

認識人工智能及網絡安全風險

- 善用數碼工具

網絡安全及科罪案調查科
高級督察陳穎

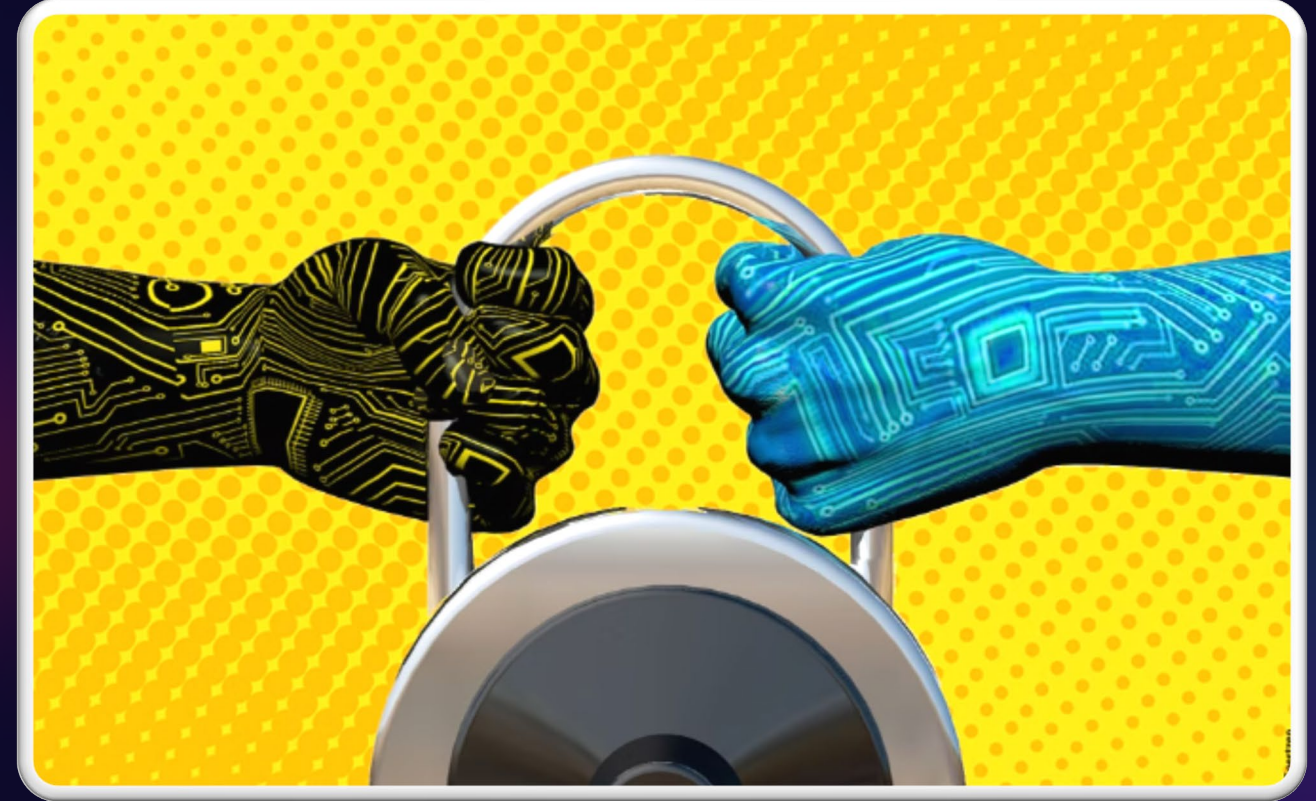


How Do You Perceive AI in Cybersecurity?



Varying Perspectives

Perceptions of AI in cybersecurity differ based on experiences and exposure.



Impact on Security

Understanding the influence of AI on cybersecurity is crucial for professionals.

The Emergence of AI Generated Content



AI Generated Text



ChatGPT



AI Generated Code



Github Copilot



AI Generated Image



Midjourney



AI Generated Video



CapCut



AI Generated Audio



Suno

AI in the Hands of Cybercriminals

1

Social Engineering

Automate and refine social engineering techniques through the analysis of vast public data

2

Impersonation

Create highly realistic deepfake videos or audios for impersonating individuals

3

Malicious Code

Assist in developing sophisticated malware, enabling faster and more effective attacks on vulnerable systems.



Use AI to Conduct Research



Please give me an overview of common IR frameworks



1. **NIST SP 800-61 Revision 2:** A guide for detecting, analyzing, and responding to incidents, emphasizing preparation, detection and analysis, containment, eradication, recovery, and post-incident activity.
2. **SANS Incident Handler's Handbook:** Outlines a six-step process for handling incidents: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.
3. **ISO/IEC 27035:** Provides international standards for incident management, including preparation, detection, reporting, response, mitigation, and learning from incidents.
4. **CERT Resilience Management Model (CERT-RMM):** A model integrating security, business continuity, and IT operations to manage and respond to incidents, focusing on operational resilience.
5. **Cyber Kill Chain:** Helps understand and prevent cybersecurity intrusions by analyzing the stages of a cyber attack, aiding in incident response and prevention.





