



เด็กก็เสี่ยง! “เปิดบัญชีม้า” อย่าหลงเชื่อ

สแกมเมอร์มักหลอกด้วยคำโฆษณา

เปิดบัญชี รับ 2,000 บาท

แค่สแกนหน้า ได้เงินทันที

งานออนไลน์ ไม่ต้องลงทุน



Facebook



LINE



เกมออนไลน์



TikTok



วิธีป้องกัน



ไม่เปิดบัญชีให้ใคร



ไม่ให้ยืมบัญชีหรือ ชีน



ไม่สแกนหน้าให้คนแปลกหน้า



ไม่ส่ง OTP หรือรหัสผ่าน



หากถูกชักชวนรับปรึกษา ผู้ปกครอง ครู หรือแจ้งตำรวจ

“งานง่าย รายได้ดี”

อาจเป็นกับดักของสแกมเมอร์

สิ่งที่สแกมเมอร์ต้องการ



บัตรประชาชน



บัญชีธนาคาร



เบอร์โทรศัพท์



Mobile Banking



สแกนใบหน้า (Face Scan)

นำไปใช้เป็น “บัญชีม้า” รับ-โอนเงินจากการหลอกลวง



มีจลาชีพโอนเงินจากการหลอกลวง



เข้าบัญชีม้า



โอนต่อ/ถอนเงินออก



นำเงินไปใช้



ผลที่ตามมา



บัญชีถูกใช้รับเงินจากการหลอกลวง



อาจถูกดำเนินคดีฐานที่เกี่ยวข้องกับ “บัญชีม้า” ผิดกฎหมาย



บัญชีถูกอายัด ไม่สามารถใช้งานได้



มีประวัติไม่ดี กระทบอนาคต เรียนต่อ ทำงาน สมัครงาน



ด้วยความห่วงใยจาก

กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น

กรมส่งเสริมการปกครองท้องถิ่น

เงินง่าย... อาจแลกด้วยอนาคต ไม่เชื่อ ไม่รับ ไม่โอน

พบเห็นการหลอกลวง แจ้งได้ที่



สายด่วนตำรวจไซเบอร์ 1441

สายด่วน AOC 1441



แจ้งความออนไลน์ www.thaipoliceonline.com



ระวัง!

“รักออนไลน์” อาจเป็นกับดักหลอกโอนเงิน

ลูกหลานช่วยกันดูแลผู้สูงอายุ ก่อนตกเป็นเหยื่อ **Romance Scam**

มิจฉาชีพ ไม่ได้หลอกด้วยกำลัง แต่หลอกด้วยความไว้วางใจ

ตัวอย่างโปรไฟล์ปลอม

Alexander James

@alex.james.world

Entrepreneur | Investor | World Traveler

Lives in Singapore

ข้อมูลน่าสนใจ

- เพิ่งรู้จักกันไม่นาน ขอโอนเงินแล้ว
- ไม่เคยวิดีโอคอล หรือหาช่องทางติดต่อ
- รูปโปรไฟล์ดูดีเกินจริง / อาจเป็น AI

สัญญาณเตือนที่ควรระวัง

- โปรไฟล์ดีเกินจริง**
 - รูปหล่อ สวย ดูภูมิฐาน
 - อาจใช้ภาพ AI หรือขโมยรูปคนอื่น
- ักมาหวาน รวดเร็ว**
 - เรียก “ที่รัก” “คิดถึง”
 - สร้างความสนิทใจในเวลาไม่นาน
- สุดท้ายจบที่เรื่องเงิน**
 - ขอคำปรึกษา / คำตัวเครื่องบิน
 - คำภาซี / ขอร่วมลงทุน
 - อ้างติดปัญหาชั่วคราว
- ไม่เคยเจอหน้าจริง**
 - อ้างติดงาน / อยู่ต่างประเทศ
 - วิดีโอคอลไม่ได้

4 ขั้นตอนของแก๊ง Romance Scam

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

ที่รักครับ คิดถึงนะ

10:30

ตอนนี้ผมมีปัญหา

10:31

ช่วยโอนเงินให้หน่อยนะครับ

10:32

คุณคือคนพิเศษของผม

10:33

จำไว้

ไม่เชื่อ • ไม่รับ • ไม่โอน
หากไม่เคยพบตัวจริง
อย่าโอนเงินเด็ดขาด!



ลูกหลาน
ช่วยผู้ใหญ่ได้



พูดคุยและ
เตือนภัย
เป็นประจำ



ช่วยตรวจสอบ
รูปภาพ
และโปรไฟล์



หากถูกขอเงิน
ให้รีบรายงาน
ครอบครัวก่อน



อย่ารีบโอน
แม้ชักนำ
จะเร่งรัด

เห็นผู้สูงอายุคุยกับคนแปลกหน้าออนไลน์

อย่าดู อย่าซ้ำ

แต่ช่วยกันตรวจสอบก่อนเงินจะหาย



ด้วยความห่วงใยจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น



หากสงสัยว่าเป็นมิจฉาชีพ
แจ้งความออนไลน์
www.thaipoliceonline.go.th



สายด่วนตำรวจไซเบอร์
1441



รู้ทัน กลโกง หยุดอาชญากรรมไซเบอร์

คาถาป้องกันภัย “ไม่เชื่อ - ไม่รับ - ไม่โอน”

3 คำง่าย ๆ ที่ช่วยป้องกันคุณจากมิจฉาชีพออนไลน์



1 กลโกงยอดฮิตที่ต้องระวัง

ปลอมเป็นเจ้าหน้าที่รัฐ
เทศบาล / อบต.

