

บทเรียนที่ 5



แนวทางการป้องกันและ
แก้ไขปัญหที่เกิดขึ้น
ในการทำธุรกรรมทางอิเล็กทรอนิกส์

สาระการเรียนรู้



1. ปัญหาในการทำธุรกรรมทางอิเล็กทรอนิกส์ที่พบมากในปัจจุบัน
2. แนวทางการป้องกันและแก้ไขปัญหาในการทำธุรกรรมทางอิเล็กทรอนิกส์



1. ปัญหาในการทำธุรกรรมทางอิเล็กทรอนิกส์ ที่พบมากในปัจจุบัน

ปัญหาในการทำธุรกรรมทางอิเล็กทรอนิกส์ที่เกิดขึ้นในปัจจุบัน มีดังนี้

1. การฉ้อโกง

ประมวลกฎหมายอาญา มาตรา 341 บัญญัติว่า “ผู้ใดโดยทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง และโดยการหลอกลวงดังว่านั้นได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สามทำ ถอน หรือทำลายเอกสาร สิทธิ ผู้นั้นกระทำความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ” และมาตรา 343 บัญญัติว่า “ถ้าการกระทำความผิดตามมาตรา 341 ได้กระทำได้ด้วยการแสดงข้อความอันเป็นเท็จต่อประชาชน หรือด้วยการปกปิดความจริงซึ่งควรบอกให้แจ้งแก่ประชาชนผู้กระทำความผิดต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ...” แสดงให้เห็นถึงลักษณะของการฉ้อโกงมีอยู่ 2 แบบ คือ การฉ้อโกงที่มุ่งเน้นการหลอกลวงผู้อื่น และการฉ้อโกงประชาชนที่มุ่งเน้นเหยื่อจำนวนมากกว่า

1 คน



รูปแบบของการฉ้อโกงในการทำธุรกรรมทางอิเล็กทรอนิกส์ในปัจจุบัน มีหลายลักษณะ ดังนี้

ลักษณะที่ 1

ผู้ขายโฆษณาขายสินค้า แต่เมื่อผู้ซื้อสั่งซื้อสินค้าทางออนไลน์และโอนเงินเพื่อชำระค่าสินค้า ผู้ขายกลับไม่ส่งสินค้า การฉ้อโกงในรูปแบบนี้ ผู้ขายมักสร้างข้อมูลส่วนตัวให้ดูดี เสนอราคาสินค้าที่ยั่วยุให้เกิดการตัดสินใจทำธุรกรรมด้วย เมื่อเหยื่อหลงเชื่อและโอนเงินซื้อสินค้า ผู้ขายจึงหลบหนีไป





ลักษณะที่ 2

ผู้ขายทำที่ปลอมข้อมูลส่วนตัวเป็นผู้มีฐานะดี เดินทางไปต่างประเทศบ่อย หรือพนักงานต้อนรับบนเครื่องบิน กัปตัน เพื่อหลอกผู้ซื้อสั่งซื้อสินค้าล่วงหน้า (Pre-Order) เมื่อเหยื่อหลงเชื่อก็หลบหนีไป

ลักษณะที่ 3

หลอกว่ามีพัสดุที่สั่งซื้อทางอินเทอร์เน็ต และให้ผู้ซื้อชำระเงินปลายทาง เมื่อเปิดหีบห่อพัสดุกลับไม่มีสินค้า หรือในหีบห่อมีสินค้าผิดกฎหมาย จากนั้นให้มิจฉาชีพปลอมตัวเป็นตำรวจเข้าจับกุมและหวานล่อมให้จ่ายเงินเพื่อไม่ดำเนินคดี

ลักษณะที่ 4

หลอกให้ลงทุน โดยอาชญากรทำที่เป็นนักลงทุนที่เสนอตอบแทนผล
ลงทุนจำนวนมาก เมื่อบุคคลตัดสินใจเข้าลงทุนก็จะถูกโกง โดยใน
ระยะแรกอาจจะให้ผลตอบแทนในอัตรา ที่สูงเพื่อชักจูงให้เหยื่อลงทุน
เพิ่มเติม จากนั้นจึงหลบหนีไป

