Managing Security and Fraud in a Data, AI and Cloud World

IN COLLABORATION WE TRUST,
CREATING LASTING VALUE

11:00 – 11:30, 24 September 2026

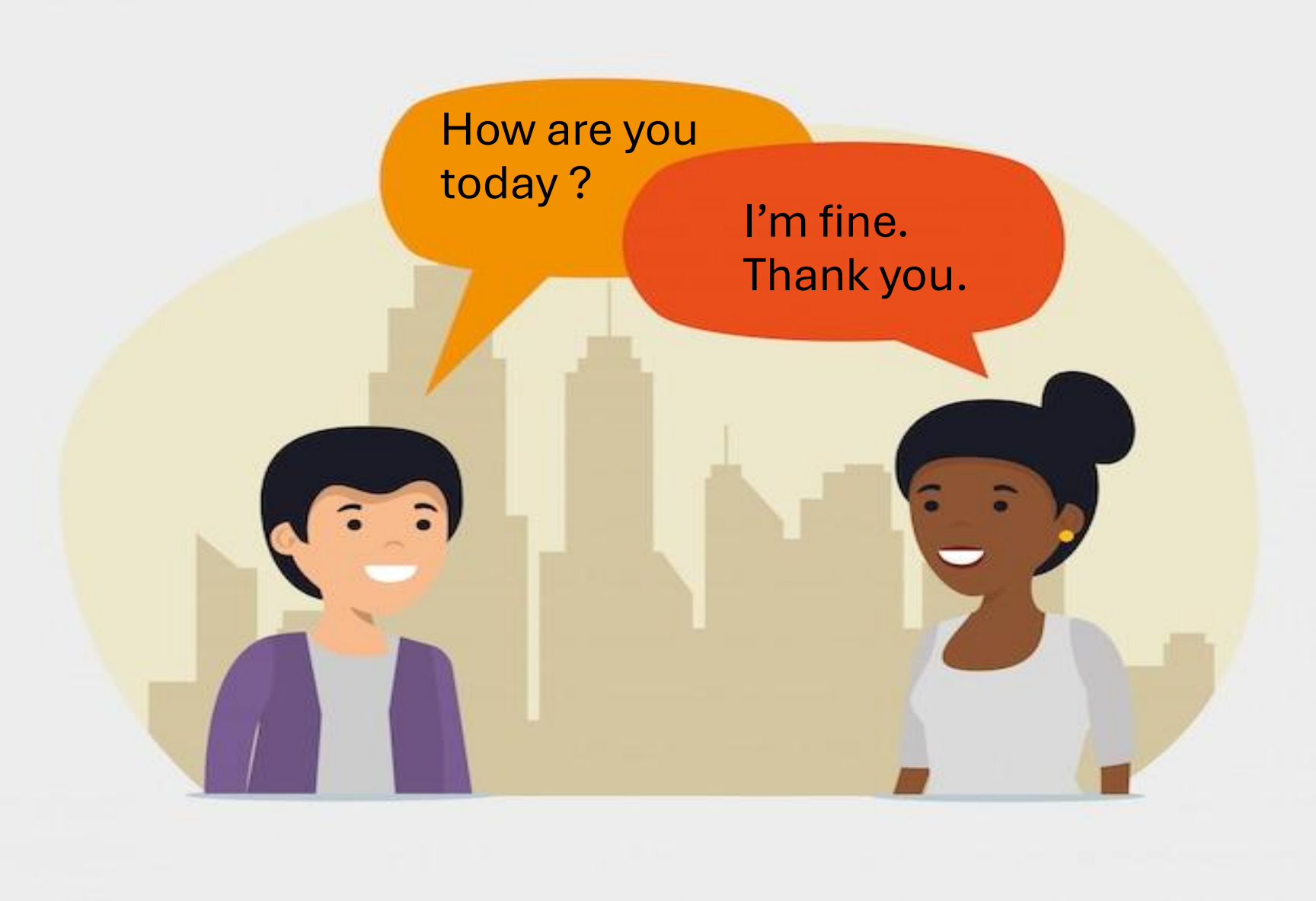
The Berkeley Hotel Pratunam

At DUGA – Powering Decision with Real-Time and AI ready Data

Kitti Kosavisutte, Ph.D.

