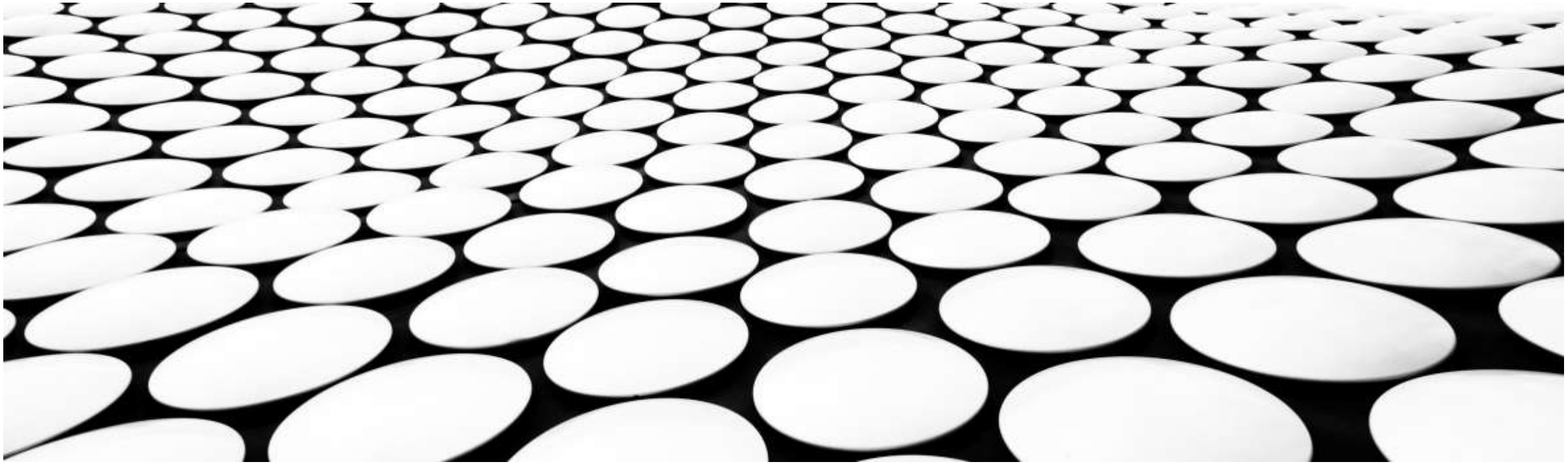
認識生活中的資安意識與風險 - 從新聞看資安學資安

高雄師範大學資安專題講座



自介

- iThome資安主編羅正漢
- 現於iThome電腦報週刊擔任資安主編，曾擔任技術編輯，負責iThome週刊、專刊與資安年鑑的內容，持續報導商用軟硬體、雲端服務、資訊安全等類型的企業IT解決，同時兼負近年Cyber IQ資安測驗與釣魚剋星企畫等相關工作，並在2020臺灣資安大會擔任防疫與防駭座談會講者及與談人。工作之餘，參與iT邦幫忙鐵人賽以《生活資安五四三！從生活周遭看風險與資訊安全》作為網路文章系列獲得Security組優選。

從新聞看基本資安意識與觀念

[學校沒教過的資安課？]

- 大家都在談行車用路安全、公共衛生安全、食品安全，那麼資訊安全呢？
- 從生活經驗中，就有很多場景是一般人可以去思考資訊安全的地方
- 風險觀念人人都有，認識資安風險讓你生活少掉許多麻煩

今日專題重點摘要

- **從新聞看基本資安意識與觀念**

  我們何時該換手機？

  你的雲端服務帳號被盜與你的錢包被偷誰比較嚴重？

- **防詐-你怎麼知道網路上所顯示是真的對方**（社群平臺、郵件、簡訊、網站

  ●認識偽冒問題 ●認識基本網域概念，讓你少掉很多麻煩

- **ChatGpt當紅，有哪些安全問題需要重視**

  建立對當前生成式AI的正確想像

- **【現代人必要有的4大資安意識】**

大家進入大學前都已經開始使用網路，但背後風險清楚嗎？

從新聞與網路威脅看起，你會更有感！分享給同學們吧

【我們何時該換手機？】

要換手機的時機，大家想到的會是？

想換新產品？還是要等電池壞了？還是手機壞了？

另外是否有人會注意，也是要看手機商不再提供安全更新？

為什麼很多安全觀念都有聽過，卻不夠重視？

大家可能曾注意過發表會的新聞，但另一則呢？

只要說要有資安意識 / 資安觀念，要小心夠嗎？

若不清楚威脅現況與生活上的威脅情資，也就無法產生警覺

新聞內容：

駭客利用植入Pegasus間諜程式

公民實驗室（Citizen Lab）通報蘋果並揭露

蘋果在2021年9月經通報後才修補

Forcedentry漏洞 CVE-2021-30860漏洞

- **手機作業系統漏洞多嗎？**
- **儘管普遍大眾很多聽過要保持更新，但多數人的觀念仍是能用就好！？**

資料來源: https://www.ithome.com.tw/news/146551

新聞內容：

這是2023年10月的新聞

蘋果公告修補裝置BUG與零時差漏洞

並釋出新版iOS系統修補上述問題

- **為何大家不清楚安全更新重要性？**
- **因為普遍媒體或過往教育，都沒有好好告訴你相關威脅的狀況與態勢，也是因為大家看的資訊很多，卻沒注意到這些網路攻擊新聞不斷**

資料來源: https://www.ithome.com.tw/news/146551

新聞內容：

安全漏洞藏匿在Framework中

允許遠端駭客透過特製的PNG檔案，在特權流程中執行任意程式

Google在2019年2月收到研究人員通報才修補

尚未發現攻擊利用行動

- **漏洞發現後不修補或想辦法緩解，問題就是會依然存在**
- **Andorid生態要稍微了解，還要等手機品牌業者釋出修補**

資料來源: https://www.ithome.com.tw/news/128669

新聞內容：

這是2023年10月的新聞

Arm修補影響Android手機使用的GPU驅動程式漏洞

Andorid的10月安全更新也修補此漏洞

接下來是手機製造商要測試更新修補才能釋出給用戶

- **漏洞發現後不修補或想辦法緩解，問題就是會依然存在**
- **Andorid生態要稍微了解，還要等手機品牌業者釋出修補**

資料來源: https://www.ithome.com.tw/news/128669

有漏洞有風險？

1. 駭客先找出未知漏洞併用於網路攻擊行動，無論是否需要使用者互動（威脅已經發生，零時差漏洞攻擊）

2.因此，軟體業者都在應對，內部或外部研究人員先找出產品或服務漏洞並發布修補，但攻擊者也可能針對沒有修補的用戶攻擊。（廠商釋出修補，用戶沒有修補，等於持續暴露於風險）

誰的責任？

廠商有，用戶也有

因應　1.自己做好安全更新　2.選擇有盡力維持安全的廠商

- **應知道**：

有安全性漏洞修補這件事

- **應理解**：

漏洞不補風險是自己要承受

呼籲安全更新已久，但多數人觀念仍是能用就好

但有許多民眾的回應，可能讓大家對於資安觀念混淆

再次提醒

- **應知道**：有安全性漏洞修補這件事
- **應理解**：漏洞不補風險是自己要承受

現在你再想一想，你知道手上的機型何時會失去安全性支援嗎？

2年？3年？5年？

現實案例：
今年4月
與朋友聊到
他的手機已經用多久

除了手機作業系統iOS、Android的更新

- **筆電、桌上型電腦的作業系統** macOS Linux
- **瀏覽器** 
- **各式電腦桌面應用程式、手機App**

只有這樣嗎？

網路設備
無線路由器
NAS
印表機
各式系統主機

再想想...

