



เด็กที่เสี่ยง! “เปิดบัญชีม้า” อย่าหลงเชื่อ

สแกนเมอร์มิกหลอกด้วยคำโฆษณา

เปิดบัญชี รับ 2,000 บาท

แค่สแกนหน้า ได้เงินทันที

งานออนไลน์ ไม่ต้องลงทุน



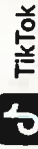
Facebook



LINE

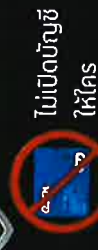


เกมออนไลน์



TikTok

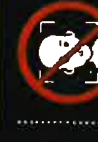
วิธีป้องกัน



ไม่เปิดบัญชี
ให้ใคร



ไม่ให้ยืมบัญชี
หรือซิม



ไม่สแกนหน้า
ให้คนแปลกหน้า



ไม่ส่ง OTP
หรือรหัสผ่าน



หากถูกชักชวน
รับปรึกษา ผู้ปกครอง ครู
หรือแจ้งตำรวจ

สิ่งที่สแกนเมอร์ต้องการ



บัตรประชาชน



บัญชีธนาคาร



เบอร์
โทรศัพท์



Mobile
Banking



สแกนใบหน้า
(Face Scan)

นำไปใช้เป็น “บัญชีม้า” รับ-โอนเงินจากการหลอกหลวง



มีอาจชีพโอนเงิน
จากการหลอกหลวง



เข้าบัญชีม้า



โอนต่อ/ถอนเงินออก



นำเงินไปใช้

ผลที่ตามมา



บัญชีถูกใช้รับเงิน
จากการหลอกหลวง



อาจถูกดำเนินคดีฐาน
เกี่ยวข้องกัน “บัญชีม้า”
ผิดกฎหมาย



บัญชีถูกอายัด
ไม่สามารถใช้งานได้



มีประวัติไม่ดี
กระทบอนาคต
เรียนต่อ ทำงาน สมัครงาน

ด้วยความห่วงใยจาก



กองป้องกันและบรรเทา
สาธารณภัยท้องถิ่น

กรมส่งเสริมการปกครองท้องถิ่น

เงินง่าย... อาจแลกด้วยอนาคต ไม่เชื่อ ไม่รับ ไม่โอน

พบเห็นการหลอกหลวง แจ้งได้ทันที



สายด่วนตำรวจไซเบอร์ 1441



สายด่วน AOC 1441



แจ้งความออนไลน์

www.thaipoliceonline.com



“รักออนไลน์” อาจเป็นกับดักหลอกโอนเงิน

Romance Scam

ลูกหลานช่วยกันดูแลผู้สูงวัย ก่อนตกเป็นเหยื่อ

มีจาวซีพ ไม่ได้หลอกด้วยกำลัง แต่หลอกด้วยความไวใจ

ตัวอย่างโปรไฟล์ปลอม



สัญญาณเตือนที่ควรระวัง

โปรไฟล์ดีเกินจริง

- รูปหล่อ สวย ดูภูมิฐาน
- อาจใช้ภาพ AI หรือขโมยรูปคนอื่น

ที่มาหวาน รวดเร็ว

- เรียก “พี่รัก” “พี่ดัง”
- สร้างความสนิทในเวลาไม่นาน

สุดท้ายจบที่เรื่องเงิน

- ขอค่ารักษา / ค่าตัวเครื่องบิน
- ค่าภาษี / ขอร่วมลงทุน
- อ้างติดปัญหาชั่วคราว

ไม่เคยเจอหน้าจริง

- อ้างติดงาน / อยู่ต่างประเทศ
- วิดีโอคอลไม่ได้

4 ขั้นตอนของแก๊ง Romance Scam

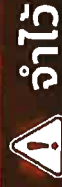
- สร้างโปรไฟล์ปลอม**
ให้น่าเชื่อถือ
- ทักแชต คุยหวาน**
สร้างความผูกพัน
- อ้างเหตุฉุกเฉิน**
ขอความช่วยเหลือ
- หลอกให้โอนเงิน**
แล้วตัดการติดต่อ

ที่รักครับ คิดถึงนะ 10:30

ตอนนี้มีปัญหา ต้องใช้เงินด่วนครับ 10:31

ช่วยโอนเงินให้หน่อยนะครับ เดี่ยวจะคืนให้แน่นอน 10:32

คุณคือคนพิเศษของผม 10:33

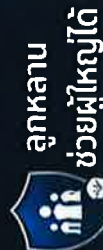


จำไว้

ไม่เชื่อ • ไม่รับ • ไม่โอน

หากไม่เคยพบตัวจริง

อย่าโอนเงินเด็ดขาด!