Risks and Considerations

1

Overreliance

Excessive trust in unsupervised LLMs risks generating biased or incorrect outputs without ethical oversight

2

Privacy Concerns

AI might inadvertently reveal personal or proprietary information, risking data privacy and intellectual security

3

Regulatory Compliance

The fast pace of AI development can lead to challenges in adhering to evolving legal standards and ethical guidelines

Case Studies

Operation SMASHSCAM 2023

Case Overview

- **Target:** Fraud syndicate using AI deepfake technology
- **Method:** Online loan applications and SIM card registrations
- **Arrests:** 6 individuals (4 males, 2 females)
- **Age Range:** 31 to 50 years old

Key Achievement

Successfully apprehended the **mastermind** of the syndicate, demonstrating law enforcement's capability to combat AI-enabled fraud.



AI Deepfake Corporate Fraud 2024

1

Initial Contact

Finance officer received text claiming to be from multinational company CFO overseas

2

Video Conference

Attended meeting with deepfake CFO and other manipulated professionals

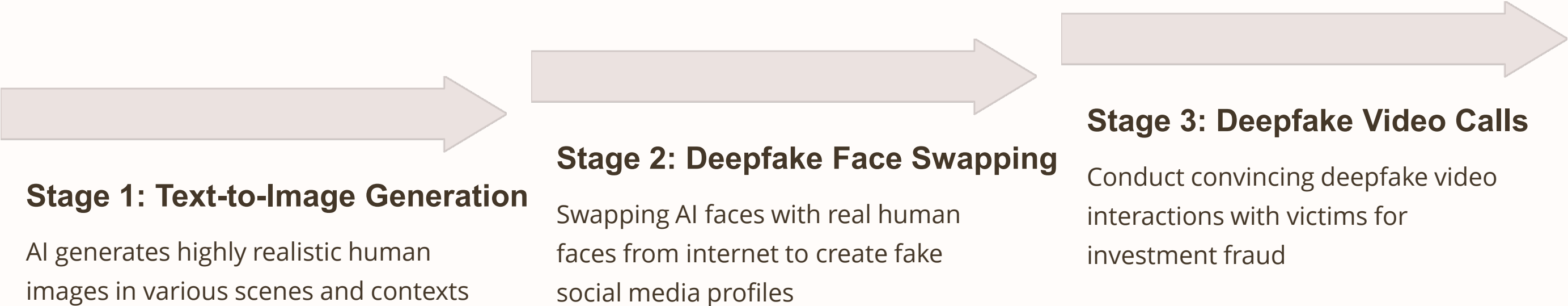
3

Fraudulent Transfer

Resulted in loss of around HK\$200 million



GenAI + Deepfake Investment Scam



Case Studies

1

SEO Poisoning

Fraudulent Websites Mimicking WhatsApp Web

2

WhatsApp Hijacking

Scan the QR code on the fake site, unknowingly giving the scammer full access of the WhatsApp account.

3

Fraudulent Transfer

Scammers use AI to clone a person's voice from short audio clips found during the WhatsApp conversation and requested for a fraudulent transfer of 145Million

