Financial Fraud:
กลโกงทางการเงินใกล้ตัวกว่าที่คิด
รุ่นที่ 2/66

7 Aug 2023

วิทยากร : คุณเดชา ศิริสุทธิเดชา CIA, CPIA

ปัจจุบัน เราคงได้ยินข่าวคราวมิจฉาชีพ ขบวนการ Call Center ที่มักมาพร้อมอุบายล่อลวงหลอกใหม่ ๆ ที่แยบยลมากขึ้น หรือการใช้บัญชีม้าเป็นเครื่องมือสำคัญในการกระทำความผิด ซึ่งกระบวนการเหล่านี้ล้วนเป็นการฉ้อโกงทางการเงิน หรือ Financial Fraud ทั้งนี้ขบวนการ Call Center ไม่ได้เป็นแค่รูปแบบเดียวของ Financial Fraud ยังมีการฉ้อโกงอีกหลายประเภท สร้างความเสียหายให้กับประชาชนและประเทศอย่างมหาศาล สิ่งที่สำคัญที่สุด คือ การสร้างความรู้ความเข้าใจให้กับประชาชนถึงภัยทางการเงินที่อยู่ใกล้ตัวกว่าที่คิด

A world of fraud

1. Fraud by impersonation: a growing risk

2. Cyber-fraud: a rising threat

5. Internal fraud: most frequent cases

4. Client risk, still at stake

3. Data theft: a major risk

Credit: Shutterstock

Introduction

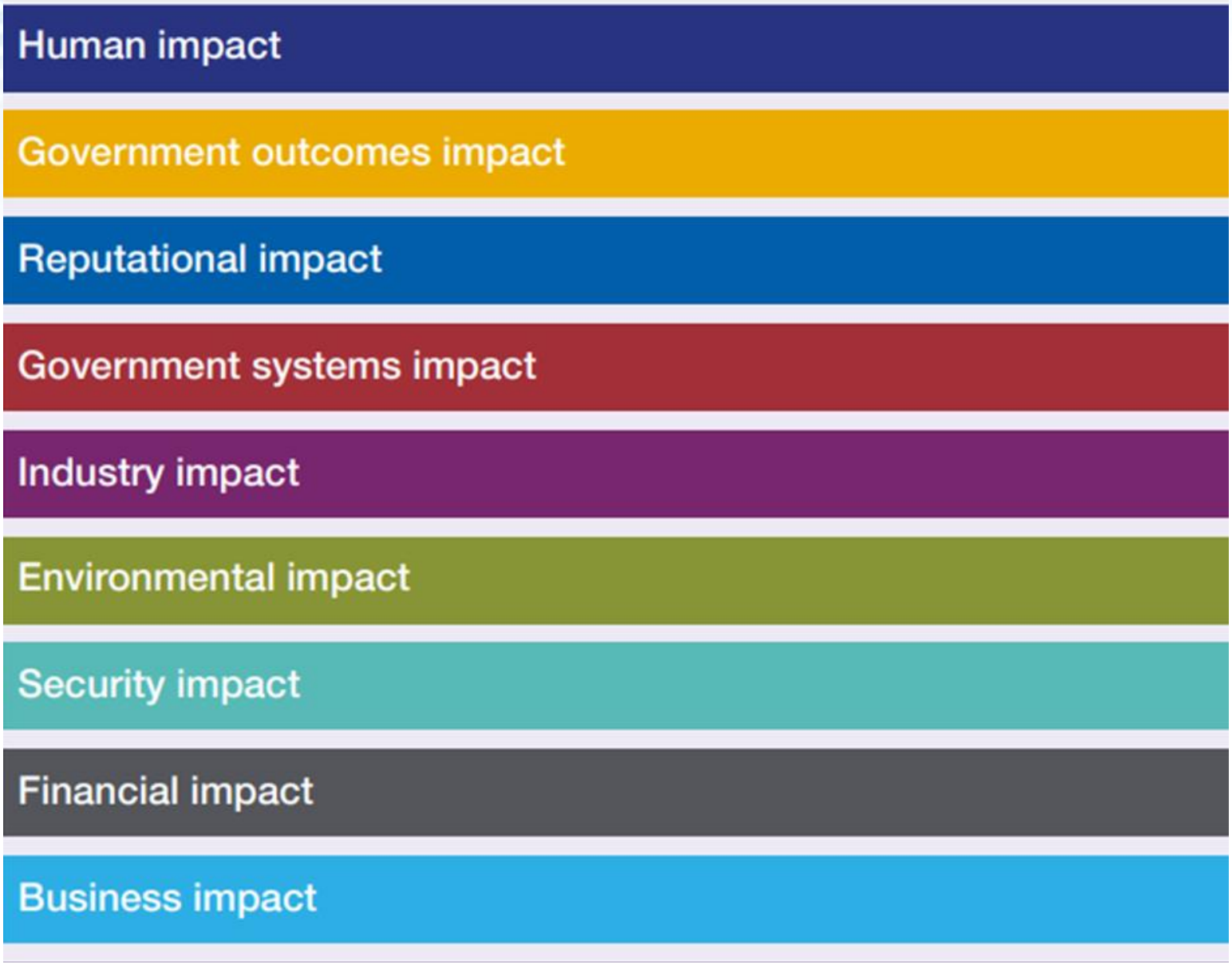
Financial fraud happens when someone deprives you of your money or otherwise harms your financial health through misleading, deceptive, or other illegal practices. This can be done through a variety of methods such as identity theft or investment fraud and more.

What is Financial Fraud ?

Financial fraud can be broadly defined as an intentional act of deception involving transactions for the purpose of a personal gain.

Fraud and financial crimes are a form of theft/larceny that occur when a person or entity takes money or property, or uses them in an illicit manner, with the intent to gain a benefit from it.

Why is Financial Fraud important?



ภูมิภาค

ฉาว! พนง.การเงิน โกยเงินหลวง 8.3 ล้านเข้ากระเป๋า รับติดพนันออนไลน์ อยากหลุดพ้นหนี้

วันที่ 11 มีนาคม 2565 - 14:01 น.

Facebook Twitter LINE Copy Link

www.matichon.co.th

นายก ทต.นิคมทุ่งโพธิ์ทะเล เดือด เจ้าหน้าที่ยักยอกเงินหลวง แอบโอนเงินเข้าบัญชีตนเองกว่า 8.3 ล้าน รับสารภาพติดพนัน

เมื่อเวลา 10.00 น. วันที่ 11 มีนาคม ผู้สื่อข่าวลงพื้นที่เทศบาลตำบล (ทต.) นิคมทุ่งโพธิ์ทะเล อ.เมือง จ.กำแพงเพชร ภายหลังทราบว่า **มีข้าราชการการเงินของ ทต.นิคมทุ่งโพธิ์ทะเล ลักลอบโอนเงินบัญชีหลวงเข้าบัญชีตนเองเป็นเงินกว่า 8 ล้าน 3 แสนบาท** โดยนายวินัย นันทะคุณ นายก ทต.นิคมทุ่งโพธิ์ทะเล เล่าว่า ทต.นิคมทุ่งโพธิ์ทะเล ได้ดำเนินการตรวจสอบหลังจากพบว่ามีปัญหาการเดินเงินหมุนเวียนของเทศบาล ซึ่งได้ตรวจสอบจากสลิปของธนาคารจากภาพวงจรปิด ซึ่งภาพเอกสารบันทึกภายในของ ทต.นิคมทุ่งโพธิ์ทะเล ที่รายงานถึงการทุจริตที่เกิดขึ้นภายในองค์กร โดยผู้ทุจริตที่ตรวจพบคือ **นางสาวปภานันท์ บุญใจ** อายุ 41 ปี ตำแหน่งเจ้าพนักงานการเงินและบัญชีชำนาญงาน เทศบาลตำบลนิคมทุ่งโพธิ์ทะเล ซึ่งเจ้าตัวโอนเงินจากบัญชี ทต.นิคมทุ่งโพธิ์ทะเล เข้าบัญชีตนเอง รวมกว่า 8.3 ล้านบาท

นายวินัยกล่าวว่า ตอนแรกไม่มีใครรู้ แต่ความแตกเมื่อวันที่ 8 มีนาคม 2565 ซึ่งตนได้ตรวจสอบรายงานทางการเงินตามปกติซึ่งจะต้องมีรายงานขึ้นมาให้ตนทุกวัน ปรากฏว่าตลอดระยะเวลา 3 เดือนที่ผ่านมา ตั้งแต่เดือนธันวาคม 2564 จนถึงเดือนกุมภาพันธ์ 2565 พบเพียงหนังสือรายงานเท่านั้น แต่ไม่มีบันทึกการเคลื่อนไหวของบัญชีธนาคารย้อนหลังผ่านเว็บไซต์ หรือแอพพ์ธนาคาร หรือสเตตเมนต์ของทางธนาคารแนบมาด้วย จึงให้น่าสเตตเมนต์มาดู ปรากฏว่ายอดเงินในหนังสือรายงานกับสเตตเมนต์ไม่ตรงกัน จึงสั่งให้มีการตรวจสอบโดยด่วน จนพบว่ามีการทุจริตเกิดขึ้นภายในองค์กร ซึ่งผู้ทุจริตได้พูดคุยพร้อมสารภาพเรื่องที่เกิดขึ้นผ่านไลน์ของเพื่อนร่วมงาน โดยมีเนื้อหายอมรับผิดทั้งหมด พร้อมขอโทษเพื่อนร่วมงานที่ทำให้เดือดร้อน และจะเข้ามอบตัวกับเจ้าหน้าที่ตำรวจเพื่อให้ดำเนินคดีตามกฎหมาย

"จากการตรวจสอบและสอบถามไปยังผู้ถูกกล่าวหา ซึ่งได้ยอมรับทั้งกับผม และทำหนังสือยอมรับการกระทำผิดเป็นลายลักษณ์อักษรว่า เป็นคนลงมือแอบยักยอกเงินของสำนักงานเทศบาลจริง ***เอาเงินไปใช้ส่วนตัวจริง เนื่องจากมีปัญหาหนี้สินส่วนตัวและติดการพนันออนไลน์*** *โดยใช้ช่วงเวลาหลังเลิกงาน หรือนอกเหนือเวลางาน แอบโอนเงินจากบัญชีในระบบออนไลน์ เนื่องจากเป็นผู้มีหน้าที่ทำธุรกรรมทางการเงิน และมีรหัสในการทำธุรกรรมทางการเงิน*

"ทำมาทั้งหมด 3 เดือน ตั้งแต่เดือนธันวาคม 2564 จนถึงเดือนกุมภาพันธ์ 2565 ยอดเงินที่โอนยักยอกไปต่อครั้งสูงสุดถึง 3 ล้านกว่าบาท รวมสูญเงินที่ทุจริตไปประมาณ 8 ล้าน 3 แสนกว่าบาท" นายก ทต.นิคมทุ่งโพธิ์ทะเลกล่าว

www.matichon.co.th

มาแล้ว หมายศาลปลอม
ให้โอนจ่ายค่าปรับ จราจร
อย่าโอน อย่า สแกน QR
เงินหมด บัญชีได้

DB.5 /..... ลำดับที่ ...22...

