資安101: 資訊安全指南

Cyber Security 101: Stay Safe Online

2025/1/23

北桃金輔導團/真理大學資管系 王柳鋐老師

輸入同步網址

https://slides.com/d/8VOEa90/live

關於我 王柳鋐

- 教育部數位機會中心「北桃金輔導團」協同主持人 2014~2025
- 真理大學 資訊管理學系 副教授 兼 圖資長
- 台灣大學資訊工程博士
- 真理大學緬甸志工團領隊 2018, 2019
- 真理大學廣西大化志工團領隊 2009~2014, 2018, 2019
- 資訊志工領隊 北桃(2014) 馬祖北竿(2009)

詐騙與資訊安全

每天騙走4億元！　為什麼台灣變成詐騙天堂?

學理上常見的資訊安全問題

- 非法入侵
  - 駭客入侵
- 惡意軟體
  - 病毒
  - 木馬程式（開後門）
  - 殭屍病毒
  - 勒索病毒
- 網路釣魚
  - 冒名網址
  - 假的網頁內容

安全漏洞

不小心下載

誤點、誤信連結

為什麼被騙?

- 缺乏足夠知識和心理脆弱
  - 資訊落差
  - 沒有警覺心、容易相信他人
- 承諾和信任
  - 朋友、家人或權威人士
  - 很難再回頭說不
- 不願意尋求幫助

求證、分辨、提高警覺

【遠見】心理師解謎：為什麼在這社會上，有些人特別容易被詐騙?

內政部警政署 https://165dashboard.tw/

詐騙手法第一名

資安課題

下載專屬投資APP、綁定網銀、約定帳戶

網銀帳密給助理代操（帳號管理）

圖片來源:165防詐儀錶板

➢常見冒用機關及詐騙特性

冒用機關	詐騙特性
●警察局 ●健保局 ●地檢署 ●醫療院所 ●165專線 ●中華電信 ●社會局 ●戶政事務所 ●郵局	① 詐騙電話大多為篡改號碼。 ② 以被害人涉及犯罪為由，檢察官須監管帳戶進行詐騙。 ③ 採取現場面交為主，交款地點大多為公園、學校等無監視器地方。 ④ 車手集團由3-4人同車方式，使用行動電話皆為公機，避免警方通聯分析找出破綻。 ⑤ 交款當時，除假冒檢察官外，另有同行者在旁監視，取得現金即返回分贓，警方無法追查資金流向。 ⑥ 詐騙與車手集團分離，採拆帳方式結合作案，且有詐騙集團與不同車手集團配合作案現象。

來源

詐騙手法第三名

詐騙公式拆解

假交友（投資詐財）詐騙

一、在社群軟體虛構異性人物活動，假意熱情、親切與關心。

二、誘騙加入假投資平台或網站，並營造小額獲利假象，誘騙再投資。

三、不讓被害人提領錢，並要求支付保證金、稅金等費用。

資安課題

虛構身份 ✕ 假冒身份

假網站 ✕ 假訊息

圖片來源:165防詐儀錶板

盜用LINE帳號詐騙流程圖

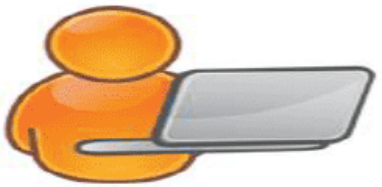
①

駭客

②

散發惡意連結
誘使被害人點擊
(釣魚網站或網頁掛馬)

