Phishing คืออะไร ?

กรมสนับสนุนบริการสุขภาพ
Department of Health Service Support

เป็นการโจมตีโดยผู้ไม่หวังดีซึ่งจะส่งอีเมล,ข้อความหรือการโทรหาเหยื่อ โดยการแอบอ้างว่ามาจากหน่วยงานที่น่าเชื่อถือ เพื่อหลอกล่อเอาข้อมูลรหัสผ่าน หรือข้อมูลส่วนตัวอื่น ๆ โดยอาจจะเป็นการหลอกเหยื่อให้คลิกลิงค์ที่แนบมา จากนั้นจะทำการส่งมัลแวร์เข้ามาในเครื่องของเหยื่อ หรืออาจจะนำไปที่เว็บไซต์อื่น ๆ เพื่อหลอกให้กรอกแบบฟอร์ม เช่น

- **Spear Phishing** : โจมตีโดยกำหนดกลุ่มเป้าหมายแบบเจาะจงกลุ่ม
- **Whaling** : มุ่งเน้นการโจมตีไปที่ผู้บริหารระดับสูง หรือผู้มีส่วนได้ส่วนเสียขององค์กร
- **Pharming** : การโจมตี Server ของ เว็บไซต์ โดยเปลี่ยนลิงค์ไปยังเว็บไซต์ปลอม เพื่อล่อให้ผู้ใช้งานเข้ามากรอกข้อมูล

การป้องกัน
การใช้หลักการ S.U.R.G.E

Sender

ผู้ส่งอีเมล
สังเกตผู้ส่งข้อความ อีเมล ที่สะกดผิด ไม่สอดคล้องกับเนื้อหา ให้ตั้งข้อสงสัยไว้ก่อน

Unusual Activity

พฤติกรรมผิดปกติ
หน่วยงานหรือบุคลลที่เราเคยติดต่อส่งอีเมลหรือข้อความที่มีพฤติกรรมผิดปกติ เช่น สิทธิพิเศษ หรือขอข้อมูลส่วนตัว

Relationship

ความสัมพันธ์ระหว่างผู้ส่ง และผู้รับ
อย่าหลงเชื่อข้อความ
หรือ อีเมลจากคนแปลกหน้า

Grammar

ไวยากรณ์
ระวังอีเมลหรือข้อความที่มีการใช้คำผิดหรือแปลไม่ตรงหลักภาษา

External link

ลิงค์ออกไปยังเว็บไซต์ภายนอก
ให้ตรวจสอบความถูกต้องของลิงค์ก่อนหากดูแล้วไม่น่าเชื่อถือไม่ควรกด หรือไฟล์ที่นามสกุลไม่คุ้นเคยไม่ควรกด

ที่มา : ธนาคารแห่งประเทศไทย

กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม
กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข
02-193-7000 ต่อ 18206 ict@hss.mail.go.th LINE @452lyxbz