บทที่ 4
รู้ทันภัยทางการเงิน . . .
ตั้งสติไว้ไม่โดนหลอก

ระยะเวลาทั้งหมด : 60 นาที

- แชร์ลูกโซ่...คุยโม้ว่าลงทุนแล้วรวยเร็ว
- แก๊ง Call center ...รับสายแล้วเผลอเชื่อ ตกเป็นเหยื่อไม่ได้เงินคืน
- โจรในโลกออนไลน์ (ไซเบอร์)...รับมือ อย่างไร แล้วจะปลอดภัย

Slide (25 นาที)

กิจกรรมที่ 4.1
เกมไฟเขียว-ไฟเหลือง-ไฟแดง
(10 นาที)

กิจกรรมที่ 4.2
เล่น เล่า เท่าทันภัยทางการเงิน
(25 นาที)

บทที่ 4

รู้ทันภัยทางการเงิน...ตั้งสติไว้ ไม่โดนหลอก

ระยะเวลา : 60 นาที

(เนื้อหาการสอน 25 นาที + กิจกรรมและการประเมินผล 35 นาที)

วัตถุประสงค์การเรียนรู้ :

เพื่อให้ผู้เรียนรู้เท่าทันกลโกง พร้อมรับมือกับภัยทางการเงินรูปแบบต่าง ๆ ในปัจจุบัน และอาจปรับเปลี่ยนตามความก้าวหน้าของเทคโนโลยีในอนาคต เพื่อไม่ให้ตกเป็นเหยื่อของแก๊งมิจฉาชีพ

หัวข้อเนื้อหาสำหรับผู้สอน

1. แชร์ลูกโซ่...คุยโม้ว่าลงทุนแล้วรวยเร็ว
2. แก๊ง Call center...รับสายแล้วเผลอเชื่อ ตกเป็นเหยื่อไม่ได้เงินคืน
3. โจรในโลกออนไลน์ (ไซเบอร์)...รับมืออย่างไร แล้วจะปลอดภัย

Slide

http://www.1213.or.th/th/Documents/toolkits/PPT_4_FinancialFraud.pptx

ข้อมูลเพิ่มเติม

1. **แชร์ลูกโซ่**
   - http://www.1359.go.th/document/law.php
2. **แก๊ง Call center**
   - แก๊งคอลเซ็นเตอร์ เหิมหนัก อ้างเป็น ปปส.ภาค 6 หลอกโอนเงินล้มคดี วันเดียวเจอ 3 ราย (17 ต.ค. 60) : https://www.matichon.co.th/news-monitor/news_698988

- กสทช. คุมเข้มบล็อคเบอร์โทรปลอมแก๊งคอลเซ็นเตอร์ (12 ม.ค. 61) : https://www.dailynews.co.th/it/621131

3. **Online banking**
   - ใช้งาน Internet banking และ Mobile banking อย่างไรให้ปลอดภัย : https://www.it24hrs.com/2014/mobile-banking-safety/
   - วิธีใช้แอปธนาคารออนไลน์ ให้ปลอดภัยจากการโดนแฮกขโมยเงิน : https://www.it24hrs.com/2018/mobile-banking-online-banking-app-safety/
   - จะเกิดอะไรขึ้นหลังทำสมาร์ทโฟนหาย โดนขโมย หรือลืมไว้ เพราะอาจร้ายกว่าที่คิด : https://www.it24hrs.com/2017/what-happen-if-my-smartphone-lost/
4. **หลอก/จ้างให้เปิดบัญชีเงินฝาก**
   - คนรู้จักหลอกจ้างเปิดบัญชี อีก 3 ปีตำรวจบอกมีคดีฉ้อโกง 5 แสน –โดนไปเกือบทั้งหมู่บ้าน (21 เม.ย. 61) : https://www.khaosod.co.th/around-thailand/news_990332

ภัยทางการเงินหรือกลโกงที่มิจฉาชีพใช้หลอกเอาเงินจากเหยื่อได้มีการปรับเปลี่ยนให้ทันสมัยขึ้นตามความก้าวหน้าของเทคโนโลยี จนสร้างความเสียหายกับประชาชนในวงกว้างและมีมูลค่าความเสียหายเพิ่มขึ้น ดังนั้น ผู้ใช้บริการทางการเงินจะต้องมีความรอบคอบ มีสติรู้เท่าทันกลโกง เพื่อไม่ให้ตกเป็นเหยื่อของแก๊งมิจฉาชีพ

ผู้ใช้บริการทางการเงินจะต้องมีความรอบคอบ มีสติรู้เท่าทันกลโกง
เพื่อไม่ให้ตกเป็นเหยื่อของแก๊งมิจฉาชีพ

ในที่นี้ขอยกตัวอย่างภัยทางการเงินยอดฮิตที่คุณหรือคนใกล้ชิดเคยเจอหรือได้ยินข่าวกันมาบ้าง ได้แก่ แชร์ลูกโซ่ แก๊ง call center และโจรในโลกออนไลน์ (ไซเบอร์)

1. แชร์ลูกโซ่...คุยโม้ว่าลงทุนแล้วรวยเร็ว

แชร์ลูกโซ่ เป็นวิธีการหลอกลวงระดมเงินจากประชาชนที่ทำกันเป็นเครือข่าย โดยโฆษณาจูงใจว่าจะได้รับผลตอบแทนสูงกว่าการลงทุนทั่วไป แชร์ลูกโซ่มักแอบแฝงมากับธุรกิจขายตรงหรือการชักชวนให้ลงทุนในธุรกิจที่มีกำไรมาก และจะหาสมาชิกใหม่ไปเรื่อย ๆ เพื่อหมุนเงินค่าสมัครมาจ่ายผลตอบแทนให้สมาชิกเดิม

วิธีสังเกตว่าธุรกิจไหนเข้าข่ายแชร์ลูกโซ่ มีดังนี้

1. **เอาธุรกิจอื่นมาบังหน้า** รูปแบบที่พบบ่อย คือ **ชวนทำธุรกิจขายตรง** โดยรายได้หลักไม่ได้มาจากการขายสินค้า แต่มาจากการหาสมาชิกเพิ่ม ถ้ามีสินค้าก็มักเป็นของที่มีราคาแพงหรืออ้างสรรพคุณเกินจริง สินค้ายอดฮิตที่นำมาแอบอ้างให้คนหลงเชื่อ เช่น อาหารเสริมสุขภาพ เครื่องสำอาง และเครื่องประดับ นอกจากนี้ มักหว่านล้อมหรือใช้หลักจิตวิทยากระตุ้นความโลภ **ชวนลงทุนที่ให้ผลตอบแทนสูง** เช่น ถือหุ้นในบริษัทที่จะจดทะเบียนในตลาดหลักทรัพย์ เก็งกำไรราคาทองคำ น้ำมันดิบ อัตราแลกเปลี่ยนเงินต่างประเทศ (FOREX) สกุลเงินดิจิทัล (คริปโตเคอเรนซี) หรือบางกรณีหลอกให้สมัครสมาชิกฌาปนกิจสงเคราะห์ โดยอ้างว่าจะจ่ายเงินสงเคราะห์ให้จำนวนมากเมื่อเสียชีวิต

