Volume 11/2566
2 สิงหาคม 2566

การป้องกันการถูกหลอกลวงให้ลงทุน: ตั้งสติ แยกแยะ ตรวจสอบข้อมูล พิสูจน์ให้ชัดเจนก่อนลงทุน

จัดทำโดย
นางสาวสุมิตรา ตั้งสมวรพงษ์
ฝ่ายวิจัย ตลาดหลักทรัพย์แห่งประเทศไทย

สรุปประเด็นสำคัญ:

- **“การหลอกลวงให้ลงทุน”** หรือ การสร้างเรื่องเกี่ยวกับการลงทุนที่ให้ผลตอบแทนสูง เพื่อหลอกให้ประชาชนหลงเชื่อและนำเงินมาร่วมลงทุน โดยที่การลงทุนนั้นๆ ไม่มีอยู่จริง ทำให้คนที่ตกเป็นเหยื่อสูญเสียเงินจำนวนมาก **เป็นปัญหาอันดับต้น ๆ ของการคุกคามทางไซเบอร์**
- **ประชาชนสามารถสังเกตและระมัดระวังการถูกหลอกลวงให้ลงทุนจาก “พฤติกรรมการหลอกลวงให้ลงทุน”** อาทิ
  - การแอบอ้างชื่อสัญลักษณ์ ผู้บริหารหรือกรรมการของบริษัท / หน่วยงานต่างๆ เพื่อสร้างความน่าเชื่อถือ
  - การสร้างเรื่องราวลงทุน อาทิ การรู้ข่าววงในทำให้ได้เปรียบนักลงทุนอื่น / ได้รับโอกาสก่อนนักลงทุนรายอื่น หรือ การสร้างเรื่องราวว่ามีผู้ประสบความสำเร็จจากการลงทุนนั้นและยกมาเป็นตัวอย่าง หรือการเร่งรัดให้ตัดสินใจ โดยอ้างข้อจำกัดต่างๆ
  - การกระตุ้นด้วยผลตอบแทน ที่มีการการันตีว่าให้ผลตอบแทนจากการลงทุนสูง
  - การใช้กลยุทธ์เครือข่ายการหาสมาชิก ชักชวนเพื่อนหรือบุคคลรอบข้างมาลงทุน
- **ที่ผ่านมา ทั้งรัฐและเอกชนต่างร่วมมือป้องกันการหลอกลวงให้ลงทุน ทั้งในด้านประเด็นกฎหมายที่มีการบังคับใช้อย่างจริงจัง** โดยเฉพาะการบังคับใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 การอายัดบัญชีม้า การยกเลิกการส่ง link ทาง SMS การทยอยยกเลิกการให้บริการธุรกรรมการเงินผ่านเว็บไซต์ การแลกเปลี่ยนและประชาสัมพันธ์เตือนภัย เป็นต้น
- **ตลาดทุน องค์กรธุรกิจ และหน่วยงานรัฐ ร่วมกันดำเนินโครงการ “ร่วมมือ - จับปลอม หลอกลงทุน” ต่อต้านการหลอกลงทุนอย่างจริงจัง** โดยให้ความสำคัญกับการสร้างภูมิคุ้มกันให้แก่ประชาชน และเพิ่มช่องทางสื่อสารข้อเท็จจริงในประชาชนตรวจสอบข่าวลงทุนต่างๆ แต่สิ่งสำคัญที่สุดที่จะทำให้ไม่ถูกหลอกลวงลงทุน ก็คือ ตัวของประชาชนเอง ตั้งสติ แยกแยะ ตรวจสอบข้อมูล พิสูจน์ให้ชัดเจนก่อนลงทุน และอย่ารีบด่วนโอนเงิน เงินอยู่ที่เราไม่ต้องรีบ ไม่ต้องกลัวเสียโอกาส เพราะมิจฉาชีพอยู่หน้าจอพร้อมโอนเงินของเราออกไปยังบัญชี / กระเป๋าเงินอิเล็กทรอนิกส์ทันทีที่เราโอนให้

