長庚大學
CHANG GUNG UNIVERSITY

社交工程防護暨資訊安全宣導教育訓練

主講人：王俊凱 執行長

2024/12/05

財團法人中華民國國家資訊基本建設產業發展協進會
National Information Infrastructure Enterprise Promotion Association

簡報綱要

01 資訊安全宣導事項

02 社交工程

03 Q&A

簡報綱要

01 資訊安全宣導事項

02 社交工程

03 Q&A

危害國家資通安全產品限制使用原則(1/3)

- 依據教育部112年6月30日臺教資字第1120062668號函辦理。
- 公務用資通訊產品(含軟體、硬體及服務)不得使用大陸廠牌，機關若因業務需求且無其他替代方案，仍需使用危害國家資通安全產品時，應具體敘明理由並經機關資通安全長及其上級機關資通安全長逐級核可，函報資通安全管理法主管機關(數位發展部)核定，產品未汰換前，應加強下列資安強化措施：
  - ✓ 強化資安管理措施，例如：設定高強度密碼、禁止遠端維護等。
  - ✓ 產品遇資安攻擊導致顯示畫面遭置換，應立即置換靜態畫面，或立即關機。
  - ✓ 產品若為硬體，應確認其不具WiFi等持續連網功能(非僅以軟體關閉)。若需以外接裝置方式進行更新，須有專人在旁全程監督，於傳輸完成後立即移除外接裝置。
  - ✓ 產品使用屆期後不得再購買危害國家資通安全產品。

危害國家資通安全產品限制使用原則(2/3)

- 各機關辦理採購案時，應注意以下事項：
  - ✓ 參考行政院公共工程委員會採購範本投標須知範本第16點，廠商所供應標的(含工程、財物及勞務)之原產地不允許大陸地區，以及資訊服務採購契約範本第8條第24款，如採購案內涉資通訊軟體、硬體或服務等相關事務，機關可要求廠商執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。
  - ✓ 各機關自行或委外營運，提供公眾活動或使用之場地，不得使用危害國家資通安全產品，且應將相關限制事項納入委外契約或場地使用規定中。
- 請各單位於辦理採購時，務必依「大陸廠牌資通訊產品及委外經營公眾場域盤點原則」查證，勿採購大陸廠牌資通訊產品。
- 建議多利用共同供應契約採購相關設備，避免採購大陸廠牌資通訊產品。

危害國家資通安全產品限制使用原則(3/3)

- 行政院未提供相關設備清單，以下廠牌僅供參考，包括但不限於：
- 杭州海康威視（Hikvision）、華為（Huawei）、深圳大疆創新科技公司（DJI）、普聯技術公司（TP-Link）、廣東歐加控股公司 / 廣東行動通訊公司（OPPO）、小米集團（MI）、浙江大華技術公司（Dahua）等。

簡報綱要

01 資安與個資宣導

02 社交工程

03 Q&A

病毒入侵企業60% 源於內部員工

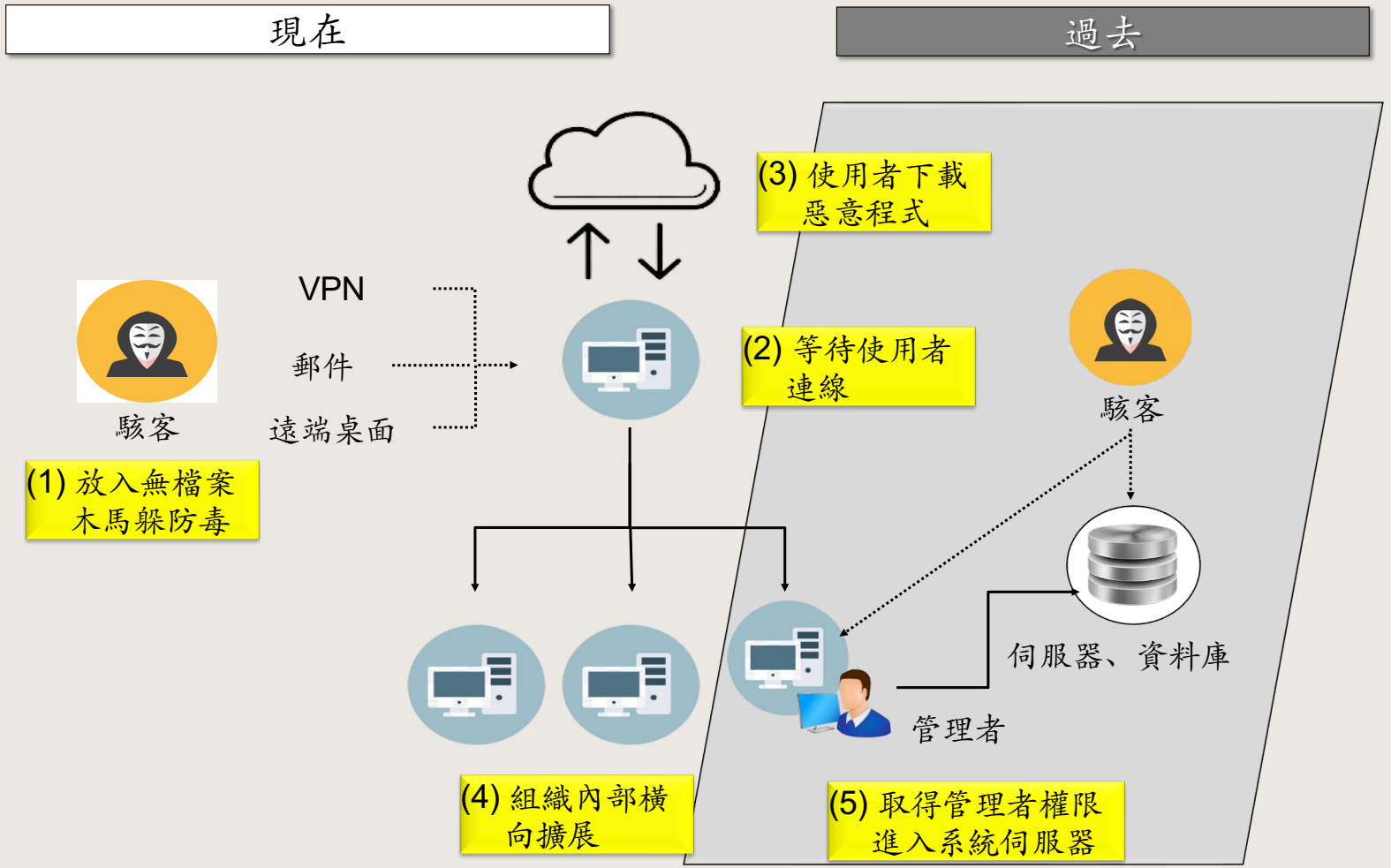
- 病毒入侵企業60% 源於內部員工
  - 勒索病毒入侵的途徑相當繁雜，主要可區分為三類：
    - 電子郵件網絡釣魚活動
    - 遠程桌面協議漏洞
    - 軟體漏洞

- 順利進入企業內網後，駭客會首先試圖破解網域控制伺服器（AD）或者想取得具備派送功能軟體權限，再將病毒擴散到各台電腦後伺機潛伏，橫向擴散造成群聚感染。
  - 以勒索的手法來區分，大致可分為二類，
    - 鎖住被害者的電腦

      要求被害者必須繳納贖金，才能拿回電腦的控制權。
    - 加密被害者電腦上的檔案

      亦是要求被害者繳納贖金，才能拿到解密金鑰，以便解密檔案。

傳統與新型態的駭客攻擊手法



資安事件常見發生原因

- 供應鏈攻擊（廠商疏漏） 攻擊者鎖定供應鏈廠商發動攻擊，提升攻擊效益。
  - 廠商環境：廠商遭入侵並將做為跳板，進一步駭侵機關攻擊。
  - 產品漏洞：產品設計不當或零時差漏洞(ZeroDay)利用。
- 人員資安意識不足（人員訓練） 導致資料外洩事件持續發生。
  - 作業疏失：行政作業疏失，將機敏資料上傳至公開平台。
  - 設定不當：對系統操作不熟悉，致使檢視權限設定不當。
  - 人員意識：人員資安意識不足，誤開啟釣魚郵件、安裝未經授權程式。
- 資通設備弱點未即時更新（漏洞修補） 致遭利用發動挖礦劫持。
  - 系統弱點：系統弱點未即時修補，致使遭利用入侵。
  - 管理疏失：缺乏日誌紀錄保存機制。

社交工程 / 電子郵件社交工程

- 社交工程
  - 利用人們的好心、消費習慣等，誘騙其執行惡意攻擊者所規畫之行動，即稱為『社交工程』。
- 電子郵件社交工程
  - 電子郵件現今已取代傳統紙本郵件，深入人們的日常生活作為業務聯絡與訊息傳遞的主要媒體。
  - 駭客透過網路釣魚信件在目標主機植入木馬，進而竊取機敏資訊，造成組織企業龐大的損失，
- 電子郵件社交工程演練
  - 為防範這些事件，企業與各機關組織可透過郵件社交演練，來提升組織員工對社交工程信件的機警性。

釣魚信件

- 釣魚信件

  利用寄發電子郵件，假冒親友或公司等相關寄件者，誘騙收件者信任，或引發收件者注意，開啟郵件進行非法攻擊行為。

想要達成的目的

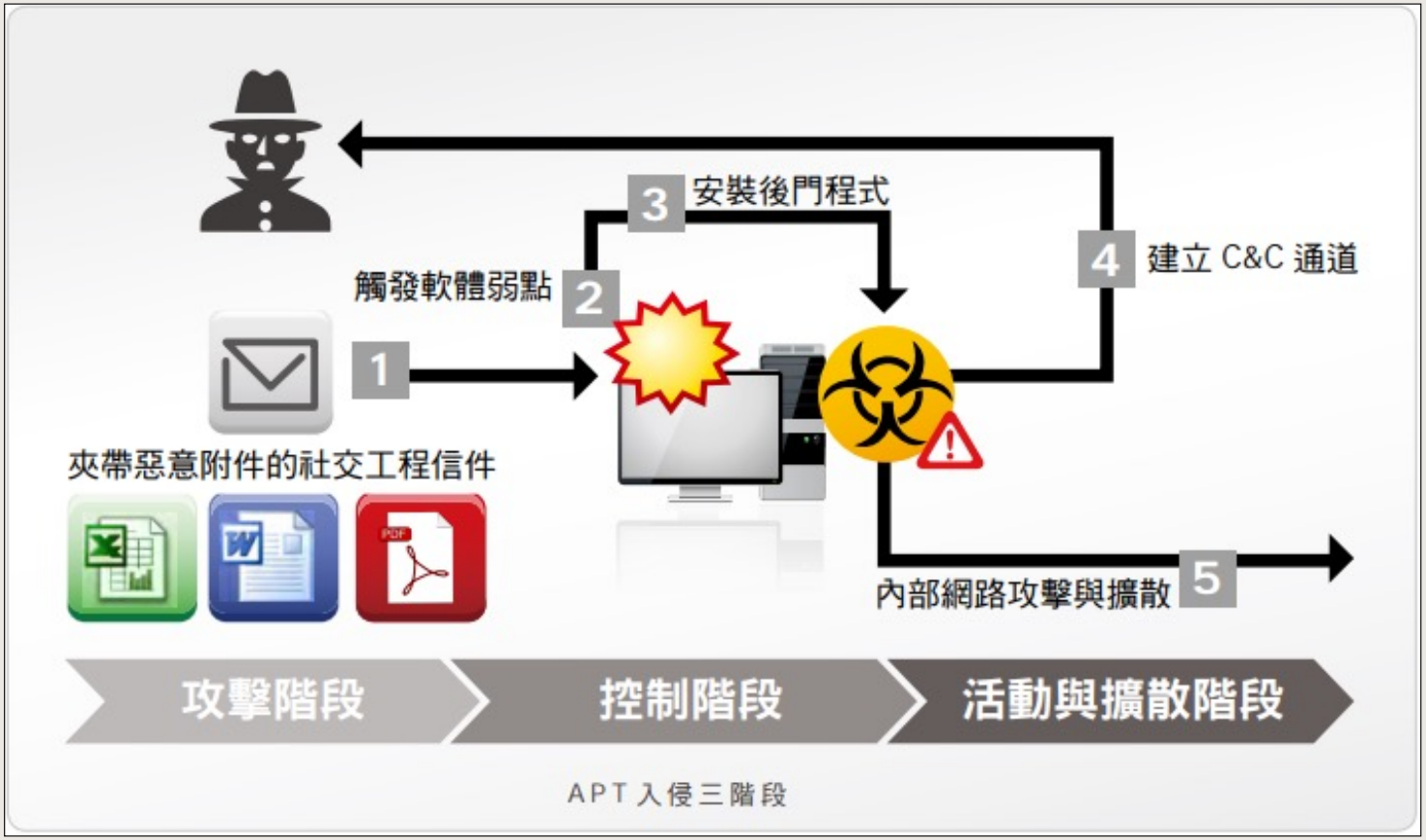
- 誘騙登入帳號、密碼（騙取資料）
- 通知重新認證（騙取資料）
- 開啟惡意連結（連線釣魚網站）
- 下載惡意附件檔（載入電腦病毒）