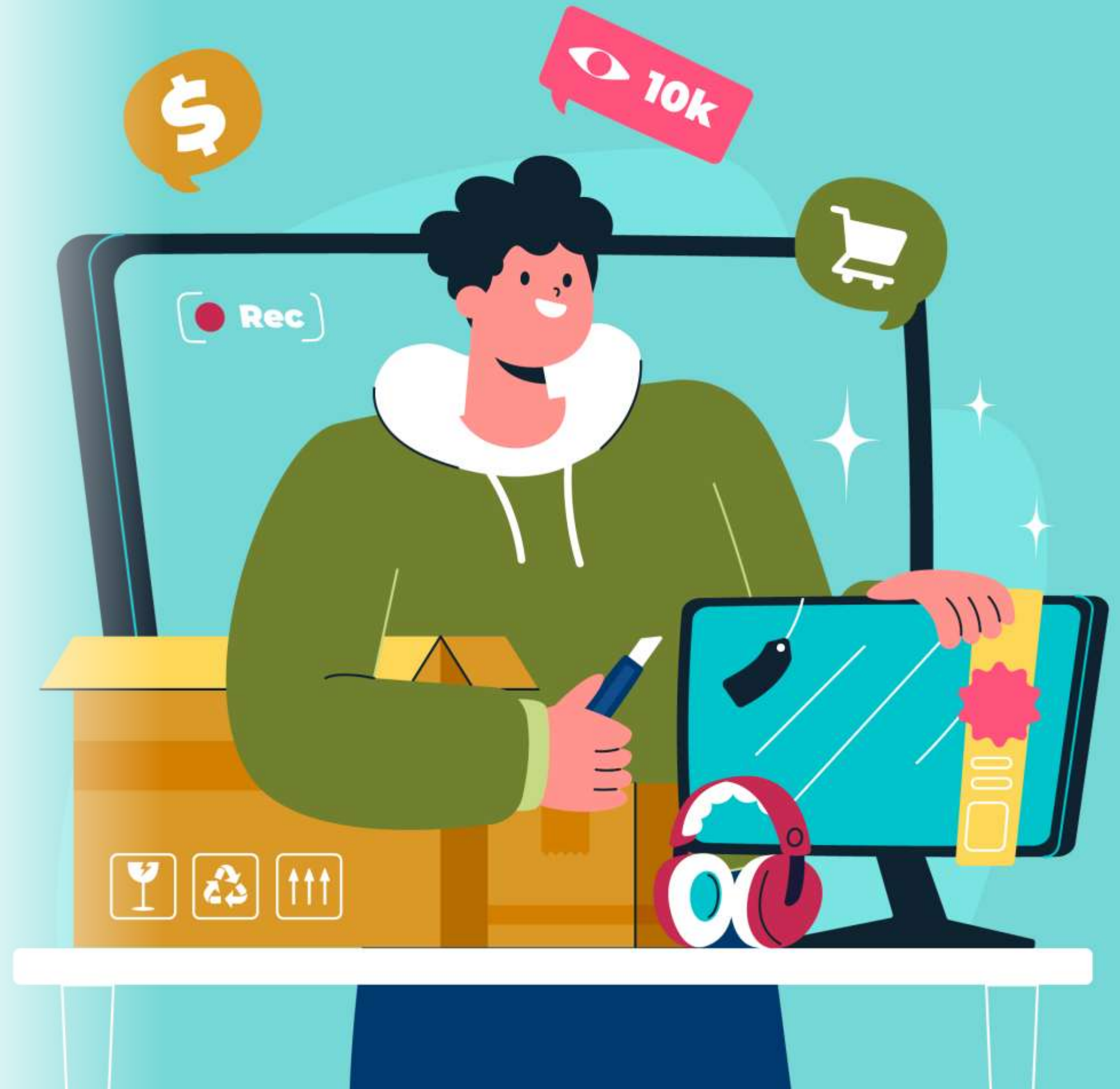
ลักษณะที่ 5

หลอกลวงให้โอนเงิน โดยวางอุบายรูปแบบต่าง ๆ เช่น มีสินค้า
ตกค้างจำเป็นต้องโอนเงินไปไถ่ออก บัญชีไปพัวพันกับการโอนเงินให้โอน
เงินไปพักยังบัญชีของราชการ มียอดคงค้างชำระบัตรเครดิต หรือกระทั่ง
การปลอมตนเป็นคนรู้จัก



