Build a Secure Cyberspace 2016
“Protect Data, Secure Transaction” Seminar
November 25th 2016 @ Hong Kong

# SAFEGUARDING YOUR EMAILS

**Albert Hui**
GREM, GCFA, GCFE, GNFA, GCIA, GCIH, GXPN, GPEN, GAWN, GSNA, GSEC, CISA, CISM, CRISC
SECURITY RONIN

# WHO AM I?

## Albert Hui

GREM, GCFA, GCFE, GNFA, GCIA, GCIH, GXPN, GPEN, GAWN, GSNA, GSEC, CISA, CISM, CRISC

SECURITY RONIN

- Co-designed the first Cyber Forensics curriculum for **Hong Kong Police**, trained cops
- CSIRT Manager at an Investment Bank
- **ACFE** (Association of Certified Fraud Examiner) Asia Pacific Fraud Conference keynote speaker
- **HTCIA** (High Tech Crime Investigation Association) Asia Pacific Forensics Conference speaker

- Technology Risk Manager at Multinational Banks
- Risk Consultant for Government and Critical Infrastructures

- **Black Hat** speaker

# UNWITTING VICTIMS OF EMAIL FRAUD

Financial Losses

Criminal Liability
(handling Proceeds of Crime)

AML & CTF
Implications

# BUSINESS EMAIL COMPROMISE (BEC) AKA "CEO FRAUD"

## Goals

- Primarily to scam victims into wiring money out
- Some scam victims to give out identity information

