หน่วยการเรียนรู้ที่ 5
ภัยทางการเงิน

สาระสำคัญ

รูปแบบการดำรงชีวิตและเทคโนโลยีที่เปลี่ยนแปลงไป ทำให้มิจฉาชีพพัฒนาสารพัดกลโกงเพื่อหลอกขโมยเงินจากเหยื่อ โดยมักจับจุดอ่อนของเหยื่อ คือ ความกลัว ความโลภ และความไม่รู้มาเป็นตัวช่วย ผู้ใช้บริการทางการเงินจึงจำเป็นต้องรู้เท่าตามทันกลโกงของมิจฉาชีพ ไม่ว่าจะเป็นกลโกงที่มาในรูปแบบของการเงินนอกระบบที่มีทั้งหนี้นอกระบบและแชร์ลูกโซ่ ภัยใกล้ตัว ภัยออนไลน์ และภัยที่แฝงมากับบัตรอิเล็กทรอนิกส์ต่าง ๆ เพื่อให้สามารถป้องกันตนเองจากภัยเหล่านี้ได้ รวมไปถึงรู้จักหน่วยงานหรือองค์กรที่ให้คำปรึกษาหากตกเป็นเหยื่อภัยทางการเงิน

ตัวชี้วัด

1. บอกประเภทและลักษณะของภัยทางการเงิน และยกตัวอย่างภัยทางการเงินที่มีในชุมชน
2. บอกวิธีการป้องกันตนเองจากภัยทางการเงิน
3. บอกวิธีแก้ปัญหาที่เกิดจากภัยทางการเงิน

ขอบข่ายเนื้อหา

เรื่องที่ 1 หนี้นอกระบบ
เรื่องที่ 2 แชร์ลูกโซ่
เรื่องที่ 3 ภัยใกล้ตัว
เรื่องที่ 4 ภัยออนไลน์
เรื่องที่ 5 ภัยธนาคารออนไลน์
เรื่องที่ 6 ภัยบัตรอิเล็กทรอนิกส์

เวลาที่ใช้ในการศึกษา 20 ชั่วโมง

สื่อการเรียนรู้

1. ชุดวิชาการเงินเพื่อชีวิต 3
2. หนังสือรู้รอบเรื่องการเงินของศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ตอน รู้รอบระวังภัย
3. เว็บไซต์ www.1213.or.th เฟซบุ๊ก www.facebook.com/hotline1213

เรื่องที่ 1 หนี้นอกระบบ

เมื่อจำเป็นต้องใช้เงิน แต่ไม่สามารถขอกู้เงินจากสถาบันการเงินได้ หลายคนคงนึกถึงการกู้เงินนอกระบบที่ได้เงินเร็ว ไม่ยุ่งยาก ไม่ต้องมีหลักประกันหรือใช้บุคคลค้ำประกัน จนอาจลืมนึกถึงเล่ห์เหลี่ยมหรือกลโกงที่อาจแฝงมากับการกู้เงินนอกระบบ

ลักษณะกลโกงหนี้นอกระบบ

1. ใช้ตัวเลขน้อย ๆ เพื่อจูงใจ

นายทุนเงินกู้นอกระบบมักบอกตัวเลขน้อยเพื่อจูงใจผู้กู้ ไม่ว่าจะเป็นจำนวนเงินผ่อนต่องวดหรือดอกเบี้ย เช่น กู้เงิน 10,000 บาท ให้ผ่อนวันละ 150 บาทเป็นระยะเวลา 90 วัน แต่เมื่อคำนวณแล้วต้องจ่ายหนี้คืน 13,500 บาทภายใน 3 เดือน ดอกเบี้ยสูงถึง 35% ต่อสามเดือนหรือ 140% ต่อปี

เจ้าหนี้บางรายก็บอกแค่อัตราดอกเบี้ย แต่ไม่ได้บอกว่าเป็นอัตราดอกเบี้ยต่อวัน ต่อเดือน หรือต่อปี เช่น เจ้าหนี้รายหนึ่งปล่อยเงินกู้ 3% ลูกหนี้เห็นว่าอัตราดอกเบี้ยน้อยกว่าสถาบันการเงินก็แห่ไปกู้เงิน แต่เมื่อคำนวณดอกเบี้ยทั้งปีแล้ว ลูกหนี้ก็ตกใจ เพราะดอกเบี้ย 3% นั้นเป็นดอกเบี้ยต่อวัน ถ้าคิดเป็นต่อปี ก็สูงถึง 1,080%

2. ให้เซ็นเอกสารที่ไม่ได้กรอกตัวเลข

นอกจากจะใช้ตัวเลขค่างวดหรือดอกเบี้ยน้อย ๆ ดึงดูดลูกหนี้แล้ว เจ้าหนี้บางรายก็ให้ลูกหนี้เซ็นสัญญากู้ยืมโดยที่ยังไม่ได้กรอกตัวเลข ลูกหนี้รายหนึ่งต้องใช้เงินคืนเจ้าหนี้ 100,000 บาท ทั้ง ๆ ที่กู้เงินมาแค่ 20,000 บาท เพียงเพราะไปเซ็นสัญญาในเอกสารที่ยังไม่ได้กรอกจำนวนเงินกู้

3. ไม่ให้ลูกหนี้อ่านเอกสารที่ต้องเซ็น

เจ้าหนี้บางรายไม่ยอมให้ลูกหนี้อ่านเอกสารที่จะต้องเซ็น เช่น เจ้าหนี้หวังจะยึดเอาที่ดินของลูกหนี้ที่นำมาค้ำประกันเงินกู้ จึงหลอกว่าเป็นการทำสัญญาจำนอง แต่แท้จริงเป็นสัญญาขายฝาก

4. บีบให้เซ็นสัญญาเงินกู้เกินจริง

เจ้าหนี้บางรายบีบบังคับให้ลูกหนี้เซ็นสัญญาเงินกู้เกินจริง เช่น ขอกู้ 10,000 บาท แต่บังคับให้เซ็นในเอกสารที่เขียนว่าขอกู้ 30,000 บาท ลูกหนี้บางรายมีความจำเป็นต้องใช้เงิน ก็จำใจเซ็นสัญญานั้น

5. ทำสัญญาขายฝากแทนสัญญาจำนอง

เจ้าหนี้หลายรายหลอกลูกหนี้ให้ทำสัญญาขายฝากแทนสัญญาจำนอง ถึงแม้เจ้าหนี้จะอ้างว่าเป็นการค้ำประกันเงินกู้เหมือนกัน แต่การบังคับหลักประกันต่างกัน สัญญาขายฝากจะทำให้กรรมสิทธิ์ของบ้านหรือที่ดินนั้นตกเป็นของเจ้าหนี้ตั้งแต่วันที่ทำสัญญา ซึ่งลูกหนี้จะต้องไถ่บ้านหรือที่ดินคืนภายในเวลาที่กำหนด หากช้าเพียงวันเดียว บ้านหรือที่ดินนั้นก็จะตกเป็นของเจ้าหนี้ทันที โดยเจ้าหนี้ไม่ต้องมีหนังสือแจ้งหรือฟ้องศาลเพื่อบังคับคดี

ด้วยเหตุนี้เจ้าหนี้นอกระบบบางคนจึงบ่ายเบี่ยง หลบหน้าลูกหนี้เพื่อไม่ให้มีโอกาสได้ไถ่ถอนบ้านหรือที่ดินนั้นคืนในเวลาที่กำหนด หรือไม่ยอมขยายเวลาไถ่ให้ (การขยายเวลาไถ่ ต้องทำหลักฐานเป็นหนังสือพร้อมลงลายมือชื่อ) โดยเฉพาะบ้านหรือที่ดินที่อยู่ในทำเลดีและมีมูลค่ามากกว่ายอดหนี้

6. หลีกเลี่ยงให้กู้โดยตรง

หลายครั้งที่สัญญาอำพรางเงินกู้ถูกนำมาใช้เพื่อหลอกล่อผู้ที่เดือดร้อนเรื่องเงิน เช่น ลูกหนี้รายหนึ่งติดต่อขอกู้เงินกับเจ้าหนี้นอกระบบจำนวน 20,000 บาท เจ้าหนี้บังคับให้ลูกหนี้ใช้บัตรผ่อนสินค้าหรือบัตรเครดิตซื้อสินค้าที่กำลังเป็นที่นิยมมูลค่า 23,000 บาทเพื่อมาแลกกับเงินกู้ 20,000 บาท

ลูกหนี้ได้เงินมาแค่ 20,000 บาท แต่กลับต้องแบกภาระเงินกู้สูงถึง 23,000 บาทกับบริษัทบัตรผ่อนสินค้าหรือบริษัทบัตรเครดิต และยังมีภาระดอกเบี้ยที่ต้องจ่ายอีกต่างหาก ส่วนเจ้าหนี้แทบจะไม่มีความเสี่ยงใดเลย แถมยังได้สินค้าในราคาถูกอีกด้วย

7. ทวงหนี้โหด

นอกจากภาระดอกเบี้ยที่แสนแพงแล้ว ลูกหนี้เงินกู้นอกระบบอาจต้องเจอกับการทวงหนี้โหดหากไม่ชำระตรงตามเวลา ซึ่งเจ้าหนี้อาจไม่ได้แค่ขู่หรือประจานให้ได้อาย แต่บางรายก็ถึงขั้นทำร้ายร่างกาย

วิธีป้องกันภัยหนี้นอกระบบ

1. หยุดใช้เงินเกินตัว – ตรวจสอบพฤติกรรมการใช้เงินของตนเองโดยการจดบันทึกรายรับ-รายจ่าย แล้ววางแผนใช้เงินอย่างเหมาะสมกับรายได้และความจำเป็น

2. วางแผนการเงินล่วงหน้า – คำนึงถึงค่าใช้จ่ายก้อนใหญ่ที่อาจเกิดขึ้นในอนาคต เช่น ค่าเล่าเรียนลูก แล้ววางแผนทยอยออมล่วงหน้า รวมถึงออมเงินเผื่อเหตุการณ์ฉุกเฉินด้วย

3. **คิดให้ดีก่อนตัดสินใจก่อหนี้** – ทบทวนดูความจำเป็นว่าต้องใช้เงินจริง ๆ หรือไม่ และหากต้องกู้จริง ๆ จะสามารถชำระหนี้ได้หรือไม่ เพราะนอกจากดอกเบี้ยที่แสนแพงแล้ว อาจต้องเจอกับเหตุการณ์ทวงหนี้แบบโหด ๆ อีกด้วย

