ชำระเงินออนไลน์อุ่นใจ... ต้องรู้จักคำว่า

PHISHING

Phishing เป็นคำพ้องเสียงจากคำว่า **Fishing** หมายถึงการตกปลา เปรียบเทียบง่าย ๆ ลองจินตนาการว่าเหยื่อล่อที่ใช้ตกปลาคือกลวิธีที่ผู้ไม่หวังดีใช้หลอกลวง โดยมักเป็นการปลอมอีเมล หรือหน้าเว็บไซต์ที่มีข้อความทำให้ผู้อ่านหลงเชื่อว่าเป็นของจริง จนตกเป็นเหยื่อ

ปลอมอีเมล

ให้ดูเหมือนของหน่วยงานที่น่าเชื่อถือ เช่น ธนาคาร
โดยเขียนข้อความในอีเมลเชิงหลอกล่อ
เพื่อให้เหยื่อส่งข้อมูลส่วนตัวกลับไปให้ผู้ไม่หวังดี
หรือให้เหยื่อคลิกลิงก์ไปยังหน้าเว็บไซต์ปลอม

ปลอมเว็บไซต์

ให้ดูเหมือนเว็บไซต์ทางการเงิน เช่น ธนาคารออนไลน์
ซึ่งเป็นช่องทางที่นำไปสู่บัญชีเก็บเงินของลูกค้า
เมื่อเหยื่อหลงเชื่อกรอกข้อมูลรหัสประจำตัว และ Password
ผู้ไม่หวังดีก็สามารถเข้าถึงและทำธุรกรรมทางการเงินของเราได้ทันที

คำแนะนำ

1 URL

ไม่คลิกลิงก์ที่แนบมาในอีเมลของคนที่เรา
ไม่รู้จัก ถ้าต้องการเข้าเว็บไซต์นั้นจริง ๆ
ขอให้พิมพ์ URL ด้วยตัวเอง

2 E-Mail

ระวังอีเมลที่ขอให้ส่งข้อมูลส่วนตัวกลับไป
หรือ อีเมลที่มาพร้อมกับลิงก์

3 HTTPS

โดยปกติธนาคารจะใช้งาน HTTPS เพื่อป้องกันการโจมตี
ทางเครือข่าย ดังนั้นควรสังเกตให้แน่ใจว่าเว็บไซต์ที่ทำ
ธุรกรรมออนไลน์เป็น HTTPS ก่อนให้ข้อมูลส่วนตัว

*แต่บางครั้งหน้าเว็บไซต์ปลอมก็มีการเปิดใช้งาน HTTPS เช่นกัน ดังนั้นผู้ใช้ควรตรวจสอบ URL ให้ถูกต้องด้วย

4 ANTI-VIRUS

ติดตั้งโปรแกรมแอนติไวรัส แอนติสแปม และไฟร์วอลล์
และหมั่นอัปเดตโปรแกรมให้เป็นเวอร์ชันล่าสุดเสมอ

ช่องทางช่วยเหลือ

HELP & SUPPORT

หากพบเห็นเว็บไซต์หลอกลวงซึ่งมีจุดประสงค์ในการขโมยข้อมูลส่วนบุคคล สามารถแจ้งได้ที่เจ้าของบริการเหล่านั้น
หรือติดต่อ ThaiCERT, a Member of ETDA **อีเมล report@thaicert.or.th** หรือ **โทร. 02-123-1212 ตลอด 24 ชั่วโมง**

ThaiCERT | ThaiCERT | thaicert.or.th

ThaiCERT Thailand Computer Emergency Response Team a member of ETDA

ETDA สพธอ www.etda.or.th

Ministry of ICT Smart Thailand