



# **Shielding the Healthcare Sector: Safeguarding against Cyber Threats**

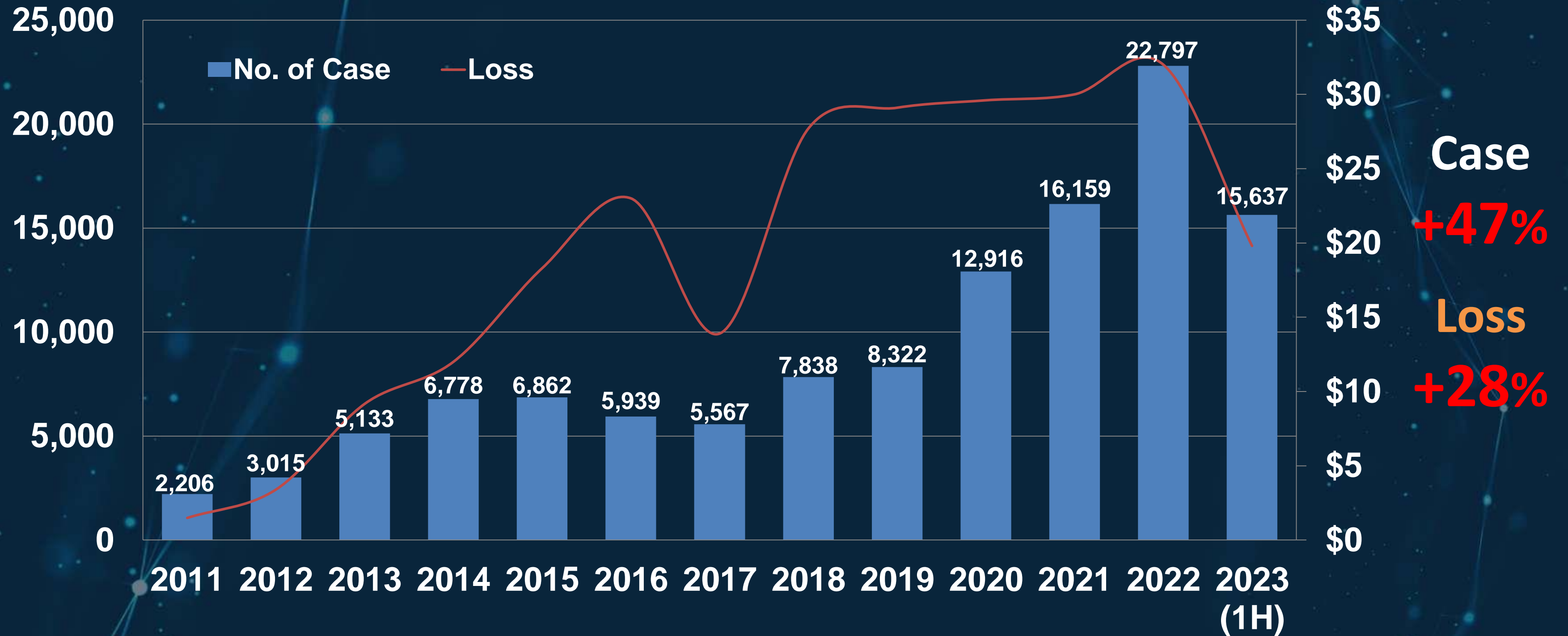
**Francis LEE**

**Senior Inspector, Cyber Security and Technology Crime Bureau  
Hong Kong Police Force**

# Agenda

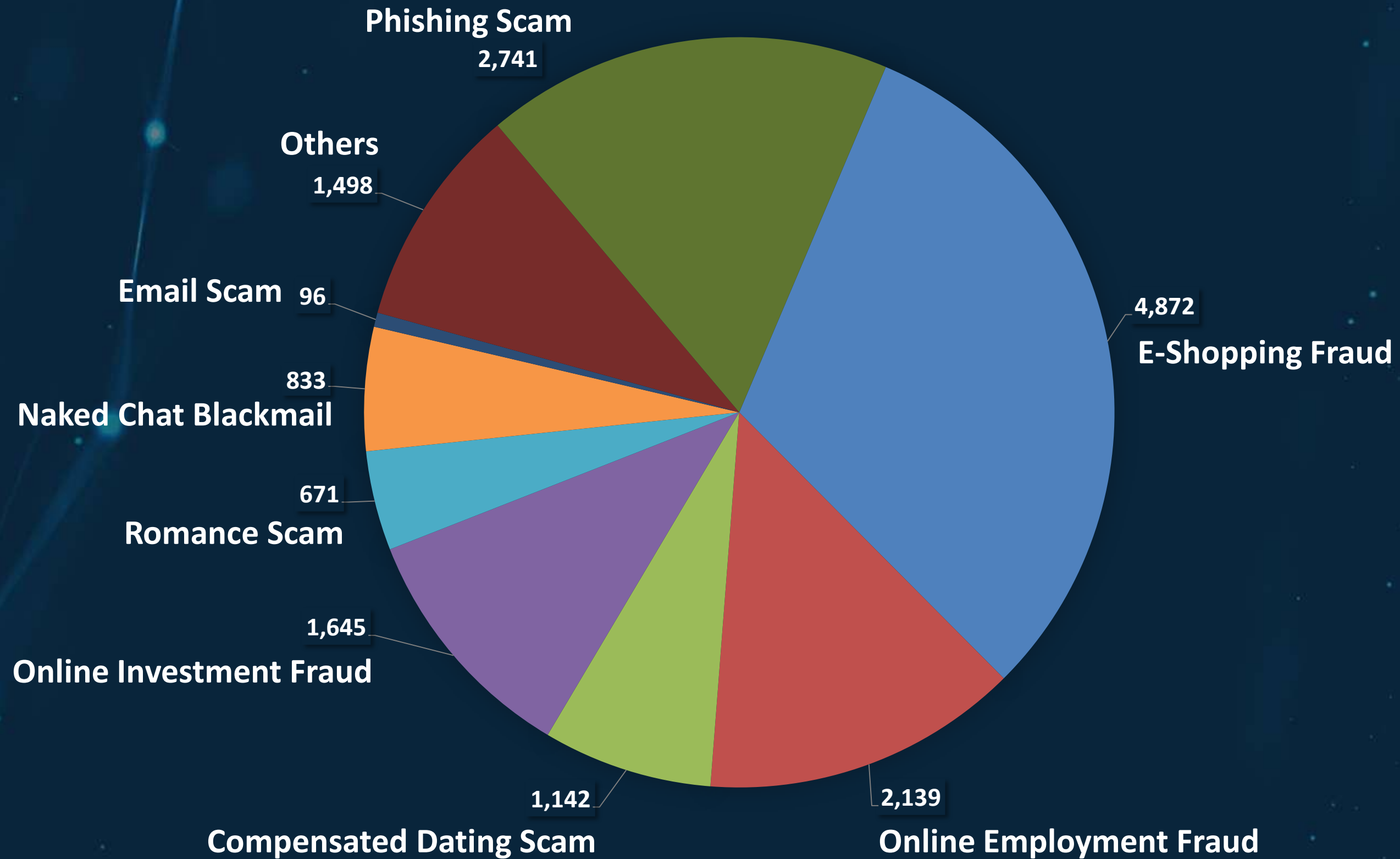
1. Technology Crime Trend in Hong Kong
2. Major Cyber Threats and Pitfalls
  - Phishing Attack, Email Scam, Ransomware, Insider Threat
3. Building Up Cyber Resiliency
4. CyberDefender, Scameter and V@nguard