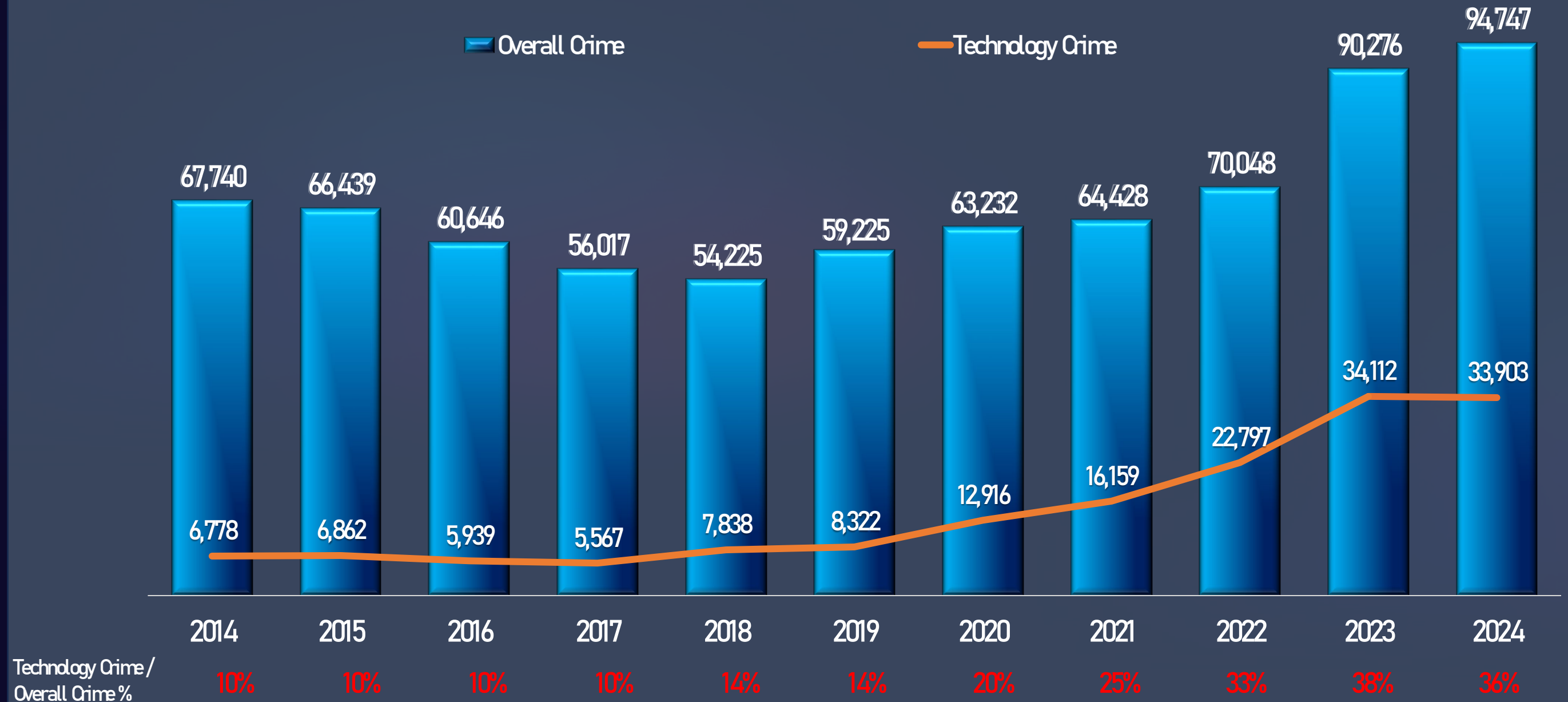


Hong Kong Legal Framework for Cybercrimes

No specific ordinance for cybercrimes including AI or deepfake. Existing laws apply based on criminal act nature.

Criminal Acts	Commonly Used Laws
Hacking	Access to Computer with Dishonest Intent (s.161, Crimes Ordinance)
Online Scams & Fraud	Obtaining Property by Deception (s.17, Theft Ordinance)Money Laundering (s.25, OSCO)
Deepfake Intimate Images	Publication of Intimate Images w/o Consent (s.159AAE, Crimes Ordinance)
Malware & Ransomware	Criminal Damage (s.60, Crimes Ordinance)Blackmail (s.23, Theft Ordinance)

Technology Crime Trend in Hong Kong



Top Three in Jan-Jun 2025

e-Shopping Fraud

No. of Cases: 6,819

Losses (HKD): \$192,200,000

Employment Fraud

No. of Cases: 2,660

Losses (HKD): \$597,400,000

Investment Fraud

No. of Cases: 2,273

Losses (HKD): \$1,480,700,000

While e-Shopping Fraud recorded the highest number of cases, Investment Fraud led to significantly larger financial losses, indicating its severe impact despite fewer reported incidents. Employment Fraud also resulted in substantial losses.