2. ลวงขาย

ประมวลกฎหมายอาญา มาตรา 271 บัญญัติว่า “ผู้ใดขายของโดยหลอกลวงด้วยประการใด ๆ ให้ผู้ซื้อหลงเชื่อในแหล่ง กำเนิด สภาพ คุณภาพ หรือปริมาณแห่ง ของนั้นอันเป็นเท็จ ถ้า การกระทำนั้นไม่เป็นความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ” การลวงขาย (Passing Off) จึงเป็นกรณีที่ผู้ซื้อและผู้ขายตกลงซื้อขายสินค้ากัน และผู้ซื้อได้รับสินค้าแล้วแต่สินค้าที่ได้มานั้นไม่เหมือนที่เคยตกลงกันไว้ ทั้งเรื่องของคุณภาพ แหล่งผลิต สภาพสินค้า ปริมาณไม่ครบจำนวน





การลงขายสินค้าอาจจะเกิดขึ้นได้หลายลักษณะ เช่น

ลักษณะที่ 1

การขายสินค้าประเภทหนึ่งแต่ผู้ซื้อได้รับสินค้าอีกประเภทหนึ่ง

ลักษณะที่ 2

การขายสินค้าและส่งสินค้าประเภทเดียวกันให้แก่ผู้ซื้อแต่สินค้าเป็นสินค้าปลอม

ลักษณะที่ 3

การขายสินค้าและส่งสินค้าประเภทเดียวกัน แต่เป็นสินค้าที่แตกหักหรือชำรุดบกพร่อง


3. โอนเงินผิด

ในอดีตบุคคลจะใช้บริการโอนเงินผ่านเคาน์เตอร์ธนาคาร ซึ่งมี
นายธนาคารคอยให้ความช่วยเหลือเกี่ยวกับการสอบถามข้อบัญญัติ
และจำนวนเงินในการโอนเงิน แต่เมื่อเปลี่ยนมาเป็นการโอนเงิน
ผ่านธนาคารอิเล็กทรอนิกส์ที่บุคคลสามารถโอนเงินได้ด้วยตนเอง
ส่งผลให้เกิดการโอนเงินผิดทั้งผิดบัญชีและผิดจำนวนสำหรับการ
โอนเงินผิดบัญชี ตามกฎหมายแล้ว ธนาคารจะไม่สามารถโอนเงิน
คืนให้แก่ผู้โอนเงินผิด หากเจ้าของบัญชีปลายทางไม่ยินยอม
เพราะธนาคารไม่มีสิทธิในการดึงเงินออกจากบัญชีโดยพลการ แต่
ธนาคารจะเป็นตัวกลางช่วยประสานงานขอคืนเงินให้เท่านั้น



ในทางกฎหมาย จะมีฐานการคืบเงินรองรับอยู่ในฐาน
ลาภมิควรได้ กล่าวคือ ประมวลกฎหมายแพ่งและพาณิชย์
มาตรา 406 บัญญัติว่า “บุคคลใดได้มาซึ่งทรัพย์สินใดเพราะ
การที่บุคคลอีกคนหนึ่งกระทำให้เพื่อชำระหนี้ก็ดี หรือได้มาด้วย
ประการอื่นก็ดี โดยปราศจากมูลอันจะอ้างกฎหมายได้ และ
เป็นทางให้บุคคลอีกคนหนึ่งนั้นเสียเปรียบไซ้รู้ ท่านว่าบุคคล
นั้นจำต้องคืนทรัพย์สินให้แก่เขา อนึ่งการรับสภาพหนี้สินว่ามี
อยู่หรือหาไม่นั้น ท่านก็ให้ถือว่าเป็นการกระทำให้เพื่อชำระหนี้
ด้วย...” ฉะนั้นผู้รับเงินที่โอนผิดไป ก็ตกอยู่ในฐานะของผู้ที่
ได้ลาภมิควรได้จะต้องคืนทรัพย์สินให้แก่ผู้นั้น



A close-up photograph of a judge's hand holding a wooden gavel with a gold band, resting it on a dark wooden surface. In the background, a hand is seen writing on a document with a pen. The scene is dimly lit, focusing on the gavel and the writing hand.