③



騙取使用者
大量帳密

尝試登入 LINE
取得使用權限

④

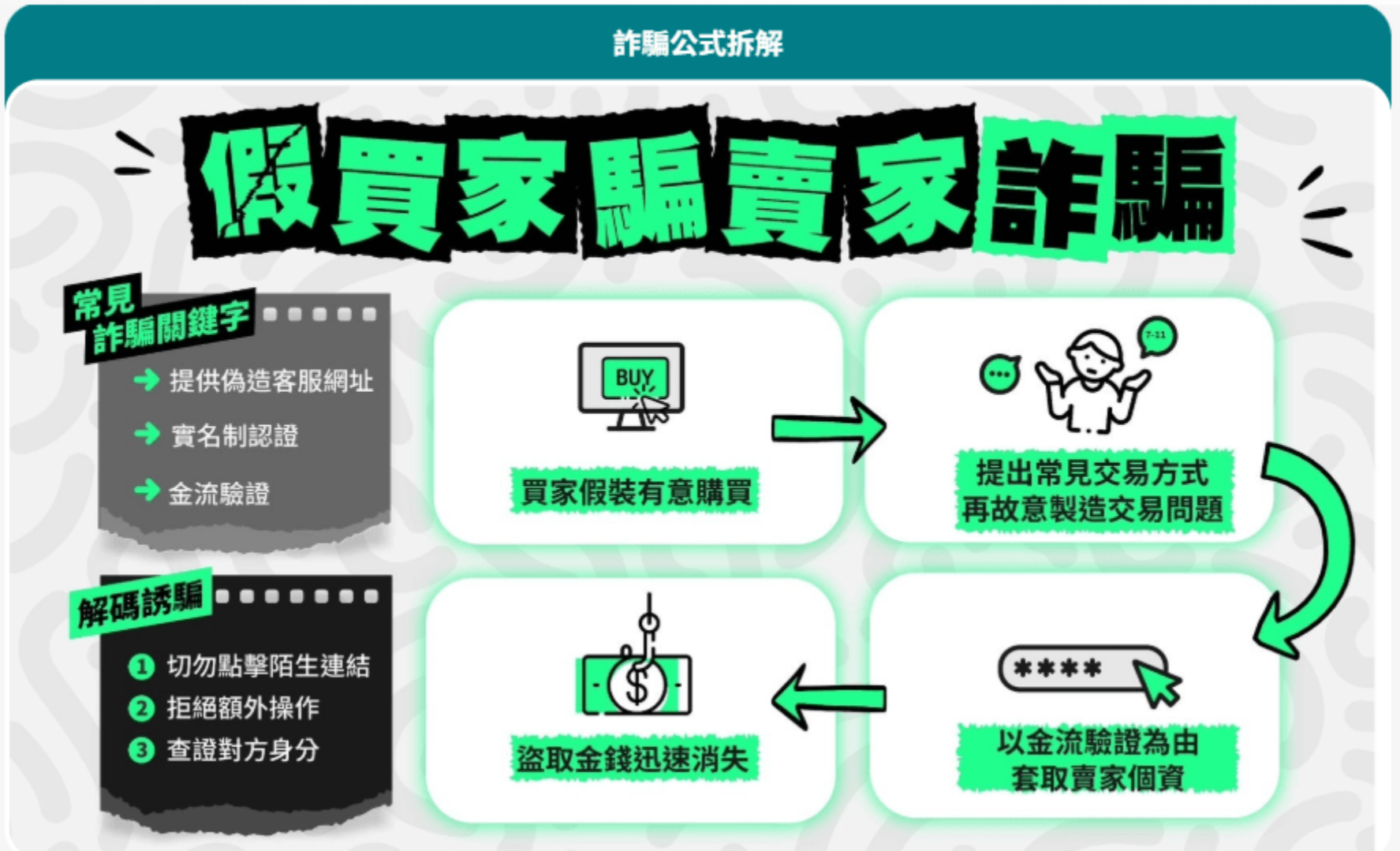
冒用 LINE 帳號者
以盜用帳號傳送訊息給
原帳號使用者的好友

常用手法：

- 謊稱手機沒電或故障，請被害人幫忙代收發簡訊並告知身分證字號與手機，進行小額付費
- 請被害人至超商購買遊戲點數，並將儲值密碼給歹徒

來源

詐騙手法第四名



資安課題

不要點擊陌生人提供的客服連結。

認清平台官網上的客服

圖片來源:165防詐儀表板

詐騙手法第五名

詐騙公式拆解

假中獎 通知詐騙

資安課題

社群網[illegible]假訊息

個資[illegible]保護

圖片來源:165防詐儀表板

惡意連結詐騙小額付費流程圖

① 

由中毒的手機發出
LINE及SMS簡訊

② 

廣發惡意連結訊息

③ 

惡意網站植入惡意程式

④ 

點擊下載後手機中毒

控制手機發送
惡意連結簡訊

繼續感染更多手機

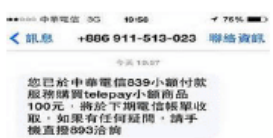
⑤ 

駭客主機

攔截簡訊

發送簡訊

電信業者簡訊平台
確認交易

⑥ 

完成小額付費簡訊

來源

手機惡意簡訊連結防範4步驟

查、看、申、報

查 察覺異樣

（接到他人來電詢問有無發送簡訊或收到小額付費交易簡訊）

看 看電話帳單是否異常

（簡訊費用暴增或有小額付費）

申 向電信公司申訴，否認交易

報 立即向警察局或 165 報案

來源

小結

- 不要下載來路不明的APP
- 保護好網銀帳密
- 不要隨意點擊別人提供的連結
- 小心求證

內政部警政署 https://165dashboard.tw/

其他資安陷阱

社交工程: 疏忽來自人性

圖片來源：https://cms.aaasec.com.tw/index.php/2020/05/19/m05/

圖片來源
https://www.finance.taichung.gov.tw/2042709/post

周杰倫數位藝術品遭竊?

周杰倫千萬元NFT被盜！ 「1條釣魚網址」幾秒內騙光

2022/04/02 18:51

網路釣魚

https://star.ettoday.net/news/2325929

網路釣魚簡訊


【國泰世華】您的銀行賬戶顯示異常，請立即登入綁定用戶資料，否則賬戶將凍結使用
www.cathay-bk.com
訊息
民眾收到惡意簡訊內容
4:08
+886 903
訊息
今天 下午3:51
【台新銀行】您的網路銀行更新失敗，請立即輸入您的驗證碼以更新資料，超時請重新輸入
www.taishinz.com
【中國信託】你的網路銀行更新失敗，請立即輸入你的驗證碼以更新資料，超時請重新輸入。 http://ctbc-

