

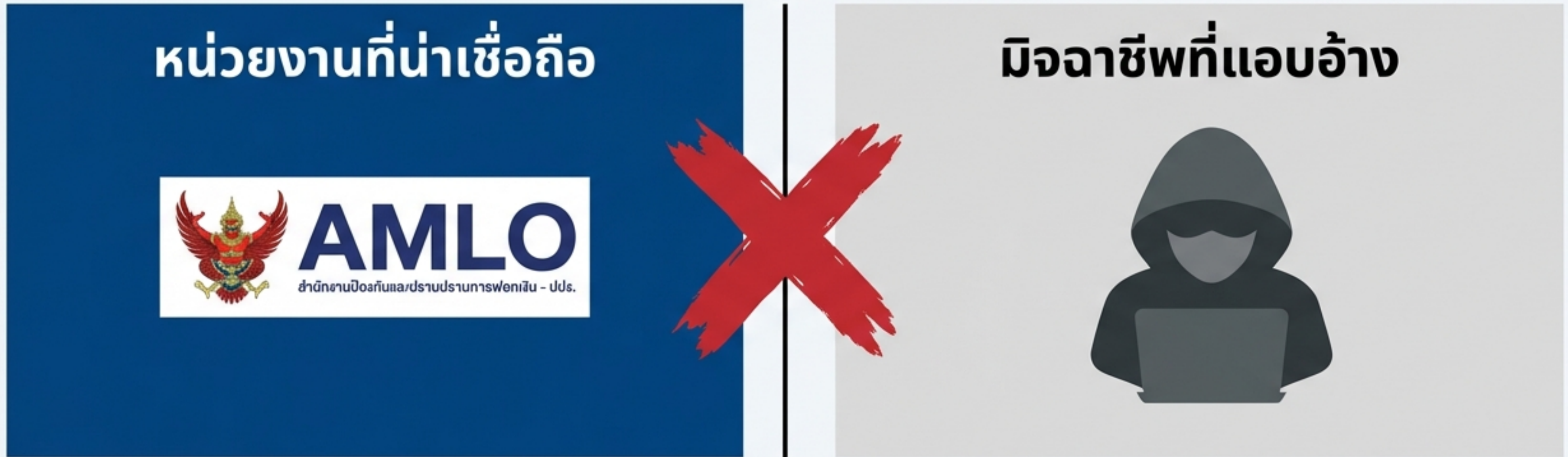


ระวัง! มีจลาชีพอ้างเป็น “ปปง.” ให้ลงทะเบียนขอรับเงินคืน

คู่มือฉบับสมบูรณ์: รู้ทันกลโกงและวิธีป้องกันตัวจากตำรวจไซเบอร์

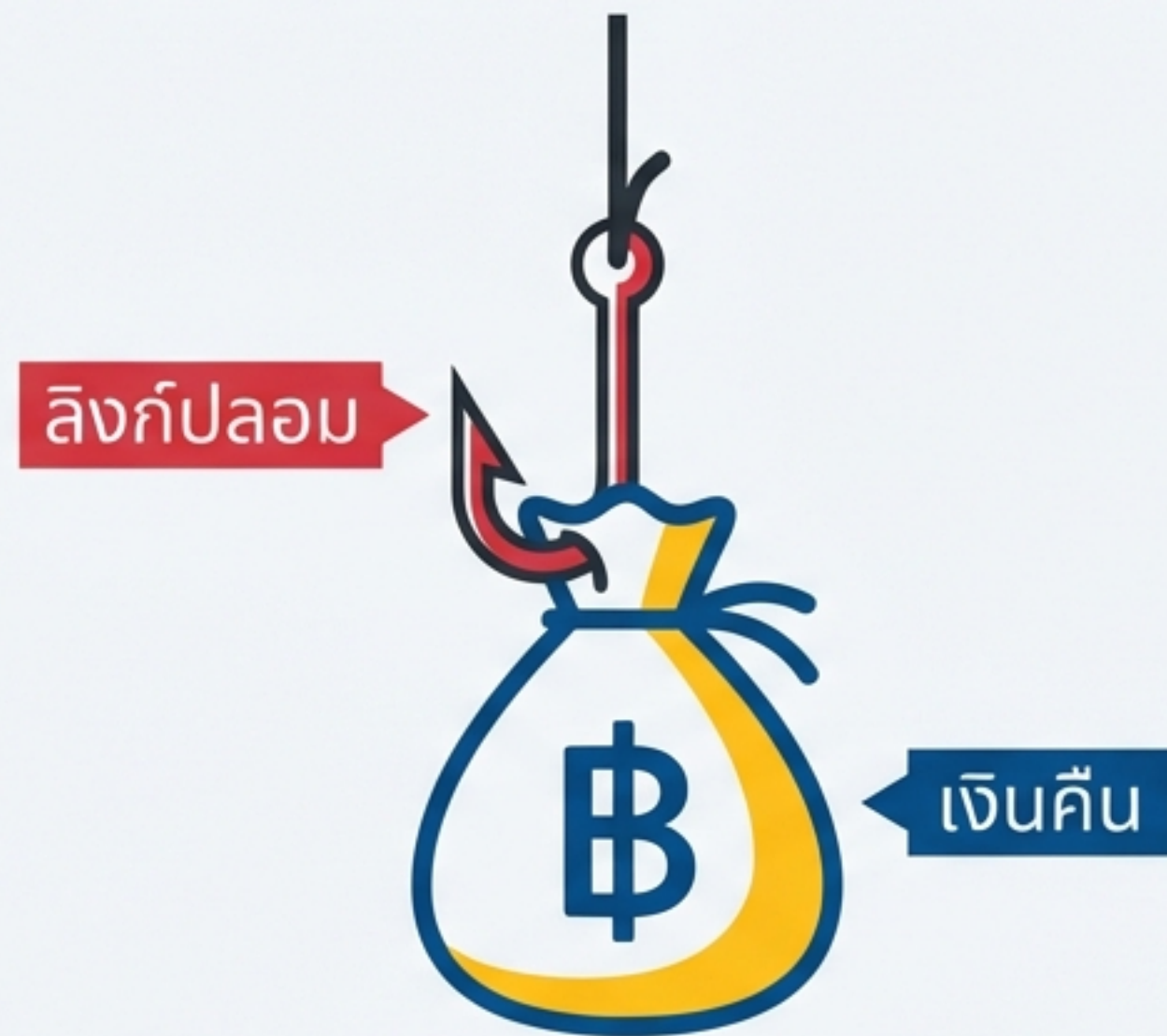


