

# 你知道什麼是身分盜用嗎?

趙汝輝先生  
資訊保安分析員  
香港電腦保安事故協調中心





# 內容

1. 身份認證

2. 身份盜用常見手法

3. 保安建議



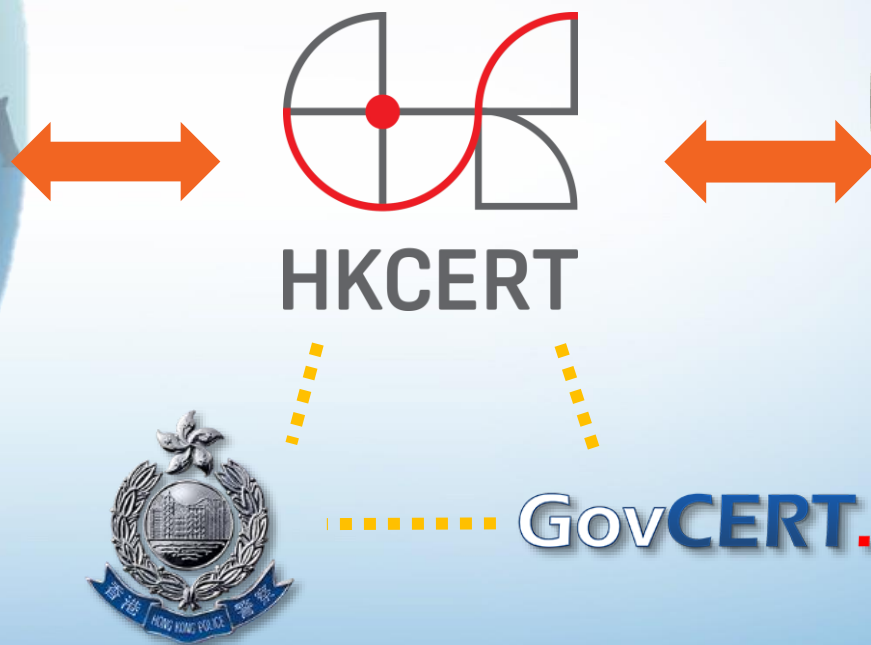
# 國際

# 本地

交換保安事故和資訊

協調保安事故及發佈警示

## HKCERT 作為樞紐



## 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

# 身份認證

# facebook

登入 Facebook

登入

[忘記帳號？](#)

或

建立新帳號

## Log on to Hang Seng Personal e-Banking



We've introduced customers to the new way to log on.  
[Learn how this new log-on method makes your online banking safer](#)

Enter your username ⓘ

▲ Please enter your username

Continue

[Forgot your username >](#)

[Haven't registered for Personal e-Banking >](#)

登入



Facebook



電子郵件信箱，使用者名稱或手機號碼

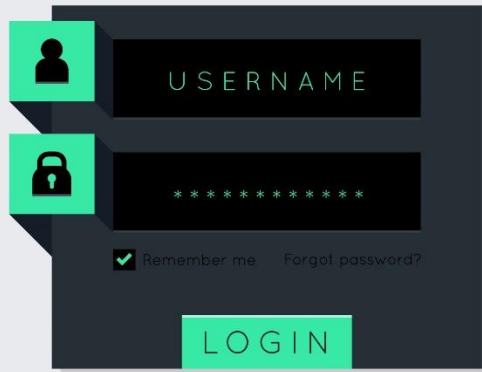
還沒有帳號嗎？[建立帳號](#)

# 身份認證

目的: 確保用戶有權瀏覽這些內容或使用服務

	現實世界 (例子：香港居民身份)	網上世界 (例子：Facebook用戶)
簽發方	 <p>中華人民共和國香港特別行政區政府 入境事務處</p>	
身份證明		<p>帳戶名稱和密碼</p>
認證方	<p>執法人員</p>	

# 身份證明方式



designed by freepik.com

Something you know



Touch ID

Something you are



designed by freepik.com

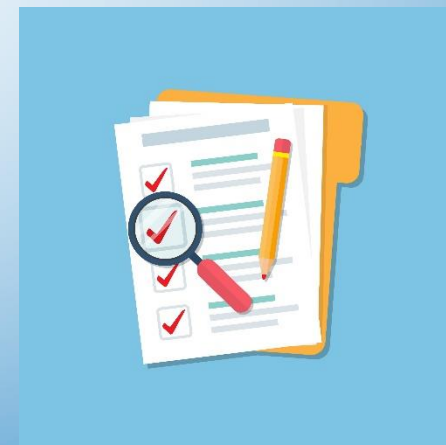
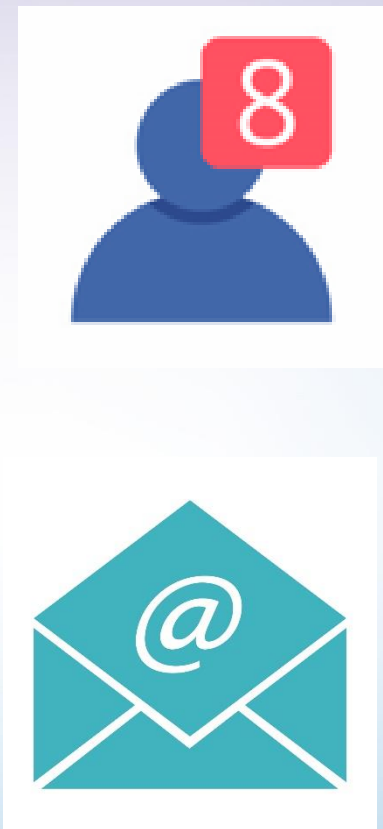
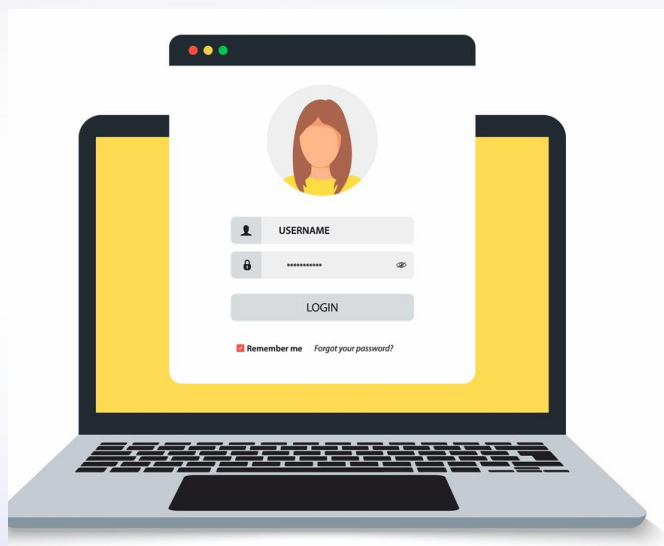
Something you have