เบอร์โทรศัพท์ติดต่อ
เจ้าหน้าที่ 061-993-9872

ใบนัดนำจ่ายสิ่งของส่งทางไปรษณีย์

Thailand Post ที่ทำการนำจ่ายภาษีเจริญ5 หมู่บ้านพุดตาน

เรียน คุณ พิสมัย เสถียรยาพนท์

ผู้อยู่อาศัยบ้านเลขที่ 371 ซ.19 หลักสอง ขาลแก กทม. 10160

ด้วยที่ทำการไปรษณีย์ภาษีเจริญ5 ได้นำจ่ายสิ่งของให้ท่าน

https://rb.gy/mzuz1p

กรุณาสแกน QR Code เพื่อนัดนำจ่าย

เลขที่สิ่งของ RK 0367 7784 8 TH

ในวันที่ ..... เดือน 4 มิ.ย. พ.ศ. 2565 เวลา 14.30 น. แต่บ้านปิด/ไม่มีคนรับ/ไม่มีผู้ลงนามรับแทน

ดังนั้นโปรดดำเนินการดังต่อไปนี้

ที่ทำการนำจ่าย ภาษีเจริญ 5
ซนจ.3 โทร. 0986197514

❶ แสกน QR Code และกรอกข้อมูล เพื่อนัดนำจ่ายใหม่อีกครั้ง

❷ มาติดต่อรับ ณ ที่ทำการนำจ่ายภาษีเจริญ 5 หมู่บ้านพุดตาน ซอย เพชรเกษม 81 จ. – อา. เวลา 7.30 น.– 14.30 น.

❸ หากมาติดต่อขอรับ ณ ที่ทำการฯ โปรดเตรียมบัตรประชาชนเพื่อประกอบการติดต่อขอรับ

****โปรดติดต่อการนำจ่ายใหม่อีกครั้งภายใน 15 วัน นับตั้งแต่วันที่ออกใบนัดนี้ ในวันและเวลาทำการ***

สถานการณ์ปัจจุบันในประเทศไทย "ดีอีเอส" ยังคงพบว่ามีมิจฉาชีพ อ้างชื่อธนาคารออมสินและกรุงไทย ผู้บริหารธนาคาร ปล่อยสินเชื่อ “เงินกู้” ชวนกู้เงินออนไลน์ ชวนลงทุน รวมทั้งการอ้างชื่อตลาดหลักทรัพย์แห่งประเทศไทย เปิดลงทุนหุ้นผลกำไรสูง ซึ่งข่าวปลอมหัวข้อลักษณะนี้แพร่กระจายต่อเนื่อง

นางสาวนพวรรณ หัวใจมั่น โฆษกกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมฝ่ายการเมือง "ดีอีเอส" เปิดเผยว่า ข่าวปลอมเกี่ยวกับการเงิน พบหลายข่าวที่มีการกล่าวอ้างของตัวบุคคล ในข่าวปลอม ว่าได้รับอนุญาตใบทะเบียนพาณิชย์ จากกรมพัฒนาธุรกิจการค้า ประกอบธุรกิจเงินกู้นอกระบบแบบออนไลน์ ธุรกิจ “เงินกู้” ถูกกฎหมายออนไลน์ หรือจดทะเบียนเป็นนิติบุคคลตามประมวลกฎหมายแพ่งและพาณิชย์

โดยผลสรุปการมอนิเตอร์ และรับแจ้งข่าวปลอมประจำสัปดาห์ของ "ดีอีเอส" ระหว่างวันที่ 2 - 8 ก.ย. 65 ของศูนย์ต่อต้านข่าวปลอม พบจำนวนเรื่องที่ต้องตรวจสอบ 173 เรื่อง และจากการประสานงานกับหน่วยงานที่เกี่ยวข้อง ได้รับผลการตรวจสอบกลับมาแล้ว 87 เรื่อง ส่วนข่าวปลอมที่มีคนสนใจสูงสุด 10 อันดับ ในสัปดาห์ล่าสุดนี้ ได้แก่
อันดับ 1 ออมสินและกรุงไทยร่วมมือกับบริษัทเอกชน ปล่อย “เงินกู้” ขั้นต่ำ 5,000 - 300,000 บาท ดอกเบี้ยร้อยละ 2 บาท ผ่านไลน์

อันดับ 2 ตลาดหลักทรัพย์แห่งประเทศไทยเปิดให้ลงทะเบียนฟรี เริ่มลงทุนเพียง 1,000 บาท

อันดับ 3 กรุงไทยปล่อยสินเชื่อ smart money ให้ “เงินกู้” ยืมผ่านไลน์ 50,000 บาท ผ่อนเดือนละ 826 บาท

อันดับ 4 เพจ Facebook และ Line เชิญชวนลงทุนการเทรดหุ้นตลาดหลักทรัพย์ โดยอยู่ภายใต้การควบคุมของสำนักงาน ก.ล.ต.

อันดับ 5 ออสเตรเลียรับสมัครคนทำสวน ที่พักฟรี รายได้สูง 80,000 บาท

อันดับ 6 เรื่อง ผลิตภัณฑ์กระเทียมดำ B-Garlic จบปัญหาความดัน ไขมันในเลือดสูง

อันดับ 7 ผลิตภัณฑ์ LIV.D ช่วยดีท็อกซ์ตับ ขับล้างสารพิษ ช่วยป้องกันปัญหาไขมันพอกตับ และตับอักเสบ

อันดับ 8 ธ. กรุงไทยส่งข้อความเชิญชวนผู้ที่ได้รับสิทธิ์ ยื่น “เงินกู้” 80,000 บาท ผ่านลิงก์

สธ. มีหน้าที่ดูแลรักษา ไม่มีภารกิจให้เงินช่วยเหลือ

ทั้งนี้ ภารกิจของกระทรวงสาธารณสุขคือการดูแลป้องกันรักษาควบคุมโรค ไม่ได้มีภารกิจเกี่ยวกับเงินช่วยเหลือประชาชน และไม่ได้มีโครงการหรือกิจกรรมที่เกี่ยวข้องกับการให้เงินช่วยเหลือโควิด 19 หรือโรคระบาดแต่อย่างใด

นพ.รุ่งเรืองกล่าวต่อว่า กลุ่มมิจฉาชีพมีการปรับเปลี่ยนวิธีการใหม่ๆ ตลอดเวลา เพื่อหลอกลวงข้อมูลจากเหยื่อ และมักแอบอ้างหน่วยงานของรัฐ เพื่อสร้างความน่าเชื่อถือ จึงขอให้พิจารณาตรวจสอบข้อมูลอย่างถี่ถ้วนก่อนทุกครั้ง

หากไม่แน่ใจแนะนำให้สอบถามกับหน่วยงานโดยตรง โดยเว็บไซต์ของกระทรวงสาธารณสุข คือ **www.moph.go.th** สามารถเข้ามาตรวจสอบข้อมูลภายในเว็บไซต์ทางการได้ ทั้งนี้ กระทรวงสาธารณสุขจะดำเนินการคดีกลุ่มมิจฉาชีพตามกฎหมายอย่างถึงที่สุด

จากกรณี ที่มีผู้เสียหายจำนวนมาก ตกเป็นเหยื่อขบวนการแชร์ลูกโซ่ โดยมิจฉาชีพอ้างว่านำเงินไปลงทุนในสินทรัพย์ดิจิทัล (Crypto Currency)

