



長庚學校財團法人

長庚科技大學

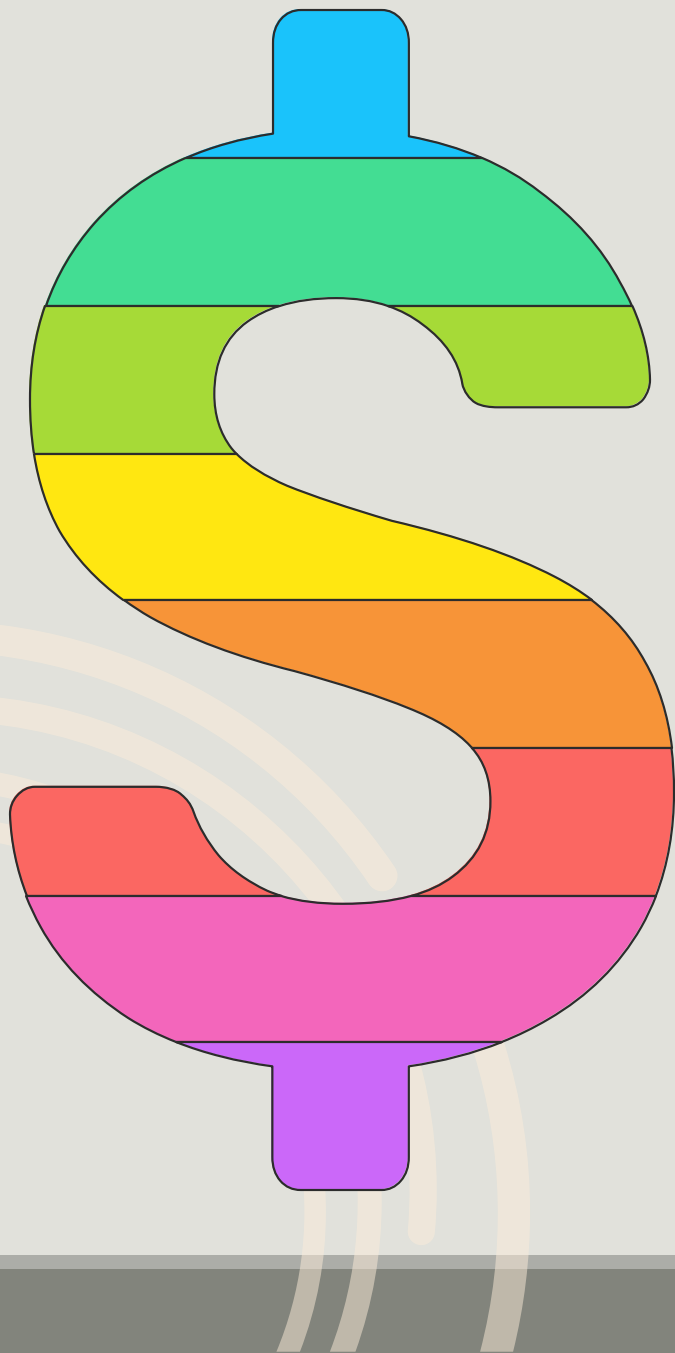
CHANG GUNG UNIVERSITY OF SCIENCE AND TECHNOLOGY

一般人員資安教育訓練

洞悉詐騙，守護數位生活

孫振聲 Jamson





2024-25全球資安事件



日常生活中的資安事件



個人裝置安全設定



社群媒體與通訊軟體風險



智慧家電設定疏忽



AI詐騙手法



資訊安全宣導



個人資料保護法

2024–25全球資安事件



從全球巨觀的角度，看資安



2024-25年全球資安事件

勒索軟體攻擊

惡意軟體加密數據以勒索贖金

臺灣特定事件

針對臺灣的網路威脅

供應鏈滲透

透過供應商入侵系統

AI 驅動的攻擊

使用 AI 進行網路攻擊

國家級駭客

政府贊助的網路間諜活動

零日漏洞

利用未知的軟體缺陷

大規模資料外洩

未經授權訪問大量數據

DDoS 攻擊

壓倒伺服器的流量



日常生活中的資安事件



資安攻擊手法不斷更新

理解趨勢以防範未然



密碼管理

Time it takes a Hacker to Brute Force your password

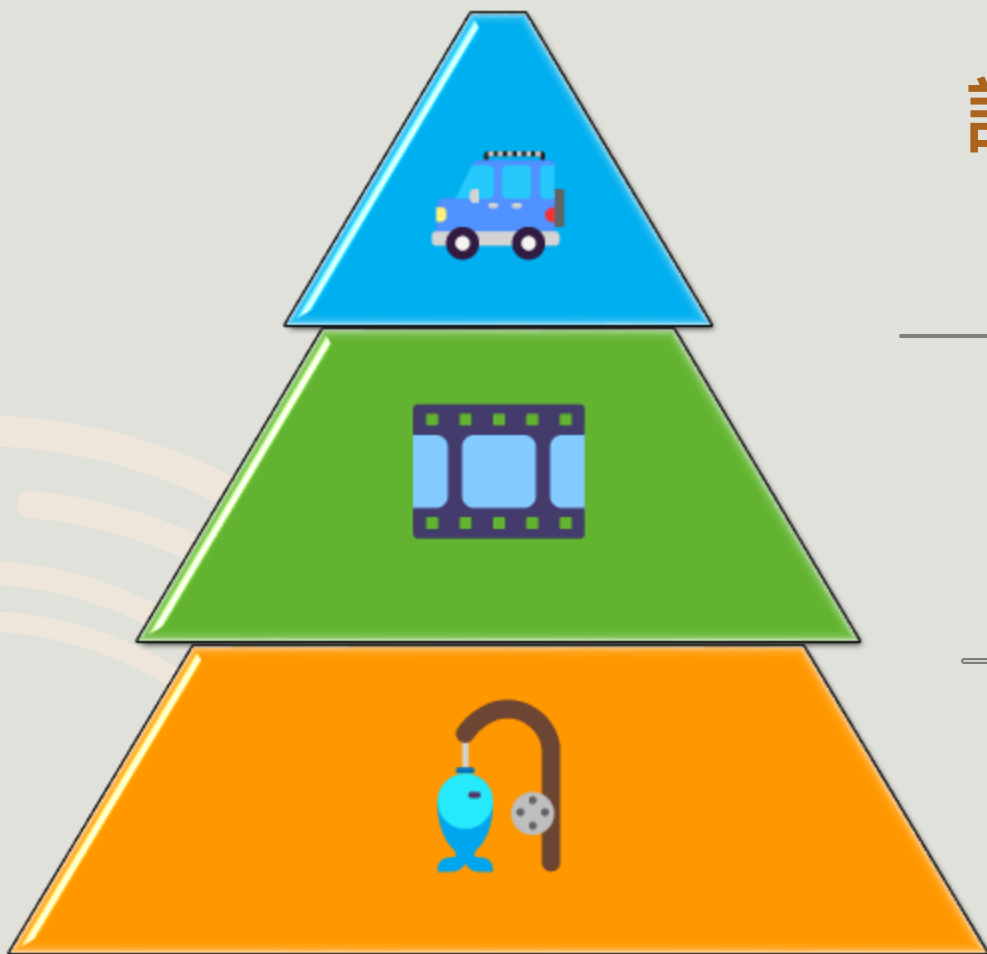
@coders.bro

Numbers of Character	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	15bn 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	100tn years	7qd years

Are you in green zone?

