

การสร้างความรู้ความเข้าใจเพื่อป้องกันการหลอกลวงทางออนไลน์ (Scammer)



สท. เตือน ! ระวัง! เฟกปลอม

อบจ. เทศบาล อบต. และหน่วยงานของรัฐ

ลักษณะเฟกปลอม

- 1 ชื่อเฟกสะกดผิด หรือใช้โลโก้คล้ายของจริง
- 2 888 เฟกสร้างเฟก ผู้ติดตามน้อย
- 3 โพสต์แจกเงิน ทุจริต ลงทุน หรือรับสิทธิพิเศษ
- 4 ส่งลิงก์หรือ QR Code ให้กด
- 5 ขอเลขบัตรประชาชน เลขบัญชี หรือ OTP

วิธีป้องกัน

- 1 ตรวจสอบชื่อเฟกและเครื่องหมายยืนยัน
- 2 เข้าเว็บไซต์หรือเฟกทางการของหน่วยงานโดยตรง
- 3 ไม่กดลิงก์จากข้อความแปลก
- 4 ไม่เปิดเผยข้อมูลส่วนบุคคลและ OTP
- 5 โทรสอบถามหน่วยงานก่อนเชื่อ

จำไว้! หน่วยงานของรัฐ ไม่มีนโยบายให้โอนเงินเพื่อรับสิทธิ และไม่ขอรหัส OTP



กรมส่งเสริมการปกครองท้องถิ่น
DEPARTMENT OF LOCAL ADMINISTRATION

ไม่เชื่อ ไม่รับ ไม่โอน

ด้วยความปรารถนาดีจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น



รู้ทัน กลโกง หยุดอาชญากรรมไซเบอร์

คาถาป้องกันภัย “ไม่เชื่อ - ไม่รับ - ไม่โอน”

3 คำง่าย ๆ ที่ช่วยป้องกันคุณจากมิจฉาชีพออนไลน์

1 กลโกงยอดฮิตที่ต้องระวัง

ปลอมเป็นเจ้าหน้าที่รัฐ เทศบาล / อบต. - อ้างเป็นหน่วยงานหลอก - ขอหักดิลก - ขอโอนเงิน	เฟกปลอม / เว็บไซต์ปลอม - แฉกของรางวัล - รับสิทธิพิเศษ - หลอกรอกข้อมูล	SMS / ลิงก์ปลอม - ส่งลิงก์ที่แปลก - หลอกล่อติดตั้งแอป - ดูดข้อมูล	ขอรหัส OTP - ขอเลขบัตรประชาชน - ขอเลขบัญชี - ขอ OTP	หลอกลวงลงทุนออนไลน์ - ผลตอบแทนสูง - ทำไวเร็ว - ไม่มีความเสี่ยง
--	--	--	--	---

2 จำให้ขึ้นใจ 3 คาถา “ไม่”

ไม่เชื่อ - ไม่เชื่อข้อความที่เร่งรัด - ไม่มีความน่าเชื่อถือ - ตรวจสอบกับหน่วยงานโดยตรง	ไม่รับ - อย่ากดลิงก์ - อย่ารับไฟล์ข้อมูล - ตั้งสติ ตรวจสอบก่อน	ไม่โอน - ไม่โอนเงินให้คนแปลกหน้า - ไม่โอนเพื่อรับสิทธิ - ไม่โอนเพื่อยืนยันตัวตน
--	--	---

3 หากสงสัยว่าถูกหลอก

ตั้งสติ หยุดการกระทำ	เก็บหลักฐาน - รูปภาพ - แชท - เลขบัญชี - ลิงก์	แจ้งความออนไลน์ www.thaipoliceonline.go.th	ติดต่อธนาคารทันที เพื่ออายัดบัญชี
---------------------------------	---	---	--

4 สัญญาณเตือน

รับโอนเงิน	รับหักดิลก	ขอ OTP	ขอข้อมูลส่วนตัว	อ้างเป็นเจ้าหน้าที่รัฐ	ผลตอบแทนสูงเกินจริง
------------	------------	--------	-----------------	------------------------	---------------------

อย่าหลงเชื่อ! มิจฉาชีพแฝงตัวมาในทุกรูปแบบ ป้องกันไว้ก่อน จะไม่ตกเป็นเหยื่อ

ไม่เชื่อ ไม่รับ ไม่โอน
ปลอดภัยกว่า 100%

ศูนย์ AOC 1441
สายด่วนภัยออนไลน์
พร้อมช่วยเหลือตลอด 24 ชั่วโมง

ด้วยความห่วงใยจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น

ระวัง!