กลลวงคือการ **'สวมรอย'** เป็นหน่วยงานที่คุณไว้ใจ



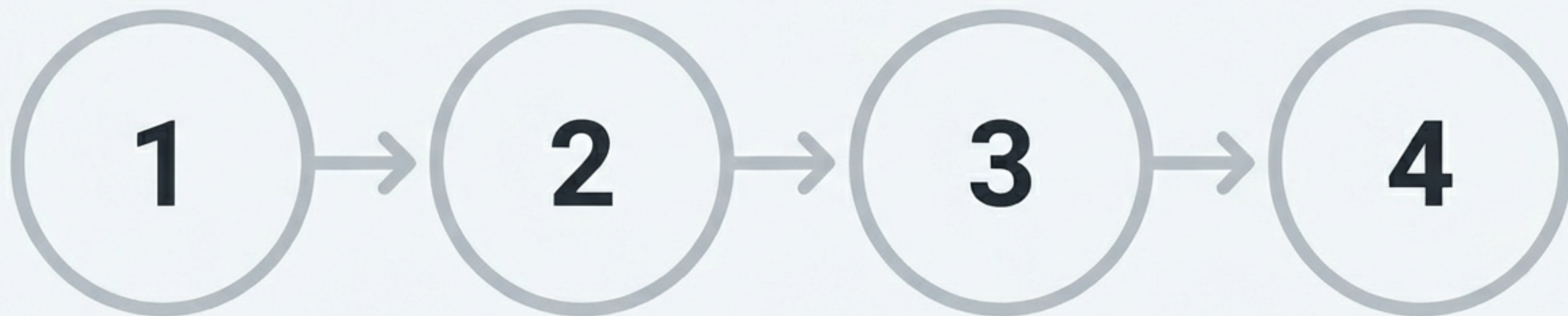
คนร้ายแอบอ้างเป็นเจ้าหน้าที่จาก **สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.)** ซึ่งเป็นหน่วยงานราชการจริง เพื่อสร้างความน่าเชื่อถือและหลอกให้เหยื่อตายใจ

เหยื่อล่อที่ใช้: ข้อเสนอ "รับสิทธิเงินคืน"



มีจาชีฟจะส่งข้อความอ้างว่าคุณมีสิทธิ์ได้รับเงินคืนจาก ปปง. เพื่อกระตุ้นให้คุณสนใจ และอยากดำเนินการต่ออย่างรวดเร็ว นี่คือจุดเริ่มต้นของกับดักทั้งหมด

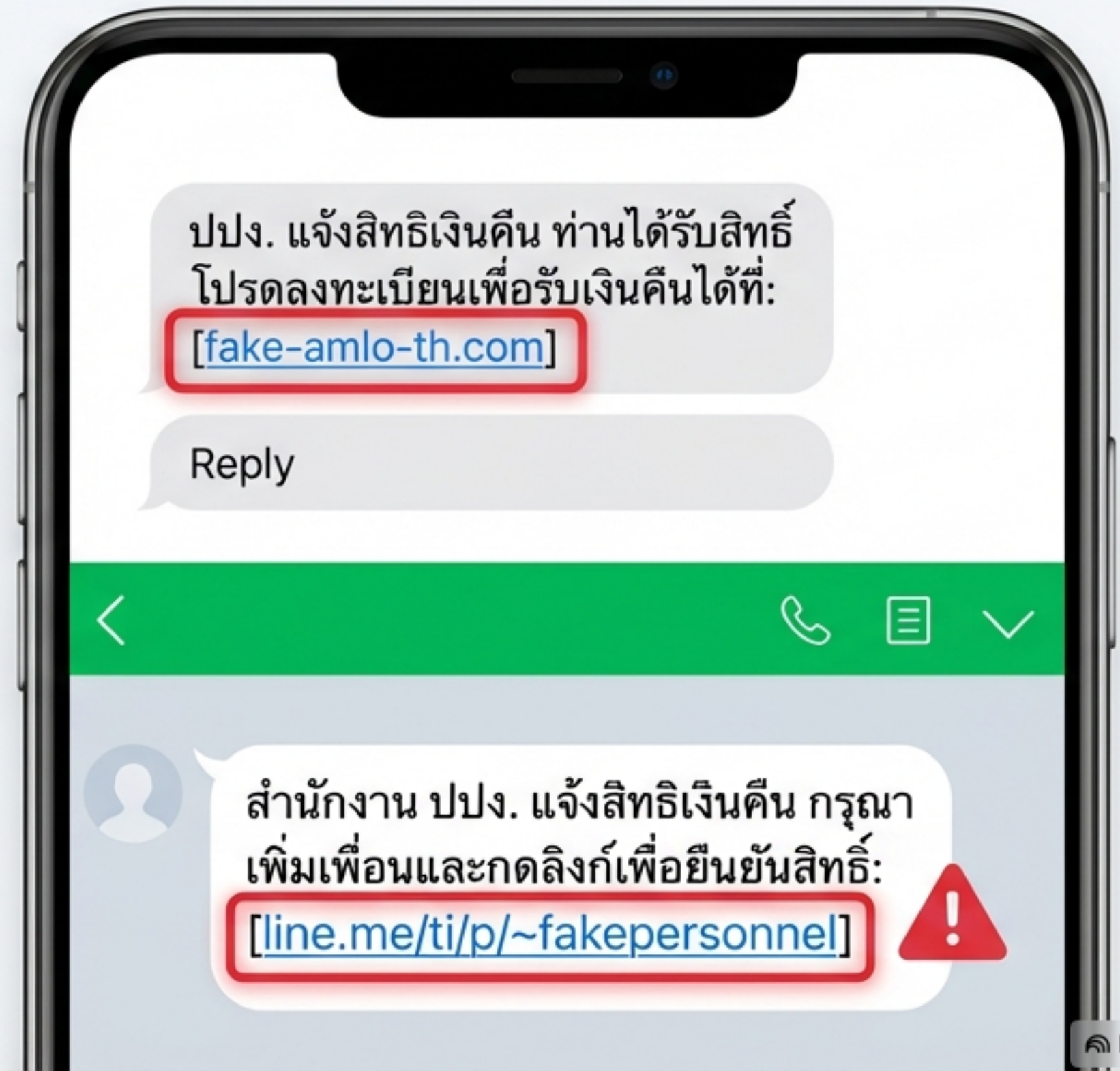
สแกนกลไก: เปิด playbook คนร้ายที่ละขั้นตอน



มีจาชีพมีรูปแบบการทำงานที่เป็นระบบและเหมือนกันแทบทุกครั้ง
การทำความเข้าใจขั้นตอนเหล่านี้คือวิธีที่ดีที่สุดในการมองเห็นกลไก
ก่อนที่คุณจะตกเป็นเหยื่อ

ขั้นตอนที่ 1: การติดต่อผ่าน SMS หรือ LINE

คุณจะได้รับข้อความ SMS หรือข้อความใน LINE ที่มีเนื้อหาว่า
“ปปง. แจ้งสิทธิเงินคืน”
พร้อมแนบลิงก์อันตรายมาด้วย
เพื่อให้คุณกด



ขั้นตอนที่ 2: การโทรศัพท์เพื่อสร้างแรงกดดัน

หลังจากส่งข้อความ คนร้ายจะโทรศัพท์หาคุณและ



เจ้าหน้าที่ปลอม

แนะนำตัว: อ้างเป็น
เจ้าหน้าที่ ปปง.
และพูดจาอย่าง
น่าเชื่อถือ



เลขอ้างอิงปลอม

สร้างเรื่อง: อ้าง
เลขคดีหรือเลขอ้าง
อิงปลอมเพื่อทำให้
ดูเป็นทางการ



กดดันด้านเวลา

เร่งรัด: กดดันให้รีบ
ทำธุรกรรมภายใน
เวลาที่กำหนด

ขั้นตอนที่ 3: กดปุ่มบนเว็บไซต์ปลอม

หากเฟลออกดลิงก์ จะถูกนำไปยังหน้าเว็บ ‘ลงทะเบียน’ ที่ออกแบบมาให้คล้ายกับเว็บไซต์ของหน่วยงานจริง และจะขอให้คุณกรอกข้อมูลส่วนตัวที่สำคัญ:

- ชื่อ-นามสกุล
- เลขบัตรประชาชน
- เบอร์โทรศัพท์
- เลขบัญชีธนาคาร

The screenshot shows a web browser window with a fake registration page. The header includes a logo and the text 'ปปง. ลงทะเบียนรับเงินคืน' (PPG. Register to receive refund). The main heading is 'แบบฟอร์มยืนยันสิทธิ' (Rights Confirmation Form). There are four input fields with corresponding labels: 'ชื่อ-นามสกุล' (Full Name), 'เลขประจำตัวประชาชน 13 หลัก' (13-digit ID Number), 'เบอร์โทรศัพท์มือถือ' (Mobile Phone Number), and 'เลขที่บัญชีธนาคาร' (Bank Account Number). Red arrows from the list on the left point to each of these fields. At the bottom is a red button labeled 'ยืนยันข้อมูล' (Confirm Information).

แบบฟอร์มยืนยันสิทธิ

ชื่อ-นามสกุล

เลขประจำตัวประชาชน 13 หลัก

เบอร์โทรศัพท์มือถือ

เลขที่บัญชีธนาคาร

ยืนยันข้อมูล

⚠️ ขั้นตอนที่ 4: จุดชี้ขาด - การขโมย OTP หรือติดตั้งแอปควบคุม

นี่คือขั้นตอนสุดท้ายและอันตรายที่สุด คนร้ายจะ:

ขอรหัส OTP



เพื่อใช้ยืนยันการทำธุรกรรมโอนเงินออกจากบัญชีของคุณ

ให้ติดตั้งแอป



หลอกให้ติดตั้งแอปพลิเคชัน 'ยืนยันตัวตน' ซึ่งแท้จริงแล้วเป็นแอปควบคุมเครื่องระยะไกล (Remote Access Trojan)



