資拓宏宇國際股份有限公司
International Integrated Systems, Inc.

學校資安認知宣導課程

是一網情深？還是一網打盡？

~ 網路安全防護面面觀

講　　師：資拓宏宇資安顧問

日　　期：2023/11/22

資拓宏宇永遠與您一起創新前進

always innovative always IISI

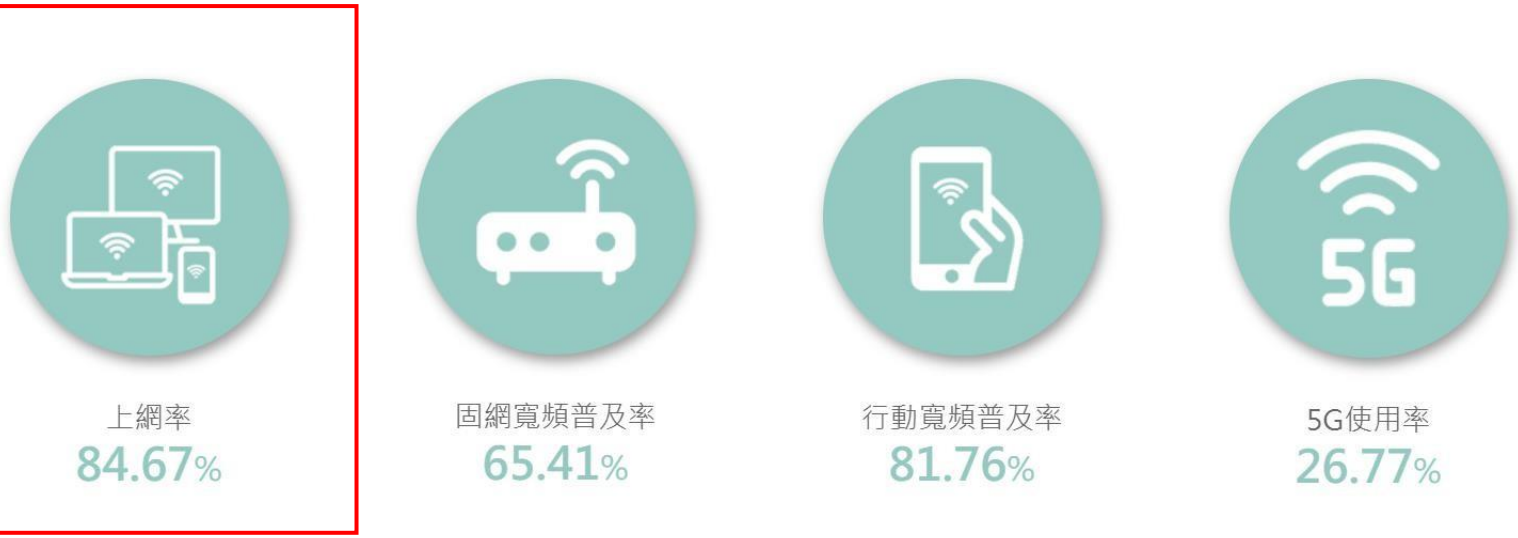
本日大綱

- 台灣網路環境報乎你知
- 令人迷失的網路世界
  - 網路釣魚
  - 網路購物
  - 網路交友
- 過度的授權將隱私拱手送人
- 猝不及防的勒索軟體攻擊
- 總結
- Q&A

台灣網路環境報乎你知

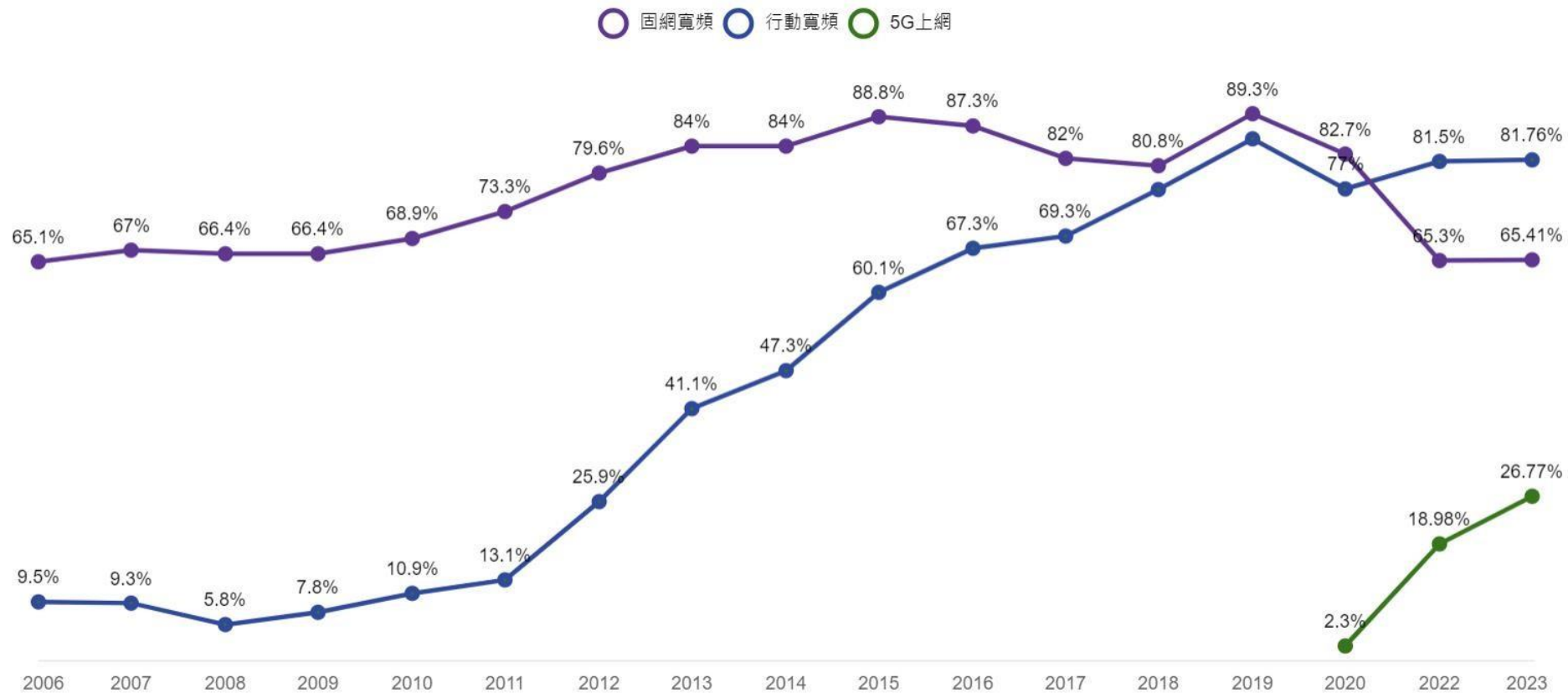
台灣網路使用情況

- 2023年台灣高達84.67%的上網率



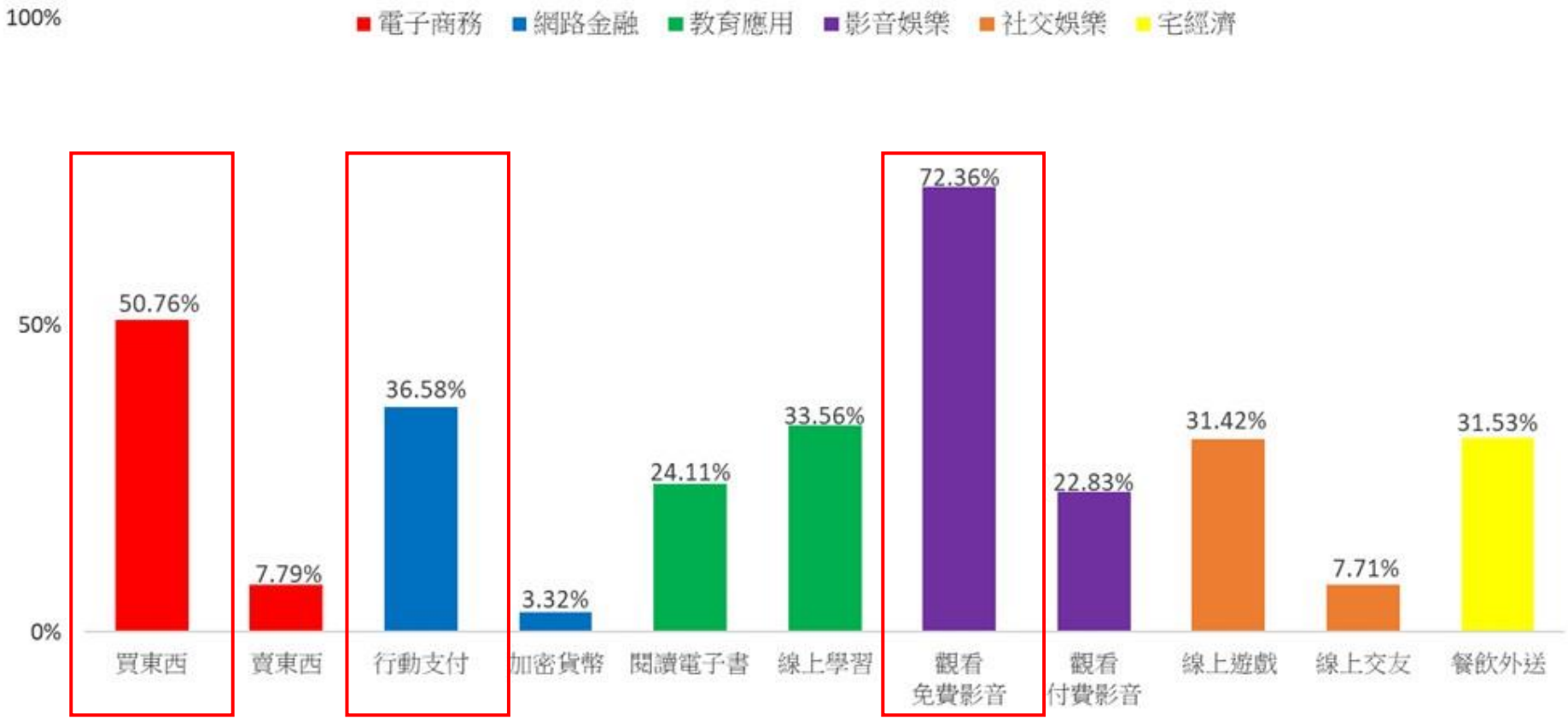
資料來源：2023台灣網路報告，執行時間2023年5月2日至5月20日，加權後數值。樣本數：2,153（雙底冊，全部樣本）