# Technology Crime Trend in Hong Kong



# Technology Crime Trend in Hong Kong

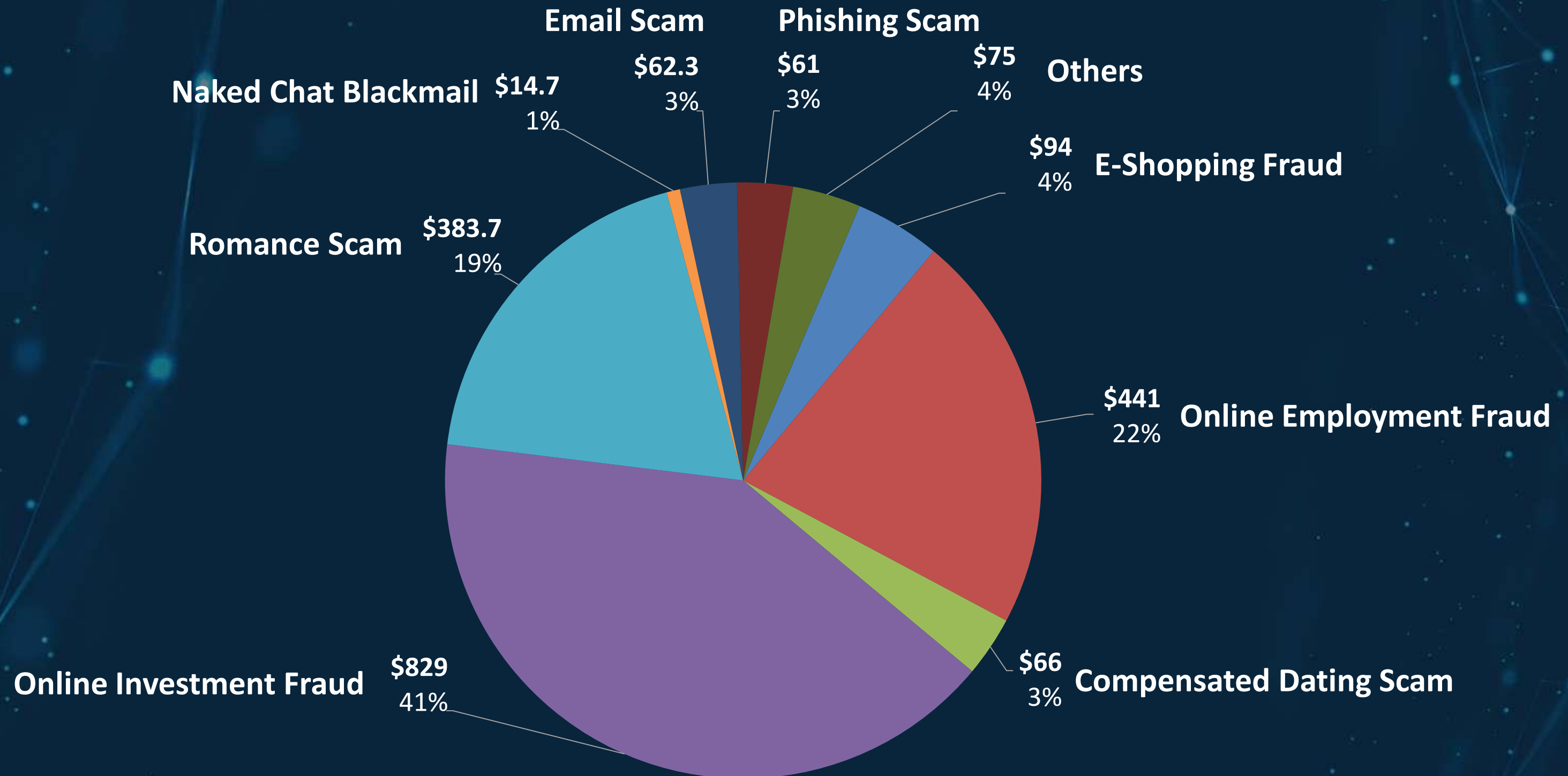
## In Terms of Case (2023 1<sup>st</sup> Half)





# Most Prevalent Technology Crime

In Terms of Loss (\$M) (2023 1<sup>st</sup> Half)



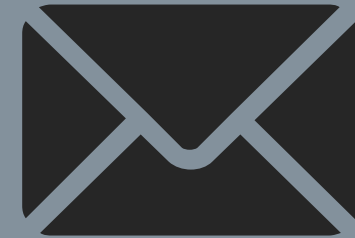


# **Major** Cyber Threats and Pitfalls

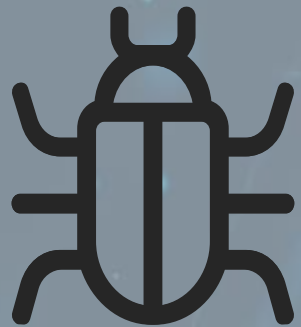
# Major Cyber Threats and Pitfalls



**Phishing Attack**



**Email Scam**



**Ransomware**



**Insider Threat**

# Phishing Email Top Subjects Globally

- most common methods to effectively perpetuate malicious attacks
- constantly refining their strategies to stay up-to-date with market trends
- distress, confusion, panic or even excitement in order to entice someone to click on a phishing link or malicious attachment





