TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

國立臺南大學

111年資訊安全暨個人資料管理規範導入顧問輔導服務案
課程名稱：資安及個資保護通識教育訓練

授課日期：111年5月26日
授課講師：德欣寰宇科技股份有限公司 資安顧問 蔡元豪

簡報大綱

一 貴校資安及個資管理政策宣導

二 社交工程防護宣導

三 資安及個資保護趨勢及日常注意事項

四 資安、個資事件案例分享及分析

貴校資安及個資管理政策宣導

本校資通安全政策

資通安全管理原則

1. 重要之資訊資產應定期清查、分類分級與進行風險評鑑，並據以實施適當的防護措施。
2. 重要資訊資產存取權限應予以區分，考量人員職務授予相關權限，必要時得採行加解密(例rar)及身分鑑別機制，以加強資訊資產之安全。
3. 對於資通安全事件須有完整的通報及應變措施，以確保資訊系統、業務的持續運作。
4. 應訂定營運持續計畫並定期演練，以確保重要系統、業務於資安事故發生時能於預定時間內恢復作業。
5. 相關人員應依規定接受資通安全教育訓練與宣導，以加強資通安全認知。
6. 定期執行資通安全稽核作業，檢視存取權限及資通安全管理制度之落實。
7. 違反本政策與資通安全相關規範者，依相關法規辦理。
8. 本政策每年至少評估一次，依業務變動、技術發展及風險評鑑的結果修訂。

本校資通安全政策-目標

資通安全目標

1. 本校全年無因資訊系統安全事件而發生教職員生密級資料外洩。
2. 本校全年無因資訊系統安全事件而發生教職員生資料遭竄改。
3. 確保本校關鍵業務系統網路機房維運服務達全年上班時間96%以上之可用性，並確保：
    A. 因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每季不得超過(含)4次。
    B. 因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過8工作小時。
4. 本校關鍵業務系統服務達全年上班時間98%以上之可用性，本校關鍵業務系統因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過8工作小時。

本校個人資料保護管理政策

個人資料之保護

1. 本校已成立個人資料保護組織，明確定義相關人員之責任與義務。
2. 本校已建立與實施個人資料管理制度（以下簡稱PIMS），以確認本政策之實行；全體員工及委外廠商應遵循PIMS之規範與要求，並定期審查PIMS之運作。
3. 為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本校個人資料保護推動委員會下設工作小組，規劃、執行各項個人資料保護作業，由各一級行政單位及學院指派一人組成，個人資料保護推動委員會執行秘書擔任工作小組召集人，並依相關法令規定辦理個人資料檔案及個人資料清冊安全維護及更新事項。
4. 個人資料檔案應建立管理制度，分級分類管理，並針對接觸人員建立安全管理規範。
5. 為確保所有個人資料安全，應強化個人資料檔案資訊系統之存取安全，防止非法授權存取，維護個人資料之隱私性，應建立安全保護機制，並定期查核。
6. 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身分之登入通行碼，並視業務及重要性，考量其他輔助安全措施。
7. 個人資料輸入、輸出、存取、更新、銷毀或分享等處理行為，應釐定使用範圍及調閱或存取權限。
8. 本校各單位如遇有個人資料檔案發生遭人惡意破壞、毀損或作業不慎等安全事件，應進行緊急因應措施，並依本校「個人資料保護緊急應變處理作業說明書」通報程序辦理。
9. 本校係以嚴密之措施、政策保護當事人之個人資料，包括本校之所有教職員工生，均受有完整之個資法及隱私權保護之教育訓練。倘有洩露個資之情事者，將依法追究其民事、刑事及行政責任。
10. 本校之委外廠商或合作廠商與本校業務合作時，均應簽訂保密契約，使其充分瞭解個人資料保護之重要性及洩露個資之法律責任。倘有違反保密義務之情事者，將依法追究其民事及刑事責任。

本校個人資料保護管理政策-目標

本校個人資料保護管理之目標如下：

1. 依「個人資料保護法」、「個人資料保護法施行細則」與相關標準/規範要求，保護個人資料蒐集、處理、利用、儲存、傳輸、銷毀之過程。
2. 為保護本校業務相關個人資料之安全，免於因外在威脅，或內部人員不當之管理與使用，致遭受竊取、竄改、毀損、滅失、或洩漏等風險。
3. 提升對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境。
4. 為提升同仁個人資料保護安全意識，每年定期辦理個人資料保護宣導教育訓練。
5. 定期針對個人資料流程進行風險評鑑，鑑別可承受風險等級。

資通安全管理法架構

資通安全事件通報及應變辦法

- 第四條

公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。

- ==>「知悉」認定，如為技服中心INT警訊通報或攻防演練通報，為收到e-Mail起算1小時內進行事件通報，其餘自行發現之資安事件，應於知悉後一小時內進行通報。

本校個人資料保護管理政策-個人資料之蒐集與處理

個人資料之蒐集與處理

1. 本校因營運所需取得或蒐集之包括但不限於個人之姓名、出生年月日、國民身分證統一編號（護照號碼）、特徵、指紋、婚姻、家庭、教育、職業等個人資料，應遵循我國個人資料保護法等法令，不過度且符合目的、相關且適當並公平與合法地從事個人資料之蒐集與處理。

個資法所稱之個人資料

一般個資

.姓名
.出生年月日
.國民身分
.統一編號
.護照號碼
.特徵
.指紋
.婚姻
.家庭
.教育
.職業
.聯絡方式
.財務情況
.社會活動

特種個資

.病歷
.醫療
.基因
.性生活
.健康檢查
.犯罪前科

得以直接或間接方式識別該個人之資料

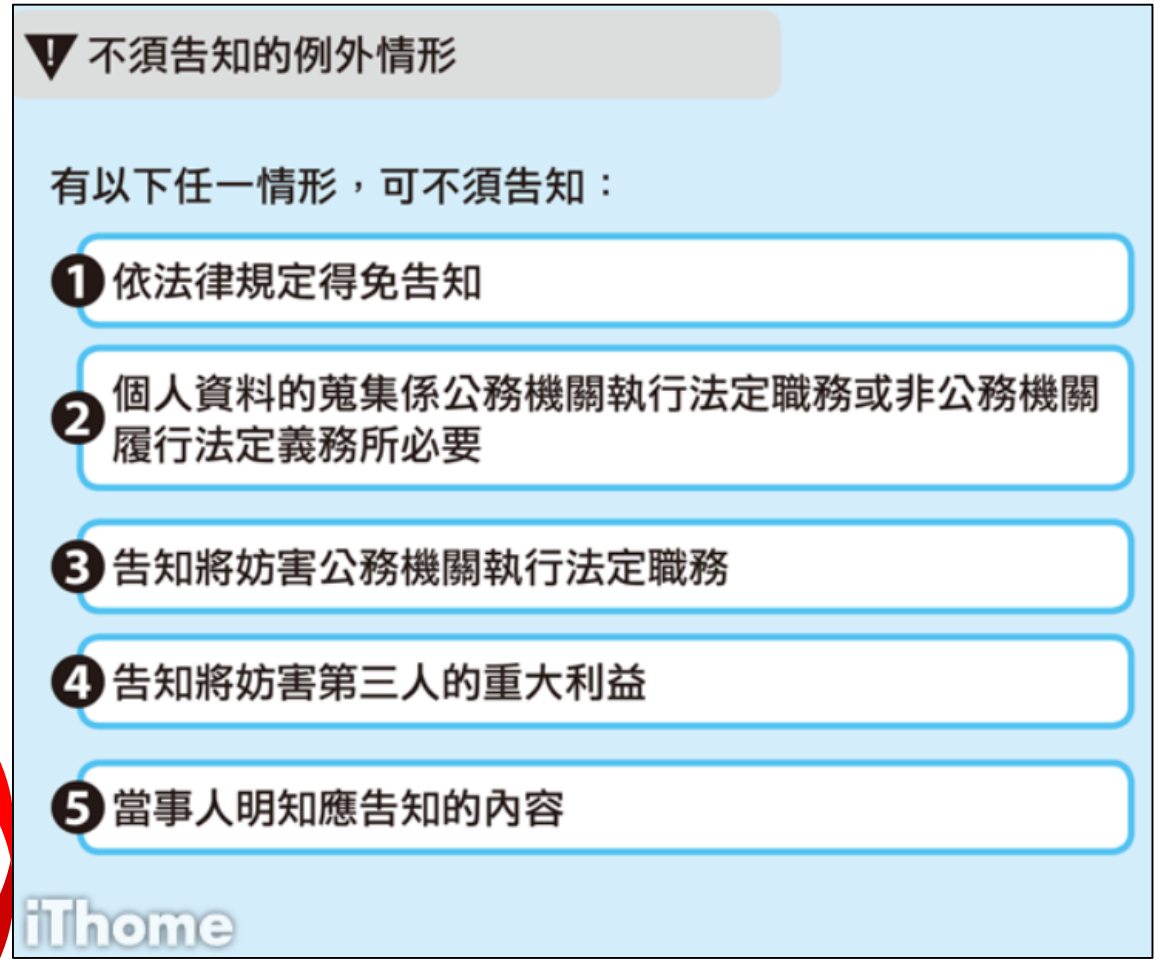
個資法所指行為定義 §2

個資法個人資料之告知義務§8

公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

- 一、公務機關或非公務機關名稱。
- 二、蒐集之目的。
- 三、個人資料之類別。
- 四、個人資料利用之期間、地區、對象及方式。
- 五、當事人依第三條規定得行使之權利及方式。
- 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響

如果是間接收集個資(非當事人提供)，需向當事人告知上述**第一項至第五項**所列事項。
(個人資料保護法§9)



本校個人資料保護管理政策-個人資料之利用及國際傳遞

個人資料之利用及國際傳遞

- 本校於利用個人資料時，除需依個資法之特定目的必要範圍內為之外，如需為特定目的以外之利用時，將依據個資法第16條之規定辦理；倘有需取得當事人同意之必要者，本校應依法取得當事人之同意。
- 本校所蒐集、處理之個人資料，應遵循我國個資法及本校個資管理制度之規範，且個人資料之使用為本校營運或業務所需，方可為本校承辦同仁利用。
- 本校取得之個人資料，如有進行國際傳遞之必要者，定謹遵不違反國家重大利益、不以迂迴方法向第三國傳遞或利用個人資料規避個資法之規定等原則辦理，又，倘國際條約或協定有特別規定、或資料接受國對於個人資料之保護未有完善之法令致有損害當事人權益之虞者，本校將不進行國際傳遞，以維護個人資料之安全。

本校個人資料保護管理政策-個人資料之例外應用(1/2)

本校因業務上所擁有之個人資料負有保密義務，除當事人之要求查閱或有下列情形外，應符合個資法第16條及相關法令規定，並以正式公文查詢外，本校不得對第三人揭露：

- 司法機關、監察機關或警政機關因偵查犯罪或調查證據所需者。
- 其他政府機關因執行公權力並有正當理由所需者。
- 與公眾生命安全有關之機關（構）為緊急救助所需者。

本校個人資料保護管理政策-個人資料之例外應用(2/2)

本校對個人資料之利用，除個資法第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：

- 法律明文規定。
- 為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、自由或財產上之危險。
- 為防止他人權益之重大危害。
- 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 經當事人同意。

此項同個資法第16條

特種個人資料之蒐集、處理及利用-個人資料保護法§6

有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

- 一、法律明文規定。
- 二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 三、當事人自行公開或其他已合法公開之個人資料。
- 四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。

當事人對自身個資之權利-個人資料保護法§3

§3，當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

一.查詢或請求閱覽。
二.請求製給複製本。
三.請求補充或更正。
四.請求停止蒐集、處理或利用。
五.請求刪除。

可拒絕當事人行使權利情形

一、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。
二、妨害公務機關執行法定職務。
三、妨害該蒐集機關或第三人之重大利益。

