กสทช.
NBTC

กสทช.

การสร้างความรู้เท่าทัน กลลวงมิจฉาชีพทางโทรศัพท์

สำหรับแหล่งองค์ความรู้และการบริหารจัดการความรู้
และช่องทางการสื่อสารภายในและภายนอกอื่น ๆ ของสำนักงาน กสทช.

บทนำ

ในยุคดิจิทัลที่เทคโนโลยีพัฒนาอย่างก้าวหน้า พัฒนาการด้านการสื่อสารมีความรวดเร็วและสะดวก ประชาชนหันมาใช้บริการออนไลน์มากขึ้น ส่งผลให้ช่องทางการหลอกลวงประชาชนผ่านช่องทางออนไลน์มีมากขึ้น โดยเฉพาะรูปแบบการหลอกลวงผ่าน “แก๊งคอลเซ็นเตอร์”

มิจฉาชีพแก๊งคอลเซ็นเตอร์ใช้กลวิธีอันแยบยล หลอกลวงให้ประชาชนโอนเงิน สูญเสียทรัพย์สินและสร้างความเสียหายอย่างมหาศาล

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือ สำนักงาน กสทช. เล็งเห็นถึงปัญหาดังกล่าว จึงรวบรวมรูปแบบของมิจฉาชีพ ในปัจจุบัน และจัดทำเป็นสื่อประชาสัมพันธ์ประเภทคู่มือเรื่อง **“การสร้างความรู้เท่ากันกลลวงมิจฉาชีพทางโทรศัพท์”** สำหรับใช้เป็นแนวทางให้ประชาชนสามารถรู้เท่าทันกลโกงของมิจฉาชีพ ป้องกันตัวและลดความเสี่ยงในการตกเป็นเหยื่อ ตลอดจน เป็นแหล่งองค์ความรู้และการบริหารจัดการความรู้ และช่องทางการสื่อสารภายในและภายนอกอื่น ๆ ของสำนักงาน กสทช. ที่สามารถนำไปใช้ประโยชน์ได้อย่างเหมาะสม เพื่อเท่าทันรูปแบบกลลวงอื่น ๆ ของมิจฉาชีพที่ปรับเปลี่ยนในอนาคต

ภายในคู่มือฉบับนี้ ประชาชนจะได้พบกับข้อมูลสำคัญ ดังนี้

- **กลโกงหลากหลายรูปแบบของแก๊งคอลเซ็นเตอร์ ที่มักใช้หลอกลวงประชาชน**
- **สัญญาณเตือนภัยที่บ่งบอกว่าสายที่คุณรับอาจเป็นมิจฉาชีพ**
- **แนวทางปฏิบัติเมื่อตกเป็นเหยื่อมิจฉาชีพ**
- **วิธีป้องกันตัวให้ปลอดภัยจากแก๊งคอลเซ็นเตอร์**
- **ช่องทางการติดต่อเพื่อขอความช่วยเหลือเมื่อถูกหลอกลวง**

สำนักงาน กสทช. หวังเป็นอย่างยิ่งว่าคู่มือฉบับนี้จะเป็นประโยชน์ต่อประชาชน ช่วยให้สามารถรู้เท่าทันกลโกงของมิจฉาชีพ ป้องกันตัวและลดความเสี่ยงในการตกเป็นเหยื่อ

“เพราะความรู้คืออาวุธที่ดีที่สุดในการต่อสู้กับมิจฉาชีพ”

โดย สำนักสื่อสารองค์กร

สารบัญ

บทที่ 1: รู้ทันกลลวง มิจฉาชีพแก๊งคอลเซ็นเตอร์ 6

แก๊งคอลเซ็นเตอร์ 6 - 7

ซิมผี บัญชีม้า 8

AI ปลอมเสียง หลอกโอนเงิน 9

ลิงก์ข้อความหลอกลวง 10

มิ(ตร)ฉาชีพ หลอกยืมเงินผ่านบัญชีไลน์ 11

หลอกให้กลัวแล้วโอนเงิน 12

App ดูดเงิน 13

บทที่ 2: 4 สัญญาณเตือน รู้ตัวก่อนโดนหลอก 14

บทที่ 3: 8 วิธีปฏิบัติ เมื่อตกเป็นเหยื่อมิจฉาชีพ 16 - 17

บทที่ 4: ป้องกันตนเองอย่างไร จากภัยมิจฉาชีพ 18

บทที่ 5: ช่องทางการติดต่อ เพื่อขอความช่วยเหลือ 19

บทที่ 6: กฎหมายที่เกี่ยวข้อง กับมิจฉาชีพทางโทรศัพท์ 20

บทที่ 7: แนะนำช่องทาง ตรวจสอบข้อมูล มิตร หรือ มิจ(ฉาชีพ) 21

บทที่ 8: สถิติ กลลวง แบบไหนที่คนไทยโดนหลอกมากที่สุด 22

รวบรวมสายด่วนแจ้งเหตุ เกี่ยวกับมิจฉาชีพทางโทรศัพท์ 23

กสทช. NBTC

บทที่ 1
รู้ทันกลลวง
มิจฉาชีพแก๊งคอลเซ็นเตอร์

ในยุคดิจิทัลที่มิจฉาชีพมีกลยุทธ์ใหม่ ๆ หลอกลวงผู้คนอยู่เสมอ เอกสารฉบับนี้จึงรวบรวม “ประเภทกลโกงมิจฉาชีพแก๊งคอลเซ็นเตอร์” ที่พบได้บ่อย เพื่อให้หน่วยงานราชการ เอกชนและประชาชนทั่วไป สามารถรู้เท่าทัน เข้าใจกลวิธี และป้องกันตัวได้อย่างมีประสิทธิภาพ

แก๊งคอลเซ็นเตอร์

แก๊งคอลเซ็นเตอร์ หมายถึง กลุ่มมิจฉาชีพที่ใช้โทรศัพท์ติดต่อหลอกลวงประชาชน โดยมักแอบอ้างเป็นเจ้าหน้าที่จากหน่วยงานรัฐ ธนาคาร บริษัทเอกชน หรือบุคคลที่น่าเชื่อถือ หลอกให้เหยื่อโอนเงิน สูญเสียข้อมูลส่วนตัว หรือกระทำการอื่น ๆ ที่ก่อให้เกิดความเสียหาย

“แก๊งคอลเซ็นเตอร์ล่าเหยื่อรายวัน! รู้ทันกลโกง ป้องกันตัวได้!”

มิจฉาชีพปลอมตัวเป็นเจ้าหน้าที่ กสทช.

มิจฉาชีพแก๊งคอลเซ็นเตอร์กลับมาอีกครั้ง! คราวนี้มาในรูปแบบใหม่ แอบอ้างเป็นเจ้าหน้าที่สำนักงาน กสทช. หลอกลวงประชาชนให้โอนเงินหรือเปิดเผยข้อมูลส่วนตัว

วิธีการของแก๊งคอลเซ็นเตอร์:

- โทรมาหาประชาชน หลอกลวงว่าเป็นเจ้าหน้าที่จากสำนักงาน กสทช.
- แจ้งว่า เบอร์โทรศัพท์ของเหยื่อถูกระงับการใช้งาน เนื่องจากมีการร้องเรียนการใช้บริการที่ผิดกฎหมาย
- ขู่ว่าจะดำเนินคดี หากไม่ดำเนินการแก้ไข
- หลอกให้เหยื่อโอนเงิน ไปยังบัญชีธนาคารเพื่อปลดล็อกเบอร์โทรศัพท์
- หลอกให้เหยื่อ เปิดเผยข้อมูลส่วนตัว เช่น รหัส OTP หรือเลขบัตรประชาชน

สำนักงาน กสทช. ขอแจ้งเตือนประชาชนว่า:

- สำนักงาน กสทช. ไม่มีนโยบาย ในการโทรหาประชาชนเพื่อแจ้งเตือนการระงับเบอร์โทรศัพท์
- ประชาชน ไม่ควรโอนเงิน หรือ เปิดเผยข้อมูลส่วนตัวให้กับบุคคลที่ไม่รู้จัก
- หากได้รับสายโทรศัพท์จากเบอร์แปลก อ้างตัวเป็นเจ้าหน้าที่สำนักงาน กสทช. ควรวางสายโทรศัพท์ทันที
- ตรวจสอบข้อมูลกับ สำนักงาน กสทช. ผ่านช่องทางการติดต่ออย่างเป็นทางการ ดังนี้
  1) เว็บไซต์: www.nbtc.go.th
  2) ศูนย์รับเรื่องร้องเรียน สำนักงาน กสทช. 1200 (โทรฟรี)
  3) โทร 1441 เพื่อแจ้งความผ่านระบบแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ: www.thaipoliceonline.go.th

มิจฉาชีพปลอมตัวเป็นเจ้าหน้าที่กรมที่ดิน

ในช่วงที่ผ่านมา มีรูปแบบการปลอมตัวของมิจฉาชีพแก๊งคอลเซ็นเตอร์ ที่มักแอบอ้างเป็นเจ้าหน้าที่กรมที่ดิน หลอกลวงประชาชนให้โอนเงินหรือเปิดเผยข้อมูลส่วนตัว

วิธีการของแก๊งคอลเซ็นเตอร์:

- โทรหาประชาชน หลอกลวงว่าเป็นเจ้าหน้าที่กรมที่ดิน
- แจ้งว่า มีเอกสารสำคัญจากกรมที่ดิน รอให้รับ
- ขู่ว่าจะดำเนินคดี หากไม่ดำเนินการรับเอกสาร
- หลอกให้เหยื่อโอนเงิน ไปยังบัญชีธนาคารเพื่อค่าจัดส่งเอกสาร หรือ หลอกให้เหยื่อ เปิดเผยข้อมูลส่วนตัว เช่น รหัส OTP หรือเลขบัตรประชาชน

สำนักงาน กสทช. ขอแจ้งเตือนประชาชนว่า:

- กรมที่ดิน มีนโยบาย ไม่โทรหา ไม่ขอแอดไลน์ ไม่มีหน้าที่เก็บภาษีที่ดินและสิ่งปลูกสร้าง และไม่มีหน้าที่อัพเดทข้อมูลอาคารชุด/หมู่บ้านจัดสรร ผ่านทางโทรศัพท์
- ประชาชน ไม่ควรโอนเงิน หรือ เปิดเผยข้อมูลส่วนตัวให้กับบุคคลที่ไม่รู้จัก
- หากได้รับสายโทรศัพท์จากเบอร์แปลก อ้างตัวเป็นเจ้าหน้าที่กรมที่ดิน ควรวางสายโทรศัพท์ทันที
- ตรวจสอบข้อมูล กับกรมที่ดิน ผ่านช่องทางการติดต่ออย่างเป็นทางการ ดังนี้
  1) ติดต่อสอบถามข้อมูลได้ที่สำนักงานที่ดินทุกแห่งทั่วประเทศ หรือโทร Call center กรมที่ดิน 02-141-5555 และ www.dol.go.th
  2) โทร 1441 เพื่อแจ้งความผ่านระบบแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ: www.thaipoliceonline.go.th

อ้างอิง: กรมที่ดิน Fanpage

มิจฉาชีพปลอมตัวเป็นเจ้าหน้าที่ไปรษณีย์ไทย

อีกหนึ่งรูปแบบการหลอกลวงของมิจฉาชีพแก๊งคอลเซ็นเตอร์ที่ไม่เคยหายไป คือการแอบอ้างเป็นเจ้าหน้าที่ไปรษณีย์ไทย หลอกลวงประชาชนให้โอนเงินหรือเปิดเผยข้อมูลส่วนตัว

วิธีการของแก๊งคอลเซ็นเตอร์:

- โทรมาหาประชาชน หลอกลวงว่าเป็นเจ้าหน้าที่ไปรษณีย์ไทย
- แจ้งว่า มีพัสดุตกค้าง รอการจัดส่ง
- ขู่ว่าจะดำเนินการส่งพัสดุคืน หากไม่ชำระค่าธรรมเนียมเพิ่มเติม
- หลอกให้เหยื่อโอนเงิน ไปยังบัญชีธนาคารเพื่อค่าธรรมเนียมการจัดส่ง หรือ หลอกให้เหยื่อ เปิดเผยข้อมูลส่วนตัว เช่น รหัส OTP หรือเลขบัตรประชาชน

สำนักงาน กสทช. ขอแจ้งเตือนประชาชนว่า:

- บุรุษไปรษณีย์ไทย จะใช้เบอร์ ๑๕๐๕ เพื่อติดต่อผู้รับจดหมายเท่านั้น
- ตั้งสติ อย่าหลงเชื่อ ต้องตรวจสอบข้อมูลจากแหล่งข้อมูลที่ถูกต้องของไปรษณีย์ไทย
- ประชาชน ไม่ควรโอนเงินหรือเปิดเผยข้อมูลส่วนตัวให้กับบุคคลที่ไม่รู้จัก
- หากได้รับสายโทรศัพท์จากเบอร์แปลก อ้างตัวเป็นเจ้าหน้าที่ไปรษณีย์ไทย ควรวางสายโทรศัพท์ทันที
- ตรวจสอบข้อมูลกับไปรษณีย์ไทย ผ่านช่องทางการติดต่ออย่างเป็นทางการ ดังนี้
  1) โทร 1505 ติดต่อกับบุรุษไปรษณีย์ไทยได้ทันทีในกรณีเร่งด่วน
  2) โทร 1545 เพื่อสอบถามข้อมูลทั่วไป ติดตามของฝากส่ง หรือร้องเรียนการให้บริการ
  3) โทร 1441 เพื่อแจ้งความผ่านระบบแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ: www.thaipoliceonline.go.th

อ้างอิง: ข่าวประชาสัมพันธ์ บริษัท ไปรษณีย์ไทย จำกัด

กสทช. NBTC

ซิมพี บัญชีม้า

ซิมผี หมายถึง เบอร์โทรศัพท์มือถือที่ไม่ระบุชื่อผู้ครอบครอง มักใช้เพื่อเปิดบัญชีธนาคารหรือแอปพลิเคชันต่าง ๆ โดยมิจฉาชีพ

บัญชีม้า หมายถึง บัญชีธนาคารหรือบัญชีแอปพลิเคชัน การเงินที่เปิดขึ้นโดยใช้ซิมผี มิจฉาชีพจะใช้บัญชีม้าเหล่านี้เพื่อรับเงินจากเหยื่อที่ถูกหลอกลวง โดยหลังจากโอนเงินแล้วมิจฉาชีพจะรีบถอนเงินออกจากบัญชีทันที ทำให้ยากต่อการติดตามและดำเนินคดี

การใช้ “ซิมผีและบัญชีม้า” เป็นการกระทำที่ผิดกฎหมาย ผู้ที่เปิดบัญชีหรือรับเงินโอนเข้าบัญชีม้า มีโอกาสถูกดำเนินคดีและถูกลงโทษตามกฎหมาย

มิจฉาชีพในปัจจุบันมีกลวิธีที่หลากหลาย แยบยลและทันสมัย เพื่อหลอกลวงผู้คนให้เปิดบัญชีม้า ซิมม้า และสูญเสียเงินทอง ข้อมูลส่วนตัว สร้างความเสียหาย

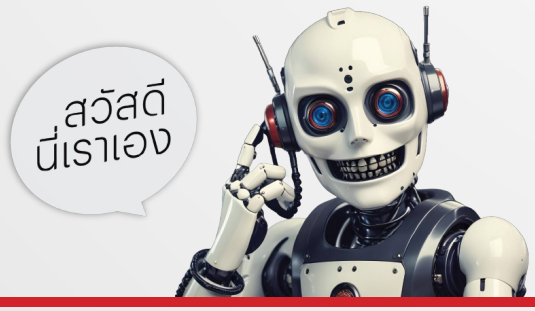
รูปแบบการหลอกลวงที่พบบ่อย:

- หลอกให้เปิดบัญชีรับเงินค่าจ้าง เสนอเงินเดือนสูง โอนเงินมัดจำ ส่งมอบงานไม่ตรงสัญญา
- หลอกให้เปิดบัญชีกู้ยืมเงินออนไลน์ อ้างดอกเบี้ยต่ำ โอนเงินค่าธรรมเนียม โอนเงินแล้วไม่ให้กู้ หรือให้กู้ไม่ครบตามวงเงิน
- หลอกให้เปิดบัญชีเล่นพนันออนไลน์ เสนอโบนัส โอนเงินเข้าบัญชี ควบคุมผลแพ้ชนะ โอนเงินออกจากบัญชีผู้เล่น
- แอบอ้างเป็นเจ้าหน้าที่หลอกให้เปิดบัญชี หลอกให้เปิดเผยข้อมูลส่วนตัว โอนเงิน กดลิงก์ปลอม ดึงข้อมูลจากบัญชี
- ซื้อบัญชีธนาคาร นำไปรับโอนเงินจากการหลอกลวง แล้วถอนเงินออกจากบัญชี ทำให้เจ้าของบัญชี ตัวจริงเดือดร้อน
- สวมรอยเป็นเจ้าของบัญชี แอบอ้างเป็นเจ้าของบัญชี แล้วเปลี่ยนแปลงข้อมูล เบิกถอนเงิน ทำให้เจ้าของบัญชีตัวจริงสูญเสียเงิน

วิธีป้องกันตนเอง:

- ห้ามเปิดบัญชีให้ผู้อื่นใช้ ไม่ว่าจะเป็นญาติหรือคนรู้จัก
- ตรวจสอบบัญชีธนาคาร หมั่นดูสมุดบัญชี หรือตั้งการแจ้งเตือนธุรกรรมในโทรศัพท์มือถือ
- ห้ามให้ข้อมูลส่วนตัว แก่บุคคลที่ไม่น่าเชื่อถือ
- ระวังมิจฉาชีพแอบอ้าง ตรวจสอบข้อมูลก่อนโอนเงิน
- แจ้งความหากถูกหลอก หรือรู้ตัวว่าเปิดบัญชีม้า ซิมม้า หรือ โทร 1441 เพื่อแจ้งความผ่านระบบแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ: www.thaipoliceonline.go.th

“เปิดซิมผีบัญชีม้า
เสียทั้งเงินและอนาคต”



AI ปลอมเสียง หลอกโอนเงิน

กลวิธีมิจฉาชีพที่ใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) เลียนเสียงบุคคลที่รู้จัก เช่น ญาติ เพื่อน หรือเจ้าหน้าที่ธนาคาร หลอกลวงให้เหยื่อโอนเงิน โดยมิจฉาชีพจะบันทึกเสียงต้นฉบับของบุคคลเป้าหมาย นำมาฝึกฝนกับโมเดล AI

เมื่อโมเดล AI เรียนรู้เสียงได้ดีแล้ว มิจฉาชีพจะใช้ AI สร้างเสียงเลียนแบบบุคคลเป้าหมาย พูดข้อความหลอกลวง เพื่อโน้มน้าวให้เหยื่อโอนเงิน

กลวิธีนี้มีความอันตรายสูง เพราะเหยื่อมักหลงเชื่อเสียงที่เหมือนจริง คิดว่าเป็นบุคคลที่รู้จักจริง ๆ ยอมโอนเงินให้ โดยไม่ทันตั้งตัว

มิจฉาชีพยุคใหม่ ใช้วิธีการอันแยบยล หลอกลวงเหยื่อด้วยเทคโนโลยี AI ปลอมเสียง สร้างความเสียหายอย่างร้ายแรง

รูปแบบการหลอกลวงที่พบบ่อย:

- โทรมาด้วยเบอร์แปลก มิจฉาชีพจะใช้เบอร์โทรศัพท์ที่ไม่คุ้นเคย โทรมาหาเหยื่อ
- อ้างตัวเป็นคนรู้จัก มิจฉาชีพจะปลอมเสียง เลียนแบบบุคคลที่เหยื่อรู้จัก เช่น ญาติสนิท เพื่อนสนิท เจ้านาย หรือแม้กระทั่งคนดัง
- ใช้เทคโนโลยีโคลนนิ่งเสียง (Voice Clone) มิจฉาชีพ หรือใช้เทคโนโลยี AI โคลนนิ่งเสียงของบุคคลที่ต้องการปลอมตัว ทำให้เสียงที่ได้เหมือนจริง ยากต่อการแยกแยะ
- สร้างสถานการณ์ฉุกเฉิน มิจฉาชีพจะสร้างสถานการณ์ที่ทำให้เหยื่อรู้สึกตื่นตระหนก ตกใจ กลัว กังวล เช่น อ้างว่าญาติประสบอุบัติเหตุ ถูกเรียกค่าไถ่ หรือกำลังถูกตำรวจจับ
- บีบให้เหยื่อโอนเงินโดยไม่ทันตั้งตัว ด้วยความตกใจ เหยื่อมักถูกมิจฉาชีพชักจูง หลอกให้โอนเงินโดยไม่ทันตั้งตัว สูญเสียทรัพย์สิน

วิธีป้องกันตนเอง:

- ตรวจสอบเบอร์โทร ถ้าไม่คุ้นเคย ให้วางสายทันที
- รอฟังเสียงปลายสาย ถ้าไม่คุ้นเคยหรือไม่แน่ใจ ให้วางสาย
- ห้ามโอนเงินหรือส่งข้อมูลทางโทรศัพท์เด็ดขาด
- ตรวจสอบชื่อบัญชี ถ้าไม่ตรงหรือไม่แน่ใจ ต้องติดต่อเจ้าของบัญชีก่อนโอน
- ตั้งสติ ไม่รีบร้อน ไม่ว่าจะฉุกเฉินแค่ไหน ต้องตรวจสอบข้อมูลก่อนตัดสินใจ
- แจ้งความหากถูกหลอก หรือรู้ตัวว่าเปิดบัญชีม้า ซิมม้า หรือโทร 1441 เพื่อแจ้งความผ่านระบบแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ: www.thaipoliceonline.go.th

“มิจฉาชีพพัฒนาเทคโนโลยี AI ปลอมเสียง หลอกเหยื่อโอนเงิน”

กสทช. NBTC

ลิงก์ข้อความหลอกลวง

“ลิงก์ข้อความหลอกลวง” หมายถึง ข้อความที่ส่งมาทาง SMS หรือช่องทางออนไลน์อื่น ๆ เช่น อีเมล แชท ฯลฯ โดยมีจุดประสงค์เพื่อหลอกลวงให้ผู้รับคลิกลิงก์

ลิงก์เหล่านี้อาจนำไปยังเว็บไซต์ปลอม แอปพลิเคชันอันตราย หรือมัลแวร์ เมื่อผู้รับคลิกลิงก์และกรอกข้อมูลอาจถูกขโมยข้อมูลส่วนตัว เช่น รหัสผ่าน ข้อมูลบัญชีธนาคาร หรือถูกติดตั้งมัลแวร์ในอุปกรณ์

ในยุคดิจิทัล มิจฉาชีพใช้วิธีการหลอกลวงรูปแบบใหม่ผ่าน “ลิงก์ข้อความหลอกลวง” แฝงตัวมาในรูปแบบ SMS อีเมลปลอมเป็นองค์กรน่าเชื่อถือ เพื่อขโมยข้อมูลส่วนตัว และดูดเงินจากบัญชีธนาคาร

รูปแบบการหลอกลวงที่พบบ่อย:

- ส่ง SMS อีเมล อ้างเป็นองค์กรน่าเชื่อถือ มิจฉาชีพจะส่ง SMS หรืออีเมล แอบอ้างเป็นธนาคาร Shopee Lazada หรือองค์กรอื่น ๆ ที่น่าเชื่อถือ หลอกลวงให้เหยื่อหลงเชื่อ
- แนบลิงก์หลอกลวง: ใน SMS อีเมล มิจฉาชีพจะแนบลิงก์หลอกลวง กระตุ้นให้เหยื่อคลิกลิงก์ เพื่อดาวน์โหลดแอปพลิเคชันหรือกรอกข้อมูลส่วนตัว
- เนื้อหาเร่งด่วน โปรโมชันพิเศษ: มิจฉาชีพจะใช้เนื้อหาที่เร่งด่วนหรือเสนอโปรโมชันพิเศษ เพื่อกระตุ้นให้เหยื่อกดลิงก์โดยไม่ทันตั้งตัว

วิธีป้องกันตนเอง:

- ตรวจสอบชื่อผู้ส่ง เนื้อหา และลิงก์
- ตรวจสอบลิงก์เว็บไซต์ว่าตรงกับองค์กรที่อ้างหรือไม่
- ห้ามกรอกข้อมูลส่วนตัว ผ่าน SMS/อีเมล
- หากสงสัย ต้องติดต่อองค์กรที่อ้าง แล้วยืนยันข้อมูล
- หากภาษาหรือไวยากรณ์ผิดปกติ มีโอกาสเป็นลิงก์หลอกลวงแน่นอน
- ระวังข้อความที่เน้นให้ตัดสินใจเร่งด่วนหรือโปรโมชันพิเศษ
- ติดตั้งแอป “กันกวน” จากสำนักงาน กสทช. เพื่อแจ้งเตือนเบอร์/SMS อันตราย
- แจ้งความหากถูกหลอก หรือรู้ตัวว่าเปิดบัญชีม้า ซิมม้า หรือโทร 1441 เพื่อแจ้งความผ่านระบบแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ: www.thaipoliceonline.go.th

“ลิงก์หลอกลวง” อันตรายรูปแบบใหม่ ระวังก่อนคลิก

มิ(ตร)ฉาชีพ หลอกยืมเงินผ่านบัญชีไลน์

ภัยแก๊งคอลเซ็นเตอร์อีกรูปแบบ คือ มิจฉาชีพที่แฮก หรือปลอมบัญชีไลน์ หรือบัญชีโซเชียลมีเดียของบุคคลอื่น เพื่อติดต่อเหยื่อทางข้อความส่วนตัว โดยอ้างตัวเป็นญาติ เพื่อนสนิท หรือบุคคลที่รู้จัก

แล้วหลอกลวงให้เหยื่อโอนเงินให้ โดยใช้วิธีการต่าง ๆ เช่น อ้างว่าประสบปัญหา ด่วน ต้องการใช้เงินฉุกเฉิน หรือเสนอผลตอบแทนพิเศษ อย่ารีบโอน! เพราะอาจเป็นกลโกงของ “มิ(ตร)ฉาชีพ”

เคยไหม? ได้รับข้อความจากเพื่อนในไลน์ ทักมายืมเงิน บอกว่าบัญชีมีปัญหา โอนเงินไม่ได้ อย่ารีบโอน! เพราะอาจเป็นกลโกงของ “มิ(ตร)ฉาชีพ” ที่แฮกบัญชีไลน์เพื่อน สวมรอยเป็นเจ้าของบัญชี ทักหาเพื่อนของเหยื่อ หลอกให้โอนเงิน

กลยุทธ์ของมิ(ตร)ฉาชีพ:

- มิจฉาชีพจะแฮกบัญชีไลน์หรือหาทางเข้าถึงบัญชีไลน์ของเหยื่อ
- สวมรอยเป็นเจ้าของบัญชี โดยการเริ่มต้นทักหาเพื่อนสนิท ญาติหรือครอบครัว
- ทักหาเพื่อนของเจ้าของบัญชี เลือกทักหาเพื่อน ที่เหยื่อไม่ค่อยคุยด้วย หรือเพื่อนสนิทที่เหยื่อไว้ใจ
- อ้างว่าบัญชีทางการเงินมีปัญหา อ้างว่าบัญชีธนาคาร บัตรเครดิต หรือแอปพลิเคชันการเงินมีปัญหา โอนเงินไม่ได้
- ขอยืมเงินด่วน รีบร้อน ขอยืมเงินจำนวนไม่มาก บอกว่าจะคืนให้เร็ว ๆ
- โอนเงินไปยังบัญชีของบุคคลที่ 3 เมื่อเหยื่อหลงเชื่อ รีบให้เหยื่อโอนเงินไปยังบัญชีของบุคคลที่ 3
- บล็อกแชท เมื่อได้เงินแล้ว รีบบล็อกแชท ตัดการติดต่อ

วิธีป้องกันตนเอง:

- ระวังข้อความจาก “มิตร” ที่ไม่คุ้นเคย โดยไม่โอนเงินให้ใครผ่านไลน์ หรือช่องทางโซเชียลมีเดียที่ไม่แน่ใจ
- โทรหาเพื่อนหรือคนรู้จักโดยตรงผ่านเบอร์โทรศัพท์ที่มั่นใจว่าถูกต้อง เพื่อตรวจสอบความถูกต้องของบัญชี
- อย่ารีบโอนเงิน ต้องยืนยันตัวตนของบุคคลที่ทักมาให้แน่ใจก่อนและโอนเงินผ่านช่องทางที่ปลอดภัย
- แจ้งความหากถูกหลอก หรือรู้ตัวว่าเปิดบัญชีม้า ซิมม้า หรือโทร 1441 เพื่อแจ้งความผ่านระบบแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ: www.thaipoliceonline.go.th

ระวัง “มิจฉาชีพ” ปลอมเป็น “มิตร” หลอกยืมเงินผ่านไลน์

กสทช. NBTC

หลอกให้กลัวแล้วโอนเงิน

อีกหนึ่งกลยุทธ์การหลอกลวงเหยื่อให้โอนเงิน คือ การ “หลอกให้กลัวแล้วโอนเงิน” โดยมิจฉาชีพจะสร้างสถานการณ์ที่น่ากลัวกดดัน หรือเร่งด่วน เพื่อกระตุ้นให้เหยื่อเสียสติตัดสินใจผิดพลาดโอนเงินให้โดยไม่ตรวจสอบ

ในยุคดิจิทัล มิจฉาชีพใช้วิธีการหลอกลวงรูปแบบใหม่ ผ่าน “ลิงก์ข้อความหลอกลวง” แฝงตัวมาในรูปแบบ SMS อีเมล ปลอมเป็นองค์กรน่าเชื่อถือ เพื่อขโมยข้อมูลส่วนตัว และดูดเงินจากบัญชีธนาคาร

รูปแบบการหลอกลวงที่พบบ่อย:

- อ้างตัวเป็นเจ้าหน้าที่รัฐ เช่น ตำรวจ ทหาร หรือเจ้าหน้าที่สรรพากร
- แจ้งว่าเหยื่อมีหมายจับ เช่น คดีเงินผิดกฎหมาย หรือคดียาเสพติด ทำให้เหยื่อหวาดกลัว ให้เหยื่อรีบโอนเงินประกันตัว
- อ้างว่าบัญชีธนาคารของเหยื่อถูกแฮก เงินในบัญชีถูกโอนออกหมด หลอกให้เหยื่อโอนเงินไปยังบัญชีปลอดภัยที่มิจฉาชีพจัดเตรียมไว้
- หลอกให้เหยื่อลงทุนในธุรกิจปลอม เสนอให้ลงทุนด้วยผลตอบแทนสูงเกินจริง
- ข่มขู่ทำร้ายเหยื่อหรือครอบครัว ว่าจะทำร้ายร่างกาย ลักพาตัว หรือฆ่าเหยื่อหรือคนในครอบครัว หากเหยื่อไม่โอนเงินให้