อย่าลงทุน!!! หากพบการชักชวนลงทุนคล้ายพฤติกรรมการหลอกลวงให้ลงทุน ทั้งการแอบอ้างชื่อ อ้างแหล่งข่าวภายใน สร้างเรื่องราวลงทุน กระตุ้นด้วยการการันตีผลตอบแทนในเกณฑ์สูง เร่งรัดให้ตัดสินใจ

จากปัญหาการคุกคามทางไซเบอร์ที่มีความรุนแรงขึ้น เราในฐานะบุคคลทั่วไปที่ใช้งานเครือข่ายอินเทอร์เน็ต และในฐานะพนักงานในองค์กร ไม่ว่าจะอยู่ในภาครัฐหรือเอกชน ควรร่วมมือกันสร้างความรู้ให้ผู้ที่เกี่ยวข้อง สร้างความตระหนักในการระวังภัย และช่วยกัน “เป็นหูเป็นตา” ช่วยกันสอดส่อง เตือนสติบุคคลที่อยู่รอบตัวไม่ให้ตกเป็นเหยื่อของมิจฉาชีพ

จากสถิติอาชญกรรมทางไซเบอร์ที่มีการแจ้งความออนไลน์ตามที่ได้นำเสนอมาแล้วในรายงาน “SET Note 10/2566 Cyber Attack โจรที่ติดตามตัวไปทุกที่ กับ Cyber Security ที่ทุกฝ่ายร่วมกันป้องกัน” แสดงให้เห็นว่า “การหลอกลวงให้ลงทุน”[1] เป็นปัญหาอันดับต้นๆ ของภัยคุกคามทางไซเบอร์ ซึ่งฝ่ายวิจัยได้สรุปพฤติกรรมที่เกี่ยวข้องกับการหลอกลวงให้ลงทุนจากการรายงานข่าวต่างๆ (ภาพที่ 1) ไว้เป็นข้อมูลเบื้องต้นให้สังเกตและระแวดระวังภัย

ภาพที่ 1 พฤติกรรมการหลอกลวงให้ลงทุน

ที่มา: รวบรวมโดยฝ่ายวิจัย ตลาดหลักทรัพย์แห่งประเทศไทย

หากพิจารณาพฤติกรรมการหลอกลวงให้ลงทุน พบว่า มีทั้งเรื่องการปลอมข้อมูล แอบอ้างชื่อผู้บริหารหรือกรรมการของหน่วยงานต่างๆ ตลอดจนการสร้างเรื่องราวลงทุน กระตุ้นด้วยการการันตีผลตอบแทนในเกณฑ์สูง สร้างตัวละครเสมือนว่ามีผู้ที่ได้รับผลตอบแทนสูงตามอ้าง เร่งรัดให้ตัดสินใจ และสร้างเครื่องมือปลอมมาใช้ในการหลอกลวงการลงทุน เมื่อถูกหลอกลวงเข้าไปแล้ว **มิจฉาชีพจะหลอกลวงโดยให้ผลตอบแทนสูงใน 2 - 3 ครั้งแรก และหลอกให้ลงทุนเพิ่มและชักจูงเพื่อนเข้ามาร่วมลงลงทุนเพิ่มเติม ทำให้การหลอกลวงลงทุนขยายวงขยายใหญ่ขึ้น และเมื่อผู้ถูกหลอกลวงต้องการนำเงินออกจากระบบหรือถอนเงินคืน จะอ้างให้นำเงินไปปิดบัญชีจึงจะนำเงินออกมาได้ และหากไม่สามารถหาเงินมาปิดบัญชีได้ มิจฉาชีพบางรายจะกล่าวอ้างเกณฑ์**

[1] การสร้างเรื่องเกี่ยวกับการลงทุนที่ให้ผลตอบแทนสูง เพื่อหลอกให้ประชาชนหลงเชื่อและนำเงินมาร่วมลงทุน โดยที่การลงทุนนั้นๆ ไม่มีอยู่จริง ทำให้คนที่ตกเป็นเหยื่อสูญเสียเงินจำนวนมาก