本校個人資料保護管理政策-個人資料之調閱與異動

個人資料之調閱與異動

- 當本校接獲個人資料調閱或異動之需求時，應依個資法及本校所訂之程序，請當事人填具「個人資料使用資訊服務申請表」，於合法範圍內進行當事人之個人資料查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理、利用、請求刪除。

資訊安全基本概念

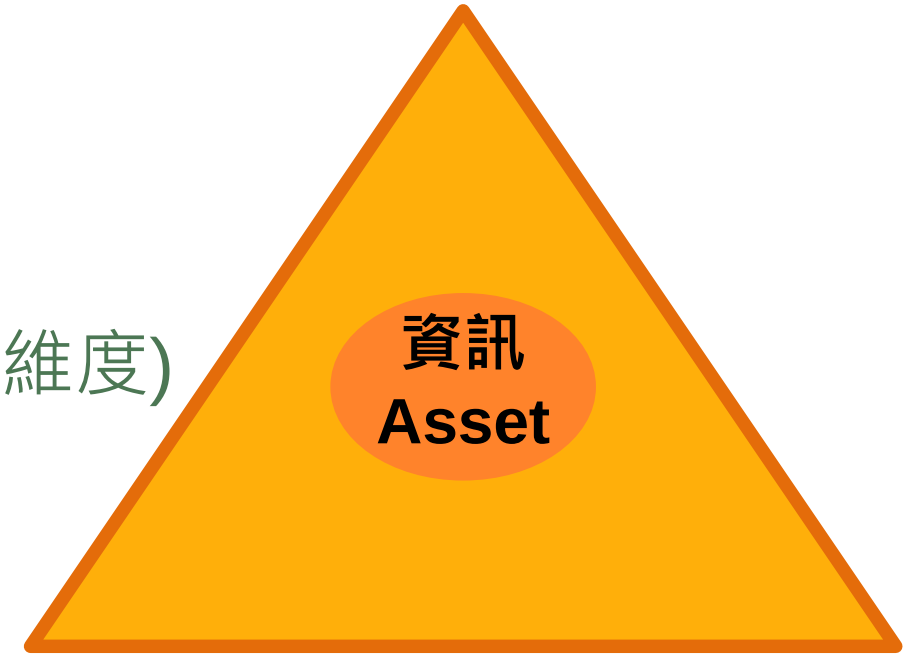
- 何謂資訊？

  資訊是一種資產，像其他重要的組織資產一樣對組織**有價值**，而且需要**適當**的**保護**。

資訊安全管理的目的

保護資訊資產，避免遭受各種威脅及降低可能危害

機密性、完整性及可用性
常被作為資訊安全CIA的三角(維度)



資訊是組織營運的資產

- 資訊是組織的重要資產並且也是所有業務流程的一部分。
- 包含營業秘密、專利、人員隱私和業務構想等。

它被視為組織的資產

建立資訊資產所需的成本、技術、時間及資源

資訊資產的資料分類是確保機密性及所有者

它是組織企業形象的一部分

資料損失會**影響**組織在不同業務活動的**投資**

個資及資訊資產盤點

- Q：為什麼要進行個資及資訊資產盤點並建立清冊？
- A：

  1、清楚各業務流程辦理所牽涉到的資產，快速了解該單位全部資產情況。

  2、人員調動時，快速、完整進行資產交接。

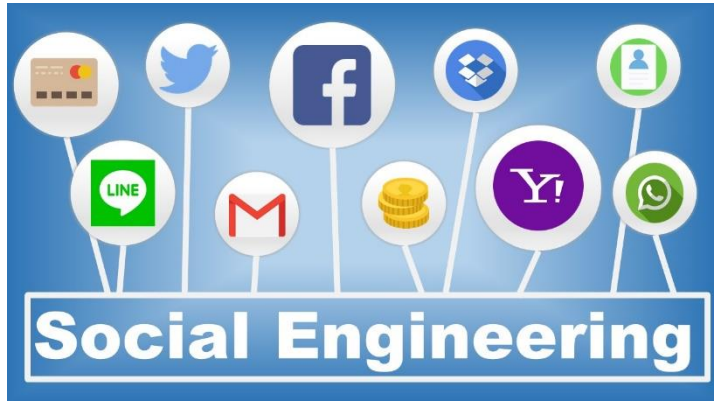
  3、識別各資產價值，進行後續風險評鑑並執行對應安全控管措施，以減少事件發生時對組織的衝擊或事件發生的可能性。

  4、倘若事件發生時能釐清管理權責，保障自身權益。

社交工程防護宣導

何謂社交工程

- 社交工程兩個基本要件：
  - 第一個是【人】
  - 第二個是【詐騙手法】
- 凡對【人】甚至於【特定對象】，
  使用各種【詐騙手法】，
  獲得不當資訊，來達到施騙者的目的，
  都可稱之為【社交工程】。



圖片來源：https://cms.aaasec.com.tw/index.php/2018/06/13/0005/

駭客如何利用員工社群網站入侵公司

社交工程攻擊手法

- 早期社交工程是使用電話或其他非網路方式來詢問個人資料，現今社交工程大都是利用電子郵件或網頁來進行攻擊。
- 透過電子郵件進行攻擊之常見手法
  - 假冒寄件者
  - 使用與業務相關或令人感興趣的郵件內容
  - 含有惡意程式的附件或連結
  - 利用應用程式之弱點 (包含零時差攻擊)

網路釣魚的威脅

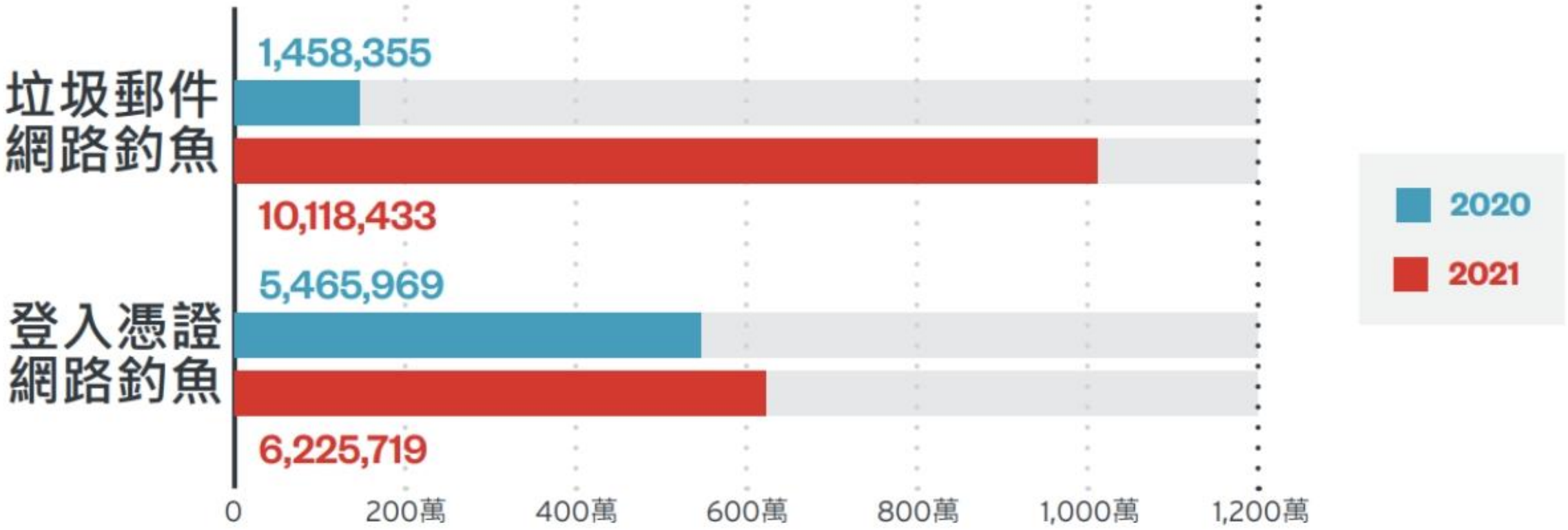


圖 3：垃圾郵件網路釣魚與登入憑證網路釣魚偵測數量比較 (2020 及 2021 年)。

資料來源：趨勢科技 Cloud App Security。

網路釣魚郵件範例

網絡釣魚攻擊的防範，包括**不隨意開啟**可疑來源發送的電子郵件。
並鼓勵用戶和組織將其瀏覽器**升級**到**最新**版本，以防止透過**漏洞**而受到損害。

資料來源：https://www.trendmicro.com/en_us/research/21/a/earth-wendigo-injects-javascript-backdoor-to-service-worker-for-.html

各類型社交工程演練郵件範例

項次	類型	演練郵件主旨
1	時事類	遠距工作挑戰多 調查：三分之二台灣企業更重視資安
2	財經類	全球經濟命脈竟都依賴台積電，「晶片危機」對台灣是好是壞？
3	保健類	遠距教學致近視度數暴增 眼科醫師3招護眼
4	科技類	快卸載！8款惡意修圖APP竊個資、盜刷手機信用卡
5	生活類	紓困4.0再放寬！2類人最多可領3萬 估60萬人受惠