มุ่งมั่นพัฒนา รักษาจรรยาบ

PCT เตือนภัย มุกใหม่ แก๊งคอลเซ็นเตอร์ ปลอมเป็น"ตำรวจ"วิดีโอคอล หลอกเหยื่อ

คมชัดลึกออนไลน์
อัพเดต 4 ชั่วโมงที่ผ่านมา • เผยแพร่ 5 ชั่วโมงที่ผ่านมา

ติดตาม

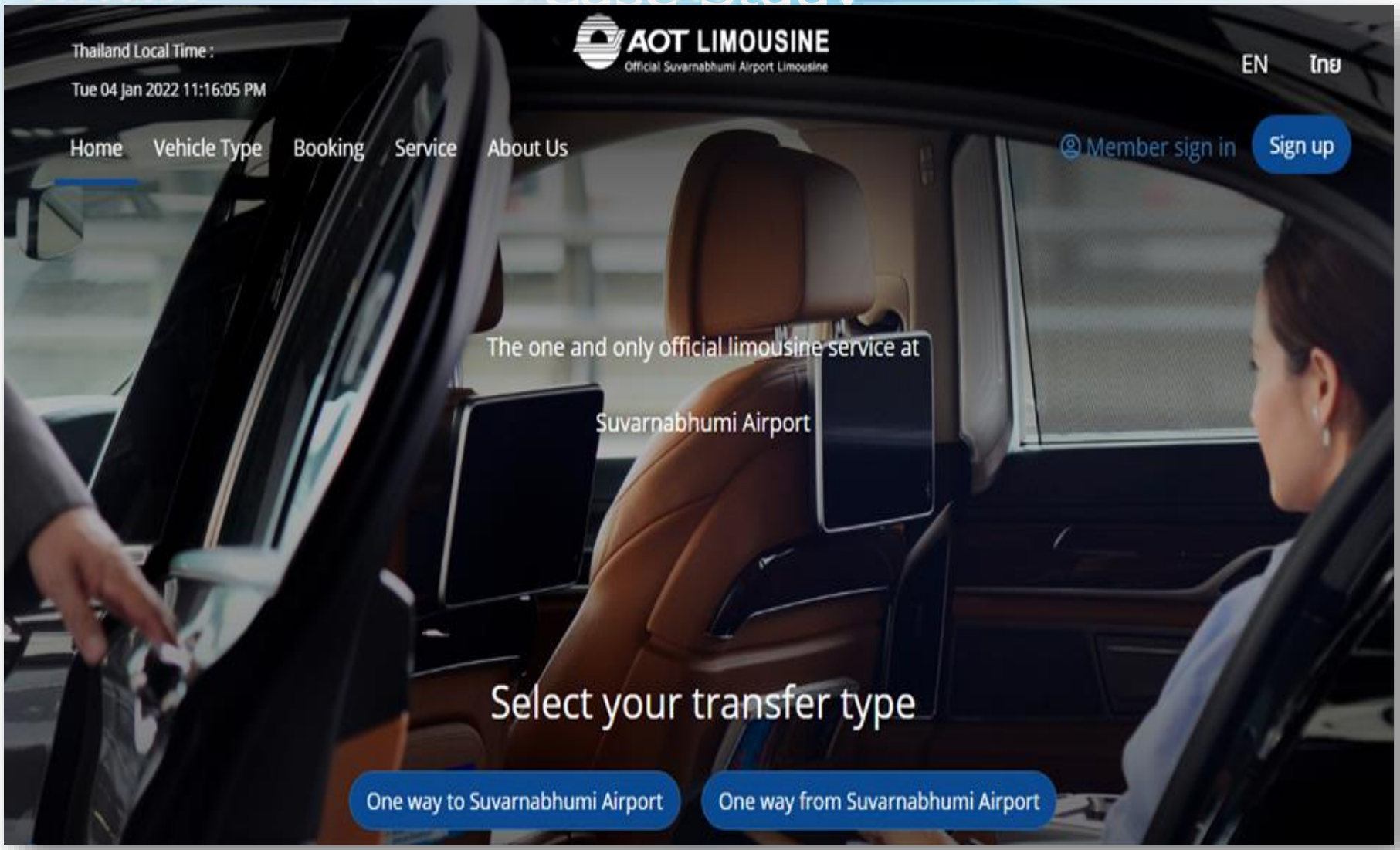
ธ.ก.ส. เตือนมิจฉาชีพลวงขอข้อมูล ยันไม่มีนโยบายให้ คอลเซ็นเตอร์ บริการรับจองสลากออมทรัพย์

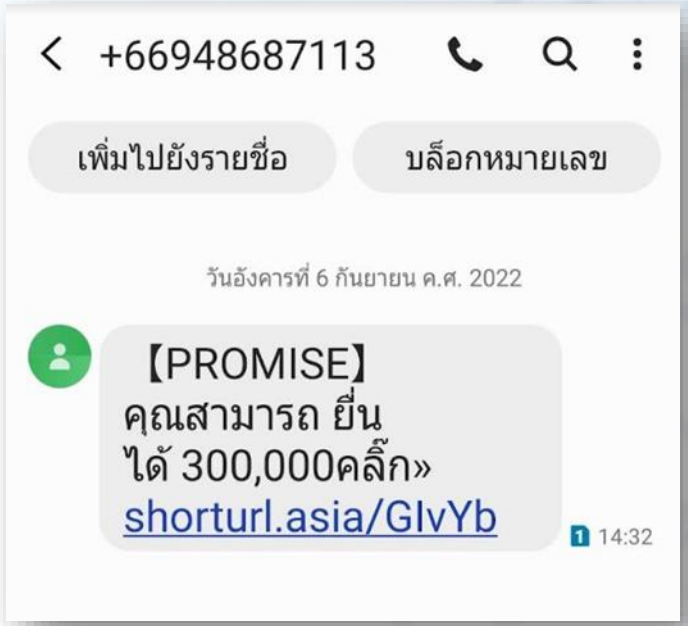
นายสมเกียรติ กิมาวหา รองผู้จัดการ **ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร** (ธ.ก.ส.) เปิดเผยว่า หลังจาก ธ.ก.ส. เปิดรับฝาก **สลากออมทรัพย์ ธ.ก.ส. ชุดเกษตรมั่งคั่ง 7** ช่วง 2 หน่วยละ 100 บาท รวมวงเงิน 22,000 ล้านบาท ลุ้นรางวัลที่ 1 สูงสุด 10 ล้าน และรางวัลอื่น ๆ

> ขอย้ำว่า ธนาคารไม่มีนโยบายให้คอลเซ็นเตอร์ โทรเชิญชวนฝากสลาก หรืออำนวยความสะดวกในการซื้อสลาก ตลอดจนการทำธุรกรรมทางการเงินแทนลูกค้าแต่อย่างใด

มุ่งมั่นพัฒน

Case Study


Thailand Local Time :
Tue 04 Jan 2022 11:16:05 PM
AOT LIMOUSINE
Official Suvarnabhumi Airport Limousine
EN
ไทย
Home
Vehicle Type
Booking
Service
About Us
Member sign in
Sign up
The one and only official limousine service at
Suvarnabhumi Airport
Select your transfer type
One way to Suvarnabhumi Airport
One way from Suvarnabhumi Airport

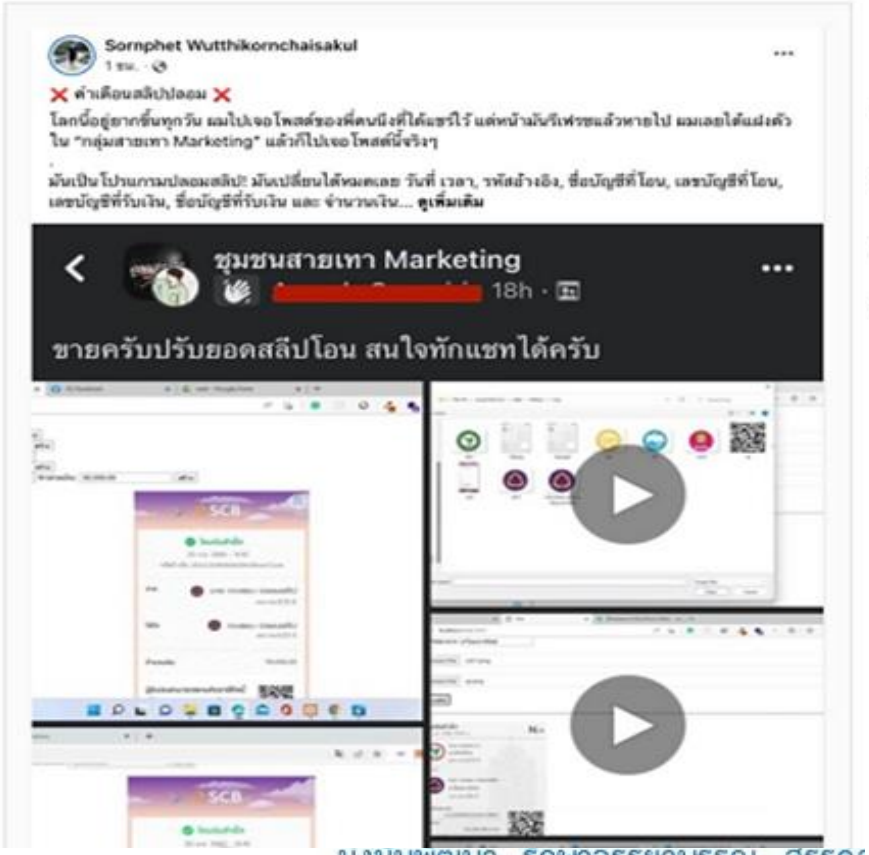


มันใช้โปรแกรมก๊อปปี้มือถือและ ถอนเงินจากบัญชีได้เลย

เจอแบบนี้ อย่ากดตกลง จะโดนก๊อปปี้ข้อมูล ให้ปิดเครื่องแล้วค่อยเปิดใหม่อีกครั้ง (ส่งต่อให้เพื่อนๆ และญาติของท่านด้วย)

เจอแบบนี้ ให้ปิดโทรศัพท์เลยนะ แล้วค่อยเปิดใหม่ อย่ากด..ตกลง.. โดนแฮกทันที

ใครที่ซื้อขายของออนไลน์ให้ดี เพราะตอนนี้มีการเสนอขายโปรแกรมปลอมสลิปผ่านออนไลน์ ซึ่งสามารถเปลี่ยนข้อมูลได้หมด ทั้งธนาคาร ยอดเงิน วันเวลาที่โอน เรียกว่าเนียนสุดๆ เรียกว่าถ้าไม่สังเกตดีๆอาจจะตกเป็นเหยื่อของมิจฉาชีพได้ เสียสินค้าแต่ไม่ได้เงินกลับมา



โปรแกรมนี้เป็นโปรแกรมสำเร็จรูป สามารถสร้างสลิปธนาคารลปมอได้หมด อยากให้โอนจากธนาคารไหนไปธนาคารไหนทำได้หมด เลือกเปลี่ยนข้อมูลได้หมด ไม่ว่าจะเป็นวันที่ เวลา, รหัสอ้างอิง, ชื่อบัญชีที่โอน, เลขบัญชีที่โอน, เลขบัญชีที่รับเงิน, ชื่อบัญชีที่รับเงิน และ จำนวนเงิน เรียกว่าเนียนสุดๆ

แน่นอนว่าโปรแกรมนั้นสามารถปลอมได้เฉพาะแค่ข้อมูลบางส่วนเท่านั้น แต่ไม่สามารถปลอม QR Code ได้ ดังนั้นใครที่ได้ได้รับแจ้งโอนเงินเข้ามาให้ตรวจสอบสลิปให้ดีก่อนว่าเป็นสลิปจริง

- สแกน QR Code ว่ามีการโอนเงินเกิดขึ้นจริง
- เช็กโดยตรงจากบัญชีธนาคารว่าเงินเข้ารึเปล่า
- ลองสังเกตสลิปให้ดี บางธนาคารเช่น SCB จะเปลี่ยนพื้นหลังสลิปในโอกาสพิเศษ หากได้พื้นหลังแบบธรรมดาให้ตั้งข้อสงสัยไว้ก่อน

CASE STUDY: Relevance of Cybersecurity Risk and Cyber Attacks to Financial Statements Audits

Deletion of Financial Reporting Data

A manufacturing company was subject to a cyber attack, which deleted some of its financial reporting data. Without appropriate data backup and recovery controls, the company may not be able to present complete and accurate financial information.

