人人必修資安防詐課

不當受害者，也不當破口

資安趨勢 · 詐騙手法 · 真實案例 · 實用防護

課程時長 **180 分鐘**

適合對象 **無資安背景的一般同仁**

開場

今天結束後,你會帶走什麼?

這堂課不談艱深技術,只談跟你切身相關的事

看得懂

認得出常見的詐騙與攻擊長什麼樣子,不再「不小心就點下去」。

記得住

用真實畫面、生活比喻與口訣,把判斷方法變成直覺反應。

做得到

帶走一份檢查清單與三步驟,今天就能用在工作與生活裡。

開場

今天的流程

三小時,依「四大威脅」循序展開,中間休息一次

0	開場與破冰	12 分
1	詐騙現況與趨勢	22 分
2	詐騙陷阱:攻擊的不是電腦,而是人性	42 分
—	中場休息	10 分
3	惡意程式:看不見的入侵者	18 分
4	個資外洩:你的帳號密碼值多少錢	22 分
5	危險 Wi-Fi:上網便利的代價	10 分
6	實務案例分享	20 分
7	個人與工作防護實務	16 分
8	總結、測驗與 Q&A	8 分

開場

為什麼資安跟「你」有關?

這些事,就發生在你我身邊

一封普發現金簡訊

2025 年政府普發一萬元期間,財政部就查到並關閉 11 個假冒的「普發現金」釣魚網站,專騙民眾的個資與帳號。

學校系統被駭

美國校園系統 PowerSchool 遭駭,外洩超過 6,200 萬名學生與 950 萬名教師的個資——老師也是受害者。

一年被騙走近 900 億

據警政署 165 打詐儀錶板,2025 年全台詐騙財損達 893 億元,受理案件 16.2 萬件。

互動時間

過去一年,你或身邊的人
有沒有遇過這些事?

- 收到假冒銀行/政府的簡訊或郵件
- 帳號被盜、被陌生登入
- 差點或真的被詐騙、被騙錢
- 完全沒遇過(真的嗎?)

開場

駭客的最愛:你的帳密 = $$

他們要的不是「你的電腦」,而是能換成錢的東西

誘騙個資

用假登入頁面、假客服,騙你自己輸入帳號密碼與個人資料。

竊取帳密

拿到帳密後,再去登入你的信箱、社群、網銀「試門」。

勒索金錢

鎖住你的檔案、或冒用你的身分向親友詐財,最終目的都是錢。

開場

如何引君入甕?先抓住「人性的弱點」

詐騙不是技術問題,是心理問題

貪便宜 · 搶免費 · 瘋購物

「免費送 iPhone」	免費、抽獎、限量——先讓你心動,再讓你手滑。
「買一送一快搶」	限時折扣讓你來不及查證,直接輸入信用卡。
「你的帳號異常」	用恐懼取代思考,讓你急著點連結「處理」。

駭客與詐團的「攻擊全景」

同一個目標,從五個方向包圍你

重點 假登入頁面、假簡訊、假郵件、假 Wi-Fi、假廣告——入口不同,目的都是你的錢與個資。

開場 · 課程主軸

網路安全 4 大威脅

今天的內容,就沿著這四條線展開

1

詐騙陷阱

攻擊的不是電腦,
而是人性

2

惡意程式

看不見的
入侵者

3

個資外洩

你的帳號密碼
值多少錢

4

危險 Wi-Fi

上網便利的
代價

開場

最重要的一個觀念

再貴的防毒軟體,也擋不住「人」按下確認

你,就是第一道防線

大多數攻擊,不是靠高深技術破解系統,而是靠「騙過一個人」。

駭客最愛的入口,就是忙碌、信任、想幫忙的你。

82.6%

的釣魚信件,如今都用 AI 生成內容

資料來源:Keepnet / VIPRE 2025

一 · 22 分鐘

1

詐騙現況與趨勢

先看清楚——現在的威脅,跟你印象中的不一樣了

一 · 趨勢

2025 的數字會說話

威脅不是變多一點點,而是整個量級的跳升

893 億

2025 全台詐騙財損
(165 打詐儀錶板)

16.2 萬

全年詐騙受理件數
平均每天逾 440 件

+45%

全球勒索軟體攻擊
較 2024 年增加
(NordStellar)

82.6%

釣魚信使用 AI 生成
(Keepnet / VIPRE)

一 · 趨勢

台灣的詐騙財損有多大?

換算成「每天」,你會更有感

1,300 億

2024 年台灣詐騙財損總額

單日約 **3 億元**

假投資仍是財損之王

單月財損曾高達 44 億元,受害人常是被「保證獲利」話術與假對帳單誘導。

長輩金額最高、年輕人頻率最高

長輩因有退休金與積蓄,單筆損失最大;年輕人則最常在網購與假投資踩坑。

查緝有成,但手法轉移

2025 年假投資財損明顯下降,但詐團立刻轉向網購詐騙,件數大幅上升。

2025/9 月詐騙總財損 67 億

怎麼看 受理件數最多的前五名手法——記下來,遇到時就會亮紅燈。

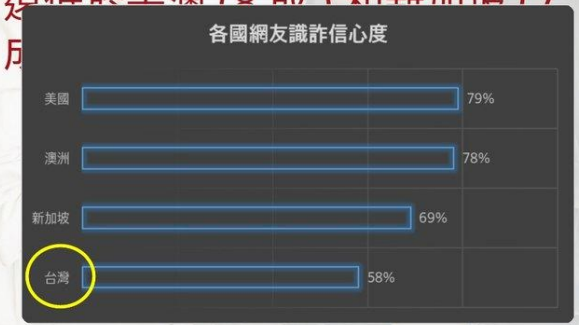
台灣民眾「識詐信心度」低 ，更憂慮家人受騙

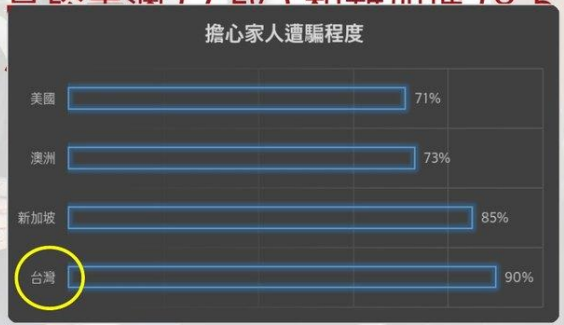
僅 5.8 成有信心識詐

遠低於美澳（8 成）和新加坡（7 成）

高達 9 成擔心家人遭騙

高於美澳（7 成）和新加坡（8.5 成）





落差在哪 台灣人「擔心家人被騙」的比例很高,但「有信心識詐」的比例卻偏低。

「這是詐騙嗎?」其實我們常猜錯

真的會被當成假的,假的反而被當成真的

調查結果 正確識詐不到 5 成、誤認詐騙超過 5 成;18–24 歲有近 5 成辨識錯誤。

一 · 趨勢 ①

AI 成了駭客的得力助手

白話說:寫詐騙訊息,從前要熬夜,現在幾分鐘搞定

文筆變完美

過去靠錯字、怪怪的中文就能認出詐騙;現在 AI 寫的信件文法通順、語氣專業。

高度客製化

AI 會參考你的職稱、近期訂單、同事名字,讓每封信都像專門寫給你的。

大量又便宜

一次能對上千人發送量身打造的釣魚信,成本卻大幅下降。

16 小時 → 5 分鐘

用 AI 製作一場逼真釣魚攻擊所需的時間,從約 16 小時縮短到只要約 5 分鐘。

來源:產業研究彙整 2025

一 · 趨勢 ②

深偽(Deepfake):眼見不再為憑

AI 能合成幾可亂真的假聲音、假影像——連視訊都能造假

它能做什麼?