開啟 信件率	連結 點選率	開啟 附件率
? %	? %	? %

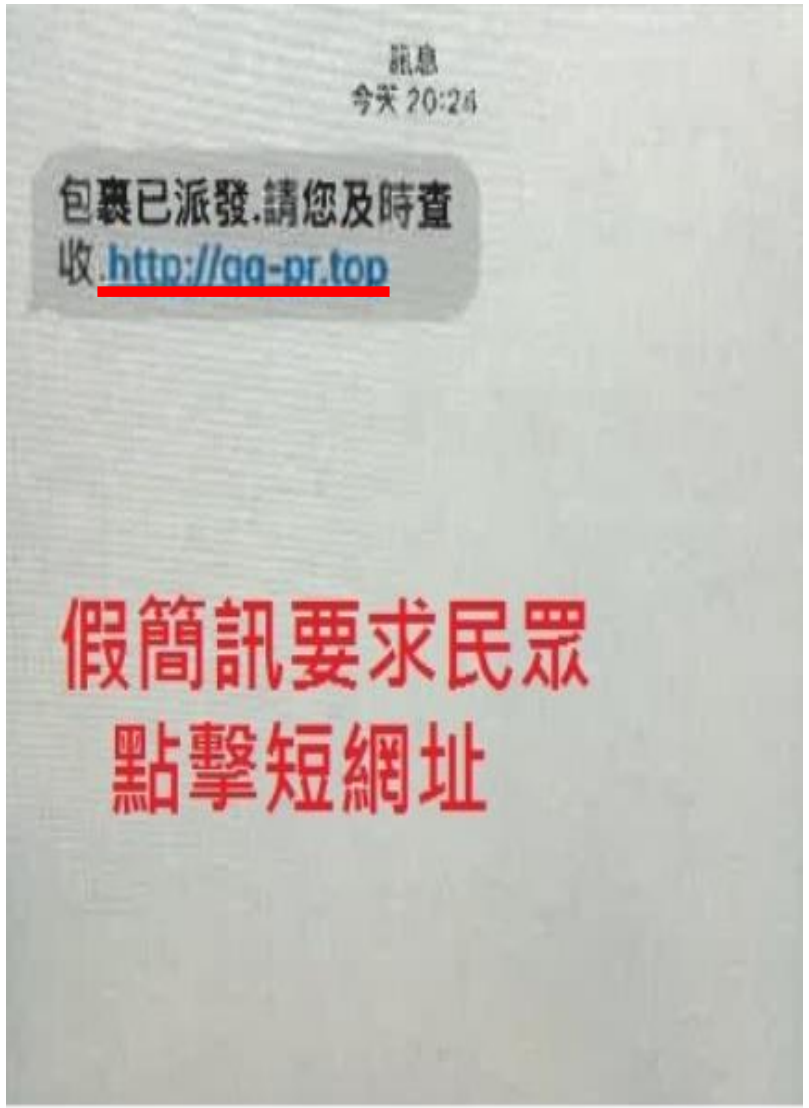
E-Mail信件潛藏的危機

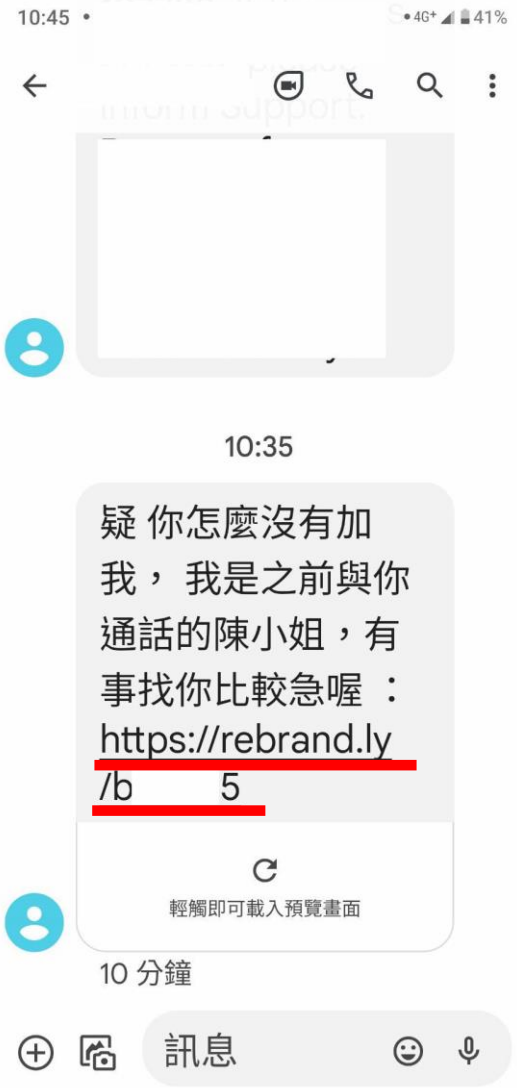
使用電子郵件信箱時，開啟來路不明郵件，可能造成**電腦中毒**；或輕信郵件的真實性，而**讓駭客有機可乘**，發動**社交工程攻擊**。

- ✓ Outlook或WebMail設定：關閉信件預覽及自動下載圖檔功能，以**純文字模式**閱讀郵件，開啟信件應注意寄件者帳號。
- ✓ 公務信箱不應作為外部社群網站之用，「外部訊息」及「個人訊息」應使用私人信箱接收。
- ✓ 接收電子郵件時保持**警覺**。
- ✓ 切勿於網頁隨意提供機密資訊，如：**公務用電子郵件帳號**、密碼、信用卡號碼等。

資料來源：https://www.twcert.org.tw/tw/cp-15-49-b8b01-1.html

釣魚簡訊夾帶不明連結





資料來源：https://www.police.ntpc.gov.tw/cp-21-64059-1.html

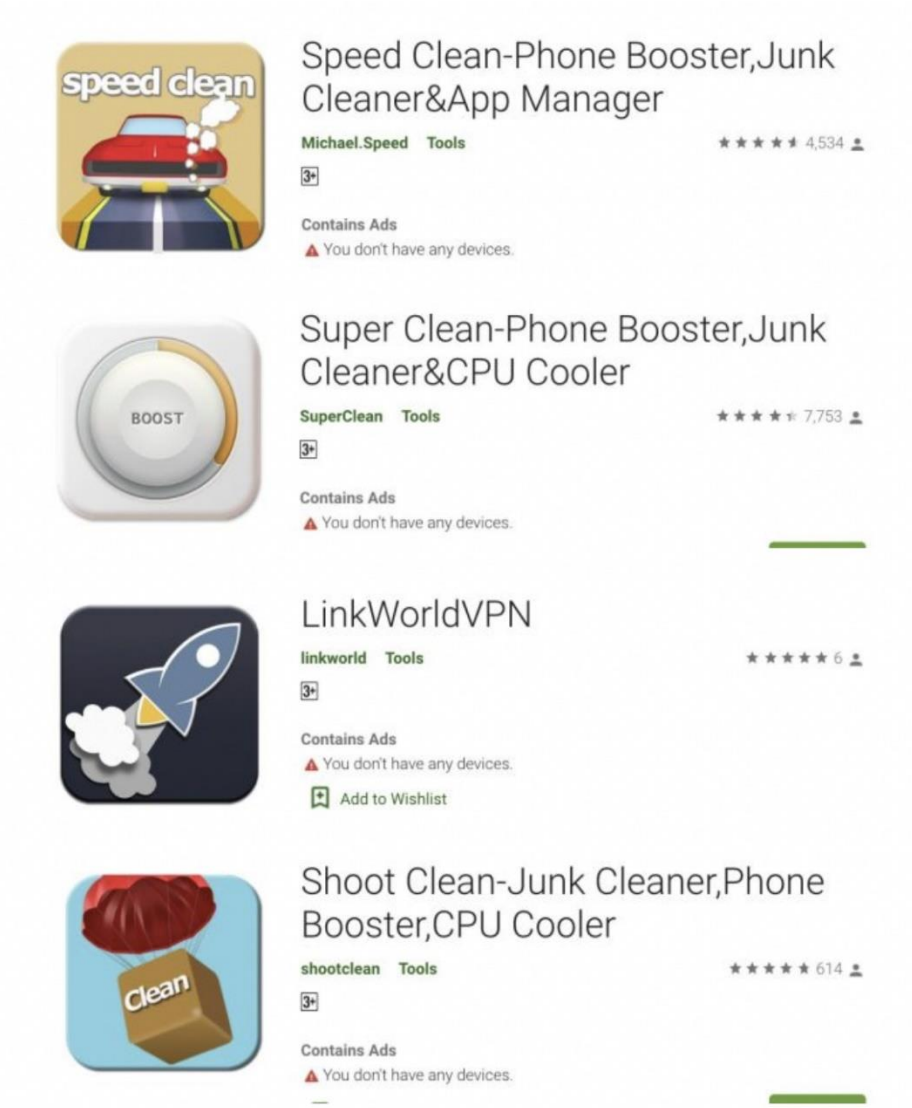
簡訊中的惡意連結

透過安裝程式
獲得手機各種權限
竊取使用者資料

資料來源：https://cert.tanet.edu.tw/prog/index.php

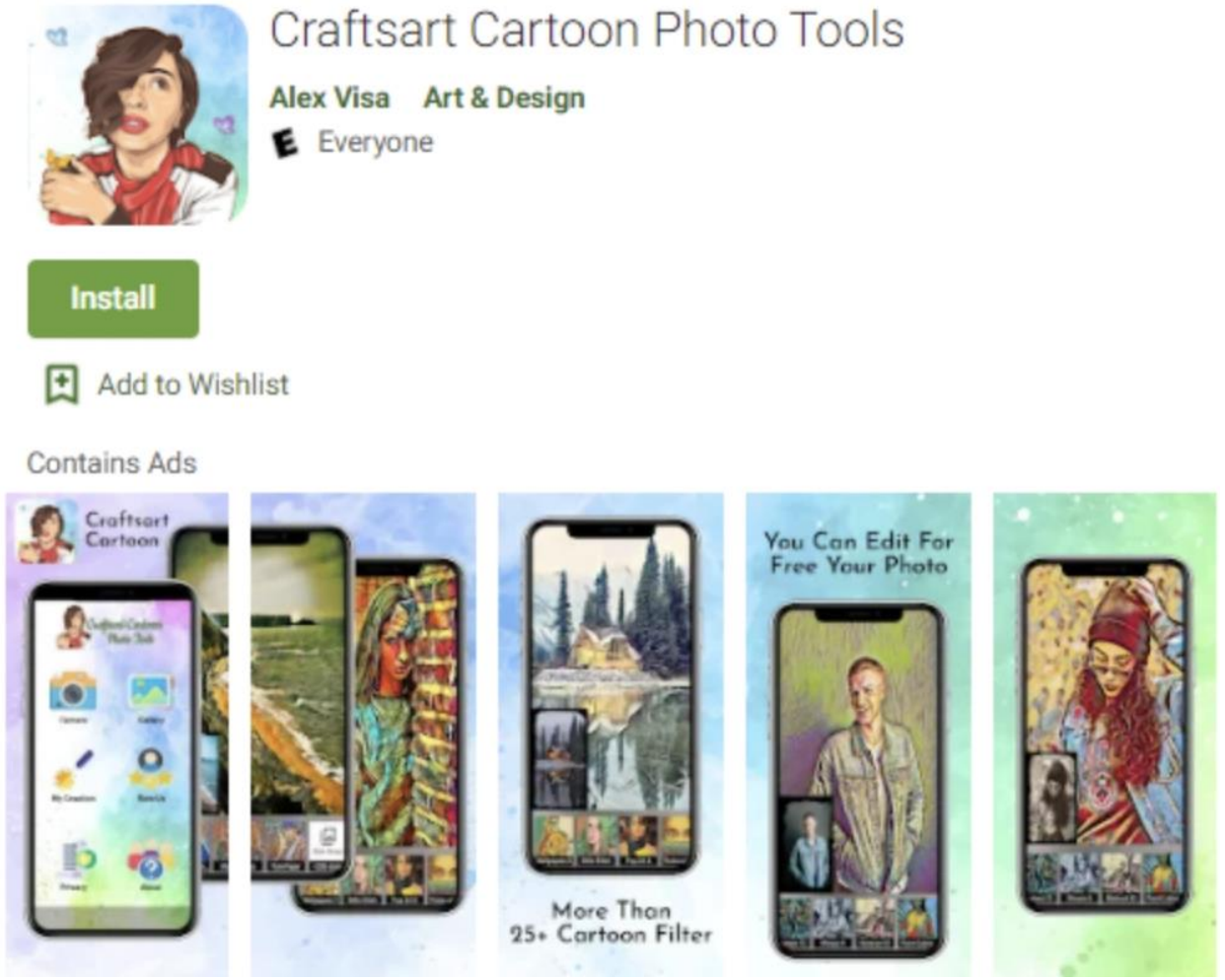
來路不明優化系統的程式

原本應該用來協助清除、整理、刪除無用檔案以優化系統的程式，化身為惡意程式。
在應用程式商店發表正面評價來推升這些惡意程式的人氣，此外不只會向受害者推送廣告,還會幫你點選彈出的廣告,來從事各種廣告詐騙,連推薦頁面底下都會顯示一些惡意廣告內容與木馬程式,並可用受害者的 Google 和 Facebook 帳號登入被遠端安裝的惡意應用程式 。