# Top Five Attack Vector Types



## Link

Phishing Hyperlink in the Email



## Spoofs Domain

Appears to Come From the User's Domain



## PDF Attachment

Email Contains a PDF Attachment



## HTML Attachment

Email Contains an HTML Attachment

## Branded



Phishing Test Link Has User's Organizational Logo and Name

# Ethical Phishing Email Campaign 2023

**Individual Staff**



**15.9%**

**Clicked into embedded phishing links**



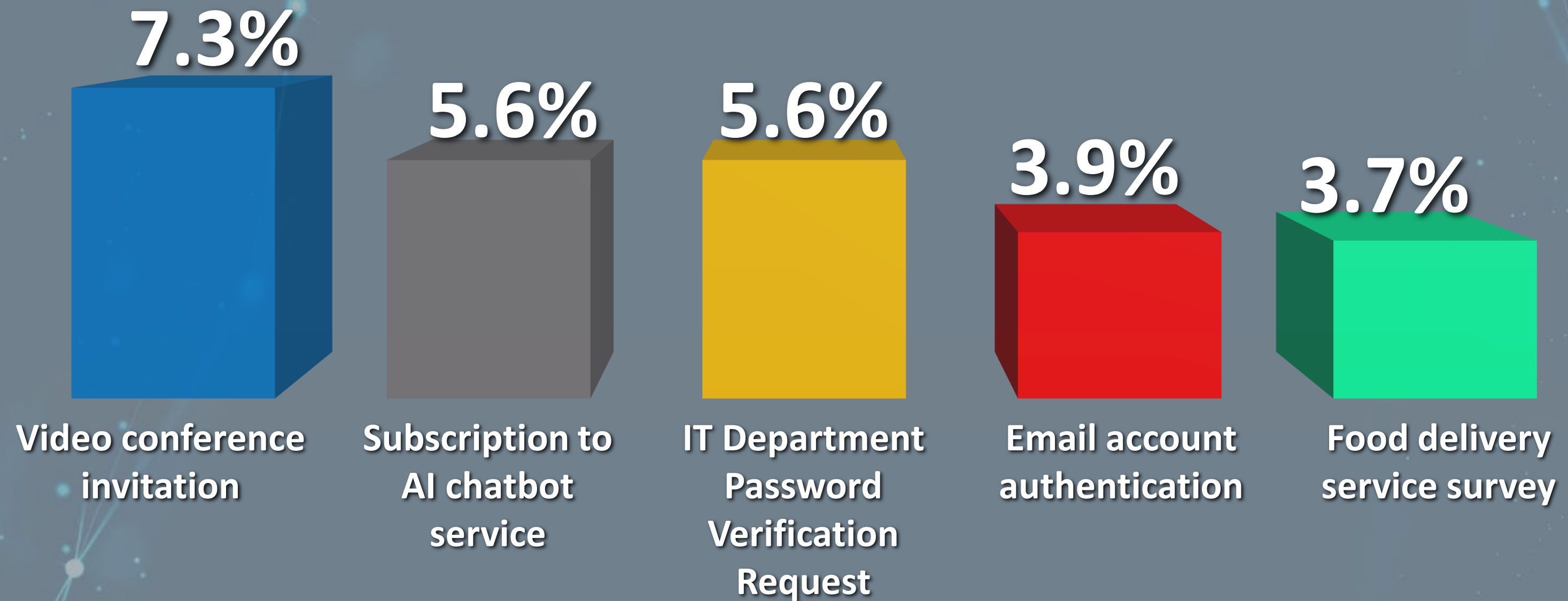
**Organization**

**61.6%**

**Had at least one employee clicked into embedded phishing links**

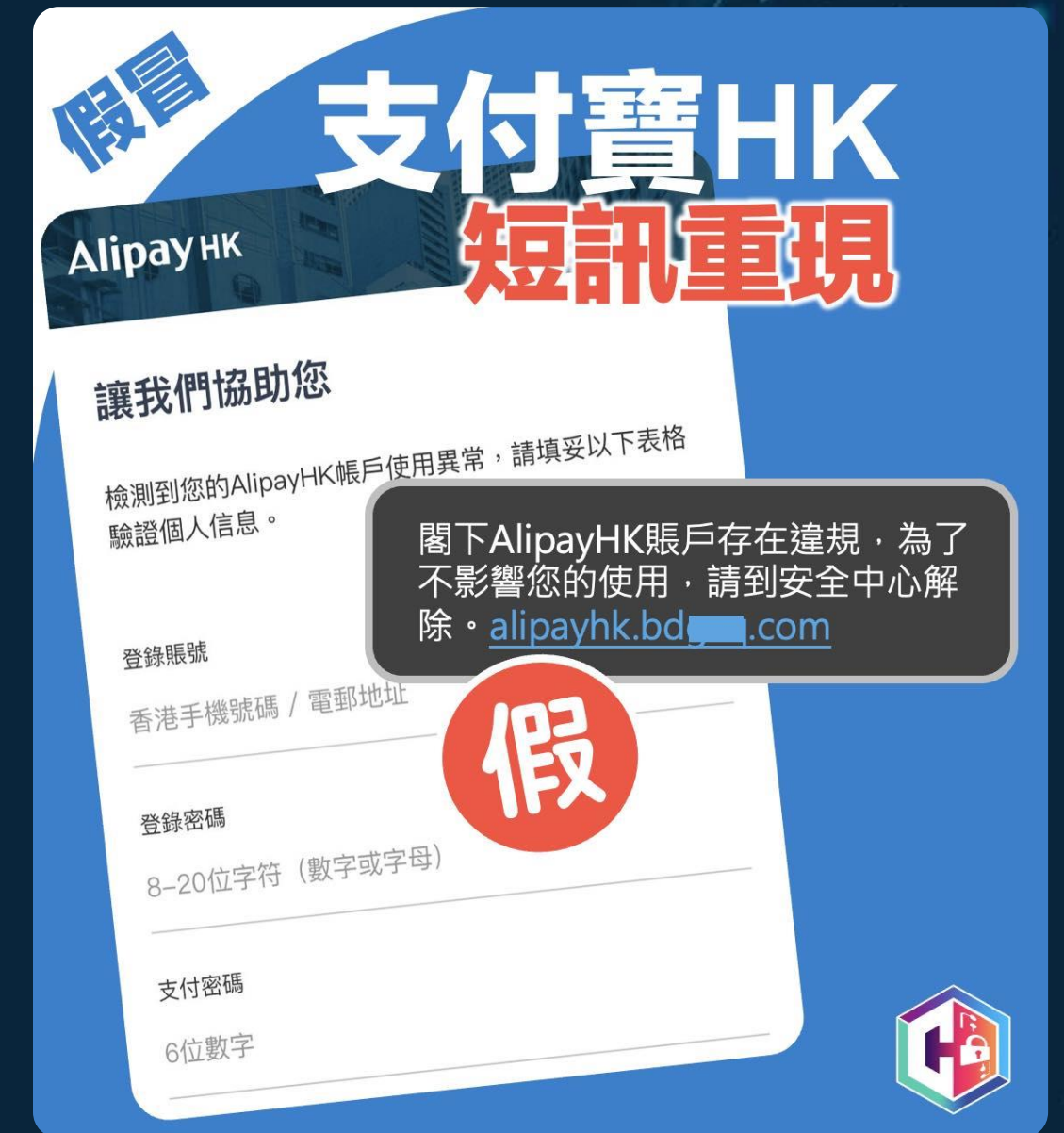
# Ethical Phishing Email Campaign 2023

## Click Rates of Pseudo-Phishing Emails





# SMS Phishing (Smishing)



- Personalized Sender ID
- Short-living phishing URLs
- High resemblance

2,300+ victims  
from Jan to May 2023!



# Social Media Phishing

器官捐贈在香港 Organ Donation at HK

**有獎遊戲**  
贏取 **HKS 100** 超市禮券

「器官捐贈3S」中的三個**S**分別代表什麼？

- A. Sign, Submit, Share
- B. Sign-up, Stand-up, Spread-out
- C. Sign-up, Speak-out, Spread-out

