資拓宏宇國際股份有限公司
International Integrated Systems, Inc.

教育部國民及學前教育署
K-12 Education Administration, Ministry of Education

113年資通安全通識教育訓練

機不可失~

行動裝置、通訊軟體及遠距作業帶來的便利與隱憂

講師：資拓宏宇顧問

日期：113年11月19日

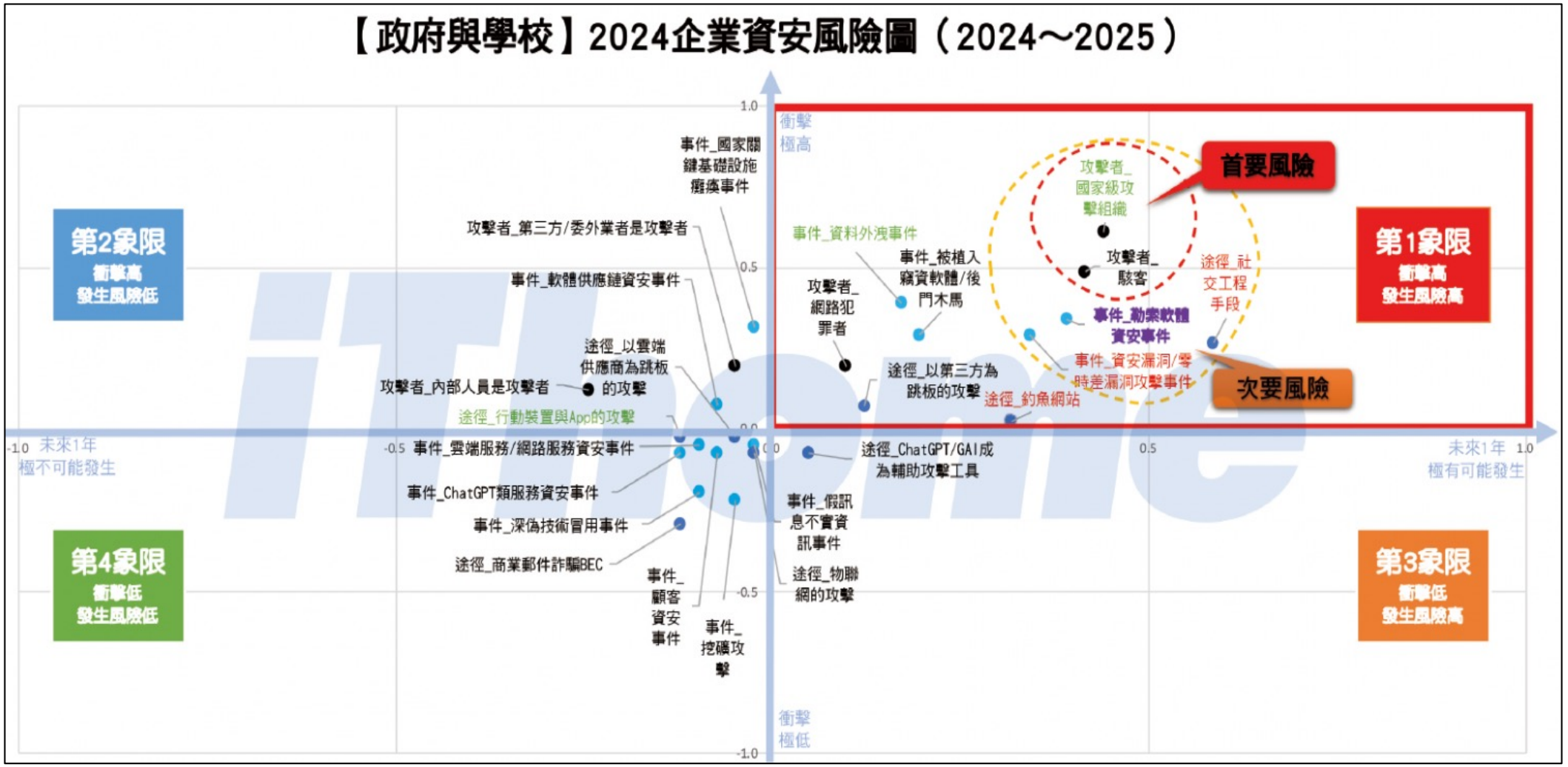
資拓宏宇永遠與您一起創新前進
always innovative always IISI

大綱

- 資通安全趨勢解析
- 降低行動裝置的風險
- 消弭通訊軟體的隱憂
- 控管遠距作業的危機
- 總結
- 提問與討論

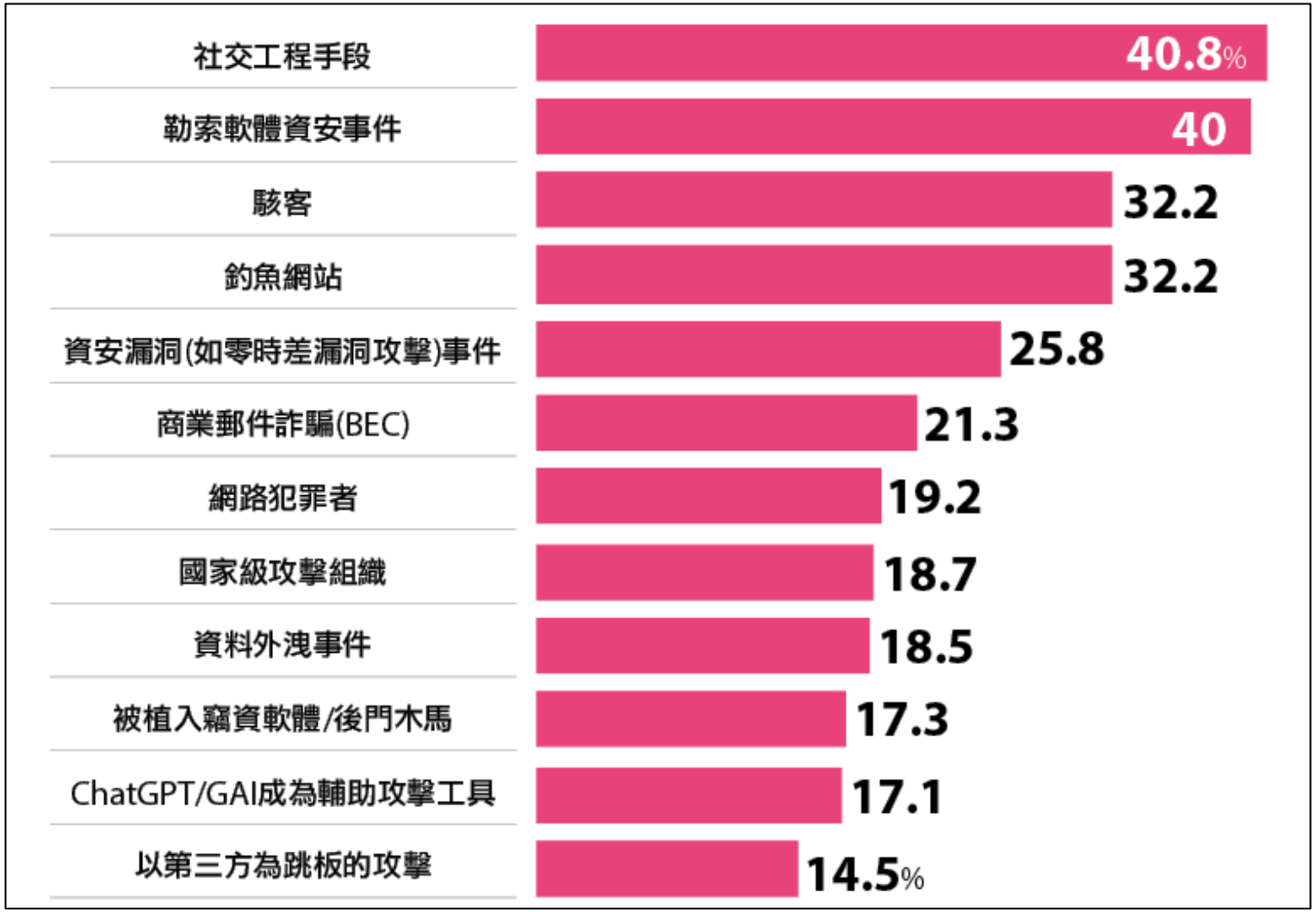
資通安全趨勢解析

政府與學校未來一年資安風險



資料來源：iThome

未來一年重大資安風險預測



資料來源：iThome 2024 CIO大調查

認識零時差攻擊

- 零時差攻擊(Zero-Day Attack)
  - 指專門針對尚未修補的漏洞進行攻擊的駭客手段，如果有組織未定期修復系統上的漏洞，持續使用有漏洞的系統時，就有極大的機會被駭客趁虛而入。就像雙方在進行一場誰先發現漏洞的比賽，一方在找尋漏洞攻擊，另一方則需積極持續修補漏洞，將威脅性降到最低。
- 零時差(零日)漏洞(Zero-Day Vulnerability)
  - 指在軟體、韌體、硬體設計中已被公開揭露但遲遲未修補的錯誤。除此之外還有另一種情況是，研究人員已公開揭露這項漏洞，且廠商和開發人員也知道該漏洞，但卻尚未釋出更新資訊來修補。

零時差攻擊手法

- **魚叉式網路釣魚**
  - 電子郵件的附件檔案 (如：微軟文件、PDF 或其他軟體的執行檔及元件) 可能暗藏零時差漏洞攻擊程式碼。
- **網路釣魚郵件以及社交工程郵件**
  - 垃圾郵件會誘騙不知情的收件人點選某個網址或連結，將使用者導向惡意或已遭入侵的網站，該網站就暗藏了漏洞攻擊手法。
- **漏洞攻擊套件**
  - 利用惡意廣告和惡意網站來暗藏漏洞攻擊手法。
- **駭客攻擊**
  - 先入侵某個系統、伺服器或網路 (透過暴力破解密碼或字典攻擊、組態設定的錯誤，或是系統暴露在網際網路上)，然後再植入含有漏洞攻擊手法的惡意程式。

零時差攻擊實例

- 國家級駭客利用思科防火牆零時差漏洞，在多國政府植入後門程式。
- 惡意軟體SSLoad攻擊亞洲、歐洲、美洲組織，攻擊者利用Cobalt Strike、ScreenConnect控制受害電腦。
- 北韓駭客Kimsuky鎖定防毒軟體發動供應鏈攻擊，透過惡意程式GuptiMiner部署後門程式、挖礦軟體。
- 駭客組織Androxgh0st入侵全球逾600臺伺服器，臺灣、美國、印度是主要目標。

資料來源：iThome 2024年4月25日資安日報

零時差攻擊因應之道

- 定期更新、修補漏洞：當軟體廠商推出新的安全套件或是提示更新時應立即更新，減少被駭客攻擊的機會。
- 採取最低授權原則：組織內部應採取最低授權原則來限制存取權限，降低駭客入侵竊取資料或破壞的風險。
- 培養良好的使用習慣：透過教育訓練讓人員養成良好的網路使用習慣，定期宣導漏洞攻擊手法，及不輕易點擊來路不明的連結或安裝不明軟體。
- 多層式資安防禦策略：建構多層次的資安防護盾，選擇防火牆與入侵防護系統能夠有效協助組織過濾惡意流量。

降低行動裝置的風險

日常生活充斥著行動裝置(Mobile device)

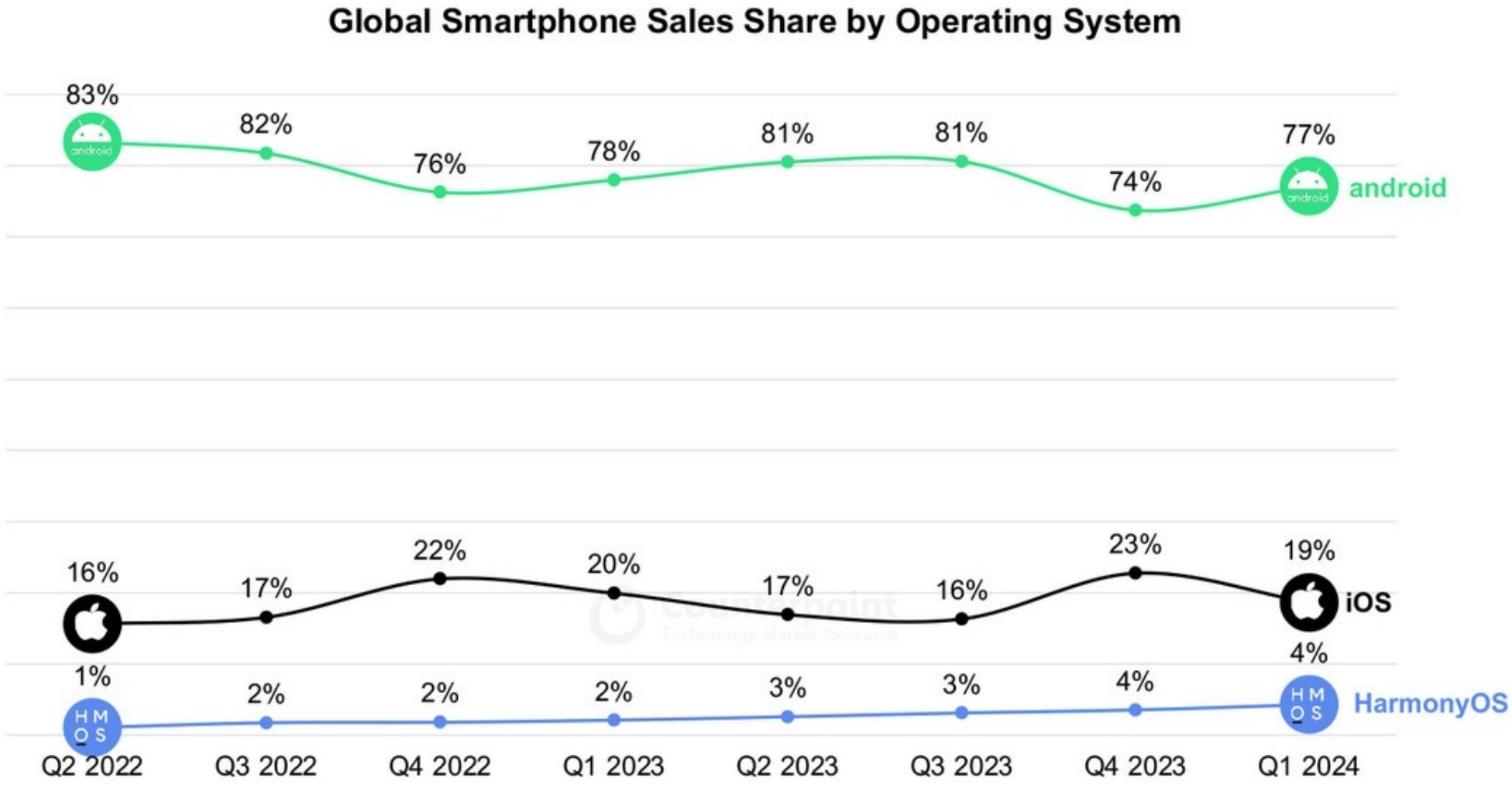
正視行動裝置的資安問題

- 「I am nobody！沒什麼值得被偷的」
- 行動支付、GPS定位導航、金融交易、個人健康偵測都是現代人經常使用的工具，因此行動裝置內的資產具有極高的價值。
- 行動裝置內存有哪些重要資產
  - 聯絡人個資 (親友的姓名、生日、電話號碼、住址...)
  - 照片
  - GPS 定位紀錄
  - 信用卡 / 銀行帳戶資訊
  - 通訊內容 (簡訊、即時通訊軟體的資訊)
  - 智慧家庭控制 (如控制家中的電器或是監看家中狀況)
  - ...