安全更新機制健全嗎？
廠商積極嗎？

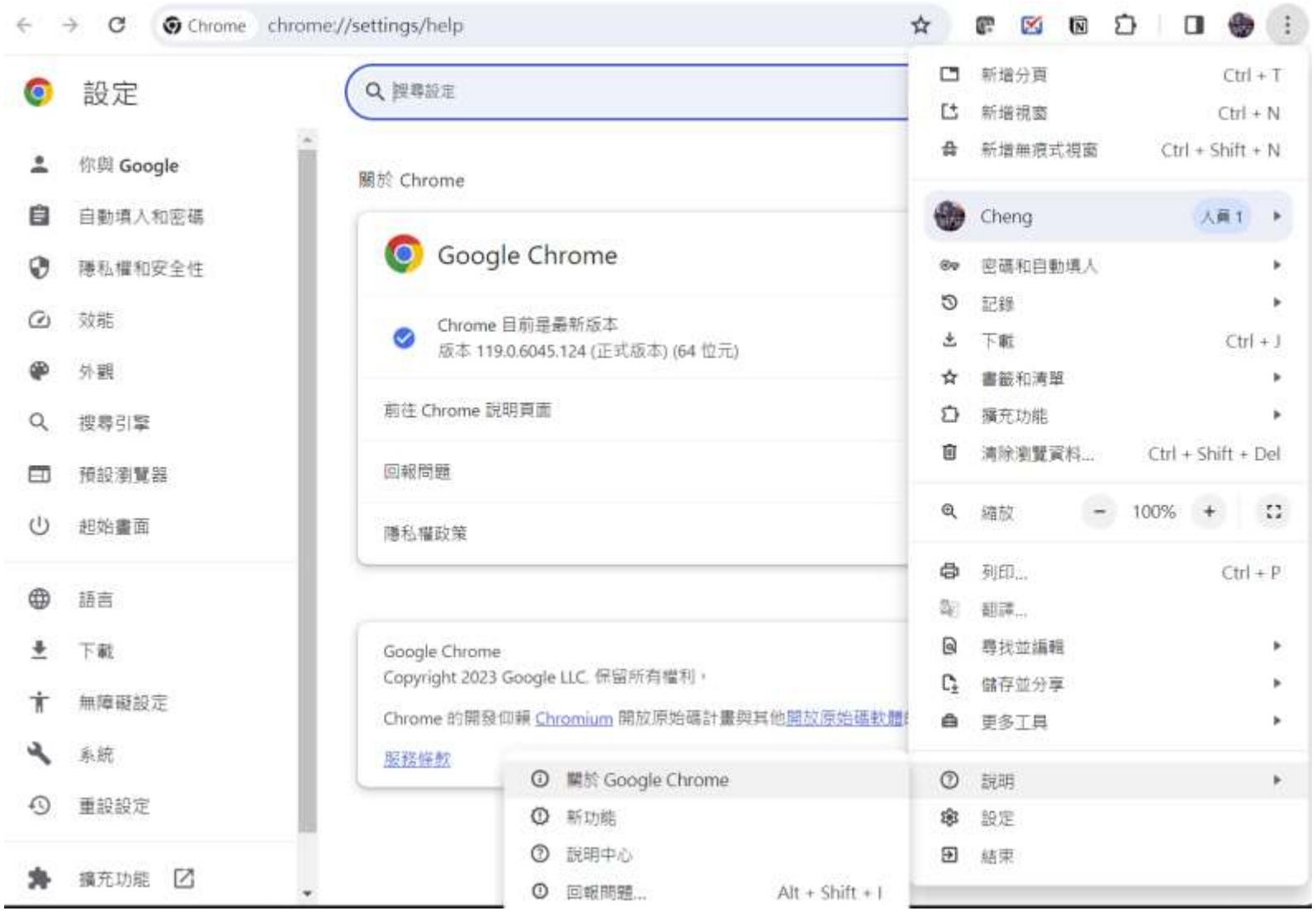
案例

瀏覽器 會自動更新
或手動檢查更新可立即更新

尚未更新的話進入
「關於Chrome」頁面就會啟動

其他瀏覽器選項不同
但邏輯上就是
找到說明或是關於

但有些產品手動下載才能更新
像是WinRAR這樣的壓縮軟體
像是老舊的網路

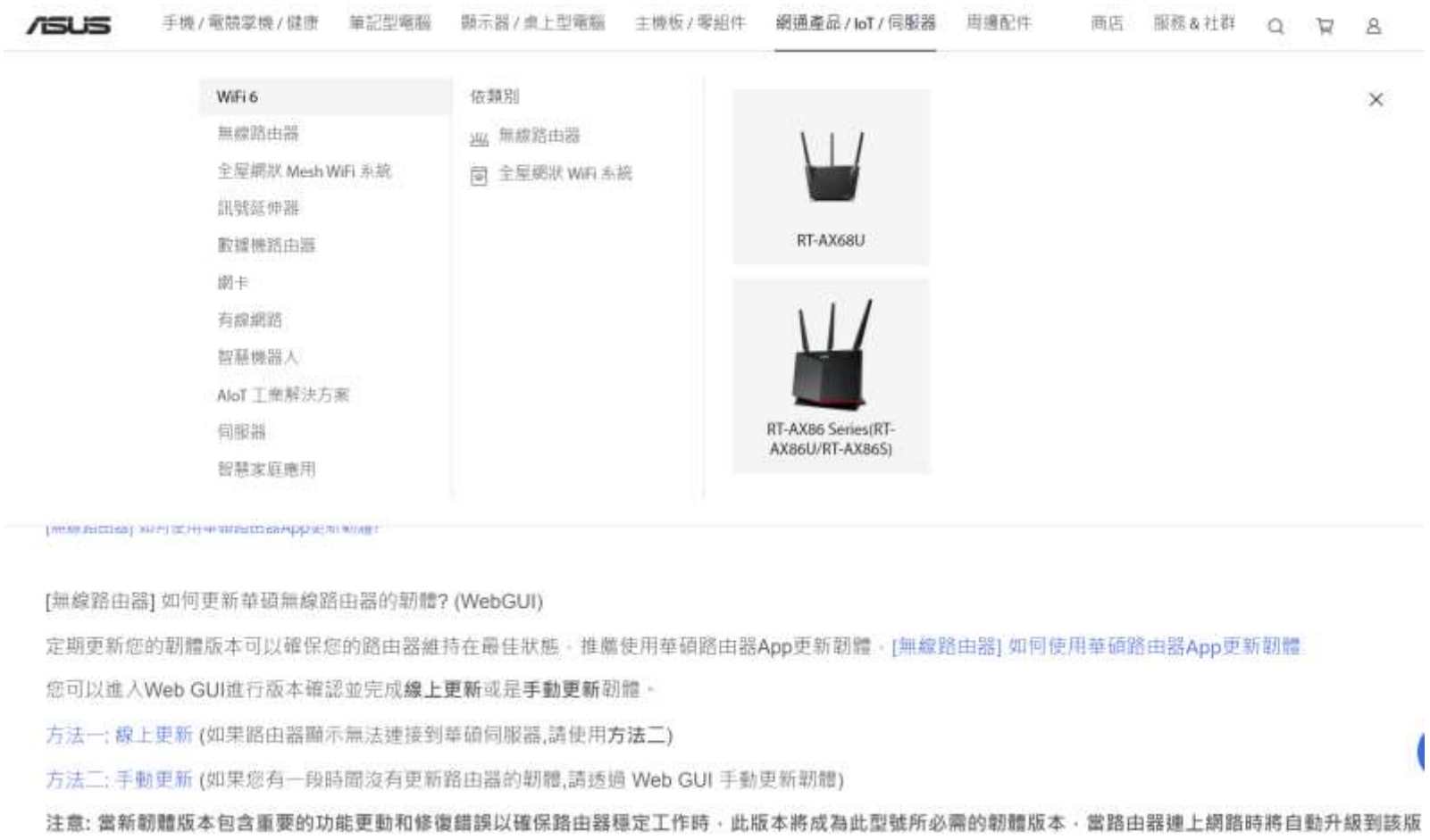


自動更新與手動更新

不只你的手機、電腦
像是家中網路分享器等網路設備

廠商也會提供韌體更新說明頁面

關於安全更新
還有更深一層的資安要當心
●廠商更新伺服器的遭駭的風險
●用戶從非官方載點的風險
更新前也注意是否有災情

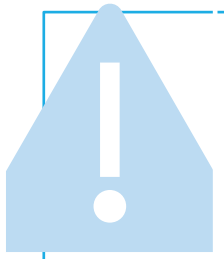


案例

2023年11月
中華電信小烏龜

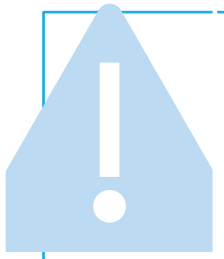
流程
1.研究人員找出漏洞
2.研究人員通報廠商發現漏洞
3.廠商收到通報後確認漏洞
4.廠商修補漏洞並釋出更新
5.CVE漏洞揭露
6.發布安全性更新公告，通知用戶修補

想一想



漏洞沒有發現會怎樣？

可能有零時差漏洞攻擊風險



漏洞沒有修補會怎樣？

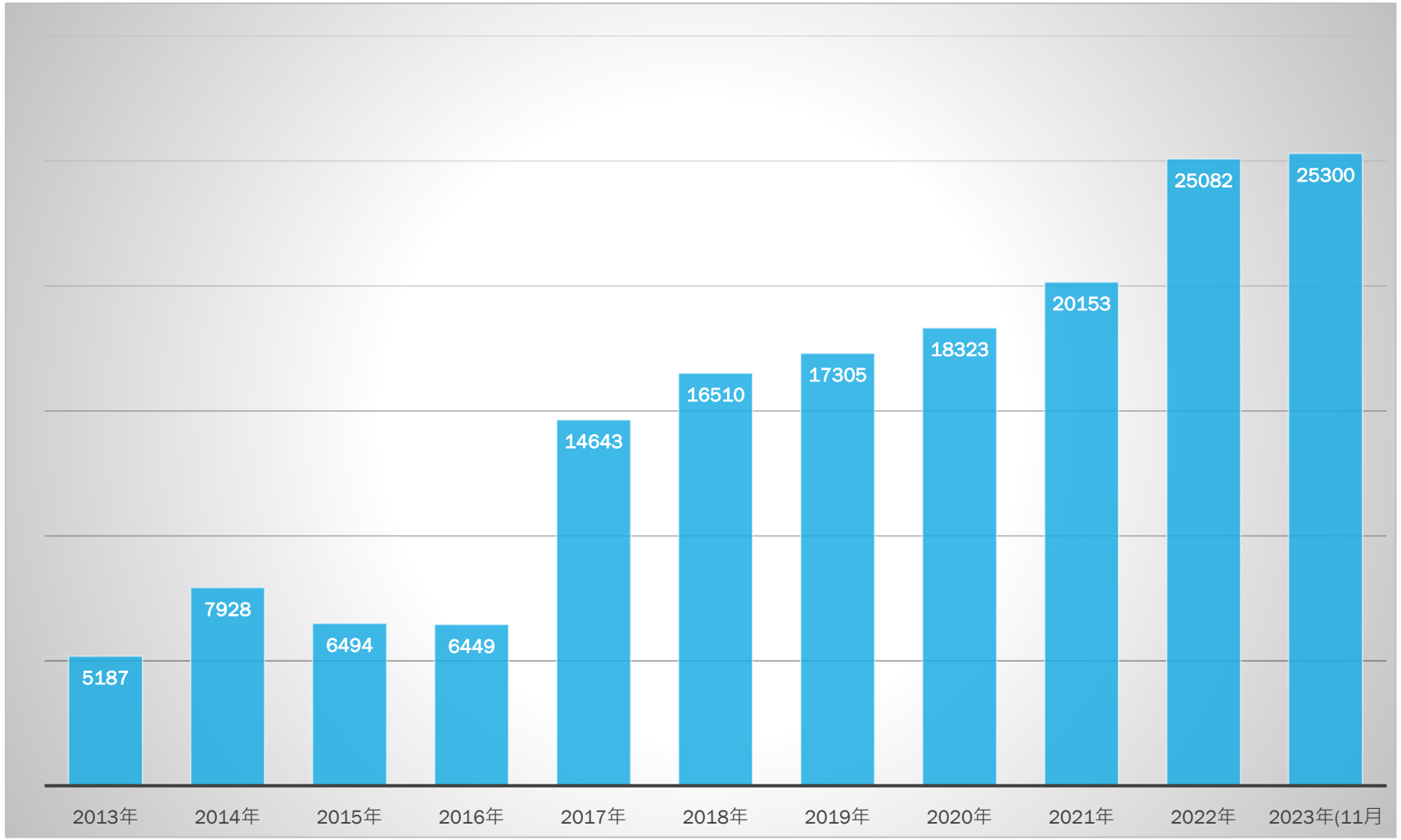
攻擊者可針對已知漏洞攻擊

如果有廠商都沒在修補的...

最近2023年10月新聞，光是攻擊者挖掘零時差漏洞就很多，還有更多攻擊者針對已知漏洞的攻擊

資料來源：https://www.ithome.com.tw/news/159484

每年有上萬漏洞揭露與修補



資料來源：CVEDetail

除了注意手機廠商安全更新，還有手機出廠即被植入木馬

iThome

臺電信品牌手機遭駭事件的4大資安教訓

近期NCC披露台灣大哥大自有品牌手機Amazing A32遭植入惡意程式，而之前已引發了一連串詐騙、身分冒用的狀況，這當中其實有相當多的受害者，同時也暴露出不同面向的資安議題，包括白牌手機資安隱憂、企業產品服務的安全管控，以及事件後的產品資安事件應變等。

檢視 編輯

文/ 羅正漢 | 2021-01-15 發表

讚 116 分享

政府與業者都需加強白牌手機資安隱憂的把關

用戶平時手機使用就要注意App和上網安全

企業對合作廠商與供應鏈要加強產品資安控管

自有品牌業者對於產品資安事件應變要主動積極

【你的電子郵件帳號被盜
與你的錢包被偷，誰比較嚴重？】

上大學了，大家應該都開始有郵局或金融開戶經驗

其實，你已有基本資安防護意識（保護你的提款卡、保護你的密碼）

但網路上....

