ความรู้ทางการเงิน
กล่องสีแดง
(ระดับอาชีวศึกษา)

โครงงาน 3-Color Box

วิทยาลัยเทคโนโลยีภาคตะวันออกเฉียงเหนือ
จังหวัดขอนแก่น

สารบัญ

เรื่อง	หน้าที่
- มารู้เท่าตามทันภัยทางการเงิน เพื่อไม่ให้ตกเป็นเหยื่อของมิจฉาชีพ	1
- กลโกงทางโทรศัพท์	2-6
- กลโกงธนาคารออนไลน์	7-14
- กลโกงบัตรต่างๆ	15-18
- กลโกงออนไลน์อื่นๆ	19-26
- กลโกงอื่นๆ	27-45

“มารู้เท่าตามทันภัยทางการเงิน เพื่อไม่ให้ตกเป็นเหยื่อของมิจฉาชีพ”

“ภัยทางการเงินไม่ใช่สิ่งที่เพิ่งเกิดขึ้นใหม่แต่อยู่คู่กับ สังคมไทยมาช้านาน มุกที่ใช้หลอกก็มักจะเป็นมุกเดิม ๆ หรืออาจปรับเปลี่ยนให้ทันสมัยตามกาลเวลา โดย เป้าหมายหลักคือหลอกเงินจากเหยื่อ และด้วยความเจริญ ของเทคโนโลยีฉับช่องทางการให้บริการของสถาบัน การเงินที่มีมากขึ้น ทำให้ภัยทางการเงินในปัจจุบัน สร้างความเสียหายในวงกว้างขึ้น มูลค่าความเสียหายก็ เพิ่มสูงขึ้นเรื่อย ๆผู้ใช้บริการทางการเงินจึงต้องใช้บริการ อย่างรอบคอบและรู้เท่าทันกลโกง

กลโกงทางโทรศัพท์

ลักษณะกลโกง

มิจฉาชีพจะสุ่มเบอร์เพื่อโทรศัพท์ไปหาเหยื่อ และใช้ข้อความอัตโนมัติสร้างความตื่นเต้นหรือตกใจให้กับเหยื่อ บางครั้งก็แอบอ้างเป็นเจ้าหน้าที่หน่วยงานต่าง ๆ หลอกให้เหยื่อทำรายการที่ตู้เอทีเอ็มเป็นเมนูภาษาอังกฤษโดยแจ้งว่าทำเพื่อล้างรายการหนี้สิน หรืออาจหลอกให้เหยื่อไปโอนเงินให้หน่วยงานภาครัฐเพื่อตรวจสอบ ซึ่งมิจฉาชีพเหล่านี้จะอาศัยความกลัว ความโลภ และความรู้ไม่เท่าทันของเหยื่อ โดยข้ออ้างที่มิจฉาชีพมักใช้หลอกเหยื่อมีดังนี้

1. บัญชีเงินฝากถูกอายัด/หนี้บัตรเครดิต

ข้ออ้างที่มิจฉาชีพนิยมใช้มากที่สุด คือหลอกว่าเหยื่อถูกอายัดบัญชีเงินฝากและเป็นหนี้บัตรเครดิต เพราะเป็นเรื่องที่สามารถสร้างความตกใจและง่ายต่อการชักจูงเหยื่อให้โอนเงิน โดยมิจฉาชีพจะใช้ระบบตอบรับอัตโนมัติแจ้งเหยื่อว่าจะอายัดบัญชีเงินฝากเนื่องจากเหตุการณ์ต่าง ๆ เช่น เป็นหนี้บัตรเครดิตหรือกระทำการผิดกฎหมาย โดยอาจมีเสียงอัตโนมัติ เช่น "คุณเป็นหนี้บัตรเครดิตกับทางธนาคาร กด 0 เพื่อติดต่อพนักงาน" เมื่อเหยื่อตกใจ ก็จะรีบต่อสายคุยกับมิจฉาชีพทันที หลังจากนั้นมิจฉาชีพจะหลอกถามฐานะทางการเงินของเหยื่อ หากเหยื่อมีเงินจำนวนไม่มากนัก มิจฉาชีพจะหลอกให้เหยื่อโอนเงินผ่านตู้เอทีเอ็ม แต่หากเหยื่อมีเงินค่อนข้างมากจะหลอกให้ฝากเงินผ่านเครื่องฝากถอนอัตโนมัติ

2. บัญชีเงินฝากพัวพันกับการค้า

ยาเสพติดหรือการฟอกเงิน เมื่อมิจฉาชีพหลอกถามข้อมูลจากเหยื่อแล้วพบว่าเหยื่อมีเงินในบัญชีเป็นจำนวนมาก จะหลอกเหยื่อต่อว่าบัญชีนั้น ๆ พัวพันกับการค้ายาเสพติดหรือติดปัญหาการฟอกเงิน จึงขอให้เหยื่อโอนเงินทั้งหมดมาตรวจสอบ

3. เงินคืนภาษี

ข้ออ้างคืนเงินภาษีจะถูกใช้ในช่วงที่มีการยื่นภาษีและมีการขอคืน โดยมิจฉาชีพจะแอบอ้างเป็นเจ้าหน้าที่สรรพากรแจ้งว่าเหยื่อได้รับภาษีคืนเป็นเงินจำนวนหนึ่ง ซึ่งจะต้องยืนยันรายการและทำตามคำบอกที่ตู้เอทีเอ็ม แต่แท้จริงแล้วขั้นตอนที่มิจฉาชีพให้เหยื่อทำนั้นเป็นการโอนเงินให้กับมิจฉาชีพ

4. โชคดีรับรางวัลใหญ่

มิจฉาชีพจะอ้างตนเป็นเจ้าหน้าที่บริษัทหรือตัวแทนองค์กรต่าง ๆ แจ้งข่าวดีแก่เหยื่อว่า เหยื่อได้รับเงินรางวัลหรือของรางวัลที่มีมูลค่าสูง เมื่อเหยื่อหลงเชื่อ จะหลอกเหยื่อให้โอนเงินค่าภาษีให้

5.ข้อมูลส่วนตัวหาย

ข้อมูลส่วนตัวหายเป็นข้ออ้างที่มิจฉาชีพใช้เพื่อขอข้อมูลส่วนตัวของเหยื่อ โดยจะอ้างตัวเป็นเจ้าหน้าที่สถาบันการเงิน เล่าเหตุการณ์ที่ทำให้ข้อมูลของลูกค้าสูญหาย เช่น เหตุการณ์น้ำท่วม จึงขอให้เหยื่อแจ้งข้อมูลส่วนตัว เช่น วัน/เดือน/ปีเกิด เลขที่บัตรประชาชน เพื่อใช้เป็นฐานข้อมูลในการใช้บริการของเหยื่อ แต่แท้จริงแล้ว มิจฉาชีพจะนำข้อมูลเหล่านี้ไปประกอบการปลอมแปลงหรือใช้บริการทางการเงินในนามของเหยื่อ

6. โอนเงินผิด

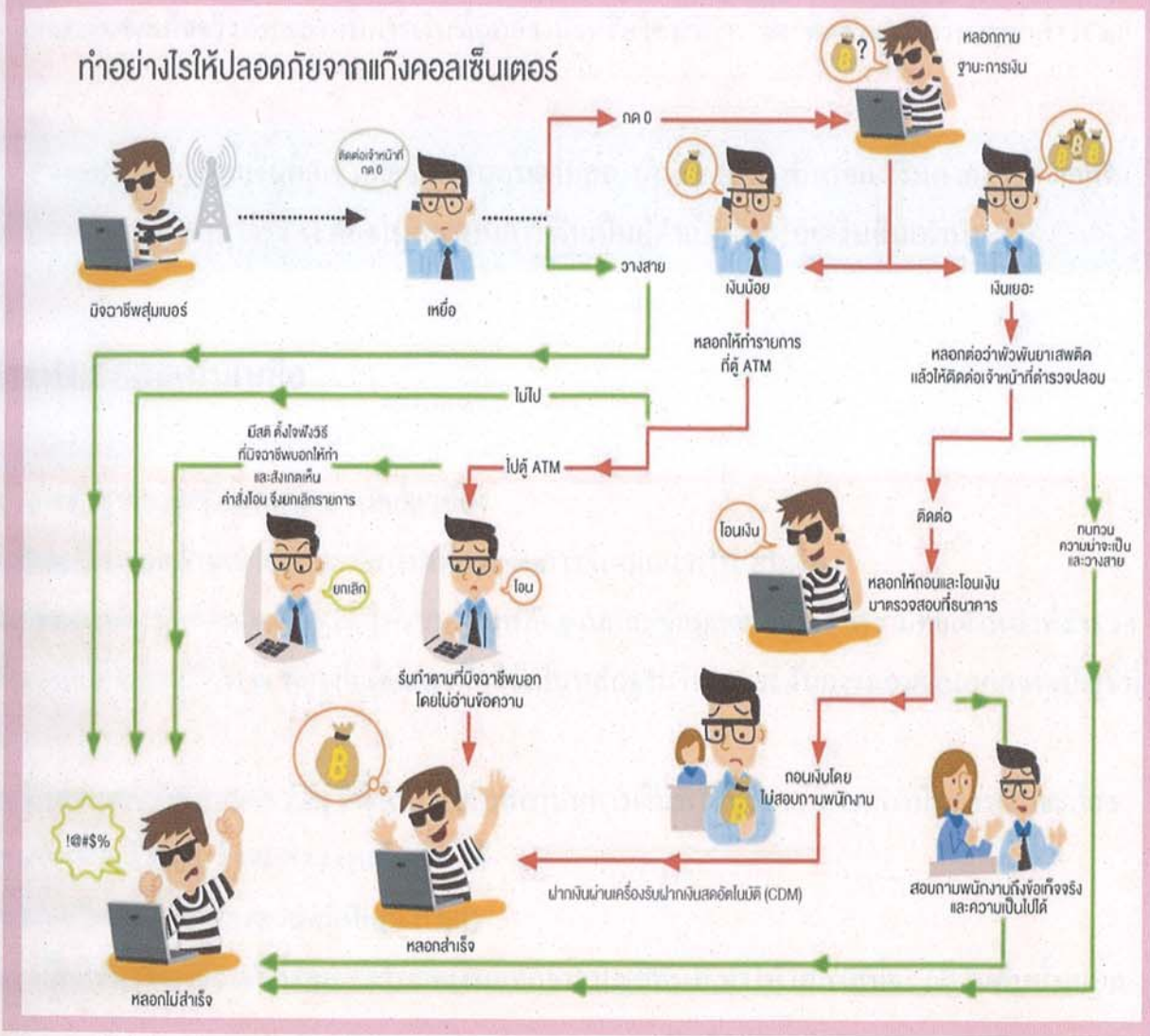
มิจฉาชีพจะใช้ข้ออ้างนี้เมื่อมีข้อมูลของเหยื่อค่อนข้างมากแล้ว โดยจะเริ่มจากโทรศัพท์ไปยังสถาบันการเงินที่เหยื่อใช้บริการ เพื่อเปิดใช้บริการขอสินเชื่อผ่านทางโทรศัพท์ เมื่อได้รับอนุมัติสินเชื่อ สถาบันการเงินจะโอนเงินสินเชื่อนั้นเข้าบัญชีเงินฝากของเหยื่อ หลังจากนั้นมิจฉาชีพจะโทรศัพท์ไปหาเหยื่ออ้างว่าได้โอนเงินผิดเข้าบัญชีของเหยื่อ ขอให้โอนเงินคืน เมื่อเหยื่อตรวจสอบยอดเงินและพบว่ามีเงินโอนเข้ามาจริง จึงรีบโอนเงินนั้นไปให้มิจฉาชีพ โดยที่ไม่รู้ว่าเงินนั้นเป็นเงินสินเชื่อที่มิจฉาชีพโทรไปขอในนามของเหยื่อ

ข้อสังเกต

1. มิจฉาชีพจะหลอกถามข้อมูลจากเหยื่อ แล้วหลอกให้เหยื่อทำรายการผ่านตู้เอทีเอ็มโดยให้เลือกทำรายการเป็นภาษาอังกฤษ

2. มิจฉาชีพจะใช้ข้ออ้างต่าง ๆ เร่งให้เหยื่อทำรายการ เพื่อไม่ให้เหยื่อมีเวลาตรวจสอบหรือสอบถามบุคคลอื่น

3. มิจฉาชีพจะโน้มน้าวให้เหยื่อโอนเงินผ่านตู้เอทีเอ็มหรือเครื่องฝากเงินอัตโนมัติ ตามภาพประกอบด้านล่าง