Online Shopping Fraud



Online Shopping Fraud

Fake Sellers

- Push for prepayment, avoid in-person meeting
- Disappear after getting money

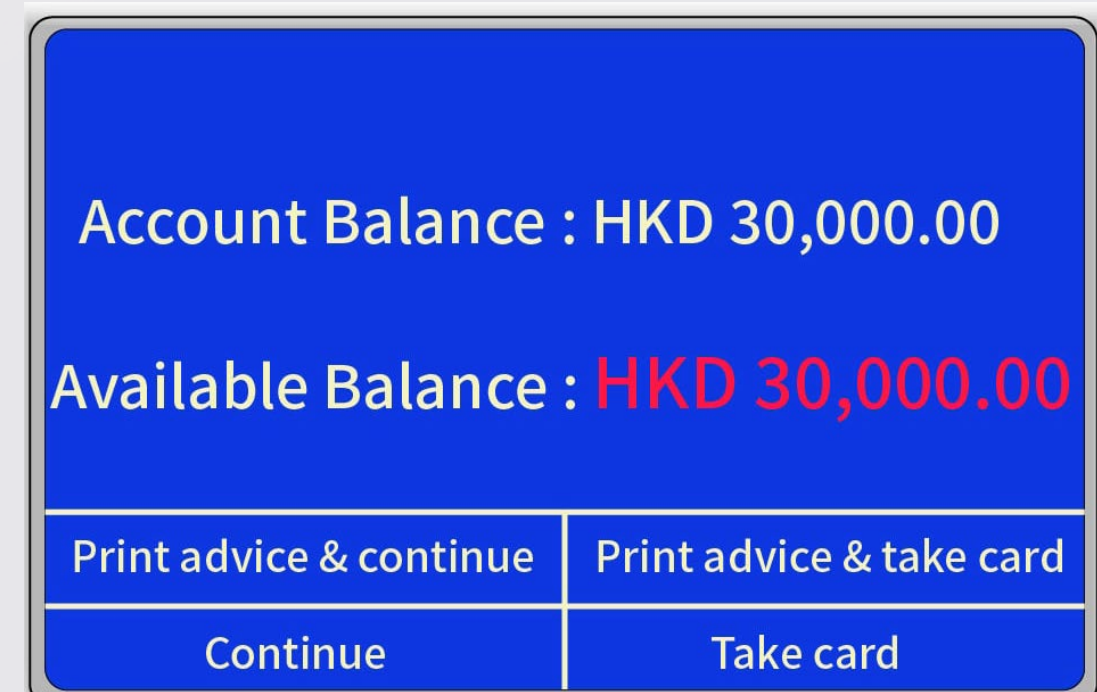
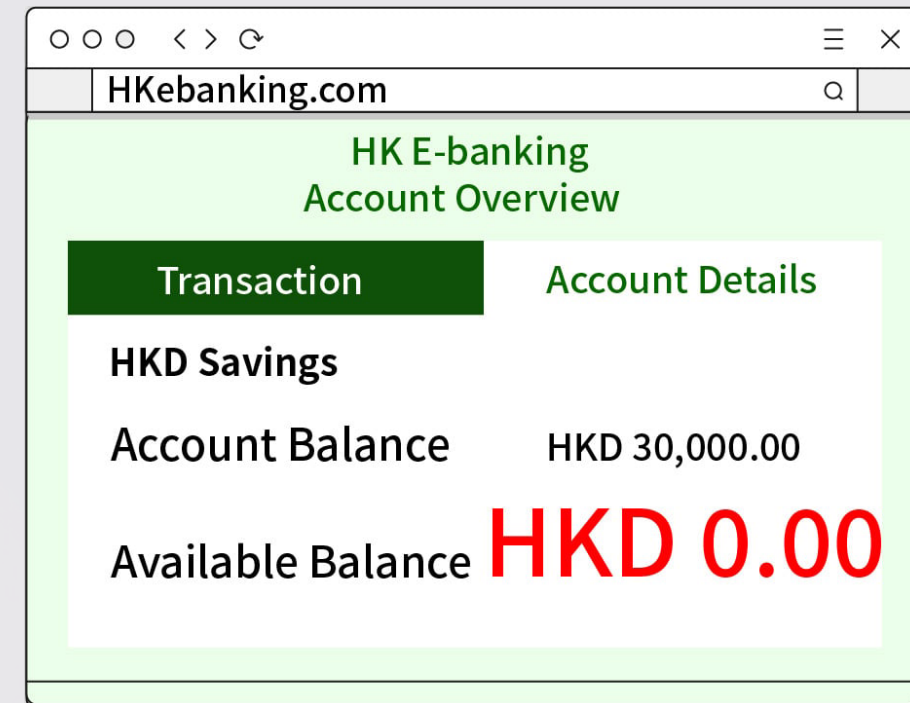
 Tip: Don't pay before seeing the goods. Meet and pay in person.



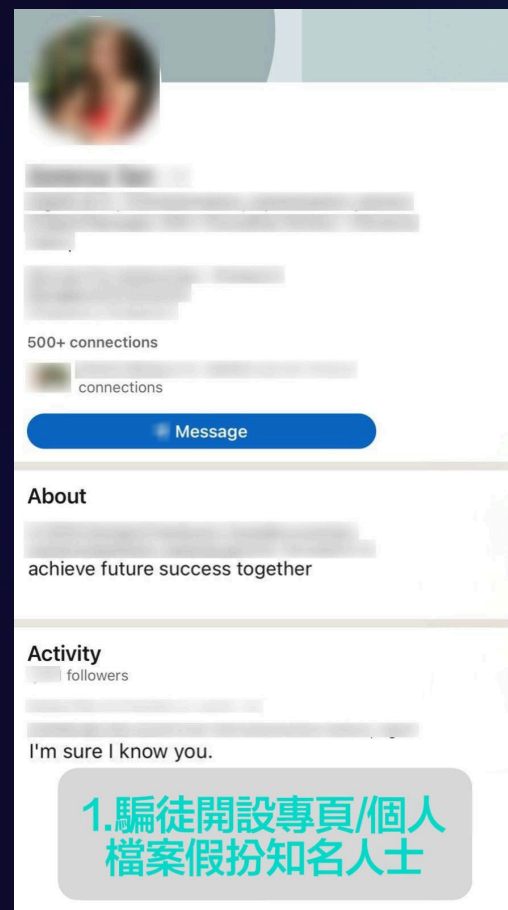
Online Shopping Fraud

Fake Buyers

- Use bounced cheques or fake deposit slips
 - Vanish after receiving product
- 💡 Tip: “Account Balance” ≠ cleared funds. Only ship after available balance confirms payment.