行動裝置的潛在資安風險

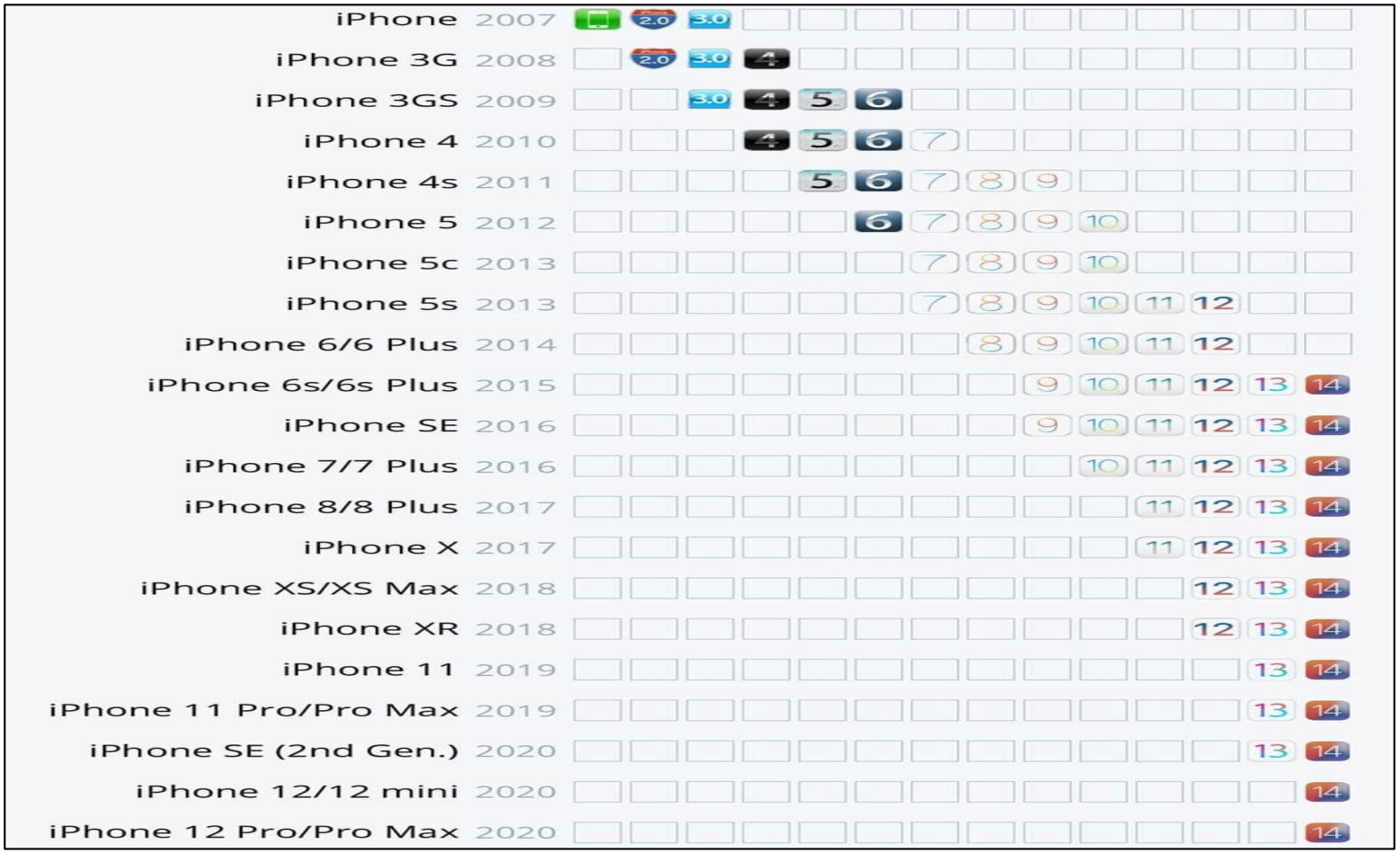
- 利用行動裝置作業平台的漏洞進行滲透攻擊。
- 透過下載安裝至行動裝置的APP或軟體植入後門程式進行攻擊。
- 誘使行動裝置連上不安全的網路進行攻擊。
- 藉由各種管道 (如簡訊、電子郵件) 發送釣魚網站連結或植入惡意軟體進行攻擊。

手機作業系統市佔率趨勢



手機的壽命有多長(IOS)

- 取決於手機型號



資料來源：Statista 統計資料

手機的壽命有多長(Android)

- 取決於手機製造商

廠商	最長系統更新和安全年限
Google Pixel	7年的系統和安全更新 （僅Pixel 8和後續機型）
Samsung	7年的系統和安全更新 （僅S24系列起新旗艦機）
SONY	2-3年系統更新、4年安全更新
小米	4年系統更新、5年安全更新 （僅限AER認證產品）
Redmi	4年系統更新、5年安全更新
OPPO	4年系統更新、5年安全更新 （僅限2023年新旗艦機型起）
ASUS	2年系統更新、2年安全更新
ZenFone	2年系統更新、2年安全更新
ROG	2年系統更新、2年安全更新
VIVO	3年系統更新
NOKIA	3年系統更新、4年安全更新

資料來源：各家廠商公開之資訊

保持行動裝置的作業系統更新

要維護 Apple 產品的安全性，你可以自行採取一些措施，而隨時將軟體更新到最新版本是其中最重要的措施之一。

- iOS 和 iPadOS 的最新版本為 17.6.1。了解如何更新 iPhone、iPad 或 iPod touch 的軟體。
- macOS 的最新版本為 14.6.1。了解如何更新 Mac 的軟體，以及如何允許安裝重要的背景更新。
- tvOS 的最新版本為 17.6.1。了解如何更新 Apple TV 的軟體。
- watchOS 的最新版本為 10.6.1。了解如何更新 Apple Watch 的軟體。
- visionOS 的最新版本為 1.3。了解如何更新 Apple Vision Pro 的軟體。

請注意，在為 iOS、iPadOS、tvOS、watchOS 和 visionOS 安裝軟體更新後，就無法降級為先前版本。

資料來源：APP 官網

檢視行動裝置作業系統安全支援期限

- Windows 10 家用版與專業版將終止服務

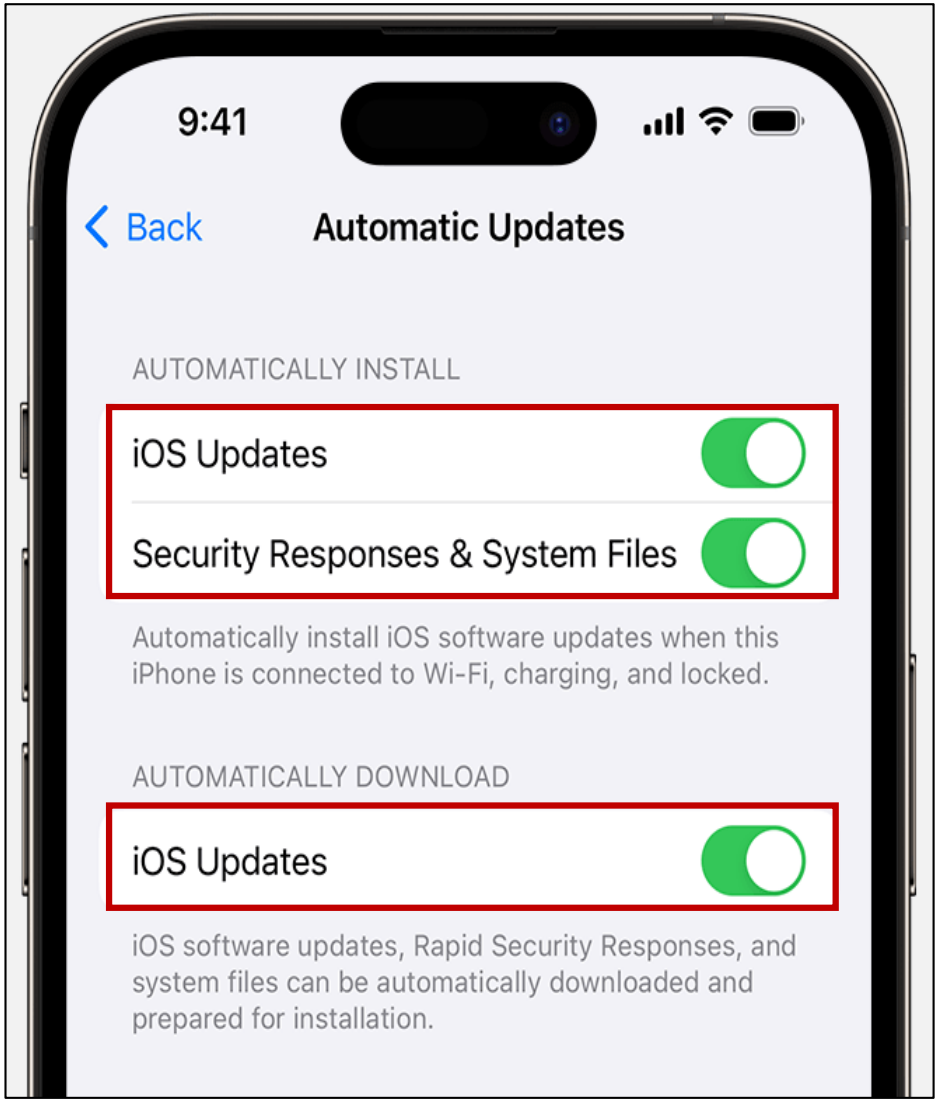
清單	開始日期	退場日期
Windows 10 家用版與專業版	2015年7月29日	2025年10月14日

Version	開始日期	結束日期
Version 22H2	2022年10月18日	2025年10月14日
Version 21H2	2021年11月16日	2023年6月13日
Version 21H1	2021年5月18日	2022年12月13日
Version 20H2	2020年10月20日	2022年5月10日

資料來源：微軟官網

檢查並設定自動安裝更新(IOS)

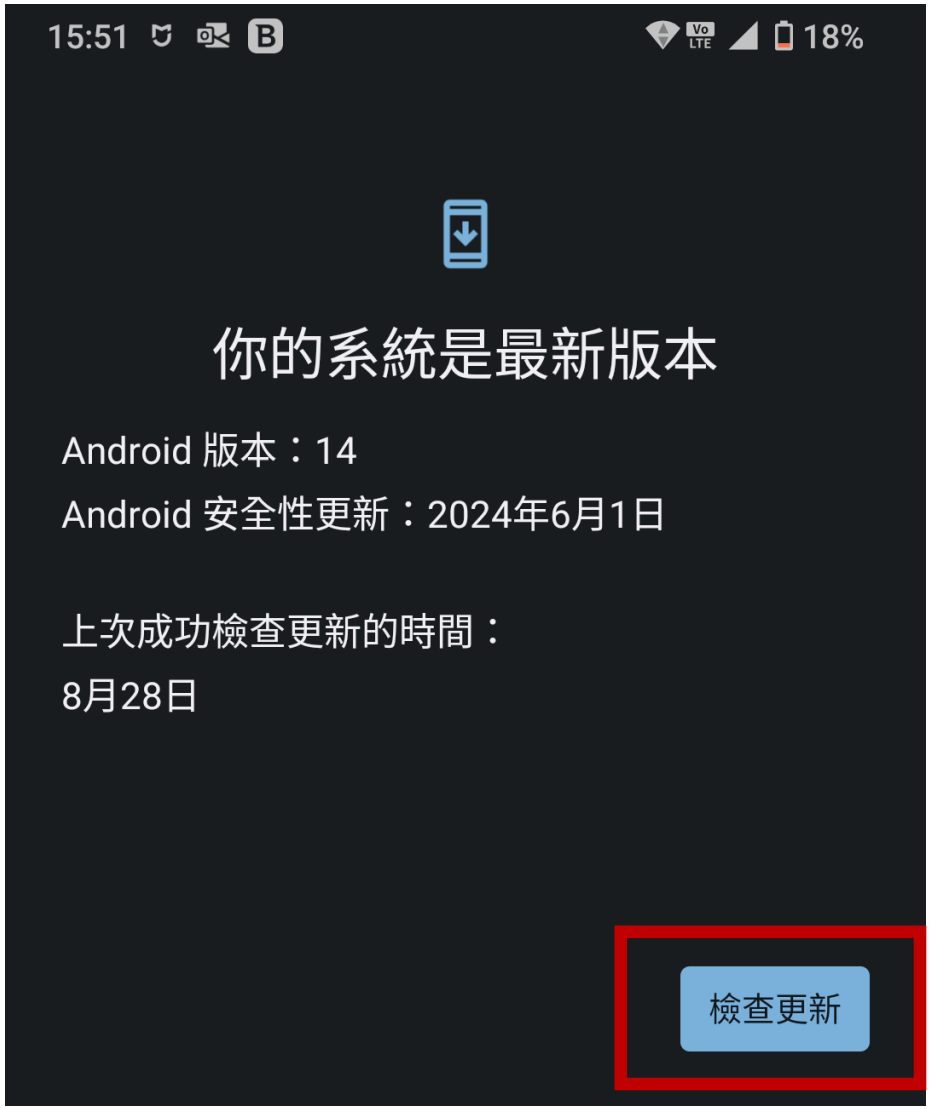
- 前往「設定」>「一般」>「軟體更新」。
- 點一下「自動更新」，然後開啟「下載 iOS 更新項目」。
- 開啟「安裝 iOS 更新項目」。你的裝置會自動更新至最新版 iOS 或 iPadOS。某些更新可能需要手動安裝。



資料來源：APPLE 官網

檢查Android手機作業系統版本

- 「設定」→「系統」→「系統更新」，檢查版本及是否可以進行更新。



資料來源：Google 官網

行動裝置中安裝了這些惡意APP嗎？

時間	2024年2月
案情	➢ 有5款惡意App，包含3款偽裝免費PDF閱讀器，已被下載20萬次，可能內含Anatsa 銀行木馬程式。 ➢ 有3款是PDF閱讀器，分別是：Phone Cleaner - File Explorer 、PDF Viewer - File Explorer和PDF Reader: File Manager。 ➢ 另2款是手機清理工具，名為：Phone Cleaner - File Explorer 、Phone Cleaner: File Explorer。
影響	➢ 竊取用戶的個人資料和網路銀行交易。 ➢ Google已將這些App從Play Store 平台上移除。

資料來源：Newstalk 新聞

飛馬非良馬~間諜軟體肆虐

- 以色列軟體監控公司NSO集團被報出開發飛馬間諜軟體，並出售給各國政府，導致國際政要、企業主管、記者等人士的手機遭監控，共涉及5萬多筆電話號碼。
- 駭客透過零時差攻擊，利用蘋果手機iMessage的安全漏洞，將該惡意軟體傳送到裝置中。
- 這種軟體可讓攻擊方察看手機中的訊息、電子郵件、使用麥克風和相機鏡頭。試圖竊取iPhone的資料和竊聽。

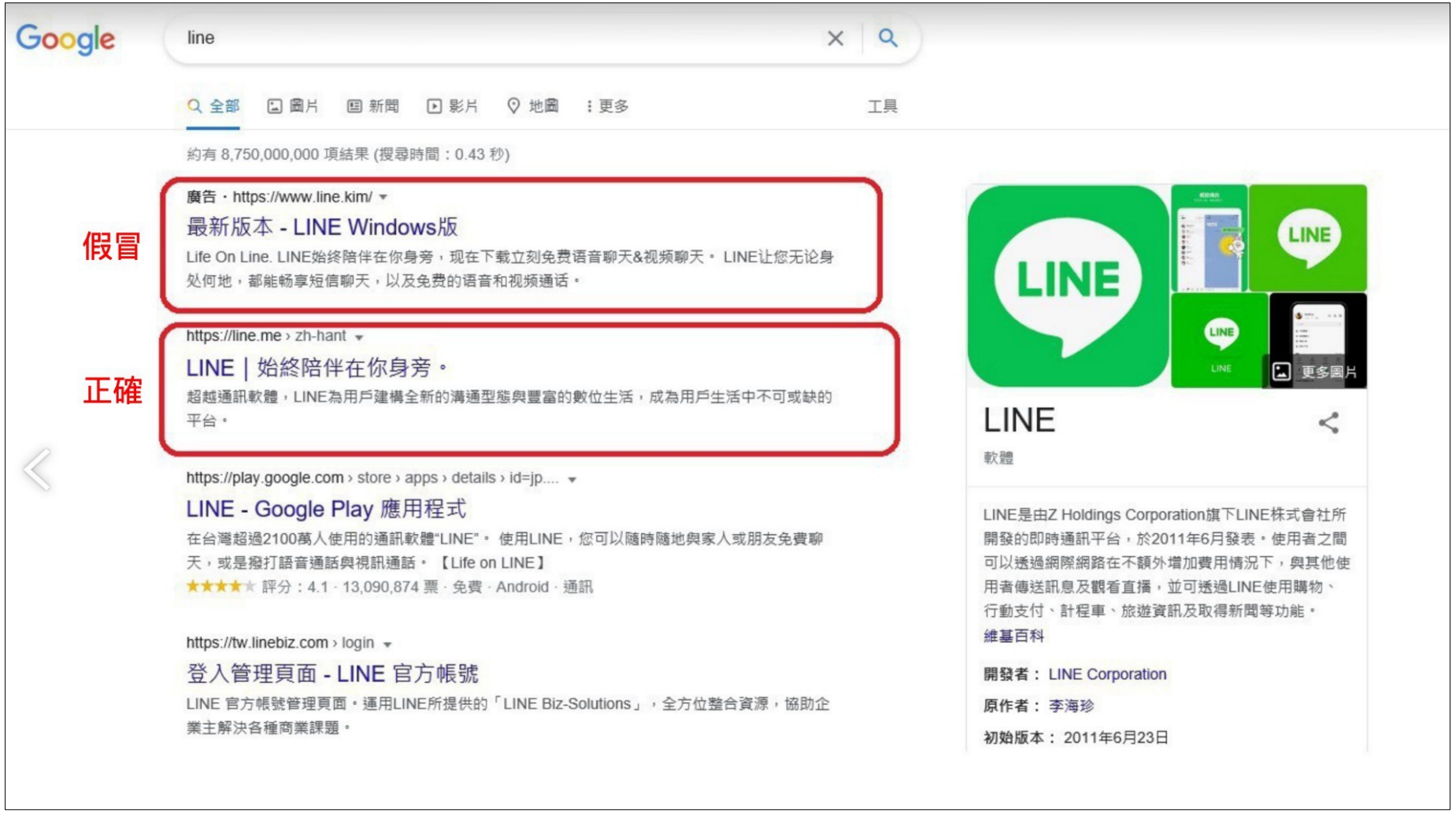
資料來源：聯合新聞網

安裝偽冒軟體之實例

- 案例說明：
  1. 資安院偵測發現某政府機關有偽冒程式之異常連線。
  2. 經調查發現是同仁先前因有網路通訊需求，於公務電腦下載安裝電腦版。
  3. Line 程式，惟不慎下載到非官方之安裝檔，導致公務電腦受駭。
- 防護建議：
  - 機關不應於公務設備安裝非公務使用軟體，如因應業務需求，亦應於官方網站下載業務需求之軟體工具。

資料來源：政府機關資安威脅與防護重點

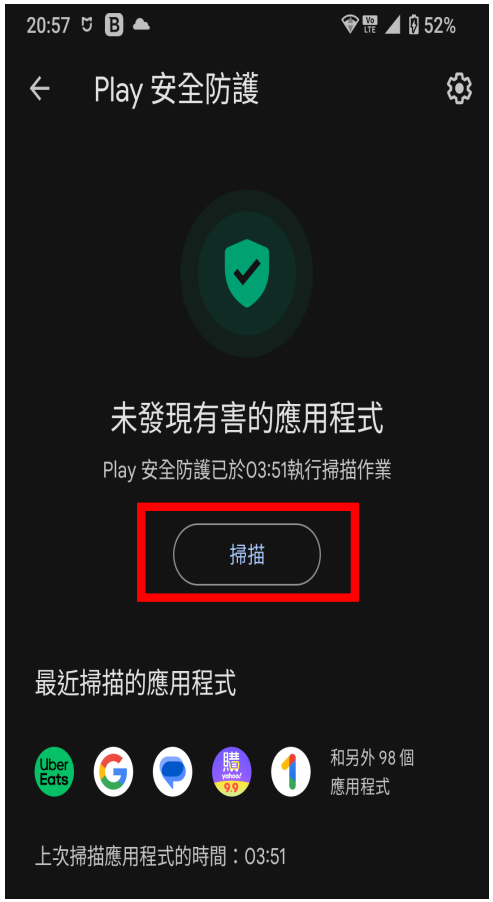
誤中陷阱安裝偽冒程式



資料來源：政府機關資安威脅與防護重點 / https://www.mygopen.com/2021/08/fake-line.html

開啟APP安全性防護(Android)

- 開啟 Google Play 商店應用程式 Google Play。
- 輕觸右上方的個人資料圖示。
- 依序輕觸「Play 安全防護」下一步「設定」圖示 設定。
- 開啟或關閉「透過 Play 安全防護掃描應用程式」。



資料來源：Google 官網

手機可能被駭的徵兆(1/2)

- **電池**
  - 檢查電池的耗電量是否異常增加，沒在使用手機，電量卻異常增加，若有不明程式或根本沒在用的程式，耗電量排前幾名，就有可能是被惡意軟體或病毒感染，最好趕緊刪掉。
- **網路**
  - 若發現行動數據量突然增加，可能是被惡意軟體或病毒感染。
- **聯絡人**
  - 不定期檢查聯絡人的訊息，因為有些駭客會傳奇怪訊息，用惡意軟體散播惡意連結。

資料來源：TVBS 新聞網

手機可能被駭的徵兆(2/2)

- **APP資料庫**
  - 查看APP資料庫中是否有出現未曾安裝的不明應用程式，若有發現就要趕快刪除，以免個資被竊取或遭到監控。
- **郵件**
  - 若收到不知名的郵件且內有相關連結和附件，千萬不要點擊。
- Face ID、Touch ID、指紋辨識
  - 若辨識解鎖裝置無故失效，或發現有人解鎖手機，最好重新製作，並檢查帳號有無異常登入或跳出其他國家的驗證碼時，若有就要馬上改密碼。

資料來源：TVBS 新聞網

5G的快速發展是必然的趨勢

	4G	5G
上傳/下載速度	0.1~1Gbps	1~10Gbps
延遲/回應時間	0.02~0.03秒	0,001秒
頻率	10 GHz 以下	30到300 GHz
優點	低頻覆蓋廣，不用大量基地台	高頻提升傳輸速率
缺點	頻寬小易壅塞	難穿透固體，訊號隨距離快速下降，需建置更多基地台
應用功能	通話、簡訊、網路、1080p影片串流	通話、簡訊、網路、4K影片串流、VR直播、自駕車、遠距手術

各類無線網路環境的安全性比較

5G 行動連網	透過新一代的身份驗證機制，可成功防止仿冒電話、詐騙計費和竊聽等問題。同時對用戶數據的完整性保護，透過加密確保數據在傳輸中的安全性，進一步確保用戶資訊的可信度。
3G/4G 行動連網	訊號傳送數據經過加密。
私設Wi-Fi連線	如辦公室或家中設置的無線網路，可設置需要密碼才能使用，亦可設定加密方式進行資料傳輸。
公共Wi-Fi熱點	如機場、咖啡廳等公共場所提供的無線網路環境，也是最不安全的網路環境，因為無法100%確認處於該環境中是否受到加密保護，除非以額外的安全通道(VPN)來與其連線。

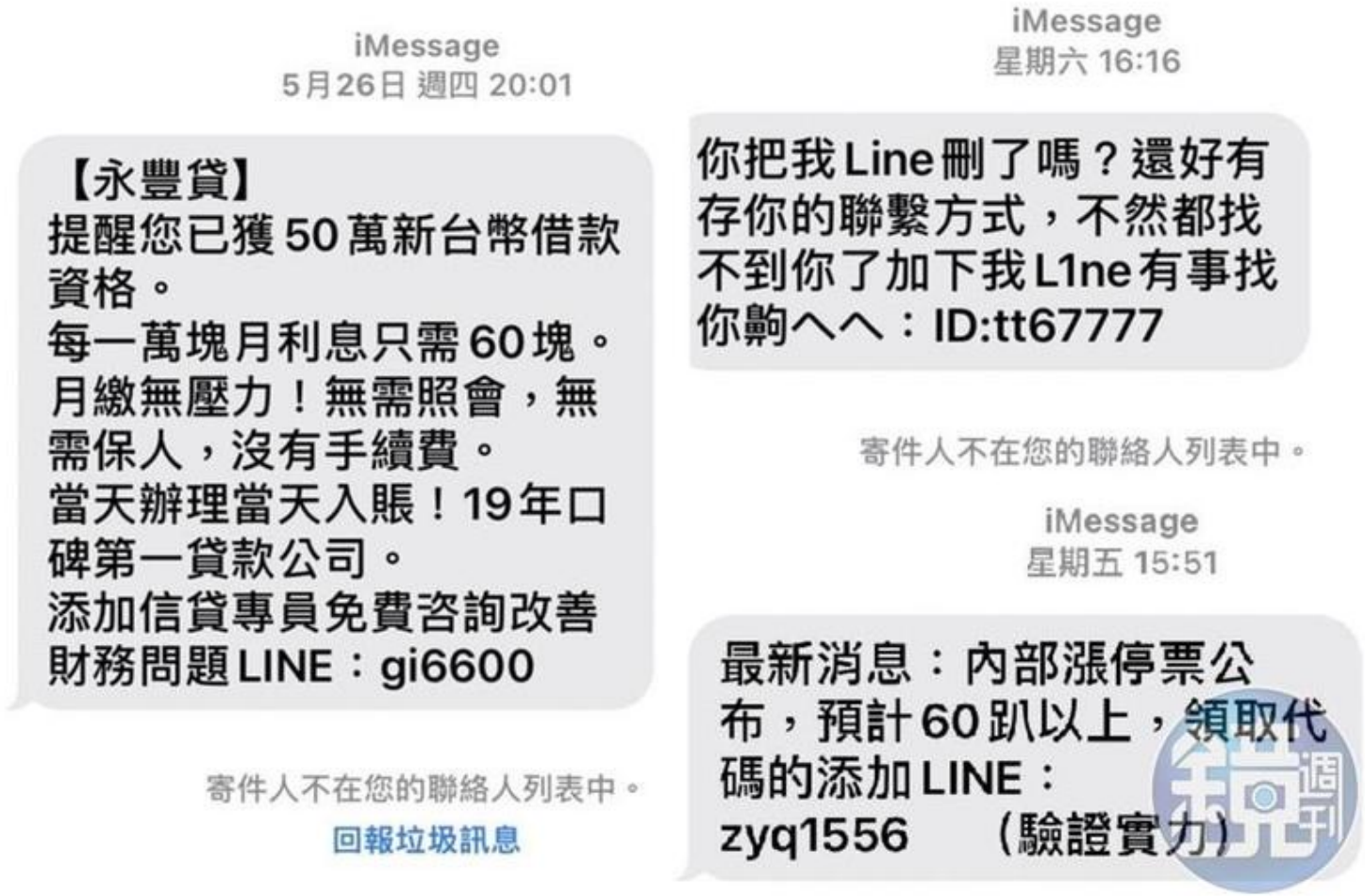
免費的Wi-Fi暗藏風險

- 來源不明且未加密的免費Wi-Fi，竊取資訊。
- 任意連線後被植入惡意程式。
- 引導至特定網頁，開啟連結後進行攻擊。

安全使用公共 WiFi 網路須知

- 確認Wi-Fi網路名稱是否正確
  - 務必檢視核對透過WiFi連線的場所名稱是否正確，以防誤陷偽裝名稱的無線網路環境。
- 避免傳送敏感資料
  - 連上公共WiFi網路，請避免傳送個人敏感資料。
- 使用完畢記得「忘記此網路設定」
  - 使用完畢公共無線網路後，一定要返回網路設置，並清除設定。
- 使用VPN私人虛擬網路
  - 是確保公共無線網路連線最安全的選擇，可以隱藏你的IP位址並可加密上網數據流量。

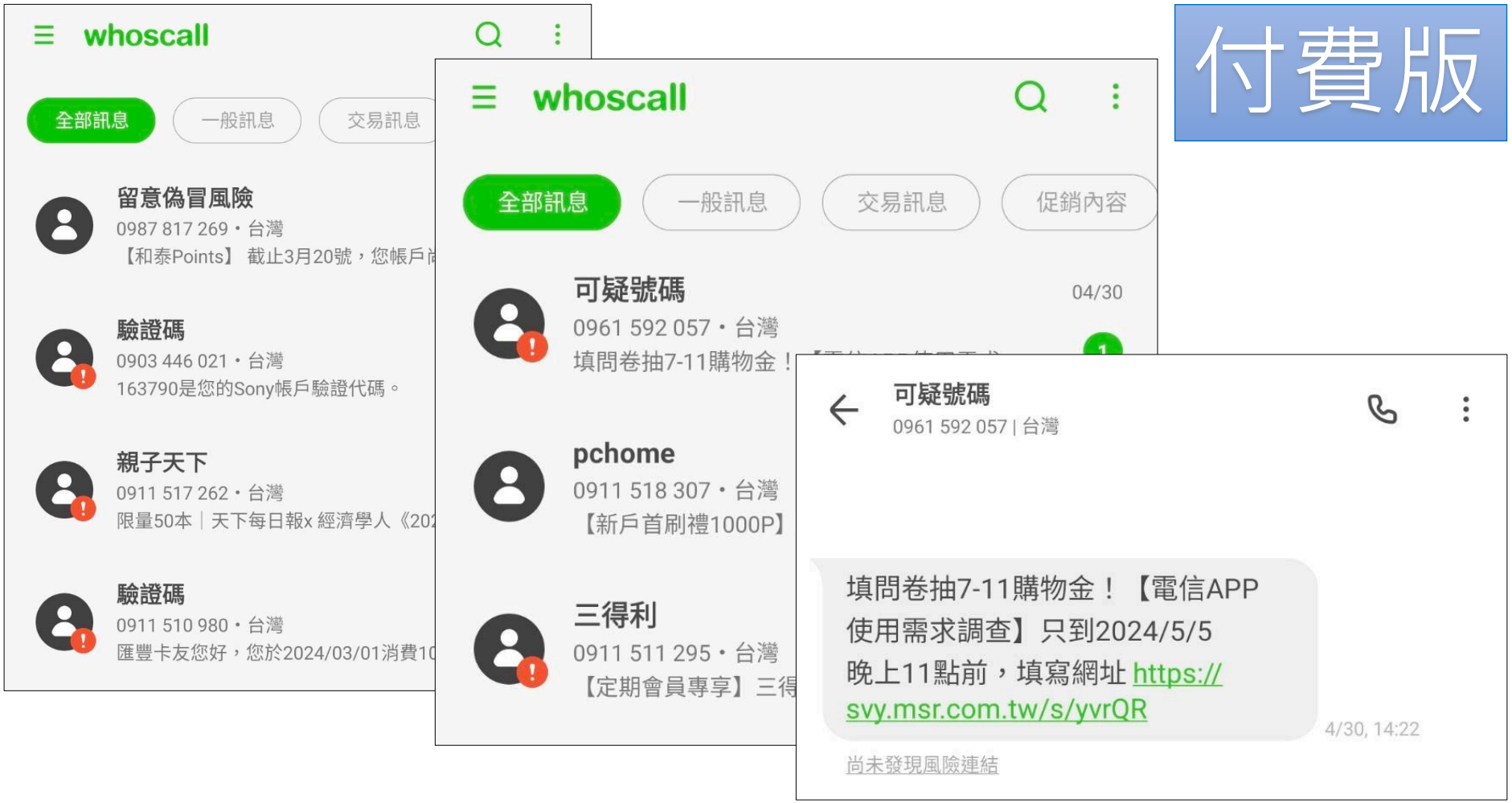
詐騙簡訊實例



資料來源：鏡週刊

使用Whoscall 阻擋惡意簡訊(1/2)

使用Whoscall 阻擋惡意簡訊(2/2)



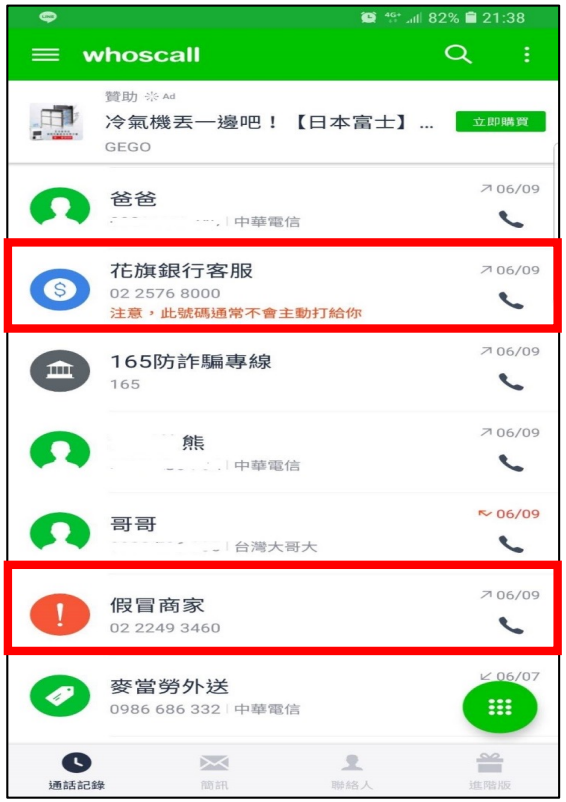
付費版

採用安全的作業系統與安裝防毒軟體

- 除了產品的品牌外更應考量所搭載的作業系統是否安全並保持更新。
- 不論電腦設備或手機均應安裝防毒軟體並定期更新。

對來電進行過濾與拒接不明來電

- 如果不確定是信任的熟人的來電最好勿接。
- 安裝來電過濾APP以過濾廣告、推銷或詐騙集團的來電。



慎防周邊裝置成為資安漏洞

- 當作贈品或意外撿到的隨身碟可能有惡意軟體藏身其中。
- 店家或陌生人提供的傳輸線(電力線)可能遭修改成具有將資料傳輸至指定位置功能的線材。
- 公共場所或店家提供作為充電的USB連接埠，可能設有擷取資訊的裝置。

採取正確措施以避免資安風險

- 不要隨意購買使用來路不明的Lightning傳輸線。
- 購買原廠充電線，或選擇有MFI認證，包裝上面有經過品牌認證的充電線。
- 建議儘可能使用自備電源，如行動電源、充電器 (豆腐頭)。
- 外接充電時應避免瀏覽或登入需輸入帳號密碼的網站，如金融機構的網站、購物網站、社群平台...等。

勿因小失大，選用安心的周邊商品

資料來源：GUSHA https://www.gusha.com.tw/

便利與安全的兩端

- NFC工具帶來便利的支付過程。
- 風險之一是近距離竊取資訊。
- 偽造POS讀取設備及偽造支付窗口可進行詐騙。

妥善使用行動支付工具

- 透過網路輸入的任何資訊都要謹慎小心。
- 妥善且嚴謹的管理自己的帳戶。
- 務必開啟螢幕鎖定功能。
- 能夠高額支付的APP請開啟鎖定功能。
- 開啟「GPS」跟「尋找裝置」功能。
- 利用安全的行動支付服務。
- 不再使用的支付APP請解除安裝。

資料來源：https://blog.trendmicro.com.tw/?p=62377

常見的網路社交工程手法

- 常見的詐騙與攻擊手法：
  - 假冒為同事或新進員工
  - 假冒廠商、客戶或政府單位
  - 假冒具有權威的人
  - 假冒系統廠商，表示欲提供系統修補程式或更新程式
  - 假冒好心人士，告訴對方如果電腦發生問題可以找他，然後製造問題，讓受害人打電話來求援...等。
  - 使用流行或特定關心的議題

都有一個假網址

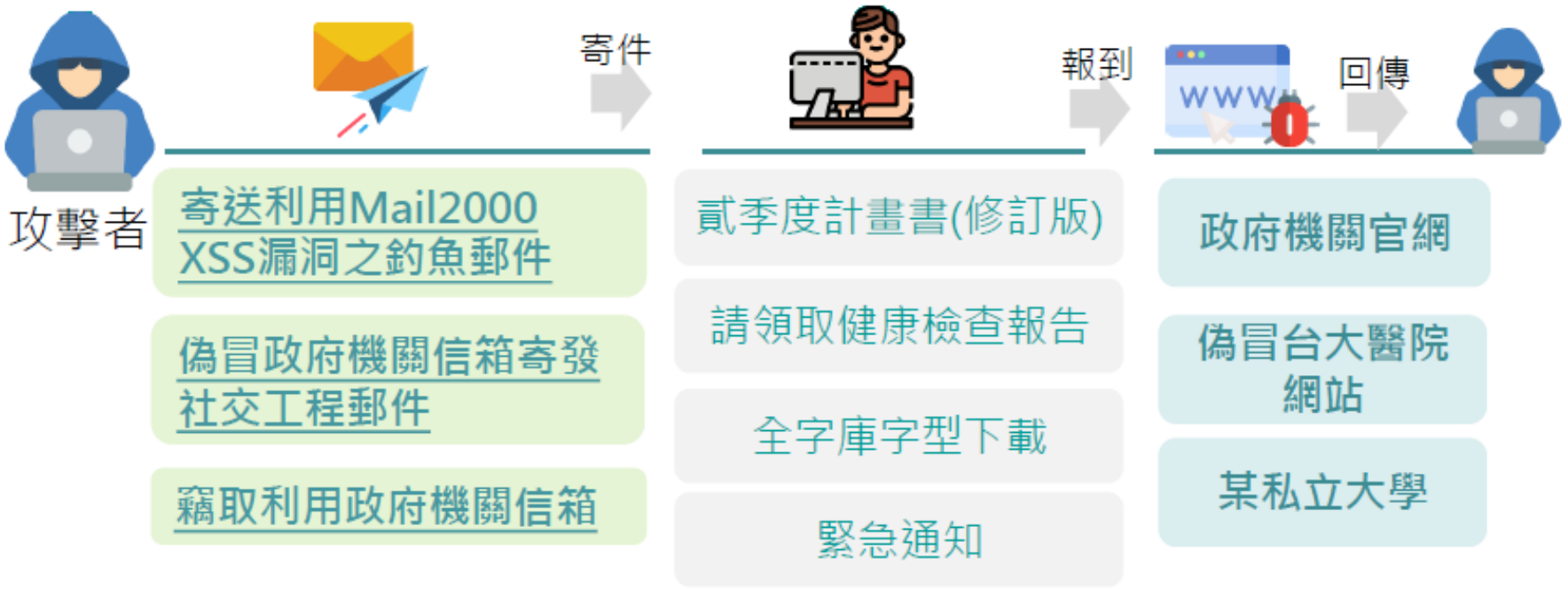
- 社交工程攻擊常鎖定的目標：
  - 一般人員
  - 新進員工或特定業務人員

社交工程郵件案例(1/2)

- 案例說明：
  1. 駭客利用 Webmail 零時差漏洞，將 XSS 跨站腳本注入社交工程郵件。
  2. 當收件者透過 Webmail 開啟社交工程郵件，將觸發 XSS 跨站腳本攻擊並連線至外部含惡意程式碼之網頁。
  3. 駭客利用 Webmail 零時差漏洞、偽冒政府機關信箱寄發釣魚郵件。
  4. 收件人誤以為是業務相關或系統管理員通知軟體更新等因素，開啟點擊惡意信件。
- 防護建議：
  1. 加強內部宣導，注意郵件來源正確性，勿開啟不明來源之郵件與相關附檔及連結。
  2. 請注意個別系統之安全修補與病毒碼更新。
  3. 確認網站連結正確性，避免點擊駭客偽裝可信網站之假網址。

資料來源：政府機關資安威脅與防護重點

社交工程郵件案例(2/2)



資料來源：政府機關資安威脅與防護重點

慎用公務電子郵件

時間	2024年3月
案情	➢ 數位部資安署最新一期資通安全網路月報，發現部分公務人員使用公務信箱註冊在非公務網站，導致帳密外洩案例。 ➢ 如果外部網站遭駭，駭客可能從公務信箱發現是公務人員，相關帳號、密碼及使用者個資等資料都將同步曝險，若個人使用在外部服務的密碼又跟公務系統相同，就可能有資安風險。使用者的電腦系統及軟體也應該定期更新及掃毒，以維護資通安全。 ➢ 近期駭客利用微軟Outlook電子郵件服務，針對政府機關人員寄送主旨為「投訴政府人員不作為」，內含惡意附檔的社交工程電子郵件，企圖誘騙收件人開啟惡意附檔以植入後門程式，進而竊取機敏資訊，相關情資已提供各機關聯防監控防護建議。
影響	● 公務電子郵件誤用導致單位資安風險

資料來源：聯合新聞網

養成良好習慣杜絕社交工程攻擊

- 勿瀏覽未受安全保護的網頁或下載不明來源的檔案。
- 勿使用狀態不明的外接裝置(USB、記憶卡等)。
- 勿點選不明的連結或開啟不明來路的信件。
- 勿使用郵件預覽功能。
- 瀏覽器安全性應設為中高等級以上。
- 瀏覽器不可設定自動記憶密碼。
- 外寄郵件如有附加機敏性檔案應加密處理。

生活習慣洩漏個資

- 健康手環、智慧家電帶來更便利及更有品質的生活，同時帶來風險。

妥善的保管及維護帳戶密碼

- 屬於財務金融或重要的網頁，不要設定自動密碼(記住密碼)的方式來進行登入。
- 密碼應定期進行更換並增加強度。
- 金融及重要網頁使用完畢務必執行登出。
- 定期檢查帳戶登入登出確保無異常狀況，並設定交易提醒。
- 勿輕易提供帳號密碼給未經查證身分的他人。

使用行動裝置之安全原則

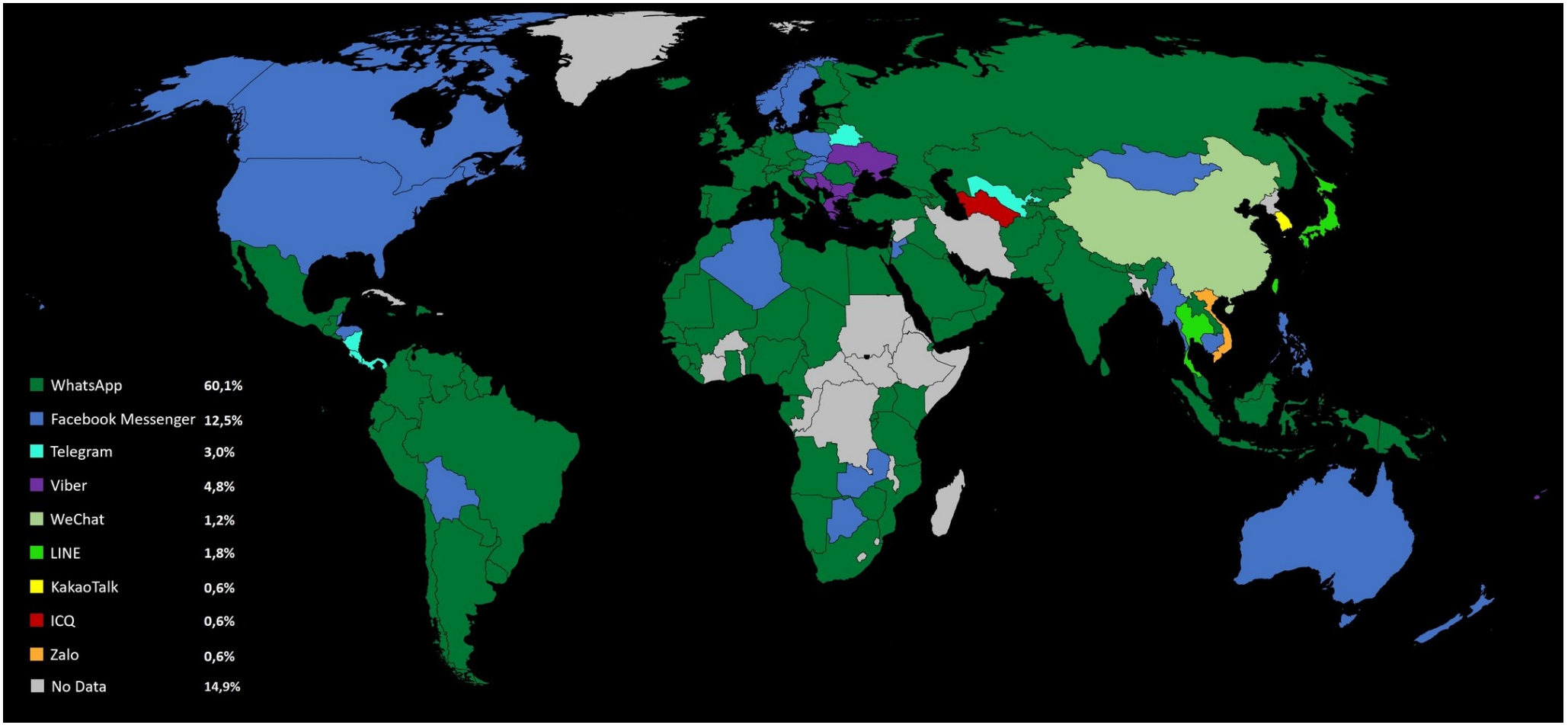
- 以連接線連結外部裝置(USB、充電設備)時務必確認是否安全。
- 不任意下載未知來源的APP，官方平台下載前先瀏覽評價與使用者留言。
- 在公共場所以手機進行金融或機敏業務時盡量使用3G/4G/5G的網路通訊並關閉藍芽。
- 過濾來電避免騷擾與詐騙。
- 使用金融或機敏服務如有雙重認證機制，務必使用。
- 不隨意將手機借與陌生人使用。以手機使用網路時，不論網頁或郵件，勿任意開啟不明的連結。
- 使用NFC裝置進行交易時，應在付款時再開啟該功能。

日常活動時要注意保護個資

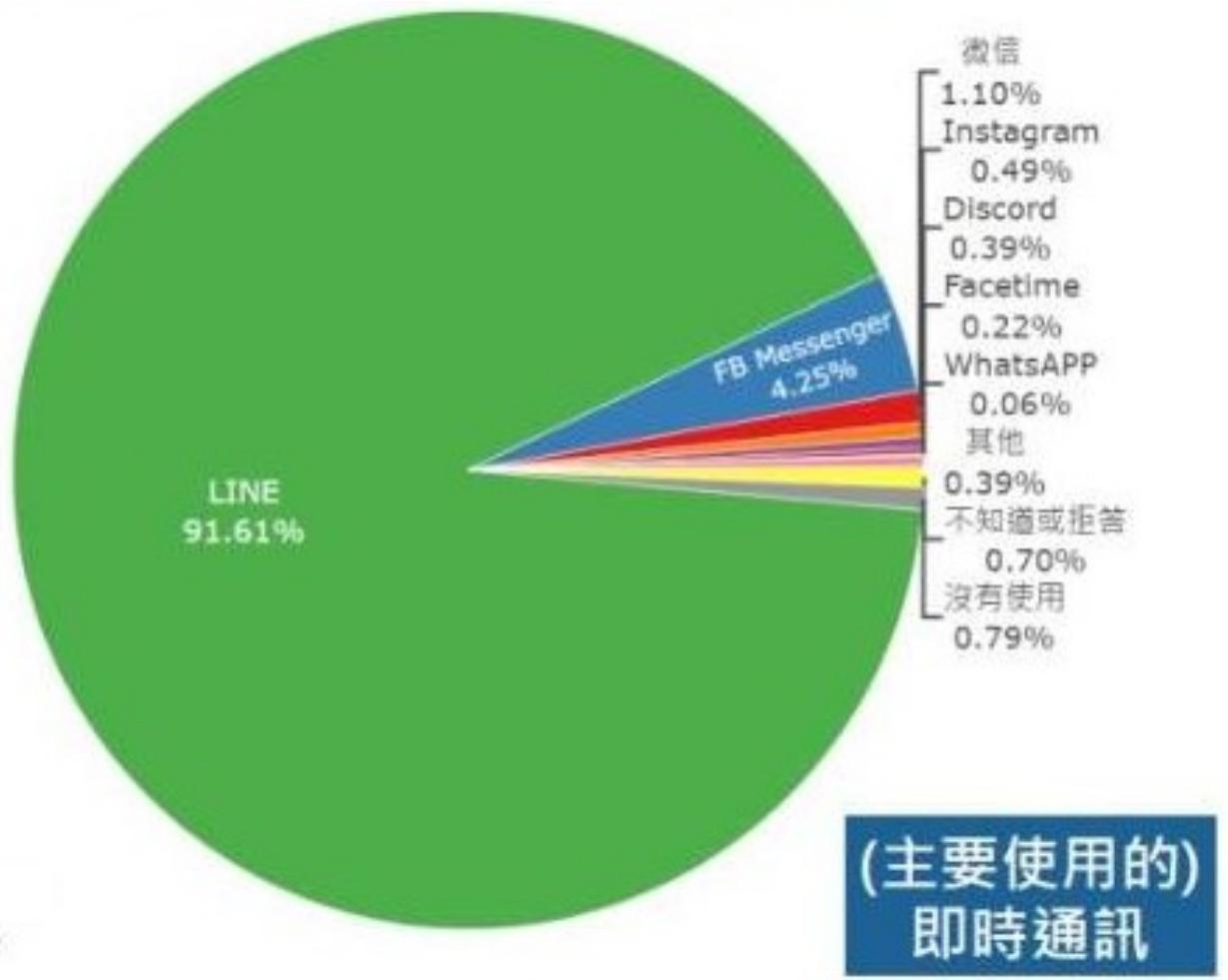
- 社交場合，非熟人勿輕易透露個人資訊。
- 可疑網站勿入、郵件勿任意開啟以防個資被竊。
- 拍照時關閉記錄拍照地點的GPS功能，或移除照片座標位置資訊。
- 拍照時要注意背景反射位置是否透漏地點資訊。
- 自拍照上傳時，除了修圖外，也要確認移除附帶的個人資訊。
- 建議將照片畫質降低，再公開到網路上。
- 含有個資的紙本資料應用碎紙或焚毀的方式處理。
- 使用需登入帳號密碼的服務時，記得於結束後登出。
- 如遇詐騙事件，即電165或報警處理。
- 關閉社群網站的公開資訊功能。

消弭通訊軟體的隱憂

各國最受歡迎通訊軟體


WhatsApp 60,1%
Facebook Messenger 12,5%
Telegram 3,0%
Viber 4,8%
WeChat 1,2%
LINE 1,8%
KakaoTalk 0,6%
ICQ 0,6%
Zalo 0,6%
No Data 14,9%

台灣使用通訊軟體之分佈(2023年)



資料來源：財團法人台灣網路資訊中心

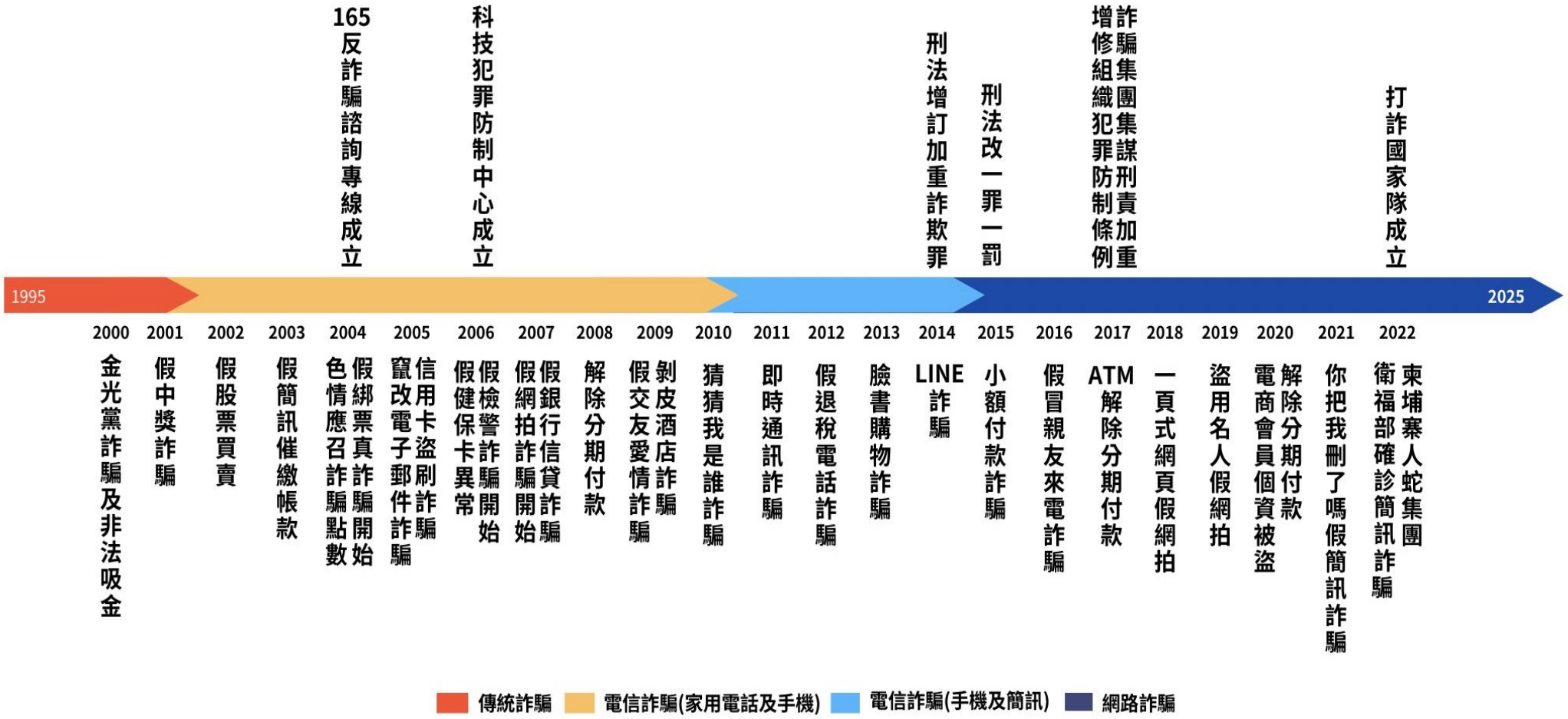
通訊軟體常見之隱患

- 不明人士的交友邀請，套取個資或重要資訊。
- 傳送不明連結或檔案，點擊或開啟後植入後門或木馬病毒。
- 盜用親友之通訊軟體帳號，行詐騙之實。
- 利用通訊軟體散佈假消息，製造恐慌或帶風向。

常見通訊軟體詐騙之手法

- 冒充詐騙
- 驗證碼詐騙
- 免費禮品卡和優惠券
- 陌生的QR Code
- 傳送假的通訊軟體程式
- 中獎詐騙
- 透過加密貨幣快速致富
- 慈善詐騙
- 視訊電話詐騙
- 客服詐騙
- 好到爆的工作機會

台灣詐騙手法之演進



資料來源：ETtoday 新聞雲

通訊軟體頻生資料外洩事件

韓通訊軟體KakaoTalk外洩至少6.5萬用戶個資遭重罰3.6億

2024/5/23 12:46（7/4 00:19 更新）

KakaoTalk是韓國國內最多用戶使用的通訊軟體服務。（路透社）

87

（中央社記者廖禹揚首爾23日專電）韓國網路龍頭之一的Kakao因旗下通訊軟體KakaoTalk漏洞，據調查至少導致6萬5000名用戶個資外洩，今天遭當局重罰約151億韓元（約新台幣3億6000萬元），刷新最高罰款紀錄。

韓國個資保護委員會今天召開全體會議，做出以上決議。KakaoTalk去年3月爆出開放聊天室用戶個資遭非法買賣，個資委就此展開調查，認定Kakao並未做好應有的資安保護措施，依違反相關規定開罰151億4976萬韓元。

Line母公司遭遇網路攻擊，44萬用戶、合作夥伴、員工個資恐外洩，臺灣也有用戶資料曝險

11月27日即時通訊軟體Line母公司LY Corporation發布資安通告，指出他們與Naver共用的資訊系統遭到入侵，估計有44萬筆用戶、合作夥伴、員工的個資外洩

文/ 周峻佑 | 2023-12-03 發表

讚 14 分享

LINEヤフー

お知らせ
2023.11.27
LINE ヤフー株式会社

不正アクセスによる、情報漏えいに関するお知らせとお詫び

LINE ヤフー株式会社は、このたび、第三者による不正アクセス（以下、本事案）を受け、ユーザー情報・取引先情報・従業者等[1]に関する情報の漏えいがあることが判明しましたのでお知らせいたします。

本件につきまして、以下の通り報告いたしますとともに、ユーザーおよび関係者の皆さまに多大なるご迷惑とご心配をおかけする事態となりましたことを、心より深くお詫び申し上げます。

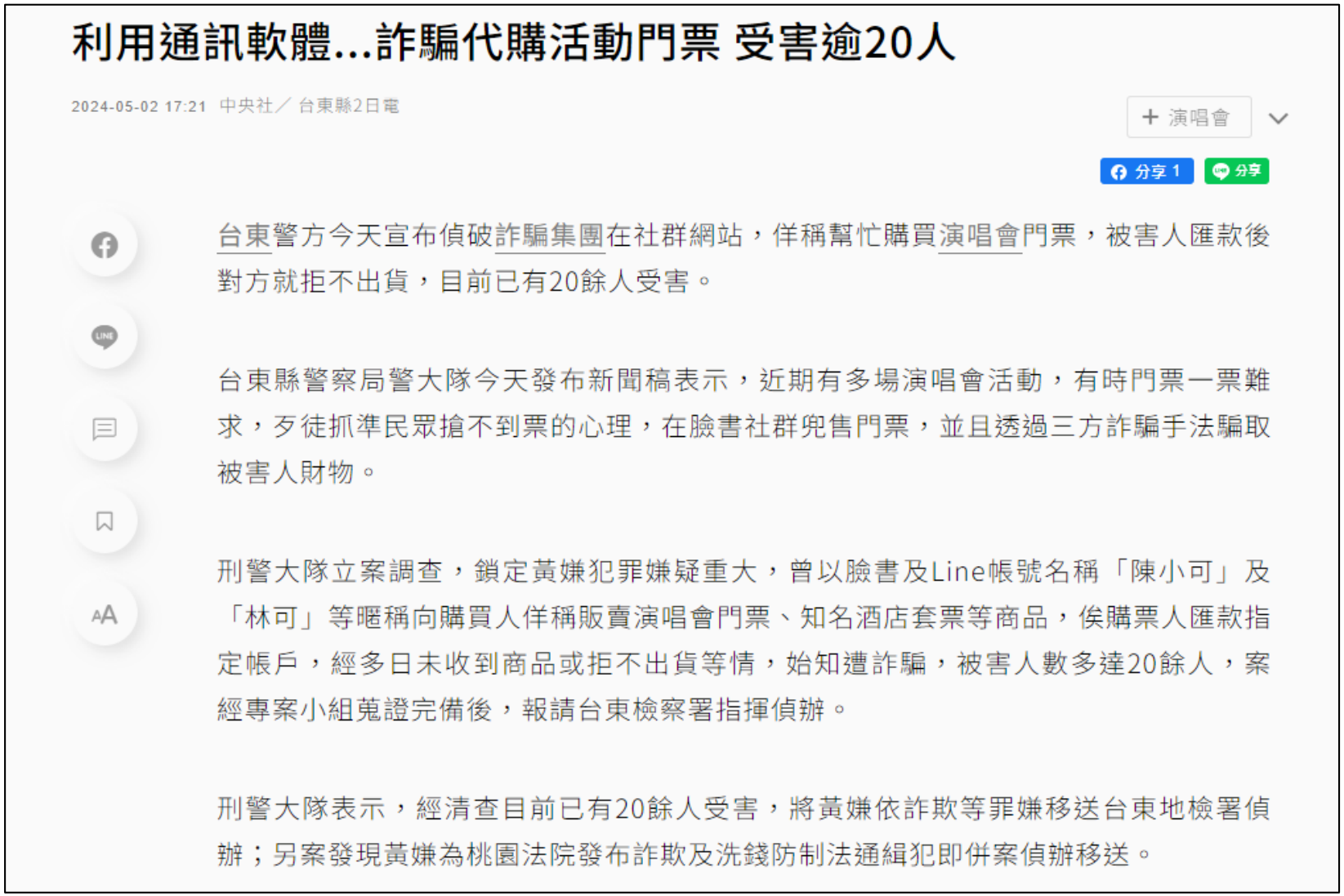
なお、後述の当社へのアクセスの経路となったと推測される当社関係会社のシステムからは、当社の各サーバーに対するアクセスを遮断しております。11 月 27 日時点でユーザー情報や取引先情報を利用した二次被害の報告は受けておりませんが、引き続き影響調査を進め必要な対応が発生した場合は速やかに対応してまいります。

兩年半前，即時通訊軟體Line日本公司傳出資料外洩疑雲，當時該公司數度發布公告，澄清用戶資料並未儲存在中國，並取消上海子公司對開發資料的存取權限，包含了Line調查機構內容管理系統（CMS）、監控業務CMS、問卷開發、頭像、Line應用程式中的OCR開發，以及Keep功能開發的權限。最近該公司再度出現資料外洩事故，但這次是供應鏈攻擊導致。

即時通訊軟體Line母公司LY Corporation（LYC，原Z Holdings）發布資安通告，指出他們偵測到未經授權的第三方於10月9日存取該公司系統，而有可能導致使用者、業務合作夥伴、員工等人士的資訊遭到洩露。

資料來源：網路新聞彙整

利用人性弱點進行詐騙



利用通訊軟體...詐騙代購活動門票 受害逾20人

2024-05-02 17:21 中央社／台東縣2日電

+ 演唱會

分享 1 分享

台東警方今天宣布偵破詐騙集團在社群網站，佯稱幫忙購買演唱會門票，被害人匯款後對方就拒不出貨，目前已有20餘人受害。

台東縣警察局警大隊今天發布新聞稿表示，近期有多場演唱會活動，有時門票一票難求，歹徒抓準民眾搶不到票的心理，在臉書社群兜售門票，並且透過三方詐騙手法騙取被害人財物。

刑警大隊立案調查，鎖定黃嫌犯罪嫌疑重大，曾以臉書及Line帳號名稱「陳小可」及「林可」等暱稱向購買人佯稱販賣演唱會門票、知名酒店套票等商品，俟購票人匯款指定帳戶，經多日未收到商品或拒不出貨等情，始知遭詐騙，被害人數多達20餘人，案經專案小組蒐證完備後，報請台東檢察署指揮偵辦。

刑警大隊表示，經清查目前已有20餘人受害，將黃嫌依詐欺等罪嫌移送台東地檢署偵辦；另案發現黃嫌為桃園法院發布詐欺及洗錢防制法通緝犯即併案偵辦移送。

資料來源：中央社

幾個徵兆識破通訊軟體詐騙

- 訊息來自陌生的號碼和群組。
- 內容含不順暢的語言，包括文法、拼字錯誤。
- 帶有未知連結和附件的電子郵件。
- 聲稱慶祝任何公司週年紀念日的消息。
- 要求你立即採取行動的訊息。

慎防通訊軟體誘騙

- 封鎖不明來源之任何訊息，勿因好奇心成為詐騙者的獵物。

資料來源：刑事警察局

更改通訊軟體設定(1/4)

- 「設定」→「隱私權設定」→ 開啟「Letter Sealing」。

更改通訊軟體設定(2/4)

- 「設定」→「我的帳號」→「允許自其他裝置登入」，如不會使用電腦或平板登入 LINE，建議將此功能關閉。

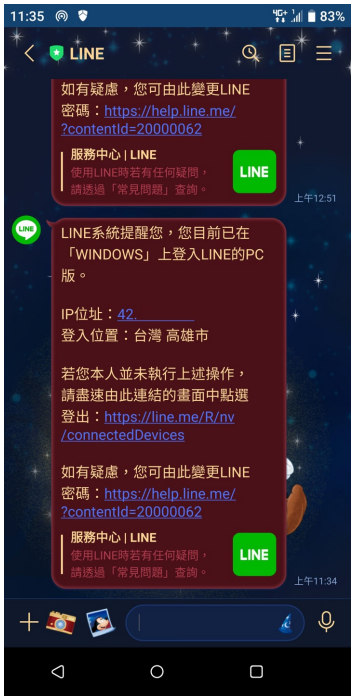
更改通訊軟體設定(3/4)

- 「設定」→「我的帳號」→ 確認「登入中的裝置」中的設備是否為您本人的，如不是則按「登出」將其登出。

註：此為開啟「允許自其他裝置登入」功能時的檢測方式。

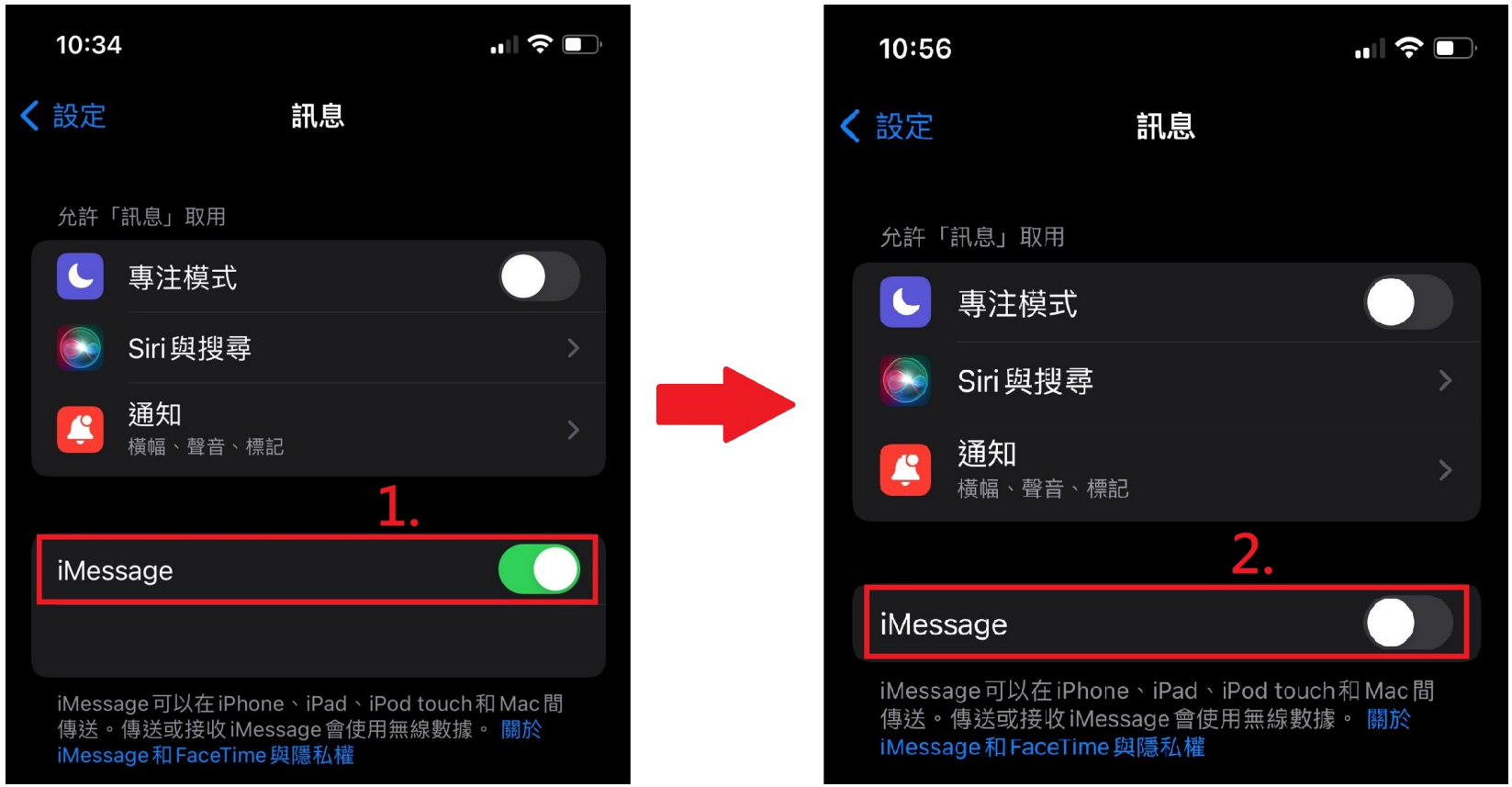
強化通訊軟體安全設定(4/4)

- 開啟「允許自其他裝置登入」，當有設備以您的帳號登入 LINE 時，您會收到 LINE 的安全性通知。如登入的不是您本人，依前述投影片 (3/4) 步驟將其登出。



iMessage 通訊軟體關閉方式(1/2)