衛生署  
Department of Health

您好，我們來自 器官捐贈在香港 Organ Donation at HK

！您可以獲得隨機禮物。祝賀隨機選擇的參與者！請輸入您的姓名、電子郵件和地址以領取獎品。我會在您註冊後的1x24小時內聯繫您。

單擊下面的按鈕進行註冊

[在這裡註冊](#)

HKeToll 易通行

首頁 服務介紹 如何使用 如何付款 消息 聯絡我們

您未能成功支付電子通行費

賬單信息

收數單位	HKeToll易通行
付款說明	補交隧道費
截止日期	2023/8/17
發票號碼	APROC6973161091282
金額	30

[補交隧道費 30](#)

# Voice Phishing (Vishing) & QR Code Phishing (Quishing)



AI-based vishing



Theft of data / money  
Malware infection



# Email Scam

## aka Business Email Compromise

### Impersonating Supplier

from:

to:

subject:

Dear Paul,

Please be informed that our company's **bank account has just been changed to 888-789-002-00X**. Please make your settlement of November to the captioned account.

- Hack into the mailbox of either side
- Request to remit fund to unknown A/C

### Impersonating CEO

from:

to:

subject:

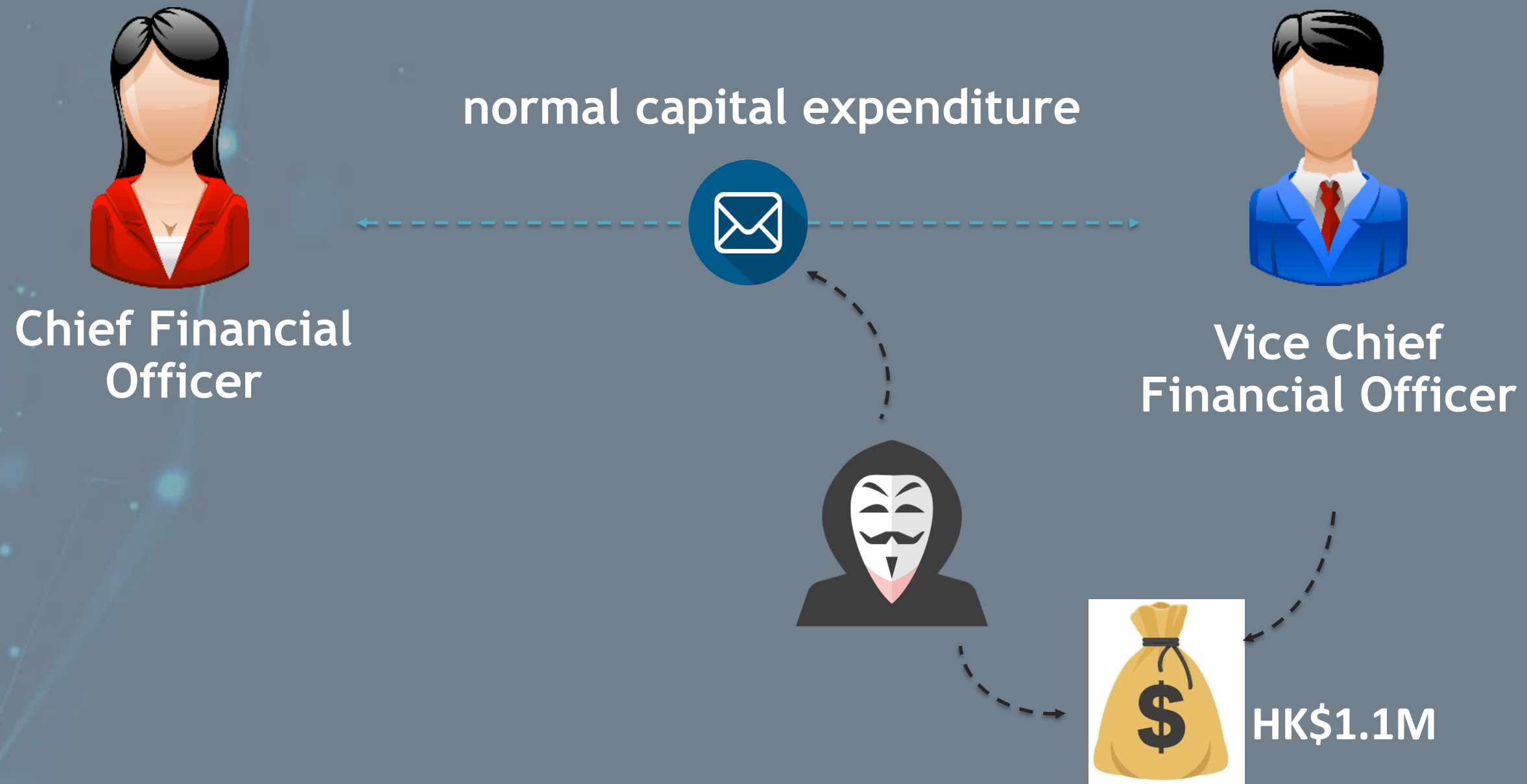
Dear Mary,

Please process a wire transfer payment in the amount of **\$250,000** and code to "admin expenses" by COB today. Wiring instructions below.....