2. **การันตีผลตอบแทนสูงผิดปกติ** โดยมีค่าสมัครสมาชิกหรือเงินก้อนแรกที่ต้องจ่ายเป็นค่าซื้อสินค้าหรือเริ่มลงทุน ซึ่งนำไปจ่ายเป็นค่าตอบแทนให้สมาชิกรายเดิมเพื่อหลอกให้ลงทุนหรือหาสมาชิกใหม่ไปเรื่อย ๆ

3. **ชวนฟังสัมมนา/แผนธุรกิจ** ผ่านญาติ พี่น้อง คนรู้จัก หรือโฆษณาผ่านเว็บไซต์/Social Media โดยจัดฉากว่าธุรกิจมีความน่าเชื่อถือด้วยการจัดงานในสถานที่หรูหรา และแอบอ้างว่ามีดารา คนมีชื่อเสียง หรือหน่วยงานภาครัฐเกี่ยวข้องด้วย นอกจากนั้น มักมีการเชิญสมาชิกที่ประสบความสำเร็จมาแชร์ประสบการณ์เพื่อให้คล้อยตามแล้วจ่ายเงินสมัครสมาชิก

4. **ไม่เคยจบสวย** ในช่วงแรกธุรกิจมักจ่ายผลตอบแทนให้สมาชิกได้ตามที่การันตี แต่ผ่านไปสักระยะ หากหาสมาชิกใหม่ไม่ได้จะเกิดปัญหาหมุนเงินไม่ทัน จนเลื่อนเวลาการจ่ายเงินสมาชิกเก่าออกไป สุดท้ายแชร์ก็ล้ม ไม่มีเงินจ่ายคืนให้สมาชิก และปิดกิจการหายตัวไปติดต่อ

Tips

คริปโตเคอเรนซี เช่น บิตคอยน์ เป็นสินทรัพย์ที่มีการซื้อ ขาย โอน แลกเปลี่ยน ทางออนไลน์ ซึ่งมีความผันผวนและความเสี่ยงสูง โดยมีมูลค่าเปลี่ยนแปลงอย่างรวดเร็ว ปัจจุบัน คริปโตเคอเรนซีไม่ถือเป็นเงินที่สามารถใช้ชำระหนี้ได้ตามกฎหมายไทย ดังนั้น หากไม่เข้าใจความเสี่ยงและที่มาของผลตอบแทนอย่างชัดเจน ควรหลีกเลี่ยงการลงทุน

ไม่ได้...**แต่แชร์ลูกโซ่ไม่เคยตาย** และจะกลับมาพร้อมมุกใหม่หลอกเหยื่อกลุ่มใหม่ให้ติดกับดัก จนเกิดความเสียหายเป็นข่าวดังอีกครั้ง

ป้องกันอย่างไรไม่ให้ถูกหลอก 5 สิ่งที่คุณควรทำเพื่อกันภัยจากแชร์ลูกโซ่ คือ

1. **ไม่โลภ** จำให้ขึ้นใจว่าผลตอบแทนสูงมาพร้อมกับความเสี่ยงที่สูงด้วย ดังนั้น ก่อนตัดสินใจลงทุน ควรคิดให้รอบคอบ นึกถึงโอกาสที่จะสูญเสียเงินต้น อย่ามองแต่โอกาสจะได้ผลตอบแทนสูงเพียงอย่างเดียว
2. **ไม่หูเบา** ไม่ให้ข้อมูลส่วนตัวในเว็บไซต์หรืออีเมลแก่คนที่ไม่รู้จักหรือไม่น่าเชื่อถือ
3. **ไม่คล้อยตาม** ปฏิเสธเมื่อถูกชักชวนให้ลงทุนในสิ่งที่ไม่เข้าใจหรือไม่แน่ใจ
4. **ไม่ใจร้อน** ศึกษาข้อมูลให้แน่ชัดก่อนลงทุน/ซื้อสินค้า
5. **ไม่หลงเชื่อ** ติดตามข่าวสารให้รู้ทันกลลวงใหม่ ๆ ของมิจฉาชีพ

ทำอย่างไรเมื่อสงสัยว่าเข้าข่ายถูกหลอกหรือตกเป็นเหยื่อแชร์ลูกโซ่

หากสงสัยว่าเข้าข่ายถูกหลอกให้ร่วมขบวนการแชร์ลูกโซ่ เช่น ได้รับเชิญให้เข้าร่วมธุรกิจขายตรง สามารถ**สอบถามเพิ่มเติมเรื่องธุรกิจขายตรง**ได้ที่สำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ. โทร. 1166) หรือ**ตรวจสอบการจดทะเบียนหรืองบการเงินของบริษัทที่ชักชวนให้ร่วมลงทุน**ได้ที่กรมพัฒนาธุรกิจการค้า (โทร. 1570) หรือสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต. โทร. 1207)

เมื่อตกเป็นเหยื่อหรือได้รับความเสียหายจากแชร์ลูกโซ่ ให้รวบรวมเอกสารทั้งหมดที่มี เช่น สัญญา หลักฐานการโอนเงิน ที่ตั้ง/เบอร์โทรสำนักงาน รูปถ่าย แล้ว**ขอคำปรึกษา**ได้ที่ศูนย์รับแจ้งการเงินนอกระบบ กระทรวงการคลัง (โทร. 1359) หรือ**แจ้งความร้องทุกข์**ได้ที่กรมสอบสวนคดีพิเศษ (DSI โทร. 1202)