你在哪裡？

無孔不入的媒體詐騙



詐騙手法不斷演進

融入我們的日常生活

社群媒體成為詐騙溫床

詐騙集團的新戰場

常見詐騙手段

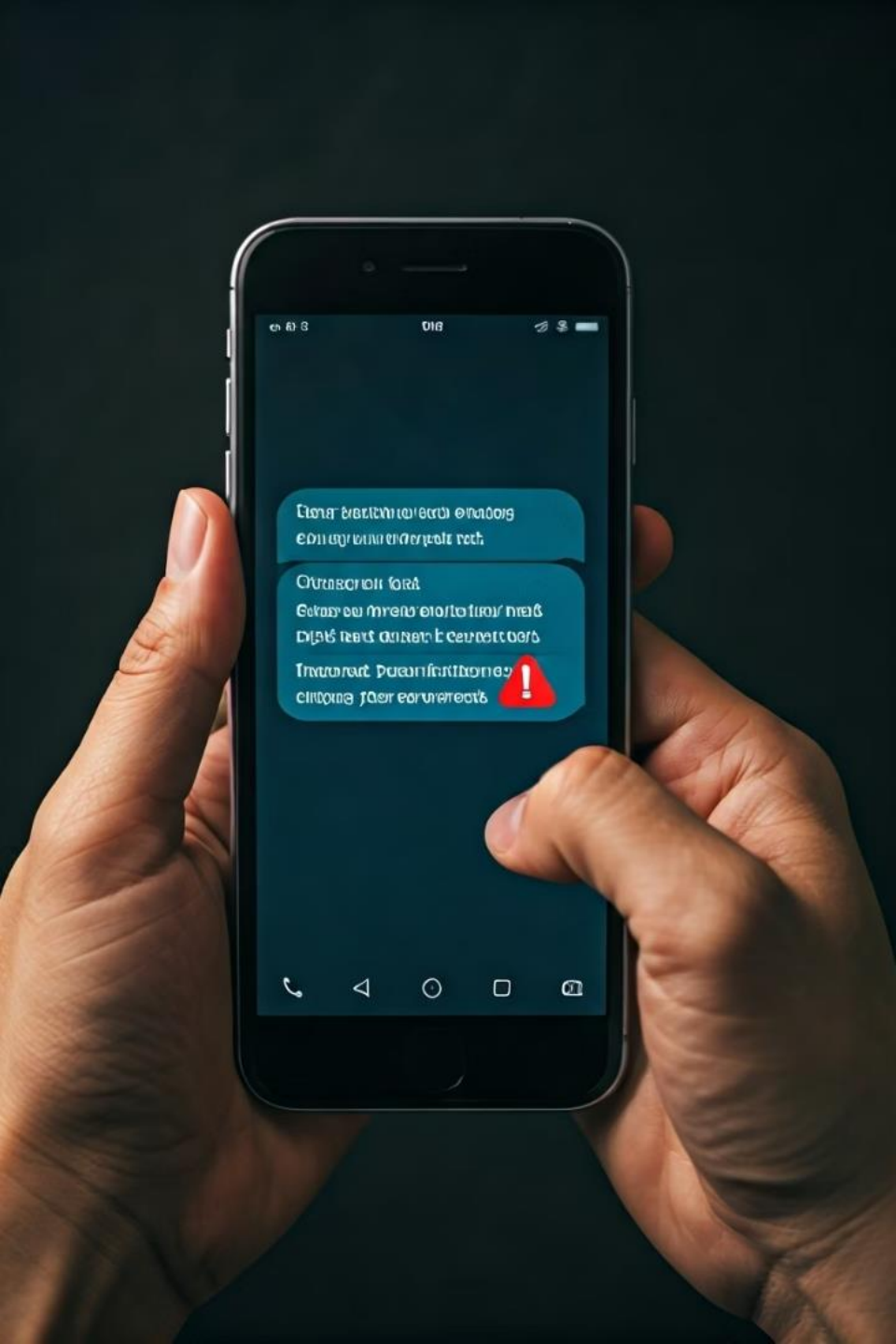
釣魚連結、假冒身份、高利誘惑

日常生活中的資安威脅

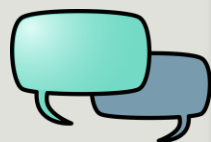


電話詐騙仍興盛！Email、社群、簡訊緊追在後





簡訊



災禍！

假冒公部門



冒充政府機構以獲取個人資訊

親友借錢



假冒親友借錢

注意最新詐騙手法

本行不會寄Email
要求確認 / 取消交易

交易通知：

以下是您交易資訊摘要：

交易金額：NT\$ 9,830

交易編號：XXX-XXXXXXXXXXXX

付款方式：信用卡/金融卡

重要提醒

如果您本人發起此交易，請忽略此通知。

若您不認識此交易，請立即取消：

取消交易

我知道了

我的投資分析



我的



信用卡



常用



理財



更多



銀行通知

發送假銀行警告
詐騙取財



不明投資連結

發送可疑投資連結以竊取資金

如何處理可疑簡訊？



不點擊、不回覆

避免潛在詐騙連結和互動

立即刪除

減少被詐騙的風險

不提供個人資料

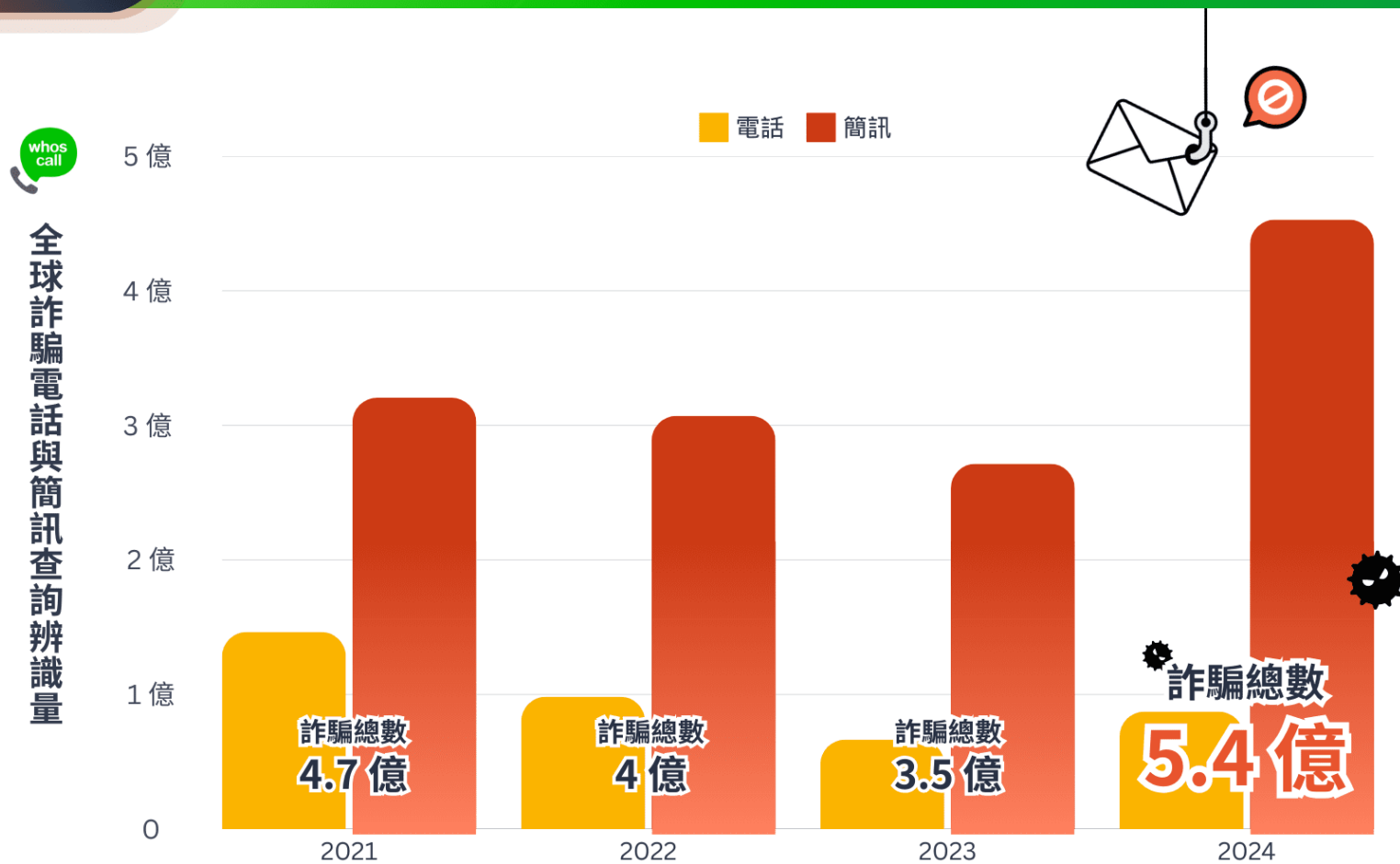
保護個資避免竊取濫用

透過官方管道查證

確認訊息的合法性

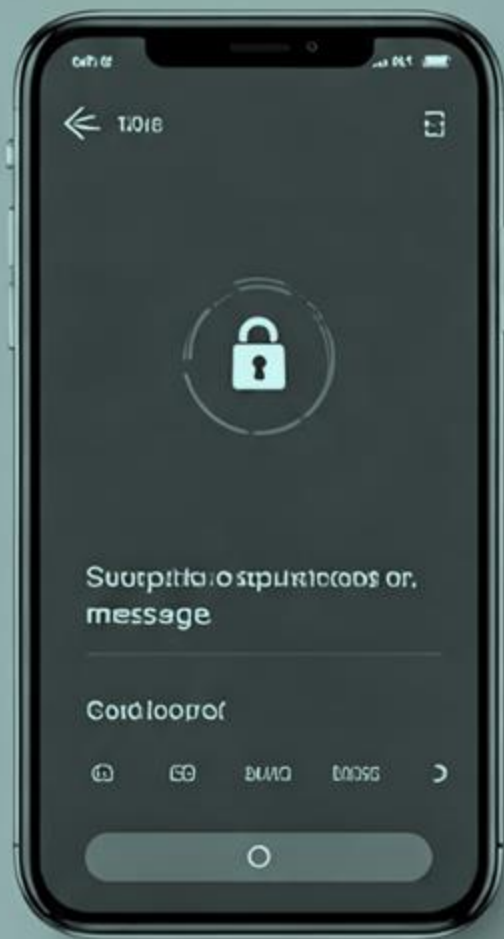
whoscall
2024 年度報告

詐騙再創新高！全球歷年電話與簡訊詐騙分析



資料來源：Whoscall (2024/1~2024/12) | 主要統計地區：台灣、泰國、馬來西亞、巴西、日本、香港、韓國、菲律賓等

LINE防詐術：先辨識真假



常見詐騙手法



電話或視訊確認



開啟雙重認證



保持警惕

LINE常見詐騙手法

假冒親友

假冒親友，藉此
借錢或尋求幫助



一頁式廣告

使用一頁式廣告，
販售假冒商品



交友詐騙

透過交友網站，
騙取受害者金錢



假冒客服

假冒客服人員，
騙取個資



投資詐騙群組

建立投資群組，
騙取投資人金錢



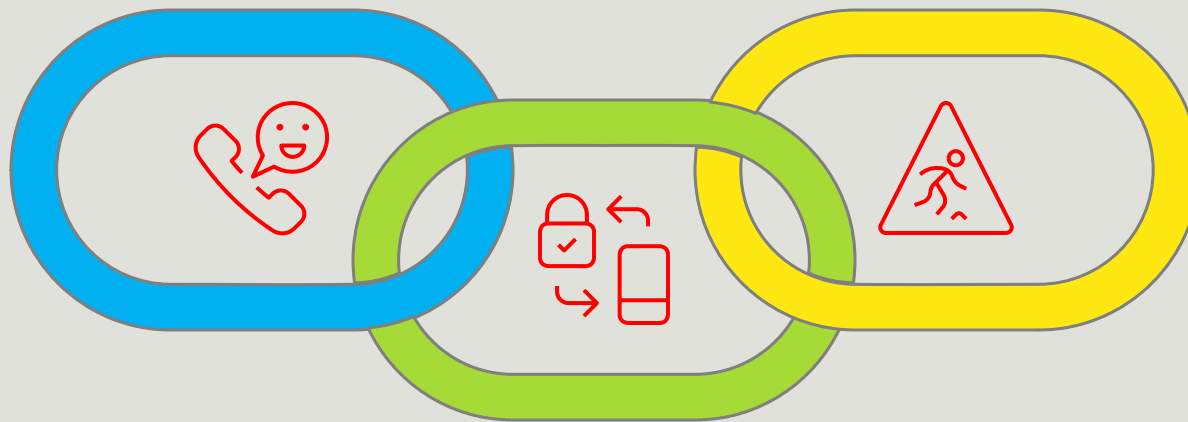
LINE防詐策略

電話或視訊確認

遇親友借錢或要求點擊連結時,務必直接通話確認

保持警惕

不輕易加入不明群組、不點擊不明連結



開啟雙重認證

提高帳號安全性,防止被盜用

LINE TODAY



守護LINE帳號 3不1提醒避詐騙

不明連結
不要點

LINE【密碼】
不告訴任何人

隨時注意
聊天中潛風險

LINE【認證碼】
不告訴任何人

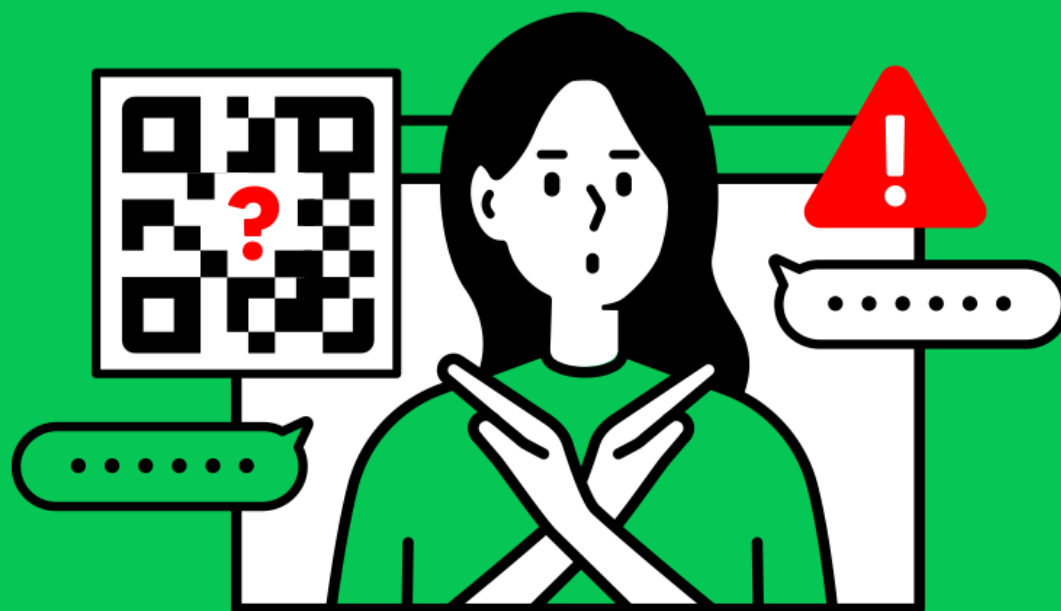
1

不肖人士會以各種話術提供 QR code 要求掃碼，一但掃碼，以下操作自救：**方案 A** 下操作自救：**方案 B**
便會讓不肖人士藉此用其他裝置登入你的 LINE 帳號

不肖人士登入的裝置，

功能

來路不明的 QR Code 請注意 一不小心帳號立刻被盜用



智慧手機、平

被好友要求提供 LINE 帳號資訊要注意



帳號被盜怎麼辦？

如何聯絡 LINE 客服流程整理



Facebook安全守則：擦亮雙眼，識別陷阱！

辨識粉專真偽

檢查藍勾勾、發文歷史



可疑抽獎活動

對太好的禮物保持警惕



投資詐騙

不貪小便宜，對誇張投資報酬率保持懷疑



安全設定

設定隱私權與安全設定，開啟雙重驗證



趨勢科技 Trend Micro
12 萬按讚數 · 12 萬位追蹤者

已驗證帳號

瞭解詳情 發送訊息 讚

貼文 關於 Mentions Reels 相片 影片 更多