วิธีป้องกันตนเอง:

- ตั้งสติ ตรวจสอบ เมื่อได้รับการติดต่อจากบุคคลที่อ้างตัวเป็นเจ้าหน้าที่ โดยตรวจสอบให้แน่ใจก่อนเสมอว่าเป็นตัวจริง
- ไม่ให้ข้อมูลส่วนตัว เช่น หมายเลขบัตรประชาชน รหัสผ่านบัญชีธนาคาร
- ไม่โอนเงินให้กับบุคคลที่ไม่รู้จัก หรือไม่เคยติดต่อมาก่อน
- ติดต่อหน่วยงานที่เกี่ยวข้องโดยตรงเพื่อตรวจสอบ
- แจ้งความหากถูกหลอก หรือรู้ตัวว่าเปิดบัญชีม้า ซิมม้า หรือโทร 1441 เพื่อแจ้งความผ่านระบบแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ: www.thaipoliceonline.go.th

“โทรมาขู่ให้กลัว อาจเป็นมิจฉาชีพชัวร์ ให้รีบแจ้งความทันที”

App ดูดเงิน

“App ดูดเงิน” หมายถึง แอปพลิเคชันบนมือถือ ที่ถูกออกแบบมาเพื่อขโมยเงินหรือข้อมูลส่วนตัวจากผู้ใช้งาน โดยมักแฝงตัวมาในรูปแบบแอปพลิเคชันทั่วไป เมื่อผู้ใช้ติดตั้งและใช้งาน แอปจะเข้าถึงข้อมูลส่วนตัว เช่น ข้อมูลบัญชีธนาคาร รหัสผ่าน หรือข้อความ และทำธุรกรรมทางการเงินโดยไม่ได้รับอนุญาต ส่งผลให้ผู้ใช้สูญเสียเงินและข้อมูลส่วนตัว

มิจฉาชีพในปัจจุบันมีกลวิธีที่แยบยล ทันสมัย และพัฒนารูปแบบการหลอกลวงอยู่เสมอ แอปดูดเงิน จึงเป็นภัยคุกคามรูปแบบใหม่ ที่มิจฉาชีพใช้หลอกลวงผู้คน เพื่อขโมยเงินจากบัญชีธนาคาร

มิจฉาชีพใช้วิธีการใด?:

- อ้างว่าเป็นพนักงานธนาคาร หน่วยงานรัฐ หรือบริษัทต่าง ๆ แล้วหลอกให้เหยื่อติดตั้งแอปผ่าน SMS หรือโทรศัพท์
- หลอกให้เหยื่อดาวน์โหลดแอปดูดเงิน ที่ดูคล้ายแอปทั่วไปจาก Play Store หรือ App Store เช่น แอปแต่งรูป แอปดูดวง
- ทำแอปให้ดูคล้ายแอปทั่วไปที่ผู้ใช้คุ้นเคย เช่น แอปธนาคาร แอปช้อปปิ้งออนไลน์ หลอกให้เหยื่อใส่ข้อมูลส่วนตัว เช่น ชื่อผู้ใช้ รหัสผ่าน OTP
- เมื่อเหยื่อติดตั้งแอปดูดเงิน มิจฉาชีพจะสามารถดักจับข้อมูล ชื่อผู้ใช้ รหัสผ่าน OTP และควบคุมโทรศัพท์ของเหยื่อ เพื่อโอนเงินออกจากบัญชีธนาคาร

วิธีป้องกันตนเอง:

- ดาวน์โหลดแอปพลิเคชันจาก Play Store หรือ App Store เท่านั้น
- อัปเดตซอฟต์แวร์เครื่องและแอปธนาคารอยู่เสมอ
- ตั้งรหัสผ่านใช้งานเครื่อง ให้แตกต่างจากรหัสใช้งานของแอปธนาคาร
- ไม่ทำการสแกนใบหน้าหรือยืนยันตัวตนผ่านแอปที่ไม่รู้จัก
- แจ้งความหากถูกหลอก หรือรู้ตัวว่าเปิดบัญชีม้า ซิมม้า หรือโทร 1441 เพื่อแจ้งความผ่านระบบแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ: www.thaipoliceonline.go.th

“แอปดูดเงิน หลอกลวงผู้ใช้ ดักข้อมูลส่วนตัว และเงินออกจากบัญชี”

กสทช. NBTC

บทที่ 2
4 สัญญาณเตือน
รู้ตัวก่อนโดนหลอก

ในยุคดิจิทัลที่การสื่อสารรวดเร็ว มิจฉาชีพมีกลยุทธ์ใหม่ ๆ หลอกลวงผู้คนอยู่เสมอ สร้างความเสียหาย และความหวาดกลัวให้กับประชาชน บทความนี้จึงได้รวบรวม 4 สัญญาณเตือนสำคัญ ช่วยให้คุณรู้ตัวทันก่อนโดนหลอก

รีบร้อน กดดัน ให้ตัดสินใจเร็ว

มิจฉาชีพมักสร้างสถานการณ์ฉุกเฉิน กดดันให้เหยื่อรีบตัดสินใจโดยไม่มีเวลาไตร่ตรอง

ตัวอย่าง:

- “บัญชีของคุณถูกอายัดด่วน! รีบโอนเงินไปยังบัญชีนี้ก่อนถูกอายัดถาวร!”
- “ตำรวจกำลังออกหมายจับคุณ รีบโอนเงินมาประกันตัวด่วน!”
- “คุณสั่งสินค้าผิด รีบโอนเงินค่าสินค้ามาด่วน ไม่งั้นจะถูกดำเนินการตามกฎหมาย!”

วิธีป้องกัน:

- ตั้งสติ คิดวิเคราะห์ อย่ารีบร้อนตัดสินใจ
- วางสายก่อน และโทรกลับไปยังหน่วยงานที่ถูกอ้างถึงโดยตรงเพื่อยืนยันข้อมูล
- ตรวจสอบข้อมูลให้ละเอียด อย่าหลงเชื่อข้อมูลเพียงฝ่ายเดียว

ขอข้อมูลส่วนตัวสำคัญ

มิจฉาชีพมักพยายามขอข้อมูลส่วนตัวสำคัญ

ตัวอย่าง:

- “กรุณาแจ้งรหัส OTP ที่ได้รับทาง SMS เพื่อยืนยันตัวตน”
- “ขอทราบเลขบัตรประชาชนของคุณเพื่อตรวจสอบข้อมูลการโอนเงิน”
- “กรุณาแจ้งรหัส PIN บัตร ATM ของคุณเพื่อทำธุรกรรม”

วิธีป้องกัน:

- ห้ามบอกข้อมูลส่วนตัวสำคัญกับใครเด็ดขาด
- ธนาคารหรือหน่วยงานที่น่าเชื่อถือ จะไม่มีวันขอข้อมูลส่วนตัวสำคัญทางโทรศัพท์
- หากไม่แน่ใจ ให้วางสาย และติดต่อหน่วยงานนั้น ๆ โดยตรง

“รู้เท่าทันภัย!
สัญญาณเตือน
ก่อนโดนหลอก
สูญทรัพย์สิน”

เสนอผลตอบแทนสูงเกินจริง

มิจฉาชีพมักเสนอผลตอบแทนที่สูงเกินจริง ล่อให้เหยื่อหลงเชื่อ

ตัวอย่าง:

- “ลงทุนหลักพัน ได้กำไรหลักหมื่น!”
- “ขายมือถือรุ่นล่าสุด ราคาถูกกว่าท้องตลาดครึ่งต่อครึ่ง!”
- “สมัครสมาชิกวันนี้ รับฟรีทองคำแท่ง!”