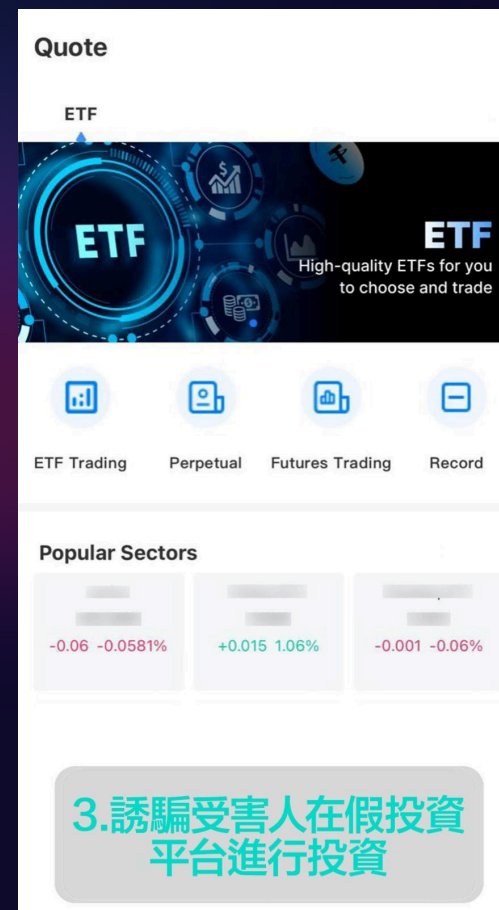
Investment Scam via LinkedIn



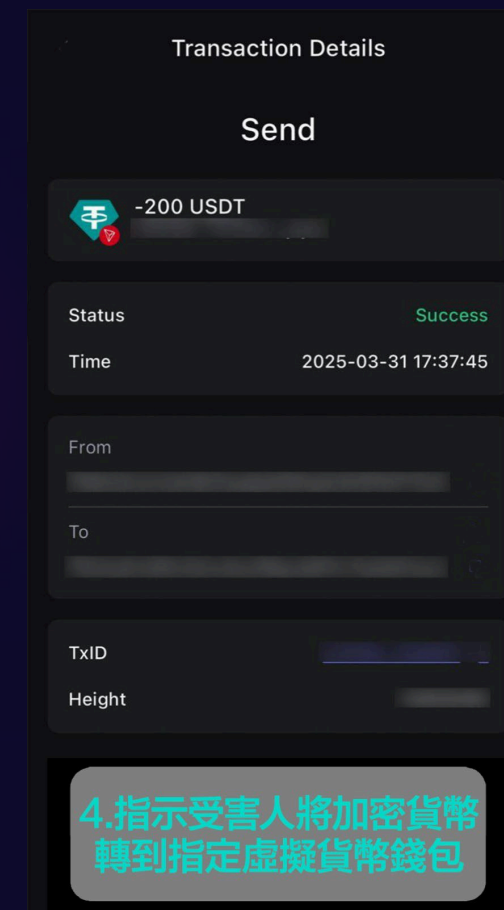
Fake profile posing as expert or executive