ในทางกฎหมาย จะมีฐานการคืนเงินรองรับอยู่ในฐานลามิควรได้ กล่าวคือ ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 406 บัญญัติว่า “บุคคลใด ได้มาซึ่งทรัพย์สินใดเพราะการที่บุคคลอีกคนหนึ่งกระทำให้ชำระหนี้ก็ดี หรือได้มา ด้วยประการอื่นก็ดี โดยปราศจากมูลอันจะอ้างกฎหมายได้ และเป็นทางให้บุคคล อีกคนหนึ่งนั้นเสียเปรียบไซ้ ท่านว่าบุคคลนั้นจำต้องคืนทรัพย์สินให้แก่เขา อนึ่งการ รับสภาพหนี้สินว่ามีอยู่หรือหาไม่นั้น ท่านก็ให้ถือว่าเป็นการกระทำให้ชำระหนี้ ด้วย...” ฉะนั้นผู้รับเงินที่โอนผิดไป ก็ตกอยู่ในฐานะของผู้ที่ได้ลามิควรได้จะต้อง คืนทรัพย์สินให้แก่ผู้นั้น

ทั้งนี้ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 412 บัญญัติว่า “ถ้า ทรัพย์สินซึ่งได้รับไว้เป็นลามิควรได้นั้นเป็นเงินจำนวนหนึ่ง ท่านว่าต้องคืน จำนวนนั้น เว้นแต่เมื่อบุคคลได้รับไว้โดยสุจริต จึงต้องคืนลามิควรได้เพียงส่วนที่ ยังมีอยู่ในขณะเมื่อเรียกคืน” หมายความว่าผู้ที่ได้รับเงินโอน หากเข้าใจโดยสุจริต ว่าเงินนั้นเป็นของตนจริง ๆ แล้วได้ใช้ไป ให้คืนแก่เจ้าของเท่าที่เหลืออยู่ ในทาง กลับกันหากบุคคลนั้นรู้แล้วว่าเงินที่ตนได้ลามิควรได้มา แต่ไม่ยอมคืนแก่เจ้าของ จะเป็นความผิดอาญาฐานยักยอกทรัพย์

4. ถูกแฮ็ก (hack)

การแฮ็กเป็นลักษณะของอาชญากรรมคอมพิวเตอร์รูปแบบหนึ่ง โดยผู้ถูกกระทำเรียกว่า แฮ็กเกอร์ (Hacker) ซึ่งเน้นการกระทำต่อข้อมูลของผู้เสียหาย แฮ็กเกอร์บางรายทำด้วยความสนุกคึกคะนอง แต่แฮ็กเกอร์บางรายนำข้อมูลของเหยื่อไปใช้ในทางมิชอบ เช่น ไปเปิดบัญชีเพื่อฟอกเงิน ไปปลอมตัวเป็นเหยื่อเพื่อยืมเงิน หรือใช้ประโยชน์จากข้อมูลในการทำธุรกรรมต่าง ๆ หรือกระทั่งเรียกค่าไถ่จากเหยื่อ โดยนำข้อมูลคอมพิวเตอร์เป็นประกันการแฮ็กกระทำได้หลายรูปแบบตั้งแต่วิธีการง่าย ๆ ด้วยการหลอกเหยื่อให้ทำธุรกรรม โดยให้เหยื่อใส่ข้อมูลของเหยื่อลงไปที่เรียกว่า ฟิชชิ่ง (Phishing) ไปจนถึงการใช้โปรแกรมโจมตีระบบคอมพิวเตอร์ขั้นสูง





2. แนวทางการป้องกันและแก้ไขปัญหา ในการทำธุรกรรมทางอิเล็กทรอนิกส์

แนวทางการป้องกันและแก้ไขปัญหการฉ้อโกงและการฉวยโอกาส

การฉ้อโกงจากการขายสินค้าและการฉวยโอกาส

1.

ตรวจสอบข้อมูลของผู้ขายสินค้าว่ามีความน่าเชื่อถือหรือไม่ เช่น เป็นร้านที่มีชื่อเสียงเปิดดำเนินการมาเป็นเวลานาน มีการให้ความเห็นจากผู้ใช้งาน (Review) เป็นไปในทางที่ดี หรือเป็นร้านที่ได้ลงทะเบียนกับหน่วยงาน

นอกจากนี้ผู้ซื้อยังสามารถตรวจสอบบัญชีธนาคารของผู้ขายจากเว็บไซต์ <https://www.blacklistseller.com> ว่าอยู่ในบัญชีดำหรือไม่



2.

ใช้วิจารณญาณไตร่ตรองความเป็นไปได้ เช่น หากมีการตั้งราคาที่ถูกกว่าความเป็นจริงมาก การให้ส่วนลดมาก ๆ ให้สันนิษฐานไว้ก่อนว่า จะเป็นมิจฉาชีพ

3.