- 假冒主管的「聲音」打電話要你匯款
- 用合成影像開一場「假視訊會議」
- 盜用名人、名醫影像假冒代言
- 只需網路上幾秒鐘的影片或語音素材

怎麼自保?

✓ 涉及金錢或機密,務必用「另一個管道」再確認(例如當面、回撥已知號碼)。

✓ 視訊中可請對方轉頭、揮手、拿筆遮臉——破綻常會出現。

✓ 越緊急、越要你保密的要求,越要懷疑。

真實案例 連「醫院院長推薦減肥藥」都能偽造——名人、名醫的臉都可能被借用。

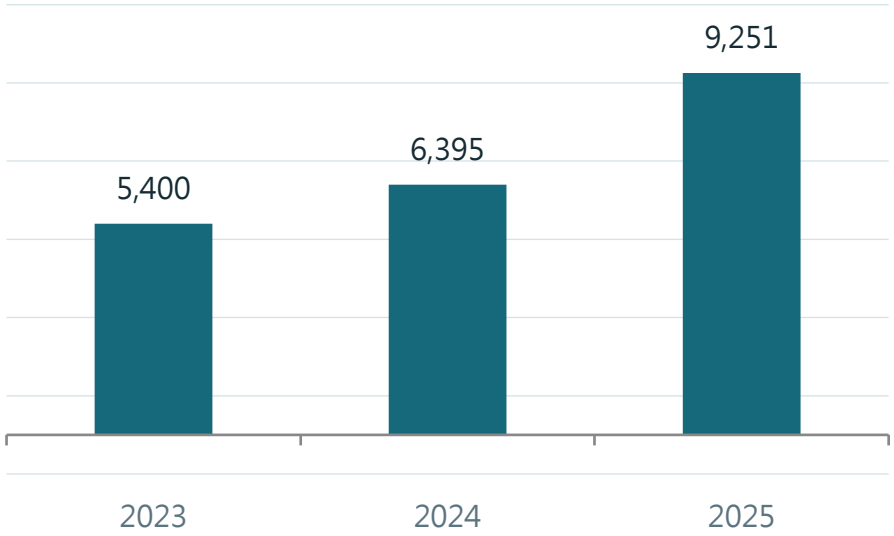
假的影像,還是有破綻可查

科技可以偵測,但你的警覺仍是第一關

怎麼防 可從臉部邊緣異常、過度平滑等特徵判斷;但最實際的做法仍是「換管道確認本人」。

勒索軟體:把你的檔案「綁架」

鎖住你的檔案勒索贖金,還威脅把資料公開



全球勒索攻擊件數逐年攀升(來源:NordStellar 2025)