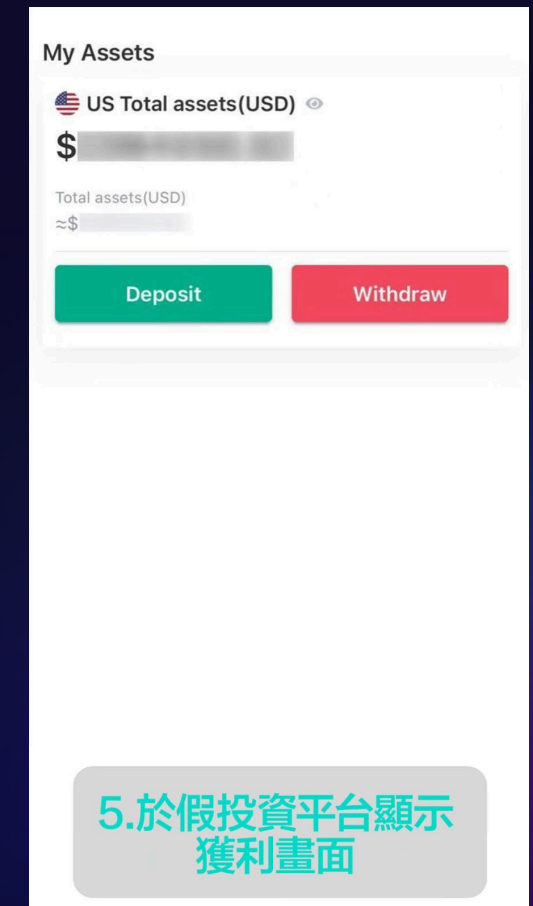
Phishing messages to lure targets



Persuades victim to join fake investment platform



Victim transfers crypto to scammer's wallet



Fake profits shown to entice further investment

Employment Fraud

1

唔好意思 打攞喇！我系 Cherry 目前我哋有幾個職位空缺，可以同你分享資料睇吓？ 15:12

好丫 15:12 ✓✓

呢排我哋幫緊幾家公司招人，免費提供各類職位空缺及發展機會 福利同待遇 良好。

(長期 / 臨時工 / 周末散工) 早晚間都有，合作公司包括大小型企業。

地點：香港各地區 ✓

條件：要求系成年者 / 銀行戶口出糧 / 履歷表 (CV) 列出工作經歷 / 知識 / 技能

歡迎任何人 / 新手 / 退休人士 ✓

我安排雇主 send 詳細工種資料, 薪資待遇畀你參考，可以了解睇吓有咩適合你嘅工作。Ok? 15:13

Cold Messages About
Job Vacancies

2

公司名：InitiativeIQ

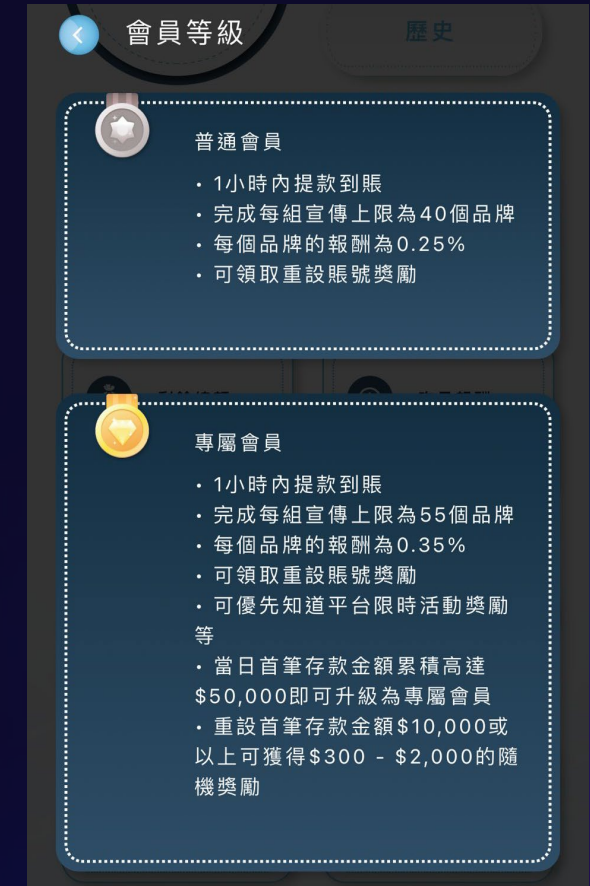
呢間公司主要做嘅就係幫助啲同公司合作嘅品牌方做宣傳，主要係利用線上宣傳 (SMM技術) 幫助提高品牌嘅知名度同時都可以刺激到品牌嘅價值 17:46

好 工作內容? 17:46 ✓✓

人工方面計日，一日400蚊-1300蚊，工作時間同地點自己定，每日喺平台運營時間完成就得，完成工作後公司會通過FPS或者網銀出糧 17:46

Fake profile posing as
expert or executive

3



Fake websites charge 'rewards'
after task completion: the
higher the deposit, the higher
the return



Scameter | Scameter+

防騙視伏器 | 防騙視伏App



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。

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。

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

Suspicious Account Alert



HONG KONG MONETARY AUTHORITY
香港金融管理局



HONG KONG INTERBANK
CLEARING LIMITED
香港銀行同業結算有限公司

THE
HONG KONG
ASSOCIATION
OF
BANKS

香港銀行公會



留意可疑帳號警示



轉數時
要醒啲

警示現已覆蓋
轉數快及
其他網上銀行轉賬

G.E.M.
鄧紫棋



CyberDefender.hk

立即了解



Cyber Defenders' Alliance (Government Department and Statutory Bodies)



