แจ้งเตือน !!! Phishing ภัยล่าสุดทางอินเตอร์เน็ตใกล้ตัวที่ท่านไม่ควรมองข้าม

เนื่องจากมีกลุ่มมิจฉาชีพ ทำการปลอมแปลง e-mail หรือ website เพื่อหลอกลวงให้ผู้ใช้กรอกข้อมูลส่วนบุคคล ได้แก่ Username, Password หรือหมายเลขบัตรประชาชน เพื่อต่ออายุการใช้งาน e-mail ได้แก่ hotmail หรือ gmail เป็นต้น และเมื่อกรอกข้อมูลดังกล่าวแล้ว ในภายหลังไม่สามารถเข้าใช้งาน e-mail นั้นได้

กลุ่มมิจฉาชีพได้นำข้อมูลส่วนบุคคลดังกล่าวไปสร้างความเสียหาย เช่น การปลอมตัวเป็นเจ้าของ e-mail นั้นและส่งข้อความไปหลอกลวง/ฉ้อโกงทรัพย์สินเงินทองจากผู้ที่ท่านรู้จัก (Contact list) ว่าท่านกำลังเดือดร้อนและให้โอนเงินมาให้ตามบัญชีที่ระบุไว้

Phishing คืออะไร

Phishing (ออกเสียงเหมือนคำว่า Fishing) คือ การหลอกลวงขั้นสูงทางอินเตอร์เน็ตในรูปแบบของการปลอมแปลง e-mail หรือข้อความที่สร้างขึ้นเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลส่วนตัว หรือข้อมูลทางด้านการเงิน ได้แก่ ชื่อผู้ใช้ (Username), รหัสผ่าน (Password) หมายเลขบัตรประจำตัว และหมายเลขบัตรเครดิต

Phishing สามารถทำได้โดยการส่ง e-mail หรือข้อความที่อ้างว่ามาจากองค์กรต่างๆ ที่ท่านติดต่อด้วย เช่น บริษัทให้บริการ Internet หรือ ธนาคาร โดยส่งข้อความเพื่อขอให้ท่าน "อัพเดท" หรือ "ยืนยัน" ข้อมูลส่วนบุคคลของท่าน หากท่านไม่ตอบกลับ e-mail ดังกล่าว อาจก่อให้เกิดผลเสียตามมาได้

เพื่อให้ e-mail ปลอมที่ส่งมานั้นดูสมจริง ผู้ส่ง e-mail ลวงนี้จะใส่ hyperlink ที่ e-mail เพื่อให้เหมือนกับ URL ขององค์กรนั้นๆ จริง ซึ่งแท้ที่จริงแล้วมันคือเว็บไซต์ปลอม หรือหน้าต่างที่สร้างขึ้น หรือที่เราเรียกว่า "เว็บไซต์ปลอมแปลง" (Spoofed Website)

เมื่อท่านเข้าสู่เว็บไซต์ปลอมเหล่านี้ ท่านอาจถูกล่อลวงให้กรอกข้อมูลส่วนตัวที่จะถูกส่งไปยังผู้ผลิตเว็บไซต์ลวงเหล่านี้ เพื่อนำข้อมูลของท่านไปใช้ประโยชน์ เช่น หลอกลวง/ฉ้อโกงทรัพย์สินเงินทองจากกลุ่มรายชื่อ หรือ contact list ของท่าน โดยหลอกว่าท่านกำลังเดือดร้อนและต้องการให้โอนเงินด่วน, การซื้อสินค้า, การสมัครบัตรเครดิต หรือแม้แต่ทำสิ่งผิดกฎหมายอื่นๆ ในนามของท่าน

วิธีการป้องกันและรับมือกับการถูกโจมตีแบบ phishing

1. หยุดคิดและพิจารณาข้อมูลที่ได้รับทางe-mail หรือข้อมูลที่เข้าไปดูในเว็บไซต์ทุกครั้ง
2. ควรลบข้อมูลที่น่าสงสัยนั้นทิ้งทันที
3. หากมีความจำเป็นต้องกรอกหรือส่งข้อมูลใดทางเว็บไซต์ ต้องพิจารณาความน่าเชื่อถือของเว็บไซต์ดังกล่าวว่ามีตัวตนหรือมีการรับรองหรือไม่ หากไม่แน่ใจควรติดต่อไปยังเจ้าของเว็บไซต์หรือเจ้าของสถาบันการเงินดังกล่าว เพื่อสอบถามข้อมูลและยืนยันข้อมูลก่อนการดำเนินการใดๆ
4. ไม่ควรเข้าไปในเว็บไซต์หรือรันไฟล์ที่แนบมากับ e-mail ซึ่งมาจากบุคคลที่ไม่รู้จัก หรือไม่มั่นใจว่าผู้ส่งเป็นใคร หรือไม่ทราบว่าไฟล์ดังกล่าวเป็นไฟล์อะไร ตลอดจนเว็บไซต์หรือไฟล์ที่ถูกส่งมาด้วยโปรแกรมสนทนาประเภทต่างๆ เช่น IRC, ICQ, MSN หรือ PIRCH เป็นต้น
5. ติดตั้งโปรแกรมปรับปรุงช่องโหว่ (patch) ของทุกซอฟแวร์ที่มีการใช้อยู่ในเครื่องคอมพิวเตอร์ของท่านอยู่เสมอ

คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสารของรัฐสภา

(ข้อมูลอ้างอิง : http://www.thaicert.nectec.or.th/
ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย)