ธนาคารแห่งประเทศไทย

รู้รอบเรื่องการเงิน

รู้รอบระวังภัย

"เมื่อรูปแบบชีวิตของเราเปลี่ยนไปตามสภาพเศรษฐกิจ สังคม และเทคโนโลยี ที่มีความซับซ้อนมากขึ้น ความต้องการบริการทางการเงินก็เปลี่ยนตามไปด้วย ไม่ว่าจะเป็นความต้องการใช้เงินที่อาจมีมากขึ้น เนื่องจากค่าครองชีพที่สูงขึ้น หรือความต้องการบริการที่ง่าย รวดเร็ว สะดวก ทันใจ และตอบโจทย์ชีวิตยุคใหม่ได้ แต่การใช้บริการทางการเงินของเราก็ต้องเป็นไปอย่างรอบคอบและเท่าทัน เพื่อจะได้ไม่ตกเป็นเหยื่อของพวกมิจฉาชีพที่คอยจับจ้องหาช่องทางยักยอก **"เงินของเรา"**

ธนาคารแห่งประเทศไทยหวังเป็นอย่างยิ่งว่า คู่มือ **รู้รอบเรื่องการเงิน** ตอน **รู้รอบระวังภัย** เล่มนี้ จะช่วยให้คุณรู้เท่าตามทันภัยที่เกิดจากบริการทางการเงินในหลากหลายรูปแบบและไม่ตกเป็น "เหยื่อ" ของพวกมิจฉาชีพเหล่านี้"

BOT

เงินด่วนทันใจ
รับเงินไว
ดอกเบี้ยถูก

1 รู้ทัน...เงินกู้นอกระบบ 6

- เงินกู้นอกระบบ...ดีหรือเสี่ยง 7
- รู้เท่าตามทัน...เล่ห์เหลี่ยมนายทุนเงินกู้ 8
- 6 วิธี...หนีห่างหนี้นอกระบบ 10
- ปลดล็อก "หนี้นอกระบบ" ก่อนสาย 11

2 แชร์ลูกโซ่...ต้องระวัง 12

- กับดัก...แชร์ลูกโซ่ 13
- รู้ทันแชร์ลูกโซ่รูปแบบต่าง ๆ 13
- คาถาระวังภัย...จากแชร์ลูกโซ่ 16

3 ระวังภัย...แก๊งคอลเซ็นเตอร์ 17

- รวมฮิตมุขเด็ค...แก๊งคอลเซ็นเตอร์ 18
- ทำอย่างไรให้ปลอดภัยจากการถูกหลอกลวง... 24
- คาถากันภัย...จากแก๊งคอลเซ็นเตอร์ 26
- 5 สิ่งที่ควรทำ...หลังตกเป็นเหยื่อแก๊งคอลเซ็นเตอร์ 27

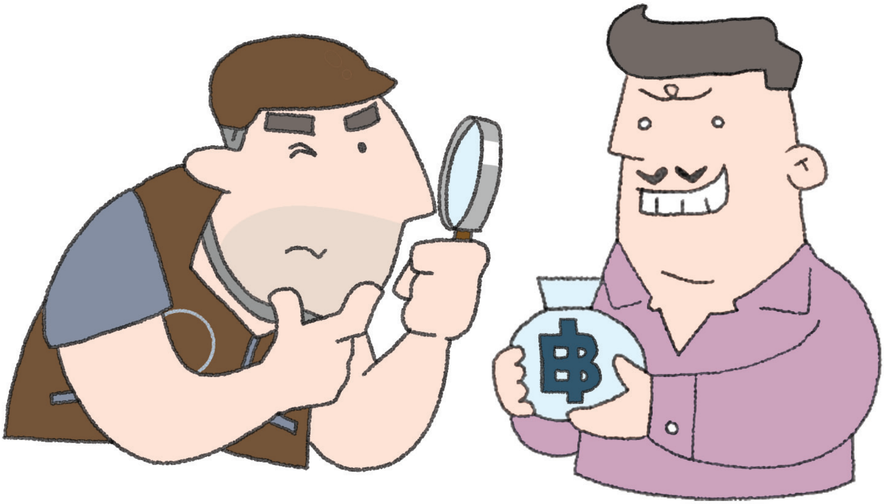
4 ภัยออนไลน์...วายร้ายไฮเทค 28

- มุขหลอก ๆ ในโลกออนไลน์ 28
- รู้ทัน...ภัยออนไลน์ 36
- วิธีจับผิดอีเมลปลอม 37
- สังเกตเว็บไซต์ธนาคารออนไลน์ปลอม 38
- ทำอย่างไร...ไม่ให้กลายเป็นเหยื่อภัยออนไลน์ 39

5 ระวังภัย...บัตรถูกสวมรอย 41

- รู้ทัน...กลวิธีปลอมแปลงบัตร 42
- ใช้บัตรอย่างไร...ให้ปลอดภัย 43

1 รู้ทัน...เงินกู้นอกระบบ



ยามที่มีปัญหาการเงิน ขอกู้เงินที่ไหนไม่ได้ จนต้องหันไปกู้หนี้นอกระบบ เพราะได้เงินเร็ว ไม่ยุ่งยาก ไม่ต้องมีหลักประกันหรือมีคนค้ำ ซึ่งต่างจากการไปขอกู้กับสถาบันการเงินต่าง ๆ ที่ต้องใช้เอกสารมากมาย แถมยังต้องรอนานกว่าจะอนุมัติ ความสะดวกเหล่านี้ ทำให้หลายคนไม่ทันได้นึกถึงผลเสียที่ตามมาจากการตัดสินใจกู้เงินจากนอกระบบนี้

เงินกู้นอกระบบ...ดีหรือเสี่ยง

"เงินด่วนทันใจ รับเงินไวภายใน 5 นาที ดอกเบี้ยถูก ติดต่อเจ๊เคียว โทร. XXX"

หลังจากที่ น้าชาติได้รับใบปลิวฉบับนี้มา ทำให้นึกถึงตู้เย็นที่อยากได้ขึ้นมาทันที จึงไม่รอช้ารีบติดต่อขอกู้เงิน 10,000 บาท โดยมีเงื่อนไขว่า เก็บเงินรายวัน วันละ 150 บาท เป็นเวลา 3 เดือน น้าชาติตัดสินใจรับเงื่อนไขทันที เพราะไม่ต้องจ่ายเงินก้อนโต แต่ลืมนึกถึงดอกเบี้ยที่ต้องจ่ายว่าเป็นเงินเท่าไร

น้าชาติอาจเป็นเหมือนใครอีกหลายคนที่ตกเป็นเหยื่อการโฆษณาชวนเชื่อของพวกนายทุนเงินกู้นอกระบบที่มักจะล่อเหยื่อให้ติดกับดัก "ตัวเลขจำนวนน้อย" โดยไม่ทันคิดให้ถี่ถ้วนเพราะถ้าลองคำนวณอัตราดอกเบี้ยที่แท้จริงที่น้าชาติจะต้องจ่ายให้เจ๊เคียวแล้ว จะเท่ากับน้าชาติจ่ายคืนเงินทั้งหมด 13,500 บาท (150x90) ในเวลาเพียงสามเดือน ค่าดอกเบี้ยจะเท่ากับ 3,500 บาทจากเงินต้น 10,000 บาทหรือ 35% ซึ่งหากแปลงเป็นอัตราดอกเบี้ยต่อปีอย่างที่สถาบันการเงินทั่วไปคิดให้ลูกค้าแล้วจะสูงถึง 140% ต่อปีเลยทีเดียว ((35 ÷ 3) x 12 = 140)

รู้เท่าตามทัน...เล่ห์เหลี่ยมนายทุนเงินกู้

จากเรื่องราวของน้าชาติสะท้อนให้เห็นเล่ห์เหลี่ยมของนายทุนเงินกู้ที่พร้อมจะตักตวงผลประโยชน์จากลูกหนี้อย่างไร้มนุษยธรรม

ตามไปดูกันว่า *หนี้นอกระบบ เป็นอย่างไร และเล่ห์เหลี่ยมของพวกนายทุนเหล่านี้มีอะไรกันบ้าง**

**หนี้นอกระบบ เป็นหนี้ที่ผู้ให้กู้ไม่อยู่ในระบบสถาบันการเงิน หรือเป็นผู้ที่ไม่ได้รับอนุญาตให้ประกอบธุรกิจให้กู้เงินตามกฎหมาย โดยมักจะคิดดอกเบี้ยเกินกว่าอัตราที่กฎหมายกำหนด (ร้อยละ 15)*

• **ใส่ตัวเลขน้อย ๆ เพื่อจูงใจให้กู้** เช่น บอกตัวเลขดอกเบี้ยที่ดูเหมือนว่าจะน้อยกว่าดอกเบี้ยเงินกู้ของสถาบันการเงิน แต่เอาเข้าจริง ๆ แล้วดอกเบี้ยแพงมหาโหด เพราะเขามักจะไม่ได้บอกเราก่อนว่า คิดดอกเบี้ยต่อวัน ต่อเดือน หรือต่อปี และมักจะบอกจำนวนเงินที่จ่ายเป็นรายวัน เพื่อให้ดูน้อยเข้าไว้ คนจะได้อยากกู้มาก ๆ

• **คิดดอกแบบคงที่ตลอดปีตลอดชาติ** นอกจากอัตราดอกเบี้ยที่แสนแพงแล้ว การคิดดอกเบี้ยคงที่ ยังทำให้ลูกหนี้ต้องจ่ายดอกเบี้ยมากกว่าการคิดดอกเบี้ยแบบลดต้นลดดอก เพราะดอกเบี้ยจะคิดจากเงินต้นที่กู้ทั้งก้อน แม้ลูกหนี้จะทยอยจ่ายคืนหนี้ทุกเดือนก็ตาม (ดูรายละเอียดวิธีคิดดอกเบี้ยแบบลดต้นลดดอกได้ที่คู่มือ *รู้รอบเรื่องการเงิน* ตอน *คิดก่อนเป็นหนี้*)

• **บีบให้ทำสัญญาเงินกู้เกินจริง** เช่น กู้ 10,000 บาท แต่สัญญาเขียน 30,000 บาท ถ้าไม่ยอมก็ไม่ให้เงิน

• **ทวงหนี้โหด** ตามที่เป็นข่าวกันหลายต่อหลายครั้งกับวิธีการทวงหนี้แบบแปลก ๆ ไม่เฉพาะขู่ หรือประจานให้ได้อายเท่านั้น แต่ถึงขั้นทำร้ายร่างกายกันก็มี

• **หลีกเลี่ยงการให้กู้โดยตรง** โดยให้คนอื่นปล่อยกู้แทนอีกหลายทอด หรือให้ลูกหนี้ที่ต้องการกู้เงินไปซื้อสินค้า เช่น เครื่องใช้ไฟฟ้าด้วยบัตรเงินผ่อนแล้วนำมาขายต่อให้นายทุนในราคาส่วนลด เช่น สินค้าราคา 20,000 บาท จะรับซื้อที่ 17,000 บาท นายทุนได้สินค้าราคาถูกไปขายต่อ ขณะที่ลูกหนี้นอกจากจะได้เงินสดไม่เต็มจำนวน เพราะจ่ายดอกเบี้ยล่วงหน้าไป 3,000 บาทแล้ว ยังต้องมาผ่อนดอกเบี้ยในส่วนของบัตรเงินผ่อนที่ยอดเงิน 20,000 บาทอีกด้วย

...รู้แบบนี้แล้วยังคิดจะกู้เงินนอกระบบอีกหรือ

6 วิธี...หนีห่างหนี้นอกระบบ

คุณสามารถที่จะถอยห่างจากวงจรหนี้นอกระบบได้ โดย...

1. วางแผนการเงินล่วงหน้า คำนึงถึงค่าใช้จ่ายที่จะเกิดขึ้น เช่น ค่าเล่าเรียนลูก และออมเงินเผื่อยามฉุกเฉิน เมื่อจำเป็นก็สามารถนำมาใช้ได้โดยไม่ต้องพึ่งเงินกู้นอกระบบ

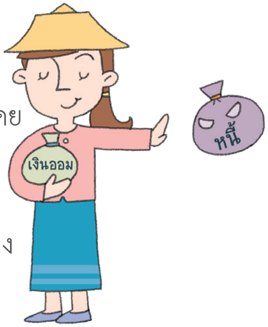
2. คิดให้ดีก่อนตัดสินใจ "ก่อหนี้" ลองคิดทบทวนดูว่า จำเป็นต้องใช้เงินจริง ๆ หรือไม่ และจะสามารถชำระหนี้ทั้งหมดได้หรือไม่

3. หยุด "ใช้เงินเกินตัว" และเรียนรู้ที่จะจดบันทึกรายรับรายจ่ายประจำวัน เพื่อวางแผนการใช้เงินอย่างเหมาะสมกับรายได้และความจำเป็น

4. ศึกษารายละเอียดผู้ให้กู้ดี ๆ หากต้องกู้ควรดูว่า ผู้ให้กู้นั้นน่าเชื่อถือหรือไม่ มีเงื่อนไขการชำระเงินหรืออัตราดอกเบี้ยที่เข้าข่ายเป็นเงินกู้นอกระบบหรือไม่

5. เลือกกู้เงินในระบบ จะดีกว่าหากจำเป็นต้องกู้จริง ๆ เพราะนอกจากจะมีหน่วยงานภาครัฐคอยดูแลแล้ว ยังระบุดอกเบี้ยในสัญญาชัดเจนและเป็นธรรมกว่ามาก

6. ใส่ใจในรายละเอียดสัญญาเงินกู้ให้มาก โดย

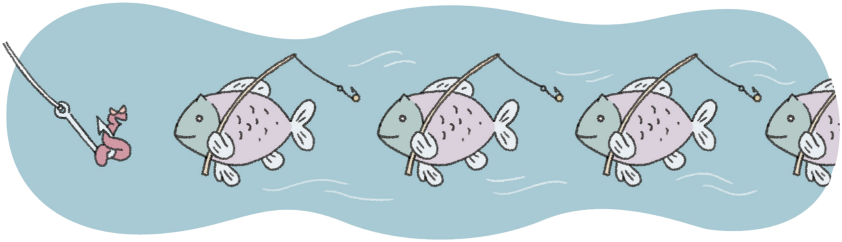


- ไม่เซ็นสัญญาเงินกู้ ที่ยังไม่กรอกข้อความหรือจำนวนเงินเด็ดขาด
- วงเงินกู้ที่ระบุในสัญญาต้องตรงกับความเป็นจริงและเขียนจำนวนเงินเป็นตัวหนังสือกำกับไว้เสมอ
- ควรมีสัญญาคู่ฉบับอีก 1 ฉบับเก็บไว้กับตัวเพื่อเป็นหลักฐานการกู้
- หากต้องนำทรัพย์สินไปเป็นหลักประกัน ควรทำสัญญาจำนองแทนการทำสัญญาขายฝาก เพราะการขายฝาก ถ้าผู้กู้ไม่มาไถ่คืนหลักประกันภายในเวลาที่ตกลงกัน กรรมสิทธิ์จะตกไปยังเจ้าหนี้ทันที แต่การจำนองคือการนำทรัพย์สินมาเป็นประกัน หากไม่ชำระเมื่อถึงกำหนด เจ้าหนี้จะบังคับจำนองโดยการฟ้องต่อศาล

ปลดล็อก "หนี้นอกระบบ" ก่อนสาย

หากคุณได้กู้เงินนอกระบบมาแล้ว ให้รีบหาเงินมาชำระหนี้ทั้งหมด อาจหาแหล่งเงินกู้ในระบบซึ่งคิดดอกเบี้ยถูกกว่ามาเพื่อปลดหนี้นอกระบบก็ได้ แต่ถ้าหาเงินกู้ในระบบไม่ได้ อาจต้องยอมสละขายทรัพย์สินบางส่วน เพื่อรักษาทรัพย์ส่วนใหญ่ไว้ดีกว่าที่จะปล่อยให้ดอกเบี้ยพอกพูนจนไม่สามารถชำระหนี้ได้ แล้วค่อยออมเพื่อซื้อสินทรัพย์กลับมาใหม่

2 แชร์ลูกโซ่...ต้องระวัง



แชร์ลูกโซ่ (Money Game) นับเป็นภัยอีกรูปแบบหนึ่งที่สร้างความเสียหายทางการเงินให้แก่คุณได้ เราไปทำความรู้จักกับภัยประเภทนี้ เพื่อจะได้ไม่ต้องตกเป็นเหยื่อกันดีกว่า

กานดาชักชวนน้าชาติให้มาร่วมลงทุนทำธุรกิจ โดยบอกว่าแม่หมูซึ่งเป็นญาติของเธอทำธุรกิจนำเข้าหมูแผ่นที่อร่อยที่สุดในโลก โดยน้าชาติไม่ต้องทำอะไรมาก แค่ซื้อหมูแผ่นไว้ 1 แผ่น ในราคา 5,000 บาท ก็จะได้ผลตอบแทน 10% ของเงินลงทุน ยิ่งลงทุนมากก็ยิ่งได้เงินคืนมาก ไม่ต้องเหนื่อยไปเดินขายสินค้า แค่รอรับเงิน หรือถ้าอยากได้เงินเพิ่มก็ชักชวนเพื่อนมาร่วมลงทุน น้าชาติก็จะได้เงินค่านายหน้าอีก 300 บาท

แม้จะเอะใจว่าหมูแผ่นอะไรจะแพงได้ถึงขนาดนั้น แต่พอแม่หมูส่งผลตอบแทนให้น้าชาติทุกเดือน น้าชาติก็ตาโตด้วยความดีใจจึงรีบชักชวนเพื่อนมาลงทุนและควักกระเป๋าตัวเองลงทุนเพิ่มด้วย เพื่อหวังที่จะได้ผลตอบแทนที่เพิ่มขึ้น

ต่อมาไม่นาน จากที่แม่หมูเคยจ่ายผลตอบแทนตรงเวลา แม่หมูก็เริ่มอึดอาด นานเข้าก็หาตัวไม่เจอ น้าชาติเครียดมากเพราะสูญเงินไปหลายบาท

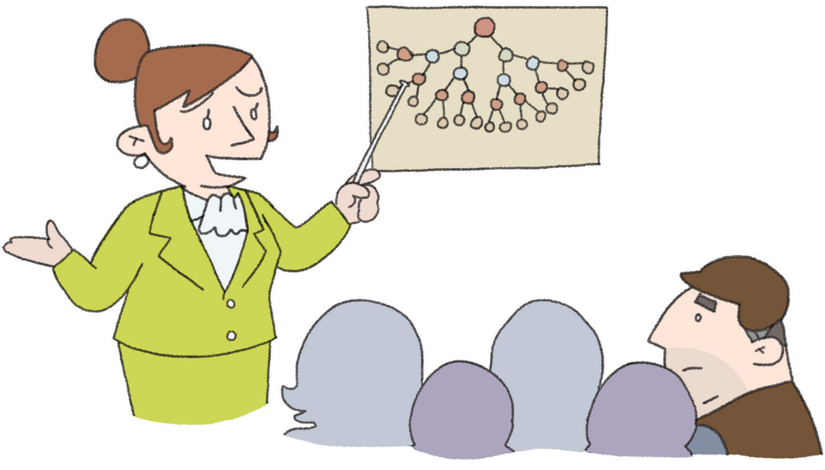
กับดัก...แชร์ลูกโซ่

ปกติแล้ว พวกเท้าแชร์ลูกโซ่จะใช้วิธีหมุนเวียนเงินลงทุนด้วยการนำเงินลงทุนหรือค่าสมัครจากเหยื่อรายใหม่มาหมุนเวียนจ่ายเป็นค่าตอบแทนให้กับสมาชิกที่สมัครก่อนหน้า โดยไม่ได้ทำธุรกิจจริง ยิ่งหาเหยื่อใหม่ ๆ ได้มากเงินทุนก็จะมากขึ้นตาม การจ่ายผลตอบแทนในช่วงแรก ๆ จึงทำได้มากและสม่ำเสมอ แต่พอเวลาผ่านไป สมาชิกใหม่เริ่มหายากขึ้น ผลตอบแทนที่เคยได้ก็จะเริ่มมีปัญหา จนต้องล้มกระดาน และโอกาสที่จะได้เงินคืนก็เป็นไปได้ยาก เพราะกว่าตำรวจจะรู้ก็ต่อเมื่อมีคนจำนวนมากมาแจ้งความ ถึงตอนนั้นพวกเท้าแชร์ลูกโซ่ก็หนีหายกันไปหมดแล้ว

รู้ทันแชร์ลูกโซ่รูปแบบต่าง ๆ

ปัจจุบันมีแชร์ลูกโซ่หลากหลายรูปแบบ และธุรกิจขายตรงก็เป็นหนึ่งในรูปแบบที่แชร์ลูกโซ่เข้าไปแฝงกายอยู่

แชร์ลูกโซ่ในคราบ...ธุรกิจขายตรง



เราสามารถแยกแยะความแตกต่างระหว่างธุรกิจขายตรงกับแชร์ลูกโซ่ที่แฝงกายในคราบธุรกิจขายตรงได้ ดังนี้

ธุรกิจขายตรง	แชร์ลูกโซ่ในคราบธุรกิจขายตรง
• สมาชิกต้องนำสินค้าไปเสนอขายต่อผู้บริโภคโดยตรง • ผลตอบแทนของสมาชิกขึ้นอยู่กับยอดขาย • ไม่บังคับให้สมาชิกต้องซื้อสินค้าเพื่อมีสิทธิในการร่วมธุรกิจ • สินค้าจะต้องเป็นสินค้าที่มีคุณภาพ	• เน้นหาสมาชิกมากกว่าขายสินค้า • ธุรกิจเติบโตจากเครือข่ายของสมาชิกมากกว่าเติบโตจากการขายสินค้า • มักเสนอผลตอบแทนที่มากเกินความเป็นจริง • ผลตอบแทนหลักไม่ได้อยู่ที่ตัวสินค้าแต่อยู่ที่จำนวนเงินลงทุนของสมาชิกเป็นหลัก • สำนักงานไม่มีหลักแหล่งแน่นอน

แชร์ลูกโซ่ในคราบธุรกิจขายตรงที่เห็นเป็นข่าวบ่อย ๆ เช่น แชร์น้ำมัน แชร์ไม้กฤษณา แชร์ประมูลเพชร แชร์ไอโฟน หรืออาจอยู่ในรูปธุรกิจอื่น ๆ เช่น การลงทุนขายเครื่องสำอางนำเข้าจากต่างประเทศที่ให้ผลตอบแทนต่อเนื่อง แต่ไม่มีการขายสินค้าจริง หรือการชักชวนให้เก็งกำไรจากอัตราแลกเปลี่ยน (แชร์ forex) โดยทำเว็บไซต์ขึ้นมาและอ้างว่าเป็นบริษัทต่างชาติที่น่าเชื่อถือ เชิญชวนให้ลงทุนเก็งกำไรเงินตราต่างประเทศ เพียงแค่สมัครสมาชิกและนำเงินมาลงทุนก็จะได้ผลตอบแทนสูง

แชร์ลูกโซ่ออนไลน์

แชร์ลูกโซ่ออนไลน์เป็นธุรกิจขายตรงที่แฝงเข้ามาในรูปแบบของอีเมลเชิญชวนให้หารายได้ทางอินเทอร์เน็ต โดยส่วนใหญ่ มักจะล่อเหยื่อโดยการ

- ส่งอีเมลหรือลงข้อความในเว็บไซต์ เชิญชวนให้หารายได้เสริม รายได้ดี แต่ไม่ได้บอกว่าทำอะไร
- จูงใจว่าทำงานหลังเลิกงาน ใช้เวลาเพียง 2–3 ชั่วโมง ก็ทำให้รวยได้
- หากเหยื่อสนใจก็จะโทรชวนให้ไปร่วมฟังสัมมนา
- ใช้จิตวิทยาโน้มน้าวให้เหยื่อสมัครสมาชิก ถ้าหาสมาชิกได้เพิ่มก็จะได้ค่าหัวคิว

เมื่อเหยื่อติดเบ็ดจนดิ้นไม่หลุด เพราะโดนบังคับให้จ่ายค่าสมาชิกแสนแพง ทางเดียวที่ทำได้คือ หาเหยื่อรายต่อไป เพื่อได้ค่าหัวคิวมาทดแทนเงินที่เสียไป และกลายเป็นวังวนของอีเมลลูกโซ่ที่ไม่รู้จบสิ้น

คาถาระวังภัย...จากแชร์ลูกโซ่

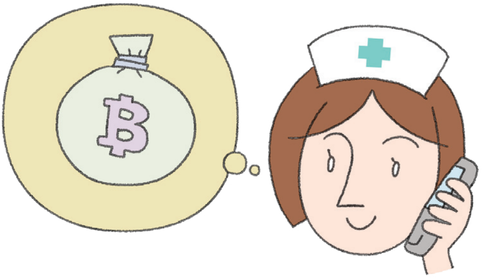
- ศึกษาที่มาที่ไปให้ดี ว่ารูปแบบการลงทุนเป็นอย่างไร มีใบขออนุญาตทำธุรกิจจริงหรือไม่
- ไม่โลภไปกับผลตอบแทนที่นำมาหลอกล่อ
- อย่าไว้ใจ หรือเกรงใจจนไม่กล้าปฏิเสธ แม้คนที่ชวนจะเป็นคนสนิทหรือคนในครอบครัว เพราะอาจถูกหลอกเหมือนกัน
- หลีกเลี่ยงการเข้าร่วมกิจกรรมต่าง ๆ กับกลุ่มธุรกิจที่ไม่แน่ใจ เพราะคนเหล่านี้จะใช้จิตวิทยาหว่านล้อมจนยากจะปฏิเสธ แม้จะเปลี่ยนใจทีหลังก็ยากจะถอนเงินลงทุนคืน

3 ระวังภัย...แก๊งคอลเซ็นเตอร์

หลายคนคงเคยได้ยินข่าว แก๊งคอลเซ็นเตอร์ข้ามชาติกันบ้างแล้ว และบางคนอาจเคยตกเป็นเหยื่อ หรือเกือบจะตกเป็นเหยื่อมาแล้วด้วยซ้ำ แล้วเราจะระวังภัยจากพวกแก๊งต้มตุ๋นเหล่านี้ได้อย่างไร ...ตามไปดูกัน

รวมฮิตมุขเด็ด...แก๊งคอลเซ็นเตอร์

แก๊งคอลเซ็นเตอร์เหล่านี้จะทำงานกันอย่างเป็นขบวนการ เริ่มจากล่อเหยื่อให้เข้ามาติดกับโดยใช้ระบบตอบรับอัตโนมัติ แอบอ้างเป็นหน่วยงานราชการที่น่าเชื่อถือ ซึ่งมิจฉาชีพเหล่านี้สามารถทำให้โทรศัพท์แสดงหมายเลขของหน่วยงานราชการต่าง ๆ ได้ จากนั้นจะสานต่อความตกใจโดยแอบอ้างถึงการกระทำที่ผิดกฎหมายของเหยื่อ หรือใช้จุดอ่อน เช่น ความโลภ ความกลัว และความไม่รู้เท่าทันมาหลอกลวง โดยมีมุขที่มักนำมาใช้แอบอ้างดังนี้



1. ล่อหลอกด้วยผลประโยชน์ที่จะได้รับจากเหตุการณ์ต่าง ๆ

- **คืนเงินค่าภาษี :** อ้างว่าเป็นเจ้าหน้าที่สรรพากร แจ้งเหยื่อว่าได้รับการลดภาษีเงินได้ และวันนี้เป็นวันสุดท้ายที่จะทำเรื่องคืนเงิน จึงโทรมาให้เหยื่อทำเรื่องขอคืนเงินผ่านตู้เอทีเอ็มตามคำสั่งทันที แต่ความจริงเป็นการโอนเงินไปให้มิจฉาชีพ

- **โชคดีรับรางวัลใหญ่ :** อ้างว่าเป็นตัวแทนของบริษัทเปิดใหม่ จึงมีการจับสลากหรือมอบรางวัลที่มูลค่าสูงให้แก่ลูกค้า แต่เหยื่อต้องจ่ายภาษีก่อนจึงจะส่งรางวัลไปให้

- **เงินคืนประกันชีวิต :** อ้างว่าเป็นเจ้าหน้าที่จากบริษัทประกันภัย แจ้งเหยื่อว่าญาติเหยื่อที่เสียชีวิตได้ทำประกันไว้เป็นเงินจำนวนมากแต่ขาดเบี้ยประกันอีกจำนวนหนึ่ง จึงหลอกให้เหยื่อจ่ายเงินส่วนนี้เพื่อแลกกับเงินค่าสินไหมทดแทนจำนวนมาก

• **นายหน้าพาเข้าทำงาน :** อ้างว่าเป็นบุคคลมีตำแหน่งเป็นผู้บริหารระดับสูงในบริษัท หรือองค์กรใหญ่ ๆ หลอกเหยื่อว่าสามารถพาเหยื่อเข้าทำงานที่องค์กรนั้นได้ แต่เหยื่อต้องจ่ายค่านายหน้า หรือค่าดำเนินการต่าง ๆ ก่อน

• **นายหน้าหาสินเชื่อ :** อ้างว่าเป็นบุคคลที่สามารถช่วยเหลือเหยื่อที่มีประวัติทางการเงินไม่ผ่านเกณฑ์เงินกู้ธนาคาร โดยอ้างว่ารู้จักกับทนายหรือเจ้าหน้าที่ธนาคารที่สามารถช่วยได้ แต่เหยื่อจะต้องจ่ายค่าธรรมเนียมในการดำเนินการก่อน

2. หลอกให้ตกใจ แล้วฉกเงินไปโดยไม่รู้ตัว

• **หนี้บัตรเครดิต :** อ้างว่าเป็นเจ้าหน้าที่สถาบันการเงิน แล้วแจ้งว่าเหยื่อเป็นหนี้บัตรเครดิต หรือค่าน้ำ ค่าไฟ ซึ่งต้องชำระภายในวันนี้

• **บัญชีเงินฝากถูกอายัด :** อ้างว่าเป็นเจ้าหน้าที่สถาบันการเงิน แล้วแจ้งว่าบัญชีของเหยื่อถูกอายัดโดยธนาคารแห่งประเทศไทย ขอให้เหยื่อยืนยันข้อมูลส่วนตัว แล้วนำข้อมูลที่ได้ไปทำธุรกรรมทางการเงินในนามของเหยื่อ หรือหลอกเหยื่อให้ไปยกเลิกรายการที่ตู้เอทีเอ็ม

• **โอนเงินผิด :** อ้างว่าได้โอนเงินผิดเข้าบัญชีของเหยื่อ ขอให้เหยื่อโอนเงินคืนให้ และเมื่อเหยื่อโอนเงินคืนให้ เหยื่อก็จะกลายเป็นหนี้ธนาคารแทน เพราะเงินที่เหยื่อโอนนั้น เป็นเงินที่มิจฉาชีพขอสินเชื่อในนามของเหยื่อ หรือเป็นเงินผิดกฎหมายที่มิจฉาชีพหลอกให้คนอื่นโอนเข้ามา

• **บัญชีเงินฝากพัวพันกับขบวนการค้ายาเสพติด :** อ้างว่าเป็นเจ้าหน้าที่ตำรวจ แจ้งว่ามีเงินโอนจากกลุ่มค้ายาเสพติดมายังบัญชีของเหยื่อ แล้วให้โอนกลับ มิฉะนั้นจะถูกอายัดทุกบัญชี

• **ข้อมูลส่วนตัวหาย :** อ้างว่าเป็นเจ้าหน้าที่สถาบันการเงิน แจ้งว่าข้อมูลของเหยื่อหายไป ให้เหยื่อแจ้งข้อมูลส่วนตัว เช่น เลขที่บัตรประชาชน เลขที่บัญชีเพื่อยืนยันการใช้บัญชี ไม่เช่นนั้นบัญชีจะถูกอายัด

หลังจากวัลลภกดรับสายโทรศัพท์ มีเสียงจากระบบแจ้งเตือนอัตโนมัติว่า

"ขณะนี้คุณเป็นหนี้บัตรเครดิตกับทางธนาคาร xxx เป็นจำนวนเงิน 24,000 บาท กด 0 เพื่อติดต่อพนักงาน"

...ด้วยความตกใจ วัลลภรีบกด 0 ทันที

พนักงาน: สวัสดีครับ สำนักงานข้อมูลเครดิต ธนาคารแห่งประเทศไทยครับ

วัลลภ : เออ ผมได้รับแจ้งว่าผมเป็นหนี้บัตรเครดิต ผมไม่มีบัตรเครดิต มีแต่บัตรเอทีเอ็ม

พนักงาน: ผมขอทราบชื่อ-นามสกุล เลขที่บัตรประชาชน เพื่อตรวจสอบด้วยครับ

วัลลภ : ชื่อวัลลภ เลขที่บัตรนะ...

พนักงาน: ข้อมูลแจ้งว่าคุณเป็นหนี้ 24,000 บาท แต่ถ้าคุณยืนยันว่าไม่มีบัตรเครดิต สงสัยว่าข้อมูลคุณคงถูกแอบอ้างใช้ทำบัตรเครดิตแล้วละครับ ถ้าอย่างนั้น ทางเราจะขอตรวจสอบรายการให้ ไม่ทราบว่าคุณมีบัตรของธนาคารไหนบ้าง และมีเงินในบัญชีเท่าไหร่ครับ

วัลลภรีบแจ้งข้อมูลบัญชีเงินฝากทั้งหมด รวมถึงบัญชีเงินฝากที่วัลลภเพิ่งเปิดสำหรับฝากเงินที่ได้รับจากการขายที่ดินด้วย...

พนักงาน: จากการเช็กข้อมูล นอกจากชื่อของคุณจะถูกแอบอ้างไปใช้ทำบัตรเครดิตแล้ว บัญชีเงินฝากของคุณยังไปพัวพันกับการฟอกเงินของขบวนการค้ายาเสพติดอีกด้วย

วัลลภ : เฮ้ย เงิน 3 ล้านนั่นเป็นเงินขายที่ดินมรดกนะ จะเกี่ยวกับยาเสพติดได้ยังไง!

พนักงาน: ครับ ๆ ผมเข้าใจ เดี๋ยวผมจะโอนสายให้คุยกับเจ้าหน้าที่กรมสอบสวนคดีพิเศษที่ดูแลเรื่องนี้ หากสายหลุด ให้ติดต่อไปที่เบอร์ XXXX นะครับ

ตู๊ด ตู๊ด ตู๊ด

ตำรวจ : สวัสดีครับ ฝ่ายสอบสวนคดีพิเศษ ดีเอสไอ (DSI) ครับ

วัลลภ : คุณตำรวจครับ ผมได้รับแจ้งว่าบัญชีเงินฝากของผมเกี่ยวข้องกับขบวนการค้ายาเสพติด แต่เงินที่มีเป็นเงินที่ได้จากการขายที่ดินมรดกนะครับ

ตำรวจ : ผมขอเช็กข้อมูลสักครู่...คุณครับเลขที่บัญชีที่มีเงิน 3 ล้านบาทนี้ถูกต้องสงสัยว่าเป็นเงินที่เกี่ยวข้องกับขบวนการค้ายาเสพติดครับ ทาง DSI คงต้องขอตรวจสอบแหล่งที่มาครับ ขอให้คุณโอนเงินจากบัญชีของคุณทุกบัญชี มายังบัญชีเลขที่ xxx ซึ่งเป็นบัญชีของธนาคารแห่งประเทศไทย และถ้าผลการตรวจสอบพบว่า คุณไม่ได้มีส่วนเกี่ยวข้องกับการค้ายาเสพติดก็จะรีบโอนเงินคืนให้แก่คุณทันที แต่ที่สำคัญ ทางเราสงสัยว่าคนใกล้ชิดหรือพนักงานธนาคารอาจมีส่วนรู้เห็น ดังนั้นคุณอย่าบอกเรื่องนี้กับใคร ไม่งั้นจะทำให้เสียรูปคดี และอาจต้องรับโทษแทนบุคคลเหล่านั้นด้วยครับ

วัลลภ : ได้ ๆ แล้วผมจะโอนยังไง

ตำรวจ : คุณไปถอนเงินที่ธนาคาร แล้วโอนเข้าบัญชีที่ผมบอก ยังไม่ต้องวางสายนะครับ ผมจะได้บอกขั้นตอนให้คุณทราบ หากสายหลุดเดี๋ยวผมจะรีบติดต่อเข้าไป คุณจะได้ไม่เปลืองค่าโทรศัพท์

วัลลภรีบไปธนาคารเพื่อถอนเงินและโอนเงินตามคำแนะนำ แต่เมื่อเวลาผ่านไป วัลลภยังไม่ได้รับเงินคืน จึงไปติดต่อที่ DSI เพื่อขอรับเงินคืน จึงได้ทราบว่าถูกหลอกลวงจากกลุ่มมิจฉาชีพเข้าเสียแล้ว...

เรื่องราวของวัลลภเป็นเพียงหนึ่งตัวอย่างในอีกหลากหลายรูปแบบการหลอกลวงของพวกแก๊งต้มตุ๋นที่มักจะแอบอ้างเป็นหน่วยงานราชการ หรือใช้หมายเลขโทรศัพท์ของหน่วยงานราชการ โทรมาหลอกลวงให้เหยื่อหลงเชื่อและโอนเงินให้ตามคำกล่าวอ้าง

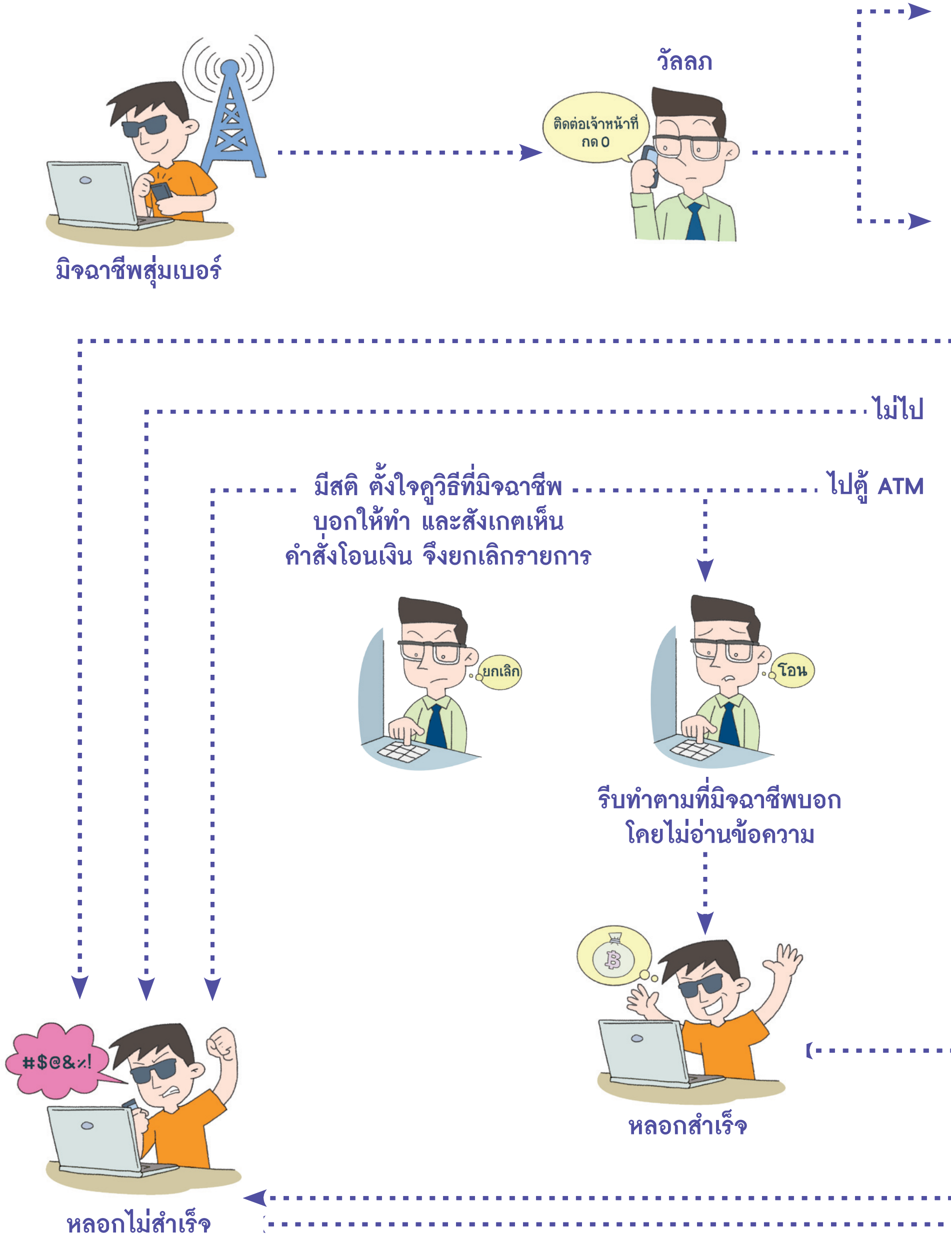
รู้หรือไม่ว่า...

บัญชีเงินฝากที่ใช้รับเงินโอน ไม่ใช่บัญชีของมิจฉาชีพ มิจฉาชีพจะไม่ใช้บัญชีของตนเองในการรับเงินโอนจากเหยื่อเพราะเสี่ยงต่อการถูกจับกุม จึงใช้วิธีการจ้างเปิดบัญชี ซึ่งมีนายหน้าเป็นผู้หาคนมารับจ้างเปิดบัญชี โดยจ่ายค่าจ้างเป็นเงินจำนวนหนึ่ง เพื่อแลกกับสมุดบัญชีและเอทีเอ็ม แล้วใช้บัญชีดังกล่าวเป็นบัญชีรับโอน

การรับจ้างเปิดบัญชีแทนผู้อื่นมีความผิดตามกฎหมาย หากไม่อยากเป็นส่วนหนึ่งของขบวนการต้มตุ๋นเหล่านี้ ต้องไม่รับจ้างเปิดบัญชีแทนผู้อื่นเด็ดขาด

นอกจากการว่าจ้างเปิดบัญชีแล้ว มิจฉาชีพยังมีวิธีหลอกให้เหยื่อใช้บัญชีตนเองเป็นบัญชีผ่าน เช่น หลอกว่าเป็นบริษัทขายของข้ามชาติไม่มีบัญชีในประเทศไทย เพื่อให้ลูกค้าโอนเงินได้สะดวก จึงขอให้ลูกค้าจ่ายเงินผ่านบัญชีของเหยื่อ โดยให้ค่านายหน้าจำนวนหนึ่ง

ทำอย่างไรให้ปลอดภัยจากการถูกหลอกลวง...



กด 0

หลอกถาม
ฐานะทางการเงิน

วางสาย

เงินน้อย

หลอกให้ทำรายการ
ที่ตู้เอทีเอ็ม

เงินเยอะ

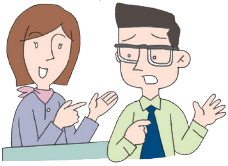
หลอกต่อว่าพัวพันยาเสพติด
แล้วให้ติดต่อเจ้าหน้าที่ตำรวจปลอม ๆ

ติดต่อ

ทบทวน
ความน่าจะเป็น
และวางสาย

หลอกให้ถอนและโอนเงิน
มาตรวจสอบที่ธนาคาร

ถอนเงินโดย
ไม่สอบถามพนักงาน



สอบถามพนักงานถึงข้อเท็จจริง
และความเป็นไปได้

คาถากันภัย...จากแก๊งคอลเซ็นเตอร์

- ตั้งสติ คิดทบทวนว่าข้อความหรือข้อมูลที่ได้รับเป็นจริงหรือไม่
- ไม่รู้จัก ไม่คุ้นเคย ไม่ให้ข้อมูลส่วนตัว เช่น เลขที่บัตรประชาชน วัน/เดือน/ปีเกิด รวมไปถึงข้อมูลการเงิน เช่น เลขที่บัญชี รหัสกดเงิน หรือแม้แต่วงเงินบัตรเครดิต หากเป็นเจ้าหน้าที่จากสถาบันการเงินจริง จะต้องทราบรายละเอียดของผู้ที่ต้องการติดต่ออยู่ก่อนแล้ว โดยไม่จำเป็นต้องถามชื่อนามสกุลเพิ่มเติม
- ไม่ทำรายการตามคำบอกผ่านทางโทรศัพท์ แม้จะได้รับการบอกกล่าวว่าเป็นเจ้าหน้าที่ของรัฐ หรือสถาบันการเงิน เพราะหน่วยงานของรัฐและสถาบันการเงินไม่มีนโยบายสอบถามข้อมูลส่วนตัวลูกค้าหรือประชาชนผ่านทางโทรศัพท์
- ไม่โลภอยากได้เงินรางวัลที่ไม่มีที่มา จำไว้ว่า "ของถูก ของดี ของฟรีไม่มีในโลก" เผลอ ๆ อาจได้ของแถม เพราะเข้าไปพัวพันกับธุรกิจผิดกฎหมาย เช่น การฟอกเงินโดยไม่รู้ตัว
- หากสงสัยต้องตรวจสอบ โดยติดต่อฝ่ายบริการลูกค้าของสถาบันการเงินหรือหน่วยงานนั้น เพื่อสอบถามข้อเท็จจริง โดยตรวจสอบเบอร์โทรจากแหล่งที่เชื่อถือได้ เช่น 1133 หรือเว็บไซต์ของสถาบันการเงินหรือหน่วยงานนั้น ๆ หรือสอบถามได้ที่ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.) ธนาคารแห่งประเทศไทย โทร. 1213

5 สิ่งที่ควรทำ... หลังตกเป็นเหยื่อแก๊งคอลเซ็นเตอร์

1. ทำ...การรวบรวมหลักฐานและข้อมูลทุกอย่างที่เกี่ยวข้องไว้ และตั้งสติให้ดี

2. ทำ...การแจ้งความต่อเจ้าหน้าที่ตำรวจ และไปลงบันทึกประจำวันไว้เป็นหลักฐาน ณ ท้องที่เกิดเหตุ เพื่อใช้เป็นหลักฐานในการระงับการโอนเงิน

3. ทำ...การแจ้งระงับการโอนเงิน ไปยังฝ่ายบริการลูกค้าของสถาบันการเงินนั้น หากถูกหลอก หรือเพื่อขอความช่วยเหลือและแก้ไขปัญหาเบื้องต้น

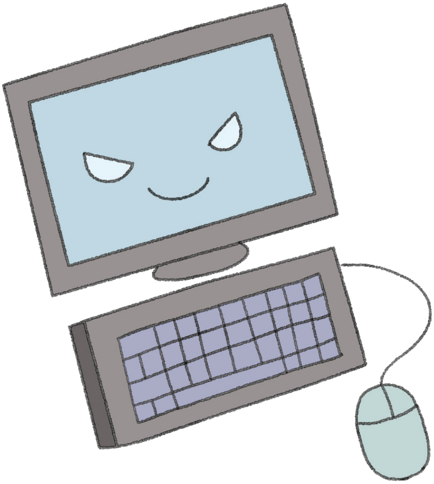
4. ทำ...การแจ้งเบาะแส ไปยังกรมสอบสวนคดีพิเศษ (DSI)

5. ทำ...ใจ เงินที่โอนไปให้มิจฉาชีพแล้ว โอกาสที่จะได้คืนนั้นมีน้อยมาก ยกเว้นผู้เสียหายสามารถแจ้งระงับการโอนก่อนที่มิจฉาชีพจะถอนเงินออกไป

4 ภัยออนไลน์...วายร้ายไฮเทค

ปัจจุบันเทคโนโลยีก้าวหน้าและอำนวยความสะดวกทางการเงินได้อย่างฉับไว แต่โอกาสเสี่ยงที่จะถูกวายร้ายไฮเทคฉกเงินไปก็มีไม่น้อยเช่นกัน

...ลองมาดูตัวอย่างวิธีการหลอกลวงของมิจฉาชีพกัน



มุขหลอก ๆ ในโลกออนไลน์

1. วิธีฉกเงินออนไลน์

สายรุ้งเดินทางไปธนาคาร xxx เพื่อสอบถามยอดเงินคงเหลือของตนเอง และก็ต้องพบกับเรื่องน่าเสียใจเมื่อพนักงานธนาคาร xxx แจ้งกับสายรุ้งว่า เงินในบัญชีสายรุ้งเหลือเพียง 117 บาท เพราะได้ใช้ระบบธนาคารออนไลน์โอนเงินจำนวน 500,000 บาท ออกจากบัญชีของเธอเองไปเมื่ออาทิตย์ที่ผ่านมา

สายรุ้งพยายามนึกทบทวนเหตุการณ์ที่เกิดขึ้น แต่นึกเท่าไหร่ก็นึกไม่ออก สายรุ้งไม่รู้ว่าผู้รับเงินของเธอเป็นใคร และไม่รู้แม้กระทั่งว่าเธอโอนเงินจำนวนดังกล่าวออกไปจากบัญชีของเธอเมื่อไหร่...

ทำไมเงินของสายรุ้งจึงหายไปจากบัญชีได้ มาดูกันว่ามิจฉาชีพฉกเงินจากบัญชีของเราได้ด้วยวิธีใดบ้าง

- **แฝงโปรแกรมร้าย (Malware) ในลิงก์ดาวน์โหลดหรือโปรแกรมต่าง ๆ**

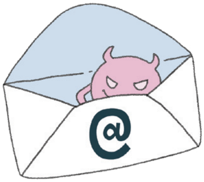
มิจฉาชีพอาจแฝงโปรแกรมร้ายในลิงก์ดาวน์โหลด ในโปรแกรม หรือในไฟล์ต่าง ๆ เช่น ลิงก์แสดงข้อความในเว็บไซต์ต่าง ๆ ที่อ้างว่าผู้เข้าชมได้รับรางวัล หรือข้อความเชิญชวนให้คลิกดูรูปภาพ เพื่อหลอกให้เหยื่อคลิกลิงก์ เพื่อติดตั้งโปรแกรมดังกล่าวในเครื่องคอมพิวเตอร์ โดยโปรแกรมร้ายอาจจะขโมยข้อมูลหรือบันทึกข้อมูลการใช้งานของเหยื่อ เช่น รหัสผู้ใช้งาน (Username) รหัสผ่าน (Password) หรืออาจจะเข้าควบคุมการใช้งาน รวมไปถึงปลอมแปลงคำขอทำธุรกรรมให้เหมือนเป็นคำสั่งจากเจ้าของบัญชี

รู้หรือไม่ว่า...

โปรแกรมร้าย หรือมัลแวร์ (Malware) เป็นโปรแกรมที่สร้างขึ้นมาเพื่อทำลายหรือสร้างความเสียหายให้กับระบบคอมพิวเตอร์ ระบบเครือข่าย รวมไปถึงข้อมูลของผู้ใช้งาน และโปรแกรมร้ายยังสามารถช่วยมิจฉาชีพขโมยเงินของคุณได้ ตัวอย่างของมัลแวร์ที่รู้จักกันดี เช่น ไวรัส โทรจัน

- **ปลอมแปลงอีเมลหลอกเหยื่อให้ข้อมูลในเว็บไซต์ปลอม**

มิจฉาชีพอาจส่งอีเมลแอบอ้างให้เหยื่อตกใจ เช่น อ้างว่าอายัดบัญชี หรืออ้างว่าอยู่ระหว่างการปรับปรุงระบบรักษาความปลอดภัยของธนาคาร และหลอกให้กรอกข้อมูลส่วนตัวในลิงก์แนบซึ่งมี URL ที่คล้ายหรือเกือบจะเหมือนกับเว็บไซต์จริง เมื่อเหยื่อหลงเชื่อกรอกข้อมูลต่าง ๆ ในเว็บไซต์ปลอม มิจฉาชีพก็จะสวมรอยเข้าไปส่งคำขอโอนเงินออกจากบัญชีของเหยื่อ



ในปัจจุบันธนาคารส่วนใหญ่จะกำหนดให้การทำธุรกรรมออนไลน์ทุกครั้ง ผู้ใช้บริการต้องกรอก "รหัสผ่านชั่วคราว" เพื่อยืนยันการทำรายการแต่ผู้ใช้บริการโดยมากมักใช้ความเคยชินในการใช้รหัสผ่านชั่วคราว โดยไม่อ่านข้อความที่ส่งมาพร้อมกับรหัสนั้นว่า "ใช้ยืนยันการทำธุรกรรมใด" จึงตกเป็นเหยื่อเมื่อกรอกรหัสดังกล่าวในคอมพิวเตอร์ โปรแกรมร้ายจะบันทึกรหัสดังกล่าวและส่งต่อให้กับมิจฉาชีพเพื่อนำไปใช้โอนเงินออกจากบัญชีของเหยื่อทันที

ดังนั้น ก่อนกรอกข้อมูลใด ๆ ในระบบธนาคารออนไลน์ ต้องตรวจสอบให้ดีก่อนว่า รายการที่กำลังทำอยู่นั้น เป็นไปตามที่ตั้งใจทำหรือไม่

รู้หรือไม่ว่า...

