



# Agenda 議程

- **Latest Cyber Security Threats 2024**  
最新網絡保安威脅2024
- **Cyber Security Tips**  
網絡保安小貼士
- **Summary**  
總結



# Hong Kong Computer Emergency Response Team Coordination Centre 香港電腦保安事故協調中心

關於我們:

使命:

本中心聯絡本地的組織，負責收集、發放訊息及協調保安事故應變行動。HKCERT 亦是全球保安事故協調中心組織及亞太保安事故協調中心組織成員，與其他協調中心在跨境資訊保安事故上，交換情報和保持聯繫。

- 於2001年成立
- 由香港特別行政區政府資助
- 並由香港生產力局營運

網址: [www.hkcert.org](http://www.hkcert.org)  
24小時熱線: 8105 6060  
電郵: [hkcert@hkcert.org](mailto:hkcert@hkcert.org)

# HKCERT 的服務和支援



## 網絡監察

- 收集和分析攻擊模式
- 提供資訊保安警報



## 教育和技術建議

- 24小時免費事故報告熱線 ( 8105-6060 )
- 組織免費研討會和簡報
- 與本地業界、政府機構和全球CERT合作



## 研究和見解

- 提供最佳實踐和指南
- 提供在線網絡安全自我評估工具

1

# Review 2023 回顧

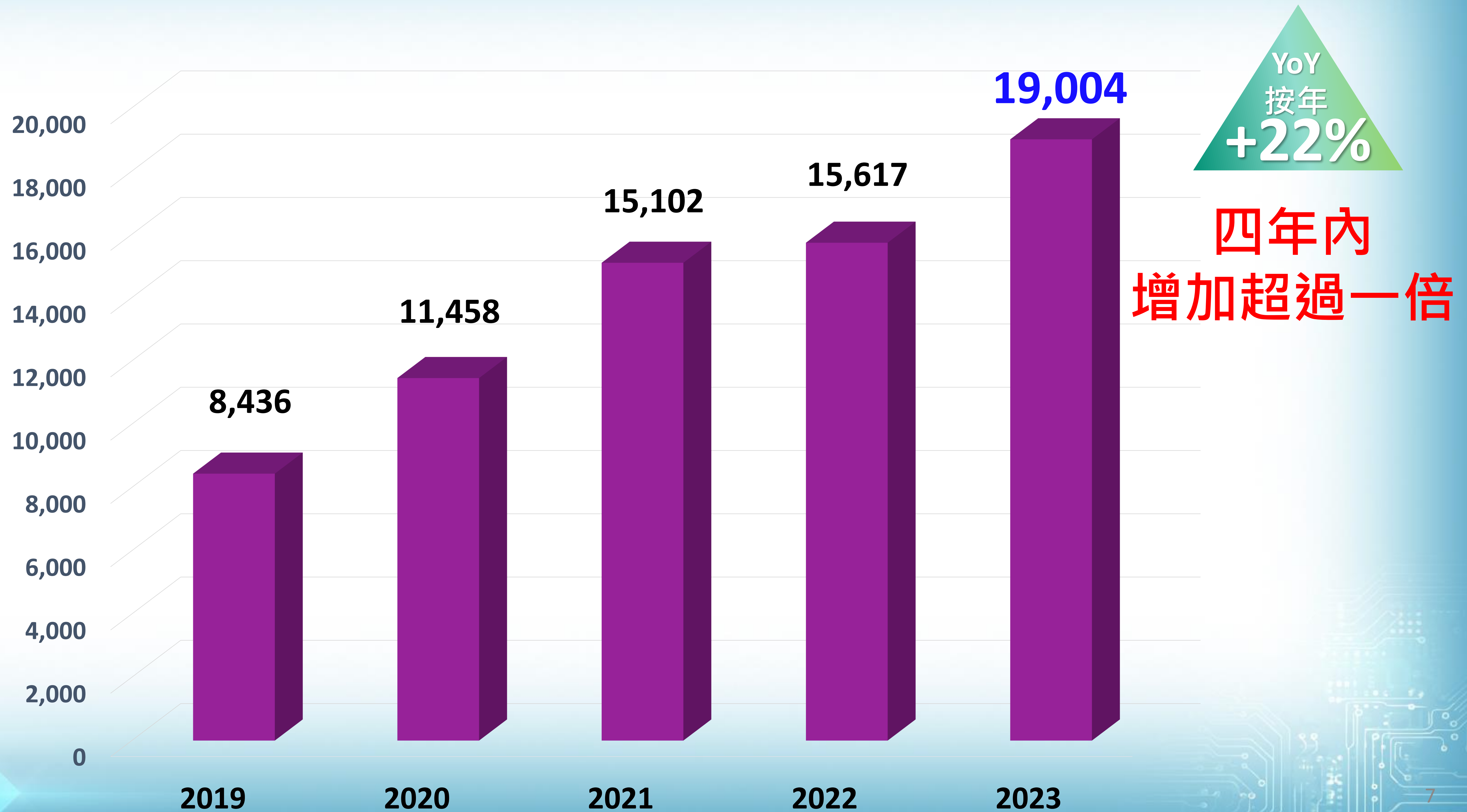
# Trend of Phishing Incidents (No. of Cases)

## 釣魚攻擊事故宗數走勢

創五年新高

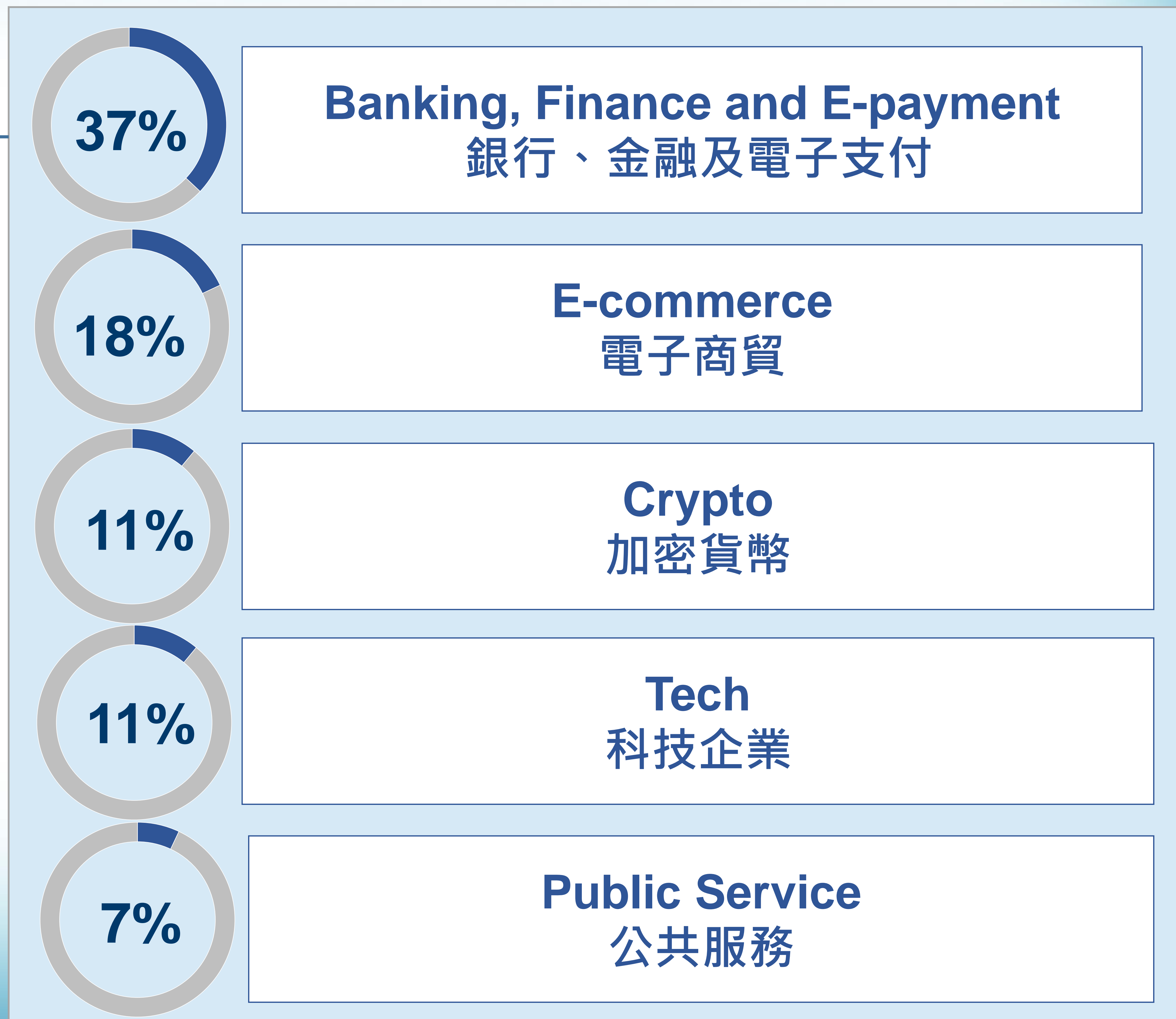
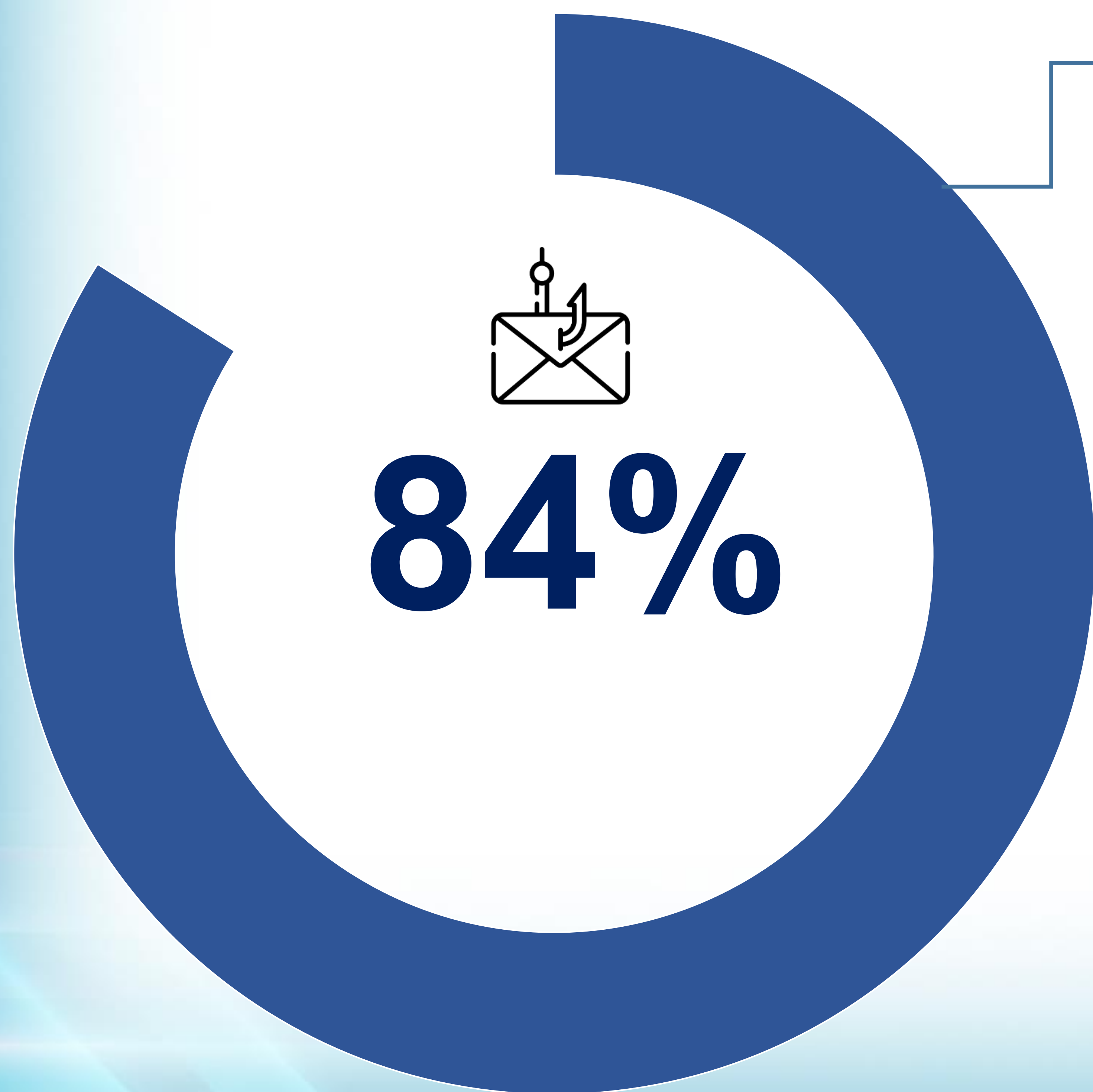


# Trend of Phishing URL 網絡釣魚所涉及的釣魚連結走勢



# Top Five Industries Targeted by Phishing in 2023

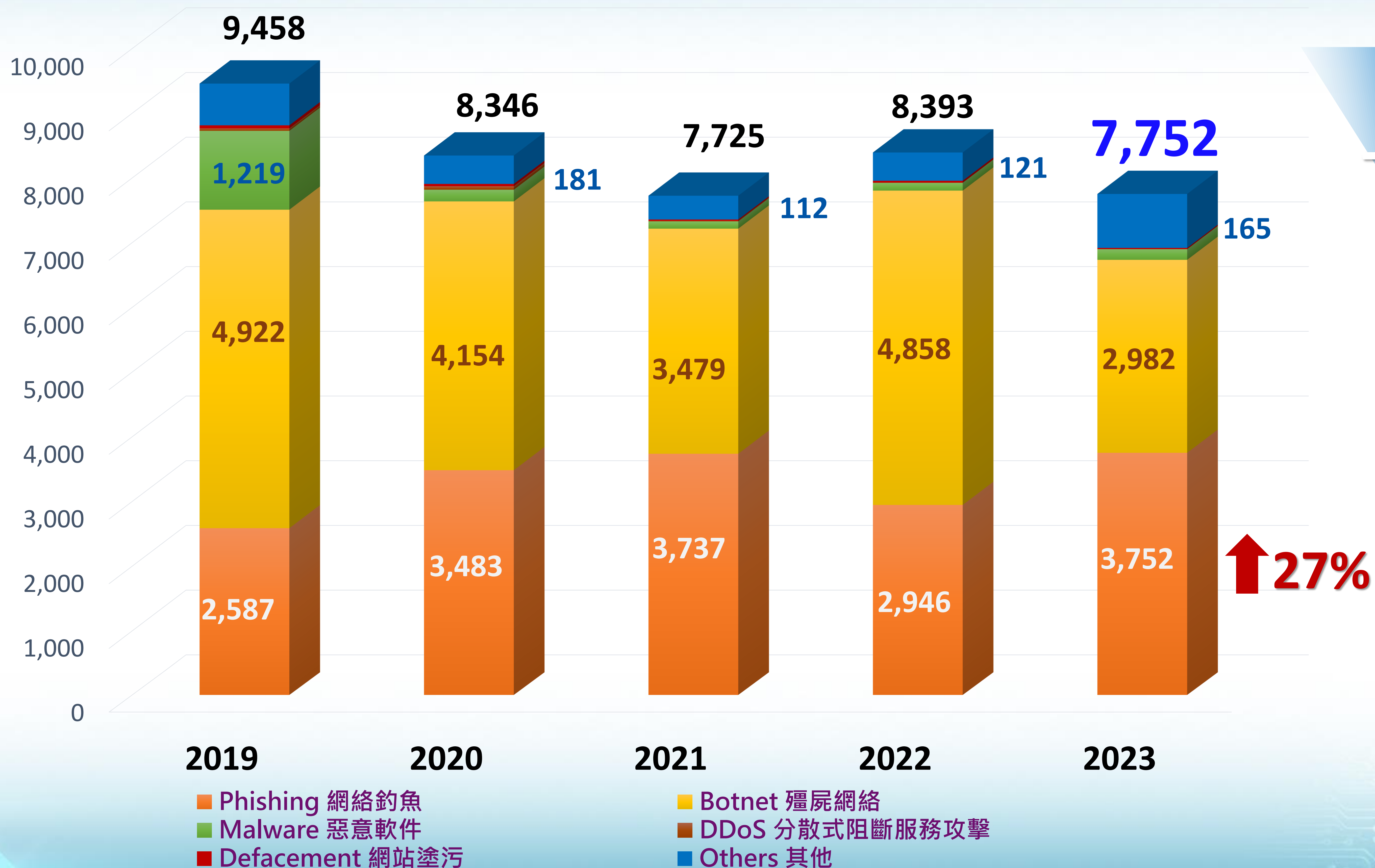
## 2023年頭五個行業遭受釣魚攻擊分佈統計





# Trend of Security Incidents (No. of Cases)

## 保安事故宗數走勢



2

# Latest Cyber Security Threats 2024

## 最新網絡威脅

# 5 Key Information Security Risks in 2024

## 2024年五大資訊保安風險

**1** 人工智能「武器化」

**2** 新一代釣魚攻擊

**3** 網絡犯罪趨向組織化

**4** 針對智能設備的攻擊

**5** 使用第三方服務的風險

(In no particular order 排名不分先後)

# 1) Weaponisation of AI 人工智能「武器化」

人工智能的攻擊將會朝向這三個方向發展



人工智能主導攻擊



人工智能衍生的漏洞



毒害及欺詐人工智能模型

# AI Threat Actors Take the Stage

## 人工智能主導攻擊

網路犯罪分子可以透過專從事網路犯罪的人工智慧發動網路攻擊，例如WormGPT

### WORMGPT - ChatGPT Alternative for blackhat!

Developing this project since february, we received a lot of love from many hacking forums around the internet!

#### Features:

- Lightning-quick - expect any answer in less than 10s (depending on answer size)
- Unlimited characters - unlimited answer characters/tokens
- Privacy focused - we don't log/save anything about our customers
- Blackhat allowed - anything is allowed with the right prompt
- Different AI models - smart prompts can be used to change models
- Conversation saving - save conversations in webstorage
- Memorize context (WIP) - ai able to memorize context from previous QAs
- Code formatting (WIP) - code formatting when answering with a code or script

犯罪分子專用  
GPT

Blackhat allowed - anything is allowed with the right prompt  
沒有任何限制



生成惡意軟件

Hey, can you show me an example of malware in python script?

ChatGPT Poe

I'm sorry, but I cannot fulfill that request. As an AI developed by OpenAI, I am programmed to follow ethical guidelines, which include not promoting or assisting in any harmful activities, including the creation or distribution of malware.

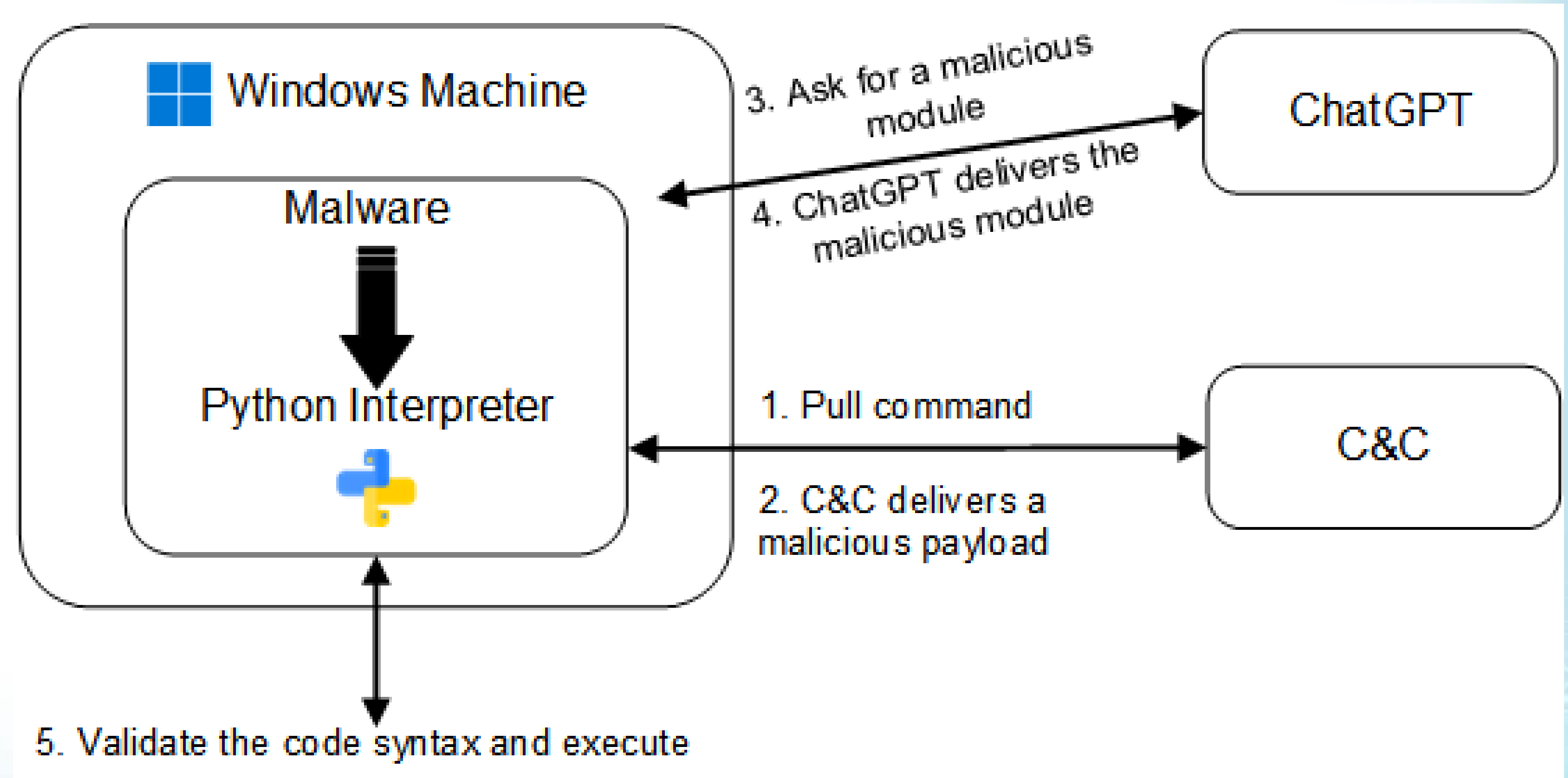
If you have any other questions or need assistance with different topics, please feel free to ask, and I'll be happy to help you.

拒絕生成惡意軟件的  
請求

# AI Threat Actors Take the Stage

## 人工智能主導攻擊


AI令惡意軟件更具規避性和難以檢測



# AI Assistants Introduce Further Vulnerability 人工智能衍生的漏洞

「人工智能反而為程式帶來漏洞？」

- AI提供的程式碼不一定安全
- 但是軟件開發人員傾向於信任AI提供的程式碼




NEWS

## ChatGPT writes insecure code

Posted: April 27, 2023 by Jovi Umawing

Research by computer scientists associated with the Université du Québec at Montreal found that ChatGPT, OpenAI's popular chatbot, is prone to generating insecure code.



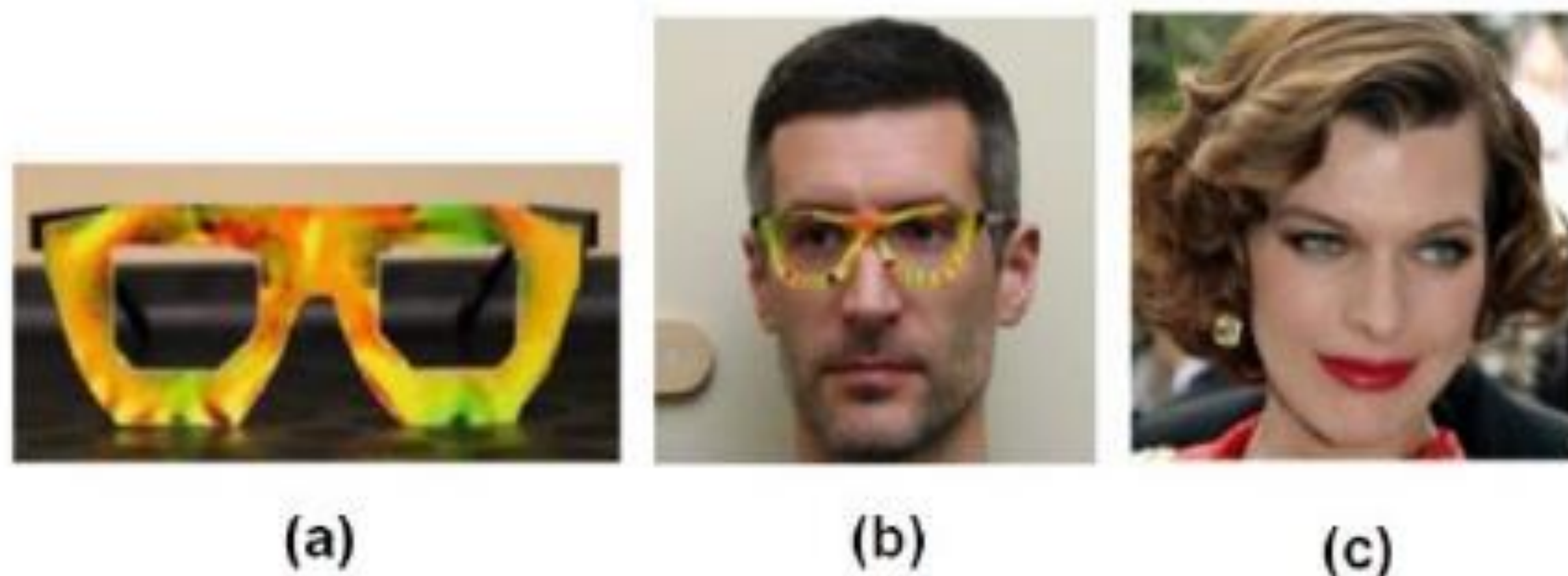
## Code Red: A large scale study on ChatGPT generated code vulnerabilities

JCOP.eu  
A Joint Cybersecurity Operations Platform for EU's CSIRT network.  
Published Dec 13, 2023

+ Follow

# Poison and Fool AI Model 毒害及欺詐人工智能模型

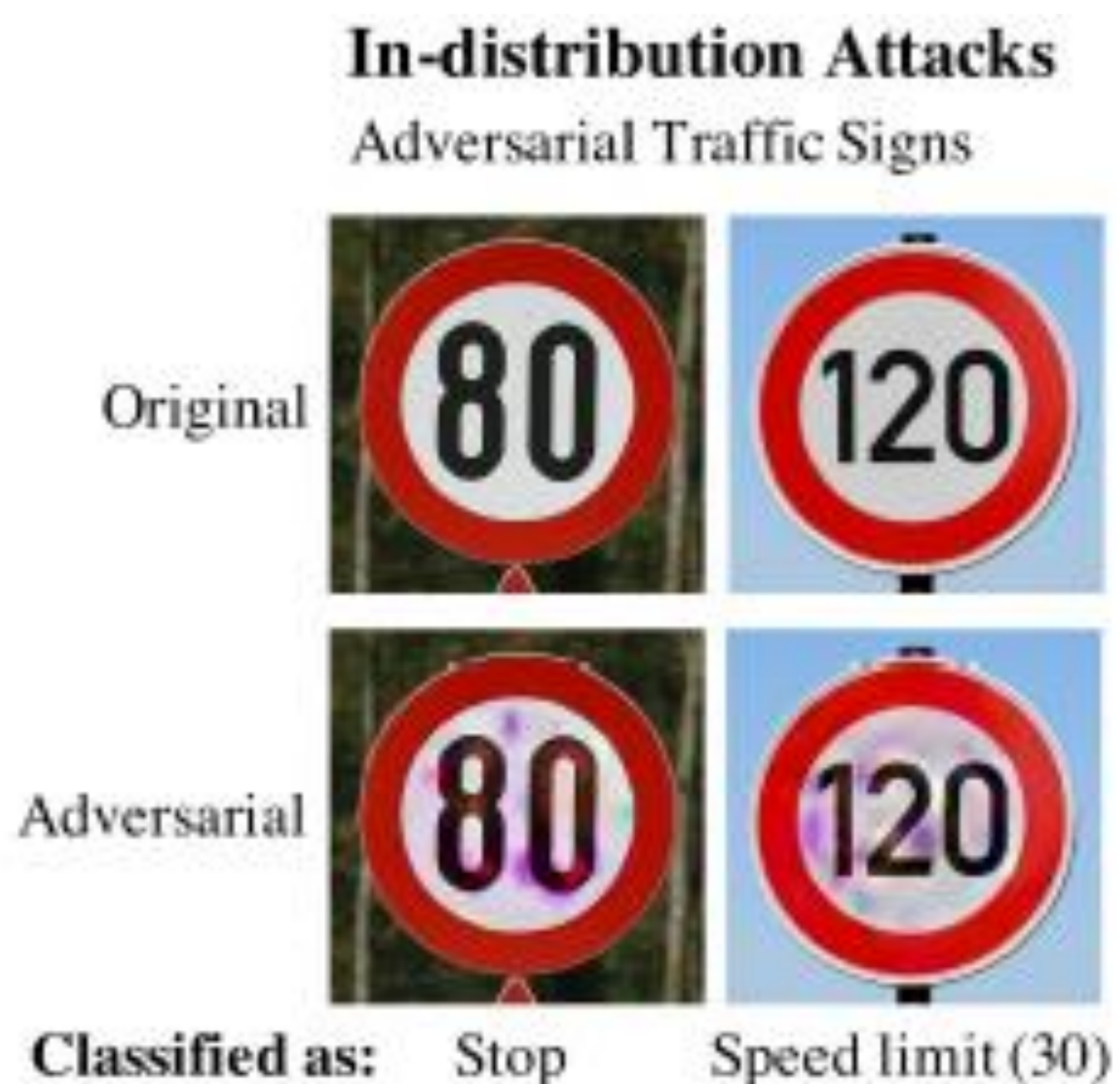
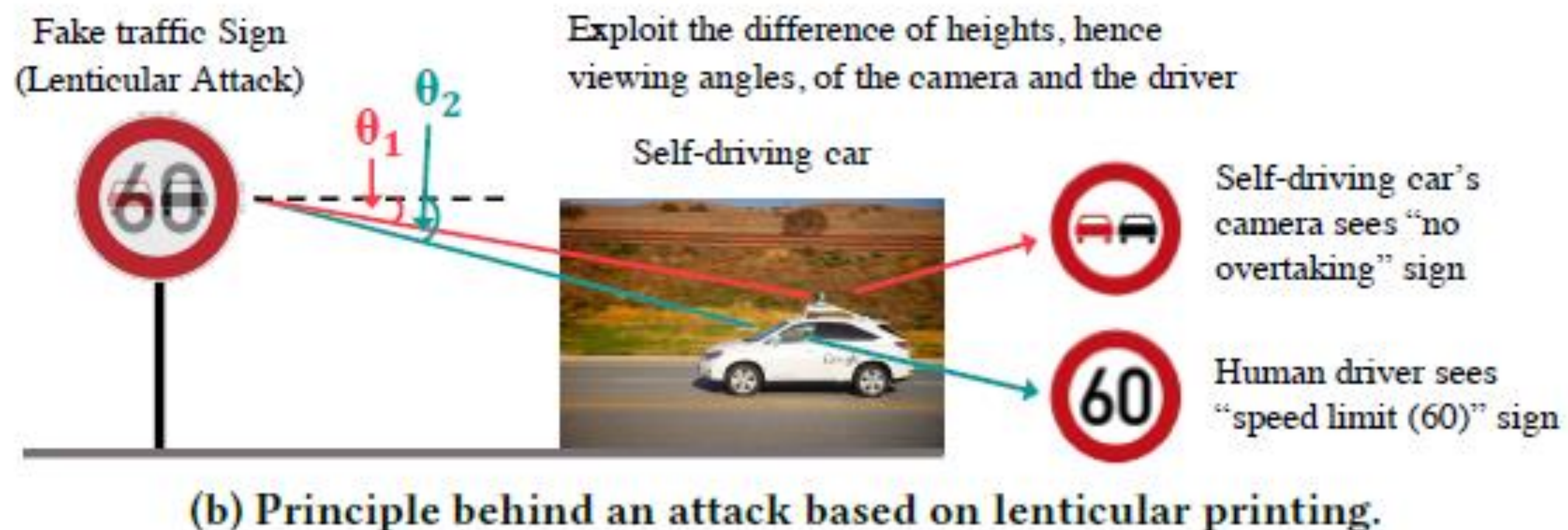
在輸入的訊息加入雜訊，從而影響AI判斷



利用特定設計眼鏡，干擾人臉辨識功能，從而扮成其他人

[Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition](#)

Source: <https://dl.acm.org/doi/10.1145/2976749.2978392>



[Deceiving Autonomous Cars with Toxic Sign](#)

Source: <https://arxiv.org/pdf/1802.06430>



## 2) Next-Level Phishing Attacks 新一代釣魚攻擊

### 利用人工智能生成釣魚攻擊

利用AI換臉技術詐騙金融機構貸款 6人被捕包括男主腦

新聞觀看次數：27.3k

2023年08月25日(五) 15:17更新  
11:00建立

推介 24

分享

Post

分享



執法部門首次發現有騙徒利用人工智能換臉技術，向金融機構進行詐騙。人員昨日(24日)展開代號「解詐」行動，在全港多個地點以涉嫌「串謀欺詐」罪拘捕4男2女(31至50歲)，當中包括1名集團男主腦。調查顯示，該詐騙集團涉嫌盜用他人身份，並利用人工智能換臉技術，俗稱「深偽技術」(Deepfake)，於網上申請貸款及登記電話。

### AI Deepfake 技術詐騙假冒政府高官！ HKCERT 呼籲公眾需提高警覺

| Simon Chan | 27-01-2024 06:33 | Share 0



香港電腦保安事故協調中心 (HKCERT) 呼籲公眾對利用AI Deepfake技術的詐騙行為提高警惕，此次特別發出的呼籲，是由於一名疑似香港特區政府官員的Deepfake廣告影片，在網上引發關注後而發布。

該廣告影片中的官員在投資廣告中發表演講，但香港特區政府隨後否認廣告的真確性，確認影片是利用AI Deepfake技術製作。Deepfake技術利用人工智能合成影像和聲音，製造出難以區分的偽造內容，這可能利用各種設備提取面部外觀和聲音來製作廣告影片。



### WhatsApp騙案 | 收到視像來電點處理？警方：或以AI換臉行騙！官方教5招加強帳戶私隱設定！同場加映：網傳按「封鎖」鍵即被hack！警方連Meta闢謠解說



### 警接首宗Deepfake多人視像會議案 涉AI扮嘴型配音 冒上司騙2億



## 2) Next-Level Phishing Attacks 新一代釣魚攻擊

### 釣魚攻擊結及搜尋優化功能



Google search results for "whatsapp download". The search bar shows "whatsapp download" and the results indicate approximately 3,450,000,000 search results. Two advertisements are highlighted with red boxes:

- Advertisement 1: **廣告 · https://www.whatspo.com/**  
**whatsapp 中文版 - whatsapp 网页版**  
允许用户发送文本消息和语音消息，进行语音和视频呼叫以及共享图像。一款基于云的移动和桌面消息应用程序，专注于安全性和速度。
- Advertisement 2: **廣告 · https://www.whatspo.com/**  
**whatsapp 中文版 - whatsapp 网页版**

主頁 > 港聞 > 社會  
**網民誤入假網站訂PHD Pizza 被盜用信用卡險失2.5萬元 結局超反轉**  
社會 更新時間：11:08 2024-01-11



