

⚠️ สด. เตือน ! ระวัง! เพจปลอม

อบจ. เทศบาล อบต. และหน่วยงานของรัฐ



มิจาชีพ
แอบอ้างเป็น
หน่วยงานรัฐ
หลอกลวงประชาชน

ลักษณะเพจปลอม



- 1  ชื่อเพจ **สะกดผิด** หรือใช้โลโก้คล้ายของจริง
- 2  **เพิ่งสร้างเพจ** ผู้ติดตามน้อย
- 3  **โพสต์แจกเงิน** ทุจเงิน ลงทุน หรือรับสิทธิพิเศษ
- 4  ส่ง **ลิงก์** หรือ **QR Code** ให้กด
- 5  ขอ **เลขบัตรประชาชน** เลขบัญชี หรือ OTP

วิธีป้องกัน



- 1  ตรวจสอบชื่อเพจและเครื่องหมายยืนยัน
- 2  เข้าเว็บไซต์หรือเพจทางการของหน่วยงานโดยตรง
- 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



รู้ทัน กลโกง หยุดอาชญากรรมไซเบอร์

คาถาป้องกันภัย “**ไม่เชื่อ - ไม่รับ - ไม่โอน**”

3 คำง่าย ๆ ที่ช่วยป้องกันคุณจากมิจฉาชีพออนไลน์



1 กลโกงยอดฮิตที่ต้องระวัง



ปลอมเป็นเจ้าหน้าที่รัฐ
เทศบาล / อบต.

- ▲ อ้างเป็นหน่วยงานหลัก
- ▲ ขอให้กดลิงก์
- ▲ ขอให้ออมเงิน



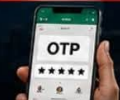
เพจปลอม /
เว็บไซต์ปลอม

- ▲ แจกของรางวัล
- ▲ รับสิทธิพิเศษ
- ▲ หลอกรอกข้อมูล



SMS /
ลิงก์ปลอม

- ▲ ส่งลิงก์ที่แปลก
- ▲ หลอกติดตั้งแอป
- ▲ ดูดข้อมูล



ขอรหัส OTP

- ▲ ขอเลขบัตรประชาชน
- ▲ ขอเลขบัญชี
- ▲ ขอ OTP



หลอกลวงทุนออนไลน์

- ▲ ผลตอบแทนสูง
- ▲ ทำได้เร็ว
- ▲ ไม่มีความเสี่ยง

2 จำให้ขึ้นใจ 3 คาถา “ไม่”



ไม่เชื่อ

- ✓ ไม่เชื่อข้อความที่เร่งรัด
- ✓ ไม่มีความน่าเชื่อถือ
- ✓ ตรวจสอบกับหน่วยงานโดยตรง



ไม่รับ

- ✓ อย่ากดลิงก์
- ✓ อย่ารับไฟล์ข้อมูล
- ✓ ตั้งสติ ตรวจสอบก่อน



ไม่โอน

- ✓ ไม่โอนเงินให้คนแปลกหน้า
- ✓ ไม่โอนเพื่อรับสิทธิ
- ✓ ไม่โอนเพื่อยืนยันตัวตน

3 หากสงสัยว่าถูกหลอก



✓ ตั้งสติ
หยุดการทำธุรกรรม



เก็บหลักฐาน
✓ รูปภาพ
✓ แชก
✓ เลขบัญชี
✓ ลิงก์



✓ แจ้งความออนไลน์
www.thaipoliceonline.go.th



✓ ติดต่อราชการทันที
เพื่ออายัดบัญชี

4 สัญญาณเตือน



รับให้โอนเงิน



รับให้กดลิงก์



ขอ OTP



ขอข้อมูล
ส่วนตัว



อ้างอิง
เจ้าหน้าที่รัฐ



ผลตอบแทน
สูงเกินจริง



อย่าหลงเชื่อ!

มิจฉาชีพแฝงตัวมาในทุกรูปแบบ
ป้องกันไว้ก่อน จะไม่ตกเป็นเหยื่อ



ไม่เชื่อ ไม่รับ ไม่โอน
ปลอดภัยกว่า 100%



ศูนย์ AOC **1441**

สายด่วนภัยออนไลน์
พร้อมช่วยเหลือตลอด 24 ชั่วโมง



ด้วยความห่วงใยจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น



ระวัง!