DoS Attack to Online Retail Platform

An online retailer experienced a distributed DoS attack to its online retail platform, an attack to make the online service unavailable by overwhelming it with traffic from multiple sources. This resulted in customers being unable to place online orders for an extended period. This represents a business risk to the retailer with an opportunity cost of lost revenue when the system is down rather than a direct impact to the financials of the entity.

Loss of Customer Information

A financial institution experienced a cyber attack which resulted in the loss of sensitive customer information (credit card information). There appear to be no direct impact to the financial statements or the entity's assets. However, there may be other consequences arising such as penalties for breaching data privacy, potential lawsuits from affected customers, reputation damage, or even potential impairment and going concern issues, especially when the breach is material.

ที่มา https://isca.org.sg/media/2240014/isca-cyber-security-risk-report.pdf

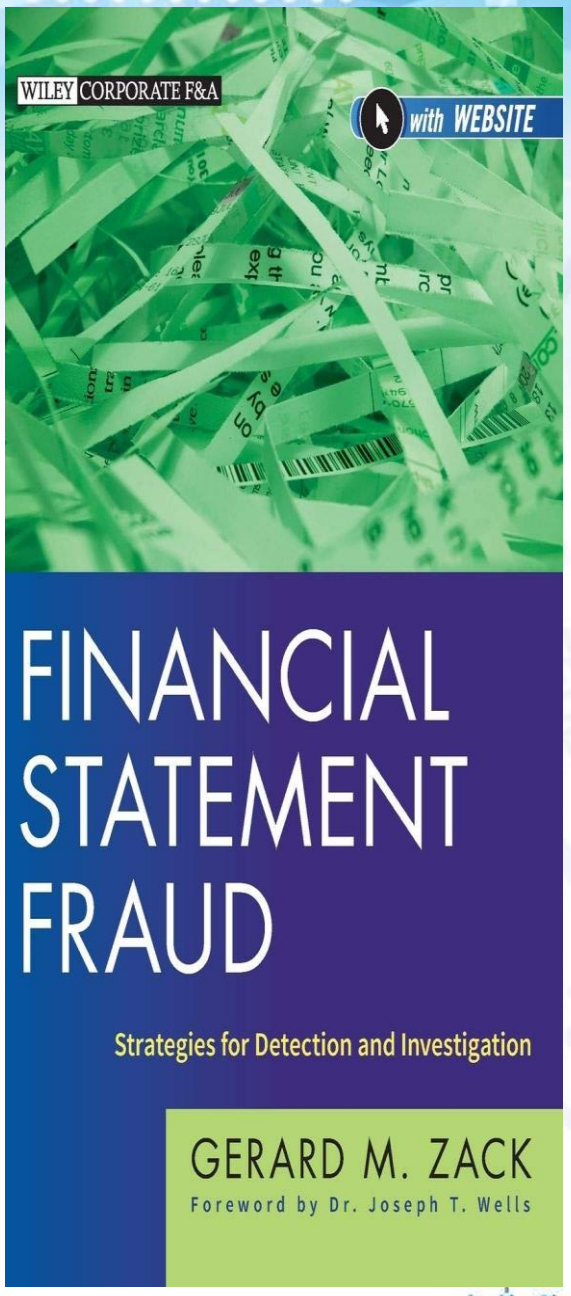
Question

นำเงินออกจากบริษัทไปใช้ส่วนตัวอย่างถูกต้องทำได้หรือไม่???

Types of financial fraud

-Financial Statement Fraud
-Financial Scam, Con and Swindle

Financial Statement Fraud



What Is Financial Statement Fraud?

Financial statement fraud is the deliberate misrepresentation of a company's financial statements, whether through omission or exaggeration, to create a more positive impression of the company's financial position, performance and cash flow.

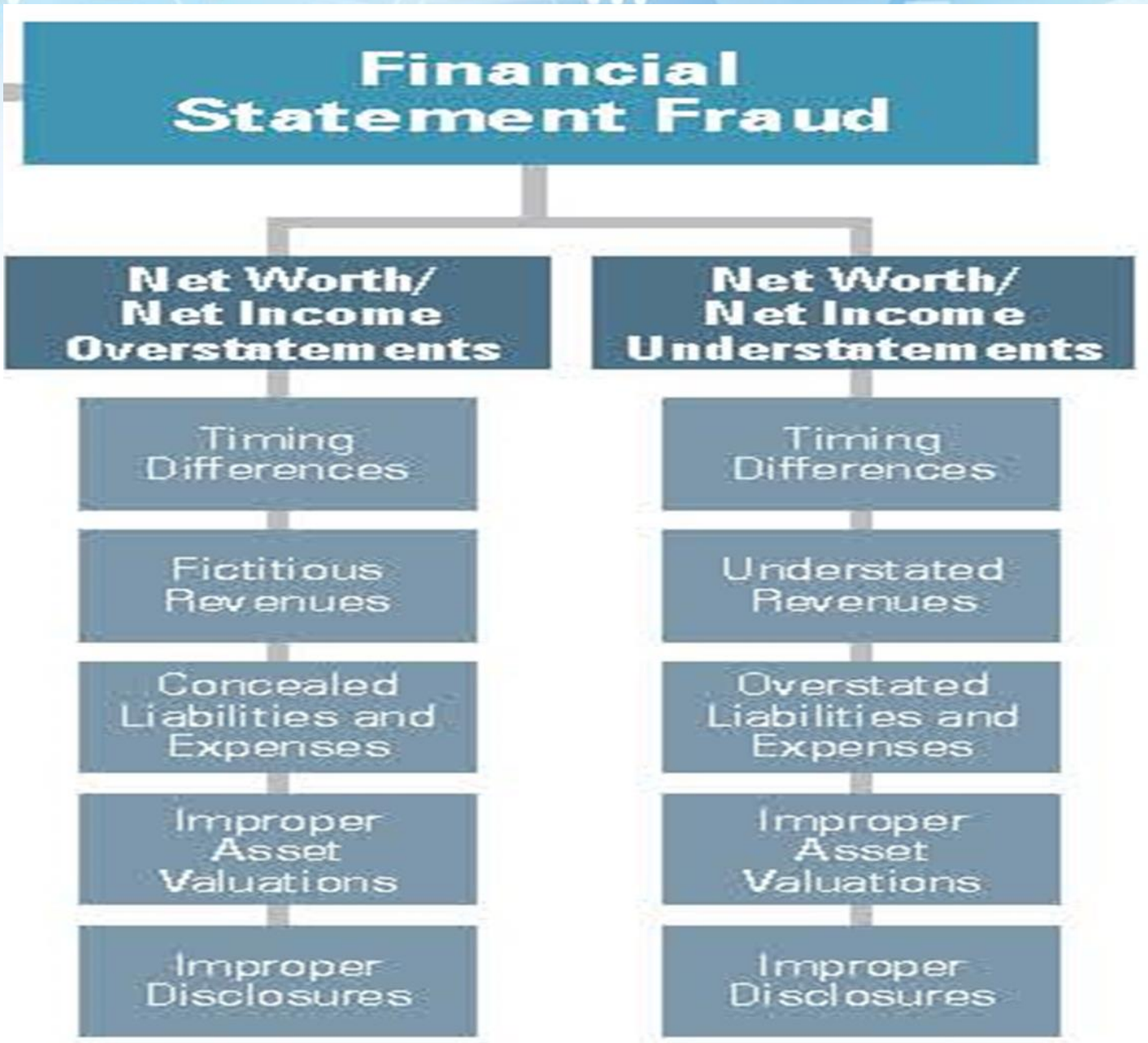
What is the purpose of financial statement fraud?

Financial statement fraud is intended to mislead the users of financial information to create a better picture of the company's financial position, performance and cash flows.

Key Takeaways

- Financial statement fraud is committed when people with access to financial documents and information manipulate data to make the company appear more successful.
- Warning signs for financial statement fraud are numerous and fall into four categories: financial, behavioral, organizational and business.
- To detect fraud, have an auditor analyze the relationships between different financial numbers and compare the ratios to years past or industry norms.
- The No. 1 way to prevent financial statement fraud is to have in place a system of strong internal controls that enforce the segregation of duties so that no single employee has authorization to view and alter all financial data. This can be automated through an enterprise resource planning (ERP) system.

Types of Financial Statement Fraud



Financial Statement Fraud Warning Signs

- Rising revenue without corresponding growth in cash flow — this is the most common warning sign of financial statement fraud.
- Consistent sales growth while competitors are struggling.
- A spike in performance in the final reporting quarter of the year.
- A significant, unexplained change in assets or liabilities.
- Unusual increases in the book value of assets, such as inventory and receivables.
- Missing or altered documents.
- Discrepancies and unexplained items and/or transactions on accounting reconciliations, such as invoices that go unrecorded in the company's financial books.
- Aggressive revenue recognition practices, such as recognizing revenue in earlier periods than when the product was sold or the service was delivered.
- Growth in sales without commensurate growth in inventory — or vice versa.
- Improper capitalization of expenses in excess of industry norms.

Behavioral warning signs

- A manager or accountant living beyond their means and/or having financial difficulties.
- Dishonest, hostile, aggressive and unreasonable management attitudes.
- Control issues, such as an unwillingness to share duties pertaining to company finances.
- Management displays inordinate concern with managing the reputation of the business.
- Loans to executives or other related parties that are written off.
- Inexperienced or lax management and/or accountants.
- Sudden replacement of an auditor resulting in missing paperwork.