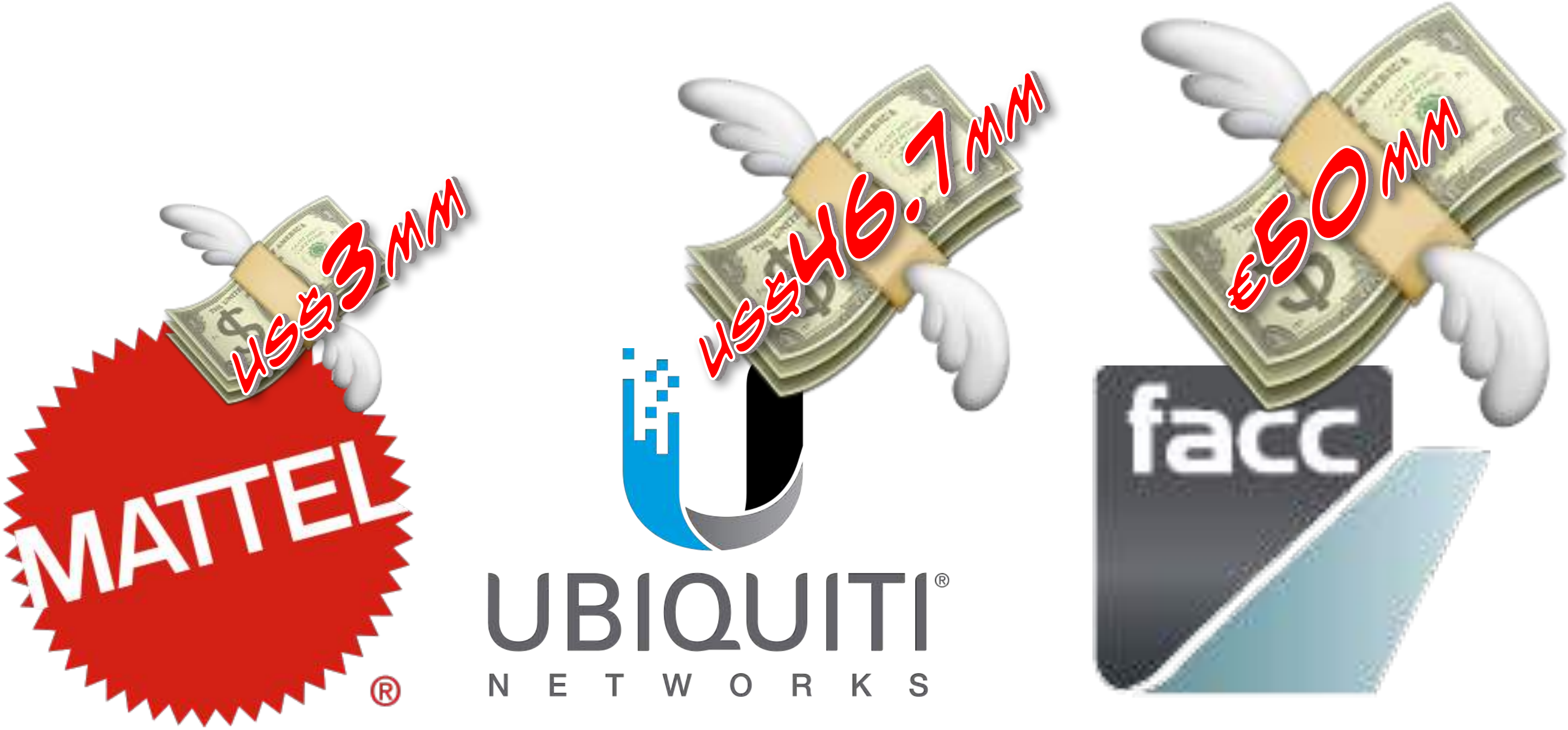
## Natures

- Targeted Attack
  - Spear Phishing
- Social Engineering Attack

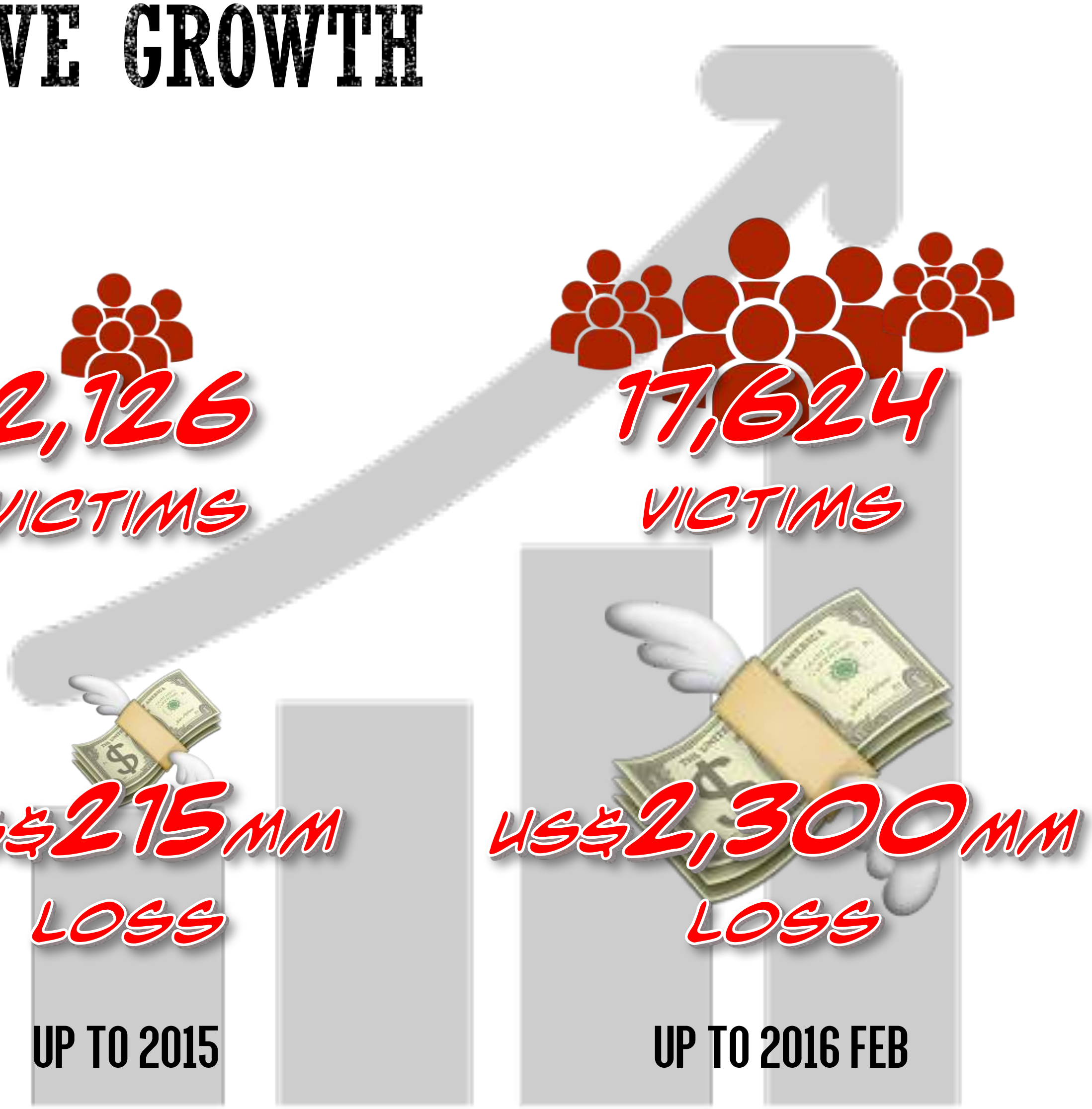
## Mechanism

- MITE (Man-in-the-Email) Attack

# HIGH PROFILE CASES



# EXPLOSIVE GROWTH



2,126

