HKCERT

Good habits to enhance cyber hygiene for the SMEs

中小企 - 養成良好習慣，加強網絡衛生

HKCERT

Agenda 程序

1. Security Incident Data 網絡保安事故數據
2. Past Security Incidents 過去網絡保安事故及分析
3. Advice 建議

HKCERT

- **Hong Kong Computer Security Incident Coordination Centre**
  香港電腦保安事故協調中心

- **Affiliated to the Hong Kong Productivity Council and funded by the Hong Kong SAR Government**
  由香港生產力促進局管理，並由香港特別行政區政府資助

- **To provide Hong Kong enterprises and Internet users with information and defense guidelines on information security incidents, incident response, and to raise cybersecurity awareness**
  為香港企業及互聯網用戶提供資訊保安事故的消息和防禦指引、事故回應及支援服務，及提高網絡保安意識

- **Responsible for liaising with Hong Kong organizations, collecting, distributing information and coordinating computer security incident response**
  負責聯絡香港組織，收集、發放訊息及協調電腦保安事故的應變

A point of contact for cross-border cyber security incidents
作為香港跨境網絡保安事件的聯絡點

International
海外

Global Researchers

FIRST

APNIC

DOT ASIA ORGANISATION

APCERT

Exchange Incidents and Information
交換網絡保安資訊

Coordinate incidents and publish alerts
協調保安事故及保安預警

HKCERT

GovCERT.HK

Local
本地

Internet Infrastructure
互聯網公司

Regulators
監管機構

Enterprises
企業

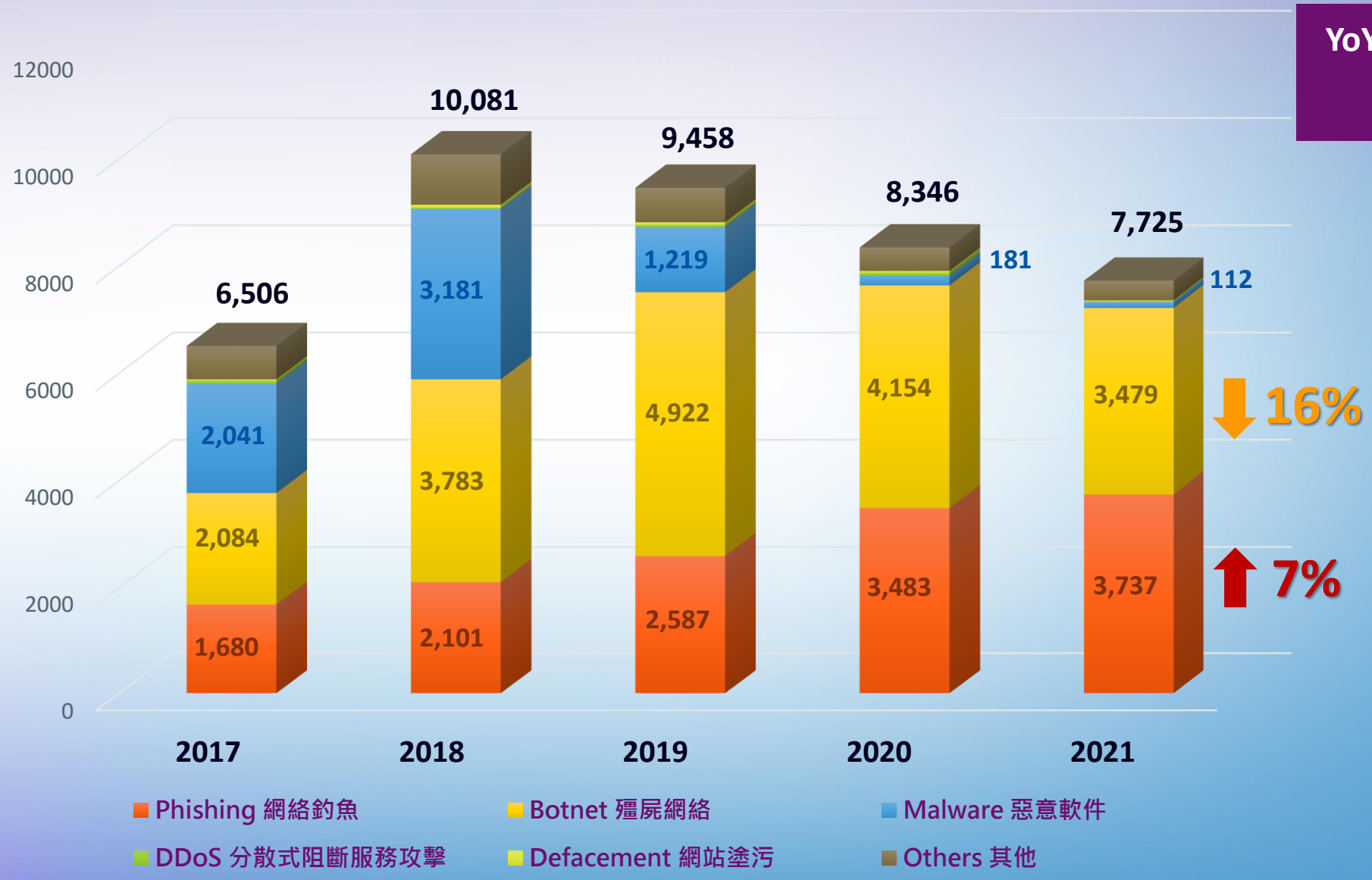
Universities & Researchers
院校及研究員

IT & Security Vendors
服務供應商

HKCERT

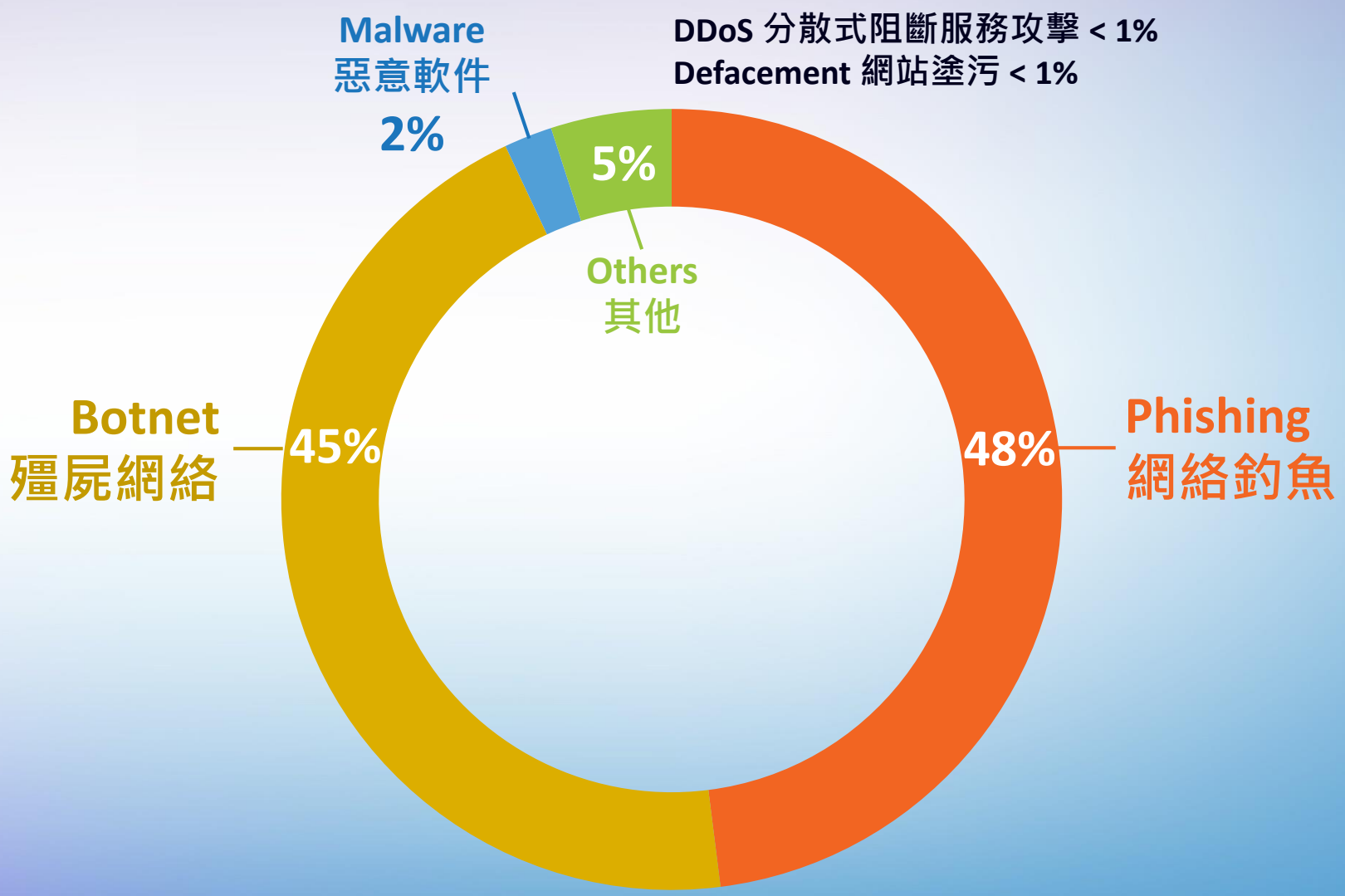
1 Security Incident Data 網絡安全事故數據

Trend of Security Incidents
保安事故走勢



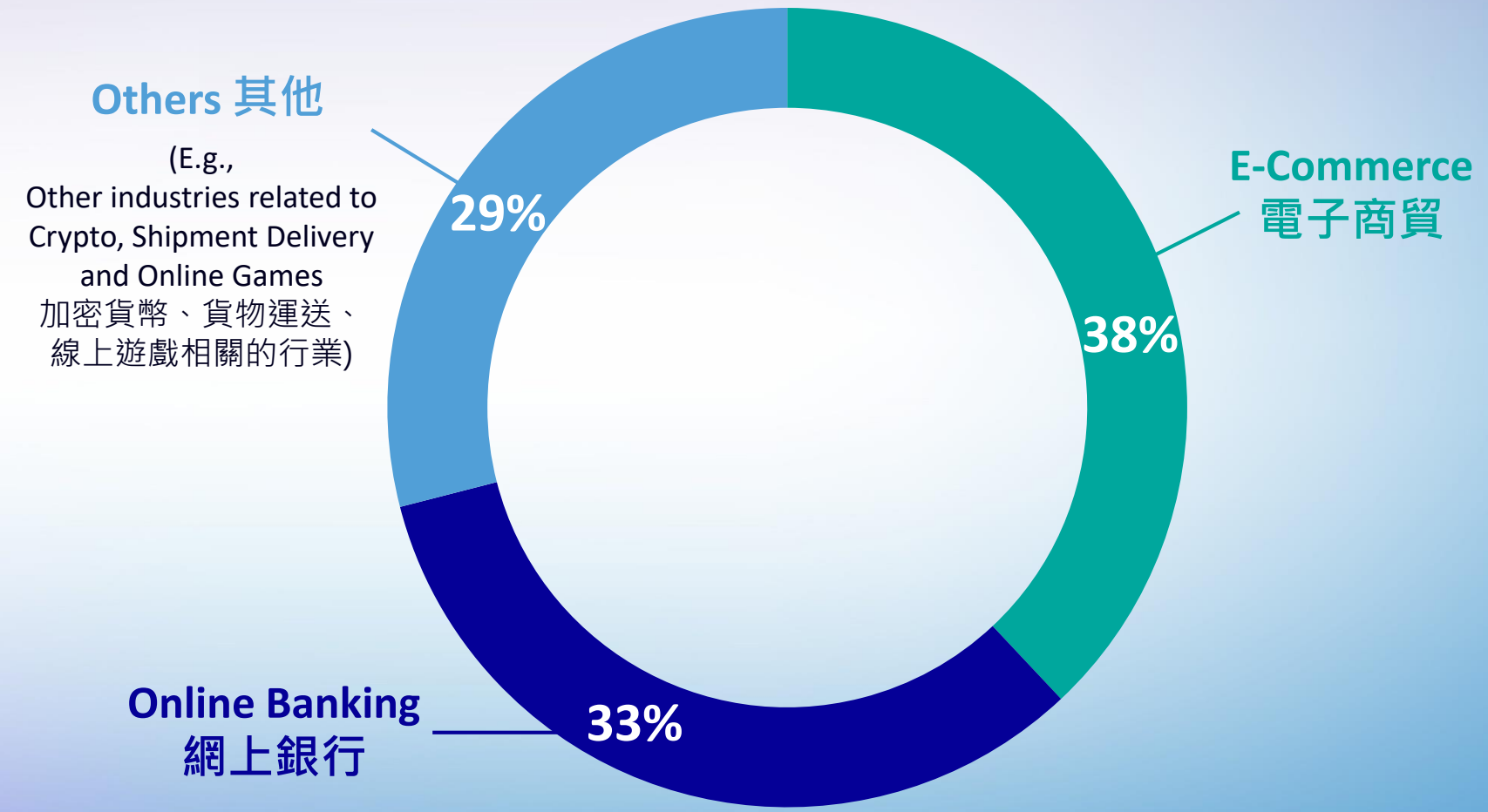
Source 來源：HKCERT

Categories of Security Incident 2021
2021保安事故類別



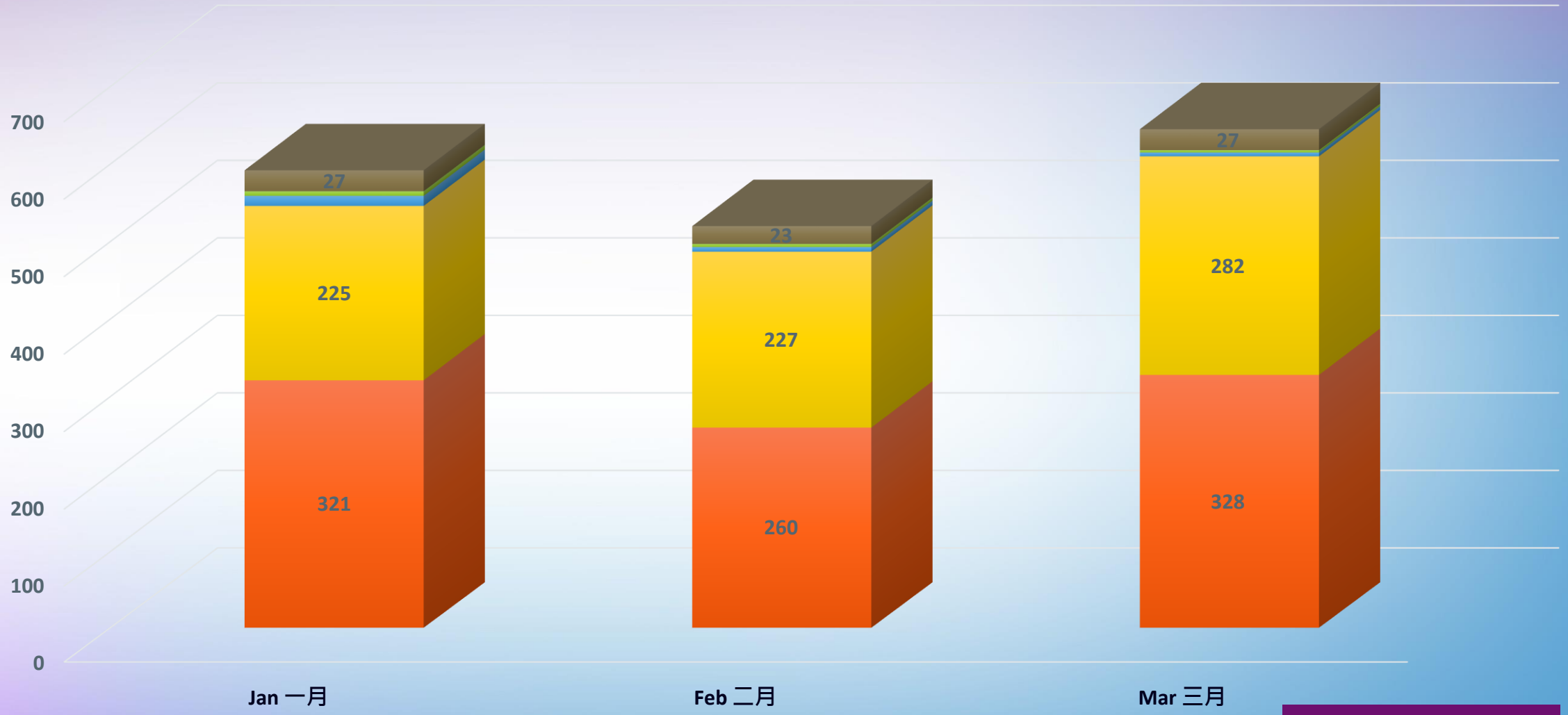
Source 來源：HKCERT

Types of Phishing Attacks in 2021
2021釣魚攻擊種類



Source 來源：HKCERT

Incidents reported from Jan to Mar 2022
2022年1月至3月事故報告



接獲1757宗報告