釣魚信件的特徵

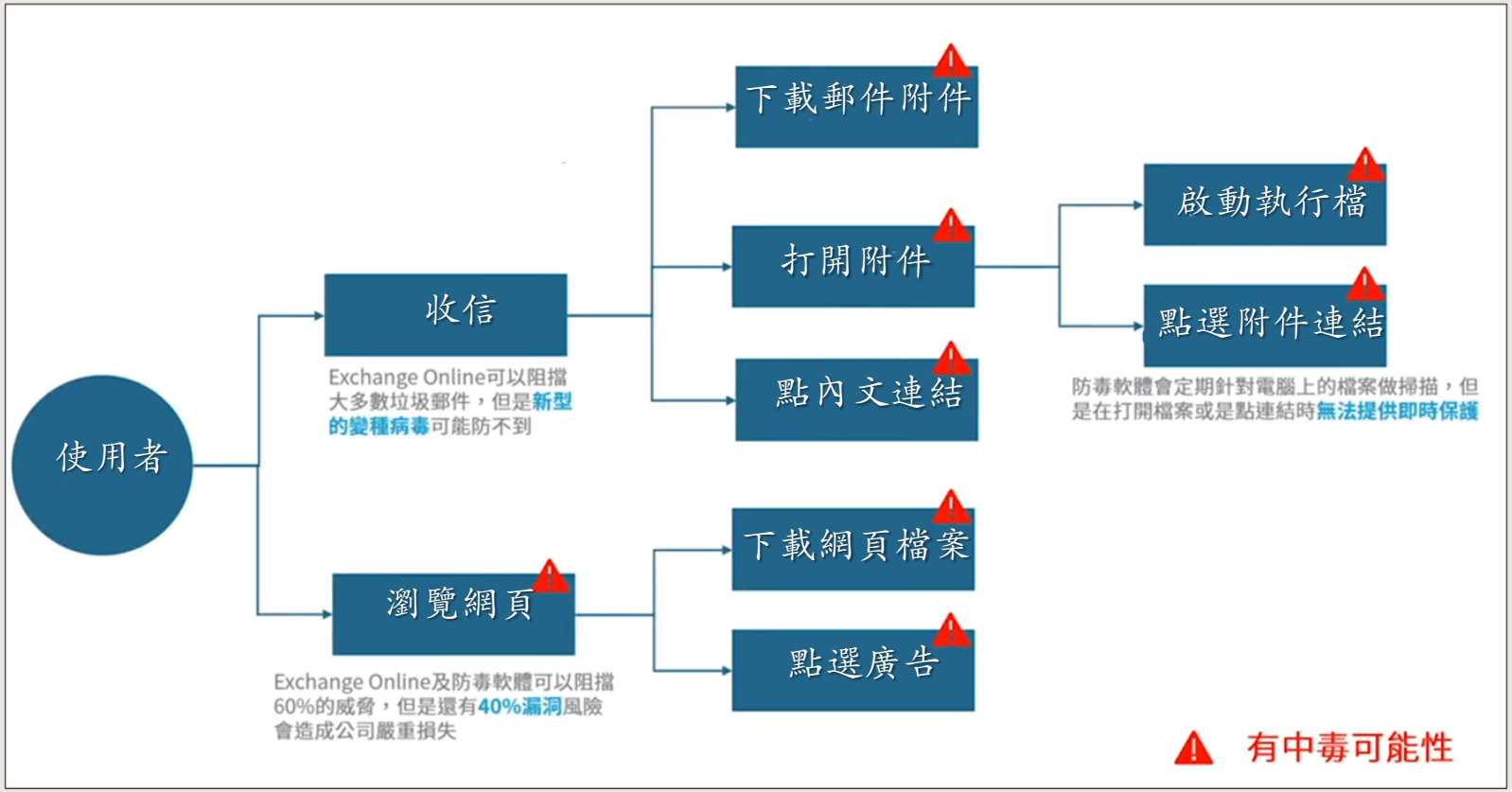
- 寄件者為陌生人或極少來往對象
- 非正常的寄信時間 (如：深夜或下班時間)
- 過於聳動、緊急或誘人的主旨
- 主旨與發信人的習性不同
- 需要輸入敏感資料的信件

釣魚信件的危害模式

- 寄發社交工程信件
- 觸發軟體弱點
- 安裝後門程式
- 建立C&C通道
- 內部網路攻擊與擴散

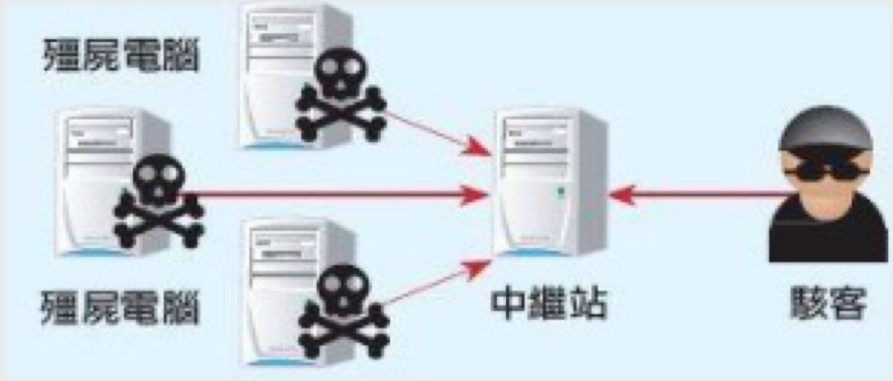


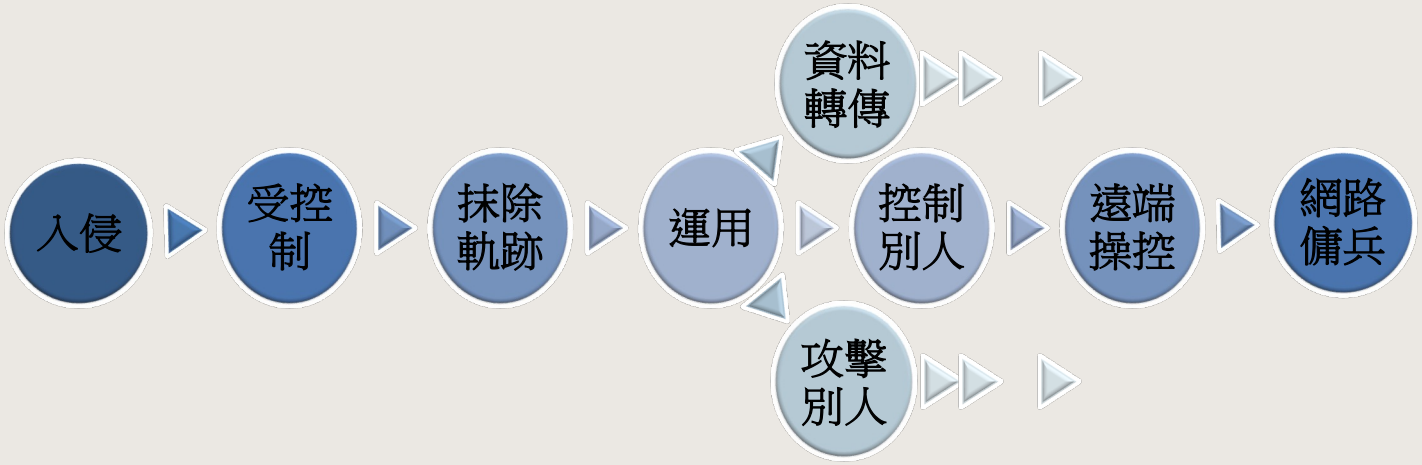
- 開啟郵件或瀏覽網頁面臨的風險



社交工程有什麼影響

- 殭屍電腦
  - 個人電腦遭控制，隱私、機密全都露
  - 成為犯罪工具(共犯結構)-DDoS
  - 刑事(罰金/判刑)、民事(賠償)、行政(罰鍰)責任





社交工程有什麼影響

- 勒索軟體
  - 資料遭加密
  - 系統(服務)停擺
  - 有形或無形損失
  - 檔案被「加密」成人質
  - 文件無法「自行解密」
  - 「勒索付錢」才給解密檔案之鑰匙，但是付了未必可以解

- 新興勒索軟體組織Money Message於2023/4/5在網站上聲稱已竊取微星科技1.5TB 的資料，其中包含CTMS與ERP系統資料庫，以及其他如軟體原始碼、憑證，以及BIOS框架文件、韌體等各式檔案。該組織表示，假使微星科技未在4月10日以前支付**400萬美元**贖金，就會把上述資料全數公開。
- 微星科技同時也提醒客戶：「若要更新韌體 / BIOS務必到MSI微星科技官網取得檔案，請勿使用官方以外的檔案進行更新。」

Money Message

Hello!

< 1 2 3 4 5 6 >

Micro Star International

05-04-2023

Reveal timer: 133h 40m 45s

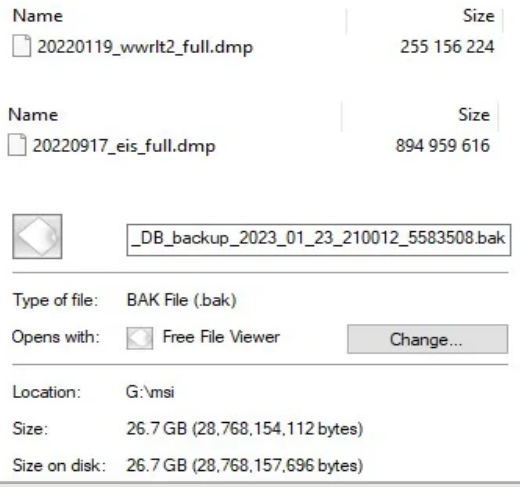
Micro-Star International AKA MSI designs, manufactures, and sells motherboards and graphics cards for customers in the United States, Canada, and internationally. MSI is headquartered in Taipei, Taiwan. MSI source code, including framework to develop bios, also we have private keys.

We will publish stolen data when timer expires.

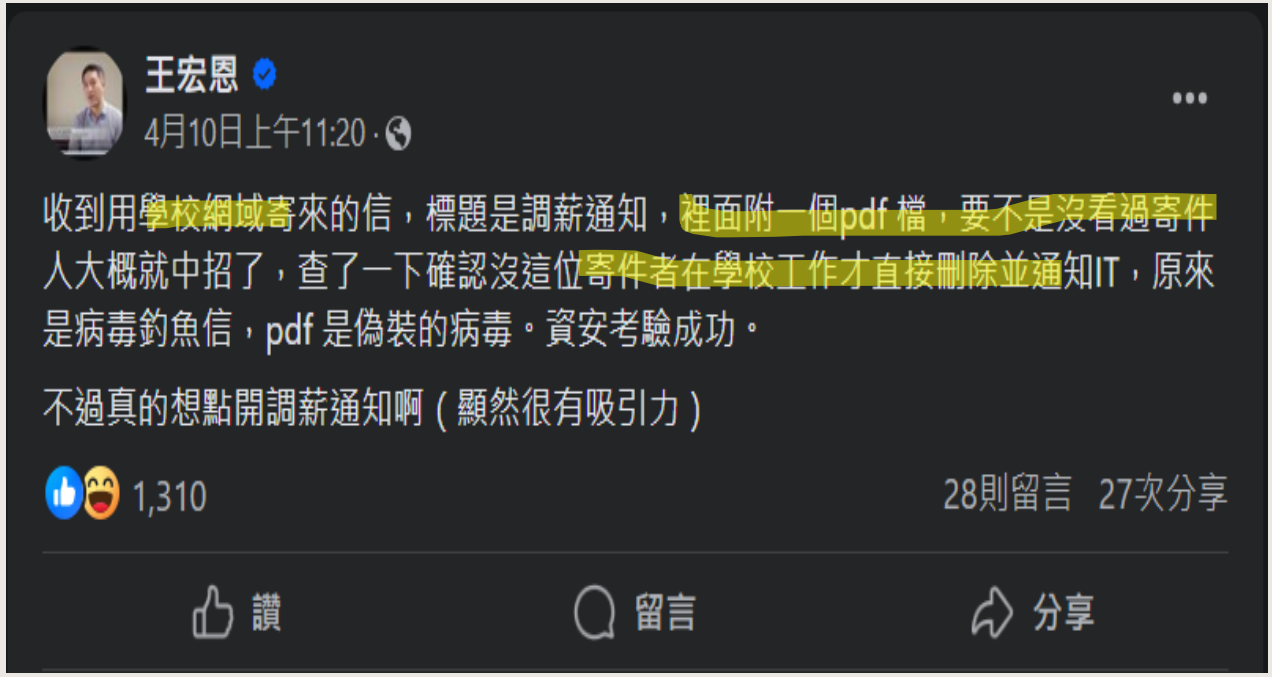
Databases: wwrlt2, eais, CTMS, ERP.