วิธีป้องกัน

1 หากได้รับโทรศัพท์จากบุคคลที่ไม่รู้จัก ควรทบทวนเรื่องราวที่เกิดขึ้นว่ามีโอกาสเป็นไปได้มากน้อยแค่ไหน

2 ไม่โลภอยากได้เงินรางวัลที่ไม่มีที่มา

3 ไม่ให้ข้อมูลส่วนตัวและข้อมูลทางการเงินแก่บุคคลอื่น ถึงแม้ผู้ติดต่อจะอ้างตัวเป็นส่วนราชการหรือสถาบันการเงิน เพราะส่วนราชการและสถาบันการเงินไม่มีนโยบายสอบถามข้อมูลส่วนตัวลูกค้าผ่านทางโทรศัพท์

4 ไม่ทำรายการที่ตู้เอทีเอ็ม หรือเครื่องฝากเงินอัตโนมัติตามคำบอกของผู้ที่ติดต่อมา

5 ควรสอบถามข้อเท็จจริงกับสถาบันการเงินที่ถูกอ้างถึงหรือใช้บริการ โดยติดต่อฝ่ายบริการลูกค้า (Call Center)

6 หากได้รับแจ้งว่ามีผู้โอนเงินผิดเข้าบัญชี ควรสอบถามสถาบันการเงินถึงที่มาของเงินดังกล่าว หากเป็นเงินที่มีการโอนผิดเข้ามาจริง จะต้องให้สถาบันการเงินเป็นผู้ดำเนินการโอนเงินคืนเท่านั้น

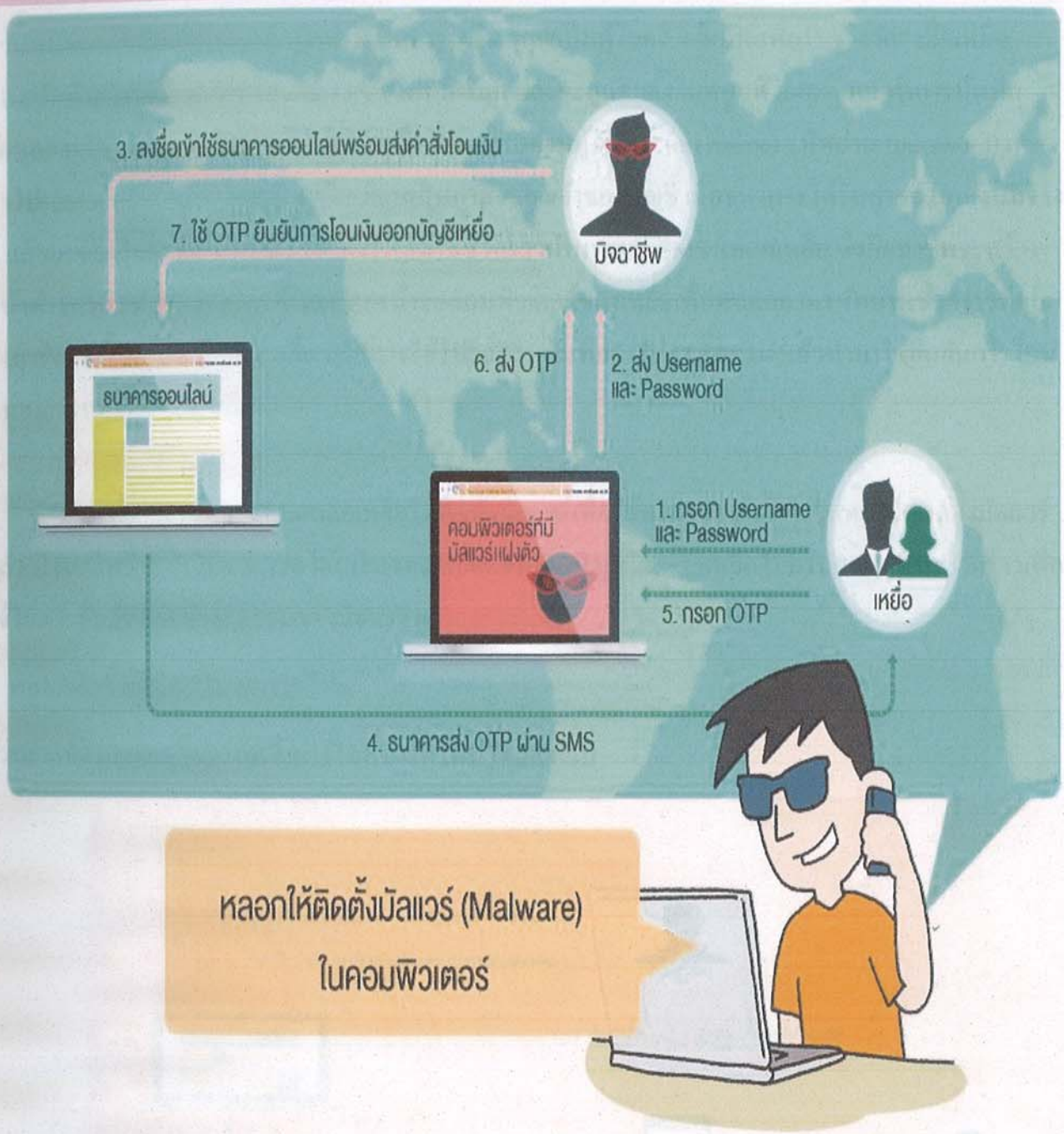
สิ่งที่ควรทำเมื่อตกเป็นเหยื่อ

1. รวบรวมหลักฐานและข้อมูลทุกอย่างที่เกี่ยวข้อง
2. ติดต่อฝ่ายบริการลูกค้าของสถาบันการเงินเพื่อระงับการโอนและการถอนเงิน
3. หากไม่สามารถระงับการโอนเงินได้ ให้รวบรวมหลักฐานและข้อมูลต่าง ๆ แจ้งความต่อเจ้าหน้าที่ตำรวจ พร้อมทั้งลงบันทึกประจำวัน ณ ท้องที่เกิดเหตุ เพื่อใช้เป็นหลักฐานในการระงับการถอนเงินออกจากบัญชีที่โอนไป
4. แจ้งระงับการถอนเงินออกจากบัญชีที่โอนไปกับสถาบันการเงินที่ใช้บริการ โดยสถาบันการเงินจะต้องตรวจสอบข้อเท็จจริงก่อน จึงจะสามารถคืนเงินได้
5. แจ้งเบาะแสไปยังกรมสอบสวนคดีพิเศษ (DSI)
6. ทำใจ... เมื่อมิจฉาชีพได้รับเงินโอน จะรีบกดเงินออกจากบัญชีทันที ทำให้โอกาสที่จะได้เงินคืนนั้นน้อยมาก

กลโกงธนาคารออนไลน์

ความก้าวหน้าของเทคโนโลยีในปัจจุบันได้เปลี่ยนแปลงวิถีชีวิตของคนเป็นอย่างมาก จากเคยที่ต้องเดินทางไปที่ธนาคารเพื่อทำธุรกรรมการเงิน ก็สามารถโอนเงิน ซื้อของ หรือทำธุรกรรมการเงินอื่น ๆ จากที่ไหนก็ได้ผ่านอินเทอร์เน็ต แต่ความสะดวกสบายเหล่านี้ หากใช้อย่างไม่ระมัดระวัง ก็อาจทำให้เกิดปัญหาตามมาได้

ลักษณะกลโกง



มิจฉาชีพจะหลอกขอรหัสผู้ใช้งาน (username) และรหัสผ่าน (password) จากเหยื่อเพื่อเข้าใช้บัญชีธนาคารออนไลน์ของเหยื่อ แล้วส่งคำสั่งโอนเงินออกจากบัญชีเงินฝาก โดยมีหลายวิธีที่มิจฉาชีพมักใช้ดังนี้

1. หลอกให้ติดตั้งมัลแวร์ในคอมพิวเตอร์

มิจฉาชีพมักแฝงมัลแวร์ (Malware) ไว้ตามลิงก์ดาวน์โหลด หรือเว็บไซต์ต่าง ๆ โดยใช้ข้อความเชิญชวนหลอกล่อให้เหยื่อคลิกเพื่อติดตั้งโปรแกรม เช่น "คุณเป็นผู้โชคดี คลิกที่นี่เพื่อรับรางวัล" เมื่อเหยื่อหลงเชื่อทำตามที่มิจฉาชีพบอก เช่น คลิกไปที่ลิงก์มัลแวร์จะถูกติดตั้งในคอมพิวเตอร์ และทำการบันทึกข้อมูลการใช้งานธนาคารออนไลน์ของเหยื่อ เช่น รหัสผ่านผู้ใช้งาน (username) รหัสผ่าน (password) เพื่อนำไปปลอมแปลงคำขอโอนเงินให้เหมือนเป็นคำสั่งของเจ้าของบัญชี เมื่อธนาคารได้รับคำขอโอนเงินที่จริง ๆ แล้วมาจากมิจฉาชีพ ธนาคารก็จะส่งรหัสผ่านชั่วคราวผ่านระบบ SMS ให้แกเหยื่อ ซึ่งมิจฉาชีพจะสร้างหน้าต่างหรือหน้าจอ pop-up ขึ้นมาบนหน้าจอคอมพิวเตอร์ของเหยื่อเพื่อหลอกถามรหัสผ่านชั่วคราวที่ถูกส่งมายังโทรศัพท์มือถือของเหยื่อ หรืออาจใช้โปรแกรมบันทึกการกดรหัสผ่าน แล้วนำมาใช้ยืนยันการโอนเงินออกจากบัญชีของเหยื่อ

ข้อควรสังเกต

มิจฉาชีพจะพยายามหลอกล่อเหยื่อให้ติดตั้งมัลแวร์เพื่อใช้ขโมยข้อมูล แต่เมื่อเหยื่อได้ติดตั้งมัลแวร์แล้ว มิจฉาชีพก็จะยังไม่สามารถโอนเงินของเหยื่อออกจากบัญชีได้ หากเหยื่อไม่กรอกรหัสผ่านชั่วคราวเพื่อใช้ในการยืนยันการทำธุรกรรมของมิจฉาชีพ

2. หลอกติดตั้งมัลแวร์ในสมาร์ตโฟน

ตัวอย่างขั้นตอนกลโกงผ่านมัลแวร์ในสมาร์ตโฟนโดยสังเขป

มัลแวร์ในสมาร์ตโฟนมีลักษณะคล้ายกับมัลแวร์ในคอมพิวเตอร์ แต่ความแตกต่างจะอยู่ที่มิจฉาชีพไม่จำเป็นต้องหลอกขอรหัสผ่านชั่วคราวจากเหยื่ออีก มิจฉาชีพจะส่งลิงก์ผ่าน SMS หรืออีเมลให้เหยื่อคลิกเพื่อติดตั้งและเปิดใช้งานมัลแวร์ในสมาร์ตโฟนหรือแท็บเล็ต แล้วหลอกให้เหยื่อกรอกรหัสผ่านผู้ใช้งาน (username) และรหัสผ่าน (password) ในหน้าจอที่คล้ายกับแอปพลิเคชันของธนาคารออนไลน์จริง เมื่อเหยื่อเลือกทำรายการต่อ มัลแวร์จะทำให้เครื่องสมาร์ตโฟนของเหยื่อค้างและใช้งานไม่ได้ ทำให้เหยื่อไม่ได้รับ SMS แจ้งรหัสผ่านชั่วคราว จากธนาคารออนไลน์จริง แต่รหัสผ่านชั่วคราวนั้นจะถูกส่งให้แก่มิจฉาชีพแทน