กฎเหล็กที่ต้องจำ: หน่วยงานรัฐไม่ทำสิ่งเหล่านี้เด็ดขาด

ไม่ส่งลิงก์ให้กรอกข้อมูลสำคัญ

ไม่ขอ OTP หรือรหัสผ่านของคุณ

ไม่สั่งให้ติดตั้งแอปพลิเคชันผ่านแชตหรือโทรศัพท์

เกราะป้องกันไซเบอร์ของคุณ: วิธีป้องกันตัวเชิงรุก



คุณสามารถป้องกันตัวเองจากกลโกงประเภทนี้
ได้ด้วยหลักการง่ายๆ แต่ทรงพลัง

2 ข้อห้ามสำคัญเพื่อความปลอดภัย



1. อย่ากดลิงก์ และอย่าแอดไลน์ที่ไม่รู้จัก

หากได้รับข้อความที่น่าสงสัย ไม่ว่าจะจากช่องทางไหน
ให้ลบทิ้งทันที อย่าตอบกลับหรือกดเข้าไปดู



2. อย่าให้ข้อมูลส่วนตัว

ห้ามให้ข้อมูลสำคัญกับใครง่ายๆ โดยเฉพาะ
เลขบัตรประชาชน, เลขบัญชีธนาคาร, และรหัส OTP

ปฏิบัติการฉุกเฉิน: ถ้าเผลอกดลิงก์หรือให้ข้อมูลไปแล้ว



หากรู้ตัวว่าพลาดไปแล้ว สิ่งสำคัญคือต้องะตั้งสติและลงมือทำตามขั้นตอน
ฉุกเฉินเหล่านี้ทันทีเพื่อสกัดกั้นและจำกัดความเสียหาย

ทำทันที: สกัดความเสียหายและรวบรวมหลักฐาน



สกัดความเสียหาย (Containment)

- รับผิดชอบต่อรหัสผ่านของแอปธนาคารและอีเมลที่เกี่ยวข้องทั้งหมด
- ติดต่อธนาคารของคุณทันทีเพื่อแจ้งเหตุและตรวจสอบความผิดปกติ



รวบรวมหลักฐาน (Evidence)

- แคปหน้าจอ (Screenshot) ข้อความ SMS/LINE ที่ได้รับ
- บันทึกภาพลิงก์ปลอม, เบอร์โทรศัพท์ และไอดีไลน์ของมิจฉาชีพ



แจ้งเบาะแสและขอความช่วยเหลือจากผู้เชี่ยวชาญ

หากคุณได้รับความเสียหายหรือต้องการแจ้งเบาะแสเกี่ยวกับมิจฉาชีพออนไลน์
ติดต่อตำรวจไซเบอร์ได้โดยตรงผ่านช่องทางเหล่านี้



แจ้งความออนไลน์
(Online Report)

www.thaipoliceonline.go.th



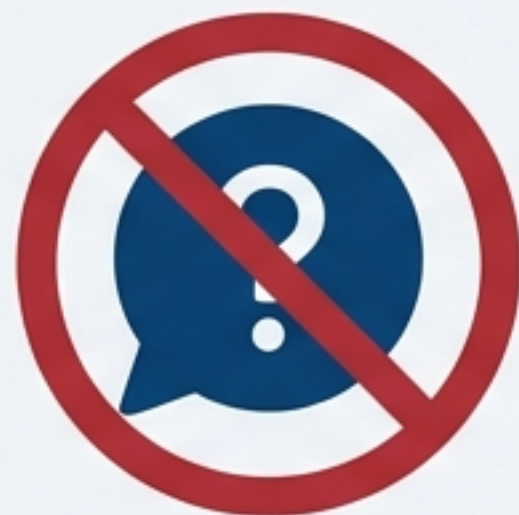
ปรึกษาและสอบถามข้อมูล
(Consultation & Inquiries)

สายด่วน 1441
(ตลอด 24 ชั่วโมง)

สรุปคาถาป้องกันตัว: รู้ทัน ไม่เชื่อ ไม่กด ไม่คุย



รู้ทัน



ไม่เชื่อ



ไม่กด



ไม่คุย

การรู้เท่าทันคือวัคซีนที่ดีที่สุดในการป้องกันอาชญากรรมออนไลน์



แชร์สไลด์นี้เพื่อช่วยปกป้องเพื่อน ครอบครัว และคนที่คุณรัก