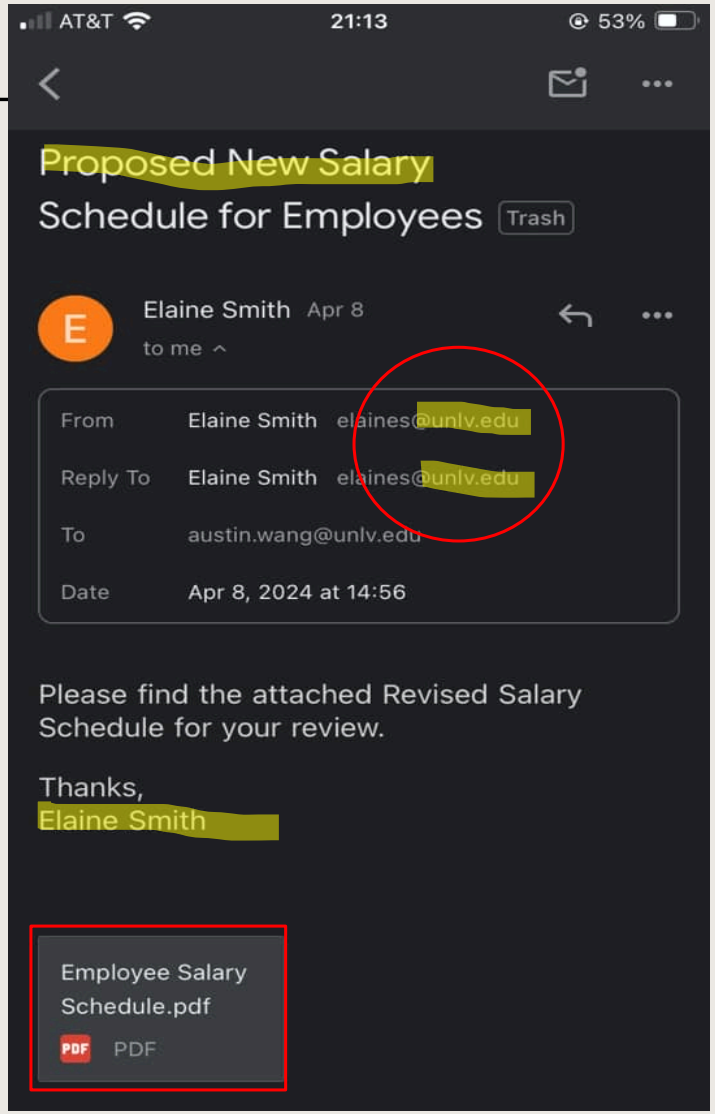
Revenue: $7B

Website: msi.com



社交工程郵件實例





圖片來源：
美國內華達大學政治系副教授王宏恩FB

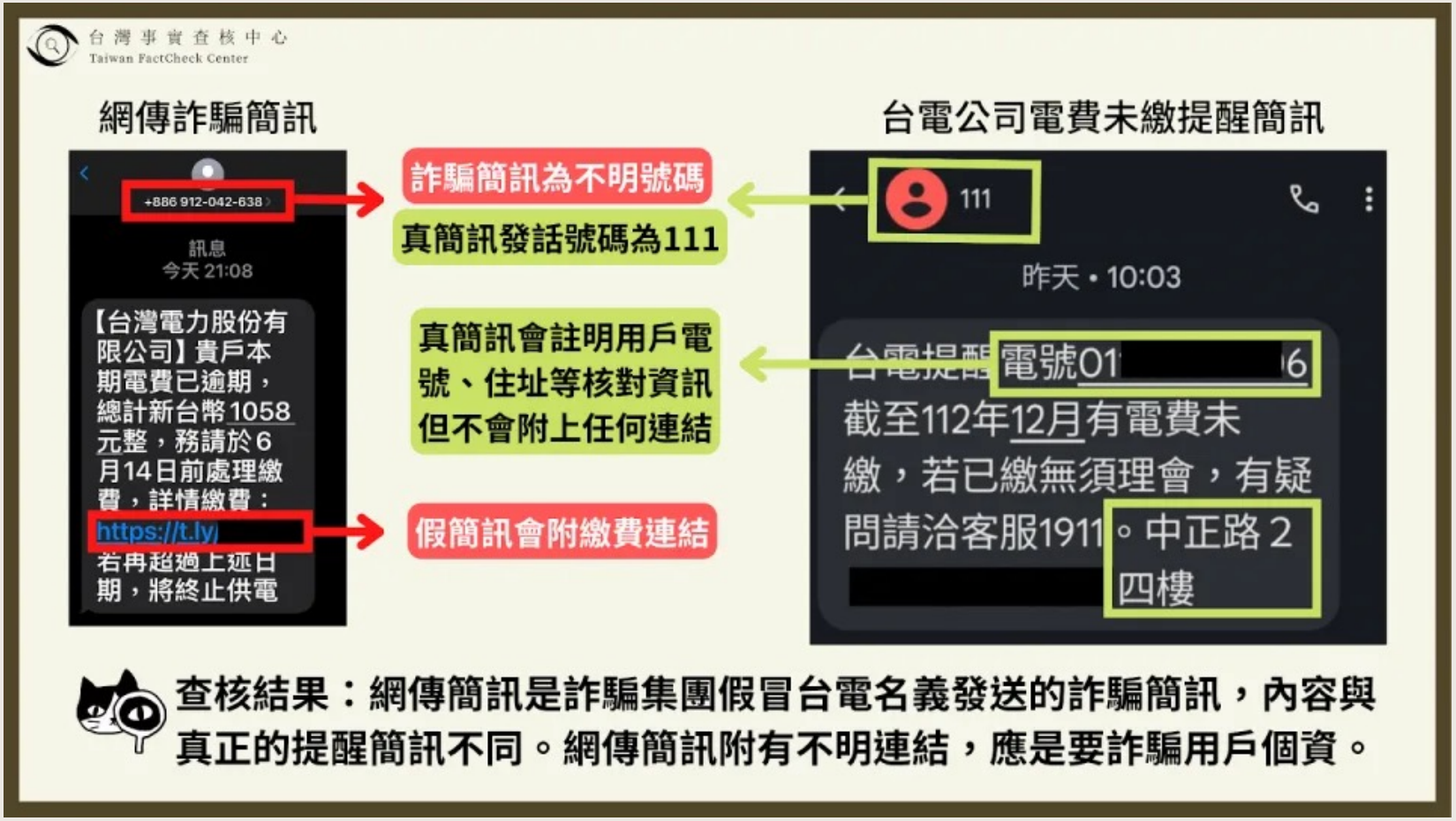
注意社群軟體，小心中大獎

- 現今長輩們變得更時尚年輕，已開始使用LINE或是FB等社群軟體。
- 使用很多標題聳動的新聞，資訊等來吸引注意力。
- 但是有很多LINE訊息、網站等，其實都是有問題的。
- 請記得，不要點，不要開！
- 如果真的好奇，請先多方查證其真實性。

（1）LINE 官方並沒有這類型的 LINE Pay 領紅包的活動，進入的網址為詐騙網站。
（2）點擊詐騙連結後會誘導分享，後續可能被盜取個資或帳號。
（3）刑事警察局提醒切勿點選連結，務必到官方網站查驗活動真偽。

社交工程攻擊手法(網路釣魚 – SMS簡訊)

社交工程攻擊手法(網路釣魚 – SMS簡訊)



釣魚網站

- 利用誘人的內容欺騙使用者點擊到偽造網站，
  使用者輸入機密資料後，即遭竊
- 技術門檻低
- 利用使用者的粗心
- 申請與原本網站類似的網址
- 大部分使用者不會很注意上方網址


假冒Apple ID 登入畫面
假非網址
154.91.237.30
Apple ID
Apple ID
管理你的 Apple 帳號
Apple ID
真Apple網址
appleid.apple.com
Apple ID
Apple ID
管理你的 Apple 帳號
Apple ID
刑事警察局
165 Anti-fraud Hotline Service

➢對網址的混淆

- 數字零(0) 與
  英文大小寫(O/o)
- 英文小寫L(l) 與
  數字壹(1)
- 英文大寫I(I) 與
  英文小寫L(l)
- 英文大寫W(W) 與
  英文大寫連兩個V (VV)
- 英文小寫M(m) 與
  英文小寫RN(rn)


Google
您的Google Pixel 4 XL檢測出(2)個病毒！
OK
Google
您的Google Pixel 4 XL檢測出
個病毒！
04 : 39 : 03
假裝系統警告的詐騙

技術面防護

- 強化郵件軟體設定
  - ✓ 關閉郵件自動預覽
  - ✓ 關閉自動下載圖片
  - ✓ 不要自動回覆
  - ✓ 以純文字格式讀取郵件
- 確認對應軟體都保持在最新修補的狀態 (如：收信軟體、瀏覽器、文書作業軟體、防毒軟體)

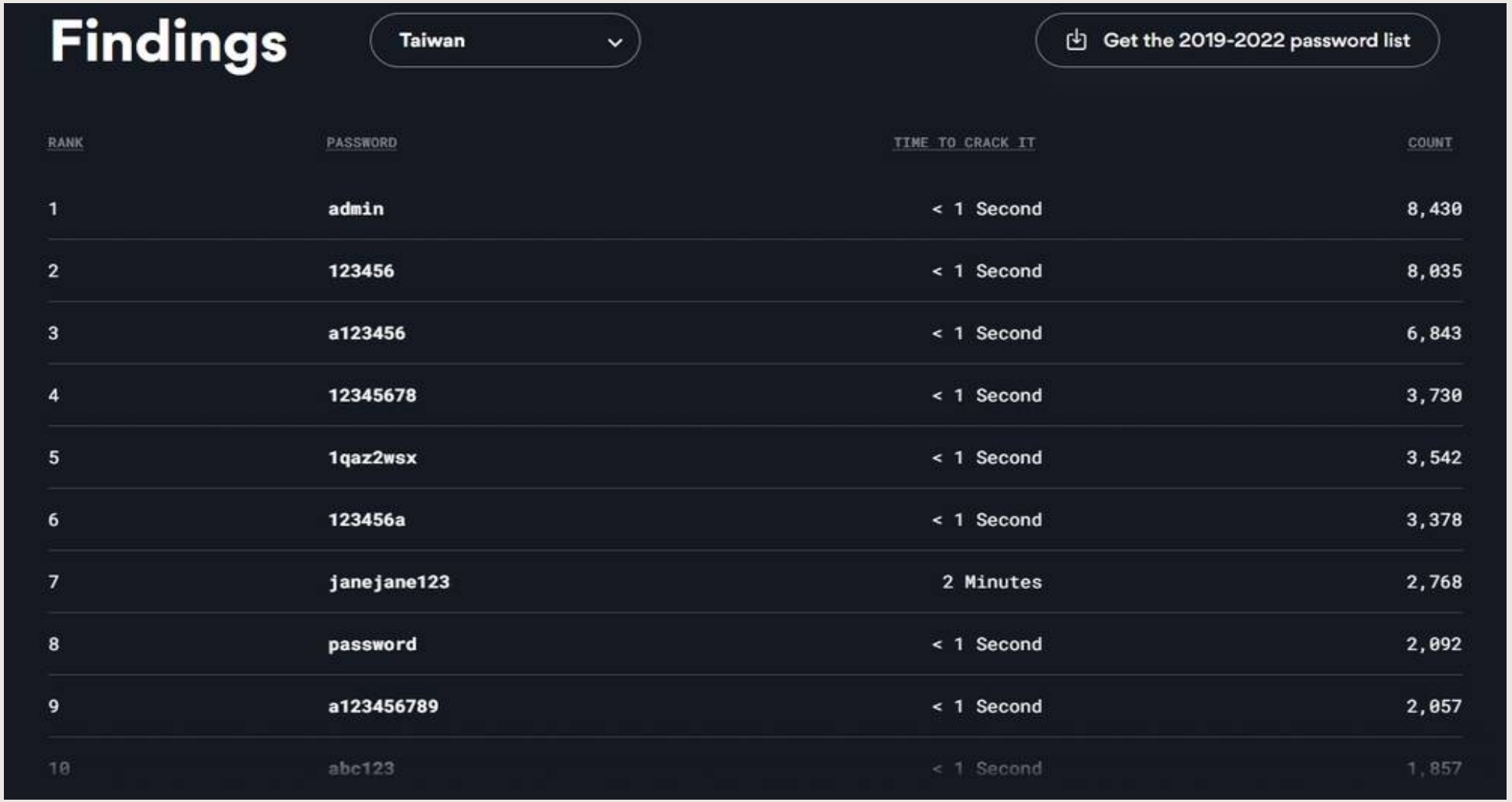
行為面防護

- 收信
  - 檢查寄件者、收件者的真偽 (例如：.gov、.org)
  - 確認信件主旨、內容的真實度，確認信件內容與公務相關
  - 不輕易開啟郵件的超連結及附件
  - 開啟超連結或附件前，確認對應軟體 (例如：Chrome、 Edge、Office、防毒軟體) 都保持在最新修補的狀態
- 轉信或寄信
  - 未經查證之訊息不要轉寄
  - 轉寄郵件前先將他人郵件地址刪除，避免別人郵件地址洩漏
  - 寄送信件給群體收件者時，應將收件者列在密件副件，以免收件人資訊外洩

制度面防護

- 強化密碼設定政策
  - 複雜度要求
    - 密碼長度至少8碼以上。
    - 密碼複雜度設定至少需由英文、大小寫、數字或特殊符號組成。
    - 避免使用與帳號相同的字元。
    - 避免使用個人資料，如生日、電話號碼與身分證字號等。
    - 避免使用單位名稱、員工編號或其他相關事項。
- 定期變更密碼（每6個月更換一次）
- 勿將密碼告訴他人

圖片來源：https://www.omnicybersecurity.com/most-common-passwords-2023/



Findings

Taiwan

Get the 2019-2022 password list

RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	admin	< 1 Second	8,430
2	123456	< 1 Second	8,035
3	a123456	< 1 Second	6,843
4	12345678	< 1 Second	3,730
5	1qaz2wsx	< 1 Second	3,542
6	123456a	< 1 Second	3,378
7	janejane123	2 Minutes	2,768
8	password	< 1 Second	2,092
9	a123456789	< 1 Second	2,057
10	abc123	< 1 Second	1,857

圖片來源： https://nordpass.com/most-common-passwords-list/

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

HIVE SYSTEMS

Cybersecurity that's approachable.
Find out more at hivesystems.io

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

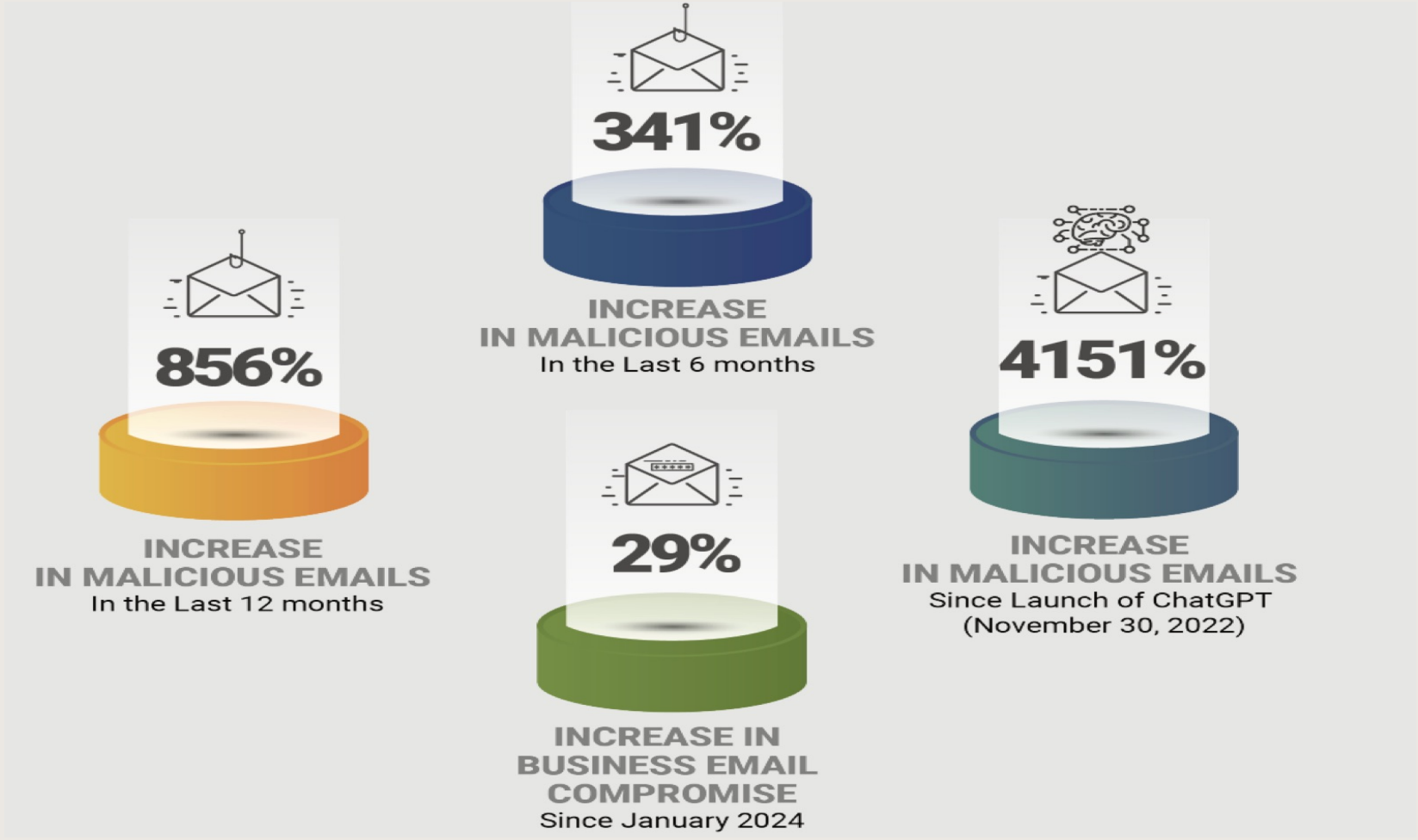
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

