BCCS 漢昕科技

資安整備專家

國立臺南大學

資通安全及個人資料保護通識教育訓練

漢昕科技 顧問　　陳俊茂

113/07/16

課程大綱

- 資安意識的習慣養成
- 如何保護資訊資產並防止駭客攻擊
- 個人資料的認識與保護
- 認識智慧財產權

- 資安意識的習慣養成
- 資安是什麼
- 資安與生活有什麼關係
- 生活中面臨哪些資安威脅

資安政策宣導

國立臺南大學資通安全宣導網

https://isms.nutn.edu.tw/Page/Index/ISMS

個資政策宣導

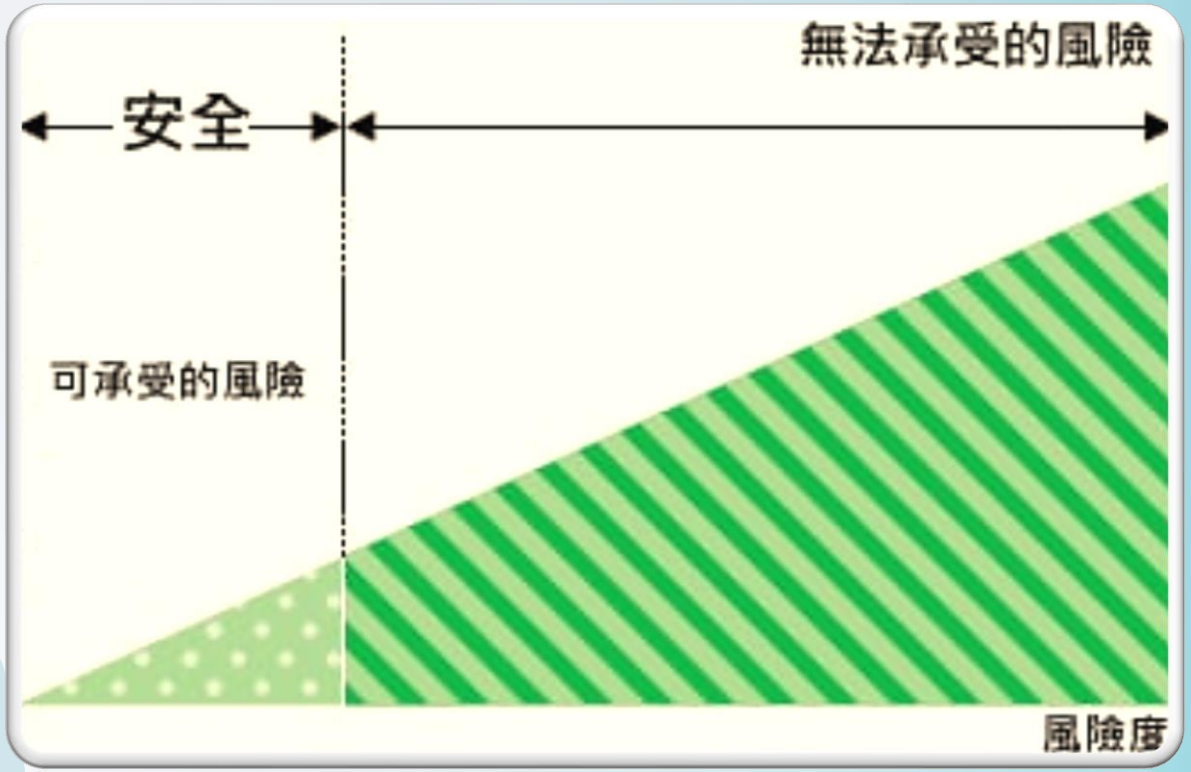
國立臺南大學個人資料保護宣導網

https://pip.nutn.edu.tw/

ISO/IEC Guide 51

「安全」的定義為免於無法承受的風險。

換句話說，將風險**降低到可承受的等級**，就能達到安全。



資通安全(Cyber Security)

指保護資訊或資通系統免於**未經授權**之

存取、使用、控制、洩漏、破壞、竄改、銷毀或**其他侵害**

以確保其**機密性、完整性**及**可用性**。

資訊安全三要素 (CIA Triad)

機密性

（Confidentiality）

指訊息不為其他不應獲得者獲得，保障訊息在對的人、對的時間、對的裝置和對的地點上被存取，用以維護用戶資訊的保密性。

完整性

（Integrity）

指在傳輸、儲存資訊或資料的過程中，資訊或資料不被未授權的篡改。

可用性

（Availability）

簡單的說，可用性就是讓一個系統處隨時可工作狀態，資訊服務不因任何因素而中斷/停止。

資訊安全三要素之間存在著互相牽制的關係

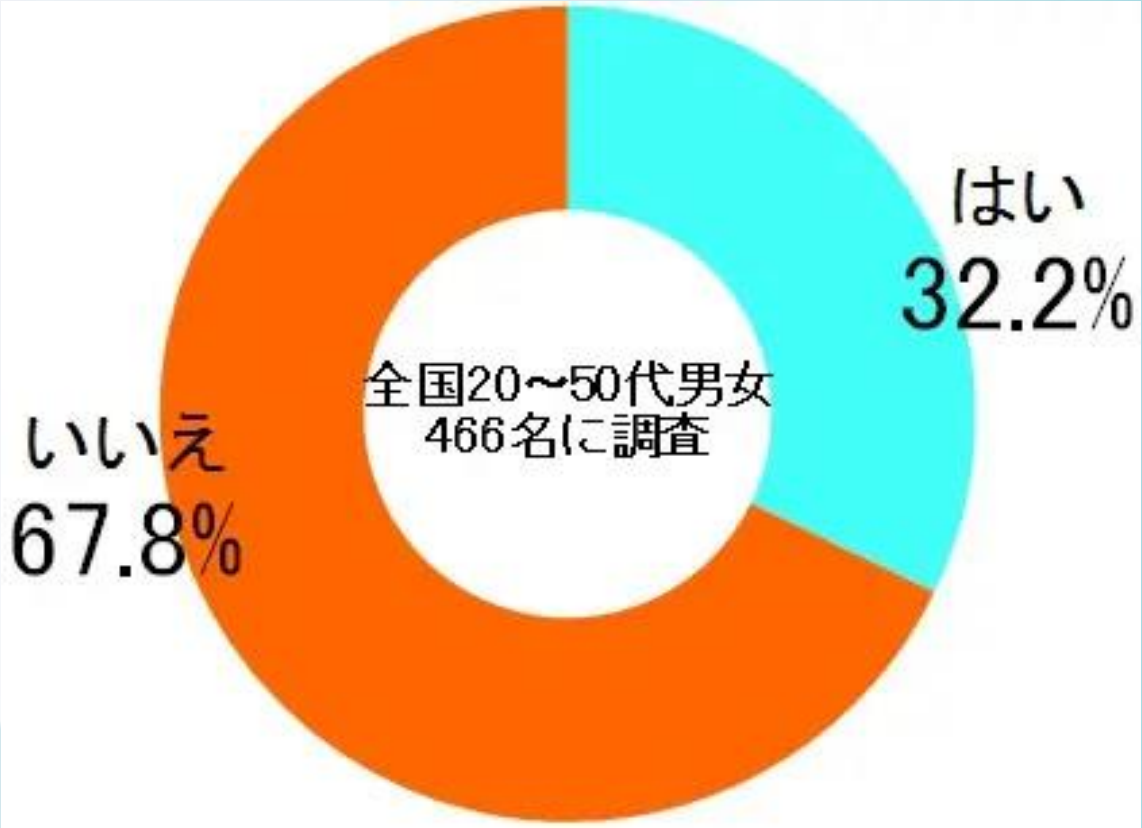
- 亦即過度強化機密性，將犧牲完整性與可用性; 擁有高可用性的系統則往往會需要在機密性與完整性上妥協。
- 如何在有限資源下，取得此三個要素之間的平衡是資訊安全管理當中重要的課題之一。

- **資安意識的習慣養成**
  - 資安是什麼
  - **資安與生活有什麼關係**
  - 生活中面臨哪些資安威脅

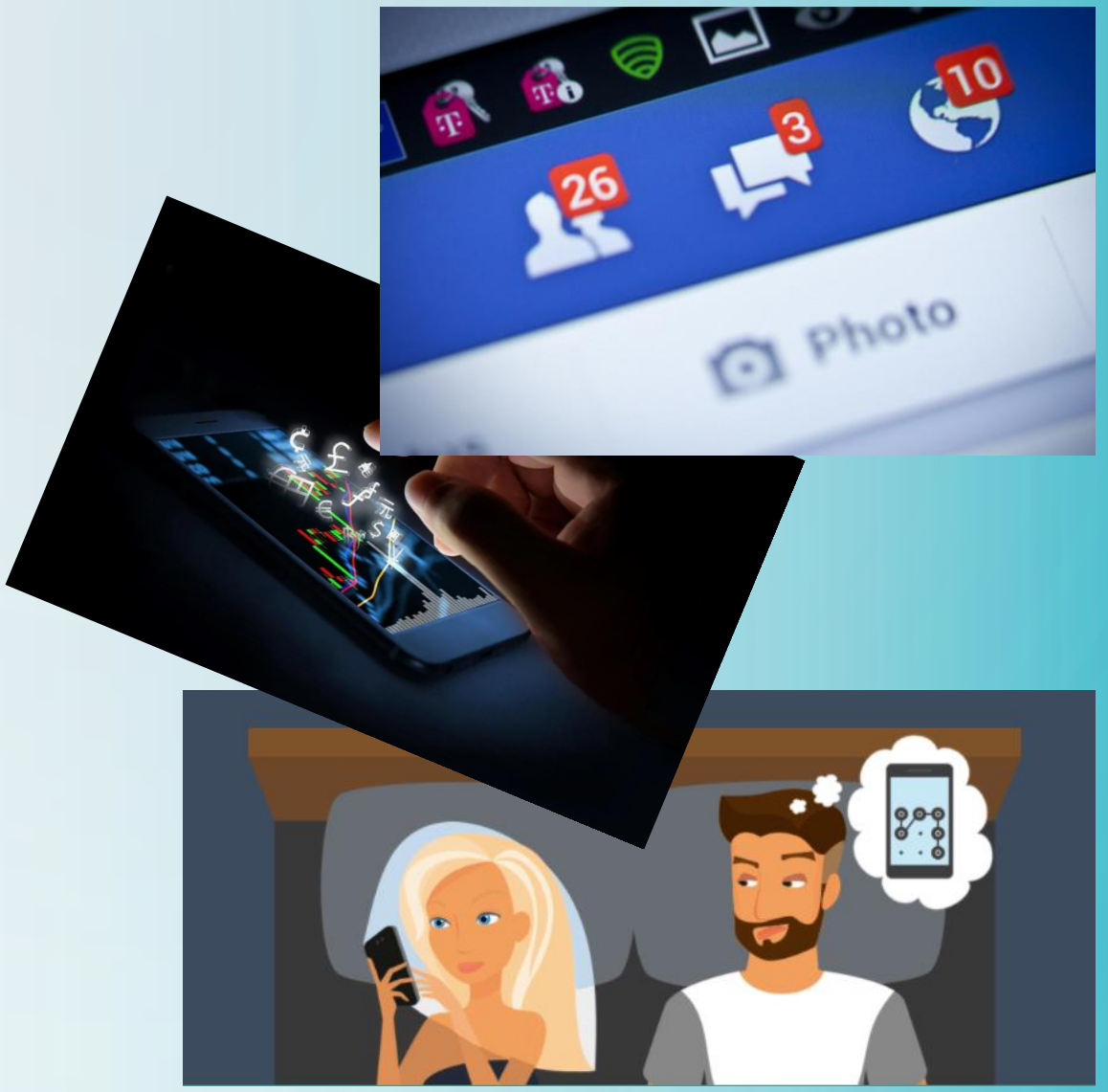
滑手機時出現.....

日本某調查網站，曾做調查：

您在火車上看過別人手機螢幕上的個人資訊嗎？



「雖然有的時候也不是故意，但就這麼剛好對方的手機畫面就這麼躺在你的視線範圍，所以就瞄了一眼內容……」



刑法315條：

「無故開拆或隱匿他人之封緘信函、文書或圖畫者，處拘役或九千元以下罰金。無故以開拆以外之方法，窺視其內容者，亦同。」

刑法315條所保護的法益是 「非公開的東西」

刑法315-1條　有下列行為之一者：

一、無故利用工具或設備**窺視**、**竊聽**他人非公開之活動、言論、談話或身體隱私部位者。

二、無故以錄音、照相、錄影或**電磁紀錄**竊錄他人非公開之活動、言論、談話或身體隱私部位者。

處**三年以下**有期徒刑、拘役或**三十萬元**以下罰金

鬧翻！公司筆電帳密未登出 離職資料遭拷貝

刑法 第三十六章 妨害電腦使用罪

第358條 （入侵電腦或其相關設備罪）	• 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第359條 （破壞電磁紀錄罪）	• 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
第360條 （干擾電腦或其相關設備罪）	• 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第361條 （加重規定）	• 對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
第362條 （製作供犯罪之電腦程式罪）	• 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

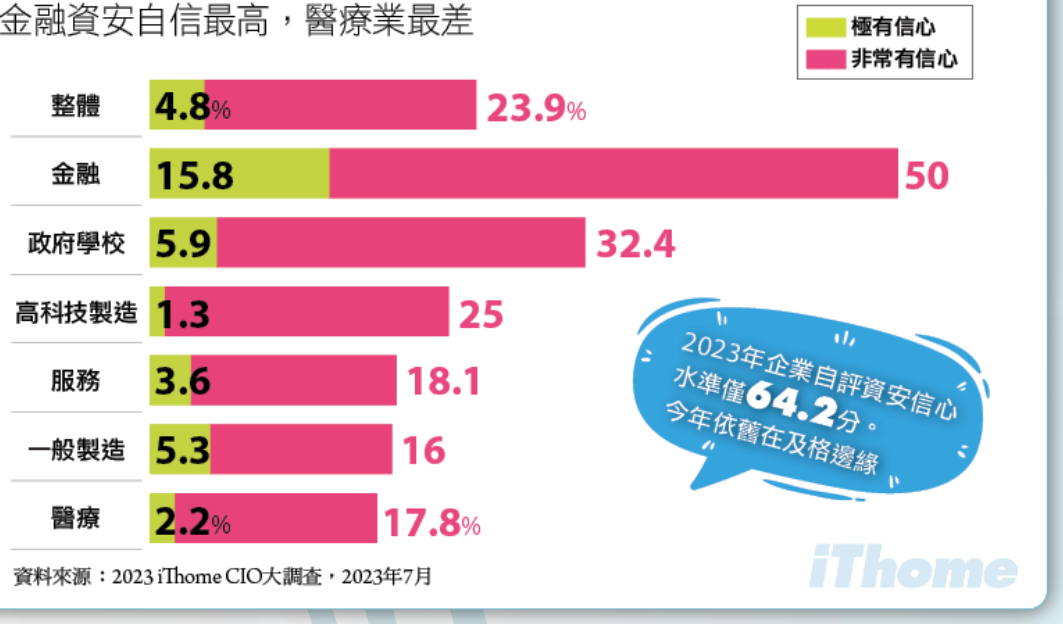
資安意識的習慣養成

- 資安是什麼
- 資安與生活有什麼關係
- **生活中面臨哪些資安威脅**


2023上市櫃公司資安事件重大訊息一覽
華航
市場產業別 上市－航運業
公告標題與說明 華航針對媒體報導提出說明（針對會員資料被公開在國外論壇，說明接獲匿名網路勒贖信件後已報警及依法通報）
裕融
市場產業別 上市－其他
公告標題與說明 針對媒體報導提出說明（說明旗下格上汽車租賃公司會員訂單資料的可被任意查詢問題的已經有所因應）
飛宏
市場產業別 上市－電子零組件業
公告標題與說明 公司發生網路資安事件
宏碁 acer
市場產業別 上市－電腦及週邊設備業
公告標題與說明 說明媒體報導（針對宏碁印度售後服務系統遭駭事件，說明係商業夥伴密碼保存與管理不當，造成產品維修等資料外洩）
立德
市場產業別 上市－電子零組件業
公告標題與說明 電子部份資訊系統及備份系統遭受網路攻擊事件說明
金鼎科
市場產業別 興櫃－其他
公告標題與說明 公司部分資料遭受駭客網路攻擊事件
正新 MAXXIS
市場產業別 上市－橡膠工業
公告標題與說明 代子公司Cheng Shin Rubber USA, Inc公告部份資訊系統遭受駭客網路攻擊事件說明
1月14日
2月1日
2月6日
2月12日
2月13日
3月6日
3月8日
3月14日
3月28日
4月7日
4月14日
5月14日
5月30日
和泰車
市場產業別 上市－汽車工業
公告標題與說明 澄清自由時報報導（說明旗下和雲行動服務公司的iRent資料庫個資曝險問題已改正）
華航
市場產業別 上市－航運業
公告標題與說明 華航已全面加強資安系統防堵 配合警方偵辦個資事件（說明查出委外電商平臺系統連線異常，5千多筆會員資料遭竊取）
宏致
市場產業別 上市－電子零組件業
公告標題與說明 公司部份資訊系統遭受駭客網路攻擊事件說明
鼎聯
市場產業別 上市－綠能環保
公告標題與說明 代子公司台鋼資源股份有限公司公告說明部份資訊系統遭受駭客網路攻擊
微星 msi
市場產業別 上市－電腦及週邊設備業
公告標題與說明 公司部分資訊系統遭受駭客網路攻擊（同時在公司網站公告）
誠品生活
市場產業別 上櫃－文化創意業
公告標題與說明 說明經濟日報112年5月14日14時10分網路新聞即時報導（針對誠品疑個資外洩狀況，表示將配合數服部通知前往說明）
環天科
市場產業別 上櫃－通信網路業
公告標題與說明 公司部分資訊系統遭受駭客網路攻擊
大樹
市場產業別 上櫃－生技醫療業
公告標題與說明 公司遭受駭客網路攻擊事件
諾貝兒
市場產業別 興櫃－生技醫療業
公告標題與說明 公司遭受網路駭客攻擊事件
中華化
市場產業別 上市－化學工業
公告標題與說明 公司部份資訊系統遭受駭客網路攻擊
中石化
市場產業別 上市－塑膠工業
公告標題與說明 公司遭受網路攻擊事件
上海商銀
市場產業別 上市－金融保險業
公告標題與說明 公告公司受金管會裁罰案之說明（原因為金管會針對該銀行個戶資料外洩案所涉缺失開罰）
6月19日
7月24日
7月28日
8月19日
10月7日
10月27日
11月12日
11月20日
11月24日
11月28日
中華
市場產業別 上市－汽車工業
公告標題與說明 公司發生網路資安事件
日馳
市場產業別 上市－電機機械
公告標題與說明 公司部份資訊系統遭受網路攻擊事件
羅昇
市場產業別 上市－電機機械
公告標題與說明 公司部份資訊系統遭受駭客網路攻擊
雄獅
市場產業別 上市－觀光餐旅
公告標題與說明 公司遭受駭客網路攻擊事件
大江
市場產業別 上櫃－生技醫療業
公告標題與說明 公司網路資安事件
資料來源：臺灣證券交易所公開股市觀測站，iThome整理，2024年3月