THAILAND BANKING SECTOR CERT
2026

Face-to-Face Greeting



Online Greeting

The Change in Human Communication Mechanism

Face-to-face

3 elements of communication

- ✓ Word
- ✓ Voice
- ✓ Body language

Online messaging

- ✓ Text
- ~~Voice~~
- ~~Body language~~

⟹

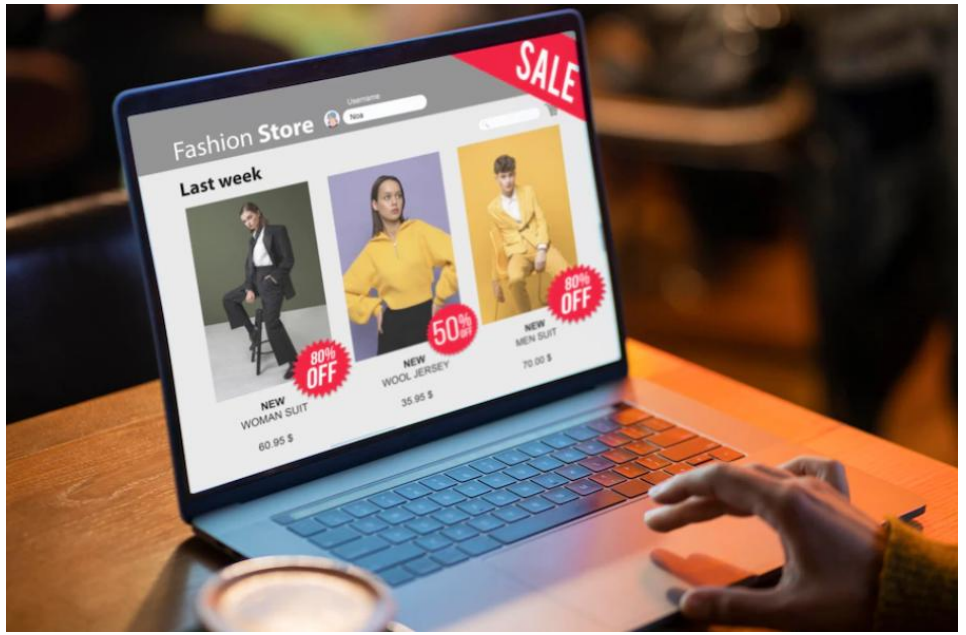
- ✓ Voice record
- ✓ emoji

→ Information dimension loss

The 3 Elements of Communication – Body Language, Voice and Words. When we communicate with someone face to face we pass the information and understanding through 3 different elements – body language, voice and words. The message isn't however communicated equally across all 3. This was demonstrated in a theory by Dr. Albert Mehrabian in 1970.

- **Words** – the actual words that make up our message – **7%**
- **Voice** – the pitch, pace, tone and volume of our voice – **38%**
- **Body Language** – the visible actions that we show to others using all parts of our body – **55%**

