



# สธ. เตือน !

## ระวัง! โฟวปลอม

อบจ. เทศบาล อบต. และหน่วยงานของรัฐ

### ลักษณะโฟวปลอม

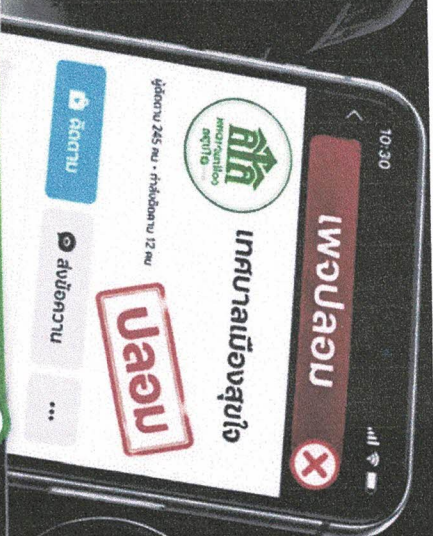


- 1 ชื่อเพจสะกดผิด หรือใช้โลโก้คล้ายของจริง
- 2 เพิ่งสร้างเพจ ผู้ติดตามน้อย
- 3 โฟวดีแถมเงิน ถูกลง สงกุน หรือรับสิทธิพิเศษ
- 4 ส่งลิงก์หรือ QR Code ให้กด
- 5 ขอเลขบัตรประชาชน เลขบัญชี หรือ OTP

### วิธีป้องกัน



- 1 ตรวจสอบชื่อเพจและเครื่องหมายยืนยัน
- 2 เข้าเว็บไซต์หรือเพจทางการของหน่วยงานโดยตรง
- 3 ไม่กดลิงก์จากข้อความแปลก
- 4 ไม่เปิดเผยข้อมูลส่วนบุคคลและ OTP
- 5 โทรสอบถามหน่วยงานก่อนเชื่อ



**ปัจจัยเสี่ยง**  
แอดอ้างเป็น  
หน่วยงานรัฐ  
หลอกลวงประชาชน



## จำไว้!

หน่วยงานของรัฐ ไม่เปิดเผยข้อมูลให้ผู้อื่นเพื่อรับสิทธิ และ ไม่ขอรหัส OTP



กรมส่งเสริมการปกครองท้องถิ่น  
DEPARTMENT OF LOCAL ADMINISTRATION

## ไม่เชื่อ ไม่รับ ไม่โอน



ด้วยความปรารถนาดีจาก  
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น  
กรมส่งเสริมการปกครองท้องถิ่น



# รู้ทัน กลโกง หยุดอาชญากรรมไซเบอร์



ฉลาดป้องกันภัย “**ไม่เชื่อ - ไม่รับ - ไม่โอน**”

3 คำง่าย ๆ ที่ช่วยป้องกันคุณจากมิจฉาชีพออนไลน์



## 1 กลโกงยอดฮิตที่ต้องระวัง

|                                                                                                                          |                                                                                                         |                                                                                             |                                                                                |                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| <p><b>ปลอมเป็นเจ้าหน้าที่รัฐ</b><br/>เทศบาล / อบต.</p> <p>▲ อ้างเป็นหน่วยงานหลัก<br/>▲ ข่มขู่กดดัน<br/>▲ ขโมยโอนเงิน</p> | <p><b>เพจปลอม / เว็บไซต์ปลอม</b></p> <p>▲ แจกของรางวัล<br/>▲ รับสิทธิพิเศษ<br/>▲ หลอกรอกรายชื่อยุติ</p> | <p><b>SMS / ลิงก์ปลอม</b></p> <p>▲ ส่งลิงก์ที่แปลก<br/>▲ หลอกล่อด้วยแอป<br/>▲ ดูดข้อมูล</p> | <p><b>ขอรหัส OTP</b></p> <p>▲ ขอลงบัญชีธนาคาร<br/>▲ ขอลงบัญชี<br/>▲ ขอ OTP</p> | <p><b>หลอกลวงออนไลน์</b></p> <p>▲ ผลตอบแทนสูง<br/>▲ ทำเร็ว<br/>▲ ไม่มีความเสี่ยง</p> |
|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|