2

# 身份盜用常見手法

# 數碼身份就是資產

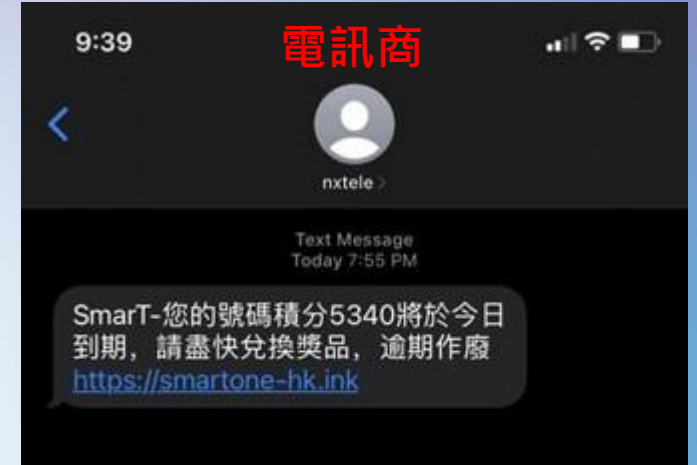


# 網絡釣魚

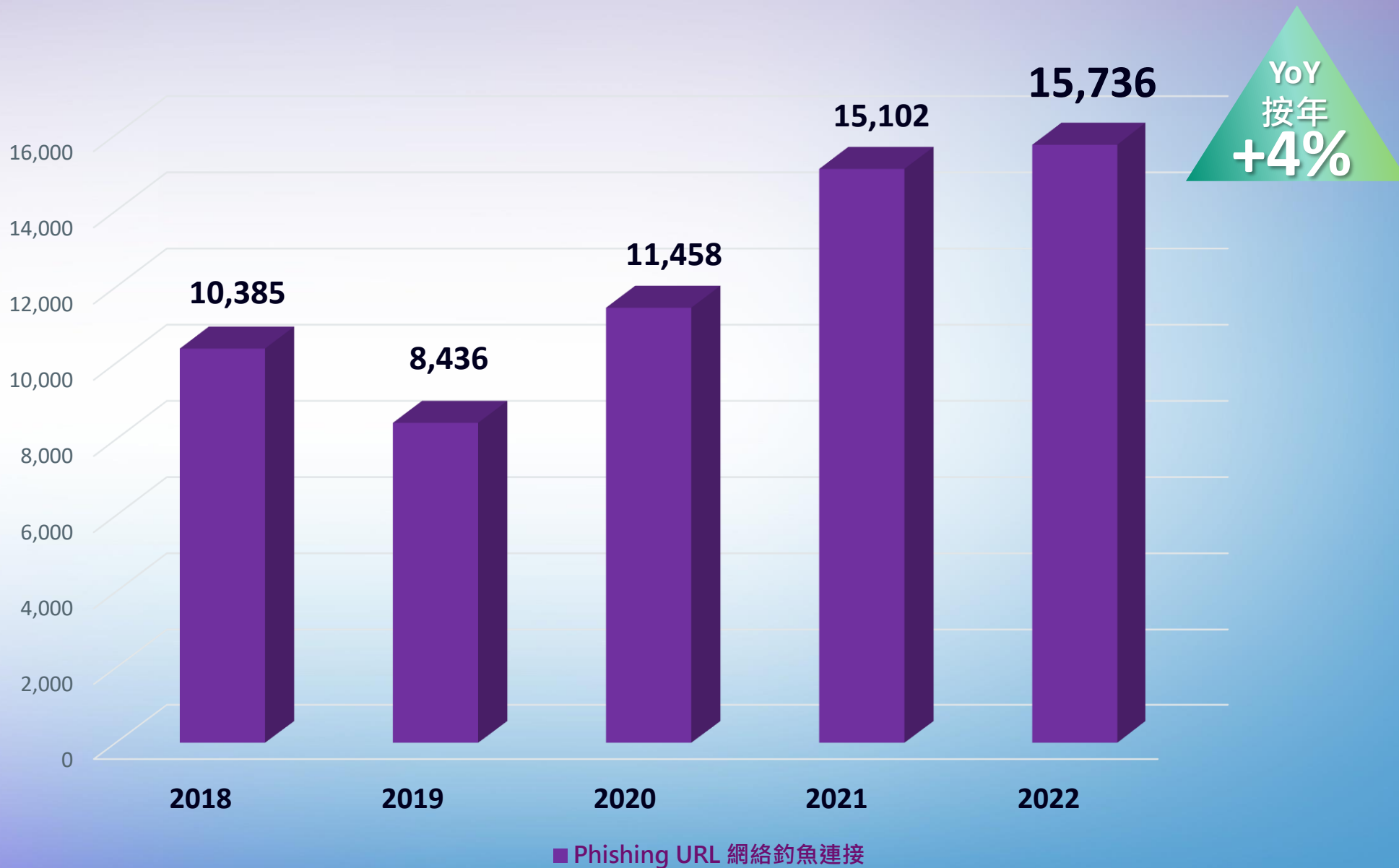
## 公共服務



## 支付平台



# 網絡釣魚所涉及的URL走勢



# 5 Key Information Security Risks in 2023

## 2023年五大 資訊保安風險

1

Identity/Credential Theft 身份 / 憑證盜用

2

Attacks Utilising A.I. 利用人工智能的攻擊

3

Crime as a Service 網絡犯罪 服務

4

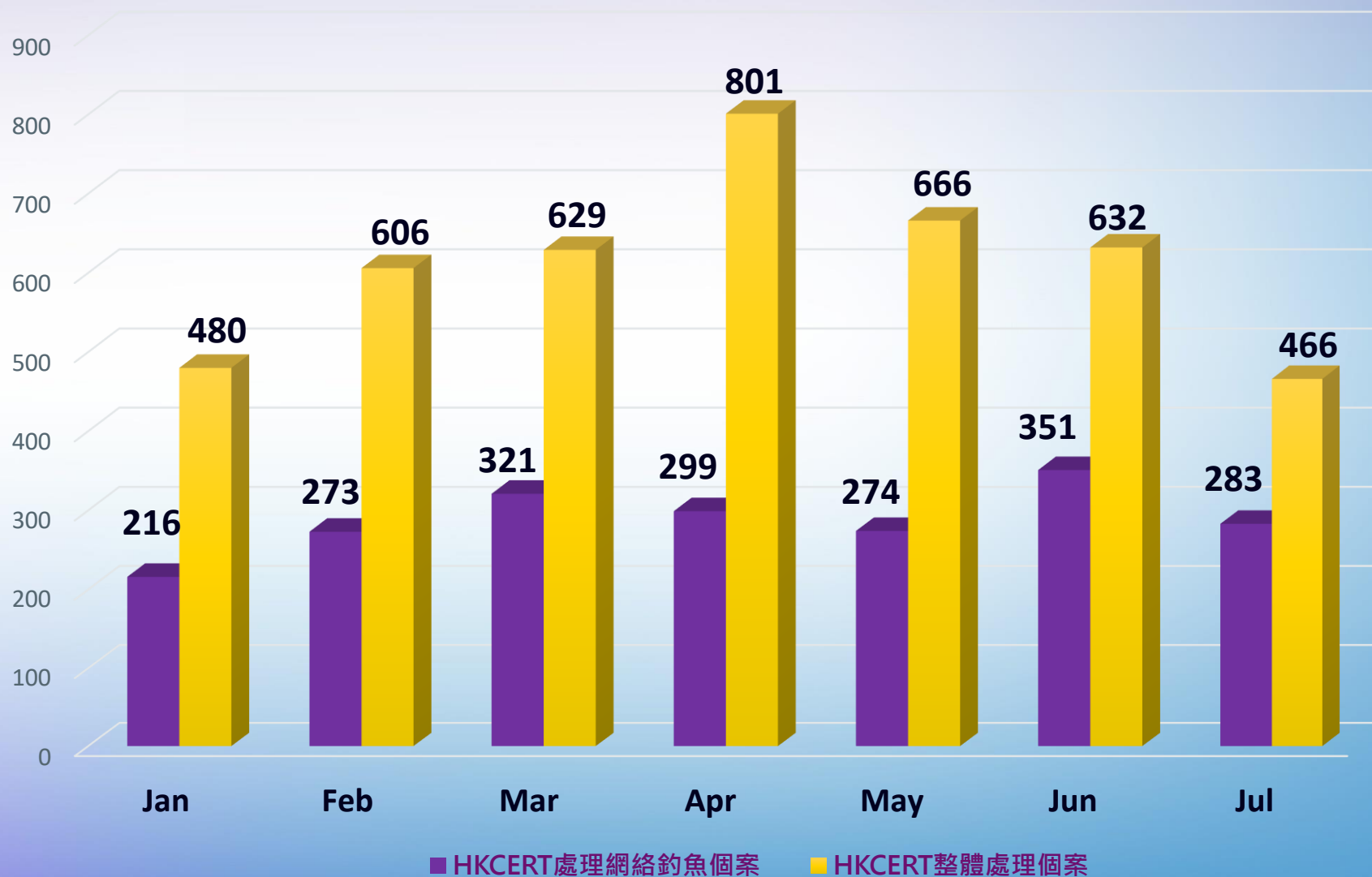
Cyber Attacks Targeting Web 3.0  
針對 Web 3.0 的攻擊

5

Attacks Arisen from Widespread Application of IoT  
IoT 廣泛應用引發的 攻擊

( In no particular order 排名不分先後 )

# 2023香港網絡釣魚數字



# 偽裝廣告



The screenshot shows a Google search for "whatsapp download". The search bar contains "whatsapp download" and the Google logo is on the left. Below the search bar, there are navigation options: "全部", "新聞", "影片", "圖片", "書籍", and "更多". The search results show approximately 3,450,000,000 results in 0.38 seconds. A red box highlights a fake advertisement for "whatsapp 中文版 - whatsapp 网页版" with a URL "https://www.whatspo.com/". A blue box highlights a real result for "WhatsApp Download" with a URL "https://www.whatsapp.com › download".

Google

whatsapp download

全部 新聞 影片 圖片 書籍 更多 工具

約 3,450,000,000 項搜尋結果 (0.38 秒)

提示：只顯示香港繁體中文搜尋結果。您可以在 使用偏好 中指定搜尋語言

廣告 · <https://www.whatspo.com/> ▾

**whatsapp 中文版 - whatsapp 网页版**

允許用戶發送文本消息和語音消息，進行語音和視頻呼叫以及共享圖像。一款基於雲的移動和桌面消息應用程序，專注於安全性和速度。

<https://www.whatsapp.com> › [download](#) ▾ [翻譯這個網頁](#)

**WhatsApp Download**

Download WhatsApp. Stay connected on WhatsApp across your devices, so you can pick up any conversation where you left off. By installing WhatsApp, you agree ...

