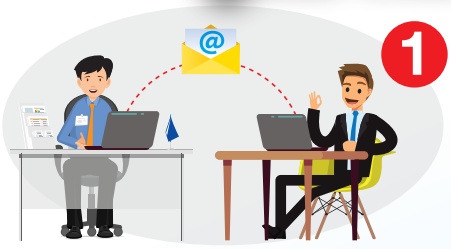
รู้ทันเกมการค้าโลก...
รู้ทัน Hacker ภัยจากโลก Cyber



1 นายชอบซื้อติดต่อสั่งซื้อสินค้าจาก Mr. John ซึ่งเป็นชาวต่างชาติที่รู้จักค้าขายกันมานาน โดยทั้งสองใช้ E-mail เป็นช่องทางหลักในการติดต่อสั่งซื้อสินค้า และส่งเอกสารระหว่างกัน

2 การสั่งซื้อทาง E-mail เป็นไปอย่างราบรื่น โดยทั้งคู่ไม่รู้ตัวว่ามี Hacker แอบลอบเข้าสู่ระบบ E-mail ของ Mr. John แล้ว

3 Hacker รู้รายละเอียดการสั่งซื้อสินค้า จำนวนเงินค่าสินค้า ชื่อธนาคาร และเลขที่บัญชีการโอนเงิน และคอยติดตามความเคลื่อนไหวของทั้งสองคนอย่างเงียบๆ ผ่านการสื่อสารทาง E-mail ระหว่างกัน จนกระทั่งถึงขั้นตอนการชำระเงินค่าสินค้า

4 พอได้จังหวะเหมาะ Hacker ก็สวมรอยเป็น Mr. John และส่ง E-mail จาก Mr. John ไปหานายชอบซื้อ แจ้งขอเปลี่ยนบัญชีที่ใช้รับโอนเงินชำระค่าสินค้าเป็นบัญชีชื่อ Mr. John แต่เปลี่ยนธนาคาร เลขที่บัญชี และประเทศรับเงินปลายทางเป็นประเทศในยุโรป* ซึ่งเป็นคนละประเทศกับ Mr. John ตัวจริง

5 นายชอบซื้อเกิดความสงสัยจึงส่ง E-mail กลับไปถามย้ำอีกครั้ง และก็ได้รับ E-mail ยืนยันการเปลี่ยนแปลงจาก Mr. John โดยไม่ทราบว่าแท้จริงแล้ว Hacker สวมรอยเป็น Mr. John และตอบยืนยันแทน

6 เพื่อความรอบคอบนายชอบซื้อติดต่อมาที่ EXIM BANK และได้รับคำแนะนำให้ตรวจสอบกลับไปยัง Mr. John อีกครั้ง โดยใช้ช่องทางอื่น เช่น การโทรศัพท์ หรือ Fax แทนการสอบถามทาง E-mail

7 เมื่อตรวจสอบก็พบว่า Mr. John ไม่ได้แจ้งขอให้เปลี่ยนบัญชี และบัญชีที่แจ้งให้ตรวจสอบไม่ใช่บัญชีของ Mr. John

** ธนาคารในยุโรปส่วนใหญ่ใช้ระบบการโอนเงินแบบ Straight Through Processing ซึ่งระบบจะนำเงินเข้าบัญชีของลูกค้าธนาคารโดยอัตโนมัติหากเลขที่บัญชีถูกต้อง*

การป้องกันการโจมตีจาก Hacker

- ควรตั้ง Password ที่เดาได้ยาก และหมั่นเปลี่ยน Password อย่างสม่ำเสมอ
- เปิดใช้ 2-Step Verification
- ระมัดระวังการติดตั้งหรือดาวน์โหลดโปรแกรมที่สุ่มเสี่ยงและไม่น่าเชื่อถือ
- ควรหมั่นสังเกตความผิดปกติต่างๆ และหากมีข้อสงสัยควรตรวจสอบกับคู่ค้าผ่านช่องทางอื่น อาทิ โทรศัพท์ หรือ Fax นอกเหนือจากทาง E-mail แต่เพียงช่องทางเดียว

“ส่งออกอย่างมั่นใจ ปรึกษา EXIM BANK”

EXIM THAILAND ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย โทร. 0 2617 2111 www.exim.go.th