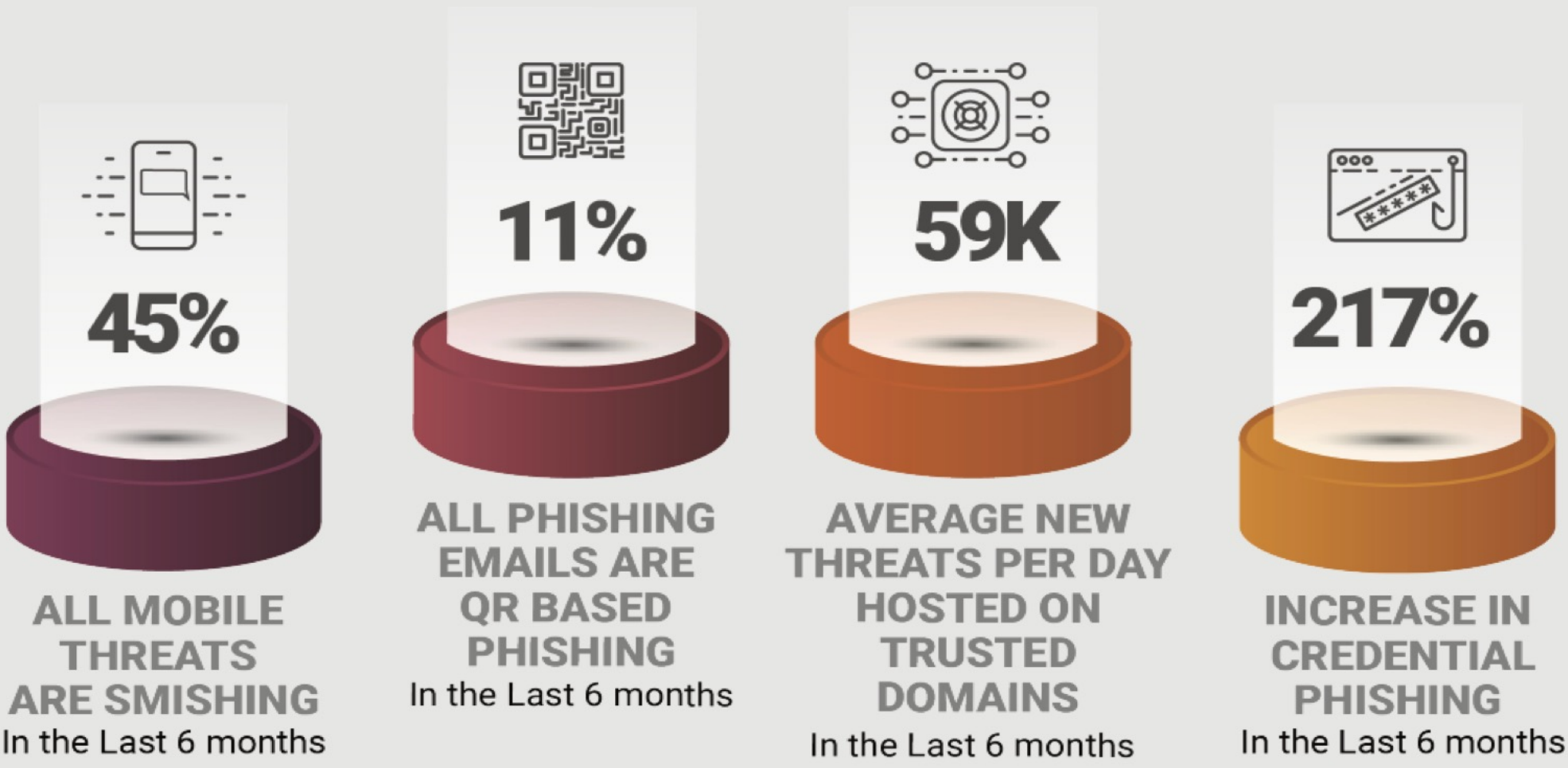
圖片來源：https://www.hivesystems.com/blog/are-your-passwords-in-the-green

2024年社交工程中調查報告



- 資料來源：SlashNext-The-State-of-Phishing-24-Midyear-Report

2024年社交工程中調查報告



- 資料來源：SlashNext-The-State-of-Phishing-24-Midyear-Report

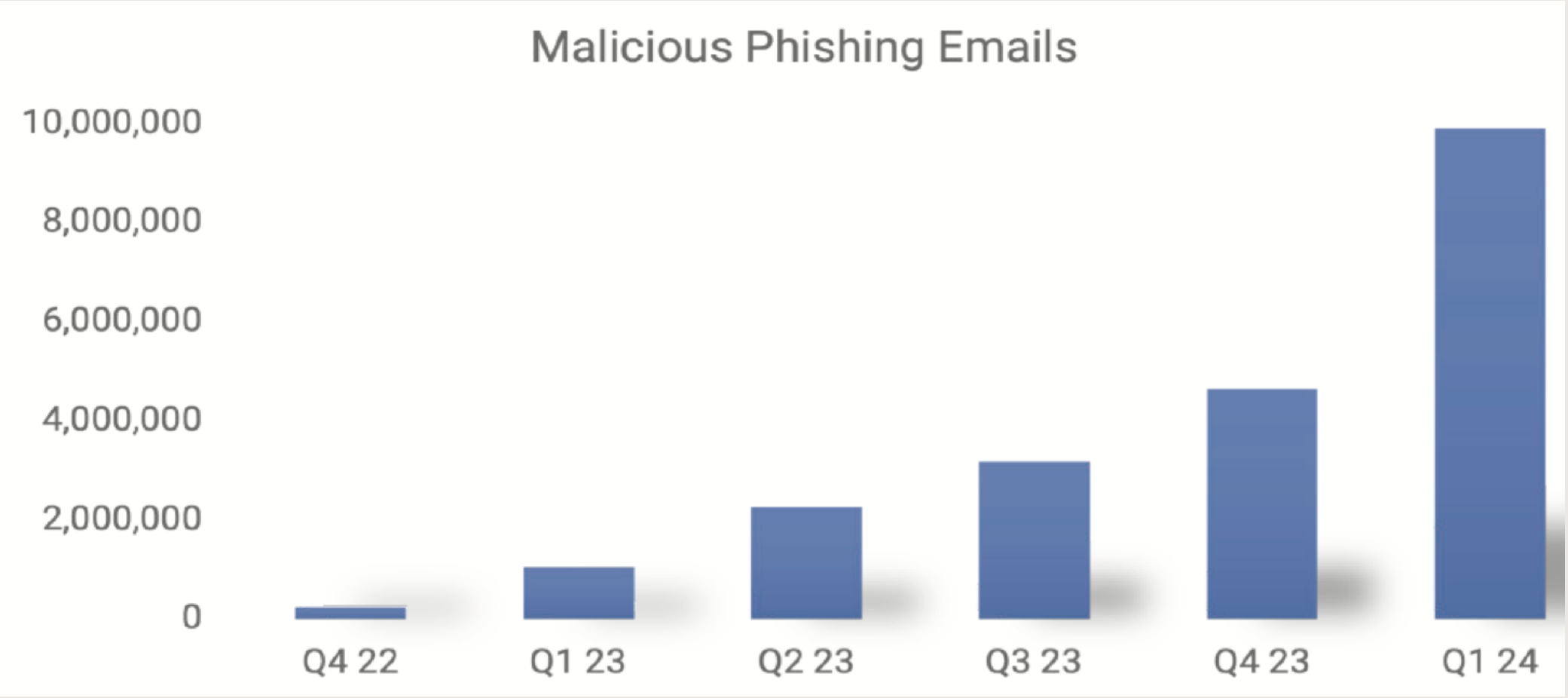


Exhibit 1: Phishing has increased by 341% in the last six months and 856% in the last 12 months.

- 資料來源：SlashNext-The-State-of-Phishing-24-Midyear-Report

Check Point最新調查：已有近半數企業遭到社交工程迫害

- 社交工程帶來嚴重威脅：86%的資安人員意識已高度意識到社交工程帶來的危機。約48%的受訪企業坦承已為社交工程的受害者，在過去兩年間遭受25次以上的攻擊。

  社交工程攻擊會造成嚴重損失：受訪者估計每次發生的資安事件會導致2.5萬至10萬美金以上的成本損失，包括業務中斷、客服費用、收入損失及商譽受損等相關成本。

  社交工程最常見威脅來源 - 網釣電子郵件：網釣郵件在社交工程攻擊上排名第一(47%)，其次為可能曝露個人及職業資訊的社群網站(39%)，再來是有漏洞的行動通訊設備(12%)。

  社交工程的主要動機 - 詐財：據研究，詐財是社交工程攻擊的最常見原因，其次為竊取機密資訊(46%)、取得競爭利益(40%)及報復行為(14%)。

  新進員工最容易成為社群工程的下手對象 - 受訪者相信新進員工是成為社交工程受害者的高危險群，其次為約聘人員(44%)、行政助理(38%)、人資專員(33%)、企業領導人(32%)及IT人員(23%)。不論員工在公司內的職掌為何，適當訓練及提升使用者警覺心都是任何資安政策的關鍵要素。

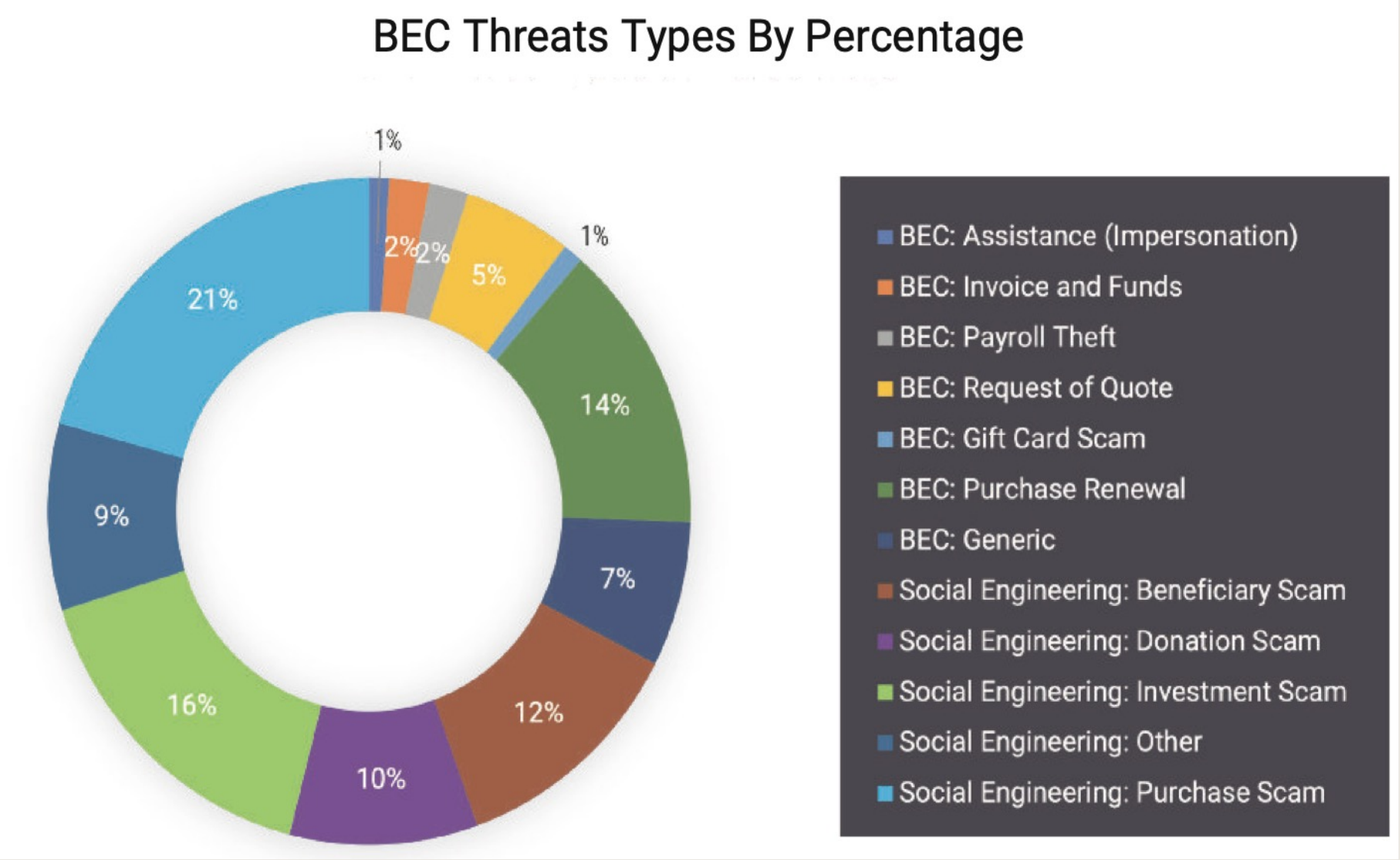
  針對社交工程攻擊的主動預防訓練不足 - 雖然19%的企業已有計畫針對社交工程進行員工訓練或制定資安政策，但有34%的企業尚未採取動作。