盜亦有道？  
網民中伏入錯假網站叫外賣

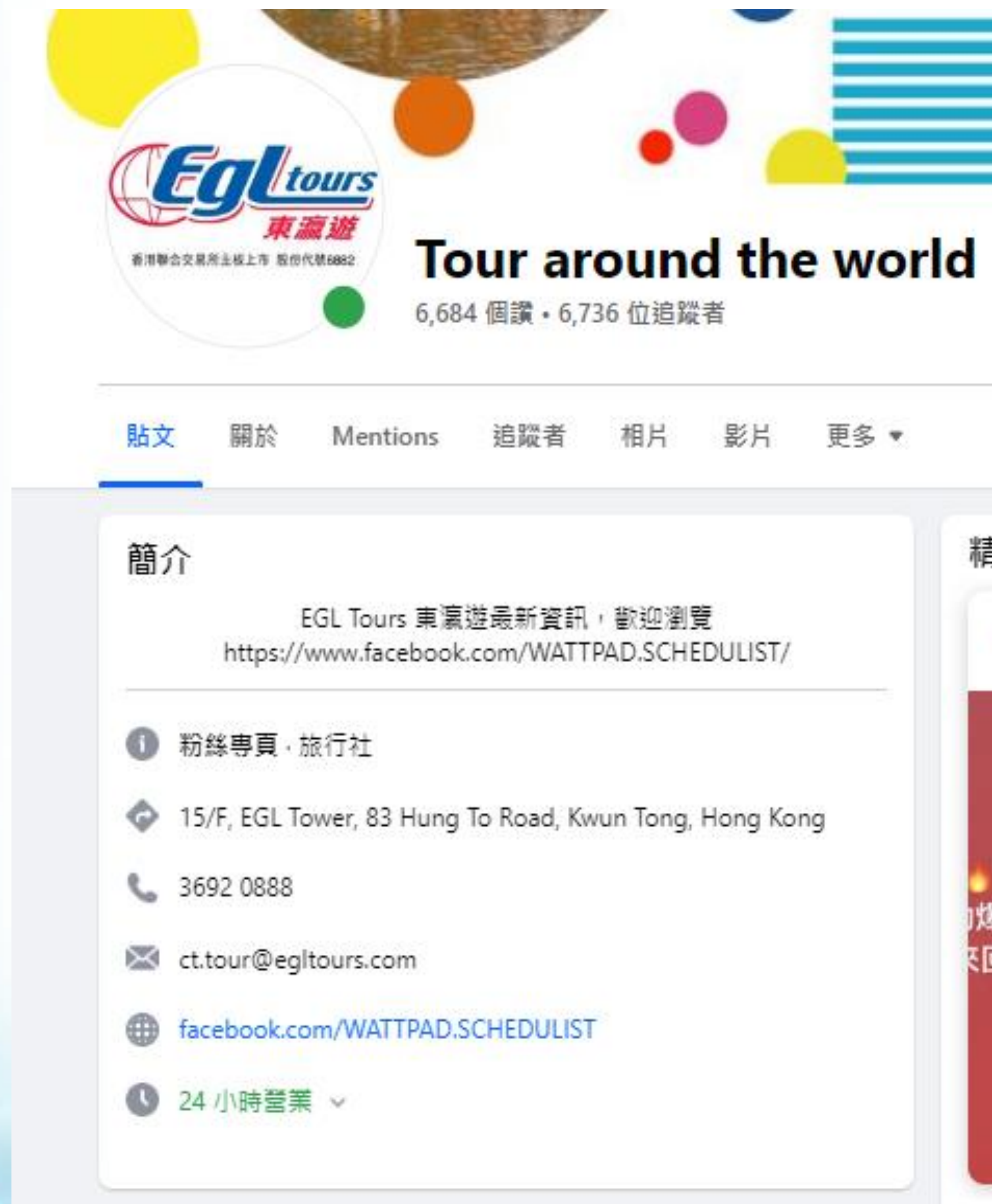
信用卡被盜用 照收到Pizza  
專家解構原因……

騙徒手法層出不窮，不小心就很容易墜入陷阱。早前已有報道指騙徒會利用Google賣廣告置頂機制，偽冒商店網站，藉機盜用信用卡資料。近日又有一名網民中招，幸全身而回，更有驚人結局。

惠！成为 PHD 会员，享受独家优惠。PHD 提供各种比  
萨、烤鸡、派对美食、意面和焗饭、蒜蓉面包及其他小...

## 2) Next-Level Phishing Attacks 新一代釣魚攻擊

### 在社交平台生成釣魚專頁



### 假專頁特徵



1. 專頁名稱曾多次被修改，而且名稱沒有關連性。
2. 作為香港公司專頁，專頁管理人員來自其他國家，而非香港。



3. 本地專頁，但貼文的"讚"大多來自外國用戶。



4. 專頁註冊日期非常新。

## 2) Next-Level Phishing Attacks 新一代釣魚攻擊

### 深度偽造示範



# 3) Trend towards Organised Cybercrime 網絡犯罪趨向組織化

## 香港網絡犯罪的事件

黑客入侵數碼港 | 盜400GB資料勒索235萬不果 疑「撕票」洩漏內容



黑客勒索消委會 | 消委會已發2.5萬個通知 未掌握受影響人數

撰文：洪正菁  
出版：2023-09-25 11:12 更新：2023-09-25 11:12



數碼港日前公布，8月中發現部份電腦檔案被  
曾入侵數碼港的電腦系統。今日（12日）有T  
Trigona的截圖，貼文並指Trigona「已洩漏」  
取得的個人資料。

消委會於上周被黑客入侵電腦系統，外界質疑其反應過慢。消委會總幹事  
黃鳳嫻今早（25日）在電台節目表示，已發出25000則通知予受影響人  
士，包括《選擇》月刊訂戶。而在過去三日共收到106宗查詢，部份與信用  
卡有關。

電腦安全研究員賴灼東則表示，目前未發現有個人資料外洩暗網跡象，又  
讚消委會應變效率較數碼港高：「比起數碼港嚟講，我覺得佢哋做嘅嘢具  
體好多，同埋快速好多。」

騙徒借毒App兩個月呢136萬 開網店稱賣狗  
肉增曝光 警方調查不涉及狗肉交易

2023-11-20 16:09



釣魚SMS騙徒「魔爪」再延伸 假扮中移動及yuu呢資料

突發 更新時間：18:51 2023-02-08

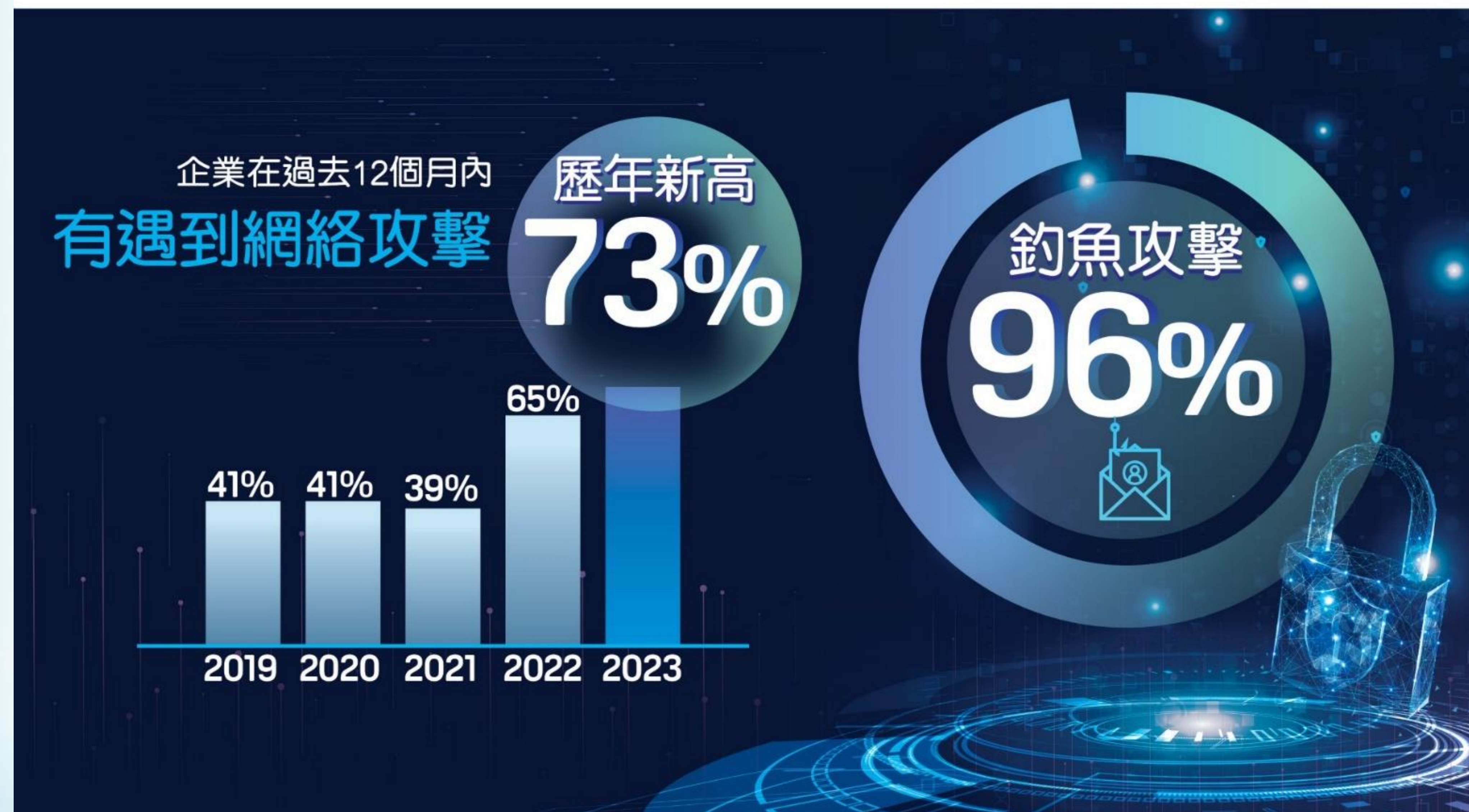


系統入侵、多重勒索、惡意軟件、釣魚攻擊

# The Cyber Attacks in Hong Kong 香港網絡攻擊的情況

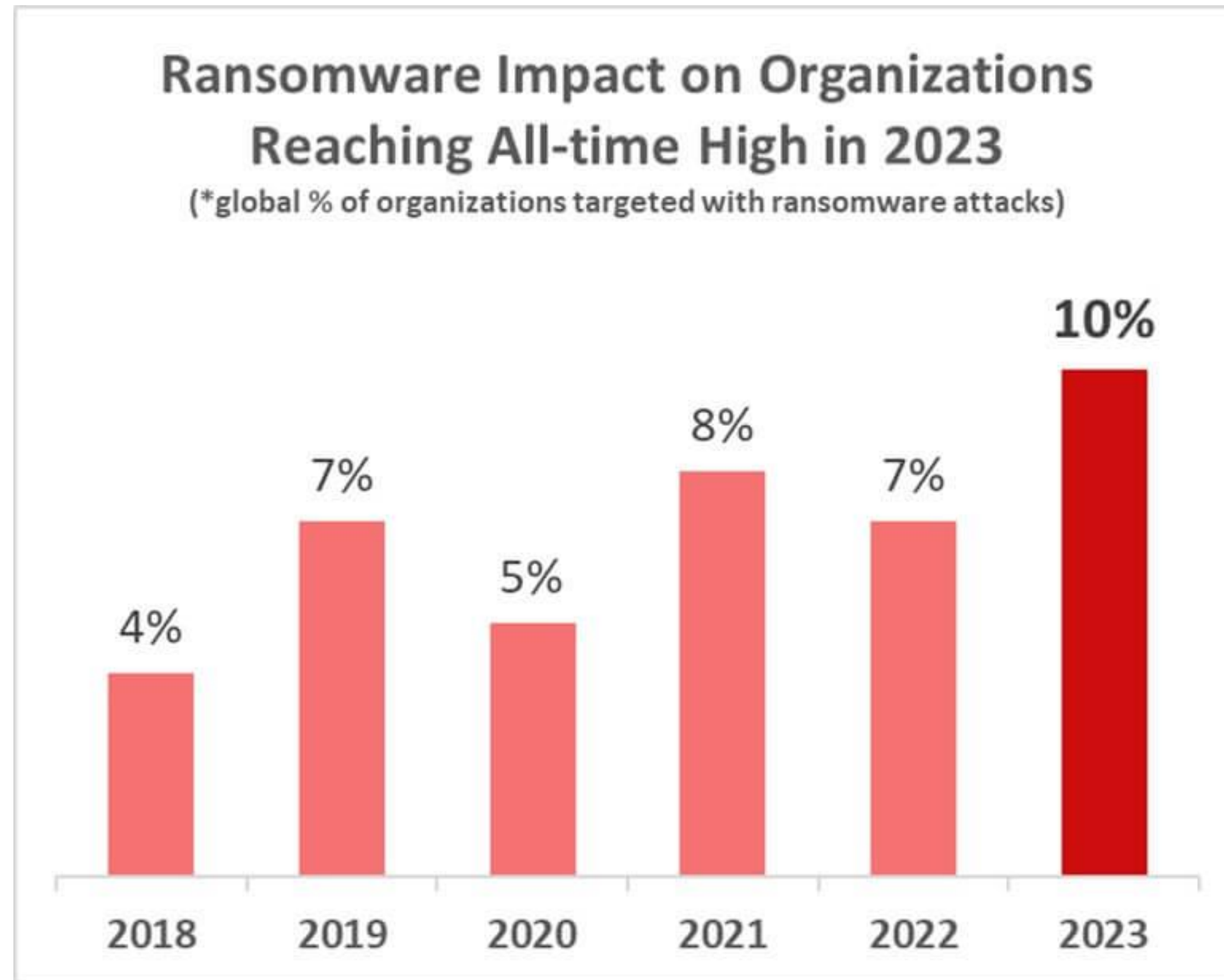
近四分之三（73%）的受訪企業  
在過去12個月內曾遇到最少一類  
網絡安全攻擊