雙重勒索

先偷走資料、再鎖住系統。就算你有備份,也用『公開外洩』逼你付錢。

贖金驚人

2025 年平均贖金約 100 萬美元;對組織的真正損失,遠不只贖金本身。

怎麼進來

最常見的入口仍是『一封釣魚信』——有人點開了夾帶的檔案或連結。

供應鏈攻擊:打你「信任的人」

駭客不直接攻擊你,而是先攻陷你信賴的廠商或軟體

對你的提醒: 看似「官方」「合作廠商」寄來的更新或通知,也可能藏有風險——保持同樣的警覺。

一 · 趨勢 ⑤

釣魚進化史:從「一眼識破」到「幾可亂真」

舊的辨識方法正在失效

以前的釣魚信

- 錯字連篇、中文怪怪的
- 排版粗糙、亂碼
- 一看就知道是假的
- 亂槍打鳥、不針對你

現在的釣魚信

- ✓ 文筆專業、毫無破綻
- ✓ 仿冒真實品牌、官網
- ✓ 提到你的名字、職務、近況
- ✓ 鎖定你個人,精準投送

其他正在升溫的風險

新的工作與生活型態,帶來新的破口

行動裝置成主戰場

詐騙越來越多透過手機簡訊、LINE、社群私訊進來,而非只在電腦的信箱。

遠距 / 在家工作

家用網路、個人裝置安全性較低,公私混用讓資料外洩風險升高。

個資外洩常態化

你的 email、電話、生日早已散落各處,讓詐騙能「叫得出你的資料」取信於你。

假 QR Code / 假網站

停車繳費、菜單、政府補助……假冒的 QR 與網站越來越多。

一 · 重點

本段重點帶走

台灣是重災區

一年財損近 900 億、單日約 3 億,而我們的識詐信心卻偏低。

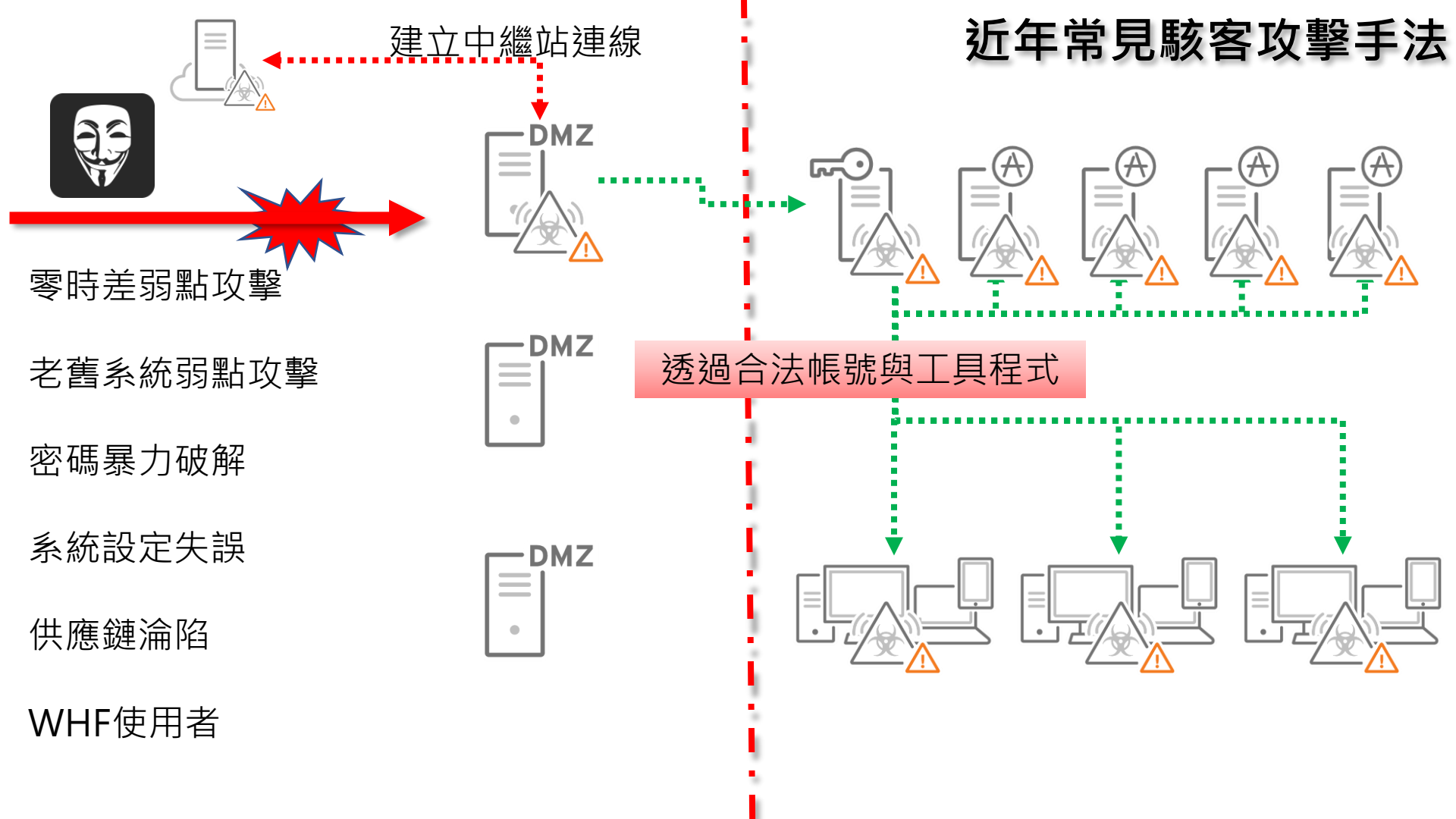
攻擊正在「工業化」

AI 讓詐騙更快、更便宜、更逼真,數量只會更多。

眼見耳聽都可能是假的

聲音、影像都能合成,涉及錢或機密一律用第二管道驗證。

近年常見駭客攻擊手法



零時差弱點攻擊

老舊系統弱點攻擊

密碼暴力破解

系統設定失誤

供應鏈淪陷

WHF使用者

2

詐騙陷阱

威脅一:攻擊的不是電腦,而是人性——這段全部看真實畫面

二

駭客其實在「演戲」

幾乎所有詐騙,都在利用同一批人性弱點

急迫

「限你 2 小時內處理,否則帳號凍結」——讓你來不及思考。

權威

假冒主管、警察、銀行、政府,讓你不敢質疑、乖乖照做。

好奇

「這是你的照片嗎?」「包裹異常」——勾起你想點開看看。

貪 / 怕

保證獲利、中獎、退稅;或恐嚇罰款、外洩——抓住你的貪念與恐懼。

二．手法 ①

社交工程

是什麼	不攻擊電腦,而是「攻擊人」——用話術騙你自己交出資訊或權限。
怎麼運作	假冒可信對象(同事、客服、長官),利用急迫、權威等心理,引導你照做。
真實長相	「我是 IT,系統升級需要你的密碼」「我是新來的廠商窗口,改一下匯款帳號」。

怎麼辨識 凡是有人要你『提供密碼 / 改帳號 / 破例處理 / 別跟別人說』,先停下來查證。

二 · 手法 ②

Email 釣魚

寄件者: service@paypa1-secure.com

主旨:【緊急】您的帳號將於 2 小時後停用!

親愛的用戶 您好,
我們偵測到您的帳號有異常登入,請立即點擊以下連結驗證身分,否則帳號將被永久凍結。

立即驗證帳號 →

⚠ 這是一封典型的釣魚信

4 個紅旗訊號

- 寄件網域怪怪的(paypa1 不是 paypal)
- 製造急迫:「2 小時內、立即」
- 稱呼籠統:「親愛的用戶」
- 要你點連結、登入或填資料

惡意及詐騙網址,無處不在

免費送 iPhone、免費遊戲、免費貼圖、買一送一.....

辨識重點 「免費」與「超低價」是最常見的餌;正常商家不會用這種方式要你點來點去。

詐騙一定會搭「全民時事」

普發一萬元,成了近期最熱門的詐騙關鍵字

規律 只要是全民都在談的事(普發現金、退稅、防疫補助),隔天就會出現對應的詐騙。

猜一猜

普發一萬元的網址,
哪一個才是真的?