รหัสผ่านชั่วคราวหรือบางครั้งเรียก OTP (One Time Password) หรือ TOP (Time Out Password) เป็นรหัสผ่านที่ธนาคารออกให้ผู้ใช้บริการธนาคารออนไลน์เพื่อใช้ยืนยันการทำธุรกรรมสำคัญ ซึ่งจะใช้ได้เพียงหนึ่งครั้งในเวลาที่กำหนด โดยธนาคารจะส่งรหัสดังกล่าวพร้อมแจ้งรายละเอียดธุรกรรมที่ผู้ใช้บริการต้องยืนยันผ่านทาง SMS ไปยังเบอร์โทรศัพท์มือถือที่ผู้ใช้บริการแจ้งไว้

เรียน ลูกค้าธนาคาร xxx

ทางธนาคาร xxx ได้ทำการใช้ระบบความปลอดภัยใหม่ ทั้งนี้เพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยในการใช้บริการออนไลน์ จึงทำให้บัญชีและเอทีเอ็มของลูกค้าถูกระงับการใช้งานชั่วคราวเพื่อตรวจสอบ จึงใคร่ขอให้ท่านลูกค้าทำการเปิดใช้บริการบัญชีและเอทีเอ็มอีกครั้ง เพื่อป้องกันการเป็นบัญชีต้องสงสัย โดยสามารถเปิดใช้บัญชีได้ใหม่ โดยคลิกที่นี่ http://xxxBank-111.com/xxxBank.co.th/www.xxxBank.com/index_en.asp.htm

ทีมบริการลูกค้า
ธนาคาร xxx

2. แอบอ้างเป็นคนรู้จัก มิจฉาชีพมักจะแอบอ้างเป็นผู้ให้บริการอีเมลหลอกขอรหัสผู้ใช้งานและรหัสผ่านเพื่อเข้าระบบบัญชีอีเมลของเหยื่อเพื่อสวมรอยส่งอีเมลไปตามรายชื่อเพื่อน ๆ ในบัญชีอีเมลของเหยื่อเพื่อหลอกเอาเงิน

From: RumYai@hotmail.com
Subject: Urgent Request
To: LynGee@hotmail.com
Hello,

How are you doing? Sorry I didn't inform you about my travelling to England for a seminar. I misplaced my wallet on my way to the hotel. My money and other valuables are gone including my credit cards. I would like you to assist me with an urgent loan of 2000 british pounds to sort out my hotel bills and get myself back home. I promise to refund the money as soon as I return home. Please do this for me and I will be grateful.

Best Regards
RumYai

สวัสดี

สบายดีไหม ขอโทษที่ไม่ได้บอกฉันเดินทางมาสัมมนาที่อังกฤษ แต่กระเป๋าสตางค์หาย...

ขอยืมเงิน 2,000 ปอนด์เพื่อจ่ายค่าโรงแรมและค่าเดินทางกลับ ฉันจะจ่ายคืนทันทีที่กลับถึงบ้าน

3. อ้างเป็นบุคคลต่าง ๆ เช่น นักธุรกิจ ผู้ใจบุญ ผู้รับมรดก หรือแม้แต่ชายหนุ่มที่ต้องการหารักแท้ และหลอกเหยื่อว่าจะโอนเงินหรือส่งของขวัญมาให้ พร้อมแสดงหลักฐานการโอนเงินหรือส่งของปลอม ๆ ให้เหยื่อดู จากนั้นจะแอบอ้างเป็นเจ้าหน้าที่องค์กรต่าง ๆ แจ้งเหยื่อว่า เงินที่ส่งมานั้นไม่สามารถโอนได้เพราะติดเงื่อนไขต่าง ๆ

ต้องการสินค้าจำนวนมาก

บริจาคเงินจำนวนมาก

ต้องการคู่ชีวิต

ขอให้ช่วยรับมรดกแทน

ข้ออ้างที่มิจฉาชีพมักใช้หลอกเหยื่อให้โอนเงิน ได้แก่

- ธนาคารแห่งประเทศไทยระงับการโอนและขอตรวจสอบ
- ธนาคารกลางของประเทศต้นทางระงับการโอนเงิน เนื่องจากสงสัยว่าเป็นการฟอกเงิน
- สหประชาชาติ หรือไอเอ็มเอฟ ขอตรวจสอบเงิน
- ศุลกากรขอตรวจสอบของขวัญที่ส่งมา เพราะมีเงินสดบรรจุมาด้วย

จากนั้นจึงขอให้เหยื่อจ่ายค่าธรรมเนียมเพื่อยกเลิกการระงับเงินโอน โดยเริ่มจากค่าธรรมเนียมเรียกเก็บน้อย ๆ แล้วค่อย ๆ เพิ่มจำนวนสูงขึ้นเรื่อย ๆ กว่าเหยื่อจะรู้ตัว ก็เสียเงินไปมากแล้ว

รู้หรือไม่ว่า...

ผู้รับสินค้าหรือรับเงินโอนจากต่างประเทศ ไม่จำเป็นต้องเสียค่าภาษีหรือค่าธรรมเนียมเป็นเงินสดให้กับเจ้าหน้าที่ในต่างประเทศ การส่งสินค้าเข้ามายังผู้รับในประเทศ เจ้าหน้าที่จะเรียกเก็บอากรจากผู้รับตามกฎหมายไทยตอนรับสินค้า โดยไม่มีการเปิดตรวจหรือเก็บภาษีที่ต่างประเทศ สำหรับการโอนเงินระหว่างประเทศ ผู้โอนสามารถจ่ายค่าธรรมเนียมเอง หรือระบุให้หักค่าธรรมเนียมจากยอดเงินโอนได้ โดยผู้รับโอนไม่จำเป็นต้องจ่ายเป็นเงินสด หากมีข้อสงสัย สามารถสอบถามเพิ่มเติมได้ที่สายด่วนศุลกากร โทร. 1164 เว็บไซต์ www.customs.go.th

ผมต้องการแต่งงานกับคุณ...
ผมชื่อ William Phillip ผมอายุ 47 ปี มาจาก Lancaster ประเทศอังกฤษ เรียนจบวิศวกรรมทางทะเลจากมหาวิทยาลัย Oxford...
ผมเห็น Profile ของคุณในอินเทอร์เน็ต และคุณเป็นผู้หญิงในสเปกของผม...

รู้หรือไม่ว่า...

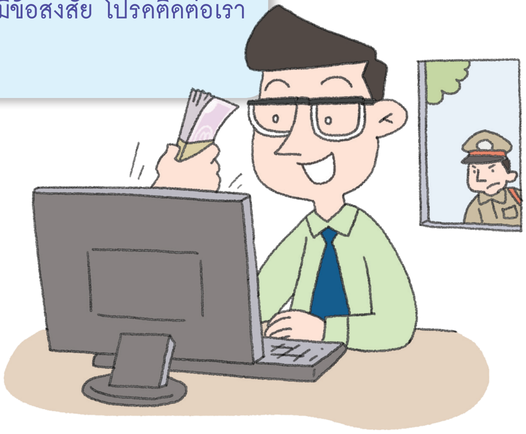
มิจฉาชีพจะสร้างความสนิทสนมคุ้นเคยก่อนหลอกเอาเงินเป็นปี มีการพูดคุยผ่านโทรศัพท์ และทำความรู้จักกับเหยื่อผ่าน Social Media ต่าง ๆ แล้วจึงเริ่มหลอกเหยื่อ ดังนั้น หากมีใครบอกว่าจะโอนเงินให้หรือส่งของขวัญมาให้ แต่ต้องจ่ายค่าธรรมเนียม หรือค่าใช้จ่ายอื่น ๆ ควรเช็กให้แน่ใจก่อน

4. ขอใช้เลขที่บัญชีเป็นที่พักเงิน โดยอ้างว่าตนเป็นนักธุรกิจ ทำการซื้อขายสินค้า ขอโอนเงินมาพักที่บัญชีเงินฝากของเหยื่อและยินดีแบ่งส่วนแบ่งให้กับเหยื่อเพื่อเป็นค่าตอบแทน หรือหลอกว่าโอนเงินเข้าผิดบัญชี ขอให้เหยื่อโอนเงินคืนให้ หรือหลอกว่ารับเหยื่อเข้าเป็นพนักงานบริษัทขายสินค้า มีหน้าที่โอนเงินค่าสินค้าให้บริษัท เมื่อเหยื่อทำตามที่ตกลง มิจฉาชีพจะได้รับเงินตามต้องการ แต่เรื่องของเหยื่อยังไม่จบแค่นี้...

เหยื่อจะได้รับการติดต่อจากเจ้าหน้าที่ธนาคารตัวจริงเกี่ยวกับเงินโอนผิดกฎหมายที่ถูกโอนเข้ามาที่บัญชีของเหยื่อ เหยื่อจะตกเป็นผู้ต้องสงสัยในการสมรู้ร่วมคิดกับแก๊งมิจฉาชีพในการกระทำผิดกฎหมาย ในขณะที่มิจฉาชีพตัวจริงก็ลอยนวลไป

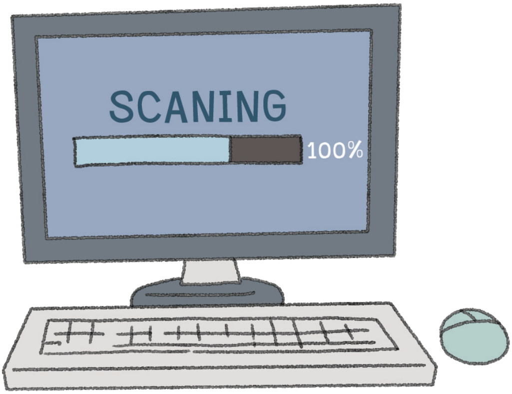
จดหมายรองรับการเป็นพนักงาน

จดหมายฉบับนี้ใช้เพื่อยืนยันว่า นายวัลลภ เป็นพนักงานของบริษัท AAA Warehouse LTD. ในตำแหน่งเจ้าหน้าที่การเงิน โดยบริษัทจะจ่ายค่านายหน้า 10% ของจำนวนเงินที่โอนพร้อมเงินเดือนจำนวน 25,000 บาท ในทุก ๆ วันที่ 28 ของเดือน หากมีข้อสงสัย โปรดติดต่อเราตามที่อยู่ที่ระบุไว้



รู้ทัน...ภัยออนไลน์

ได้เห็นถึงความพยายามของเหล่ามิจฉาชีพกันแล้ว คราวนี้มาดูกันว่าเราจะมีวิธีสังเกต และระวังภัยที่อาจเกิดขึ้นจากการใช้บริการทางการเงินออนไลน์ได้อย่างไรกันบ้าง