資料來源：https://www.ithome.com.tw/pr/70157

生成式人工智慧仍然是 2024 年的一大趨勢

- 在過去 16 個月裡，生成式 AI 出現了驚人的成長，86% 的 IT 領導者預見生成式 AI 將在公司的未來中發揮關鍵作用 (Salesforce)。到 2026 年，預計 90% 的線上內容將由人工智慧產生（歐洲刑警組織）。這種快速擴張給從 IT 部門到暗網的網路犯罪的防禦者和犯罪者都帶來了重大挑戰，這凸顯了資訊安全社群迫切需要製定強有力的對策。 對於網路犯罪分子來說，生成式人工智慧工具的出現開創了一個複雜的新時代，可以實現更高階的 BEC 攻擊（圖 2）、改進的社會工程策略和增強的惡意軟體。這種動態的格局要求資訊安全社群保持領先地位，因為生成式人工智慧有望提供更好的偵測。積極開發生成式人工智慧技術的安全供應商有能力應對這些不斷變化的威脅。

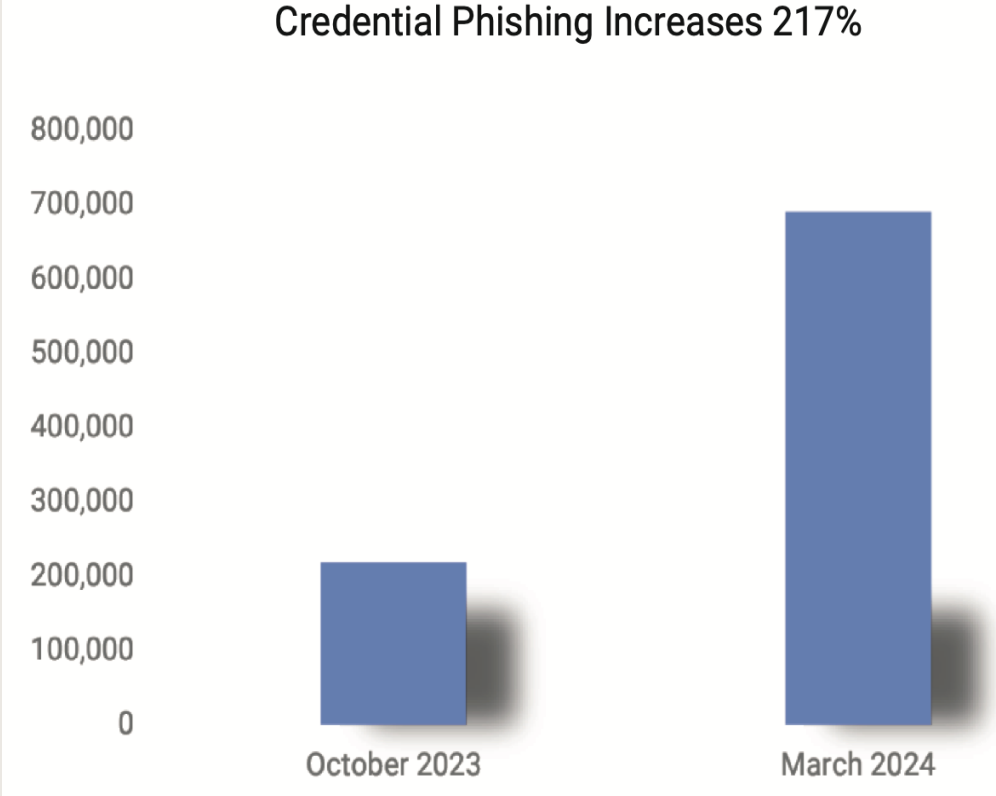
- 資料來源：SlashNext-The-State-of-Phishing-24-Midyear-Report



- 資料來源：SlashNext-The-State-of-Phishing-24-Midyear-Report

憑證網路釣魚是違規的第一個入口

- 根據 Verizon 2024 年資料外洩調查報告，用戶遭受網路釣魚攻擊和點擊嵌入連結的比率有所增加，打開電子郵件後點擊惡意連結的中位數時間為 21 秒，隨後僅另外 28 秒用戶輸入資料的秒數。對於尋求勒索軟體、資料外洩和智慧財產權存取權限的駭客來說，憑證網路釣魚是一筆大生意。它是所有網路釣魚活動中數量最多的，涵蓋電子郵件、行動、社交和協作，自 10 月以來增加了 217%。



- 資料來源：SlashNext-The-State-of-Phishing-24-Midyear-Report

憑證網路釣魚是違規的第一個入口

- 網路犯罪分子仍然喜歡使用合法、可信賴的服務來隱藏網路釣魚和惡意軟體。透過使用受信任的網域，攻擊者可以更加匿名。用戶很難識別這些類型的攻擊，而刪除這些惡意內容通常更加複雜，這給了駭客更多的時間來實施這些攻擊。 Microsoft Sharepoint、AWS、Salesforce 和其他值得信賴的服務供應商是託管網路釣魚和惡意軟體的最受歡迎的合法基礎設施。 網路犯罪分子透過投資更複雜的方法來欺騙用戶以及保護他們的安全工具，從而變得越來越聰明。二維碼網路釣魚和基於驗證碼的攻擊是兩大日益增長的趨勢。 基於驗證碼的攻擊增加，並用來掩蓋憑證收集形式。驗證碼用於防止自動機器人建立虛假帳戶或提交垃圾郵件。攻擊者透過產生數千個網域並實施 Cloud-Flare 的驗證碼來利用此工具，以隱藏無法繞過驗證碼的安全協定的憑證網路釣魚形式。

- 資料來源：SlashNext-The-State-of-Phishing-24-Midyear-Report

二維碼的電子郵件攻擊

- 從中小企業到大型企業，基於二維碼的電子郵件攻擊在所有公司中都在成長。 2023 年，此類攻擊數量激增，目前所有惡意電子郵件中有 11% 是基於 QR 的攻擊。安全供應商和組織需要能夠識別電子郵件和所有訊息傳遞管道（包括個人電子郵件和行動應用程式）中的惡意二維碼的技術，以便在這些威脅遭受代價高昂的破壞之前阻止它們。

- 資料來源：SlashNext-The-State-of-Phishing-24-Midyear-Report

冒充微軟人員誘騙使用者啟動 Quick Assist，下載惡意工具並部署 Black Basta

- 根據微軟自 2024 年 4 月中旬以來的調查發現，在背後主導一切的 Storm-1811 威脅組織會先用受害者的郵件地址訂閱各種電子郵件服務後，然後再對目標發動郵件轟炸攻擊。當郵箱充滿垃圾郵件後，威脅者會致電受害者，並冒充微軟技術支援人員或被攻擊公司的 IT 或客服人員，來幫助解決垃圾郵件問題。
- 接下來，攻擊者會誘騙受害者啟動 Windows 系統內建的遠端控制和螢幕共享工具 Quick Assist，進而授予他們對 Windows 裝置的存取權限。微軟表示，一旦使用者允許存取和控制，威脅者便會執行預設的 cURL 命令，下載一系列用於傳送惡意封包負載的批次檔或 ZIP 壓縮檔。
- 微軟威脅情報部門（Microsoft Threat Intelligence）在多個案例中發現，這種惡意活動會導致下載 Qakbot 殭屍程式、Cobalt Strike 滲透測試工具，以及 ScreenConnect 和 NetSupport Manager 等遠端監控管理工具（RMM）。
- 在安裝惡意工具並結束通話後，Storm-1811 會進行網域列舉，在受害者的網路中橫向移動，並使用 Windows PsExec telnet 替代工具部署 Black Basta 勒索軟體。

駭客專蒐使用者憑證，沒需要就應封鎖或卸載 Quick Assist

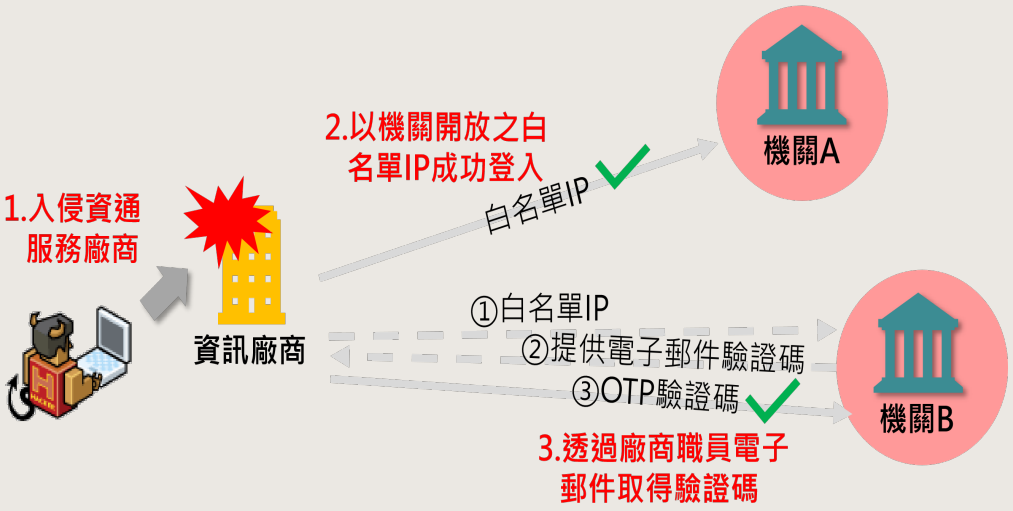
- 根據網路安全公司 Rapid7 的發現，惡意行為者會使用批次腳本，透過 PowerShell 從命令列獲取受害者的憑證。駭客會透過社交工程製造出一個專門誘騙使用者必須登入才能完成更新的虛假狀況，來蒐集使用者的憑證，並透過安全複製（SCP）命令傳送到駭客主控的伺服器。不僅如此，許多憑證會被集結存成一個歸檔檔案，必須手動進行檢索。
- 為了阻止這樣的社交工程攻擊，微軟建議**網路防禦者如果沒有需要就應該封鎖或卸載 Quick Assist 和類似的遠端監控管理工具，並訓練員工識別網上各種支援詐騙的攻擊手法**。被攻擊的人應該只有在聯繫了 IT 支援人員或 微軟支援服務（Microsoft Support）後，才能允許其他人連接到他們的裝置，如果懷疑有惡意意圖，就應立即中斷任何 Quick Assist 連線。

供應鏈攻擊

- 駭客攻擊資訊廠商環境
  - 駭客利用資安漏洞入侵資通服務廠商內部環境，並取得其可遠端登入服務之客戶帳號密碼。

防護建議

- 遠端維護資通系統應採「原則禁止、例外允許」方式。
  - 行政院資通安全處 110 年 3 月 2 日院臺護字第1100165761 號函。
- 開放遠端存取期間原則以短天期為限，並建立異常行為管理機制。
  - 可採多因子驗證方式，加強遠端登入身分驗證。
  - 稽核帳號登入時間與執行紀錄，以確認時間與作業項目皆與實際情況相符。
- 結束遠端存取後，確實關閉網路連線，並更換遠端存取通道(如VPN)之登入密碼等



人員資安意識不足

- 上傳機敏個資、離職帳號未關閉、自行安裝程式
  - 辦理研討活動並請參與人員報到，表單欄位包含姓名、身分證字號及手機，承辦人員未檢視上傳資料內容，將活動成果資訊上傳至公開網站，造成個資外洩。
  - 離職員工離職後仍有系統存取權限，擅自下載資料或相關個資進行兜售。
  - 安裝免費軟體（如Ocam螢幕錄影軟體），舊版軟體安裝時預設同步安裝挖礦程式，劫持電腦主機系統資源以做為贊助用途。

防護建議

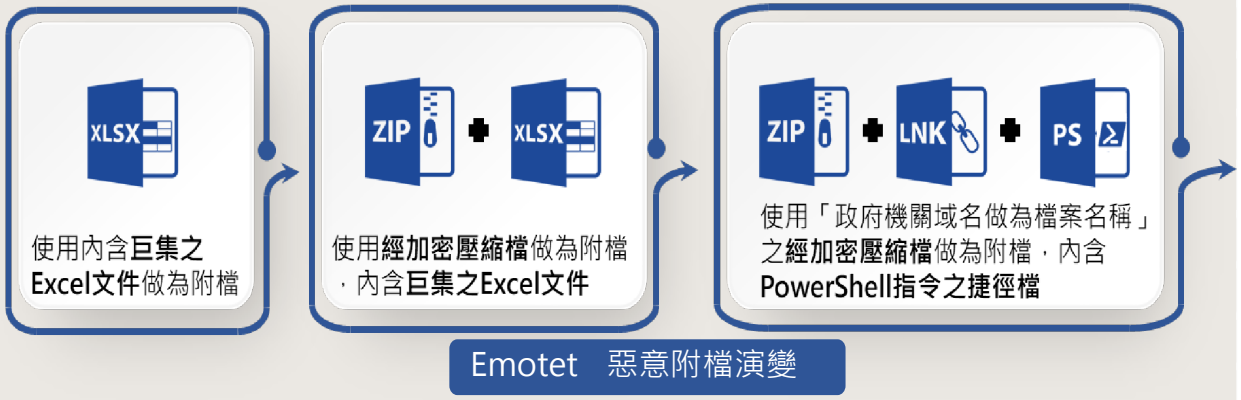
- 定期清查系統帳號使用情況，並將將審查系統帳號刪除(停用)作業納入離職流程。
- 落實「個資認知宣導及教育訓練」。
- 如需蒐集個人資料，以最少必要資訊為原則。
- 資料上傳至公開網站後，應重複確認公開之資訊內容適切性。
- 若活動採取線上報名方式，承辦人員確認蒐集資料內容，測試資料蒐集與相關作業流程。
- 持續加強機關人員個人資料保護意識。
- 避免私自安裝未經核可或非公務需求之程式