台灣網路使用情況



資料來源：2006至2023台灣網路報告。註：本次調查對象為18歲以上民眾；2020及往年調查對象為年滿12歲以上民眾。

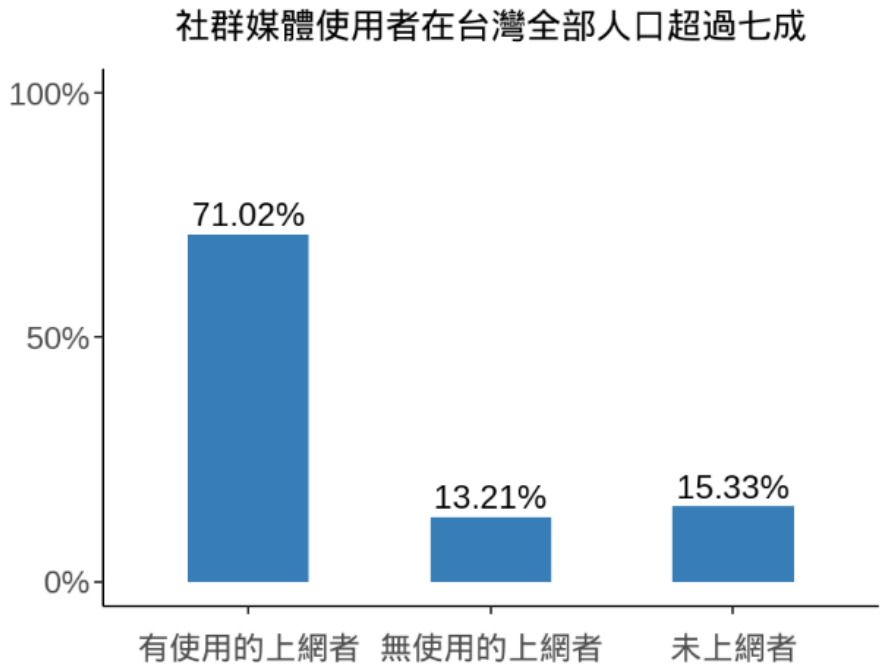
網路應用服務(整體使用情況)

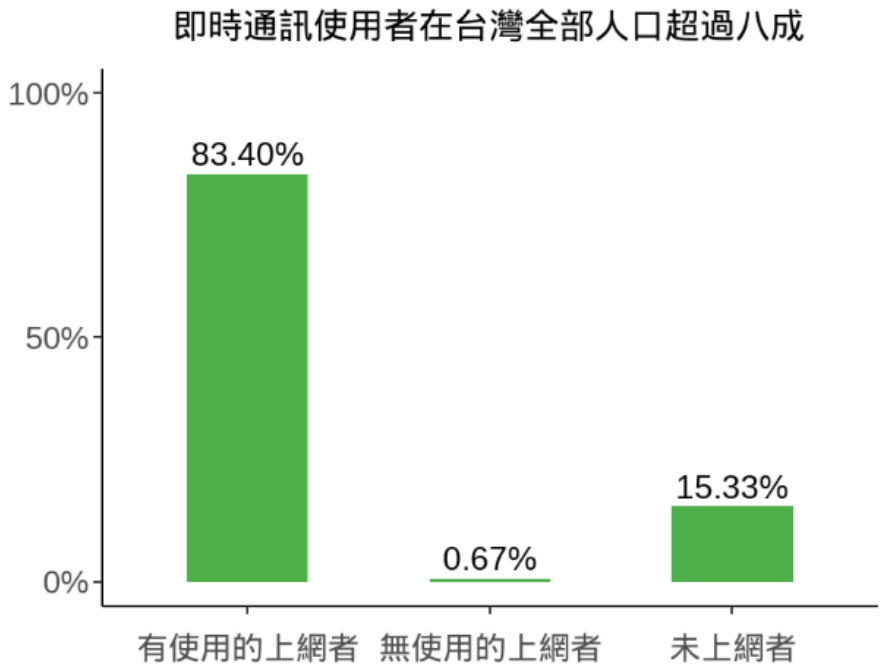


資料來源：2023台灣網路報告，執行時間2023年5月2日至5月20日，加權後數值。樣本數：1,084（市話樣本）

網路應用服務(社群媒體與即時通訊)