ข้อควรสังเกต

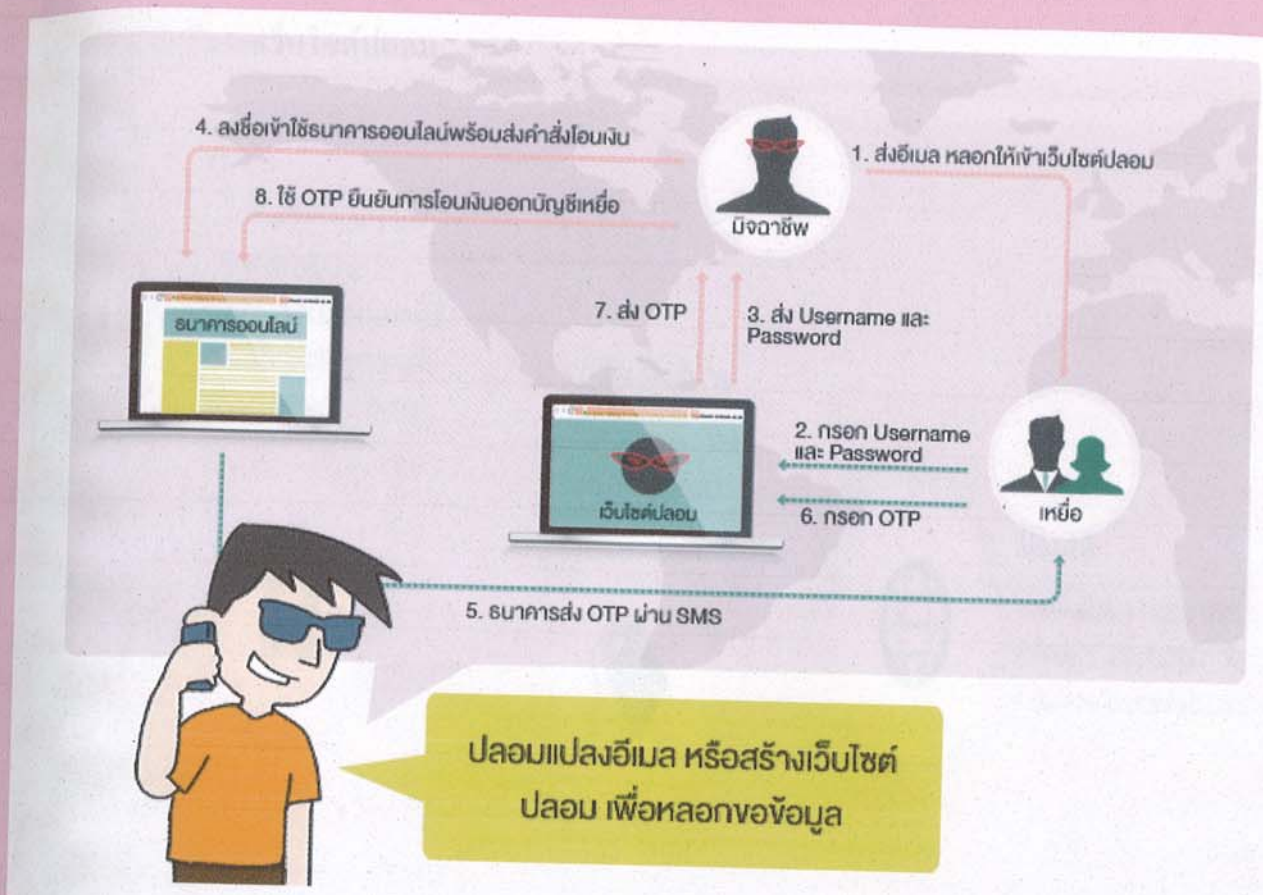
การหลอกลวงวิธีนี้ เมื่อเหยื่อหลงกลติดตั้งมัลแวร์ มิจฉาชีพไม่จำเป็นต้องหลอกขอรหัสผ่านชั่วคราวจากเหยื่ออีก เพราะมัลแวร์จะทำหน้าที่ดัก SMS แจ้งรหัสผ่านชั่วคราวไว้แล้วส่งให้แก่มิจฉาชีพ มิจฉาชีพจึงสามารถโอนเงินออกจากบัญชีเหยื่อได้

3. ปลอมแปลงอีเมลหรือสร้างเว็บไซต์ปลอม เพื่อหลอกขอข้อมูล

อีเมลปลอมก็เป็นอีกวิธีหนึ่งที่มิจฉาชีพมักใช้เพื่อหลอกเอาข้อมูลที่จำเป็นในการใช้งานธนาคารออนไลน์จากเหยื่อ โดยมิจฉาชีพจะทำอีเมลแอบอ้างเป็นอีเมลของธนาคารอ้างการปรับปรุงระบบรักษาความปลอดภัย แล้วหลอกให้เหยื่อยืนยันการใช้งานบัญชีธนาคารออนไลน์ผ่านการกรอกข้อมูลในอีเมล หรือคลิกลิงก์เชื่อมโยงไปยังเว็บไซต์ธนาคารออนไลน์ปลอมที่มี URL ที่คล้ายหรือเกือบเหมือนเว็บไซต์จริง ซึ่งเมื่อเหยื่อบอกรหัสผ่านผู้ใช้งาน (username) และรหัสผ่าน (password) ในลิงก์ปลอมเหล่านั้น มิจฉาชีพก็สามารถนำข้อมูลไปใช้แอบอ้างเป็นเจ้าของบัญชีแล้วส่งคำสั่งโอนเงิน และสร้างหน้าต่างปลอมหรือหน้าจอ pop-up หลอกให้เหยื่อกรอกรหัสผ่านชั่วคราว ในหน้าจอคอมพิวเตอร์ของเหยื่ออีก ทำให้มิจฉาชีพสามารถโอนเงินออกจากบัญชีของเหยื่อสำเร็จ

ข้อควรสังเกต

มิจฉาชีพมักหลอกขอข้อมูลจากเหยื่อผ่านอีเมลหรือเว็บไซต์ปลอมที่ลักษณะคล้ายกับเว็บไซต์จริงเกือบทุกประการ แต่อีเมลหรือเว็บไซต์ปลอมมีจุดน่าสังเกตดังนี้



(1) จุดสังเกตอีเมลปลอม

(2) จุดสังเกตเว็บไซต์ปลอม

วิธีป้องกัน

การใช้งานธนาคารออนไลน์ทั่วไป

- ไม่ควรใช้รหัสผ่าน (password) ที่ง่ายต่อการคาดเดา เช่น 123456 หรือ วัน/เดือน/ปีเกิด
- ก่อนเข้าใช้ธนาคารออนไลน์ จะต้องมั่นใจหรือตรวจสอบให้แน่ใจว่าเป็นอุปกรณ์ที่ใช้นั้นไม่มีมัลแวร์ (Malware) แฝงอยู่
- ติดตั้งโปรแกรมป้องกันไวรัสที่ถูกกฎหมาย พร้อมตรวจสอบและอัพเดตโปรแกรมอยู่เสมอ
- ไม่ติดตั้งหรือดาวน์โหลดโปรแกรมแปลก ๆ หรือโปรแกรมที่ไม่ถูกกฎหมาย เพราะอาจเป็นช่องทางให้มัลแวร์เข้ามาในคอมพิวเตอร์ สมาร์ตโฟน หรือแท็บเล็ตได้
- ไม่ใช้ลิงก์เชื่อมโยงที่มากับอีเมลหรือในเว็บไซต์ต่าง ๆ เพื่อเข้าสู่ระบบธนาคารออนไลน์ แต่ควรพิมพ์ URL ด้วยตัวเอง
- ไม่ทำธุรกรรมการเงินผ่านอินเทอร์เน็ตสาธารณะ แต่หากจำเป็น ให้เปลี่ยนรหัสผ่านหลังจากใช้งานทันที
- ตรวจสอบรายการเคลื่อนไหวในบัญชี และการเข้าใช้ระบบธนาคารออนไลน์อยู่เสมอ ว่าเป็นรายการที่ได้ทำไว้หรือไม่
- ควร "ออกจากระบบ" (logout) ทุกครั้งเมื่อไม่ใช้งาน
- จำกัดวงเงินในการทำธุรกรรมผ่านธนาคารออนไลน์ เพื่อลดความเสี่ยงในกรณีถูกมิจฉาชีพขโมยรหัสผ่าน
- ธนาคารไม่มีนโยบายส่ง SMS หรือ email เพื่อให้ดาวน์โหลด ติดตั้งโปรแกรม หรือเข้าสู่ระบบธนาคารออนไลน์
- หากคลิกลิงก์ต้องสงสัย ให้รีบติดต่อเจ้าหน้าที่ธนาคารหรือฝ่ายบริการลูกค้าของธนาคารทันทีและขอคำปรึกษาเกี่ยวกับการใช้งานที่ปลอดภัย
- ติดตามข่าวสารกลโกงธนาคารออนไลน์เป็นประจำ เพื่อรู้เท่าทันเล่ห์เหลี่ยมกลโกง

สำหรับการใช้งานธนาคารออนไลน์ผ่านสมาร์ตโฟนหรือแท็บเล็ต

- ไม่เก็บเอกสารหรือข้อมูลสำคัญไว้ในสมาร์ตโฟนหรือแท็บเล็ต เช่น เลขที่บัตรประชาชน เลขที่บัญชีเงินฝาก
- หลีกเลี่ยงการดาวน์โหลด หรือติดตั้งโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ โดยเฉพาะอุปกรณ์ที่ใช้งานธนาคารออนไลน์
- หลีกเลี่ยงการใช้งานธนาคารออนไลน์ผ่านอุปกรณ์ที่มีการดัดแปลง หรือแก้ไขระบบปฏิบัติการ (jailbreak หรือ root) เพราะมีความเสี่ยงสูงที่จะถูกขโมยข้อมูล

สิ่งที่ควรทำเมื่อตกเป็นเหยื่อ

- หากพบเว็บไซต์ปลอมของธนาคาร ให้รีบแจ้งสถาบันการเงินนั้น ๆ ทันที เพื่อดำเนินการปิดเว็บไซต์ดังกล่าว
- หากได้รับข้อความหรือได้คลิกลิงก์เพื่อดาวน์โหลดโปรแกรมต้องสงสัยหรือให้ข้อมูลในเว็บไซต์ปลอมไปแล้ว ให้รีบติดต่อเจ้าหน้าที่ธนาคารทันที
- หากได้รับรหัสผ่านชั่วคราวโดยที่ไม่ได้ส่งคำสั่งโอนเงิน ให้แจ้งเหตุการณ์ที่เกิดขึ้นแก่เจ้าหน้าที่ธนาคารหรือฝ่ายบริการลูกค้าของธนาคารทันทีและขอคำปรึกษาเกี่ยวกับการใช้งานที่ปลอดภัย

กลโกงบัตรต่าง ๆ

บัตรอิเล็กทรอนิกส์ เช่น บัตรเครดิต บัตรเดบิต บัตรกดเงินต่าง ๆ เป็นบัตรที่อำนวยความสะดวกในการทำธุรกรรมทางการเงินของเจ้าของบัตร เช่น ถอนเงิน โอนเงิน ชำระเงิน ซึ่งบัตรเหล่านี้จะบันทึกข้อมูลส่วนตัวและข้อมูลทางการเงินของเจ้าของบัตรไว้ หากมิจฉาชีพเข้าถึงข้อมูลเหล่านี้ได้จากการขโมยบัตรหรือขโมยข้อมูลในบัตร มิจฉาชีพก็จะสามารถนำข้อมูลเหล่านี้ไปปลอมเป็นเจ้าของบัตรทำธุรกรรมทางการเงินต่าง ๆ ไม่ว่าจะถอนเงินออกจากบัญชี หรือใช้วงเงินสินเชื่อของเหยื่อที่เป็นเจ้าของบัตร

ลักษณะกลโกง

1.คัดลอกข้อมูลจากแถบแม่เหล็กของบัตรโดยเครื่องสกิมเมอร์ (Skimmer) ที่ติดตั้งไว้ที่ตู้เอทีเอ็ม

มิจฉาชีพมักติดตั้งเครื่องสกิมเมอร์ที่ช่องเสียบบัตรของตู้เอทีเอ็ม เพื่อคัดลอกข้อมูลจากบัตร พร้อมติดตั้งแป้นครอบกดตัวเลขเพื่อบันทึกรหัสผ่านที่เหยื่อกด หรืออาจติดตั้งกล้องจิ๋วเพื่อแอบดูรหัสผ่าน

2. คัดลอกข้อมูลจากแถบแม่เหล็กของบัตรโดยเครื่องสกิมเมอร์ขนาดพกพาหรือเครื่องแฮนด์เฮลด์สกิมเมอร์ (Handheld Skimmer)