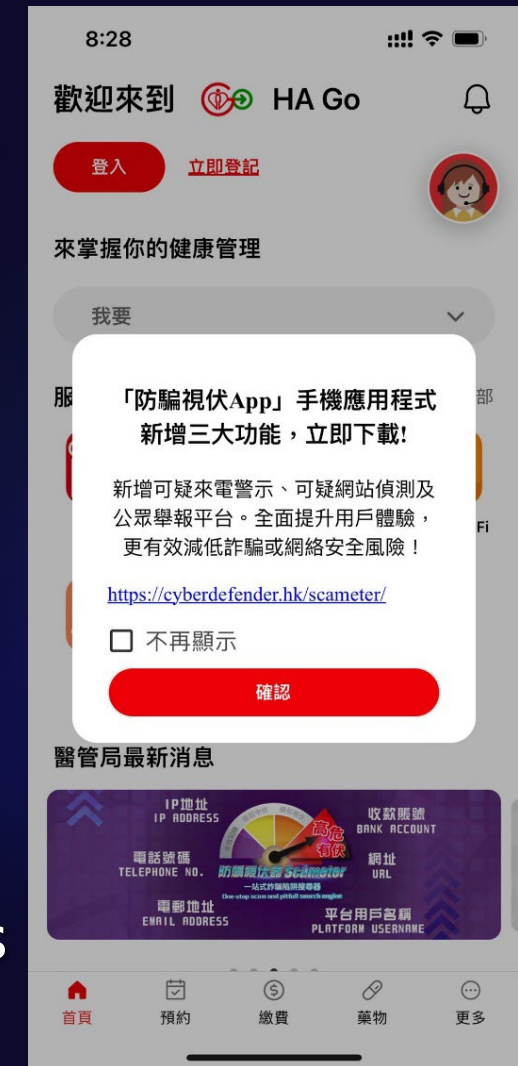
Tram Body Photography Contest



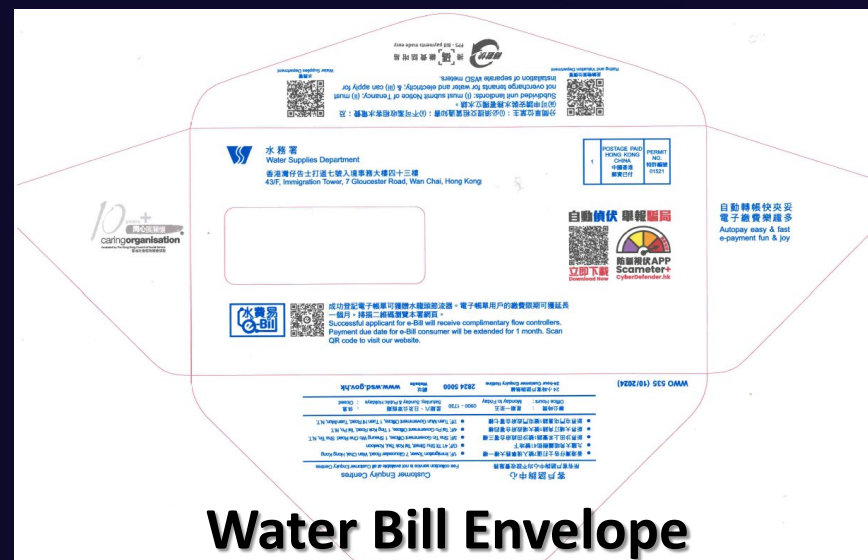
Flash Mobs Activities



Social Media Posts



Pop-up notification



Water Bill Envelope



E-banner

Cyber Defenders' Alliance (Private Corporations)



Free Advertisement Area

恒生銀行 Hang Seng Bank
21小時 · 21小時 · 21小時

【升級版防騙視伏 APP】

騙子十面埋伏，2023年每 13 分鐘就有一宗騙案，每日騙案平均損失高達 2,500 萬。
為減低市民受騙風險，香港警務處網絡安全及科技罪案調查科升級版「防騙視伏APP」新增三大功能，包括：…… 查看更多

每13分鐘·一宗騙案
升級版 每日損失·\$2,500萬
防騙視伏App

立即下載

防中伏 疑似有伏 高危險 自動偵伏 舉報騙局

一站式詐騙陷阱搜尋器
網址、電郵、電話、平台帳戶、收款賬戶等
疑似遇到詐騙？用「防騙視伏APP」check吓嘅！

可疑來電警示 開啟
可疑網站偵測 開啟
公眾舉報平台 已登記

防騙熱線 18222
CyberDefender.hk

Social Media Posts

下載「防騙視伏器」

一站式詐騙陷阱搜尋器「防騙視伏器」，協助公眾辨識詐騙及網絡陷阱。公眾遇到可疑來電、網購賣家、交友邀請、招聘廣告、投資網站，均可在「防騙視伏器」輸入相關平台帳戶名稱或號碼、收款賬戶、電話號碼、電郵地址、網址等，以評估詐騙及網絡安全風險。

本搜尋器的資料或評級來自不同來源，包括市民向警方報案的資料、機構提供的資料(如香港金融管理局、香港電腦保安事故協調中心等)、可疑電話號碼舉報資料庫(HKJunkCall)，以及資訊安全公司的資料庫及實時分析的評分。

最新升級版「防騙視伏App」已經推出，除原有功能外，是次升級亦新增了以下3個功能：

- 可疑來電警示**
此功能自動將你收到的來電與最新的詐騙資料庫作比對，如發現潛在詐騙或網絡安全風險，會即時發出警告提醒你，但你可選擇接聽與否。
- 可疑網站偵測**
此功能自動將你瀏覽的網站與最新的詐騙資料庫作比對，如發現潛在詐騙或網絡安全風險，會即時發出通知，建議你不要瀏覽該網站。
- 公眾舉報平台**
當你發現疑似詐騙的網站或電話號碼，可以透過此功能即時舉報。所舉報的資料經分析後可能會被納入詐騙資料庫，供所有用戶使用，以減低其他用戶受騙的風險。

Alerts Through Mobile App

We Think Digital Hong Kong

Posts About Photos More

We Think Digital Hong Kong is with CyberDefender 守網者.

1m ·

⚠️ 重要嘅事情要定時重提 - 記得定期登出「已連結裝置」，同絕對唔好輸入不明來歷的「代碼」呀！

See translation

CyberDefender 守網者

1h ·

【騙徒扮WhatsApp客服「八字代碼」一輸入即被盜帳號】... See more

See translation

騙徒扮WhatsApp客服
安全中心提醒
這是WhatsApp官方安全提醒，長時未進行安全認證，請選擇使用iPhone驗證或Android驗證。
你好，請複製以上8位安全代碼，根據圖片所示步驟打開WhatsApp，按輸入代碼後，系統即可驗證。本次安全碼時效為3分鐘，超時重新獲取。

定期登出「已連結裝置」
預防WhatsApp帳戶被竊劫
1 開啟WhatsApp設定
2 登出所有不明裝置
新增群組
新增群組訊息名單
已連結裝置
已標上星號
全部標示為已讀
設定
其他提防小貼士
啟用雙重認證
不要重覆搜尋結果
避免連接公共WiFi
切勿隨意透露密碼
使用防騙視伏器