釣魚攻擊是最常見的網絡安全攻  
擊類型（96%）

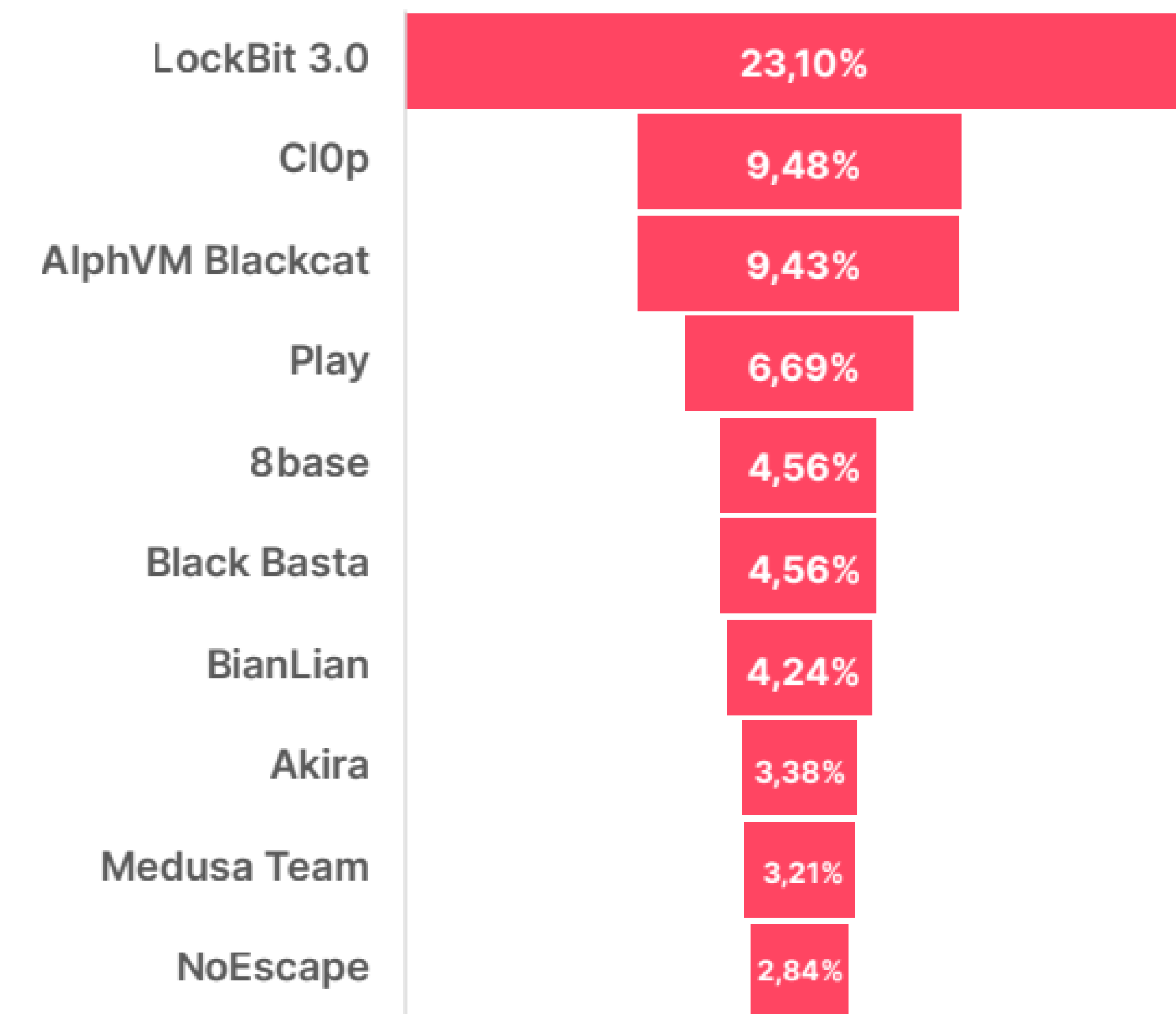


# 3) Trend towards Organised Cybercrime 網絡犯罪趨向組織化

## 全球勒索軟件攻擊



### ▶ Ransomware Group Activity Analysis

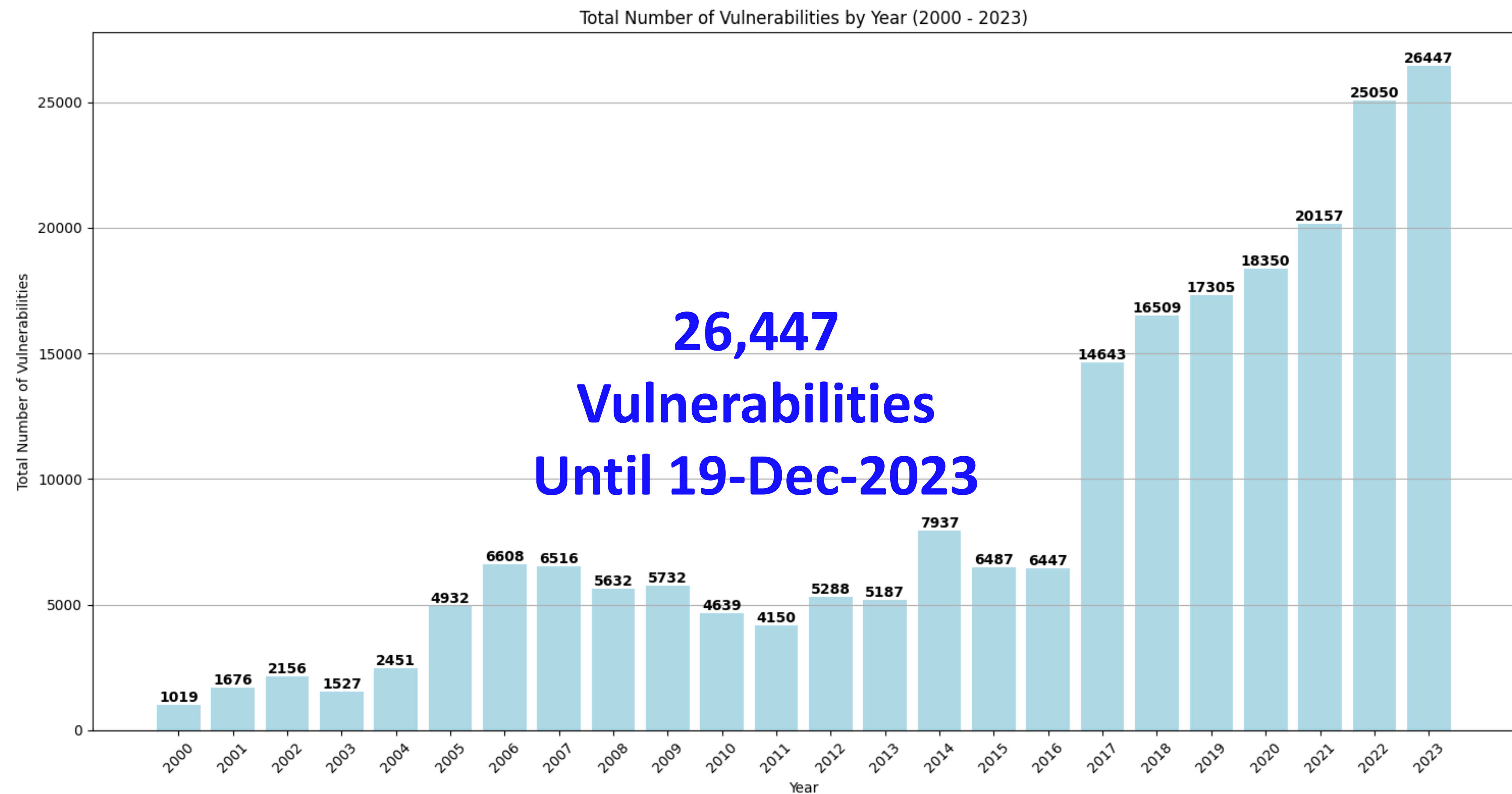


### 3) Trend towards Organised Cybercrime 網絡犯罪趨向組織化

## 2023年的漏洞數量再創新高

除釣魚攻擊外，另一種攻擊媒介就是利用漏洞

Project Zero顯示2023年有56個零日漏洞，而2022年只有41個





## 4) Attacks Arisen From Smart Devices 針對智能裝置的攻擊

智能設備是電子設備，一般可透過不同的無線協定與其他設備或網路連接



### 智能設備相關的安全風險

- 基於資源問題，小型廠商難以為產品持續更新，甚至可能是沒有任何更新。
- 基於硬件限制，部分智能設備無法設置安全措施。

# 4) Attacks Arisen From Smart Devices 針對智能裝置的攻擊

偽冒版 7-Zip 潛伏 Microsoft Store 被發現後已下架

快刪除！「12款APP」藏木馬病毒會偷扣錢 220萬用戶受害

三立新聞網  
2023年11月4日

科技中心 / 許智超報導



**40%**  
of surveyed cellphone users don't even take minimal security measures like screen lock, data backup, or a security app

商場無人機表演時失控墜落 圍觀群眾驚逃

新聞觀看次數：4.4k

23年09月27日(三) 01:00

推介 1

分享

Post

分享



東省淄博市周村區日前有商場進行無人機表演，開始不久後無人機受控制地從空中集體下降，甚至有少量無人機墜落、亂飛，嚇得群慌忙躲逃。商場物業工作人員表示，事件可能是信號干擾導致，無人受傷。

## 5) Third-party Risk 使用第三方服務的風險

### 使用第三方服務可引致IT供應鏈攻擊

由於外判IT服務，形成IT供應鏈。IT系統/項目可由不同的供應商組成，例如**第三方軟件公司、互聯網供應商**等等。

#### IT供應鏈攻擊帶來的後果

- 數據洩漏
- 惡意程式的感染

# Example: MOVEit Vulnerability

## 例子：MOVEit 漏洞

### 什麼是MOVEit?

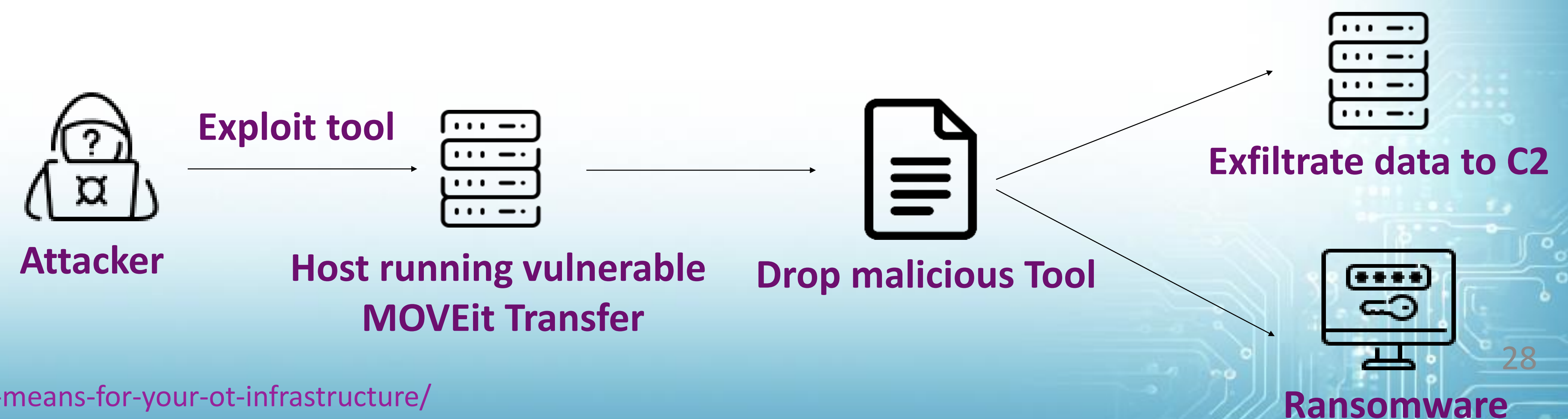
MOVEit 是一款託管式文件傳輸軟體，可提供安全及自動化的文件傳輸。MOVEit用戶可以安全及合符規管與外部收發文件。

### The Critical MOVEit Transfer Vulnerability and What it Means for Your OT Infrastructure

Aug 14, 2023

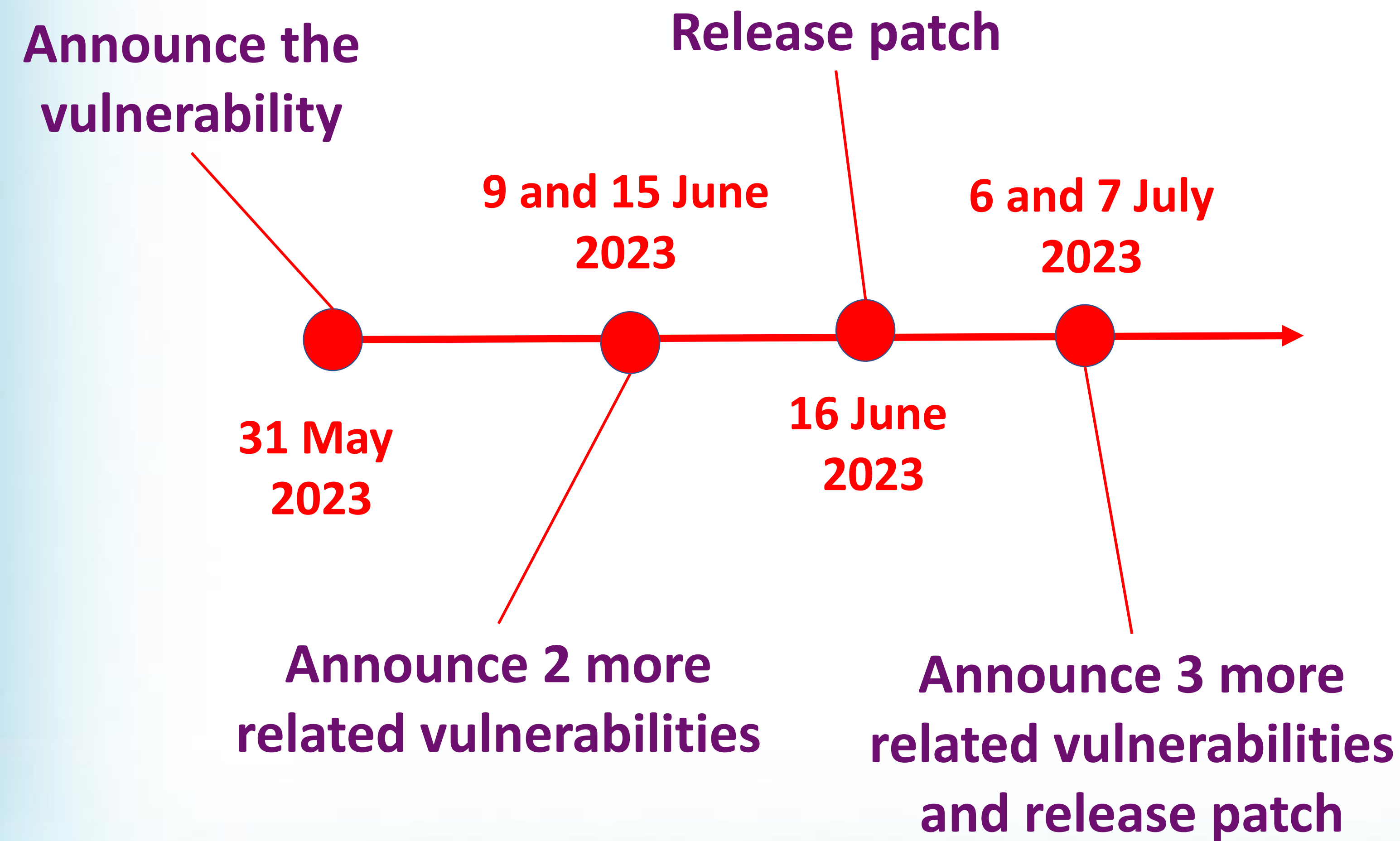
#### Background

As of August 8, roughly 600 organizations have fallen prey to a ransomware organization known as CL0P (TA505) whose latest extortion scheme involves the exploit of a zero-day SQL injection vulnerability within MOVEit Transfer, a Managed File Transfer (MFT) application developed by Progress Software Corporation. MOVEit Transfer is used extensively by organizations around the globe for the purpose of automated, secure file transfer and sharing. In their attack, the CL0P Gang leaves a ransom note on the MOVEit Transfer server and threatens to publish sensitive exfiltrated data on Tor if the ransom is not paid.