4. **เลือกกู้ในระบบ** – หากจำเป็นต้องกู้ ควรเลือกกู้ในระบบดีกว่า เพราะนอกจากจะมีหน่วยงานภาครัฐคอยดูแลแล้ว ยังระบุดอกเบี้ยในสัญญาชัดเจนและเป็นธรรมกว่า

5. **ศึกษารายละเอียดผู้ให้กู้** – ดูว่าผู้ให้กู้นั้นน่าเชื่อถือหรือไม่ มีเงื่อนไขชำระเงินหรืออัตราดอกเบี้ยที่เอาเปรียบผู้กู้เกินไปหรือไม่

6. **ศึกษาวิธีคิดดอกเบี้ย** – หนี้นอกระบบมักคิดอัตราดอกเบี้ยด้วยวิธีเงินต้นคงที่ (flat rate) ซึ่งทำให้ลูกหนี้ต้องจ่ายดอกเบี้ยมากกว่าการคิดดอกเบี้ยแบบลดต้นลดดอก (effective rate) เพราะดอกเบี้ยจะถูกคิดจากเงินต้นทั้งก้อนแม้ว่าจะทยอยจ่ายคืนทุกเดือนก็ตาม

7. **หากจำเป็นต้องกู้เงินนอกระบบต้องใส่ใจ**
   - ไม่เซ็นสัญญาในเอกสารที่ยังไม่ได้กรอกข้อความหรือวงเงินกู้ไม่ตรงกับความจริง
   - ตรวจสอบข้อความในสัญญาเงินกู้ รวมถึงดูว่าเป็นเงื่อนไขที่เราทำได้จริง ๆ
   - เก็บสัญญาคู่ฉบับไว้กับตัวเพื่อเป็นหลักฐานการกู้
   - ทำสัญญาจำนองแทนการทำสัญญาขายฝาก เพราะการขายฝากจะทำให้กรรมสิทธิ์ตกเป็นของเจ้าหนี้ทันทีหากผู้กู้ไม่มาไถ่คืนตามกำหนด

8. **ติดตามข่าวสารกลโกงเป็นประจำ**

ทำอย่างไรเมื่อตกเป็นเหยื่อหนี้นอกระบบ

หากเป็นเหยื่อหนี้นอกระบบแล้ว ผู้กู้ควรหาแหล่งเงินกู้ในระบบที่มีดอกเบี้ยถูกกว่ามาชำระคืน แต่หากไม่สามารถกู้ยืมในระบบได้ ผู้กู้อาจต้องยอมขายทรัพย์สินบางส่วนเพื่อนำมาชำระหนี้ เพื่อแก้ไขปัญหาดอกเบี้ยที่เพิ่มขึ้นจนไม่สามารถชำระคืนได้ ทั้งนี้ ลูกหนี้เงินกู้นอกระบบสามารถขอรับคำปรึกษาได้จากองค์กรดังต่อไปนี้

1. **ศูนย์รับแจ้งการเงินนอกระบบ** กระทรวงการคลัง โทร. 1359
2. **กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับการคุ้มครองผู้บริโภค** สำนักงานตำรวจแห่งชาติ โทร. 1135
3. **สายด่วนรัฐบาล** สำนักนายกรัฐมนตรี โทร. 1111

4. **สำนักงานคุ้มครองสิทธิและช่วยเหลือทางกฎหมายแก่ประชาชน** สำนักอัยการสูงสุด โทร. 0 2142 2034

5. **ศูนย์ช่วยเหลือลูกหนี้และประชาชนที่ไม่ได้รับความเป็นธรรม** กระทรวงยุติธรรม โทร. 0 2575 3344

6. **ศูนย์ดำรงธรรม** กระทรวงมหาดไทย โทร. 1567

7. **หน่วยงานที่รับเรื่องร้องเรียนเกี่ยวกับการทวงถามหนี้ไม่เหมาะสม** ได้แก่ กรมการปกครอง สำนักงานเศรษฐกิจการคลัง ที่ทำการปกครองจังหวัด กองบัญชาการตำรวจนครบาล สถานีตำรวจท้องที่ และที่ว่าการอำเภอทุกแห่ง

กิจกรรมท้ายเรื่องที่ 1 หนี้นอกระบบ

(ให้ผู้เรียนไปทำกิจกรรมท้ายเรื่องที่ 1 ที่สมุดบันทึกกิจกรรมการเรียนรู้)

เรื่องที่ 2 แชร์ลูกโซ่

แชร์ลูกโซ่เป็นภัยทางการเงินที่อาจสร้างความเสียหายได้ตั้งแต่เงินจำนวนน้อย ๆ จนไปถึงเงินหลักแสนหลักล้าน มิจฉาชีพมักใช้ “โอกาสรวย” หรือ “สินค้าราคาถูกมาก” มาหลอกล่อให้เหยื่อร่วมลงทุนหรือซื้อสินค้าแล้วเชิดเงินหนีไป

ลักษณะกลโกงแชร์ลูกโซ่

1. แชร์ลูกโซ่ในคราบธุรกิจขายตรง

มิจฉาชีพจะโฆษณาชวนเชื่อให้เหยื่อทำธุรกิจขายตรงที่มีผลตอบแทนสูง โดยที่เหยื่อไม่ต้องทำอะไร เพียงแค่ชักชวนเพื่อนหรือญาติพี่น้องให้ร่วมทำธุรกิจ ไม่เน้นการขายสาธิต หรือทำให้สมาชิกเข้าใจในตัวสินค้า เมื่อเหยื่อเริ่มสนใจ จะให้เหยื่อเข้าร่วมฟังสัมมนา และโน้มน้าวหรือหลอกล่อให้เหยื่อจ่ายค่าสมัครสมาชิก หรือซื้อสินค้าแรกเข้าซึ่งมีมูลค่าที่ค่อนข้างสูง (สินค้าส่วนมากมักไม่มีคุณภาพ) หรืออาจให้เหยื่อซื้อหุ้นหรือหน่วยลงทุนโดยไม่ต้องรับสินค้าไปขาย แล้วก็รอรับเงินปันผลได้เลย

ค่าสมัครสมาชิก ค่าซื้อสินค้าแรกเข้า ค่าหุ้นหรือค่าหน่วยลงทุนของสมาชิกใหม่จะถูกนำมาจ่ายเป็นผลตอบแทนให้กับสมาชิกเก่า เมื่อไหร่ที่ไม่สามารถหาสมาชิกใหม่ได้ แชร์ก็จะล้มเพราะไม่สามารถหาเงินมาจ่ายผลตอบแทนและเงินที่ลงทุนคืนสมาชิกได้

ปัจจุบันยังมีการโฆษณาชักชวนผู้ลงทุนผ่านอินเทอร์เน็ตอีกด้วย โดยมิจฉาชีพจะหลอกให้เหยื่อกรอกข้อมูลส่วนตัวในอินเทอร์เน็ต แล้วติดต่อเหยื่อเพื่อชักชวนให้เข้าร่วมงานสัมมนาโดยอ้างว่ามีบุคคลที่มีชื่อเสียงเข้าร่วมด้วย

2. แชร์ลูกโซ่หลอกลงทุน

มิจฉาชีพมักอ้างว่ามีสิทธิพิเศษ หรือได้โควตาซื้อสินค้าราคาถูกเป็นจำนวนมาก หรือมีการลงทุนที่ให้ผลตอบแทนสูงและแน่นอน จึงอยากชักชวนให้เหยื่อลงทุนร่วมกัน เช่น โควตาจำหน่ายสลากกินแบ่งรัฐบาล (แชร์ลอตเตอรี่) อุตสาหกรรมปลูกป่าเพื่อส่งขายตลาดในต่างประเทศ (แชร์ไม้) เก็งกำไรจากอัตราแลกเปลี่ยน (แชร์ FOREX) โดยสร้างเว็บไซต์เพื่อให้ดูน่าเชื่อถือ หรือบางรายก็อ้างว่ามีสาขาในต่างประเทศ แต่ความจริงแล้ว ไม่ได้ทำธุรกิจดังกล่าวจริง

มิจฉาชีพจะใช้วิธีหมุนเงินจากผู้ลงทุนรายใหม่ไปจ่ายเป็นผลตอบแทนให้แก่ผู้ลงทุนรายเก่า จึงต้องพยายามหาผู้ลงทุนรายใหม่อยู่เรื่อย ๆ เพื่อให้มีเงินไปจ่ายเป็นผลตอบแทน แต่หากไม่สามารถหาผู้ลงทุนรายใหม่ได้ ก็จะไม่สามารถจ่ายผลตอบแทนคืนให้แก่รายเก่าได้

3. แชร์ลูกโซ่หลอกขายสินค้าผ่านอินเทอร์เน็ต

มิจฉาชีพจะแฝงตัวเป็นพ่อค้าหรือแม่ค้า แล้วอ้างว่าสามารถหาสินค้าหายากหรือสินค้าที่กำลังอยู่ในความต้องการของตลาด (เช่น สินค้ารุ่นใหม่ล่าสุด หรือยังไม่มีขายในประเทศไทย) ได้ในราคาถูก จึงประกาศขายสินค้าดังกล่าวในราคาที่ถูกกว่าท้องตลาดเป็นจำนวนมากผ่านทางอินเทอร์เน็ต

เมื่อเหยื่อหลงเชื่อสั่งซื้อสินค้าและโอนเงินให้แก่มิจฉาชีพในครั้งแรก มิจฉาชีพจะส่งสินค้าให้เหยื่อตามจำนวนที่สั่งซื้อ และเมื่อเหยื่อได้สินค้าในราคาถูก ก็จะบอกต่อชักชวนญาติพี่น้องหรือเพื่อนฝูงให้มาซื้อสินค้าเป็นจำนวนมากแล้วโอนเงินค่าสินค้าทั้งหมดให้แก่มิจฉาชีพ หลังจากนั้นมิจฉาชีพก็จะเชิดเงินนั้นหนีไปโดยไม่ส่งสินค้าใด ๆ ให้แก่เหยื่อเลย

วิธีป้องกันภัยแชร์ลูกโซ่

1. ไม่โลภไปกับผลตอบแทนหรือสินค้าราคาถูกที่นำมาหลอกล่อ เพราะผลตอบแทนยิ่งสูง ยิ่งมีความเสี่ยงมากที่จะเป็นแชร์ลูกโซ่