2. แก๊ง Call center...รับสายแล้วเผลอเชื่อ ตกเป็นเหยื่อไม่ได้เงินคืน

แก๊ง Call center ทำงานกันเป็นทีม โดยจะสุ่มเบอร์เพื่อโทรศัพท์ไปหาเหยื่อหรือใช้ข้อความอัตโนมัติ และ**แอบอ้างว่าเป็นเจ้าหน้าที่ของรัฐ ตำรวจ หรือพนักงานธนาคาร เพื่อหลอกให้เหยื่อตกใจกลัว ตื่นเต้นดีใจ หรือเกิดความโลภ จนหลงเชื่อแล้วรีบไปทำรายการที่ตู้ ATM ตามคำบอกโดยไม่ทันรู้ตัวว่ากำลังโอนเงินให้มิจฉาชีพ**

ข้ออ้างที่มิจฉาชีพมักใช้หลอกเหยื่อ เช่น

1. **หลอกให้ตกใจโดยอ้างว่า**

- **เป็นตำรวจ/เจ้าหน้าที่ ป.ป.ส.** (สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด) **หรือเจ้าหน้าที่ ปปง.** (สำนักงานป้องกันและปราบปรามการฟอกเงิน) **หลอกว่าเหยื่อเกี่ยวข้องกับยาเสพติด/การฟอกเงิน จะต้องถูกอายัดบัญชีเงินฝากและดำเนินคดี** จึงให้เหยื่อโอนเงินมาเพื่อตรวจสอบประวัติทางการเงิน แล้วจะโอนเงินคืนให้เมื่อตรวจสอบเสร็จ ในกรณีนี้มิจฉาชีพมักห้ามเหยื่อบอกผู้อื่นโดยอ้างว่าจะทำให้เสียรูปคดี แต่แท้จริงแล้วเพื่อป้องกันไม่ให้เหยื่อได้ตรวจสอบความจริง

- **เป็นพนักงานธนาคาร/เจ้าหน้าที่แบงก์ชาติ หลอกว่าเหยื่อจะถูกอายัดบัญชี/มีหนี้บัตรเครดิตค้างชำระ** แล้วบอกให้โอนเงินโดยอ้างว่าเป็นการทำรายการแก้ไขตัวเลขหนี้สินให้ถูกต้อง รวมถึงหลอกให้เปิดบัญชีและทำบัตร ATM ใหม่ แล้วขอให้แจ้งเลขบัตร ATM และส่งเอกสารมาให้ เพื่อจะได้ออกหนังสือรับรองว่าไม่มีหนี้ค้างชำระ แต่พอทำตาม เงินในบัญชีที่เปิดใหม่จะถูกมิจฉาชีพแอบถอนออกไป

2. **หลอกให้ตื่นเต้นดีใจโดยอ้างเป็นเจ้าหน้าที่สรรพากร หลอกว่าเหยื่อได้เงินคืนภาษี** แล้วให้ไปทำรายการที่ตู้ ATM ด่วนภายในวันนี้เพื่อรับเงินคืนภาษี หรือ**อ้างเป็นบริษัทเอกชนหลอกว่าเหยื่อได้รับรางวัลใหญ่จากการชิงโชค** แต่ต้องโอนเงินค่าภาษีมาก่อน แล้วจะส่งมอบรางวัลต่อไป แต่พอทำตามก็จะเสียเงินในบัญชีไป โดยไม่ได้เงินคืนภาษีหรือรางวัลใหญ่อะไรเลย

Clip

รวมมุกหลอกของแก๊ง Call center (1.06 นาที): https://bit.ly/2CiCPeM

ที่มา: สำนักงานตำรวจแห่งชาติ

Tips

ตัวอย่างกลลวงของแก๊ง Call center

- **หลอกถามข้อมูลส่วนตัวของเหยื่อ** เช่น วันเดือนปีเกิด เลขที่บัตรประชาชน เลขที่บัญชีเงินฝาก เลขบัตร ATM/บัตรเครดิต Username หรือ Password สำหรับใช้บริการ Online banking เพื่อนำไปขโมยเงินออกจากบัญชี หรือสมัครขอใช้บริการทางการเงินในชื่อของเหยื่อ เช่น กู้เงิน หรือเปิดบัญชีเพื่อรับเงินไม่สุจริต
- **จ้างหรือหลอกให้ผู้อื่นเปิดบัญชีเงินฝากธนาคารและทำบัตร ATM เพื่อใช้รับเงินที่เหยื่อโอนมา** โดยไม่มีหลักฐานผูกมัดตนเอง แต่เจ้าของบัญชีอาจถูกดำเนินการตามกฎหมายทั้งคดีอาญาฐานเป็นผู้สนับสนุนการกระทำความผิด และคดีฟอกเงิน

3. **หลอกให้สงสาร** โดยแอบนำเอกสารหรือข้อมูลส่วนตัวของเหยื่อไปใช้ยื่นกู้ในชื่อของเหยื่อโดยที่เหยื่อไม่รู้ตัว เมื่อธนาคารอนุมัติและโอนเงินกู้เข้าบัญชีของเหยื่อ มิจฉาชีพจะโทรไปหาเหยื่อโดย**อ้างว่าโอนเงินผิดเข้าบัญชี** และขอให้เหยื่อรีบโอนเงินคืน เมื่อเหยื่อตรวจสอบว่ามีเงินเข้ามาจริง จึงรีบโอนเงินคืนให้โดยไม่รู้ว่าเงินนั้นเป็นสินเชื่อที่มิจฉาชีพกู้มาในชื่อของตน ทำให้ต้องชดใช้หนี้ก้อนนั้นแทนมิจฉาชีพที่ได้เงินไปแล้ว

ป้องกันอย่างไรไม่ให้แก๊ง Call center หลอก แม้จะได้รับโทรศัพท์ที่อ้างว่าเป็นเจ้าหน้าที่ของรัฐหรือพนักงานธนาคาร ก็ต้องตั้งสติให้ดี เพราะหากหลงเชื่อให้ข้อมูลทางการเงินหรือโอนเงินไป มิจฉาชีพก็จะถอนเงินและหลบหนีไปทันที ทำให้คุณแทบไม่มีโอกาสได้รับเงินคืนเลย ดังนั้น คุณควรมีวิธีการป้องกันดังนี้

1. **คิดทบทวนอย่างมีสติ** เช่น เคยยื่นขอคืนภาษี เปิดบัญชีธนาคาร มียอดค้างชำระหนี้บัตรเครดิต หรือร่วมชิงรางวัลกับหน่วยงานที่โทรมาแอบอ้างจริงหรือไม่