想一想

- 你主要的電子郵件信箱有多重要？
- 社群平臺帳號、網拍帳號被盜、遊戲帳號被盜問題大嗎？
- 若平臺提供**MFA（多因素驗證）**，大家有開啟嗎？

只要說要有資安意識 / 資安觀念，要小心夠嗎？

不清楚威脅現況與生活上的威脅情資，也就無法產生警覺

新聞內容：

此案嫌犯破解方式很傳統

猜民眾以電話號碼作為密碼習慣，嘗試暴力破解

找出金融往來資料、密碼，以及身分證件

撥打電話給銀行客服，以變更存戶電話為歹徒持有的電話，登入網銀盜轉金融帳戶

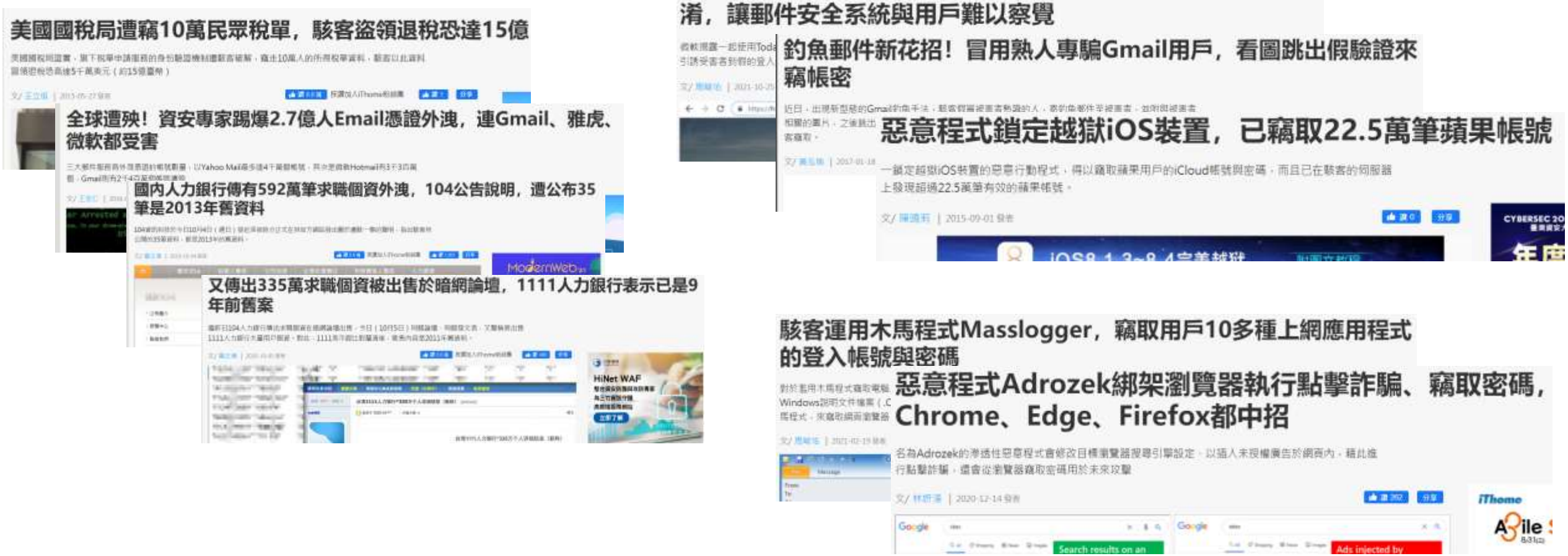
被盜的用戶都沒有開啟雙因素認證

- **帳號安全是否會去注意!?**
- **你的Email帳戶，存在比你想像要多的數位資產**

資料來源: https://www.ithome.com.tw/news/125782

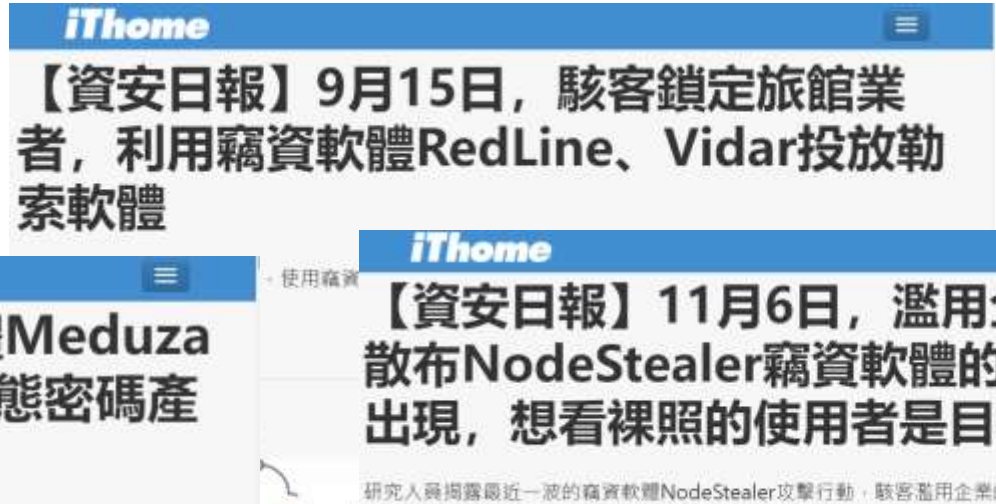
首先大家要對「帳密被竊取這件事頻傳」能有所認識

例如各式資料外洩中有包含帳密外洩，而用戶方遭網釣攻擊竊密也嚴重情形



首先大家要對「帳密被竊取這件事頻傳」能有所認識

資安業者公布竊資軟體的消息，其實超級多



帳號被駭風險？

資料、金錢被竊取？

被他人冒充你的身分做更多壞事？

成為人頭帳戶？

- 網路銀行帳號
- 電商帳號
- 論壇帳號
- 社交平臺與即時通訊帳號
- 電子郵件帳號
- 遊戲帳號

駭客如何可以取得你的網路服務帳號密碼？

從諸多資安新聞中，我歸納如下：

- **攻擊服務業者**
  - ●從許多資料外洩事件中，有些駭客組織偷企業商業機密，有些偷機敏資訊、客戶資料，也會有鎖定網路服務平臺的帳號資料庫來攻擊，攻擊一次就可取得大批用戶帳密
  - ●利用網站漏洞將惡意程式碼植入網站，暗中攔截相關資料
  - ●將惡意程式碼植入網站，並利用瀏覽器漏洞，讓瀏覽該網頁的受害者電腦被暗中植入竊密軟體
- **攻擊用戶端**
  - ●以社交工程假冒官方名義，透過郵件、社群平臺、通訊軟體，引誘你前往**釣魚網站**
  - ●透過社交工程手法，引誘你開啟郵件副檔，或開啟檔案，或是散步免費破解軟體，暗藏惡意程式，以**植入鍵盤側錄程式**或**金融木馬**或**竊資軟體**或**劫持Session Cookie**
- **無技術含量手法**
  - ●從地下管道購得已經外洩個資，用生日、電話嘗試破解
  - ●猜使用者使用弱密碼

此外，這邊所指安裝竊密，也可都換成各式惡意程式，滲透企業內部

知道駭客如何取得你的網路服務帳號密碼，所以?

從諸多資安新聞中，我歸納如下：

- **駭客會攻擊擊服務業者**
  - ●所以服務業者要做好保護
  - ●以及提供更安全的登入機制
  - ●**假設服務業者遭駭，對於用戶而言，也等於不要在不同服務使用同組帳密**
- **駭客會擊用戶端或猜出密碼**
  - ●要對不請自來的訊息有警覺，要懂識別釣魚網站
  - ●認識駭客會使用的社交工程手法
  - ●**假設自己會遭駭，不要使用弱密碼，不要使在不同服務使用同組帳密，更必要的作法，請啟用MFA來提高防護**
  - ●**不亂點連結、檔案，做好安全更新，啟用電腦防護**

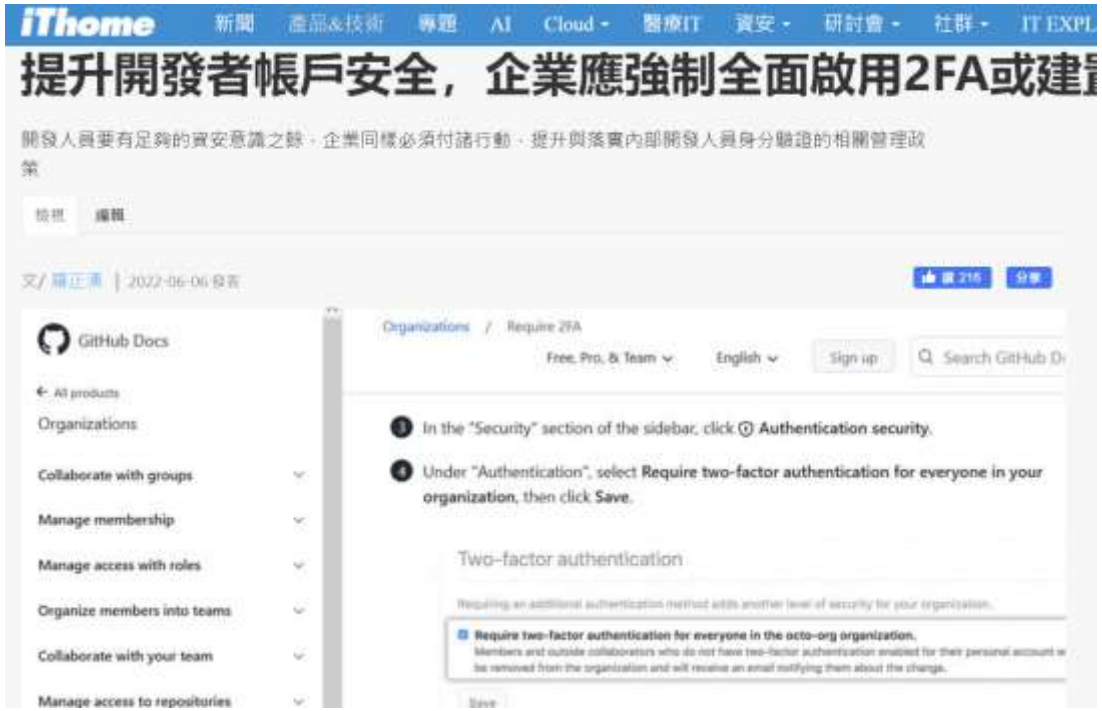
很多宣導只強調帳密安全，知道攻擊者普遍採取的手段，你才會更懂得要重視密碼管理軟體、啟用MFA、使用強式MFA是現在所談重點

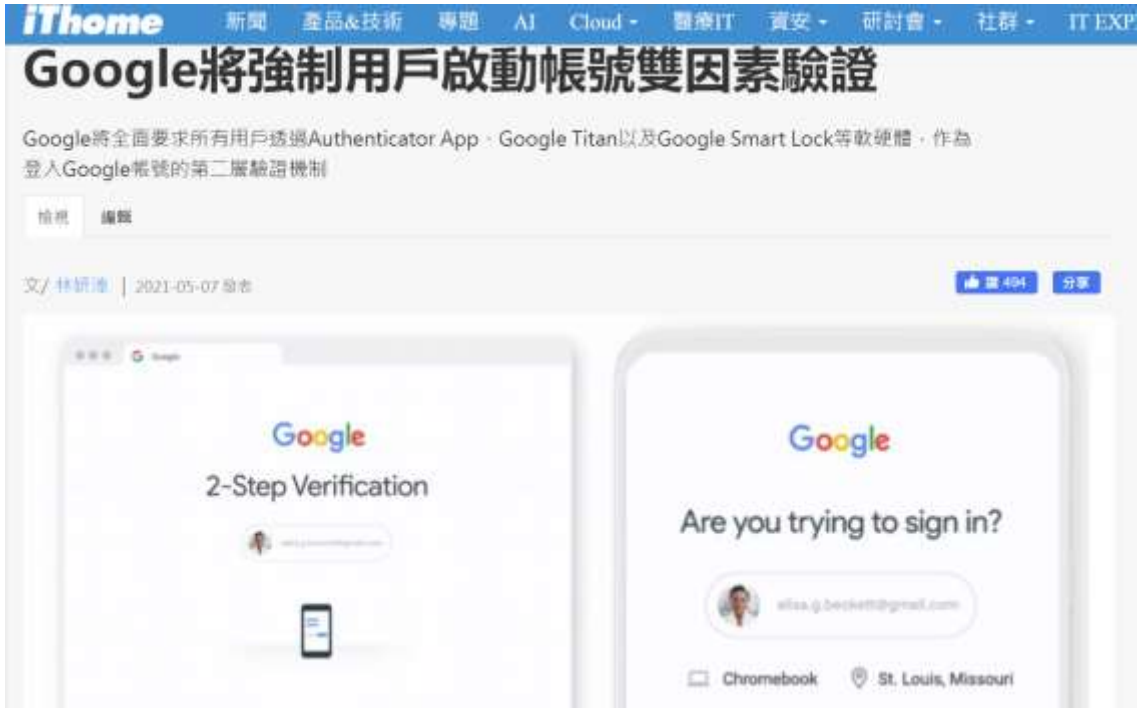
認識啟用多因素驗證（MFA）的重要性，並要知道MFA也有強度之分

認證形式		面臨威脅與抵擋能力	安全強度
抗網釣MFA	FIDO/WebAuthn認證	● 可抵抗網釣攻擊 ● 可抵擋登入通知推送訊息的轟炸、利用SS7協定漏洞，以及SIM卡劫持的攻擊	最強
	基於PKI		
基於App認證	基於一次性密碼（OTP）	● 面對網釣攻擊會有弱點 ● 可抵抗通知推送轟炸的攻擊 ● 不會面對利用SS7協定漏洞，以及SIM卡劫持的攻擊	強
	具有數字配對的行動推送登入通知		
	基於Token的OTP		
基於App認證	透過不具數字配對能力的行動應用程式，推送身分登入的通知	面對通知推送訊息轟炸的攻擊仍有弱點，用戶可能因為太多訊息而犯錯，導致有可乘之機	稍強
簡訊或語音		面對網釣攻擊會有弱點，無法抵禦利用SS7協定漏洞，以及SIM卡劫持的攻擊	一般