多少企業對自家資安能力很有信心？

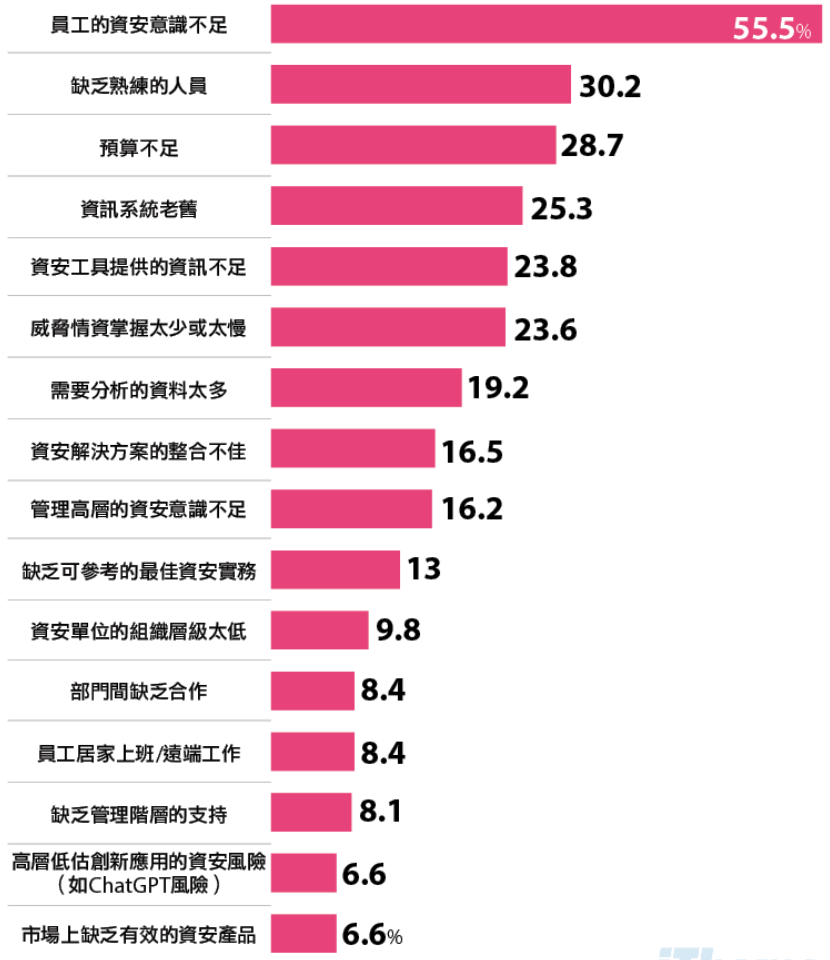
金融資安自信最高，醫療業最差



資料來源：2023 iThome CIO大調查，2023年7月

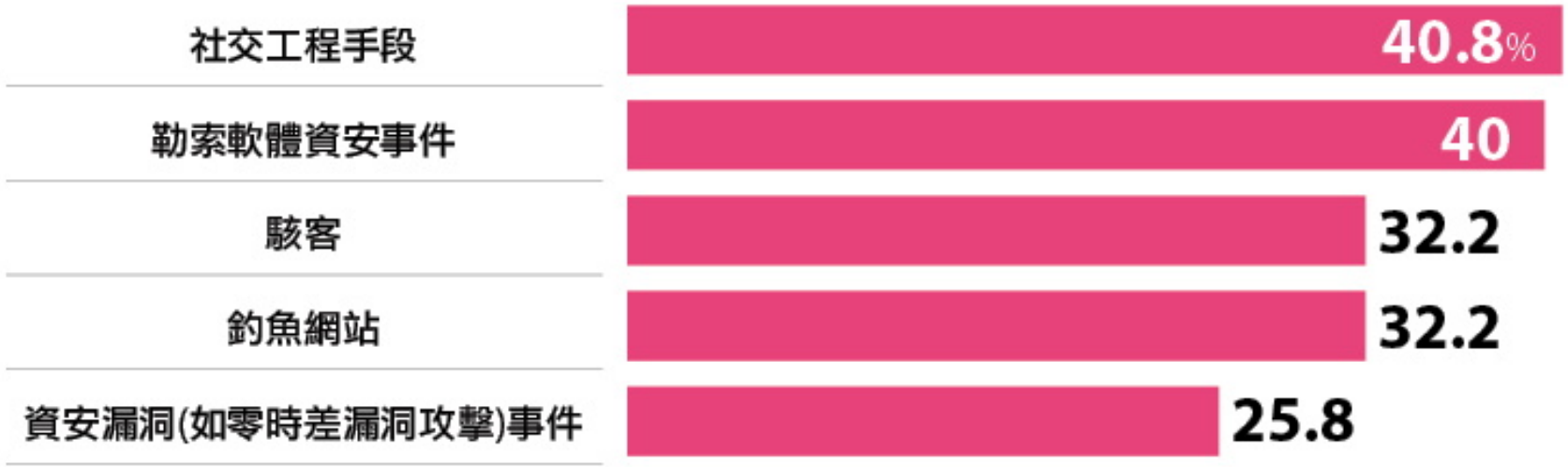
為何企業難以抵抗資安攻擊（2023 資安弱點排名）

5 成多企業員工資安意識不足，3 成企業缺乏資安老手



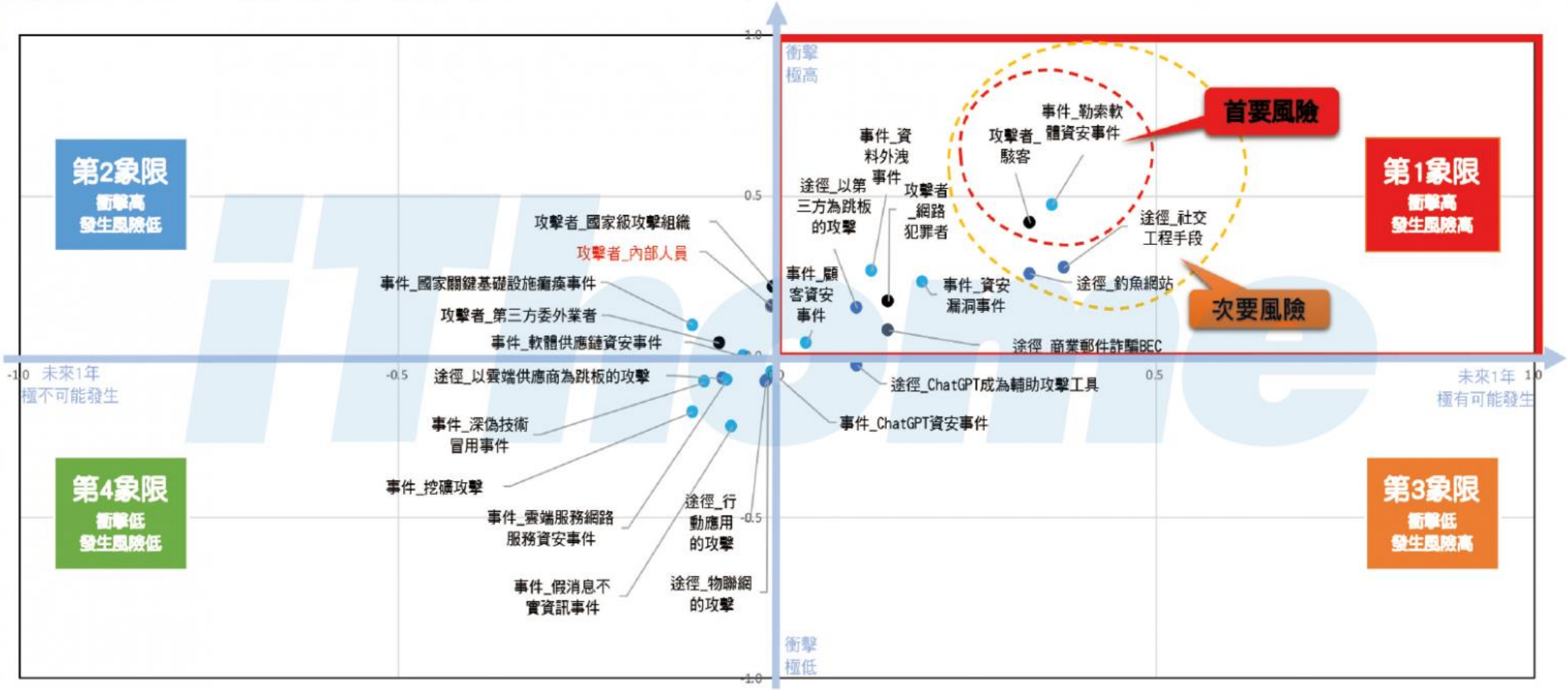
資料來源：2023 iThome CIO大調查，2023年7月

未來一年 5 大資安風險



資料來源：2024 iThome CIO大調查，2024年4月

整體產業企業資安風險圖（2023 ~ 2024）



世界首例，烏克蘭大停電證實是遭駭客入侵

2015年12月23日，就在平安夜的前一天，俄羅斯駭客斷然採取一次重大行動。

駭客駭入並控制烏克蘭輸電網路的電腦，將斷路器接連關閉。除此之外，他們還關閉緊急電話線並切斷了配電中心的備用電源，迫使作業人員只能在黑暗中摸索。

使得首都基輔部分地區和西部的140 萬名居民遭遇了一次長達數小時的大規模停電，至少三個電力區域被攻擊，佔據全國一半地區。

同一批俄羅斯駭客於2016年12月切斷烏克蘭的電力。他們這次切斷的是核心城市基輔的暖氣與電力，以展現他們的膽識與技術。

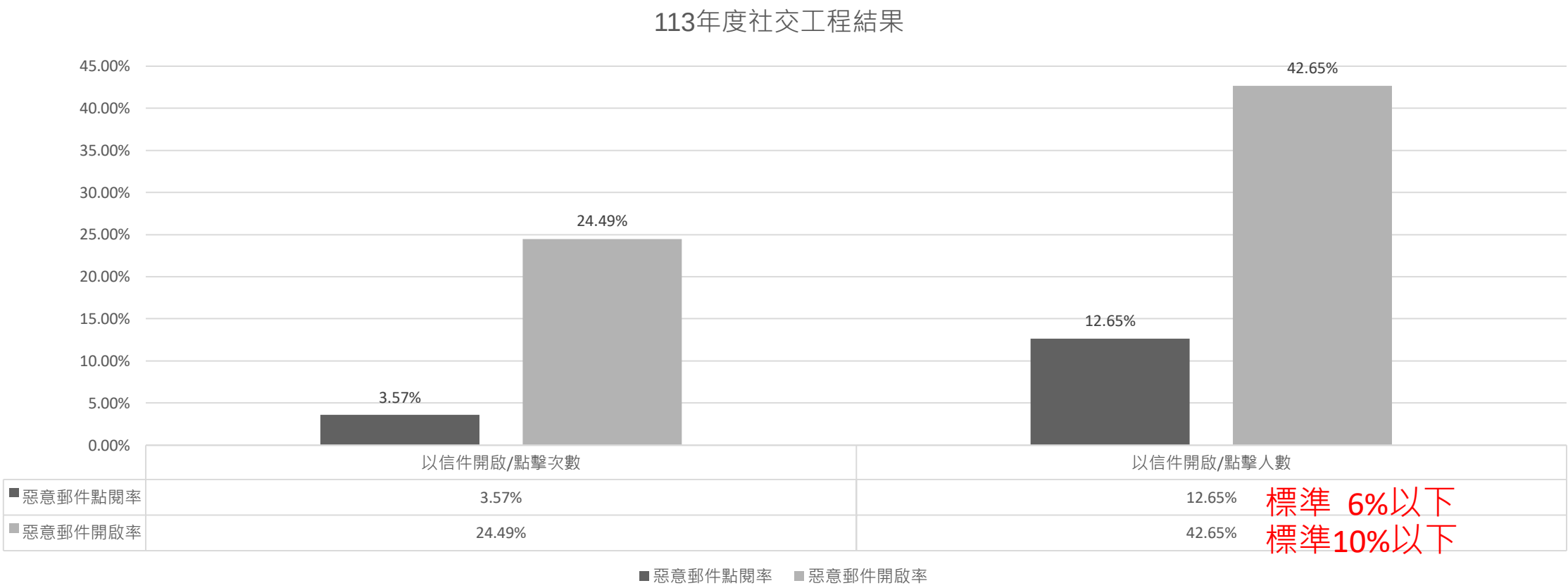
台灣前3季每週遭網攻逾1500次 居全球之冠

資安威脅影響層面

國家	企業	個人
• 關鍵資訊基礎設施遭駭引發政經民心動亂	• 經濟損失 • 商譽受損 • 機密外洩	• 檔案勒索 • 財務盜刷 • 個資外洩

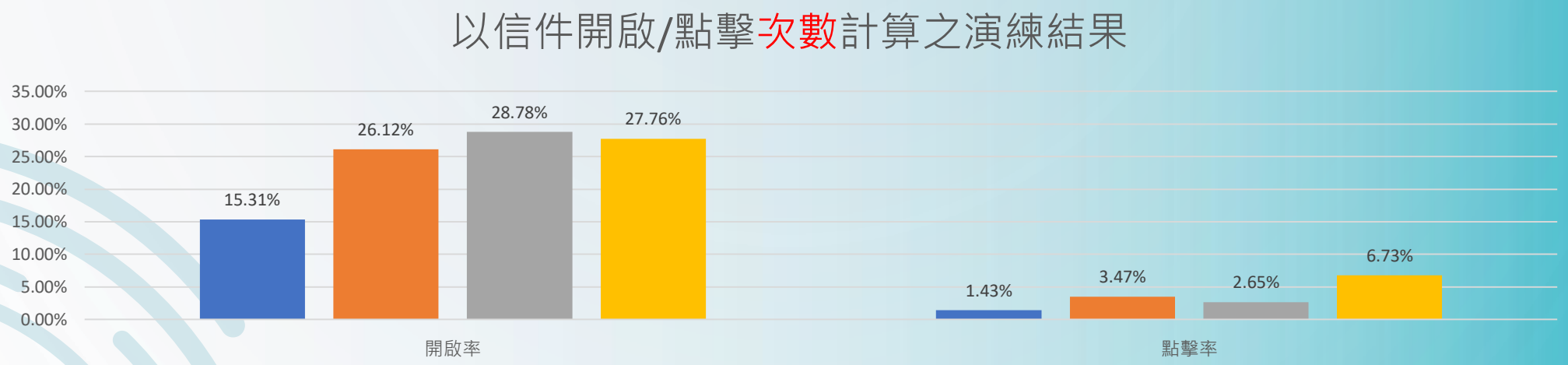
- 如何保護資訊資產並防止駭客攻擊
- 社交工程攻擊與防範
- 勒索病毒攻擊與防範
- 行動裝置資安防護

113年度社交工程結果



主管機關為中央A級機關，其惡意郵件開啟率及點閱率須分別達10%及6%以下；中央A級機關以外之其餘主管機關，其惡意郵件開啟率及點閱率須分別達10%及6%以下

以信件開啟/點擊次數計算之演練結果



Uber 疑遭駭侵者透過社交工程攻擊，入侵內部系統

2022年 9 月 15 日發布資安通報

某位員工遭到一名年僅 18 歲的駭侵者，透過社交攻擊手法取得該公司內部系統的登入資訊。

該名駭侵者為了取得兩步驟登入驗證密碼，更透過大量發送垃圾通知的手法讓該名遭駭員工不斷收到推送通知，接著再於 WhatApp 上假冒 Uber IT 人員和該員工對話，進而取得兩步驟驗證碼的存取權。

在取得兩步驟驗證碼後，隨即進入 Uber 內部網路，同時很快就在其內網的某個檔案中找到許多具有極高權限的登入資訊。

該名駭侵者立即使用這些登入資訊存取 Uber 內部各項系統，包括產品系統、企業 EDR 控制台、Uber 內部的 Slack 管理介面等等。

甚至還公開 Uber 各個內部系統的螢幕擷圖，包括內部財務系統的報告畫面，以及 Uber 透過 HackerOne 舉辦漏洞發現懸賞的多份報告在內。資安專家擔憂駭侵者可能會將這些漏洞資訊對外販售。

社交工程(Social Engineering)