簡介

【我們是不用槍的007！】
趨勢科技多次與國際刑警組織 (INTERPOL) 聯手,破獲上千多台駭客幕後操縱伺服器。

【我們不只是資安專家】
AI防詐達人用說的也可以, 9-99歲都可輕鬆防詐

【我們是台灣之光】
年年榮獲台灣最佳國際品牌獎

精選



趨勢科技 Trend Micro
5月23日下午5:14
隨著 AI 重塑現代軟體架構, 企業必須重新思考其安全策略, 從被動防禦轉向主動預測和即時反應, 以確保在利用 AI 創造價...



趨勢科技 Trend Micro
4月10日
太酷了, 只要說:「嘿, Siri是詐騙嗎?」就可以輕鬆查證詐騙
9-99歲都可以輕鬆上手...



星巴克咖啡同好會 (Starbucks Coffee)
2.2M likes · 2.2M followers

已驗證帳號

Posts About Mentions Reels Photos Videos More

Intro

星巴克線上門市: www.starbucks.com.tw/onlineshopping

Page · Coffee shop

Posts



星巴克咖啡同好會 (Starbucks Coffee)
6h
在畢業季, 獻上真摯的祝福

Security and Login > Two-Factor Authentication



Recovery Codes
Use these codes for when you don't have your phone with you, for example when you're traveling.

10 OF 10 REMAINING [Get New Codes](#)

CODE #1	0363 7213	✓
CODE #3	0708 6642	✓
CODE #5	1295 8940	✓
CODE #7	1689 8004	✓
CODE #9	3155 2614	✓
CODE #11	4507 9529	✓
CODE #13	6624 9961	✓
CODE #15	8401 3099	✓
CODE #17	8461 7006	✓
CODE #19	8845 1763	✓

[Close](#) [Print Codes](#)

Allow logins without a second factor

Added Security
After entering your password, you'll receive a second factor to verify your identity.



Text Message
We'll send a text message to your phone.



Authentication app
You'll receive a code from an app on your phone.

Add a Backup
Set up a backup option so you can restore your account if you lose your phone.



Security Key
If you have a security key, you can use it to sign in.



Recovery Codes
Use these codes for when you don't have your phone with you, for example when you're traveling.

Remove number

Remove app

Setup

Setup

22

帳號管理中心

管理你在 Facebook、Instagram 和 Meta Horizon 等 Meta 技術的互聯體驗和帳號設定。
[瞭解詳情](#)