張大眼睛，不要掉入釣魚網站陷阱

釣魚網站

註：正確網站應為
www.cathaybk.com

我們的身邊充滿「照騙」

你以為這樣

實際上這樣

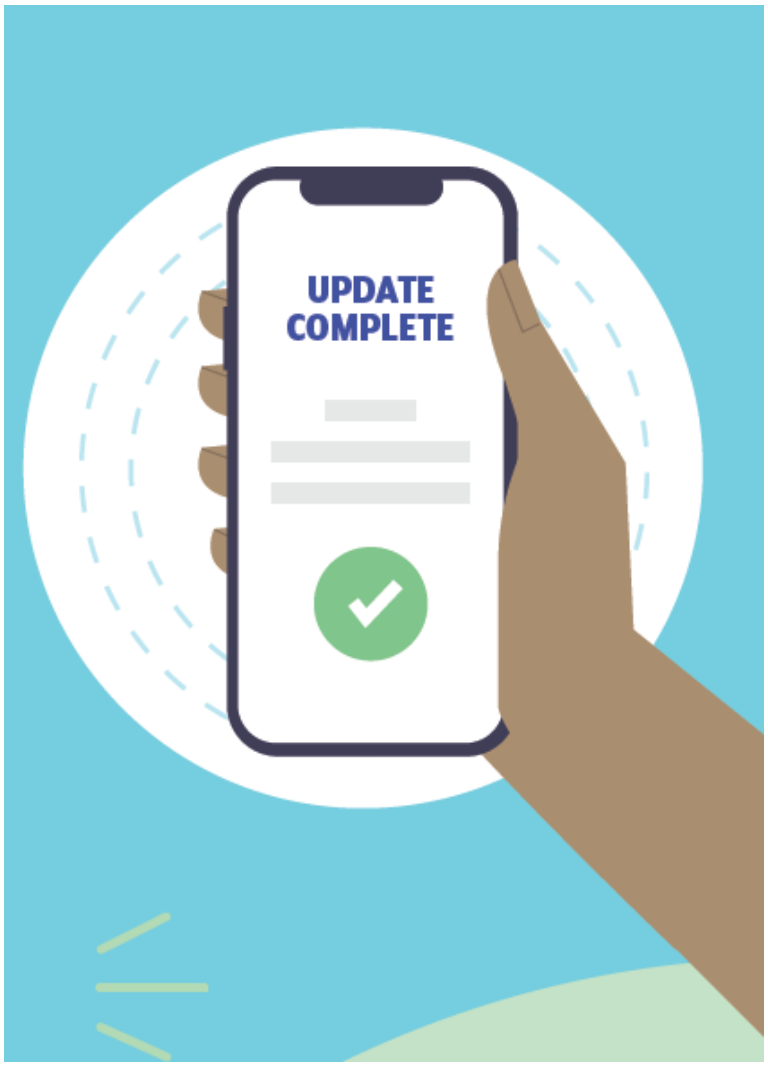
圖片來源

深度偽造Deepfake，簡稱深偽

利用人工智慧AI技術，變聲、變臉（刑事局 變聲篇）

指南

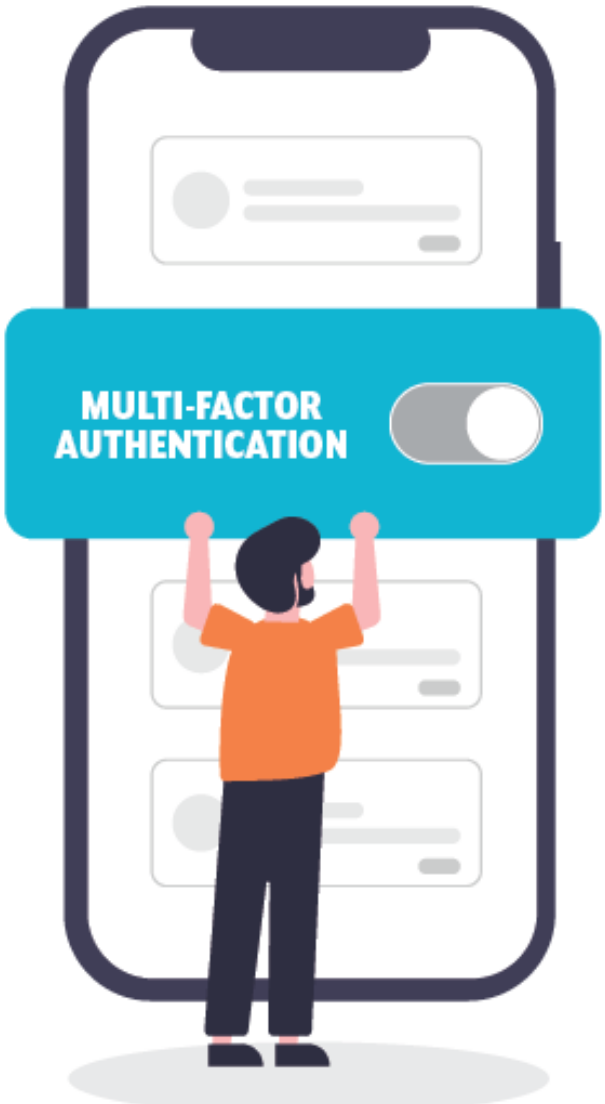