- Hack into target company's mailbox
- Instruct to remit fund to unknown A/C

# Impersonating CFO

## Local Healthcare Technology Company





# Ransomware

## 勒索軟件攻擊

Your computer has been infected!

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - u4a88- Decryptor

You can do it right now. Follow the instructions below. But remember that you do not have much time

u4a88 - Decryptor price

You have 2 days 11:22

香港警務處  
網絡安全及科技罪案調查科

ANTRISCAM  
防騙中心  
18222

- Attack Vectors: RDP Brute force, Phishing or Vulnerability Exploitation
- Encrypt some or all files, demand for ransom for decryption
- Targeted Sectors:
  - Government, Banking & Finance, Supply Chain, Healthcare, Transport, IT Firms etc.

# Ransomware Extortion Tactics

## Double Extortion

- Infect the target computer
- Data in the computer cannot be read
- Theft of sensitive information
- Online disclosure of stolen documents

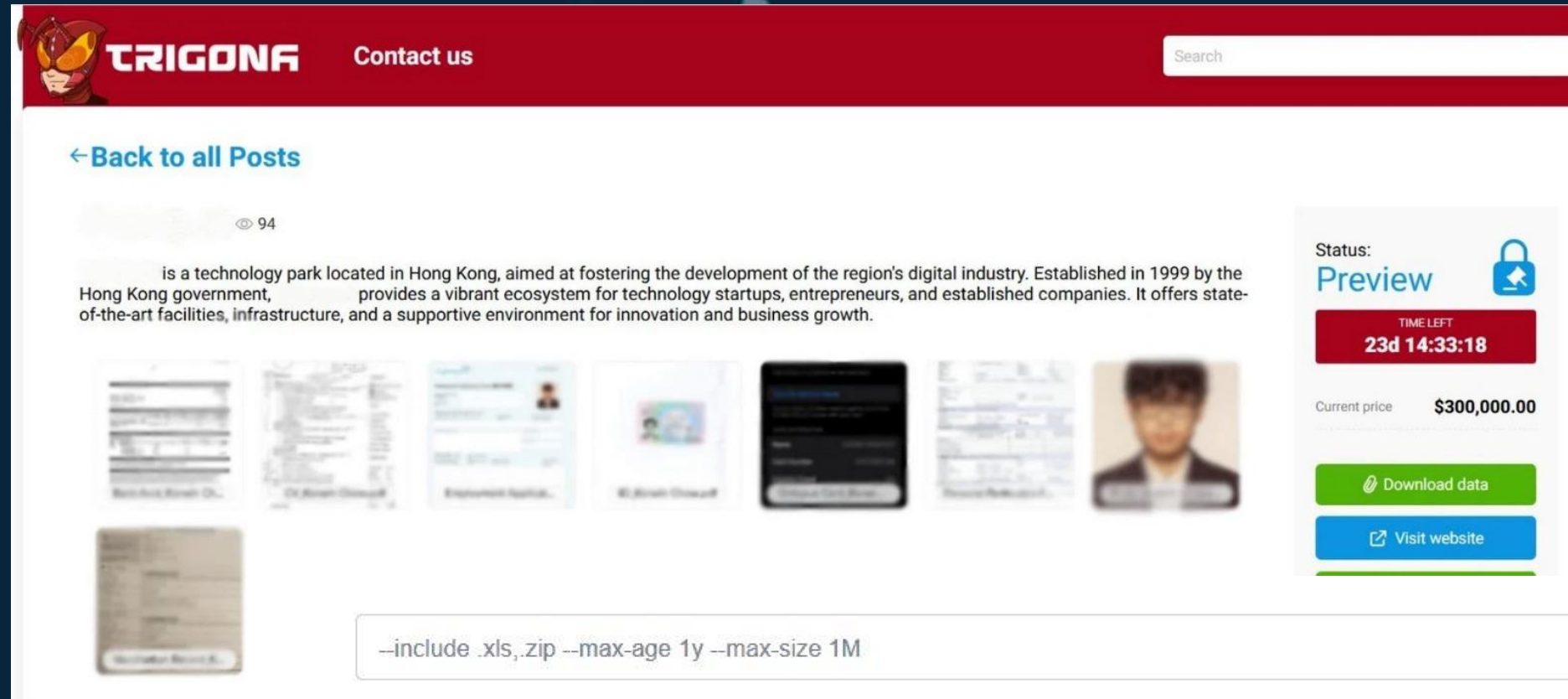
## Triple Extortion

- Theft of sensitive information from the target company & trade secrets from dealings with customers or business partners
- Threatening the target company and its customers or business partners

## Quadruple Extortion

- Distributed denial of service attack after triple ransom
- Paralyzes massive network traffic and steals sensitive data
- Force the target company to pay a ransom

# Leaked Sites on Dark Web



TRIGONA Contact us Search

[← Back to all Posts](#)

94

is a technology park located in Hong Kong, aimed at fostering the development of the region's digital industry. Established in 1999 by the Hong Kong government, provides a vibrant ecosystem for technology startups, entrepreneurs, and established companies. It offers state-of-the-art facilities, infrastructure, and a supportive environment for innovation and business growth.