 個人檔案

 互聯體驗

帳號設定


 密碼和帳號安全

 個人資料

 你的資訊和權限

 廣告偏好

 Meta Pay

 帳號

密碼和帳號安全

登入和復原

管理你的密碼、登入偏好設定和復原方式。

變更密碼



雙重驗證



儲存的登入資料



通行密鑰



帳號安全檢查

針對各個應用程式、裝置和寄出的電子郵件進行檢查，審視安全問題。

你登入的位置



登入警告



最近的電子郵件



帳號安全檢查



Instagram 防詐：保護帳號，識破誘惑！



常見詐騙手法



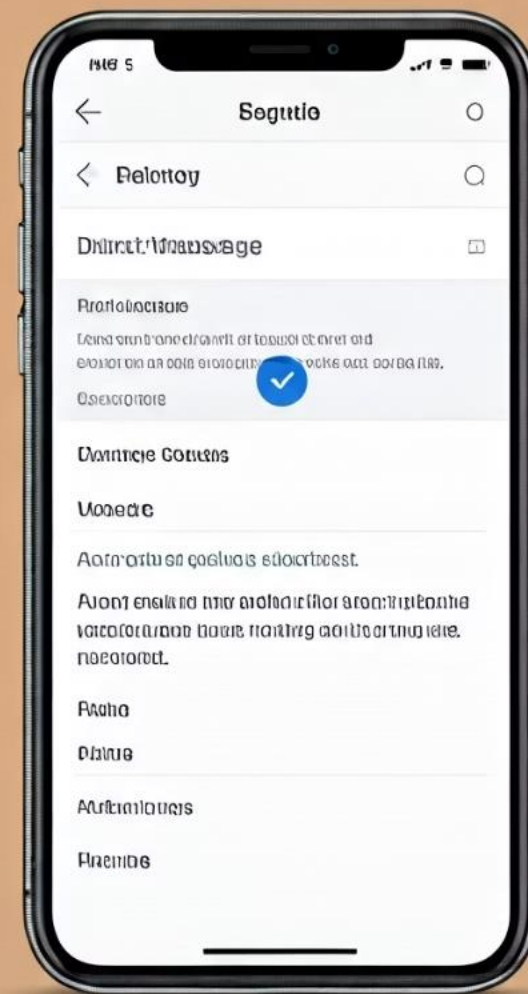
連結安全



檢查帳號細節



帳號保護



Instagram上常見詐騙

交友詐騙

保持警惕並驗證身份
以避免交友詐騙

品牌代購詐騙

驗證代購的真實性與合法性
避免詐騙

假冒抽獎

檢查抽獎的真實性以
防止被騙

投資詐騙

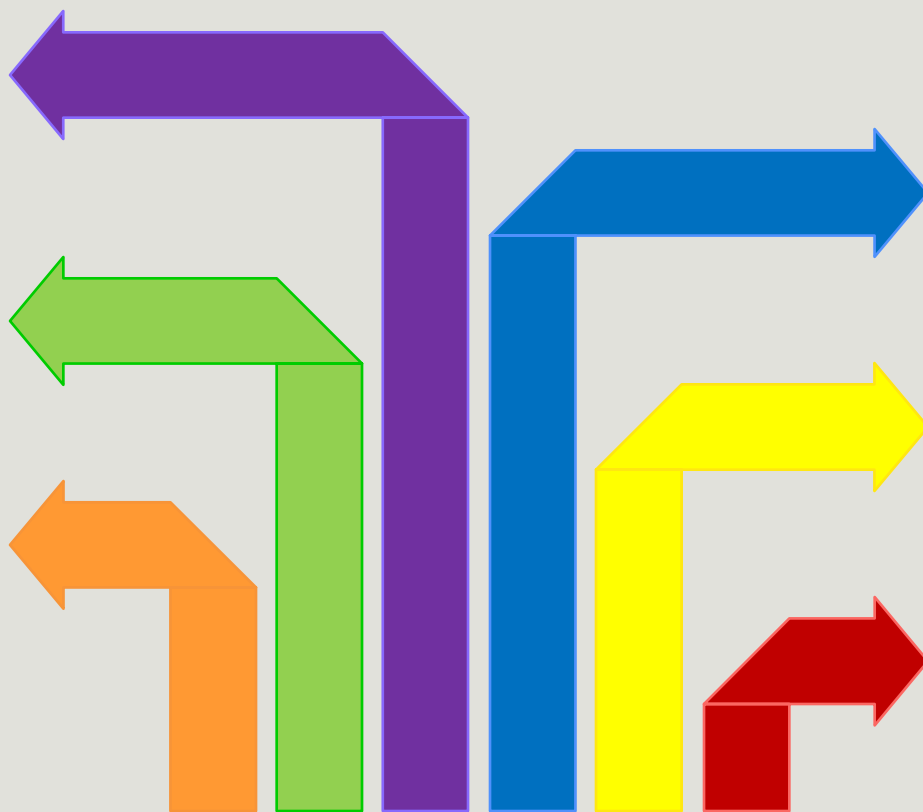
確認投資機構與投資標的
的真實性以避免投資詐騙

假冒官方通知

驗證通知的來源以確
保其合法性

假冒網紅/名人合作

驗證合作的合法性以
避免詐騙



Instagram防詐

檢查連結安全

確保點擊連結是安全的，利用工具(如沙箱、防駭軟體)檢查

檢查帳號細節

驗證帳號的合法性，以免遭詐騙

保護帳號安全

啟用雙重驗證並使用強密碼，增強安全性

不回應陌生訊息

避免與未知來源互動，減少詐騙風險



 Meta

Accounts Center

Manage your connected experiences and account settings across Meta technologies like Facebook, Instagram and Meta Horizon.
[Learn more](#)



Profiles



Connected experiences

Account settings



Password and security



Personal details



Your information and permissions



Ad preferences



Meta Pay



Accounts

Password and security

Login & recovery

Manage your passwords, login preferences and recovery methods.

Change password



Two-factor authentication



Saved login



Security checks

Review security issues by running checks across apps, devices and emails sent.

Where you're logged in



Login alerts



Recent emails



Security Checkup



釣魚郵件：你就是「魚」！



常見釣魚類型

假冒內部信件、外部機構、社交工程、附件型釣魚、變臉詐騙



詳細檢查

檢查寄件者信箱、主旨與內容細節

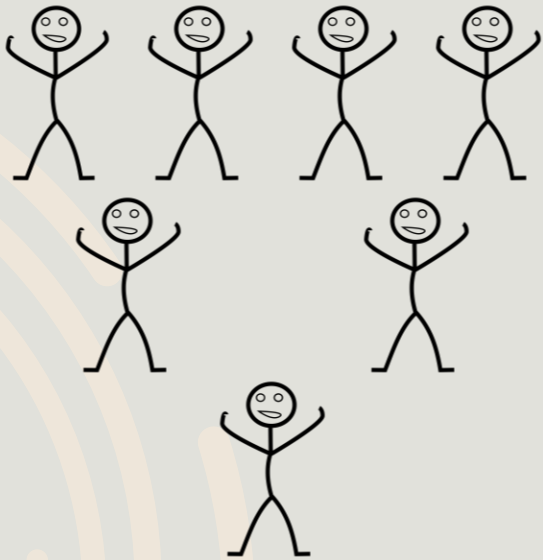


防範措施

不隨意點擊連結、不隨意開啟附件、再三查證、啟用多因素驗證

資訊安全的認知

- 世界上不存在100%安全的資訊防護系統
- 任何防護系統最薄弱的一環，永遠是人
- 資訊安全、人人有責



社交工程

- **社交工程(Social Engineering)** 是指一種操弄人類心理，採取特定行動來蒐集機密資訊的技巧
- **方法：**利用人性弱點或利用人際之信任關係來進行詐騙，是一種技術性的資訊安全攻擊方式，藉由人際關係的互動進行犯罪行為
- **目的：**以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破組織的資通安全防護，遂行其非法的存取、破壞行為

郵件種類

- 廣告信件
- 病毒信件
- 釣魚（ Phishing ）信件
- 木馬（ Trojan ）信件
- 網頁綁架信件
- 勒索軟體信件



郵件內容

- 政治
- 色情
- 休閒
- 贈品、抽獎、好康的
- 愛心捐獻
- 影音媒體
- 業務職務相關
- 趣聞





jamson

,You have won an T-Mobile 📱iPhone 16 Pro ®...Confirmation-0539*ZKAG



垃圾郵件 x

金



T-Mobile® <fgoufhnyruu@pvfzvtxsz.xuuuuuuuuuazioazuioaz.sampoowered.it.com> (寄件者 Trusted Sender)

有行旅賞楓名旅 日本山形、伊豆、高野山 楓情萬種旅程說明會預約中



垃圾郵件 x



聯合報系會員特刊 <newsletter@edm.udndigital.com.tw>

寄給我 ▾

6月20日 週五 上午3:20 (3 天前)

為什麼系統將這封郵件歸類為垃圾郵件？這封郵件的內容與先前歸類為垃圾郵件的郵件相似。



回報為非垃圾郵件

發行日期：2025.06.20

由於您的會員資料顯示已同意訂閱由 udn.com 發出的市場相關訊息，若您不欲收取相關訊息，請按此 [取消訂閱](#)。

[聯絡我們](#) | [會員服務條款](#) | [著作權聲明](#) | [隱私權聲明](#) | [會員權益](#)

Copyright © 2013 udngroup.com All Rights Reserved.

[未顯示完整郵件內容] [查看整封郵件](#)

Exclusively for you
iPhone 16 Pro!

雲 男子猥褻4姪偷拍存雲端，最小僅3歲！Google跨海通報台灣警方逮人



造咖生活流行媒體

2025年6月4日



台灣一名男子猥褻4名未成年姪女，當中包括3歲與4歲幼童，他甚至還將兒少性影像上傳至「Google雲端」遭系統偵測異常後，Google 跨海通報台灣刑事局，整件事才曝光，掀起性犯罪與資安相關議題討論與重視！

Google跨海通報台灣警方逮人

警方調查出男子利用零食降低4名姪女的戒心，再對其騷擾偷拍，而Google在發現男子從中國網站下載超過2千部兒少性影像之後，又將影片上傳到自己的Google雲端遭系統偵測異常，Google 因而通報美國相關單位再由台灣警方逮捕，嫌犯遭逮捕時不敢相信錯愕喊：「我存在雲端的東西，怎麼會被發現？」目前該名男子遭到起訴並羈押，防止他再靠近被害人。

常見 AI 詐騙手法

AI 詐騙的隱藏深度

你看到的詐騙

Deepfake 語音詐騙

AI 成的假語音

AI 釣魚郵件

AI 生成的詐騙郵件

AI 投資詐騙

AI 生成的假投資建議

假新聞

AI 生成的假新聞



Deepfake 影像詐騙

AI 生成的假影像

假冒客服

AI 假冒客服

假 QR Code

導向詐騙/惡意網站

調查局對於深偽技術詐騙 識詐說明



0:00 / 2:38



【識詐宣導】詐騙集團如何使用深偽技術(Deepfake)變臉？調查官教您破解騙術



中華民國法務部

4860位訂閱者

訂閱



61



分享



下載



剪輯片段



所有家長都需要看這篇 🤖 !!

