

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Deepfake และ Voice Cloning เครื่องมือที่นิยมนำมาใช้หลอกลวง

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบรายงานของ Gartner บริษัทวิจัยและให้คำปรึกษาด้านเทคโนโลยีสารสนเทศและธุรกิจชั้นนำได้ออกรายงาน The Gartner 2026-2027 ThreatScape ซึ่งให้เห็นถึงว่า Deepfakes เป็นเครื่องมือที่ผู้ไม่หวังดีใช้ประโยชน์เพื่อให้เกิดภัยคุกคามในระดับวิกฤตสูงที่สุด และถูกนำมาใช้อย่างมาก ยากต่อการตรวจจับเนื่องจากมีความซับซ้อนรวมทั้ง อาจมีการนำ AI มาใช้เป็นเครื่องมือในการทำ Deepfake และ Voice Cloning ซึ่งสามารถใช้งานได้ง่าย ออกผลลัพธ์ได้อย่างรวดเร็ว และสามารถโจมตีเหยื่อหลายรายพร้อมกันได้

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อหน่วยงานในตลาดทุน จึงขอแนะนำส่งข้อมูล Cyber Hygiene เพื่อให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการ raise awareness ตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติงานของบริษัท

Deepfake Horizon:

เส้นแบ่งใหม่ระหว่างจริงกับปลอม

01 Deepfake คืออะไร

เทคโนโลยี Generative AI ที่สร้างสิ่งสังเคราะห์ ใช้ Deep Learning เรียนรู้จากข้อมูลใบหน้า น้ำเสียง และพฤติกรรมส่วนบุคคล สามารถสร้างภาพนิ่ง เสียง และวิดีโอที่เสมือนบุคคลจริงชุดหรือแสดงออกจริงจนแยกแยะไม่ออกด้วยตาเปล่า

Deepfake สามารถสร้าง

- ภาพนิ่งเสมือนจริง
- เสียงแบบเสียงธรรมชาติ
- วิดีโอเหมือนบุคคลจริงทั้งภาพและเสียง

02 Deepfake ทำงานอย่างไร

วิธีที่ 1: Face Swap การปลอมใบหน้าที่
สลับใบหน้าเป้าหมายเข้าไปในวิดีโอต้นฉบับ พร้อมเลียนแบบเสียง และท่าทางของบุคคลนั้น

วิธีที่ 2: Full Synthesis Face Reenactment
AI สร้างใบหน้าและเสียงใหม่ทั้งหมด ควบคุมแสง การกะพริบตา และการแสดงออกได้อิสระ

03 Red flag: จับผิด Deepfake

ใบหน้าและร่างกาย

การกะพริบตาผิดปกติ การแสดงออกไม่ธรรมชาติ อารมณ์และสีหน้าไม่เข้ากัน แสง สี ขาวผิดปกติ ขลุ้ ไม่สอดคล้องตามบริบทตามกัน

คุณภาพวิดีโอ

ภาพเบลอหรือแสดงเงาบนใบหน้าไม่สม่ำเสมอ แสง-เงาผิดปกติ ความละเอียดเปลี่ยนแปลง ไม่เหมาะสม มีลักษณะเบลอๆ ขรุขระ หรือเป็นจุดภาพ

เสียงไม่ตรงปาก

ปากกับเสียงไม่ตรงกัน ริมฝีปาก-ฟัน ไม่สัมพันธ์ ป้ายเสียงผิดปกติ ไร้เหตุผล เสียงเบลอๆ หรือขาดภาพเสียงไม่สม่ำเสมอ

บริบทและแหล่งที่มา

🔍 แหล่งที่มาไม่น่าเชื่อถือ
🧠 เนื้อหาผิดปกติดจากพฤติกรรมจริง
📍 ส่งผ่านช่องทางไม่น่าเชื่อถือ

04 มาตรการป้องกัน/แนวปฏิบัติ

ตั้งค่า 2FA สำหรับการยืนยันตัวตนในระบบ

เข้าร่วมอบรม Deepfake Awareness

ยืนยันผ่านช่องทางอื่นก่อนดำเนินการตามคำขอ

ใช้ AI Detection Tools ตรวจสอบแหล่งที่มาของสื่อ

สัญญาณเตือนสำหรับตลาดทุน

ก.ล.ต. และผู้ประกอบการควรเพิ่มความระมัดระวัง ในการยืนยันตัวตนผ่านวิดีโอคอล เพราะ Deepfake สามารถหลอกระบบที่ไม่มี Liveness Detection ที่แข็งแกร่งได้

TCM-CERT
Thai Capital Market CERT

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์