

Anti-Phishing Awareness

ING Life Limited

February 2007

ทำความรู้จัก Phishing (1)

- Phishing (ฟิชซิง) คือกระบวนการหลอกลวงให้ลูกค้าเปิดเผยข้อมูลทางการเงิน หรือข้อมูลส่วนบุคคลอื่นๆ โดยใช้เทคนิคที่ทันสมัยผ่านทาง อีเมล เว็บไซต์ หรือช่องทางอื่นๆ เพื่อให้ผู้โจมตี (phisher) สามารถเข้าถึงบัญชีการเงินของลูกค้า และทำธุรกรรมจากบัญชีของลูกค้าได้โดยมิชอบ
- ในปัจจุบัน กระบวนการ Phishing นิยมทำผ่าน 3 ช่องทาง

1. อีเมล (email based phishing)

อีเมลเหล่านี้จะถูกส่งไปยังลูกค้าโดยพยายามลวงให้ลูกค้าเข้าใจผิดว่า อีเมลนี้ส่งมาจากองค์กรหรือสถาบันที่ลูกค้าติดต่ออยู่

เนื้อหาของอีเมลจะโน้มน้าวให้ลูกค้าคลิกลิงค์ไปยังเว็บไซต์ปลอมที่ถูกสร้างเลียนแบบเว็บไซต์สถาบันการเงินที่น่าเชื่อถือ เพื่ออัปเดตข้อมูลส่วนตัวของตนหรือเพื่อทำธุรกรรมอื่นๆ ทั้งนี้ที่ลูกค้ากรอกข้อมูลผู้ใช้ และรหัสผ่านของตน phisher จะบันทึกข้อมูลเหล่านั้น และนำมาใช้เข้าบัญชีจริงของลูกค้าเพื่อทำธุรกรรมในเว็บไซต์จริง

2. ทางโทรศัพท์ (phishing by phone)

ลูกค้าอาจได้รับโทรศัพท์จากบุคคลซึ่งแสดงตนว่ามาจากสถาบันการเงินหรือองค์กรที่เชื่อถือได้ อ้างว่าองค์กรมีปัญหาทางระบบ ต้องการให้ลูกค้าแจ้ง อัพเดทข้อมูลส่วนตัว เช่น เลขบัญชี, เลขบัตรประชาชน, รหัสผ่าน เป็นต้น หลังจากที่ลูกค้าให้ข้อมูลของตนแล้ว phisher จะบันทึกและนำข้อมูลเหล่านั้นมาใช้เข้าบัญชีจริงของลูกค้าเพื่อทำธุรกรรมต่อไป

3. ทางไวรัส (Trojan horse)

Phisher สามารถจู่โจมเครื่องคอมพิวเตอร์ลูกค้าหรือพนักงานด้วยไวรัส Trojan horse ไวรัสนี้จะเข้าก่อวินาศกรรมการทำงานของคอมพิวเตอร์และโปรแกรมการอ่านเอกสารทางอินเทอร์เน็ต Trojan horse สามารถจับข้อมูลการพิมพ์ของคีย์บอร์ดเมื่อลูกค้าเยี่ยมชมเว็บไซต์ทางการเงิน ด้วยวิธีนี้ phisher สามารถรวบรวมรหัสชื่อผู้ใช้ และรหัสผ่านของลูกค้าและสามารถทำธุรกรรมจากบัญชีของลูกค้าได้โดยมิชอบ

แจ้งเหตุการณ์ Phishing ได้ที่นี่

อาชญากรรมทางอินเทอร์เน็ตหรือ phishing เป็นภัยที่เริ่มแพร่หลายมากขึ้นในปัจจุบันและเป็นสิ่งที่เราทุกคนไม่ควรมองข้าม ทั้งนี้ความเสียหายที่เกิดจากภัย phishing ไม่เพียงแค่สร้างความไม่พอใจแก่ลูกค้าโดยตรง แต่ยังส่งผลกระทบต่อในแง่ลบแก่ชื่อเสียงบริษัทอันอาจนำมาซึ่งความเสียหายทางการเงินอีกด้วย

เพื่อให้บริษัทสามารถป้องกันและจัดการภัยจากอาชญากรรมเหล่านี้ได้อย่างมีประสิทธิภาพ ING จึงมีนโยบาย anti-phishing (แอนติ-ฟิชซิง) ขึ้น โดยมาตรการจะควบคุมและจัดการผ่าน 4 ช่องทางหลักดังนี้

1. มาตรการทางระบบ IT
2. มาตรการป้องกันและจัดการบนเว็บไซต์ต่างๆของบริษัท
3. มาตรการป้องกันทาง call center และ agency support
4. มาตรการฝึกอบรมแก่พนักงานทั่วไป

ทั้งนี้หากท่านได้รับการแจ้งภัย phishing จากลูกค้าหรือได้รับอีเมล, โทรศัพท์ หรือพบความผิดปกติในระบบการทำงานของคอมพิวเตอร์อันเป็นเหตุให้สงสัยว่าท่านอาจเป็นเหยื่อของอาชญากรรม phishing โปรดแจ้งเหตุการณ์โดยทันทีที่ antiphishing@inglife.co.th