5 วิธีใช้ธนาคารออนไลน์อย่างปลอดภัย

1. ไม่ใช้ลิงก์เชื่อมโยงที่แนบมากับอีเมล หรือในเว็บไซต์ต่าง ๆ ที่ไม่น่าเชื่อถือ

2. ติดตั้งโปรแกรมตรวจจับไวรัสที่มีลิขสิทธิ์ และควรอัพเดตโปรแกรมบ่อย ๆ

3. หลีกเลี่ยงการทำธุรกรรมการเงินผ่านอินเทอร์เน็ตสาธารณะ หรือ ฟรี Wi-Fi รวมถึงปิด Bluetooth และ Wi-Fi เมื่อไม่ใช้งาน เพื่อป้องกันการถูกขโมยข้อมูล

4. พิจารณาข้อความที่ได้รับพร้อมรหัสผ่านชั่วคราว ว่ารหัสดังกล่าวใช้ยืนยันการทำธุรกรรมใด หากพบว่าธุรกรรมที่ต้องยืนยันไม่ตรงกับธุรกรรมที่ต้องการทำ ให้ออกจากระบบธนาคารออนไลน์ ติดต่อฝ่ายบริการลูกค้าของธนาคารนั้น ๆ ทันที เพื่อปรึกษาวิธีการใช้งานที่ปลอดภัยต่อไป

5. หลีกเลี่ยงการเข้าใช้เว็บไซต์ธนาคารออนไลน์ผ่านสมาร์ทโฟนและแท็บเล็ต โดยเฉพาะเครื่องที่ผ่านการเจลเบรก (Jailbreak) หรือรูท (Root) เพราะมีความเสี่ยงที่จะถูกขโมยข้อมูล

วิธีจับผิดอีเมลปลอม

1. ชื่อผู้ส่ง

มิจฉาชีพมักแอบอ้างโดยปลอมแปลงชื่อผู้ส่งให้เป็นชื่อขององค์กร จึงควรตรวจสอบชื่อบัญชีอีเมลควบคู่ไปด้วย

2. ชื่อบัญชีอีเมล

มักจะไม่ใช่ขององค์กรที่ถูกอ้างถึง ซึ่งโดยส่วนมากหากเป็นชื่อบัญชีอีเมลของสถาบันการเงินจริง ๆ ก็มักลงท้ายด้วยตัวย่อขององค์กรนั้น ๆ เช่น xxx@bot.or.th ซึ่งมาจาก Bank of Thailand

From: xxx Bank <info@aanetsetal.com>

Subjuct: xxx-Bank Account Suspended

IMPORTANT ALERT

Dear xxx Bank Customer,

We activated the NEW [xxx Bank Security]. Due to increased security.

Your account/ATM was disabled for verification.

Your are required to re-activate your account/ATM now to avoid suspension.

Activate Now!-http://xxxBan-111.com/xxxBank.co.th/www.xxxBank.com/index_en_asp.htm

Support@xxxbank

Than you.

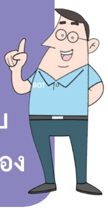
Xxx Bank.

3. URL

ตรวจสอบว่าเป็น URL ของสถาบันการเงินนั้นจริง ๆ โดยดูว่าขึ้นต้นด้วย https:// หรือไม่ และควรสะกดถูกต้องทุกตัวอักษร

รู้หรือไม่ว่า...

ธนาคารไม่มีนโยบายแนบลิงก์เข้าระบบธนาคารออนไลน์มากับอีเมล โดยลูกค้าต้องพิมพ์ URL เอง



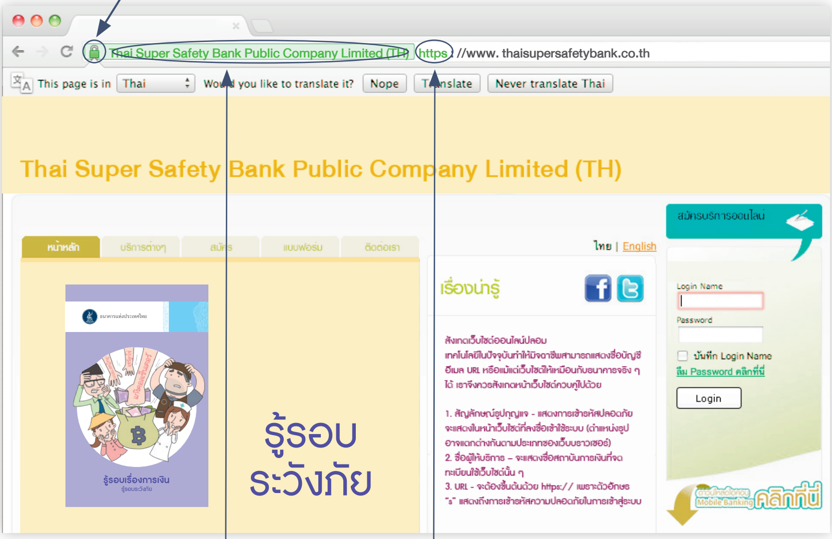
สังเกตเว็บไซต์ธนาคารออนไลน์ปลอม

เทคโนโลยีในปัจจุบันทำให้มิจฉาชีพสามารถแสดงชื่อบัญชีอีเมล URL หรือแม้แต่เว็บไซต์ให้เหมือนกับธนาคารจริง ๆ ได้ เราจึงควรสังเกตจุดอื่น ๆ ในหน้าเว็บไซต์ควบคู่ไปด้วย ดังนี้

1. สัญลักษณ์รูปกุญแจ แสดงการเข้ารหัสปลอดภัยจะแสดงในหน้าเว็บไซต์ที่ลงชื่อเข้าใช้ระบบ (ตำแหน่งรูปอาจแตกต่างกันตามประเภทของเว็บบราวเซอร์)

รู้หรือไม่ว่า...

สมาร์ทโฟนหรือแท็บเล็ตบางรุ่นก็ไม่แสดงสัญลักษณ์รูปกุญแจ ลูกค้าควรดาวน์โหลดแอพพลิเคชั่น (Application) ของธนาคารจากแหล่งที่เชื่อถือได้เพื่อเข้าใช้งานธนาคารออนไลน์



2. ชื่อผู้ให้บริการ จะแสดงชื่อสถาบันการเงินที่จดทะเบียนใช้เว็บไซต์นั้น ๆ

3. URL จะต้องขึ้นต้นด้วย https:// เพราะตัวอักษร "s" แสดงถึงการเข้ารหัสความปลอดภัยในการเข้าสู่ระบบ

ทำอย่างไร...ไม่ให้กลายเป็นเหยื่อภัยออนไลน์

เหตุผลสำคัญที่มักทำให้คนตกเป็นเหยื่อ คือ ความเชื่อใจ ความโลภ ความไม่รู้ และไม่เข้าใจเพียงพอในเรื่องกฎระเบียบ กฎหมาย และวิธีปฏิบัติในการทำธุรกรรมการเงินต่าง ๆ ดังนั้น เพื่อหลีกเลี่ยงการตกเป็นเหยื่อ

- **ควรตรวจสอบข้อเท็จจริงจากหน่วยงานหรือองค์กรที่น่าเชื่อถือ** หรือสามารถขอรับคำปรึกษาได้ที่ศูนย์คุ้มครองผู้ใช้บริการทางการเงินก่อนดำเนินการโอนเงิน
- **ควรติดตามข่าวสาร** เกี่ยวกับภัยทางการเงินอย่างสม่ำเสมอ เพื่อให้รู้เท่าทันกลลวงของมิจฉาชีพ
- **ควรพิจารณาให้รอบคอบ** หากได้รับข้อความแจกรางวัลที่มีมูลค่าสูง ให้คิดดูว่าเราเคยได้ร่วมลุ้นรางวัลนั้นหรือไม่ หากไม่เคย ให้สงสัยได้เลยว่าถูกหลอกแน่
- **อย่าหลงเชื่อข้อความชักชวนให้เข้าใช้โปรแกรมหรือเว็บไซต์ที่ไม่รู้จัก** เพราะอาจเสียรู้มิจฉาชีพ และสูญเสียเงินได้
- **อ่านรายละเอียดและตรวจสอบธุรกรรมทุกครั้งก่อนใช้รหัสผ่านชั่วคราว (OTP)**

...แต่หากคุณได้กลายเป็นเหยื่อของพวกมิจฉาชีพไปโดยไม่ทันระวัง สิ่งที่คุณสามารถทำได้หลังจากที่รู้ตัว คือ

- **เปลี่ยนรหัสผ่านทันที** เมื่อบังเอิญคลิกเชื่อมโยงไปยังเว็บไซต์ปลอมหรือคลิกลิงก์ที่สงสัยว่ามีโทรจันแฝงอยู่ และไม่ควรใช้รหัสที่ง่ายต่อการคาดเดา เช่น วัน/เดือน/ปีเกิด

- **แจ้งความและลงบันทึกประจำวัน** และรีบนำหลักฐานโอนเงินพร้อมหลักฐานการแจ้งความไปติดต่อกับสาขาของสถาบันการเงินเพื่อระงับการโอนเงิน

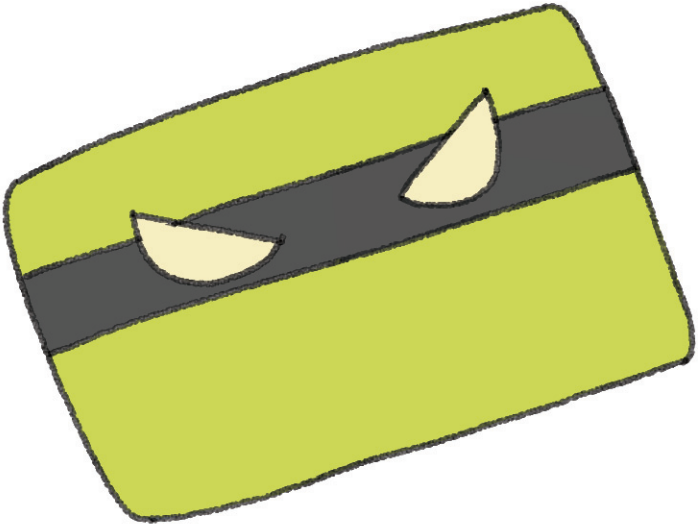
- **แจ้งฝ่ายบริการลูกค้าของผู้ให้บริการธนาคารออนไลน์หากพบเว็บไซต์ปลอม** เพื่อให้ดำเนินการปิดเว็บไซต์ดังกล่าว พร้อมปรึกษาวิธีการใช้งานอย่างปลอดภัย

- **หากถูกแอบอ้างใช้งานบัญชีอีเมล ให้รีบแจ้งเจ้าหน้าที่ด้านเทคนิค (Technical support)** ของผู้ให้บริการบัญชีอีเมลเพื่อเปลี่ยนรหัสผ่าน

- **ตรวจหาไวรัสในเครื่องคอมพิวเตอร์** พร้อมติดตั้งและอัพเดตโปรแกรมตรวจจับไวรัส (Anti-Virus) ที่มีลิขสิทธิ์อย่างสม่ำเสมอ