<https://www.whatsapp.com> › [android](#) ▾

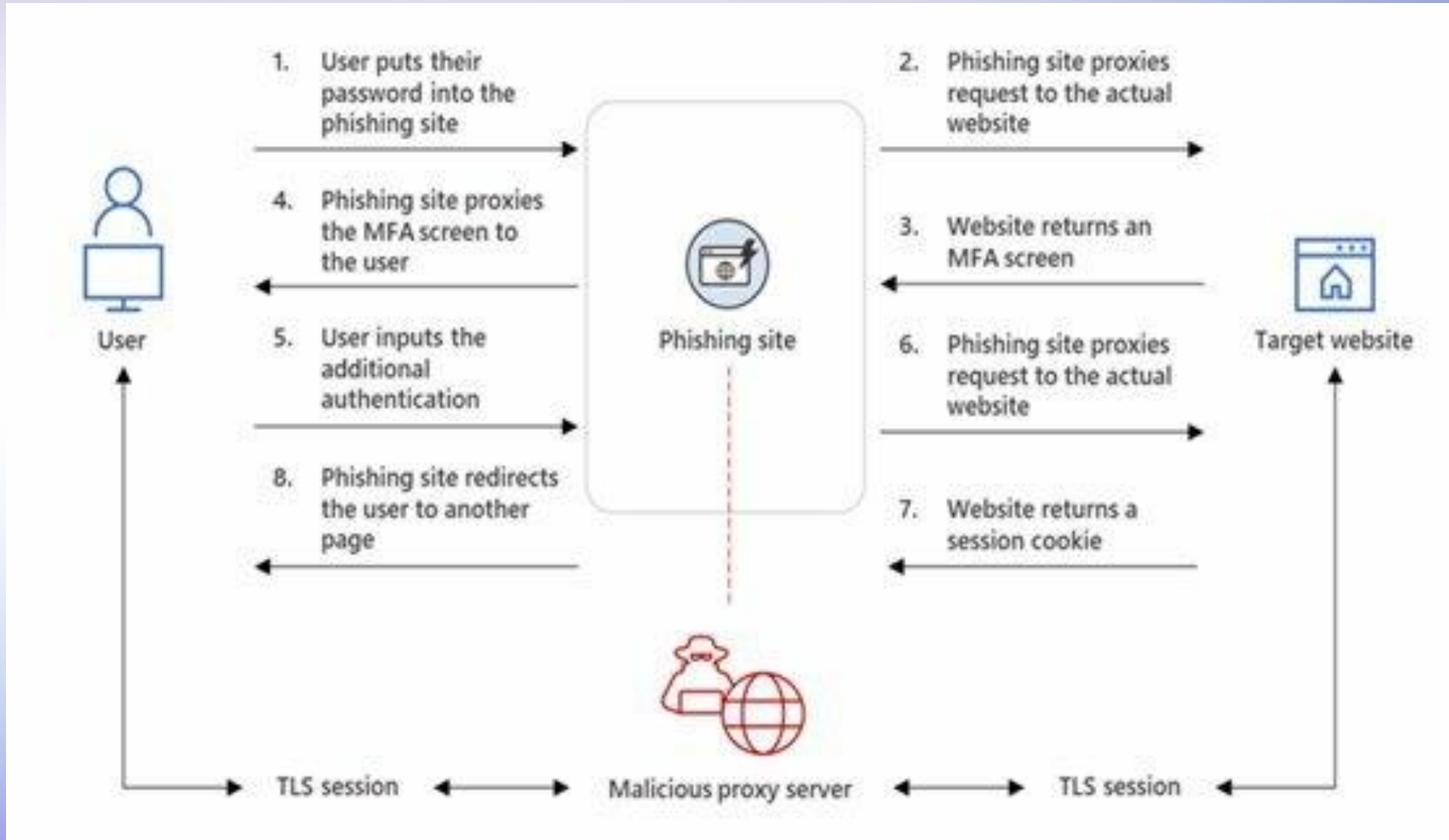
**下載Android 版WhatsApp**

下載Android 版WhatsApp. 到Google Play 下載. 套件安裝程式. 最低需求 (適用於版本 2.22.13.77) Android 作業系統4.0.3 或更新版本建議使用行動上網吃到飽方案不支援 ...