更新系統、更新APP



更新：解決漏洞造成的資安問題

提昇效能

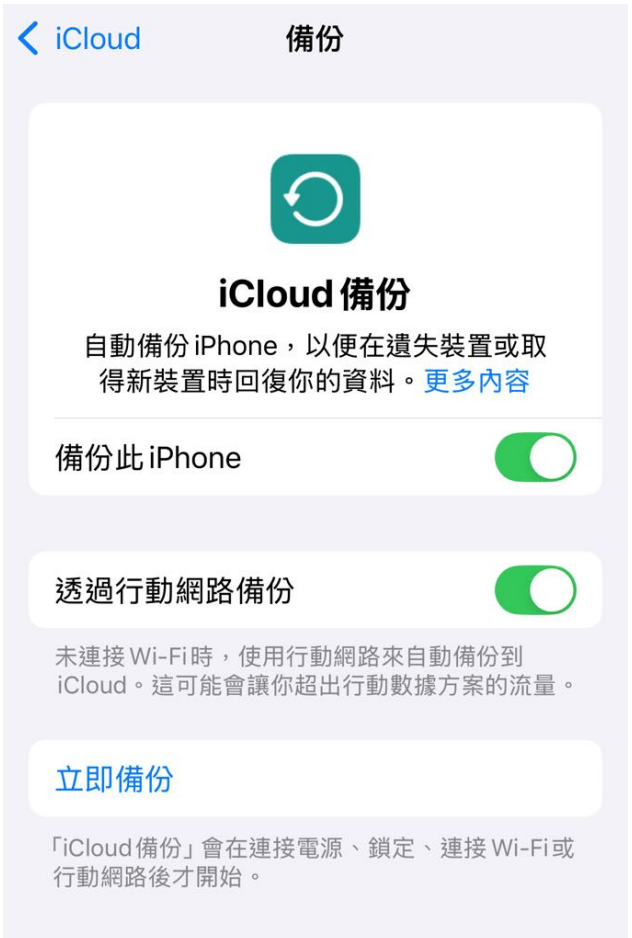
多因子認證、雙重認證



- 你所知道的訊息
  密碼、PIN 碼、安全問題的答案。
- 你實際擁有的東西
  手機、USB金鑰、員工證或門禁卡片
- 個人生物特徵
  指紋、人臉辨識或虹膜