Traditional Shopping and Online Shopping



- ✓ Feel, touch, taste
- ✓ Negotiation
- ✓ Body language

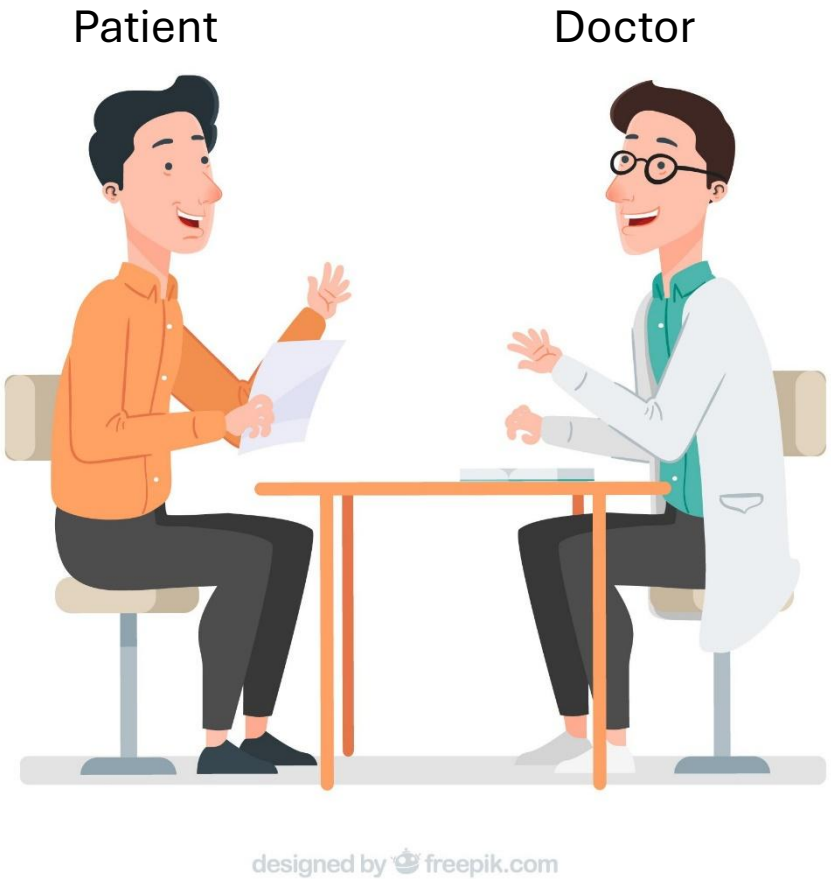
- ~~Feel, touch, taste~~ ➡ • Picture
- ~~Negotiation~~ ➡ • Review & comment
- ~~Body language~~ ➡ • Own experience

The weaknesses in transforming to digital/online services are due to the loss of information dimensions.

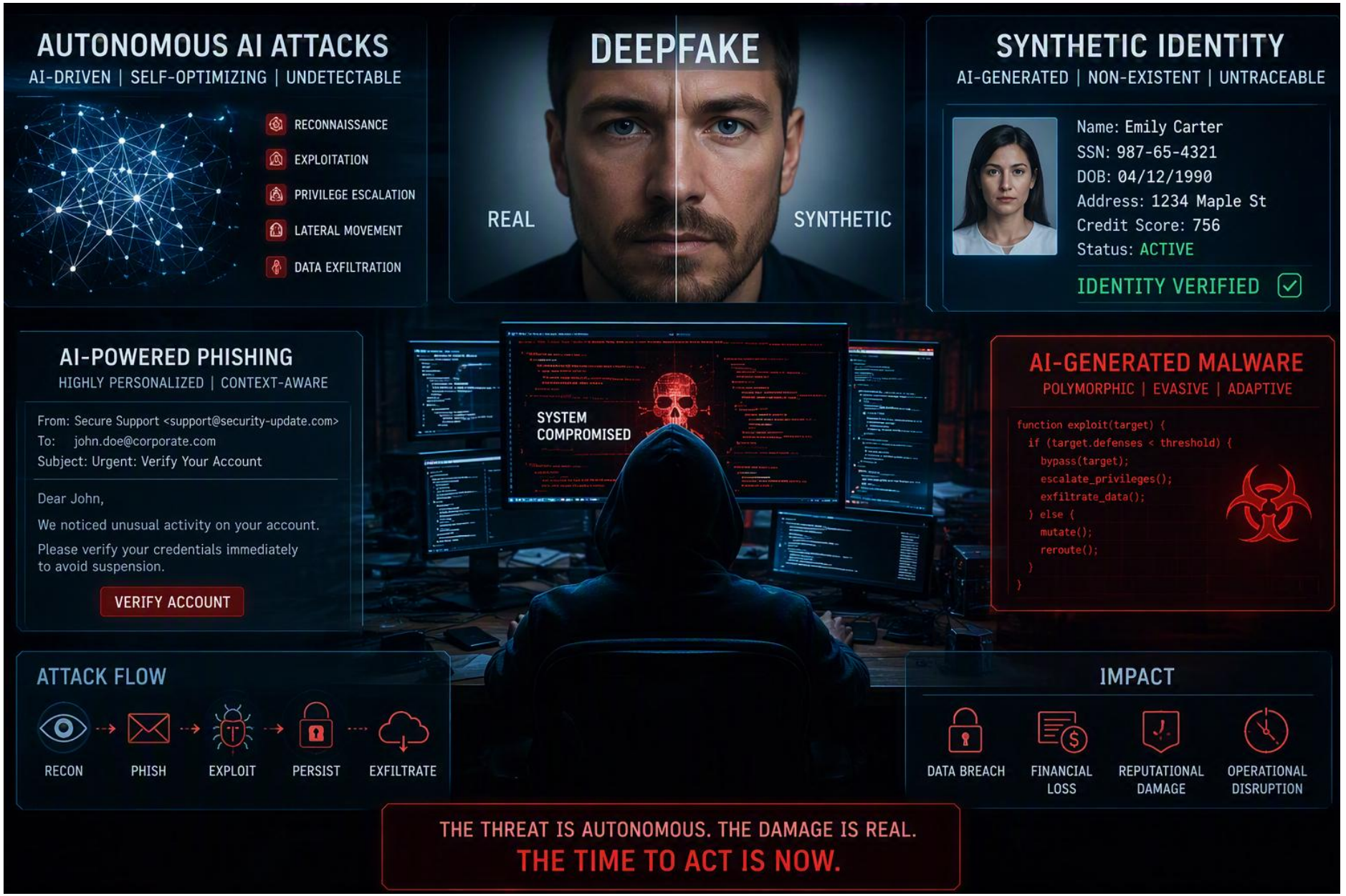
Now, Let’s Listen to the Interesting Story