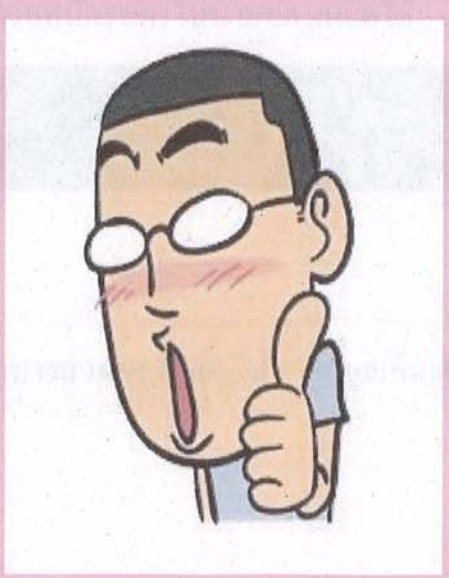
แฮนด์เฮลด์สกิมเมอร์เป็นเครื่องคัดลอกข้อมูลในแถบแม่เหล็กขนาดเล็กที่สามารถพกพาได้ ซึ่งมิจฉาชีพมักจะถือไว้ในฝ่ามือ และนำบัตรของเหยื่อมารูดพร้อมทั้งดูรหัสปลอดภัยจากด้านหลังบัตรโดยไม่ให้เหยื่อสังเกตเห็น ซึ่งอาจเกิดขึ้นที่ใดก็ได้ ไม่ว่าจะเป็นร้านค้า ร้านอาหาร สถานีบริการน้ำมัน หรือมิจฉาชีพอาจแอบอ้างเป็นเจ้าพนักงานธนาคารยื่นหน้าตู้เอทีเอ็ม ขอดูบัตรของเหยื่อ หรืออาจทำทีเสนอความช่วยเหลือแก่เหยื่อหากบัตรติดตู้เอทีเอ็ม แล้วคัดลอกข้อมูลผ่านเครื่องแฮนด์เฮลด์สกิมเมอร์เมื่อเหยื่อเผลอ

3. ปลอมแปลงเอกสารสมัครบัตรเครดิต

มิจฉาชีพอาจปลอมแปลงหรือใช้เอกสารส่วนตัวของเหยื่อ เช่น สำเนาบัตรประชาชนที่ได้ขโมยมา แล้วนำไปใช้สมัครบัตรเครดิต หรือแจ้งเปลี่ยนที่อยู่ เปลี่ยนบัตร โดยแจ้งให้สถาบันการเงินส่งเอกสารและบัตรที่ออกใหม่ให้กับมิจฉาชีพโดยตรง เมื่อได้รับบัตรเครดิตก็นำไปใช้จ่ายในนามของเหยื่อ

4. ขโมยข้อมูลจากใบบันทึกรายการ (ATM Slip)

มิจฉาชีพจะเก็บใบบันทึกราย (ATM Slip) ตามตู้เอทีเอ็มที่มียอดคงเหลือค่อนข้างมากไปใช้ค้นหาข้อมูลสำคัญ ๆ ในการทำธุรกรรมทางการเงิน เช่น วันเดือนปีเกิด หมายเลขบัตรประชาชน โดยใช้วิธีที่แตกต่างกันออกไป เช่น แอบอ้างเป็นข้าราชการไปขอข้อมูลทะเบียนราษฎรจากเจ้าหน้าที่ฝ่ายปกครอง หรือค้นหาเลขที่บัญชีให้ครบ 10 หลักแล้วนำไปทดลองโอนผ่านธนาคารออนไลน์เพื่อให้ทราบชื่อเจ้าของบัญชี



เมื่อได้ข้อมูลของเหยื่อแล้ว มิจฉาชีพจะปลอมแปลงบัตรประจำตัวราชการปลอมโดยใช้ชื่อของเหยื่อเป็นเจ้าของบัตรแต่ติดรูปภาพของมิจฉาชีพ แล้วนำบัตรดังกล่าวไปขอเปิดบัญชีเงินฝากและทำบัตรเอทีเอ็มใหม่ของธนาคารเดียวกันแต่คนละสาขา พร้อมทั้งขอเปิดใช้บริการธนาคารออนไลน์กับทุกบัญชีเงินฝากของเหยื่อ เพื่อโอนเงินทั้งหมดไปที่บัญชีเงินฝากที่เปิดใหม่ แล้วใช้บัตรเอทีเอ็มถอนเงินออกไป

ข้อควรสังเกต

01

เครื่องสกิมเมอร์

มิจฉาชีพจะติดตั้งเครื่องดังกล่าวไว้ที่ตู้เอทีเอ็ม ดังนั้น มิจฉาชีพมักจะเลือกตู้เอทีเอ็มในบริเวณที่มีคนไม่พลุกพล่าน ง่ายต่อการติดตั้ง

02

เครื่องแฮนด์เฮลด์สกิมเมอร์

มิจฉาชีพจะรูดบัตรของเหยื่อกับเครื่องแฮนด์เฮลด์สกิมเมอร์ ดังนั้น มิจฉาชีพจะต้องหลอกขอบัตรจากเหยื่อ

03

การปลอมแปลงเอกสาร

มิจฉาชีพจะต้องมีเอกสาร หรือข้อมูลส่วนตัวของเหยื่อ จึงจะสามารถสมัครบัตรในนามของเหยื่อได้

04

ขโมยข้อมูลจากใบบันทึกรายการตู้เอทีเอ็ม

มิจฉาชีพจะต้องมีใบบันทึกรายการ (Slip) ซึ่งมีข้อมูลบัญชีเงินฝากบางส่วนของเหยื่อไปหาข้อมูลเพิ่มเติม

วิธีป้องกัน

1. รหัสผ่านของบัตรควร

เป็นรหัสผ่านที่ยากต่อการคาดเดา แต่เจ้าของบัตรต้องจำได้ไม่จดรหัสผ่านไว้คู่กับบัตร หรือในที่ที่ผู้อื่นสามารถเข้าถึงได้ไม่ใช้รหัสผ่านที่สถาบันการเงินส่งมาให้ และควรทำลายเอกสารแจ้งรหัสผ่าน เปลี่ยนรหัสอย่างน้อยทุก 3 เดือนหรือบ่อยกว่าเก็บรักษารหัสผ่านเป็นความลับ และไม่ควรให้ข้อมูลส่วนตัวหรือข้อมูลทางการเงินแก่ผู้อื่น

2. ก่อนใช้งานตู้เอทีเอ็มควร

หลีกเลี่ยงการใช้ตู้เอทีเอ็มในสถานที่เปลี่ยว เพราะมีโอกาสที่มิจฉาชีพจะติดตั้งเครื่องคัดลอกข้อมูลไว้ได้โดยง่ายสังเกตช่องเสียบบัตร แป้นกดตัวเลข หรือบริเวณตู้เอทีเอ็ม ว่ามีสิ่งผิดปกติ เช่น แป้นครอบตัวเลข กล่องหรืออุปกรณ์ที่ติดไว้ในระยะมองเห็นการกดรหัสหรือไม่

3. หากใช้บัตรกับร้านค้าควร

หลีกเลี่ยงร้านค้าที่มีความเสี่ยงที่จะเกิดการทุจริต เช่น สถานบริการน้ำมัน สถานบันเทิง ควรอยู่ในบริเวณที่มองเห็นการทำรายการ และให้บัตรอยู่ในสายตาตลอดเวลา เพื่อป้องกันพนักงานนำบัตรไปรูดกับเครื่องสกิมเมอร์

4. เมื่อใช้งานบัตรควร

ใช้มือปิดบังไม่ให้ผู้อื่นมองเห็นแป้นกด ในขณะที่กำลังกดรหัสผ่านเก็บใบบันทึกรายการทุกครั้ง เพื่อเป็นหลักฐานในการตรวจสอบยอดการใช้จ่ายตรวจสอบรายการใช้จ่ายหรือยอดเงินอย่างสม่ำเสมอ หากมีรายการผิดปกติ ให้แจ้งธนาคารหรือบริษัทผู้ออกบัตรเพื่อตรวจสอบและดำเนินการแก้ไข

5. ไม่ควรให้เอกสารข้อมูลส่วนตัว และข้อมูลทางการเงินแก่บุคคลอื่น

6. หากบัตรสูญหายหรือถูกขโมย ควรแจ้งธนาคารหรือบริษัทผู้ออกบัตรเพื่ออายัดบัตรทันที

7. ติดตามข่าวสารกลโกง เพื่อรู้เท่าทันกลโกงใหม่ ๆ

สิ่งที่ควรทำเมื่อตกเป็นเหยื่อ

1. เมื่อพบรายการถอนเงินหรือโอนเงินผิดปกติ ควรแจ้งอายัดบัตรทันที พร้อมตรวจสอบยอดเงินใช้จ่ายหรือยอดเงินคงเหลือกับเจ้าหน้าที่ธนาคารหรือบริษัทผู้ออกบัตร

2. แจ้งความต่อเจ้าหน้าที่ตำรวจ

3. ทำใจ...เพราะเงินที่ถูกมิจฉาชีพขโมยไป โอกาสจะได้คืนนั้นน้อยมาก โดยเฉพาะในกรณีที่มิจฉาชีพได้ข้อมูลบัตรเพราะความประมาทของผู้ถือบัตร ทั้งนี้ กรณีที่เป็นการ skimming ที่ตู้เอทีเอ็มของธนาคารจริง ธนาคารจะชดใช้เงินให้แก่ลูกค้าที่ได้รับความเสียหาย

ข่าวกลโกงที่เกี่ยวข้อง

คลี่ปมปริศนา CSI THAILAND: ไขคดี!แก๊งฉกเงินผ่านอินเทอร์เน็ต ล้วงข้อมูลแบงก์จากสลิปเอทีเอ็ม

กลโกงออนไลน์อื่น ๆ

อินเทอร์เน็ตทำให้ชีวิตประจำวันของเราสะดวกสบายมากขึ้น การติดต่อสื่อสารเป็นไปได้โดยง่าย เพื่อนฝูง ญาติพี่น้อง หรือคนไม่รู้จักก็สามารถติดต่อสื่อสารกันได้อย่างรวดเร็ว แต่ความสะดวกสบายนี้ก็มีอันตรายแฝงมาด้วย โดยเป็นเครื่องมือที่ช่วยทำให้มิจฉาชีพที่อยู่ไกลจากเหยื่อสามารถเข้ามาใกล้ชิด หลอกลวงเงินไปจากเหยื่อได้โดยง่ายหากไม่ระมัดระวัง เราลองมาทำความรู้จักกับกลโกงออนไลน์ที่พบบ่อย ๆ กัน

1. หลอกขอรหัสผ่านการใช้งานบัญชีอีเมล

มิจฉาชีพจะส่งอีเมลแอบอ้างเป็นผู้ให้บริการบัญชีอีเมล หลอกขอชื่อบัญชีผู้ใช้งาน (email address) และรหัสผ่าน (password) โดยอ้างว่าเจ้าของอีเมลจะต้องยืนยันการใช้งานอีเมล แล้วใช้รหัสผ่านที่ได้มาเข้าใช้งานบัญชีอีเมลแทนเจ้าของอีเมลนั้น (ซึ่งถือได้ว่าเป็นเหยื่อคนที่ 1)

เมื่อเข้าใช้งานในบัญชีอีเมลของเจ้าของบัญชีอีเมลที่กลายเป็นเหยื่อคนที่ 1 ได้แล้ว มิจฉาชีพก็จะส่งอีเมลไปหาเพื่อนของเจ้าของบัญชีอีเมล แล้วหลอกขอให้เพื่อนโอนเงินให้ เช่น อ้างว่าเจ้าของบัญชีอีเมลไปต่างประเทศแล้วกระเป๋าเงินหาย จึงต้องการความช่วยเหลือเรื่องเงินโดยด่วน โดยมักจะให้โอนเงินผ่านบริการรับโอนเงินซึ่งไม่จำเป็นต้องมีเอกสารแสดงตนในการรับเงินในต่างประเทศ ซึ่งทำให้เจ้าหน้าที่ไม่สามารถติดตามจับคนร้ายได้ และเพื่อนก็สูญเงินโดยไม่มีโอกาสได้คืน (กลายเป็นเหยื่อคนที่ 2)

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 ขอโทษที่ไม่ได้บอก
ฉันเดินทางมาสัมมนาที่อังกฤษ แต่กระเป๋าสตางค์หาย...ขอยืมเงิน 2,000 ปอนด์
เพื่อจ่ายค่าโรงแรมและค่าเดินทางกลับ
ฉันจะจ่ายคืนทันทีที่กลับถึงบ้าน