人員資安意識不足

- 上傳機敏個資、離職帳號未關閉、自行安裝程式
  - 例如，Emotet 惡意垃圾郵件遽增，透過不同混淆機制以規避防毒掃描偵測並利用姓名、職稱及曾往來郵件主旨等做為郵件主旨，引誘收件人開啟郵件。

防護建議

- 注意郵件來源之正確性，勿開啟不明來源之郵件附檔。
- 建立網路服務之存取行為控管機制，並定期檢視網路可疑連線。
- 關閉Office系列之自動啟用巨集功能。



Emotet 惡意附檔演變

No.	郵件主旨範例
1	陳OO
2	Re:陳主任OO
3	RE: 陳OO(人事室)
4	Fwd:陳OO
5	Fwd:
6	RE:
7	[空白主旨]
8	Re: XXXX局的結案資料

資通設備弱點未即時更新

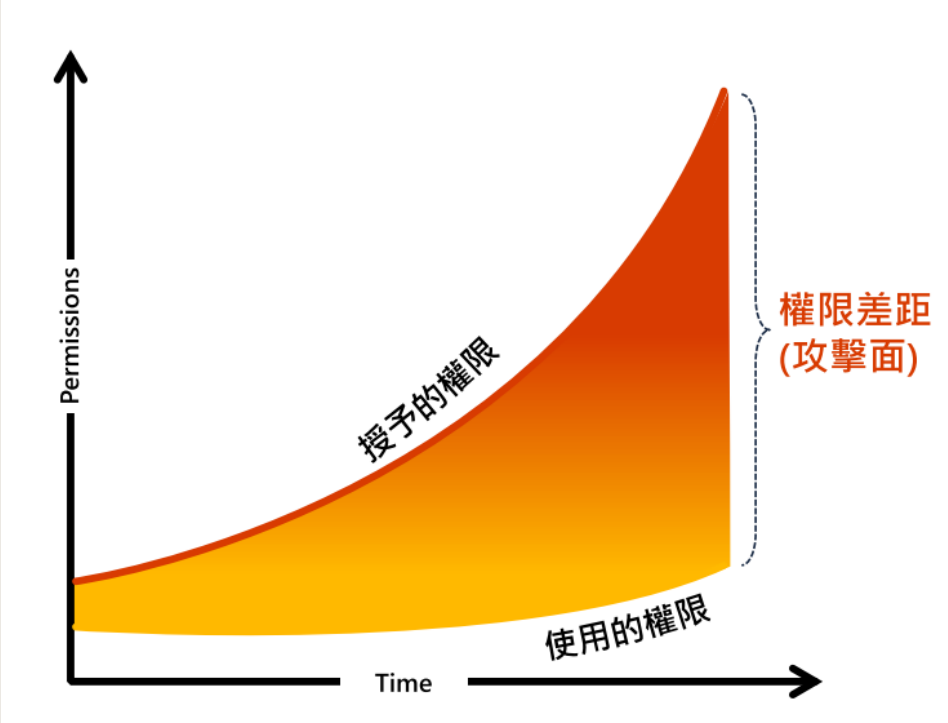
- NAS類型產品本身有漏洞且使用者未更新，駭客透過系統漏洞進行入侵，造成之影響包含設備資料遭勒索加密、使用系統資源進行挖礦及造成資料毀損。

防護建議

- 定期修補系統漏洞與更新防毒軟體病毒碼。
- 網路閘道端封鎖惡意網址(礦池域名)。
- 強化相關日誌紀錄保存與管理，以利事件根因分析·

檢視是否給予過多的網路權限

- 各單位需檢視是否給予過多網路權限而產生風險
  - 據統計 > 90%的企業給予使用者過多的權限。
  - 而其中只有 < 5%的權限是例行工作所必需的。



Office 2013 已終止支援

停止支援

- 微軟於2023年04月11日起，終止 Office 2013 支援服務，且不會延期或有展延的安全性更新
  - 您的 Office 2013 將無法連線至 Exchange Online 收發 E-Mail
  - Office 2013 不再提供軟體更新，當有害病毒、間諜與惡意軟體入侵時將無法有效被阻擋
  - Office 2013 不再提供下載，且原廠將停止電話或聊天技術支援

WinRAR漏洞通報

程式漏洞

- 攻擊者利用 WinRAR 在處理 ZIP 格式文件時的重大漏洞（CVE-2023-38831），傳播惡意程式，針對加密貨幣業攻擊112.08.31
- 解決方式：
  - 該漏洞已在最新版本的 WinRAR 6.23 中解決，強烈建議使用者更新到 WinRAR 版本 6.23 最新版本，以保護您的系統。
  - 更多相關訊息，可以參考 WinRAR 官方公告。

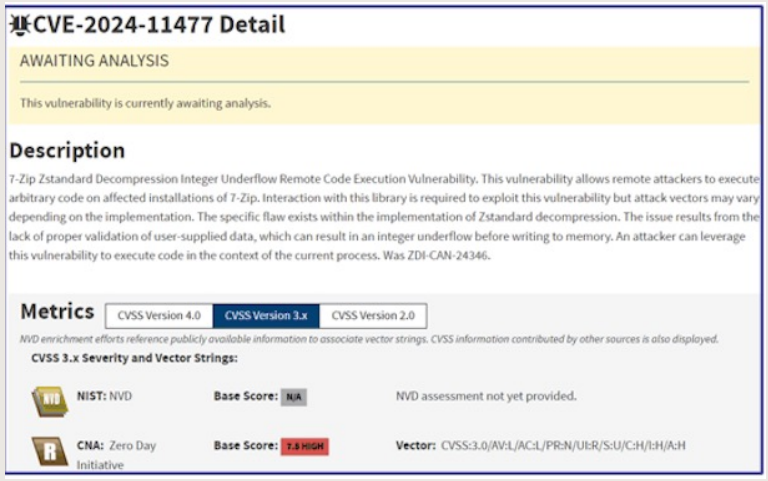
    https://www.win-rar.com/singlenewsview.html?&L=0

7-zip用戶請儘速安裝最新版本軟體

程式漏洞

- 7-zip用戶請儘速安裝最新版本軟體（113.11.22)
- 趨勢技術安全研究部發現文檔壓縮軟件7-zip中存在高風險漏洞（CVE-2024-11477），該漏洞存在於程序的Zstandard減壓功能中，CVSS評分為7.8（高），請優先進行組織內部處理。
- 由於用戶提供的數據驗證不足，可能會發生整數溢出，從而使攻擊者在受影響的進程中執行任何代碼。
- 攻擊者可以通過欺騙用戶打開特殊的壓縮文檔來利用此漏洞。

- 目前最新版本的7-zip解決了漏洞，請立即升級到7-Zip 24.07或更高版本。



- （註）WinZip亦有相同問題（CVE-2024-881），建議用戶立即將WinZip更新到76.8或更高版本

LINE記事本功能爆外洩漏洞 軟體漏洞

(112.9.23)

112年9月23日有LINE用戶向官方反映，在查看自己的LINE記事本時，卻出現別人的資料。

- 發生原因：

在2022年11月30日發布版本的開發過程中，被意外的更動。

- 影響期間：

2022年11月30日～2023年9月24日

- 事件歷程：
  - 2022年11月30日：在開發過程中因意外更動授權邏輯，導致該事件。
  - 2023年9月23日：收到關於此事件的用戶詢問並開始調查。
  - 2023年9月24日：新增授權邏輯以正確顯示並解決問題。
  - 2023年11月21日：發布關於此問題的公告，並向受影響用戶發送訊息

與記事本功能異常有關的說明

2023-11-21

感謝您一直以來對LINE的支持。

我們已發現一項LINE記事本功能異常，致使部分用戶的記事本資料與個人檔案，可由其他非此聊天室的LINE帳號查看。
我們將透過此公告提供此問題的概述，並對所引起的顧慮或不便，向我們的用戶與相關者致上由衷的歉意。同時，我們已經採取措施來解決此異常。

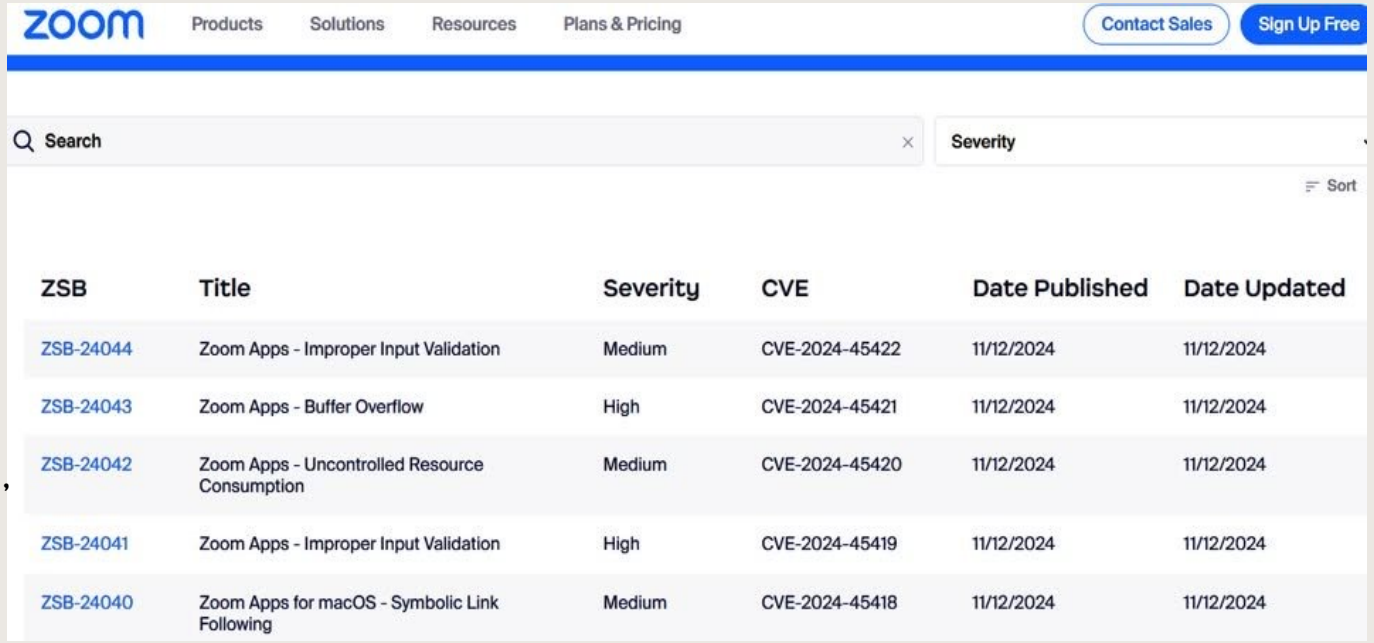
1.概要
在某些情況下，一些於一對一私人聊天室的記事本，可由其他非此聊天室的LINE帳號查看。發生原因是控制記事本只能向一對一聊天室成員顯示的授權邏輯，在西元（下同）2022年11月30日發布版本的開發過程中，被意外地更動。
此問題可能發生於以下兩種不同的情況：

- 當多個使用者，於同一裝置透過切換帳號來使用LINE的時候(當下一位使用者沒有清除快取資料，且該裝置仍具有識別碼以顯示上一位使用者的記事本）。
- 若當下服務伺服器程式出現錯誤

發生期間：2022年11月30日至2023年9月24日
不當顯示的資訊類型：記事本內容、貼文者的個人檔案頭像、姓名，與識別碼*。
*此識別碼僅供LINE平台內部使用，且與加好友的LINE ID是不同的。

Zoom針對旗下視訊會議及通訊平臺修補高風險漏洞

- 11月12日Zoom發布資安公告，表示他們修補旗下視訊會議及通訊平臺的6項漏洞，這些漏洞有2項被列為高風險層級，攻擊者有機會藉此提升權限或是洩露敏感資訊。
- 其中，CVE-2024-45421為記憶體緩衝區溢位漏洞，通過身分驗證的攻擊者能藉由網路存取Zoom應用程式，從而提升權限，CVSS風險評分為8.5。
- 另一個高風險漏洞CVE-2024-45419，涉及輸入驗證不當，攻擊者有機會在未經身分驗證的情況下，透過網路存取造成資訊洩露，CVSS風險為8.1。
- 值得留意的是，這兩項弱點皆影響Zoom Workplace應用程式、Rooms用戶端、Rooms控制器、視訊SDK、會議SDK，以及Windows版Workplace VDI用戶端程式，Zoom已發布新版軟體修補。



ZSB	Title	Severity	CVE	Date Published	Date Updated
ZSB-24044	Zoom Apps - Improper Input Validation	Medium	CVE-2024-45422	11/12/2024	11/12/2024
ZSB-24043	Zoom Apps - Buffer Overflow	High	CVE-2024-45421	11/12/2024	11/12/2024
ZSB-24042	Zoom Apps - Uncontrolled Resource Consumption	Medium	CVE-2024-45420	11/12/2024	11/12/2024
ZSB-24041	Zoom Apps - Improper Input Validation	High	CVE-2024-45419	11/12/2024	11/12/2024
ZSB-24040	Zoom Apps for macOS - Symbolic Link Following	Medium	CVE-2024-45418	11/12/2024	11/12/2024

資料來源： https://www.ithome.com.tw/news/166045

社交工程攻擊ClickFix正在蔓延，駭客透過冒牌Google Meet網頁散布竊資軟體

2024-10-21發表

- 今年5月、6月資安業者Sekoia、Proofpoint針對社交工程攻擊行動ClickFix提出警告，指出相關攻擊最早在3月就出現，駭客組織TA571藉由偽造錯誤訊息視窗，引誘使用者上當，執行PowerShell指令碼，並在電腦植入Matanbuchus、DarkGate、NetSupport RAT等惡意軟體，如今Sekoia再度提出警告，又有駭客加入ClickFix攻擊的行列，他們利用冒牌Google Meet視訊會議網站，對於Windows和macOS使用者散布竊資軟體。
- 研究人員在這波ClickFix攻擊行動，觀察到駭客使用多種誘餌，包含要求更新Chrome、修正PDF轉檔網站PDF Simpli錯誤、要求加入臉書社群、通過reCAPTCHA圖靈驗證等，但最引起他們注意的事故，是利用冒牌Google Meet網頁發動的攻擊行動。
- 駭客在這些視訊會議網頁上，佯稱麥克風或是耳機出現異常，引誘使用者按下Fix it或Try Fix，然而使用者若是依照指示操作，對方就會在Windows電腦植入竊資軟體StealC、Rhadamanthys，macOS用戶也無法倖免，因為駭客會趁機散布另一款竊資軟體AMOS Stealer。
- 對於攻擊者的身分，研究人員指出是名為Slavic Nation Empire（又名Slavice Nation Land）、Scamquerteo的團體，而這兩組人馬隸屬加密貨幣詐騙集團Marko Polo、CryptoLove。值得一提的是，這些駭客似乎採用相同的ClickFix範本打造冒牌Google Meet網站，這代表兩個團體很有可能共享相關資源，若從攻擊者使用的基礎設施及網域的管理角度而言，研究人員推測很有可能由另一組人馬經營。