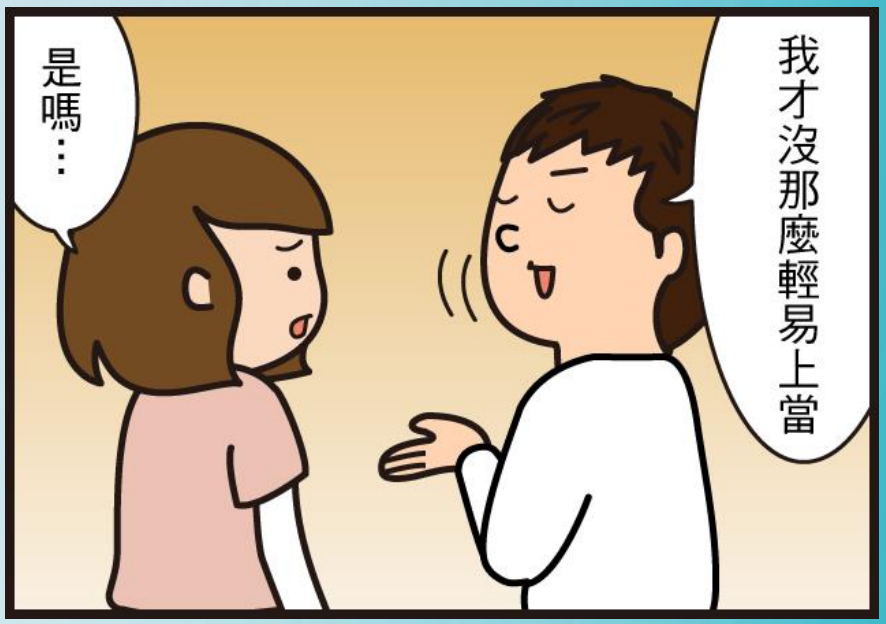
攻擊者 → 用簡單的溝通和欺騙技巧

利用人性的弱點 → 如信任、貪念或恐懼

誘導個人或團體 → 獲取機敏資料、金錢或達成其他不正當目的的行為。

常見社交工程手法

- 通知民眾中獎、退稅等詐騙方式
- 美女錯傳簡訊
- 威脅恐嚇



詐團IG冒社福團體騙抽獎

常見社交工程類型

網路釣魚 /
偽造網址或網頁

惡意電子郵件

即時通訊軟體 /
社群網站

偽裝 App /
修補程式等軟體

電話詐騙

電郵變臉詐騙
BEC
Business Email Compromise

網路釣魚(Phishing)

不法人士將詐騙、可竊取資料或有病毒的網站及郵件，偽裝並假冒成正常管道、正常網頁或熟識的寄件人，當使用者進入這類網站填寫資料或開啟偽冒的惡意郵件之附件時，使用者的重要資訊就會立即外洩，甚至讓裝置中毒、被勒索或被自動安裝惡意程式，提供駭客駭入電腦與系統的快速途徑。

網路釣魚的目的

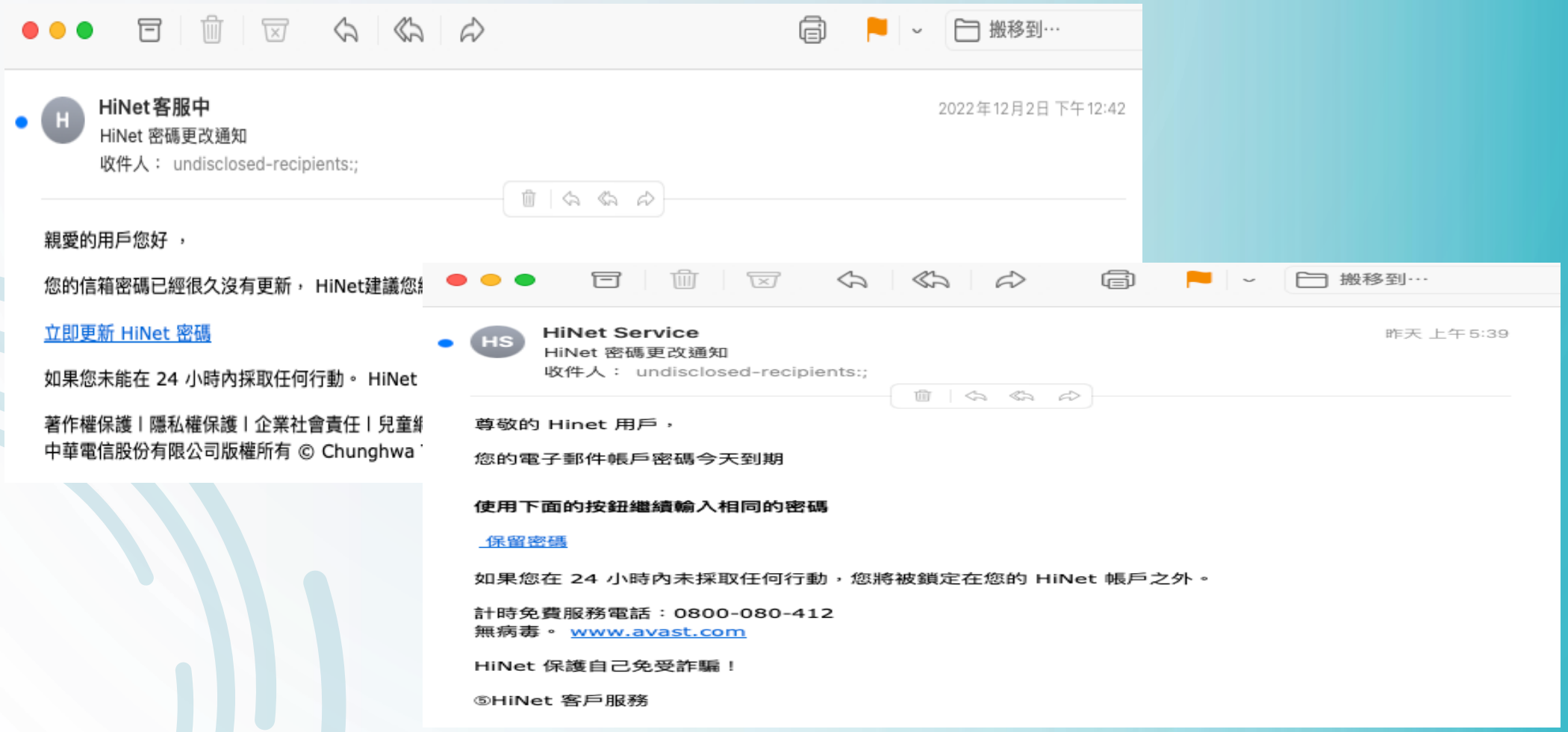
- 竊取機敏資料
- 騙取金錢財物
- 誘導執行惡意程式

常見的網路釣魚手法

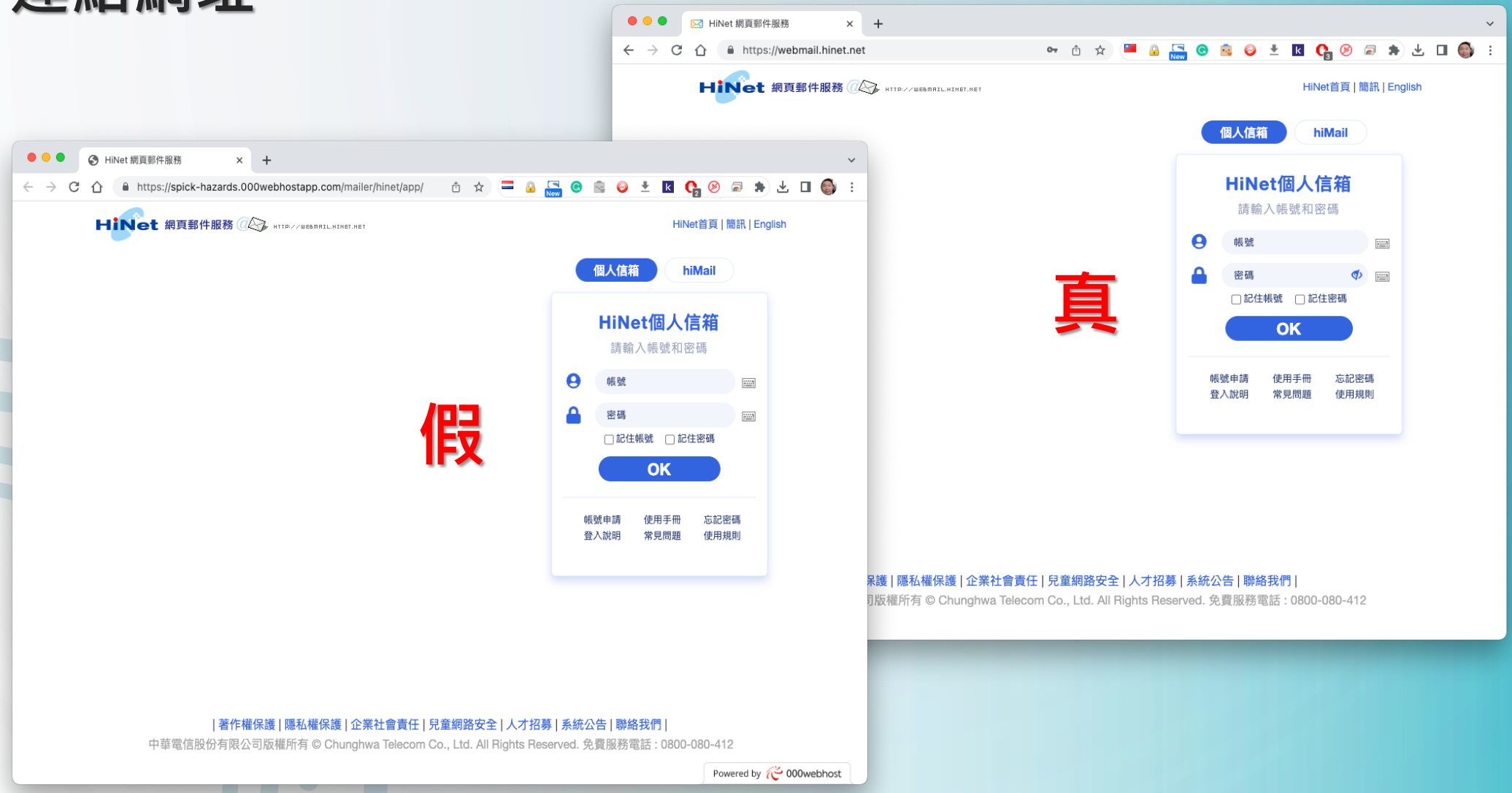
1.電子郵件釣魚

- 發送看似來自信任的公司或組織的電子郵件，要求受害者點擊連結或提供個人信息。這些電子郵件通常會冒用銀行、社交媒體平台、電子支付服務等知名品牌。

釣魚郵件範例


搬移到…
HiNet客服中
HiNet 密碼更改通知
收件人： undisclosed-recipients:;
2022年12月2日 下午12:42
親愛的用戶您好 ，
您的信箱密碼已經很久沒有更新， HiNet建議您
立即更新 HiNet 密碼
如果您未能在 24 小時內採取任何行動。 HiNet
著作權保護 | 隱私權保護 | 企業社會責任 | 兒童
中華電信股份有限公司版權所有 © Chunghwa
搬移到…
HS
HiNet Service
HiNet 密碼更改通知
收件人： undisclosed-recipients:;
昨天 上午5:39
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

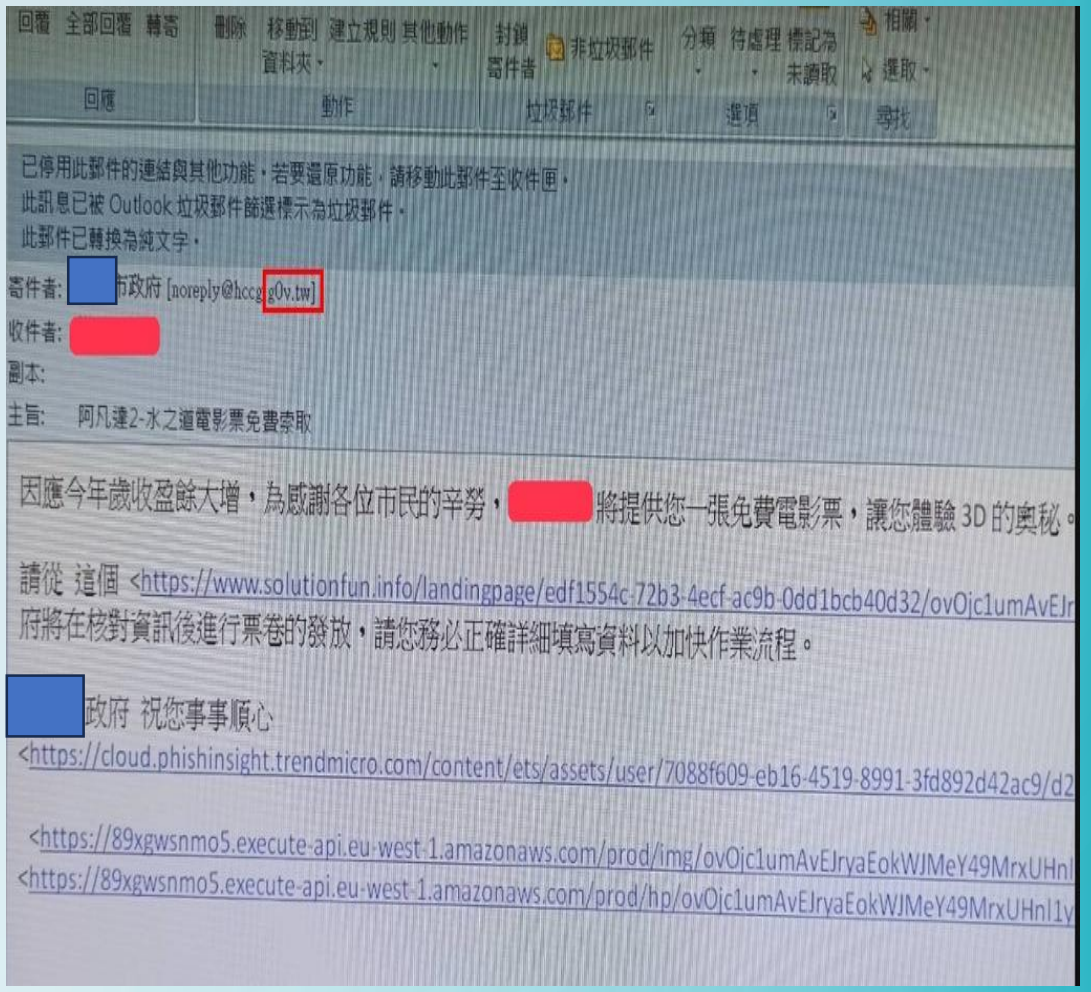
連結網址


HiNet 網頁郵件服務
https://webmail.hinet.net
HiNet 網頁郵件服務 http://webmail.hinet.net
HiNet首頁 | 簡訊 | English
個人信箱
hiMail
HiNet個人信箱
請輸入帳號和密碼
帳號
密碼
記住帳號 記住密碼
OK
帳號申請 使用手冊 忘記密碼
登入說明 常見問題 使用規則
真
HiNet 網頁郵件服務
https://spick-hazards.000webhostapp.com/mailer/hinet/app/
HiNet 網頁郵件服務 http://webmail.hinet.net
HiNet首頁 | 簡訊 | English
個人信箱
hiMail
HiNet個人信箱
請輸入帳號和密碼
帳號
密碼
記住帳號 記住密碼
OK
帳號申請 使用手冊 忘記密碼
登入說明 常見問題 使用規則
假
| 著作權保護 | 隱私權保護 | 企業社會責任 | 兒童網路安全 | 人才招募 | 系統公告 | 聯絡我們 |
中華電信股份有限公司版權所有 © Chunghwa Telecom Co., Ltd. All Rights Reserved. 免費服務電話：0800-080-412
Powered by 000webhost

「O市免費送阿凡達電影票」郵件是假的！

此惡意人士是冒用市府名義寄發社交工程郵件，係刻意將寄件者email網址尾碼改成g0v.tw（數字0）寄送，企圖讓民眾誤以為是由政府機關網址gov.tw（英文字母o）所發送的郵件，同時又用「阿凡達2–水之道電影票免費索取」的誘因，造成民眾降低防範甚至被吸引而誤開啟惡意郵件及其連結。

2023/02/07 中時



釣魚郵件辨識

寄件者

- 檢查 @ 後面的網域名稱是否正確
- 有無正式署名（系統信不適用）

仿冒對象	山寨版	備註
Paypal	paypa1	英文字母「l 」魚目混珠成數字「 1」 *英文字母「o」魚目混珠成數字「 0」也是常用手法
Google	goog1e	
	google	「g」其實是一個拉丁字母，而不是我們平常常見的「G」。
Binance	bịnạnce	「i」和「a」下方多兩個小點