八字代碼
一輸入即被盜帳號

Share of Cyber Defender's Facebook post

「守網聯盟」遊戲卡



遊戲卡

- ◆目的: 透過遊戲加深市民對科技罪案的認識
- ◆對象: 高小及中學生
- ◆參與人數: 最少2個，最多6個
- ◆遊戲時間: 20 至 30 分鐘
- ◆體驗版: 全套180張
- ◆隨機包裝版: 一包10張
- ◆五大等級:
N (Normal，普通), R (Rare，稀有), SR (Super Rare，超稀有), SSR (Specially Super Rare，特別超級稀有), UR (Ultra Rare，極稀有)
- ◆只有隨機包裝版包含SSR 及UR 卡
- ◆各「守網聯盟」盟友吉祥物會用於設計SSR 及UR 卡

將防騙資訊融入4款遊戲卡



攻擊卡

● 不同類型的科技罪案



陷阱卡

● 詐騙手法



防禦卡

● 日常加強抵禦網絡詐騙的方法



技能卡

● 遇到詐騙時應對方法

攻擊卡

陷阱卡



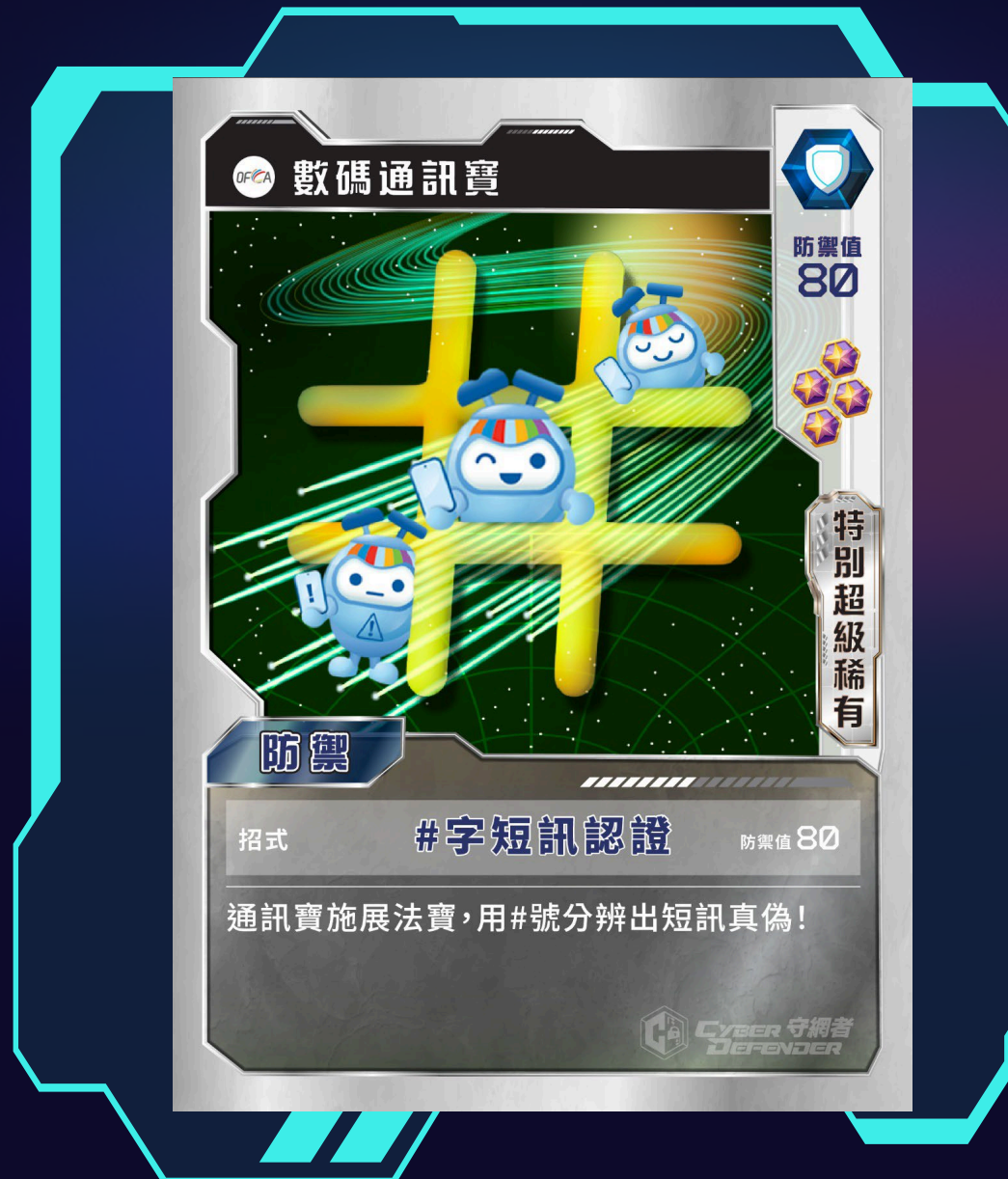
防禦卡

技能卡



Specially Super Rare

特別超級稀有



Ultra Rare 極稀有卡



Ultra Rare 極稀有卡



CyberDefender.hk



Scameter+