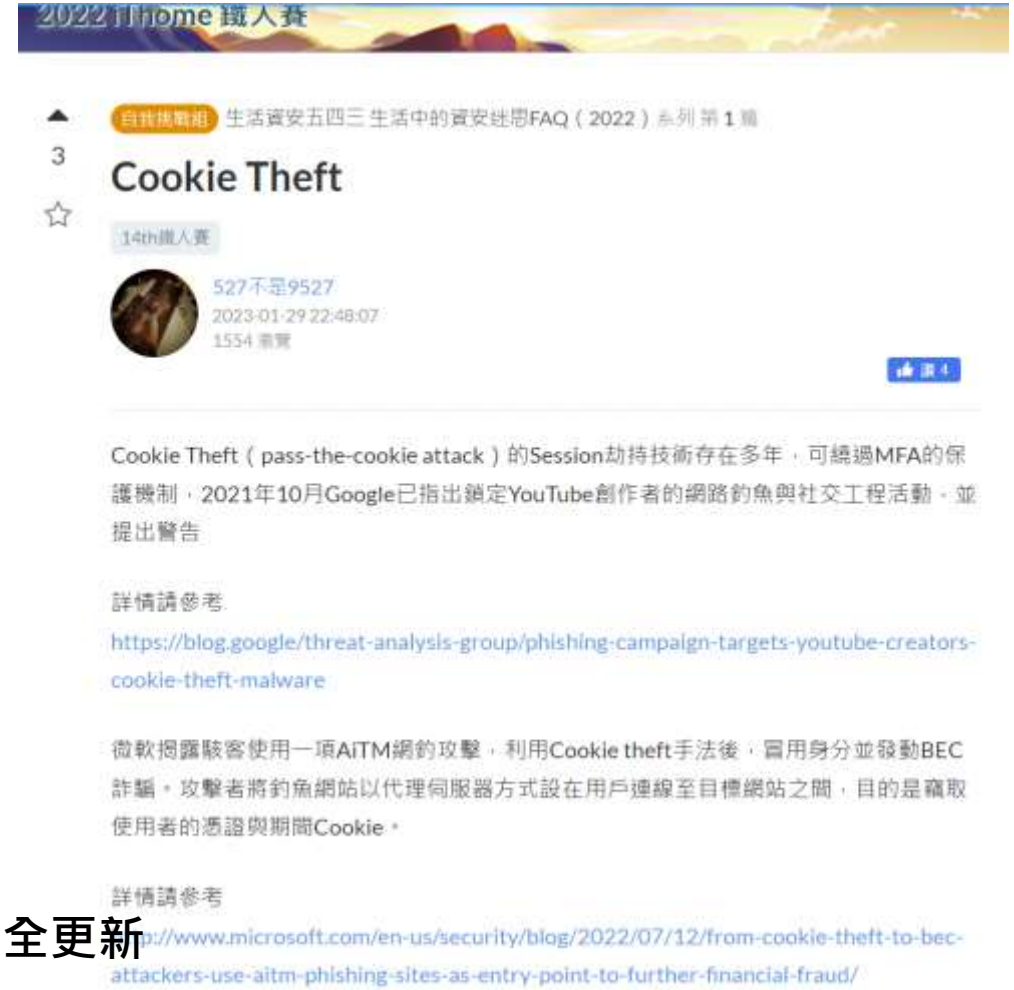
資料來源：美國CISA，iThome整理，2023年1月

科技大廠網路服務，原本MFA是選項，現在朝向預設啟用





安全有比較性，有MFA是基本，使用抗網釣的MFA更好
但駭客還有繞過MFA的招數要小心



Cookie Theft

這也是為何

1.不要亂點連結

2.不要隨意安裝太多應用程式APP

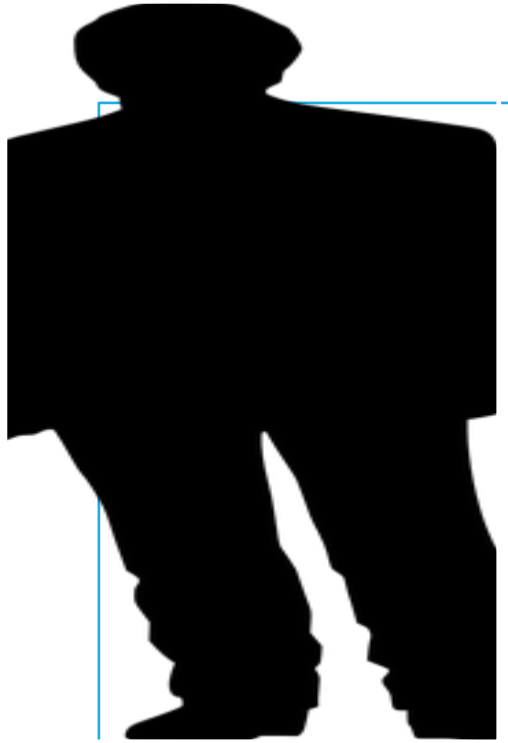
限縮攻擊面

3.以及需要持續注意安全更新

【防詐】

你怎麼知道網路上所顯示是真的對方

要大家小心詐騙、注意上網安全...
但社會上還是看到有很多人不太有警覺去分辨，為什麼？



社群平臺通訊交友詐騙氾濫，想一想

網路背後另一方真的是對方嗎？

想一想，網路背後另一方真的是對方？

容易忘記一些基本處世道理

陌生人給的糖果不要吃

害人之心不可有，防人之心不可無

有備無患（消防隊、鐵窗）

容易忘記網路世界什麼人都有

跟實體世界一樣，有好人也有壞人

網路上的壞人要追查出更不容易

必需知道：

許多詐騙手法邏輯其實類似

關鍵發現：

基本網路社交風險概念太缺乏

30年前網友多，現實朋友少

現在手機2010盛行，每個人都在上網

從玩線上遊戲看網路文化與資安意識

- **應知道**：

  網路暱稱的常態

  網路上開分身的常態

  有外掛內掛

- **應理解**：

  本尊？分身？還是偷聽公開對話的假冒

  猜猜我是誰 假小號忘記帳密騙帳密

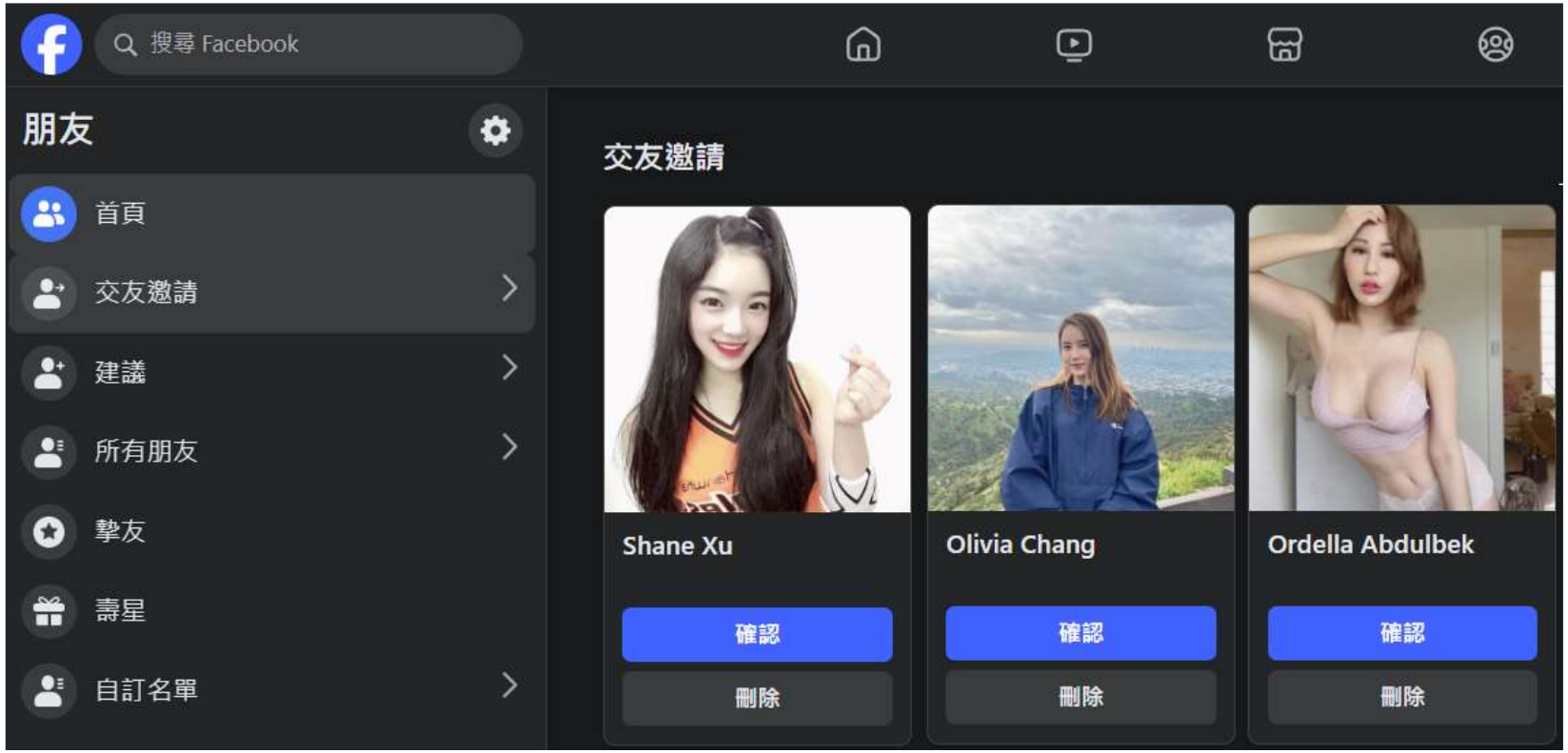
  交易懂得要小心（多種交易騙術，用取消交易讓你不耐煩先按確認、交易內容物圖案相似的騙、遊戲金幣＋物品的交易，金幣少0）