釣魚郵件辨識

郵件內容

- 開頭**稱謂**是否為模糊的泛稱
- 出現**非本國慣用詞彙**、文法怪異

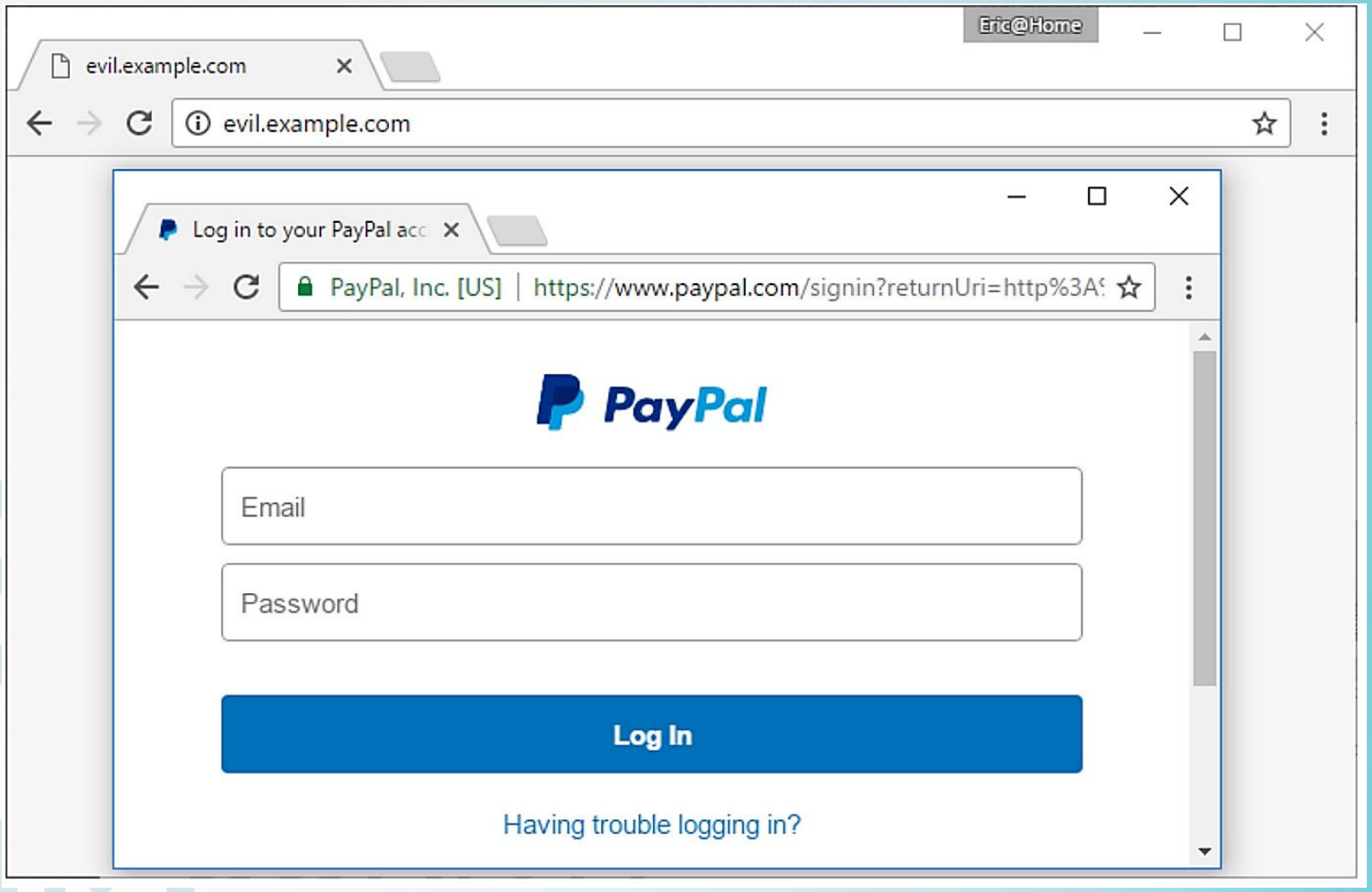
△ **不下載**未確認來源的附件

常見的網路釣魚手法

2.釣魚網站

建立看似合法的網站，與真實的網站外觀相似，以騙取受害者的登錄資訊。他們可能會通過偽造的登錄頁面或彈出式視窗要求受害者提供帳戶名稱和密碼。

釣魚網頁


Eric@Home
evil.example.com
evil.example.com
Log in to your PayPal acc
PayPal, Inc. [US] | https://www.paypal.com/signin?returnUri=http%3A
PayPal
Email
Password
Log In
Having trouble logging in?

假官網詐騙！

〔即時新聞／綜合報導〕民眾購物前還得多注意，自己搜尋的購物網站是否為安全網頁。有民眾上網蒐尋好市多賣場，結果卻跳出「假的」官網，畫面如同原本的官網，讓他差點就登進信用卡資料，事後便發文提醒其他民眾小心受騙。

2021/09/23 自由時報

常見的釣魚手法

3.釣魚簡訊

通過電話、簡訊、社交媒體等方式與受害者**互動**，以獲取個人信息。他們可能**假裝**是銀行員工、客戶服務代表或IT支援人員，試圖誘使受害者提供敏感資料。

通過短信向受害者發送**詐騙簡訊**，試圖引誘他們進行操作或訪問惡意網站。這些簡訊通常聲稱是來自銀行、快遞公司或獎品抽獎等。

釣魚簡訊


常見簡訊連結詐騙手法
1 假冒送貨業者
您的包裹地址不正確，無法送達您指定的地址。請重新提交您的地址：
https://twporev.com
2 假冒政府機關
【衛福部】疫情補貼根据条件你可领五萬，即將過期请網路領取點註冊提 https://www.margov.tv 領申请(複製網址到瀏覽器打開)
刑事警察局165反詐騙諮詢專線關心您
3 假冒帳單欠費
【eTag】您的eTag帳單自動扣款失敗，請在24小時內完成更新，詳細信息請訪問：https://s.id/1jmdE
4 假冒金融機構
【玉山銀行】親愛的顧客您好：您的網路銀行已暫停，請致電本行或查看帳戶詳細信息：https://s.id/1oHQx
詐騙簡訊提醒
遠傳電信溫馨提示
親愛的用戶您好，截止2023年3月25日您的遠傳幣餘額：5559，將於三個工作日內到期，為避免影響，請及時兌換獎賞。
https://www.fetnete.cn
請回复1激活鏈接領取
中華電信：會員回饋提示，您的賬戶5340積分將於今日內到期，逾期將作廢，請及時兌換獎品： http://www.chtcom-vip.com
請回复1激活鏈接領取
請蘋果用戶請儘速升級為iOS 16.2以上版本
避免收到iMessage詐騙訊息
刑事警察局
165 Anti-fraud Hotline Service

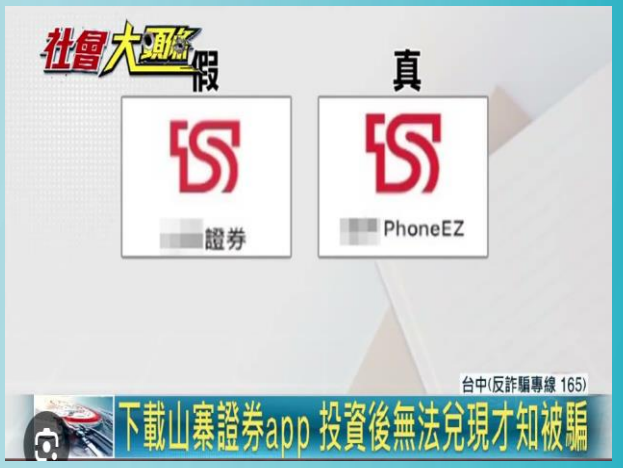
通訊軟體詐騙


19:52
今天 19:30
週一通知買入（1453
大將）盤中亮燈，連
AI新型態詐騙
晚間新聞
PTS EVENING NEWS
可疑連結別亂點 通訊軟體常見4大詐騙招數

假「證券App」詐騙！

一個假投資詐欺集團去年大肆散發投資獲利高的簡訊，再假冒台新銀行理財專員，慫恿被害人下載假的「台新證券App」，已知至少廿人受騙、失金二千五百萬元；警方從去年底至上月，陸續逮捕有三條詐欺案被通緝的曹姓主嫌與廿一名共犯，依詐欺等罪送辦。

2023/04/15 自由時報



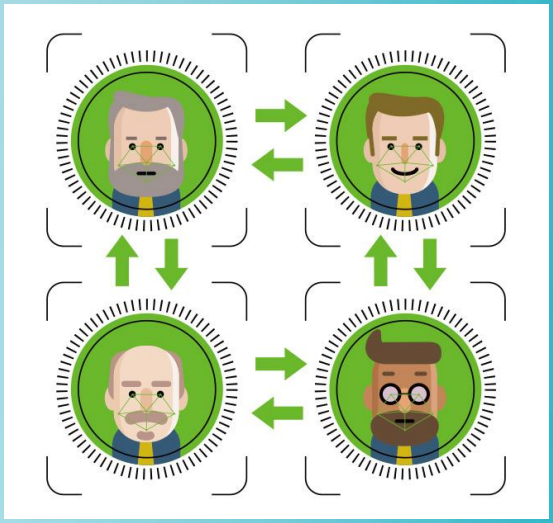
詐騙集團成員告知朋友自己是凱基信託的一級帳戶，是主力專門使用的，能夠增加抽籤申購的機率、可以在盤後用較低價格買進股票，還能夠借券後立刻賣出，功能讓朋友聽得十分心動，於是下載來使用。

2023/01/20 ETtoday財經雲

《Deepfake深偽技術》是什麼？

深偽技術（Deepfake）又稱深度偽造，是英文「deep learning」（深度學習）和「fake」（偽造）的混成詞，專指基於人工智慧的人體圖像合成技術或聲音的應用。

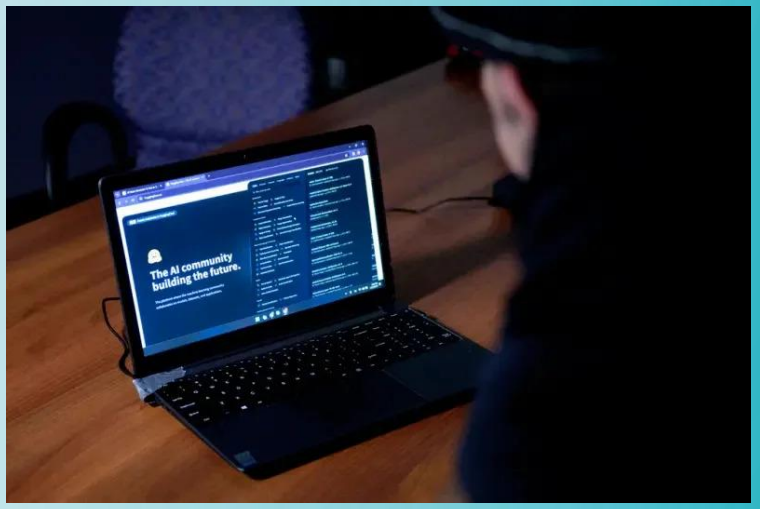
AI深偽（Deepfake）變臉技術，可以製造出逼真的虛假影像和聲音，仿真度極高，AI變臉軟體還內建許多來自不同人種的臉部圖片，甚至連名人、明星照片也有，且使用者可自由選擇性別及種族。



Deepfake假冒公司老闆！騙過員工得手1640萬

這起詐騙案發生在本月20日，一間總部位在英國的香港分公司，一位女員工在WhatsApp收到詐騙集團訊息，詐騙集團謊稱是人在英國的老闆，並且冒用了真正老闆的頭像照片，女員工不疑有他，對方於是要求隔天進行視訊會議。

而在會議上，詐騙集團透過Deepfake技術，偽造老闆的影像與聲音，向女員工發出指令，以要開設分公司為由，要求女員工將近400萬港幣的款項匯入指定帳戶。由於聲音與外貌都偽造的惟妙惟肖，女員工傻傻上當，匯款後另外向總公司詢問時，才發現受騙。



2024年5月30日　NOWnews 今日新聞


當心有詐
AI深偽科技詐騙
FAKE
深偽技術 高度逼真
影像聲音 皆可偽造
實際案例
李男某日接到總公司長官一通電話，要求3小時內將320萬元匯到指定供應商帳戶，李男聽到長官聲音相當熟悉，便不疑有他，立即派人轉帳，事後等到查帳時，才發現遭到深偽技術變造聲音詐騙。
請轉傳分享共同預防詐騙
臺南市政府警察局關心您

立院三讀 電腦合成深偽影像聲音詐騙最高關7年

為遏止詐騙集團用電腦合成等方法製作不實影像詐欺，立法院會今天三讀修正通過**刑法第339條之4**條文，若以電腦合成或其他科技方法製作不實影像、聲音或電磁紀錄來詐欺，處1年以上7年以下有期徒刑，得併科100萬元以下罰金。

2023/05/16 中央通訊社

第 三十二 章 詐欺背信及重利罪

第 339 條 意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付者，處五年以下有期徒刑、拘役或科或併科五十萬元以下罰金。

以前項方法得財產上不法之利益或使第三人得之者，亦同。

前二項之未遂犯罰之。

第 339-4 條 犯第三百三十九條詐欺罪而有下列情形之一者，處一年以上七年以下有期徒刑，得併科一百萬元以下罰金：

一、冒用政府機關或公務員名義犯之。

二、三人以上共同犯之。

三、以廣播電視、電子通訊、網際網路或其他媒體等傳播工具，對公眾散布而犯之。

四、以電腦合成或其他科技方法製作關於他人不實影像、聲音或電磁紀錄之方法犯之。

前項之未遂犯罰之。

社交工程手法

偽裝維護人員、
上級單位人員，
騙取帳號及密碼。

利用工具軟體、
檔案、圖片誘騙
下載，乘機
植入惡意程式，
暗中收集
機敏性資料。

利用電話
佯裝資訊人員，
騙取帳號及
密碼。

利用電子郵件
誘騙開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料。

利用電子郵件
誘騙使用者
登入偽裝網站，
騙取帳號及
密碼。

利用通訊軟體，偽裝親友來訊，誘騙點選連結後，植入惡意程式。

社交工程會造成什麼影響？

遭到詐騙，金錢損失。

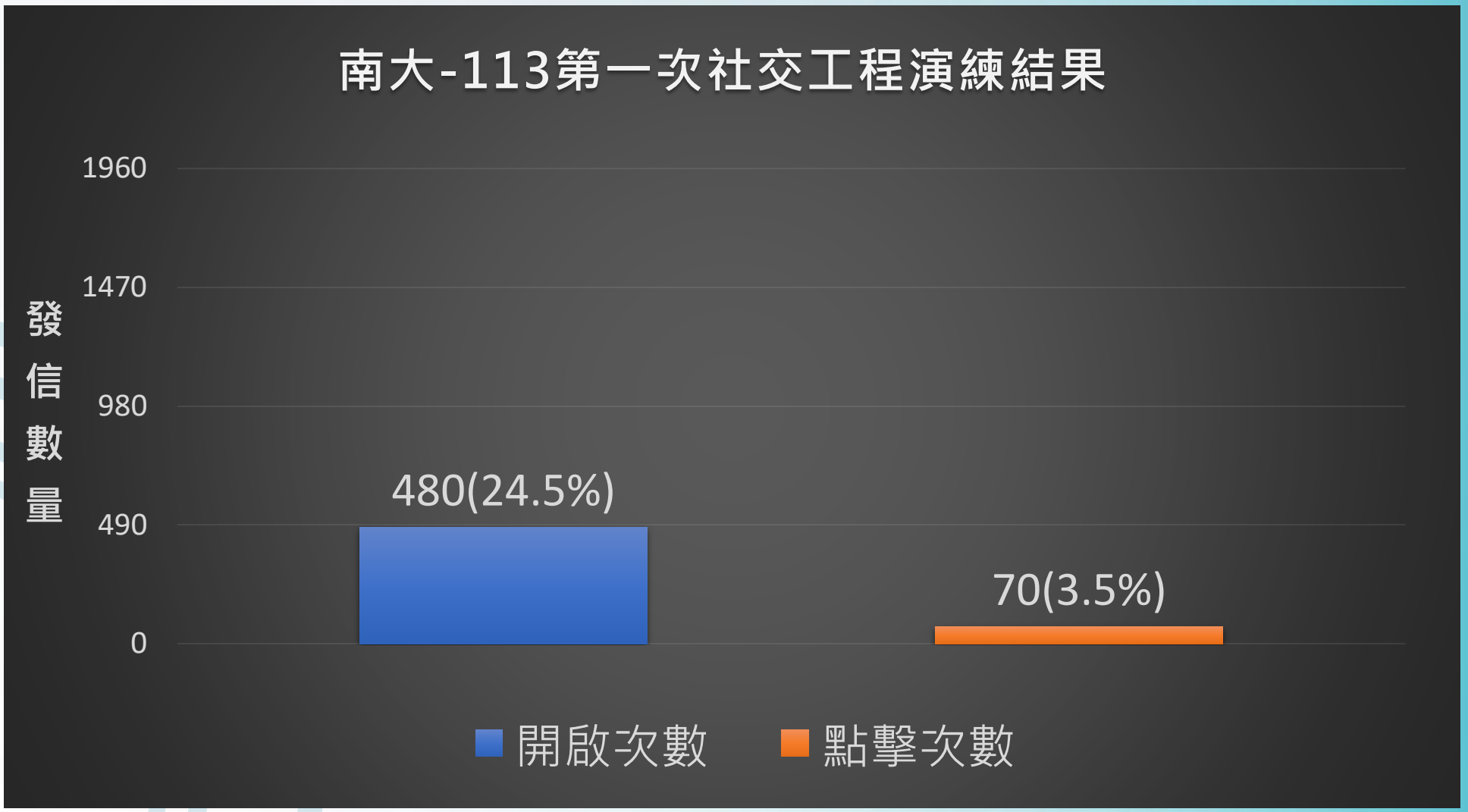
造成資料損失及癱瘓系統、產線停擺。

機敏資料外洩。

挖礦病毒挖走設備資源。

僵屍網路，攻擊打手。

社交工程演練-執行狀況


南大-113第一次社交工程演練結果
1960
1470
980
490
0
發信數量
480(24.5%)
70(3.5%)
開啟次數
點擊次數

社交工程演練-執行結論

- 本次電子郵件社交工程檢測發現，測試人員490人，總發信數為1960封信，共計有480次開啟信件的紀錄，若以人數統計，共有209人曾開啟信件。
- 依比例來看約有42.65%(209/490)的人員曾開啟了測試信件，該比例稍高，建議可定期安排社交工程演練，宣導資安意識，加強人員資安意識訓練，以避免未來的社交工程攻擊。

如何防範社交工程？

社交工程防範措施

1. 提高警惕

a. 來自陌生人不請自來的訊息。
b. 內容看似十分緊急，需要你馬上處理。
c. 要求你點擊連結或開啟附件。
d. 內文包含許多拼寫錯誤或文法錯誤。
e. 對方試圖從你那裡獲取個人資訊。
f. 對話時帶著強烈的緊迫感或攻擊性。
g. 不要輕易使用未授權的軟體。
h. 釣魚網站模仿功力幾可亂真，瀏覽時務必小心檢查網址。

2. 強化密碼安全

a. 首次獲得臨時密碼時,立即更改為自行設定的複雜密碼,避免密碼在傳輸過程中遭竊取。
b. 不要將密碼直接書寫或儲存在電腦文件中。
c. 避免使用自動登入功能。
d. 不同系統和應用程式應使用獨立的複雜密碼,避免重複使用。
e. 一旦發現密碼外洩徵兆,應立即通報並重設所有相關密碼。
f. 定期更換密碼,增加被盜用時的防護力。

3. 多因素身份驗證


多因素身份驗證
密碼
圖形鎖
手勢
What you know
自己的設備
NFC 卡片
穿戴裝置
What you have
臉部辨識
聲音辨識
指紋辨識
Who you are
地理位置
網路行為
擊鍵模式
What you do
Sorry, try again
User name:
john_smith
Password:
PASSCODE:
"Hello Knomi, please verify my identity."