ที่สำคัญคือ ต้องทำใจกับเงินที่อาจมิได้กลับคืน เพราะมิจฉาชีพมักรีบโอนเงินออกจากบัญชีทันทีที่ได้รับเงิน ทำให้โอกาสที่จะได้เงินคืนกลับมามีน้อยมาก

5 ระวังภัย...บัตรถูกสวมรอย



ปัจจุบัน บัตรอิเล็กทรอนิกส์ต่าง ๆ ถูกใช้กันอย่างแพร่หลาย ไม่ว่าจะเป็น บัตรเครดิต บัตรเดบิต บัตรเอทีเอ็ม หรือบัตรกดเงินสด ซึ่งภายในบัตรจะมีการบันทึกข้อมูลของผู้ใช้ไว้ เช่น ชื่อ-นามสกุล หมายเลขบัญชี รหัสในการใช้บริการ จึงมีคำเตือนเจ้าของบัตรอยู่เสมอว่า

"ให้ระมัดระวังการใช้บัตรอิเล็กทรอนิกส์และเก็บรักษาในที่ปลอดภัยอยู่เสมอ"

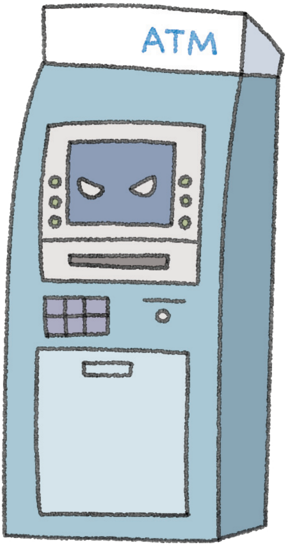
รู้ทัน...กลวิธีปลอมแปลงบัตร

สิ่งที่พวกมิจฉาชีพต้องการจากบัตรของเรา คือ ข้อมูล ซึ่งเป็นกุญแจสำคัญที่ทำให้สามารถฉกเงินจากบัญชีของเราไปได้นั่นเอง

เครื่องมือสำคัญที่พวกมิจฉาชีพนิยมใช้เพื่อขโมยข้อมูลจากบัตร เช่น

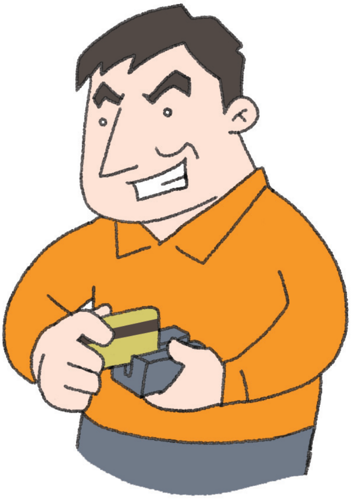
- **Skimmer : เครื่องขโมยข้อมูลในแถบแม่เหล็ก**

ใช้สำหรับลักลอบบันทึกข้อมูลที่เก็บอยู่ในแถบแม่เหล็กบนบัตรอิเล็กทรอนิกส์ และนำข้อมูลไปผลิตบัตรอิเล็กทรอนิกส์ปลอม ก่อนนำไปใช้ในนามของเหยื่อ โดยมิจฉาชีพจะนำเครื่องนี้ไปติดตั้งที่ตู้เอทีเอ็มที่คนไม่พลุกพล่าน เพื่อป้องกันการถูกจับระหว่างการติดตั้ง พร้อมกับติดตั้งแป้นครอบกดตัวเลข หรือติดกล้องขนาดจิ๋ว เพื่อแอบถ่ายข้อมูลรหัสบัตรระหว่างที่เจ้าของบัตรกำลังกดเงิน



• Scanner : อุปกรณ์คัดลอกข้อมูล

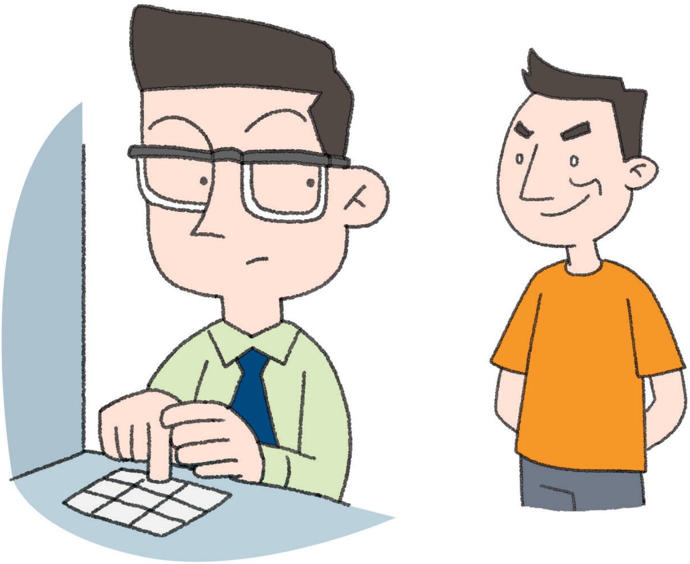
มิจฉาชีพจะนำบัตรอิเล็กทรอนิกส์ของเหยื่อมารูดกับอุปกรณ์คัดลอกข้อมูล พร้อมทั้งบันทึกรหัสปลอดภัย 3 ตัวด้านหลังบัตรไว้ ซึ่งวิธีนี้จะใช้ได้เฉพาะบัตรอิเล็กทรอนิกส์ชนิดที่เป็นแถบแม่เหล็ก ส่วนบัตรอิเล็กทรอนิกส์ชนิดที่บันทึกข้อมูลด้วยชิพ (chip) การคัดลอกข้อมูลจะทำได้ยากกว่า



ใช้บัตรอย่างไร...ให้ปลอดภัย

• หลีกเลี่ยงการใช้บัตรกับตู้เอทีเอ็มที่ตั้งอยู่ในสถานที่เปลี่ยว เพราะง่ายต่อการติดตั้งอุปกรณ์บันทึกข้อมูล และสังเกตว่าตู้เอทีเอ็มมีลักษณะผิดปกติหรือไม่

• หากต้องใช้บัตรชำระค่าสินค้าและบริการ เจ้าของบัตรควรอยู่ในบริเวณที่มองเห็นการทำรายการ เพื่อป้องกันพนักงานนำบัตรไปรูดกับเครื่องคัดลอกข้อมูล (Scanner) และหลีกเลี่ยงการใช้บัตรกับร้านค้าที่มีความเสี่ยงที่จะเกิดการทุจริต เช่น ปั๊มน้ำมัน สถานบันเทิง



- **ใช้มือปิดบังระหว่างกดรหัสผ่านเสมอ** เพื่อป้องกันการขโมยรหัส

- **ไม่บอกรหัสผ่านหรือข้อมูลทางการเงินแก่ผู้อื่น** หรือไม่เขียนรหัสผ่านไว้บนบัตรหรือในกระเป๋าสตางค์

- **ทำลายเอกสารแจ้งรหัสผ่าน** และเปลี่ยนรหัสผ่านบ่อย ๆ

- **ไม่ควรใช้รหัสผ่านที่ง่ายต่อการคาดเดา** เช่น วัน/เดือน/ปีเกิด หรือใช้รหัสเดียวกันสำหรับบัตรทุกใบ

- **เก็บใบบันทึกรายการไว้ทุกครั้ง** เพื่อเป็นหลักฐานในการตรวจสอบยอดการใช้จ่าย

- **ตรวจสอบรายการใช้จ่าย** หรือยอดเงินอย่างสม่ำเสมอ หากมีเหตุสงสัยหรือผิดปกติ ให้รีบแจ้งธนาคารเพื่อตรวจสอบและดำเนินการแก้ไขทันที

• **หากบัตรสูญหายหรือถูกขโมย** ให้รีบแจ้งธนาคารเพื่ออายัดบัตรทันที

• **ติดตามข่าวสาร** เพื่อรู้เท่าทันเล่ห์เหลี่ยมกลโกง

...เพียงเท่านี้ เราก็จะได้ไม่ต้องตกเป็น "เหยื่อ" ของพวกมิจฉาชีพ ที่คอยจ้องฉกเงินของเราได้แล้ว

อยากรู้รอบเรื่องการเงิน
ติดตามอ่านเล่มอื่น ๆ ด้วยนะครับ
BOT

"รู้รอบระวังภัย
เงินทองปลอดภัยจากมิจฉาชีพ"

รู้อย่างนี้แล้ว
ก็มาเริ่มต้นระวังภัยกันเลย

ดอกเบี้ยธนาคาร
หุ้น
ผลตอบแทน
กองทุน

ดอกเบี้ยธนาคาร
หุ้น
ผลตอบแทนกองทุน

ดอกเบี้ยธนาคาร

หุ้น

ผลตอบแทน
กองทุน

สร้างความมั่นคงในอนาคตของคุณ

วางแผนการเงินอย่างชาญฉลาด

รู้รอบระวังภัย

รักษาสิทธิ รู้หน้าที่ มีเป้าหมายการเงิน

คิดก่อนเป็นหนี้

พิมพ์ครั้งที่ 3 เดือนกันยายน พ.ศ. 2556
จำนวนพิมพ์ 20,000 เล่ม
จำนวน 52 หน้า
สงวนลิขสิทธิ์โดย ธนาคารแห่งประเทศไทย

ขอคำปรึกษาหรือร้องเรียนได้ที่
ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.)
โทร. 1213
แฟกซ์ 0 2283 6151
อีเมล fcc@bot.or.th
เว็บไซต์ www.bot.or.th/fcc
เฟซบุ๊ก www.facebook.com/hotline1213
จดหมาย
ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน
ธนาคารแห่งประเทศไทย สำนักงานใหญ่
(อาคาร 3 ชั้น 5) 273 ถนนสามเสน
เขตพระนคร กรุงเทพฯ 10200

ส่วนคุ้มครองและให้ความรู้ผู้ใช้บริการทางการเงิน
ธนาคารแห่งประเทศไทย
สำนักงานภาคตะวันออกเฉียงเหนือ
393 ถ.ศรีจันทร์ ต.ในเมือง อ.เมือง
จ.ขอนแก่น 40000

ส่วนคุ้มครองและให้ความรู้ผู้ใช้บริการทางการเงิน
ธนาคารแห่งประเทศไทย
สำนักงานภาคเหนือ
68/3 ถ.โชตนา ต.ช้างเผือก อ.เมือง
จ.เชียงใหม่ 50300

ส่วนคุ้มครองและให้ความรู้ผู้ใช้บริการทางการเงิน
ธนาคารแห่งประเทศไทย
สำนักงานภาคใต้
472 ถ.เพชรเกษม อ.หาดใหญ่
จ.สงขลา 90110

โทร.1213
ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน
ธนาคารแห่งประเทศไทย