ด้วยความห่วงใยจาก กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น กรมส่งเสริมการปกครองท้องถิ่น

ด้วยความห่วงใยจาก

กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น กรมส่งเสริมการปกครองท้องถิ่น

หากสงสัยว่าเป็นมิจฉาชีพ

แจ้งความออนไลน์

www.thaipoliceonline.go.th

สายด่วนตำรวจไซเบอร์

1441

เห็นผู้สูงวัยคุยกับคนแปลกหน้าออนไลน์

อย่าดู อย่าซ้ำ

แต่ช่วยกันตรวจสอบก่อนเงินจะหาย





รู้ทัน กลโกง หยุดอาชญากรรมไซเบอร์



คาตาป้องกันภัย “ไม่เชื่อ - ไม่รับ - ไม่โอน”

3 คำง่าย ๆ ที่ช่วยป้องกันคุณจากมิจฉาชีพออนไลน์

1 กลโกงยอดฮิตที่ต้องระวัง



ปลอมเป็นเจ้าหน้าที่รัฐ
เทศบาล / อบต.

- ▲ อ้างเป็นหน่วยงานหลัก
- ▲ ขอให้กดลิงก์
- ▲ ขอโอนเงิน



เฟสปลอม /
เว็บไซต์ปลอม

- ▲ แอดของรางวัล
- ▲ รับสิทธิพิเศษ
- ▲ หลอกกรอกข้อมูล



SMS /
ลิงก์ปลอม

- ▲ ส่งลิงก์ที่แปลก
- ▲ หลอกติดดั่งแอป
- ▲ ดูปข้อมูล



ขอรหัส OTP

- ▲ ขอเลขบัตรประชาชน
- ▲ ขอเลขบัญชี
- ▲ ขอ OTP



หลอกลงทุนออนไลน์

- ▲ ผลตอบแทนสูง
- ▲ กำไรเร็ว
- ▲ ไม่มีความเสี่ยง

2 จำให้ขึ้นใจ 3 คาตา “ไม่”



ไม่เชื่อ

- ✓ ไม่เชื่อข้อความที่เร่งรัด
- ✓ ไม่มีความน่าเชื่อถือ
- ✓ ตรวจสอบกับหน่วยงานโดยตรง



ไม่รับ

- ✓ อย่ากดลิงก์
- ✓ อย่ารับไฟล์ข้อมูล
- ✓ ตั้งสติ ตรวจสอบก่อน



ไม่โอน

- ✓ ไม่โอนเงินให้คนแปลกหน้า
- ✓ ไม่โอนเพื่อรับสิทธิ์
- ✓ ไม่โอนเพื่อขึ้นชั้นตัวตน

3 หากสงสัยว่าถูกหลอก



ตั้งสติ
หยุดการทำธุรกรรม



เก็บหลักฐาน

- ✓ รูปภาพ
- ✓ แชท
- ✓ เลขบัญชี
- ✓ ลิงก์



แจ้งความออนไลน์
www.thaipoliceonline.go.th



ติดต่อธนาคารทันที
เพื่ออายัดบัญชี

4 สัญญาณเตือน



รับโอนเงิน



รับให้กดลิงก์



ขอ OTP



ขอข้อมูล
ส่วนตัว



อ้างเป็น
เจ้าหน้าที่รัฐ



ผลตอบแทน
สูงเกินจริง



อย่าหลงเชื่อ!

มีอาชีพแฝงตัวในทุกรูปแบบ
ป้องกันไว้ก่อน จะไม่ตกเป็นเหยื่อ



ไม่เชื่อ ไม่รับ ไม่โอน
ปลอดภัยกว่า 100%



ศูนย์ AOC 1441
สายด่วนภัยออนไลน์
พร้อมช่วยเหลือตลอด 24 ชั่วโมง



ด้วยความห่วงใยจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น

! สด. เตือน! ระวัง! เพลปลอม

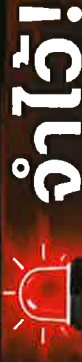
อบจ. เทศบาล อบต. และหน่วยงานของรัฐ

ลักษณะเพลปลอม

- 1  ชื่อเพลสะกดผิด หรือใช้โลโก้คล้ายของจริง
- 2  2555 เพิ่งสร้างเพล ผู้ติดตามน้อย
- 3  โฟสต์แจกเงิน ทุเงิน ลงทุน หรือรับสิทธิพิเศษ
- 4  ส่งลิงก์หรือ QR Code ให้กด
- 5  ขอเลขบัตรประชาชน เลขบัญชี หรือ OTP

วิธีป้องกัน

- 1  ตรวจสอบชื่อเพล และเครื่องหมายยืนยัน
- 2  เข้าเว็บไซต์หรือเพจทางการของหน่วยงานโดยตรง
- 3  ไม่กดลิงก์จากข้อความแปลก
- 4  ไม่เปิดเผยข้อมูลส่วนบุคคลและ OTP
- 5  โทรสอบถามหน่วยงานก่อนเชื่อ



จำไว้!

หน่วยงานของรัฐ ไม่เป็นนโยบายให้โอนเงินเพื่อรับสิทธิ และไม่ขอรหัส OTP



กรมส่งเสริมการปกครองท้องถิ่น
DEPARTMENT OF LOCAL ADMINISTRATION

ไม่เชื่อ ไม่รับ ไม่โอน



ด้วยความปรารถนาดีจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น



มีอาชีพร
แอมอ้างเป็น
หน่วยงานรัฐ
หลอกลวงประชาชน