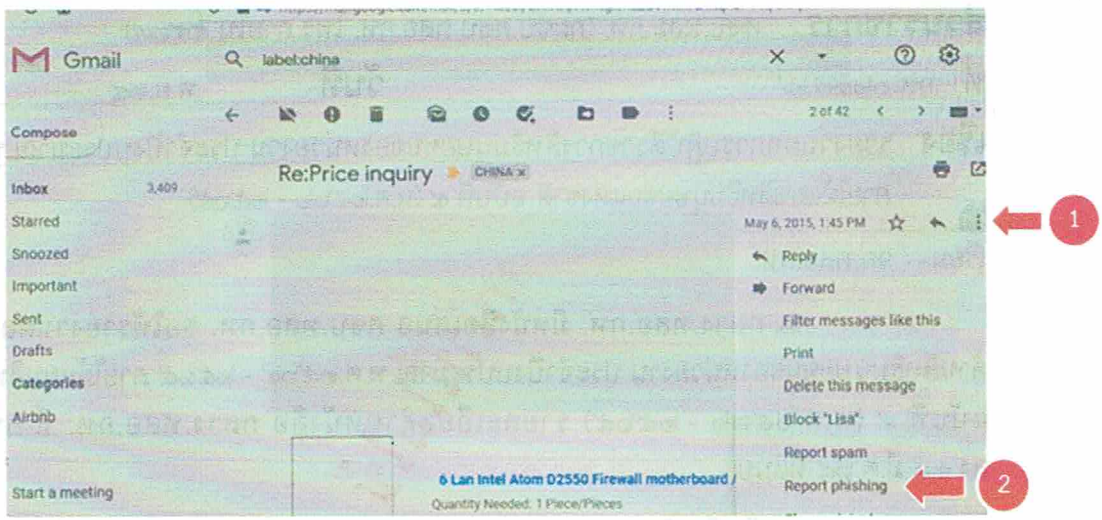


E-mail Gmail - Report Spam Mail



E-mail

Gmail - Report Phishing Mail

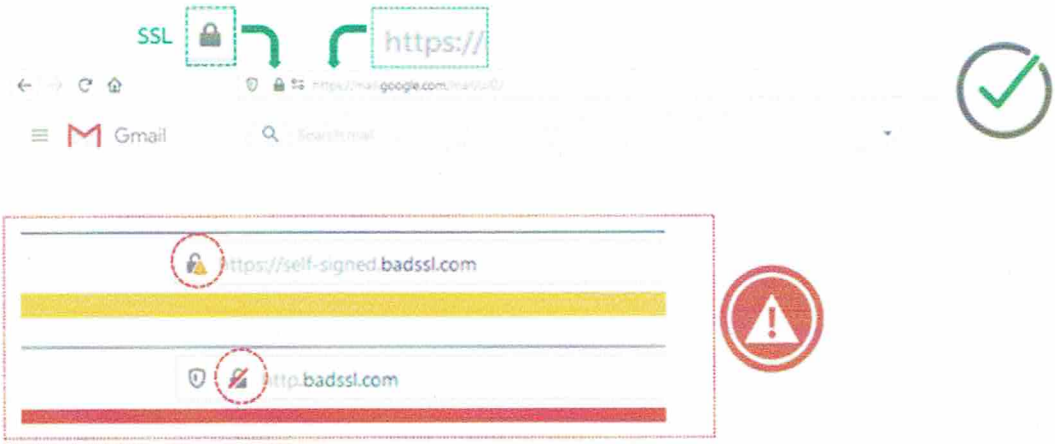


Website

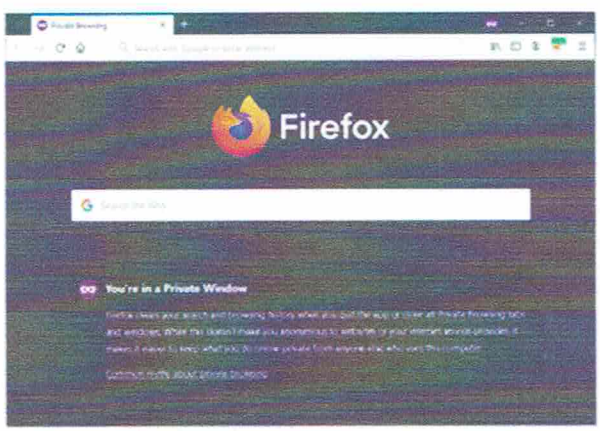
สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ
2. ไม่ควรทำการบันทึก Password ต่างๆ บน Browser
3. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
4. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น
5. ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ
6. ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing
7. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