ข้อสังเกต

มิจฉาชีพจะอ้างเป็นผู้ให้บริการบัญชีอีเมลแต่ชื่อบัญชีอีเมล (email address) ที่แสดง จะไม่ใช่ชื่อบัญชีอีเมลของผู้ให้บริการอีเมลจริง (อ่านเพิ่มเติมจุดสังเกตอีเมลปลอม) นอกจากนั้น ข้อความในอีเมลที่มิจฉาชีพส่งให้เหยื่อคนที่ 2 มักเป็นภาษาอังกฤษหรือเป็นภาษาไทยที่ไม่คุ้นเคย เช่น ใช้สรรพนามต่างจากที่เคยใช้สนทนากัน

2. แอบอ้างเป็นบุคคลต่าง ๆ หลอกว่าจะโอนเงินหรือส่งของให้เหยื่อ

มิจฉาชีพจะแอบอ้างเป็นบุคคลต่าง ๆ แล้วหลอกเหยื่อว่าจะโอนเงิน หรือส่งของให้เหยื่อ เช่น

- เป็นนักธุรกิจที่ต้องการสั่งซื้อสินค้าเป็นจำนวนมาก โดยส่งหลักฐานการโอนเงินจำนวนมากเพื่อจ่ายค่าสินค้ามาให้เหยื่อดู
- เป็นผู้ที่ได้รับมรดกเป็นจำนวนมาก แต่ติดเงื่อนไขต่าง ๆ ทำให้ไม่สามารถรับเงินได้ด้วยตนเอง จึงขอให้เหยื่อรับเงินแทน
- เป็นผู้ใจบุญที่ต้องการบริจาคเงินเป็นจำนวนมหาศาลให้มูลนิธิหรือองค์กรการกุศลต่าง ๆ เมื่อแจ้งว่าจะบริจาคเงินให้กับเหยื่อแล้ว จะส่งหลักฐานการโอนเงินปลอมมาให้เหยื่อดู
- เป็นชาวต่างชาติที่ต้องการหารักแท้ โดยอ้างว่าพร้อมที่จะย้ายมาอยู่กับเหยื่อเพื่อสร้างครอบครัวร่วมกัน จึงโอนเงินค่าบ้าน ค่ารถ หรือเงินทั้งหมดที่มีมาให้เหยื่อ หรืออาจหลอกเหยื่อว่าจะส่งของหรือเงินสดมาให้เหยื่อทางไปรษณีย์

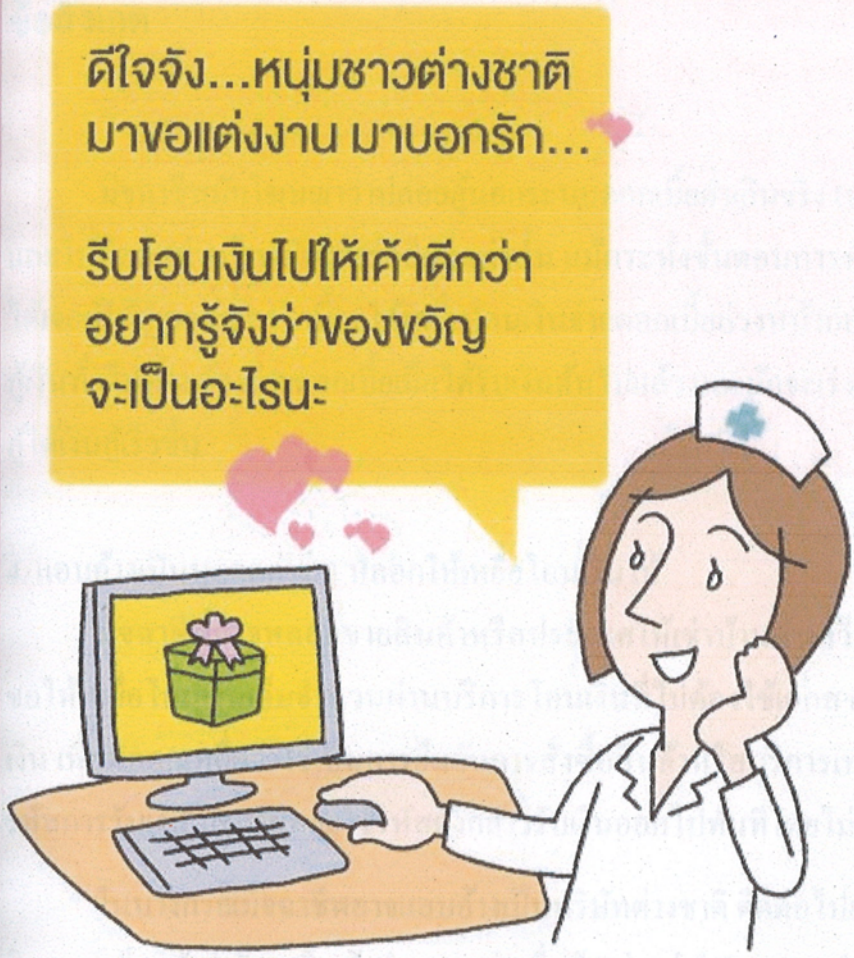
เมื่อเหยื่อได้รับหลักฐานการโอนเงินหรือการส่งของจากมิจฉาชีพ ก็มักหลงเชื่อว่ามิจฉาชีพได้โอนเงินหรือส่งของนั้นมาจริง ๆ เมื่อเวลาผ่านไป มิจฉาชีพจะแจ้งเหยื่อ หรืออาจมีมิจฉาชีพคนอื่นมาแสดงตนเป็นเจ้าหน้าที่และแจ้งเหยื่อว่าไม่สามารถโอนเงินหรือส่งของให้เหยื่อได้ เพราะติดด้วยเงื่อนไขต่าง ๆ เช่น

- ธนาคารแห่งประเทศไทยระงับการโอนเงินและขอตรวจสอบ
- ธนาคารกลางของประเทศต้นทางระงับการโอนเงิน เพราะสงสัยว่าเป็นการฟอกเงิน
- สหประชาชาติ หรือกองทุนการเงินระหว่างประเทศ (IMF) ขอตรวจสอบ
- กรมศุลกากรขอตรวจสอบของที่ส่งมาจากต่างประเทศ เพราะมีเงินสดบรรจุมาด้วย

จากนั้นจะเรียกเก็บค่าธรรมเนียมต่าง ๆ จากเหยื่อ เช่น ค่าธรรมเนียมการโอนเงิน ค่าดำเนินการ ค่าทนาย โดยจะเรียกเก็บในจำนวนน้อยแล้วเพิ่มจำนวนเงินขึ้นเรื่อย ๆ ซึ่งเหยื่อก็จะคิดว่าเป็นเรื่องจริง และเห็นว่าจ่ายอีกนิดก็จะได้รับเกินก้อนใหญ่ ซึ่งกว่าจะรู้ตัวว่าถูกหลอกก็อาจหมดเงินไปจำนวนมากแล้ว และโอกาสที่จะติดตามรับเงินคืนก็เป็นไปได้ยากมาก เพราะมิจฉาชีพมักอยู่ในต่างประเทศ และให้เหยื่อโอนเงินผ่านบริการโอนเงินที่มิจฉาชีพรับเงินได้โดยไม่ต้องมีเอกสารแสดงตน

ข้อสังเกต

มิจฉาชีพจะหลอกให้เหยื่อโอนเงินผ่านบริการโอนเงินที่มิจฉาชีพสามารถรับเงินได้โดยไม่ต้องมีเอกสารแสดงตน เพราะยากต่อการติดตามหน่วยงานราชการ หรือองค์กรระหว่างประเทศต่าง ๆ ที่ยกตัวอย่างมีหน้าที่ชัดเจน และส่วนใหญ่จะไม่ติดต่อกับประชาชนโดยตรง อย่างไรก็ตาม หากหน่วยราชการใดมีกิจต้องติดต่อกับประชาชน การแจ้งให้ประชาชนดำเนินการใด ๆ จะมีเอกสารหลักฐานเป็นลายลักษณ์อักษร หากมีผู้แอบอ้างว่าเป็นเจ้าหน้าที่เหล่านั้น โดยเฉพาะอย่างยิ่งกรณีต้องมีการโอนเงินหรือชำระเงิน ควรตรวจสอบไปยังหน่วยงานนั้นโดยตรงก่อน โดยไม่ใช้อีเมลหรือหมายเลขโทรศัพท์ที่ได้รับแจ้งมา



3. โฆษณาปล่อยเงินกู้นอกระบบ

มิจฉาชีพแอบอ้างเป็นผู้ให้บริการเงินกู้แล้วโฆษณาผ่านเว็บไซต์ต่าง ๆ หรือส่งอีเมลหาเหยื่อโดยตรงว่าให้บริการเงินกู้นอกระบบดอกเบี้ยต่ำ อนุมัติเงินเร็ว ไม่ต้องซื้อสินค้า ไม่ตรวจสอบเครดิตบูโร เมื่อเหยื่อติดต่อไปและขอกู้เงิน ผู้ให้กู้จะอ้างว่าจะส่งสัญญาให้กับผู้ขอกู้เพื่อลงลายมือชื่อ พร้อมทั้งขอให้เหยื่อโอนเงินชำระค่าทำสัญญา ค่าเอกสาร ค่ามัดจำ หรือดอกเบี้ยภายในเวลาที่กำหนด เช่น ก่อน 18.00 น. เพื่อผู้ให้กู้จะโอนเงินกู้ให้ก่อนเวลา 20.00 น. โดยสามารถยกเลิกและขอเงินโอนล่วงหน้าดังกล่าวคืนได้

เหยื่อส่วนมากมักจะรีบร้อน และกลัวว่าจะไม่ได้เงินกู้ จึงรีบโอนเงินให้กับผู้ให้กู้ในเวลาที่กำหนด แต่เมื่อติดต่อกลับผู้ให้กู้เพื่อขอรับเงินกู้ กลับไม่สามารถติดต่อผู้ให้กู้ได้อีกเลย และสูญเงินไปโดยไม่มีโอกาสได้เงินคืน

ข้อสังเกต

มิจฉาชีพมักโฆษณาว่าปล่อยกู้นอกระบบดอกเบี้ยต่ำเกินจริง (บางรายต่ำกว่าดอกเบี้ยเงินกู้ในระบบ) และให้ติดต่อผ่านโทรศัพท์หรืออีเมลเท่านั้น แม้กระทั่งขั้นตอนการทำสัญญาเงินกู้ ผู้ขอกู้ก็จะไม่มีโอกาสได้เจอผู้ให้กู้เลย นอกจากนี้จะให้เหยื่อโอนเงินจ่ายดอกเบี้ยล่วงหน้าก่อนที่จะได้เงินกู้ซึ่งจะแตกต่างจากการกู้เงินทั่วไปที่จะต้องจ่ายดอกเบี้ยเมื่อได้รับเงินต้นไปแล้ว และมักจะเร่งการตัดสินใจโดยอ้างว่าจะทำให้ผู้ขอกู้ได้เงินกู้เร็วขึ้น

4. แอบอ้างเป็นบุคคลต่าง ๆ หลอกให้เหยื่อโอนเงินให้

มิจฉาชีพอาจหลอกขายสินค้าหรือประกาศให้เช่าบ้านผ่านเว็บไซต์ต่าง ๆ และเมื่อเหยื่อสนใจ จะขอให้เหยื่อโอนเงินเต็มจำนวนผ่านบริการโอนเงินที่ไม่ต้องใช้เอกสารแสดงตนโดยระบุชื่อเหยื่อเป็นผู้รับเงิน เพื่อหลอกเหยื่อว่าใช้เป็นการยืนยันการสั่งซื้อสินค้าหรือบริการเท่านั้น แต่เมื่อเหยื่อโอนเงินพร้อมแจ้งรหัสการรับเงิน มิจฉาชีพจะใช้รหัสดังกล่าวรับเงินออกไปทันทีโดยไม่มีสินค้าเสนอขายจริง

ในบางกรณีมิจฉาชีพอาจแอบอ้างเป็นบริษัทต่างชาติ ติดต่อไปยังเหยื่อที่ประกาศสมัครงานในอินเทอร์เน็ตแจ้งว่ารับเหยื่อเข้าทำงาน แต่เหยื่อต้องจ่ายค่าใบอนุญาตทำงานในต่างประเทศ ทั้ง ๆ ที่บริษัทนั้นไม่มีอยู่จริง

ข้อสังเกต

มิจฉาชีพมักประกาศขายสินค้าดีในราคาถูกกว่าท้องตลาดมาก ๆ และเร่งการตัดสินใจโดยอ้างว่ามีผู้ติดต่อขอซื้อหลายรายจึงขอให้เหยื่อโอนเงินค่ามัดจำผ่านบริการโอนเงินที่มิจฉาชีพสามารถรับเงินได้โดยไม่ต้องมีเอกสารแสดงตน เพราะยากต่อการติดตาม