假

真

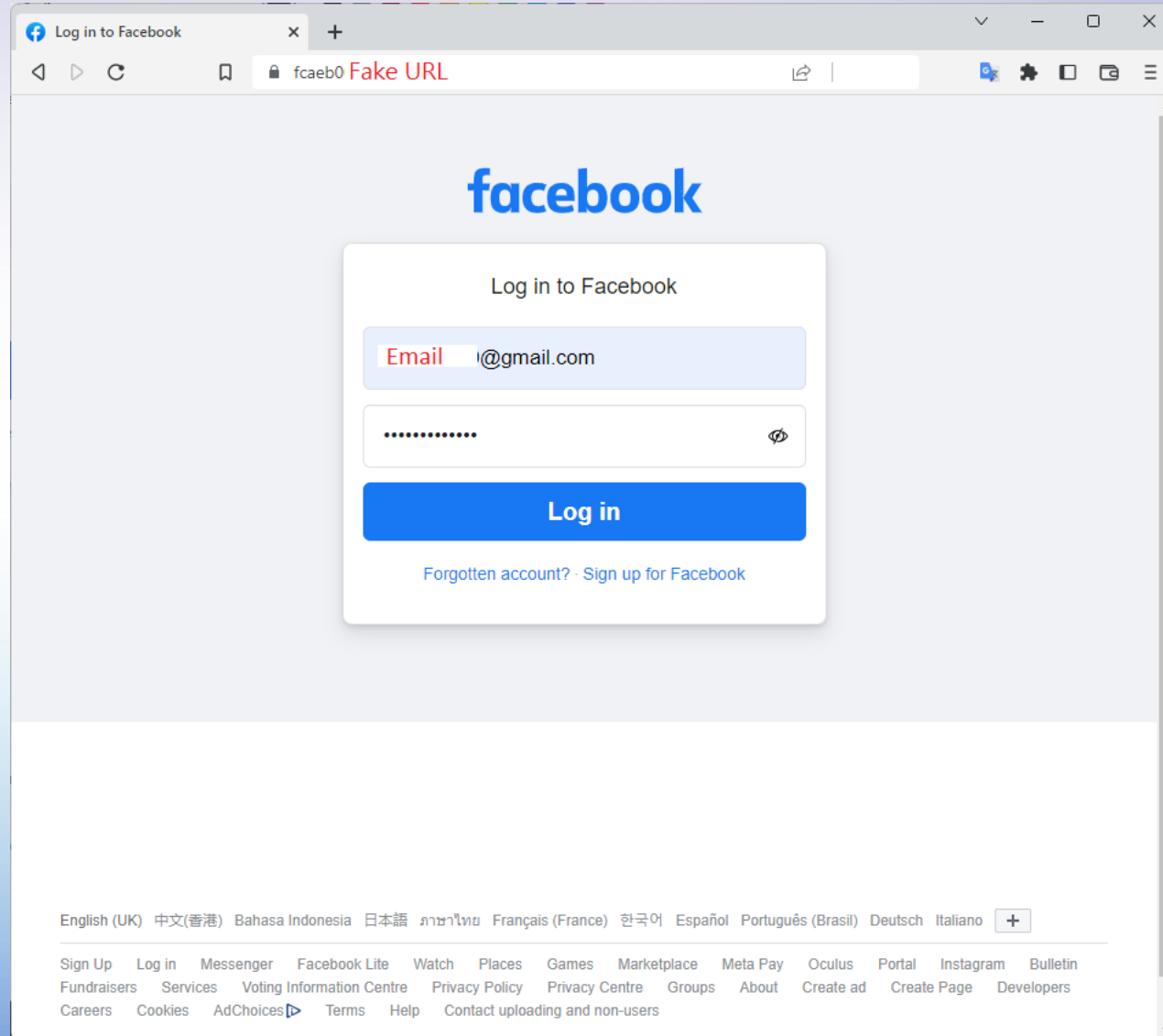
# 中間人攻擊(AiTM)釣魚





# 例子：中間人攻擊 (AiTM) 捕獲Facebook帳戶

## Step 1



# 例子：中間人攻擊 (AiTM) 捕獲Facebook帳戶

```
[09:13:45] [+++] [0] Username: [Email]@gmail.com]
[09:13:48] [+++] [0] all authorization tokens intercepted!
: sessions

+-----+-----+-----+-----+-----+-----+
| id | phishlet | username | password | tokens | remote ip | time |
+-----+-----+-----+-----+-----+-----+
| 1 | facebook | [Email]@gmai... | 3[Password] | captured | 2[User Login IP] | 2023-02-02 09:13 |
+-----+-----+-----+-----+-----+-----+

: sessions 1

id : 1
phishlet : facebook
username : [Email]@gmail.com
password : 3[Password]
tokens : captured
landing url : https://www.fcaeb0[Phishing URL]
user-agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
remote ip : 2[User Login IP]
create time : 2023-02-02 09:12
update time : 2023-02-02 09:13

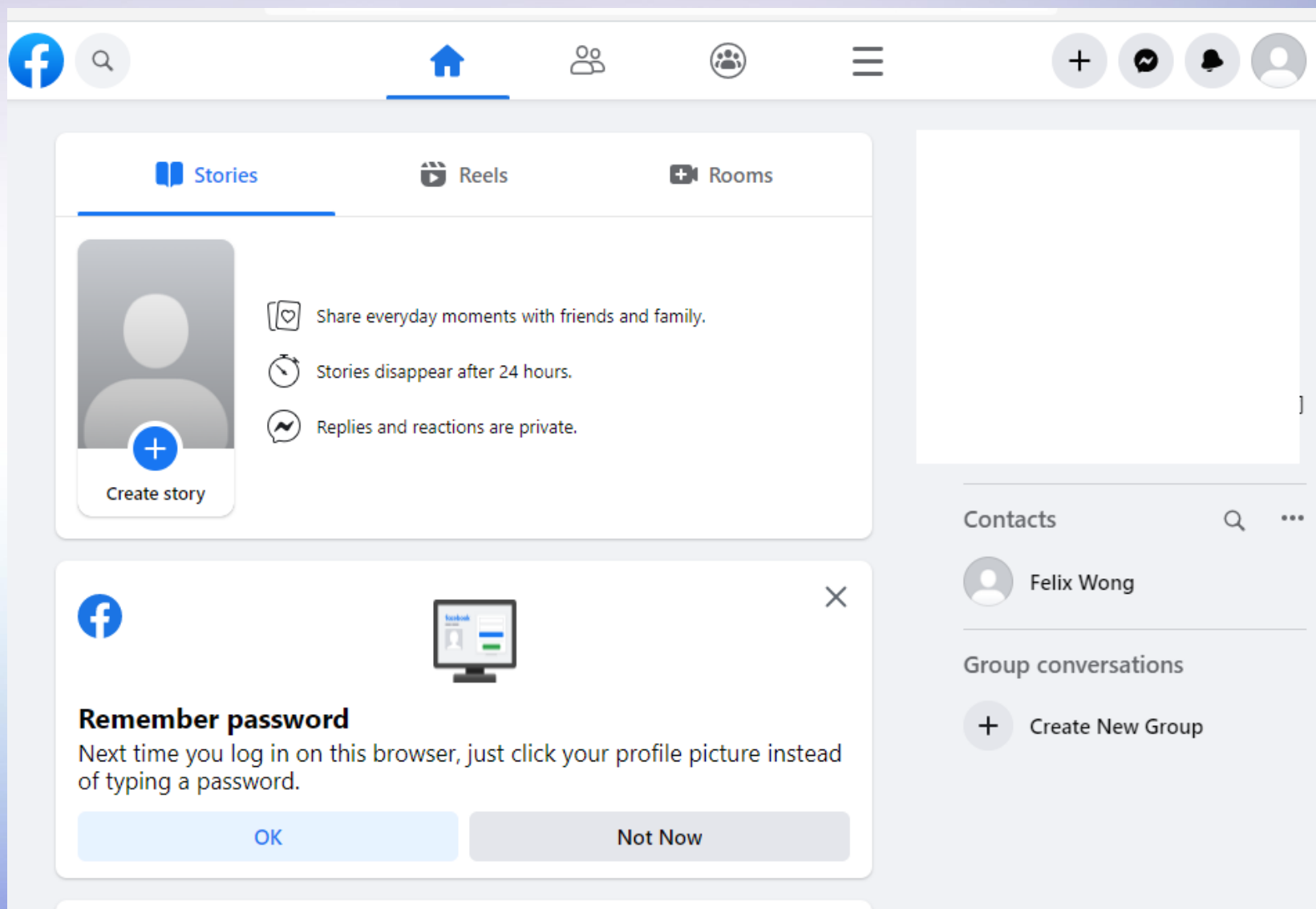
[{"path":"/", "domain":"facebook.com", "expirationDate":1706865258, "value":"[Cookies Value]ame":"c
_user"}, {"path":"/", "domain":"facebook.com", "expirationDate":1706865258, "value":"[Cookies Value]
BH", "name":"sb", "httpOnly":true}, {"path":"/", "domain":"facebook.com", "expirationDate":1706865258,
"value":"9%[Cookies Value]503", "name":"xs", "httpOnly":true}]

;
```