## 2 จำให้ขึ้นใจ 3 คำว่า “ไม่”

|                                                                                                                     |                                                                                            |                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| <p><b>ไม่เชื่อ</b></p> <p>✓ ไม่เชื่อข้อความที่เร่งรัด<br/>✓ ไม่มีความน่าเชื่อถือ<br/>✓ ตรวจสอบกับหน่วยงานโดยตรง</p> | <p><b>ไม่รับ</b></p> <p>✓ อย่ากดลิงก์<br/>✓ อย่ารับไฟล์ข้อมูล<br/>✓ ดังสติ ตรวจสอบก่อน</p> | <p><b>ไม่โอน</b></p> <p>✓ ไม่โอนเงินให้แก่แปลกหน้า<br/>✓ ไม่โอนเพื่อรับสิทธิ<br/>✓ ไม่โอนเพื่อยืนยันตัวตน</p> |
|---------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|

## 3 หากสงสัยว่าถูกหลอก

|                                          |                                                                                |                                                                                                              |                                                     |
|------------------------------------------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| <p><b>แจ้งสติ</b><br/>หยุดการธุรกรรม</p> | <p><b>เก็บหลักฐาน</b></p> <p>✓ รูปภาพ<br/>✓ แอป<br/>✓ เลขบัญชี<br/>✓ ลิงก์</p> | <p><b>แจ้งความออนไลน์</b><br/><a href="http://www.thaipoliceonline.go.th">www.thaipoliceonline.go.th</a></p> | <p><b>ติดต่อธนาคารทันที</b><br/>เพื่ออายัดบัญชี</p> |
|------------------------------------------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|

## 4 สัญญาณเตือน

|                          |                             |                      |                               |                                      |                                   |
|--------------------------|-----------------------------|----------------------|-------------------------------|--------------------------------------|-----------------------------------|
| <p><b>รับโอนเงิน</b></p> | <p><b>รับให้กดลิงก์</b></p> | <p><b>ขอ OTP</b></p> | <p><b>ขอข้อมูลส่วนตัว</b></p> | <p><b>อ้างเป็นเจ้าหน้าที่รัฐ</b></p> | <p><b>ผลตอบแทนสูงเกินจริง</b></p> |
|--------------------------|-----------------------------|----------------------|-------------------------------|--------------------------------------|-----------------------------------|

**อย่าหลงเชื่อ!**

มิจฉาชีพแฝงตัวมาในทุกรูปแบบ  
ป้องกันไว้ก่อน จะไม่ตกเป็นเหยื่อ



**ไม่เชื่อ ไม่รับ ไม่โอน**  
ปลอดภัยกว่า 100%



ศูนย์ AOC **1441**  
สายด่วนภัยออนไลน์  
พร้อมช่วยเหลือตลอด 24 ชั่วโมง



ด้วยความห่วงใยจาก  
**กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น**  
กรมส่งเสริมการปกครองท้องถิ่น



# ระวัง!

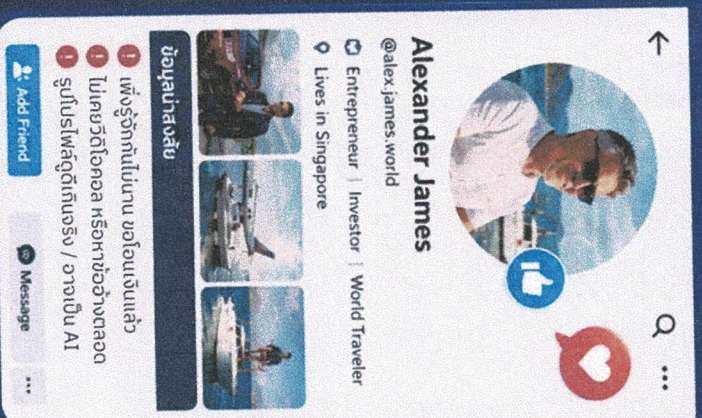
## “รักออนไลน์” อาจเป็นกับดักหลอกโอบเงิน