4.定期更新作業系統和軟體

4.定期更新作業系統和軟體

5. 使用安全防護工具

安裝防毒軟體、防火牆等安全防護工具，能夠有效地檢測和阻止惡意軟體的傳播，提高系統的安全性。

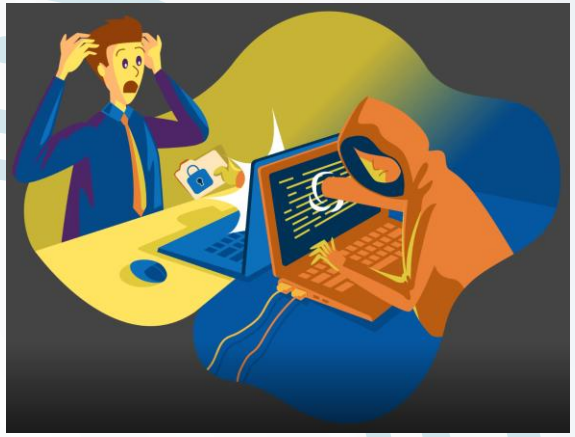
6. 教育訓練

定期舉辦資安教育訓練。

定期\不定期舉行社交工程演練。

人心最堅強也最脆弱，

當駭客抓準你的脆弱點的時候，



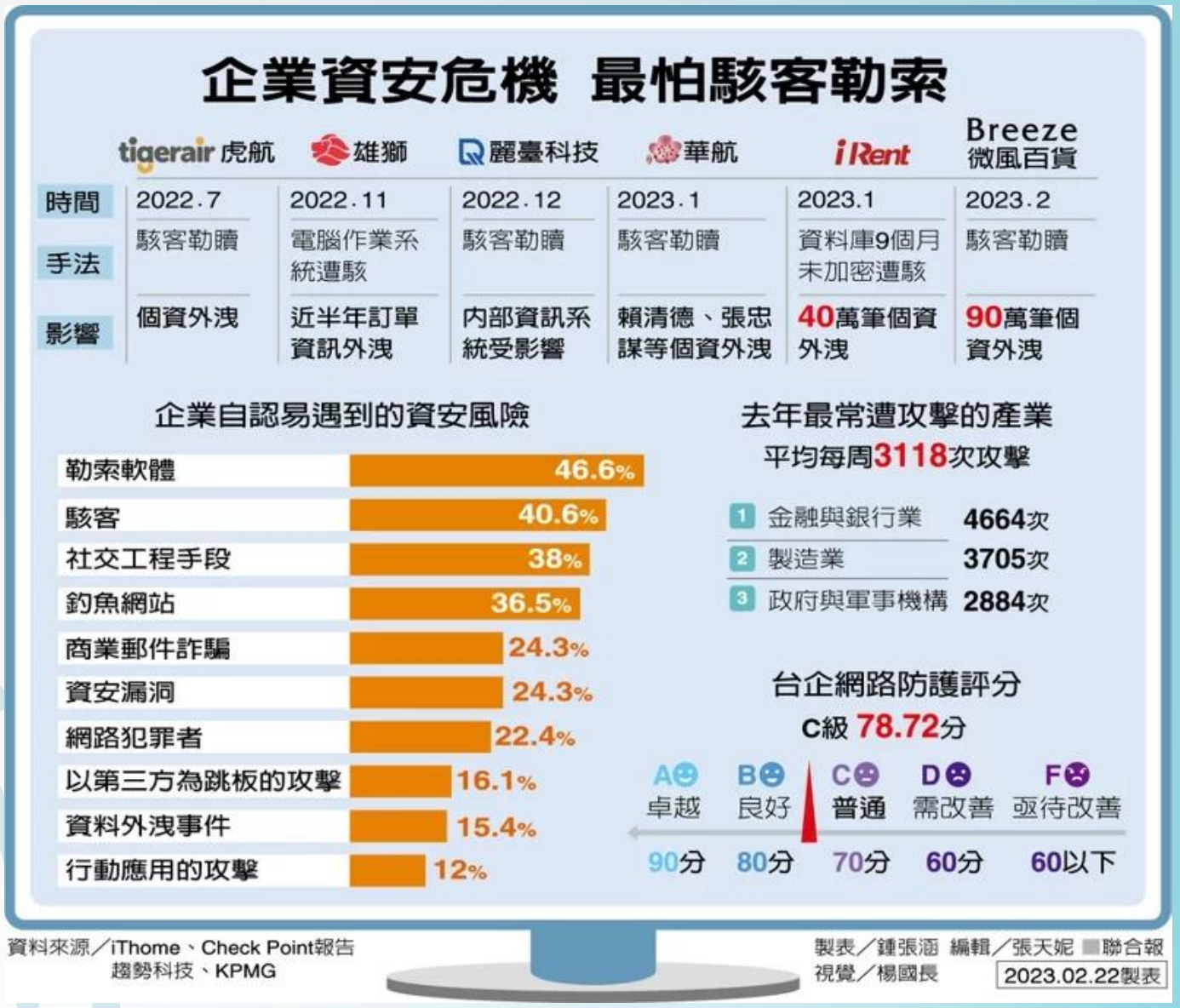
就是最容易騙到你的時刻！

- **如何保護資訊資產並防止駭客攻擊**
- 社交工程攻擊與防範
- **勒索病毒攻擊與防範**
- 行動裝置資安防護

勒索病毒(ransomware)

係一種阻斷存取式攻擊（denial-of-access attack），透過對使用者之資料加密行為，讓受害者無法正常存取欲使用的資料，進而勒索錢財，達成攻擊之目的。

十全果菜市場中勒索病毒 付1200美元贖金


企業資安危機 最怕駭客勒索
tigerair 虎航
雄獅
麗臺科技
華航
iRent
Breeze 微風百貨
時間
手法
影響
2022.7
駭客勒贖
個資外洩
2022.11
電腦作業系統遭駭
近半年訂單資訊外洩
2022.12
駭客勒贖
內部資訊系統受影響
2023.1
駭客勒贖
賴清德、張忠謀等個資外洩
2023.1
資料庫9個月未加密遭駭
40萬筆個資外洩
2023.2
駭客勒贖
90萬筆個資外洩
企業自認易遇到的資安風險
勒索軟體 46.6%
駭客 40.6%
社交工程手段 38%
釣魚網站 36.5%
商業郵件詐騙 24.3%
資安漏洞 24.3%
網路犯罪者 22.4%
以第三方為跳板的攻擊 16.1%
資料外洩事件 15.4%
行動應用的攻擊 12%
去年最常遭攻擊的產業
平均每周3118次攻擊
1 金融與銀行業 4664次
2 製造業 3705次
3 政府與軍事機構 2884次
台企網路防護評分
C級 78.72分
A 卓越 90分
B 良好 80分
C 普通 70分
D 需改善 60分
F 亟待改善 60以下
資料來源／iThome、Check Point報告
趨勢科技、KPMG
製表／鍾張涵 編輯／張天妮 聯合報
視覺／楊國長
2023.02.22製表

常見勒索病毒入侵手段

釣魚信件

- 利用社交工程技巧，誘使受害者自主點擊惡意連結或附件。
- 如偽裝成可信賴寄件人或企業，向受害者發送釣魚郵件，讓受害者降低戒心，幫助勒索病毒進入系統。

不安全的連結

- 駭客會在網路上散佈惡意網站或放置病毒連結的方式，當使用者不小心點入，勒索病毒就會透過程式碼傳送至受害者的系統中。

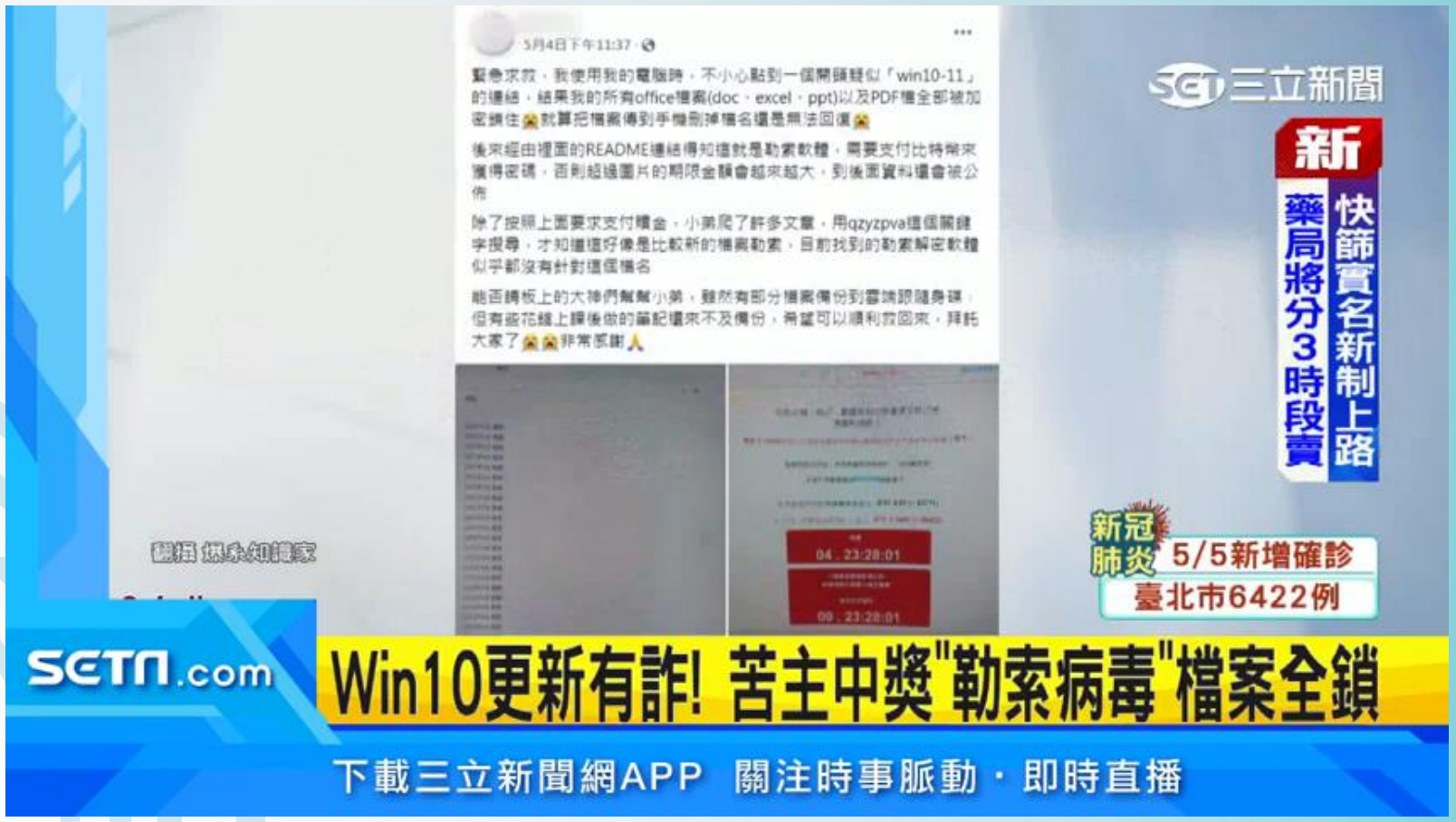
惡意檔案

- 駭客會將勒索病毒隱藏在看似無害的檔案中，例如壓縮檔、執行檔或各類文檔。
- 當受害者下載並執行這些檔案時，勒索病毒就會被釋放。

漏洞

- 透過已知的系統或軟體漏洞，針對受害者的弱點進行入侵，並在受害者的系統中安裝勒索病毒。

Win10更新有詐！苦主中獎「勒索病毒」檔案全鎖




Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
Chinese (traditional)
我的電腦出了什麼問題？
您的一些重要文件被我加密保存了。
照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因此不能正常打開。
這和一般文件損壞有本質上的區別。您大可在網上找找恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。
有沒有恢復這些文檔的方法？
當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的恢復服務。
但這是收費的，也不能無限期的推遲。
請點擊 <Decrypt> 按鈕，就可以免費恢復一些文檔。請您放心，我是絕不會騙你的。
但想要恢復全部文檔，需要付款點費用。
是否隨時都可以固定金額付款，就會恢復的嗎，當然
對你不利。
最好3天之內付款費用，過了三天費用就會翻倍。
還有，一個禮拜之內未付款，將會永遠恢復不了。
對了，忘了告訴你，對半年以上沒錢付款的窮人，會
Payment will be raised on
5/15/2017 23:41:55
Time Left
02:23:55:59
Your files will be lost on
5/19/2017 23:41:55
Time Left
06:23:55:59
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to th
12t9YDPgwueZ9NyMgw519p7A
Check Payment
Trick or Bitcoin
：
不給錢，
就刪檔！

社交工程造成的危害

資料外洩

電腦無法使用

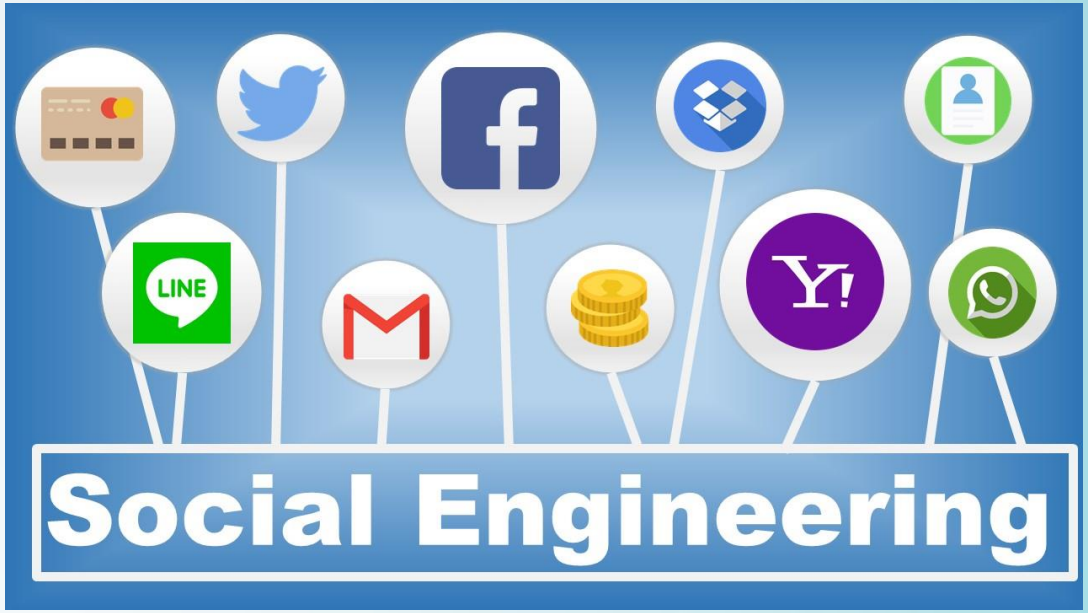
金錢損失


遇到
勒索病毒
攻擊怎麼辦?
4步緊急處理方式

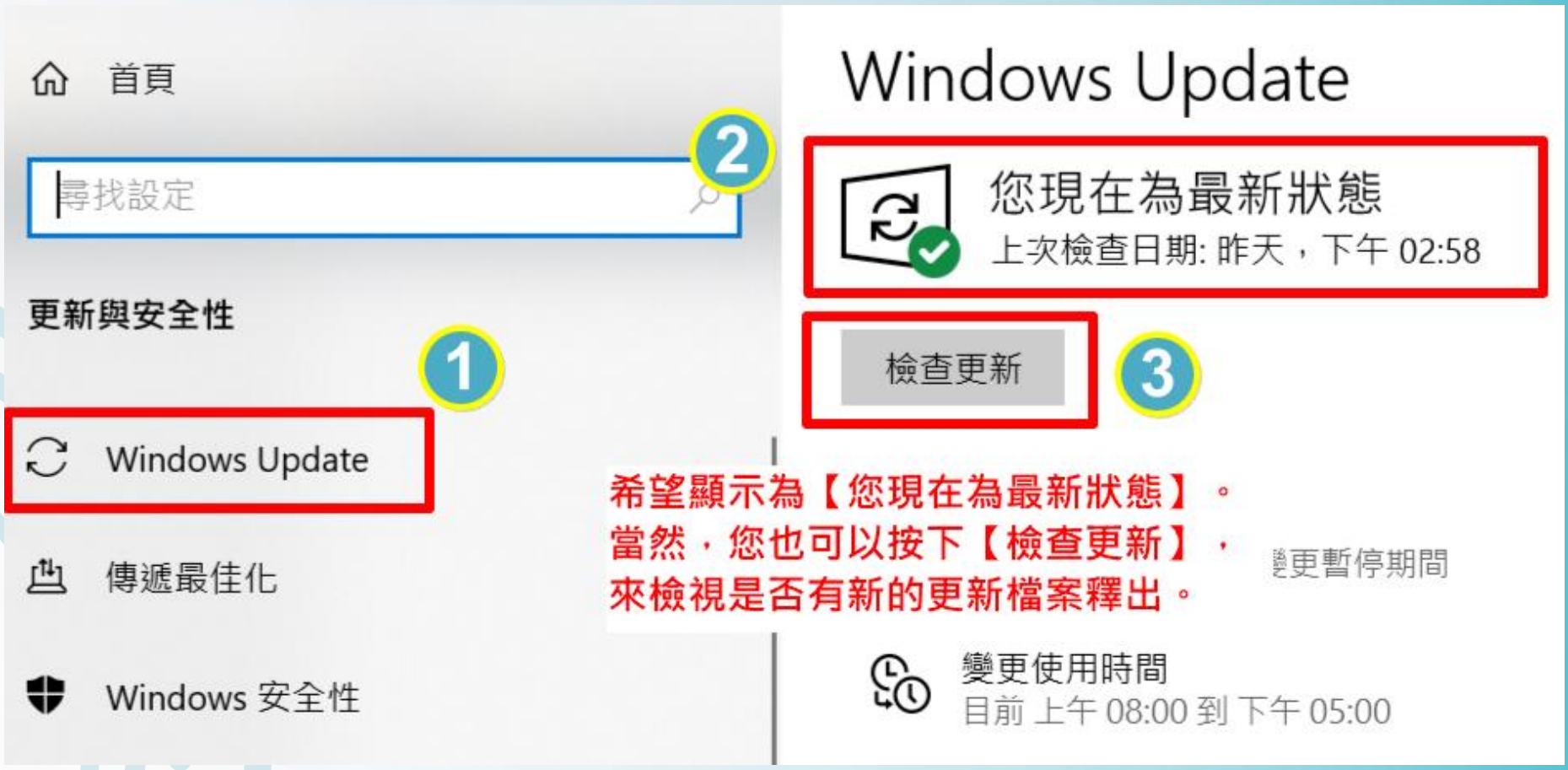
流程	說明
中斷網路連線	避免勒索軟體持續與C&C Server溝通，不致於使災情擴大
即刻發現，馬上關機	取出硬碟，以外接的方式將未加密的檔案保存下來，切記勿再點選已被加密之檔案
評估災情	了解是感染哪種類型的勒索軟體，已有廠商提供解密工具，或許能將檔案救回
系統重灌	將受感染之電腦重灌，並將所有應用程式與防毒軟體更新到最新的狀態