2. **ไม่ให้ข้อมูลส่วนตัว** เพราะหน่วยงานรัฐหรือธนาคารมีข้อมูลของประชาชนหรือลูกค้าอยู่แล้ว และจำไว้ว่าหน่วยงานรัฐหรือธนาคารไม่มีนโยบายโทรไปสอบถามข้อมูลส่วนตัว ยกเว้นกรณีคุณโทรไปติดต่อหน่วยงานนั้น คุณอาจต้องตอบข้อมูลส่วนตัวเพื่อยืนยันตัวตนก่อน

3. **ไม่ทำรายการตามคำบอก** เพราะอาจถูกหลอกให้โอนเงินไปให้มิจฉาชีพโดยไม่รู้ตัว เช่น หลอกให้ทำรายการที่ตู้ ATM โดยเปลี่ยนหน้าจอเป็นภาษาอื่น หรือเร่งให้กดเร็ว ๆ จนอ่านไม่ทัน

4. **ไม่รีบร้อนโอนเงินให้คนอื่น** เพราะหากเป็นการโอนผิดบัญชีจริง ควรให้ธนาคารเป็นผู้แก้ไขรายการเพื่อโอนคืนเท่านั้น

5. **ตรวจสอบก่อนทำรายการ** โดยสามารถสอบถาม Call center ของหน่วยงานหรือธนาคารที่ถูกอ้างถึงโดยตรง หรือไปติดต่อที่สาขาธนาคาร

Tips

มิจฉาชีพอาจใช้โปรแกรม **เพื่อเปลี่ยนเบอร์โทรศัพท์เป็นเบอร์ Call center ธนาคาร** หรือเลือกที่จะ**ไม่แสดงเบอร์โทรเข้า** (Private number) บนหน้าโทรศัพท์มือถือของเหยื่อ **หรือแสดงหมายเลขที่ยาวกว่าปกติ** เพื่อให้เหยื่อหลงเชื่อว่าเป็นเบอร์ที่โทรมาจากต่างประเทศตามที่แอบอ้าง

ในทางกลับกัน แก๊ง Call center ที่อยู่ในต่างประเทศอาจใช้โทรศัพท์ผ่านระบบอินเทอร์เน็ตเพื่อเพิ่มความแนบเนียนในการหลอกลวงผู้เสียหาย โดย **กำหนดให้หมายเลขที่แสดงบนหน้าจอโทรศัพท์มือถือเป็นหมายเลขเดียวกับเบอร์โทรศัพท์ของหน่วยงานที่มิจฉาชีพอ้าง**

ดังนั้น หากได้รับการติดต่อทางโทรศัพท์โดยผู้โทรอ้างเป็นเจ้าหน้าที่รัฐ หรือพนักงานธนาคาร ต้องตรวจสอบหมายเลขโทรศัพท์ที่โทรเข้ามาให้แน่ใจก่อน เช่น **โทรถาม Call center ของหน่วยงานนั้น ๆ โดยตรง**

ทำอย่างไรเมื่อตกเป็นเหยื่อแก๊ง Call center สิ่งแรกที่คุณต้องทำ คือ **รีบติดต่อธนาคาร**ที่คุณมีบัญชี เพื่อระงับการโอนและถอนเงิน หลังจากนั้นรวบรวมเอกสารที่เกี่ยวข้อง แล้ว **รีบแจ้ง ปปง.** ทันที (โทร. 1710) และหากมีข้อสงสัย สามารถสอบถามและขอคำปรึกษาเพิ่มเติมได้จาก**ธนาคารแห่งประเทศไทย** (ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน โทร. 1213)

3. โจรในโลกออนไลน์ (ไซเบอร์)...รับมืออย่างไร แล้วจะปลอดภัย

กลลวงต่าง ๆ ที่โจรในโลกออนไลน์มักนำมาใช้เพื่อหลอกถามข้อมูล หรือหลอกให้โอนเงิน มีดังนี้

1. **ปลอมเป็นธนาคาร** ส่ง SMS หรืออีเมลหลอกเหยื่อ (Phishing) ว่าได้รับรางวัลหรือบัญชีกำลังจะถูกอายัด จึงจำเป็นต้องอัปเดตข้อมูลที่ธนาคารมีอยู่ให้เป็นปัจจุบัน โดยให้เหยื่อกรอกข้อมูลในเว็บไซต์ธนาคารปลอมหรือแอปพลิเคชันปลอม (หน้าตาคล้ายของจริง) ที่แนบมาใน SMS หรืออีเมล เพื่อ**หลอกถามข้อมูลส่วนตัว หรือฝังมัลแวร์ขโมย Username และ Password ในการทำรายการผ่าน Online banking** แล้วนำไปใช้ขโมยเงินออกจากบัญชี

2. **สวมรอยเป็นคุณใน Social media** (เช่น Facebook หรืออีเมล) เพื่อหลอกครอบครัวหรือเพื่อนว่ากำลังเดือดร้อน ขอให้โอนเงินมาช่วยด่วน

3. **หลอกว่ารัก (Romance scam)** เริ่มจากการติดต่อผ่านเว็บไซต์หาคู่หรือ Social media โดยใช้รูป Profile เป็นชาวต่างชาติหน้าตาดี พอพูดคุยสักระยะจนเหยื่อตายใจหรือมีความหวังก็จะหลอกเหยื่อว่าจะมอบทรัพย์สินหรือของขวัญให้ แต่เหยื่อต้องโอนเงินบางส่วนให้ก่อน เช่น จะให้เงินมาซื้อบ้านในเมืองไทยแต่โอนไม่ได้ เพราะต้องจ่ายค่าธรรมเนียม จึงหว่านล้อมให้เหยื่อโอนค่าธรรมเนียมไปให้ก่อน แต่เมื่อโอนไปแล้วก็ติดต่อไม่ได้อีกเลย

4. **ปลอมเป็นร้านค้าออนไลน์** โฆษณาขายสินค้าที่หายากหรือมีราคาถูกกว่าท้องตลาดมาก โดยขอให้เหยื่อโอนค่าสินค้ามาก่อน แต่กลับไม่ส่งสินค้าให้และหนีหายไป

ป้องกันอย่างไรไม่ให้เป็นเหยื่อโจรในโลกออนไลน์ นอกจากความรอบคอบมีสติ และละเอียดถี่ถ้วนในการใช้งานแล้ว คุณควรป้องกันภัยที่มาจากโลกออนไลน์ ดังนี้

1. **จำกัดวงเงินการโอนต่อครั้งหรือต่อวัน** และ**แยกบัญชีที่ใช้ทำรายการออนไลน์ออกจากบัญชีเงินออม** เพื่อลดความเสียหายหากถูกขโมยเงิน