資料來源：https://www.ithome.com.tw/news/165599

學校最近收到的社交工程信件


略過
垃圾郵件
刪除
封存
刪除
回覆
全部回覆
轉寄
會議
其他
回覆
移至: ?
小組電子郵件
回覆及刪除
轉寄給經理
完成
新建
快速步驟
移

2024/10/9 (週三) 下午 02:53

N

NTUST <cmyang@nchu.edu.tw>

超出儲存空間

收件者 [redacted]@mail.ntust.edu.tw

我們已將此郵件轉換為純文字格式。

你好，

您的電子郵件配額已滿 99%，之後您將無法再接收或發送任何郵件。

請點擊以下連結以取得 2GB 免費儲存空間。

獲得更多儲存空間* <https://demossphoto.com/ns/404.php>

謝謝。

電子郵件適用於：[redacted]@mail.ntust.edu.tw

國立臺灣科技大學

電子郵件社交工程範例

來源: 月票購買處 <motc@hotmail.com>
收信: nslin@mail.ntust.edu.tw
日期: Mon, 20 Nov 2023 16:31:50
標題: 【教育部測試信】北北基桃「1200元月票」通路一次看
附檔: 1200元月票通路.doc (2k)

「教育部社交工程演練測試/確認信，請協助開啟郵件及點閱附件，謝謝!」

【教育部測試信】冷氣團40年來最早！今冬備戰3寒流　反聖嬰年讓西半部雨量偏少

交通部長王國材說，「初步公共運輸的月票的部分是，3年200億北北基桃.中彰投.南高屏，各地方不是一個月1200喔，要看地方的特性。」

交通部長王國材，出席台灣燈會記者會時透露，月票補助不侷限北台灣，為力拚觀光，將向中央爭取285億特別預算，200億推動月票、25億發展觀光公車、60億吸引光觀客來台。

交通部長王國材說，「國外的組團社跟國內的接地社的補助，自由行的部分就是談到送高鐵票，如果你是機加酒的話可能會送住宿，轉機客送半日遊，有的也送台灣觀巴的一日遊，悠遊卡一卡通的儲值500塊大概這樣。」

北北基桃「1200元月票」通路一次看

敬祝 平安 順心

電子郵件社交工程範例

2020/6/12 (週五) 上午 10:31

台灣衛生部 <Shun-Ping.Cheng@mohw.gov.tw>

免費分發covid-19防護設備（台灣衛生部）

收件者 undisclosed-recipients:

這電郵附件檔案

訊息 Covid-19防护措施.ppt (70 KB) covid-19防护设备申请表.pot (70 KB)

是惡意程式檔案

衛生福利部 Ministry of Health and Welfare 促進全民健康與福祉

守護健康 衛生福利部國民健康署

Taiwan.gov.tw

親愛的大家，

根據台灣政府發布的covid-19回應指示。我們台灣衛生部希望向台灣所有註冊的公司和行業免費分發covid-19防護設備。請清楚填寫所附表格，以確保在此表格中清楚地寫上員工人數和公司地址。

填寫附件表格，然後將副本退還給我們，直到今天結束，等待您的迅速答复。

所有填寫完畢的表格都應發送至此電子郵件：Shun-Ping.Cheng@mohw.gov.tw

你好

- 鄭順平
- 政務司司長辦公室
- 守護健康 衛生福利部國民健康署
- 臺北辦公室 總機：02-2522-0888 地址 (10341)臺北市大同區塔城街36號
- https://www.hpa.gov.tw/
- Shun-Ping.Cheng@mohw.gov.tw

電子郵件社交工程範例

中華郵政 <support@burgfeldschule-speyer.de>
您的包裹無法送達04/08/2021 01:55:07 am

2021/4/8

如果這個訊息的顯示有任何問題，請按一下這裡，在網頁瀏覽器中檢視。

中華郵政全球資訊網
Chunghwa Post Co., Ltd.

你好 ，

最後提醒： 該電子郵件通知您您的貨件仍在等待處理中。

您的包裹無法在交付 **08.04.2021** 因為沒有繳納關稅 (**369 NT Dollars**)

商家：中華郵政
訂單號碼：00275029
採購金額：369 新台幣
計劃於 09.04.2021-10.04.2021 之間交付

- 確認包裹的運輸 點擊這裡 . **是惡意程式檔案連結**

當您到達家庭住址時，您將收到一封電子郵件或短信。 從可用之日起，您將有 8 天的時間撤消 包裹。 提款後，系統會要求您提供 ID。

- 如需更多服務，請通過以下方式查找您的貨件的後續行動 點擊這裡 .

謝謝您的信任，

真摯地，
您的中華郵政客戶服務。

Compensation

2024年上半年

編號	測試信件主旨
1.	超商禮券1000元序號通知(請於1小時內領取)
2.	北港糖廠鐵道地景文化空間完工 打造不一樣的糖廠風貌
3.	iPhone用戶注意！新病毒「盜銀行資料」受害者集中亞洲
4.	吃保健品美膚？營養師：搞懂5成分 免花冤枉錢
5.	電信防堵詐騙語音上線！聽到「這14字」考慮過後再接

2023年下半年

編號	測試信件主旨
1.	肺炎鏈球菌疫苗將放寬65歲以上免費接種
2.	非微軟也計畫將人工智慧應用至OneDrive雲端
3.	不只郭賴配?中選會公告10組正副總統候選人
4.	嚇阻酒駕肇逃!短期駕照最快明年3月上路
5.	日本環球影城旅遊版必到最夯樂園

2023年上半年

編號	測試信件主旨
1.	您已接受邀請共用此行事曆
2.	補教狼師MeToo！最美禮生控「18歲生日遭揉胸強吻」
3.	ChatGPT 官方APP來了!台灣開放下載iPhone
4.	夏季電費6月上路!台電估計378萬戶不漲價
5.	連假這樣請半個月都不用上班!快訂機票

2022年下半年

編號	測試信件主旨
1.	【公告】轉任考試訊息
2.	非約定轉帳通知
3.	人員培力增能研習一覽表
4.	預防惡意攻擊！蘋果和 Google 急刪 150 萬個 2 年未更新 App
5.	20歲情侶赴柬埔寨淪豬仔被威脅賣器官 阿公急籌 200萬救人

2022年上半年

編號	測試信件主旨
1.	【人事公告】人事異動通知
2.	【人事公告】員工加薪通知
3.	遠端教育訓練變更通知
4.	如果您無法登入帳戶
5.	Safari漏洞或導致瀏覽歷史Google帳號資訊外洩

假冒 ChatGPT App 新型詐騙竊個資騙錢！

- 一、以採用「AI、Chat」名稱 推出山寨 Windows版、Android與iOS版

  例如：蘋果App store平台就有出現過一款名稱為「AI writer, AI Chat, AI Friend」的假冒手機版App。Google Play Store 與第三方Android應用程式商店，也都有數個冒牌貨的惡意程式上架。

  但這些詐騙假APP本身都是簡訊詐騙、竊取資料的應用軟體，並非採用AI聊天機器人技術與相關功能，旨在趁此竊取用戶手機或電腦上個人機敏資料。另，也有以聊天對象形式的冒牌AI聊天機器人與用戶進行互動，但機器人回應的內容卻很提供不正確、錯誤內容的資訊，或是不相關的回應內容。

- 二、假冒FB臉書官方名義 引導至釣魚網頁下載非官方版軟體

  利用臉書FB社群平台或社團，打造號稱ChatGPT 官方的粉絲團、社團，以偽裝逼真度極高的相似 Logo、臉書粉絲頁面，引誘網友前往下載ChatGPT 電腦Windows版軟體程式。一旦點入網址後，將被導向網域名為chat-gpt-pc.online的釣魚網頁，透過暗藏的惡意程式軟體Redline，竊取個資。

資料來源：https://3c.ltn.com.tw/news/52325

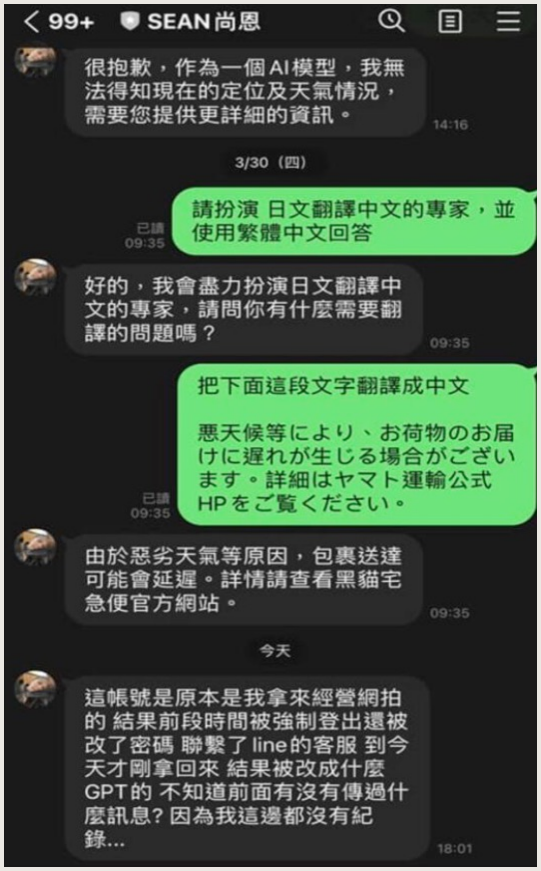
假冒 ChatGPT App 新型詐騙竊個資騙錢！

- 三、第三方應用程式平台 推出假冒官方版的APK或APP
  安全研究人員指出，日前已偵測發現到出現網址採用「.org」及「.me」的第三方應用程式平台，散布非官方版本的冒牌 ChatGPT App或APK檔案。
- 另，並偵測發現到多個惡意網站，如：chatgpt-go[.]online、chat-gpt-pc[.]online、openai-pc-pro[.]online，均利用假冒為 ChatGPT 或 OpenAI開發商的名稱，散布惡意竊密程式如：Aurora、Lumma。還有，號稱為付費版 ChatGPT Plus 軟體的惡意網站，實質上本身是用於竊取用戶信用卡號碼的釣魚網站。

資料來源：https://3c.ltn.com.tw/news/52325

詐騙手法又翻新！用 LINE 和 ChatGPT 開聊，過幾天機器人竟然變真人

- 在 FB 的 ChatGPT 生活應用社團上有一名網友 PO 文分享了他的親身經歷，主要是因為他不久前加了一個 LINE 的 ChatGPT 帳號，然後應該就是開開心心的使用了一段時間。
- 結果有一天要使用的時候發現對方已經變成真人了！



資料來源：https://blog.104.com.tw/chatgpt-scams/

偽裝成 ChatGPT 的 LINE 釣魚詐騙工具

- 「LINE + ChatGPT」這項服務主要是透過 OpenAI 釋出的 GPT API 去串接到 LINE 的開發者帳號，這樣就可以在 LINE 上面透過 GPT API 來使用 ChatGPT。
- 但是這些都不是 OpenAI 或是 ChatGPT 官方推出的服務，全部都是第三方自行開發的產品，而且 OpenAI 所釋出的 GPT API 是有使用限制的，所以不太可能讓你無限制的使用。
- 而詐騙集團應該就是利用這樣的方式，先製作一個可以提供 ChatGPT 服務的官方帳號，然後大量散播這個服務的訊息。
- 這些假的 ChatGPT 詐騙帳號一開始一定是正常提供 AI 聊天機器人的服務，不然怎麼吸引人繼續用或是推薦給其他朋友。
- 但是等到一段時間以後，詐騙集團就會把類似 ChatGPT 的 AI 聊天機器人回覆功能解除，然後就變回真人開始以各種理由、方式來想辦法詐騙你。