VICTIMS

US$215MM

LOSS

UP TO 2015

17,624

VICTIMS

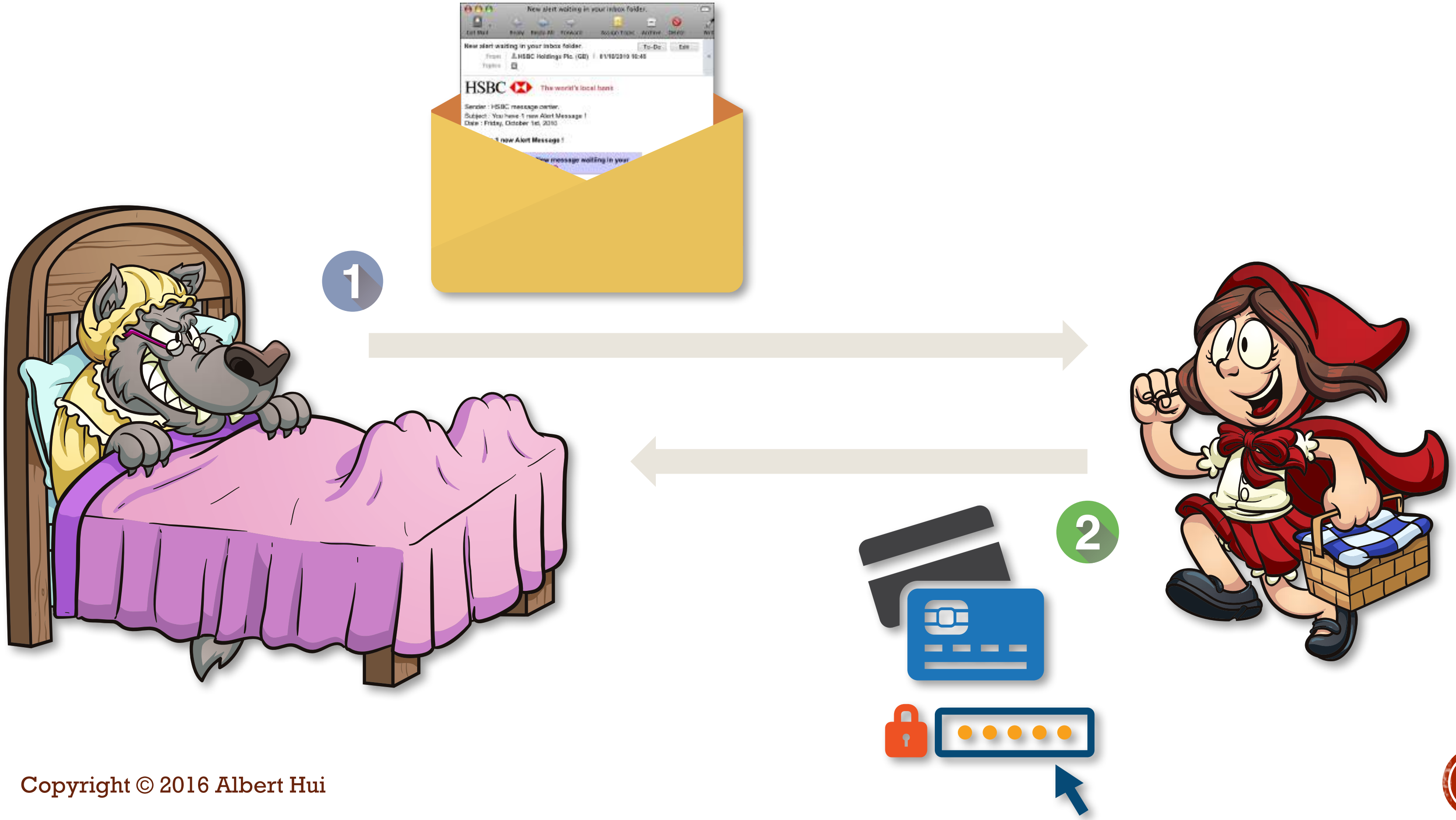
US$2,300MM

LOSS

UP TO 2016 FEB

Source: FBI IC3 Alert

# HOW DOES TRADITIONAL PHISHING WORK?



New alert waiting in your inbox folder.