2. ไม่กรอกข้อมูล หรือให้ข้อมูลส่วนตัวในเว็บไซต์ หรือตอบกลับอีเมลที่ไม่น่าเชื่อถือ เพราะอาจกลายเป็นเหยื่อแชร์ลูกโซ่

3. หลีกเลี่ยงการเข้าร่วมกิจกรรมกับกลุ่มธุรกิจที่ไม่แน่ใจ เพราะอาจถูกหว่านล้อมให้ร่วมลงทุนในธุรกิจแชร์ลูกโซ่

4. อย่าเกรงใจจนไม่กล้าปฏิเสธ เมื่อมีคนชักชวนทำธุรกิจที่มีลักษณะคล้ายแชร์ลูกโซ่ เพราะอาจทำให้สูญเสียเงินได้

5. ศึกษาที่มาที่ไปของการลงทุนหรือสินค้าให้ดีก่อนการลงทุน โดยเฉพาะธุรกิจหรือสินค้าที่ให้ผลตอบแทนสูงมากในเวลาอันสั้น หรือมีราคาถูกผิดปกติ

6. ติดตามข่าวสารกลโกงเป็นประจำ

ทำอย่างไรเมื่อตกเป็นเหยื่อแชร์ลูกโซ่

หากตกเป็นเหยื่อแชร์ลูกโซ่ ควรรวบรวมเอกสารที่เกี่ยวข้องทั้งหมด แล้วติดต่อขอรับคำปรึกษาได้ที่

ส่วนป้องปรามการเงินนอกระบบ
สำนักนโยบายพัฒนาระบบการเงินภาคประชาชน
สำนักงานเศรษฐกิจการคลัง กระทรวงการคลัง
ซอยอารีย์สัมพันธ์ ถนนพระราม 6 สามเสนใน
พญาไท กรุงเทพฯ 10400
โทร. 1359

กิจกรรมท้ายเรื่องที่ 2 แชร์ลูกโซ่

(ให้ผู้เรียนไปทำกิจกรรมท้ายเรื่องที่ 2 ที่สมุดบันทึกกิจกรรมการเรียนรู้)

เรื่องที่ 3 ภัยใกล้ตัว

หลายครั้งที่ความโลภกลายเป็นจุดอ่อนที่มิจฉาชีพใช้โจมตีเหยื่อ โดยนำผลประโยชน์จำนวนมากมาหลอกล่อ ให้เหยื่อยอมจ่ายเงินจำนวนหนึ่งให้ก่อน แล้วนำเงินหนีไป

ลักษณะกลโกงของภัยใกล้ตัว

1. เบี้ยประกันงวดสุดท้าย

มิจฉาชีพจะแอบอ้างเป็นพนักงานบริษัทประกันชีวิตติดต่อญาติของผู้ตายว่าผู้ตายทำประกันชีวิตไว้กับบริษัท แต่ขาดการชำระเบี้ยประกันงวดสุดท้าย หากญาติจ่ายค่าเบี้ยประกันที่ค้างอยู่ ก็จะได้รับเงินคืนตามกรมธรรม์ซึ่งเป็นจำนวนเงินค่อนข้างมาก เมื่อเหยื่อจ่ายเงินให้ ผู้ที่อ้างว่าเป็นพนักงานบริษัทประกันภัยก็จะหายตัวไปพร้อมเงินประกันงวดสุดท้าย

2. ตกทอง/ลอตเตอรี่ปลอม

มิจฉาชีพจะอ้างว่ามีทองหรือลอตเตอรี่รางวัลที่หนึ่ง แต่ไม่มีเวลาไปขายหรือขึ้นเงิน จึงเสนอขายให้เหยื่อในราคาถูก กว่าจะรู้ว่าเป็นทองหรือลอตเตอรี่ปลอม มิจฉาชีพก็หายไปพร้อมกับเงินที่ได้ไป

3. นาย (พัน) หน้า...หลอกลวงเงิน

มิจฉาชีพจะแอบอ้างว่าเป็นเจ้าหน้าที่ในองค์กรหรือสถาบันการเงินที่สามารถช่วยเหยื่อหางาน หรือขอสินเชื่อจากสถาบันการเงินได้ แต่เหยื่อต้องจ่ายค่านายหน้าให้ก่อน มิจฉาชีพบางรายก็หลอกให้เหยื่อเป็นนายหน้าขายที่ดิน โดยทำงานกันเป็นทีม คนแรกหลอกว่าอยากขายที่ดิน คนที่สองหลอกว่าอยากซื้อที่ดิน แล้วขอให้เหยื่อเป็นนายหน้าให้ จากนั้นคนซื้อจะอ้างว่าเงินไม่พอจ่ายค่ามัดจำจึงขอให้เหยื่อช่วยออกเงินค่ามัดจำ สุดท้ายคนซื้อและคนขายหนีหาย เหยื่อไม่ได้ค่านายหน้าแถมยังเสียเงินค่ามัดจำไปอีกด้วย

4. แก๊งเงินดำ

มิจฉาชีพจะอ้างว่ามีธนบัตรดอลลาร์สหรัฐฯ ที่เคลือบด้วยสารเคมีสีดำเป็นจำนวนมาก และมีน้ำยาพิเศษที่สามารถล้างน้ำยานั้นออกได้ พร้อมทั้งสาธิตการล้างเงินดำให้เหยื่อดู เมื่อเหยื่อหลงเชื่อ จะหลอกเหยื่อว่า น้ำยาพิเศษนั้นอยู่ที่สถานทูต แต่ไม่สามารถนำออกมาได้เพราะต้องจ่ายค่าธรรมเนียมในการดำเนินการค่อนข้างสูง

มิจฉาชีพจึงชักชวนเหยื่อให้ร่วมหุ้นจ่ายค่าธรรมเนียม แล้วจะแบ่งธนบัตรดอลลาร์สหรัฐฯ ที่ล้างเรียบร้อยแล้วให้เหยื่อ หากเหยื่อหลงเชื่อจ่ายเงินไป มิจฉาชีพก็จะหายไปพร้อมกับเงินของเหยื่อ

วิธีป้องกันจากภัยใกล้ตัว

1. **ไม่โลภ** ไม่อยากได้เงินรางวัลที่ไม่มีที่มา หากมีคนเสนอให้ ควรสงสัยไว้ก่อนว่าอาจเป็นภัยทางการเงิน
2. **ไม่รู้จัก...ไม่ให้** ไม่ให้ทั้งข้อมูลส่วนตัว เช่น เลขที่บัตรประจำตัวประชาชน วัน/เดือน/ปีเกิด และข้อมูลทางการเงิน เช่น เลขที่บัญชี รหัสบัตรเอทีเอ็ม/บัตรเดบิต และไม่โอนเงิน แม้ผู้ติดต่อจะอ้างว่าเป็นหน่วยงานราชการหรือสถาบันการเงิน
3. **ศึกษาหาข้อมูล** ก่อนเซ็นสัญญา ตกลงจ่ายเงิน หรือโอนเงินให้ใคร ควรศึกษาข้อมูล เงื่อนไข ข้อตกลง ความน่าเชื่อถือและความน่าจะเป็นไปได้ก่อน
4. **อ้างใคร ถามคนนั้น** อ้างถึงใครให้สอบถามคนนั้น เช่น ธนาคารแห่งประเทศไทย โทร. 1213 หรือ DSI โทร. 1202
5. **สงสัยให้ปรึกษา** ควรหาที่ปรึกษาที่ไว้ใจได้ หรือปรึกษาเกี่ยวกับภัยทางการเงินได้ที่ ศคง. โทร. 1213 และศูนย์รับแจ้งการเงินนอกระบบ โทร. 1359
6. **ติดตามข่าวสารกลโกงเป็นประจำ** เพื่อรู้เท่าทันเล่ห์เหลี่ยมกลโกง

รู้ไว้...ไม่เสี่ยงเป็นเหยื่อ

1. **อ้างหน่วยงานราชการไม่ได้แปลว่าเชื่อถือได้** มิจฉาชีพมักอ้างถึงหน่วยงานราชการหรือองค์กรขนาดใหญ่เพื่อสร้างความน่าเชื่อถือ หากมีการอ้างถึง ควรสอบถามหน่วยงานนั้นโดยตรง
2. **ธุรกิจที่จดทะเบียนแล้วไม่ได้แปลว่าไม่โกง** บางธุรกิจจดทะเบียนอย่างถูกต้องตามกฎหมายจริง แต่ไม่ได้ประกอบธุรกิจตามที่ขออนุญาตไว้
3. **ไม่มี “ทางลัดรวยที่มีน้อยคนรู้”** หากทางลัดนี้มีจริง คงไม่มีใครอยากบอกคนอื่นให้รู้ แอบรวยเงียบ ๆ คนเดียวดีกว่า
4. **หัวขโมยไม่หมิ่นเงินน้อย** มิจฉาชีพไม่ได้มุ่งหวังเงินหลักแสนหลักหมื่นเท่านั้น มิจฉาชีพบางกลุ่มมุ่งเงินจำนวนน้อยแต่หวังหลอกคนจำนวนมาก
5. **อย่าระวังแค่เรื่องเงิน** มิจฉาชีพบางรายก็หลอกขอข้อมูลส่วนตัวหรือข้อมูลที่ใช้ทำธุรกรรมการเงิน เพื่อนำไปทำธุรกรรมทางการเงินในนามของเหยื่อ
6. **มิจฉาชีพไม่ใช้บัญชีตนเองรับเงินจากเหยื่อ** มิจฉาชีพบางรายจ้างคนเปิดบัญชีเพื่อเป็นที่รับเงินโอนจากเหยื่ออีกรายหนึ่ง เพื่อหนีการจับกุมของเจ้าหน้าที่ตำรวจ

รู้หรือไม่ว่า

การรับจ้างเปิดบัญชีหรือการหลอกให้ผู้อื่นโอนเงินให้เข้าข่ายฉ้อโกงประชาชนซึ่งเป็นหนึ่งในความผิดมูลฐานตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 60 ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี หรือปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท หรือทั้งจำทั้งปรับ ดังนั้น การเห็นแก่ค่าจ้างเพียงไม่กี่บาทจึงอาจทำให้คุณต้องตกเป็นผู้ต้องหาและไปใช้ชีวิตในเรือนจำได้ จึงไม่ควรหลงเชื่อหรือรับจ้างเปิดบัญชีโดยเด็ดขาด

กิจกรรมท้ายเรื่องที่ 3 ภัยใกล้ตัว

(ให้ผู้เรียนไปทำกิจกรรมท้ายเรื่องที่ 3 ที่สมุดบันทึกกิจกรรมการเรียนรู้)

