การป้องกันตัวในยุคดิจิทัล

**การคุกคามทางอินเทอร์เน็ต**

**Doxxing** หรือการล่าแม่มด เป็นการขุดคุ้ยรูปถ่าย โพสต์ หรือสิ่งใด ๆ ที่เหยื่อได้โพสต์ไว้บนอินเทอร์เน็ตเพื่อนำมาประจาน โดยจุดประสงค์เพื่อให้ผู้ถูกล่าเกิดความเสียหายและอับอาย

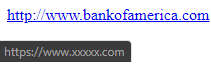
**Cyberbullying** ต่างจาก Doxxing ตรงที่ไม่ขุดข้อมูลเก่ามาประจาน แต่จะเน้นการโพสต์หรือตัดต่อภาพ

**Spam**(สแปม) เป็นการส่งข้อมูลซ้ำ ๆ ไปยังเครื่องเป้าหมาย อาจจะเป็นข้อมูลโฆษณา หรือฝังมัลแวร์แนบมาด้วย

**Sniffing** (ดักข้อมูล) การใช้อินเทอร์เน็ตสาธารณะเช่น โรงแรม มหาวิทยาลัย ล้วนมีความเสี่ยงในการถูกดักฟังข้อมูล การแฮกนั้นจะปลอมเครื่องตัวเองเพื่อดักฟังข้อมูล

**Phishing** (ล่อลวง) ใช้วิธีการส่งอีเมลไปยังอีเมลเป้าหมายและให้ผู้ใช้คลิกไปยังเว็บไซต์ปลอมที่ทำเหมือนกับเว็บทั่วไป เช่น ปลอมเป็นสถาบันการเงิน การหลอกล่อมีรูปแบบที่นิยมใช้กัน ดังนี้

* + HTML นั้นสามารถกำหนดลิงค์ใด ๆ บนแท็กลิงค์ได้ ซึ่งสามารถพาไปเว็บอื่นได้เช่นกัน ดังตัวอย่างที่มีข้อความไฮเปอร์ลิงค์ไปที่ bankofamerica.com แต่เมื่อชี้กลับแสดงเส้นทางจริงไปยังเว็บ xxxxx.com แทน



* + การจดโดเมนให้คล้ายกับเว็บของธนาคารโดยจงใจให้มีการผิดหรือตกตัวใดตัวหนึ่ง ทำให้ผู้ใช้งานไม่ทันสังเกต

http://www.bankofamerca.com (จงใจทำให้ตัว i หาย)

* + การใส่สับโดเมนให้เหมือนกับเว็บของธนาคาร และดันให้ตัวโดเมนจริงของคนร้ายตกขอบแสดงผล

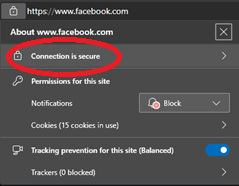
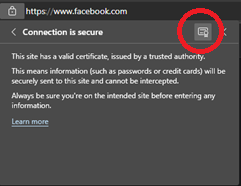
https://www.bankofamerica.invalidaccount.securityverification.xxxxx.com

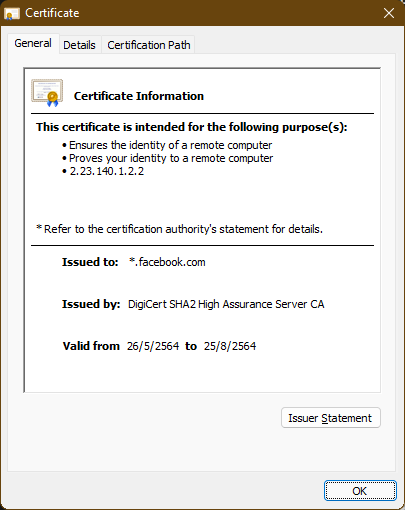
**การป้องกัน**

* + ไม่คลิกลิงค์นั้นแล้วเข้าเว็บองค์กรนั้น ๆ ด้วยตัวเอง
  + การตรวจสอบกุญแจสาธารณะ
  + ตรวจสอบชื่อโดเมน
  + กรณีที่อาจถูกดักฟัง ให้ใช้ VPN