New alert waiting in your inbox folder.

From: HSBC Holdings Plc. (GB) | 01/10/2010 10:46

Topics:

HSBC The world's local bank

Sender : HSBC message center.

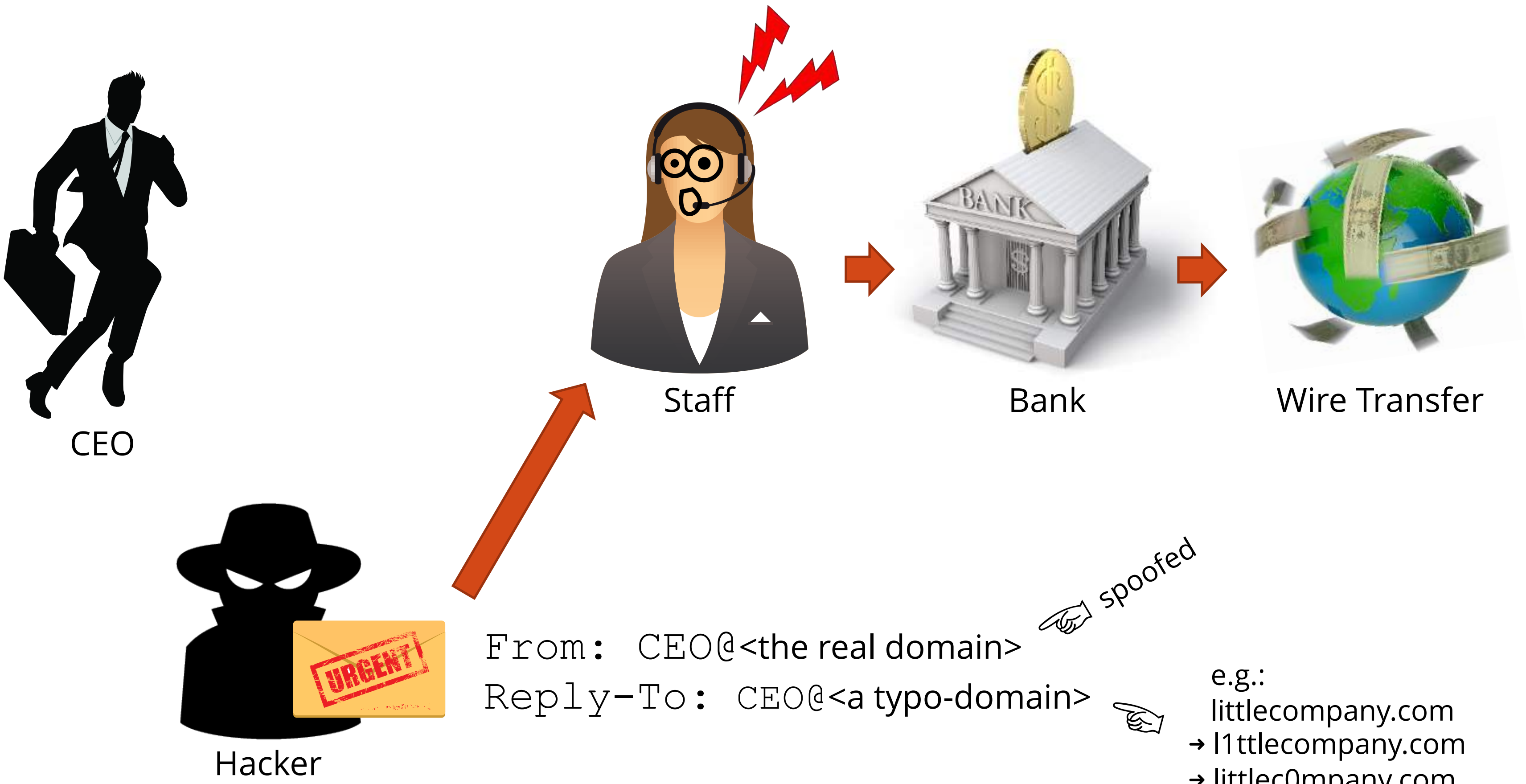
Subject : You have 1 new Alert Message !