  買點數給天幣交易被騙

認識偽冒問題

現在大家玩社群平臺，很多是一樣邏輯

1.收到不明網路正妹交友邀請



2.收到不明貼文（臉書動態牆不只餵給你好友訊息，可是會自動推薦或廣告）

- **應知道：**

  網路暱稱的常態

  網路上開分身的常態

  有外掛內掛

- **應理解：**

  本尊？分身？還是偷聽對話的假冒

  猜猜我是誰 忘記帳密騙帳密

  多種交易騙術（用取消交易讓你先按確認、交易內容物圖案相似的騙、遊戲金幣＋物品的交易，金幣少0）

  買點數給天幣交易被騙

現在大家玩社群平臺，很多是一樣邏輯

1.收到不明網路正妹交友邀請
2.收到不明貼文（臉書動態牆不只餵給你好友訊息，可是會自動推薦或廣告）

- **應知道：**

  網路暱稱的常態

  網路上開分身的常態

  有外掛內掛

- **應理解：**

  本尊？分身？還是偷聽對話的假冒

  猜猜我是誰 忘記帳密騙帳密

  多種交易騙術（用取消交易讓你先按確認、交易內容物圖案相似的騙、遊戲金幣＋物品的交易，金幣少0）

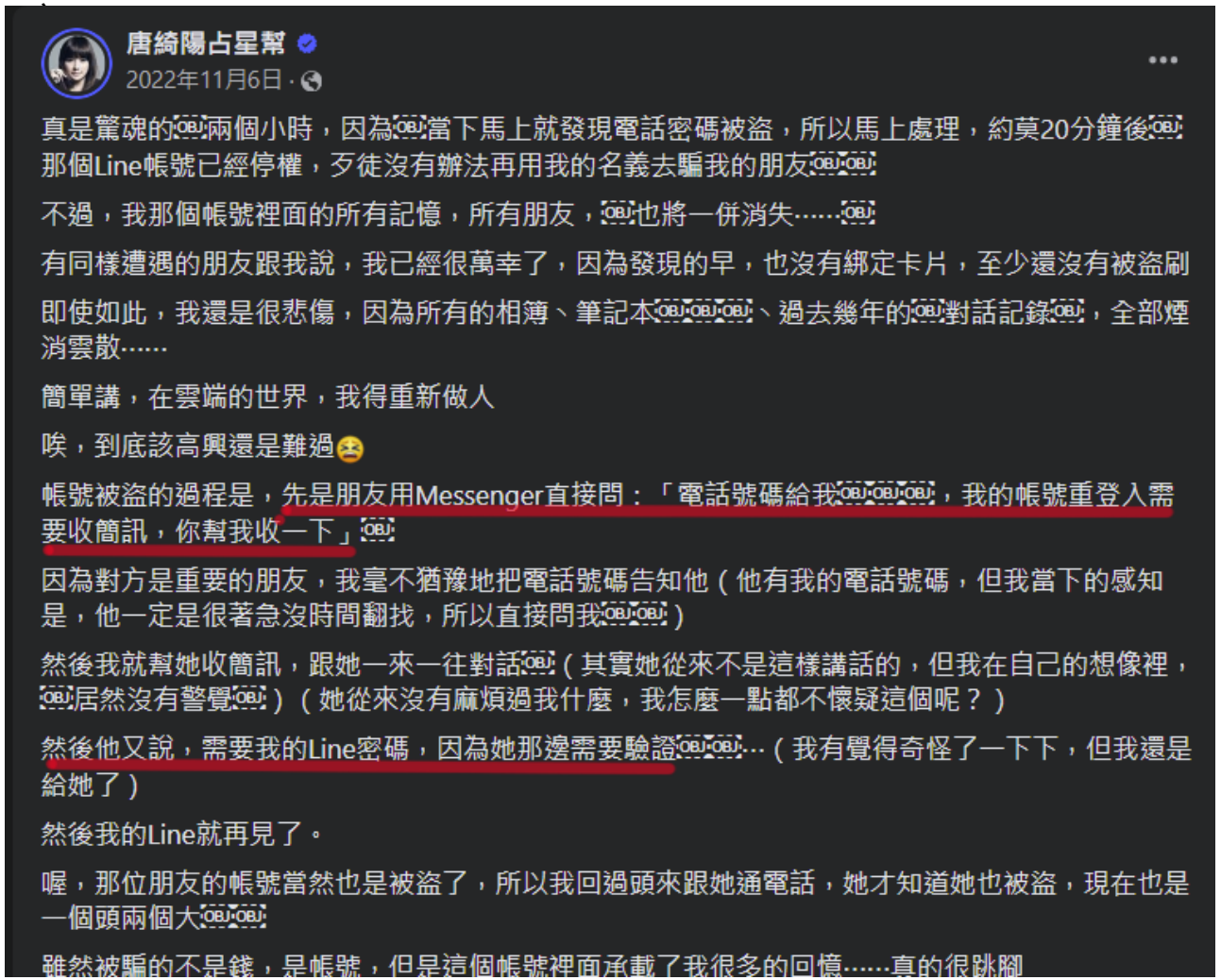
  買點數給天幣交易被騙

有概念就有警覺
第一個念頭 假的嗎？

- 是否拿別人照片放大頭照
- 臉書暱稱或粉專取名仿冒
- 貼文放人物圖片又怎樣？

現在大家玩社群平臺，很多是一樣邏輯

3.詐騙者除了開帳號來偽裝、假冒，還可以盜用真的帳號來偽裝、假冒對



唐綺陽占星幫
2022年11月6日 ·

真是驚魂的兩個小時，因為當下馬上就發現電話密碼被盜，所以馬上處理，約莫20分鐘後那個Line帳號已經停權，歹徒沒有辦法再用我的名義去騙我的朋友

不過，我那個帳號裡面的所有記憶，所有朋友，也將一併消失……

有同樣遭遇的朋友跟我說，我已經很萬幸了，因為發現的早，也沒有綁定卡片，至少還沒有被盜刷

即使如此，我還是很悲傷，因為所有的相簿、筆記本、過去幾年的對話記錄，全部煙消雲散……

簡單講，在雲端的世界，我得重新做人

唉，到底該高興還是難過😫

帳號被盜的過程是，先是朋友用Messenger直接問：「電話號碼給我，我的帳號重登入需要收簡訊，你幫我收一下」

因為對方是重要的朋友，我毫不猶豫地把電話號碼告知他（他有我的電話號碼，但我當下的感知是，他一定是很著急沒時間翻找，所以直接問我）

然後我就幫她收簡訊，跟她一來一往對話（其實她從來不是這樣講話的，但我在自己的想像裡，居然沒有警覺）（她從來沒有麻煩過我什麼，我怎麼一點都不懷疑這個呢？）

然後他又說，需要我的Line密碼，因為她那邊需要驗證…（我有覺得奇怪了一下下，但我還是給她了）

然後我的Line就再見了。

喔，那位朋友的帳號當然也是被盜了，所以我回過頭來跟她通電話，她才知道她也被盜，現在也是一個頭兩個大

雖然被騙的不是錢，是帳號，但是這個帳號裡面承載了我很多的回憶……真的很跳腳

- **應知道：**

  網路暱稱的常態

  網路上開分身的常態

  有外掛內掛

- **應理解：**

  本尊？分身？還是偷聽對話的假冒

  猜猜我是誰 忘記帳密騙帳密

  多種交易騙術（用取消交易讓你先按確認、交易內容物圖案相似的騙、遊戲金幣＋物品的交易，金幣少0）

  買點數給天幣交易被騙

對於**帳號密碼、驗證碼**，應特別提高警覺，是否能立即聯想對方可能被盜？非同步即時通訊，對方真的是對方嗎？

現在大家玩社群平臺，很多是一樣邏輯

4.詐騙者偽裝網路求才，騙不熟網路風險的人

韓國真實案件「N號房事件」，是2018下半至2020年3月期間發生的性剝削案件。
Netflix韓國記錄片：**網路N號房**

為什麼受害者會受騙，主嫌專挑年紀尚小、不熟網路風險的女生，或是在經濟上有需求的女生，讓她們一步步掉入陷阱，

當中其實就是點出網路背後暗藏的風險，你無法知道網路背後的人是好是壞，不信任的前提下，自己能說到什麼程度，等等，有時可以暢所欲言是因為不在自己生活圈，但有沒有過多資訊會被追蹤，必須注意。像是記錄片中，除了探討網路性犯罪的問題，同時也讓外界了解，犯罪者是如何針對不熟悉網路風險的青少女，誘騙她們上當，因為她們沒有太多網路使用經驗，任人擺佈就陷入圈圈而不懂及早求助。

鬧上社會新聞不斷的解除分期詐騙

普遍新聞都提到，你知道可能是詐騙，但對方知道你訂單、個資又忘記是詐騙

關鍵：不只是要知道詐騙，要知道對方因為取得外洩資料知道你的購買與個人資訊

冒名電商 來電詐騙

網路上查有沒有同樣詐騙

重要：自行請第三方管道查詢，去電求證。

重要：不要對方說出你購買過的商品與個資就相信對方

（你看過這方面新聞就該知道有這樣的情形）

大家喜歡看網紅，當中有些說明詳細的內容可以做為借鑒與了解攻擊手法

右邊是討論區最新的一起受害事件（知道詐騙，卻不知道竊取訂單資訊、個資已經屢屢發生）

【心得】我因為健**廠的洩漏個資被騙了

綜合討論

樓主 紅月 四味知識家幫幫忙 fr523321

前天 22:01 編輯

如提

我知道我接下來說的一定有人認為我無腦
或是白癡才會被騙
我也希望不要被韓得太慘
我心真的很累
我大前年得到了一個癌症
前年才剛化療完
想說到健身房運動
就辦了健工的會員
這是我在健工的第二年了
我幾乎每天都去
很少休息超過兩天的
我真的很努力很努力的把自己身體練回來

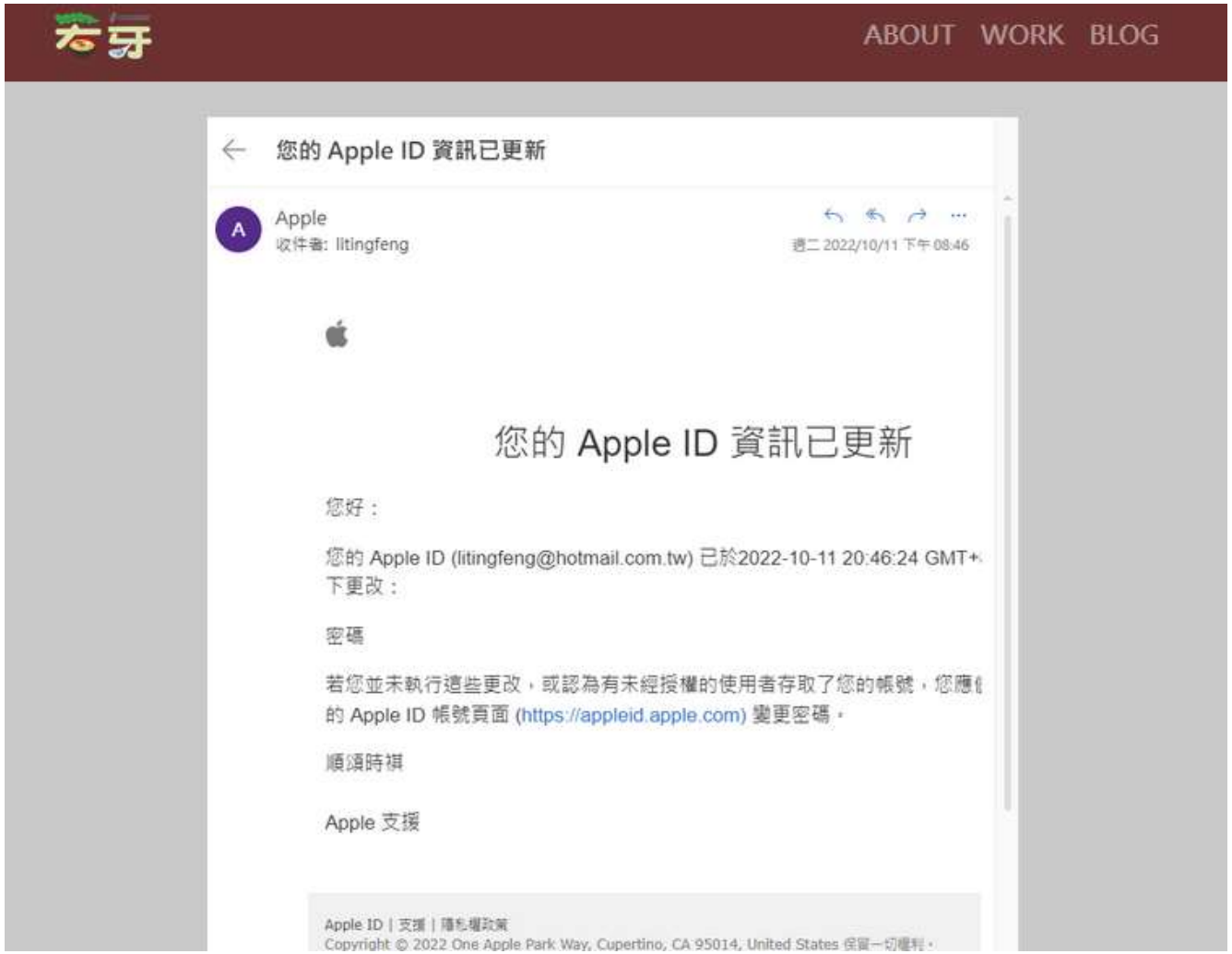
但我還是要說說當下的情況
當時是晚上8點多
打來了一通02的電話
我的健身顧問也常常這個時間打來
然後開始跟我比對資料
我剛開始也想說是詐騙
不太想理他
結果我們在比對資料時
發現他可以完整說出我的個資
哪個健身房
連我信用卡用哪張(我兩年用不同的信用卡)
每個月刷多少錢
還說我續約的價格(續約跟第一年的金額不同)
用哪張卡刷
甚至連我前兩天去的時間都知道
我就開始不疑有他了
後來他說扣款錯誤
等等我這張信用卡銀行的人會連絡我
過了半個小時
的確一個一銀的行員打來了
我看了看電話號碼
數字的確是一銀的24小時客服
我就跟他對了對資料
他就說要幫我開通一個會員資料
才能更改我的資料