2. **ดูแลคอมพิวเตอร์หรือสมาร์ทโฟนให้ปลอดภัย** เพื่อป้องกันโจรคัดลอกข้อมูล โดยใช้โปรแกรมป้องกันไวรัส ไม่ใช้โปรแกรมเถื่อน ไม่ Jailbreak/Root สมาร์ทโฟน ตั้งรหัสล็อคหน้าจอ ใช้ 3G, 4G ในการทำธุรกรรมทางการเงินแทน Free wifi หรือหลีกเลี่ยงการใช้คอมพิวเตอร์สาธารณะ เพราะอาจถูกดักจับ Username และ Password หรืออนุญาตให้เครื่องจำข้อมูลโดยไม่ตั้งใจ

3. **คิดก่อนคลิก-ใช้เว็บไซต์/แอปพลิเคชันที่ปลอดภัย** ก่อนเปิดลิงก์ ไฟล์แนบ หรือดาวน์โหลดแอปพลิเคชันที่ผู้ส่งอ้างว่าเป็นธนาคาร ต้องตรวจสอบให้ดีว่าผู้ส่งเป็นธนาคารจริงหรือไม่ และพิมพ์ชื่อเว็บไซต์ธนาคารเองแทนการค้นหาจาก Google ซึ่งสามารถสังเกตเว็บไซต์ที่ปลอดภัยได้จาก https://.... ที่มีรูปแม่กุญแจล็อก 

เพื่อหลีกเลี่ยงเว็บไซต์ปลอมที่หลอกขโมยข้อมูล รวมทั้งควรดาวน์โหลดแอปพลิเคชันด้วยตนเองผ่านทาง App Store หรือ Google Play หรือให้เจ้าหน้าที่ธนาคารแนะนำ

4. **ตั้ง Username หรือ Password ให้เดายาก แต่จำได้แม่น** ควรเปลี่ยน Password สม่ำเสมอ และเมื่อเลิกใช้งานอย่าลืม Log out ทุกครั้ง นอกจากนี้ อย่าใช้ Password เดียวกันทุกที่ (Online banking/ อีเมล/ Social media) ห้ามบอก Username หรือ Password แก่ผู้อื่น รวมทั้งไม่ตั้งค่าให้คอมพิวเตอร์หรือสมาร์ทโฟนจำ Password และถ้าเป็นไปได้คุณควรมีอีเมลสำรองสำหรับกู้คืนบัญชี หรือรีเซ็ต Password

5. **ตรวจสอบความถูกต้องก่อนยืนยันการทำรายการทุกครั้ง และตรวจความเคลื่อนไหวของเงินในบัญชี** ทั้งรายการใช้จ่าย การโอนเงิน และยอดเงินคงเหลือผ่าน SMS หรืออีเมลที่ลงทะเบียนให้ธนาคารแจ้งเตือน

Tips

ทำอย่างไรเมื่อโทรศัพท์มือถือหาย เพื่อลดความเสี่ยงที่ข้อมูลส่วนตัวจะรั่วไหล ถูกสวมรอยหรือถูกขโมยเงินจากบัญชี ให้รีบ**ระงับการใช้บริการ Mobile banking และเปลี่ยน Password ใหม่ทันที**ทั้งอีเมลและ Social media ต่าง ๆ หลังจากนั้นคุณอาจตามหาพิกัดของโทรศัพท์มือถือ (ถ้าตั้งค่าเปิดใช้งานไว้) และแจ้งความเพื่อป้องกันกรณีมีคนนำโทรศัพท์มือถือไปใช้ผิดกฎหมายในภายหลัง

6. **รีบติดต่อธนาคารหากพบรายการผิดปกติ หรือเปลี่ยนเบอร์โทรศัพท์ อีเมล หรือที่อยู่**

7. **เปิดเผยข้อมูลส่วนตัวใน Social media เท่าที่จำเป็น และติดตามข่าวสารอยู่เสมอ**

ทำอย่างไรเมื่อตกเป็นเหยื่อโจรในโลกออนไลน์ หากคุณเผลอคลิกลิงก์เปิดไฟล์แนบในอีเมลปลอม ดาวน์โหลดโปรแกรมที่น่าสงสัย หรือพบเหตุการณ์ผิดสังเกต เช่น ยอดเงินในบัญชีลดลงหรือได้รับ One Time Password (OTP) ทั้ง ๆ ที่คุณไม่ได้ทำธุรกรรม ให้รีบติดต่อธนาคารทันที

กิจกรรมที่ 4.1 เกมไฟเขียว-ไฟเหลือง-ไฟแดง

ผู้เรียนจะได้เข้าใจภัยทางการเงินรูปแบบต่าง ๆ ที่มีอยู่ในปัจจุบัน และรู้จักวิธีป้องกันหรือหลีกเลี่ยงการตกเป็นเหยื่อของมิจฉาชีพ

Tips

OTP เพิ่มความปลอดภัยในการใช้งานได้อย่างไร

OTP เป็นรหัสผ่านที่ใช้ได้เพียงครั้งเดียว ซึ่งธนาคารส่งให้กับผู้ใช้งานทาง SMS ผ่านเบอร์โทรศัพท์มือถือที่ลงทะเบียนไว้เมื่อจะทำธุรกรรมทางการเงินด้วย Online banking โดยมีระยะเวลาการใช้งานจำกัด ซึ่ง OTP จะช่วยเพิ่มความปลอดภัยในการพิสูจน์ตัวตนผู้ใช้งานเพิ่มเติมจากการระบุ Username และ Password

อย่างไรก็ตาม บางธนาคารอาจให้ผู้ใช้งานทำรายการบางประเภทได้โดยไม่ต้องใช้ OTP เช่น จ่ายบิล เติมเงินโทรศัพท์ หรือโอนเงินให้ตนเอง

กิจกรรมที่ 4.2 เล่น เล่า เท่าทันภัยทางการเงิน

ผู้เรียนจะได้มีความรู้ความเข้าใจ สามารถตัดสินใจและปฏิบัติตนได้อย่างเหมาะสม เมื่อเผชิญกับภัยทางการเงินที่อาจเกิดขึ้นในชีวิตประจำวัน

ผู้สอนสามารถวัดความรู้ความเข้าใจ (Awareness) และการฝึกปฏิบัติ (Practice) ของผู้เรียนในการนำความรู้ที่ได้รับมาประยุกต์ใช้ในการตัดสินใจ และการจัดการกับภัยทางการเงิน

กิจกรรมที่ 4.1 เกมไฟเขียว-ไฟเหลือง-ไฟแดง (ประมาณ 10 นาที)

