เตือนภัยไซเบอร์...รับมือ Hacker จู่โจม

Phishing วิธีการหลอกลวงให้ผู้ใช้งานอินเทอร์เน็ตหลงเชื่อ โดยส่วนใหญ่ Hacker จะปลอมแปลง email หรือ website ติดต่อกับผู้ใช้งานแล้วนำข้อมูลส่วนตัวของเหยื่อไปใช้ในทางที่ไม่ถูกต้อง

จำนวนครั้งของการโจมตีด้วย Phishing ที่ตรวจจับได้

ไตรมาส 2 ปี 2563

เวียดนาม	อินโดนีเซีย	มาเลเซีย	ไทย
219,653	213,638	137,427	103,378

Hacker เป็นภัยร้ายที่สร้างความเสียหายให้แก่ผู้ประกอบการอย่างต่อเนื่อง โดยเฉพาะในช่วง COVID-19 ระบาด เนื่องจากผู้ซื้อและผู้ขายเปลี่ยนมาติดต่อกันผ่านอินเทอร์เน็ตแทน จึงเปิดช่องให้อาชญากรไซเบอร์เข้ามาแสวงหาผลประโยชน์มากขึ้น สอดคล้องกับผลสำรวจจาก Kaspersky บริษัทด้านความปลอดภัยทางไซเบอร์ระดับโลก ซึ่งเปิดเผยว่าในช่วงไตรมาส 2 ปี 2563 มีความพยายามโจมตีบริษัทขนาดกลาง (พนักงาน 50-250 คน) ในเอเชียตะวันออกเฉียงใต้ ด้วยวิธีการ Phishing เพิ่มขึ้น 24.3% จากช่วงเดียวกันของปีก่อน และในช่วงครึ่งแรกของปี 2563 มีภัยคุกคามทางไซเบอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้สูงถึงกว่า 268 ล้านครั้ง

นอกจากนี้ มีข้อสังเกตว่าปัจจุบัน Hacker พัฒนาวิธีหลอกลวงได้แนบเนียนขึ้นมาก **จากเดิมที่ผู้ประกอบการมักจับพิรุธได้ทันทีที่ได้รับ email แจ้งขอเปลี่ยนบัญชีปลายทางที่ต้องโอนเงินค่าสินค้าเป็นบัญชีใหม่ซึ่งอยู่คนละประเทศกับบัญชีเดิม แต่ปัจจุบันพบว่า Hacker เปลี่ยนมาใช้วิธี email แจ้งให้เปลี่ยนบัญชีปลายทางเป็นอีกบัญชีหนึ่งที่อยู่ในประเทศเดียวกันกับบัญชีเดิม** ทำให้ผู้ซื้อไม่ทันระวังตัวจนเกิดความสูญเสีย ดังตัวอย่างล่าสุดที่เกิดขึ้นกับ “นายชอบค้า”

“นายชอบค้า” ทำการค้ากับ “บริษัท A” ซึ่งเป็นผู้ส่งออกสินค้าอยู่ในประเทศจีน โดยใช้ email เป็นเครื่องมือหลักในการติดต่อสั่งซื้อสินค้าและแจ้งธุรกรรมการโอนเงินค่าซื้อ-ขายสินค้าระหว่างกัน ล่าสุดเมื่อใกล้ถึงกำหนดที่ “นายชอบค้า” จะต้องชำระเงินค่าสินค้าก็ได้รับ email จาก “บริษัท A” แจ้งขอเปลี่ยนแปลงบัญชีรับโอนเงินชำระค่าสินค้า ซึ่งเปลี่ยนทั้งชื่อบริษัทผู้ขายและธนาคารผู้รับเงินใหม่แต่ยังเป็นประเทศจีนเหมือนเดิม โดยอ้างว่าบริษัทถูกหน่วยงานราชการของจีนตรวจสอบบัญชีอยู่ แม้ “นายชอบค้า”จะเกิดความสงสัยแต่เห็นว่า email ที่ “บริษัท A” ติดต่อมายังเป็น email เดิมที่ใช้ติดต่อกันเป็นประจำ อีกทั้งบัญชีใหม่ที่ให้โอนเงินเป็นบัญชีที่อยู่ในประเทศเดิม จึงไม่น่าจะมีปัญหาอะไร เพราะ “นายชอบค้า” เคยได้ยินมาว่า Hacker มักจะ email แจ้งเปลี่ยนบัญชีรับโอนชำระค่าสินค้าเป็นบัญชีที่เปิดในประเทศแถบยุโรป เช่น ผู้ขายอยู่ในจีนแต่ให้เปลี่ยนไปโอนเงินเข้าบัญชีที่อยู่ในฝรั่งเศส ทำให้ “นายชอบค้า” ไม่คิดว่าตนเองกำลังตกเป็นเป้าจู่โจมของ Hacker จึงโอนเงินค่าสินค้าเข้าบัญชีใหม่ตามที่ได้รับแจ้งมา ก่อนจะพบว่าตนเองเสียรู้ให้กับ Hacker ไปแล้ว

สิ่งที่ต้องฉุกคิดในการใช้ email ติดต่อกับผู้ขาย

- มี email จากผู้ขายขอเปลี่ยนเลขที่บัญชี ชื่อธนาคาร และประเทศ จากที่เคยตกลงกันไว้
- ชื่อผู้ขายและผู้รับชำระเงินปลายทางเป็นคนละคนกัน
- ประเทศของผู้รับเงินกับธนาคารผู้รับเงินอยู่คนละประเทศกัน
- Email ของผู้ขายเปลี่ยนแปลงไป อาทิ มีตัวอักษรเพิ่มขึ้น เช่นจากชื่อ Somsri เป็น Somsrii (มี i เพิ่มมาตอนท้าย 1 ตัว)
- รูปแบบตัวอักษร (front) ในเอกสารไม่เหมือนเดิม หรือมีการใช้ตัวอักษรหลายรูปแบบในเอกสารเดียวกัน

วิธีป้องกันตัวเบื้องต้นจากการถูก Hacker หลอกลวง

มีข้อตกลงกับคู่ค้าว่าหากมีการเปลี่ยนแปลงหมายเลขบัญชีปลายทาง หรือชื่อคู่ค้า จะต้องมีการยืนยันเป็นลายลักษณ์อักษร

ทุกครั้งที่มีการเปลี่ยนแปลงข้อมูลการโอนเงินเราควรตรวจสอบกับคู่ค้าผ่านช่องทางอื่นนอกเหนือจาก email อาทิ โทรศัพท์หรือโทรสารหาคู่ค้าโดยตรง

ตอบ email โดยไม่ใช้ปุ่ม Reply แต่ใช้วิธีพิมพ์หรือคัดลอกที่อยู่ email หรือเลือก email จาก Contact ที่เก็บไว้ในเครื่องคอมพิวเตอร์

หมั่นดูแลระบบรักษาความปลอดภัยของคอมพิวเตอร์ให้รัดกุม อาทิ ใช้ 2 Step Verification ระมัดระวังการติดตั้งหรือดาวน์โหลดโปรแกรมที่สุ่มเสี่ยงและไม่น่าเชื่อถือ และ Update โปรแกรมป้องกันไวรัสคอมพิวเตอร์อย่างสม่ำเสมอ