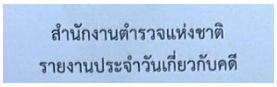
การลงทุนขององค์กรต่าง ๆ เพื่อยึดเงินไปหรือปิดการติดต่อและหนีไป ส่งผลให้เกิดความเสียหายเป็นวงกว้าง ทั้งจากผู้ถูกหลอกลวงลงทุน หรือผู้ที่ถูกชักชวนให้มาร่วมลงทุนในภายหลัง **ส่วนหนึ่งที่มิจฉาชีพยังคงใช้วิธีการเดิมได้ เนื่องจาก ผู้ถูกหลอกลวงไม่เชื่อการกล่าวตักเตือนของคนรอบตัว หรือ ผู้ถูกหลอกลวงยังไม่สามารถยอมรับได้ว่าถูกหลอกลวงลงทุนและยังเพิ่มเงินลงทุนต่อไป หรือบางรายพบว่าเมื่อถูกหลอกลวงลงทุนและเกิดความเสียหายขึ้นแล้วแต่ไม่กล้าแจ้งความดำเนินคดี เนื่องจากกลัวเสียหน้าหรือกลัวได้รับคำตำหนิจากคนรอบตัว**

จากการสัมภาษณ์ผู้เสียหายบางกรณี รวมทั้งเจ้าหน้าที่ตำรวจ และพนักงาน พบว่า บุคคลที่ถูกหลอกลวงให้ลงทุนมีทั้งผู้มีความรู้การศึกษาระดับสูงและประชาชนทั่วไป **“ส่วนใหญ่ประชาชนที่พลาดตกเป็นเหยื่อมิจฉาชีพ เนื่องจาก ถูกเร่งรัดให้ตัดสินใจโดยมิจฉาชีพด้วยการกล่าวอ้างข้อจำกัดต่าง ๆ ที่ทำให้เหยื่อเข้าใจว่าจะพลาดโอกาส ทำให้ขาดความระมัดระวังในการตรวจสอบข้อมูล” และมีโอกาสติดตามเงินกลับมายากมาก** เนื่องจาก

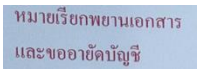
หลังจากที่เหยื่อโอนเงินเข้าบัญชีของมิจฉาชีพ (ส่วนใหญ่จะตรวจพบว่าเป็นบัญชีม้า) **มิจฉาชีพจะโอนเงินของเหยื่อไปยังบัญชี / กระเป๋าเงินอิเล็กทรอนิกส์ ทันทีและมิจฉาชีพจะโอนเงินต่อไปยังบัญชีอีกหลายทอด ทำให้ยากต่อการติดตามเงินของเหยื่อผู้เสียหายกลับคืนมาได้** [2]

อย่างไรก็ตาม แม้ปัจจุบันในประเทศไทยจะบังคับใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ที่**ผู้เสียหายสามารถแจ้งธนาคารอายัดบัญชีปลายทางได้ทันทีที่ทราบ หรือภายใน 72 ชั่วโมง และสามารถแจ้งความได้ตลอด 24 ชั่วโมง แต่ในข้อเท็จจริงในทางปฏิบัติแล้ว เป็นไปได้ยากที่จะได้เงินคืน** เนื่องจาก

- **ไม่ทัน เพราะรู้ตัวช้าว่าถูกหลอก**: เหยื่อผู้เสียหายกว่าจะทราบว่าตัวตนเองถูกหลอกลวง เวลาก็ผ่านไปนานแล้ว
- **ไม่ทัน เพราะกระบวนการช้า แต่มิจฉาชีพเร็ว:** กรณีผู้เสียหายรู้ตัวเร็วแต่ก็ไม่ทันมิจฉาชีพ เนื่องจาก
  - ผู้เสียหายต้องประสานงานไปยังธนาคารที่เป็นบัญชีต้นทางหรือธนาคารที่ผู้เสียหาย ที่ทำโอนเงินออก ผ่านทาง “ศูนย์รับแจ้งภัยมิจฉาชีพทางการเงิน” ของแต่ละธนาคาร (ตามเอกสารแนบ 1) เพื่อขอให้ธนาคารประสานงานไปยังธนาคารปลายทางหรือธนาคารที่รับโอนเงิน เพื่อขออายัดบัญชีของผู้รับโอนเงิน โดยธนาคารของผู้เสียหายจะให้ “Bank Case ID” ให้ผู้เสียหายนำไปเป็นหลักฐานในการส่งแจ้งความในขั้นตอนต่อไป
  - ในกรณีที่ผู้เสียหายเดินทางไปแจ้งความที่สถานีตำรวจ ผู้เสียหายต้อง
    - รอต่อคิวลำดับการให้บริการ
    - ต้องผ่านกระบวนการสอบสวน และดำเนินการแจ้งความลงบันทึกใน “รายงานประจำวันเกี่ยวกับคดี”