1 1OOOO.gov.tw

2 10000.gov.tw

3 10000.gy.tw

4 10000-gov.tw

提示:政府機關的網址結尾一定是「.gov.tw」,而 gov 前面一定是「.」

答案:只有「10000.gov.tw」是真的

其他都是把網址動一兩個字元的假網站

帶走的方法 認網址要從「結尾」看起:必須是 .gov.tw;gov 前面是「.」,不會冠其他英文或數字。

二 · 手法升級

詐騙會「組合技」:普發現金 + 假檢警

一個劇本走完四步,受害者一路被牽著走

1

假冒郵局來電

詐騙者假冒郵局人員,謊稱有人拿你的證件領普發現金 1 萬元。

2

轉接「假警察」

電話被「轉接」給假冒的警察、檢察官,營造官方處理的假象。

3

加 LINE 一對一「控管」

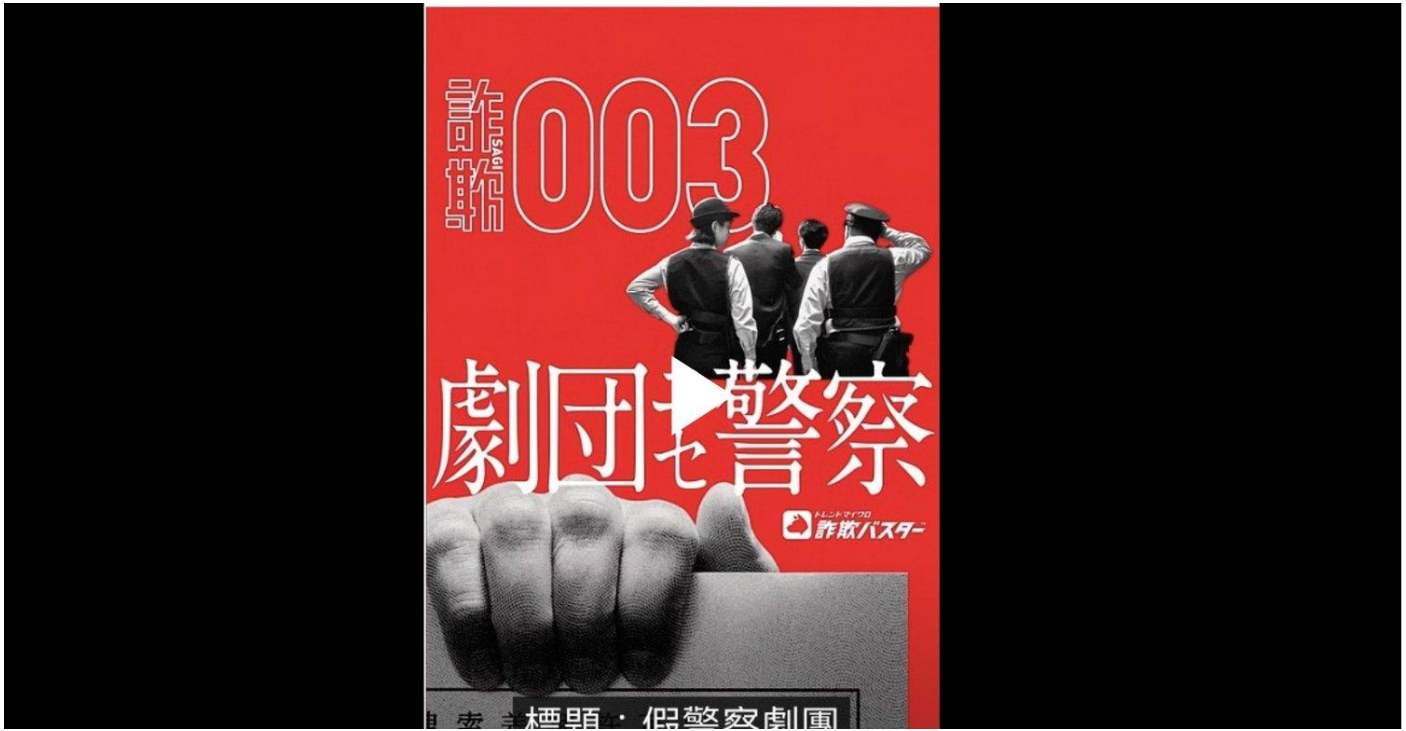
要求加 LINE 私訊聯絡,指示你不要跟家人朋友說,避免被勸阻。

4

要求交付款項

以「監管帳戶」「清查金流」為由,要你交付現金或轉帳。

鐵則 檢警不會用電話要你交付金錢、監管帳戶,更不會叫你「不要告訴家人」。



看清本質 詐團連「劇本」與「角色」都準備好了——你接到的每通電話都可能是排練過的。

FB 網購詐騙:從假廣告到盜刷

惡意賣家大量投放廣告,誘騙你下單並輸入刷卡資料

常見結局 冒用名人代言、透過合法廣告管道擴大散播;結果是貨不對版、不送貨,甚至信用卡被盜刷。

LINE 網購詐騙:順便偷走你的帳號

騙完錢還騙你的 LINE 帳號,再拿去騙你的親友

為什麼危險 詐騙會引誘你把假連結轉傳給親友——你的「信任」成了他們的擴散工具。

假宅配簡訊:最常見的手機釣魚

還會依照你的手機系統,換不同的騙法

手法差異 Android 誘你下載惡意程式;iOS 則做一個假的 Apple ID 登入頁,連雲端帳號一起偷。

真假「宅配」你分得出來嗎?

兩個畫面幾乎一樣,差別只在網址

答案與理由 先看網址、再看內容。宅配業者不會用奇怪網域要你「重新輸入信用卡」。

假網銀簡訊:三個辨認訣竅

詐騙集團偽冒銀行寄「登入通知」騙你的帳密

當場可測 ① 網址怪 ② 帳密隨便打都能「登入」 ③ 其他按鈕都按不動——這三點一出現就是假的。

真假「網銀」哪個是真的?

cathay-bk 還是 cathaybk?

答案 多一個減號、少一個字母,就是完全不同的網站——這是最常見的仿冒手法。

連「搜尋結果」也可能是假的

詐騙集團會購買搜尋廣告,把山寨網站排到最前面

重要觀念 搜尋結果的第一筆不一定是官方;認證方式是看網域,而不是看排名。

二．手法 ③

簡訊釣魚 與 假 QR Code

是什麼	把釣魚連結藏在手機簡訊、LINE 訊息,或印成 QR Code 讓你掃描。
怎麼運作	冒充物流、銀行、政府(如「普發現金」「包裹補運費」),連結到假網站騙個資。
真實長相	「您的包裹地址有誤,請點此更新」「普發一萬請點此登記領取」。

怎麼辨識 政府網址結尾一定是「.gov.tw」;不明連結別點、陌生 QR 別掃,直接用官方 App 或打官方電話查。

二 · 手法 ④

電話詐騙 與 AI 語音

是什麼	用電話施壓,假冒檢警、客服、親友;進階版會用 AI 合成熟人的聲音。
怎麼運作	製造恐慌(「你涉及洗錢」)或急難(「我出車禍急需錢」),逼你立刻轉帳。
真實長相	「這裡是地檢署,你的帳戶涉案,需配合監管」「媽,我手機壞了,先借我錢」。

怎麼辨識 檢警不會用電話要你交付金錢或監管帳戶;聽到熟人急著要錢,務必掛掉、回撥本人確認。

紅旗字眼 「飆股」「保證獲利」「老師帶你賺」——這些字眼出現,就是詐騙。

二 · 手法 ⑤

投資詐騙的固定劇本:養、套、殺

從看到廣告到血本無歸,通常走完這四步

① 看到假廣告

FB、YouTube 出現假投資廣告,常冒用名人或財經名嘴。

② 加入假群組

被邀進 LINE 投資群組,群裡「大家」都在曬獲利對帳單。

③ 下載假 App

誘導安裝假投資 App,先讓你小額獲利、順利出金嚐甜頭。

④ 加碼後出不了金

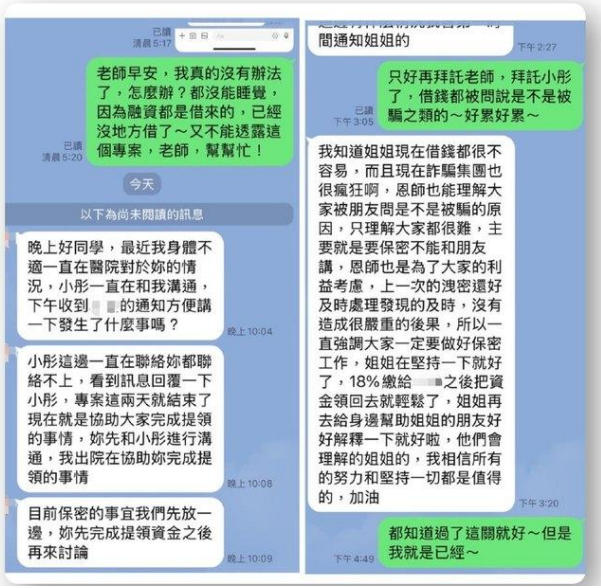
誘你加碼甚至貸款投入,最後網站關閉、群組解散。

關鍵 「一開始真的賺到錢」正是最危險的地方——那是餌,不是獲利。

詐騙意圖分析 – 假投資廣告

科技幫忙 現在也有工具能協助分析訊息意圖,標示可疑之處——但最後判斷仍在你手上。

詐騙意圖分析－投資詐騙 Line



使用時機 可疑的投資群組訊息,也能先讓工具幫你看一眼再決定要不要回。

二 · 手法 ⑥

BEC 商業郵件詐騙

是什麼	假冒老闆、財務或合作廠商,用 email 指示你匯款或變更付款帳號。
怎麼運作	駭客先潛伏觀察往來信件,再在關鍵時刻插入一封以假亂真的指示信。
真實長相	「這是我私人處理的急件,先匯到這個新帳號,別跟其他人說」。