一個AI生成的9歲女孩影片
訴說了讓人不寒而慄的事



任何人都可以下載或利用

Dr Arpit Gupta



dbstudio_tw

追蹤

有孩子的父母請看看，在這 AI 強大的時代，分享孩子 ...



29



7



常見 AI 詐騙手法與防護對策

AI 詐騙手法	說明	實際案例	防護作為
Deepfake 語音詐騙	利用 AI 模仿親友、主管聲音要求轉帳或提供資訊	香港銀行高層遭語音深偽詐騙損失 2,500 萬美元	多管道確認身份、多重簽核機制
Deepfake 影像/影片詐騙	假冒名人或主管影片要求投資或散播假訊息	印度財長深偽影片造成數百萬盧比損失	保持懷疑、使用反向搜尋驗證影片
AI 釣魚郵件/簡訊	AI 自動生成個人化釣魚訊息	台灣民眾常收到假物流、銀行簡訊詐騙	不點可疑連結、檢查寄件來源、防詐 App
假冒客服/AI 聊天機器人	冒充銀行或電商客服詐取個資	假冒 Amazon/PayPal 客服機器人詐騙	僅透過官方管道聯繫、不輸入敏感資料
AI 假投資建議/金融詐騙	利用 AI 假投資報告或平台	AI 加密貨幣詐騙 2024 年激增 456%	不信零風險投資、確認合法平台
假 QR Code/偽網站	AI 生成釣魚網站與假 QR Code	台北車站出現 AI 假影片推播 QR 詐騙	檢查網址、手動輸入官網網址
AI 假新聞/假訊息	AI 生成假新聞散播社群平台	LINE、FB 出現假投資/醫療新聞	不轉傳來源不明資訊、查核平台驗證



個人裝置安全設定

藍牙



隱私權設定



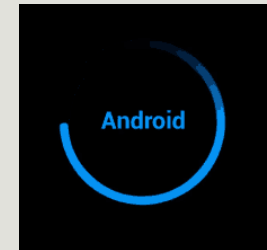
密碼(螢幕鎖定)



裝置定位



作業系統更新



防毒軟體安裝
/更新





藍牙設備漏洞

瞄準iPhone + iPad + MacBook攻擊

▲ 據科技網站AppleInsider報道，有研究團隊披露了一項藍牙無線通訊協定中的新安全漏洞，指出任何符合標準的藍牙設備皆可能受到攻擊。

美圖秀秀呼叫資訊被疑洩隱私

新浪綜合 01-23 20:44

美圖秀秀靠手繪自拍躡紅美國調用多項資訊引發隱私外洩擔憂

來源：澎湃新聞

靠著新上線的手繪自拍功能，美圖公司旗下應用美圖秀秀在美國AppStore免費應用程式榜單上的排名，從1,000名以外迅速躡升到第11位。不過，在美圖秀秀的隱私政策中，卻發現其調用了用戶的地理位置、聯絡人、相機、麥克風等敏感資訊，陷入了竊取和洩漏用戶隱私的風險爭議。



美國網路新聞部落格Mashable為川普和希拉蕊的照片加入了美圖秀秀的手繪自拍濾鏡

CNN（CNN）在1月20日發布的一篇報道中稱，在過去兩周里風靡美國的中國App美圖秀秀陷入了麻煩，因為該應用會蒐集用戶信息用於廣告目的。

密碼鎖(螢幕鎖定)

手機遺失遭盜用支付
預設鎖定回覆造成盜刷



獨／偷手機還關機避追查 仍可搜尋定位！賊2小時落網

2023-02-23 19:51 東森新聞

聽新聞



00:00

A-

A+



分享



新北市五股一家自助洗衣店，老闆娘的iPhone 14 Pro被竊賊拿走，原本以為找不回來，但抱著姑且一試的心態，打開平板，用搜尋功能尋找，結果發現雖然手機被關

作業系統更新

WannaCry 勒索病毒

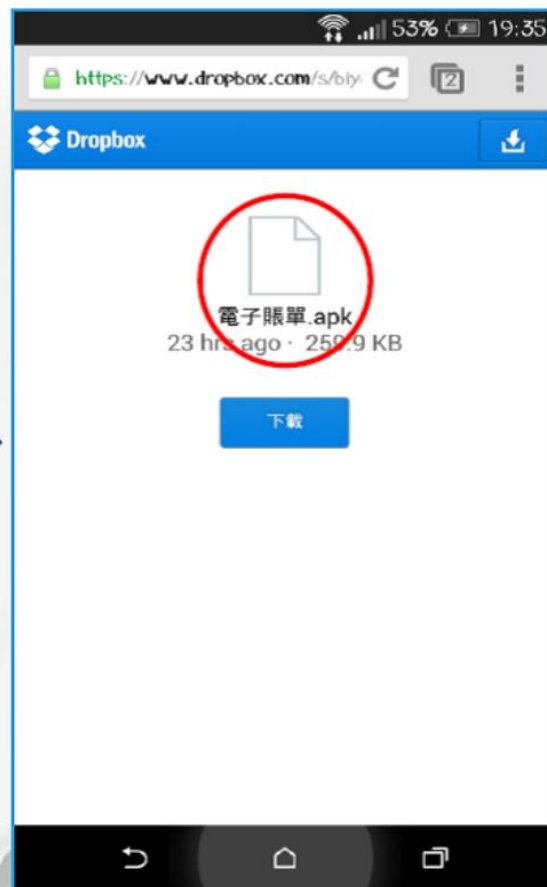
台積電病毒事件



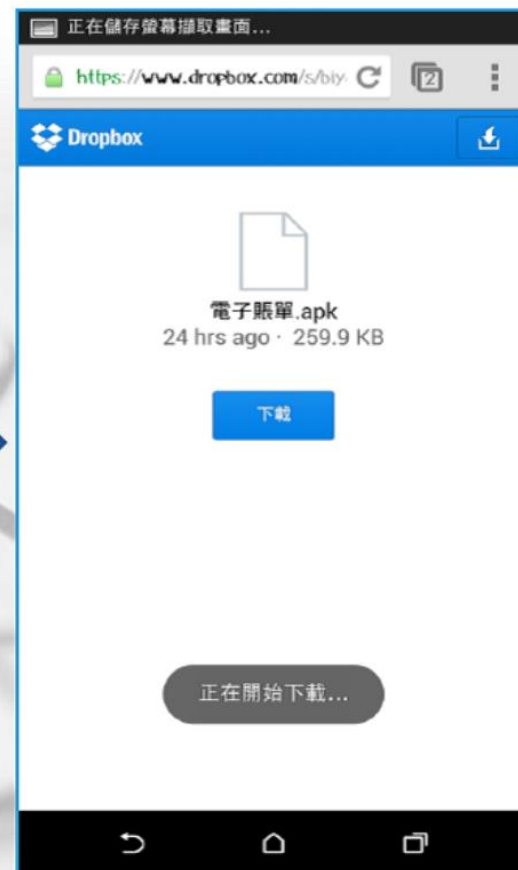
➤ 惡意連結與濫發簡訊：



接到惡意簡訊
並點擊連結



點擊後下載惡意程式(手機
未必會有此畫面)