- 社群媒體與即時通訊已成多數人日常

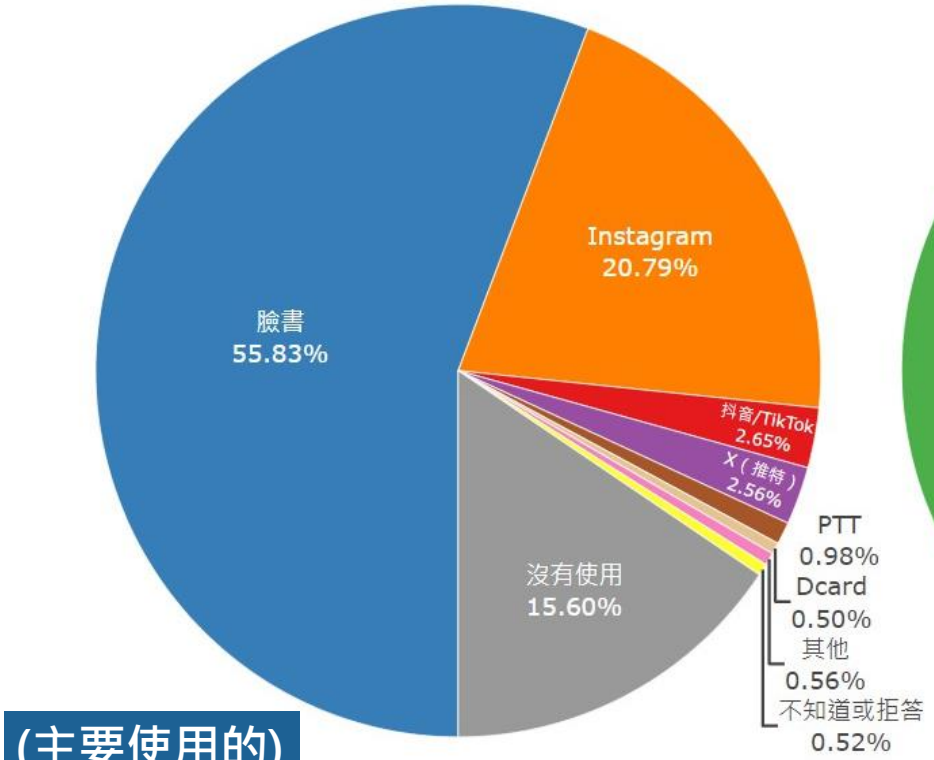




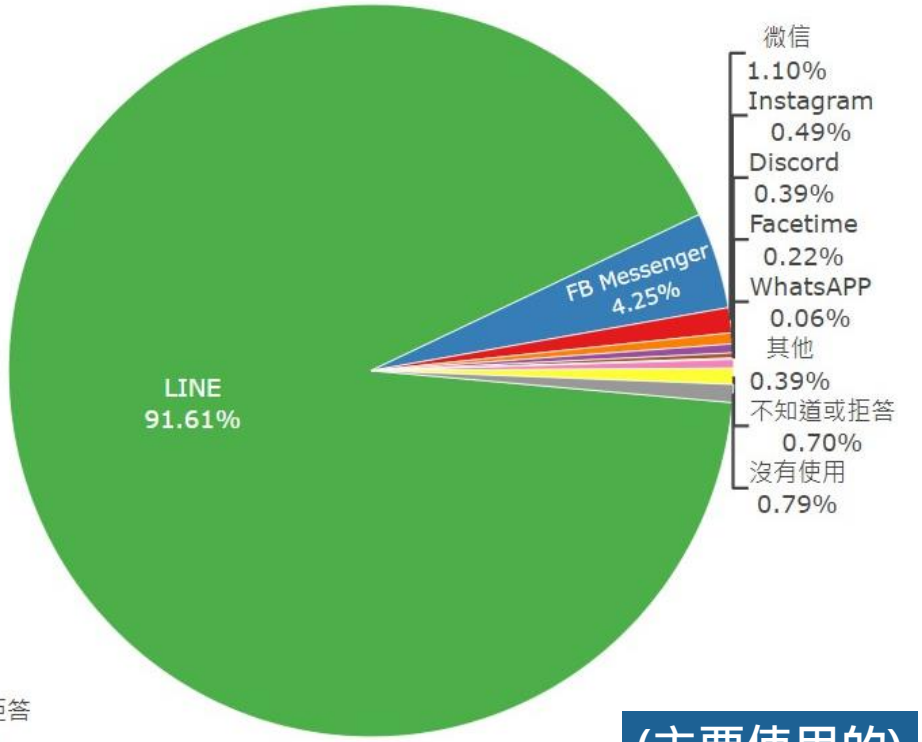
資料來源：2023台灣網路報告，執行時間2023年5月2日至5月20日，加權後數值。樣本數：社群媒體2153，即時通訊2153 (雙底冊，全部樣本)
附註：未顯示「不知道或拒答」：社群媒體0.44%、即時通訊軟體0.60%

網路應用服務(社群媒體與即時通訊)

- 以臉書與LINE做為主要社群、通訊管道的使用者分佔五成多與九成多



(主要使用的)
社群媒體



(主要使用的)
即時通訊

資料來源：2023台灣網路報告，執行時間2023年5月2日至5月20日，加權後數值。樣本數：1823 (雙底冊，上網者樣本， 加權後數值)

台灣受到網路威脅高

- 每秒1.5萬次網路攻擊，台灣慘居亞太之冠！

每秒1.5萬次網路攻擊，台灣慘居亞太之冠！駭客從
亂槍打鳥變「企業化」，5大資安威脅一次看

https://www.businesstoday.com.tw/article/category/183015/post/202308170006/

常見的網路威脅

- 惡意連結網路威脅 (e.g. 網路釣魚/網路購物/網路交友)
- 權限管理不當，個資外洩
- 勒索軟體

令人迷失的網路世界

惡意連結網路威脅

定義	通過電子郵件、訊息或社交媒體發送含有惡意連結的訊息給目標受害者。這些連結看似合法，但實際上會導向帶有惡意軟體的網站或用於盜取用戶資訊的釣魚網站。
症狀	➢ 社交媒體、電子郵件或訊息出現來路不明、怪異或誘人的連結。 ➢ 點擊連結後，系統要求輸入個人資訊或直接下載檔案。 ➢ 經常性彈出窗口警示，聲稱你的裝置有安全問題或中獎，需點擊連結處理。
目的	➢ 盜取個人資料，如帳號、密碼或信用卡信息。 ➢ 植入惡意軟體，控制受害者的電腦進行犯罪活動。 ➢ 進行詐騙活動，如假冒官方機構騙取金錢。
傳播形式與途徑	➢ 社交媒體訊息：在社交平台上發送含有惡意連結的私人訊息或貼文。 ➢ 假冒網站：建立看似合法但旨在盜取資料的釣魚網站。 ➢ 簡訊或即時通訊：透過手機簡訊或應用程式發送包含惡意連結的訊息。 ➢ 廣告軟體：在合法網站的廣告中植入惡意連結，誘導用戶點擊。