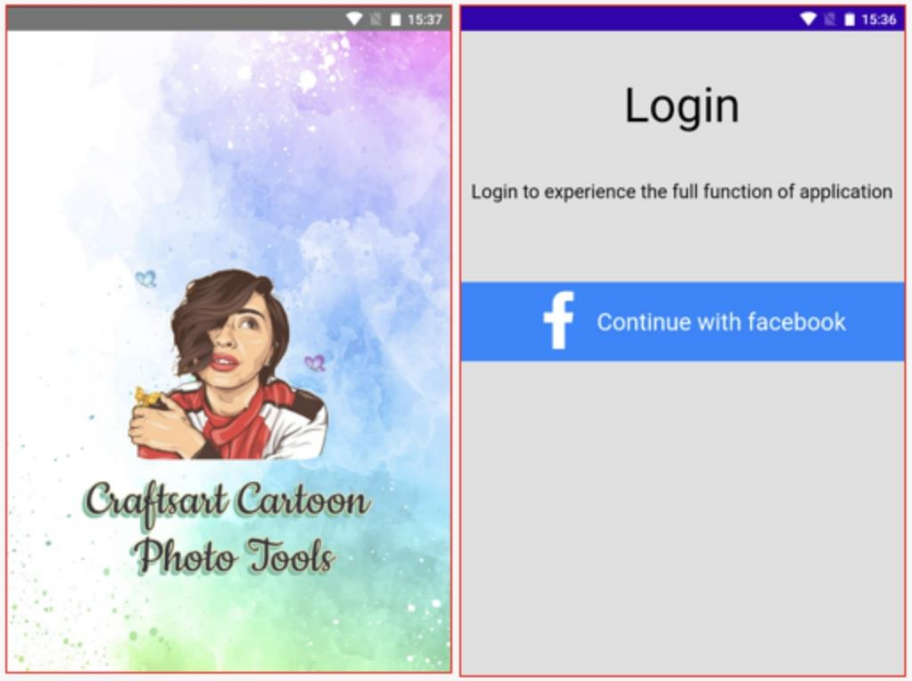
手機應用程式的風險

一款程式的名稱為Craftsart Cartoon Photo Tools，號稱可協助使用者將照片編輯成卡通人物



應用程式要求登入使用者帳戶

轉跳Facebook登入頁面，實際為釣魚頁面，目的在於盜取使用者登入資訊



圖片來源 / Pradeo

當使用任何程式時，轉跳出類似登入畫面都要有所警惕！

手機中毒時症狀

①耗電量大幅增加
②過熱
③不時彈出不明視窗
④數據使用量（網路流量）異常
⑤出現不明應用程式
⑥電話帳單出現不明費用

(圖翻攝自Ibtimes)

APP免費試用訂閱的陷阱

Android 和 iPhone 手機上的 App 常遇到只要 “訂閱” 就可以免費試用付費功能一些時間（如：1個禮拜或1個月等），但這些 App 往往會在你不知情的情況下，讓你於試用期結束之後持續付費訂閱服務，在試用期後就開始自動續約扣款。

在收到帳單後有的人才把 App 刪除了，以為這樣就能夠取消被扣款，殊不知過了該月後還是收到扣款訊息？

Android取消訂閱(步驟1-4)

IOS取消訂閱(步驟1-2)

1

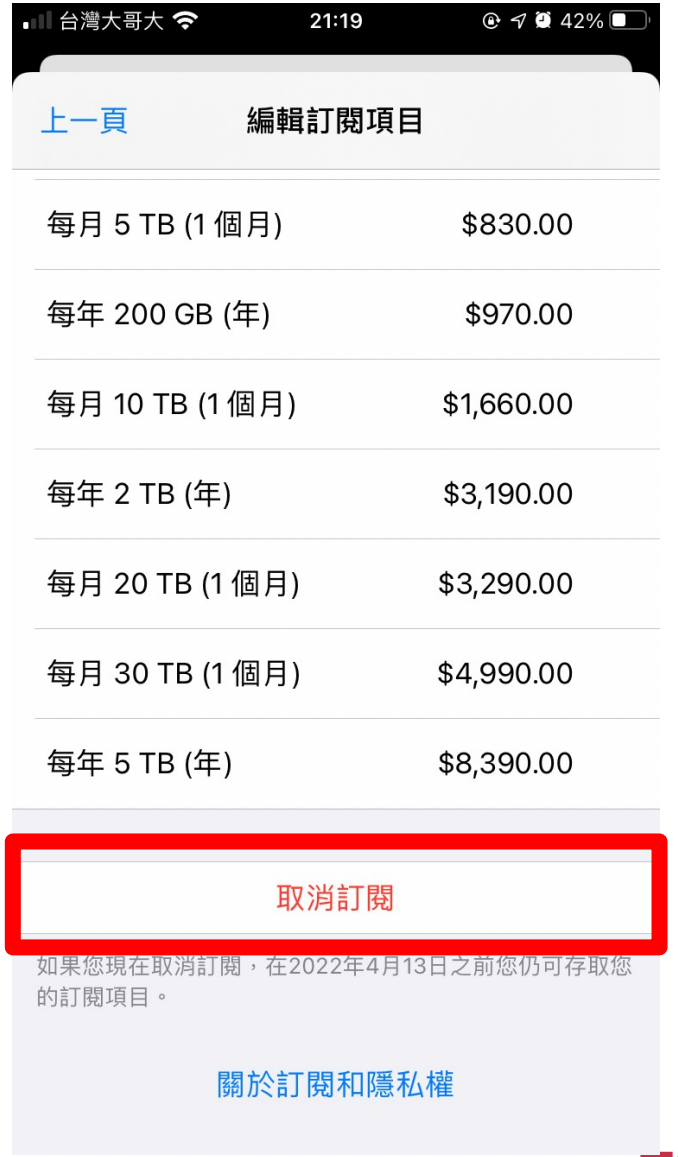
2

下一頁

IOS取消訂閱(步驟3-4)

3

4



陌生來電顯示

Whoscall 來電號碼辨識APP

警政署為增強防制力道，協助辨識來電者真實身份，從2016年6月份起，與Whoscall公司合作，透過政府165反詐騙專線的大數據整合，目前民眾利用Whoscall APP可協助辨識超過6000萬筆電話號碼，大幅阻擋詐騙、推銷、騷擾等惡意電話。

資料來源：https://blog.whoscall.com

什麼是釣魚網站？

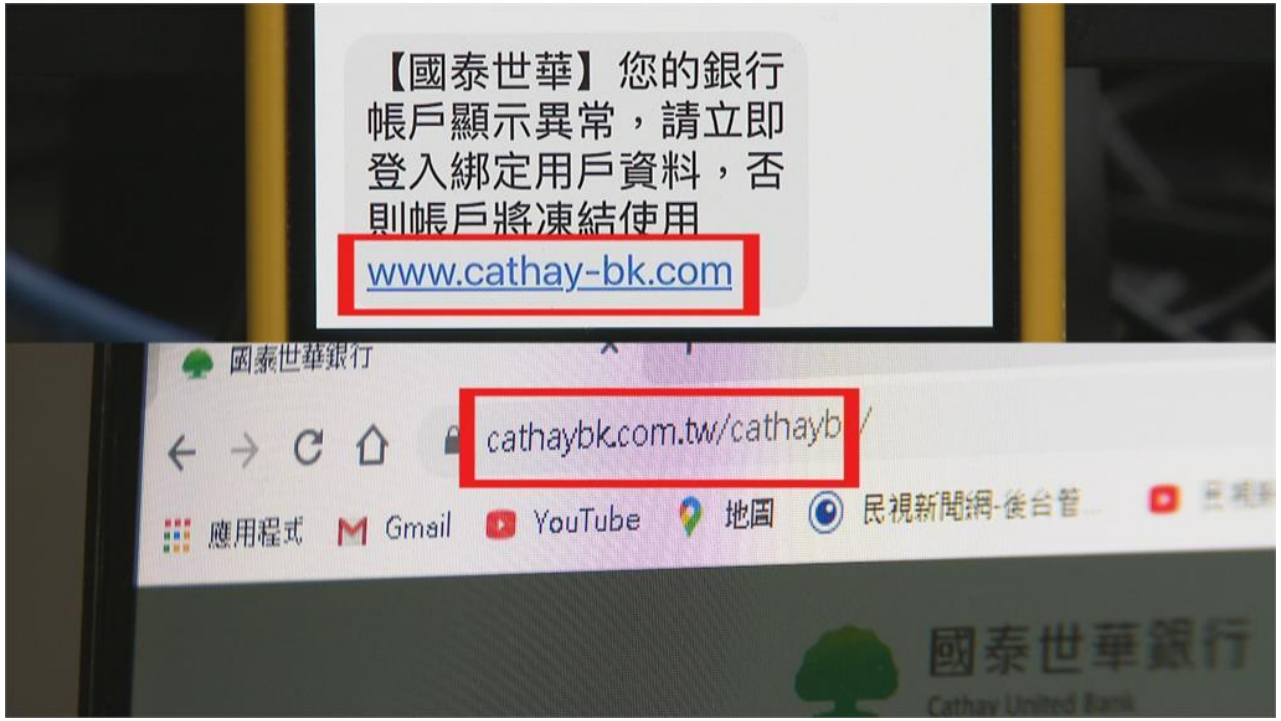
http://www.landbank.com.tw

銀行網址??

- 不明連結
- 電子郵件連結
- 簡訊連結

http://www.1andbank.com.tw (釣魚網頁)

銀行釣魚簡訊 3天21人被騙300萬



假的國泰銀行網站和正版官網幾乎做的一模一樣，27日到29日短短3天，就有83人檢舉，多達21個人受騙，詐騙金額300多萬，不過目前釣魚網站已經下架。

圖片來源：https://news.tvbs.com.tw/local/1459350
資料來源：https://www.ftvnews.com.tw/news/detail/2022131F04M1

假以亂真的釣魚網頁

看起來很像google登入頁

網頁網址像這樣

http://login.google.com.evilphishingsite.com/index.html

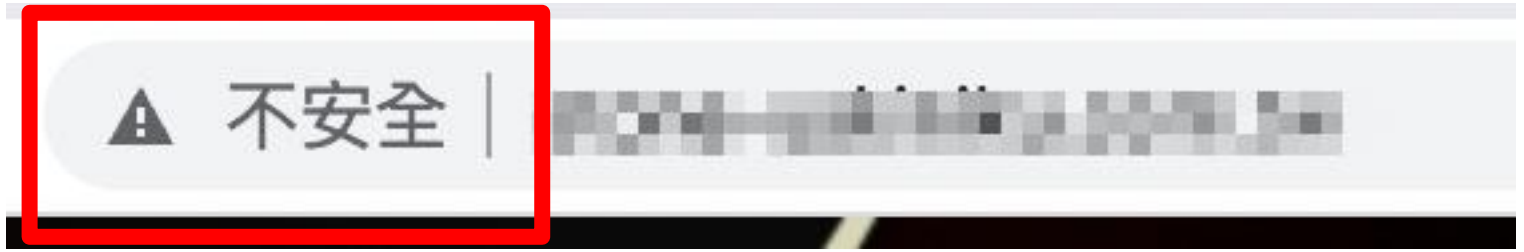
網址中夾帶可疑文字?

不是https?