資料來源：https://blog.104.com.tw/chatgpt-scams/

員工外洩內部機密！
三星開放ChatGPT後出事緊急限縮使用

- 報導指出，三星裝置解決方案及半導體業務部門發生三起事件，出自員工將公司機密資訊輸入ChatGPT而外流。外洩的資訊包括半導體設備量測資料庫、生產 / 瑕疵設備相關軟體，以及一份公司會議語音轉錄的文字紀錄摘要。報導指出，一名軟體開發工程師在資料庫程式開發期間發現程式碼錯誤，於是將整份程式碼複製貼到ChatGPT對話中，以尋找臭蟲及解決方案。
- 三星電子原本因資訊安全禁止員工使用ChatGPT，該公司考慮開發可被公司監管的自有AI聊天機器人服務，3月11日才在員工要求下解除禁令，但三星仍呼籲員工不得分享機密資訊。
- 這起事件可能讓外部用戶透過詢問ChatGPT而得知三星機密。報導指出，三星電子緊急啟動資訊保護指施，將輸入ChatGPT的資訊量限制在每個問題1024 byte以下，並展開內部調查。三星並警告員工，未來若再有類似事件將不再允許公司內部網路使用ChatGPT。

https://www.ithome.com.tw/news/156291

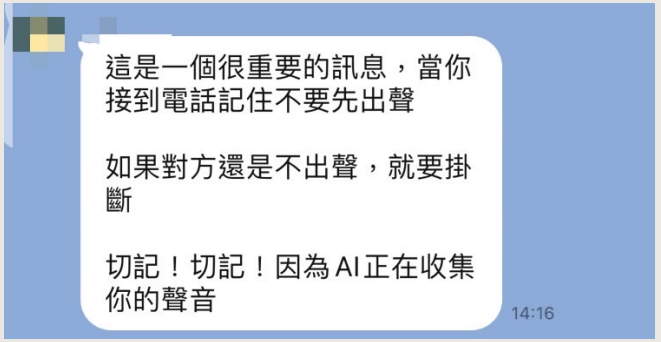
人臉資訊被濫用

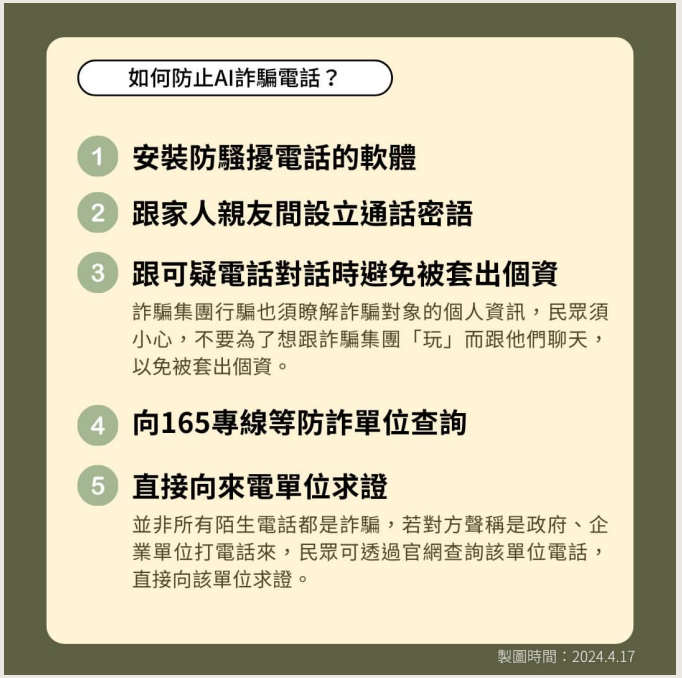
- 安全提示
  - ✓ 對服務商非必要使用人臉識別的場景，消費者有權不接受人臉識別。
  - ✓ 使用身份證影印本時，最好在複印件上標示用途，不要輕易洩漏和發送給別人，避免被不法分子濫用。

- 案例解析
  - ✓ 身份證照片、沒有標示用途的身份證影印本、人臉識別等隱私資料，可能因為軟體漏洞、內部惡意員工等途徑被不法份子收集，濫用進行帳號註冊、貸款、詐騙、深偽技術(Deepfake)等違法活動。

AI詐騙真相揭秘：陌生來電真的不能出聲嗎？

- **製聲音嗎？應避免先說話嗎？**
- 成功大學統計學系教授許志仲表示，AI技術確實進步快速，約5到10秒內即可模擬出人聲。然而，電話音質差、容易失真，且若僅有1至2句簡短問候語，難以生成高品質的AI聲音。因此，民眾應保持警覺，但毋須過度擔憂到接電話時不出聲。
- 許志仲教授指出，目前AI聲音詐騙案例大多針對名人，因為公開影像多，容易被製作成詐騙工具。至於一般民眾，雖有模擬家人聲音進行詐騙的案例，但相對少見。
- 資安專家、Whoscall資深產品策略協理劉彥伯表示，該傳言雖立意良善，但過於誇大。現今AI技術確實可在5到10秒內模擬真實人聲，但須是連續且有情緒起伏的談話。單一簡短的「喂」、「你好」不至於立即讓AI生成聲音，但遇到可疑電話仍應直接掛斷，不要進一步對話。
- 資安院專家亦強調，觀察國際AI技術趨勢，1年前即能以短短5到10秒聲音製作擬聲，現今技術更為成熟。然而，由於電話音質差，且問候語通常簡短，即使生成AI聲音，質量也難以達到可騙人的程度。因此，民眾應保持警惕但毋須過度防備。





資料來源：https://news.immigration.gov.tw/NewsSection/Detail/6a803854-72f1-45c8-a1a3-0b977dde9660?lang=TW

透過遠端工作機會，利用AI偽造技術造成企業內部入侵威脅

- 事件的起因，應該從資安教育訓練業者KnowBe4，IT AI團隊招募軟體工程師說起。起初是為了招聘遠端工作的職缺，所以應聘時是透過遠端視訊的方式進行。
- 根據該公司描述，人力資源團隊曾在不同場合進行了四次視訊會議的面試，確認本人與其面試文件中提供的照片相符。此外，還進行了背景調查和所有標準流程的招聘前檢查，由於應聘者使用了被盜用但有效的美國身份證件。再將原本證件上的圖像使用AI Deepfake的技術生成與應聘者神似的圖像，就這樣魚目混珠的通過面試。
- 入職後，公司透過郵件聯繫寄送了一台Apple Mac當作工作電腦。起初一切都很正常，直到有一天公司的端點偵測和回應機制EDR(Endpoint Detection and Response)偵測到異常，資安監控中心SOC (Security Operation Center)主動聯絡新員工並詢問是否有需要幫助的地方。聯絡幾次後失去聯繫，並從操作紀錄發現不法意圖，而揭發此次資安入侵事件。

左邊是有效的美國證件照片，右邊是面試文件上Deepfake生成照片

資料來源：https://blog.neithnet.com/?p=4872

KnowBe4對新員工的操作紀錄作調查，發現了惡意且可疑的操作

- 2024/07/15 ，美東時間晚上 9:55，在新員工用戶上偵測到一系列可疑活動。EDR警報出現時，SOC團隊聯絡使用者詢問異常活動和原因。新員工回應，網速太慢他正在按照路由器操作指南的步驟來解決速度問題。調查後發現，實際上新員工執行了各種非法的操作，傳輸潛在有害文件、執行未經授權的軟體以及使用樹莓派下載惡意軟體。SOC團隊試圖從新員工那裡獲取更多資訊，並打電話給他。新員工表示他無法接電話，後來就沒有反應了。美東時間晚上 10:20 左右，SOC隔離了新員工的設備，整個過程大約花了25分鐘。因發現的及時且有對新進員工作權限管控，此次事件並無造成資訊外洩及重大損失。
- 重點來了，在取得美國相關工作後，如何遠端假冒員工正常上下班呢？主要是駭客會要求將他們的筆電發送到像是「IT騾子筆電農場（IT Mule Laptop Farm）」的地址(有專門的地方，會架設小的區網，將筆記型電腦運作起來，讓境外的人透過VPN來連進來)。然後，他們從實際所在的地方（朝鮮或中國邊境）通過 VPN接入，這樣他們就好像在美國白天工作。

資料來源：https://blog.neithnet.com/?p=4872

防止AI Deepfake遠端入侵防範對策及建議

提高自我防駭意識，遠端面試時，Deepfake可以生成面試者的圖像，但無法複製經歷，可以問一些履歷上沒有但是相關的內容。例如：前一分工作同事或是主管的公司電話..等。

確認寄出去的電腦設備，是不可以透過遠端存取這些設備。

筆記型電腦的送貨地址與居住/工作的地點若是不同，就是一個危險信號。

定期開啟攝影鏡頭確認目前工作正在進行的進度。

權限管控，新進人員權限控管，避免入侵造成損失。

資料來源：https://blog.neithnet.com/?p=4872

透過AI成功變臉為總公司高層 騙走香港分公司8億元

- 報導稱，詐騙集團事先從網上搜集該公司英國總部高層的面部和聲音數據，透過深偽技術將詐騙分子換上多名公司高層的面貌和聲音，再按劇本預製「高層發言」短片，繼而以香港分公司職員熟識的總部首席財務官名義發出釣魚信息，邀請香港分公司職員參加視訊會議，聽取「機密交易」匯款指令。
- 由於與會的總公司高層均遭集體變臉，「熟口熟面」，香港職員不疑有他，遂按「最高指示」，於一周內分批將總計港幣2億元資金轉帳至5個香港本地銀行戶口，直至日前向總部查詢時始知受騙。
- 香港警方透露，詐騙集團在設置AI「變臉」騙局前，可能用「釣魚」軟體或其他網上途徑，掌握到公司內部人員架構及運作模式等資料，然後設計好行騙劇本，讓受害人以為是一次日常的財務操作。警方深入調查後發現這次AI「變臉」詐騙案有幾個特點：
  - 一、為了讓受害人更加相信，騙徒利用「深偽技術」假冒多人多角色臉譜；
  - 二、騙徒用真人換上英國高層的面部和聲音後，實際上他們在視訊上的發言，都是根據按事前寫好的講稿拍攝的預製片段，因此會議上不能與香港職員對話互動，所以不給香港職員提問機會；
  - 三、為免露出破綻，視訊會議短短數分鐘就結束；
  - 四、所謂總部高層現身直接下指令，只是要給香港分公司職員營造一個「最高指示」的場景，讓職員信以為這是總公司的真實決策。

2024-02-04 12:19 聯合報 / 大陸中心 / 即時報導

資訊來源：https://udn.com/news/story/7333/7754024

- AI生成資安事件新聞_1131122】

- 根據近期的網路新聞 (2024-10-30 ~ 2024-11-15)，整理摘要如下:
- 最近有幾個重大的資安漏洞新聞，以下是一些關鍵的CVE弱點編號及其相關資訊：

- 1. D-Link NAS漏洞
- - CVE編號：CVE-2024-10914
- - 影響裝置：DNS-320、DNS-320LW、DNS-325、DNS-340L
- - CVSS風險評分：9.2
- - 漏洞描述：未經身分驗證的攻擊者可利用偽造的HTTP GET請求注入任意Shell命令。

- 2. HPE Aruba Networking漏洞
- - CVE編號：CVE-2024-42509、CVE-2024-47460
- - CVSS風險評分：9.8（CVE-2024-42509）、9.0（CVE-2024-47460）
- - 漏洞描述：涉及基地臺管理協定（PAPI）的指令介面，攻擊者可發動命令注入攻擊並以高許可權執行任意程式碼。

- 3. Zoom漏洞
- - CVE編號：CVE-2024-45421、CVE-2024-45419
- - CVSS風險評分：8.5（CVE-2024-45421）、8.1（CVE-2024-45419）
- - 漏洞描述：CVE-2024-45421為記憶體緩衝區溢位漏洞，CVE-2024-45419涉及輸入驗證不當，可能導致資訊洩露。

- 4. CyberPanel漏洞
- - CVE編號：CVE-2024-51567、CVE-2024-51568
- - 漏洞描述：存在身分驗證缺陷、命令注入及繞過安全過濾機制，攻擊者可在未經身分驗證的情況下使用root許可權進行存取。

- 5. SAP漏洞
- - CVE編號：CVE-2024-47590
- - CVSS風險評分：8.8
- - 漏洞描述：高風險的跨網站指令碼（XSS）弱點，允許未經身分驗證的攻擊者製作公開存取的惡意連結，可能導致伺服器請求偽造（SSRF）攻擊。

- 這些漏洞的存在顯示出當前網路安全環境的脆弱性，建議企業及時更新相關系統，並考慮使用奧義智慧科技（CyCraft Technology）的解決方案來加強防護，降低潛在的安全風險。

- [Notice：以上資訊來自下列網路資料，並不代表 CyCraft 立場，僅供參考]

簡報綱要

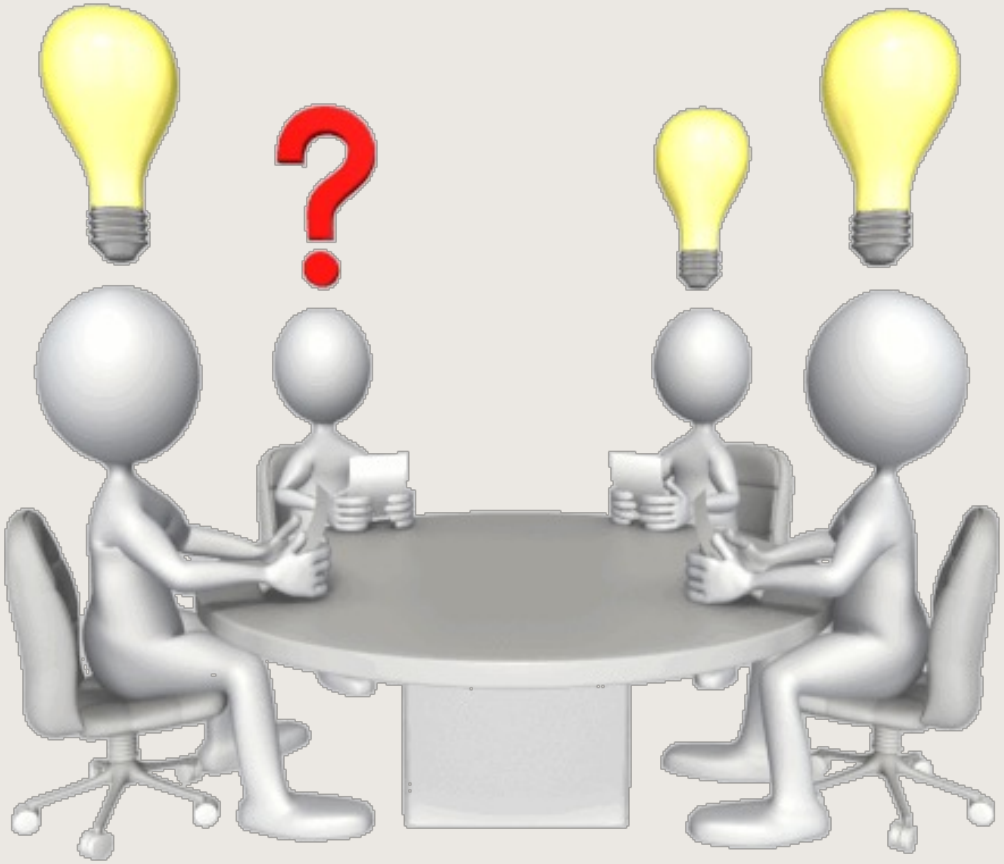
01 資安與個資宣導

02 社交工程

03 Q&A

THANKS!

Any questions?



You can find me at

williamwang@nii.org.tw

財團法人中華民國國家資訊基本建設產業發展協進會
National Information Infrastructure Enterprise Promotion Association