วัตถุประสงค์

เพื่อให้ผู้เรียนเข้าใจภัยทางการเงินรูปแบบต่าง ๆ ที่มีอยู่ในปัจจุบัน และรู้จักวิธีป้องกันหรือหลีกเลี่ยงการตกเป็นเหยื่อของมิจฉาชีพ

อุปกรณ์/ สิ่งที่ต้องเตรียม

ใบกิจกรรม “เกมไฟเขียว-ไฟเหลือง-ไฟแดง” ตามจำนวนกลุ่มผู้เรียน

วิธีการ

1. ผู้สอนแบ่งผู้เรียนเป็นกลุ่ม กลุ่มละ 5 คน (อาจเปลี่ยนแปลงได้ตามความเหมาะสม)
2. ผู้สอนแจกใบกิจกรรมให้ผู้เรียนและชี้แจงวิธีการทำกิจกรรมดังนี้

2.1 อธิบายความหมายของสัญลักษณ์ไฟเขียว ไฟเหลือง และไฟแดง

- **ไฟเขียว** หมายถึง ความปลอดภัย เป็นพฤติกรรมที่ดี ควรทำต่อ (Continue)
- **ไฟเหลือง** หมายถึง สถานการณ์ที่เป็นจุดตัดสินใจ ควรระมัดระวัง (Beware)
- **ไฟแดง** หมายถึง ความเสี่ยง เป็นพฤติกรรมที่เสี่ยง ควรหลีกเลี่ยง/ หยุดทำ (Stop)

2.2 ให้ผู้เรียนแต่ละกลุ่ม**เลือกเหตุการณ์กลโกง**ดังต่อไปนี้ **(1) แชร์ลูกโซ่ (2) แก๊ง Call center หรือ (3) โจรในโลกออนไลน์ (ไซเบอร์)** มา 1 เหตุการณ์ (ทั้งห้องต้องเลือกครบ 3 เหตุการณ์ เพื่อให้มีความหลากหลาย) และระบุรายละเอียดของเหตุการณ์ที่มิจฉาชีพมักใช้หลอกเหยื่อ โดยผู้เรียนสามารถค้นหาข้อมูล/ ข่าวสารเพิ่มเติมได้จากอินเทอร์เน็ตเพื่อให้ได้ข้อมูลสมจริงและทันเหตุการณ์ รวมทั้งส่งเสริมให้เกิดการเรียนรู้ด้วยตนเอง

2.3 ให้ผู้เรียนแต่ละกลุ่ม**สวมบทบาท (Roleplay) เป็นเหยื่อของแก๊งมิจฉาชีพ** แล้วช่วยกันระดมความคิดเห็นและ**เขียนลงในใบกิจกรรมเกี่ยวกับสิ่งที่ควรทำ สิ่งที่ควรระวัง และสิ่งที่ควรหลีกเลี่ยง/ หยุดทำ** เพื่อป้องกันไม่ให้ตกเป็นเหยื่อ/ หลงเชื่อมิจฉาชีพ

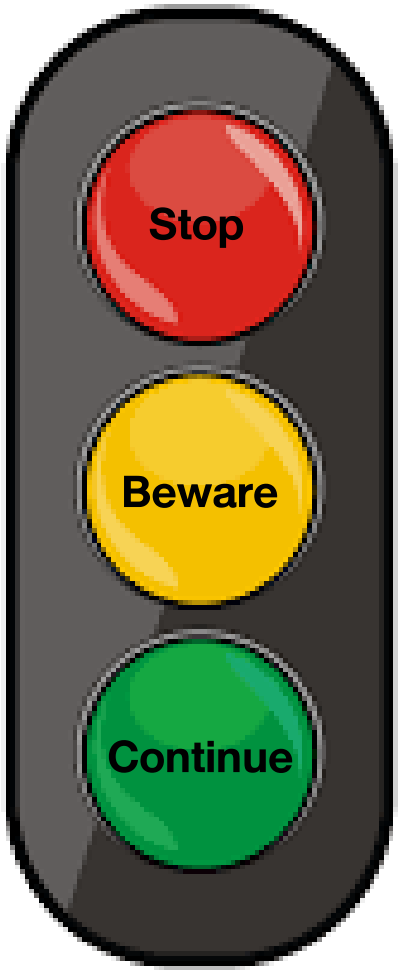
2.4 ให้ตัวแทนของผู้เรียนแต่ละกลุ่มนำเสนอ เพื่อแลกเปลี่ยนความคิดเห็นกับผู้เรียนกลุ่มอื่น ทั้งนี้หากมีเวลามากพอ ผู้สอนอาจให้ผู้เรียนวิเคราะห์สถานการณ์และเขียนลงในใบกิจกรรมเป็นรายบุคคลแล้วแลกเปลี่ยนความเห็นกับผู้เรียนคนอื่น

3. ผู้สอนอธิบายตัวอย่างเพิ่มเติม (ถ้ามี)

ใบกิจกรรม “เกมไฟเขียว-ไฟเหลือง-ไฟแดง” (สำหรับผู้เรียน)

เหตุการณ์ที่เลือก (เลือกเหตุการณ์เดียว)	☐ แชร์ลูกโซ่ ☐ แก๊ง Call center ☐ โจรในโลกออนไลน์ (ไซเบอร์)
รายละเอียดของเหตุการณ์	....
	**สิ่งที่ควรหลีกเลี่ยง/ หยุดทำ (Stop)** ● ..... ● ..... ● ..... ● ..... สิ่งที่ควรระวัง (Beware) ● ..... ● ..... ● ..... ● ..... สิ่งที่ควรทำ (Continue) ● ..... ● ..... ● ..... ● .....