frog

magic pill



Fraud and New Perspectives from AI and the Digital Ecosystem



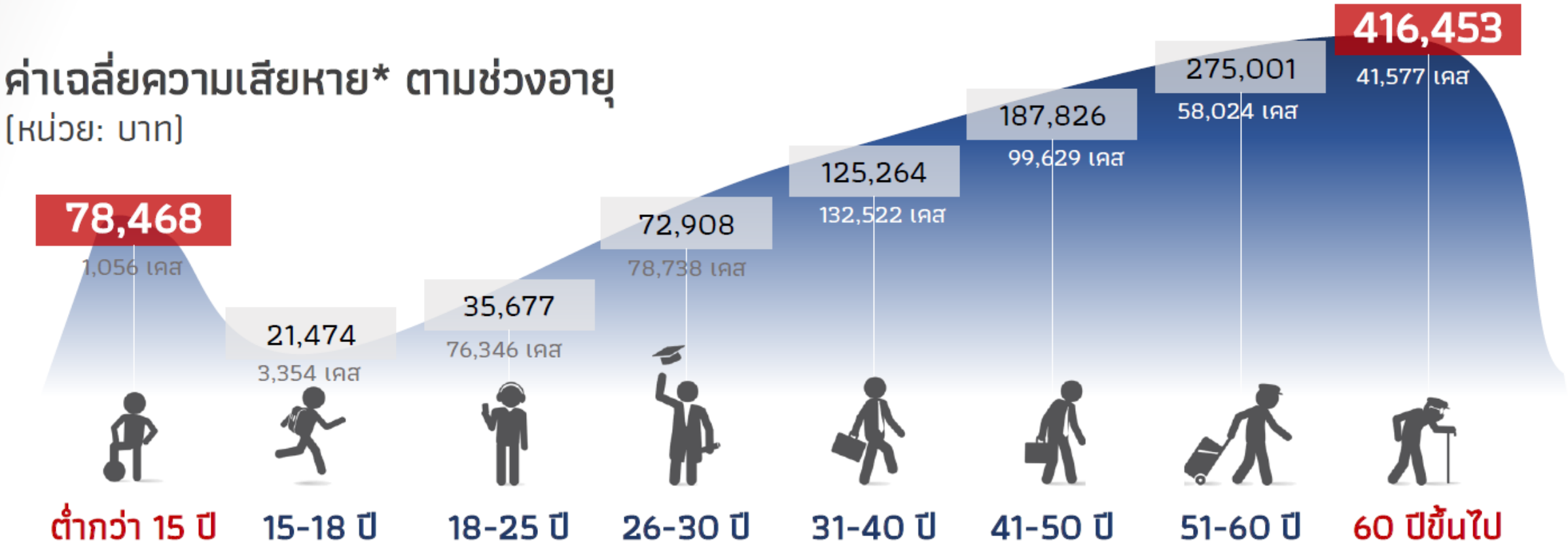
Fraud and New Perspectives from AI

- Autonomous AI attack
- Hyper-realistic deepfake
- Synthetic identity
- AI-Powered phishing & malware

Etc.