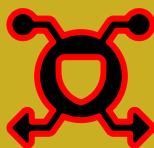
下載惡意程式
至裝置

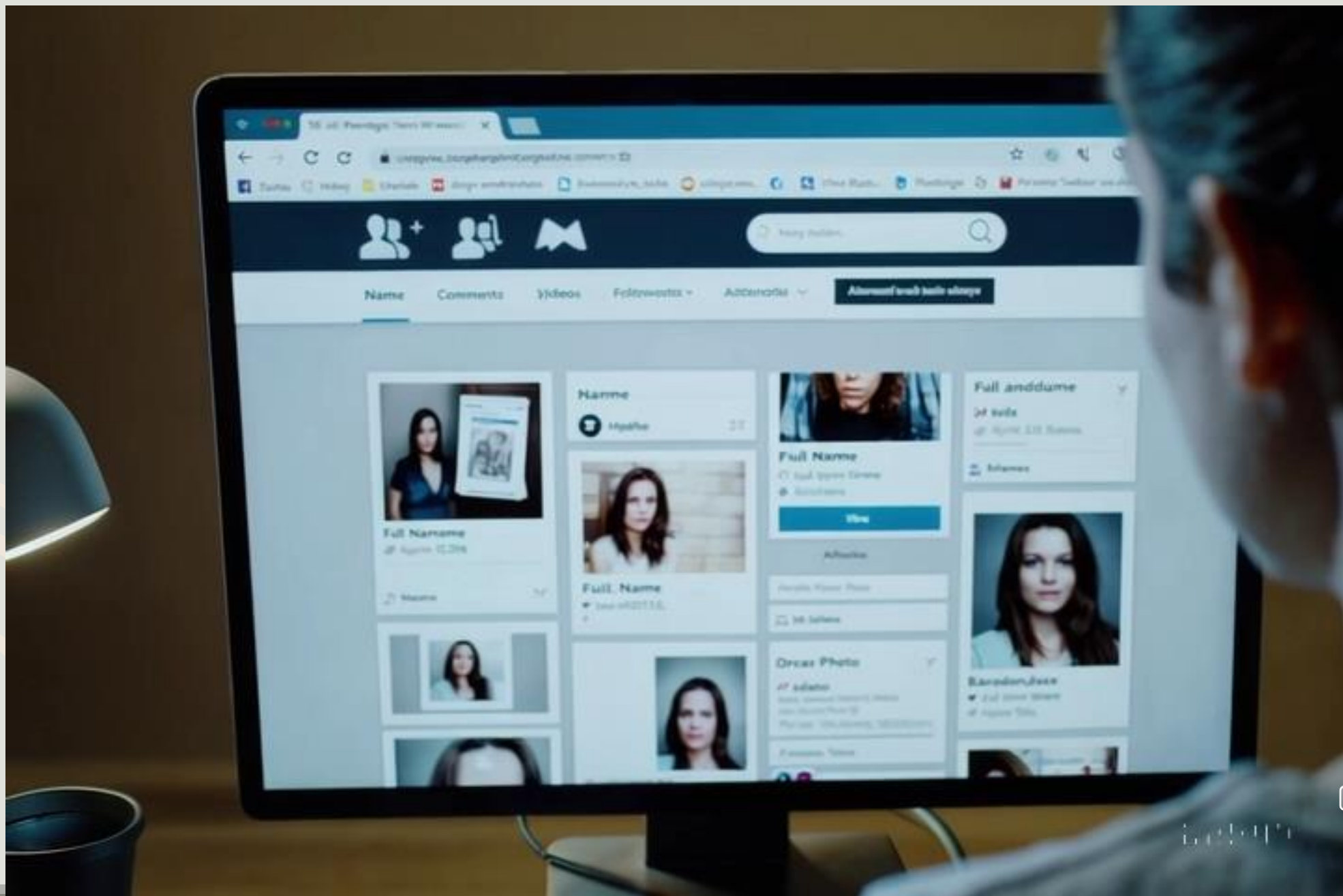
社群媒體與通訊軟體常見 風險行為

過度分享個資

點擊不明連結

第三方插件風險







PERSONAL LEAKS

PASSWORD L

Don't let your answers be
key for hackers!

Let's play a Q&A game!
What was the name of
your first car? 🚗

Honda Civic

08/15

Toyota

02/24



Reset I

First car's na

Honda Civ

Mother's birt

08/15



Pa
SU

POSTING TRAVELS TEMPTS BURGLARS

Don't let your vacation post
invite a break-in.



Off to the airport
at last—two weeks in
Italy starts now! 🇮🇹



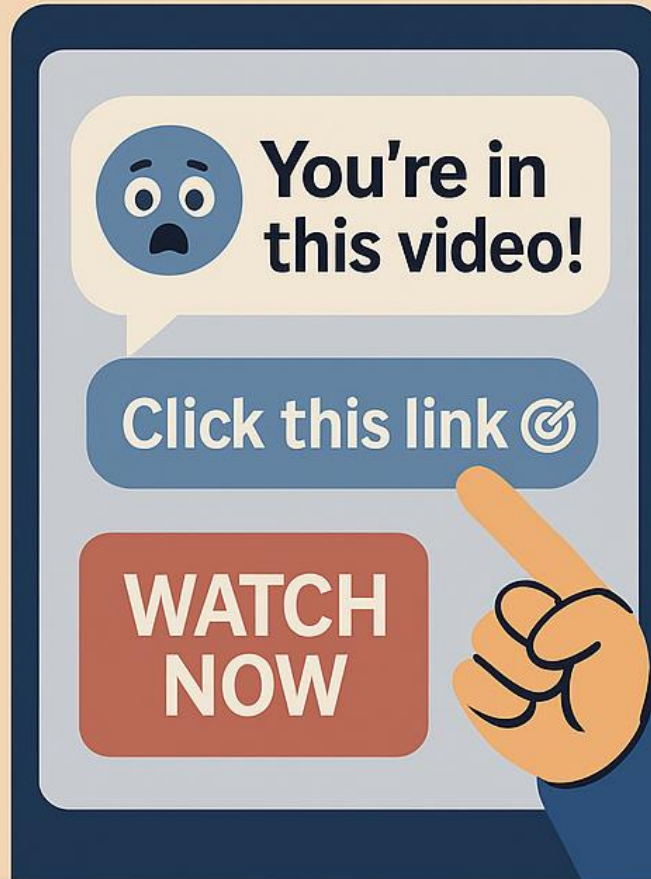
WAIT TO SHARE, KEEP HOME SAFE

'Help m



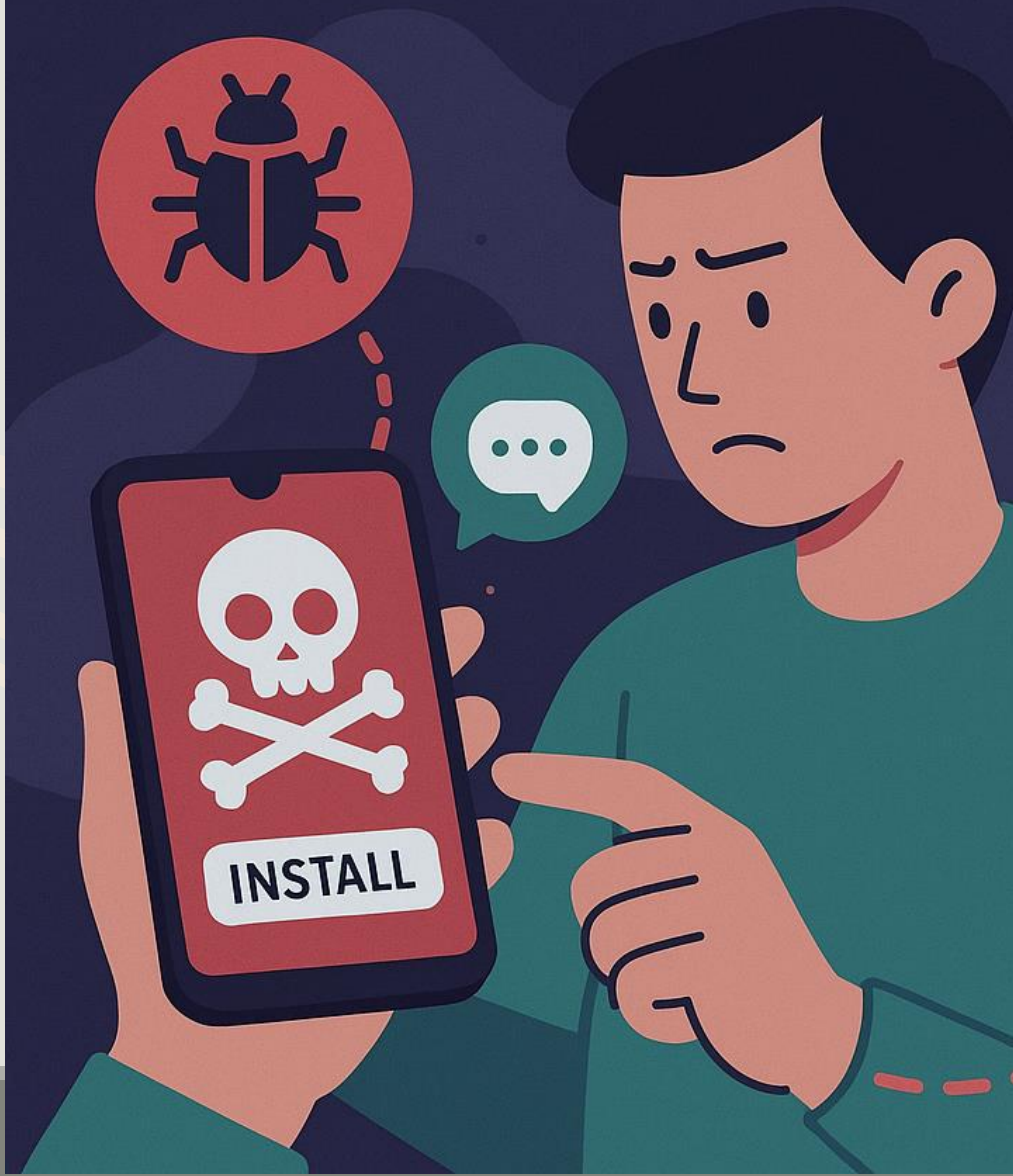
Don't fall for t

You're in this video!'



Fake link, real danger.