    - ต้องขอให้เจ้าหน้าที่ตำรวจออก “หมายเรียกพยานเอกสาร และขอยัดบัญชี” ไปยังธนาคารของผู้รับโอน
  - ต้องเดินทางไปยังธนาคารปลายทาง (สาขาใดก็ได้) เพื่อยื่นรายงานประจำวันฯ และหมายเรียกฯ ต่อธนาคารปลายทาง และรอคิวการดำเนินธุรกรรมที่ธนาคาร



จะเห็นได้ว่า **กระบวนการที่กล่าวมาขั้นต้นต้องใช้เวลา โดยตั้งแต่กระบวนแจ้งความจนกระทั่งการเดินทางไปยื่นหมายเรียกที่เร็วที่สุด ภายในครึ่งชั่วโมง แต่ก็ไม่ทันการโอนเงินออกจากบัญชีของมิจฉาชีพ ซึ่งจะทำการโอนเงินออกจากบัญชีทันทีที่เหยื่อผู้เสียหายโอนเงินเข้าบัญชี**

[2] ข้อมูลจากการสัมภาษณ์ตัวต่อตัวจากผู้ได้รับความเสียหายกรณีหลอกลวงลงทุน ครอบครัวของผู้ที่ถูกหลอกลวงลงทุน และจากผู้ที่ถูกผู้ถูกหลอกลวงติดต่อขอกู้ยืมเงินเพื่อปิดบัญชี

ทุกคนต้องจำไว้ว่า “เงินอยู่ที่เราปลอดภัยกว่า ไม่ต้องรีบด่วนโอนเงิน ไม่ต้องกลัวเสียโอกาส เพราะมิจฉาชีพอยู่หน้าจอ พร้อมโอนเงินของเราออกไปยังบัญชี / กระเป๋าเงินอิเล็กทรอนิกส์ของมิจฉาชีพทันทีที่เราโอนให้”

ทุกภาคส่วนในประเทศไทยร่วมต้านภัยคุกคามทางไซเบอร์: ภาคตลาดทุน องค์กรธุรกิจ และหน่วยงานรัฐ ร่วมกันดำเนินโครงการ “ร่วมมือ - จับปลอม หลอกลงทุน” ต่อต้านการหลอกลงทุนอย่างจริงจัง โดยให้ความสำคัญกับการสร้างภูมิคุ้มกันให้กับประชาชน และเพิ่มช่องทางสื่อสารข้อเท็จจริงให้ประชาชนตรวจสอบข่าวลงทุนต่าง ๆ

ตลอดเวลาที่ผ่านมา ทุกภาคส่วนทั้งภาครัฐและเอกชนได้ร่วมมือกันสร้างความตระหนักรู้ให้ประชาชน และช่วยกันปิดช่องโหว่ / ช่องว่างที่เกิดขึ้น (ตารางที่ 1) เพื่อลดโอกาสไม่ให้ประชาชนถูกหลอกลวงในการทำธุรกรรมทางการเงิน (เอกสารแนบ 2)