“รักออนไลน์” อาจเป็นกับดักหลอกโอนเงิน ลูกหลานช่วยกันดูแลผู้สูงวัย ก่อนตกเป็นเหยื่อ **Romance Scam**

มีจาชัพ ไม่ได้หลอกด้วยกำลัง แต่หลอกด้วยความไวใจ

ตัวอย่างโปรไฟล์ปลอม



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

ข้อมูลน่าสงสัย

- ! เพิ่งรู้จักกันไม่นาน ขอโอนเงินแล้ว
- ! ไม่เคยวิดีโอคอล หรือหาข้ออ้างตลอด
- ! รูปโปรไฟล์ดูดีเกินจริง / อาจเป็น AI

สัญญาณเตือนที่ควรระวัง

- โปรไฟล์ดีเกินจริง**
 - รูปหล่อ สวย ดูมีฐานะ
 - อาจใช้ภาพ AI หรือรูปโมยคนอื่น
- ักมาหวาน รวดเร็ว**
 - เรียก “ที่รัก” “คิดถึง”
 - สร้างความสนิทในเวลาไม่นาน
- สุดท้ายจบที่เรื่องเงิน**
 - ขอค่ารักษา / ค่าตัวเครื่องบิน
 - ค่าภาษี / ขอร่วมลงทุน
 - อ้างติดปัญหาชั่วคราว
- ไม่เคยเจอหน้าจริง**
 - อ้างติดงาน / อยู่ต่างประเทศ
 - วิดีโอคอลไม่ได้

4 ขั้นตอนของแก๊ง Romance Scam

- สร้างโปรไฟล์ปลอมให้น่าเชื่อถือ**
- ทักแชต คอยหวาน สร้างความผูกพัน**
- อ้างเหตุฉุกเฉิน ขอความช่วยเหลือ**
- 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

พูดคุยและเตือนภัยเป็นประจำ

ช่วยตรวจสอบรูปภาพและโปรไฟล์

หากถูกขอเงิน ให้ปรึกษาคนในครอบครัวก่อน

อย่ารีบโอน แม้จิกฝ่ายจะเร่งรัด

เห็นผู้สูงวัยคุยกับคนแปลกหน้าออนไลน์
อย่าดู อย่าซ้ำ
แต่ช่วยกันตรวจสอบก่อนเงินจะหาย



ด้วยความห่วงใยจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น

หากสงสัยว่าเป็นมีจาชัพ
แจ้งความออนไลน์
www.thaipoliceonline.go.th

สายด่วนตำรวจไซเบอร์
1441





ระวัง!

“รักออนไลน์” อาจเป็นกับดักหลอกโอนเงิน ลูกหลานช่วยกันดูแลผู้สูงวัย ก่อนตกเป็นเหยื่อ **Romance Scam**

มีจอาชีพ ไม่ได้หลอกด้วยกำลัง แต่หลอกด้วยความไวใจ

ตัวอย่างโปรไฟล์ปลอม



Alexander James

@alex.james.world

Entrepreneur | Investor | World Traveler

Lives in Singapore



ข้อมูลน่าสงสัย

- ! เพิ่งรู้จักกันไม่นาน ขอโอนเงินแล้ว
- ! ไม่เคยวิดีโอคอล หรือหาข้ออ้างตลอด
- ! รูปโปรไฟล์ดูดีเกินจริง / อาจเป็น AI

Add Friend

Message



สัญญาณเตือนที่ควรระวัง



โปรไฟล์ดีเกินจริง

- รูปหล่อ สวย ดูภูมิฐาน
- อาจใช้ภาพ AI หรือรูปคนอื่น



ักมาหวาน รวดเร็ว

- เรียก “ที่รัก” “คิดถึง”
- สร้างความสนิทในเวลาไม่นาน



สุดท้ายจบที่เรื่องเงิน

- ขอค่ารักษา / ค่าตัวเครื่องบิน
- ค่าภาษี / ขอร่วมลงทุน
- อ้างติดปัญหาชั่วคราว



ไม่เคยเจอหน้าจริง

- อ้างติดงาน / อยู่ต่างประเทศ
- วิดีโอคอลไม่ได้

4 ขั้นตอนของแก๊ง Romance Scam



1 สร้างโปรไฟล์ปลอม
ให้น่าเชื่อถือ



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



พูดคุยและ
เตือนภัย
เป็นประจำ



ช่วยตรวจสอบ
รูปภาพ
และโปรไฟล์



หากถูกขอเงิน
ให้ปรึกษาคนใน
ครอบครัวก่อน



อย่ารีบโอน
แม้ชักจูง
จะเร่งรัด

เห็นผู้สูงวัยคุยกับคนแปลกหน้าออนไลน์

อย่าดู อย่าซ้ำ

แต่ช่วยกันตรวจสอบก่อนเงินจะหาย



ด้วยความห่วงใยจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น



หากสงสัยว่าเป็นมิจฉาชีพ
แจ้งความออนไลน์
www.thaipoliceonline.go.th



สายด่วนตำรวจไซเบอร์
1441