**ขั้นตอนการตรวจสอบว่าเป็นเว็บไซต์จริงหรือไม่**

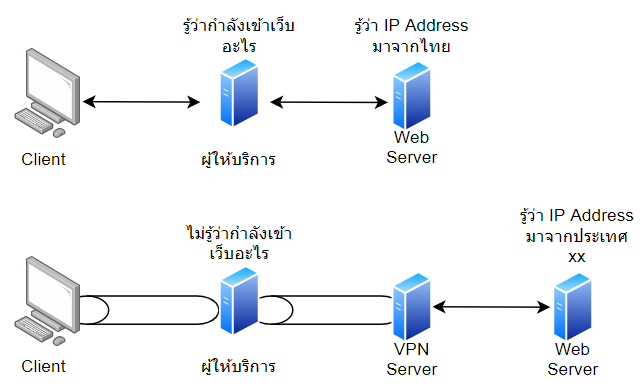
Google chrome คลิกที่สัญลักษณ์แม่กุญแจ -> เลือก Connection is secure (ในบางเว็บจะขึ้นว่า Connection is not secure) -> คลิกที่สัญลักษณ์ใบประกาศ จะปรากฎว่าเว็บนี้ใช้กุญแจสาธารณะที่ตรงกับชื่อโดเมนและไม่หมดอายุ (ปลอดภัย)



**VPN คืออะไร**

VPN คือการสร้างช่องทางเชื่อมต่อจากเครื่องคอมพิวเตอร์ของตัวเองออกไปยังที่ต่าง ๆ ทำให้ผู้ให้บริการ (ISP) ไม่ทราบว่าเรากำลังเข้าเว็บไหน และบริการอะไร



**การคุกคามที่มีผลจากการโพสต์ข้อมูลลงเว็บสาธารณะ และอื่น ๆ**

* พัสดุเก็บเงินปลายทางที่เราไม่ได้สั่ง
* หลอกลวงว่าเป็นเจ้าหน้าที่รัฐแล้วขอนำเงินในบัญชีไปตรวจสอบ
* โฆษณาขายของต่าง ๆ
* ผู้ร้ายนำข้อมูลไปเปิดบัญชีธนาคาร
* ถูกสวมซิมและขโมยรหัส OTP
* Skimmer, พนักงานจดเลขของบัตรเดบิต/เครดิต

**การป้องกัน**

* ไม่ควรโพสต์ชื่อ ที่อยู่ของตัวเอง และอีเมลลงในเว็บสาธารณะ สื่อโซเชียลเช่น เพจเฟสบุ๊ค ช่องความเห็นในยูทูป
* ถ่ายสำเนาบัตรประจำตัวประชาชนเพียงด้านหน้าพอ และขีดคร่อมว่านำไปใช้กับอะไร
* อย่าให้พนักงานจดเลขบัตรเดบิต/เครดิตโดยเด็ดขาด ควรส่องดูว่าพนักงานเอาไปทำอะไร หรือใช้จ่ายผ่าน QR Code ปลอดภัยกว่า

**มารยาทในการใช้อินเทอร์เน็ต**

* การพิมพ์ตัวใหญ่ล้วนในภาษาอังกฤษถือว่าเป็นการตะโกนและไม่สุภาพ
* ดราม่า ในอดีตเรียกว่า Flame War เป็นการเถียงโต้ตอบ(ทั้งสุภาพและไม่สุภาพ)ในเว็บ

**ความรู้อื่น ๆ**

**MEME** เป็นคำย่อของ Internet Meaning คือการนำภาพมาเป็นสัญลักษณ์ล้อเลียนมุขตลก

**Emoji** (สัญรูป) คือสัญลักษณ์แสดงความหมาย เช่น 🤣😊😢❤️💕 โดยสัญลักษณ์เหล่านี้จะแสดงผลแตกต่างกันไปในแต่ละระบบปฏิบัติการ

**Emoticon** คล้ายกับอีโมจิ มาจากการรวมสองคำ คือ Emotion + Icon คือการนำตัวอักษรมาเรียงให้เกิดเป็นความหมาย เช่น

* + :) ยิ้ม
  + ;( ร้องไห้
  + xoxo กอดจุ๊บ
  + :P แลบลิ้น

**Clickbait** คือการพาดหัวข่าว ข้อความ หรือใช้รูปที่เตะตา โดยมีวัตถุประสงค์เพื่อเรียกยอดวิว