ตารางที่ 1 ความพยายามในการต้านและป้องกันภัยคุกคามทางไซเบอร์

พฤติการณ์	ความพยายามในการต้านและป้องกันภัยคุกคามทางไซเบอร์
แอบอ้างหน่วยงาน /บุคคล	• ประชาสัมพันธ์แจ้งเตือนประชาชน พร้อมแจ้งสื่อทางการ (official media) ของแต่ละหน่วยงาน • แจ้งเตือนและขอความร่วมมือผู้ที่พบเห็นข้อความหลอกลวง กดแจ้งไปยังเจ้าของสื่อต่างๆ ว่าเป็นข้อความหลอกลวง • แลกเปลี่ยนข่าวสารข้อมูลระหว่างสื่อโซเชี่ยลมีเดียต่างๆ เพื่อเพิ่มช่องทางการมองเห็นข่าวประชาสัมพันธ์เตือนประชาชน • ดำเนินคดี กรณีที่มีการนำสัญลักษณ์หรือรูปผู้บริหาร ทำสื่อหลอกลวงลงทุน
ใช้บัญชีม้าในการโอนเงิน	• อายัดบัญชีม้า[3] 58,000 บัญชีในปี 2565 • บังคับใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มีผลบังคับไปแล้วเมื่อ 17 มีนาคม 2566 ที่ออกมาเพื่อแก้ไขปัญหาความเดือดร้อนของประชาชนจากการถูกหลอกหลวงฉ้อโกงออนไลน์[4]
หลอกลวงโอนเงินผ่านโทรศัพท์มือถือ	• ปิดซิมหมายเลขโทรศัพท์มือถือลวงแสนกว่าเบอร์ • สถาบันการเงิน ทยอยยกเลิกการส่ง SMS / อีเมล / Facebook ที่แนบ link เพื่อลดโอกาสที่มิจฉาชีพจะหลอกให้ลูกค้ากด link อันตราย และในขั้นตอนการยืนยันการทำธุรกรรมการเงินของลูกค้า ระบบของธนาคารจะเพิ่มเตือนก่อนทำการยืนยัน และแจ้งเตือนภัยรูปแบบใหม่ๆ ให้ทราบลูกค้าสถาบันการเงินทราบอย่างต่อเนื่อง[5] • แสดงสัญลักษณ์หรือข้อความเตือน ในขณะจะทำการโอนเงิน
ปลอมแปลงเวบไซต์ / แอปพลิเคชั่น	• บางธนาคารยกเลิกการให้บริการอินเทอร์เน็ตแบงก์กิ้งผ่านทางเว็บไซต์ เพื่อป้องกันการปลอมแปลงเว็บไซต์ • ให้ประชาชนยืนยันตัวตนเพิ่มเติมด้วย Biometric comparison บน Mobile banking เมื่อการทำธุรกรรมที่มีมูลค่าสูงหรือความถี่สูง การทำธุรกรรมมีความผิดปกติต้องสงสัย เป็นต้น เพื่อป้องกันไม่ให้มิจฉาชีพโอนเงินออกจากบัญชีได้โดยง่าย

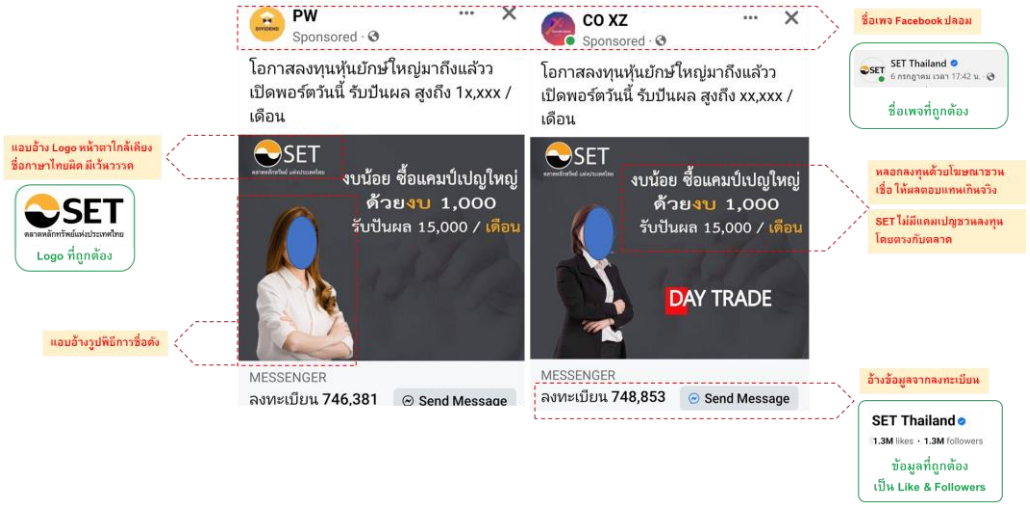
ที่มา: รวบรวมโดยฝ่ายวิจัย ตลาดหลักทรัพย์แห่งประเทศไทย