Date : Friday, October 1st, 2010

1 new Alert Message !

New message waiting in your

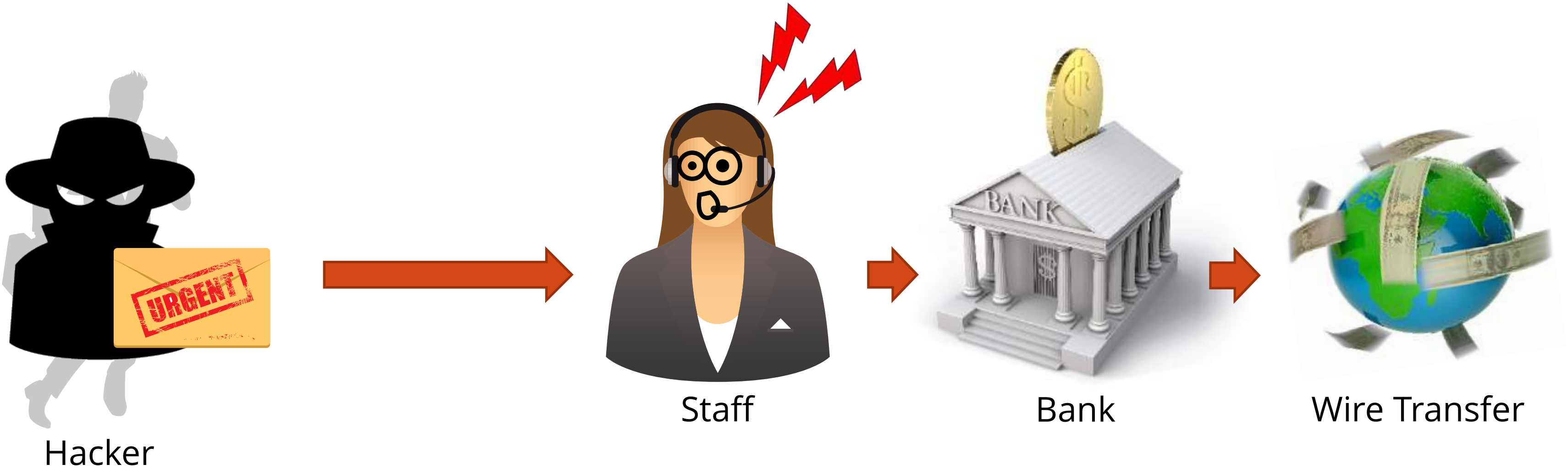
# HOW DOES CEO FRAUD WORK?



From: CEO@<the real domain> ☜ spoofed
Reply-To: CEO@<a typo-domain> ☜

e.g.:
littlecompany.com
→ l1ttlecompany.com
→ littlec0mpany.com
→ llttlecompany.com
→ etc.