HTTP與HTTPS

HTTPS的S代表意義為使用SSL/TLS來加密封包

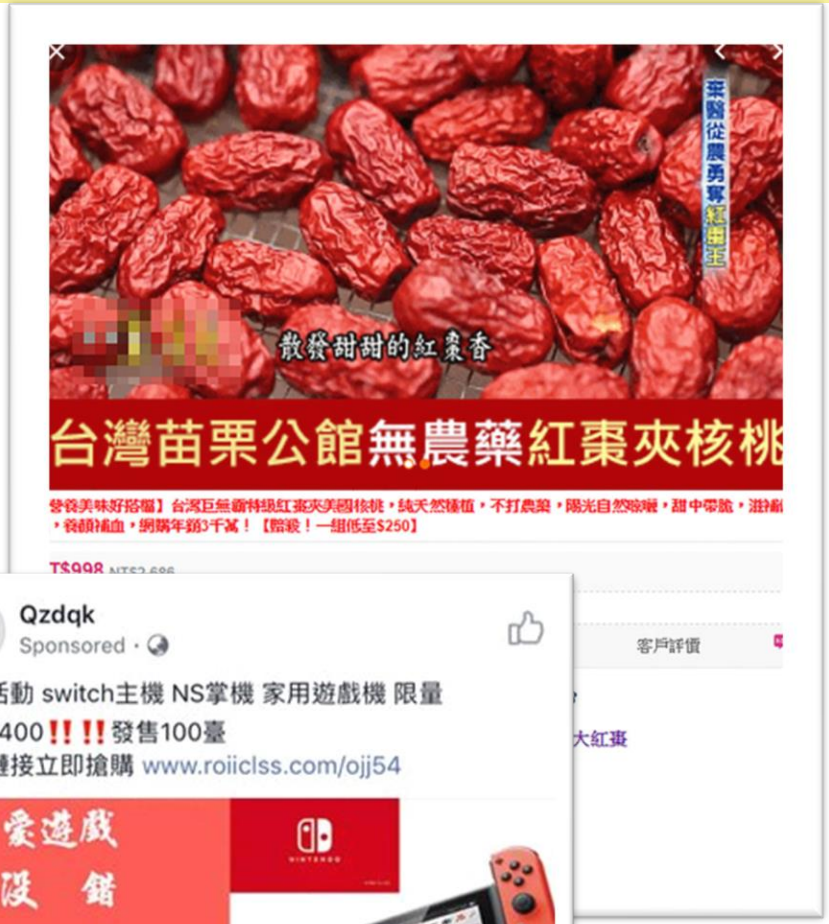
傳輸過程未加密

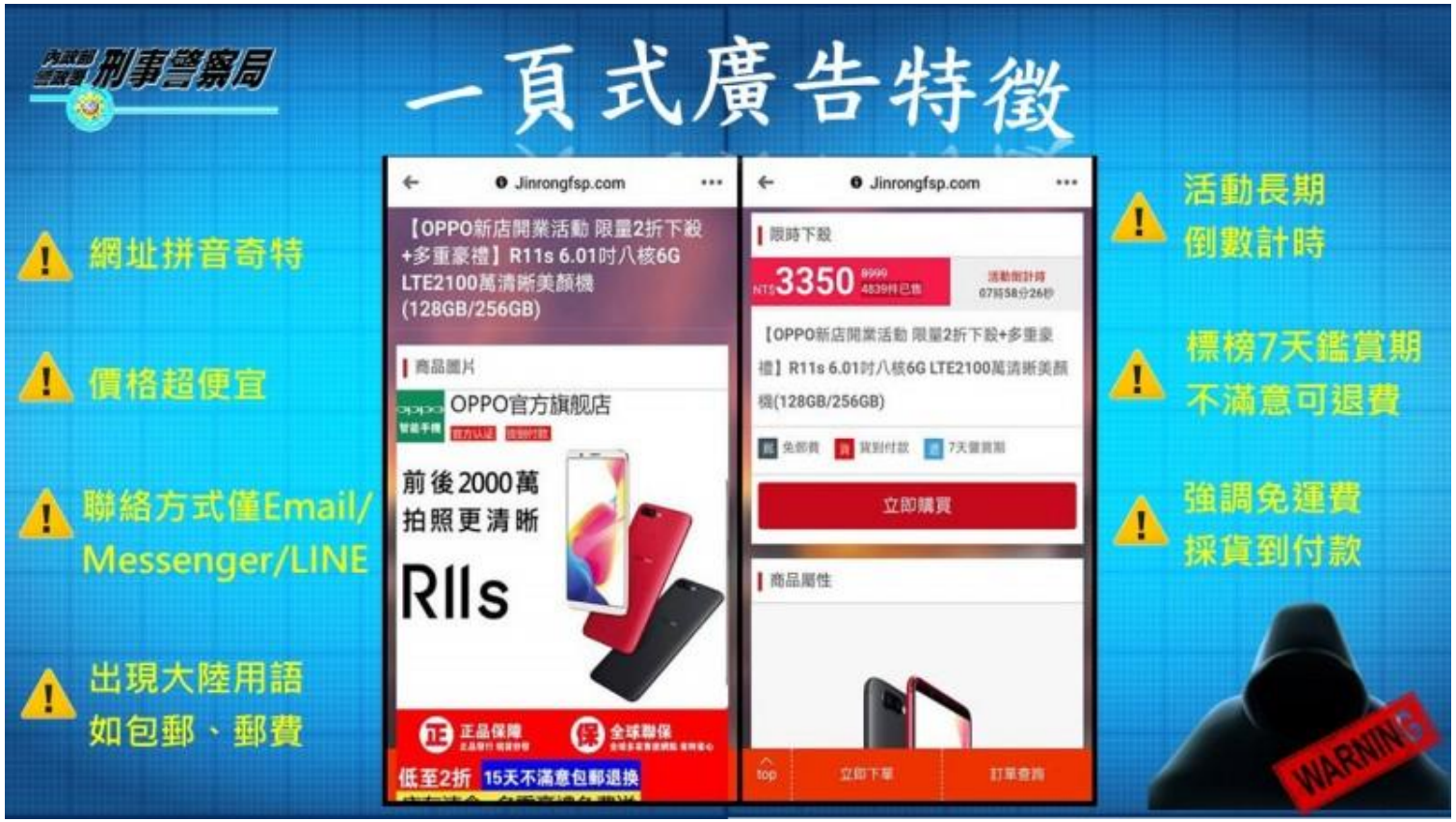


切記：勿在不安全的網站內輸入任何重要資訊

傳輸過程加密

越來越像真的電商平臺





圖片來源：https://www.tucheng.police.ntpc.gov.tw/cp-530-61328-19.html

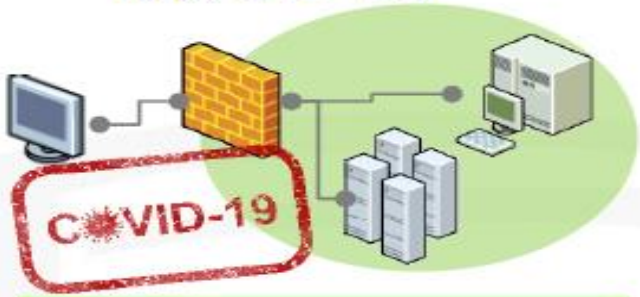
突然跳出廣告頁面

不要掉入陷阱！

資安及個資保護趨勢及日常注意事項

全球資通安全威脅趨勢

- 綜整110年全球資安威脅與相關研究報告，歸納全球資安威脅趨勢



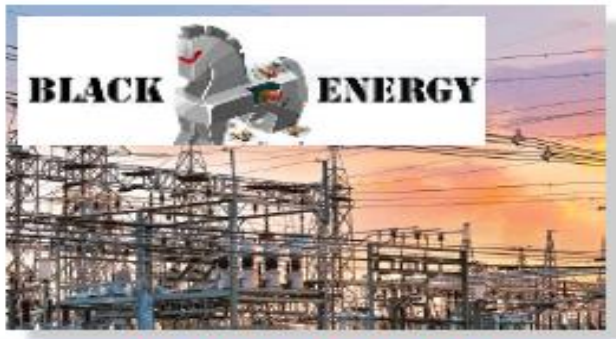
遠距工作型態
促使網路攻擊提升

勒索軟體攻擊
風險激增

社交工程手法仍頻繁

國家層級駭客
攻擊仍頻繁

資安(訊)供應商持續遭
駭破壞供應鏈安全



關鍵基礎設施
資安風險倍增

資料來源：1.ENISA Threat Landscape 2021
2.ACSC Annual Cyber Threat Report
3.Microsoft Digital Defense Report
4.Fortinet Global Threat Landscape Report

認識勒索病毒

勒索病毒的威脅

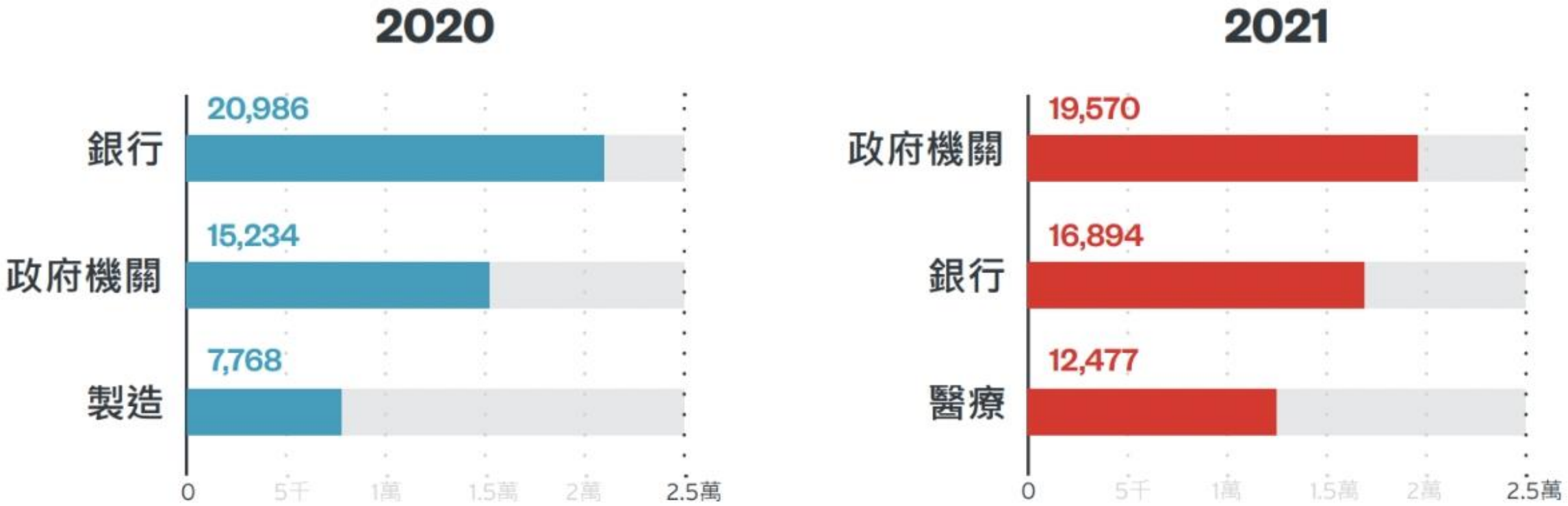


圖 1：勒索病毒檔案偵測數量前三名的產業 (2020 及 2021 年)。

資料來源：趨勢科技 Smart Protection Network™ 。

如何防範勒索病毒?

- ✓資安意識
- ✓定期備份
- ✓防毒軟體
- ✓定期更新

圖片來源：https://briian.com/28172/

何謂虛擬貨幣？

「虛擬貨幣 Virtual Currency」又稱數位貨幣或加密貨幣，由非國家政府之開發者發行及管控，通常不包含國家發行之電子貨幣（信用卡幣、悠遊卡幣）。

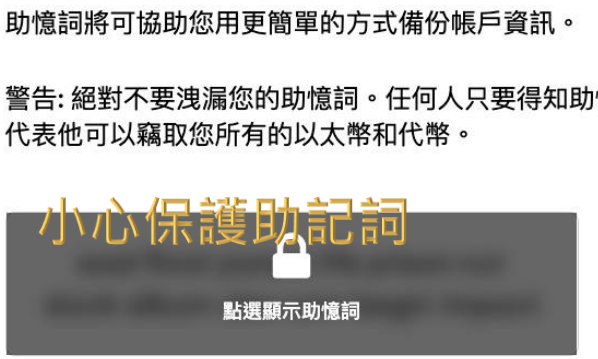
虛擬貨幣最大特色：**「去中心化」**，意即為去中心化的貨幣系統，一反傳統貨幣，有中央銀行在負責貨幣的發行管理，其與傳統貨幣不同在於：可避免中央銀行的不良政策與人為干擾所造成的通貨膨脹緊縮，還可降低交易成本，並具**匿名性**。