เรื่องที่ 4 แก๊งคอลเซนเตอร์

แก๊งคอลเซนเตอร์มักใช้วิธีสุ่มเบอร์โทรศัพท์เพื่อโทรไปหาเหยื่อแล้วใช้ข้อความอัตโนมัติสร้างความตื่นเต้นหรือตกใจให้แก่เหยื่อ บางครั้งก็แอบอ้างเป็นเจ้าหน้าที่หน่วยงานต่าง ๆ หลอกให้เหยื่อทำรายการที่เครื่องเอทีเอ็มเป็นเมนูภาษาอังกฤษ โดยแจ้งว่าเป็นการทำรายการเพื่อล้างหนี้ หรืออาจหลอกให้เหยื่อไปโอนเงินให้หน่วยงานภาครัฐเพื่อตรวจสอบ

ลักษณะกลโกงแก๊งคอลเซนเตอร์

1. บัญชีเงินฝากถูกอายัดหรือเป็นหนี้บัตรเครดิต

มิจฉาชีพจะหลอกเหยื่อว่า บัญชีเงินฝากถูกอายัด หรือเป็นหนี้บัตรเครดิตจำนวนหนึ่ง โดยเริ่มจากการใช้ระบบตอบรับอัตโนมัติแจ้งเหยื่อว่าจะอายัดบัญชีเงินฝากเนื่องจากเหตุการณ์ต่าง ๆ เช่น เป็นหนี้บัตรเครดิตหรือกระทำการผิดกฎหมาย โดยอาจมีเสียงอัตโนมัติ เช่น “คุณเป็นหนี้บัตรเครดิตกับทางธนาคาร กด 0 เพื่อติดต่อพนักงาน” ซึ่งเหยื่อส่วนมากมักจะตกใจและรีบกด 0 เพื่อติดต่อพนักงานทันที

หลังจากนั้นมิจฉาชีพจะหลอกถามฐานะทางการเงินของเหยื่อ หากเหยื่อมีเงินฝากจำนวนไม่มากนัก มิจฉาชีพอาจหลอกให้เหยื่อโอนเงินผ่านเครื่องเอทีเอ็มโดยหลอกว่าเป็นการทำรายการเพื่อล้างบัญชีหนี้

2. บัญชีเงินฝากพัวพันกับการค้ายาเสพติดหรือการฟอกเงิน

แต่หากมิจฉาชีพพบว่า เหยื่อมีเงินฝากค่อนข้างมาก ก็จะหลอกเหยื่อให้ตกใจว่า บัญชีเงินฝากนั้นพัวพันกับการค้ายาเสพติดหรือการฟอกเงิน และจะให้เหยื่อโอนเงินทั้งหมดผ่านเครื่องเอทีเอ็ม / เครื่องฝากเงินอัตโนมัติ (CDM หรือ ADM) เพื่อทำการตรวจสอบกับหน่วยงานราชการ ทั้งนี้ เพื่อป้องกันไม่ให้เหยื่อได้มีโอกาสสอบถามความจริงจากพนักงานธนาคาร

3. เงินคืนภาษี

นอกจากจะหลอกให้เหยื่อตกใจแล้ว มิจฉาชีพบางรายก็อ้างว่าตนเป็นเจ้าหน้าที่สรรพากร หลอกให้เหยื่อตื่นเต้นดีใจว่า เหยื่อได้รับเงินคืนค่าภาษี แต่ต้องทำรายการยืนยันการรับเงินที่เครื่องเอทีเอ็ม และวันนี้เป็นวันสุดท้ายที่จะยืนยันรับเงินคืน หากเลยกำหนดเวลาแล้ว เหยื่อจะไม่ได้รับเงินคืนค่าภาษี ด้วยความรีบเร่งและกลัวว่าจะไม่ได้เงินคืน เหยื่อก็จะรีบทำตามที่มิจฉาชีพบอก โดยไม่ได้สังเกตว่ารายการที่มิจฉาชีพให้ทำที่เครื่องเอทีเอ็มนั้น เป็นการโอนเงินให้แก่มิจฉาชีพ

4. โชคดีได้รับรางวัลใหญ่

มิจฉาชีพบางรายก็หลอกให้เหยื่อดีใจว่า เหยื่อได้รับรางวัลใหญ่ที่มีมูลค่าสูง จากการจับสลากรางวัล หรือเปิดบริษัทใหม่จึงจับสลากมอบรางวัลแก่ลูกค้า แต่ก่อนที่ลูกค้าจะรับรางวัล ลูกค้าจะต้องจ่ายค่าภาษีให้กับทางผู้แจกรางวัลก่อน จึงจะสามารถส่งของรางวัลไปให้

5. ข้อมูลส่วนตัวหาย

มิจฉาชีพประเภทนี้จะโทรศัพท์แอบหลอกถามข้อมูลส่วนตัวของเหยื่อเพื่อใช้ประกอบการปลอมแปลงเอกสาร หรือใช้บริการทางการเงินในนามของเหยื่อ โดยมิจฉาชีพจะอ้างว่าตนเป็นเจ้าหน้าที่ของสถาบันการเงินที่เหยื่อใช้บริการอยู่ แต่เกิดเหตุการณ์ที่ทำให้ข้อมูลส่วนตัวของลูกค้าสูญหาย เช่น น้ำท่วม จึงขอให้เหยื่อแจ้งข้อมูลส่วนตัวเพื่อยืนยันความถูกต้อง เช่น วัน/เดือน/ปีเกิด เลขที่บัตรประชาชน เลขที่บัญชีเงินฝาก

เมื่อได้ข้อมูลส่วนตัวของเหยื่อแล้ว มิจฉาชีพจะนำข้อมูลเหล่านี้ไปแอบอ้างใช้บริการทางการเงินในนามของเหยื่อ เช่น ขอสินเชื่อ

6. โอนเงินผิด

หากมิจฉาชีพมีข้อมูลหรือเอกสารส่วนตัวของเหยื่อ มิจฉาชีพอาจใช้วิธีหลอกเหยื่อว่าโอนเงินผิดแล้วขอให้เหยื่อโอนเงินคืน โดยเริ่มจากใช้เอกสารและข้อมูลส่วนตัวของเหยื่อติดต่อขอสินเชื่อ เมื่อได้รับอนุมัติสินเชื่อ สถาบันการเงินจะโอนเงินกู้ที่ได้รับอนุมัติเข้าบัญชีเงินฝากของเหยื่อ หลังจากนั้นมิจฉาชีพจะโทรศัพท์ไปแจ้งเหยื่อว่า โอนเงินผิดเข้าบัญชีของเหยื่อและขอให้เหยื่อโอนเงินคืนให้

เมื่อเหยื่อตรวจสอบบัญชีเงินฝากของตนเองและพบว่ามีเงินโอนเงินเข้ามาในบัญชีจริง เหยื่อก็รีบโอนนั้นให้แก่มิจฉาชีพทันที โดยไม่รู้ว่าเงินนั้นเป็นเงินสินเชื่อที่มิจฉาชีพขอในนามของเหยื่อ

วิธีป้องกันภัยแก๊งคอลเซนเตอร์

1. คิดทบทวน ว่าเรื่องราวที่ได้ยินมามีความเป็นไปได้มากน้อยแค่ไหน เคยทำธุรกรรมกับหน่วยงานที่ถูกอ้างถึงหรือไม่ หรือเคยเข้าร่วมชิงรางวัลกับองค์กรไหนจริงหรือเปล่า

2. ไม่รู้จัก ไม่คุ้นเคย ไม่ให้ข้อมูล ทั้งข้อมูลส่วนตัว เช่น เลขที่บัตรประชาชน วัน/เดือน/ปีเกิด และข้อมูลทางการเงิน เช่น เลขที่บัญชี รหัสกดเงิน

3. ไม่ทำรายการที่เครื่องเอทีเอ็มตามคำบอก แม้คนที่โทรมาจะบอกว่าเป็นเจ้าหน้าที่ของรัฐหรือสถาบันการเงิน เพราะหน่วยงานของรัฐและสถาบันการเงินไม่มีนโยบายสอบถามข้อมูลส่วนตัวของประชาชนหรือลูกค้าผ่านทางโทรศัพท์

4. ไม่โอนเงินคืนเอง หากมีคนโอนเงินผิดเข้าบัญชี ควรสอบถามโดยตรงกับสถาบันการเงินถึงที่มาของเงินดังกล่าว หากเป็นเงินที่โอนผิดจริง จะต้องให้สถาบันการเงินเป็นผู้ดำเนินการโอนเงินคืนเท่านั้น

5. ตรวจสอบข้อมูลก่อนโอนเงิน สอบถามสถาบันการเงินหรือหน่วยงานที่ถูกอ้างถึงโดยตรง โดยติดต่อฝ่ายบริการลูกค้า (call center) หรือสาขาของสถาบันการเงินนั้น ๆ

ทำอย่างไรเมื่อตกเป็นเหยื่อภัยแก๊งคอลเซนเตอร์

1. ติดต่อฝ่ายบริการลูกค้า (call center) ของสถาบันการเงินนั้น ๆ เพื่อระงับการโอนและถอนเงิน โดยรวบรวมเอกสารที่เกี่ยวข้องเพื่อเป็นข้อมูลประกอบการขอระงับการโอนและถอนเงิน ทั้งนี้ แต่ละสถาบันการเงินมีวิธีปฏิบัติที่แตกต่างกัน ควรติดต่อสอบถามขั้นตอนจากสถาบันการเงินโดยตรง

2. แจ้งเบาะแสไปยังกรมสอบสวนคดีพิเศษ (DSI) เลขที่ 128 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210 โทร. 1202

กิจกรรมท้ายเรื่องที่ 4 แก๊งคอลเซนเตอร์

(ให้ผู้เรียนไปทำกิจกรรมท้ายเรื่องที่ 4 ที่สมุดบันทึกกิจกรรมการเรียนรู้)

เรื่องที่ 5 ภัยออนไลน์

อินเทอร์เน็ตเป็นช่องทางการสื่อสารที่สะดวกและรวดเร็ว ทำให้เพื่อนฝูง ญาติพี่น้อง หรือคนที่ไม่รู้จัก สามารถติดต่อหากันได้อย่างง่ายดาย ความสะดวกสบายเหล่านี้นอกจากจะเอื้อประโยชน์ต่อผู้ใช้บริการแล้ว ก็เอื้อประโยชน์ต่อมิจฉาชีพเช่นกัน อินเทอร์เน็ตจึงกลายเป็นอีกช่องทางที่มิจฉาชีพจะเข้ามากอบโกยผลประโยชน์จากเหยื่อ