แนวคำตอบกิจกรรม “เกมไฟเขียว-ไฟเหลือง-ไฟแดง” (สำหรับผู้สอน)

<table>
<tr><td>เหตุการณ์ที่เลือก (เลือกเหตุการณ์เดียว)</td><td>☑ แชร์ลูกโซ่
☐ แก๊ง Call center
☐ โจรในโลกออนไลน์ (ไซเบอร์)</td></tr>
<tr><td>รายละเอียดของเหตุการณ์</td><td>มีคนมาชวนไปฟังสัมมนา ชักชวนให้ลงทุนในผลิตภัณฑ์อาหารเสริมสุขภาพที่ให้ผลตอบแทนสูง 20% ต่อเดือน โดยอ้างว่ามีดาราดังและข้าราชการชั้นผู้ใหญ่ร่วมทำธุรกิจนี้มาหลายปีแล้ว</td></tr>
<tr><td rowspan="3"> 
</td><td>สิ่งที่ควรหลีกเลี่ยง/ หยุดทำ (Stop)
ชวนเพื่อนรักไปงานสัมมนาและชักชวนให้ลงทุนด้วยกัน (ชวนกันรวย)
ถอนเงินฝากในบัญชีธนาคารมาลงทุน เพราะคาดหวังผลตอบแทนสูง โดยลืมว่าอาจสูญเสียเงินต้น (หวังผลสูง)
ให้ข้อมูลส่วนตัวในเว็บไซต์หรืออีเมลแก่คนที่ไม่รู้จักหรือไม่น่าเชื่อถือ</td></tr>
<tr><td>สิ่งที่ควรระวัง (Beware)
ไม่เชื่อในทันที ต้องตรวจสอบให้แน่ชัดว่า คนที่มาชวนให้ร่วมลงทุนเป็นใคร มาจากบริษัทอะไร บริษัทนั้นมีการจดทะเบียนการค้าถูกต้องหรือไม่</td></tr>
<tr><td>สิ่งที่ควรทำ (Continue)
ติดตามข่าวกลโกงจะได้รู้ทันมิจฉาชีพ
คิดให้รอบคอบ นึกถึงโอกาสที่จะสูญเสียเงินต้น อย่ามองแต่โอกาสจะได้ผลตอบแทนอย่างเดียว (ไม่แน่ใจ ไม่ลงทุน)</td></tr>
</table>

กิจกรรมที่ 4.2 เล่น เล่า เท่าทันภัยทางการเงิน (ประมาณ 25 นาที)

วัตถุประสงค์

1. เพื่อให้ผู้เรียนมีความรู้ความเข้าใจ สามารถตัดสินใจและปฏิบัติตนได้อย่างเหมาะสม เมื่อเผชิญกับภัยทางการเงินที่อาจเกิดขึ้นในชีวิตประจำวัน
2. เพื่อให้ผู้เรียนมีโอกาสวิเคราะห์ และแลกเปลี่ยนความคิดเห็นกับเพื่อนเกี่ยวกับภัยทางการเงินที่อาจเกิดขึ้นในชีวิตประจำวัน

อุปกรณ์/ สิ่งที่ต้องเตรียม

บัตรกิจกรรมที่ระบุสถานการณ์ภัยทางการเงินต่าง ๆ พร้อมคำถาม

วิธีการ

1. ผู้สอนแบ่งกลุ่มผู้เรียนออกเป็น 5 กลุ่ม (อาจเปลี่ยนแปลงได้ตามความเหมาะสม)
2. ผู้สอนแจกบัตรกิจกรรมกลุ่มละ 1 ใบ
3. ผู้สอนให้สมาชิกในแต่ละกลุ่มร่วมกันวิเคราะห์สถานการณ์ และตอบคำถามที่ได้รับจากบัตรกิจกรรม หลังจากนั้นให้แต่ละกลุ่มส่งตัวแทน เพื่อแสดงบทบาทสมมติเกี่ยวกับสถานการณ์ที่ได้รับ และตอบคำถามที่คิดวิเคราะห์ไว้ พร้อมอธิบายเหตุผลประกอบว่าควรปฏิบัติตนอย่างไรให้รอดพ้นจากการตกเป็นเหยื่อภัยทางการเงิน

คำแนะนำ

ผู้สอนสังเกตการวิเคราะห์ของผู้เรียนกลุ่มต่าง ๆ หากผู้เรียนยังไม่เข้าใจสถานการณ์ ผู้สอนอาจยกตัวอย่างข่าวที่เกิดขึ้นจริงในสังคมเพื่อให้ผู้เรียนเห็นภาพ โดยกระตุ้นให้ผู้เรียนคิดว่าหากเหตุการณ์ที่ยกตัวอย่างนั้นเกิดขึ้นกับตนเองแล้วจะปฏิบัติอย่างไร

ผู้สอนชี้แจงให้ผู้เรียนเห็นว่าเมื่ออยู่ในเหตุการณ์จริง ความตกใจ หรือความโลภอาจส่งผลต่อการตัดสินใจได้ ดังนั้น สิ่งที่สำคัญคือ การมีสติ คิดทบทวนเหตุการณ์อย่างรอบด้าน รวมถึงผู้สอนควรกระตุ้นให้ผู้เรียนศึกษาหาความรู้ และติดตามข่าวสารเรื่องภัยทางการเงินอย่างต่อเนื่อง

ผู้สอนอาจพิจารณาปรับสถานการณ์จำลองให้สอดคล้องกับเหตุการณ์ภัยทางการเงินที่เกิดขึ้นในช่วงที่สอนได้

การประเมินผล

วัตถุประสงค์ : เพื่อวัดความรู้ความเข้าใจ (Awareness) และฝึกปฏิบัติ (Practice) ของผู้เรียนในการนำความรู้ที่ได้รับมาประยุกต์ใช้ในการตัดสินใจ และการจัดการกับภัยทางการเงิน

วิธีการประเมินผล : ผู้สอนสังเกตพฤติกรรมของผู้เรียนในการคิดวิเคราะห์เพื่อตัดสินใจให้เหมาะสมในสถานการณ์ต่าง ๆ ผ่านการแสดงบทบาทสมมติ

เกณฑ์การประเมินผล : ผ่านการประเมิน เมื่อผู้เรียนให้เหตุผลได้อย่างเหมาะสม ทั้งนี้ ผู้สอนสามารถศึกษาแนวคำตอบกิจกรรม “เล่น เล่า เท่าทันภัยทางการเงิน” เพื่อใช้ประกอบการอธิบายผู้เรียนได้

บัตรกิจกรรม (สำหรับผู้เรียน)

1. **สถานการณ์ :** มีคนอ้างว่าเป็นเจ้าหน้าที่ธนาคารแห่งประเทศไทย หรือแบงก์ชาติ โทรมาขอข้อมูลชื่อจริง เลขประจำตัวประชาชน เลขที่บัญชีธนาคาร โดยแจ้งว่าบัญชีของคุณจะถูกอายัด ถ้าไม่ให้ข้อมูล เนื่องจากสงสัยว่าเกี่ยวข้องกับคดีค้ายาเสพติด