Status: **Preview**

TIME LEFT  
**23d 14:33:18**

Current price **\$300,000.00**

[Download data](#)

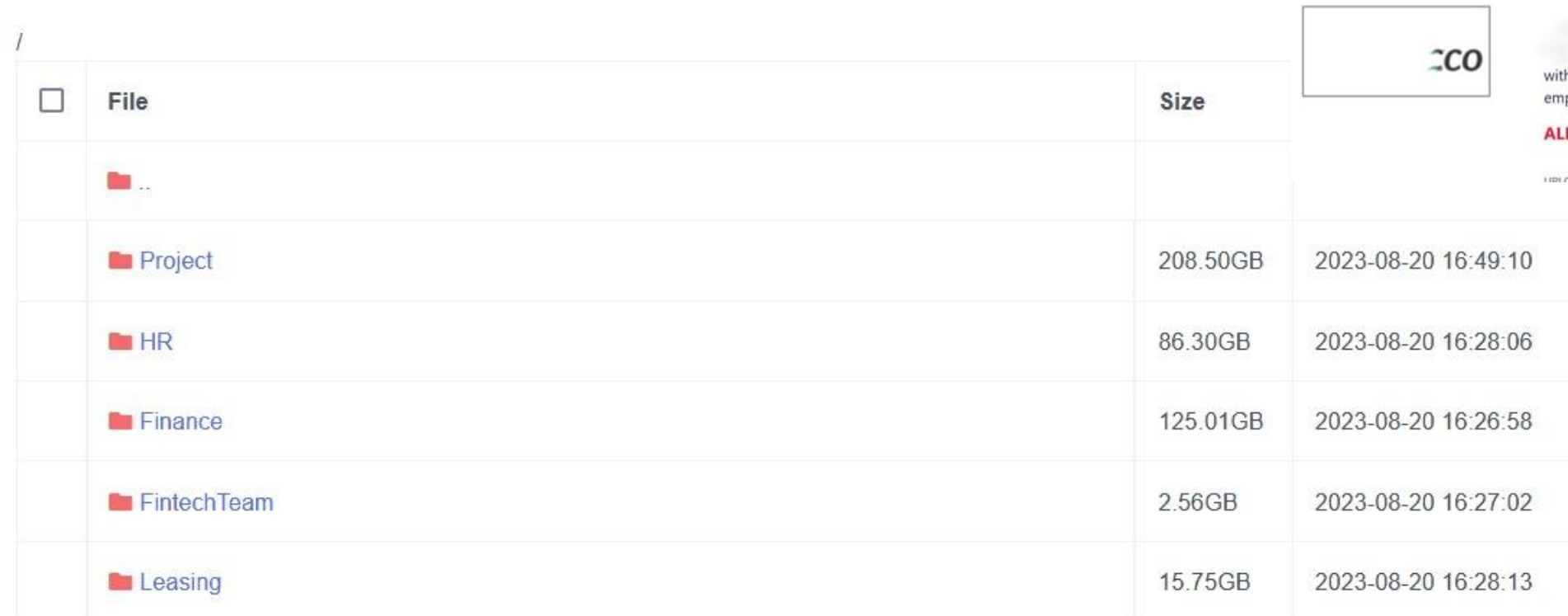
[Visit website](#)

--include .xls,.zip --max-age 1y --max-size 1M



**FILES  
ARE  
PUBLISHED**

Deadline: 15 Mar, 2023 09:20:56 UTC



<input type="checkbox"/>	File	Size	
	..		
	Project	208.50GB	2023-08-20 16:49:10
	HR	86.30GB	2023-08-20 16:28:06
	Finance	125.01GB	2023-08-20 16:26:58
	FintechTeam	2.56GB	2023-08-20 16:27:02
	Leasing	15.75GB	2023-08-20 16:28:13



**co.com**

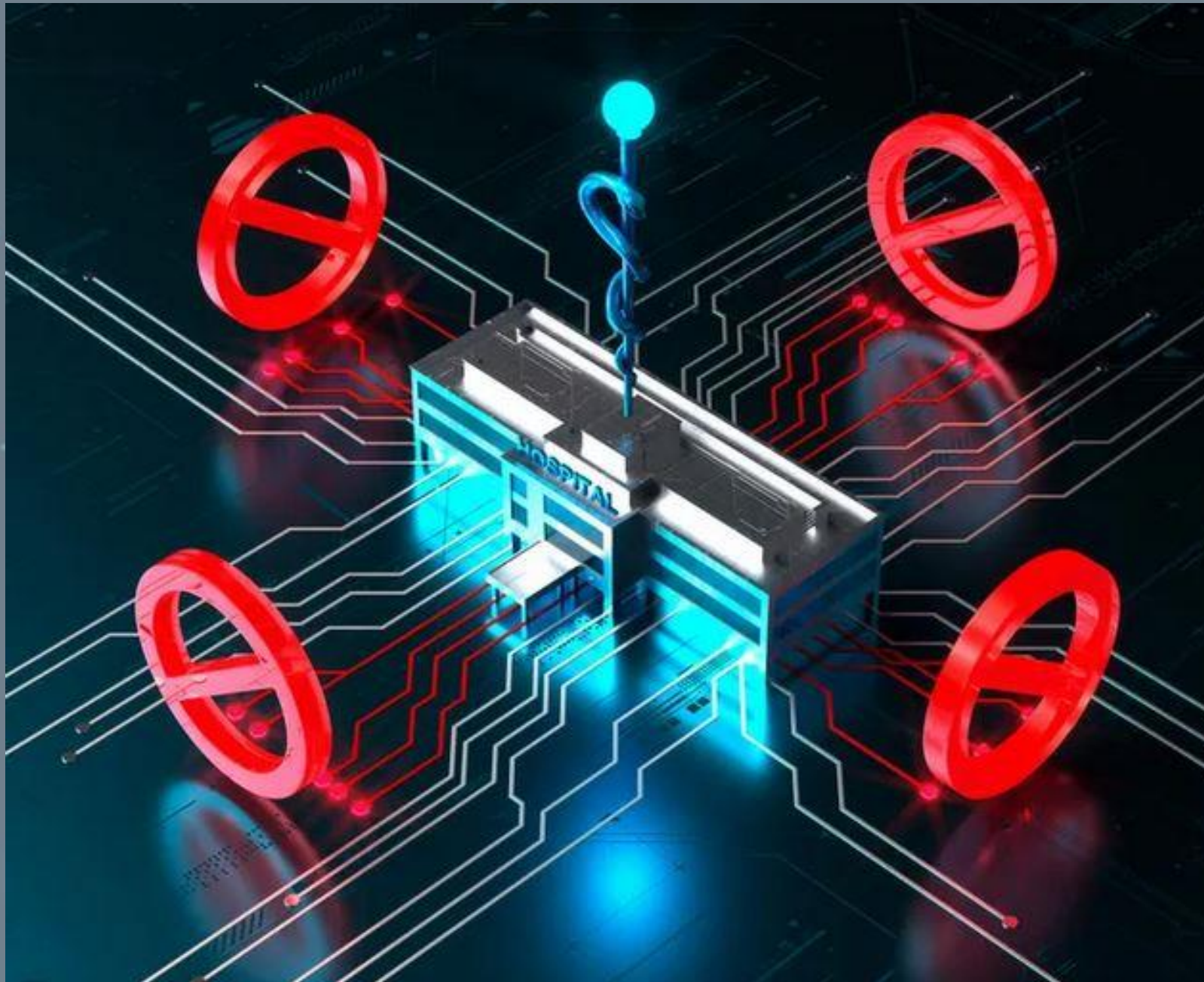
Company Limited is one of the world's leading independent aircraft engineering and maintenance groups with its head office located at Hong Kong International Airport. Established in 1950, the Group comprises 16 operating companies, employing around 15,000 staff in Hong Kong, Chinese Mainland, Europe and the United States.