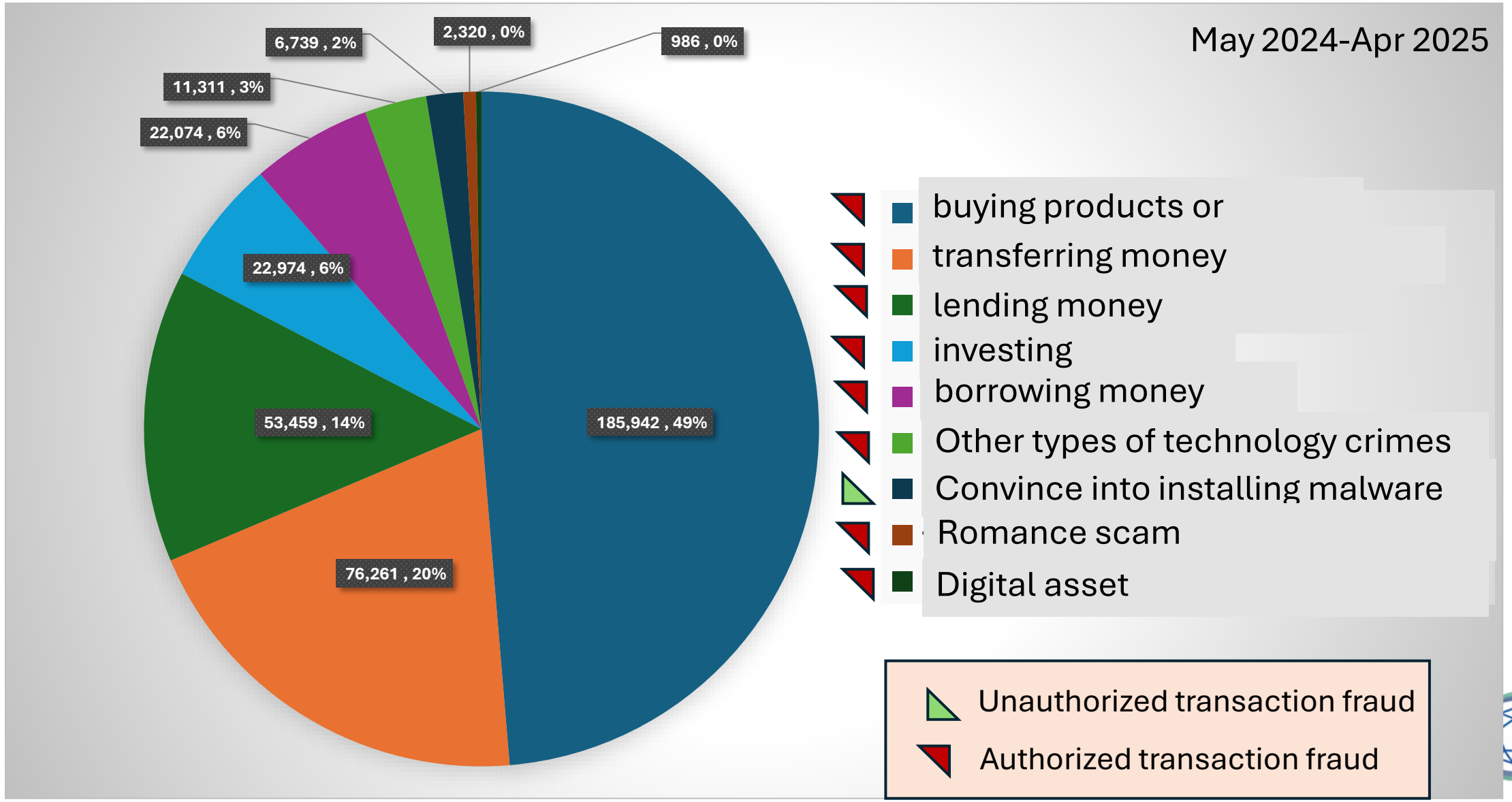
Statistic of Fraud Cases

เด็กและผู้สูงอายุมักเป็นเป้าหมายของมิจฉาชีพ



* ข้อมูลสะสมตั้งแต่ 1 มี.ค. 65 – 30 มิ.ย. 68 โดยไม่รวมเคสหลอกลวงซื้อขายสินค้าหรือบริการ
ที่มา : ระบบ Thai Police Online