- ▲ อ้างเป็นหน่วยงานหลอก
- ▲ ขอให้กดลิงก์
- ▲ ขอโอนเงิน

เพจปลอม /
เว็บไซต์ปลอม

- ▲ แจกของรางวัล
- ▲ รับสิทธิ์พิเศษ
- ▲ หลอกกรอกข้อมูล

SMS /
ลิงก์ปลอม

- ▲ ส่งลิงก์ที่แปลก
- ▲ หลอกติดตั้งแอป
- ▲ ดูดข้อมูล

ขอรหัส OTP

- ▲ ขอเลขบัตรประชาชน
- ▲ ขอเลขบัญชี
- ▲ ขอ OTP

หลอกลงทุนออนไลน์

- ▲ ผลตอบแทนสูง
- ▲ ทำได้เร็ว
- ▲ ไม่มีความเสี่ยง

2 จำให้ขึ้นใจ 3 คาถา “ไม่”

ไม่เชื่อ

- ✓ ไม่เชื่อข้อความที่เร่งรัด
- ✓ ไม่มีความน่าเชื่อถือ
- ✓ ตรวจสอบกับหน่วยงานโดยตรง

ไม่รับ

- ✓ อย่ากดลิงก์
- ✓ อย่ารับไฟล์ข้อมูล
- ✓ ตั้งสติ ตรวจสอบก่อน

ไม่โอน

- ✓ ไม่โอนเงินหากคนแปลกหน้า
- ✓ ไม่โอนเพื่อรับสิทธิ์
- ✓ ไม่โอนเพื่อยืนยันตัวตน

3 หากสงสัยว่าถูกหลอก

✅ ตั้งสติ
หยุดการทำธุรกรรม

เก็บหลักฐาน

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

✅ แจ้งความออนไลน์
www.thaipoliceonline.go.th

✅ ติดต่อธนาคารทันที
เพื่อยกบัญชี

4 สัญญาณเตือน

รับโอนเงิน

รับให้กดลิงก์

ขอ OTP

ขอข้อมูล
ส่วนตัว

อ้างเป็น
เจ้าหน้าที่รัฐ

ผลตอบแทน
สูงเกินจริง



อย่าหลงเชื่อ!

มิจฉาชีพแฝงตัวมาในทุกรูปแบบ
ป้องกันไว้ก่อน จะไม่ตกเป็นเหยื่อ



ไม่เชื่อ ไม่รับ ไม่โอน
ปลอดภัยกว่า 100%



ศูนย์ AOC **1441**
สายด่วนภัยออนไลน์
พร้อมช่วยเหลือตลอด 24 ชั่วโมง



ด้วยความห่วงใยจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น

! สด. เตือน ! ระวัง! เฟกปลอม

อบจ. เทศบาล อบต. และหน่วยงานของรัฐ



มิดาซีฟ
แอปอ้างเป็น
หน่วยงานรัฐ
หลอกลวงประชาชน

ลักษณะเฟกปลอม

- 1  ชื่อเพจ **สะกดผิด** หรือใช้โลโก้คล้ายของจริง
- 2  **2888** เพิ่งสร้างเพจ ผู้ติดตามน้อย
- 3  **โพสต์แจกเงิน** ทุเงิน ลงทุน หรือรับสิทธิพิเศษ
- 4  **ส่งลิงก์หรือ QR Code** ให้กด
- 5  **ขอเลขบัตรประชาชน เลขบัญชี หรือ OTP**

วิธีป้องกัน

- 1  ตรวจสอบชื่อเพจและเครื่องหมายยืนยัน
- 2  เข้าเว็บไซต์หรือ **เพจทางการ** ของหน่วยงานโดยตรง
- 3  **ไม่กดลิงก์** จากข้อความแปลก
- 4  **ไม่เปิดเผย** ข้อมูลส่วนบุคคลและ OTP
- 5  **โทรสอบถาม** หน่วยงานก่อนเชื่อ



จำไว้!

หน่วยงานของรัฐ **ไม่มีนโยบาย** ให้โอนเงินเพื่อรับสิทธิ และ **ไม่ขอรหัส OTP**



กรมส่งเสริมการปกครองท้องถิ่น
DEPARTMENT OF LOCAL ADMINISTRATION

ไม่เชื่อ ไม่รับ ไม่โอน



ด้วยความปรารถนาดีจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น