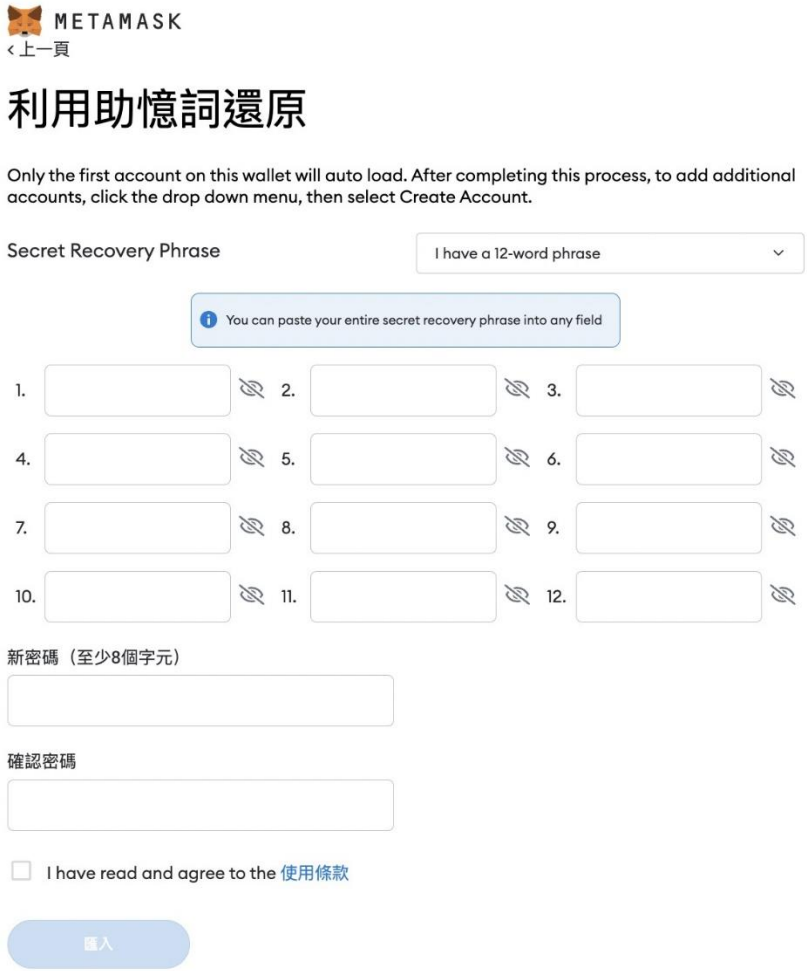
虛擬貨幣衍生風險

- 假交易平台
- 假虛擬貨幣錢包
- 助記詞詐騙
- 假行情（資金盤）

虛擬貨幣錢包註記詞的重要性？

雖首次創建錢包時會要求設定個人密碼，
如更換設備或需使用新設備需登入您的錢包時，
主要靠的是**系統原始產生**的**助記(憶)詞**，
而不是您創建錢包時設定的個人密碼。





魷魚幣

110年10月26日，魷魚幣交易價值只有1美分，才不到一個星期的時間，魷魚幣價值飆高到2856美元，隨後創辦人將貨幣大量變現，導致虛擬貨幣價格迅速崩跌，根據加密貨幣數據網站CoinMarketCap顯示，魷魚幣的幣值現在下跌了99.99%，幾乎歸零，沒有任何價值。

狗狗幣

特斯拉（Tesla）執行長伊隆．馬斯克（Elon Musk）在推特上的發文，以及大陸全面封殺虛擬貨幣、各國加強監管機制等影響下，導致狗狗幣幣值暴漲又暴跌，從5月約0.74美元的高點，崩盤至6月底的0.16美元，短短1個月大跌逾78%。

虛擬貨幣的行情大起大落

鮭魚幣（Squid）

狗狗幣、多吉幣（Doge）

何謂NFT?

NFT（Non-Fungible Token）「非同質化代幣」

- 透過區塊鏈公開透明、不可竄改的特性，將數位資產的所有權紀錄，透過代幣（token）的方式交易，舉凡音樂、藝術創作、體育卡牌等，都可以有一個數位版的所有權。
- 每一個NFT都是獨一無二、不可相互替代的，而且交易時不可以被分拆。

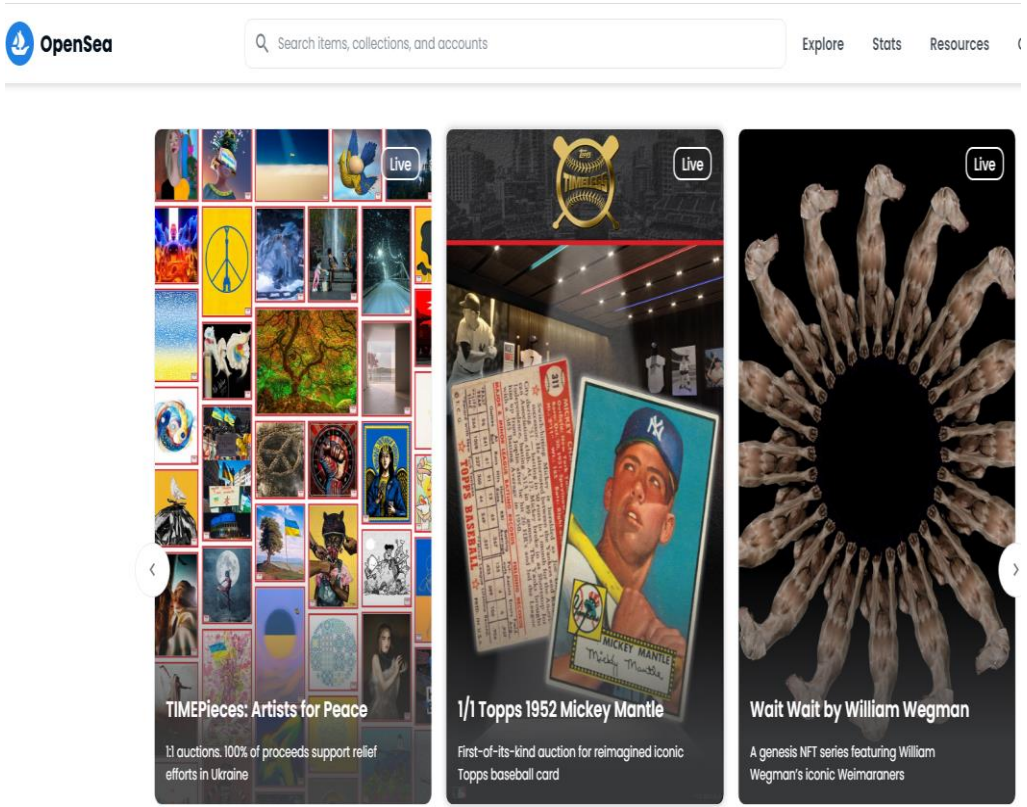
數位藝術家Beeple的作品，以6,900萬美元（約新台幣19億元）賣出

名人紛紛推出聯名NFT

- 2022年元旦，亞洲流行音樂天王周杰倫旗下潮牌PHANTACi選在這一天與平台Ezek共同推出NFT（非同質化代幣）「Phanta Bear」（幻想熊）。
- 一萬隻NFT須用虛擬貨幣「以太幣」（ETH）交易，一隻起價高達0.26顆以太幣（當時價值約2.8萬元新台幣），但只花了40分鐘就完售，短短7天更在全球最大的NFT交易平台OpenSea總榜登上全球第一名。

NFT交易平台

- 全球最大的非同質化代幣（Non-Fungible Token，NFT）市集OpenSea於（2/18）更新合約，隔天就傳出遭到駭客開採，有用戶的NFT被盜。
- 不過，OpenSea共同創辦人暨執行長Devin Finzer表示，看起來像是用戶遭到網釣攻擊，而非OpenSea平臺的安全問題。



參考資料：https://opensea.io/
https://www.ithome.com.tw/news/149472

NFT相關詐騙手法

1-假NFT網站（釣魚網站）

2-優惠價格販售（低於行情價）

3-假技術支援

- 透過Discord
- 透過電子郵件

4-以贈品方式贈送

5-假NFT專案或項目（抽地毯詐騙）~~（割韭菜）~~

避免落入NFT騙局(1)

1-檢查價格

詐騙如果一個網站上的NFT報價**遠低於**OpenSea等合法網站上的報價，則可能是一場騙局。

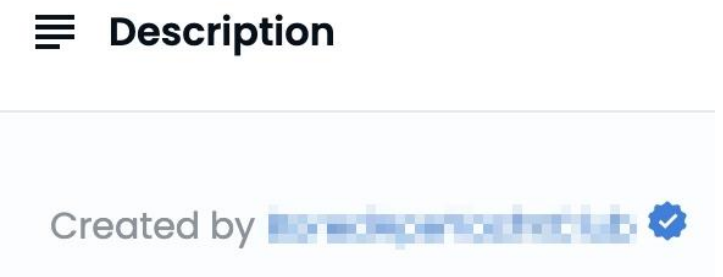
2-檢查驗證標記

大多數合法NFT賣家的使用者名稱旁邊會出現**藍色勾勾標記**。

3-檢查描述（Created by Someone)

它應該說明NFT**是在哪裡或誰鑄造**。

可以查看創作者網站來確認資訊的真實性。



4-聯絡NFT交易網站的官方客服

需要幫助時請聯絡NFT交易網站的官方客服，而不是透過其他社群媒體上出現的**人、連結及資訊**。

避免落入NFT騙局(2)

5-小心使用錢包憑證資訊

小心使用你的錢包憑證資訊，切勿分享你的**助記詞（回復碼）**。

6-使用合法擴充程式

使用合法錢包應用程式和瀏覽器擴充程式以避免**網路釣魚**。

有很多惡意應用程式會冒充成官方應用程式。

7-啟用雙因子身份認證

使用**強密碼**並啟用雙因子身份認證（2FA）來保護你的帳號。

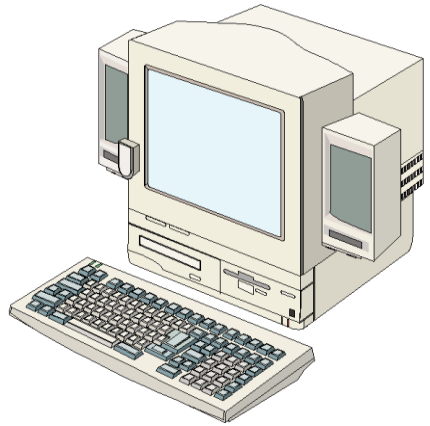
（如：交易或登入需要密碼及**簡訊認證**、提領現金需要提款卡及密碼等）

8-勿點開來路不明的連結

切勿點開來路不明的**連結**或**附件**。

日常所使用的密碼安全嗎？

常見的低強度密碼設置如下：



- 多組帳戶使用**相同密碼**
- 使用**生日**當密碼（如：19820101）
- 純**數字**無夾帶其他字元（如：123456）
- 密碼長度**太短**，不足8碼（如：awed92）
- 與**帳號相同**
- 常見或有意義**單字**（如：password）
- 連續或有**規律**字母（如：abcdefg、zxcvb)

密碼暴力破解

HIVE SYSTEMS 的報告中指出，由於現行繪圖卡上的繪圖處理器計算能力大幅提升，因此能在更短的時間內，利用**暴力破解**，快速破解**字元數不足**或**複雜度不足**的密碼。

字元組合	密碼長度	破解速度
僅有數字	8	**立即**
僅有小寫英文字	8	**5秒**
英文字（含大小寫）	8	**22分鐘**
數字＋英文字大小寫	8	**1小時**
數字＋英文字大小寫＋標點符號	8	**8小時**

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

資料來源：HIVE SYSTEMS

多因子驗證機制

身分驗證技術依其所運用的驗證因子 (Authentication factor)，可概分為三類：

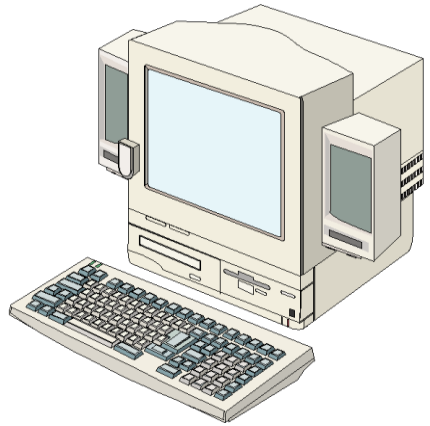
(一) 知識(Knowledge)因子：使用者所知之事 (Something the user knows)，
如： 使用者帳號及密碼、通行密碼片語、安全問題等。