Authorized Transaction Fraud Statistic - Number of cases by type



มาตรการ ธปท. มีส่วนช่วยแก้ปัญหา

จำนวนเคสแอปดูดเงิน

ที่มา : สง. 17 แห่ง

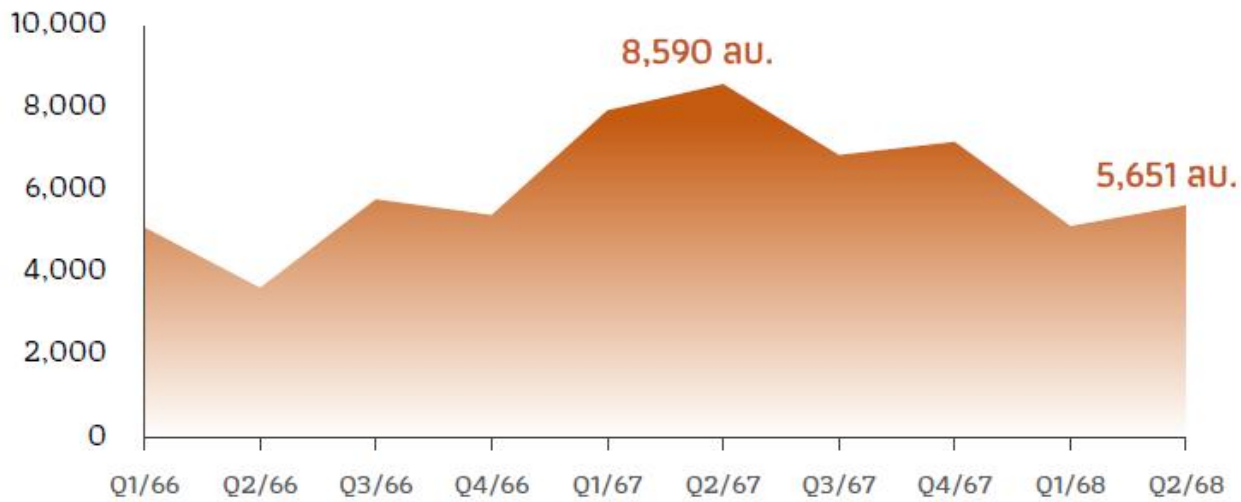
การระงับบัญชีม้า* (ณ ก.ค. 68)

บัญชีม้าที่ถูกระงับ **2.8 ล้านบัญชี**
รายชื่อม้า **1.97 แสนรายชื่อ**

* ข้อมูลสะสมจาก ปปง. Central Fraud Registry (CFR) และ สง. 17 แห่ง
ม้าดำสะสมตั้งแต่ มี.ค. 66/ม้าเทาและม้าน้ำตาลสะสมตั้งแต่ ม.ค. 67

แต่ยังเกิดเหตุจำนวนมาก ที่เหยื่อถูกหลอกให้โอนเงินเอง

มูลค่าความเสียหายกรณีหลอกให้โอนเอง



ที่มา : สำนักงานตำรวจแห่งชาติ

สถิติการฉ้อโกงออนไลน์ 4 เดือนแรกปี 2569

สำหรับรูปแบบการหลอกลวง พบว่าแบ่งออกเป็น 3 ประเภทหลัก ได้แก่

1.**การหลอกลวงด้านสินค้าและบริการ** มีจำนวนคดีสูงที่สุด 85,215 คดี คิดเป็น 69.9% ของคดีทั้งหมด ความเสียหายเฉลี่ยต่อคดีอยู่ที่ 15,727 บาท
โดยมีทั้งการหลอกผู้ซื้อและผู้ขาย โดยใช้ เพจ/บัญชีปลอม ในการชายสินค้า สร้างเอกสารการชำระเงินปลอมเป็นต้น

2.**กลุ่มหลอกลวงเชิงผลประโยชน์/ ลงทุน** สร้างมูลค่าความเสียหายสูงสุด 5,997.7 ล้านบาท หรือ 80.2% ของมูลค่าทั้งหมด ความเสียหายเฉลี่ยต่อคดี 166,449 บาท
โดยการหลอกให้ทำงาน หลอกลงทุน แอบอ้างเป็นผู้มีอำนาจ รวมถึงการหลอกให้รักผสมผสานอยู่ด้วย