## Step 2

# 例子：中間人攻擊 (AiTM) 捕獲Facebook帳戶

## Step 3



# 利用深度偽造(Deepfake)進行身份盜用

內地破獲79宗「AI換臉」案 拘捕515人

08月10日(四) 16:03

推介 1



公安部召開新聞發布會。

公安部周四(10日)召開新聞發布會,通報打擊電信网络诈骗犯罪成效情況。其中在「淨網」行動中,破獲「AI(人工智能)換臉」案件,抓獲515名犯罪嫌疑人。



隨著AI科技升級,詐騙手段亦不斷變化出新。近日,有某科技公司商人在10分鐘內被呃走430萬人民幣,騙子利用的正是智能AI換臉和擬聲技術。

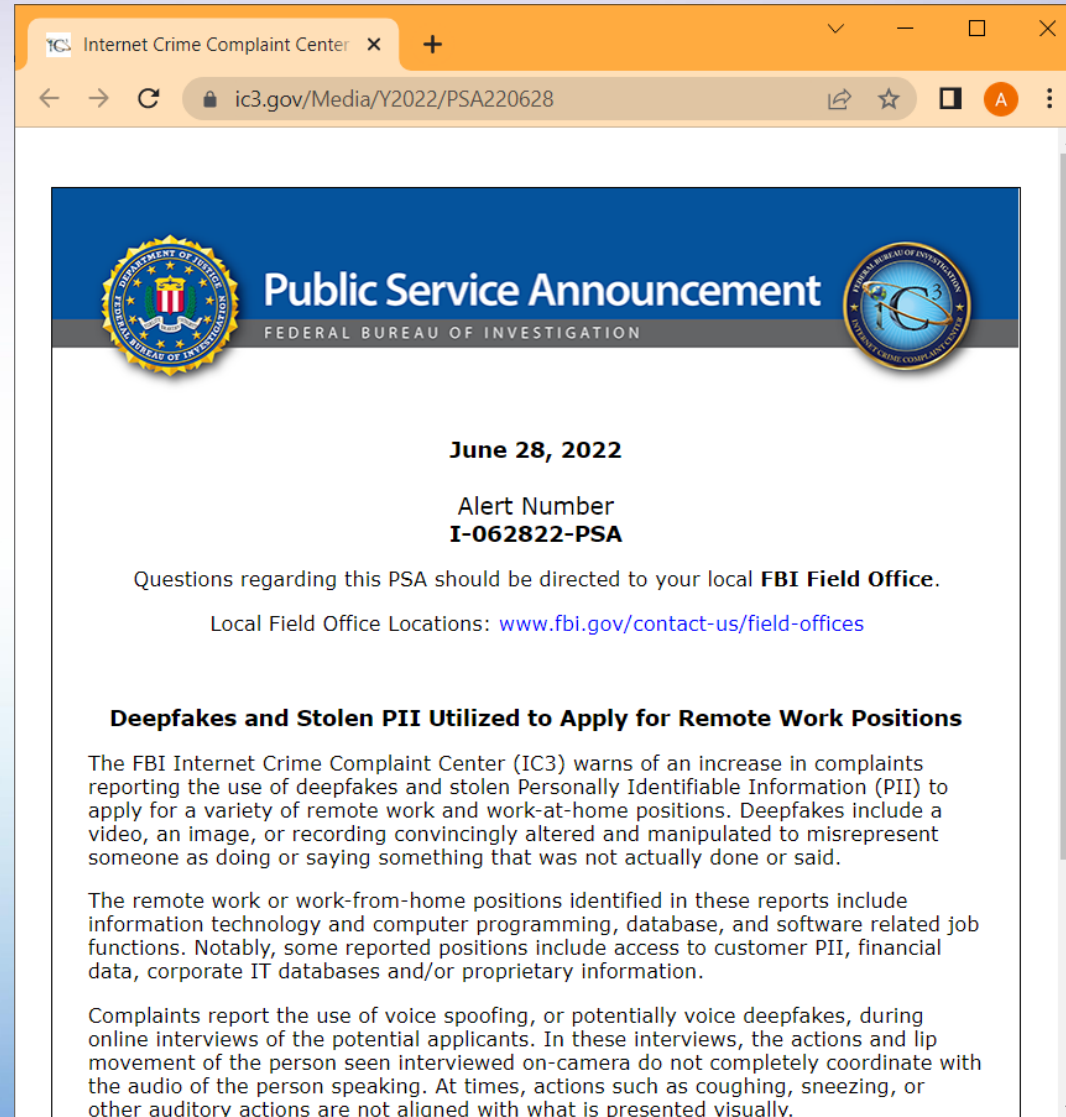
據悉,當事人郭先生為福州市某科技公司法人代表。4月20日中午,郭先生的好友突然通過微信視訊聯絡他,指朋友在外地競標,需要430萬保證金,且需要公對公賬戶過賬,想藉郭先生公司的帳戶走賬。基於對好友的信任,加上已經視訊通話核實身份,郭先生沒有核實錢款是否到賬,便分兩筆將430萬轉到了好友朋友的銀行卡上。

