

จับไต๋กลโกงออนไลน์: The Digital Self-Defense Playbook



คู่มือเผื่อระวังภัยผู้บริโภคมยุคใหม่

8 กลโกงที่พบบ่อย: รู้ทันก่อนตกเป็นเหยื่อ



ภัย #1: ร้านค้าล่อหน



ภัย #2: ลิงก์ลวงดูดเงิน



ภัย #3: สินค้ามายา (ไม่ตรงปก)



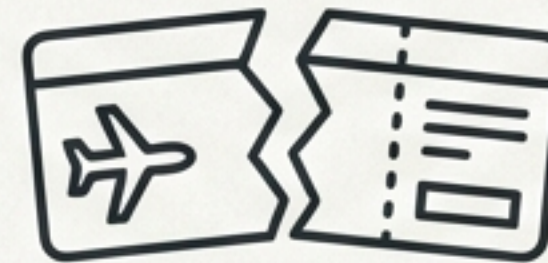
ภัย #4: กัดดักการลงทุน



ภัย #5: แอปเงินกู้เถื่อน



ภัย #6:
คลินิกเสริมความงามปลอม



ภัย #7: ทัวรทิพย์ ตัวผี



ภัย #8: อ้างเป็นเจ้าหน้าที่รัฐ

มาถอดรหัสแต่ละกลโกง เพื่อให้คุณนำหน้าหนึ่งก้าวเสมอ



ภัย #1: ร้านค้าล่อหน

พบบ่อยใน: Facebook, Instagram

ลักษณะ (The Lure)

เสนอสินค้าราคาถูกกว่าปกติอย่าง
น่าสงสัย

ไม่มีที่อยู่ร้านหรือข้อมูลนิติบุคคล
ที่ชัดเจน

เร่งรัดให้รีบตัดสินใจและโอนเงิน

สัญญาณเตือน (Red Flags)

🚩 ปิดช่องแสดงความคิดเห็น
หรือมีแต่คอมเมนต์หน้าม้า

🚩 เพจมีการเปลี่ยนชื่อบ่อยครั้ง

🚩 บัญชีรับโอนเป็นชื่อบุคคล
ธรรมดา

ป้องกัน (Your Defense)

🛡 ตรวจสอบประวัติเพจ (Page
Transparency) และดูรีวิวจาก
ผู้ซื้อจริงในหลายๆ แหล่ง

🛡 เลือกใช้ช่องทางการชำระเงินที่
คุ้มครองผู้ซื้อ (เช่น ผ่าน
แพลตฟอร์ม e-commerce)

🛡 ขอหลักฐานยืนยันตัวตนผู้ขาย
หากจำเป็น



ภัย #2: ลิงก์ลวงดูดเงิน (Phishing)

ลักษณะ (The Lure)

- อ้างว่าจะคืนเงินภาษี
- อ้างว่ามีพัสดุตกค้าง หรือได้รับรางวัลใหญ่
- สร้างเรื่องเร่งด่วนที่ต้องจัดการผ่านลิงก์ทันที

สัญญาณเตือน (Red Flags)

- 🚩 ส่งลิงก์แปลกๆ ไม่คุ้นตามมาทาง SMS, Line, หรือ Email
- 🚩 หน้าเว็บที่ลิงก์ไป ขอข้อมูลส่วนตัว, รหัสบัตรเครดิต, หรือ OTP
- 🚩 URL ของเว็บไซต์ไม่ตรงกับชื่อของหน่วยงานทางการ (เช่น .cc, .xyz แทนที่จะเป็น .go.th, .co.th)

ป้องกัน (Your Defense)

- 🛡️ ห้ามกดลิงก์เด็ดขาด หากไม่แน่ใจแหล่งที่มา
- 🛡️ พิมพ์ชื่อเว็บไซต์ของหน่วยงานทางการในเบราว์เซอร์โดยตรง
- 🛡️ หน่วยงานจริงจะไม่ขอข้อมูลบัตรหรือ OTP ผ่านลิงก์



ภัย #3: สินค้ามายา (ไม่ตรงปก)

ลักษณะ (The Lure)

- ใช้ภาพโฆษณาสวยงาม ดูดี เกินจริง
- สินค้าจริงที่ได้รับมีคุณภาพ ต่ำกว่าที่โฆษณาไว้มาก
- สินค้าไม่มีเครื่องหมาย มอก. หรือฉลากภาษาไทยกำกับ (สำหรับสินค้าที่ต้องมี)

สัญญาณเตือน (Red Flags)