RISK OF UNOFFICIAL APP PLUGINS



**ONLY INSTALL
VERIFIED APP
PLUGINS**



**UNVERIFIED PLUGINS
MAY INCLUDE MALWARE
OR BACKDOORS**

被駭/害人常見社群網站風險行為

- 👹 把社群網站當公布欄，將生活動態公布在社群網站
- 👹 不設定使用隱私安全設定
- 👹 不使用私訊，隱私在公開頻道上傳送
- 👹 社群網站上過度分享個人資訊，如名字、生日及就讀學校
- 👹 使用傻瓜密碼或是社群網站找得到答案的密碼提示答案

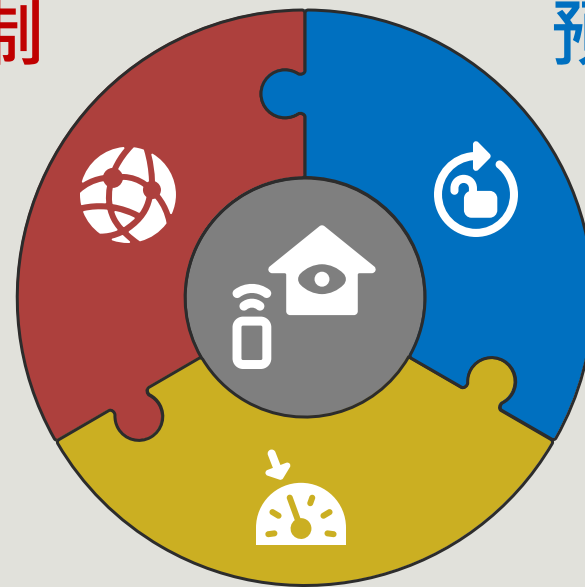
SMART HOME



智慧家電(IoT)資安風險

遠端連線未限制

預設密碼未更改

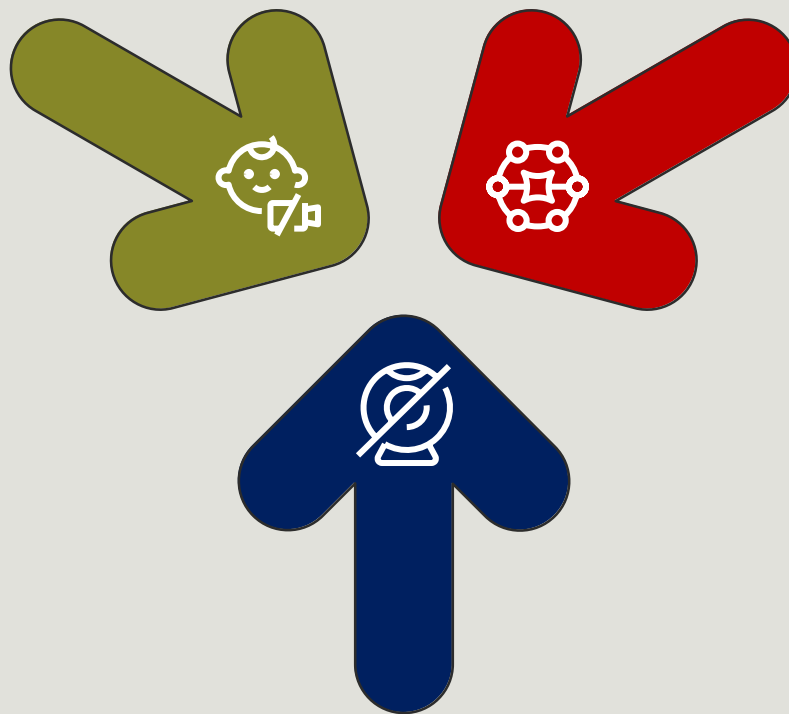


未更新韌體

預設密碼未更改

寶寶監視器漏洞

寶寶監視器中的安全漏洞
導致隱私洩露



監視器遭駭入侵私

未受保護的監視器允許未經授權的訪問

Mirai 殭屍網路

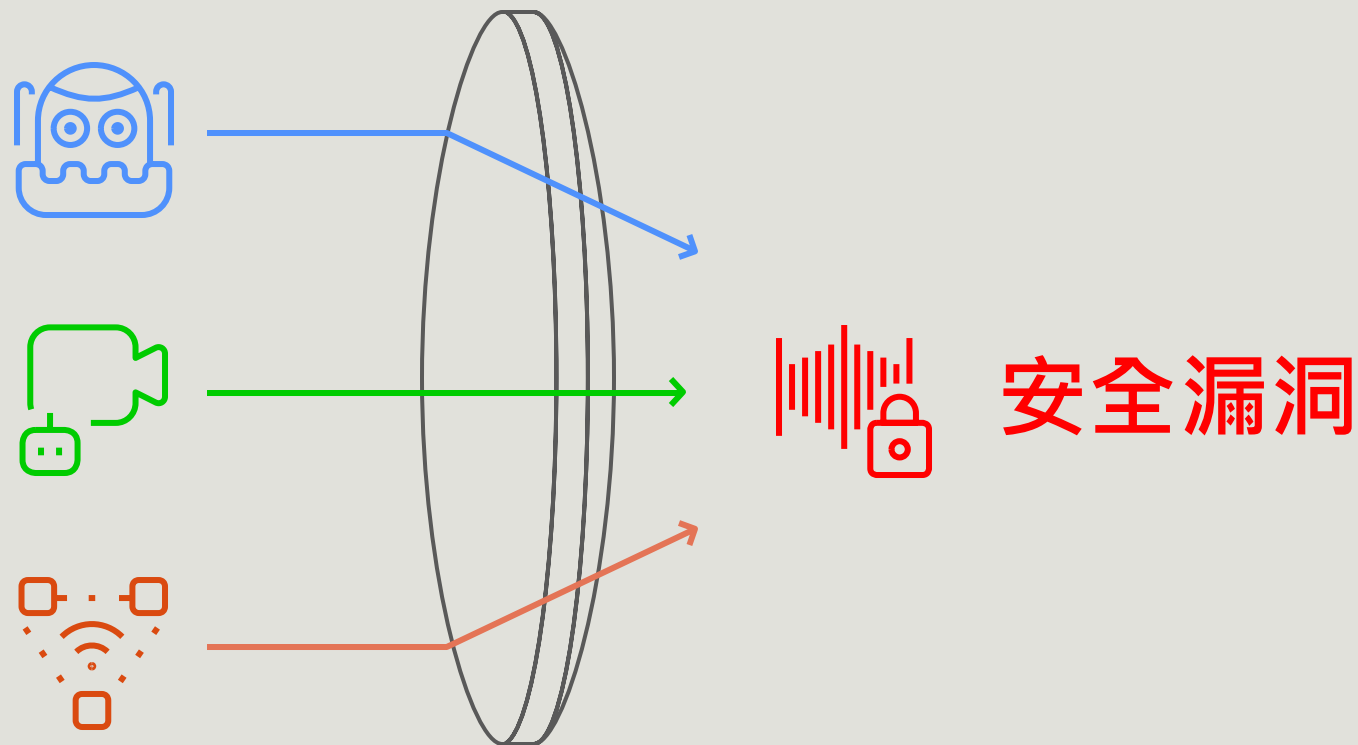
利用未受保護的IOT設備發起DDoS攻擊

遠端連線未限制

魚缸溫控器入侵

監視器公共串流

未隔離的智慧裝置



未更新韌體

解決VPN過濾器攻擊

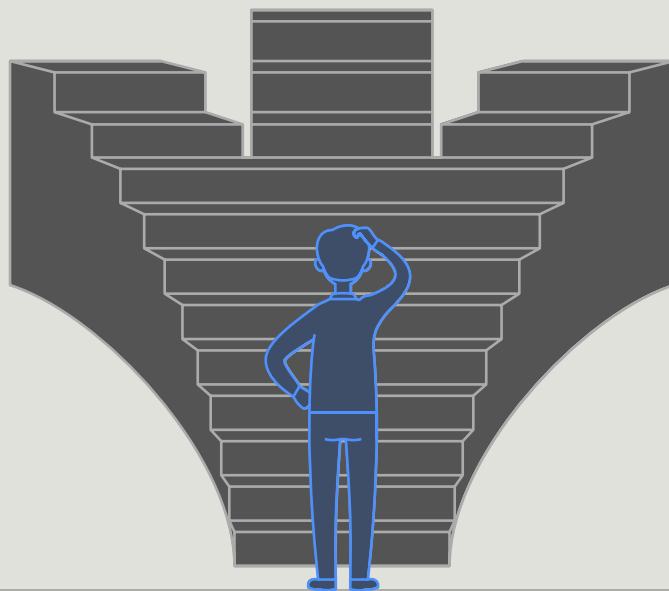
更新網路裝置韌體避免被植入惡意程式

解決零日漏洞

應用補丁並更新韌體以關閉漏洞

解決智慧門鎖回應遲緩

檢查並更新門鎖的軟體和硬體維持運作正常



165反詐騙



內政部警政署 **165全民防騙網**

National Police Agency, Ministry of the Interior



—— 165 反詐騙諮詢專線 ——



內政部警政署


National Police Agency, Ministry of The Interior

165 打詐儀錶板


資安宣導




資訊安全專區



社交工程
演練專頁



校園保護智慧
財產權宣導



個人資料管理

資安政策

資訊安全政策
隱私權聲明

教育訓練

資安教育訓練
社交工程演練專業頁
個人資料管理PIMS
校園保護智慧財產權宣導

資安規定

禁用大陸廠牌規定
資安條款採購注意事項
出租場地資安注意事項

資安專章

個人電腦安全防護措施
資安專章評核指標

禁用大陸廠牌規定

首頁 / 資訊安全專區 / 資安規定 / 禁用大陸廠牌規定

禁用大陸廠牌規定

資通訊產品之定義

資通訊產品包含軟體、硬體及服務等項，另具連網能力、資料處理或控制功能者皆屬廣義之資通訊產品。

◎軟體：資通系統，如應用軟體、系統軟體、開發工具、客製化套裝軟體、APP及電腦作業系統等。

◎硬體：包括具連網能力、資料處理或控制功能者皆屬廣義之資通訊設備，如個人電腦、筆記型電腦、伺服器、智慧型手機、平板電腦、行動電話機、網路通訊設備（如網路交換器、無線網路分享器等）、無人機、虛擬實境設備、影像攝錄設備、印表機、投影機、可攜式設備、物聯網設備等。