5. ขอเลขที่บัญชีเงินฝากเป็นที่พักเงิน

มิจฉาชีพจะประกาศรับสมัครงานผ่านอินเทอร์เน็ต หลอกเหยื่อว่าเป็นบริษัทต่างประเทศที่ขายสินค้าในประเทศไทยเป็นจำนวนมาก จึงขอให้เหยื่อทำหน้าที่เป็นผู้รวบรวมเงินให้ โดยอาจจ่ายค่าจ้างเป็นสัดส่วนกับเงินที่ได้รับ เช่น ร้อยละ 25 ของเงินค่าสินค้า

เมื่อมีเงินโอนเข้าบัญชีของเหยื่อ บริษัทจะแจ้งเหยื่อให้หักค่าจ้างไว้ แล้วโอนเงินที่เหลือทั้งหมดให้แก่บริษัทแม่ในต่างประเทศทันทีผ่านบริการโอนเงินที่ไม่ต้องใช้เอกสารแสดงตน โดยที่เหยื่อไม่รู้เลยว่าเงินที่โอนเข้ามาในบัญชีเหยื่อนั้นเป็นเงินผิดกฎหมายที่มิจฉาชีพหลอกให้คนอื่นโอนมาให้ กว่าเหยื่อจะรู้ตัวก็อาจเป็นตอนที่พนักงานธนาคารติดต่อเพื่ออายัดบัญชีของเหยื่อหรือถูกตำรวจจับแล้ว

ข้อสังเกต

หากมีการทำธุรกิจในประเทศไทยจริง บริษัทที่ทำธุรกิจนั้นสามารถเปิดบัญชีเงินฝากในประเทศไทยได้ โดยไม่จำเป็นต้องใช้บัญชีของบุคคลอื่นในการรับเงินจากลูกค้า นอกจากนี้ มิจฉาชีพจะให้เหยื่อโอนเงินส่งต่อให้แก่บริษัทที่ร่วมมือกับมิจฉาชีพผ่านบริการโอนเงินที่มิจฉาชีพสามารถรับเงินได้โดยไม่ต้องมีเอกสารแสดงตน เพื่อไม่ให้เจ้าหน้าที่ตำรวจติดตามได้

วิธีป้องกัน

1. เปิดเผยข้อมูลในโซเชียลเน็ตเวิร์คเท่าที่จำเป็น เพื่อป้องกันไม่ให้มิจฉาชีพนำข้อมูลไปแอบอ้างใช้ทำธุรกรรม

2. ควรเปลี่ยนรหัสผ่าน (password) ในการเข้าใช้บัญชีอีเมลหรือบัญชีโซเชียลเน็ตเวิร์คเป็นประจำ

3. เมื่อได้รับการติดต่อแจ้งให้โอนเงินให้ ควรตรวจสอบข้อเท็จจริงก่อนโอนเงิน เช่น ติดต่อหน่วยงานที่ถูกอ้างถึงโดยตรง อาทิ กรมศุลกากร โทร. 1164 ธนาคารแห่งประเทศไทย โทร. 1213 หรือสำนักงานตัวแทนในประเทศไทยของหน่วยงานต่างชาติ

4. ไม่โลภต่อเงินที่ไม่มีที่มา หรือผลตอบแทนที่สูงเกินจริง ควรพิจารณาให้รอบคอบถึงความเป็นไปได้ในความเป็นจริง

5. ตรวจหาไวรัสในเครื่องคอมพิวเตอร์เป็นประจำ เพื่อป้องกันการขโมยข้อมูลการใช้งาน

6. ติดตามข่าวสารกลโกงอย่างสม่ำเสมอ

สิ่งที่ควรทำเมื่อตกเป็นเหยื่อ

1. หากถูกแอบอ้างใช้บัญชีอีเมล ควรติดต่อผู้ให้บริการอีเมลทันที เพื่อแจ้งเปลี่ยนรหัสผ่าน

2. ในกรณีที่โอนเงินให้แก่มิจฉาชีพแล้ว...

ติดต่อฝ่ายบริการลูกค้าของสถาบันการเงินเพื่อระงับการโอนและการถอนเงิน หากไม่สามารถระงับการโอนเงินได้ ให้รวบรวมหลักฐานและข้อมูลต่าง ๆ แจ้งความต่อเจ้าหน้าที่ตำรวจ พร้อมทั้งลงบันทึกประจำวัน ณ ท้องที่เกิดเหตุ เพื่อใช้เป็นหลักฐานในการระงับการถอนเงินออกจากบัญชีที่โอนไปแจ้งระงับการถอนเงินออกจากบัญชีที่โอนไปกับสถาบันการเงินที่ใช้บริการ โดยสถาบันการเงินจะต้องตรวจสอบข้อเท็จจริงก่อน จึงจะสามารถคืนเงินได้

3. ทำใจ... เงินที่โอนไปให้มิจฉาชีพแล้ว มิจฉาชีพจะรีบถอนออกทันที ซึ่งทำให้ยากต่อการติดตาม

กลโกงอื่น ๆ

นอกจากการหลอกลวงที่เกี่ยวข้องกับบริการของสถาบันการเงินแล้ว มิจฉาชีพอาจหาทางหลอกลวงเหยื่อด้วยวิธีอื่น ๆ อีก เช่น เข้ามาทำความรู้จักและเสนอผลประโยชน์ที่เหยื่อจะได้เป็นสิ่งจูงใจ เพื่อหลอกล่อเหยื่อให้หลงเชื่อและนำเงินหรือของมีค่าอื่น ๆ มาให้มิจฉาชีพ

ลักษณะกลโกง

มิจฉาชีพอาจใช้ข้ออ้างดังต่อไปนี้

1. นายหน้าพาเข้าทำงาน

มิจฉาชีพจะอ้างกับเหยื่อว่าตนเป็นเจ้าหน้าที่ระดับสูงในบริษัท หรือรู้จักกับเจ้าหน้าที่ระดับสูงของบริษัทนั้น สามารถช่วยเหลือเหยื่อให้เข้าทำงานได้ โดยจะรับหน้าที่เจรจากับทางบริษัทให้ แต่เหยื่อต้องจ่ายเงินเพื่อเป็นค่าจ้างหรือค่านายหน้าในการช่วยเหลือให้เหยื่อได้เข้าทำงานให้ก่อน

ข้อควรสังเกต

มิจฉาชีพมักจะขอเงินล่วงหน้าจากเหยื่อ โดยที่ยังไม่ได้ดำเนินการหรือติดต่อใด ๆ กับบริษัท เพราะในความเป็นจริงแล้วมิจฉาชีพไม่สามารถทำตามที่สัญญากับเหยื่อไว้ได้

2. นายหน้าหาสินเชื่อ

มิจฉาชีพจะอ้างกับเหยื่อว่าสามารถเจรจากับเจ้าหน้าที่ธนาคารให้ปล่อยสินเชื่อให้แก่ผู้ที่มีประวัติทางการเงินไม่ดีได้ แต่ขอให้เหยื่อจ่ายค่าจ้างในการเจรจาก่อนจึงจะไปเจรจาให้

ข้อควรสังเกต

มิจฉาชีพจะร้องขอค่านายหน้าก่อนที่จะช่วยเหลือเหยื่อเพราะจริง ๆ แล้วมิจฉาชีพไม่สามารถช่วยเหลือเหยื่อได้ นอกจากนี้ สถาบันการเงินมีเงื่อนไขและเกณฑ์ในการพิจารณาสินเชื่ออยู่แล้ว ซึ่งผู้ที่จะขอกู้ได้จะต้องมีคุณสมบัติตามเกณฑ์ที่สถาบันการเงินกำหนด

3. เงินคืนประกันชีวิต

มิจฉาชีพอ้างกับเหยื่อซึ่งเป็นญาติผู้ตายในงานศพว่าเป็นเจ้าหน้าที่จากบริษัทประกันชีวิตที่ผู้ตายได้ทำไว้ แต่ผู้ตายขาดชำระเบี้ยประกันอีกเพียงหนึ่งงวด หากญาติชำระค่าเบี้ยประกันแทนผู้ตาย ก็จะได้รับเงินก้อนใหญ่ตามที่ระบุไว้ในกรมธรรม์

ข้อควรสังเกต

การทำประกันชีวิตจะมีกรมธรรม์ที่บอกรายละเอียดสัญญาระหว่างผู้รับประกันและผู้เอาประกัน จึงไม่ควรผลีผลามรีบจ่ายเงินทันที แต่ควรหากรมธรรม์ตัวจริงของผู้ตายให้เจอและทำความเข้าใจกับเงื่อนไขก่อนจ่ายเงินใด ๆ และควรติดต่อบริษัทประกันชีวิตที่ถูกอ้างถึงโดยตรงเพื่อสอบถามข้อเท็จจริง

4. นายหน้าขายที่

กลโกงลักษณะนี้จะมีมิจฉาชีพมากกว่า 2 คน มิจฉาชีพคนแรกจะแอบอ้างว่าเป็นเจ้าของที่และต้องการขายที่แปลงหนึ่ง และขอร้องให้เหยื่อช่วยติดต่อหากมีผู้สนใจซื้อ เมื่อเวลาผ่านไป มิจฉาชีพคนที่สองจะแสดงตัวว่าเป็นผู้ที่ต้องการซื้อที่ดินของมิจฉาชีพคนแรก จึงขอให้เหยื่อติดต่อเจ้าของที่ให้

เมื่อเหยื่อพามิจฉาชีพคนที่สองไปพบกับมิจฉาชีพคนหนึ่ง มิจฉาชีพคนที่สองจะทำทีว่าต้องการที่ดินนั้นเป็นอย่างมากแต่มีเงินไม่พอจ่ายค่ามัดจำ จึงขอให้เหยื่อช่วยจ่ายค่ามัดจำโดยสัญญาว่าจะจ่ายคืนให้ในวันซื้อขายพร้อมค่านายหน้าจำนวนหนึ่ง เมื่อเหยื่อหลงเชื่อช่วยจ่ายเงินค่ามัดจำไป มิจฉาชีพทั้งสองก็จะหายไปโดยไม่มีการซื้อขายที่ดินใด ๆ ทั้งสิ้น นอกจากนี้แล้วที่ดินที่กล่าวถึงนั้น ก็ไม่ได้เป็นของมิจฉาชีพคนที่หนึ่ง

ข้อสังเกต

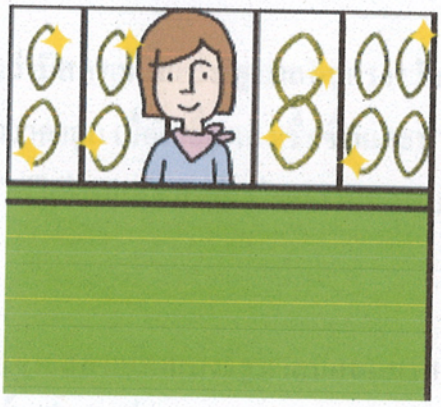
มิจฉาชีพจะทำทีว่าต้องการที่ดินเป็นอย่างมากเพื่อเร่งการตัดสินใจของเหยื่อ โดยไม่ให้เหยื่อมีเวลาทบทวนหรือปรึกษาคนอื่น

5. ตกทอง

มิจฉาชีพจะทำทีว่าเก็บทองได้แต่ติดธุระต้องรีบไป จึงเสนอให้เหยื่อนำทองไปขายโดยจะต้องจ่ายส่วนแบ่งให้กับมิจฉาชีพก่อน เมื่อเหยื่อหลงเชื่อจ่ายเงินสดให้แก่มิจฉาชีพ แล้วนำทองไปขาย ก็จะพบว่าทองนั้นเป็นทองปลอม

ข้อควรสังเกต

มิจฉาชีพจะทำทีว่ารีบ และเร่งให้เหยื่อตัดสินใจ เพื่อให้เหยื่อไม่มีเวลาคิดทบทวน และตรวจสอบทองปลอมที่มิจฉาชีพถือมาให้



6. หวยปลอม

มิจฉาชีพอ้างว่ามีสลากกินแบ่งรัฐบาลที่ถูกรางวัลที่หนึ่งอยู่ แต่ไม่สะดวกที่จะนำไปแลกรางวัล จึงเสนอขายให้เหยื่อในราคาถูก เมื่อเหยื่อหลงเชื่อซื้อและนำสลาก ฯ ไปขึ้นรางวัล จึงพบว่าสลาก ฯ นั้นเป็นของปลอม นอกจากไม่ได้เงินแล้ว ยังต้องโทษตามกฎหมายอีกด้วย