- 🚩 นโยบายร้านระบุชัดเจนว่า "ไม่รับเปลี่ยนหรือคืนสินค้า"
- 🚩 ร้านค้าไม่สามารถออกใบเสร็จหรือใบกำกับภาษีได้
- 🚩 รีวิวสินค้ามีแต่ภาพสวยๆ ที่ดูเหมือนภาพจากอินเทอร์เน็ต ไม่ใช่ภาพจากผู้ซื้อจริง

ป้องกัน (Your Defense)

- ✅ เลือกร้านค้าที่มีนโยบายการคืนเงิน/คืนสินค้าที่ชัดเจนและเป็นธรรม
- ✅ อ่านรีวิวจากผู้ซื้อจริงอย่างละเอียด
- ✅ เก็บหลักฐานการสั่งซื้อและการชำระเงินไว้เสมอ



ภัย #4: กับดักการลงทุน

ลักษณะ (The Lure)

การันตีผลตอบแทนสูงในระยะ
เวลาสั้น

ชักชวนให้เข้าร่วมกลุ่มลงทุน
ลับใน Line หรือ Telegram

สร้างโปรไฟล์ปลอม โซเชียลฟ
สไต์ลัทธิหรือจากการลงทุน

สัญญาณเตือน (Red Flags)

🚩 โซเชียลกราฟหรือตัวเลขกำไร
ปลอมเพื่อสร้างความน่า
เชื่อถือ

🚩 ไม่เปิดเผยข้อมูลบริษัท หรือ
ไม่มีตัวตนจริง

🚩 กดดันให้รีบลงทุนเพิ่ม โดย
อ้างว่า "โอกาสมีจำกัด"

ป้องกัน (Your Defense)

🛡️ ตรวจสอบใบอนุญาตประกอบ
ธุรกิจจากหน่วยงานกำกับดูแล
(เช่น ก.ล.ต.) ก่อนเสมอ

🛡️ อย่าโอนเงินลงทุนเข้าบัญชีชื่อ
บุคคลธรรมดาเด็ดขาด

🛡️ การลงทุนมีความเสี่ยง ไม่มี
ผลตอบแทนใดที่ "การันตีได้"



ภัย #5: แอปเงินกู้เถื่อน

ลักษณะ (The Lure)

- อนุมัติง่ายและรวดเร็ว ไม่ตรวจสอบเครดิตบูโร
- ใช้แค่บัตรประชาชนใบเดียวก็กู้ได้
- โฆษณาผ่าน SMS หรือโซเชียลมีเดีย

สัญญาณเตือน (Red Flags)

- 🚩 เรียกเก็บค่าธรรมเนียมหรือค่าดำเนินการก่อนได้รับเงินกู้
- 🚩 แอปพลิเคชันขอสิทธิ์เข้าถึงข้อมูลส่วนตัวในโทรศัพท์ เช่น รายชื่อผู้ติดต่อ, รูปภาพ
- 🚩 อัตราดอกเบี้ยโหดและเงื่อนไขไม่ชัดเจน

ป้องกัน (Your Defense)

- 🛡️ เลือกใช้ผู้ให้บริการสินเชื่อที่ถูกต้องตามกฎหมายและอยู่ภายใต้การกำกับของธนาคารแห่งประเทศไทยเท่านั้น
- 🛡️ อย่าให้สิทธิ์แอปพลิเคชันเข้าถึงข้อมูลส่วนตัวโดยไม่จำเป็น
- 🛡️ ห้ามโอนเงินค่าธรรมเนียมใดๆ ก่อนได้รับอนุมัติ



ภัย #6: คลินิกเสริมความงามปลอม

ลักษณะ (The Lure)

- โฆษณาโปรโมชันหรือคอร์สราคาถูกเกินจริง
- ใช้ภาพ Before/After ที่เกินจริง
- กดดันหรือบังคับให้ซื้อแพ็คเกจใหญ่หลังเข้ารับบริการ

สัญญาณเตือน (Red Flags)

- ❗ ไม่แสดงใบอนุญาตประกอบสถานพยาบาลและใบประกอบวิชาชีพของแพทย์อย่างชัดเจน
- ❗ ไม่สามารถตอบคำถามเกี่ยวกับผลิตภัณฑ์หรือขั้นตอนการรักษาได้อย่างละเอียด
- ❗ สถานที่ดูไม่สะอาด ไม่ได้มาตรฐาน

ป้องกัน (Your Defense)

- ✅ ตรวจสอบใบอนุญาตของสถานพยาบาลและแพทย์จากเว็บไซต์ของแพทยสภา
- ✅ อย่าหลงเชื่อโฆษณาเกินจริง และอย่าตัดสินใจซื้อคอร์สภายใต้ความกดดัน
- ✅ ขอใบเสร็จรับเงินที่ระบุรายละเอียดการบริการชัดเจนทุกครั้ง