怎麼辨識 任何『改匯款帳號 / 急匯款 / 要你保密』的要求,務必當面或電話向本人二次確認。

二．手法 ⑦

內部疏忽與不小心的外洩

是什麼	不一定是壞人——更多是『不小心』造成的資料外洩。
怎麼運作	誤把檔案寄錯人、群組貼錯訊息、隨手拍含個資的螢幕、隨意插不明 USB。
真實長相	把全班學生個資的 Excel,不小心副本(cc)給了錯誤的收件人。

怎麼辨識 寄送含個資檔案前再三確認收件人;不撿用來路不明 USB;敏感畫面別隨手外拍。

二 · 總整理

一眼看穿可疑訊息:紅旗清單

符合越多項,越可能是詐騙——請拍照存下這頁

製造急迫

限時、立即、否則停用/罰款

假冒權威

自稱銀行、檢警、政府、長官

可疑連結

網域怪、要你點連結登入

索取機密

要密碼、驗證碼、個資、帳號

牽涉金錢

要你匯款、改帳號、買點數卡

要求保密

「別跟別人說」「私下處理」

二 · 重點

本段重點帶走

看「動作」不看「外表」

畫面可以做得一模一樣,重點是它要你做什麼。

網址從「結尾」看起

政府是 .gov.tw;搜尋排名與廣告位置都不代表可信。

要你保密就是詐騙

任何隔離你、不讓你找家人商量的要求,一律拒絕。

中場休息

休息 10 分鐘,稍後回來看「惡意程式」

三 .

3

惡意程式

威脅二:看不見的入侵者——包括你手機裡的

惡意軟體 與 勒索軟體

是什麼	讓你不知不覺安裝有害程式,藉以竊取資料、監控、或鎖住你的檔案勒索。
怎麼運作	夾帶在 email 附件、假更新彈窗、盜版軟體、來路不明的安裝檔中。
真實長相	「您的 Flash 需更新,請點此安裝」「附件是發票.exe,請查收」。

怎麼辨識 不開不明附件、不裝盜版、更新只從官方來源;副檔名是 .exe/.scr 的「文件」要特別警覺。

三 · 真實畫面

假新聞也是餌:「別打開那支影片」

災難、疫情、名人八卦——都是散播惡意程式的好時機

提醒 重大事件發生時,「聳動影片/檔案」特別容易被轉傳;先查證再轉,別當轉傳的一環。

勒索病毒專挑「你最在意的檔案」

而且會連你的備份一起加密

勒索病毒一旦執行，就會搜尋在所有本機與雲端網路上的儲存裝置，尋找可加密的檔案。它會攻擊它認為對您企業或個人重要的檔案，也包括可讓您復原資料的備份檔案。

以下是幾種勒索病毒經常鎖定的檔案類型：

- Microsoft Office ： .xlsx 、 .docx 、 .pptx 以及舊版的檔案
- 影像： .jpeg 、 .png 、 .jpeg 、 .gif
- 業務相關影像： .dwg
- 資料： .sql 與 .ai
- 影片： .avi 、 .m4a 、 .mp4

所以要離線備份 Office 文件、照片、影片、設計圖、資料庫都是目標;連線中的備份也可能一起被鎖。

三 · 口訣

防勒索病毒:牢記「三不三要」

六個動作,能擋掉大部分的感染機會

不 不點選來路不明連結

不 不開啟不明郵件附件

不 不安裝盜版/破解軟體

要 要定期更新修補漏洞

要 要定期離線備份資料

要 要開啟防護並保持更新

四個徵兆 手機當然會中毒:變慢、發燙、視窗亂跳、很快沒電,都是常見徵兆。

手機被盯上的其他跡象

不只變慢——有時是「錢」先出事

帳單無故暴增

惡意 App 可能攔截簡訊驗證碼,偷偷幫你訂閱付費服務或啟用代扣繳。

偷偷「挖礦」耗電

假的雲端挖礦或美肌 App,不但賺不到錢,還會偷扣款、耗盡電量。

出現沒裝過的 App

來源不明的側載安裝,可能夾帶你沒同意過的程式。

帳號被異地登入

收到陌生的登入通知,代表帳密可能已經外流。

三 · 處理步驟

手機出現徵兆,該怎麼辦?

照這五步做,先止血再處理

1

刪除可疑 App

把近期安裝的可疑應用程式移除。

2

掃描病毒

用信譽良好的防護軟體做全機掃描。

3

變更密碼

修改網銀、社群等重要帳號密碼並開啟多因素驗證。

4

通知電信業者

帳單有不明費用,立即聯絡電信業者處理。

5

必要時重設手機

情況嚴重時,考慮恢復原廠設定(記得先備份)。

別忘了 只要涉及金錢或個資,同時通知單位資安窗口與撥打 165。

三 · 重點

本段重點帶走

三不三要要背起來

不點不明連結、不開不明附件、不裝盜版;要更新、要離線備份、要開防護。

手機一樣會中毒

變慢、發燙、亂跳視窗、電量異常、帳單暴增,都要立刻檢查。

備份一定要留離線的一份

勒索病毒會連線上備份一起加密,拔掉的那份才救得了你。

四 ·

4 個資外洩

威脅三:你的帳號密碼值多少錢?答案可能比你想的低

四 · 個資外洩

帳號與密碼攻擊

是什麼	盜取或猜出你的密碼,進而登入你的信箱、社群、銀行帳號。
怎麼運作	利用『弱密碼』、以及你『多個網站用同一組密碼』——一個外洩,全部淪陷。
真實長相	某購物網站資料外洩後,駭客拿同一組帳密去登入你的 email、網銀「撞」門。

怎麼辨識 每個重要網站用不同的強密碼,搭配密碼管理器;最重要的是開啟「多因素驗證」。

四 · 現實檢驗

愛用「懶人密碼」?駭客也最愛你

台灣人最常用、也最容易被破解的密碼

1. admin
2. 123456
3. a12345
4. 12345678
5. 1qaz2wsx

萬用密碼 = 萬靈丹

對你來說方便,對駭客來說也方便——一組密碼就能開你所有的門。

四 · 有感練習

你的帳號密碼,值多少錢?