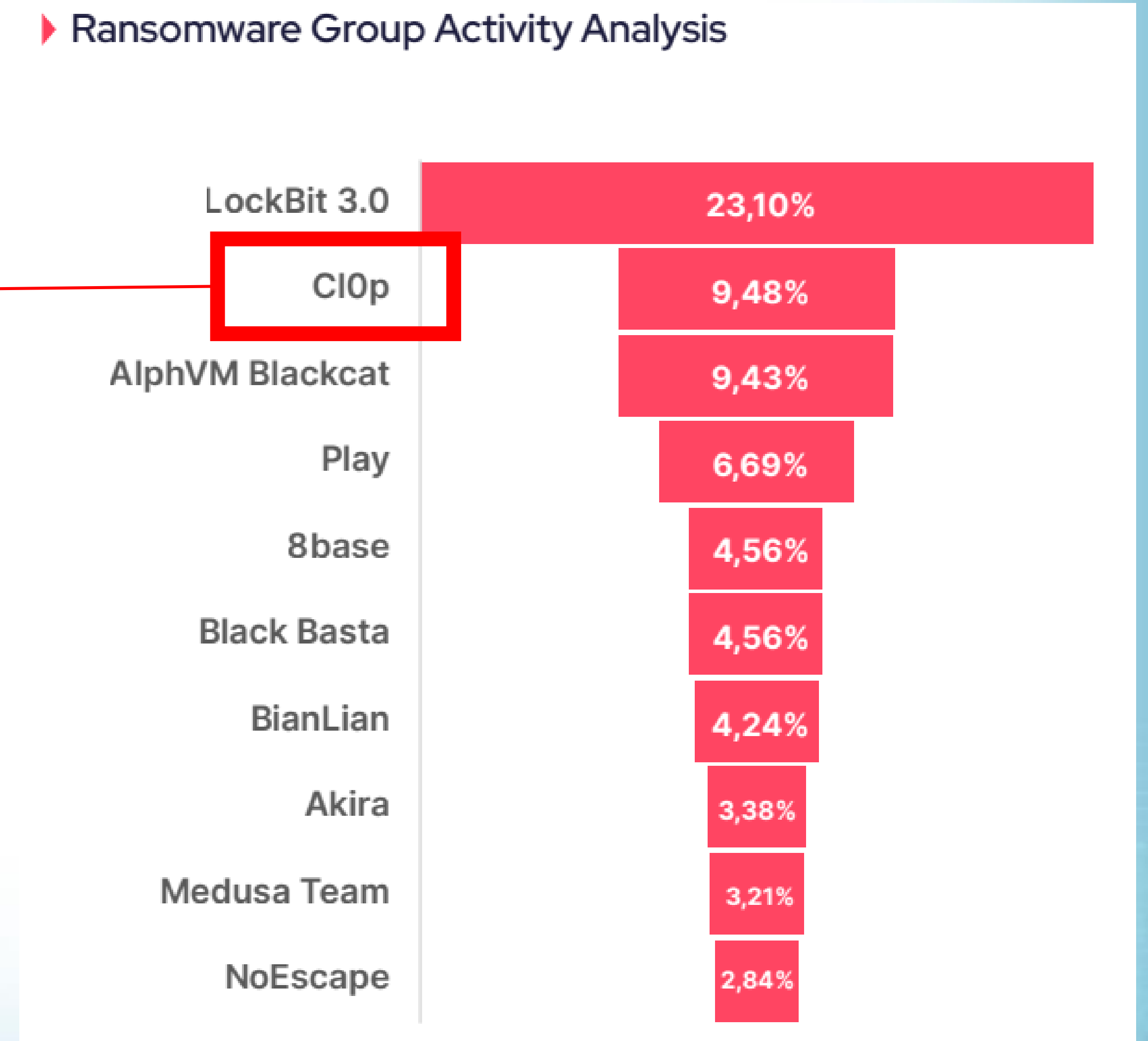


# MOVEit Vulnerability MOVEit 漏洞

MOVEit 漏洞是一個SQL漏洞, 同時是零日漏洞



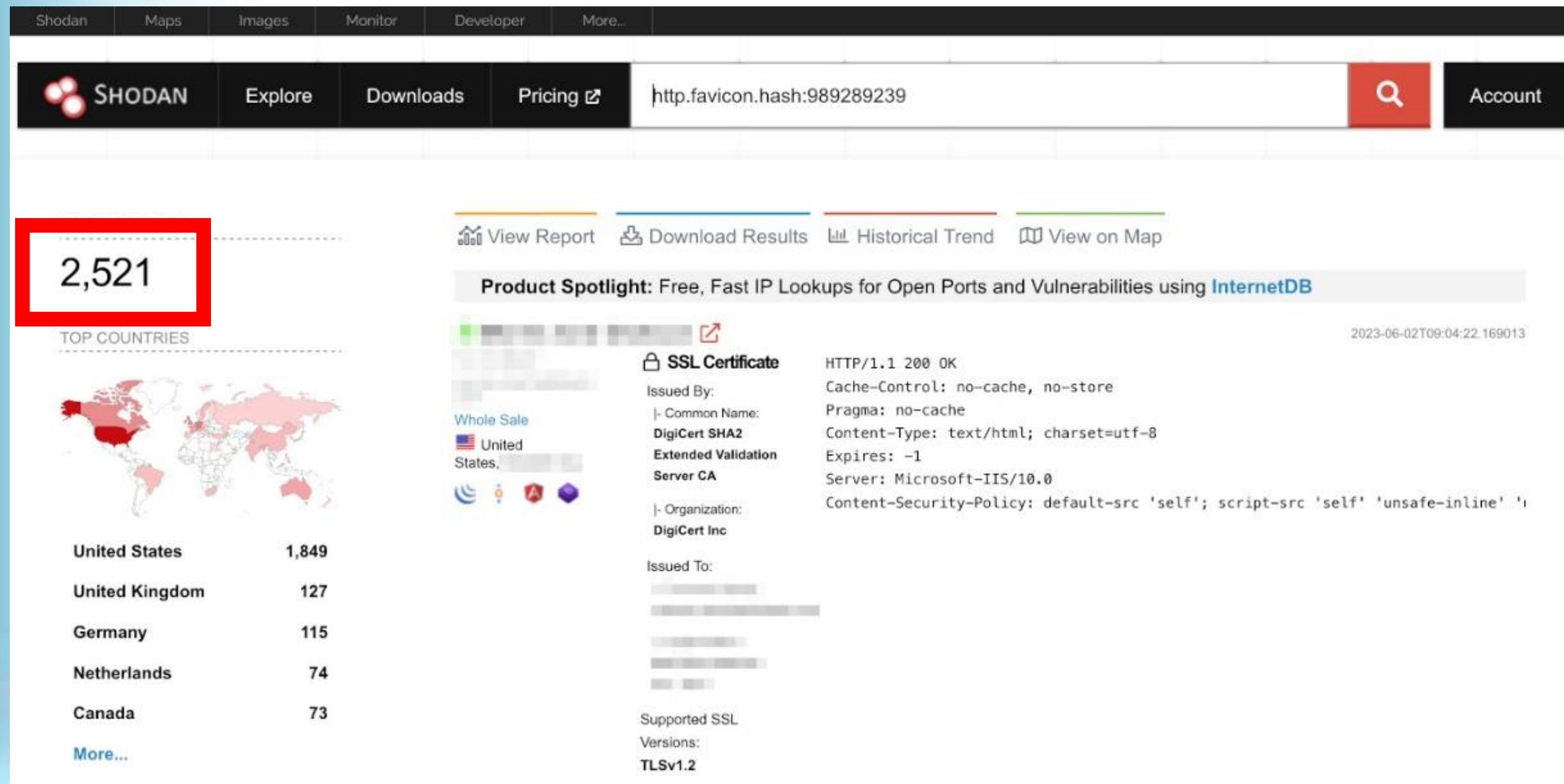
Cl0p 勒索軟件集團廣泛利用MOVEit漏洞



# Victims from MOVEit Vulnerability

## MOVEit 漏洞的受害人

全球超過2,500企業正在使用MOVEit應用



### Deloitte joins fellow Big Four MOVEit victims PWC, EY

Updated on: November 15, 2023 12:53 PM



**Sony Breached Via MOVEit Zero-Day Vulnerability**



## 5) Third-party Risk 使用第三方服務的風險

### 依賴第三方服務可引致內部網絡安全風險

IT外判服務亦包含人力資源的外判，例如經第三方僱用一些臨時IT人員以應付公司的過渡發展。這些外判人員有機會為公司內部帶來網絡安全風險。

以下是其中原因

- 對於內部與外判員工管控措施不一致
- 給予外判員工過高權限


3

# Cyber Security Tips


## 網絡保安小貼士

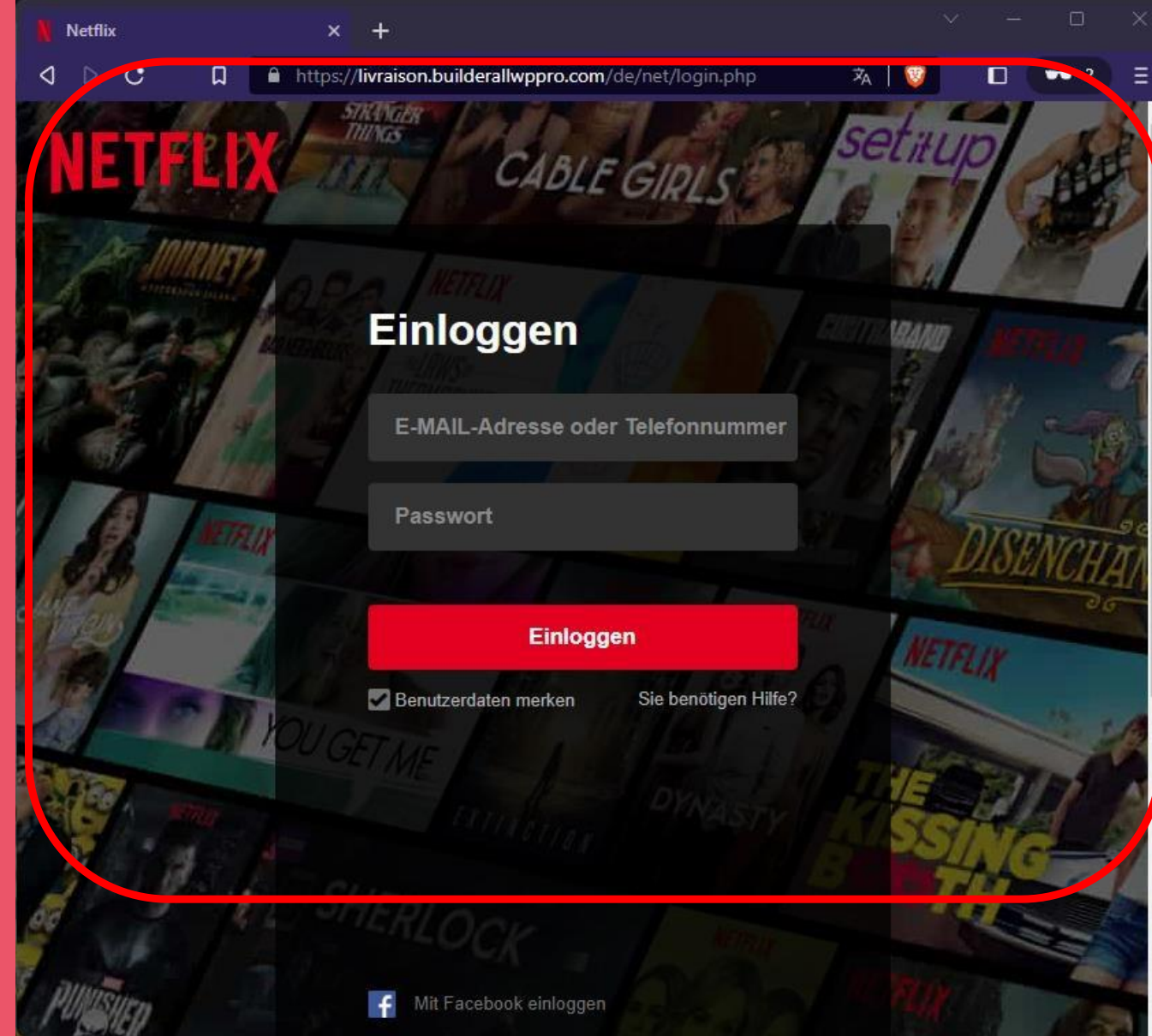


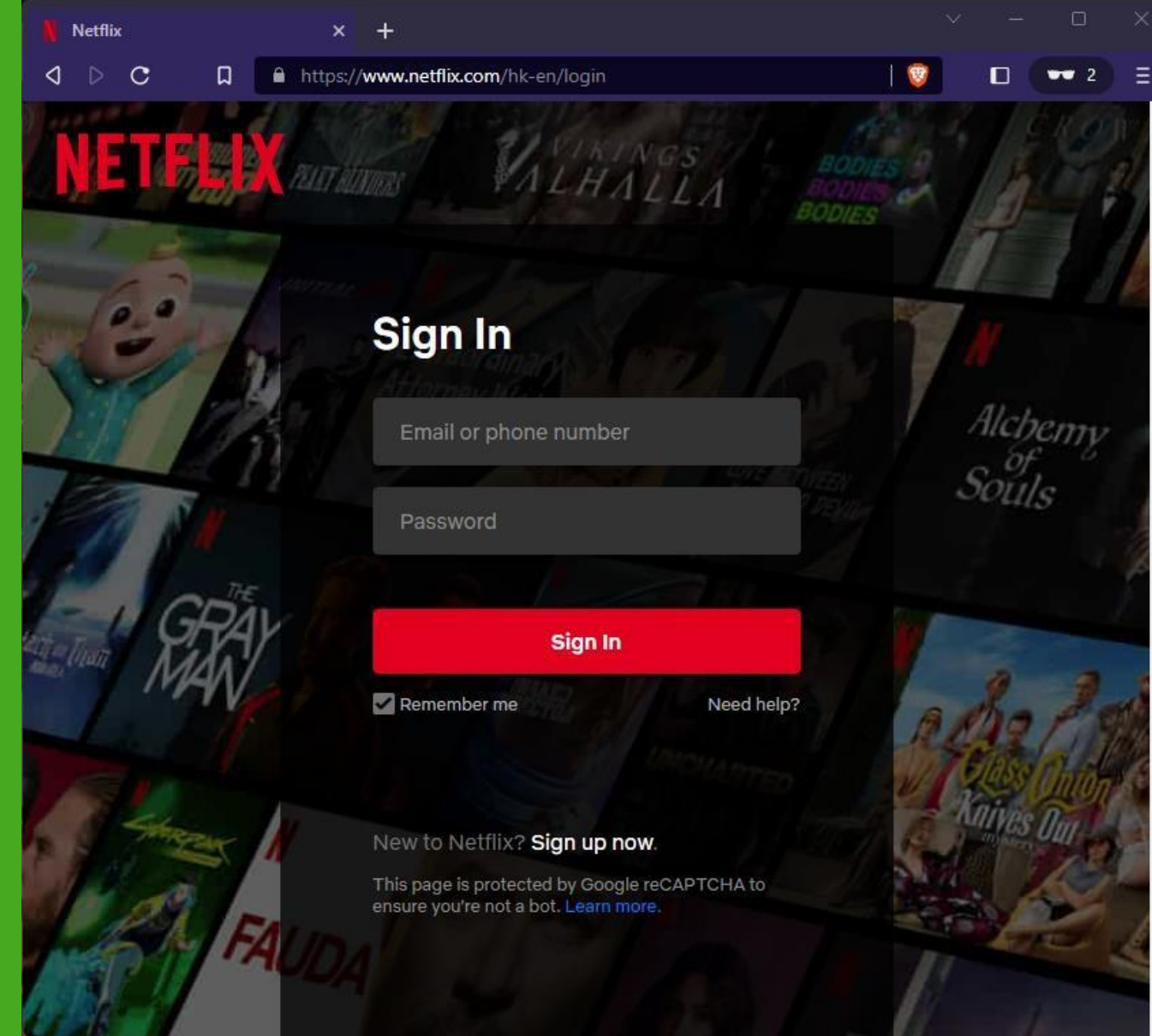
# Tips to spot phishing 洞悉釣魚攻擊小貼士




**複製真實網站界面**  
Replication of legitimate site




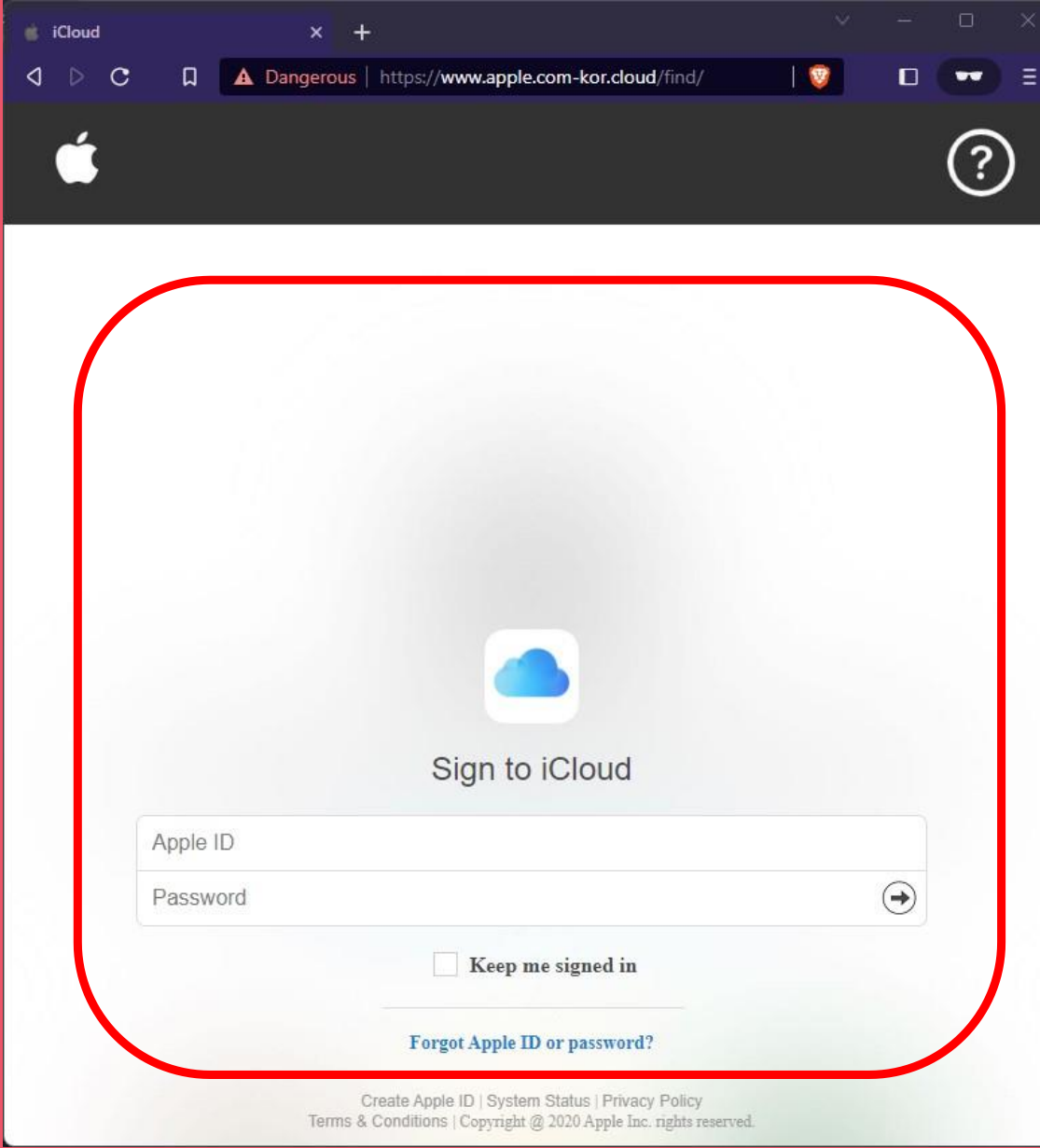


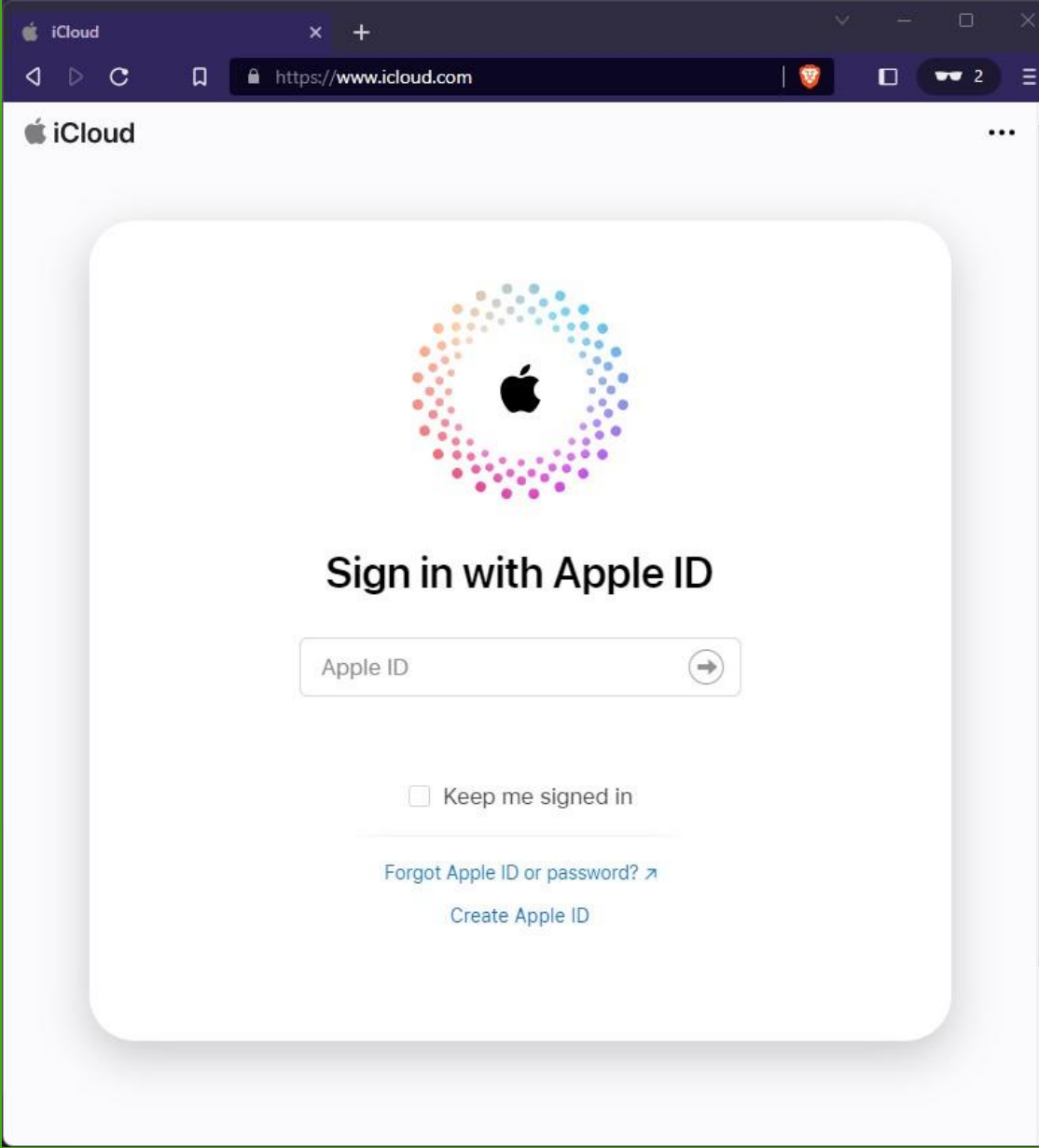





**視覺設計不佳**  
Poor visual design




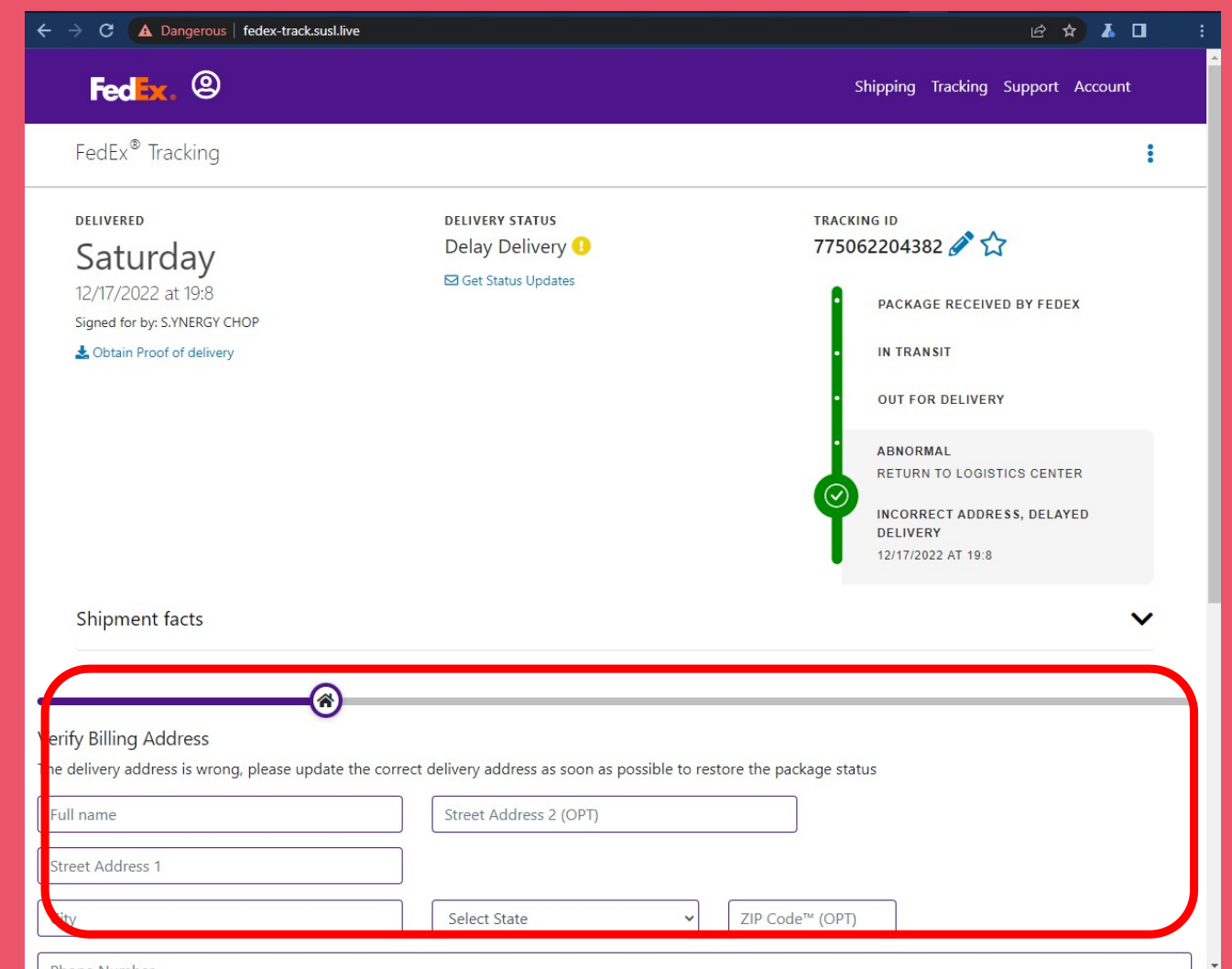


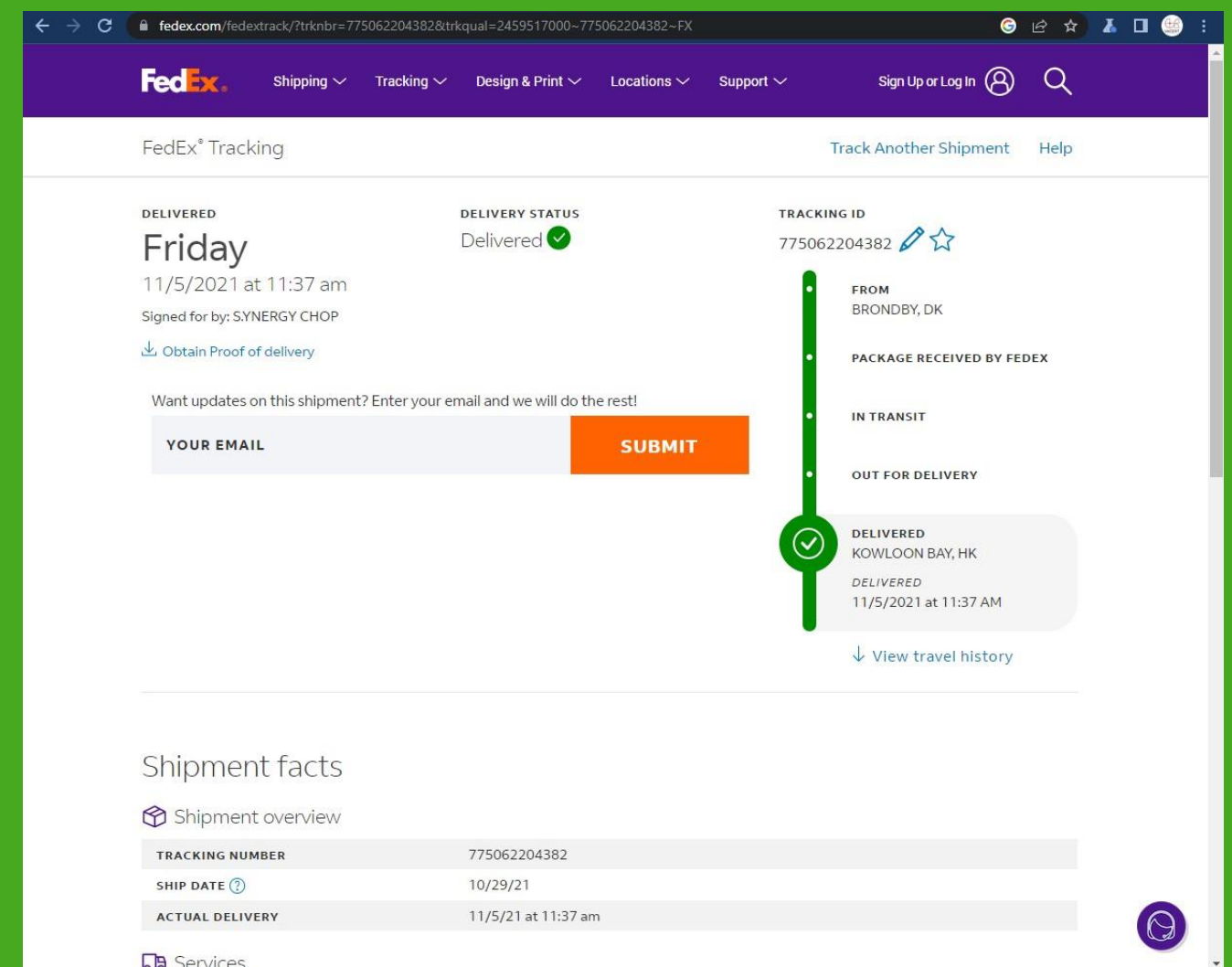





**意圖竊取個人 / 敏感資料**  
Intent to steal personal/sensitive data




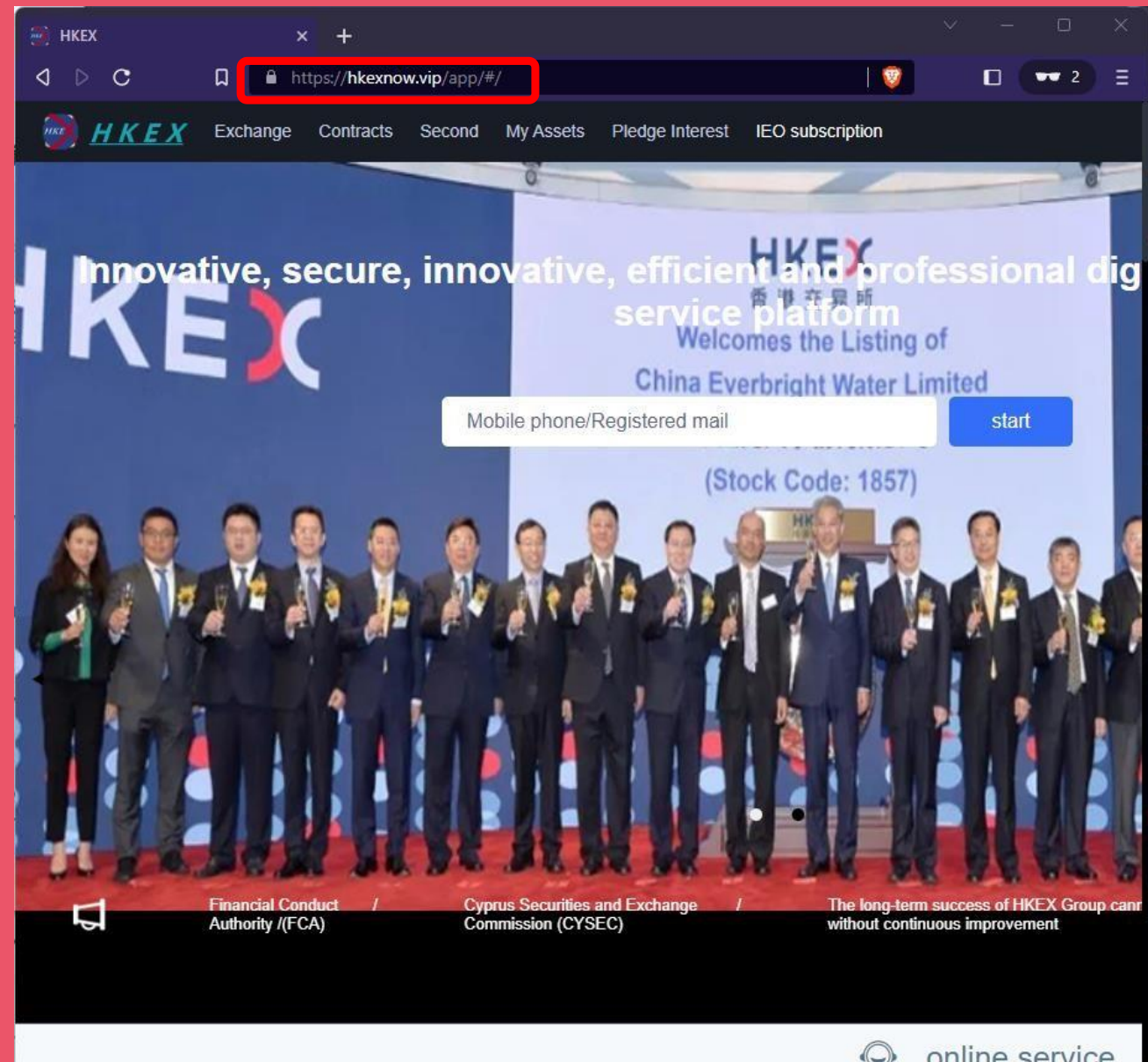


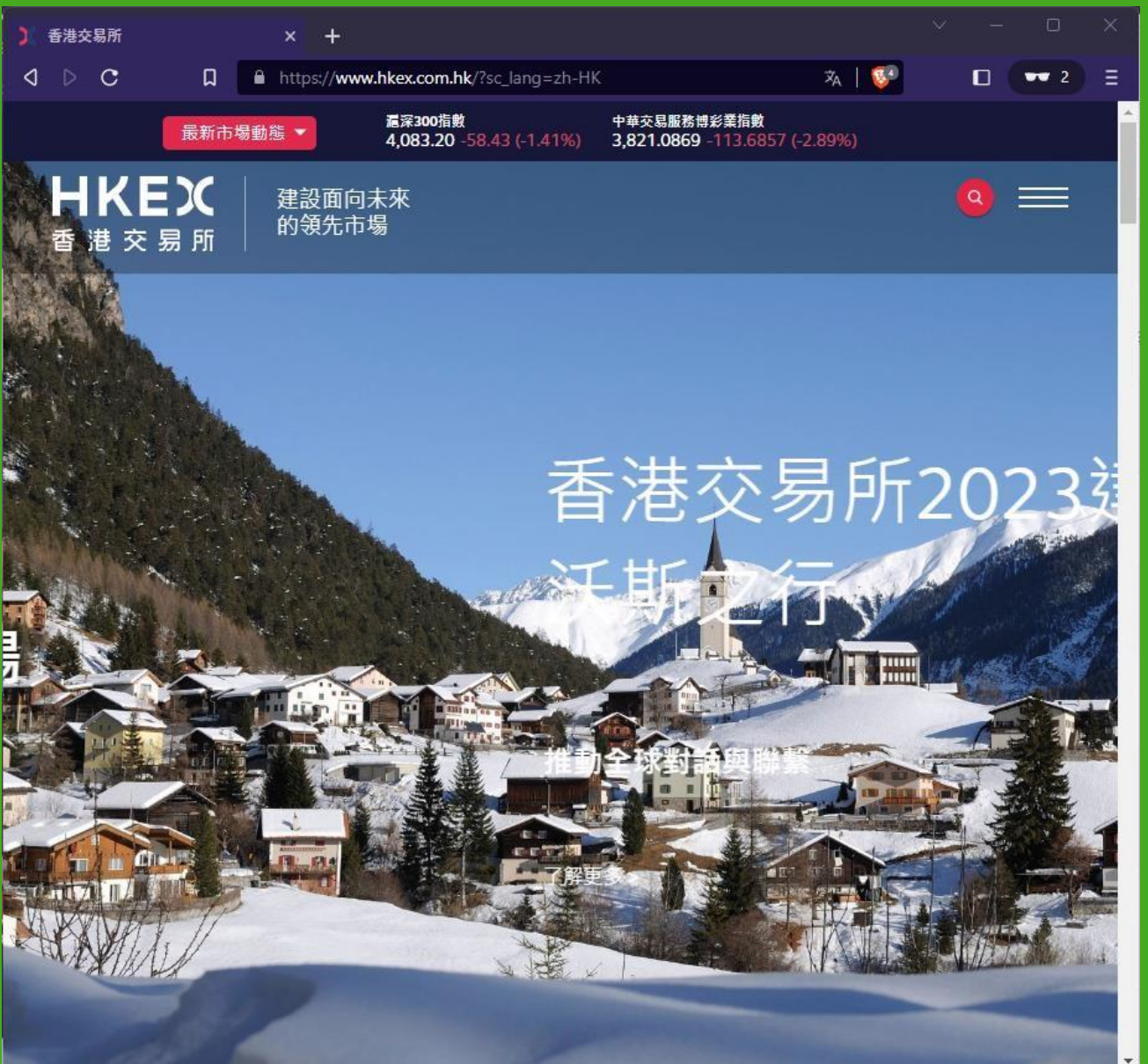