錢款轉賬後,郭先生給好友微信發了一條消息,稱事情已經辦妥,但好友竟回復一個問號。郭先生撥打好友電話,對方說沒有這回事,他才意識到被騙,隨後報警。



rthk.hk 中文新聞  
新聞主頁 即時新聞 視像新聞 新聞專題 新聞節目 新聞圖片 新聞簡報  
2023.08.22 星期二 33°C 68%  
即時新聞 主頁 即時新聞 本地  
騙徒以人工智能換臉換聲詐騙 警籲留意視像眼神口型  
2023-07-03 HKT 08:36 推介 70 分享工具  
騙徒以人工智能換臉換聲詐騙 警籲留意視像眼神口型



# FBI呼籲提防Deepfake



The image shows a browser window displaying a public service announcement from the FBI Internet Crime Complaint Center (IC3). The browser's address bar shows the URL [ic3.gov/Media/Y2022/PSA220628](https://ic3.gov/Media/Y2022/PSA220628). The page header features the FBI seal on the left and the IC3 logo on the right, with the text "Public Service Announcement" and "FEDERAL BUREAU OF INVESTIGATION" in the center. The announcement is dated June 28, 2022, and has an alert number of I-062822-PSA. It advises that questions should be directed to local FBI field offices and provides a link to find their locations. The main body of the text discusses a warning about deepfakes and stolen personally identifiable information (PII) used to apply for remote work positions. It notes that deepfakes can be videos, images, or recordings that are altered to misrepresent someone. The announcement also mentions that some reported positions involve access to sensitive data like customer PII, financial data, and corporate IT databases. Finally, it states that complaints often report voice spoofing or voice deepfakes during online interviews, where the person's actions and lip movements do not match the audio.

Internet Crime Complaint Center x +

← → ↻ ic3.gov/Media/Y2022/PSA220628

 **Public Service Announcement**   
FEDERAL BUREAU OF INVESTIGATION

**June 28, 2022**

Alert Number  
**I-062822-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: [www.fbi.gov/contact-us/field-offices](https://www.fbi.gov/contact-us/field-offices)

**Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions**

The FBI Internet Crime Complaint Center (IC3) warns of an increase in complaints reporting the use of deepfakes and stolen Personally Identifiable Information (PII) to apply for a variety of remote work and work-at-home positions. Deepfakes include a video, an image, or recording convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said.

The remote work or work-from-home positions identified in these reports include information technology and computer programming, database, and software related job functions. Notably, some reported positions include access to customer PII, financial data, corporate IT databases and/or proprietary information.

Complaints report the use of voice spoofing, or potentially voice deepfakes, during online interviews of the potential applicants. In these interviews, the actions and lip movement of the person seen interviewed on-camera do not completely coordinate with the audio of the person speaking. At times, actions such as coughing, sneezing, or other auditory actions are not aligned with what is presented visually.

# 深度偽造(Deepfake)



# 即時Deepfake



Source: Youtube <https://youtu.be/Jr8yEgu7sHU?si=EfJ09BQhgxWqBTgh>

3

# 保安建議





## 識別釣魚內容

- 陌生的寄件者或可疑的電郵地址  
使用其他電郵地址，例如 [hkcert@hkcert.xyz](mailto:hkcert@hkcert.xyz)
- 內容有很多文法或拼寫錯誤
- 帶誤導性或陌生的連結  
例如 [hlcert.org](http://hlcert.org) 模仿 [hkcert.org](http://hkcert.org)
- 使用語調緊急或是帶威嚇性的標題  
例如「你是特選客戶優惠最後今天，立即登入領取」

# 預防釣魚攻擊方法

- 切勿假設搜索引擎搜尋結果顯示的全為合法網站
- 應小心檢查網址串法，核實網站真偽
- 收到可疑電子郵件或SMS簡訊時，切勿打開任何連結或附件
- 向任何人或機構提供個人資料前要小心考慮清楚
- 避免在不同平台或服務使用相同的賬號和密碼
- 使用網上服務後謹記登出及關閉瀏覽器
- 開啟瀏覽器的反釣魚網站功能