2023台灣惡意連結網路威脅前三名

根據趨勢科技在2023年台灣的偵測統計數據，來自手機的惡意連結數量飆破一百三十萬筆，相較於去年同期的八十多萬大幅增加近60％，前三大方式分別為:

- 網路釣魚
- 網路購物
- 網路交友

資料來源：科技新報

令人迷失的網路世界

網路釣魚

惡意連結網路威脅(網路釣魚)

- **2023 台灣所偵測的惡意連結以「網路釣魚」數量高居第一**

操作手段:

- 透過假冒知名企業官網的網址或網頁外觀，利用熱搜關鍵字做為釣餌來降低使用者戒心。
- 利用時事新聞、流行事件或節日等話題，制造緊迫感或好奇心，促使受害者點擊釣魚連結。
- 使用看起來與真正網站相似的URL，但包含微妙的拼寫錯誤或使用不同的頂級域名（例如.com變成.co）
- 通過短信發送看似正式的消息，包括要求點擊連結以解決賬戶問題或領取獎品的文字。

網路釣魚新聞案例

小心別上當！普發6000元出現假的「釣魚網站」

吳栢妤 | Yahoo財經特派記者
2023年3月25日

線上登記6000元要注意！財政部昨日傍晚透過即時監控機制發現與普發現金相似之偽冒網址(tw.gov6000.top)，提醒民眾務必認明正確網址「6000.gov.tw」，避免遭釣魚網站盜用資料。

普發現金官網3月22日晚正式上線（圖／中央社提供）

樂享生活

普發6千元假網站流竄，3點辨別陷阱！釣魚網站最愛冒用十大平台「Netflix也在內」

2023-03-21　1,536 人次

https://www.edh.tw/lohas/article/30801

普發6000元 假釣魚網站!

時間	2023年3月間
案情	➢ 政府普發六千元，詐騙集團發送釣魚簡訊，誤導民眾進入假網站 ➢ 唯一登記的網址應該是「https://6000.gov.tw」，假網址被動手腳，包括網址多了com或是0改成o
影響	● 誤導民眾，導致個資外洩和金融安全問題。 ● 民眾對政府補助措施信心下降，疑慮增加。 ● 提升釣魚網站成功騙取信息的機率。 ● 使真實政府網站訪問量下降，影響補助發放效率。

https://www.edh.tw/lohas/article/30801

網路釣魚預防方法(1/2)

預防方法：

- **使用網址管理插件或服務**：安裝瀏覽器擴展或使用服務，網址安全檢查插件可以自動檢測和警告你訪問的可能是釣魚網站。
- **直接輸入網址**：不透過搜尋結果點擊網站鏈接，特別是涉及財務交易的網站，最好手動輸入網址或使用已儲存的書籤訪問官方網站。
- **對熱門關鍵字保持警惕**：避免點擊基於熱搜關鍵字的搜尋結果廣告，尤其是在尋找銀行、金融服務或購物網站時。
- **安裝廣告攔截插件**：瀏覽器廣告攔截插件可以阻擋惡意廣告和有害網站，降低你不小心點擊假冒廣告的機會。

網路釣魚預防方法(2/2)

預防方法：

- **識別品牌官方認證：**識別企業官方網站上的安全標誌，如鎖定圖標、正確的網站設計和官方域名。

- **使用網路安全工具：**使用綜合網路安全解決方案，包括具有網路釣魚保護的防病毒軟件。

- **檢查搜尋引擎的安全功能：**許多搜尋引擎提供安全搜尋過濾功能，可以過濾掉已知的惡意網站和釣魚連結。

令人迷失的網路世界

網路購物

惡意連結網路威脅(網路購物)