ขอประกันการชำระค่าบริการหรือการคืนเงินในทุกกรณีที่สินค้าไม่ตรงกับที่เสนอขาย

4.

เมื่อโอนเงินให้ระบุในบันทึกว่าโอนเพื่อซื้ออะไร ให้พอเข้าใจ รายละเอียด และเก็บหลักฐานการโอนเงิน

5.

ติดตามการนำส่งเลขพัสดุจากผู้ขาย หากมีอะไรไม่ชอบมาพากลหรือ ผู้ขายเริ่มบ่นย่ำเบียงอ้างเหตุติดขัด ให้ขอคืนเงินกลับมาก่อน





6. เมื่อพัสดุสินค้ามาถึง ให้ถ่ายวิดีโอขณะเปิดบรรจุหีบห่อเพื่อเป็นหลักฐานว่าสินค้าส่งมาตรงหรือไม่ หรือเกิดความชำรุดบกพร่องหรือไม่

7. เมื่อพบความชำรุดบกพร่องให้ประสานผู้ขายหรือแพลตฟอร์มที่เราได้ซื้อสินค้า เพื่อให้รับผิดชอบต่อสิ่งที่เกิดขึ้น หากได้รับการปฏิเสธให้รวบรวมพยานหลักฐานแจ้งความเจ้าหน้าที่ตำรวจเพื่อดำเนินคดีหรือร้องเรียนไปยังหน่วยงานที่เกี่ยวข้อง ได้แก่

- ◆ ศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์ สายด่วน 1212
- ◆ สำนักงานคณะกรรมการอาหารและยา สายด่วน 1556
- ◆ กรมการค้าภายในกระทรวงพาณิชย์ สายด่วน 1569
- ◆ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค สายด่วน 1166

การฉ้อโกงจากการลงทุน/การหลอกให้โอนเงิน

1. ตรวจสอบข้อมูลของผู้ที่ชักชวนให้ลงทุนหรือให้โอนเงินให้แน่ชัดว่าเป็นใคร มีตัวตนจริงหรือไม่

2. ใช้วิจารณญาณไตร่ตรองข้อมูลเกี่ยวกับความเป็นไปได้ของผลตอบแทน การไม่ดำเนินการในธุรกิจที่ผิดกฎหมาย

3. เมื่อโอนเงินให้ระบุในบันทึกว่าโอนเพื่อลงทุนอะไร ให้พอเข้าใจรายละเอียด และเก็บหลักฐานการโอนเงิน

4. หากแน่ชัดแล้วว่าถูกโกงจากการฉ้อโกงจากการลงทุน/โอนเงิน สามารถติดต่อขอความช่วยเหลือได้ที่ ศูนย์ปราบปรามอาชญากรรมเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ สายด่วน 1599 หรือ www.pct.police.go.th



การโอนเงินผิดบัญชี/ผิดจำนวน

กรณีเป็นผู้โอน

1.

เก็บหลักฐานการโอนที่โอนผิดบัญชีติดต่อสถาบันตำรวจเพื่อขอหลักฐานบันทึกประจำวัน โดยระบุข้อมูลในเอกสาร ดังนี้

- ◆ ชื่อธนาคารที่ทำรายการ ทั้งฝั่งต้นทางและปลายทาง
- ◆ วันที่และเวลาที่ทำรายการ
- ◆ จำนวนเงินที่โอน
- ◆ ช่องทางการโอนเงิน เช่น เครื่องอิเล็กทรอนิกส์ (ATM/CDM /VTM), Mobile Banking, Internet Banking
- ◆ ชื่อบัญชี และเลขที่บัญชี ของผู้ทำรายการโอน (บัญชีต้นทาง)
- ◆ ชื่อบัญชี และเลขที่บัญชี ของผู้ที่ได้รับเงินผิด (บัญชีปลายทางที่โอนผิด)
- ◆ ชื่อบัญชี และเลขที่บัญชี/หมายเลขพร้อมเพย์ ของปลายทางที่ต้องการโอนที่ถูกต้อง





2.