วิธีป้องกัน:

- ตั้งสติ คิดก่อน ว่าผลตอบแทนที่เสนอมา เป็นไปได้หรือไม่
- เปรียบเทียบราคากับร้านค้าอื่น ๆ
- อย่าโลภ หลงเชื่อผลตอบแทนที่สูงเกินจริง

ใช้ช่องทางการติดต่อที่ไม่เป็นทางการ

มิจฉาชีพมักใช้ช่องทางการติดต่อที่ไม่เป็นทางการ เช่น โทรศัพท์มือถือส่วนตัว แชทส่วนตัว หรือโซเชียลมีเดีย

ตัวอย่าง:

- ติดต่อผ่านเบอร์ส่วนตัว ไม่ใช่เบอร์ที่ระบุไว้บนเว็บไซต์
- ส่งข้อความมาทางแชทส่วนตัวในโซเชียลมีเดีย
- แอดไลน์ส่วนตัว อ้างว่าเป็นตัวแทนจากหน่วยงานหรือบริษัท

วิธีป้องกัน:

- ติดต่อหน่วยงานหรือบริษัทผ่านช่องทางที่ระบุไว้บนเว็บไซต์อย่างเป็นทางการ
- ตรวจสอบข้อมูลการติดต่อให้ละเอียด
- เปรียบเทียบชื่อบัญชีธนาคารกับชื่อบริษัทหรือหน่วยงานที่ถูกอ้างถึง
- ตรวจสอบรีวิวจากลูกค้าจริง

บทที่ 3
8 วิธีปฏิบัติ
เมื่อตกเป็นเหยื่อมิจฉาชีพ

“โดนหลอกลวง?
อย่าเสียเวลา!
รีบแจ้งระงับบัญชี
และรีบแจ้งความ”

เมื่อท่านตกเป็นเหยื่อมิจฉาชีพ สิ่งสำคัญคือต้องตั้งสติเพื่อรีบอายัดบัญชี รวบรวมหลักฐาน แจ้งความ และดำเนินการตามขั้นตอน ดังต่อไปนี้

1. อายัดบัญชี

- แจ้งอายัดบัญชีของตัวเอง เพื่อระงับการโอนเงินออกจากบัญชีของคุณ
- แจ้งความประสงค์ขออายัดบัญชีของคนร้าย โทร 1441 หรือแจ้งความออนไลน์และประสานงานให้ธนาคาร (ทุกธนาคาร) อายัดบัญชีคนร้าย จากนั้นจะได้เลขคำขอแจ้งความออนไลน์และ Bank ID เพื่อไปแจ้งความที่สถานีตำรวจในท้องที่
- ตรวจสอบความผิดปกติของธุรกรรมที่เกิดขึ้นในบัญชีของคุณ
- เปลี่ยนรหัสผ่านบัญชีธนาคาร และบัญชีอื่น ๆ ที่เกี่ยวข้อง

2. รวบรวมหลักฐาน

- เก็บข้อความแชท อีเมล หรือบันทึกการสนทนาทางโทรศัพท์ที่เกี่ยวข้องกับการหลอกลวงไว้ให้ครบถ้วน หากเป็นไปได้ควรบันทึกหน้าจอหรือถ่ายภาพเก็บไว้
- เก็บใบเสร็จรับเงิน บิล หรือหลักฐานข้อมูลทางการเงินอื่น ๆ ที่แสดงธุรกรรมการเงินที่เกี่ยวข้องกับมิจฉาชีพ
- รวบรวมข้อมูลส่วนตัว สำเนาบัตรประชาชน สำเนาทะเบียนบ้านและเอกสารสำคัญอื่น ๆ ที่เกี่ยวข้อง
- เก็บหลักฐานอื่น ๆ ที่อาจเป็นประโยชน์ เช่น รูปภาพ วิดีโอ หรือข้อความที่โพสต์บนโซเชียลมีเดีย

3. แจ้งความที่สถานีตำรวจ

- รีบไปแจ้งความที่สถานีตำรวจท้องที่ เพื่อลงบันทึกประจำวันไว้เป็นหลักฐาน
- นำหลักฐานทั้งหมดที่รวบรวมไว้ ไปแสดงต่อเจ้าหน้าที่ตำรวจ
- ให้ข้อมูลเกี่ยวกับมิจฉาชีพเท่าที่จะทราบ เช่น เบอร์โทรศัพท์ ข้อความ รูปภาพ หรือข้อมูลอื่น ๆ ที่อาจเป็นประโยชน์ต่อการสืบสวน
- ขอใบแจ้งความเก็บไว้เป็นหลักฐาน สำหรับติดต่อหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

4. แจ้งหน่วยงานที่เกี่ยวข้อง

- แจ้งข้อมูลร้องเรียน เกี่ยวกับมิจฉาชีพและวิธีการหลอกลวง เพื่อให้หน่วยงานที่เกี่ยวข้องดำเนินการตรวจสอบ
- แจ้งสำนักงาน กสทช. เกี่ยวกับเบอร์ โทรศัพท์หรือข้อความ SMS ที่ใช้ในการหลอกลวง เพื่อดำเนินการตรวจสอบและดำเนินคดี

5. ป้องกันมิจฉาชีพติดต่อกลับ

- หากมิจฉาชีพทราบเบอร์โทรศัพท์ของคุณ ควรเปลี่ยนเบอร์โทรศัพท์
- ตั้งค่าความเป็นส่วนตัว ในโซเชียลมีเดียและแอปพลิเคชันต่าง ๆ เพื่อจำกัดการเข้าถึงข้อมูลส่วนตัวของคุณ
- ระวังการติดต่อจากบุคคลที่ไม่รู้จัก โดยเฉพาะทางโทรศัพท์ อีเมลหรือโซเชียลมีเดีย
- ตรวจสอบความน่าเชื่อถือของบุคคลที่ติดต่อมาก่อน ก่อนที่จะให้ข้อมูลส่วนตัวหรือทำธุรกรรมใด ๆ

6. ปรึกษาผู้เชี่ยวชาญ

- ปรึกษาทนายความ หากต้องการคำแนะนำทางกฎหมายเกี่ยวกับการดำเนินคดีกับมิจฉาชีพ
- มีหน่วยงานหลายแห่งที่ให้บริการปรึกษา และให้ความช่วยเหลือทางกฎหมายฟรี เช่น สำนักงานช่วยเหลือประชาชนทางกฎหมายของเนติบัณฑิตยสภา สภาทนายความ หรือมูลนิธิทนายความเพื่อสิทธิมนุษยชน

7. ดูแลสภาพจิตใจ

- การตกเป็นเหยื่อมิจฉาชีพ อาจส่งผลต่อสภาพจิตใจ ควรพักผ่อนให้เพียงพอ ทานอาหารที่มีประโยชน์ และออกกำลังกายสม่ำเสมอ
- พูดคุยกับผู้อื่น พูดคุยกับครอบครัว เพื่อน หรือผู้เชี่ยวชาญด้านสุขภาพจิต เพื่อระบายความรู้สึกและขอคำแนะนำ
- เข้าร่วมกลุ่มช่วยเหลือ สำหรับผู้ที่เคยตกเป็นเหยื่อมิจฉาชีพ ซึ่งสามารถแลกเปลี่ยนประสบการณ์ และให้กำลังใจซึ่งกันและกัน

8. แชร์ประสบการณ์

- แชร์ประสบการณ์ของคุณกับผู้อื่น เพื่อเป็นอุทาหรณ์และช่วยเตือนให้คนอื่นระวัง
- สอนวิธีป้องกันตนเองจากมิจฉาชีพให้กับครอบครัว เพื่อนและคนใกล้ชิด
- ช่วยกันร่วมรณรงค์ ให้สังคมตระหนักถึงภัยมิจฉาชีพ เพื่อป้องกันไม่ให้มีผู้ตกเป็นเหยื่อ