ลักษณะกลโกงภัยออนไลน์

1. แอบอ้างเป็นบุคคลต่าง ๆ

มิจฉาชีพจะแอบอ้างเป็นบุคคลต่าง ๆ และหลอกเหยื่อว่าจะโอนเงินจำนวนมากให้แก่เหยื่อ พร้อมทั้งส่งหลักฐานการโอนเงินปลอมให้ดูว่ามีการโอนเงินจริง แต่แท้จริงไม่มีการโอนเงินใด ๆ ทั้งสิ้น หลังจากนั้นจะแอบอ้างเป็นเจ้าหน้าที่องค์กรหรือหน่วยงานต่าง ๆ เช่น ธนาคารกลางของประเทศต้นทาง ธนาคารแห่งประเทศไทย หรือสหประชาชาติ แจ้งเหยื่อว่า **เงินที่โอนมาถูกระงับและขอตรวจสอบเงิน**

จากนั้นจะ**ขอให้เหยื่อจ่ายค่าธรรมเนียมเพื่อยกเลิกการระงับเงินโอน** โดยจะเริ่มจากค่าธรรมเนียมที่ไม่มากนักแล้วค่อย ๆ เพิ่มมูลค่าสูงขึ้นเรื่อย ๆ จนกว่าเหยื่อจะรู้ตัว เหยื่อบางรายโอนเงินให้แก่มิจฉาชีพมากกว่าสิบครั้ง มูลค่าความเสียหายรวมกันเป็นหลักล้าน ซึ่งมิจฉาชีพเหล่านี้มักใช้มุกอ้างดังนี้

- **นักธุรกิจต้องการสั่งสินค้าจำนวนมาก** – เหยื่อส่วนมากเป็นผู้ประกอบธุรกิจขายสินค้าทางอินเทอร์เน็ต มิจฉาชีพจะส่งอีเมลแอบอ้างเป็นนักธุรกิจต่างชาติที่ต้องการสั่งซื้อสินค้าจำนวนมาก แล้วส่งหลักฐานการโอนเงินปลอมให้เหยื่อตายใจว่าโอนเงินแล้ว ส่วนเหยื่อ นอกจากจะไม่ได้เงินค่าสินค้าแล้ว ยังเสียเงินทุนและเวลาในการผลิตสินค้าตามคำสั่งซื้ออีกด้วย (บางรายส่งสินค้าไปให้มิจฉาชีพแล้ว)
- **ผู้ใจบุญต้องการบริจาคเงินจำนวนมาก** – เหยื่อมักจะเป็นองค์กรการกุศลที่เปิดรับเงินบริจาคอยู่แล้ว โดยมิจฉาชีพจะส่งอีเมลติดต่อเหยื่อว่า ต้องการบริจาคเงินพร้อมทั้งขอเลขที่บัญชีของเหยื่อ เมื่อได้ข้อมูลทางการเงินของเหยื่อแล้ว มิจฉาชีพจะนำข้อมูลดังกล่าวไปสร้างหลักฐานการโอนเงินปลอมแล้วส่งมาให้เหยื่อดูเสมือนว่ามีการโอนเงินจริง
- **ทายาทที่ไม่สามารถรับมรดกได้** – มิจฉาชีพมักติดต่อเหยื่อผ่านช่องทางโซเชียลมีเดีย (social media) ต่าง ๆ แล้วอ้างว่าตนเองได้รับมรดกเป็นเงินจำนวนมากในประเทศหนึ่ง แต่ไม่สามารถรับมรดกนั้นได้ด้วยติดเหตุผลทางการเมืองหรือเหตุผลอื่น ๆ จึงขอใช้

ชื่อและเลขที่บัญชีเงินฝากของเหยื่อในการรับมรดก แล้วส่งหลักฐานการโอนเงินปลอมให้เหยื่อดูเสมือนว่ามีการโอนเงินมรดกไปให้เหยื่อจริง

- **ชายหนุ่มที่ต้องการหารักแท้** – มิจฉาชีพจะเริ่มทำความรู้จักกับเหยื่อผ่านทางโซเชียลมีเดียโดยอ้างว่าตนเป็นชาวต่างชาติที่มีรายได้และหน้าที่การงานที่ดี แล้วใช้เวลาตีสนิทเป็นปีก่อนจะบอกว่าอยากย้ายมาแต่งงานและอยู่เมืองไทยกับเหยื่อ และหลอกว่าได้โอนเงินมาให้เพื่อเตรียมซื้อบ้านพร้อมส่งหลักฐานการโอนเงินปลอมมาให้แก่เหยื่อ

นอกจากหลอกว่าจะโอนเงินมาให้เหยื่อแล้ว มิจฉาชีพบางรายก็อ้างว่าส่งของขวัญพร้อมเงินสดมาให้เหยื่อ แล้วอ้างตัวเป็นกรมศุลกากรเรียกเก็บค่าภาษี หรือค่าธรรมเนียมในการนำเงินสดออกมา

- **องค์กรใจดีแจกเงินทุนหรือรางวัล** – เหยื่อจะได้รับอีเมลแจ้งว่าเหยื่อได้รับเงินทุนหรือรางวัล แต่เหยื่อจะต้องปฏิบัติตามขั้นตอนที่แจ้งมาตามอีเมล ซึ่งจะต้องจ่ายค่าเปิดบัญชี ค่าธรรมเนียม ค่าเอกสารต่าง ๆ สุดท้ายก็ไม่ได้รับเงินทุนหรือรางวัลใด ๆ

รู้หรือไม่ว่า

ผู้รับสินค้าหรือรับเงินโอนจากต่างประเทศ ไม่จำเป็นต้องเสียภาษีหรือค่าธรรมเนียมเป็นเงินสดแก่เจ้าหน้าที่ในต่างประเทศ สำหรับการส่งสินค้าเข้ามาให้ผู้รับในประเทศ เจ้าหน้าที่จะเรียกเก็บอากรจากผู้รับตามกฎหมายไทยในขั้นตอนการรับสินค้า โดยไม่มีการเปิดตรวจหรือเก็บภาษีที่ต่างประเทศ หากมีข้อสงสัย สามารถสอบถามเพิ่มเติมได้ที่สายด่วนศุลกากร โทร. 1164 หรือ www.customs.go.th

สำหรับการโอนเงินระหว่างประเทศ ผู้โอนสามารถเลือกได้ว่าจ่ายค่าธรรมเนียมเอง หรือระบุให้หักค่าธรรมเนียมจากยอดเงินโอนได้โดยผู้รับโอนไม่จำเป็นต้องจ่ายเป็นเงินสด

2. แอบอ้างเป็นคนรู้จัก

มิจฉาชีพบางรายอาจแอบอ้างเป็นผู้ให้บริการอีเมลโดยส่งอีเมลแจ้งเหยื่อว่าจะปิดการให้บริการบัญชีอีเมลของเหยื่อ หากเหยื่อไม่ทำการยืนยันการใช้งานโดยการ**กรอกข้อมูลชื่อบัญชีผู้ใช้อีเมล (email address) และรหัสผ่าน (password) ในหน้าจอของอีเมลที่ส่งมา** หากไม่ยืนยันก็จะปิดบัญชีอีเมลของเหยื่อ

เหยื่อหลายรายหลงเชื่อและกรอกชื่อบัญชีผู้ใช้อีเมลและรหัสผ่านไป **มิจฉาชีพจึงนำข้อมูลดังกล่าวไปเข้าใช้บัญชีอีเมลของเหยื่อ หลังจากนั้นจะส่งอีเมลหาเพื่อนของเหยื่อโดยสร้างเรื่องเพื่อหลอกให้โอนเงิน** เช่น เหยื่อไปต่างประเทศและได้ทำกระเป๋าเงินหาย จึงใช้ความเป็นห่วงเพื่อนในการหลอกให้เพื่อนของเหยื่อโอนเงินให้แก่มิจฉาชีพ

3. หลอกขายของออนไลน์

มิจฉาชีพมักประกาศขายสินค้าดีราคาถูกในเว็บไซต์แล้วหลอกให้เหยื่อโอนเงินค่าสินค้าหรือเงินมัดจำให้ เมื่อถึงเวลาส่งของ ผู้ซื้อก็ไม่ได้รับสินค้าและไม่สามารถติดต่อคนขายได้ เงินค่าสินค้าหรือเงินมัดจำที่โอนไปก็ไม่ได้คืน เมื่อตรวจสอบก็พบว่า **มิจฉาชีพใช้วิธีจ้างคนอื่นเปิดบัญชีหรือหลอกใช้บัญชีคนอื่นรับเงินโอนเพื่อหลีกหนีการจับกุม**

มิจฉาชีพบางรายก็ประกาศขายสินค้าโดยใช้เลขที่บัญชีของผู้ขายรายอื่น เมื่อมีเหยื่อสั่งซื้อและโอนเงินให้ **มิจฉาชีพจะติดต่อเจ้าของบัญชีนั้นแล้วอ้างว่าตนโอนเงินผิดไปและขอรับคืนเป็นเงินสด** ขณะเดียวกันเหยื่อที่สั่งซื้อสินค้าก็ไม่ได้รับสินค้า เจ้าของบัญชีรายนั้นจึงกลายเป็นผู้ต้องสงสัยทันที ดังนั้น หากมีผู้อื่นอ้างว่าได้โอนเงินผิดเข้าบัญชี ไม่ควรถอนเงินสดหรือโอนเงินคืนด้วยตนเอง ควรให้ผู้ที่อ้างว่าโอนผิดติดต่อแจ้งยกเลิกการโอนเงินและขอเงินคืนผ่านธนาคาร

4. ขอเลขที่บัญชีเงินฝากเป็นที่พักเงิน

มิจฉาชีพจะประกาศรับสมัครงานผ่านทางอินเทอร์เน็ตหรืออาจติดต่อเหยื่อไปเองว่าเป็นบริษัทจากต่างประเทศที่ส่งสินค้าเข้ามาขายในประเทศไทย **ต้องการพนักงานที่คอยรวบรวมเงินค่าสินค้าในประเทศไทย จึงต้องใช้บัญชีเงินฝากของเหยื่อเป็นที่พักเงิน โดยตกลงว่าจะแบ่งส่วนแบ่งจากการขายสินค้าให้** (เช่น ร้อยละ 25 ของเงินค่าสินค้า)