(二) 持有(Ownership)因子：使用者所持之物 (Something the user has)，如：
智慧卡、 晶片卡、憑證、動態密碼產生器等、手機簡訊。

(三) 固有(Inherence)因子：使用者所具之形 (Something the user is or does)，
如： 使用者的臉型、指紋、DNA、虹膜、掌紋等生物特徵。

加強密碼安全性

密碼設置建議如下：

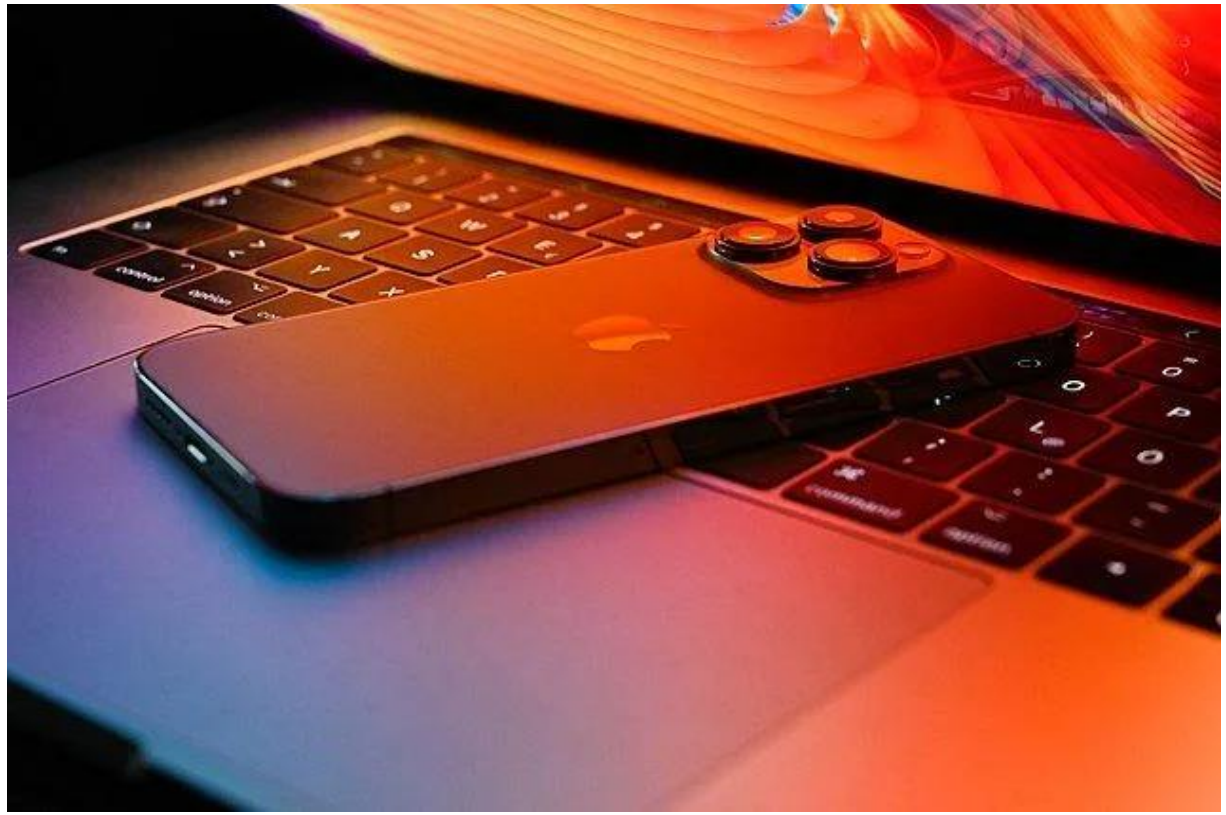


- 多組帳戶使用**不同密碼**
- 密碼長度越長越好，最低不小於12碼
- 根據**帳戶重要性**決定密碼強度
- 使用**多因子認證**
- 產生**疑慮**時應修改密碼（如：新聞或有帳戶已遭盜用時）
- 使用**無意義字母大小寫、符號及數字組合而成**（如：Eacte65@94537UB）

無密碼登入

為了將網路打造成對大眾而言更安全、更易於使用的空間，蘋果（Apple）、
谷歌（Google）和微軟（Microsoft）於5月5日聯合宣布，計畫擴展FIDO（Fast IDentity Online，線上快速身份驗證）聯盟和全球資訊網聯盟（W3C）共同制定的「無密碼登入」標準。

未來在不同平台、設備登入時，
都不需要輸入傳統密碼，不僅快速便利，
更能防止網路釣魚事件發生。



資安、個資事件案例分享及分析

供應鏈遭駭，政府機關受波及

案情提要

- 機關發現多個設備遭感染勒索病毒，影響機關日常作業，且核心資通系統無法於可容忍中斷時間內回復正常
- 經查為設備**維護廠商維運使用之帳號密碼遭外部暴力破解**，駭客利用該帳號登入維運設備後，再橫向擴散至其他設備

【機關處置方式】

–後續以白名單限制存取系統並鎖定來源IP、限制維護廠商帳號與管理者權限帳號專機專用，並重新設置維運使用之帳號密碼

防護建議

- 密碼設置應符合複雜性原則，並避免使用常見之排列組合如!qaz2wsx
- 廠商遠端連線原則禁止例外開放，現場維護可降低資安風險

物聯網設備韌體未更新，遭植入惡意程式

案情提要

- 機關某廠牌監視器發現遭植入Mirai家族惡意程式，並至中繼站報到
- 經調查該監視器遭揭漏存在存在路徑走訪(Path Traversal)、緩衝區溢位(Buffer Overflow)及命令注入(Command Injection)漏洞等安全性漏洞

【機關處置方式】

–重置設備、變更監視器預設帳號密碼，並更新韌體版本至最新版本

防護建議

- 應評估設備供外部連線之必要性
- 設置新購資訊設備應立即變更預設帳號密碼
- 定期檢視並更新設備系統/韌體版本

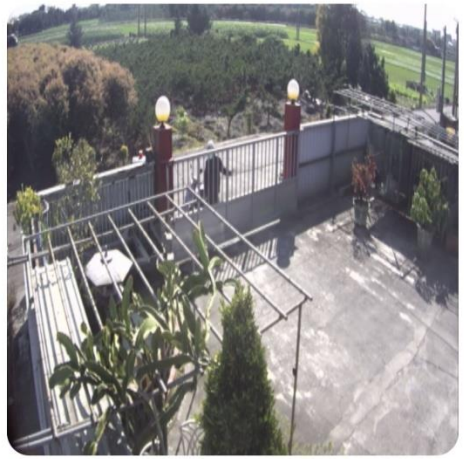
使用預設密碼的監視器

Insecam Most popular Manufacturers Countries Places Cities Timezones New online cameras FAQ Contacts

ENHANCED BY Google

Live cameras: Taiwan, Province Of

1 2 3 4 5 6 7 8 9 10 ... 158 »



Live camera in Taipei, Taiwan, Province Of

Live camera in Taipei, Taiwan, Province Of

Live camera in Taipei, Taiwan, Province Of

系統漏洞導致個資外洩

線上商店的客戶刷卡資料遭盜除了可能會造成客戶的財務損失，或是讓客戶個資淪落黑市之外，也將危及商家的聲譽，而在感恩節過後，緊接而來的就是聖誕節的年底購物季，購物網站也應趁早檢查自家系統的安全性。

英國的國家網路安全中心（National Cyber Security Centre，NCSC）110年11月最後一週發布訊息，已有4,151家的線上商店遭到駭客入侵，駭客於這些網站的結帳頁面植入了側錄程式，盜走網站客戶的刷卡資料，其中絕大多數的攻擊行動是透過Magento系統（開源電子商務平臺）的已知漏洞，因而在感恩節購物季的前夕，提醒全球線上商店要多加注意。

資料來源：https://www.ithome.com.tw/news/147985

社交工程導致用戶個人資料外洩

今年110年7月才登上美國那斯達克股市的股票暨加密貨幣交易程式Robinhood在110年11月8日揭露，有未經授權的第三方於11月3日存取了該公司系統，造成部份客戶的個人資料外洩，包括500萬用戶的電子郵件，200萬用戶的姓名，以及310名用戶的姓名、生日與郵遞區號，另有10名客戶被存取更多的資料。

Robinhood說明，此一未經授權的第三方是透過電話假冒為該公司負責客戶支援的員工，成功地進行了社交工程攻擊，而得以存取特定的客戶支援系統。

資料來源：https://www.ithome.com.tw/news/147737

合理且適當使用個資-個人資料保護法§5

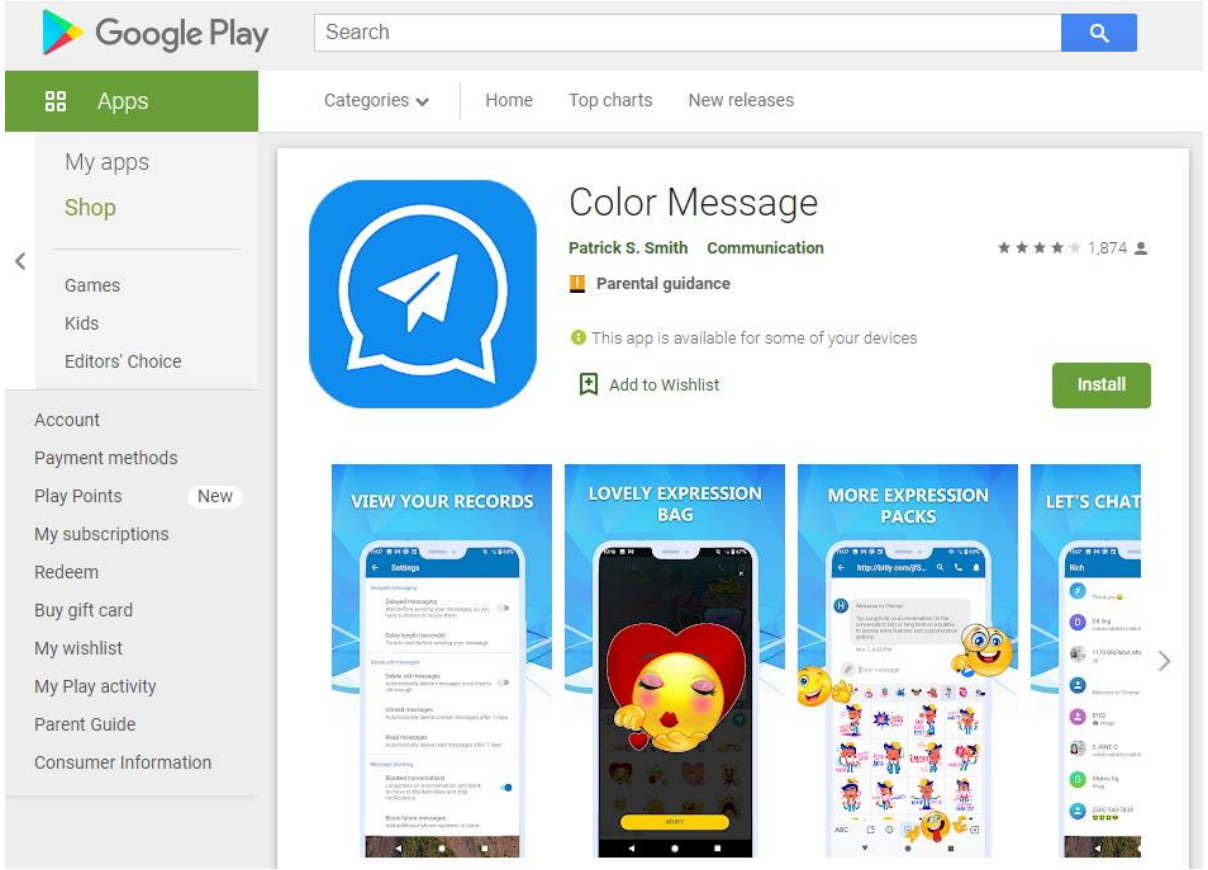
個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