ภัย #7: ทัวรทิพย์ ตัวผี

ลักษณะ (The Lure)

- เสนอขายแพ็คเกจทัวร์หรือตั๋วเครื่องบินในราคาที่ถูกกว่าตลาดมาก
- มักมาในรูปแบบโปรไฟล์ใหม่หรือโปรหลุดจอง

สัญญาณเตือน (Red Flags)

- ❏ ไม่มีสัญญาณการเดินทางที่ชัดเจน หรือไม่ออกเอกสารการจองที่เป็นทางการให้
- ❏ หลังจากโอนเงินมัดจำแล้ว ผู้ขายเริ่มบ่ายเบี่ยง เลื่อนการเดินทาง หรือติดต่อไม่ได้
- ❏ บริษัทไม่มีที่อยู่เป็นหลักแหล่ง ตรวจสอบไม่ได้

ป้องกัน (Your Defense)

- 🛡 ตรวจสอบทะเบียนผู้ประกอบการธุรกิจนำเที่ยวเกี่ยวกับกรมการท่องเที่ยว
- 🛡 เลือกซื้อกับบริษัททัวร์ที่มีชื่อเสียงและน่าเชื่อถือ
- 🛡 ชำระเงินผ่านช่องทางที่ตรวจสอบได้ และเก็บหลักฐานทุกอย่างไว้



ภัย #8: อ้างเป็นเจ้าหน้าที่รัฐ

ลักษณะ (The Lure)

- โทรศัพท์หรือ Line อ้างว่าเป็นตำรวจ, เจ้าหน้าที่สรรพากร, หรือพนักงานธนาคาร
- ใช้จิตวิทยาข่มขู่ว่าคุณพัวพันกับคดีร้ายแรง หรือมีหนี้สิน/บัญชีผิดปกติ

สัญญาณเตือน (Red Flags)

- ▶ สร้างความตกใจและกดดันให้โอนเงินเพื่อตรวจสอบทันที
- ▶ ขอข้อมูลส่วนตัวทั้งหมด เช่น เลขบัตรประชาชน, รหัสผ่าน, OTP
- ▶ ห้ามไม่ให้คุณวางสายหรือปรึกษาใคร

ป้องกัน (Your Defense)

- 🛡️ **วางสายทันที** นี่คือการขึ้นตอนที่สำคัญที่สุด
- 🛡️ อย่าให้ข้อมูลส่วนตัวใดๆ ทั้งสิ้น
- 🛡️ หากไม่สบายใจ ให้โทรกลับไปเบอร์ทางการของหน่วยงานนั้นๆ โดยตรง (ค้นหาเบอร์จากเว็บไซต์ทางการ) เพื่อตรวจสอบข้อเท็จจริง

หากตกเป็นผู้เสียหาย: 3 ขั้นตอนที่ต้องทำทันที

- 1 ตั้งสติและรวบรวม**
Action: เก็บหลักฐานทั้งหมดที่มี
Details: ภาพหน้าจอแชต, สลิปการโอนเงิน, ลิงค์ URL, ชื่อบัญชี, ใบเสร็จ (ถ้ามี)
- 2 ระบุและติดต่อ**
Action: ติดต่อธนาคารทันที
Details: ติดต่อธนาคารทันที
Details: เพื่อระบุบัญชีหรือบัตรเครดิตที่ใช้ทำธุรกรรม ลดความเสียหายเพิ่มเติม
- 3 แจ้งและร้องเรียน**
Action: ดำเนินการทางกฎหมาย
 - แจ้งความกับตำรวจ ณ สถานีตำรวจใกล้บ้าน หรือผ่านระบบออนไลน์
 - ร้องเรียนหน่วยงานคุ้มครองผู้บริโภค
 - แจ้งแพลตฟอร์มที่เกิดเหตุ (Facebook, Shopee, Lazada, TikTok) เพื่อให้ระงับร้านค้า/บัญชีของมิจฉาชีพ

คุณคือด่านป้องกันที่ดีที่สุด



กลโกงออนไลน์เปลี่ยนรูปแบบไปเรื่อยๆ แต่หลักการป้องกันยังคงเหมือนเดิม:
คิด ก่อนเชื่อ, **เช็ก** ก่อนโอน, และ **แชร์** ความรู้นี้ให้คนรอบข้าง

เฝ้าระวังอย่างชาญฉลาด เพื่อให้โลกดิจิทัลเป็นพื้นที่ที่ปลอดภัยสำหรับทุกคน