ติดต่อธนาคารเจ้าของบัญชีของเรา เพื่อให้เป็นผู้ประสานงานต่อไป หากบัญชีธนาคารของผู้รับโอนเป็นธนาคารเดียวกับผู้โอน ธนาคารจะติดต่อผู้รับโอนโดยตรง แต่หากบัญชีของการโอนเงินผิดบัญชี/ผิดจำนวนผู้รับโอนเป็นบัญชีต่างธนาคาร ธนาคารจะติดต่อไปยังธนาคารของผู้รับโอน เพื่อให้ธนาคารของผู้รับโอนติดต่อผู้รับโอนอีกทอดหนึ่ง

3.

รอธนาคารแจ้งผล หากผู้รับโอนยังไม่ดำเนินการ ผู้โอนสามารถแจ้งความดำเนินคดีได้

กรณีเป็นผู้รับโอน

1. เมื่อมีผู้ทวงถามเราว่าโอนเงินผิด อย่าเพิ่งโอนเงินกลับ เพราะคนทวงอาจเป็นมิจฉาชีพ ให้เราดซื้อบัญชี ยอดเงินบัญชี และเวลาการโอนไว้เพื่อตรวจสอบ
2. ตรวจสอบเงินเข้าบัญชีของเรา หากไม่ใช่ยอดเงินที่ได้รับจากมูลหนี้ ให้ติดต่อธนาคารโดยธนาคารจะเป็นตัวกลางในการรับโอน ไม่จำเป็นต้องคืนเงินโดยตรงหากไม่รู้จักเจ้าของบัญชี
3. หากได้รับการโอนเงินผิดจริงผู้รับโอนจะต้องคืนเงินนั้นเพราะหากไม่คืนจัดเป็นความผิดฐานยักยอกทรัพย์



การแฮ็ก

1.

หลีกเลี่ยงการตั้งรหัสผ่าน (Password) ที่ง่ายต่อการคาดเดา เช่น เลขเรียงเลขเหมือน เลขวันเดือนปีเกิด ไม่บอกรหัสเข้าใช้ (User ID) และรหัสผ่าน (Password) เข้าระบบชำระเงินอิเล็กทรอนิกส์แก่ผู้อื่น หากเป็นไปได้ ควรเปลี่ยนรหัสผ่าน (Password) เข้าระบบชำระเงินอิเล็กทรอนิกส์ เป็นระยะอย่างต่อเนื่อง

2.

หลีกเลี่ยงการเข้าถึงหรือเว็บไซต์ที่ไม่คุ้นเคยที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือข้อความในโทรศัพท์มือถือ ที่ให้เรากรอกข้อมูลส่วนตัว รวมถึงการถามข้อมูลทางโทรศัพท์ด้วย



3.

ติดตั้งโปรแกรมรักษาความปลอดภัยระบบคอมพิวเตอร์รวมทั้งในโทรศัพท์มือถือให้ทันสมัยอยู่เสมอ สแกนมัลแวร์ในระบบคอมพิวเตอร์อยู่เสมอ

4.

ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ส่วนตัวหรืออุปกรณ์สาธารณะ หากใช้งานเสร็จแล้วจะต้องออกจากระบบ (Log Out) ทุกครั้งเสมอ อย่าปิดเฉพาะโปรแกรมจากหน้าต่างใช้งานหรือเฉพาะตัวเครื่อง

5.

หากมีระบบการให้บริการรองรับการเปิดบริการการใช้งานยืนยันตัวตนแบบสองระดับ (Two-Factor Authentication) เช่น นอกจากใส่รหัสผ่านแล้ว อาจต้องใส่รหัส OTP ที่ส่งเข้าทางโทรศัพท์มือถือด้วย

6.

เมื่อมีข้อสงสัย อย่างนึงนอนใจ ให้ติดต่อธนาคารที่เกี่ยวข้องทุกครั้ง





ทั้งนี้ แม้ว่าการระบบการเข้าถึงลายมือชื่ออิเล็กทรอนิกส์จะค่อนข้างซับซ้อน แต่ก็จัดว่ายังมีการปลอมแปลงกันได้ง่ายกว่าการปลอมลายมือชื่อ เพราะเพียงแค่ผู้ปลอมแปลงทราบข้อมูลในการระบุตัวผู้เป็นเจ้าของลายมือชื่อทางอิเล็กทรอนิกส์เท่านั้น เจ้าของลายมือชื่ออิเล็กทรอนิกส์จึงต้องดำเนินการด้วยความระมัดระวัง ไม่ให้มีการแอบอ้างนำไปใช้ในทางที่ผิด