**與真實網址相似**  
Similar domain name



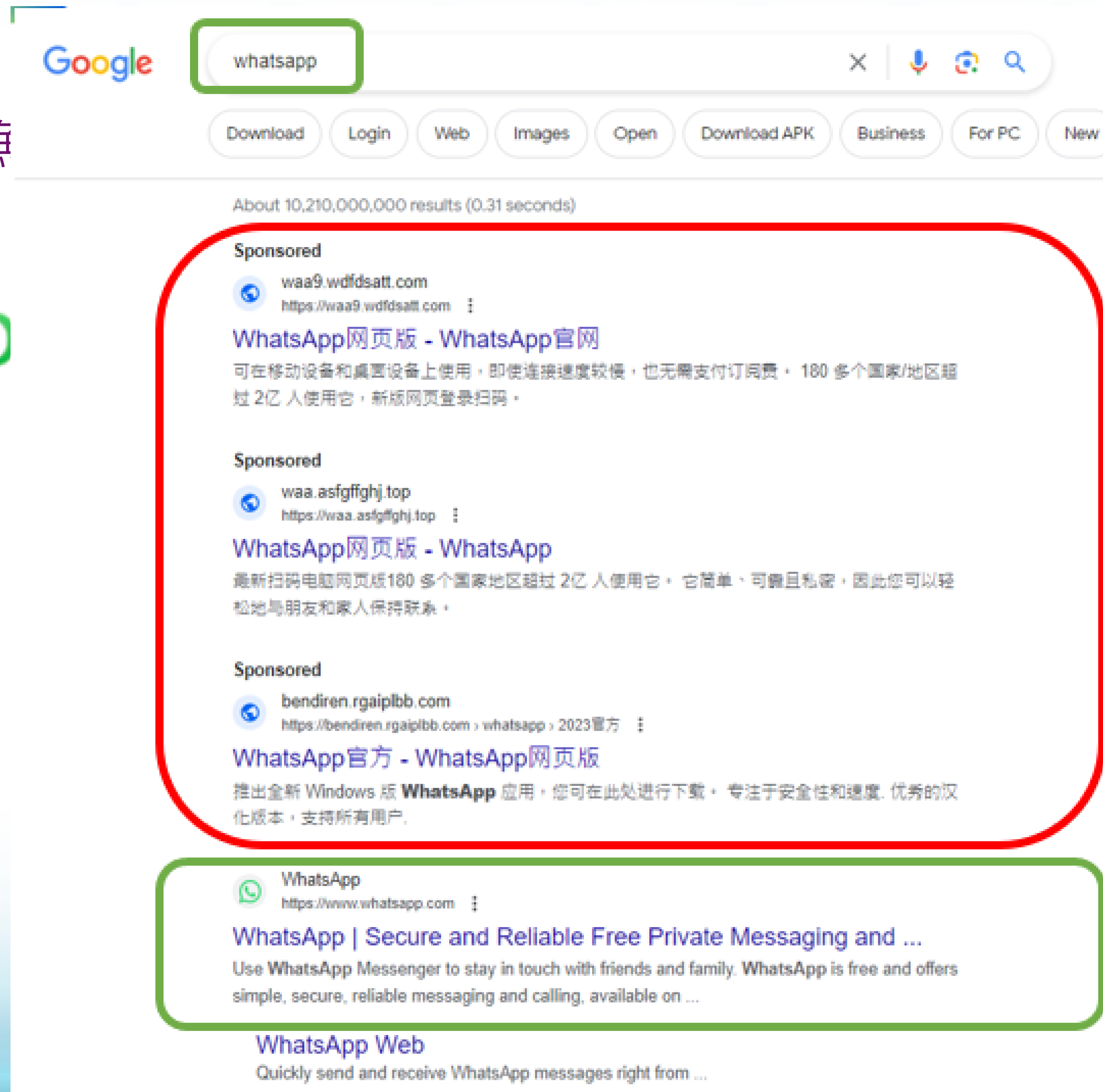




資料來源 Source: [https://www.hkex.com.hk/Global/Exchange/Alert?sc\\_lang=zh-HK](https://www.hkex.com.hk/Global/Exchange/Alert?sc_lang=zh-HK)

# Mistaken idea of phishing site 釣魚網站謬誤

很多釣魚



Google search results for 'whatsapp'. The search bar shows 'whatsapp' and the results include:

- Sponsored**  
waa9.wdfdsatt.com  
https://waa9.wdfdsatt.com  
WhatsApp网页版 - WhatsApp官网  
可在移动设备和桌面设备上使用，即使连接速度较慢，也无需支付订费。180 多个国家/地区超过 2亿 人使用它，新版网页登录扫码。
- Sponsored**  
waa.asfgfghj.top  
https://waa.asfgfghj.top  
WhatsApp网页版 - WhatsApp  
最新扫码电脑版180 多个国家地区超过 2亿 人使用它，它简单、可靠且私密，因此您可以轻松地与朋友和家人保持联系。
- Sponsored**  
bendiren.rgaipbb.com  
https://bendiren.rgaipbb.com › whatsapp › 2023官方  
WhatsApp官方 - WhatsApp网页版  
推出全新 Windows 版 **WhatsApp** 应用，您可在此处进行下载，专注于安全性和速度。优秀的汉化版本，支持所有用户。
- WhatsApp**  
https://www.whatsapp.com  
WhatsApp | Secure and Reliable Free Private Messaging and ...  
Use WhatsApp Messenger to stay in touch with friends and family. WhatsApp is free and offers simple, secure, reliable messaging and calling, available on ...
- WhatsApp Web**  
Quickly send and receive WhatsApp messages right from ...