對你的價值,和對駭客的售價,是兩件事

網路銀行帳號

$180 萬

依存款而定

信用卡帳號

$15 萬

依額度而定

百萬粉專帳號

無價

多年心血與粉絲數

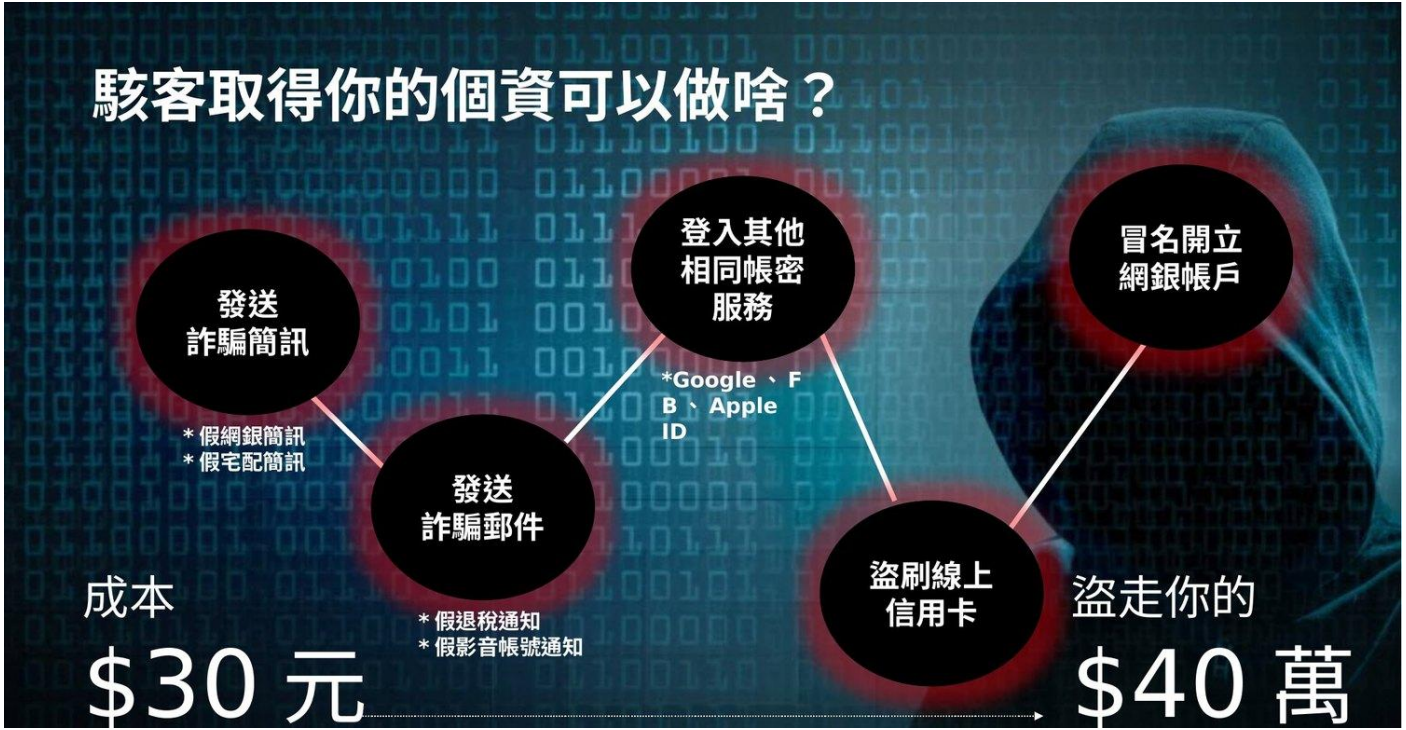
但在暗網裡,它可能只賣 1~2 美元

你辛苦累積的一切,在黑市被當成廉價商品成批販賣——這就是要保護帳密的理由。

現實是 大型平台外洩動輒影響數億人——你可能早就在名單上,只是不知道。

資料去哪了 外洩的帳密、信用卡、身分資料,會被打包在暗網上販售。

冰山比喻 我們平常用搜尋引擎找到的,只是網路世界的表層而已。



投資報酬率 成本約 30 元的個資,可能讓你損失 40 萬——不對等的代價。

四 · 防護 ①

密碼:別再用「一把鑰匙開全家門」

重點不是多複雜,而是「夠長」且「不重複」

這樣設密碼

- ✓ 用一句好記的長句子,例如「我家小狗2019愛吃地瓜」
- ✓ 每個重要網站用「不同」密碼
- ✓ 用密碼管理器幫你記,只記一組主密碼

別這樣設密碼

- ✗ 123456、password、生日、電話
- ✗ 所有網站用同一組密碼
- ✗ 把密碼寫在便利貼貼在螢幕上
- ✗ 用瀏覽器存在公用電腦上

四 · 防護 ②

多因素驗證(MFA):最划算的一道鎖

就算密碼被偷,駭客也少了第二把鑰匙進不來

它是什麼?

登入時,除了密碼,還要再加一道驗證——例如手機上的一次性驗證碼、或按一下「是你本人嗎?」的通知。

優先為這些開啟:

email、網銀、LINE、臉書 / IG、公司帳號

怎麼開?

到帳號的「設定 → 安全性」,找「兩步驟驗證 / 多因素驗證」並開啟。

密碼與個資防護 5 大秘訣

這五件事做到,個資外洩的傷害就能大幅降低

建立強密碼	混合英數字與符號,8 個字元以上;更好的是用長句子。
不使用重複密碼	尤其 email、網銀,務必與其他網站不同。
使用雙重驗證(2FA)	最有效的一道防線,重要帳號一律開啟。
定期變更密碼	得知服務外洩時,立刻更換該站與相同密碼的其他站。
善用防護工具	使用密碼管理器與個資外洩監控服務。

四 · 重點

本段重點帶走

假設你的資料已經外洩了

重點不是防止外洩,而是讓外洩的資料「不好用」。

不同網站,不同密碼

這一件事就能阻止「一處外洩、全盤淪陷」。

今天就把 MFA 打開

五分鐘的設定,擋掉絕大多數的帳號盜用。

五 ·

5

危險 Wi-Fi

威脅四:上網便利的代價——免費的最貴

駭客如何在你用免費 Wi-Fi 時襲擊你?