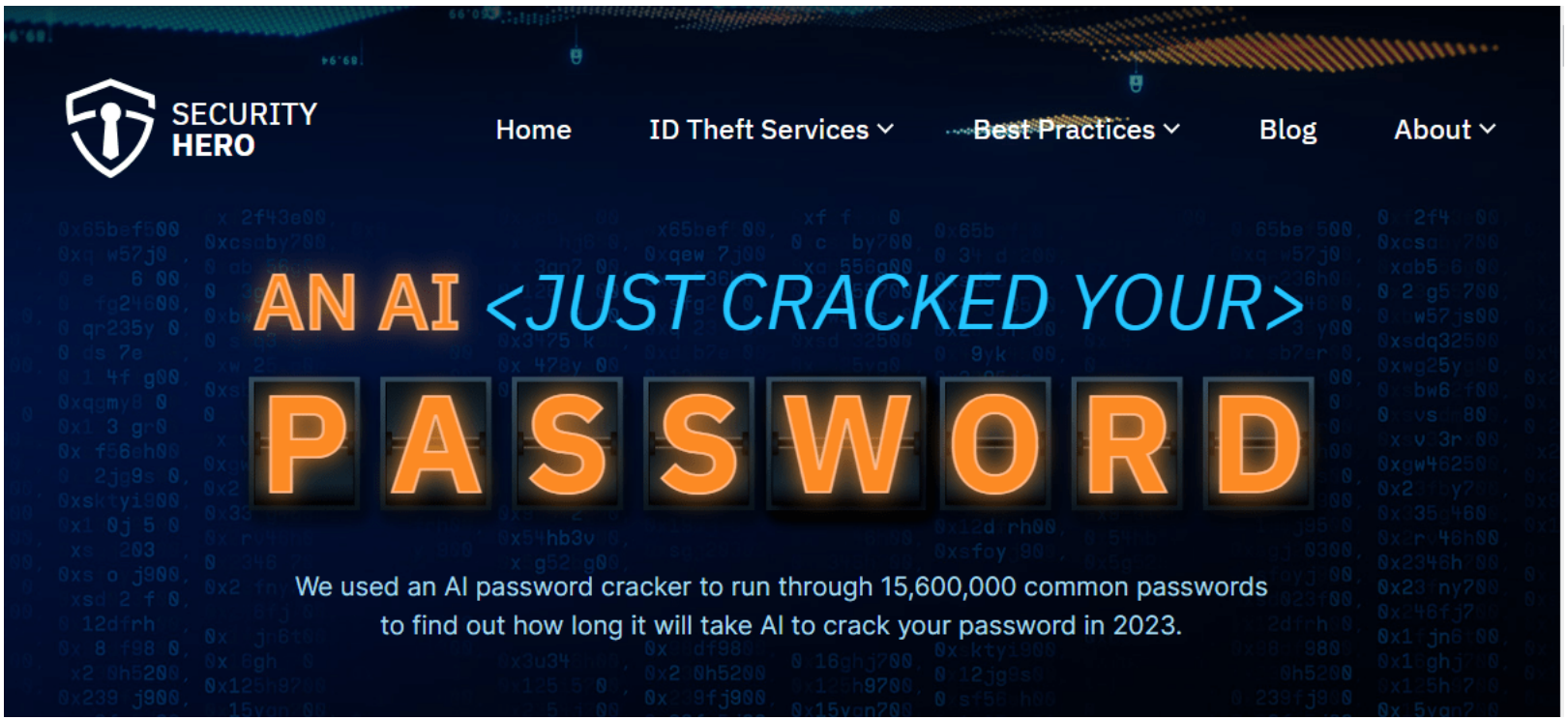
雙重認證：登入時使用兩種以上

備份



- 重要內容備份到雲端、電腦
- 視資料重要性：留意備份時間間隔

你的密碼多快被AI破解?