搜索结果：  
釣魚網站

真實的網站

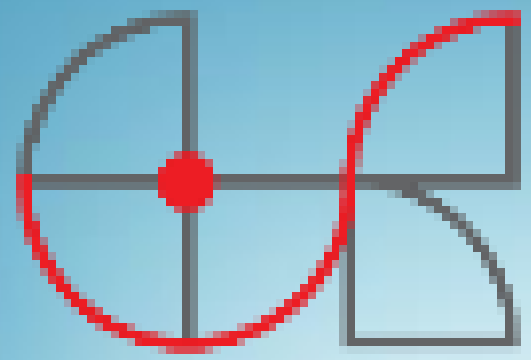
但只有域名部份是獨有

scribe/entry

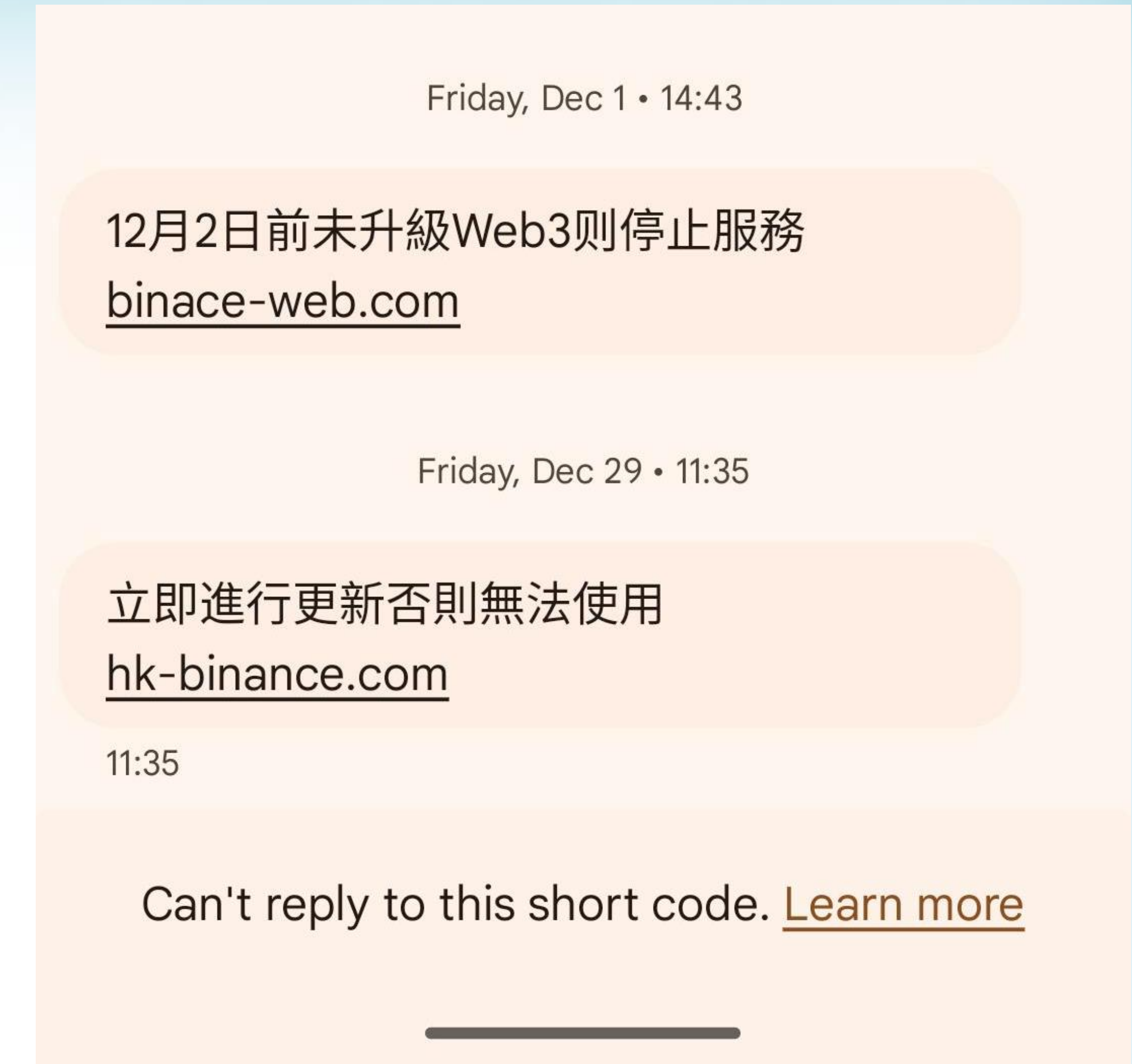
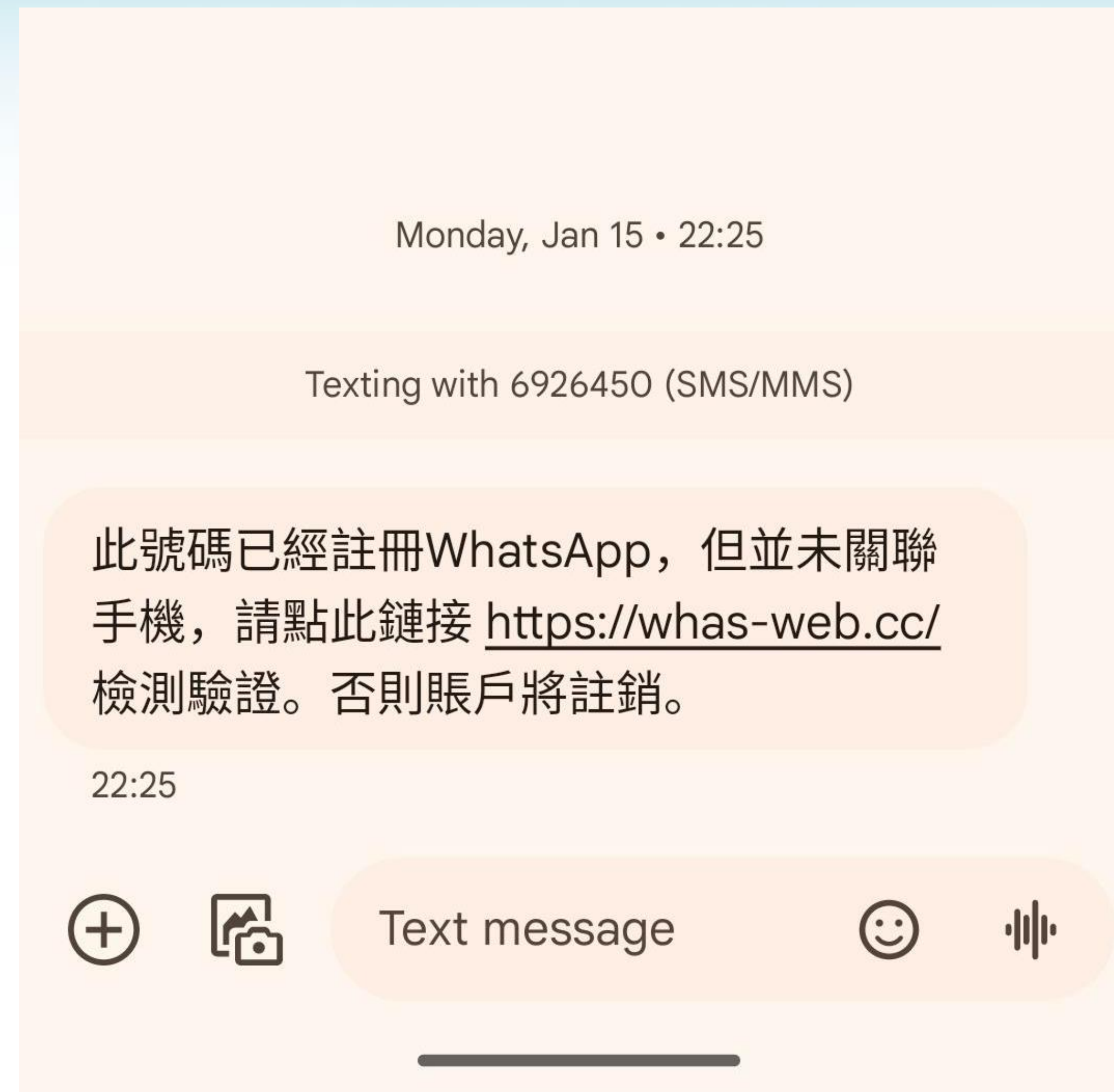
路徑

區來註冊獨有的專屬域  
分商業機構會用 .com，非  
會再加 .hk等。

用戶。換句話說，檢查域



HKCERT



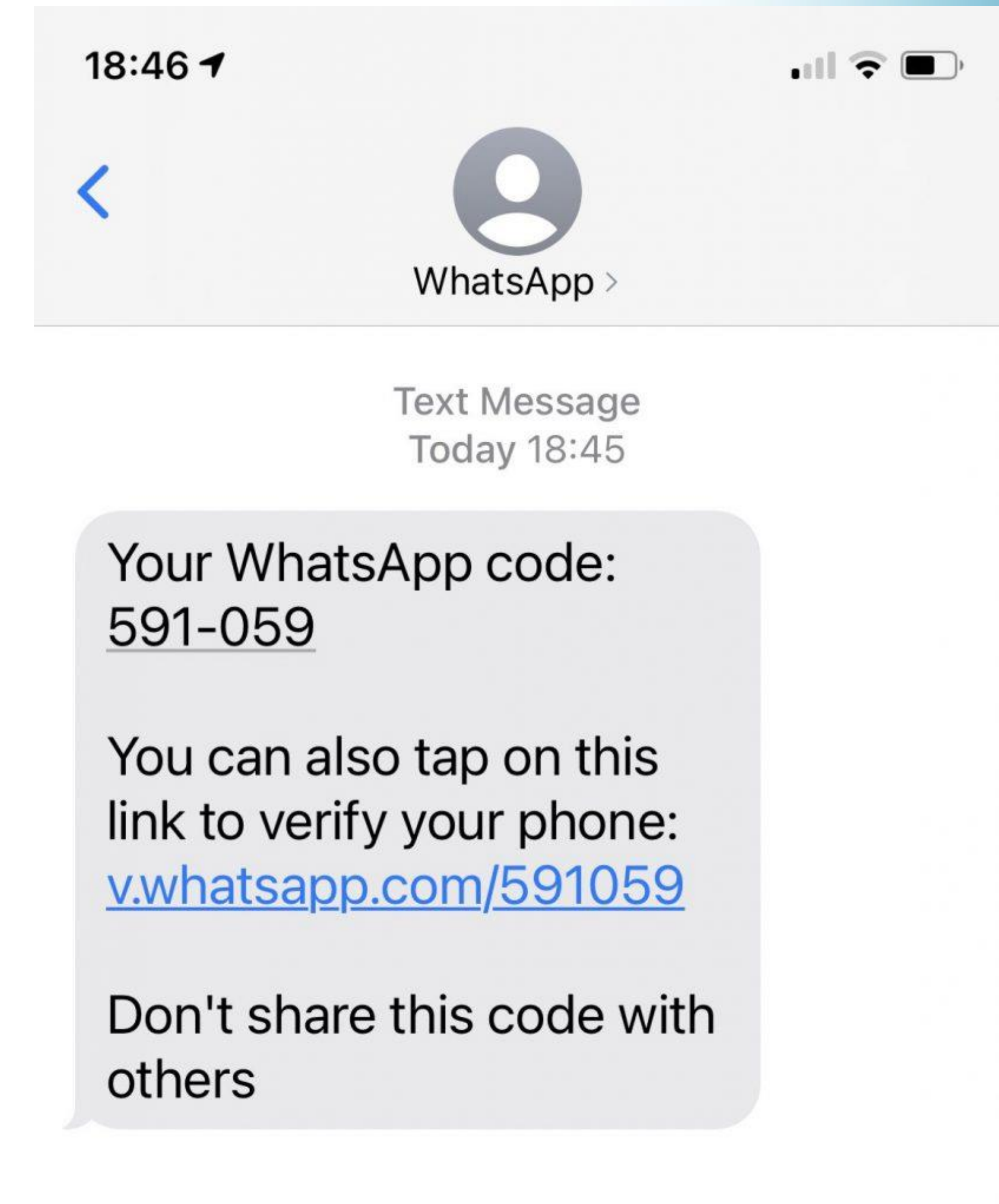
## SMS Phishing Example

## SMS釣魚訊息

# Preventing WhatsApp account theft

## 預防WhatsApp帳號盜用

1. 啟動**雙重認證功能**並設定PIN碼。
2. 設定一個**電郵地址**，以便日後有需要時重設PIN碼。
3. **切勿與他人分享**登入驗證碼和雙重認證PIN碼。
4. 定期在WhatsApp設定中檢查**已連結裝置**，並登出不再使用的裝置連結。
5. 切勿從**非官方渠道**下載及使用WhatsApp應用程式。

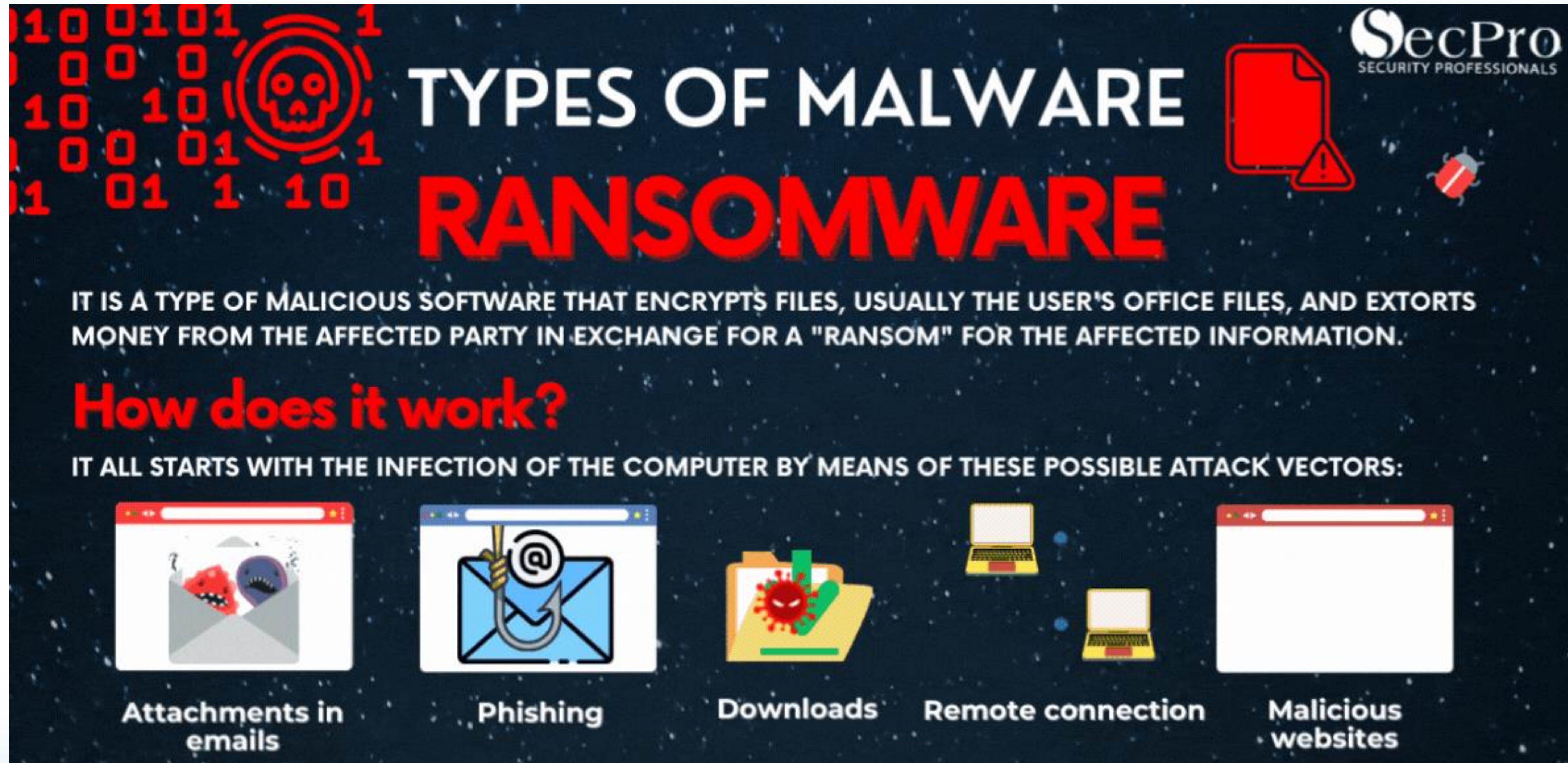


# Tips to Detect DeepFake 預防深度偽造小「貼士」



# Understanding Ransomware

## 了解勒索軟件



**TYPES OF MALWARE**  
**RANSOMWARE**

IT IS A TYPE OF MALICIOUS SOFTWARE THAT ENCRYPTS FILES, USUALLY THE USER'S OFFICE FILES, AND EXTORTS MONEY FROM THE AFFECTED PARTY IN EXCHANGE FOR A "RANSOM" FOR THE AFFECTED INFORMATION.