Organizational warning signs

- Frequent organizational changes, such as unusually high turnover in management or key accounting personnel.
- Unexplained or disproportionate management bonuses based on short-term targets.
- Operating and financial decisions dominated by a single person or a few people acting in concert.
- A board of directors full of insiders.
- Undue emphasis on meeting quantitative targets.
- Sloppy or manual management/operational business processes, as opposed to automated processes embodied in business software.

Business warning signs

- Profitability and/or operating margins that are out of line with peers.
- Significant investments in volatile industries or during industry turndowns.
- Unusually high revenue and low expenses at times that can’t be explained by seasonality.
- Operating results that are highly sensitive to economic factors, like inflation, interest rates and unemployment.

Tips to Prevent Financial Statement Fraud

- Institute strong internal controls
- Perform periodic audits of financial statements
- Set a tone of honesty at the top
- Use enterprise resource planning (ERP) accounting software
- Establish an internal hotline/reporting system
- Don’t tie management bonuses and compensation to short term goals
- Follow up on gut instincts

การทุจริตโดยการตกแต่งบการเงิน

การทุจริตโดยการตกแต่งบการเงินมีแนวโน้มเพิ่มสูงขึ้นและมีมูลค่าความเสียหายต่อผู้ใช้งบการเงินเป็นอย่างมาก จะเห็นได้จากการล้มละลายของบริษัทขนาดใหญ่ในต่างประเทศหลายแห่ง

การตกแต่งบการเงินเพื่อให้ราคาหุ้นของบริษัทเพิ่มสูงขึน้ และสร้างความมั่งคั่งให้กับกิจการ การตกแต่งบการเงิน เช่น การตกแต่งการเลื่อนการรับรู้รายได้ การตกแต่งมูลค่าสินทรัพย์ การตกแต่งรายได้ปลอม การตกแต่งการปกปิดหนี้สิน การตกแต่งไม่ตั้งค่าเผื่อหนี้สงสัยจะสูญ และการตกแต่งค่าใช้จ่ายจ่ายล่วงหน้า

การตกแต่งดังกล่าว ส่งผลกระทบต่อความน่าเชื่อถือในระบบการจัดทำและการนำเสนองบการเงิน ทำให้ผู้ใช้งบการเงิน ไม่ว่าจะเป็น เจ้าหนี้ ผู้ผู้ถือหุ้น หรือผู้ที่เกี่ยวข้องนำไปใช้ประโยชน์ในการตัดสินใจผิดพลาด โดยเฉพาะนักลงทุนที่ต้องการลงทุนในตลาดทุน

Financial Scam, Con and Swindle

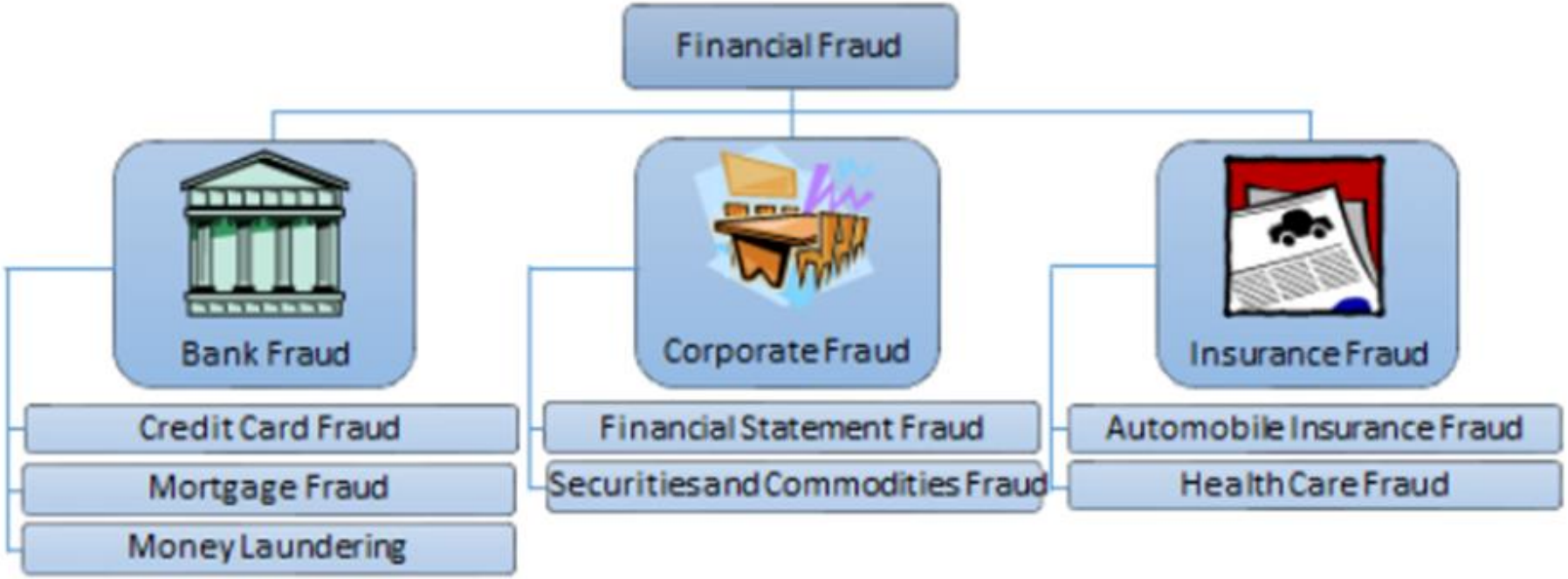


Fig. 1. Common financial fraud categories.

Most Common Types of Financial Fraud To Beware Of

- Identity theft that leads to loan fraud, credit fraud, and bank scams
- Advance fee fraud
- Cashier’s check or fake check fraud
- Tax refund fraud
- Fraudulent charities
- Credit card fraud
- Financial account takeovers
- Ponzi schemes and other investment frauds
- Small business fraud (embezzlement, employee theft, etc.)
- Romance scams or pig butchering scams.

1. Identity Theft Leading to Credit, Bank, or Loan Fraud

Identity theft refers to any kind of fraud committed by stealing personal information. An identity thief uses your personally identifiable information (PII) — such as your name, birthday, and Social Security number (SSN) — to gain access to your accounts and assets.

An identity thief can drain your bank account, or open new loans in your name.

How does identity theft happen?

Criminals have a few options when it comes to stealing your sensitive information.

They might target you with a phishing attack where they email, call, or text pretending to be from your bank. Or, they could target you with a cyber attack to get you to install malware on your devices that steals your logins and passwords.

the easiest way to steal your identity is to buy your personal information off the Dark Web.

Hackers have stolen billions of pieces through data breaches.

How do you know you're being targeted?

- Unfamiliar transactions on your credit card.
- Strange charges on your bank statements.
- New credit cards or loans in your name.
- Calls from debt collectors about purchases you didn’t make.
- Calls verifying unfamiliar purchases.
- Fraud alerts from your bank or credit monitoring service.

What to do if you're a victim

- You'll need to take different actions depending on what financial fraud a criminal has committed under your name. But in all cases, you'll want to:
- Contact all impacted companies and financial institutions.
- Contact police .
- Freeze or cancel affected accounts.
- Set up a credit freeze or lock to stop further financial fraud.
- Review your credit report and dispute any fraudulent activity
- Change your account passwords .
- Enable two-factor authentication (2FA) using an authenticator app.

2. Advance Fee Fraud

Advance fee fraud is when a thief requires you to send money in advance for payments, products, or services. But in the end, they either aren't what was promised, or never arrive.

One common example is a con artist claiming to get you a better deal on a loan or reverse mortgage in return for a “finder’s fee”. They’ll ask you to sign a contract that requires you to pay the fee once they introduce you to the financing source.

What are the warning signs?

- A business asking you for prepayment for services such as securing a loans
- Businesses or individuals that operate out of PO boxes or mail drops.
- Individuals that you can’t reach directly (i.e., they’re never in when you call but will call you back later).
- Asking you to sign a contract like a non-disclosure agreement (NDA) that limits you from discussing the deal with other people.

What to do if you're a victim

if you've been a victim of advance fee fraud, there usually isn't a way to get your money back.

Be wary of any offer that seems too good to be true

3. Cashier’s Check and Fake Check Fraud

The cashier’s check fraud is a simple bank scam that relies on the fact that it can take weeks for a cashier’s check to be verified. Reports of this scam have grown by 65% since 2020 prompting all the more reason to be aware.

How does cashier's check fraud happen?

Scammers send a forged cashier's check with false information, which you're able to deposit without a problem. They ask you to make a withdrawal of some or all of the money and send it to them or a third party and keep some of the money for yourself.

When the check is discovered to be bank fraud or the check bounces a few days later, the scammer is gone and the money will be taken out of your account

What to do if you’re a victim

If you’ve deposited a cashier’s check and sent the scammer a wire transfer, there isn’t a way to get your money back.

If you’ve only deposited a cashier’s check, don’t send money back to the scammer unless you received money.

4. Tax Refund Fraud

Most people get stressed when dealing with their taxes. That makes tax fraud an appealing target for financial scams. One of the most common ones is tax refund fraud.

How does tax refund fraud happen?

Tax refund fraud is a type of identity theft

In 2020,5.2 million tax returns as fraudulent

A fraudster pretends to be from the revenue department and demands personal information or payment for taxes owing.

What to do if you’re a victim

If you’ve given them your bank information, call your financial institution’s fraud department.

5. Fraudulent Charities

Charity fraud entails creating a fake charity and collecting “donations”.

How does charity fraud happen?

Scammers create fake charities that sound like ones you know and trust. These scams are especially common during natural disasters or international news events.

What are the warning signs?

Pressuring you to donate or even offering to pick up the money in person.

Using unsecured websites. (A secure website uses “https://” not “http://”).

What to do if you’re a victim

If you’re a victim of charity fraud,there usually isn’t a way to reclaim the money you’ve given.

Be wary of unfamiliar charities asking for donations.

6. Credit Card Fraud

There are several ways that criminals can steal your credit card information. They could steal your physical card, trick you into entering information on a phishing website or email, or buy your details on the Dark Web

Hackers can also create a clone of your physical card using just your credit card numbers.