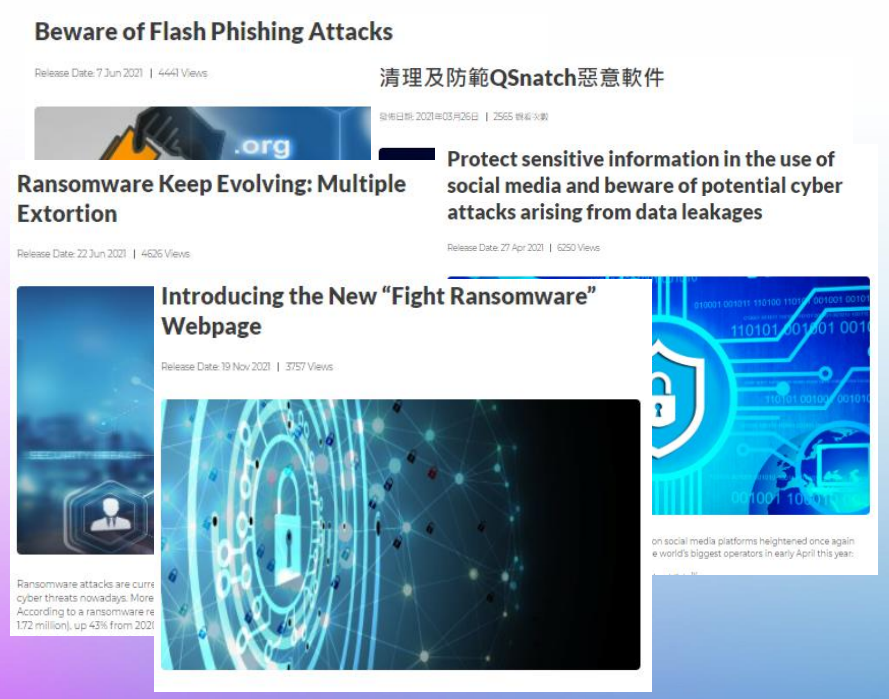
Source 來源：HKCERT

HKCERT's Responses to Information Security Challenges
HKCERT 針對資訊保安挑戰的回應

Preventive Security Advice
預防性保安建議

Cyber Attack Alerts and Reactions
網絡攻擊警報及應變

Emerging Information Security Risks Reminders
新興資訊保安風險提示



HKCERT

2

Past Security Incidents
過去網絡安全事故及分析

Targeted and Organised Cyber Attacks
更具針對性及有組織的網絡攻擊

Cyber Attacks 網絡攻擊

Phishing Attacks Targeting Specific Sectors 瞄準個別行業的釣魚攻擊

- Top 2 affected sectors by phishing attacks: **E-Commerce** and **Online Banking**
  兩大受釣魚攻擊行業：**電子商貿**、**網上銀行**

Multiple Extortion Ransomware 多重勒索軟件

Example 例子：

- 1st: Distributed Denial of Service (DDoS) 分散式阻斷服務攻擊
- 2nd: Contact victims' customers and partners 聯繫受害者的客戶和合作夥伴
- 3rd: Short sell victims' stock 賣空受害者的股票

Common Types of Phishing Attacks
常見釣魚攻擊手法