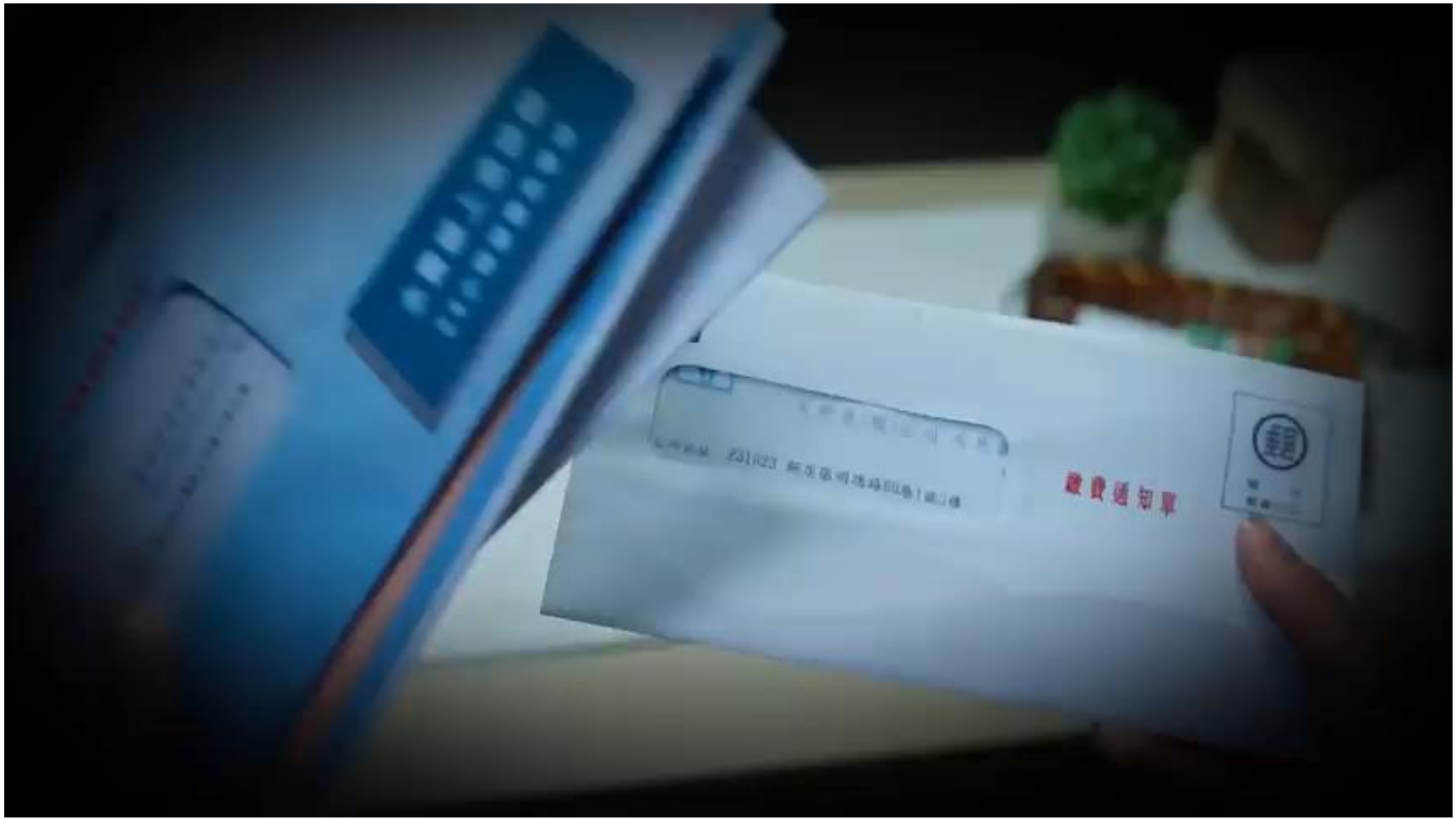
操作手段:

- **社群網站貼文(假網拍詐騙)**：
  冒用名人肖像或引人注目的廣告台詞吸引消費者購買，實際上販售與品項不符或有瑕疵之商品。
- **釣魚簡訊**：
  引誘民眾點擊網址，前往假冒品牌的購物頁面進行下單，或是假到貨真詐騙的釣魚簡訊，使民眾誤以為有訂購包裹而前往付款領取，進一步騙取民眾錢財或個人資訊。
- **一頁式購物網頁**：
  多為高價品低價賣的話術，聲稱可以貨到付款、有七天鑑賞期，實際上收到的根本不是購買的商品。
- **電話假冒客服**：
  因訂單設定錯誤、要求依照指示匯款或操作ATM以解除分期付款。

https://stu.nkust.edu.tw/p/406-1007-70662,r1586.php

惡意連結網路威脅(網路購物)

一頁式購物收假貨？



網路購物詐騙新聞案例

速食店優惠券也可能是詐騙！ 女下單竟遭盜刷5萬

13:27 2023/07/02 | 中時 | 洪靖宜

警方提醒高心山賣優惠券，下單填寫優惠卷卻遭盜刷信用卡。（翻攝照片／高雄消防局提供）

臉書下單速食被盜刷 民眾遭釣魚網站詐騙

薛宜家 莊志成 / 綜合報導　發布時間：2023-07-02 19:31　更新時間：2023-07-02 20:55

金融卡　網站　Facebook　速食店　...

優惠券詐騙! 遭盜刷5萬!

時間	2023年7月間
案情	➢ 高雄市一女子被49元漢堡套餐廣告誘騙，輸入個人及信用卡資料後，遭盜刷至5萬元，陷入網路釣魚詐騙。 ➢ 警方指出，受害者在購買後才發現賬戶遭到盜刷，透過銀行簡訊才得知損失了新台幣5萬元。 ➢ 社群網站多起冒用知名速食店官方優惠券詐騙案，同個月已有逾30人受騙，警方提醒民眾核實官方網站以防上當。
影響	● 詐騙活動導致消費者財產損失，信用卡遭盜刷引發經濟損害。 ● 個資外洩增加受害者遭遇後續詐騙風險，個人隱私受侵。 ● 惡意釣魚連結損害速食品牌信譽，消費者對正品折扣產生疑慮。 ● 社會治安受影響，民眾對網路交易安全感減少，需警惕性提高。

網路購物威脅預防方法(1/2)

預防方法：

- **使用安全軟體：**安裝並維持更新優質的防毒軟體和網路安全程序，這些工具可以幫助識別並阻止訪問惡意網站。

- **網址審查：**在點擊任何購物相關的連結之前，仔細檢查URL。確認網址是否正確無誤，尤其是域名的拼寫，以及是否為安全的連接（即以https://開頭，而非http://）。