กสทช.
NBTC

บทที่ 4
ป้องกันตนเอง อย่างไร
จากภัยมิจฉาชีพ

“ปกป้องเงิน
ปกป้องข้อมูล
ป้องกันตัว
จากมิจฉาชีพ”

ในยุคดิจิทัลที่เต็มไปด้วยเทคโนโลยี มิจฉาชีพก็มีกลยุทธ์ใหม่ ๆ หลากหลายรูปแบบ เพื่อหลอกลวงและเอาเปรียบประชาชน บทความนี้จะแนะนำวิธีการป้องกันตัวจากภัยมิจฉาชีพ เพื่อให้คุณสามารถใช้ชีวิตในยุคดิจิทัลได้อย่างปลอดภัย

กลวิธีที่มิจฉาชีพใช้:

- สร้างสถานการณ์ฉุกเฉิน กดดันให้เหยื่อตัดสินใจเร็ว ๆ โดยไม่ทันตั้งตัว เช่น อ้างว่าบัญชีถูกอายัด ตำรวจออกหมายจับ หรือมีสินค้าส่งผิด
- สร้างความน่าเชื่อถือ อ้างชื่อหน่วยงาน หรือบุคคล ที่มีชื่อเสียง เช่น ธนาคาร ตำรวจ การไฟฟ้า สำนักงาน กสทช. หรือแม้แต่ญาติสนิท
- หลอกให้เหยื่อเชื่อว่ารู้ข้อมูลส่วนตัว เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ เลขบัตรประชาชนหรือข้อมูลบัญชีธนาคาร
- สร้างความกลัว ข่มขู่ คุกคาม ว่าจะดำเนินคดี หรือทำให้เกิดความเสียหาย
- เล่นกับความโลภ เสนอผลตอบแทนสูง ๆ หรือโปรโมชันพิเศษที่น่าดึงดูดใจ

วิธีป้องกันตัว:

- ตั้งสติ คิดวิเคราะห์ อย่ารีบร้อนตัดสินใจ หากได้รับสายที่น่าสงสัย ให้วางสายก่อน และตั้งสติวิเคราะห์สถานการณ์
- ตรวจสอบข้อมูลด้วยการโทรหาหน่วยงานที่ถูกอ้างถึงโดยตรง เพื่อยืนยันข้อมูล อย่าเชื่อข้อมูลเพียงฝ่ายเดียว
- ไม่ให้ข้อมูลส่วนตัวเด็ดขาด โดยเฉพาะข้อมูลสำคัญ เช่น รหัสผ่าน OTP เลขบัตรประชาชน ข้อมูลบัญชีธนาคาร ข้อมูลเหล่านี้เป็นข้อมูลลับ ห้ามบอกใครเด็ดขาด
- ไม่กดลิงก์จากแหล่งที่มาที่ไม่น่าเชื่อถือ หมั่นตรวจสอบ URL ของเว็บไซต์ก่อนกดทุกครั้ง
- วางสาย หากไม่มั่นใจ ให้วางสายทันที และโทรหาหน่วยงานที่เกี่ยวข้องเพื่อขอคำแนะนำ
- โทร 1441 แจ้งความออนไลน์ หากถูกหลอก ให้รีบแจ้งความทันที เพื่ออายัดบัญชีคนร้าย และติดต่อธนาคาร เพื่อระงับบัญชีตัวเอง

บทที่ 5
ช่องทางการติดต่อ
เพื่อขอความช่วยเหลือ

เมื่อท่านตกเป็นเหยื่อมิจฉาชีพ สิ่งสำคัญคือต้องรีบแจ้งความและขอความช่วยเหลือโดยเร็วที่สุด เนื้อหาส่วนนี้รวบรวมช่องทางการติดต่อหน่วยงานที่เกี่ยวข้อง เพื่อให้ท่านสามารถเข้าถึงความช่วยเหลือได้อย่างสะดวกและรวดเร็ว

ช่องทางการติดต่อเพื่อขอความช่วยเหลือ:

- สายด่วนตำรวจไซเบอร์ 1441 แจ้งความออนไลน์ เพื่อแจ้งระงับ-อายัดบัญชีคนร้ายได้ ตลอด 24 ชั่วโมง หรือแจ้งความออนไลน์ผ่านเว็บไซต์ thaipoliceonline.go.th
- สายด่วน ปปง. 1710 ยื่นคำร้องขอคุ้มครองสิทธิผู้เสียหายหลายรายคดี สำนักงานป้องกันและปราบปรามการฟอกเงิน หรือเว็บไซต์สำนักงาน ปปง. www.amlo.go.th
- สายด่วน สำนักงาน กสทช. 1200 แจ้งเบาะแสเบอร์โทรศัพท์มิจฉาชีพ
- เว็บไซต์กรมคุ้มครองผู้บริโภค https://www.ocpb.go.th สำนักงานคณะกรรมการคุ้มครองผู้บริโภค รับเรื่องร้องทุกข์
- เว็บไซต์มูลนิธิเพื่อผู้บริโภค www.consumerthai.org รับเรื่องร้องเรียน

จำไว้ว่า มิจฉาชีพมีกลโกงหลากหลายรูปแบบ ต้องหมั่นศึกษาข้อมูลข่าวสาร และตั้งสติก่อนทำธุรกรรมใด ๆ ร่วมด้วยช่วยกันปราบปรามมิจฉาชีพ ตลอดจน ต้องแลกเปลี่ยนเรียนรู้กลโกงมิจฉาชีพทางโทรศัพท์อย่างสม่ำเสมอ เพื่อทำให้ตนเองและคนรอบตัวปลอดภัย

“ถ้าโดนหลอกลวง
ให้รีบติดต่อ
ขอความช่วยเหลือ”

กสทช. NBTC

บทที่ 6
กฎหมายที่เกี่ยวข้อง
กับมิจฉาชีพทางโทรศัพท์

"รู้ไว้ป้องกัน
กฎหมายที่จัดการ
มิจฉาชีพ
ทางโทรศัพท์"

มิจฉาชีพทางโทรศัพท์เป็นภัยร้ายแรงที่สร้างความเสียหายทั้งต่อทรัพย์สินและจิตใจ ปัจจุบันมีกฎหมายหลายฉบับที่เกี่ยวข้องกับมิจฉาชีพ เนื้อหาส่วนนี้จะแนะนำกฎหมายที่สำคัญ เพื่อให้ประชาชนสามารถเข้าใจและรู้เท่าทันกลโกงของมิจฉาชีพ และสามารถดำเนินการทางกฎหมายเพื่อเอาผิดผู้กระทำความผิดได้

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

- มาตรา 9 ผู้ใดเปิดหรือยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของตน โดยมิได้มีเจตนาใช้เพื่อตนหรือเพื่อกิจการที่ตนเกี่ยวข้อง หรือยินยอมให้บุคคลอื่นใช้หรือยืมใช้เลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ของตน ทั้งนี้ โดยประการที่รู้หรือควรรู้ว่าจะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ
- มาตรา 10 ผู้ใดเป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อขาย ให้เช่า หรือให้ยืม บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ เพื่อใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุก ตั้งแต่ 2 ปี ถึง 5 ปี หรือปรับตั้งแต่ 200,000 บาท ถึง 500,000 บาท หรือทั้งจำทั้งปรับ
- มาตรา 11 ผู้ใดเป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อหรือขายเลขหมายโทรศัพท์ สำหรับบริการโทรศัพท์เคลื่อนที่ ซึ่งลงทะเบียนผู้ใช้บริการในนามของบุคคลหนึ่งบุคคลใดแล้ว แต่ไม่สามารถระบุตัวผู้ใช้บริการได้ ต้องระวางโทษจำคุกตั้งแต่ 2 ปี ถึง 5 ปี หรือปรับตั้งแต่ 200,000 บาท ถึง 500,000 บาท หรือทั้งจำทั้งปรับ