วันหนึ่งเหยื่อได้รับโทรศัพท์จากมิจฉาชีพแจ้งว่า มีคนโอนค่าสินค้า ให้เหยื่อหักส่วนแบ่งไว้ตามที่ตกลงกัน และให้โอนเงินที่เหลือให้แก่บริษัทแม่ เมื่อเหยื่อตรวจสอบบัญชีเงินฝาก ก็พบว่ามีเงินเข้ามาจริง จึงโอนเงินที่เหลือหลังหักส่วนแบ่งแล้วให้แก่มิจฉาชีพ

เวลาผ่านไป เหยื่อได้รับการติดต่อจากเจ้าหน้าที่ตำรวจว่า เงินที่เข้ามาในบัญชีเงินฝากของเหยื่อนั้นเป็นเงินที่มิจฉาชีพไปหลอกเหยื่อรายอื่นมา สุดท้ายเหยื่อกลายเป็นผู้ต้องสงสัย ส่วนมิจฉาชีพตัวจริงก็ลอยนวลหายไป

5. เงินกู้ออนไลน์

เหยื่อรายหนึ่งต้องการใช้เงินอย่างเร่งด่วนแต่ไม่มีเงินสำรองไว้ จึงคิดหาทางออกโดยการกู้เงินนอกระบบ พอดีได้อ่านประกาศบริการเงินกู้นอกระบบดอกเบี้ยต่ำในอินเทอร์เน็ต จึงรีบติดต่อไปยังเบอร์โทรศัพท์ที่ให้ไว้ทันที

เมื่อเหยื่อติดต่อไป มิจฉาชีพ (ผู้ให้กู้) ก็อ้างว่าจะส่งสัญญามาให้เหยื่อเซ็น โดย**เหยื่อจะต้องชำระค่าทำสัญญา ค่าเอกสาร ค่ามัดจำ หรือดอกเบี้ยล่วงหน้าภายในเวลาที่กำหนด** เช่น ภายในวันนี้เวลา 18.00 น. (เพื่อเร่งให้เหยื่อตัดสินใจโดยไม่ไตร่ตรอง) แต่เมื่อเหยื่อโอนเงินไปแล้ว กลับไม่สามารถติดต่อผู้ให้กู้ได้อีกเลย

6. เรียกค่าไถ่ข้อมูลด้วยมัลแวร์

มิจฉาชีพจะแอบอ้างเป็นหน่วยงานหรือองค์กรต่าง ๆ เช่น บริษัทขนส่งสินค้า ส่งอีเมลที่แนบไฟล์เรียกค่าไถ่หรือไฟล์แรนซัมแวร์ (ransomware) หรือแนบลิงก์ให้เหยื่อติดตั้งแรนซัมแวร์ในคอมพิวเตอร์ของเหยื่อ ซึ่งแรนซัมแวร์เป็นมัลแวร์ (malware) หรือไวรัสชนิดหนึ่ง เมื่อถูกติดตั้งในคอมพิวเตอร์จะทำการเข้ารหัสลับ (encryption) ในไฟล์เอกสารต่าง ๆ ที่อยู่ในเครื่องคอมพิวเตอร์นั้น ทำให้**ผู้ใช้งานไม่สามารถเปิดใช้งานหรือแก้ไขไฟล์ได้ หากไม่มีรหัสจากผู้สร้างแรนซัมแวร์เพื่อถอดรหัสลับข้อมูล (decryption) เสมือนถูกเรียกค่าไถ่**

หลังจากนั้นหน้าจอจะแสดงหน้าต่างเรียกค่าไถ่ โดยผู้ใช้งานจะต้องจ่ายเงินจำนวนหนึ่งเพื่อแลกกับการถอดรหัสใช้งานไฟล์ดังกล่าว แต่ก็ไม่มีใครรับประกันว่าจ่ายเงินแล้วเราจะได้รับรหัสหรือใช้ไฟล์งานเอกสารเหล่านั้นหรือไม่ เหยื่ออาจต้องลบข้อมูลทั้งหมดเครื่องคอมพิวเตอร์เพื่อกำจัดแรนซัมแวร์

วิธีป้องกันภัยร้ายบนโลกออนไลน์

1. คิดทบทวน ว่าเรื่องที่เจอหรือได้ยินมามีความน่าเชื่อถือมากน้อยแค่ไหน หากโอนเงินไปแล้วมีปัญหา จะมีโอกาสได้คืนไหม

2. เปิดเผยเท่าที่จำเป็น โดยเฉพาะข้อมูลส่วนตัวในโซเชียลมีเดียที่มิจฉาชีพอาจนำไปแอบอ้างใช้ทำธุรกรรมต่าง ๆ ได้

3. ตรวจสอบข้อมูลก่อนโอนเงิน หากอ้างถึงบุคคล หน่วยงาน หรือองค์กรใด ๆ ควรติดต่อสอบถามบุคคลนั้น หรือองค์กรนั้น ๆ โดยตรง

4. ติดตามข่าวสารกลโกงเป็นประจำ เพื่อรู้เท่าทันเล่ห์เหลี่ยมกลโกง

ทำอย่างไรเมื่อตกเป็นเหยื่อภัยร้ายบนโลกออนไลน์

1. หากถูกแอบอ้างใช้บัญชีอีเมล ให้ติดต่อผู้ให้บริการอีเมลทันที เพื่อเปลี่ยนรหัสผ่านหรือปิดบัญชี

2. หากโอนเงินให้มิจฉาชีพแล้ว ให้

1) ติดต่อฝ่ายบริการลูกค้า (call center) ของธนาคารนั้น ๆ เพื่อระงับการโอนและถอนเงิน โดยรวบรวมเอกสารเพื่อเป็นข้อมูลประกอบการขอระงับการโอนและถอนเงิน ทั้งนี้แต่ละธนาคารมีวิธีปฏิบัติที่แตกต่างกัน ควรติดต่อสอบถามขั้นตอนจากธนาคารโดยตรง

2) แจ้งเบาะแสแก่เจ้าหน้าที่ตำรวจเพื่อติดตามคนร้าย

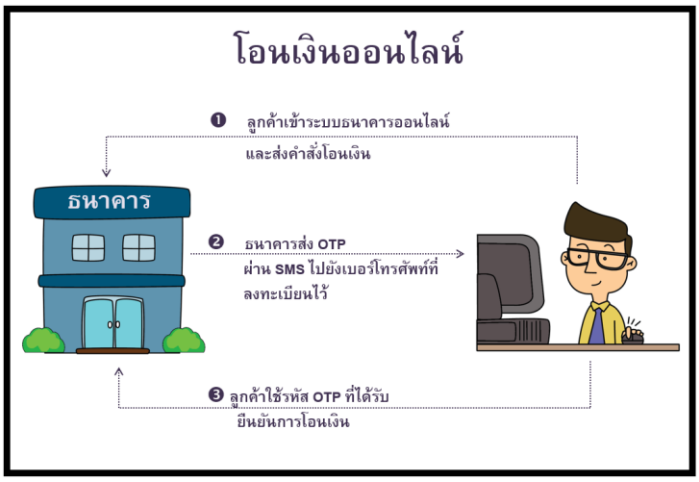
กิจกรรมท้ายเรื่องที่ 5 ภัยออนไลน์

(ให้ผู้เรียนไปทำกิจกรรมท้ายเรื่องที่ 5 ที่สมุดบันทึกกิจกรรมการเรียนรู้)

เรื่องที่ 6 ภัยธนาคารออนไลน์

เทคโนโลยีที่พัฒนาก้าวหน้าทำให้ธนาคารอยู่เพียงปลายนิ้วมือ ผู้ใช้บริการสามารถจัดการบัญชีเงินฝากของตนเองผ่านทางอินเทอร์เน็ตได้โดยไม่ต้องเดินทางไปธนาคาร ซึ่งขั้นตอนหลัก ๆ ในการโอนเงินผ่านทางอินเทอร์เน็ต (โอนเงินออนไลน์) มีดังนี้

1. ผู้ใช้บริการเข้าระบบธนาคารออนไลน์โดยใช้รหัสผู้ใช้งาน (username) และรหัสผ่าน (password) และส่งคำสั่งโอนเงิน
2. ธนาคารส่งรหัสผ่านชั่วคราว (OTP หรือ One Time Password) ผ่านทาง SMS ไปยังโทรศัพท์มือถือที่ผู้ใช้บริการลงทะเบียนไว้ เพื่อให้ผู้ใช้บริการยืนยันการทำธุรกรรมที่ต้องการทำ ซึ่ง OTP นี้เป็นรหัสผ่านที่ธนาคารออกให้ผู้ใช้บริการเพื่อใช้ยืนยันการทำธุรกรรมธนาคารออนไลน์ที่สำคัญ โดยจะใช้ได้เพียงหนึ่งครั้งภายในเวลาที่กำหนด ทั้งนี้ ธนาคารจะส่ง OTP มาพร้อมกับรายละเอียดของธุรกรรมที่จะใช้ OTP นั้น
3. เมื่อผู้ใช้บริการได้รับ OTP แล้ว ก็กรอก OTP เพื่อยืนยันการโอนเงิน



ความสะดวกสบายในการทำธุรกรรมผ่านทางอินเทอร์เน็ตนี้ ทำให้ผู้ใช้บริการสามารถจัดการเงินในบัญชีได้อย่างง่ายดาย แต่ใครจะรู้...ธนาคารออนไลน์ที่มาพร้อมกับความสะดวกสบายเหล่านี้หากใช้ไม่ระวัง เงินที่อยู่ในบัญชีอาจหายไปได้

ลักษณะกลโกงที่แฝงอยู่ในธนาคารออนไลน์

1. แฝงโปรแกรมร้ายหรือมัลแวร์ (Malware) มาให้ดาวน์โหลด

1) โปรแกรมร้ายในคอมพิวเตอร์

โปรแกรมร้าย หรือมัลแวร์ (Malware) เช่น ไวรัส โทรจัน เป็นโปรแกรมที่สร้างขึ้นมาเพื่อทำลายหรือสร้างความเสียหายให้แก่ระบบคอมพิวเตอร์ ระบบ

เครือข่าย รวมถึงขโมยข้อมูลของผู้ใช้งาน ซึ่งมิจฉาชีพสามารถนำข้อมูลดังกล่าวไปทำธุรกรรมทางการเงินแทนเหยื่อได้