[3] บัญชีม้า คือ บัญชีที่เจ้าของบัญชีตัวจริงไม่ได้เปิดเพื่อใช้เอง แต่ขายบัญชีให้คนร้าย ยอมให้คนร้ายเอาไปใช้หรือถูกคนร้ายขโมยข้อมูล หรือถูกสวมตัวตนมาเปิดบัญชี ใช้เป็นช่องทางในการรับ / โอนเงินที่ได้มาจากการกระทำความผิดเพื่อปกปิดไม่ให้มีหลักฐานหรือถูกเชื่อมโยงมาถึงตัวได้ (https://www.kasikornbank.com/th/personal/digital-banking/kbankcyberrisk/pages/sellingbankaccount.html)

[4] บทลงโทษเครือข่ายอาจจะทำที่รุนแรงขึ้นทั้งบัญชีม้า คนจัดหาบัญชีม้า:
กรณีเปิดบัญชีม้า: ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ (บัญชีม้า)
กรณีจัดหาบัญชีม้า: ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกตั้งแต่ 2 ปี ถึง 5 ปี และปรับตั้งแต่ 200,0000 บาท ถึง 500,000 บาท หรือทั้งจำทั้งปรับ

[5] https://www.bot.or.th/th/research-and-publications/articles-and-publications/articles/Article_27Feb2022.html

ภาพที่ 2 ตัวอย่าง Facebook ที่แอบอ้างตราสัญลักษณ์ของตลาดหลักทรัพย์แห่งประเทศไทย



ที่มา: รวบรวมโดยฝ่ายวิจัย ตลาดหลักทรัพย์แห่งประเทศไทย

ตลาดหลักทรัพย์แห่งประเทศไทย ได้ประชาสัมพันธ์เตือนภัยให้ประชาชนรับทราบผ่านทางสื่อของตลาดหลักทรัพย์ฯ ทั้งใน เว็บไซต์ และ Social Media อาทิ ใน Facebook เป็นต้น และการเผยแพร่รายชื่อสื่อและโซเชียลมีเดียที่เป็นทางการของตลาดหลักทรัพย์ฯ เพื่อให้ประชาชนได้รับทราบ และไม่ตกเป็นเหยื่อของการถูกหลอกลวงลงทุนโดยสื่อและโซเชียลมีเดียปลอม รวมถึงการเปิดรับข้อมูลการหลอกลวงลงทุนผ่านทาง SET Contact Center หมายเลขโทรศัพท์ 02-009-9999 และได้เผยแพร่วิธีการสังเกตเพจ Facebook ที่เป็นทางการของตลาดหลักทรัพย์แห่งประเทศไทย ตามภาพที่ 3