App內含惡意程式

研究人員發現一隻在Google Play Store上下載次數超過50萬的App，內含惡意程式Joker。

這款App為Color Message，看似文字通訊的外掛程式，可為文字訊息加入表情符號及攔阻垃圾訊息。
Color Message內含一隻叫Joker的惡意程式。後者是一種騙錢軟體（Fleeceware），主要活動是模擬點擊以及攔截簡訊，目的在偷偷代用戶訂閱貴死人的付費服務。

Color Message不是第一隻內含Joker的App，研究人員過去兩年發現Joker已經感染了數百個下載次數都超多的App。
去年Google也曾從Play Store上移除1,700多個內含Joker的應用程式。



資料來源：https://www.ithome.com.tw/news/148496

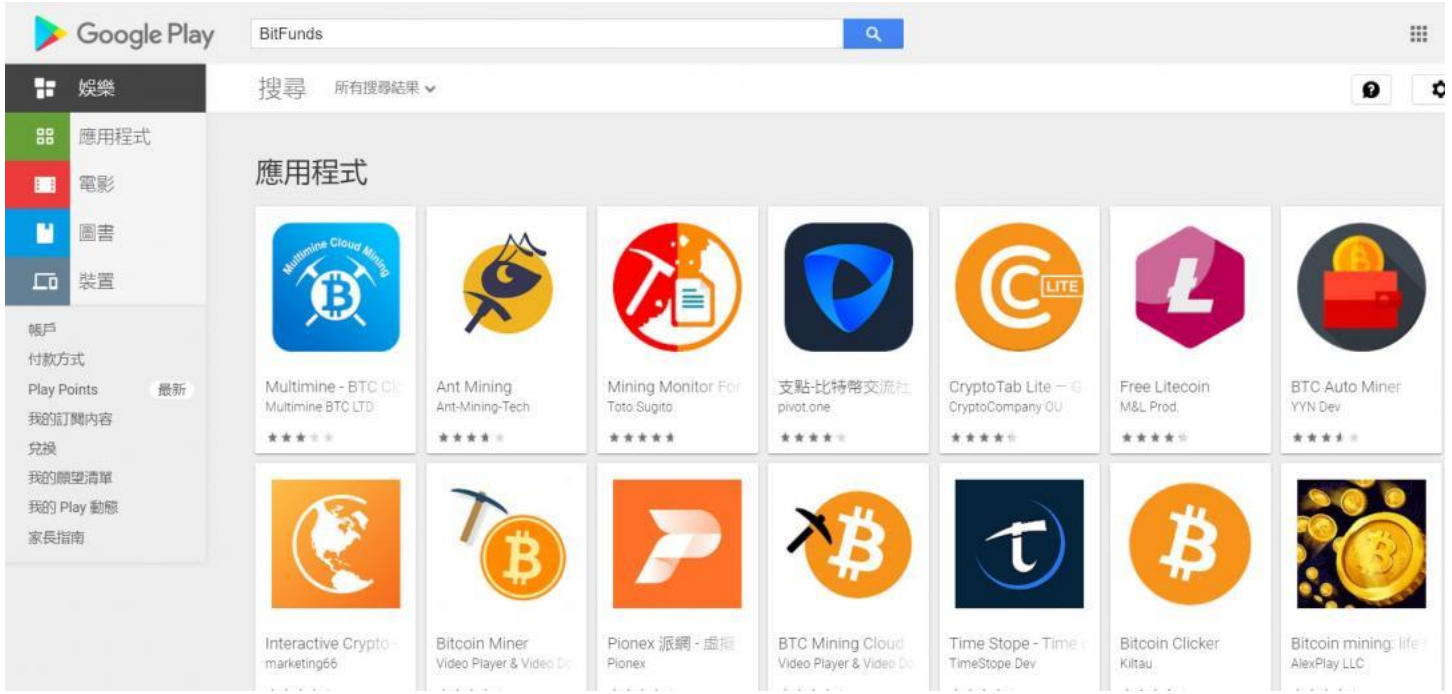
下載非法熱門影片實際為惡意程式

據資安業者Reason Cybersecurity 偵測發現，
近期在網路上已湧現一波大量提供以假冒《蜘蛛人：無家日》影片為名義的惡意程式。

能躲避Windows Defender防毒軟體偵測，與各式監控工具如Process Explorer、Process Hacker、Perfmon與工作管理員等能力，一旦下載該非法影片後，挾帶挖礦軟體Monero就會入侵電腦，導致CPU資源被過度佔用，不但電腦效能會因此無故變慢，甚至還可能因為被植入挖礦軟體後消耗的電力，導致電費金額急遽攀升。

資料來源：https://3c.ltn.com.tw/news/47171

號稱可以雲端挖礦的APP



據外媒《Threatpost》報導，在Google Play 商店上有8款假冒「雲端挖礦」名義的Android App，聲稱可幫用戶挖掘各式加密貨幣（如比特幣等），然而實際下載後，卻是以假冒的UI介面提供挖礦計數器之類的顯示畫面，實際上卻在暗中進行各種詐騙、投放垃圾廣告賺取不當牟利，甚至還會假借提供可強化挖礦算力的訂閱方案向用戶敲竹槓，或暗中私自幫用戶擅自訂閱偷扣款。

資料來源：https://3c.ltn.com.tw/news/47171

資訊安全的最後一道防線

沒辦法確保檔案做到百分之百的防禦，
功能再強的設備、程式都有可能出現漏洞，
導致有心人士有機可趁，
檔案加密是資訊安全中的最後一道防線。

電腦使用習慣

建議養成良好的電腦使用習慣：

- 定期更新防毒軟體&電腦作業系統
- 定期備份重要資料
- 密碼設置強度（長度及複雜度）
- 避免下載不明軟體（破解版）
- 避免點擊不明連結

檔　　號:
保存年限:

教育部 函

地址：10051 臺北市中山南路5號
承辦人：林鉦烜
電話：02-7712-9078
電子信箱：esora@mail.moe.gov.tw

受文者：國立臺南大學

發文日期：中華民國110年6月29日
發文字號：臺教資(四)字第1100085899號
速別：普通件
密等及解密條件或保密期限：
附件：重大資安事件根因分析及建議措施（A09000000E_11027085899_doc2_Attach1.odt）

主旨：教育體系近期發生多起重大資通安全事件，導致個資外洩及機關名譽之損害，為降低資安風險，請查照辦理。

說明：

一、本(110)年教育體系發生多起因管理不當導致之重大資通安全事件，相關根因分析及建議措施如附件，請貴校(機關)據以檢核自身資安管理情形，避免類似資通安全事件發生。

二、針對本部所屬機關及大專校院，即日起將加強相關措施如下：

(一)機關、學校因管理不當導致資通安全事件，本部將以不遮蔽該機關、學校方式作為教育體系內部案例宣導。

(二)針對發生重大資通安全事件之機關、學校，本部將辦理專案實地稽核，未落實稽核缺失改善者，將循相關機制提報懲處。

正本：各公私立大專校院、各國立大學附設醫院及農林場
副本：電子公文交換章 2021/06/29 10:18:10

國立臺南大學 電子計算機中心 1100010850

檔　　號:
保存年限:

教育部 函

地址：10051臺北市中山南路5號
聯絡人：林文信
電　話：02-7712-9092

受文者：國立臺南大學

發文日期：中華民國110年12月30日
發文字號：臺教資(四)字第1100179797號
速別：普通件
密等及解密條件或保密期限：
附件：國立大專校院資通安全維護作業指引（0179797A00_ATTCH3.pdf）

主旨：檢送「國立大專校院資通安全維護作業指引」，請查照。

說明：

一、鑒於近期教育體系發生多起重大資通安全事件，相關根因分析顯示各校資通安全維護計畫施行範圍未涵蓋全校。

二、為強化教育體系資通安全環境，並推動全校落實資通安全管理法相關規定，訂定旨揭作業指引。

三、自111年起，旨揭作業指引第二點各款事項列入本部所屬大專校院資通安全維護計畫實施情形重點審查事項，各校執行成果納入次年度本部績效型補助款衡量指標計算。

正本：各國立大專校院
副本：本部高等教育司、本部技術及職業教育司、本部資訊及科技教育司(均含附件)
電子公文交換章 2021/12/30 16:37:27

國立臺南大學 電子計算機中心 1100022839

檔　　號:
保存年限:

教育部 函

地址：100217 臺北市中正區中山南路5號
承辦人：林鉦烜
電話：02-7712-9078
電子信箱：esora@mail.moe.gov.tw

受文者：國立臺南大學

發文日期：中華民國111年4月18日
發文字號：臺教資(四)字第1112701315號
速別：普通件
密等及解密條件或保密期限：
附件：1_教育部111至112年度資通安全稽核計畫、1-1-1_資通安全實地稽核項目檢核表(適用公務機關)、1-1-2_資通安全實地稽核項目檢核表(適用特定非公務機關)、1-2_受稽機關現況調查表、1-3_技術檢測評分表、1-4_實地稽核評分表(A09000000E_1112701315_senddoc2_Attach1.pdf、A09000000E_1112701315_senddoc2_Attach2.odt、A09000000E_1112701315_senddoc2_Attach3.odt、A09000000E_1112701315_senddoc2_Attach4.odt、A09000000E_1112701315_senddoc2_Attach5.odt、A09000000E_1112701315_senddoc2_Attach6.odt)

主旨：檢送本部111至112年度對所屬公務機關及所管特定非公務機關資通安全稽核計畫（如附件），請查照辦理。

說明：

一、請貴機關預做整備，本部將依旨揭計畫於稽核前1個月通知受稽機關。

二、為瞭解貴機關資通安全維護規劃現況，請於文到七日內提交機關資通安全維護計畫，免備文以電子郵件寄至本部楊小姐(cjyang@mail.moe.gov.tw，聯絡電話02-77129088)，相關交付情形將納入稽核遴選參考。

三、另本部所屬機關、學校，亦應依資通安全管理法相關規定稽核其所屬機關、監督機關、所管特定非公務機關之資通安全維護計畫實施情形。請相關機關依下列時程規劃辦理，並於稽核實施前一個月將稽核計畫報部備查：

(一)國家運動訓練中心：由體育署制定及實施資安稽核，於111年至112年間至少辦理1次。

(二)醫院以外之大學附設機構：由上級機關（所屬大學）制定及實施資安稽核，於111年至112年間至少辦理1次。

(三)大學附設醫院：各醫院之分院應由上級機關（總院）制定及實施資安稽核。

(四)國立高級中等以下學校及國民及學前教育署（下稱國教署）轄管之財團法人：由國教署統籌規劃辦理，制定及實施資安稽核。

正本：部屬機關(構)、各國立大專校院、財團法人私立學校興學基金會、財團法人高等教育國際合作基金會、財團法人社教文化基金會、財團法人臺灣省童軍文教基金會、財團法人吳健雄學術基金會、財團法人教育部接受捐助獎學基金會、財團法人大學入學考試中心基金會、財團法人高等教育評鑑中心基金會、財團法人蔣經國國際學術交流基金會
副本：本部政風處、高等教育司、國際及兩岸教育司、終身教育司、秘書處(均含附件)

電子公文交換章 2022/04/18 14:39:53

國立臺南大學 電子計算機中心 1110006848

TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

Q/A

TSC CAPITAL GROUP

The Bridge to the Asia Pacific Region

感謝您的參與

歡迎於活動後與講師討論您的任何疑問

本公司的臉書粉絲團及部落格可以找到更多資訊

TSC – FB Site

TSC – Blog Site