

# ฟิชซิง (PHISHING)

ฟิชซิง (Phishing) เป็นเทคนิคการหลอกลวงทางอินเทอร์เน็ตประเภทหนึ่ง ซึ่งมักจะมาในรูปแบบของการปลอมแปลงอีเมล หรือข้อความที่สร้างขึ้น เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลทางการเงินหรือข้อมูลส่วนตัวต่าง ๆ เช่น ชื่อบัญชีผู้ใช้ รหัสผ่าน หมายเลขบัตรเครดิต และหมายเลขบัตรประจำตัวประชาชน เป็นต้น

ผู้ประสงค์ร้ายจะส่งอีเมลหลอกลวงโดยใช้ชื่อผู้ส่งและเนื้อความที่น่าเชื่อถือ โดยเป็นข้อความในลักษณะแจ้งเตือน และเร่งให้ดำเนินการหากไม่ต้องการให้เกิดผลเสีย เมื่อเหยื่อหลงเชื่อ ก็จะดำเนินการตามความต้องการของผู้ประสงค์ร้าย เช่น เข้าเว็บไซต์เพื่อกรอกข้อมูลส่วนตัว รหัสผ่าน หรือตอบกลับอีเมลด้วยข้อมูลส่วนตัว เป็นต้น

## วิธีการสังเกตอีเมลหลอกลวง

**Sender:** ThaiBank <thaibank@phishing.com> **1** — ชื่อผู้ส่งอีเมลคล้ายกับธนาคาร หรือผู้ที่มีความน่าเชื่อถือ

**To:** customer@abc.com

**Subject:** Emergency

.....

**Username:** **2** — อาจมีการขอชื่อบัญชีและรหัสผ่าน

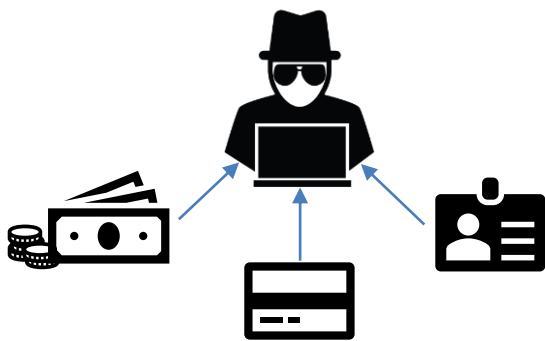
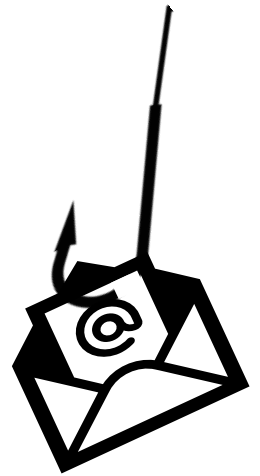
**Password:**

.....

**http://login.thaibank.com/** **3** — ชื่อเว็บไซต์ที่น่าสงสัย ซึ่งอาจจะปลอมให้ใกล้เคียงกับชื่อเว็บไซต์ของธนาคาร บางครั้งชื่อเว็บไซต์ที่อยู่ในอีเมลไม่ตรงกับลิงค์ หรือถึงการใช้ชื่อเว็บไซต์รูปแบบย่อ (Short URL)  
<http://login.phishing.com>

Best regards,  
 ThaiBank

Notice ..... **4** — ข้อความแจ้งเตือนว่า เร่งด่วน หรือสำคัญมาก ให้รีบดำเนินการตามเนื้อความในอีเมล



## ผลกระทบที่อาจเกิดขึ้น

- สูญเสียทรัพย์สินหรือเงินในบัญชีธนาคาร
- สูญเสียข้อมูลสำคัญ เช่น รหัสผ่าน เลขที่บัตรเครดิต และข้อมูลส่วนตัวต่าง ๆ เป็นต้น
- สูญเสียชื่อเสียงจากการส่งข้อมูลต่อไปให้ยังรายชื่อผู้ติดต่อ หรือการแอบอ้างชื่อของเหยื่อในการกระทำความผิดอื่นต่อไป

## วิธีการป้องกัน

1. อย่าหลงเชื่อลิงค์ที่มาพร้อมกับอีเมลที่ไม่แน่ใจแหล่งที่มา โดยห้ามเปิดลิงค์แนบอย่างเด็ดขาด
2. ห้ามเปิดเผยข้อมูลส่วนตัวใด ๆ ผ่านการร้องขอผ่านทางอีเมล หากไม่แน่ใจให้ทำการติดต่อกลับไปยังธนาคารโดยตรง
3. หากพบอีเมลที่สงสัยว่าจะเป็นฟิชซิงที่เกี่ยวข้องกับธนาคาร กรุณาติดต่อธนาคารทันที
4. ในกรณีหลงเชื่อและเปิดเผยรหัสผ่านแล้ว ให้ติดต่อไปยังธนาคารเพื่อทำการเปลี่ยนรหัสผ่านทันที