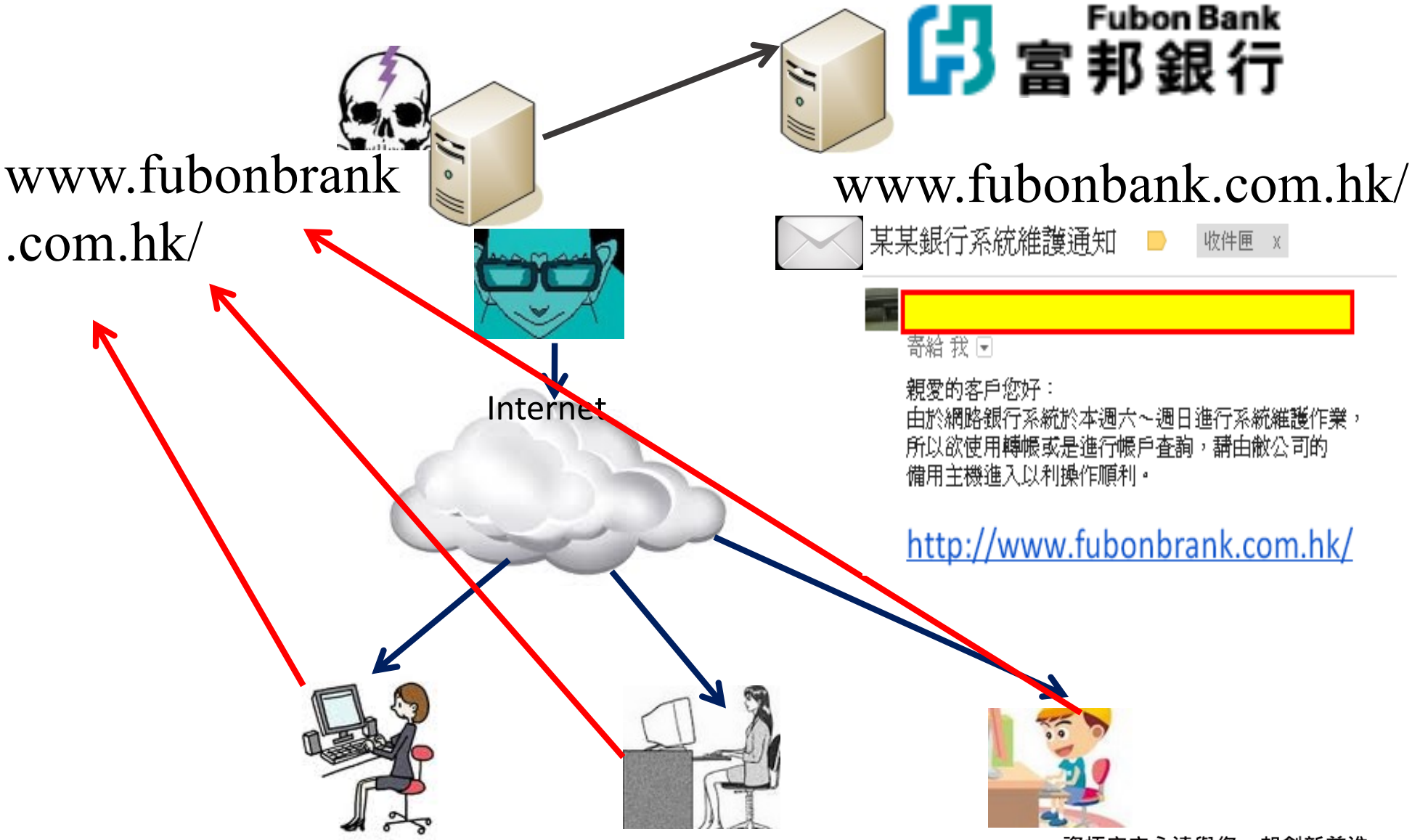
- Android 及 iOS 建議可安裝 Whoscall。
- iOS 如未使用 iMessage，建議可關閉 (如下圖)。



網路釣魚(Phishing)

- 是一種駭客讓用戶傳送敏感資訊的手法，例如傳送密碼與身分證號碼等。
- 一般來說包含傳送看起來像是來自可信任來源的垃圾郵件或通訊軟體中的訊息，例如親友、常用銀行或其他權威機構，內含檔案或連結，點擊後連結到一個假冒的詐騙網站。
- 受害人未經查證就輸入了駭客想要的資訊，並認為自己正在瀏覽自己信任的網站。

網路釣魚概念示意(1/2)


www.fubonbrank
.com.hk/
Fubon Bank
富邦銀行
www.fubonbank.com.hk/
某某銀行系統維護通知
收件匣 x
寄給 我
親愛的客戶您好：
由於網路銀行系統於本週六~週日進行系統維護作業，
所以欲使用轉帳或是進行帳戶查詢，請由敝公司的
備用主機進入以利操作順利。
http://www.fubonbrank.com.hk/
Internet

網路釣魚概念示意(2/2)

某某銀行系統維護通知 收件匣 x

寄給 我

親愛的客戶您好：
由於網路銀行系統於本週六~週日進行系統維護作業
所以欲使用轉帳或是進行帳戶查詢，請由敝公司的
備用主機進入以利操作順利。

http://www.fubonbrank.com.hk/

www.fubonbrank.com.hk/

簽入項目: 請選擇..
身分證號/統一編號:
使用者代碼:
動態鍵盤 密碼:

www.fubonbrank.com.hk/

登入失敗. 原因: EP36 身分證字號/統一編號或使用者代碼錯誤 .
一般網銀客戶簽入 | Login with ATM card
簽入項目: 請選擇..
身分證號/統一編號:
使用者代碼:
動態鍵盤 密碼:
晶片金融卡簽入說明 確定 清除

www.fubonbank.com.hk/

簽入項目: 請選擇..
身分證號/統一編號:
使用者代碼:
動態鍵盤 密碼:

詐騙Line ID

編號	帳號	通報日期
1	wanq01268	2024-08-29 00:00
2	andylin178	2024-08-29 00:00
3	@525llidb	2024-08-29 00:00
4	yuhuan758	2024-08-29 00:00
5	@198oxuyx	2024-08-29 00:00
6	ccc_158_	2024-08-29 00:00
7	li606147	2024-08-29 00:00
8	fy495	2024-08-29 00:00
9	@854gqsol	2024-08-29 00:00
10	btproy	2024-08-29 00:00
11	ktm35790	2024-08-29 00:00
12	@828geuox	2024-08-29 00:00
13	jian6888668	2024-08-29 00:00
14	yzj8866	2024-08-29 00:00
15	lp889900	2024-08-29 00:00
16	yashq223344	2024-08-29 00:00

資料來源：刑事警察局

投資詐騙網址

網站名稱	網址	件數
天宏證券櫃買中心	www.nsjer.com	16
兆品	www.reutyfjkg.com	16
唐吉訶德	www.oupeidesrlf.com	16
CFT	tw.cftbit.com	9
Etoro	www.fgfgr.com	9
利億	www.clsoie.com	9
恆上智選	www.sivvm.top	9
LSE（London Stock Exchange）	www.yjzzuz.shop	8
TikTok Shop	appdownload.apptiktokshop.top	8
格林證券	app.pztvap.top/pztvap/	8
Arbilrum HDEA Bridge	www.naeabridgef.com	7
BSF Exchange	bsfexchange.com	7
coinlion	www.coinlionr.com	7
FTUK	www.ftukwez.com	7

資料來源：刑事警察局

慎防網路釣魚(1/2)

掛斷電話勿回撥，查詢官方資訊安全高

掛電話勿回撥，查詢官方客服電話及網址確認資訊，切勿直接從簡訊或E-Mail上點擊連結。

善用工具識別網站安全性

- 檢視網址列是否出現“不安全”網站提示。
- 利用如Virustotal資安檢測工具檢測網站安全性。

識破釣魚網址偽裝術

部分按鈕、連結可能會在點選之後沒有反應，也可能出現輸入任何帳號密碼都可以輕易登入的狀況。

救人一命，勝造七級浮屠

撥打165反詐騙專線舉報。

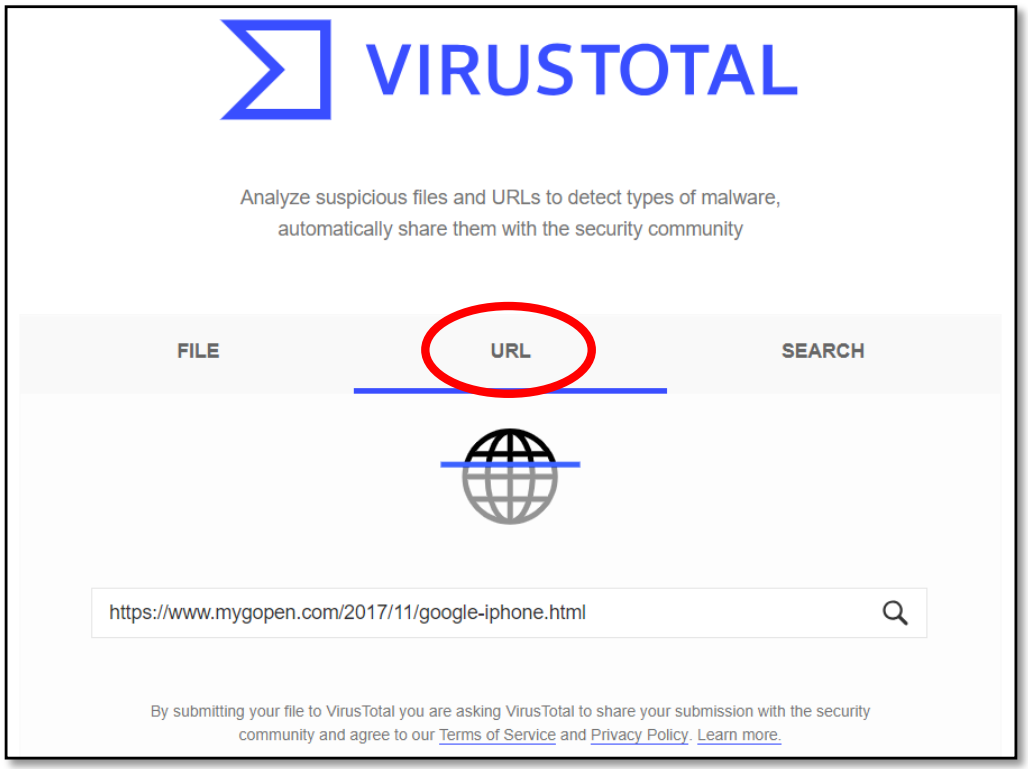
資料來源： https://blog.trendmicro.com.tw/?p=66948

慎防網路釣魚(2/2)

- 對於詢問您個人資料的對話提高警覺
- 不要隨意點選訊息中的網址連結及開啟附件
- 勿貪小便宜點選好康連結
- 定期檢查交易紀錄與網站帳號
- 如需要傳送個人資料或敏感檔案請用其他途徑
- 使用安全有效的防護產品
- 主動回報釣魚網站資訊

VirusTotal 網址檢測(1/2)

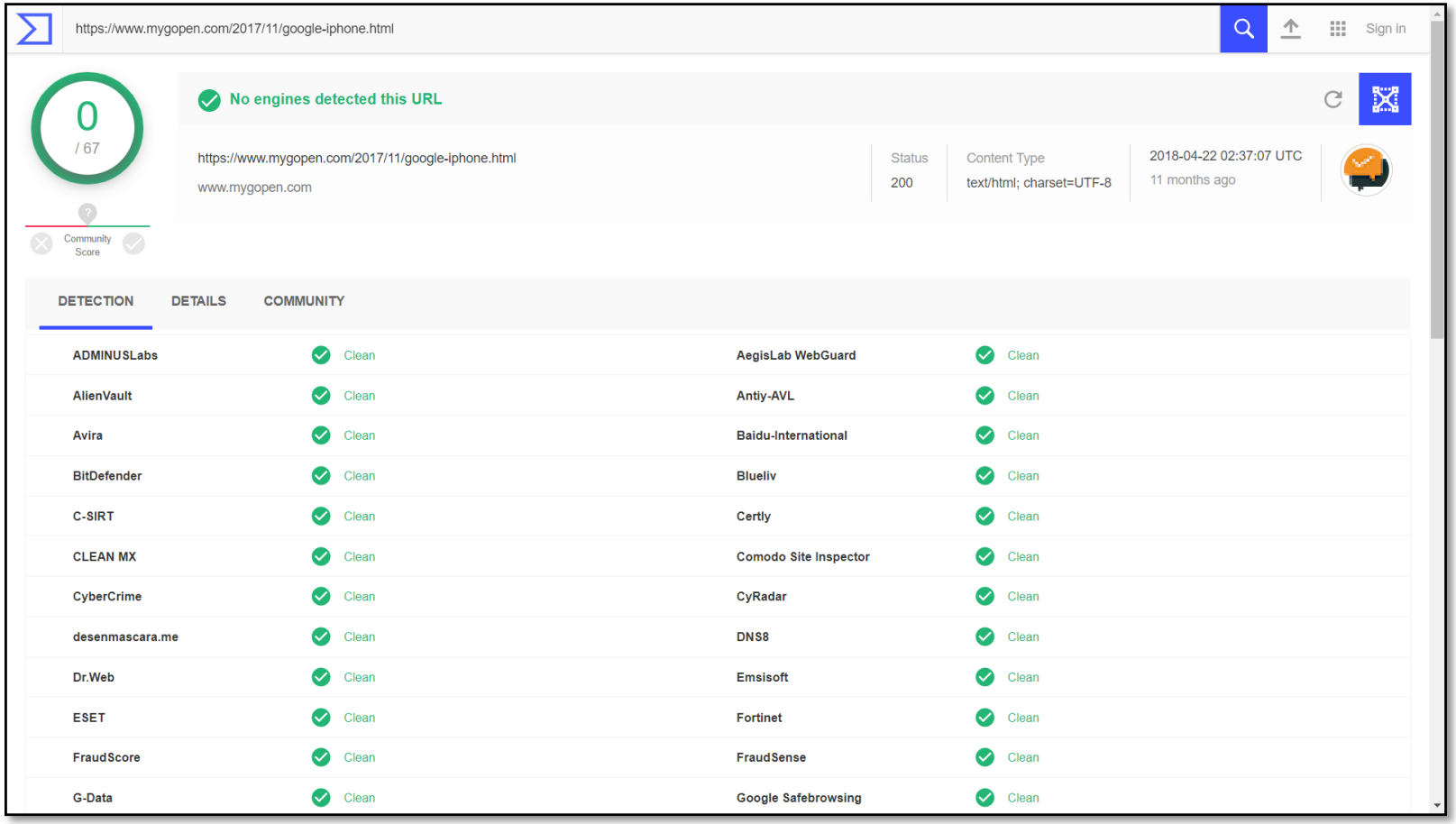
- 從 Google 旗下的 VirusTotal 輸入網址，按下「搜尋或掃描 URL」就可迅速得知網站是否潛藏著威脅。