餐廳、咖啡廳、飯店、機場、加油站——都可能是現場

偽裝熱點

架設一個和店家同名的假 Wi-Fi,誘你連上,監看你傳輸的所有資料。

監聽封包

在未加密的網路上竊聽你傳輸的內容,取得檔案與交易資料。

窺探隱私

從遠端偷看你的螢幕內容與按鍵,例如你正在輸入的登入帳密。

五 · 危險 WI-FI

公共 Wi-Fi 與假熱點

是什麼	在咖啡廳、車站等地架設「免費 Wi-Fi」假熱點,攔截你傳輸的資料。
怎麼運作	你連上後,駭客可能看到你輸入的帳密,或把你導到假網站。
真實長相	看到「Free_Airport_WiFi」就連,結果是駭客架的同名熱點。

怎麼辨識 公共 Wi-Fi 上避免登入網銀、輸入密碼;不確定就用手機行動網路,或使用公司 VPN。

VPN:在公用 Wi-Fi 上多一層保護

把你的連線「包起來」,讓旁人看不到內容

它幫你做什麼

- ✓ 把連線加密,降低被監聽的風險
- ✓ 在飯店、機場等場所保護隱私
- ✓ 公司提供的 VPN 請優先使用

但它不是萬能

- ✗ 不能防止你連上詐騙或惡意網站
- ✗ 不保證完全匿名,業者可能留存紀錄
- ✗ 免費 VPN 風險高,可能把你的資料賣給廣告商

五 · 重點

本段重點帶走

公共 Wi-Fi 不做敏感操作

不登入網銀、不輸入密碼、不購物付款。

同名熱點你分不出來

與其分辨,不如直接改用自己的手機行動網路。

VPN 有用但不是萬能

它加密連線,但不會幫你擋詐騙網站;免費的風險更高。

六 ·

6

實務案例分享

真實發生的事件——換作是你,你會在哪一步擋下它?

六 · 怎麼看案例

每個案例,問自己這五件事

別只看『被騙好慘』,要看『我能在哪裡擋下』

發生什麼

事件經過

什麼手法

對應前面學的

破口在哪

人/流程/技術

損失多少

後果與代價

我能擋哪步

換作是你

六 · 案例一

香港 Arup:深偽視訊騙走 2,560 萬美元

事件經過

一名財務員工收到「英國 CFO」的轉帳指示信,起初覺得可疑。但後續一場視訊會議裡,「CFO」與多位「同事」都在線上、長相聲音都對,他放下戒心,分 15 筆共匯出約 2 億港幣。事後與總部確認,才發現會議裡每個人都是 AI 深偽。

造成損失 約 2 億港幣(2,560 萬美元)遭詐,款項難以追回。

使用手法

深偽(假視訊)+ BEC 商業郵件詐騙,結合急迫與權威。

關鍵破口

看到「熟悉的臉與聲音」就放下戒心,沒有用第二管道驗證高額轉帳。

你能擋的一步 高額匯款前,用已知電話回撥本人確認——一通電話就能擋下。

六 · 案例二

PowerSchool:校園系統被駭,師生個資外洩

事件經過

北美廣泛使用的校園資訊系統 PowerSchool 遭入侵,攻擊者透過外洩的帳號憑證進入系統,竊取大量資料,外洩超過 6,200 萬名學生與約 950 萬名教師的個人資料,事後甚至再以資料勒索校方。

造成損失 逾 6,200 萬名學生、約 950 萬名教師個資外洩,並遭勒索。

使用手法

供應鏈攻擊 + 帳號憑證外洩 + 勒索。

關鍵破口

對信任的供應商系統缺乏防護;單靠帳密、未普遍開啟多因素驗證。

你能擋的一步 不同服務用不同密碼、開啟多因素驗證,降低帳密外洩的連鎖傷害。

六 · 案例三

普發一萬:假冒政府的釣魚網站

事件經過

2025 年政府發放普發現金一萬元期間,詐騙集團架設大量假冒的「普發現金」網站,透過簡訊、社群散布,誘導民眾在假網站輸入身分證、銀行帳號與驗證碼。財政部短時間內就查獲並停止解析 11 個假網站。

造成損失 民眾個資、帳號恐遭竊;財政部緊急關閉 11 個假網站。

使用手法

簡訊/網站釣魚,搭上時事與「政府」權威。

關鍵破口

民眾分不清官方網址,看到「領錢」就急著點連結登記。

你能擋的一步 認明官網結尾「.gov.tw」;政府不會用簡訊或 email 通知你領錢。

六 · 案例四

假投資「養套殺」:台灣財損之王

事件經過

詐騙集團在社群投放廣告、假冒名人或老師,把被害人拉進 LINE 投資群組。群組裡「大家」都在曬獲利對帳單,先讓你小額試水賺到錢,再誘你加碼、甚至貸款投入,最後網站關閉、群組消失。長輩受騙金額最高。

造成損失 積蓄甚至貸款全數投入後血本無歸,長輩受創最深。

使用手法

社交工程 + 假投資 + 深偽名人代言,長期經營(養→套→殺)。

關鍵破口

「保證獲利」的貪念,加上群組營造的從眾與信任感。

你能擋的一步 記住保證獲利就是詐騙;投資只透過合法券商,不靠 LINE 群「老師」。

六 · 案例五

勒索軟體癱瘓整個組織的營運

事件經過

2025 年全球多起勒索事件中,醫療、製造、教育機構都受重創。攻擊者常從一封釣魚信或一組外洩帳密進入,潛伏數天後同時加密大量系統,使醫院掛號、工廠產線或學校系統全面停擺,並威脅公開竊得的資料。

造成損失 醫院、工廠、學校系統全面停擺,資料遭威脅公開。

使用手法

釣魚 / 帳密外洩為入口,雙重勒索(加密 + 公開威脅)。

關鍵破口

一個人點開釣魚信、或一組弱密碼,就成為整個組織的破口。

你能擋的一步 不點不明連結附件;重要資料定期備份,並離線保存一份。

六 · 案例六

LINE / 社群帳號被盜,假冒你向親友借錢

事件經過

你的 LINE 或臉書帳號被盜後,駭客假冒你,向你的親友、同事發訊息:「在嗎?幫我代收一筆款」「幫我買遊戲點數卡,急用」。因為訊息來自「你本人」的帳號,親友容易卸下心防而上當。

造成損失 親友被假冒的你騙走金錢或點數卡,信任受損。

使用手法

帳號盜用 + 社交工程,利用人際信任。

關鍵破口

帳號沒開多因素驗證被盜;親友未向本人查證就匯款。

你能擋的一步 帳號開啟多因素驗證;收到借錢訊息先用電話確認本人。

六 · 橫向比較

六個案例,同一個結論

破口幾乎都在「人」,而擋下它的動作也都很簡單

案例	核心手法	能擋下的一個動作
Arup 深偽	深偽 + BEC	高額匯款回撥本人確認
PowerSchool	供應鏈 + 帳密	不同密碼 + 多因素驗證
普發一萬釣魚	簡訊/網站釣魚	認明 .gov.tw、不點連結
假投資養套殺	社交工程 + 假投資	拒絕「保證獲利」
勒索軟體	釣魚 + 雙重勒索	不點附件 + 離線備份
帳號盜用	帳號盜用 + 社交	多因素驗證 + 電話確認