防範五大措施

1. 不開啟非公務相關電子郵件，簡訊或各類即時通訊軟體 (包含Line與FB Messenger等)之內容請小心查證，不點擊不明附件檔及網頁連結，不執行來路不明檔案。



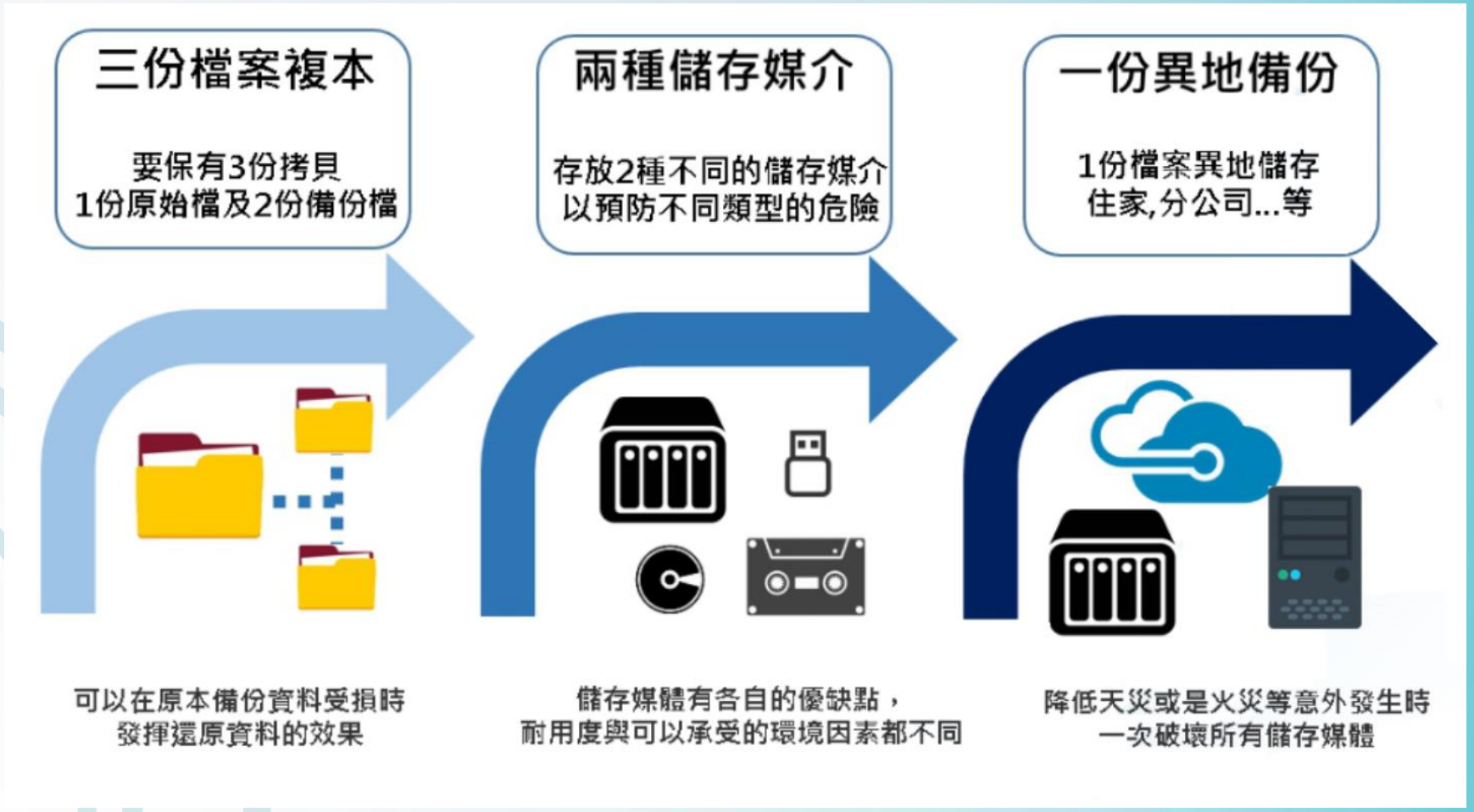
2. 定期進行系統更新


首頁
尋找設定
更新與安全性
Windows Update
傳遞最佳化
Windows 安全性
Windows Update
您現在為最新狀態
上次檢查日期: 昨天，下午 02:58
檢查更新
1
2
3
希望顯示為【您現在為最新狀態】。
當然，您也可以按下【檢查更新】，
來檢視是否有新的更新檔案釋出。
更暫停期間
變更使用時間
目前 上午 08:00 到 下午 05:00

3. 安裝防毒軟體並應更新至最新病毒碼

4. 做好備份作業

321 備份法則



5. 勿妥協交付贖款

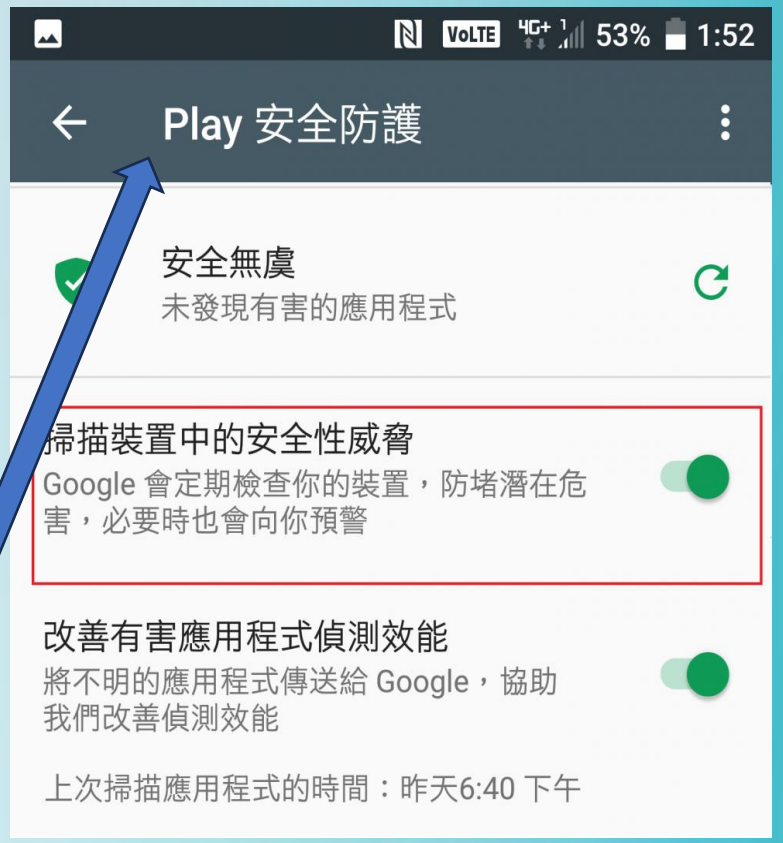
如何保護資訊資產並防止駭客攻擊

- 社交工程攻擊與防範
- 勒索病毒攻擊與防範
- 行動裝置資安防護

安卓系統安全設定-避免安裝惡意軟體

PLAY商店

PLAY安全防護



安卓系統安全設定-非PLAY商店APP不安裝

設定

安全性

未知的來源

安卓系統安全設定-避免安裝惡意軟體

設定

鎖定螢幕

安卓系統安全設定-購物設定

PLAY商店

設定

通過驗證後才能購物

iOS系統安全設定-密碼跟Face ID(或 Touch ID)

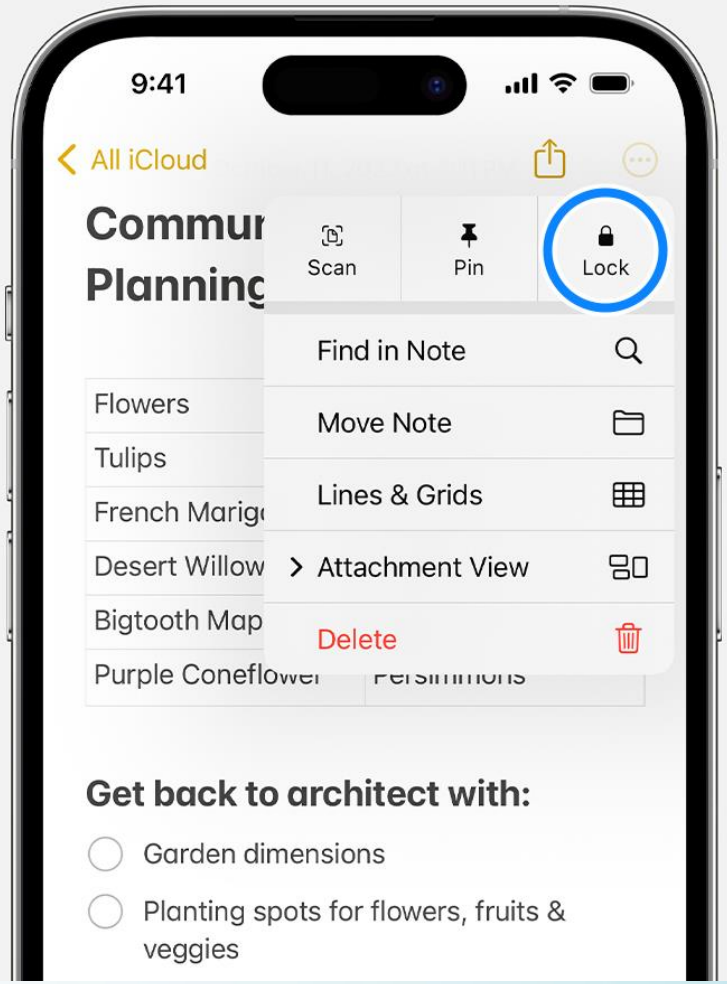
設定

Face ID與密碼

iOS系統安全設定-密碼跟Face ID(或 Touch ID)

項目	Apple ID	Face ID	Touch ID
功能	可存取所有Apple ID服務帳戶	透過前置鏡頭即可解鎖臉部	透過系統儲存的指紋辨識用戶身分
設定方式	於初始設定、App Store、Mac、網頁瀏覽器設定	於設定中供感應器掃描2次	將手指放在Home鍵上，讓系統新增指紋
注意事項	Touch ID/Face ID過於方便，容易忘記Apple ID密碼	若機體遭撞擊原深感測鏡頭可能無法啟動解鎖	若機體及手指上有油汙或水分，需清潔後感應

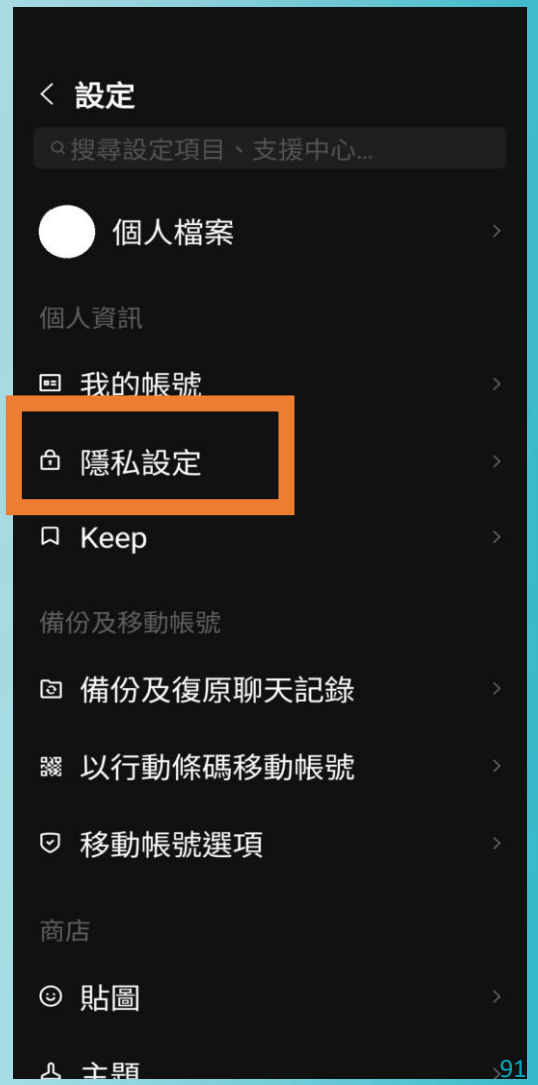
iOS系統安全設定-備忘錄上鎖



LINE安全設定

LINE–加強LINE隱私設定：防止陌生訊息

- 打開 LINE App ，點選右上角「設定」圖示，進入 LINE 設定頁面
- 點選擇「**隱私設定**」，將「阻擋訊息」開啟，能避免會收到陌生訊息，



LINE–開啟點對點訊息保護（Letter Sealing）

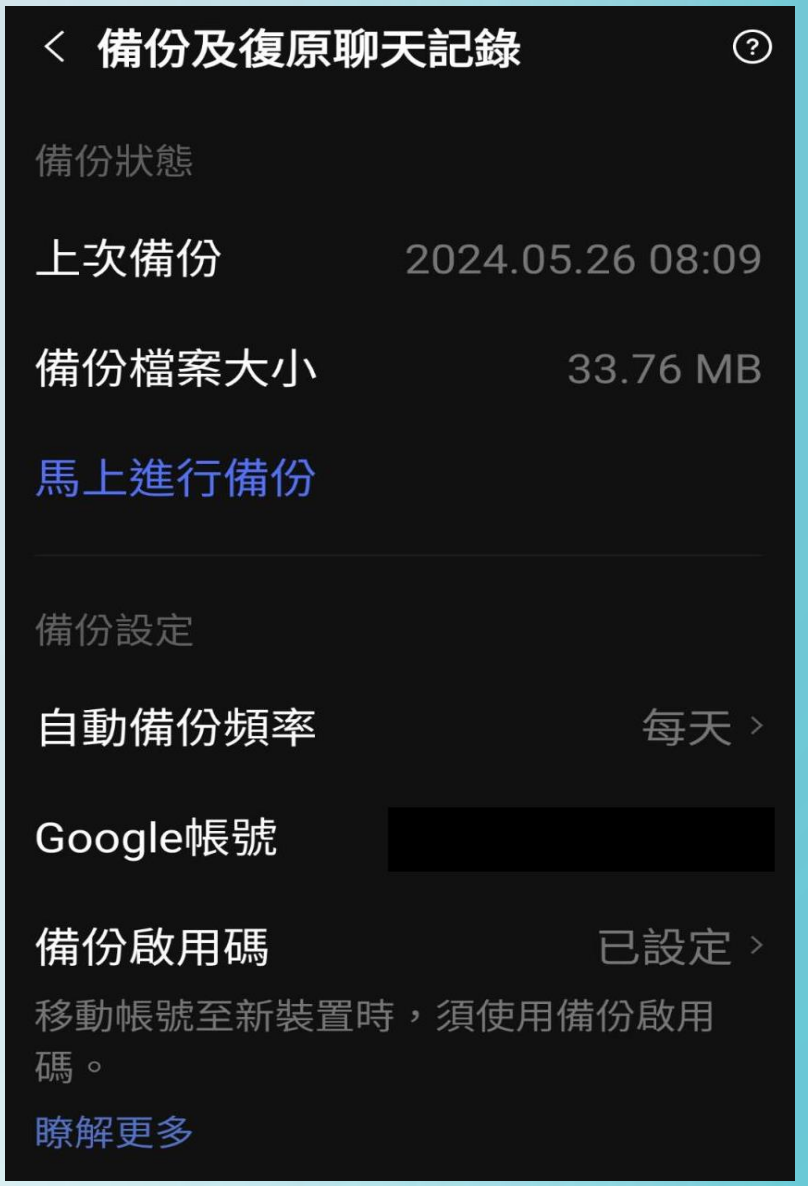
開啟聊天訊息點對點加密「訊息保護（Letter Sealing）」，可替「**文字對話（單人 / 50人群組）、位置訊息和通話**」加密

LINE–帳號安全基本設定

在「**好友**」設定頁面中，可以先將「**自動加入好友**」和「**允許被加入好友**」全部關閉，能有效防止陌生人或廣告帳號隨意加入好友

LINE–聊天對話定期備份

打開「**LINE自動備份**」功能，避免會忘記備份。設定位置在LINE「設定」>「聊天」>「備份聊天記錄」



LINE–開啟密碼鎖定

LINE 密碼鎖設定，可以透過 LINE「設定」>「隱私設定」開啟「密碼鎖定」，後續打開 LINE App 就會要求輸入解鎖密碼，另外也可以搭配 Face ID 或 Touch ID 來使用。