ข้อควรสังเกต

มิจฉาชีพมักจะหลอกขายสลากกินแบ่งรัฐบาลปลอมมาหลังจากที่มีการประกาศรางวัลแล้ว เพื่อให้เหยื่อเข้าใจว่าสลาก ฯ ใบนั้นเป็นใบที่ถูกรางวัลจริง

7. เงินกู้เพื่อเกษตรกร

มิจฉาชีพจะหลอกใช้เครือข่ายในชุมชน เช่น ผู้นำชุมชนหรือผู้กว้างขวาง กระจายข่าวหรือประกาศผ่านสื่อต่าง ๆ ว่าได้รับเงินทุนจากองค์กรต่างประเทศจำนวนมาก เพื่อนำมาให้เกษตรกรหรือคนในชุมชนกู้ยืมในระยะยาว ดอกเบี้ยต่ำ และไม่ต้องมีหลักประกัน โดยคนที่สนใจสามารถสมัครเป็นสมาชิกโดยไม่เสียค่าใช้จ่าย แต่ต้องจ่ายค่าธรรมเนียมในการดำเนินการ หรือค่าจัดทำเอกสาร เช่น รายละ 200 – 500 บาท เมื่อเหยื่อหลงเชื่อสมัครและจ่ายเงิน มิจฉาชีพจะแจ้งเหยื่อว่า ยังไม่สามารถให้เงินกู้ได้ด้วยเหตุผลต่าง ๆ เช่น เงินอยู่ระหว่างการตรวจสอบของธนาคารแห่งประเทศไทยหรือองค์กรอื่น ๆ รวมทั้งอาจมีเอกสารที่แสดงการติดตามเรื่องถึงนายกรัฐมนตรี เพื่อซื้อเวลาและสร้างความมั่นใจว่าไม่ได้หลอกลวง โดยอาจขอให้เหยื่อจ่ายค่าธรรมเนียมหรือค่าดำเนินการอื่น ๆ เพิ่มเติม

ดังนั้น หากมีคนชักชวนให้เข้าร่วมโครงการในลักษณะนี้ ควรตรวจสอบข้อเท็จจริงจากที่ว่าการอำเภอ ศาลากลางจังหวัด หรือหน่วยงานที่มิจฉาชีพนำมาแอบอ้างโดยตรง ก่อนที่จะตัดสินใจเข้าร่วมโครงการ หรือจ่ายเงินค่าธรรมเนียมต่างๆ ไม่ควรหลงเชื่อจากคำโฆษณา และหรือเอกสารที่ผู้ชักชวนนำมาแสดงเพียงฝ่ายเดียว เพราะอาจเป็นเอกสารปลอม หรือเอกสารที่จงใจทำขึ้นเพื่อหลอกลวงเกษตรกรได้

วิธีป้องกัน

ทบทวนข้อมูลที่ได้รับจากมิจฉาชีพว่ามีความน่าจะเป็นมากน้อยแค่ไหน

หากมีการกล่าวอ้างถึงสถาบันการเงิน หรือบุคคลที่สาม ควรติดต่อกับสถาบันการเงินหรือบุคคลนั้น ๆ เพื่อสอบถามข้อเท็จจริง

ไม่ควรหลงเชื่อกับผลประโยชน์ที่มิจฉาชีพนำมาหลอกล่อ

สิ่งที่ควรทำเมื่อตกเป็นเหยื่อ

รวบรวมเอกสารและหลักฐาน (หากมี) แจ้งความต่อเจ้าหน้าที่ตำรวจ เพื่อเป็นหลักฐานและเบาะแสในการติดตามคนร้าย

ทำใจ...เมื่อจ่ายเงินหรือให้ของแก่มิจฉาชีพแล้ว มิจฉาชีพจะรีบหนีออกจากพื้นที่ ซึ่งทำให้ยากต่อการติดตาม

แชร์ลูกโซ่ ภัยร้ายคู่สังคมไทย จะมีวิธีสังเกตได้อย่างไรว่าธุรกิจไหนมีความเสี่ยง เพื่อป้องกันการตกเป็นเหยื่อของกลุ่มมิจฉาชีพ

ขบวนการหลอกลวงอย่าง "**แชร์ลูกโซ่**" อยู่คู่กับสังคมไทย ทุกยุค ทุกสมัย และไม่เคยหายห่างไปไหนเลย แม้ปัจจุบันเราจะสามารถเข้าถึงข้อมูลข่าวสารได้อย่างรวดเร็ว ก็ยังมีหลายคนหลงเชื่อไปกับกลุ่มมิจฉาชีพเป็นจำนวนมาก เพราะความโลภ และความอยากรวยทางลัด จึงเป็นจุดอ่อนให้มิจฉาชีพหลอกเอาเงินไปได้ แม้กระทั่งในยุคที่การติดต่อสื่อสารสะดวกรวดเร็วมากขึ้น แต่ทว่านี่กลับเป็นดาบสองคมที่ถูกกลุ่มมิจฉาชีพนำจุดนี้มาหลอกลวงให้คนตกเป็นเหยื่อ สร้างเครือข่ายจำนวนมากได้อย่างรวดเร็ว

โดยปัจจุบันการหลอกลวงแฝงมากับธุรกิจที่ซับซ้อนขึ้น และปรับเปลี่ยนรูปแบบให้ตอบโจทย์คนในแต่ละยุคสมัย ทำให้มีคนตกเป็นเหยื่อได้อย่างไม่น่าเชื่อ ตั้งแต่ สินค้าเกษตร น้ำมัน เงินตราต่างประเทศ การจัดสัมมนาขายตรง หรือแม้แต่ธุรกิจทัวร์ต่างประเทศเอง ก็ยังมีมิจฉาชีพนำมาแปรสภาพเพื่อหลอกลวงต้มตุ๋นเอาเงินไปได้แบบเนียน ๆ

เพราะฉะนั้น เพื่อไม่ให้ตกเป็นเหยื่อของขบวนการแชร์ลูกโซ่ มาดูกันว่าจะมีวิธีสังเกตเบื้องต้นอย่างไรบ้าง ว่าธุรกิจนั้น เข้าข่ายแชร์ลูกโซ่หรือเปล่า และยังมีกลลวงอะไรอีกที่เราต้องรู้เท่าทัน จะได้ไม่ตกเป็นเหยื่อง่าย ๆ

แชร์ลูกโซ่ คืออะไร

ก่อนอื่นมาทำความเข้าใจกันก่อนว่า แชร์ลูกโซ่นั้นคืออะไร โดยแชร์ลูกโซ่ **จะเน้นการระดมทุนจากสมาชิก จูงใจด้วยผลตอบแทนสูง และมักอ้างว่านำไปลงทุนในธุรกิจที่มีกำไรดี แต่จริง ๆ แล้วต้องการที่จะหาสมาชิกใหม่ให้ได้มาก ๆ เพื่อนำเงินจากรายใหม่มาจ่ายให้รายเก่า ซึ่งจะทำแบบนี้เป็นทอด ๆ กันเป็นลูกโซ่** ท้ายที่สุดจนเมื่อถึงจุดที่ธุรกิจหมุนเงินไม่ทัน ก็จะเริ่มเลื่อนการจ่ายผลตอบแทน และหนีไปในที่สุด ทิ้งสมาชิกจำนวนมากไว้เบื้องหลัง

ภาพจาก ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน

สังเกตได้อย่างไร ว่านี่คือแชร์ลูกโซ่

1. เปิดระดมทุนไม่อั้น

ไม่ว่าใครก็สามารถเข้ามาลงทุนกับธุรกิจเครือข่ายนี้ได้ รวมทั้งยังได้รับเงินส่วนต่างพิเศษเพิ่มอีก หากมีการชักชวนคนอื่นให้เข้ามาลงทุนด้วย

2. การันตีผลตอบแทนสูงมาก

มีการรองรับผลตอบแทนที่จะได้สูงมาก ๆ จากการลงทุนในระยะเวลาอันสั้น เพื่อเรียกความสนใจให้เราเข้าไปลงทุน และหว่านล้อมด้วยวิธีต่าง ๆ ให้เรารีบตัดสินใจเข้าลงทุน

3. ตรวจสอบข้อมูลการเงินไม่ได้

เป็นบริษัทที่ไม่สามารถตรวจสอบงบการเงิน หรือข้อมูลการทำธุรกิจได้ ว่าได้กำไรมาจากไหน เอาเงินที่ได้ไปทำอะไรบ้าง รวมถึงไม่สามารถตรวจสอบงบการเงินที่ได้รับรองจากหน่วยงานที่น่าเชื่อถือได้ ทั้งนี้ เราสามารถตรวจสอบงบการเงินเบื้องต้นของแต่ละบริษัทได้จากเว็บไซต์ของกระทรวงพาณิชย์ หรือเว็บไซต์ตลาดหลักทรัพย์แห่งประเทศไทย

4. เชียร์ให้รีบตัดสินใจลงทุน

ธุรกิจแชร์ลูกโซ่ มีจุดประสงค์หลักคือขยายเครือข่ายไปให้มากที่สุด ดังนั้นจึงต้องหาสมาชิกเข้ามาลงทุนด้วยมาก ๆ ซึ่งหากสังเกตได้ว่ามีการหว่านล้อมให้เรารีบเข้าลงทุนโดยเร็ว หรือสร้างบรรยากาศต่าง ๆ ให้คนอยากเข้าลงทุนมากจนเกินปกติ ก็มีโอกาสสูงที่จะเป็นธุรกิจแชร์ลูกโซ่

5. จัดอบรมสัมมนาใหญ่โต

มีการจัดงานอบรมสัมมนาใหญ่โต แล้วเชิญเราเข้าไปรับฟังแผนธุรกิจต่าง ๆ ของบริษัท แต่จริง ๆ แล้วมีจุดประสงค์เพียงแค่ต้องการให้คนเข้าร่วมสัมมนาคล้อยตามและรีบสมัครเป็นสมาชิก

6. อ้างว่ามีบุคคลที่มีชื่อเสียงร่วมลงทุนด้วย

เป็นวิธีหลอกล่อให้คนสนใจร่วมลงทุนมากขึ้น โดยการอ้างบุคคลที่มีชื่อเสียง ไม่ว่าจะเป็นนักแสดง นักร้อง หรือนักธุรกิจชื่อดัง ว่าได้ร่วมลงทุนในธุรกิจนี้เช่นกัน

แชร์ลูกโซ่มีกี่รูปแบบ อะไรบ้าง ?

แชร์ลูกโซ่มีการปรับเปลี่ยนอยู่ตลอดเวลา ออกมาเป็นหลากหลายรูปแบบ และได้ระบาดไปทั่วทุกสายอาชีพ ประกอบกับยังมีความสลับซับซ้อนมากขึ้นเรื่อย ๆ เรามาดูกันว่าแชร์ลูกโซ่ที่เรามีโอกาสพบเห็นมีแบบไหนบ้าง

1. ลงทุนในสินค้าเกษตร

เป็นรูปแบบที่เกิดขึ้นมานาน แต่ก็ยังมีการนำมาหลอกลวงด้วยการปรับเปลี่ยนวิธีอยู่เรื่อย ๆ โดยหลัก ๆ จะเป็นการหลอกให้เข้ามาลงทุนกองทุนสินค้าเกษตร และการันตีผลตอบแทนที่สูง ซึ่งจะมีการปั่นราคาสินค้าชนิดนั้นในตลาด เพื่อหลอกให้เหยื่อสนใจ ซึ่งที่ผ่านมามีสินค้าเกษตรหลายชนิดที่ถูกนำไปใช้เป็นเครื่องมือ เช่น พันธุ์ไม้กฤษณา ไม้สัก มะม่วง เป็นต้น

2. ขายตรง

ธุรกิจขายตรงบางแห่ง มักแฝงมากับขบวนการแชร์ลูกโซ่ โดยใช้สินค้าเป็นตัวบังหน้าเท่านั้น แต่ต้องการเพียงขยายฐานสมาชิก โดยจะมีการเก็บค่าสมัครสมาชิกและบังคับให้ซื้อสินค้าที่มีคุณภาพต่ำ ในราคาสูง