ลูกหลานช่วยกันดูแลผู้สูงอายุ ก่อนตกเป็นเหยื่อ

**Romance Scam**

**มีงานให้ ไม่ได้หลอกด้วยกำลัง แต่หลอกด้วยความไว้วางใจ**

ตัวอย่างโปรไฟล์ปลอม



สัญญาณเตือนที่ควรระวัง

**โปรไฟล์ดีเกินจริง**

- รูปหล่อสวย ดูมีฐานะ
- ว่างใช้ภาพ AI หรือใช้รูปคนอื่น

**ักบพหวน รวดเร็ว**

- เรียก “ที่รัก” “คิดถึง”
- สร้างความสนิทในเวลาไม่นาน

**สุดท้ายขอเบาะเรื่องเงิน**

- ขอค่ารักษา / ค่าตัวเครื่องบิน
- ค่าภาษี / ขอร่วมลงทุน
- อ้างติดปัญหาชั่วคราว

**ไม่เคยเจอหน้าจริง**

- อ้างติดงาน / อยู่ต่างประเทศ
- ระวังหลอกไปต่อ

4 ขั้นตอนของแก๊ง Romance Scam

1 สร้างโปรไฟล์ปลอม

ให้น่าเชื่อถือ

2 ักบพหวน รวดเร็ว

สร้างความผูกพัน

3 อ้างเหตุฉุกเฉิน

ขอความช่วยเหลือ

4 หลอกให้โอนเงิน

แล้วจัดการติดต่อ

**จำไว้**

**ไม่เชื่อ • ไม่รับ • ไม่โอน**  
หากไม่เคยพบตัวจริง  
**อย่าโอนเงินเด็ดขาด!**

เห็นผู้สูงอายุคุยกับคนแปลกหน้าออนไลน์  
**อย่าดู อย่าซ้ำ**  
แต่ช่วยกันตรวจสอบก่อนเงินจะหาย

**ลูกหลาน**  
ช่วยผู้ใหญ่ได้



พูดคุยและเตือนภัยเป็นประจำ



ช่วยตรวจสอบรูปภาพและโปรไฟล์



หากถูกขโมยเงินให้รีบรายงานในครอบครัว



อย่ารีบโอนแต่อีกฝ่ายจะเร่งรัด

หากสงสัยว่าเป็นมิจฉาชีพ  
แจ้งความออนไลน์  
[www.thaipoliceonline.go.th](http://www.thaipoliceonline.go.th)

สายด่วนตำรวจไซเบอร์  
**1441**



ด้วยความห่วงใยจาก  
**กองบังคับการและบรรเทาสาธารณภัยท้องถิ่น**  
กรมส่งเสริมการปกครองท้องถิ่น



# เตือนเสียง! “เปิดบัญชีม้า” อย่างหลงเชื่อ

สแกนเบอร์ม้าหลอกด้วยคำโฆษณา

เปิดบัญชี รับ 2,000 บาท

แค่สแกนหน้า ได้เงินทันที

งานออนไลน์ ไม่ต้องลงทุน



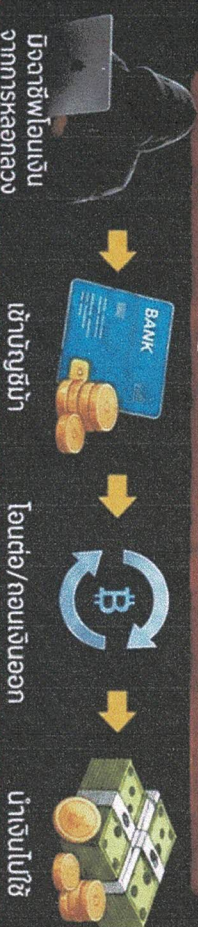
“งานง่าย รายได้ดี”

อาจเป็นกับดักของสแกนเนอร์

สิ่งทีสแกนเนอร์ต้องการ



นำไปใช้เป็น “บัญชีม้า” รับ-โอนเงินจากการหลอกหลวง



❌ ไม่เปิดบัญชีให้ใคร



❌ ไม่ให้ยืมบัญชีหรือซิม



❌ ไม่สแกนหน้าให้คนแปลกหน้า



❌ ไม่ส่ง OTP หรือรหัสผ่าน



✅ หากถูกชักชวนรับปรึกษา ผู้ปกครอง ครู หรือแจ้งตำรวจ



วิธีป้องกัน

เงินง่าย... อาจแลกด้วยอนาคต  
ไม่เชื่อ ไม่รับ ไม่โอน



กองป้องกันและบรรเทา  
สาธารณภัยท้องถิ่น

กรมส่งเสริมการปกครองท้องถิ่น

พบเห็นการหลอกหลวง แจ้งได้ที่



สายด่วนตำรวจไซเบอร์ 1441

สายด่วน AOC 1441



แจ้งความออนไลน์ [www.thaipoliceonline.com](http://www.thaipoliceonline.com)

ผลที่ตามมา



บัญชีถูกใช้รับเงิน  
จากการหลอกหลวง



อาจถูกดำเนินคดีฐาน  
เกี่ยวข้องกับ “บัญชีม้า”  
ผิดกฎหมาย



บัญชีถูกอายัด  
ไม่สามารถใช้งานได้



มีประวัติไม่ดี  
กระทบอนาคต  
เรียนต่อ ทำงาน สมัครงาน