ภาพที่ 3 วิธีการสังเกตเพจตลาดหลักทรัพย์แห่งประเทศไทย Facebook ที่เป็นทางการ

ที่มา: Facebook ตลาดหลักทรัพย์แห่งประเทศไทย

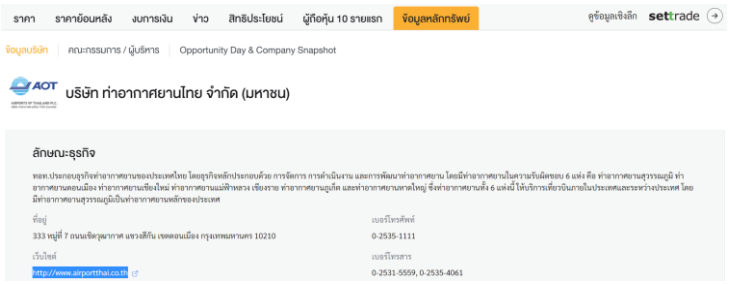
ล่าสุดเมื่อวันที่ 24 กรกฎาคม 2566 ที่ผ่านมา ตลาดหลักทรัพย์แห่งประเทศไทย ร่วมมือกับพันธมิตรภาคตลาดทุน องค์กรธุรกิจ และหน่วยงานรัฐ ได้แก่ ก.ล.ต. สภาธุรกิจตลาดทุนไทย สมาคมธนาคารไทย สมาคมบริษัทจดทะเบียนไทย สมาคมบริษัทจดทะเบียนในตลาดหลักทรัพย์ เอ็ม เอ ไอ สมาคมบริษัทหลักทรัพย์ไทย สมาคมบริษัทจัดการลงทุน กองทุนส่งเสริมการพัฒนาตลาดทุน ศูนย์ต่อต้านข่าวปลอมประเทศไทย และกองบัญชาการตำรวจสืบสวนสอบสวน อาชญากรรมทางเทคโนโลยี **ร่วมกันดำเนินโครงการ “ร่วมมือ - จับปลอม หลอกลงทุน” ต่อต้านการหลอกลงทุนอย่างจริงจัง** โดยประสานงานกันเพื่อเตือนภัยผู้ลงทุน โดยให้ความสำคัญกับการสร้างภูมิคุ้มกันให้แก่ประชาชน และเพิ่มช่องทางสื่อสารข้อเท็จจริงในประชาชนตรวจสอบข่าวลงทุนต่าง ๆ นอกจากนี้ หากมีการพบเห็นการเชิญชวนลงทุนโดยให้ผลตอบแทนสูงเกินจริงภายในระยะเวลาสั้น ๆ หรือแอบอ้างองค์กรและบุคคลที่มีชื่อเสียง อย่าเพิ่งหลงเชื่อร่วมลงทุน และตรวจสอบข้อมูลอย่างรอบคอบ โดยสามารถสอบถามไปยังองค์กรที่ถูกอ้างถึงโดยตรง หรือตรวจสอบรายชื่อบุคคล ผู้ประกอบธุรกิจหรือบริการทางการเงินว่าได้รับอนุญาตจากหน่วยงานกำกับดูแล

อย่างไรก็ตาม สิ่งสำคัญที่สุดที่ช่วยป้องกันภัยจากการถูกหลอกลวงให้ลงทุน ก็คือ ตัวของประชาชนเอง ตั้งสติ คิดแยกแยะ ตรวจสอบข้อมูล พิสูจน์ให้ชัดเจนจากสื่อที่เป็นทางการของแต่ละหน่วยงาน และอย่ารีบด่วนโอนเงิน เงินอยู่ที่เราไม่ต้องรีบ ไม่ต้องกลัวเสียโอกาส เพราะมิจฉาชีพอยู่หน้าจอพร้อมโอนเงินของเราออกไปยังบัญชี / กระเป๋าเงินอิเล็กทรอนิกส์ทันทีที่เราโอนให้