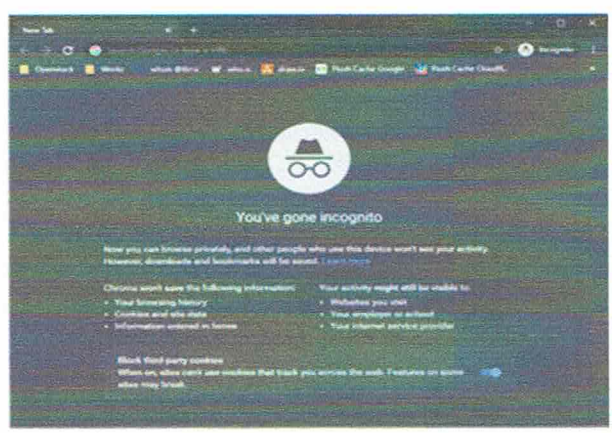
Website เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น



Website ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing

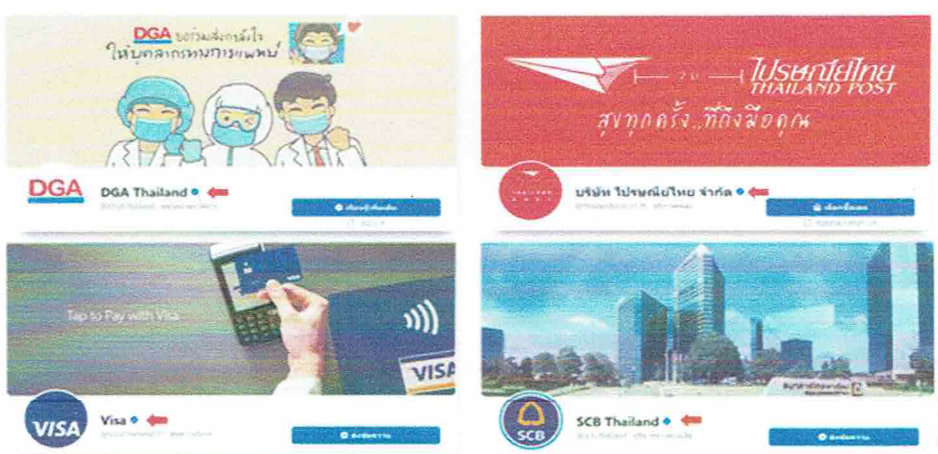


Firefox คือ Private Windows



Google Chrome คือ Incognito mode หรือ โหมดแบบไม่ระบุตัวตน

Website Facebook ที่ผ่านการยืนยันความถูกต้อง



Messaging

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่ควรบันทึก Password ไว้ที่โปรแกรม
2. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
3. มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา
4. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

เพิ่มเติม

ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

Fake News

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

วิธีการสังเกตุข่าวปลอม

1. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ
2. ระบุที่มาของข่าวไม่ได้
3. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
4. สำนวนการเขียนออกแนวการโฆษณา



Add sticky note
Use drawing tool

Fake News









ที่มา https://www.antifakenewscenter.com

Conference



สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ใช้สถานที่เหมาะสมกับการ Conference
2. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
3. แชร์เอกสารต่างๆ อย่างระมัดระวัง
4. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
5. มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

เพิ่มเติม

ควรมีการขออนุญาตผู้เข้าร่วมประชุม conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

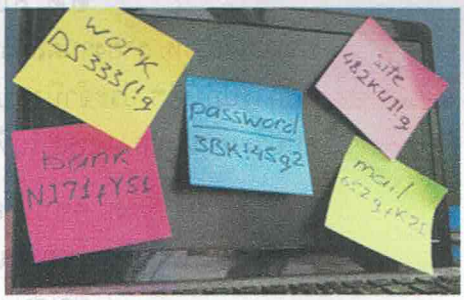
Cloud Storage



สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. แยก User ในการใช้งานของแต่ละบุคคล
2. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
3. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
4. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ
6. มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

Computer



สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
2. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
4. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
7. มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

Free WIFI



สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
2. หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

Mobile

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์
2. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
3. กำหนด Application permission ให้เหมาะสม
4. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ



Internet Connection

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย



1. เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน
2. เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ
3. กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น