



เด็กก็เสี่ยง! “เปิดบัญชีม้า” อย่าหลงเชื่อ

สแกมเมอร์มักหลอกด้วยคำโฆษณา

เปิดบัญชี รับ 2,000 บาท

แค่สแกนหน้า ได้เงินทันที

งานออนไลน์ ไม่ต้องลงทุน



Facebook



LINE



เกมออนไลน์



TikTok

“งานง่าย รายได้ดี”

อาจเป็นกับดักของสแกมเมอร์

สิ่งที่สแกมเมอร์ต้องการ



นำไปใช้เป็น “บัญชีม้า” รับ-โอนเงินจากการหลอกลวง



ผลที่ตามมา



บัญชีถูกใช้รับเงิน
จากการหลอกลวง



อาจถูกดำเนินคดีฐาน
ที่เกี่ยวข้องกับ “บัญชีม้า”
ผิดกฎหมาย



บัญชีถูกอายัด
ไม่สามารถใช้งานได้



มีประวัติไม่ดี
กระทบอนาคต
เรียนต่อ ทำงาน สมัครงาน

วิธีป้องกัน



ไม่เปิดบัญชี
ให้ใคร



ไม่ให้ยืมบัญชี
หรือ PIN



ไม่สแกนหน้า
ให้คนแปลกหน้า



ไม่ส่ง OTP
หรือรหัสผ่าน



หากถูกชักชวน
รับปรึกษา ผู้ปกครอง ครู
หรือแจ้งตำรวจ



เงินง่าย... อาจแลกด้วยอนาคต ไม่เชื่อ ไม่รับ ไม่โอน

พบเห็นการหลอกลวง แจ้งได้ที่ | สายด่วนตำรวจไซเบอร์ 1441 | สายด่วน AOC 1441 | แจ้งความออนไลน์ www.thaipoliceonline.com



ด้วยความห่วงใยจาก
กองป้องกันและบรรเทา
สาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น



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

+ Add Friend Message ...

สัญญาณเตือนที่ควรระวัง

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

4 ขั้นตอนของแก๊ง Romance Scam

- 1** สร้างโปรไฟล์ปลอมให้น่าเชื่อถือ
- 2** ทักแชต คอยหวาน สร้างความผูกพัน
- 3** อ้างเหตุฉุกเฉิน ขอความช่วยเหลือ
- 4** หลอกให้โอนเงิน แล้วตัดการติดต่อ

ที่รักครับ คิดถึงนะ ❤️ 10:30

ตอนนี้ผมมีปัญหา ต้องใช้เงินด่วนครับ 😞 10:31

ช่วยโอนเงินให้หน่อยนะครับ เดี๋ยวจะคืนให้แน่นอน 10:32

คุณคือคนพิเศษของผม ❤️ 10:33

จำไว้

ไม่เชื่อ • ไม่รับ • ไม่โอน

หากไม่เคยพบตัวจริง

อย่าโอนเงินเด็ดขาด!

ลูกหลาน ช่วยผู้ใหญ่ได้

พูดคุยและเตือนกันเป็นประจำ

ช่วยตรวจสอบรูปภาพและโปรไฟล์

หากถูกขอเงิน ให้รีบรายงานให้ครอบครัวก่อน

อย่ารีบโอน แม้ชักนำจะเร่งรัด

เห็นผู้สูงอายุคุยกับคนแปลกหน้าออนไลน์

อย่าดู อย่าซ้ำ

แต่ช่วยกันตรวจสอบก่อนเงินจะหาย



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
- ▲ หลอกกดลิงก์แอป
- ▲ 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



มิจฉาชีพ
แอบอ้างเป็น
หน่วยงานรัฐ
หลอกลวงประชาชน

ลักษณะเฟกปลอม



- 1  ชื่อเพจ **สะกดผิด** หรือใช้โลโก้
คล้ายของจริง
- 2  888 **เพิ่งสร้างเพจ** ผู้ติดตามน้อย
- 3  **โพสต์แจกเงิน** ทุเงิน ลงทุน
หรือรับสิทธิพิเศษ
- 4  **ส่งลิงก์หรือ QR Code**
ให้กด
- 5  **ขอเลขบัตรประชาชน เลขบัญชี**
หรือ OTP

วิธีป้องกัน



- 1  ตรวจสอบชื่อเพจและเครื่องหมายยืนยัน
- 2  เข้าเว็บไซต์หรือ **เพจทางการ** ของหน่วยงาน
โดยตรง
- 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