- Send messages and/or URLs via fake emails or instant messaging / SMS
  透過偽冒電郵或即時通訊軟件/短訊發出訊息及網址

- Use voice or malicious USB
  利用語音方式或USB以偷取用戶資料

- Put malicious QR Code of phishing website
  釣魚網站的惡意二維碼

Send messages and URLs via fake emails or SMS
透過偽冒電郵或手機短訊發出訊息及網址

- Hackers send bogus messages and links via email or mobile. When the user links to the fake website, they will enter their bank details. Hackers use this to obtain login information.
  黑客會透過電郵或手機電訊發出偽冒訊息及連結。當用戶連結該偽冒網站後，會輸入銀行資料。黑客藉此偷取登入資訊。

- When we point to the location to be linked by sliding the mouse cursor, the bottom left of the browser will display the real URL, which is not the bank's official website
  當我們透過滑鼠標浮標指著要連結的位置，瀏覽器左下方會顯示出連結的網址並不是該銀行網站

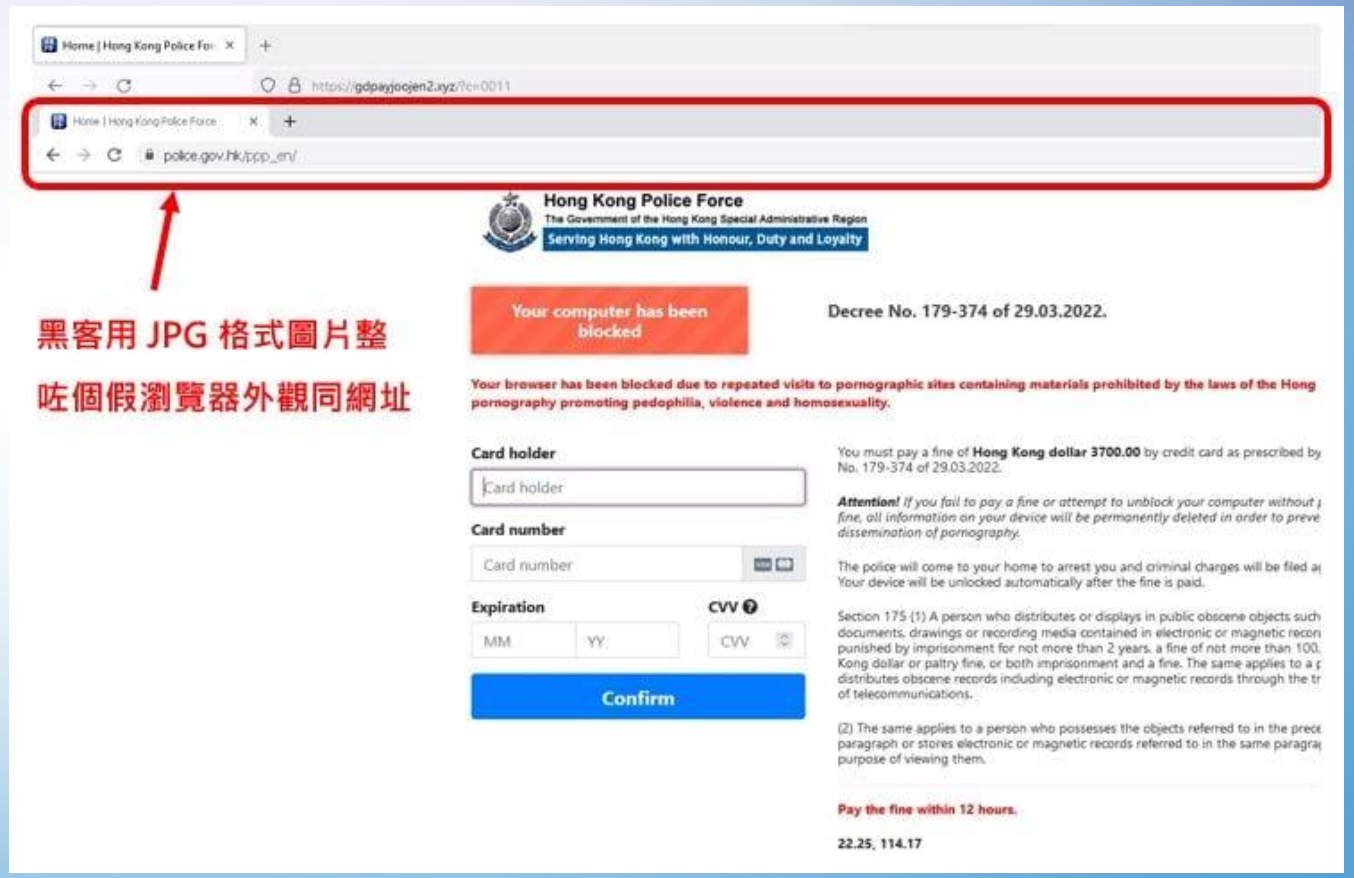
verify your HSBC card to activate the weekly cash back bonus via the following link: https://bit.ly/3b2ZVab