What are the warning signs?

- Suspicious transactions on your credit card or bank statement.
- Small unfamiliar charges on your account.
- Fraud alerts from your bank, credit card issuer, or credit monitoring service.
- Calls from creditors about purchases you didn't make or new accounts you didn't open.
- Transactions from locations you haven't been (i.e., foreign countries).

What to do if you're a victim

If a scammer has access to your credit card, you'll want to act fast and shut down your compromised accounts and prevent credit card fraud.

Contact card issuer, or financial institution and explain the situation. They'll be able to help you freeze or close your accounts and get new cards. Contact police if your physical card was stolen.

Next, review your credit report for any fraudulent activity and dispute the charges. Finally, you'll want to set up a credit freeze or fraud alert to stop further transactions.

If a criminal has access to your credit card, they most likely have other sensitive information. Change all your account passwords to be more secure.

7. Financial Account Takeovers

When an identity thief scams you online to gain access to one of your online financial accounts it's known as an account takeover. A recent study showed that as many as 38% of consumers had been victims of account takeovers

How do financial account takeovers happen?

someone gains access to your email and password through phishing, a data breach, or an emerging cyber threat such as they steal your credentials while using public Wi-Fi.

Hackers not only want access to your accounts at financial institutions, there are plenty of other valuable accounts that many users don't secure. For example, a thief can buy goods with access to your Amazon account.

if you reuse passwords or use single-sign on accounts (i.e., log-in with Facebook), they can access multiple accounts with a single takeover.

What are the warning signs?

- Being locked out of your financial or social media accounts.
- Notifications of failed login attempts or two-factor authentication codes you didn't ask for.
- Your account looks different.
- Strange messages sent from your social media accounts.
- Alerts that someone logged into your account from a different IP address or location.
- The email or phone number associated with the account is changed without your permission

What to do if you're a victim

Contact the impacted companies .

You'll want to change all your passwords. Use strong pass phrases that combine letters, numbers, and symbols. Consider a password manager for keeping them safe.

Whenever possible, enable two-factor authentication (2FA) on your online accounts. This is a special, one-time code that's required to log into your accounts along with your password and username.

8. Ponzi Schemes and Other Investment Fraud

investment fraud gets you to put money into an investment that isn't real. like Ponzi schemes, the most common fraud schemes are simple: the thief disappears with your money.

How does investment fraud happen?

Fraudsters often lure victims with promises of large gains, little risk, and once-in-a-lifetime opportunities. In many cases, investment schemes target affinity groups — such as people who share a common religion or cultural background — to build trust.

Sometimes the supposed investors are asked to sign non-disclosure agreements, which can keep victims quiet once the thieves disappear

What are the warning signs?

- Special investment offers sent though unsolicited emails.
- One-of-a-kind or too-good-to-be-true opportunities.
- Investment schemes where the company is new or you can’t find additional information about them online.
- Investors asking you to sign an NDA before sending payment.

What to do if you’re a victim

Victims of investment fraud should report the fraud to police it’s unlikely you’ll recover money from this type of scam.

9. Small Business Financial Fraud (Embezzlement, Misuse, etc.)

If you're a business owner or entrepreneur, you're at risk for financial fraud. Losses from employee theft, embezzlement, and misuse of funds makes up for $50 billion dollars a year.

Your employees can steal from your business in several ways. The most common scams are embezzlement and misappropriation of funds.

Generally, white-collar crimes occur when employees have financial power without oversight and control.

Often the fraudsters are trusted employees, which makes this an emotionally devastating type of financial crime

What are some warning signs?

- Missing inventory or a higher-level of loss than you expect.
- Unexplained expenses on your company credit card.
- Employees who suddenly show signs of financial gain they can’t explain.

What to do if you’re a victim

If you suspect an employee is embezzling money from your company, speak to a lawyer and other experts. These are sensitive cases. You’ll need legal advice to handle the situation correctly.

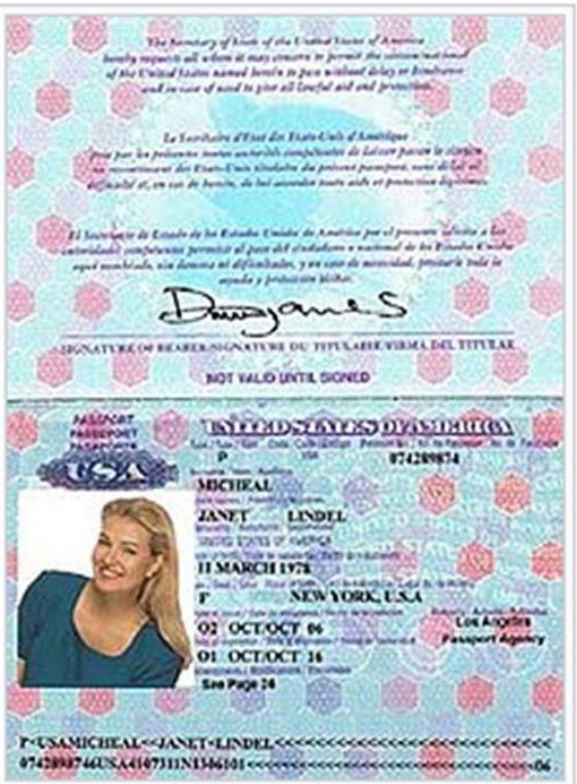
In the future, restrict access to financial information to only trusted employees who need access for their day-to-day work and perform regular audits.

10. Romance Scams

A romance scam is a confidence trick involving feigning romantic intentions towards a victim, gaining the victim's affection, and then using that goodwill to get the victim to send money to the scammer under false pretenses or to commit fraud against the victim.

The scammer’s intention is to establish a relationship as quickly as possible, endear himself to the victim, and gain trust. Scammers may propose marriage and make plans to meet in person, but that will never happen. Eventually, they will ask for money.

10. Romance Scams



This falsified passport was used in an actual Internet romance scam. The deception can be obvious to observers — for example, the photo on this passport does not comply with regulations for size or pose — but victims often overlook these signs.[1]

10. Romance Scams

https://www.youtube.com › watch

สาวพลาดท่าถูกผู้พันทหารบกหลอกเงิน 3 แสน | คุยข่าวเย็นช่อง8

สาวร้อง ถูกชายที่รู้จักกันทางเฟซบุ๊ก อ้างเป็น**ทหาร**ยศ "ผู้พัน" ทำงานใกล้ชิดน้องนายกฯ **หลอกยืมเงิน** 3 แสนบาท#ข่าวช่อง8 #**ถูกหลอก**...

YouTube · ข่าวช่อง8 · 14 พ.ค. 2565

https://www.youtube.com › watch

สาวถูกมิจฉาชีพอ้างเป็นทหารฝรั่ง ตุ๋นเงินกว่าแสนบาท | เกาะข่าวเที่ยง

ไปกันที่จังหวัดชุมพร **สาว**ใหญ่เจ้าของสวนยางหลงกลมิจฉาชีพอ้างเป็น**ทหาร**ฝรั่งทักเฟซบุ๊กตีสนิทให้เชื่อใจ**โอนเงิน**ให้สูญ1.6 แสนบาท...

YouTube · GMM25Thailand · 28 ก.ย. 2564

https://www.youtube.com › watch

สาวไทยถูกหนุ่มต่างชาติหลอกโอนเงิน | 28-02-62 | ข่าวเย็นไทยรัฐ

หญิงคนหนึ่งที่จังหวัดสงขลา นำหลักฐานลงบันทึกประจำวันกับตำรวจ หลัง**ถูก**ชายชาวต่างชาติหน้าตาดี อ้างว่าเป็น**ทหาร**อเมริกัน ...

YouTube · Thairath Online · 28 ก.พ. 2562

Tips for Avoiding Romance Scams:

- Be careful what you post and make public online. Scammers can use details shared on social media and dating sites to better understand and target you.
- Research the person's photo and profile using online searches to see if the image, name, or details have been used elsewhere.
- Go slowly and ask lots of questions.
- Beware if the individual seems too perfect or quickly asks you to leave a dating service or social media site to communicate directly.
- Beware if the individual attempts to isolate you from friends and family or requests inappropriate photos or financial information that could later be used to extort you.
- Beware if the individual promises to meet in person but then always comes up with an excuse why he or she can't. If you haven't met the person after a few months, for whatever reason, you have good reason to be suspicious.
- Never send money to anyone you have only communicated with online or by phone.

SEC
Office of Investor Education and Advocacy
Before You Invest, Investor.gov

Protect Yourself From Investment Scams

Office of Investor Education and Advocacy

United States Securities and Exchange Commission

Name

Date

Fraud: A Growing Problem in Crypto Markets

What is Crypto Fraud?

Crypto fraud refers to all events or transactions which lead to individuals losing their crypto assets to fraud and scams,

Happens due to the use of fake and stolen identities by fraudsters. Fraudsters have exploited security weaknesses in crypto exchanges and other crypto and DeFi organisations due to the lack of strong Identity Verification and Authentication.

Investing in cryptocurrency and other crypto assets are all decentralised investments and therefore it can be seen as DeFi fraud .

They are typically stored, transferred, or traded electronically. Crypto assets include cryptocurrencies such as Bitcoin and Ethereum, andsecurity tokens.

4 Scenarios of Crypto Fraud

Many ways in which crypto fraud can happen, but they have the same objective: to steal the user's hard-earned crypto assets.

The following are a few of many scenarios:

1. Fraudsters can hack a user's crypto wallet and steal their cryptocurrency and other crypto assets. The most common way which fraudsters gain access and control to the user's wallet accounts is through phishing, and installing malware on their devices.

2. Fraudsters often use social media platforms to convince users about investment or mining opportunities offering high profits. Asking for a payment in cryptocurrency, making them victims of investment fraud too. The crypto exchange can't do anything to retrieve the user's assets because they're not regulated.

3. Initial coin offering scams refers to the first offering of a cryptocurrency. They make users buy a promising cryptocurrency which has been purely fabricated for fraud and scam purposes.