# HOW DOES CEO FRAUD WORK? (VARIANT WITH HACKING)



✓ No spoofing, no typo-domain

✓ Very realistic: Modified from previous emails, bear correct signature

# FRAUDSTERS COMMONLY POSING AS...

CEO or other senior exec

Foreign Suppliers

Attorney

# VICTIMS

Small Companies

Large Enterprises

Banks / FIs

# WHY SO EFFECTIVE?

## By Nature

- Delayed detection
- Efficient underground money laundering mechanisms

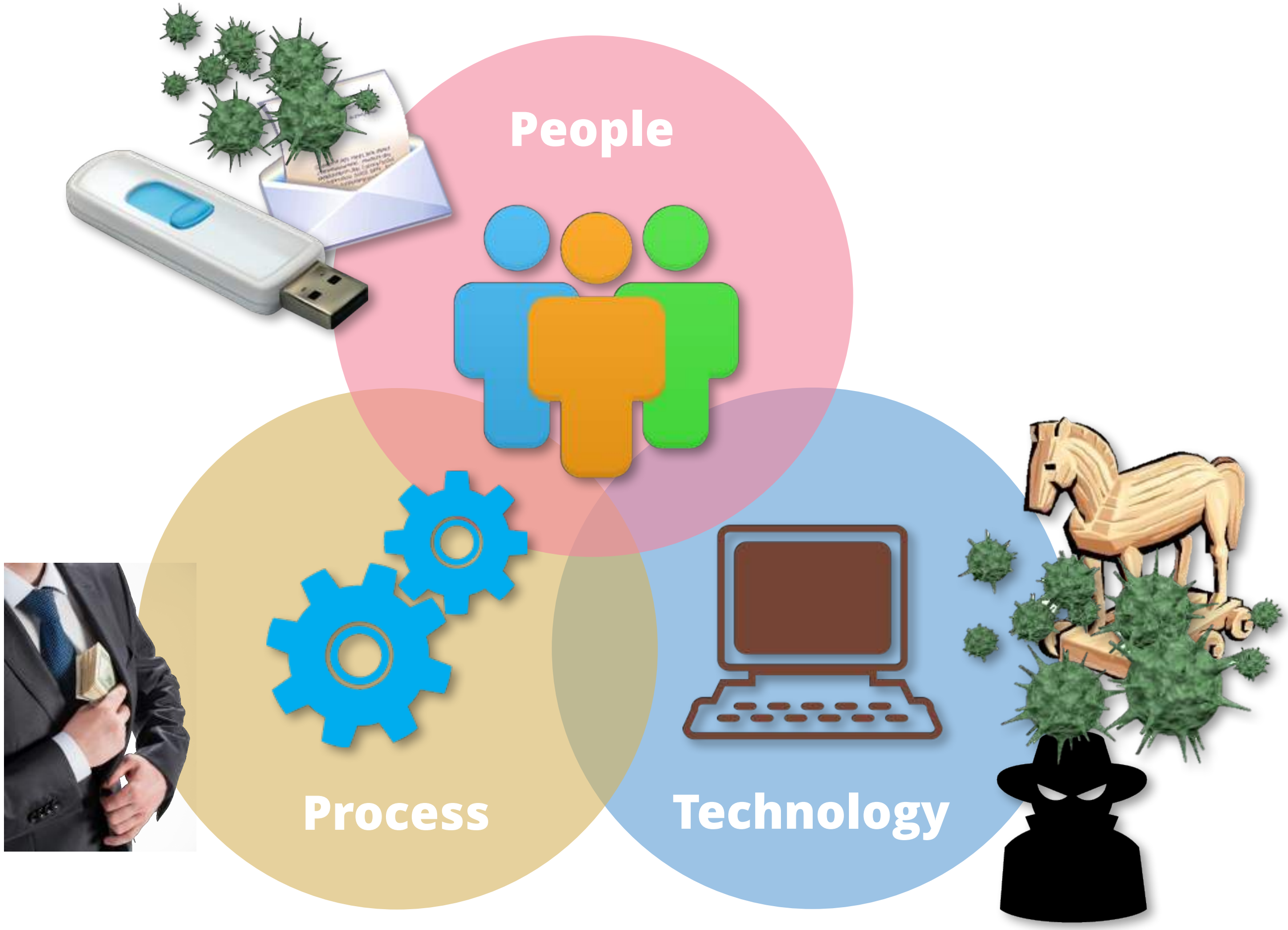
## Defeat Cybersecurity Controls

- No malicious payload or links to detect
- Bypass dual-custody
- Bypass 2FA

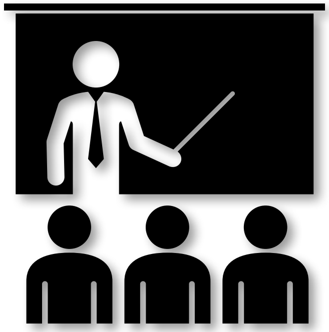
## Defeat Procedural Controls

- Bypass bank call-back

# THREE PILLARS

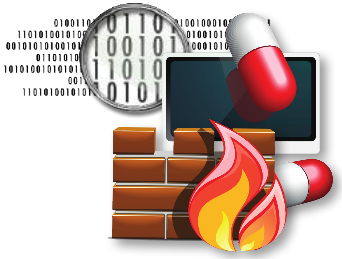


# COUNTERMEASURES



Awareness Training

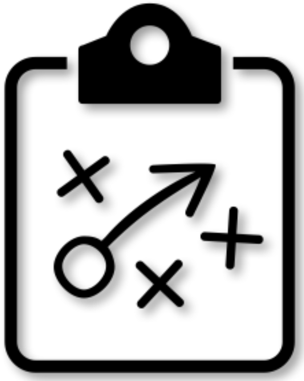
Management Buy-In



IT Security Controls

Verification Protocol

Check for typo-domains
Alert on
payment instruction changes
…more (see next slide)



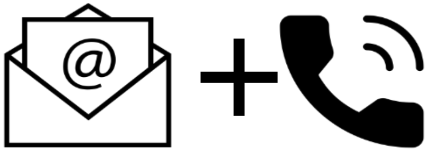