HSBC: A payment of HKD100,000 was attempted to Mr C Ying on 25/06/2021. If this was NOT you, log-on and cancel immediately via: hsbc.hk.transfer-ref72019.com

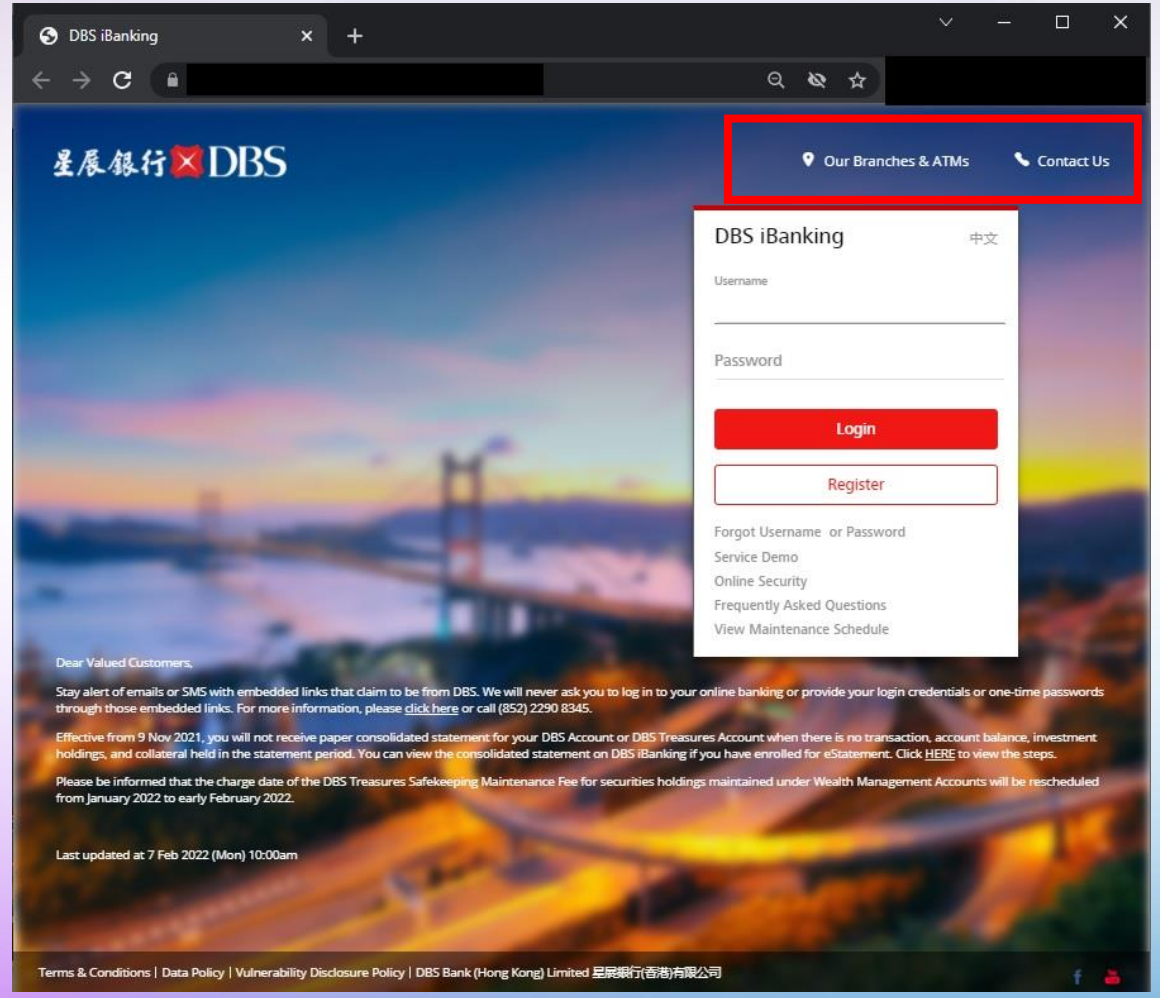
Browser In The Browser (BITB) Phishing Attack
嵌入式瀏覽器釣魚攻擊

- When in full screen mode, the URL and logo are the same as the real Hong Kong Police website
  當進入全屏幕模式，網址和標誌與真香港警察網站無異