https://www.securityhero.io/ai-password-cracking/

簡單密碼易遭黑客破解 澳人損失近2億

截至2023年，澳洲人因使用簡單密碼而遭黑客詐騙，損失了近2億澳元。圖為網攻示意圖。(Philippe Huguen/Getty Images)

https://www.epochtimes.com/b5/23/6/23/n14021759.htm

懶人密碼遭破解 富商損失百萬

圖為竊盜集團成員盜領畫面。（記者陳文嬋翻攝）

2013/12/10 06:00

https://news.ltn.com.tw/news/local/paper/737444

2018-11-28

2018 年

你的帳號被駭了！解析勒索信件攻擊手法

網擎資訊產品經理 張峰銘

近兩個月來 Openfind 資安團隊於亞太地區雲端資料中心偵測到大量勒索信件，經分析後發現，這類勒索信件都是以匿名方式寄出，攻擊者宣稱已在受害者電腦植入木馬程式，可掌握受害者的隱私資料或帳號密碼，對方必須在 48 小時內透過比特幣支付贖金，否則就會在網路上散布受害者的隱私資料或產生更嚴重的後果。這是一種新型態釣魚攻擊，這些勒索信件中沒有任何 URL 連結或惡意附檔，攻擊者企圖利用個資帳密，迫使受害者心生恐懼，進一步達成詐騙目的。

2018 年 8 月，隸屬於 FBI 的網路犯罪通報中心（Internet Crime Complaint Center，IC3）就已發布「詐騙集團利用個資恐嚇受害者」的威脅報告。在當時，這類勒索攻擊主要出現在澳洲與美國地區，直到 10 月左右才出現在亞太地區。雖然這些勒索信件有很多變化，但它們通常具有某些共通點，以下歸納說明：

https://www.openfind.com.tw/taiwan/markettrend_detail.php?news_id=24493

密碼安全性


你的密碼夠強嗎？
超過八碼
大小寫英文都有
不用生日
無明顯含意
不用身分證
定期更新
加入特殊字元
輸入法變化
英文與數字穿插

法務部及所屬機關資訊系統存取控制管理規範

五、密碼安全管理

（一）除系統程式使用之帳號及系統採用多重身分認證方式外，一般靜態密碼之強度及使用應符合下列規定：

1.禁止使用空白密碼。

2.密碼長度**至少為八個字元**，管理者密碼**至少為十個字元**。

3.密碼**變更**時，新密碼**不得與前三次**密碼相同。

4.密碼設定**應包括數字及英文字母**，建議包括**特殊字元**。

5.重要系統之密碼以**至少每六個月更換**一次為原則。

6.避免使用與個人有關資料（如生日、身分證字號、單位簡稱、電話號碼等）作為密碼。

（二）使用者密碼須妥善保管，避免他人知悉。

良好的使用習慣

問題

朋友志明在FB上分享家族聚會照片，結果被不認識的人轉傳、濫用，你應該?

1. 志明可以在FB上分享聚會照片嗎?

2. 分享照片，有哪些風險可能發生?

3. 在這種情況下，我們應該如何保護自己的隱私

4. 志明是你的朋友，你會提醒他/她嗎？爲什麼?

問卷不要隨便填！個人資料外洩風險

示意圖，非真實詐騙個案！！

圖片來源

簡單訣竅

三「不」、三「要」

<不上當>
不被吸引標題欺騙，看清郵件賦予的資訊。

<不開啟>
不隨意開啟郵件中夾帶的附件。

<不點擊>
不隨意點選郵件的附上的連結。

<要確認>
要確認寄件者的身份。

<要更新>
電腦、軟體、瀏覽器要保持更新狀態。

<要備份>
重要資料請務必隨時備份。

圖片來源: https://cc.tcu.edu.tw/wp-content/uploads/2022/04/image_5.png

檢舉詐騙、了解最新手法

https://165.npa.gov.tw/#/report/statement

內政部警政署165全民防騙網
https://165.npa.gov.tw/#/

總結

- 認識詐騙手法與資安的關聯
- 安全的網路使用行為
  - 避免點擊可疑連結
  - 不隨意點擊電子郵件、簡訊或社群媒體上的可疑連結
  - 更新、備份
- 密碼保護的認知
  - 強密碼使用
  - 定期更換密碼
  - 多因素身份驗證

感謝聆聽

圖片來源