“รักออนไลน์” อาจเป็นกับดักหลอกโอนเงิน

ลูกหลานช่วยกันดูแลผู้สูงอายุ ก่อนตกเป็นเหยื่อ **Romance Scam**

มีจาชีพ **ไม่ได้หลอกด้วยกำลัง แต่หลอกด้วยความไว้วางใจ**

ตัวอย่างโปรไฟล์ปลอม

Alexander James
@alex.james.world
Entrepreneur | Investor | World Traveler
Lives in Singapore

ข้อมูลน่าสนใจ

- เพิ่งรู้จักไม่นาน ขอโอนเงินแล้ว
- ไม่เคยวิดีโอคอล หรือหาข้ออ้างตลอด
- รูปโปรไฟล์ดูเกินจริง / อาจเป็น AI

สัญญาณเตือนที่ควรระวัง

- โปรไฟล์ดีเกินจริง**
 - รูปหล่อ สวย ดูมีฐานะ
 - อาจใช้ภาพ AI หรือรูปคนอื่น
- ักมาหาวน รวดเร็ว**
 - เรียก “คิ๊ง” “คิ๊งคิ๊ง”
 - สร้างความสนิท ไม่เวลาไม่นาน
- สุดท้ายจบที่เรื่องเงิน**
 - ขอค่ารถเช่า / ค่าตั๋วเครื่องบิน
 - ค่าภาษี / ขอร่วมลงทุน
 - อ้างติดปัญหาชั่วคราว
- ไม่เคยเจอหน้าจริง**
 - อ้างติดงาน / อยู่ต่างประเทศ
 - วิดีโอคอลไม่ได้

4 ขั้นตอนของแก๊ง Romance Scam

- สร้างโปรไฟล์ปลอมให้น่าเชื่อถือ
- ักแซด คอยหวาน สร้างความผูกพัน
- อ้างเหตุฉุกเฉิน ขอความช่วยเหลือ
- หลอกให้โอนเงิน แล้วตัดการติดต่อ

ที่รักครับ คิดถึงนะ 10:30

ตอนนี้ผมมีปัญหา ต้องใช้เงินด่วนครับ 10:31

ช่วยโอนเงินให้หน่อยนะครับ เดี๋ยวจะคืนให้แน่นอน 10:32

คุณใจดีมากครับผม 10:33

จำไว้

ไม่เชื่อ • ไม่รับ • ไม่โอน

หากไม่เคยพบตัวจริง **อย่าโอนเงินเด็ดขาด!**

ลูกหลาน ช่วยผู้ใหญ่ได้

ด้วยความห่วงใยจาก กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น กรมส่งเสริมการปกครองท้องถิ่น

หากสงสัยว่าเป็นมิจฉาชีพ แจ้งความออนไลน์ www.thaipoliceonline.go.th

สายด่วนตำรวจไซเบอร์ **1441**

เด็กก็เสี่ยง! “เปิดบัญชีม้า”

อย่าหลงเชื่อ “งานง่าย รายได้ดี” อาจเป็นกับดักของสแกมเมอร์

สแกมเมอร์มักหลอกด้วยคำโฆษณา

- เปิดบัญชี รับ 2,000 บาท
- แค่สแกนหน้า ได้เงินทันที
- งานออนไลน์ ไม่ต้องลงทุน

Facebook
LINE
เกมออนไลน์
TikTok

สิ่งที่สแกมเมอร์ต้องการ

บัตรประชาชน → บัญชีธนาคาร → เบอร์โทรศัพท์ → Mobile Banking → สแกนใบหน้า (Face Scan)

นำไปใช้เป็น “บัญชีม้า” รับ-โอนเงินจากการหลอกหลวง

มิจฉาชีพโอนเงินจากการหลอกหลวง → เข้าบัญชีม้า → โอนต่อ/ถอนเงินออก → นำเงินไปใช้

ผลที่ตามมา

- บัญชีถูกใช้รับเงินจากการหลอกหลวง
- อาจถูกดำเนินคดีฐานเกี่ยวข้องกับ “บัญชีม้า” ผิดกฎหมาย
- บัญชีถูกอายัด ไม่สามารถใช้งานได้
- มีประวัติไม่ดี กระทบอนาคต เรียนต่อ ทำงาน สมัครงาน

วิธีป้องกัน

- ไม่เปิดบัญชีให้ใคร
- ไม่ให้ยืมบัญชีหรือซิม
- ไม่สแกนหน้าให้คนแปลกหน้า
- ไม่ส่ง OTP หรือรหัสผ่าน
- หากถูกชักชวนรับบริการ ผู้ปกครอง ครู หรือแจ้งตำรวจ

เงินง่าย... อาจแลกด้วยอนาคต

ไม่เชื่อ ไม่รับ ไม่โอน

กรมส่งเสริมการปกครองท้องถิ่น

พบเห็นการหลอกหลวง แจ้งได้! | สายด่วนตำรวจไซเบอร์ 1441 | สายด่วน AOC 1441 | แจ้งความออนไลน์ www.thaipoliceonline.com