4. Fraudsters also commit what are known as "scams on scams." They target existing victims who are vulnerable and promise to help them get their losses back. But instead, they just end up taking more money from them.

Centralised Finance (CeFi) and Decentralised Finance (DeFi)

Centralised Finance refers to the traditional financial practices by banking institutions which are controlled centrally. On the other hand, Decentralised Finance (DeFi) is a recent shift from traditional centralised financial systems. Instead of having third party intermediaries which are typically involved in traditional banking such as brokerages and exchanges.

DeFi enables with the use of decentralised technologies and cryptocurrency which are built on the blockchain. The purpose of this is to manage financial transactions. Such revolutionary financial changes may also bring threats that naturally happen as we adapt to them. With the rise of DeFi, there has also been a large increase in crypto fraud.

DeFi has a lot of potential for fraud because there are no intermediaries between users. All activity is automated with smart contracts. A recent article points out the absence of regulations within DeFi.

The Blockchain and Cryptocurrency

All digital data is stored in blockchains electronically. A blockchain stores a distributed database which is shared on the nodes of a computer network.

Blockchains remove the need for a third party and regulators as records of transactions are meant to be secured and decentralised.

Cryptocurrency is the most well-known type of crypto asset and with the increase of interest in digital assets, there is also an increase in fraud.

All decentralised activity takes place on the blockchain, and because blockchain technologies aren't regulated. If crypto assets are lost, there are gone forever.The main reason is due to the lack of having a central entity that traditional banks have, and they aren't protected by organizations like the FCA (The Financial Conduct Authority)or FSCS (The Financial Services Compensation Scheme)in the UK or FTC(Federal Trade Commission)in the USA.

Ways to prevent crypto fraud

The golden rule when it comes to crypto fraud and scams is if users have to question themselves twice about it then it's worth avoiding it. So, the best way for now until there are stronger fraud prevention methods in place, is to create awareness about the dangers around DeFi if there isn't knowledge about the vulnerabilities which users face daily in the world of crypto and DeFi.

Users should not trust strangers on social media channels. If someone reaches out offering to help, they should think twice before believing them. Fraudsters often ask for 'investment' payments in cryptocurrency. They even offer to help to set up a crypto wallet too, for those that don't have one.

Avoiding unknown links or attachments which have been received via email, text message or on social media. Fraudsters trick people by sending a malicious attachment which contains malware that will instantly be downloaded on the device to steal data, users must be particularly careful with excel attachments.

User must only invest in projects that have a proven roadmap and years or development or that have founders that have been in the crypto space for a long time and have good reputation.Having enough knowledge about DeFi and crypto assets before investing or managing any crypto elements is key, to make sure to take a smart and careful approach when investing.

Key findings

From January 2021 to March 2022, there has been a $1 billion loss to cryptocurrency scams alone. As opposed to bank transfer or payment fraud losses amounting to $756 million in the whole of 2021.

Fraud losses through DeFi platforms increased from $1.5 billion in 2021 to $10.5 billion in 2022. Resulting in a 600% increase.

From January 2021 through March 2022, $417 million in cryptocurrency was lost to fraud originating on social media. $273 million of these losses were to investment fraud, $69 million lost to romance and $35 million lost to business imposters.

The first three months of 2022 fraudsters have stolen over $1.22 million across DeFi projects.

From January 2021 to March 2022, there has been a **$1 billion** loss to cryptocurrency scams alone. As opposed to bank transfer or payment fraud losses amounting to **$756 million** in the whole of 2021

Fraud losses through DeFi platforms increased from **$1.5 billion** in 2021 to **$10.5 billion** in 2022 Resulting in a **600% increase**

The first three months of 2022 fraudsters have stolen **over $1.22 million** across DeFi projects

From January 2021 through March 2022, people reported to the FTC that **$417 million** in cryptocurrency was lost to fraud originating on **social media**

$273 million of these losses were to investment fraud

$69 million lost to romance

$35 million lost to business imposters

fraud.com

Crypto Fraud Prevention with Strong Identity Verification

The crypto and DeFi sector is still considered new and innovative, but regulations around fraud detection and prevention are evolving, mainly to prevent money laundering and identity theft. The use of fake and stolen identities to take over someone's account and steal their crypto assets is a growing concern.

As interest for crypto assets increases, organisations should also increase their safety when it comes to verifying the identity of their users. It is very important to authenticate users to ensure that it is not a fraudster.

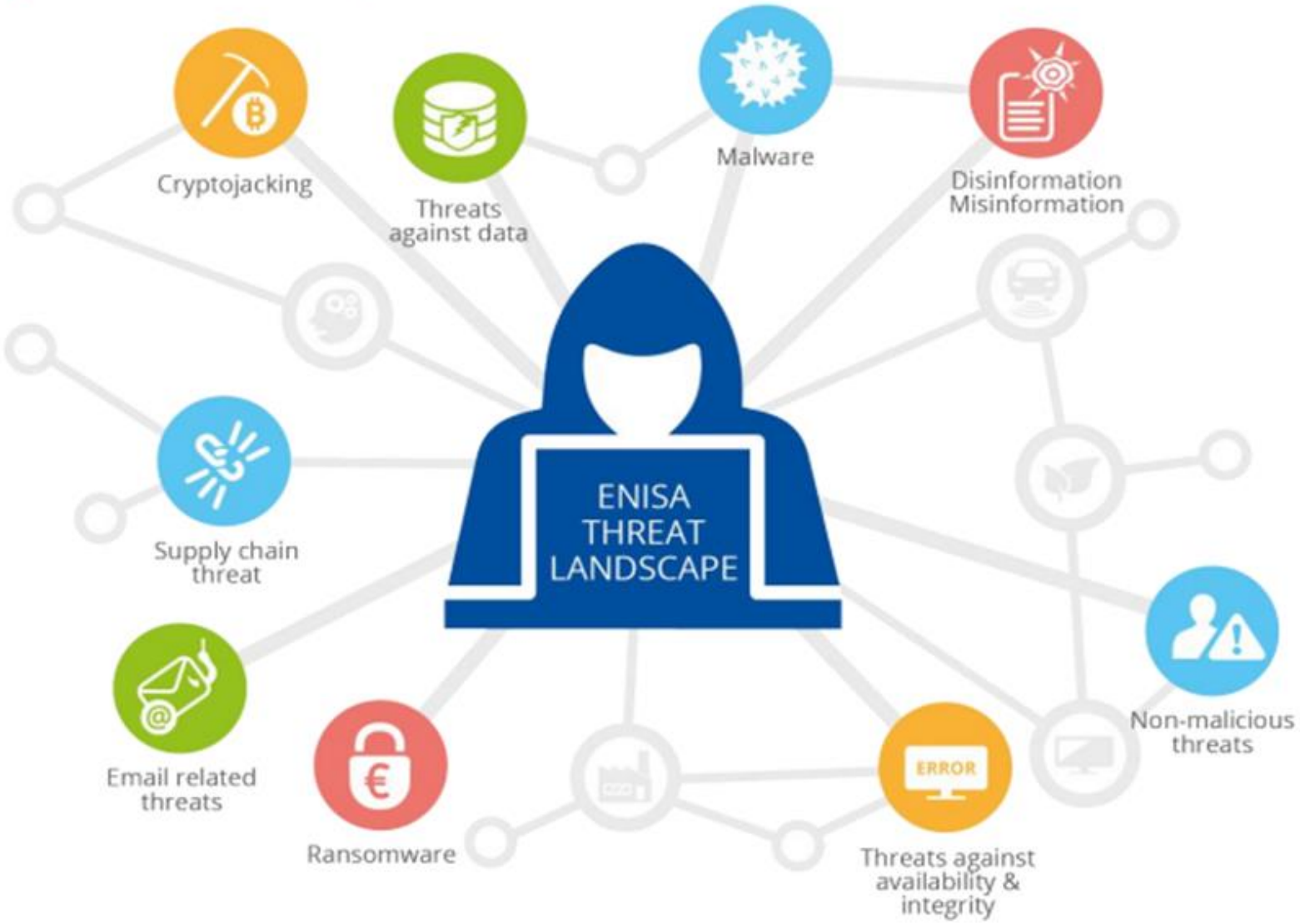
This can be achieved with powerful and advanced facial recognition and biometric liveness detection. This is to prevent fraudsters from easily accessing and controlling a user's assets. This can happen through account takeover, phishing scams, malicious attachments, or any of the other many ways fraudsters steal data.

Crypto Fraud Prevention with Strong Identity Verification

The safety of the users' assets should be achieved by having strong fraud detection and prevention systems in place to protect the customers and their data. If there are stronger KYC procedures in place to verify and authenticate the real customer.

The attraction to DeFi and crypto assets is spreading fast, thus there is still plenty of room for growth in this area. Organisations must be competent to keep up with fraudsters' attacks.