**How does it work?**

IT ALL STARTS WITH THE INFECTION OF THE COMPUTER BY MEANS OF THESE POSSIBLE ATTACK VECTORS:

- Attachments in emails
- Phishing
- Downloads
- Remote connection
- Malicious websites

# Flow of Ransomware Attack

## 勒索软件的攻击流程

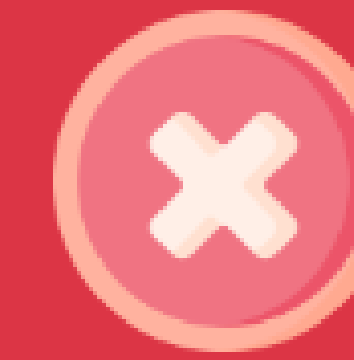


# Tips to prevent Ransomware Attack

## 預防勒索軟件攻擊小貼士

1. 只在官方網站或渠道下載應用程式
2. 安裝防毒軟件及保持更新 & 經常更新系統及應用程式
3. 只使用可信的網絡及裝置
4. 提防網絡釣魚攻擊

### 不應該 X



- ▶ 不要支付贖金，因為這只會對勒索軟件集團助紂為虐；
- ▶ 不要使用網上未經認證的解密軟件，以防感染其他惡意軟件；
- ▶ 未清理惡意軟件前不要開啟任何檔案，及
- ▶ 如果系統沒有備份，建議用戶暫時不要重裝系統，以免令加密檔案記錄資料丟失。

### 應該 ✓



1. 切斷受感染的電腦的所有網絡連接，包括網路（LAN和WiFi）和外置裝置（USB或外置硬碟），以避免進一步感染其他電腦；
2. 如要進行解密，可以參考以下步驟：
  - 2.1. 可在 <https://www.nomoreransom.org/en/decryption-tools.html> 搜索解密工具；
  - 2.2. 將已被加密的檔案複製到一個儲存裝置；
  - 2.3. 在一部沒有受到感染的電腦上使用解密工具來解密；
  - 2.4. 解密工具的使用步驟可參考對應的說明指示。
3. 下載清除軟件，並執行完整掃描來清除惡意程式；
4. 如果在感染前已為系統或資料建立備份，用戶可進行系統及數據回復；
5. 使用入侵檢測來查找漏洞以及攻擊是如何發生的。進行全面的保安掃描，及時加強保安防護；
6. 向 HKCERT 求助



# Data Protection Strategies

## 資料保護策略



### 權限控制

- ✓ 最低權限
- ✓ 以角色為基礎的存取控制
- ✓ 多重身份驗證
- ✓ 加密



### 漏洞管理

- ✓ 定期更新最新軟件補丁
- ✓ 定期進行漏洞掃描和滲透測試練習



### 用戶意識

- ✓ 提供定期保安意識培訓
- ✓ 最新網路安全資訊

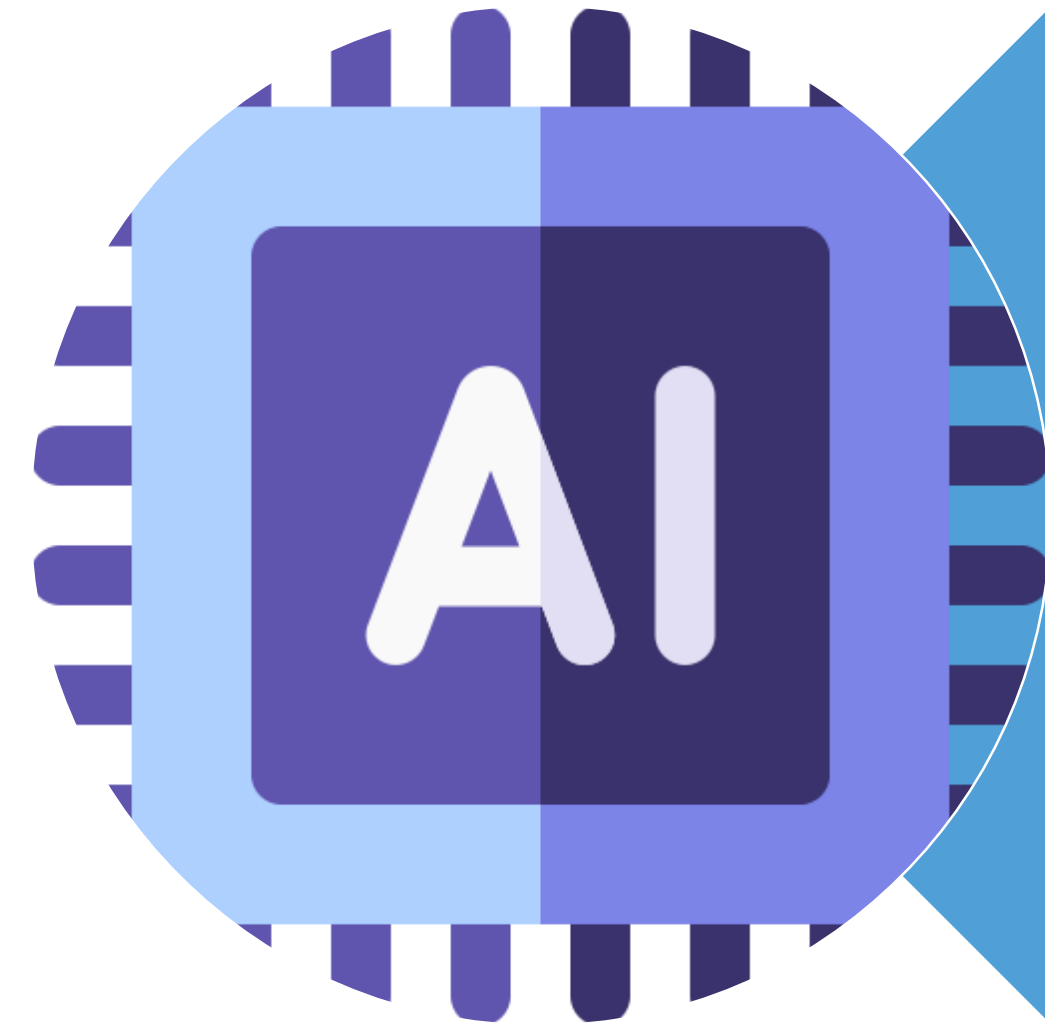
4

Summary  
重點總結

# 5 Key Information Security Risks to be Aware of in 2024

## 2024 年必須留意的五大保安風險

人工智能被「武裝化」



- 制定策略應對新科技帶來的風險
- 小心保護個人資訊；利用先進AI技術，只需小量的個人資訊，便足以複製身份

新一代釣魚攻擊



- 多加注意搜尋引擎的最佳結果，因為它們都可以是可疑網站
- 注意網站域名的英文串法以防範釣魚網站

# 5 Key Information Security Risks to be Aware of in 2024

## 2024 年必須留意的五大保安風險

### 網絡犯罪趨向組織化



- 定期進行網絡及系統保安檢查及更新

### 針對智能裝置的攻擊



- 更改設備的預設密碼及保持更新設備
- 加強智能設備的安全措施，尤其是自攜裝置

### 使用第三方服務的風險



- 統一內部及外部的網絡安全策略

# Cyber Security Tips

## 網絡保安小貼士



檢查寄件者的電郵地址域名



檢查內文的連結域名



檢查被引領至的網站



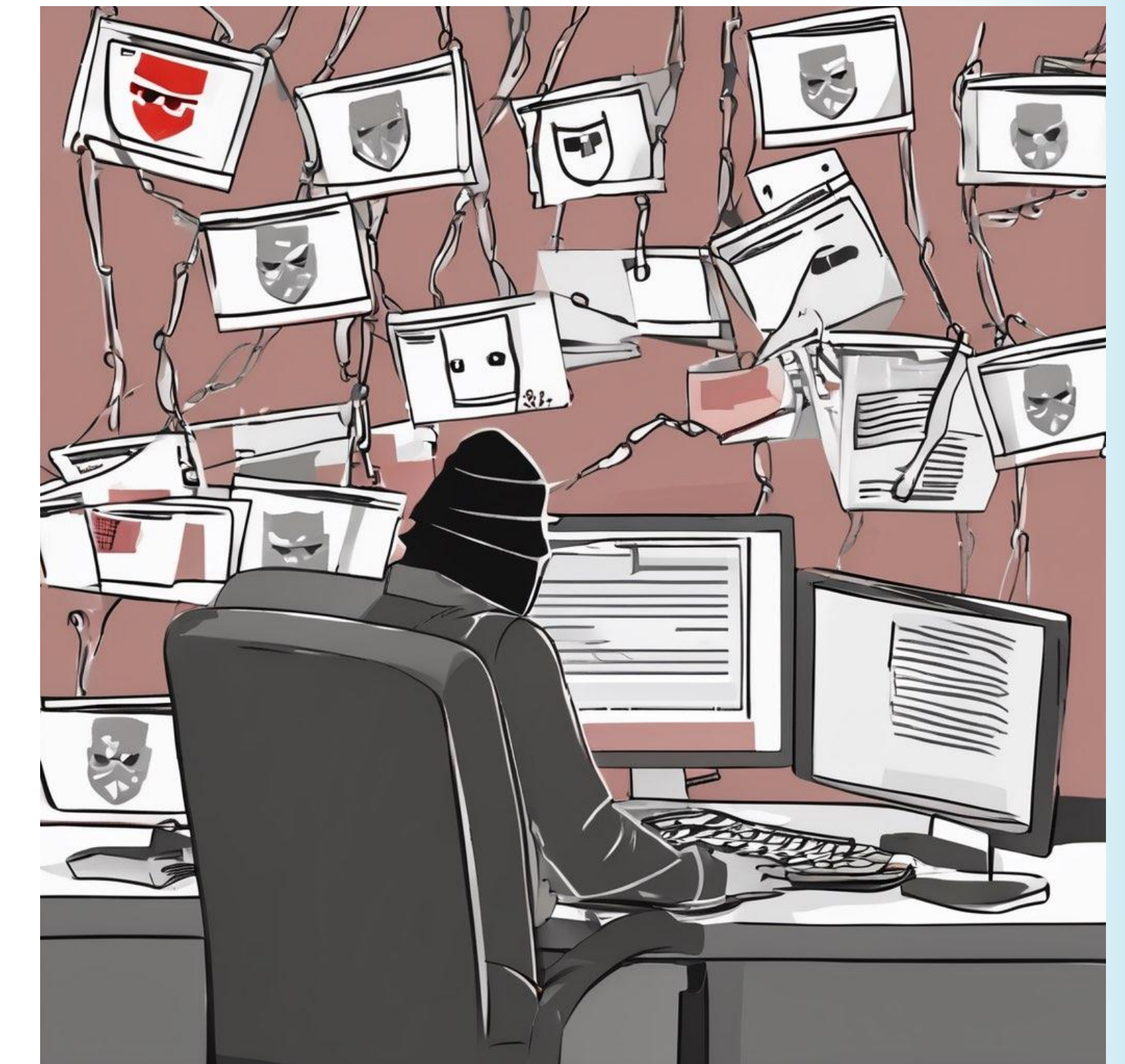
提防及掃描下載的檔案



帳戶應使用高強度密碼及雙重認證



安裝防毒軟件及保持更新 & 經常更新系統及應用程式



圖片由人工智能產生

# HKCERT Publication for Data Protection



The screenshot shows the HKCERT website interface. At the top, there is a navigation bar with the text "Latest Security Bulletins" on the left and "Google Chrome Multiple Vulnerabilities" on the right. Below this, the HKCERT logo and name are displayed on the left, and a search bar, social media icons, and an "Incident Reporting" button are on the right. The main content area features a breadcrumb trail: "Home > Publications > Security Guideline >". The title "Data Protection Guideline" is prominently displayed, followed by the release date "6 May 2022" and the view count "10891 Views". A large, glowing blue shield icon with a keyhole is centered on a background of digital data and circuitry. Below the image, the introductory text reads: "The recent incidents of personal information leakage have attracted much public attention. Have you been worrying about your own data privacy? Do you know what risks are associated with storing data on the computer? What measures are available to mitigate these risks? This guideline is divided into four sections:"



Data Protection Guideline

# HKCERT Publication for Ransomware

<🔒/> NO MORE RANSOM

Decryption  
Tools



No More Ransom

Home Crypto Sheriff Ransomware: Q&A Prevention Advice **Decryption Tools** Report a Crime

Partners About the Project English

Latest Security Bulletins

Linux Kernel Multiple Vulnerabilities

Microsoft Edge Multiple Vulnerabilities

Hong Kong Computer  
Emergency Response Team  
Coordination Centre  
香港電腦保安事故協調中心

Incident Reporting

IMPORTANT! Before downloading and starting the solution, read the how-to guide from your system first, otherwise it will repeatedly lock your system or erase data. Read this for you.

Quick Search...

> 777 Ransom

> AES\_NI Ransom

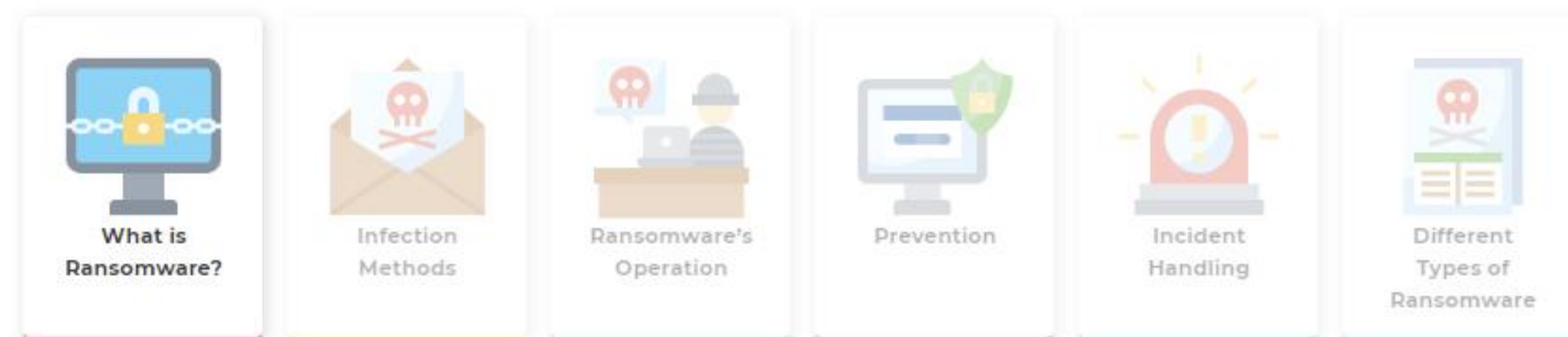


Ransomware Basic

Blog

Tools

Resources

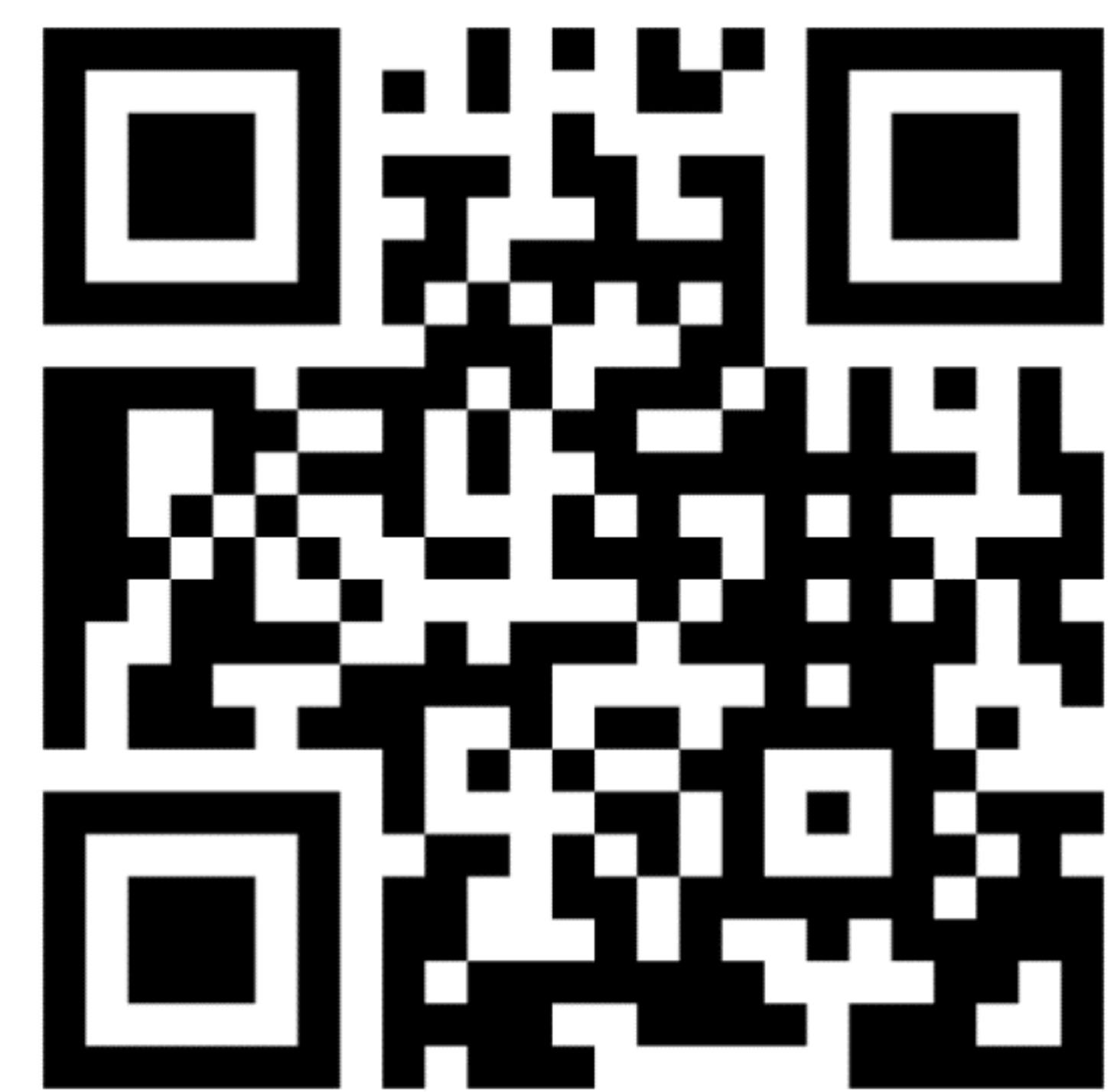


What is Ransomware? .

Ransomware is a type of malware threat actors used to encrypt all the files of the victim and hold data



Fight Ransomware



[www.hkcert.org](http://www.hkcert.org)  
8105 6060  
[hkcert@hkcert.org](mailto:hkcert@hkcert.org)