六 · 重點

本段重點帶走

真實損失往往很大

從個人積蓄到組織營運,代價遠超想像。

破口幾乎都在「人」

不是系統被破解,而是有人被騙、按下了確認。

擋下它的動作都很簡單

回撥確認、開多因素驗證、不點連結——你都做得到。

七 · 16 分鐘

7

個人與工作防護實務

不講大道理,只給你「回去馬上能做」的具體動作

為什麼你容易被騙?因為詐騙懂心理學

它不跟你的理智對話,它直接跟你的情緒對話

限時 · 免費 · 好康

製造焦慮,讓你不思考就點下去

焦慮讓人失去判斷

當你覺得「來不及了」,大腦會跳過查證直接行動。

從眾讓人放下懷疑

群組裡「大家都賺錢」,你就會覺得自己才是落後的。

權威讓人不敢多問

自稱檢警、主管,你會怕追問顯得不禮貌或有問題。

七 · 核心口訣

識詐口訣:不急、不貪、多查證

拆成三個動作就是——停、看、查

停

不急

越是急迫、越要你「馬上」,越要踩煞車。

看

不貪

看寄件者、看網址、看它要你做什麼;好康先當假的。

查

多查證

換「另一個管道」查證:官方 App、打本人電話,或撥 165。

七 · 黃金法則

黃金法則:換一個管道,向「本人」確認

這一招,幾乎能擋下今天看過的所有案例

只要訊息牽涉到 **匯款 / 改帳號 / 提供密碼或驗證碼 / 急件保密** ——不論看起來多可信,都先暫停。

打電話

用你「原本就知道」的號碼回撥本人,不要用訊息裡給的號碼。

當面問

如果是同事或長官,直接走過去、或當面問一句最快。

撥 165

不確定是不是詐騙,直接打 165 反詐騙專線查證。

七 · 基本功

把基本功做好:更新、來源、防護、備份

不起眼,但能擋掉一大半的自動化攻擊

保持更新

作業系統、瀏覽器、App 出現更新就裝——很多更新是在補安全漏洞。

只裝官方來源

從官方商店或官網下載;不裝盜版、破解、來路不明的程式。

開啟防護軟體

保持防毒/內建防護開啟並更新,當作最後一道自動防線。

重要資料備份

重要檔案定期備份,最好留一份離線——勒索軟體就拿你沒辦法。

保護你手上的「別人的資料」

行政、教學、業務同仁手上,往往有最敏感的個資

個資要當心

姓名、身分證、聯絡方式、成績、照片——外洩會造成真實傷害。

寄送前確認收件人

含個資的檔案寄出前停一秒確認對象;群組貼訊息前確認貼對地方。

公私裝置盡量分開

盡量不用個人裝置處理大量個資;公務資料不隨意存到私人雲端。

敏感畫面不外流

含個資的螢幕、名冊別隨手拍照上傳社群。

詐騙 24 小時不間斷

從上班、午休到通勤、追劇,每個時段都有對應的攻擊

為什麼要養成習慣 威脅是「快閃、多變」的,所以防護不能只靠記住某一種手法,要養成固定的判斷習慣。

七 · 帶走守則

暢遊網路 6 大不 NG 守則

把這六件事變成習慣,你就贏過大多數人

1

保持更新

系統、App、防毒軟體都要更新

2

強化密碼安全

密碼不重複,並開啟多因素驗證

3

安全安裝 App

只用官方商店,注意權限要求

4

慎用公共 Wi-Fi

不做敏感操作,必要時使用 VPN

5

定期備份

重要資料定期備份,並留離線一份

6

留意帳號異常

定期檢查登入紀錄與帳單

萬一中招了,怎麼辦?

越早回報,損失越小——回報不是丟臉,是負責

立即停止

別再操作,立刻中斷:斷網、別再點、別再轉帳。

改密碼

盡快更改受影響帳號的密碼,並開啟多因素驗證。

馬上回報

通知單位 IT / 資安窗口,讓專業的人接手處理。

對外求助

涉及金錢或詐騙,撥打 165;必要時報警、通知銀行。

我們單位的資安/IT 通報窗口:〔請填入 — 例如 分機 / Email / 通報表單 〕

七 · 帶走清單

資安好習慣 · 檢查清單

把這頁拍下來,回去一項一項打勾

- 重要帳號都用「不同」的密碼
- email、網銀、社群都開了多因素驗證
- 收到可疑訊息會「停、看、查」
- 牽涉錢/帳號,一定換管道向本人確認
- 系統與 App 保持更新,不裝盜版
- 重要資料定期備份,留一份離線
- 認得官網「.gov.tw」,不亂點連結
- 公共 Wi-Fi 不登入網銀、不輸密碼
- 手機只從官方商店安裝 App
- 知道中招時要找誰回報、打 165

八 ·

8

總結、測驗與 Q&A

用幾個情境題驗收今天的學習,再帶走最重要的三件事

情境小測驗:你會怎麼做?

用舉手或喊出答案——A 還是 B?

Q1	收到「主管」email,急著要你改一個匯款帳號並保密。	A 照做 / B 打電話跟主管確認
Q2	簡訊說「普發一萬請點此登記」,附一個連結。	A 點進去登記 / B 自己開官方 App 查
Q3	「IT 人員」來電,要你提供帳號密碼以「修復系統」。	A 提供密碼 / B 拒絕並向 IT 查證
Q4	LINE 上「好友」傳訊,急著要你幫買遊戲點數卡。	A 先買再說 / B 打電話跟本人確認
Q5	在咖啡廳看到兩個同名的免費 Wi-Fi,想查一下網銀。	A 連上查詢 / B 改用手機行動網路

八 · 解答

答案都是 B——而且原因一樣

凡是牽涉錢、密碼、急迫保密,一律「換管道確認」

Q1 打電話跟主管確認	經典 BEC,改帳號 + 保密就是最大警訊。
Q2 自己開官方 App 查	認明 .gov.tw,連結用查的不用點的。
Q3 拒絕並向 IT 查證	真正的 IT 永遠不會跟你要密碼。
Q4 打電話跟本人確認	帳號可能被盜,代購點數卡是典型騙術。
Q5 改用手機行動網路	同名熱點分不出真假,別在公共 Wi-Fi 登入網銀。

今天請帶走這三件事

1. 你是第一道防線

再強的技術,也擋不住一個人被騙。你的警覺最重要。

2. 不急、不貪、多查證

收到可疑訊息,先踩煞車,對照紅旗,換管道查證。

3. 兩個動作今天就做

密碼不重複、重要帳號開多因素驗證。

謝謝大家!

不當受害者,也不當破口 —— 有任何問題,現在就提出來

165 反詐騙專線

懷疑被詐騙、想查證,隨時撥打。

數位發展部 網路詐騙通報查詢網

查詢與通報可疑網址、訊息。

單位內部資安窗口

〔 請填入 — 分機 / Email / 表單 〕