- **教育自己：**了解惡意連結的常見標誌，例如拼寫錯誤、誘人的「太好而不真實」的優惠，以及不明來源的電子郵件或訊息。

- **使用網路購物專用信用卡：**使用一張專門用於網路購物的信用卡，設定較低的消費限額，這樣即便資訊被竊取，損失也能降到最低。

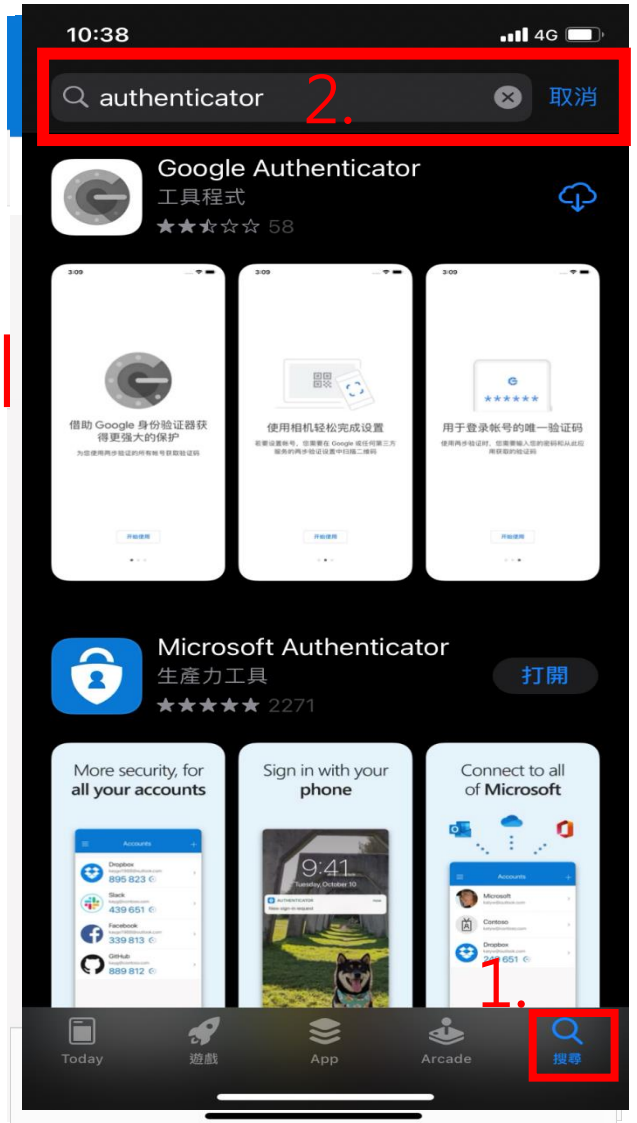
網路購物威脅預防方法(2/2)

預防方法：

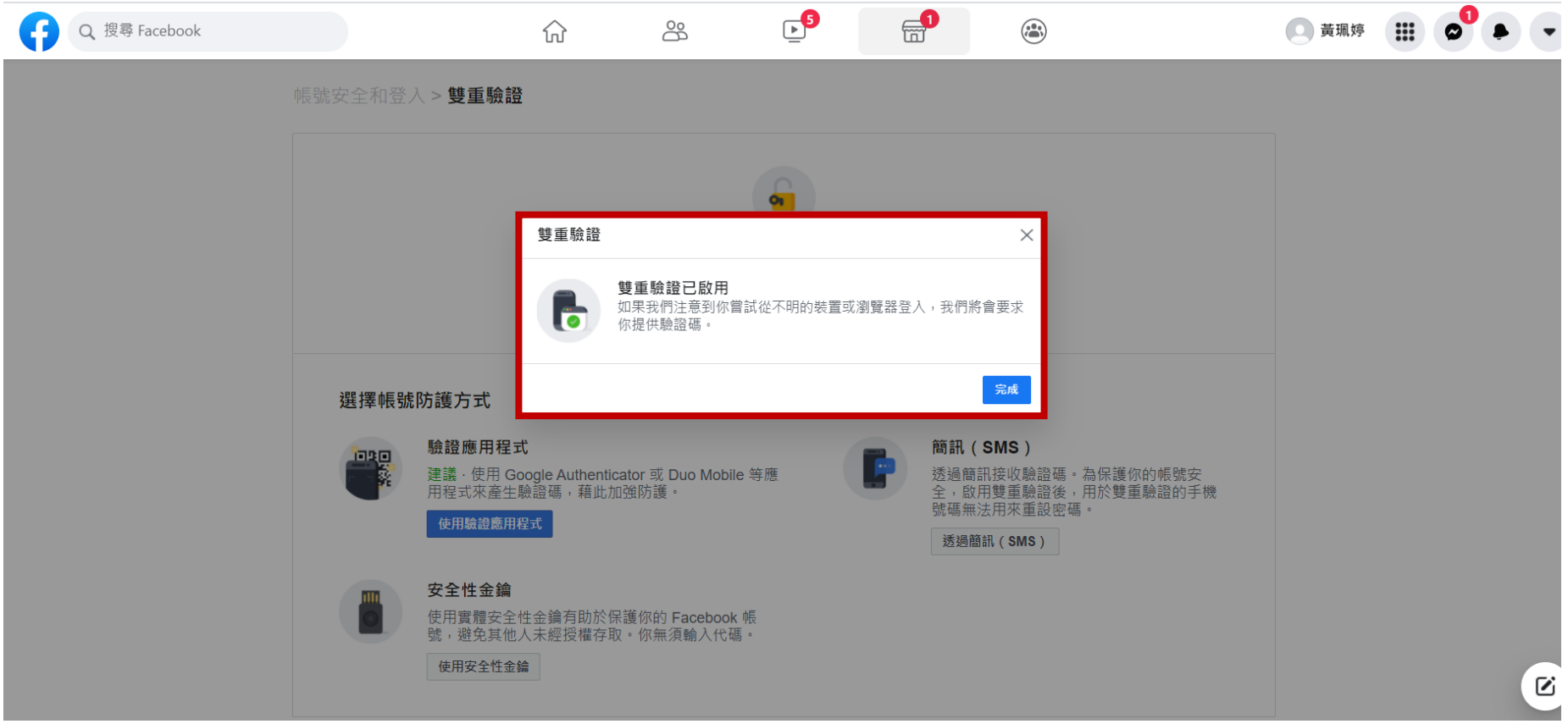
- **雙因子認證：**啟用雙因子認證（2FA）對您的賬戶提供額外保護，即使有人獲得了您的密碼，未經您的第二次確認也難以訪問您的賬戶。
- **購物前做調查：**在購買前，搜尋賣家的評價，看看其他購物者的經驗和評論，避免與可疑或評價低的賣家交易。
- **不點擊可疑連結：**不要點擊社群媒體、即時通訊應用、電子郵件中陌生人發送的連結，即使它們看起來來自您認識的人，也要經過核實。
- **更新操作系統和瀏覽器：**定期更新您的操作系統和瀏覽器至最新版本，以保護您免受新發現漏洞的影響。