面對釣魚網址

認識基本網域概念，讓你少掉很多麻煩

先看看一封釣魚郵件

先前Apple ID被盜消息
又不時傳出為例



引用來源: https://wakame.tw/blog/blog9.html

假冒系統通知信！

對於破綻很大的釣魚郵件，應該馬上察覺
更要注意假冒逼真的

寄件者名稱、電子郵件信箱　　傻傻分不清楚？

引用來源: https://wakame.tw/blog/blog9.html

網路釣魚常用的手法有哪些？

什麼是社交工程手法？
社交工程(Social Engineering)是一種技術門檻不高，攻擊者利用與人互動和操弄來達到目的的技術。通常涉及說服受害者為了攻擊者的金錢或資訊利益而危害自身安全或破壞安全最佳作法。駭客經常會用社交工程來偽裝自己及動機，通常是冒充成可信任的對象。

有哪些常見社交工程陷阱？

1.網路釣魚（假冒身分、假技術支援、假系統通知警報、身分盜用）

2.誘餌（停車場故意丟UBS）

3.尾隨（跟著前一人門禁刷卡通過）

以常見的社交工程陷阱為例

釣魚（Phishing）

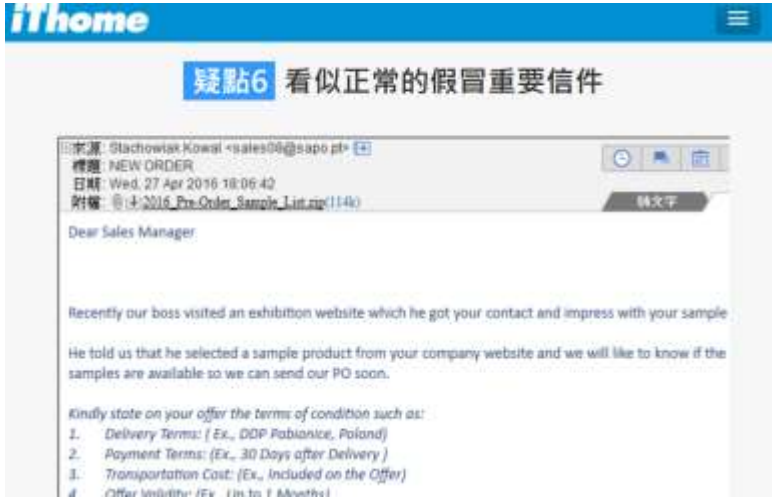
早年管道：**電子郵件**
當心的藉口：帶有腥羶色聞的郵件主旨與檔案、聲稱好康優惠。
利用人性：好奇心

現在管道：**電子郵件、社群平臺、簡訊、電話**
當心的藉口：假冒系統通知信、假冒身分（還有身分盜用）
利用人性：偽裝成像正常郵件一般，企圖讓使用者因疏忽而犯錯，或是降低使用者的警覺性

網路上有太多案例，一定要認識其概念

假冒客戶

給你惡意檔案
惡意連結



假冒系統通知

甚至以你被駭的名義
讓你急忙想處裡

騙你網路服務登入帳號

利用外洩密碼
謊稱知道你密碼
騙稱電腦被窺視
恐嚇騙錢

關鍵時刻
假冒合作鍵夥伴
變更匯款帳號

案例

HS

HiNet Service

昨天 上午5:39

HiNet 密碼更改通知

收件人： undisclosed-recipients:;

尊敬的 Hinet 用戶，

您的電子郵件帳戶密碼今天到期

使用下面的按鈕繼續輸入相同的密碼

保留密碼

如果您在 24 小時內未採取任何行動，您將被鎖定在您的 HiNet 帳戶之外。

計時免費服務電話：0800-080-412
無病毒。 www.avast.com

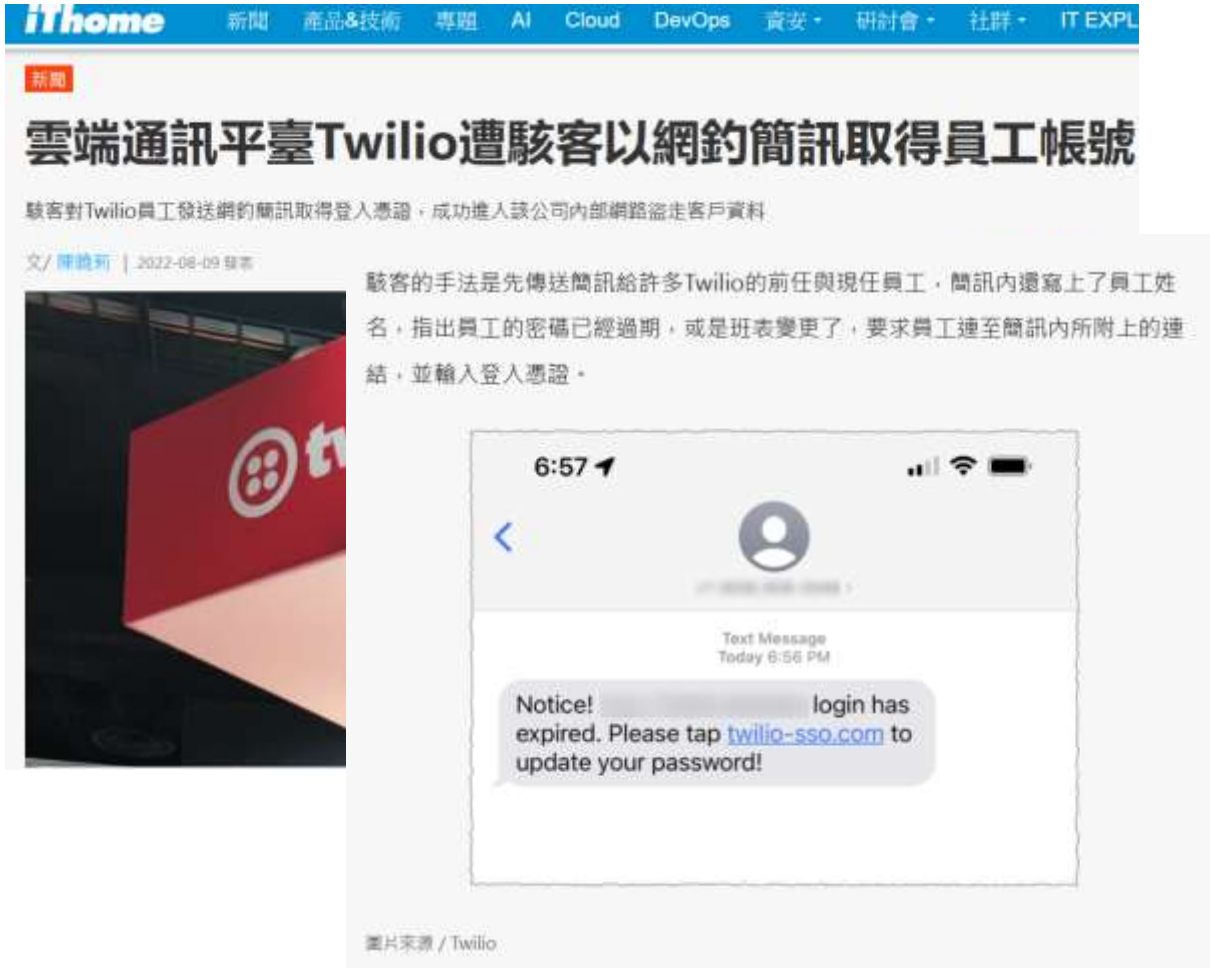
HiNet 保護自己免受詐騙！

⑤HiNet 客戶服務

假冒系統通知2

騙稱密碼到期
要你輸入密碼登入後
改密碼

鎖定企業員工的釣魚簡訊、釣魚郵件都存在



釣魚連結更是從郵件蔓延到簡訊，OTP碼也要騙

當時，多家銀行也配合警方先行發布防詐騙提醒！

說明近期發生多起假藉銀行名義要求登入網銀綁定用戶資料的簡訊。

說明本行不會以簡訊、電子郵件主動請客戶進行變更設定。

通知銀行客戶收到可以簡訊或電子郵件，請勿點選連結登入。

目的：藉由釣魚連結，誘騙銀行客戶連上偽裝的釣魚網站，騙客戶的帳密、綁定到歹徒裝置，然後盜轉金錢

資料來源: https://www.ithome.com.tw/news/142711

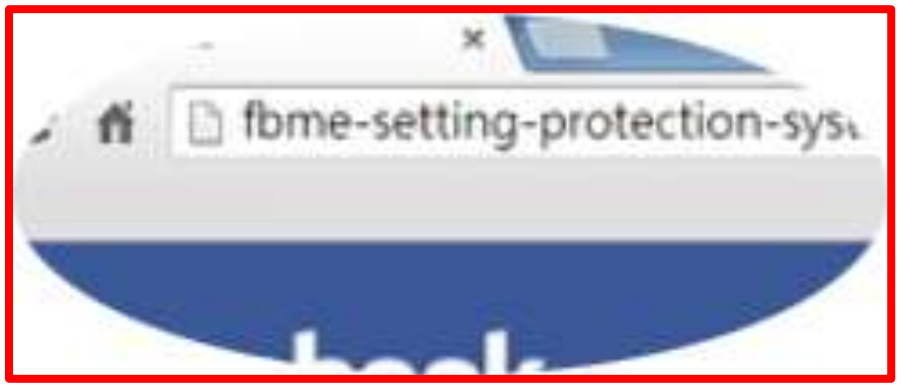
許多釣魚網站詐騙並非新手法，假冒名義的話術百百種、網域識別才是重點

大家可以想像，**網路世界的門牌號碼就是「網域」**，

如果你走錯， 就不會走到你要到的地方

而釣魚網站就是讓你誤以為走到是你要走的地方，但其實，只是門面布置得相像，實際門牌號碼根本不同。

家門口布置的一樣，但門牌號碼不一樣阿！！



就跟前面MFA可被繞過一樣

還一種從DNS下手的攻擊，你輸入正確門牌也會被解析至其他IP位址

釣魚網址最常見，如果懂得一些關鍵容易應對！

知道威脅態勢自然就會小心

即便不知道，會思考就有警覺性
思考一：這個簡訊真的是業者發送的嗎？
思考二：這個連結會是騙人的嗎？
思考三：銀行會這樣通知客戶嗎？

2022/11/7新增「疑似偽冒玉山銀行寄送釣魚簡訊，竊取個人敏感性資料」。
1.釣魚簡訊內容摘要：【玉山銀行】親愛的顧客您好：您的網路銀行存在問題，請在24小時內處理，致...。
2.釣魚連結：
hxxps://s[.]id/1mPKO（2022年11月7日更新：連結已失效）
hxxps://o[.]my-esun-bank[.]life（2022年11月7日更新：連結已失效）

網域識別才是重點

國人現在熟知的LINE，官方網站是什麼？

網域（Domain Name）
識別連結的真實網域
https://line.me/zh-hant/（真）
https://fact-checker.line.me/（真）

https://hub.line.me/search/2021.html（真還假？）
https:/line.me.mailru382.co/efaxdelivery/2017Dk4h325RE3（真還假？）

如何確認網域正確？
你熟悉的門牌沒問題，不熟悉的請自己從不同管道查詢正確資訊

生活資安五四三！從生活周遭看風險與資訊安全（第二版）

為了讓你更清楚真實網域的位置在那，以下我再用底色標示該連結的真實網域：

https://hub.line.me/search/2021.html（真）

https:/line.me.mailru382.co/efaxdelivery/2017Dk4h325RE3（假）

https://line.me.login.en.zkiki.com/login/en/?ref=http%3A%2F%2Fline.me. %2Fd3%2Fen%2Findex（假）