LINE–確認登入中的裝置

如果懷疑自己的 LINE 帳號是不是有被其他裝置偷偷登入，想要確認有哪些裝置登入過，可以透過 LINE「**設定**」>「**我的帳號**」>「**登入中的裝置**」，就可以**查詢所有 LINE 帳號登入過的紀錄**，如發現裝置列表出現一些奇怪的裝置登入，或是登入的IP位置是在國外，那就要點擊裝置右側「登出」按鈕，並且立即更改 LINE 密碼。

LINE–防止其他裝置登入

除了可以查詢登入 LINE 裝置紀錄外，如果想要防止有其他設備會突然登入，平時可能只會用手機來登入 LINE ，就建議將 LINE「設定」>「我的帳號」並且將「**允許自其他裝置登入**」關閉，就能提升 LINE 帳號安全性。

行動裝置安全防護

竊取資訊的APP

- 手機安裝APP，注意開發商的背景是否可疑？
- 使用者評價為何？
- 要求操作權限？

偽裝通知的簡訊

- 簡訊通知內容，若帶有URL網址，要求點擊，要特別注意偽冒網站與下載檔案。

偽裝登入的網站

- 不論電子郵件或是簡訊，其中帶有登入網址的要求或是登入網頁，
  都是危險釣魚網站訊息。

行動裝置安全防護

偽裝感染病毒或中獎的網頁

- 網頁出現類似訊息的畫面，可能是惡意詐騙網站，請勿點擊或下載安裝APP的按鍵。
  並儘速離開這個網站。

假新聞與假帳號

- 不論是FB臉書或是LINE社群避免陌生帳號加入自己的社群帳號，是自我防衛的最佳方式之一。
  同時，不要轉傳來路不明的圖片或新聞，以免陷入假新聞風暴。

- 個人資料與認識與保護
- 個資法介紹與案例分享
- 學校使用資通系統或服務蒐集及使用個人資料注意事項

個人資料保護法(個資法)

個人資料保護法第1條開宗明義

「為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，

並促進個人資料之合理利用，特制定本法。」

個資法對於人權的保障，有兩個重要的觀念：

保障人格權、隱私權

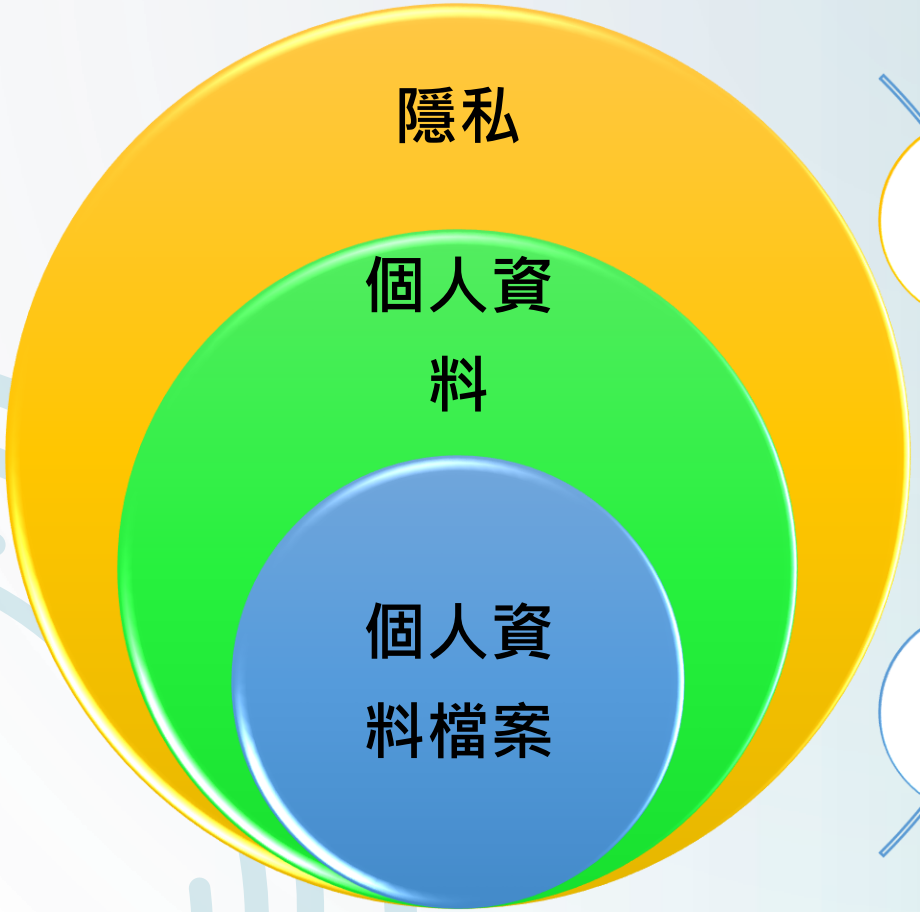
美國大法官Louis Brandeis的一句隱私權名言：
「人民有獨處不被干擾的權利。（The Right To Be Alone.）」

個人資料自主決定權

每個人都有權利決定是否要揭露其個人資料，允許其個人資料被何人使用，如何被使用，在哪一段時間使用其個人資料等等。

因此當你要利用他人的個資時，亦要等同對待，充分告知當事人其個資被運用的資訊。

隱私保護與個資保護之關聯



- 隱私:私生活不被隨意公開的自由
- 個人資料(PII)：足以識別個人的特定資料
- 個人資料檔案：集合個人特定資料的媒體檔案

個人資料是什麼？


小明
聯絡資訊
地址
小明社區100號
生日
1983/10/17
電話
+88612345678
email
email@email.com

個人資料(自然人的以下資料)

個人資料保護法施行細則 第4條

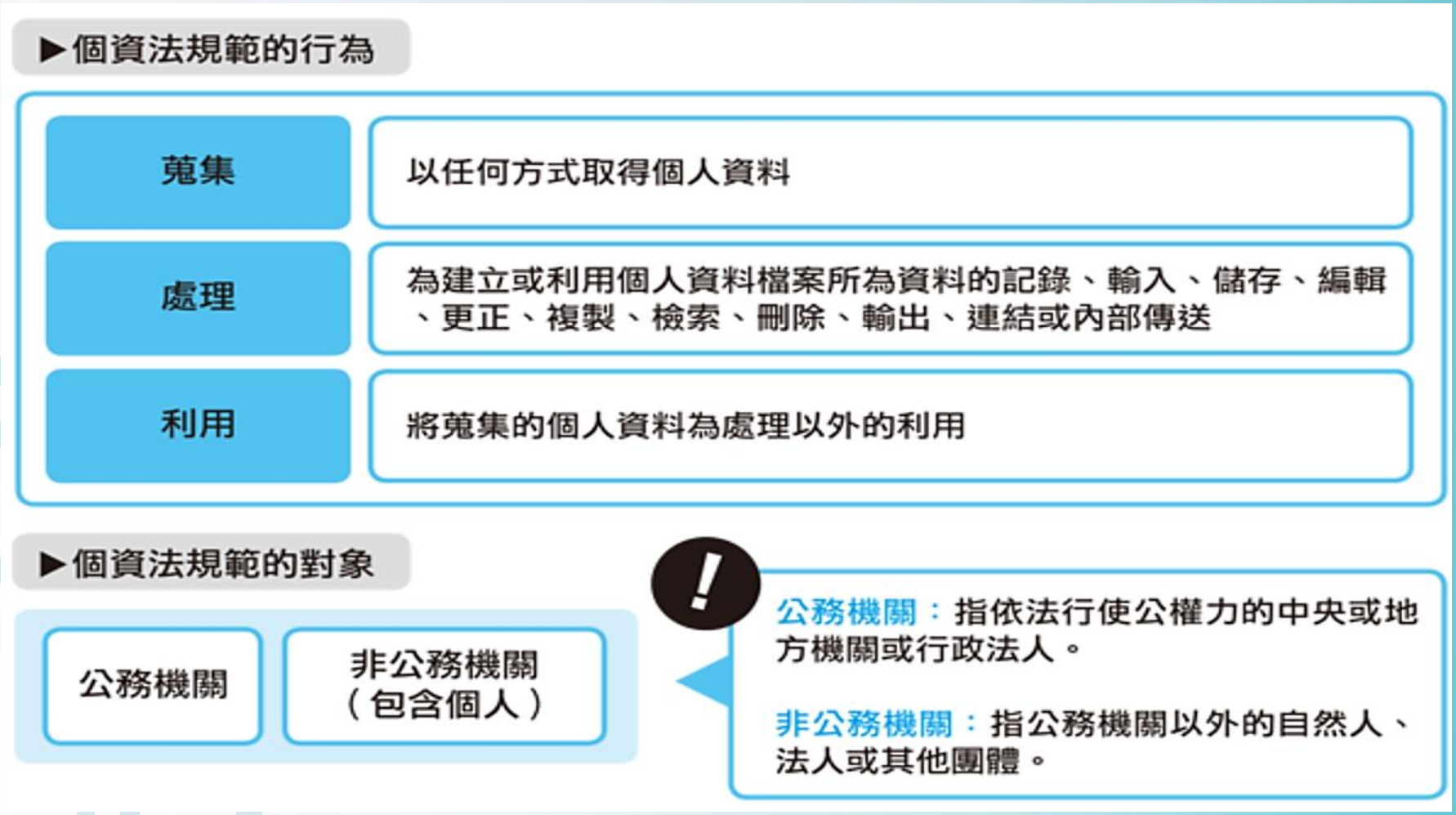
病歷	• 指醫療法第六十七條第二項所列之各款資料
醫療	• 指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由， 所為之診察及治療
基因	• 指由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息
性生活	• 指性取向或性慣行之個人資料
健康檢查	• 指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料
犯罪前科	• 指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄

何謂可間接識別之個人資料？

個資法施行細則 第3條

針對間接方式識別之定義為僅以該資料不能識別，須與其他資料**對照、組合、連結**等，始能識別該特定個人者。

個資法規範的對象與行為



蒐集個人資料的告知義務

向當事人蒐集個人資料時，必須明確告知當事人，法定告知事項：

1. 蒐集者的名稱（公務機關或非公務機關的名稱）
2. 蒐集的目的
3. 個人資料的類別
4. 個人資料利用的期間、地區、對象及方式
5. 個資當事人擁有的權利：查詢、請求閱覽、製給複製本、補充、更正、「停止蒐集、處理或利用」、刪除。
6. 當事人得自由選擇提供個人資料時，不提供將對其權益的影響。

告知方式

告知方式不限，只要足以認當事人知悉的方式皆可。

言詞	電話	書面	簡訊
傳真	電子郵件	電子文件	其他方式

個資當事人的權利

▶個資當事人擁有以下權利

1. 查詢或請求閱覽
2. 請求製給複製本
3. 請求補充或更正
4. 請求停止蒐集、處理或利用
5. 請求刪除

不得預先拋棄或以特約限制

▶可拒絕當事人行使權利的情形

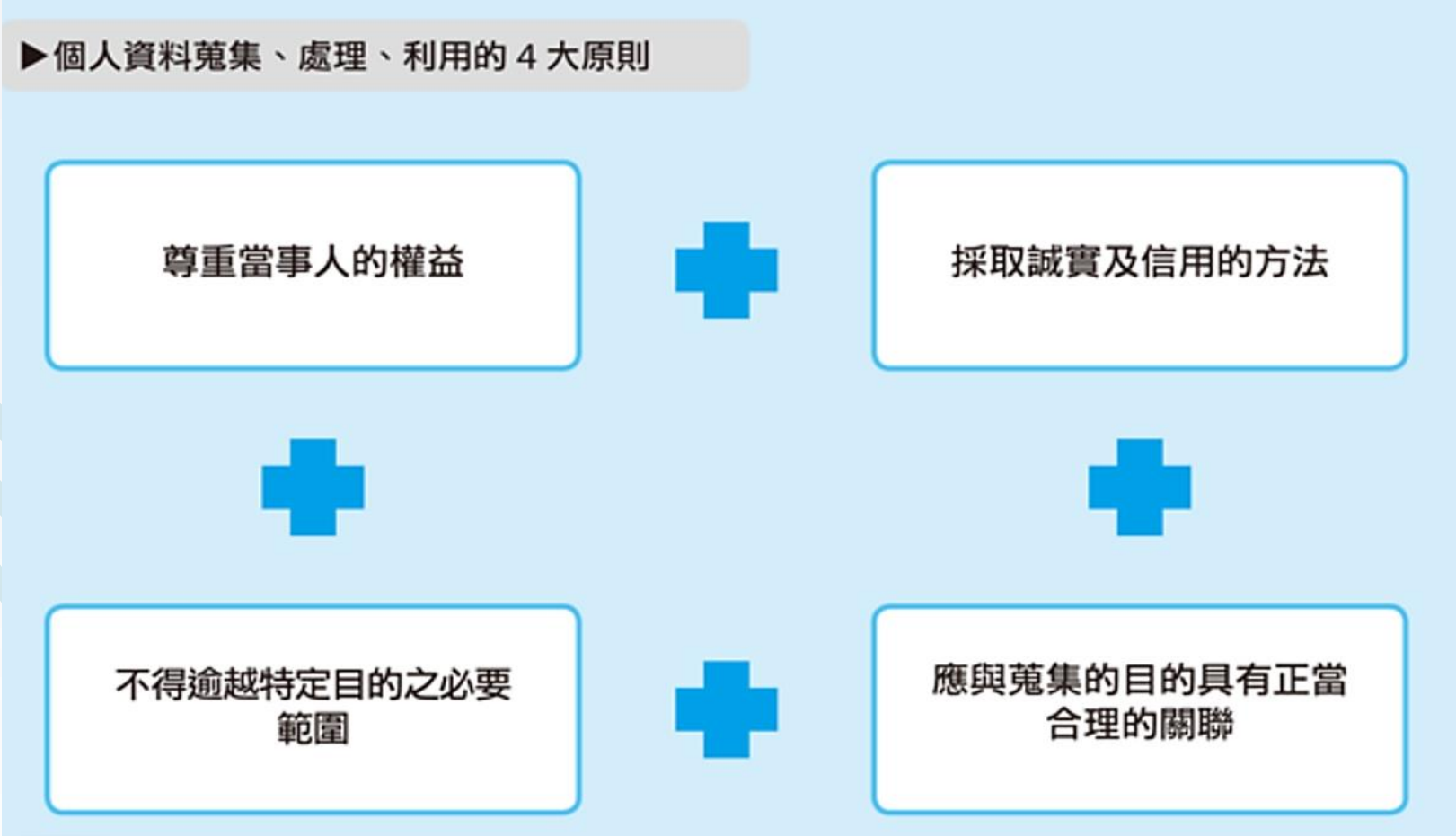
可拒絕查詢、提供閱覽或製給複製本的情形：

1. 妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。
2. 妨害公務機關執行法定職務
3. 妨害該蒐集機關或第三人的重大利益

個人資料正確性有爭議時，可拒絕當事人請求停止處理或利用的情形：

1. 執行職務或業務所必需
2. 經當事人書面同意

個人資料蒐集、處理、利用的原則



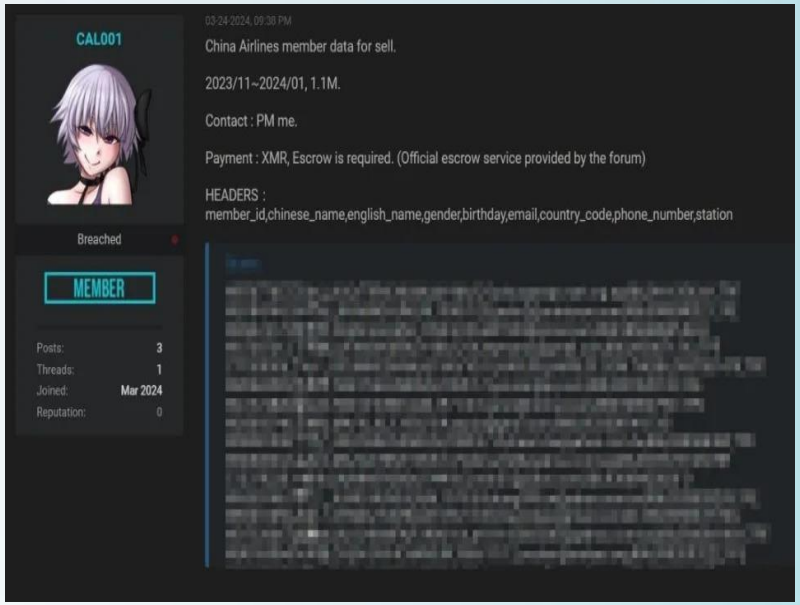
請問以下四種資料，哪一種是《個人資料保護法》保護的個人資料？

台馬個資外洩嚴重 估1040萬國人手機號碼流出

2023年1月駭客於國外論壇公開華航會員資料

又遭駭？上百萬會員個資「暗網外流」 華航回應了

今年3月24日，駭客在暗網上曝光100多筆個資內容，其中包含會員編號、中英文姓名、性別、出生年月日、電子信箱、手機號碼與國碼，同時宣稱：「這次將出售2023年11月至2024年1月期間，高達110萬筆個資。」以此勒索華航總部。



2024/03/26聯合新聞網

門戶大開代表：iRent、Line Pay

1. 資安措施若未完善，防禦效果近似於無？iRent就是打開自家大門的代表性例子，其**暫存資料庫未妥善阻擋外部連線**，造成外人可以隨意登入查詢的防護性缺口，客戶個資形同攤在網路世界的陽光之下，無所遁形。

台視新聞網
iRent遭重罰20萬！ 個資外洩40萬筆「改正未...