◎服務：資通服務，如客服服務及軟硬體資產維護服務等。

大陸廠牌之定義

所有屬大陸廠牌者，無論其原產地於我國、大陸地區或第三地區等，均列入限制使用範圍。

行政院在2020年原本要列出禁止採購清單，考量狀況複雜，最後沒有所謂的資安黑名單。

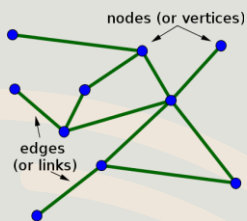
在經濟部投資審議委員會可查詢陸資資訊產業、陸資來台投資事業，這些業者在台灣生產銷售的資通訊產品是否被認定屬大陸廠牌而限制使用仍未明確，原則上建議盡量避免購置。

更多參考資訊請見-【數位發展部資通安全署】資安法常見問題：<https://moda.gov.tw/ACS/laws/faq/28/646#qaH742>

本校禁用大陸廠牌名單

1. 名單請見：[長庚科大禁用大陸廠牌名單\(隨時更新\)](#)
2. 名單僅列出常見廠牌，大陸廠牌認定方式，由本校參考政府認定或建議者為原則。
3. 如遇其他無法辨別者，建議請廠商提供說明或證明文件是否非大陸品牌。
4. 「在台陸資廠商」詳情請參閱：[陸資投資資訊產業事業清冊](#)

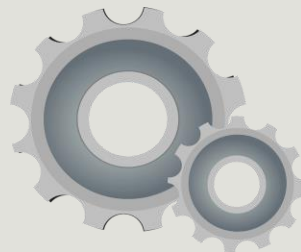
個人資料保護法



架構



定義



運用




個人資料保護法架構

章別	主題	包含條文	概括內容
第一章	總則	1~14	立法目的、用詞定義、當事人權利、委外的規定、書面同意的方式、告知義務及個資維護規定
第二章	公務機關對個人資料之蒐集、處理及利用	15~18	公務機關蒐集、處理、利用個人資料的要件、個人資料檔案公開、安全維護義務
第三章	非公務機關對個人資料之蒐集、處理及利用	19~27	非公務機關蒐集、處理、利用個人資料的要件、不得跨國傳輸個資、行政檢查與安全維護義務的規定
第四章	損害賠償及團體訴訟	28~40	民事損害賠償責任規定、團體訴訟的相關規定
第五章	罰則	41~50	違反個資法的刑事責任與行政處罰
第六章	附則	51~56	例外情形、其他規定

『個資』的定義

一般個資



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

特種個資

個資法用詞定義

蒐集 — 以任何方式取得的個人資料

處理 — 記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結、內部傳送

利用 — 將蒐集來的個資用作處理以外的用途

國際傳輸 — 指將個人資料作跨國(境)之處理或利用

公務機關 — 指依法行使公權力之中央或地方機關或行政法人

非公務機關 — 指公務機關以外之自然人、法人或其他團體

個資行使權利

要求查詢或閱覽

要求製作複製本

要求補充或更正

要求停止蒐集處理或利用

要求刪除

簽名之前

仔細查看

不讓個資
被濫用

個人資料運用流程

1. 蒐集個人資料
2. 資料處理目的
3. 資料通知與說明
4. 合法依據
5. 資料安全措施
6. 資料保存期限
7. 資料存取權限
8. 資料共享與轉移

個資蒐集處理利用－1/2

什麼時候能蒐集、處理個資？

- 有特定目的
- 符合下列三種情形之一
 - ✓ 執行法定職務必要範圍內(如：稅捐機關為了執行課徵所得稅的職務，蒐集納稅人之所得資料)
 - ✓ 經當事人同意
 - ✓ 對當事人權益無侵害

個資蒐集處理利用－2/2

什麼時候能利用個資

- 執行法定職務的必要範圍內
- 與蒐集的特定目的相符

符合下列情形可做特定目的外利用

- 法律明文規定
- 維護國家安全或增進公共利益所必要

- 為免除當事人之生命、身體、自由或財產上危險
- 為防止他人權益之重大危害
- 基於公共利益為統計或學術研究，且資料經處理後，或奇揭露方式，無從識別特定當事人
- 有利於當事人權益
- 經當事人同意

個人資料3原則 & 蒐集/處理/利用4大原則

不要**拿**

不要**留**

不要**傳**

尊重當事人
的權益

採取誠信及
信用的方法

不得逾越特
定目的之必
要範圍

應與收集的
目的具有
正當合理的
關聯

違反個人資料保護法罰則

民事責任

- 每人每一事件新臺幣**500 ~ 20,000**
- 同一原因事實造成多數當事人權利受侵害，合計最高總額新臺幣**2億元**
- 如該原因事實所涉利益**超過新臺幣2億元者**，以**該所涉利益為限**。

刑事責任

- **五年以下有期徒刑**、拘役或科或併科新臺幣一百萬元以下罰金
- **中華民國人民在我國領域外對中華民國人民**觸犯本法第41條、第42條之罪者，亦適用本法。
- **公務員**假借職權犯罪者，**加重**其刑至**二分之一**

歷年公務機關與企業個資外洩案例_1

部門名稱	時間	事件內容	洩露筆數
中華郵政	105/5	中華郵政商城，因網站漏洞遭中國駭客入侵	約17,000筆 (News Lab)
勞動部(就業通)	105/7	勞動部就業通網站，遭催債公司駭入	約58,000 筆 (News Lab)
台北市政府資訊局	106/1	資訊局薪資管理系統被駭，市府公職人員姓名、職等、銀行帳號、所得稅等細目外洩	約 70,000筆 (News Lab, 財團法人民間司法改革基金會)
外交部	106/2	出國登錄系統被駭，中文姓名、護照號碼、電話、電子信箱等10項資料洩漏	約15,000 筆 (News Lab, 財團法人民間司法改革基金會)
高雄市政府(果菜公司網)	107/4	高雄果菜公司遭駭，資料被勒索或外洩	規模未公開(利害相關) (National Communications Commission)
臺北市政府衛生局	107/8	遭駭客入侵，市民資料外洩	約 298 萬筆 (勞動部勞動力發展署北基宜花金馬分署全球資訊網)
台灣高鐵	107/12	高鐵票務系統被駭客攻擊	洩露規模未報導具體筆數 (National Communications Commission)
台北市政府衛生局	108/1	衛生局市民醫療資料外洩	約 298 萬筆 (National Communications Commission, News Lab)
銓敘部(含機敏單位)	108/6	中央及地方公務人員歷史審核資料外洩，含國安局、調查局等機敏單位，實際外洩年份為 2012–2013	約 59 萬筆(影響超過 24 萬人) (National Communications Commission, Cyber Taiwan)

歷年公務機關與企業個資外洩案例_2

部門名稱	時間	事件內容	洩露筆數
內政部 / 戶政資料	111/10	全台戶役政資料在暗網販售，包括身分證號、戶籍等資訊	約 2,357 萬筆 (National Communications Commission, CW Taiwan)
內政部 / 戶政資料	111/12	BreachForums 販售全國戶役政資料，內容涵蓋身分證號、戶籍、家庭成員等	約 2300 萬筆 (Tahr, Yahoo News, 法律白話文運動)
雄獅旅遊	106/5	遭駭客入侵，旅客資料外洩	約36萬餘筆
1111人力銀行	108/7	求職者身分證字號、姓名、生日、電子郵件、電話號碼地址以及工作公司等個資遭外洩	20餘萬筆
蝦皮購物 / 誠品生活	111/5	未依《個資法》落實安全防護措施，被數位發展部裁罰	外洩筆數未具體公布，但蝦皮罰20萬 誠品生活罰10萬 (hiyun.com.tw)
LINE雅虎(LY Corp)	112/10	系統遭駭外洩使用者紀錄檔與部分員工資料	約44萬筆；其中台灣用戶近百筆 (hiyun.com.tw)
中華電信	113/2	資安團隊疑似發現資料外流，立即啟動防禦並通報	未公布具體筆數 (hiyun.com.tw)
OwlTing(旅遊平台公司)	113/7	AWS S3 儲存槽設定錯誤，旅客訂房資料外洩	約76.5萬名用戶資料，總洩漏紀錄近 900 萬筆 (informationsecurity.com.tw)
台新銀行	114/5	催收信函和信用卡帳單錯寄導致地址與帳單混亂	影響 1,447 人 (GVM)

如何避免個資外洩

- 不直接將個資傳遞(明碼傳送)
- 加密(壓縮檔、PDF)
- 檔案及文字分開
- 不使用 USB 等隨身裝置
- 紙本資料非必要保存時直接銷毀(碎紙機)
- 注意傳送個資管道是否正確(用什麼軟體、傳給誰?)
- 個資遮罩(Ex. 林○玲)

謝 謝 聆 聽