3. ระดมทุนตั้งบริษัทเข้าตลาดหลักทรัพย์

เป็นการขายฝันเพื่อชักชวนให้เข้าร่วมถือหุ้นในบริษัท โดยหลอกว่าบริษัทมีแผนจะเข้าจดทะเบียนในตลาดหลักทรัพย์ แต่ต้องการที่จะหาสมาชิกให้มากพอก่อน เพื่อจะได้ให้เราไปชักชวนคนอื่นมาร่วมลงทุนด้วย

4. ผลิตภัณฑ์อวดอ้างสรรพคุณรักษาได้สารพัดโรค

หลอกลวงเงินของชาวบ้าน โดยการจำหน่ายผลิตภัณฑ์รักษาโรค แล้วแอบอ้างว่ามีสรรพคุณพิเศษผ่านการใช้โฆษณาชวนเชื่อ จนมีคนหลงเชื่อซื้อมาใช้ จากนั้นจึงสร้างเครือข่ายสมาชิกหลอกให้คนนำเงินมาร่วมลงทุน ทำให้ผู้ตกเป็นเหยื่อเสียทั้งทรัพย์สิน และอาจมีความเสี่ยงต่อสุขภาพจากการทานยาที่ไม่มีคุณภาพอีกด้วย

5. ลงทุนเก็งกำไรอัตราแลกเปลี่ยนต่างประเทศ

เป็นการชักชวนให้เข้าลงทุนในตลาดอัตราแลกเปลี่ยนระหว่างประเทศ ซึ่งแสดงให้เห็นถึงผลตอบแทนจำนวนมาก ทำให้หลายคนหลงเชื่อเข้าไปลงทุน โดยที่ไม่รู้ว่าธุรกิจดังกล่าวผิดกฎหมาย และไม่ได้รับการรับรองจากธนาคารแห่งประเทศไทย

6. ลงทุนทองคำ และน้ำมัน

มีการจูงใจให้คนเข้ามาร่วมลงทุนเก็งกำไรในราคาทองคำและน้ำมันดิบ โดยหลอกว่าหากเข้ามาลงทุนด้วยจะได้รับผลตอบแทนที่สูงกว่าท้องตลาด รวมถึงยังการันตีผลตอบแทนทุกเดือน

7. คนดังชวนลงทุนทำธุรกิจ

ใช้ชื่อเสียงของคนดังต่าง ๆ ออกมาโฆษณาชักชวนให้คนร่วมลงทุนทำธุรกิจด้วย โดยเอาชื่อเสียงตัวเองการันตีว่าไม่มีการหลอกลวง และให้ตอบแทนที่คุ้มค่าแน่นอน ทำให้หลายคนหลงเชื่อ ตกเป็นเหยื่อจำนวนมาก

8. แชร์ลูกโซ่ออนไลน์

แชร์ลูกโซ่ออนไลน์เป็นการหลอกลวงทาง Social Media ต่าง ๆ เช่น Line Facebook โดยชักชวนให้เล่นแชร์เป็นแพ็กเกจ มีการจ่ายดอกเบี้ยเป็นเงินปันผลทุกสัปดาห์ และเมื่อวงแชร์มีขนาดใหญ่มากพอ ก็จะปิดวงแชร์แล้วหลบหนีเอาเงินไป

9. ฌาปนกิจสงเคราะห์ปลอม

พบเห็นได้มากในต่างจังหวัด โดยเป็นการชักชวนให้สมัครเป็นสมาชิกเพื่อจ่ายเงินสมทบกองทุนสวัสดิการฌาปนกิจสงเคราะห์รายเดือน โดยมีการจ่ายค่าสมัครครั้งแรก และจ่ายเงินสมทบเข้าทุก ๆ เดือน

ซึ่งเมื่อครบตามกำหนดจะได้เงินค่าฌาปนกิจศพ สุดท้ายก็นำเงินหลบหนีไป ไม่จ่ายตามสัญญา

10. ขายทริปเที่ยวในฝัน

เป็นกรณีที่เกิดขึ้นเร็ว ๆ นี้ จากการสร้างธุรกิจเครือข่ายที่นำแพ็กเกจท่องเที่ยวราคาถูกมาเป็นตัวล่อให้มีการจ่ายค่าสมัครแรกเข้า และจ่ายค่าสมาชิกรายเดือน เพื่อมีสิทธิ์ในการซื้อแพ็กเกจท่องเที่ยว รวมทั้งยังมีการหลอกให้ซื้อแพ็กเกจราคาถูกกว่าปกติ เพื่อจูงใจคน แล้วเอาเงินที่ได้หลบหนีไป

ทั้งนี้ เป็นเพียงตัวอย่างลักษณะแชร์ลูกโซ่ที่มีโอกาสพบเห็นได้บ่อย แต่ยังมีอีกหลากหลายรูปแบบที่กลุ่มมิจฉาชีพนำมาปรับเปลี่ยนวิธีการเพื่อใช้หลอกลวงอยู่เรื่อย ๆ

แชร์ลูกโซ่ ผิดกฎหมายหรือไม่

แชร์ลูกโซ่ ถือว่าเป็นการกระทำที่ผิดกฎหมายอย่างแน่นอน เพราะเข้าข่ายการฉ้อโกง และหลอกลวงผู้บริโภคให้หลงเชื่อ ซึ่งเกี่ยวข้องกับประมวลกฎหมายอาญา ความผิดฐานฉ้อโกง และพระราชกำหนดการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน พ.ศ. 2527 โดยมีโทษจำคุกกระทงละ 3-5 ปี และโทษปรับวันละ 1 หมื่นบาท

รวมทั้งอาจยังเข้าข่าย ความผิดฐานฟอกเงินตาม พ.ร.บ.ป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มีโทษจำคุกตั้งแต่ 1-10 ปี หรือปรับตั้งแต่ 20,000 – 200,000 บาท หรือทั้งจำทั้งปรับ

อย่างไรก็ตาม การที่จะเอาผิดแชร์ลูกโซ่ในปัจจุบัน ยังทำได้ยากและไม่สามารถเข้าจับกุมได้ทันที ต้องรอให้มีผู้เสียหายร้องให้ดำเนินคดีก่อน ประกอบกับต้องมีการสอบสวนรวบรวมหลักฐานอย่างยาวนานกว่าคดีจะ

สิ้นสุด ดังนั้น จึงควรระวังตัวเพื่อไม่ให้ตกเป็นเหยื่อตั้งแต่แรกจะดีที่สุด

ตกเป็นเหยื่อแชร์ลูกโซ่แล้ว ทำอะไรได้บ้าง

หากใครที่รู้ตัวว่าหลงกลให้กับกลุ่มมิจฉาชีพไปแล้ว ให้รีบดำเนินการตามนี้ได้เลย

1. เก็บรวบรวมหลักฐานทุกอย่างที่เกี่ยวข้องไว้ ไม่ว่าจะเป็น หนังสือสัญญา หลักฐานการโอนเงิน เบอร์โทรศัพท์ ที่อยู่สำนักงาน หรือรูปถ่ายต่าง ๆ ที่เกี่ยวข้อง

2. รีบเข้าแจ้งความร้องทุกข์ เพื่อดำเนินคดีเอาผิดตามกฎหมาย โดยสามารถเข้าแจ้งความร้องทุกข์ หรือแจ้งเบาะแสที่น่าสงสัยได้ที่ กรมสอบสวนคดีพิเศษ (ดีเอสไอ) หรือโทร. 1202

นอกจากนี้ ยังสามารถใช้แอปพลิเคชัน บนมือถือของดีเอสไอที่ชื่อว่า **"DSI (กรมสอบสวนคดีพิเศษ)"** ทั้งระบบ Android และ iOS เพื่อใช้ในการร้องเรียน ร้องทุกข์ แจ้งเบาะแส ได้อีกทาง

ภาพจาก กรมสอบสวนคดีพิเศษ

ย้อนบทเรียน 3 คดีแชร์ลูกโซ่ชื่อดัง

1. แชร์แม่ชม้อย

นางชม้อย ทิพย์โส อดีตพนักงานขององค์การเชื้อเพลิง ได้จัดให้มีการระดมเงิน โดยอ้างว่านำไปลงทุนในธุรกิจน้ำมัน และกำหนดวิธีการเล่นให้ลงเงินเป็นทุนในการซื้อรถขนน้ำมัน ซึ่งมีคนมาลงเงินจำนวนมาก เพราะได้รับผลตอบแทนทันทีใน 15 วัน ที่อัตราเดือนละ 6.5% หรือปีละ 78% จึงมีคนสนใจนับหมื่นราย

แต่แท้จริงแล้ว นางชม้อย ได้นำเงินจากผู้ลงทุนรายใหม่ มาจ่ายเป็นผลตอบแทนให้กับผู้ลงทุนรายแรก ๆ วนซ้ำไปเรื่อย ๆ จนในที่สุดไม่สามารถนำเงินมาจ่ายได้ เพราะไม่มีผู้เล่นเพิ่มเติม ซึ่งมีผู้เสียหายจากคดีดังกล่าวกว่า 16,000 ราย มีการเข้าแจ้งความเอาผิดกับนางชม้อยและพวก รวมมูลค่าความเสียหายถึง 4,500 ล้านบาท ทำให้นางชม้อยถูกตัดสินจำคุก 154,005 ปี

2. แชร์ลูกโซ่ยูฟัน

มาจากที่ บริษัท ยูฟัน สโตร์ จำกัด ซึ่งเป็นบริษัทสัญชาติมาเลเซีย ได้เข้ามาจดทะเบียนจัดตั้งในไทย ด้วยทุนจดทะเบียน 10 ล้านบาท โดยแจ้งประกอบธุรกิจขายปลีกทางอินเทอร์เน็ต และมีการออกสกุลเงินเองเรียกว่า ยูโทเคน (UToken Cash) ซึ่งเป็นสกุลเงินรูปแบบดิจิทัล เพื่อใช้ซื้อขายแลกเปลี่ยนในโลกออนไลน์ โดยมีค่าสมัครเป็นสมาชิกคนละ 17,000 บาท จนถึง 1,750,000 บาท

อีกทั้งมีการชักชวนให้สมาชิกเข้ามาร่วมเครือข่าย และได้รับผลตอบแทนจากการชวนบุคคลอื่นเข้าร่วม ทำให้มีผู้หลงเชื่อตกเป็นเหยื่อถูกหลอกสูญเงินเป็นจำนวนมาก ซึ่งคดีนี้มีผู้เสียหายทั้งหมด 2,451 คน มูลค่าความเสียหายกว่า 356 ล้านบาท

ภาพจาก ข่าวช่อง8

3. คดีซินแสโชกุน

ซินแสโชกุน หรือ นางสาวพสิษฐ์ อริญชย์ลาภิศ ได้ทำการหลอกลวงโดยการชักชวนให้ผู้เสียหายเข้าเป็นสมาชิกของบริษัทผลิตภัณฑ์อาหารเสริม และอ้างว่าจะมีสิทธิ์ได้เดินทางไปท่องเที่ยวต่างประเทศ อาทิ ญี่ปุ่น ฮ่องกง เกาหลี โดยหลอกให้สมาชิกเชื่อใจ จากการพาไปเที่ยวต่างประเทศจริง ใน 3-4 ครั้งแรก เพื่อให้กลุ่มสมาชิกที่ได้ไปเที่ยวชักชวนคนอื่น ๆ เข้ามาสมัครเพิ่มเติม จนสุดท้ายกลับมีการลอยแพสมาชิกที่จะเดินทางไปประเทศญี่ปุ่น ให้ตกค้างที่สนามบินสุวรรณภูมิ โดยคดีดังกล่าวมีมูลค่าความเสียหายกว่า 51 ล้านบาท

เป็นเรื่องที่ทุกคนต้องระวังตัวอย่างยิ่ง เพื่อไม่ให้ตกเป็นเหยื่อของกลุ่มมิจฉาชีพ เพราะความโลภของตนเอง ซึ่งธุรกิจแชร์ลูกโซ่ยังมีรูปแบบที่หลากหลาย เพราะฉะนั้นควรหมั่นติดตามข่าวสาร และมีสติอย่าหลงเชื่ออะไรง่าย ๆ ซึ่งหากไม่มั่นใจว่าธุรกิจไหนมีความเสี่ยง สามารถสอบถามข้อมูลเพิ่มเติมกับหน่วยงานที่เกี่ยวข้องดังต่อไปนี้

- สำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.) โทร. 1166
- กรมสอบสวนคดีพิเศษ (ดีเอสไอ) โทร. 1202
- กรมพัฒนาธุรกิจการค้า โทร. 1570
- สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ โทร. 1207
- ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน โทร. 1213