เอกสารแนบ 1 หมายเลขโทรศัพท์รับแจ้งเหตุภัยทางการเงินจากมิจฉาชีพ

ที่มา: ธนาคารแห่งประเทศไทย

เอกสารแนบ 2 แนวทางเบื้องต้นในการตรวจสอบข้อมูลก่อนลงทุน

การหลอกลวง	สิ่งที่ประชาชนควรตรวจสอบ
อ้างชวนลงทุน	
• บริษัทใหม่ เติบโตเร็ว อยู่ระหว่างรอจดทะเบียนเข้าซื้อในตลาดหุ้นไทย	• ตรวจสอบตัวตนของบริษัท โดยการสถานะของบริษัท จาก website กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ https://datawarehouse.dbd.go.th/index
• บริษัทจดทะเบียนจดทะเบียนในตลาดหุ้นไทย	• ตรวจสอบตัวตนของบริษัท จาก website ของตลาดหลักทรัพย์แห่งประเทศไทย https://www.set.or.th/th/market/get-quote/stock/ • ตรวจสอบเรื่องราวลงทุน ○ บริษัทจดทะเบียนที่สามารถเสนอขายหลักทรัพย์เพื่อระดมทุนในตลาดหุ้นไทยได้ ต้องเป็น “บริษัท (มหาชน) จำกัด” เท่านั้น ○ ต้องมีการขออนุญาตออกหลักทรัพย์ที่สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ https://market.sec.or.th/public/idisc/th/Product/Filing
อ้างตัวเป็นเจ้าหน้าที่ติดต่อด้านการลงทุน	
• อ้างเป็นเจ้าหน้าที่ติดต่อนักลงทุน /มาร์เก็ตติ้ง / นักวิเคราะห์ ของบริษัทหลักทรัพย์ / บริษัทหลักทรัพย์จัดการลงทุน	• ตรวจสอบตัวตนของผู้ที่แอบอ้าง จากรายชื่อบุคคลที่ได้รับอนุญาต / ขึ้นทะเบียน จาก website สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ https://www.set.or.th/th/market/get-quote/stock/ • ติดต่อสอบถามโดยตรงที่บริษัท / องค์กรที่ถูกแอบอ้าง
ให้ติดต่อผ่านสื่อโซเชียลต่าง ๆ ที่แอบอ้างว่าเป็นของบริษัท / องค์กร นั้น ๆ ที่ชวนลงทุน	
• มิจฉาชีพทำ website ปลอม เลียนแบบ website จริง	• ตรวจสอบ URL ของ website ของบริษัท / องค์กรที่ถูกแอบอ้าง ก่อน Click เข้าสู่ website ซึ่งกรณี website ของบริษัทจดทะเบียนในตลาดหุ้นไทย สามารถดูได้จาก https://www.set.or.th/th/market/get-quote/stock/ พิมพ์ชื่อย่อหลักทรัพย์ แล้วเลือก “ข้อมูลหลักทรัพย์” จะมี url ของ website ที่เป็นทางการของแต่ละบริษัท  • ไม่เข้า website ผ่านทาง link จากการใช้ Search Engine • เมื่อเข้าสู่ website ให้สังเกต URL ต้องขึ้นต้นด้วย “HTTPS” (Hypertext Transfer Protocol Secure) ซึ่งจะเป็น website ที่มีความปลอดภัยเพิ่มมากขึ้น
• มิจฉาชีพให้สื่อสารผ่านช่องทางโซเชียลมีเดียปลอม	• ตรวจสอบโซเชียลมีเดียที่เป็นทางการ จาก website ของแต่ละบริษัท / องค์กร ไม่ติดต่อลงทุนในโซเชียลมีเดียอื่น
หลอกให้โอนเงินเพื่อทำธุรกรรมการลงทุนผ่านยังบัญชีอื่น นอกเหนือจากบัญชีทางการของบริษัท / องค์กร นั้น ๆ	
• มิจฉาชีพอ้างให้โอนเงินในการธุรกรรมผ่านบัญชีของมาร์เก็ตติ้ง / ฝ่ายบัญชี / ฝ่ายการเงิน	• ให้ตรวจสอบชื่อบัญชีที่จะทำการโอนเงินทุกครั้ง ต้องเป็นบัญชีที่บริษัท / องค์กรนั้นๆ กำหนด และเปิดเผยไว้ใน website / Application ที่เป็นทางการของบริษัท / องค์กร เท่านั้น ไม่ทำการโอนไปยังบัญชีบุคคลใดๆ หรือฝ่ายงานใดๆ ตามที่กล่าวอ้าง • หากชื่อบัญชีธนาคารที่ต้องการทำการโอน ไม่ตรงกับบุคคลที่เราติดต่อ ห้ามทำการโอนโดยเด็ดขาด ให้ตรวจสอบจนแน่ใจจึงทำการการโอน

ที่มา: รวบรวมโดยฝ่ายวิจัย ตลาดหลักทรัพย์แห่งประเทศไทย