資料來源：https://free.com.tw/virustotal/

VirusTotal 網址檢測(2/2)

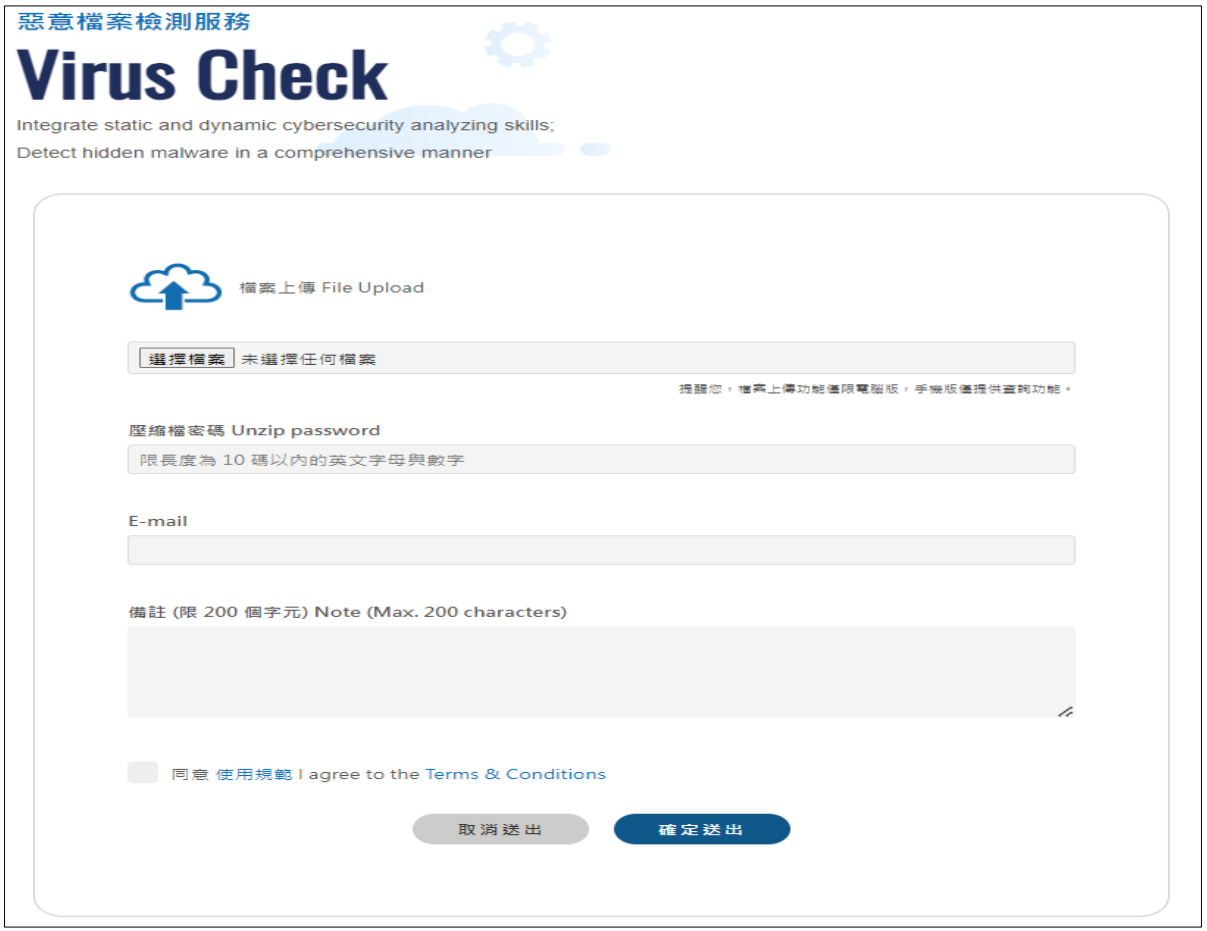
- VirusTotal 會在結果頁面分析該網站的安全性



資料來源：https://free.com.tw/virustotal/

惡意檔案檢測服務

- Virus Check，提供本土化的檔案檢測服務



資料來源：https://free.com.tw/virustotal/

假消息(新聞)的特徵

- 太過於誇張、聳動、讓人不禁想點擊的標題，都有可能是惡意的「點擊誘餌」。
- 網址很可疑，魚目混珠。
- 新聞內容出現許多錯字或網站版面編排不正常。
- 很多明顯經過刻意修圖的照片或圖片。
- 沒有附註發布日期。
- 未註明作者、消息來源或相關資料。

避免成為假消息的受害者與加害者

- 提高警覺：不輕信令人嘩然的影片、圖片或文章。
- 查證消息來源：判斷消息的可信度。
- 不要只看標題：可能文不對題，要看完內文。
- 注意日期：檢查報導日期，是否舊聞新推。
- 搜尋相片：利用Google圖片搜尋，看看是否舊圖亂用，或文圖不符。
- 有片未必有真相：要判斷片段前後發生甚麼事。
- 調查及統計數據要細心讀：避免統計誤植。
- 小心斷章取義：要審視邏輯，有無扭曲。
- 立即提出異議或通報，以防錯誤消息散佈。

消息查證管道

- 收到可疑訊息(新聞、郵件、簡訊...等)，可至『Cofacts 真的假的』網站，以及『趨勢科技防詐達人』查詢訊息的真偽。
  - 網址：https://cofacts.tw/
  - Facebook：https://zh-tw.facebook.com/cofacts.tw/

趨勢科技

防詐達人

到底哪些是真哪個是假？
傳給我馬上知道！

加入好友

控管遠距作業的危機

後疫情時代的作業變化

- 生活習慣改變，養成使用(依賴)線上服務的習慣。
- 疫情期間多數組織歷經數位轉型的變化。
- 遠距工作與科技設備使用的頻率提升。
- 視訊設備、無人化設備、雲端服務、與電商產業(宅經濟)延續成為日常生活之必須。

遠距作業(設備)的風險

- **遠距環境複雜**
  - 無論是家中或組織外的工作環境不但危險且難以監控，如果使用私人設備要求安裝監控機制又涉及隱私。
- **資料外洩或不當使用**
  - 遠距工作容易發生資料外洩或不當使用，將造成嚴重的損失。
- **設備遺失、遭竊**
  - 使用遠距設備當遺失或遭竊時，都有資料外洩的風險。
- **授權或存取控制難度高**
  - 短時間內提供大量遠距員工進行外部存取，勢必無法兼顧「可用性」與「安全性」。

遠距作業(設備)可能遭致的攻擊

- **VPN 撞庫攻擊**
  - 使用者使用VPN連線組織內部資源的帳號密碼與其例常使用於外部網站的帳號密碼相同，遭到駭客破解利用，且組織未嚴謹隔離網段，造成入侵組織內部網路，取得各種機敏資料。
- **VPN 漏洞**
  - 駭客攻擊VPN 漏洞取得控制權後，從而獲得電腦控制權，取得公司機密文件。
- **中間人攻擊**
  - 居家使用的電腦安裝了含有惡意程式的盜版軟體。駭客透該電腦發動中間人攻擊，劫持並破解取得 VPN 帳號密碼，成功進入組織內網。

遠距作業(設備)管理者須知(1/2)

- **妥善規劃遠距工作流程及建立使用原則**
  - 規劃遠距工作流程以確保安全與產出
  - 盤點所有資料現狀與去向以掌握軌跡
  - 設定遠距會議軟硬體設備與會議內容
  - 設立遠距工作資安事件處理團隊及應變流程
  - 建立僅知、最小權限原則
  - 可選用MDM(Mobile Device Management)工具管理遠端設備
  - 遠端設備選用全機加密

遠距作業(設備)管理者須知(2/2)

- **強化網路管理**
  - 盤點VPN 帳號並審查權限
  - 嚴管VPN 帳號權限範圍及內網分區
  - 監控確認 VPN 流量及行為
  - 只允許白名單設備取得 IP 位址
  - 開啟VPN帳號多因子認證
  - 確保 VPN 伺服器為最新版本
  - 使用 E2EE 通訊工具
  - 確認遠距設備連線IP位址對應正確，個人防火牆啟用
- **加強使用者帳號管理**
  - 使用密碼管理工具並強制使用者設定「強密碼」
  - 開啟2FA / MFA機制增加帳號防護

遠距作業(設備)使用者須知(1/2)

- **恪守保密義務與責任**
  - 專機專用，切勿專機私用或交由他人使用
- **小心使用遠距設備**
  - 開啟遠距裝置協尋、鎖定、清除功能
  - 設定設備登入密碼
- **妥善設置密碼**
  - 各應用系統設置不同密碼以確保安全
- **保全網路使用**
  - 避免使用公用 Wi-Fi 連接組織網路
  - 禁止使用公用電腦登入組織系統
  - 遠距工作時關閉不必要的其他連線

遠距作業(設備)使用者須知(2/2)

- **資料管理**
  - 公務用資料只留存在公務設備中
  - 協助記錄資料使用的歷程
  - 重要文件與郵件附件加密處理
  - 將重要資料進行備份處理
- **實體安全**
  - 離開電腦時立刻鎖定螢幕
  - 禁止插入來路不明的隨身碟或外部裝置
  - 慎防外人偷窺螢幕或碰觸設備
  - 切忌遠距設備離開視線
  - 將工作區域關門或上鎖

安全的視訊(線上)會議

- 確保為線上會議加上密碼保護。
- 不要在公開平台上分享會議資訊。
- 善用主持人(Host)功能。
- 利用等候室或大廳功能過濾參與者。
- 通知使用者該會議是否正在被錄製(個資與隱私)。
- 停用檔案傳輸功能。
- 保持使用之會議軟體更新至最新版本。
- 避免使用有疑慮的視訊會議軟體。

目前主流的視訊會議軟體

	Google Meet	Zoom	Microsoft Teams	Webex	Butter
適合用途	團體臨時會議 例行會議 線上講座	線上互動型課程 線上專業型課程 線上講座 例行會議	團隊例行會議 企業線上辦公 企業訓練研討會	團隊例行會議 線上專業型講座 線上課程	線上互動型課程 線上工作坊 線上研討會
本公司(TMR)使用案例	行銷資料科學週會 行銷企劃例行會議 對外小型演講	跨團隊多人會議	企業大數據部門合作 內訓	對外大型演講	—
免費容納人數	100人	100人	300人	100人	100人
安裝軟體(參與方)	不需要	需要	不需要	不需要	不需要
免費在線時間	24 小時(1 對 1) 1 小時(3 人以上)	24 小時(1 對 1) 40分 (3 人以上)	24小時	50分	x
分組討論	付費版	o	付費版	o	o
主持人開關麥權限	o	o	o	o	o
白板	o (需安裝jamboard)	o	o	o	o (外接miro)
表情符號	x	o	o	o	o
舉手功能	付費版	o	o	o	o
虛擬背景	o	o	o	o	x
會議錄影	付費版	o	付費版	o	x
共享畫面	o	o (可多人共享)	o	o	o
支援行動裝置	o	o	o	o	x
遠端操控	x	o	o	o	x
客製化個人會議室	x	o	x	o	x

資料來源：https://www.ithome.com.tw/news/132508

慎防密碼猜測攻擊

- 攻擊者在嘗試猜測出帳號密碼，進而取得帳號控制權的方式，其攻擊方法可區分成4種

攻擊手法	定義
暴力破解	使用所有可能的密碼組合，嘗試登入系統。
字典攻擊	收集常見的密碼納入猜測字典，然後用來嘗試登入系統。
密碼潑灑	只使用單一弱密碼，對所有帳號進行測試。
帳號填充	利用外洩帳號資料庫的密碼組合，嘗試登入系統。
彩虹表	指透過雜湊演算法，將密碼轉成特定文字列表。

弱密碼遭暴力破解案例(1/2)

- 案例說明：
  1. 資安院發現多個機關郵件帳號密碼外洩，共發布15則資安警訊通知機關應處。
  2. 經機關調查發現多為設置弱密碼遭成功暴力破解。
  3. 機關雖規定密碼設置原則，人員為方便記憶而將密碼設置為Aa123456或與帳號相似密碼。
- 防護建議：
  1. 清查郵件伺服器之郵件帳號，停用或刪除未使用之郵件帳號，確認系統上所有郵件帳號密碼均符合密碼複雜性需求。
  2. 加強宣導避免設置常見、與帳號相似或鍵盤排序等具規則之弱密碼。

資料來源：政府機關資安威脅與防護重點

弱密碼遭暴力破解案例(2/2)

近期政府機關外洩密碼

Aa123456

密碼與帳號相關

- 密碼與帳號相同
- 帳號重複兩次
- 帳號+@
- 帳號+@123

密碼與縣市名稱相關

- 縣市名稱+@1234
- 縣市名稱+@+123

資料來源：政府機關資安威脅與防護重點

強化密碼管理

- 定期更換密碼，建議三個月或每半年改一次。
- 不同網站使用不同的密碼。
- 不使用過於簡單的密碼，如：abc1234。
- 使用大小寫、數字以及特殊符號混雜而成的密碼。
- 開啟雙重驗證功能，將帳號與手機綁定，避免帳號被其他人直接登入。
- 勿用臉書或Google當萬用帳號，建議使用不同帳號及不同密碼登錄
- 建立自己的密碼提示問題，建議使用與問題完全不相干的答案。
- 定期修補並更新已安裝的軟體。
- 刪除不再需要的帳號。
- 使用密碼管理軟體。

慎防駭客利用工具進行攻擊

- Google是駭客搜尋攻擊目標相關資訊的好工具
- Google Hacking是利用Google強大的搜尋能力，尋找
  - 包含機密資訊或限制存取的網頁
  - 有弱點的網頁
  - 帳號與密碼
  - 後台管理介面
  - 有用的系統資訊
  - 個人隱私資訊
  - .....
- 技術難度低，成果驚人

總結

時時警覺可保安全無虞

- 使用行動裝置與通訊軟體時須注意防護措施，避免資安與個資疑慮。
- 遠端作業應優先考量連線安全重於便利性。
- 各項設備安裝的作業系統與應用軟體應注意更新與掃毒。
- 隨時吸收最新資安與個資新知以提高警覺。
- 資通安全，人人有責。

提問與討論

- 敬請指教 -

資拓宏宇永遠與您一起創新前進

always innovative always IISI

資拓宏宇國際股份有限公司
International Integrated Systems, Inc.