**ALL AVAILABLE DATA PUBLISHED !**



# Ransomware

## Overseas: Israeli Hospital



- A Medical Center in Israel, was victimized in August 2023
- Disabled the hospital's computer systems in record keeping, resulting the hospital unable to accept new patients
- Threat actor took 1TB of data and later leaked personal information, internal email, finances, medical cards



# Ransomware






## Local: Healthcare Companies



- One medical centre and one dental clinic were victimized in 2023
- Servers containing customers' personal information and medical records were encrypted
- Threat actors demanded for ransom discussion

# Ransomware

## What should I do if get infected?

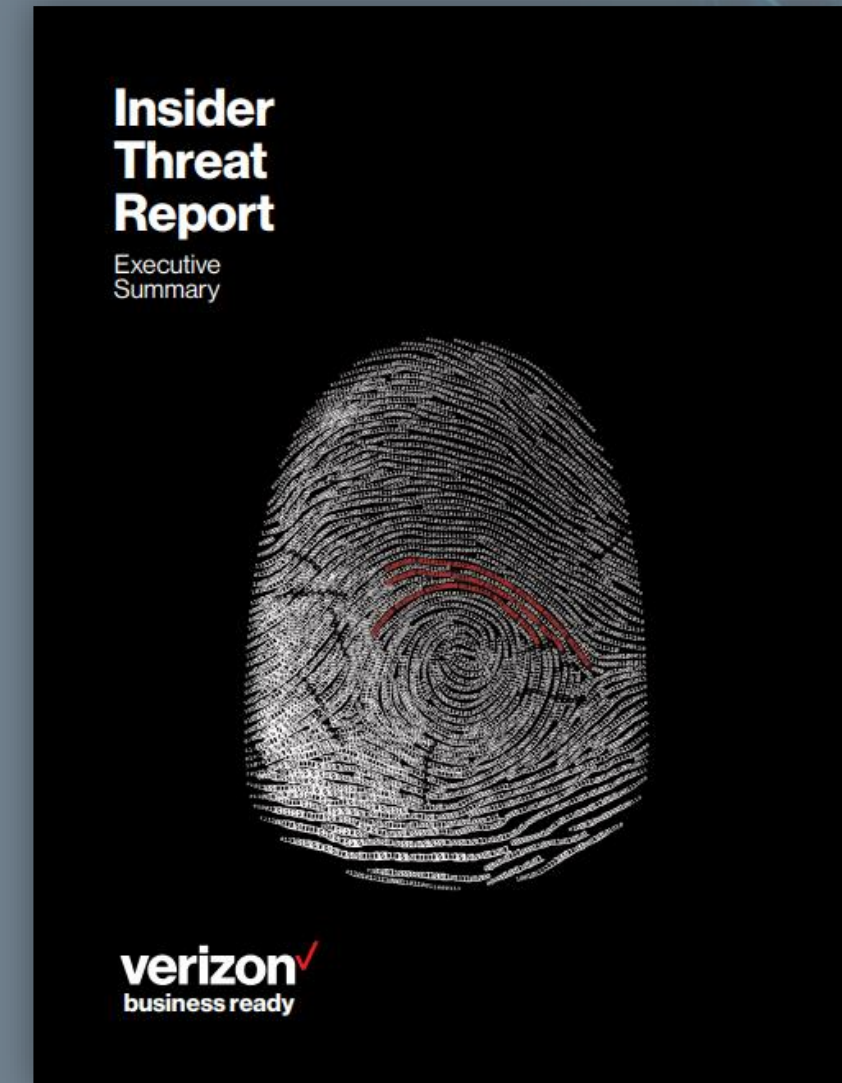
-  Disconnect the infected computer from the network
-  Turn off the power to the computer
-  Write down the programs and files that were run, emails opened and websites visited before the infection
-  Restore the computer from the backup
-  Do not pay the ransom

## Security Tips

- Backup regularly
- Implement latest patch
- Update anti-malware software
- Scan device regularly
-  Click open suspicious email / link
-  Visit suspicious website