กฎหมายอื่น ๆ ที่เกี่ยวข้อง ตามรูปแบบการกระทำความผิดที่เฉพาะเจาะจงและเอาผิดผู้กระทำความผิด

- ประมวลกฎหมายอาญา เช่น ความผิดฐานกรรโชก รีดเอาทรัพย์ ชิงทรัพย์และปล้นทรัพย์ (มาตรา 337) ความผิดฐานฉ้อโกง (มาตรา 341)
- พระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2562 ความผิดเกี่ยวกับคอมพิวเตอร์ (มาตรา 8)

บทที่ 7
แนะนำช่องทาง
ตรวจสอบข้อมูล มิตร หรือ มิจ(ฉาชีพ)

“รู้ทันกลโกง!
ตรวจสอบให้แน่ชัด
ว่าเป็นมิตร
หรือ มิจ(ฉาชีพ)”

การตรวจสอบความถูกต้องของข้อมูลก่อนเชื่อถือหรือส่งต่อเป็นสิ่งสำคัญอย่างยิ่ง เพื่อป้องกันการแพร่ระบาดของข่าวปลอมและมิจฉาชีพทางโทรศัพท์ สำนักงาน กสทช. จึงขอแนะนำแนวทางการสืบค้นข้อมูลและช่องทางการตรวจสอบข้อมูลที่น่าเชื่อถือ เพื่อช่วยให้ประชาชนสามารถแยกแยะได้ว่าข้อมูลที่ได้รับนั้นมาจากแหล่งที่น่าเชื่อถือจริงหรือไม่

ช่องทางและแหล่งข้อมูลภาครัฐ::

- สำนักงานตำรวจแห่งชาติ www.royalthaipolice.go.th
- กองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี www.cib.go.th
- สำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.) www.ocpb.go.th
- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม www.mdes.go.th
- ศูนย์ชัวร์ก่อนแชร์ www.antifakenewscenter.com
- สำนักงาน กสทช. www.nbtc.go.th

ช่องทางภาคธนาคารและค่ายมือถือ:

- เว็บไซต์ธนาคารที่ใช้บริการอยู่ เช่น ธนาคารกรุงเทพ ธนาคารกสิกรไทย ธนาคารกรุงไทย ธนาคารทหารไทยธนชาต ธนาคารไทยพาณิชย์ ธนาคารกรุงศรีอยุธยา ธนาคารเกียรตินาคินภัทร ธนาคารออมสิน
- เอไอเอส www.ais.th
- ดีแทค www.dtac.co.th
- ทรู www.true.th

ช่องอื่น ๆ

- มูลนิธิเพื่อผู้บริโภค www.consumerthai.org
- สำนักงานป้องกันและปราบปรามการฟอกเงิน www.amlo.go.th
- แอปพลิเคชั่นที่ช่วยในการเช็คเบอร์มิจฉาชีพ บล็อกเบอร์ SMS โฆษณาพนันออนไลน์ เช่น
  - WhosCall (Android และ iOS)
  - TrueCaller (Android และ iOS)
  - Mr. Number (Android และ iOS)
  - Call Control (Android และ iOS) หรือ
  - Hiya (Android และ iOS)

บทที่ 8
สถิติ กลลวง

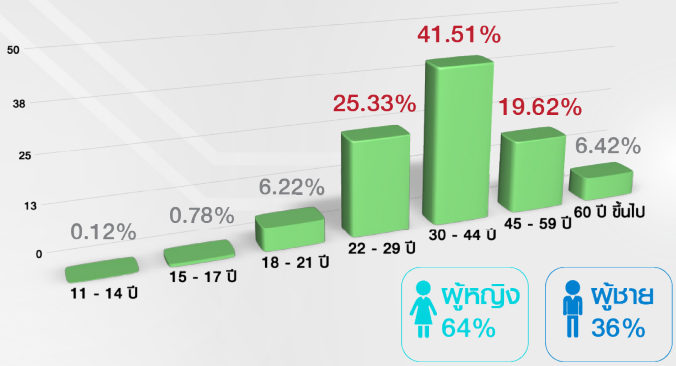
แบบไหนที่คนไทย โดนหลอกมากที่สุด

การรู้เท่าทันกลโกงของมิจฉาชีพ นับเป็นสิ่งสำคัญอย่างยิ่ง สำหรับใช้ป้องกันข้อมูลส่วนตัวและทรัพย์สิน ข้อมูลและสถิติเกี่ยวกับรูปแบบการหลอกลวงที่คนไทยโดนหลอกมากที่สุด จึงสามารถทำให้ประชาชนเข้าใจกลวิธีของมิจฉาชีพและเตรียมพร้อมรับมือกับภัยร้ายเหล่านี้ได้อย่างมีประสิทธิภาพ

อ้างอิงจากข้อมูล โดยสำนักงานตำรวจแห่งชาติ รายงานว่าตั้งแต่ 1 มี.ค.2565 - 30 มิ.ย.2567 เกิดคดีอาชญากรรมทางเทคโนโลยีแล้วกว่า 575,507 เรื่อง มูลค่าความเสียหายรวมกว่า 65,715 ล้านบาท เฉลี่ยความเสียหายวันละกว่า 80 ล้านบาท โดยคดีออนไลน์ที่มีการแจ้งความมากที่สุด 10 อันดับแรก คือ

อันดับ 1 หลอกลวงซื้อขายสินค้าหรือบริการไม่เป็นขบวนการ
181,565 เรื่อง ความเสียหาย 2,605,660,173 บาท
อันดับ 2 หลอกให้โอนเงินเพื่อทำงาน
55,624 เรื่อง ความเสียหาย 6,996,292,003 บาท
อันดับ 3 หลอกให้กู้เงิน
47,422 เรื่อง ความเสียหาย 2,156,248,393 บาท
อันดับ 4 หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์
36,318 เรื่อง ความเสียหาย 20,001,574,842 บาท
อันดับ 5 ข่มขู่ทางโทรศัพท์ (Call Center)
29,741 เรื่อง ความเสียหาย 7,546,200,539 บาท
อันดับ 6 หลอกเป็นบุคคลอื่นเพื่อยืมเงิน
17,248 เรื่อง ความเสียหาย 514,577,052 บาท
อันดับ 7 หลอกให้ติดตั้งโปรแกรมควบคุมระบบ
13,796 เรื่อง ความเสียหาย 1,931,459,338 บาท
อันดับ 8 หลอกให้โอนเงินเพื่อรับรางวัล
13,392 เรื่อง ความเสียหาย 1,125,954,045 บาท
อันดับ 9 หลอกลวงซื้อขายสินค้าหรือบริการเป็นขบวนการ
8,549 เรื่อง ความเสียหาย 69,985,581 บาท
อันดับ 10 กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์
4,130 เรื่อง ความเสียหาย 979,326,633 บาท

จากสถิติดังกล่าวยังพบอีกว่า **ผู้เสียหายส่วนใหญ่อยู่ในวัยทำงาน (อายุ 30 - 44 ปี)** โดยจำแนกรายละเอียดตามกลุ่มอายุดังต่อไปนี้



อ้างอิง: สถิติประเภทคดี จากการแจ้งความออนไลน์ ตั้งแต่ 1 มี.ค.2565 - 30 มิ.ย.2567 โดยสำนักงานตำรวจแห่งชาติ

"คนไทยสูญเงินรวมกว่า 5.9 หมื่นล้านบาท และถูกหลอกจากการซื้อขายสินค้าหรือบริการมากที่สุด"

รวบรวม
สายด่วนแจ้งเหตุ
เกี่ยวกับมิจฉาชีพทางโทรศัพท์

ข้อมูลอ้างอิง ณ วันที่ 31 กรกฎาคม 2567

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
87 ถนนพหลโยธิน ซอย 8 แขวงสามเสนใน เขตพญาไท กรุงเทพฯ 10400 โทร : 0 2670 8888
Call Center 1200 (โทรฟรี) E-mail : 1200@nbtc.go.th