   คำถาม : คุณจะให้ข้อมูลส่วนตัวหรือไม่

2. **สถานการณ์ :** เพื่อนชวนไปลงทุนขายครีมหน้าใสนำเข้าจากเกาหลี บอกว่าไม่ต้องจ่ายเงินก้อนเพื่อซื้อสินค้ามาสต๊อก จ่ายแค่ค่าสมัครสมาชิก 1,000 บาท โพสต์รูปโปรโมทสินค้า และหาสมาชิกเพิ่มก็ได้เงินเดือนละเป็นหมื่น

   คำถาม : คุณจะสมัครสมาชิกตามคำชวนของเพื่อนหรือไม่

3. **สถานการณ์ :** ขณะเล่นเกมออนไลน์ มีลิงก์ให้ดาวน์โหลดโปรแกรมที่ไม่รู้จักซึ่งจะช่วยให้ได้เงินในเกมเพิ่มฟรี

   คำถาม : คุณจะกดลิงก์ดาวน์โหลดหรือไม่

4. **สถานการณ์ :** ได้รับอีเมลจากธนาคาร แจ้งว่าจะปรับปรุงระบบรักษาความปลอดภัย ให้คลิกลิงก์เพื่อยืนยันตัวตนเพื่อป้องกันไม่ให้บัญชีถูกอายัด

   คำถาม : คุณจะกดลิงก์และทำตามขั้นตอนเพื่อยืนยันตัวตนหรือไม่

5. **สถานการณ์ :** เพื่อนชาวต่างชาติที่รู้จักกันผ่าน Facebook บอกว่าส่งของขวัญซึ่งมีราคาสูงมาให้ แต่ของติดอยู่ที่ด่านศุลกากร ให้โอนเงินไปชำระค่าธรรมเนียมเพื่อรับของด่วน ถ้าไม่ทำจะถูกศุลกากรยึดของ

   คำถาม : คุณจะโอนเงินเพื่อชำระค่าธรรมเนียมหรือไม่

แนวคำตอบกิจกรรม “เล่น เล่า เท่าทันภัยทางการเงิน” (สำหรับผู้สอน)

1. **สถานการณ์ :** มีคนอ้างว่าเป็นเจ้าหน้าที่ธนาคารแห่งประเทศไทย หรือแบงก์ชาติ โทรมาขอข้อมูลชื่อจริง เลขประจำตัวประชาชน เลขที่บัญชีธนาคาร โดยแจ้งว่าบัญชีของคุณจะถูกอายัด ถ้าไม่ให้ข้อมูล เนื่องจากสงสัยว่าเกี่ยวข้องกับคดีค้ายาเสพติด

   คำถาม : คุณจะให้ข้อมูลส่วนตัวหรือไม่

   เฉลย : ไม่ให้ข้อมูลส่วนตัว เนื่องจากมิจฉาชีพมักแอบอ้างเป็นเจ้าหน้าที่เพื่อหลอกนำข้อมูลส่วนตัวของคุณไปใช้ในทางที่ผิดกฎหมาย และธนาคารแห่งประเทศไทยไม่มีนโยบายโทรไปสอบถามข้อมูลในลักษณะดังกล่าวกับประชาชน

2. **สถานการณ์ :** เพื่อนชวนไปลงทุนขายครีมหน้าใสนำเข้าจากเกาหลี บอกว่าไม่ต้องจ่ายเงินก้อนเพื่อซื้อสินค้ามาสต๊อก จ่ายแค่ค่าสมัครสมาชิก 1,000 บาท โพสต์รูปโปรโมทสินค้า และหาสมาชิกเพิ่มก็ได้เงินเดือนละเป็นหมื่น

   คำถาม : คุณจะสมัครสมาชิกตามคำชวนของเพื่อนหรือไม่

   เฉลย : ไม่สมัครสมาชิกตามคำชวนทันที หากสนใจควรศึกษาข้อมูลให้ถี่ถ้วนก่อน เนื่องจากธุรกิจที่ไม่เน้นการขายสินค้าแต่เน้นการหาเครือข่าย มีลักษณะเข้าข่ายเป็นแชร์ลูกโซ่

3. **สถานการณ์ :** ขณะเล่นเกมออนไลน์ มีลิงก์ให้ดาวน์โหลดโปรแกรมที่ไม่รู้จักซึ่งจะช่วยให้ได้เงินในเกมเพิ่มขึ้นฟรี

   คำถาม : คุณจะกดลิงก์ดาวน์โหลดหรือไม่

   เฉลย : ไม่กดลิงก์ดาวน์โหลด เนื่องจากอาจเสี่ยงเจอการขโมยข้อมูลผ่านมัลแวร์ที่ฝังมากับลิงก์ดังกล่าว

4. **สถานการณ์ :** ได้รับอีเมลจากธนาคาร แจ้งว่าจะปรับปรุงระบบรักษาความปลอดภัย ให้คลิกลิงก์เพื่อยืนยันตัวตนเพื่อป้องกันไม่ให้บัญชีถูกอายัด

   คำถาม : คุณจะกดลิงก์และทำตามขั้นตอนเพื่อยืนยันตัวตนหรือไม่

   เฉลย : ไม่กดลิงก์เนื่องจากธนาคารไม่มีนโยบายแนบลิงก์เข้าระบบออนไลน์มากับอีเมลเพื่อให้ลูกค้ากรอกข้อมูลส่วนตัว และควรแจ้งไปยังธนาคารว่าได้รับข้อมูลดังกล่าวด้วย

5. **สถานการณ์ :** เพื่อนชาวต่างชาติที่รู้จักกันผ่าน Facebook บอกว่าส่งของขวัญซึ่งมีราคาสูงมาให้ แต่ของติดอยู่ที่ด่านศุลกากร ให้โอนเงินไปชำระค่าธรรมเนียมเพื่อรับของด่วน ถ้าไม่ทำจะถูกศุลกากรยึดของ

   คำถาม : คุณจะโอนเงินเพื่อชำระค่าธรรมเนียมหรือไม่

   เฉลย : ไม่โอนเงินเพื่อชำระค่าธรรมเนียม หนึ่งในวิธีการที่มิจฉาชีพมักใช้ คือ การเข้ามาทำความรู้จักหรือเป็นเพื่อนกับเหยื่อ จากนั้นจะล่อลวงโดยอ้างว่าจะให้ของขวัญหรือเงินก้อนใหญ่ แต่ต้องจ่ายเงินเพื่อค่าขนส่งหรือค่าธรรมเนียมบางอย่าง เมื่อเหยื่อหลงเชื่อจ่ายเงินดังกล่าวไป มิจฉาชีพก็จะติดต่อไม่ได้ นอกจากคุณจะไม่ได้ของแล้วยังต้องเสียเงินอีกด้วย