3.**กลุ่มการโจมตีทางเทคนิคเชิงรุก** และคดีฉ้อโกงเทคโนโลยีอื่นๆ เป็นภัยคุกคามที่ต้อง อาศัยทักษะทางเทคนิคของคนร้าย หากนับเชิงปริมาณ ถือว่า น้อยที่สุด มี
จำนวนคดี 673 คดี คิดเป็น 0.55% แต่ค่าเฉลี่ยความเสียหายต่อคดีกลับอยู่ที่ 211,686 บาท ถือว่าสูงที่สุด และเป็นภัยคุกคามขั้นสูง
โดยใช้ ฟิชชิ่งในการขโมยข้อมูลประจำตัว เจาะระบบ รวมไปถึงใช้ malware/ransomware ในการเรียกค่าไถ่มูลค่าสูง

จากข้อมูลพบว่ารูปแบบนี้มีการขยายตัวอย่างน่ากังวล โดยเฉพาะในเดือน มี.ค. มีจำนวน 385 คดี มูลค่าความเสียหาย 87.7 ล้านบาท พบมาจากการ Phishing / Hacking ขนาดใหญ่ และคดี Ransomware ที่มีมูลค่าต่อคดีพุ่งสูง

ทั้งนี้ในช่วง1-2 เดือนหลังนี้ พบการหลอกลวงกลุ่ม นักศึกษา ด้วยการใช้รางวัลหลอกล่อ มีสถิติสูงขึ้น

ข้อมูลอ้างอิง: ศูนย์ต่อต้านการฉ้อโกงออนไลน์ (ACSC)

User Journey and Layered Control Stack

	Customer	User Device	Communication	Service	Data
Risk	✓ Deception ✓ Giving information unawares	✓ Insecure device ✓ Malicious application ✓ Excessive permission ✓ Obsolete OS	✓ Eavesdrop ✓ Fake SMS sender	✓ Insecure application ✓ Weak identification ✓ Weak authentication	✓ Information leakage
Control Stack	✓ Identity proofing ✓ Awareness communication	✓ Application initiation ✓ Application tampering ✓ Face recognition ✓ OS security check	✓ Secured communication ✓ SIM owner check	✓ Application security ✓ Identity verification ✓ Authentication ✓ Transfer limit	✓ Strengthen data protection by all related parties ✓ Threat intelligence ✓ Fraud detection ✓ Velocity check ✓ Monitoring ✓ Investigation ✓ Digital risk protection

Human Centric Attack

- Cybersecurity threats that originate from predictable human behaviors, decisions, error or interactions whether intentional or unintentional, which adversaries can exploit to compromise systems, data or operations. Key characteristics are
  - Predictable patterns of user behavior
  - Lack of security awareness or training
  - Overthrust in digital systems or social actors
  - Bypassing security for convenience
  - Cognitive biases impacting judgment

Shared Responsibilities

Financial Institution

- Mobile app security
- Mobile owner verification
- 1 device 1 mobile app account
- User identification by Face recognition
- Strengthen KYC process and account opening process
- Real-time alert in high-risk activities and outgoing payment transaction
- Central fraud registry system (CFR)
- **Information sharing via TB-CERT**
- Awareness communication

Platform Provider

- Take down fake content (Social Media)
- Strengthen OS and mobile environment (Mobile Platform-Android)

Regulator

- Mobile app security standard across banking sector for bank and non-bank under supervision
- Establish policy preventive measures
- Collaborate with regulators, government agencies and FIs

Law Enforcement

- Forensics investigation
- Collaboration with banks to freeze or trace fraudulent transaction/accounts

Police crack down on mule account smuggling

Mobile Operator

- Prevent fake sender name
- Filter link on SMS message
- Strengthen SIM registration

User

- Practice good cyber hygiene and never giving away their personal or account credentials to anyone
- No click link
- Verify in-bound contact
- No root/jailbroken phone
- Secure mobile device
- Regular update mobile OS

IN COLLABORATION WE TRUST,
CREATING LASTING VALUE

Thank you

THAILAND BANKING SECTOR CERT
2026