# 預防深度偽造(Deepfake)

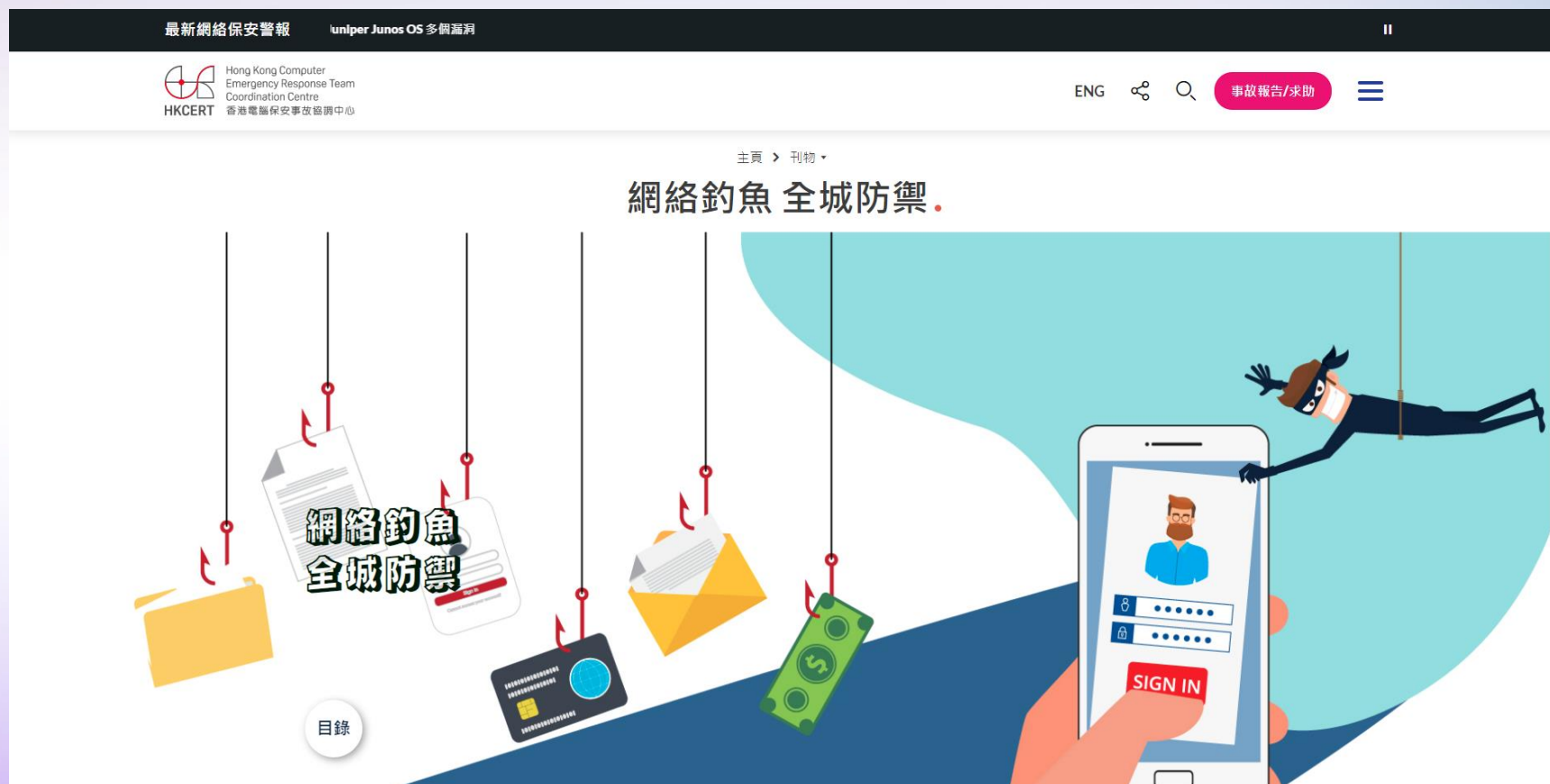


# 預防深度偽造(Deepfake)



## 如不慎中招，可以怎樣做？

- 更改所有已洩漏的網上服務帳戶密碼，以及聯絡相關服務供應商通報事故
- 暫停被盜用的信用卡。
- 密切監察你的帳戶是否有可疑交易或活動
- 留意任何冒充你身份的可疑即時通訊
- 向HKCERT報告

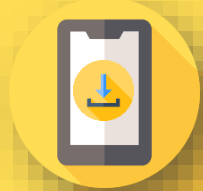


## 網絡釣魚 全城防禦



# 流動宣傳車





# 下載防騙視伏APP

電郵地址  
電話號碼  
IP 地址

未有紀錄  
提防中伏  
疑似有伏

**高危  
有伏**

收款帳號  
平台用戶名稱  
網址

防騙視伏APP  
立即下載

每20分鐘  
就有一宗騙案發生!





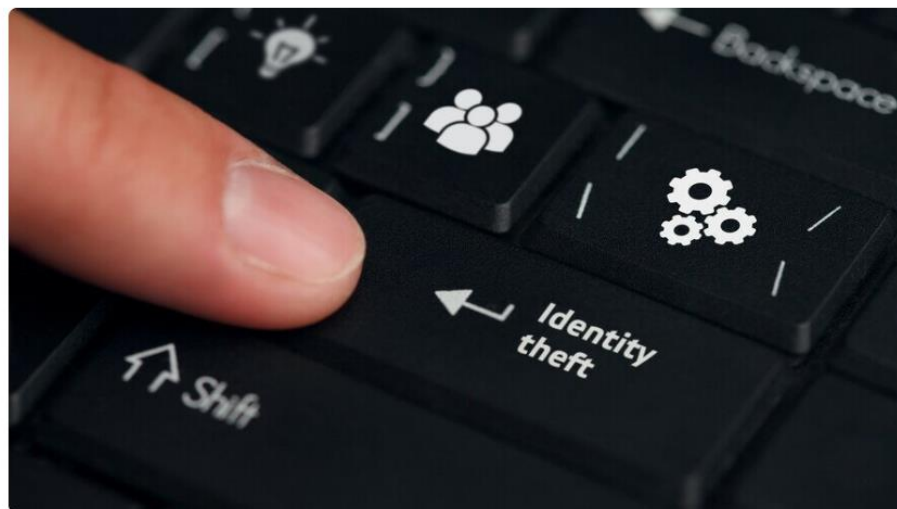
# 生產力促進局大樓 LG1 攤位



## 你知道什麼是身份/憑證盜用嗎?

身份和憑證的網上盜用並不是一個新事物。然而，2019冠狀病毒病疫情加速了大家在工作和生活上對網上服務的日益依賴，從而為網絡犯罪分子創造更多竊取個人資料以謀取私利的機會。因此，HKCERT 將身份/憑證盜用列為 2023 年五大資訊保安風險之一。

發佈日期: 2023年03月27日 | 2200 觀看次數



你知道什麼是身份/憑證盜用嗎?



# Capture The Flag



# 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>

SUBSCRIBE





## 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](http://www.hkpc.org)