Figure 1: ENISA Threat Landscape 2021 - Prime threats



wealthmeup.com

สถิติ Financial Fraud ในไทย ปี 2564

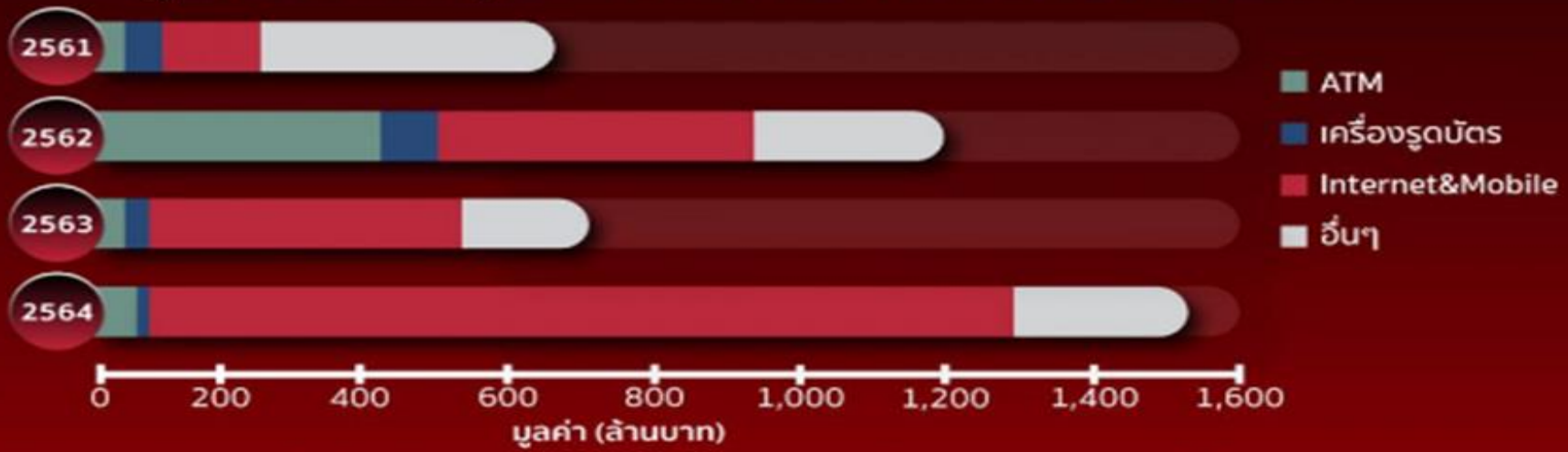
แก๊ง Call Center

- **คนไทยกว่า 21%** เคยเจอแก๊ง Call Center โทรมา
- จำนวนโทรศัพท์หลอกลวง **6.4 ล้านครั้ง**
  เพิ่มขึ้นจากปี 2563 = **270%**

SMS หลอกลวง

เพิ่มขึ้นจากปี 2563 = **57%**

มูลค่าการฉ้อโกงธุรกรรมการเงินแยกรายช่องทางการชำระเงิน



หมายเหตุ: มูลค่าถูกฉ้อโกงที่สถาบันการเงินดำเนินการพิสูจน์จนถึงที่สุดแล้วว่าเกิดการฉ้อโกงขึ้นจริง

1. WHAT: Financial Fraud คืออะไร?

Financial Fraud หรือ การฉ้อโกงทางการเงิน

ตัวอย่าง

การฉ้อโกงทางบัตรอิเล็กทรอนิกส์

การขโมยบัตร/ข้อมูลบนบัตร เพื่อนำไปซื้อสินค้าออนไลน์

การขโมยตัวตน/บัญชีม้า

เพื่อนำไปสวมรอยเปิดบัญชีธนาคาร หรือ บัตรอิเล็กทรอนิกส์

การหลอกลวงผ่านอินเทอร์เน็ต

กรณีมิจฉาชีพหลอกลวงทางออนไลน์ให้เหยื่อโอนเงิน

การหลอกลวงผ่านโทรศัพท์

แก๊ง Call Center หลอกลวงให้เหยื่อโอนเงิน

2. WHY: รู้ให้เท่ากัน

การหลอกลวงทางโทรศัพท์

1. 

มิจฉาชีพโทรมาอ้างว่าเป็นเจ้าหน้าที่ แจ้งว่ามีการ**ปลอมแปลงเอกสารของเหยื่อไปทำบัตรเครดิต ซึ่งเกี่ยวข้องกับการฟอกเงินที่เกี่ยวกับยาเสพติด**

2. 

เหยื่อปฏิเสธว่า**ไม่เคยไปเปิดบัญชีและไม่มีบัตรเครดิตของธนาคาร**

3. 

มิจฉาชีพอ้างว่าจะมีการ**ส่งเรื่องให้กับตำรวจตรวจสอบ พร้อมขอ Line ID**

4. 

ชายแต่งชุดตำรวจ Video Call มาขอตรวจสอบและแจ้งว่าเป็นคดีที่เกี่ยวข้องกับ**การฟอกเงินจากยาเสพติดและส่งเว็บไซต์หมายจับของศาลให้เหยื่อ**

5. 

เหยื่อเริ่มหลงเชื่อและโอนเงินเกือบ **'สองล้านบาท'** ให้มิจฉาชีพที่อ้างว่า เพื่อ**ให้ตำรวจตรวจสอบและหากเป็นเงินที่ได้มาถูกกฎหมายจะโอนเงินกลับคืนให้เหยื่อ**

6. 

เหยื่อถูกบล็อกและไม่สามารถติดต่อมิจฉาชีพได้
ปัจจุบันมีการแจ้งความออนไลน์และออกหมายอายัดบัญชีทันที

3. NOW: 'บัญชีม้า'
กับการจัดการในปัจจุบัน

บัญชีม้า คืออะไร?

การใช้บัญชีธนาคาร หรือ e-Wallet ของผู้อื่น เพื่อไปใช้ในการทุจริต
เช่น หลอกขายสินค้าทางออนไลน์ หรือแก๊ง Call Center แบ่งเป็น 2 ประเภท คือ

- ม้าสมัครใจ คือ การขายบัญชีธนาคาร/e-Wallet ให้ผู้อื่น และนำข้อมูลบัญชีไปขายต่อกลุ่มมิจฉาชีพ
- ม้าแบบไม่ตั้งใจ/ถูกสวมรอย คือ ถูกหลอกเอาข้อมูลไปเปิดบัญชีธนาคาร/e-Wallet ในการทำธุรกรรมทุจริต

การจัดการในปัจจุบัน

1. สำนักงานตำรวจแห่งชาติ (สตช.)
- การแจ้งความออนไลน์ ผ่านเบอร์โทรศัพท์ หรือ เว็บไซต์
- ออกหมายอายัดบัญชีทางออนไลน์ อายัดได้ทันทีไม่เกิน 24 ชั่วโมง

2. สมาคมธนาคารไทย
- ปรับปรุงกระบวนการอายัดบัญชีของผู้กระทำผิดให้เร็วขึ้น
- ทำบัญชี Watchlist และแจ้งเตือนให้ระวังก่อนโอนเงินใน Mobile Banking

3. สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.)
- ระงับการโทรจากต่างประเทศกรณีหมายเลขต้นทางผิดปกติ
- เพิ่ม Prefix +66 กรณีการโทรเข้าจากต่างประเทศที่ไม่กำหนดเลขหมายต้นทาง

4. Future: ปัญหาและแนวทางแก้ไข

ปัญหาปัจจุบัน

1. ไม่มีกฎหมายรองรับชัดเจน ในการเอาผิดโดยตรง **กับคนรับจ้างเปิดบัญชี หรือมอบบัญชีตนเองให้มิจฉาชีพ**
2. กระบวนการส่งข้อมูล และตรวจสอบเพื่อแจ้ง **อายัดบัญชีที่ใช้ฉ้อโกงยังล่าช้า**
3. การทำ KYC เพื่อแสดงตน ของผู้เปิดบัญชี ยังมีช่องโหว่ **ในกรณีที่มีการขายบัญชีตนเอง เนื่องจากเป็นการยินยอม ของเจ้าของบัญชี**

แนวทางแก้ไข

สำนักงานป้องกันและปราบปราม การฟอกเงิน (ปปง.) **อยู่ระหว่าง การแก้ พ.ร.บ. และหารือแนวทาง**

ปรับปรุงรูปแบบหรือช่องทาง และกำหนดเวลาให้ชัดเจน ในการ**แลกเปลี่ยนข้อมูลและอายัดบัญชี ระหว่างหน่วยงานที่เกี่ยวข้อง**

มีนโยบายหรือการสื่อสารจากภาครัฐ ที่ให้ความสำคัญกับการป้องกัน และ**แก้ไขบัญชีม้า และให้ความรู้ กับประชาชนผ่านช่องที่หลากหลาย**

The total impacts of financial fraud

The impacts of fraud set out in this guide are:

Human impact

Fraud against public bodies is not a victimless crime. Fraud can be a traumatic experience that often causes real and irreversible impacts for victims, their families, carers and communities. Those who rely on government services, such as the elderly, the vulnerable, the sick and the disadvantaged, are often the ones most harmed directly or indirectly by fraud. Fraud can have a devastating and compounding effect on these victims; amplifying the disadvantage, vulnerability and inequality they suffer. Fraud can also cause lasting mental and physical trauma for victims, and in some cases, take people's lives.

Government outcomes impact

Fraud against public bodies compromises the government's ability to deliver services and achieve intended outcomes. Money and services are diverted away from the intended targets and the services delivered can be substandard or unsafe. This can lead to program failure. It also leads to lost opportunities for individuals and businesses.

The total impacts of financial fraud

Reputational impact

Fraud happens and can affect any public body. However, when it is handled poorly, fraud against government programs can result in an erosion of trust in government and industries, and lead to a loss of international and economic reputation. This is particularly true when fraud is facilitated by corruption.

Government system impact

Fraud drains government resources across multiple areas including investigations and compliance, prosecution, prison, welfare, identification and computer systems.

Industry impact

Fraud against public bodies can result in distorted markets where fraudsters obtain a competitive advantage and drive legitimate business out. It can affect services delivered by business and expose other sectors to further instances of fraud. It can also result in greater burdens on charities and community services who assist those affected by fraud against public bodies.

The total impacts of financial fraud

Environmental impact

Fraud against public bodies can lead to immediate and long term environmental damage through pollution and damaging ecosystems and biodiversity. It can also result in significant clean-up costs.

Security impact

Fraud against public bodies can compromise national defence and security, putting service men and women, and citizens at risk. It can also damage international standing and affect the ability of nations to get international support. Fraud against government programs can be used to fund organised crime groups and terrorism, potentially leading to further crime and terrorist attacks.

Financial impact

Based on international estimates, public bodies generally lose between 0.5% and 5% of their spending to fraud and related loss.The majority of fraud is hidden and undetected and can be difficult to categorise. Calculating the financial impact can assist agencies understand their potential losses and how to mitigate them.

Business impact

Business costs for dealing with fraud against government programs are significant and extensive and go well beyond the direct financial loss. They can include assessment, detection, investigation and response costs as well as potential restitution. In addition, further costs can include program review and audits and retrofitting or redesigning programs.

Contact :
08 6733 0477
dechadecha@gmail.com

THANK YOU

https://www.tfac.or.th

@TFAC.FAMILY

tfac@tfac.or.th

https://www.facebook.com/TFAC.FAMILY

https:// www.youtube.com/TFACFamily

02 685 2500