Response Plan

How to handle compromisse?
Who to call, what parties to notify?
Legal support (freezing order, etc.)
etc.

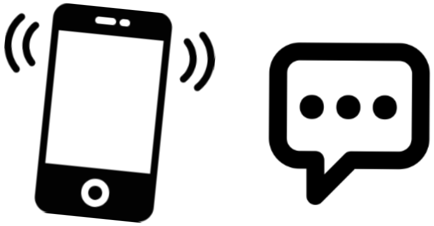
# VERIFICATION RULES-OF-THUMB

1. Use out-of-band verification mechanisms

e.g.

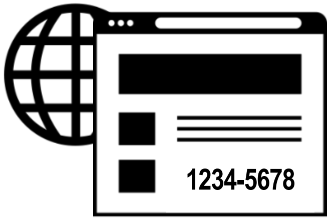


2. Do not trust incoming calls or SMS messages



3. Do not authenticate yourself before the counterparty identity is verified (or contact information comes from trusted source)

e.g.



☜ Look up phone number on trusted site

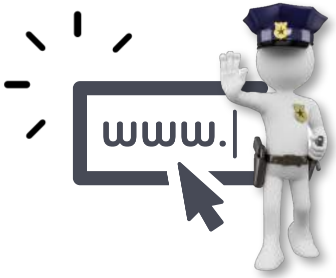
# TECHNICAL CONTROLS

On top of IT hacking defences…

1. Typo-domain monitoring services

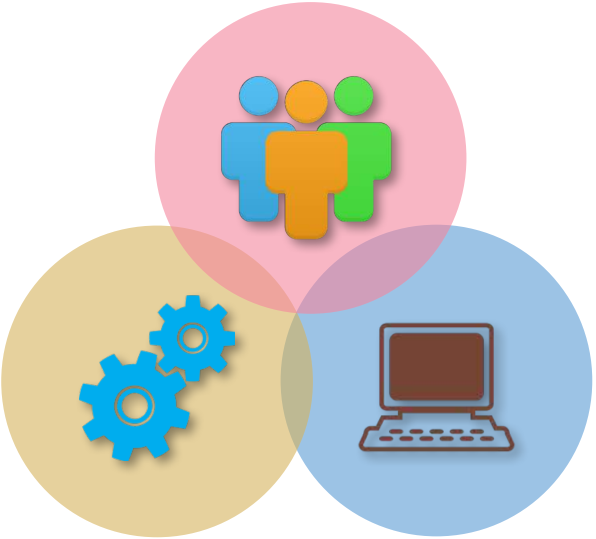
Oo0… lliI…

2. Reputation-based email filtering (reject known spams and red-flag newly-registered domains)



# SUMMARY

- Security demands not just IT security controls…
- …but also Process and People security controls
- People often the weakest link



# THANK YOU!

SECURITY RONIN

albert@securityronin.com