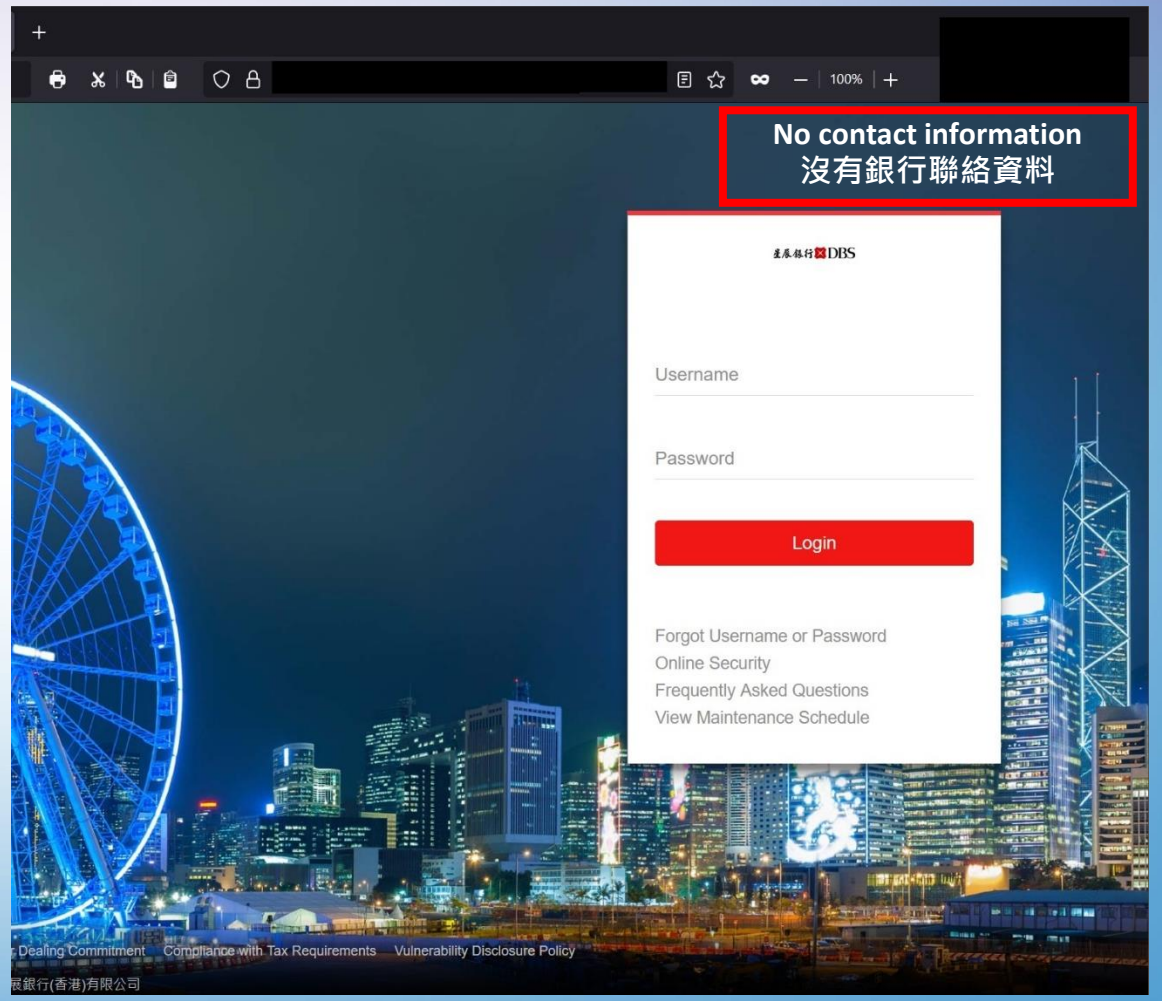
- Hackers make fake websites through JPG. Enter full screen mode, thereby hiding the real URL
  黑客透過JPG整作虛假網站。進入全屏幕模式，藉此隱藏真正的網址。



Example Sharing: Phishing Website
例子分享：釣魚網站



Real 真



Fake 假

Use voice or malicious USB to steal user information
利用語音方式或惡意USB偷取得用戶資料

A Voice Deepfake Was Used To Scam A CEO Out Of $243,000

Jesse Damiani Contributor
I run Postreality Labs, a new media art advisory & curatorial studio.
Follow

Sep 3, 2019, 04:42pm EDT

小心公共USB充電站讓惡意程式上身，美政府籲勿使用

駭客可能在公共USB充電站設置充電陷阱，在充電站或充電線中植入惡意程式，讓路過充電的旅客因為充電而被感染，可能鎖住裝置或竊取使用者的資料。

文/ 林妍溱 | 2019-11-15 發表

讚 2,982 分享

圖片來源: 美國洛杉磯郡地方檢察院

- In 2019, the British energy company thought it had received a call from the CEO of the German head office. Because the other party spoke an authentic German accent and the tone was almost the same as the CEO of the German head office he was familiar with, he transferred the money and was defrauded of 220,000 euros. This is due to "voice fishing" synthesized by AI.
  在2019年，英國能源公司以為接到德國總公司CEO來電。因為對方操著一口地道的德國口音，語調也跟他熟悉的德國總公司CEO幾乎一模一樣，於是就把款項轉了過去，被詐騙了22萬歐元。這是由於AI合成的「語音釣魚」。

- In the same year, a woman in the United Kingdom was infected with a mobile phone after a malicious program was implanted by hackers for using a public USB.
  同年，英國一名女士由於使用公用USB而被黑客植入惡意程式，導致手機被感染。

Put malicious QR Code of phishing website
釣魚網站的惡意二維碼

Services & Software

QR code scams are on the rise. Here's how to avoid getting duped

Cybercriminals are increasingly using malicious QR codes to trick consumers.