如此一來，你應該更清楚知道真實網域的位置。

資料來源: 生活資安五四三！從生活周遭看風險與資訊安全

懂得自行查證

整理更多例子給大家看看，以下這些都是「真的」LINE官方服務網站喔！

- LINE產品官網 https://**line.me**/zh-hant/
- LINE原創市集 https://creator.**line.me**/zh-hant/
- LINE購物首頁 https://buy.**line.me**/
- LINE旅遊官網 https://travel.**line.me**/
- LINE MUSIC官網 https://music-tw.**line.me**/
- LINE訊息查證 https://fact-checker.**line.me**/
- LINE HUB首頁 https://hub.**line.me**/

僅有少數LINE的服務沒有使用line.me網域，主要是LINE與商業夥伴，或新創團隊所攜手打造的服務，因此，雖然也隸屬於LINE家族服務，但使用了自己的網域，在這裏一起跟大家介紹。以下是正確官網：

- LINE MOBILE官網 https://tw.**linemobile**.com/sale/home/ (攜手遠傳電信)
- LINE TV官網 https://www.**linetv.tw**/ (攜手巧克科技團隊)
- LINE TAXI官網 https://**linetaxi.com.tw**/ (攜手TaxiGo團隊)
- LINE for Business (企業解決方案) https://www.**linebiz.com**/tw/ (LINE B2B網域)
- LINE企業官網 https://**linecorp.com**/zh-hant/pr/news/ (LINE企業官網網域)

此外，LINE的官方頻道，除了官網，還有官方帳號。官方帳號「名稱有LINE + 綠色盾牌」，才是正確的LINE官方頻道，這裡面傳送的資訊，是您可以安心相信的。

案例

釣魚簡訊


與+44 7761 714543進行的 RCS
即時通訊
MyFone提醒您門號尚有3022點將於今日到期，請盡快兌換獎品，逾期作廢 https://gov.taiwamlibk.xyz
輕觸即可載入預覽畫面
昨天 • 下午6:23
此為與 +44 7761 029396 進行的 RCS 即時通訊。瞭解詳情
【監理服務網】您違反道路交通管理事件，即將過線上處理期限，請於11/14之前盡快處理 https://mvedis.cc
【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
收到惡意簡訊內容
【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-bonk.com/


iMessage
今天 下午1:27
【遠通電收】提醒您，您有一筆NT$50臨時停車費用未繳清，逾期將處新臺幣三百元罰鍰。請複製官方網站連結並進行線上繳費 https://fecnet.top/


台灣自來水公司：您的水費已經欠費，今晚12點將停水.請您前往 https://wetargov.com 盡快繳費，給您帶來不便敬請諒解。

案例

在FB收到一個訊息...

識別釣魚連結的其他二三事

短網址服務
網路上的短網址服務，不容易識別真實連結

政府短網址
對於民眾來說，除了過去認明「gov.tw」網域名稱結尾的URL網址，現在也可認明「https://gov.tw/」開頭的連結。

認識濫用問題
一個Google、Onedrive、Dropbox的雲端硬碟的連結，是科技大廠提供的網路服務，但攻擊者將惡意檔案放在雲端硬碟上(要知道駭客很多會濫用合法工具的手法)

瀏覽器中的瀏覽器
簡單來說，就是透過JavaScript模擬一個假的瀏覽器來實現與真實網站URL一樣的網站

DNS
偽造、劫持，不同手法，造成類似結果
將使用者所連線目的地網站，改為惡意網站或詐騙網站，而不是前往正確網站
一般人難以防範和發覺

ChatGpt當紅，有哪些安全問題需要重視

AI技術仍在持續演進？現在的焦點

發展負責任的AI

發展可信任的AI

安全的使用AI

用AI為改善資安

人們對AI的信心和理解存在差距

很多電影小說 描繪的AI程度都已經很高，現在呢？

今年，生成式AI讓大家看到很方便，但我們要注意什麼？

為何強調機敏資料內容不能輸入（詢問）到生成式AI？

如同檔案上傳到外部雲端硬碟

使用生成式AI，也要辨別資訊有用或正確

如同使用搜尋得到一堆結果

了解是誰提供的生成式AI？

什麼是哪個應用面的生成式AI？

未來專屬領域生成式AI增加

了解當前生成式AI能力與強項

雖然比過去進步不少，到達堪用的程度，但仍很初期

生成式AI，駭客也在用，先前談的詐騙威脅更嚴峻

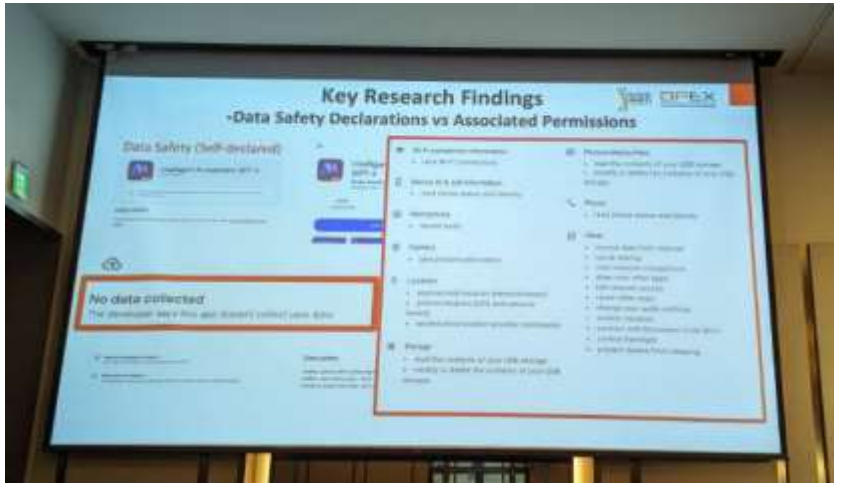
資料來源：https://www.ithome.com.tw/news/139454

先前談假冒，假生成式AI同樣超多

資料來源：https://www.ithome.com.tw/news/156736

這周參加GASA全球反詐聯盟，有資安專家分享現在很多App都說自己是生成式AI

但們要求的權限，根本是在蒐集你的資料



【必要有的4大資安意識】

美國CISA向民眾宣導
立即在帳戶上啟動MFA

2021年網路安全宣導月:
儘到您的責任。#BECYBERSMART

多重身份驗證

您是否注意到這幾天安全漏洞、數據被盜和身份盜竊經常成為頭版新聞？也許您或您認識的某個人是網絡犯罪分子竊取個人資訊、銀行憑據或更多事件的受害者。隨著這些事件變得越來越普遍，您應該考慮使用多重身份驗證，也稱為強力身份驗證或雙重身份驗證。您可能已經熟悉這種科技，因為許多銀行和金融機構需要密碼和以下其中一項才能登入：電話、電子信件或包含代碼的簡訊。通過將這些驗證原則應用在您的更多個人帳戶，例如電子信件、社交媒體等，您可以更好地保護您的線上資訊和身份！

那是什麼

多重身份驗證 (MFA) 被定義為一個保障安全的過程，需要來自獨立來源的多種身份驗證方法來驗證用戶的身份。換句話說，只有在提供唯一能識別該人的兩條或更多條訊息之後，才允許希望使用該系統的個人獲准使用。

這怎麼運作

憑證分為三類：您所知道、擁有或特徵的東西，以下是每個類別中的一些例子。

您所知道的事情
- 密碼/密碼短語

您有的東西
- 安全令牌或應用程式

您擁有的特徵
- 指紋

名和密碼
時間之內

立即在您的帳戶上啓動MFA

想要瞭解如何在您的帳戶上啓動 MFA，請前往鎖定您的登入網站，該處提供了有關如何將這種更強而有力的保護形式應用於您可能使用的許多常見網站和軟體產品的說明。如果您的任何帳戶未在該資源網站上列出，請查看您的帳戶設置或用戶配置文件並檢查 MFA 是否是一個可用的選項。如果您在那裡看到它，請考慮立即執行它！用戶名和密碼不再足以保護具有敏感資訊的帳戶。通過使用多重身份驗證，您可以保護這些帳戶並降低線上欺詐和身份盜竊的風險。還可以考慮在您的社交媒體帳戶上啓動此功能！

MFA 使未
盡可能使
組織會要
[您的數據

立即在您的帳戶上啓動MFA

想要瞭解如何在您的帳戶上啓動 MFA，請前往鎖定您的登入網站，該處提供了有關如何將這種更強而有力的保護形式應用於您可能使用的許多常見網站和軟體產品的說明。如果您的任何帳戶未在該資源網站上列出，請查看您的帳戶設置或用戶配置文件並檢查 MFA 是否是一個可用的選項。如果您在那裡看到它，請考慮立即執行它！用戶名和密碼不再足以保護具有敏感資訊的帳戶。通過使用多重身份驗證，您可以保護這些帳戶並降低線上欺詐和身份盜竊的風險。還可以考慮在您的社交媒體帳戶上啓動此功能！

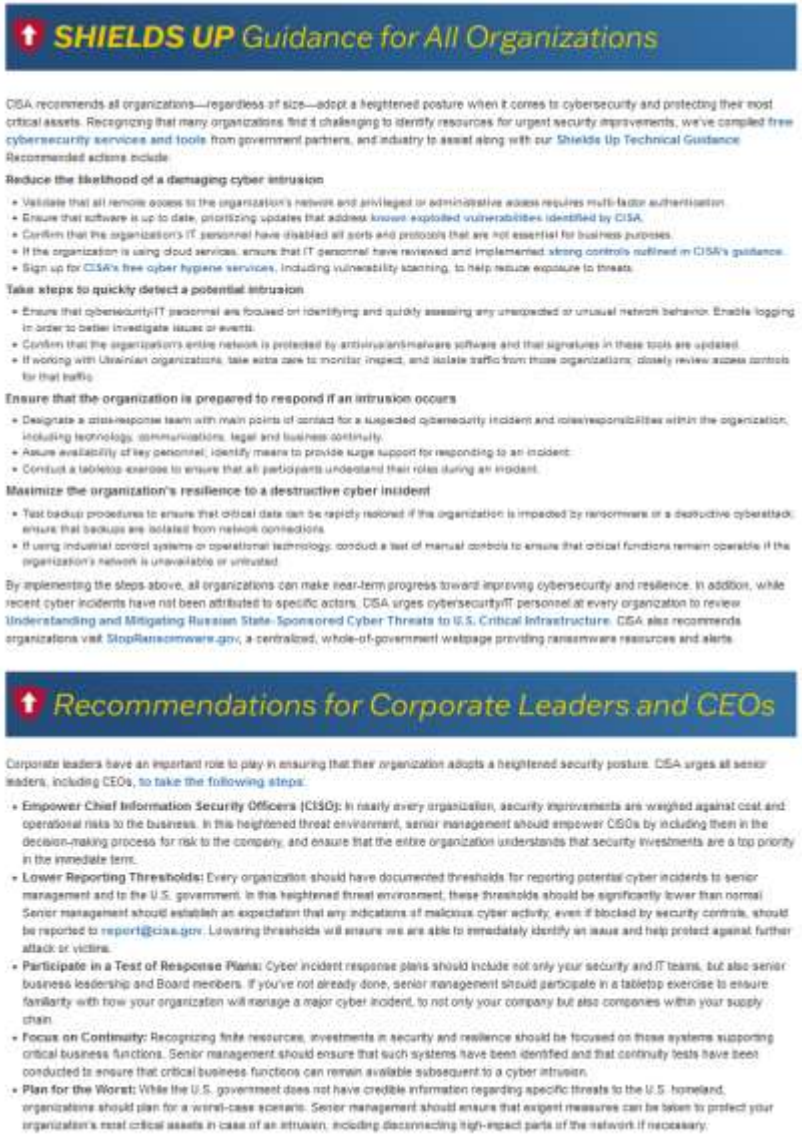
資料來源: https://www.cisa.gov/sites/default/files/publications/Chinese%20-%20Cybersecurity%20Awareness%20Month%202021%20-%20MFA%20Tip%20Sheet.pdf

你是否注意過國際上政府也在宣導企業做資安

資料來源: https://www.ithome.com.tw/news/150239、Shields Up | CISA

- 當中提供**企業通用資安防護指引**

- 不單強調設置資安長的重要性，還**強調資安長也要加入企業風險決策過程**



SHIELDS UP Guidance for All Organizations

CISA recommends all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets. Recognizing that many organizations find it challenging to identify resources for urgent security improvements, we've compiled free cybersecurity services and tools from government partners, and industry to assist along with our Shields Up Technical Guidance. Recommended actions include:

Reduce the likelihood of a damaging cyber intrusion

- Validate that all remote access to the organization's network and privileged or administrative access requires multi-factor authentication.
- Ensure that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA.
- Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.
- If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls outlined in CISA's guidance.
- Sign up for CISA's free cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats.