2. Line Pay也在2021年9月，誤將台灣用戶的**行銷活動資料上傳至GitHub**，察覺不對勁時已有外部瀏覽紀錄，估計損及逾7萬人的權益。

台視新聞網
Line Pay爆交易個資外洩台灣、泰國、日...

駭客入侵代表：微風集團

1. 微風集團在收到**勒索情資**後，第一時間啟動了資安應變措施，清查後也確認所謂的外流資料與內部資料並不完全相同，然而**駭客論壇Breach Forums聲稱竊取資料庫會員機敏資料**，在微風集團消費過的民眾們無不擔心自身個資安全。

網拍釣魚代表：蝦皮、旋轉拍賣

1. 電子商務發展入門門檻較低，但也容易在擴展業務的過程中忽略資安問題，含括商城與個人賣家的蝦皮購物，以及主攻二手物品賣場的旋轉拍賣，都在2023年被駭客鎖定發起釣魚攻擊，盜取大量個資。
2. 其中蝦皮更在高風險賣場之排名中打敗其他電商品牌，躍為首位，後因資安防護措施未改善而遭罰20萬元。

接到詐騙代表：誠品、博客來

1. 民眾在誠品生活購買書籍後，直接接到詐騙集團來電，引起社會大眾嘩然。行政檢查發現誠品在帳號管理上執行未確實，事後要求提供補充或佐證資料，個資盤點資料仍不完整，且針對委外廠商監督管理未落實執行，因此數位部 依據《個資法》第48條第4款併第50條規定處分，業者併同其負責人罰鍰新台幣10萬元。
2. 同為連鎖書店的博客來也曾在2022年發生駭客入侵事件，經由警方調查發現已洩漏超過3000件個資，更傳出實際財損破億元，損失甚鉅。

違反個資法的罰則

民事責任	⊙每人每一事件可求償 5 百元～ 2 萬元。 ⊙同一件事，最高可求償 2 億元。
刑事責任	⊙最高可處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。 ⊙意圖營利，可加重求處 5 年以下有期徒刑，得併科新臺幣 1 百萬元以下罰金。
行政處罰	⊙最高可處新臺幣 5 萬元以上 50 萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰。

個資外洩可能造成的影響

1. 破解其他使用相同帳密的帳號，造成其他帳號安全風險。
2. 登入網路銀行帳號取款，損失財產。
3. 以被害者名義申辦銀行帳戶或信貸，損害信用評等。
4. 被利用身份進行不法犯罪，可能發展成詐騙、社交工程攻擊等事件，讓被害者陷入法律糾紛。

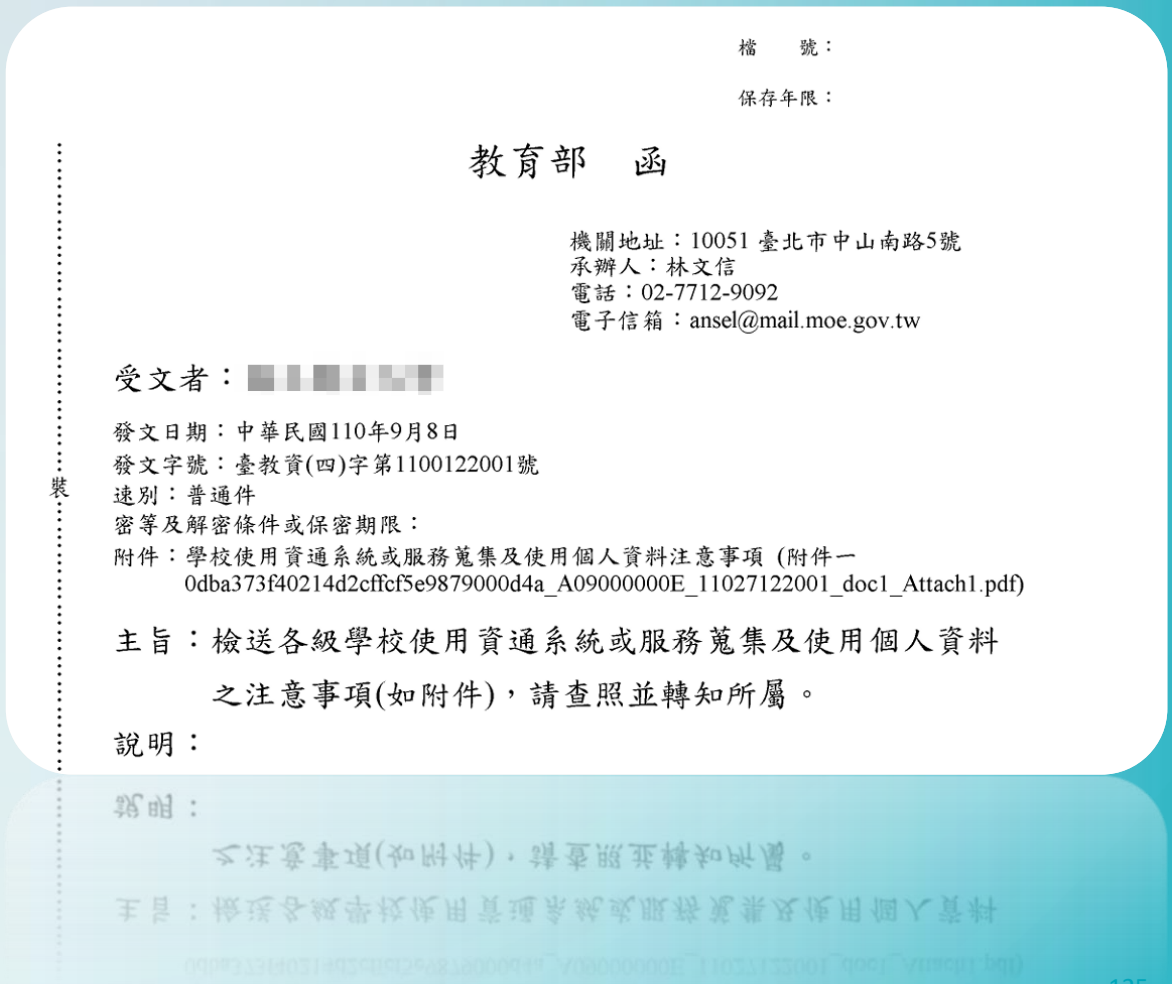
如何妥善保護個人資料

1. 安裝防毒軟體、防間諜及防火牆等保護軟體，定期掃毒並時常更新病毒碼，將安全防護設定盡可能設到最高等級。
2. 使用複雜的密碼，切記勿與個人名字或身份資料相關，避免總是使用同一組密碼，並定期更換密碼。
3. 不要將密碼、或其他能識別個人身分等機密資料張貼於桌面四周或儲存在電腦文件中。
4. 避免透過電子郵件或即時通訊軟體等傳送個人的使用者帳號、密碼、個人資料或其他機密資料。
5. 進行網路線上交易時，使用可信任的電腦，避免使用公用電腦，與無線網路。
6. 確認在可信任的購物網站，並且在有安全保護機制，以https:// 開頭之網址下進行信用卡交易。
7. 不要在不可信任的網站留下個人資料。
8. 在網路上加入會員填寫個人資料時，應詳細閱讀契約內容。
9. 不要將個人隱私資料放在網路上。
10. 不要開啟來路不明的郵件或可疑的附件、檔案等。

- 個人資料與認識與保護
- 個資法介紹與案例分享
- 學校使用資通系統或服務蒐集及使用個人資料注意事項

學校使用資通系統或服務蒐集及使用個人資料注意事項

鑒於學校使用雲端資通服務(如Google表單等)蒐集個人資料時，可能因設定不當而增加個資外洩及資安風險，請各校使用資通系統或雲端資通服務蒐集教職員、學生及家長個人資料者，應注意旨揭事項，以「最小化」為原則，降低風險，並請各校主管機關加強宣導並督導所轄學校。



檔　　號：
保存年限：

教育部　函

機關地址：10051 臺北市中山南路5號
承辦人：林文信
電話：02-7712-9092
電子信箱：ansel@mail.moe.gov.tw

受文者：[redacted]

發文日期：中華民國110年9月8日
發文字號：臺教資(四)字第1100122001號
速別：普通件
密等及解密條件或保密期限：
附件：學校使用資通系統或服務蒐集及使用個人資料注意事項 (附件一 0dba373f40214d2cffcf5e9879000d4a_A09000000E_11027122001_doc1_Attach1.pdf)

主旨：檢送各級學校使用資通系統或服務蒐集及使用個人資料之注意事項(如附件)，請查照並轉知所屬。

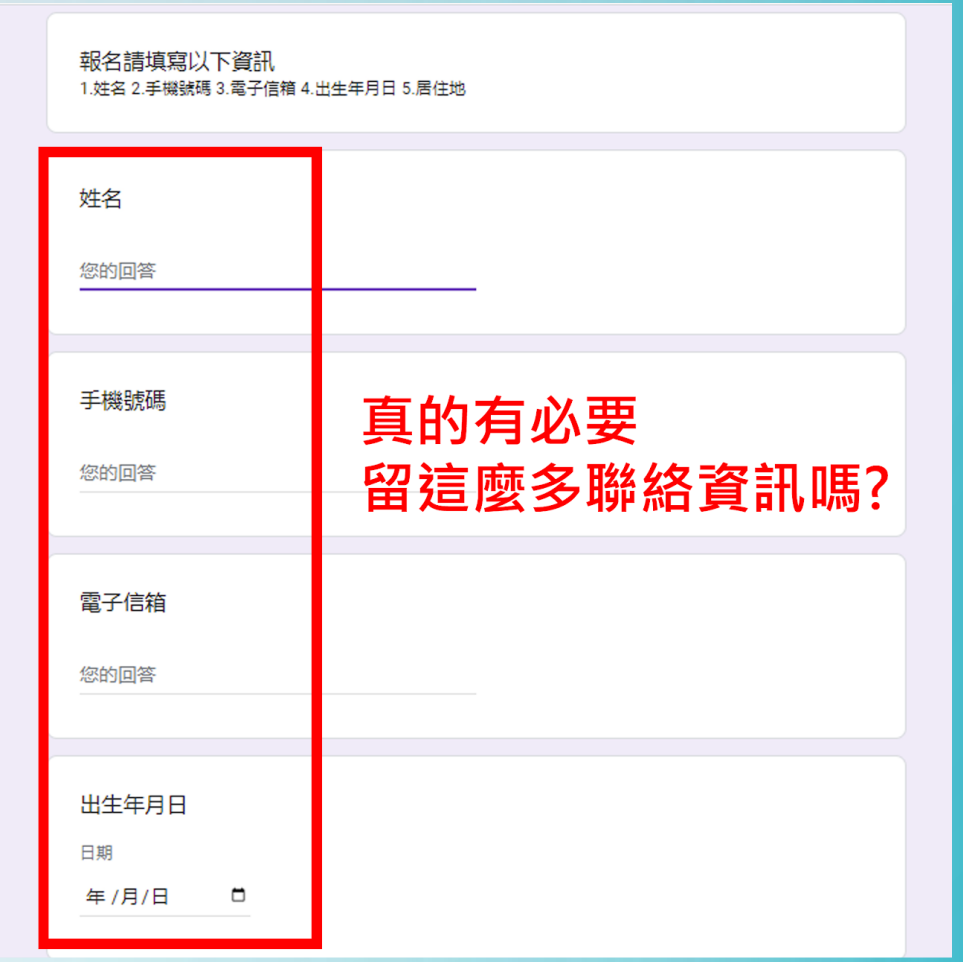
說明：

裝

學校為行政目的使用資通系統或雲端資通服務（如Google表單、Microsoft Forms 等問卷調查服務）涉及蒐集個人資料者，應注意下列事項：

一. 資料蒐集最小化：

僅蒐集適當、相關且限於處理目的所必要之個人資料，處理及利用時，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。



學校為行政目的使用資通系統或雲端資通服務（如Google表單、Microsoft Forms 等問卷調查服務）涉及蒐集個人資料者，應注意下列事項：

二. 存取控制：應注意檔案存取權限設定，應採最小權限原則，僅允許使用者依目的，指派任務所需之最小授權存取。

三. 使用雲端資通服務者，應詳閱設定內容，不宜使用者共同編輯個人資料檔案清冊，並應注意避免設定允許顯示其他使用者作答內容（如Google表單不應勾選「顯示摘要圖表和其他作答內容」），避免使用者能瀏覽其他使用者資料，造成個人資料外洩。公佈前應確實做好相關設定檢查，並實際操作測試，確認無誤後再行發布。

學校為行政目的使用資通系統或雲端資通服務（如Google表單、Microsoft Forms 等問卷調查服務）涉及蒐集個人資料者，應注意下列事項：

四. 傳輸之機密性：網路傳輸應採用網站安全傳輸通訊協定（HTTPS）加密傳輸，並使用TLS 1.2以上版本傳輸。

五. 資料儲存安全：如涉及蒐集個人資料保護法第6條之個人資料或其他敏感個人資料，應以加密方式儲存。

六. 應訂定個人資料保存期限，並於期限或業務終止後將蒐集之個人資料予以刪除或銷毀，避免個人資料外洩。

教職員工在處理個人資料時，應注意以下法規：

一. 個人資料保護法第28條第1項「公務機關違反個人資料保護法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。」

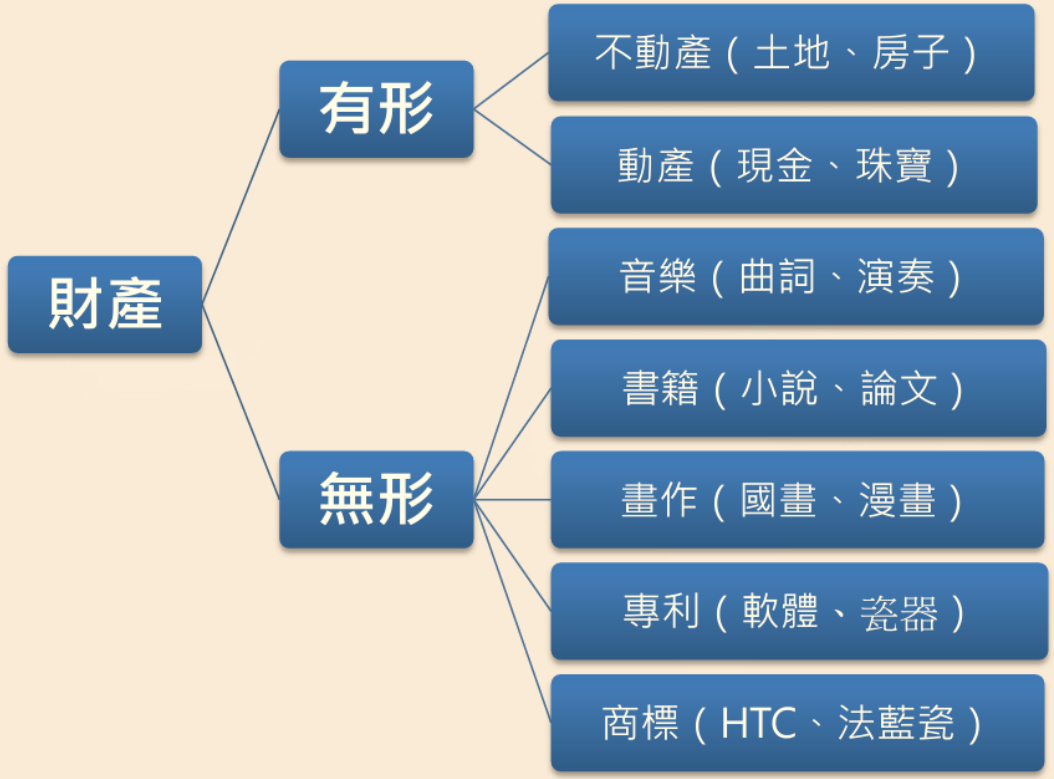
二. 個人資料保護法第41條第1項「違反個人資料保護法有關特種資料的蒐集、處理或利用規定，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。

認識智慧財產權

台灣阿龍抄襲！


TVBS新聞台 HD
更多新聞在這裡
台灣阿龍是山寨! 台文館認:廠商證據造假
掌握新聞脈動 ▶ 訂閱TVBS NEWS頻道

智慧財產



智慧財產，有別於一般的資產，是人類**基於思想進行創作活動**而產生的精神上、智慧上**無形**產物。

何謂智慧財產權

Definition

智慧財產權 (Intellectual Property Rights,簡稱IPR)

是指人類用腦力所創造的智慧產物，此種精神活動的成果，能產生財產上的價值，形成一種權利，而由法律規定保護的制度。

由於智慧創意的提出，使社會或產業達成進步及提升，而造福人群，所以政府為鼓勵並追求人類福祉，而賦予創作者各種特權，作為有效的獎勵及酬勞。

智慧財產權之相關法律


相關法律
保護內容
智慧財產權
專利法
商標法
著作權法
積體電路電路布局保護法
營業秘密法
植物品種及種苗法
發明專利
新型專利
設計專利
商標
標章
著作財產權
製版權
積體電路電路布局
營業秘密
植物品種

智慧財產權的應用

著作權
美術藝術品之創作有美術著作、拍成照片有攝影著作

發明專利
坯體表面密佈短小倒角陶瓷裝飾品的製造方法可申請發明專利

新型專利
陶製品坯體自動澆注之構造可申請新型專利

商標權
商品品牌可申請商標

設計專利
瓷器形狀、花紋及色彩之外觀可申請設計專利

尊重智慧財產權

1. 不使用未經授權之電腦軟體。
2. 不違法下載、拷貝受著作權法保護之著作。
3. 未經著作權人之同意，不可將受保護之著作上傳於公開之網站上。
4. 線上討論區之文章，未經作者同意，不可任意轉載。
5. 架設網站不可提供公眾違法受保護之著作。
6. 其他可能涉及侵害智慧財產權之行為。

喜歡就下載，小心觸法！


Q&A

評量連結

網址：

https://docs.google.com/forms/d/e/1FAIpQLSeyyaVUL1mXW196DGHUn8AmXSyUpy3unZmOYvTvIgDbb8Apww/viewform


THANK
YOU
FOR
YOUR
ATTENTION