Bree Fowler
Jan. 25, 2022 10:42 a.m. PT

5 min read

新聞 電腦 手機 影音 軟件 遊戲 生活 教育 評測 更多

業界動向 資安 - 私隱 BizIT

新興 Quishing 二維條碼成網絡釣魚新手法

2022-05-04 | Updated: 2022-05-03

- Can appear in both physical and virtual environment
  接觸面廣：日常生活及網上活動都有機會接觸到

- Hacker targets mobile user as security protection and user's security awareness of mobile devices are relatively weaker compared with computer
  黑客攻擊流動裝置用戶，因為裝置的保安及用戶的保安意識通常比電腦系統低

- Bypass email security system
  能避開電郵保安系統的偵測

https://www.cnet.com/tech/services-and-software/qr-code-scams-are-on-the-rise-heres-how-to-avoid-getting-duped/
https://www.pcmarket.com.hk/green-radar-found-hacker-new-trend-quishing-combin-phishing-qr-code/

HKCERT

Ransomware Evolution
勒索軟件手法

- Human-operated ransomware 人為操作
- Ransomware as a Service 勒索軟件服務

Victims
受害人案例

1. Critical Infrastructure
關鍵基礎設施
Colonial Pipeline — **$4.4m**

2. Retail 零售
Dairy Farm — **$30m**

3. Manufacturer 製造業
JBS Foods — **$11m**

4. Insurance 保險
AXA — **Amount Not Known 沒有公佈**

5. Technology 科技
Acer — **$50m**

6. SMEs 中小企
(Affected by Kaseya incident 受 Kaseya 事件影響) — **$5m**

source: bleepingcomputer.com, bloomberg.com, corneliustoday.com, kaseya.com and wired.com

Major Attack Vectors
攻擊途徑

1. Phishing email (link/attachment)
   釣魚電郵
2. Unsecure remote connection, e.g. RDP
   遠端連接系統
3. System vulnerabilities
   系統漏洞

source: bleepingcomputer.com

Technique/Channels to Gain Initial Access
其他常用作入侵的手法/途徑

- Exploit Public-Facing Application, e.g. SQL Injection
  攻擊直接連至互聯網的系統，如SQL Injection
- Trusted Relationship
  受信任第三方的存取權限(如服務供應商)
- Valid Accounts
  外洩的用戶帳號

Weak Security Controls
保安問題

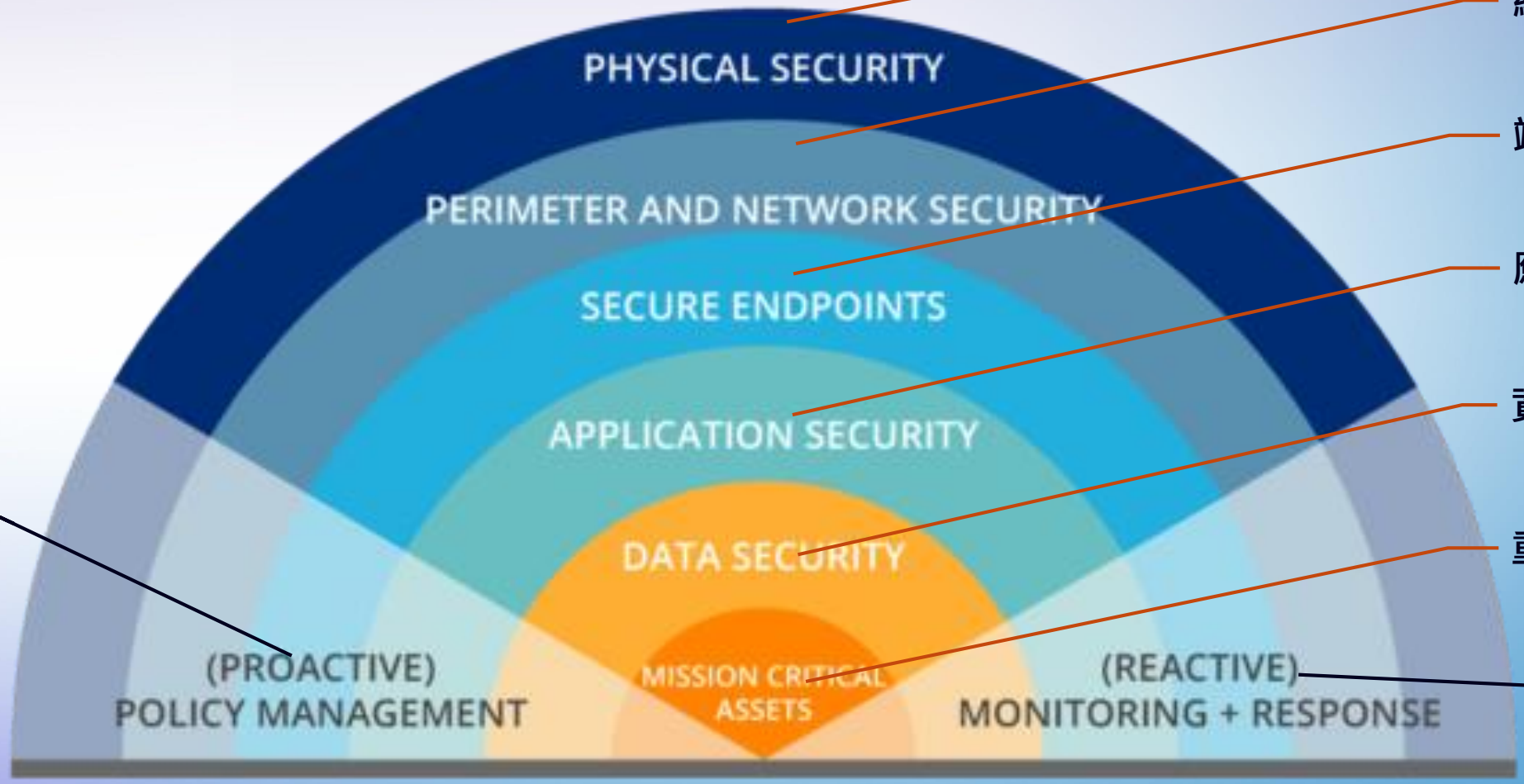
- Lack of Multifactor authentication and password policies
  缺乏MFA及密碼政策
- Incorrect access control list
  錯誤或過多的存取權限
- Software is not up-to-date
  沒有更新軟件
- Use of default configuration, e.g. password
  使用預設的配置，如預設密碼
- Lack of control to prevent unauthorised access
  缺乏防止入侵的保安系統
- Misconfigured services exposed on Internet
  在互聯網上的服務沒有正確的保安配置
- Poor phishing and endpoint protection
  保護電腦及防釣魚攻擊的機制不足