Take steps to quickly detect a potential intrusion

- Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.
- Confirm that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated.
- If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.

Ensure that the organization is prepared to respond if an intrusion occurs

- Designate a crisis-response team with main points of contact for a suspected cybersecurity incident and roles/responsibilities within the organization, including technology, communications, legal and business continuity.
- Assure availability of key personnel; identify means to provide surge support for responding to an incident.
- Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.

Maximize the organization's resilience to a destructive cyber incident

- Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.
- If using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.

By implementing the steps above, all organizations can make near-term progress toward improving cybersecurity and resilience. In addition, while recent cyber incidents have not been attributed to specific actors, CISA urges cybersecurity/IT personnel at every organization to review Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure. CISA also recommends organizations visit StopRansomware.gov, a centralized, whole-of-government webpage providing ransomware resources and alerts.

Recommendations for Corporate Leaders and CEOs

Corporate leaders have an important role to play in ensuring that their organization adopts a heightened security posture. CISA urges all senior leaders, including CEOs, to take the following steps:

- **Empower Chief Information Security Officers (CISO):** In nearly every organization, security improvements are weighed against cost and operational risks to the business. In this heightened threat environment, senior management should empower CISOs by including them in the decision-making process for risk to the company, and ensure that the entire organization understands that security investments are a top priority in the immediate term.
- **Lower Reporting Thresholds:** Every organization should have documented thresholds for reporting potential cyber incidents to senior management and to the U.S. government. In this heightened threat environment, these thresholds should be significantly lower than normal. Senior management should establish an expectation that any indications of malicious cyber activity, even if blocked by security controls, should be reported to report@cisa.gov. Lowering thresholds will ensure we are able to immediately identify an issue and help protect against further attack or victims.
- **Participate in a Test of Response Plans:** Cyber incident response plans should include not only your security and IT teams, but also senior business leadership and Board members. If you've not already done, senior management should participate in a tabletop exercise to ensure familiarity with how your organization will manage a major cyber incident, to not only your company but also companies within your supply chain.
- **Focus on Continuity:** Recognizing finite resources, investments in security and resilience should be focused on those systems supporting critical business functions. Senior management should ensure that such systems have been identified and that continuity tests have been conducted to ensure that critical business functions can remain available subsequent to a cyber intrusion.
- **Plan for the Worst:** While the U.S. government does not have credible information regarding specific threats to the U.S. homeland, organizations should plan for a worst-case scenario. Senior management should ensure that exigent measures can be taken to protect your organization's most critical assets in case of an intrusion, including disconnecting high-impact parts of the network if necessary.

資料來源: https://www.ithome.com.tw/news/150239、Shields Up | CISA

TAKE AWAY

1. 在你的網路服務帳戶上，啟用多因素身分驗證。
2. 更新你的軟體，開啟自動更新。
3. 點擊之前請深思。
4. 使用強密碼。

Steps You Can Take To Protect Yourself & Your Family

Every individual can take simple steps to improve their cyber hygiene and protect themselves online. In fact there are 4 things you can do to keep yourself cyber safe. CISA urges everyone to practice the following:

- **Implement multi-factor authentication on your accounts.** A password isn't enough to keep you safe online. By implementing a second layer of identification, like a confirmation text message or email, a code from an authentication app, a fingerprint or Face ID, or best yet, a FIDO key, you're giving your bank, email provider, or any other site you're logging into the confidence that it really is you. Multi-factor authentication can make you significantly less likely to get hacked. So enable multi-factor authentication on your email, social media, online shopping, financial services accounts. And don't forget your gaming and streaming entertainment services!
- **Update your software. In fact, turn on automatic updates.** Bad actors will exploit flaws in the system. Update the operating system on your mobile phones, tablets, and laptops. And update your applications – especially the web browsers – on all your devices too. Leverage automatic updates for all devices, applications, and operating systems.
- **Think before you click.** More than 90% of successful cyber-attacks start with a phishing email. A phishing scheme is when a link or webpage looks legitimate, but it's a trick designed by bad actors to have you reveal your passwords, social security number, credit card numbers, or other sensitive information. Once they have that information, they can use it on legitimate sites. And they may try to get you to run malicious software, also known as malware. If it's a link you don't recognize, trust your instincts, and think before you click.
- **Use strong passwords**, and ideally a password manager to generate and store unique passwords. Our world is increasingly digital and increasingly interconnected. So, while we must protect ourselves, it's going to take all of us to really protect the systems we all rely on.

資料來源: https://www.ithome.com.tw/news/150239、Shields Up | CISA

上述案例

重點就是在釣魚連結、釣魚信

大家不論生活或工作都可能遇到，你真得有警覺嗎？

為何常說不要亂點連結？
點擊前請三思。

另外，請體認備份的重要性

自己從學生時代就「備份」，並要要妥善的備份。
基本觀念
●備份是存在不同儲存裝置都保有相同的檔案，不是同一台電腦C槽D槽
●注意資料同步不等於備份。
●一式三份、連線備份

隱私面
● 「愛愛在雲端」電影， 一對夫妻因為錄下親密關係無意間分享到之前已經送給友人的iPad

企業面
●許多勒索軟體攻擊事件駭客也會針對企業備份系統加密，讓企業無法復原

最後

下一頁整理出**「從新聞看資安」，透過10大專題報導**，讓個人可以更懂企業資安，當中一些部分，對於個人的資安認知也有幫助。
畢竟，未來大家也要出社會

Take Away

1.資訊安全是每個人的責任，而資訊安全專責單位也將給予各位協助
2.資安不是無限上綱，風險因應有一定成本
3.資訊安全事件有時無法避免，事情發生後重點在如何妥善處理而非互相指責

看資安新聞學資安觀念			
臺灣資安即國安戰略意涵大公開，推動資安不只是政府的事（2021-12-17）	資安是全民的事，從前行政院資通安全處處長的演說中，讓大家可以更深入理解，政府是如何看待資安威脅的問題，並且何以與國安有關，當中不僅可以幫助大家建立資安相關背景認知的輪廓，也提到資安並不是要無限上綱的觀念。	**化被動為主動，企業開始懸賞抓漏**（2018-09-29）	漏洞的產生是不可避免的，發布漏洞獎勵計畫（Bug Bounty），藉助全球駭客之力已是全球大型企業都在做的事，因為可以讓自己的資安做得更好，但也要認知到現況，可能不是每家企業對於漏洞通報的觀念都處於正面。
https://www.ithome.com.tw/news/148415		https://www.ithome.com.tw/article/126023	
NIST CSF網路安全框架當紅，靈活彈性易上手（2019-09-26）	資安不是只有從防護著手、避免駭客入侵，從網路安全風險管理的生命週期來看，美國NIST分為五大階段：識別、保護、偵測、回應與復原，同時資安成熟度的概念也相當重要	**回收紙的大問題，紙本文件控管與銷毀**（2011-09-09）	機密資料保護從很多年就是企業重視的問題，但也有不經意的舉動，呈現出控管不當的問題，像是回收紙引發的關注中，其實也反應出機密資料分級、資料生命週期等、安全銷毀等議題。
https://www.ithome.com.tw/article/133173		https://www.ithome.com.tw/article/91142	
從防疫學防駭（2020-07-25）	從借鏡防疫上與防駭上的共通概念，讓一般人對資安防護更有感，體認到每個人都是破口。從情資重要性、情資查核、敵我意識、疫情中心與應變團隊、傳染病防治法與資安防駭準則、每日記者會與溝通、勤洗手戴口罩與資安衛生習慣、防疫國家隊與資安產業、簡訊細胞與情資分享，到疫調不獵巫與看待資安的正向態度。	**聯網安全管理瀕臨失控，威脅事件頻傳**（2017-05-27）	在網路威脅與日遽增下，各式連網設備都存在被利用或濫用，或成為跳板的可能性，以學校印表機遭他人擅自印出帶有威脅內容的文字為例，這種顯性的威脅其實都是警訊，與網站內容置換、廣告看板內容置換相同，還有更多不易直接察覺遭入侵的威脅。
https://www.ithome.com.tw/article/138913		https://www.ithome.com.tw/article/114125	
肆虐升溫，勒索軟體災情擴大的7項原因（2016-07-23）	為什麼勒索軟體威脅持續橫行之今，不只讓原本用於保護資料的技術，變成駭客要脅利用的手法，虛擬加密貨幣的興起，其高匿蹤性連帶也讓黑色產業在有利可圖的驅動下而活躍。	**美國升起資安防護罩**（2022-04-02）	資安威脅加劇之下，已成全球重大風險，不指臺灣推動資安即國安，其實全球也都是如此，美國白宮不僅要求聯邦組織機構，並在2022年3月發布公告，要求企業、關鍵基礎設施業者積極提升防護力，並頒布了一份全國資安防護指引計畫Shields Up，當中有針對企業的通用指引，給企業高階主管的建議，還有勒索軟體應變，以及個人與家庭的自保資安觀念。
https://www.ithome.com.tw/news/107150		https://www.ithome.com.tw/article/150240	
防護釣魚郵件成為資安當務之急（2018-01-21）	透過電子郵件管道的網路威脅存在多年，僅管防護功能不斷演進，但釣魚郵件也在進化，2018年時又有愈來愈多網路攻擊以此做為開端，因此提醒企業與民眾，需重新認識釣魚郵件威脅，並揭露最新網路犯罪使用的釣魚詐騙手法	2019國家級資安事件：勒索軟體侵襲臺灣醫院（2019-11-14）	徹底揭露2019年臺灣全臺多家醫療院所遭勒索軟體的攻擊事件，同時也從院方的實際經驗，讓大家清楚有些醫院為何被感染了卻能快速復原，以及有些醫院為何能成功擋下勒索病毒，讓大家更具體認識如何處理類似事件。
https://www.ithome.com.tw/article/117070		https://www.ithome.com.tw/article/134112	

謝謝大家

https://www.facebook.com/ithomecyber

https://www.ithome.com.tw/security

「生活資安五四三！：從生活周遭看風險與資訊安全」

作者：羅正漢

目前也擔任iThome電腦報資安主編

「生活資安五四三！從生活周遭看風險與資訊安全」第二版https://www.books.com.tw/products/0010942493

撰寫此系列文章的原因，與筆者這幾年的工作有關，筆者是在企業 IT 媒體「iThome 電腦報週刊」，從技術編輯到資安主編，陸續報導許多企業 IT 的資安產品、技術與新聞事件，還有各式各樣的 封面故事與專題，不過因為報導形式都是針對企業用戶的讀者，提供給企業的資訊，因此角度就會以企業該知道的事為主。

但除了專業領域的資安議題，有些普遍性的資安議題，其實也與一 般人的資安意識有關。例如，很多網路攻擊事件是從一封釣魚郵件 而起，以及有些企業會定期舉辦資安意識相關的教育訓練課程，或是網路攻擊者假冒企業名義散布釣魚簡訊，引起一般使用者上當。因此，一般民眾也該了解，自己也該有要注意的資安意識與觀念。 只是，普遍給一般大眾閱讀的專業大眾媒體與專業網路科技媒體， 有些寫得不錯，但常有資訊量不足的情況，如同前面所提，這些資訊通常分散在新聞資訊中，少有綜合性的整理。 而這次能夠獲得優選出書，最重要目的，就是希望讓大家先增進對 資安的興趣，能夠多去認識資安。雖然一開始，其實也怕自己談不 深，畢竟資安的東西接觸多了，就會知道資安下的每個領域都是一 門專業；但同時也怕自己談不淺，畢竟大家對資訊、網路與資安的 程度不一，如何能讓一般人都有興趣，我想是更重要的關鍵。

iThome電腦報資安主編羅正漢 聯絡方式:laulau@mail.ithome.com.tw