มิจฉาชีพจะแฝงโปรแกรมร้ายในลิงก์ดาวน์โหลด ไฟล์ หรือโปรแกรมต่าง ๆ และมักจะใช้ข้อความหลอกล่อให้คลิกลิงก์หรือติดตั้งโปรแกรม เช่น “คุณเป็นผู้โชคดี คลิกที่นี่เพื่อรับรางวัล” “คลิปฉาวลับสุดยอดของคู่จิ้นเบอร์ 1 ของวงการ คลิกที่นี่”

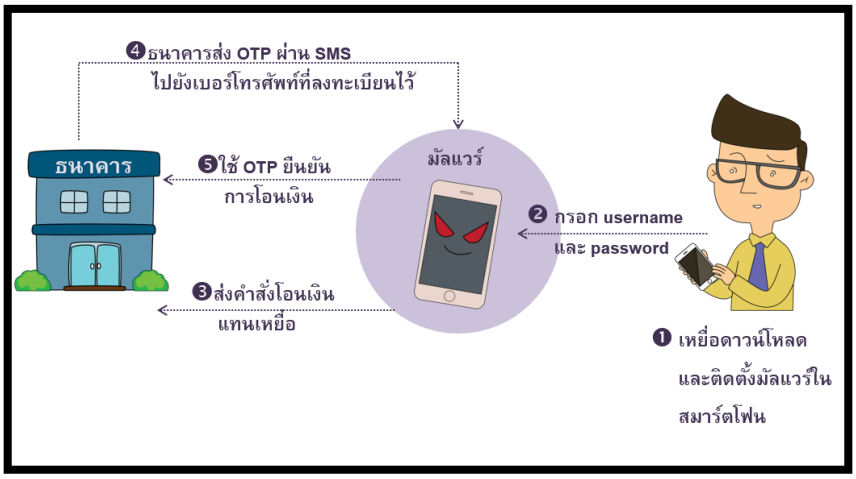
เมื่อโปรแกรมร้ายถูกติดตั้งในเครื่องคอมพิวเตอร์ จะทำหน้าที่ขโมยข้อมูลหรือบันทึกข้อมูลการใช้งานของเจ้าของเครื่อง เช่น รหัสผู้ใช้งาน (username) รหัสผ่าน (password) หรืออาจเข้าควบคุมการใช้งาน รวมไปถึงปลอมแปลงคำขอทำธุรกรรมการเงินให้เหมือนเป็นคำสั่งจากเจ้าของบัญชี

หากปลอมแปลงคำสั่งโอนเงินแล้ว โปรแกรมร้ายจะสร้างหน้าต่างปลอมหรือหน้าจอ pop-up เพื่อหลอกถาม “รหัสผ่านชั่วคราว (OTP)” หรืออาจใช้โปรแกรมบันทึกการกด OTP แล้วนำมาใช้ยืนยันการโอนเงินออกจากบัญชีเงินฝากของเหยื่อ

2) แอปพลิเคชันร้ายในสมาร์ตโฟน

ไม่เฉพาะเครื่องคอมพิวเตอร์เท่านั้นที่มีโปรแกรมร้ายแฝงอยู่ ในสมาร์ตโฟนก็มีแอปพลิเคชันร้ายแฝงอยู่ได้เช่นกัน โดย**มิจฉาชีพจะส่งลิงก์ผ่าน SMS หรืออีเมลให้เหยื่อติดตั้งแอปพลิเคชันร้ายในสมาร์ตโฟนหรือแท็บเล็ต**

เมื่อแอปพลิเคชันร้ายถูกติดตั้งในสมาร์ตโฟนแล้ว จะทำหน้าที่เหมือนโปรแกรมร้ายในคอมพิวเตอร์คือขโมยข้อมูล หรือบันทึกข้อมูลการใช้งาน หรือเข้าควบคุมการใช้งานธนาคารออนไลน์ของเหยื่อ รวมถึงเข้าใช้งานธนาคารออนไลน์แทนเหยื่อ



2. ปลอมแปลงอีเมลหลอกเหยื่อให้ข้อมูลในเว็บไซต์ปลอม

นอกจากการแฝงโปรแกรมร้ายในเครื่องคอมพิวเตอร์หรือสมาร์ตโฟนแล้ว มิจฉาชีพก็อาจ**สร้างอีเมลและเว็บไซต์ปลอมขึ้นมาเพื่อหลอกขอข้อมูลจากเหยื่อ** โดยเริ่มจากส่งอีเมลที่สร้างเรื่องโกหกขึ้นมาเพื่อทำให้เหยื่อตกใจ เช่น อ้างว่าจะอายัดบัญชี หรืออยู่ระหว่างการปรับปรุงระบบความปลอดภัย จึงขอให้เหยื่อกรอกข้อมูลในเว็บไซต์ตามลิงก์ที่แนบมา

เมื่อเหยื่อหลงเชื่อคลิกลิงก์ เหยื่อจะถูกเชื่อมต่อไปยังหน้าเว็บไซต์ปลอมที่มีลักษณะคล้ายหรือเกือบจะเหมือนเว็บไซต์จริง หากเหยื่อไม่ระวัง ลงชื่อเข้าใช้ธนาคารออนไลน์ในหน้าเว็บไซต์ปลอม ทำให้ข้อมูลรหัสผู้ใช้งาน (username) และรหัสผ่าน (password) ในการใช้งานธนาคารออนไลน์ของเหยื่อ ถูกมิจฉาชีพบันทึกเก็บไว้และนำไปเข้าใช้ทำธุรกรรมธนาคารออนไลน์เพื่อถอนเงินเหยื่อออกมา

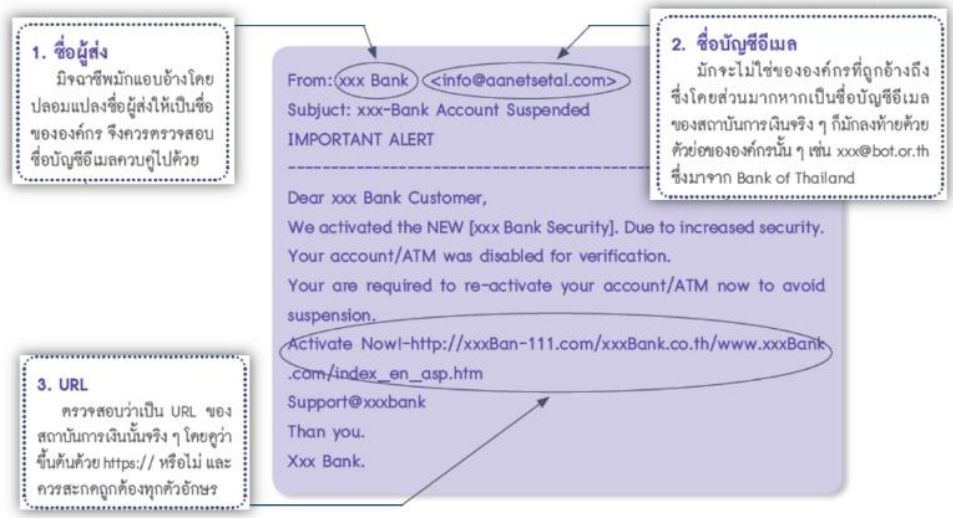
วิธีป้องกันภัยธนาคารออนไลน์

1. ไม่ติดตั้งหรือดาวน์โหลดโปรแกรมแปลก ๆ หรือผิดกฎหมาย เพราะอาจเป็นช่องทางให้มัลแวร์เข้ามาในอุปกรณ์ที่ใช้ (คอมพิวเตอร์ สมาร์ตโฟน หรือแทบเล็ต) ได้

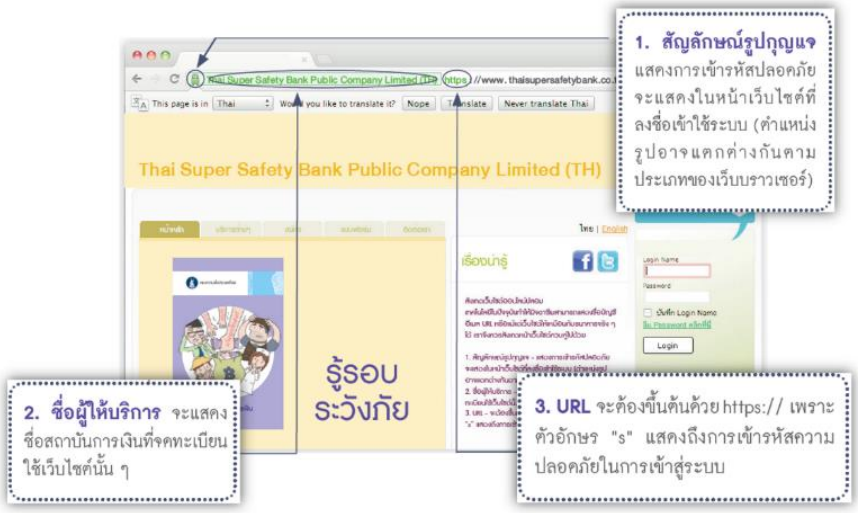
2. ตรวจสอบอุปกรณ์ที่ใช้ทำธุรกรรมออนไลน์เป็นประจำว่ามีมัลแวร์แฝงอยู่หรือไม่ โดยใช้โปรแกรมตรวจสอบและป้องกันไวรัสที่ถูกกฎหมายและเป็นปัจจุบัน

3. สังเกตอีเมลและเว็บไซต์ ก่อนคลิกลิงก์หรือลงชื่อเข้าใช้งานธนาคารออนไลน์ โดยสามารถสังเกตจุดต่าง ๆ ดังนี้

1) **อีเมล**



2) **เว็บไซต์**



4. จำกัดวงเงินในการทำธุรกรรมผ่านธนาคารออนไลน์ เพื่อลดความเสียหายหากถูกแอบเข้าใช้บัญชี

5. ตรวจสอบรายการเคลื่อนไหวในบัญชี และการเข้าใช้ระบบธนาคารออนไลน์อยู่เสมอว่าเป็นรายการที่ได้ทำไว้หรือไม่

6. หลีกเลี่ยงการทำธุรกรรมทางการเงินผ่านอินเทอร์เน็ตสาธารณะ หรือฟรี Wi-Fi เพื่อป้องกันการดักขโมยข้อมูล แต่หากจำเป็นต้องใช้ ให้รีบเปลี่ยนรหัสผ่านหลังจากการใช้งาน

7. หลีกเลี่ยงการใช้งานธนาคารออนไลน์ผ่านอุปกรณ์ที่มีการดัดแปลง หรือแก้ไขระบบปฏิบัติการ เพราะมีความเสี่ยงสูงที่จะถูกขโมยข้อมูล