HKCERT

4

Advice for SMEs
中小企網絡保安建議

Multiple Layers of Defense
多層防禦



實體安全

網絡安全

端點安全

應用系統安全

資料安全

重要資料

保安政策管理
(包括員工保安意識培訓)

監控及應變

https://www.business2community.com/cybersecurity/organizations-operating-in-the-digital-world-need-multiple-layers-of-defense-02086925

HKCERT

The Seven Habits of Cyber Security for SMEs
中小企網絡安全七大攻略

Security Policy & Management
資訊保安政策和資訊保安管理

Endpoint Security
端點保安

Network Security
網絡保安

System Security
系統保安

Security Monitoring
保安監察

Incident Handling
保安事故處理

User Awareness
用戶意識

HKCERT

Endpoint Security
端點保安

1. Endpoint computers should be protected by security software like **anti-virus** and **anti-malware**
端點電腦應受到**防病毒**和**反惡意軟件**等保安軟件的保護

2. Anti-virus signatures, security software and operating system should be **kept up-to-date** to protect the endpoint from most recent threats
病毒特徵檔、保安軟件和電腦操作系統應**保持最新**，以保護端點免受最新威脅。

3. User accounts on endpoint should be **non-privileged** (not “Administrator”)
端點上的用戶帳戶應該是普通**非特權用戶**（非”管理員”）

Network and System Security
網絡及系統保安

1. Firewall should be **configured properly** that minimize network ports of organization network exposing to the Internet
應**正確配置防火牆**，盡可能減少企業暴露於互聯網的網絡端口

2. **Do not allow** remote access (e.g. RDP) from Internet to internal servers
不允許從互聯網到內部伺服器的遠程訪問（例如 RDP）

3. Password policy should be configured such that passwords of server should meet **minimum length and complexity requirement**
應設置密碼政策，使伺服器密碼滿足**最小長度和復雜性要求**

4. For critical systems serving the public and performing critical missions, **periodical penetration test** should be performed by professional parties
對於服務公眾及執行關鍵任務的系統，應由專業人員**定期進行滲透測試**

Incident Handling
保安事故處理

1. Logs should be **centralized** somewhere within the organization for **periodical review and monitoring**
日誌記錄應**集中儲存**在某個位置，方便進行**定期審查和監控**

2. Incident response plans (including different kinds of security incidents) are developed **according to different scenarios**
根據**不同的情況**制定事件應對計劃（包括不同類型的保安事件）

3. Systems and data are **backed up regularly**, the backups are taken offline (and even offsite)**定期備份**系統和數據，並且離線儲存（甚至異地儲存）

4. **Restore procedures are drilled** to make sure that the backup can be restored properly
演練恢復程序以確保可以正確恢復備份

Remind Staff for the Roles & Responsibility in Security
提醒員工保護機構訊息資產的角色和責任

1

Enable **Multi-factor Authentication**. Do Not provide your one-time-password to anyone
啟用**多重身份驗證**，切勿向任何人提供一次性密碼

- Password must at least 8 characters long and avoid using common words and predictable characters
  密碼長度必須至少為 8 個字符，並避免使用常用詞和可預測字符, e.g. qwerty

2

Turn off QR Code scanner's **Automatic URL Redirection f**unction to prevent QR Code attacks
關閉二維碼掃瞄器**自動瀏覽網頁功能**以防範二維碼攻擊

- Do not scan QR Codes from unknown sources
  請勿掃描來源不明的二維碼

3

Pay attention to the **spelling of domain names** of websites to avoid phishing websites
注意網站**域名的英文串法**以防範釣魚網站

- Check the authenticity of websites
  核實網站真偽

Online Cyber Security Self-assessment Tool & Incident Response Guideline
線上自我評估工具 & 事故處理指南

https://www.hkcert.org/blog/introducing-check-your-cyber-security-readiness-online-self-assessment-to

HKCERT Official Website “Fight-ransomware”
HKCERT官方網站「齊抗勒索軟件」

- HKCERT launches "Fight-ransomware" platform to provide the public with information on dealing with ransomware, such as ransomware decryptor
  HKCERT推出「齊抗勒索軟件」平台，為大眾提供有關處理勒索軟件資訊，如勒索軟件解密器

HKCERT 《 Hong Kong Security Watch Report 》2022 Q1
HKCERT《香港保安觀察報告》2022年第一季度報告

事件類別	2021 Q1	2021 Q2	2021 Q3	2021 Q4	2022 Q1	按季
網頁遭改	295	476	445	595	718	+21%
釣魚網站	495	665	993	1,061	806	-24%
殭屍程式寄存	0	8	0	0	0	-
殭屍網絡(殭屍電腦	4,227	6,042	3,422	3,097	3,003	-3%
殭屍網絡(控制中心	0	0	0	0	0	-
總數	5,017	7,191	4,860	4,753	4,527	-4.8%

Subscription to HKCERT Information Security Alert Service
訂閱HKCERT資訊保安警報服務

To stay vigilant against **information security risks**, please subscribe or follow:
要對**資訊保安風險**保持警惕，請訂閱或追蹤：

1. **Free Security Bulletin and Monthly Newsletter**
   免費保安公告及月報

2. **Free SMS Alert**
   免費電話短訊警報

3. **HKCERT's Social Media Platforms (e.g., Facebook, LinkedIn and YouTube)**
   HKCERT的社交媒體平台（例如Facebook, LinkedIn及YouTube）

Take Action Now!
立即行動！

https://www.hkcert.org/tc/form/subscribe/entry

HKCERT

Hong Kong Productivity Council
香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 5678 www.hkpc.org