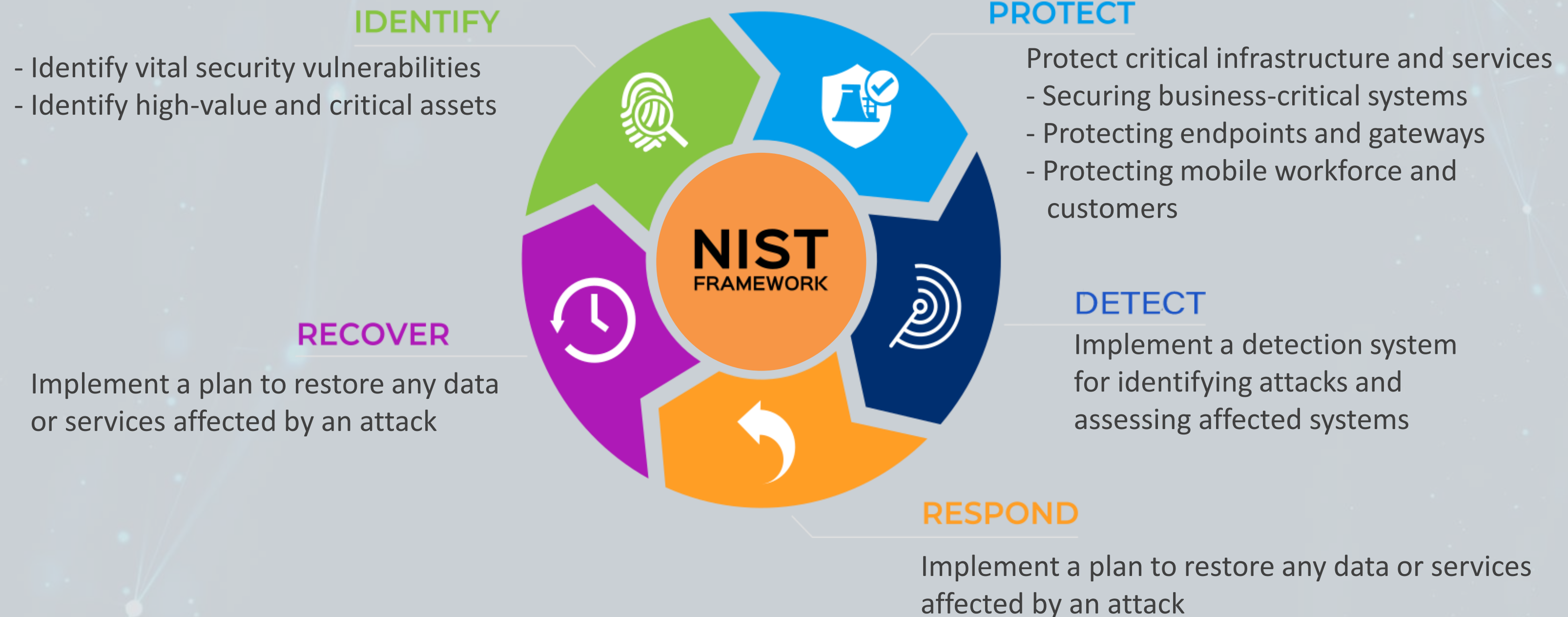
# Insider Threat Warning Signs

- **Erratic access**
  - ◆ Sudden increase in privileged account use
- **Excessive access**
  - ◆ High number of privileged accounts accessed in a burst of time
- **No need-to-know**
- **Off-peak access**
  - ◆ Accounts only accessed at unusual times of day





# Building Up Cyber Resiliency



# Building Up Cyber Resiliency

## Strategic Mindset

- Keep a disaster recovery plan ready
- Implement zero trust architecture
- Choose vendors wisely and monitor routinely
- Limit access to sensitive files and assets
- Educate staff, vendors, and partners

Source: NIST: Cybersecurity Framework Overview



**CYBER 守網者**  
**DEFENDER**

# One-Stop Cyber Information Platform



網絡常識

保護你的裝置

家長及老師

網絡罪案

資源及活動

簡 EN

疑似詐騙 / 網絡陷阱？

用「防騙視伏器」Check吓啦！

網址、電郵、電話、平台帳戶、收款賬戶等

如不確定資料類型，便無需選擇。

- ✓ 請選擇類型
- 平台帳戶名稱
- 平台帳戶號碼
- 電話號碼
- 電郵地址
- 網址
- 收款賬戶**
- IP 地址
- 雜湊值



可疑網站

網上情緣

網購陷阱

白撞証

陌生來電

# 全城守網

為免「失去了一切」立即下載  
全方位詐騙陷阱搜尋器 防騙視伏APP  
減低受騙風險！

**CyberDefender.hk**





# Scameter | Scameter+

## 防騙視伏器 | 防騙視伏App

疑似詐騙 / 網絡陷阱 ?

用「視伏器」檢測吓啦!

apkgk.com/com.mtel 選擇類型

你已搜尋: apkgk.com/com.mtel.androidbea

### 與釣魚詐騙舉報有關

- 避免與對方進行交易或匯款予對方。
- 切勿輸入個人資料、信用卡資料或登入憑證。
- 切勿打開任何連結或附件。



#### 免責聲明

1. 以上搜尋結果僅供參考,請自行判斷及查證。
2. 如你認為視伏器提供任何資料(包括你的個人資料)被不當標籤,請與我們或資料來源單位聯絡。
3. 你可以到警署或透過電子報案中心舉報罪案。
4. 當你使用視伏器,即代表你同意本網站的重要告示與私隱政策所載的條款。

#### 個人資料(私隱)告示

「視伏器」所提供的個人資料,謹供防止或偵測罪行之用途。如將資料用作其他用途,可能干犯香港法例第486章《個人資料(私隱)條例》的有關條文。

### 防騙視伏器



一站式詐騙陷阱搜尋器

立即搜尋

網址 電話號碼  
平台用戶名稱 社交帳號  
收款帳號  
電郵地址 IP地址

更多活動



守網者



最新消息



防騙視伏器



有用連結



設定



# Scameter | Scameter+

防騙視伏器 | 防騙視伏App

## ■ Facilitates KYC / CDD check

- ✓ Bank account
- ✓ Phone number
- ✓ Email address
- ✓ FPS proxy
- ✓ URL
- ✓ Crypto address





# V@nguard

## Suspicious Email Detection System

[⚠️ ⚠️ FROM NEW SENDER ⚠️ ⚠️] Payment Details [🔗](#)



寄件者 DEF Logistics <def1logistics@aol.com>

收件者 wills@vanguard-email.com <wills@vanguard-email.com>

日期 2023-10-02 12:01

[✉️ 概覽](#) [📧 標頭](#) [☰ 純文字](#)

**ALERT !!**

**The Email domain is first seen.  
Beware of any hyperlink, attachment and  
BANK ACCOUNT information unless you ensure  
the authenticity of the sender.**

**注意 !!**

這是首次接收到的電郵地址。除非您確保其真確性，  
否則請留意當中所附有的超連結，附件或銀行帳戶資料。  
如有疑問，請尋求技術人員的支援。





# Cyber Security Awareness Initiatives

主辦單位：   策略合作夥伴：

## 狩網運動2023

2023年6月至7月·香港

全港首個公私營合辦的  
漏洞檢測計劃



### 企業免費獲得

- 網頁漏洞檢測服務
- 網絡安全報告
- 一對一諮詢服務



### IT專才登記成為 賞金獵人

賺取額外收入



## 釣魚電郵演習2023

提高員工防範可疑電郵的意識



立即登記



費用全免 >>>

2023年5月13日截止報名





CyberDefender.hk



Scameter+