8. ควรกดปุ่ม "ออกจากระบบ" (log out) ทุกครั้งเมื่อไม่ใช้งาน

ทำอย่างไรเมื่อตกเป็นเหยื่อภัยธนาคารออนไลน์

1. หากได้รับอีเมลหรือ SMS ที่ต้องสงสัย หรือเผลอคลิกลิงก์เพื่อดาวน์โหลดโปรแกรมที่แนบมา หรือหลงเชื่อให้ข้อมูลในเว็บไซต์ปลอมไป รวมทั้งได้รับรหัสผ่านชั่วคราวโดยที่ไม่ได้ส่งคำสั่งโอนเงิน ให้แจ้งเหตุการณ์แก่เจ้าหน้าที่ธนาคารหรือฝ่ายบริการลูกค้า (call center) ของธนาคารทันที พร้อมทั้งขอคำปรึกษาเกี่ยวกับวิธีแก้ไขและการใช้งานที่ปลอดภัย

2. หากพบเว็บไซต์ปลอมของสถาบันการเงิน ให้รีบแจ้งสถาบันการเงินนั้น ๆ ทันที เพื่อดำเนินการต่อไป เช่น แจ้งปิดเว็บไซต์ดังกล่าว ดำเนินคดี

กิจกรรมท้ายเรื่องที่ 6 ภัยธนาคารออนไลน์

(ให้ผู้เรียนไปทำกิจกรรมท้ายเรื่องที่ 6 ที่สมุดบันทึกกิจกรรมการเรียนรู้)

เรื่องที่ 7 ภัยบัตรอิเล็กทรอนิกส์

บัตรอิเล็กทรอนิกส์ถูกใช้กันอย่างแพร่หลาย ไม่ว่าจะเป็นบัตรเครดิต บัตรเดบิต บัตรเอทีเอ็ม หรือบัตรกดเงินสด ซึ่งข้อมูลของผู้ใช้จะถูกบันทึกไว้ภายในบัตร ซึ่งข้อมูลเหล่านี้เป็นกุญแจสำคัญในการเข้าถึงบัญชีของเจ้าของบัตร จึงเป็นสิ่งที่เหล่ามิจฉาชีพต้องการ

ลักษณะกลโกงภัยบัตรอิเล็กทรอนิกส์

1. ขโมยข้อมูลในบัตรแถบแม่เหล็ก (ผ่านเครื่องขโมยข้อมูล)

1) สกิมเมอร์ (Skimmer): เครื่องขโมยข้อมูลในบัตรที่เครื่องเอทีเอ็ม

มิจฉาชีพจะติดตั้งอุปกรณ์ คือ เครื่อง skimmer ไว้ที่ช่องสอดบัตรที่เครื่องเอทีเอ็ม และแป้นครอบตัวเลขหรือกล้องขนาดจิ๋วไว้บริเวณที่มองเห็นการกดรหัส เมื่อเหยื่อใช้บัตรที่เครื่องเอทีเอ็ม เครื่อง skimmer จะทำหน้าที่อ่านข้อมูลที่อยู่ในแถบแม่เหล็กของบัตรแล้วบันทึกเก็บไว้ ในขณะเดียวกันแป้นครอบตัวเลขหรือกล้องขนาดจิ๋วจะทำหน้าที่บันทึกการกดรหัสผ่านของผู้ใช้บริการ

เมื่อได้ข้อมูลครบ มิจฉาชีพจะนำข้อมูลดังกล่าวไปผลิตบัตรปลอมแล้วนำไปใช้โอนเงินของเหยื่อออกจากบัญชี ซึ่งส่วนมากจะนำบัตรไปใช้ในต่างประเทศเพื่อป้องกันการถูกเจ้าหน้าที่ตำรวจจับกุม

2) แฮนด์เฮลด์ สกิมเมอร์ (Handheld Skimmer): เครื่องขโมยข้อมูลขนาดพกพา

เครื่อง handheld skimmer เป็นเครื่องขโมยข้อมูลขนาดเล็กที่สามารถพกพาได้ มิจฉาชีพจะใช้เล่ห์เหลี่ยมขอบัตรจากเหยื่อ เช่น แฝงตัวเป็นพนักงานเก็บเงินในร้านค้า หรืออ้างเป็นเจ้าหน้าที่ธนาคารที่คอยให้ความช่วยเหลือที่หน้าเครื่องเอทีเอ็ม เมื่อเหยื่อเผลอ ก็จะนำบัตรมารูดกับเครื่องขโมยข้อมูลที่ซ่อนไว้

2. ปลอมเอกสารสมัครบัตร/บัญชีสินเชื่อ

มิจฉาชีพจะขโมยเอกสารส่วนตัวของเหยื่อ เช่น สำเนาบัตรประจำตัวประชาชน แล้วนำไปสมัครบัตรเครดิตหรือบัตรกดเงินสด หรืออาจนำเอกสารดังกล่าวไปแจ้งเปลี่ยนบัตรพร้อมทั้งเปลี่ยนที่อยู่ในการส่งบิลเรียกเก็บ แล้วนำบัตรไปใช้ในนามของเหยื่อกว่าเหยื่อจะรู้ตัวก็โดนทวงหนี้แล้ว

3. ขโมยข้อมูลจากใบบันทึกรายการ (ATM Slip)

มิจฉาชีพจะเลือกใบบันทึกรายการที่ตกอยู่บริเวณเครื่องเอทีเอ็ม โดยเลือกใบบันทึกรายการที่มียอดเงินคงเหลือมาก ๆ หลังจากนั้นจะนำข้อมูลในใบบันทึกรายการไปหาข้อมูลส่วนตัวของเหยื่อเพื่อใช้ทำบัตรประจำตัวปลอม (ที่มีรูปเป็นของมิจฉาชีพแต่ชื่อเป็นของเหยื่อ)

เมื่อได้บัตรประจำตัวปลอมที่มีรูปเป็นของมิจฉาชีพแต่ชื่อเป็นของเหยื่อแล้ว มิจฉาชีพจะนำบัตรนั้นไปขอเปิดบัญชีเงินฝากและทำบัตรเอทีเอ็มเพิ่มในชื่อของเหยื่อ พร้อมทั้งขอเปิดบริการธนาคารออนไลน์กับบัญชีเงินฝากที่เป็นของเหยื่อจริง ๆ ทุกบัญชี แล้วโอนเงินทั้งหมดมาไว้ในบัญชีที่เปิดใหม่ แล้วถอนออกด้วยบัตรเอทีเอ็มที่เพิ่งเปิดใหม่

วิธีป้องกันภัยบัตรอิเล็กทรอนิกส์

1. ไม่บอกข้อมูลส่วนตัวแก่บุคคลอื่น ไม่ว่าจะเป็นรหัสบัตรเอทีเอ็ม บัตรเครดิต หรือข้อมูลทางการเงิน หรือให้คนอื่นทำธุรกรรมแทน

2. สังเกตเครื่องเอทีเอ็ม ว่ามีสิ่งแปลกปลอมติดอยู่ที่ช่องสอดบัตร แป้นกดตัวเลข และบริเวณโดยรอบว่ามีกล้องขนาดจิ๋วแอบดูการกดรหัสหรือไม่

3. เปลี่ยนรหัสผ่านอย่างน้อยทุก 3 เดือน หรือบ่อยกว่า โดยรหัสผ่านจะต้องเดายาก เป็นความลับ แต่เจ้าของบัตรต้องจำได้

4. อยู่ในระยะที่มองเห็นการทำรายการเมื่อใช้บัตรที่ร้านค้า เพื่อป้องกันพนักงานนำบัตรไปรูดกับเครื่องขโมยข้อมูล

5. ตรวจสอบใบบันทึกรายการของบัตรเอทีเอ็มทุกครั้ง และควรเก็บไว้เพื่อเป็นหลักฐานในการตรวจสอบ

6. ตรวจสอบรายการใช้จ่ายของบัตรเครดิตอย่างสม่ำเสมอ

7. แจ้งธนาคารผู้ออกบัตรทันที หากมีรายการผิดปกติ

ทำอย่างไรเมื่อตกเป็นเหยื่อภัยบัตรอิเล็กทรอนิกส์

1. หากพบรายการถอนเงินหรือโอนเงินผิดปกติ ควรแจ้งอายัดบัตรทันที พร้อมทั้งตรวจสอบรายการและยอดเงินคงเหลือ

2. หากถูกขโมยข้อมูลจากเครื่อง skimmer ที่ติดอยู่กับเครื่องเอทีเอ็มของธนาคาร ให้ปฏิบัติดังนี้

1) ทบทวนเหตุการณ์ที่เกิดขึ้น แล้วรีบติดต่อฝ่ายบริการลูกค้า (call center) ของธนาคารเพื่ออายัดบัตร และขอทราบวิธีการและขั้นตอนการแก้ไขปัญหา ทั้งนี้ แต่ละธนาคารมีวิธีปฏิบัติที่แตกต่างกันไป

2) รวบรวมข้อมูลที่เกี่ยวข้อง เช่น ตำแหน่งที่ตั้งเครื่องเอทีเอ็ม และไปแจ้งความ ณ สถานีตำรวจในท้องที่ที่เกิดเหตุ

ทั้งนี้ หากพิสูจน์แล้วว่าลูกค้าดำเนินการตามขั้นตอนปกติและสูญเสียเงินจากการที่บุคคลภายนอกใช้เครื่อง skimmer ติดกับเครื่องเอทีเอ็มและลักลอบบันทึกข้อมูลในแถบแม่เหล็กหรือกระทำทุจริตอื่น ๆ จนเกิดความสูญเสียต่อลูกค้า ธนาคารจะต้องรับผิดชดใช้ความสูญเสียให้แก่ลูกค้ารายนั้น (ตามประกาศ ธปท. เลขที่ สนส. 26/2551 เรื่อง การอนุญาตให้ธนาคารพาณิชย์ให้บริการการเงินทางอิเล็กทรอนิกส์ ลงวันที่ 3 สิงหาคม 2551)

3. **แจ้งเบาะแส** แก่เจ้าหน้าที่ตำรวจเพื่อติดตามคนร้าย

กิจกรรมท้ายเรื่องที่ 7 ภัยบัตรอิเล็กทรอนิกส์

(ให้ผู้เรียนไปทำกิจกรรมท้ายเรื่องที่ 1 ที่สมุดบันทึกกิจกรรมการเรียนรู้)