安裝第三方驗證應用程式

- 手機安裝第三方驗證應用程式
  Google Authenticator
  Microsoft Authenticator
- 以Apple手機為例:
  先到App Store→搜尋→在搜尋列
  輸入Authenticator →安裝
  Google / Microsoft Authenticator
  →開啟App→加入帳戶→其他→
  掃描Qrcode代碼→加入成功



完成二階段驗證啟用



驗證二階段驗證啟用

登出Facebook→重新登入Facebook
→輸入第三方應用程式的6位數驗證碼

請不要記住瀏覽器

對來電進行過濾與拒接不明來電

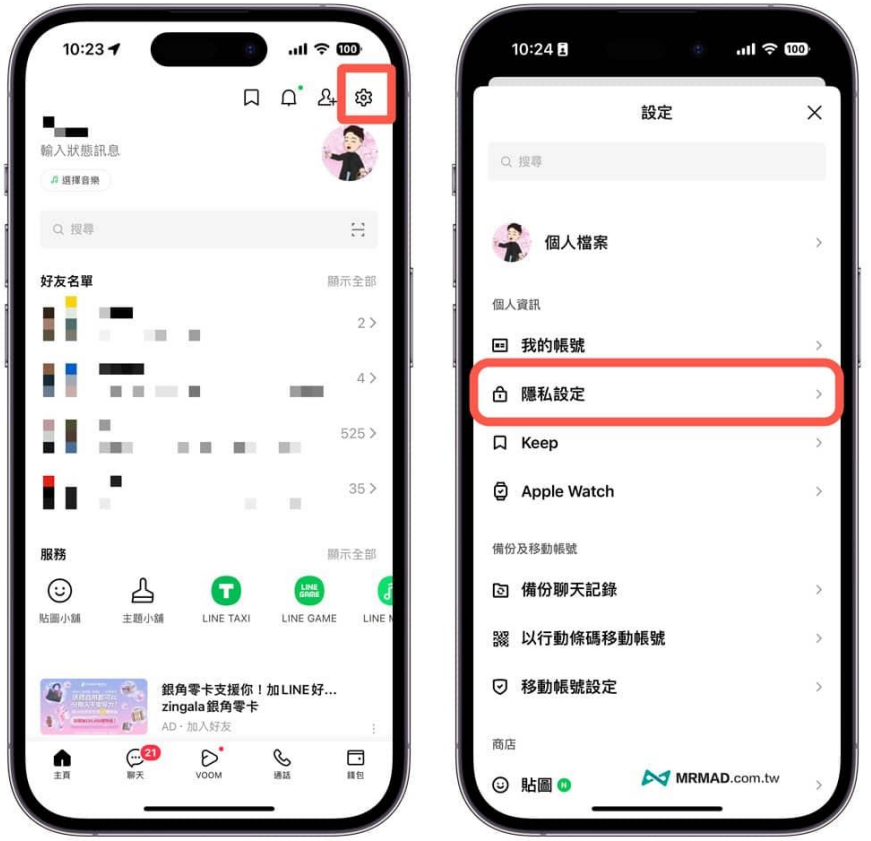
- 如果不確定是信任的熟人的來電最好勿接。
- 安裝來電過濾APP以過濾廣告、推銷或詐騙集團的來電。

LINE廣告關閉教學(1/8)

如何把 LINE 廣告關掉？5招最實用的關閉LINE廣告技巧教學

方法 1. 停用 LINE 隱私「關閉個人化廣告」追蹤

- 開啟 LINE APP 點選右上角「**設定**」（齒輪圖示）
- 選擇「**隱私設定**」



https://mrmad.com.tw/line-ads-close

LINE廣告關閉教學(2/8)

方法 1. 停用 LINE 隱私「關閉個人化廣告」追蹤

- 點選「**廣告相關設定**」
- 將「**使用網路活動紀錄接收個人化廣告**」與「**使用LINE內部識別碼接收個人化廣告**」都關閉。

LINE廣告關閉教學(3/8)

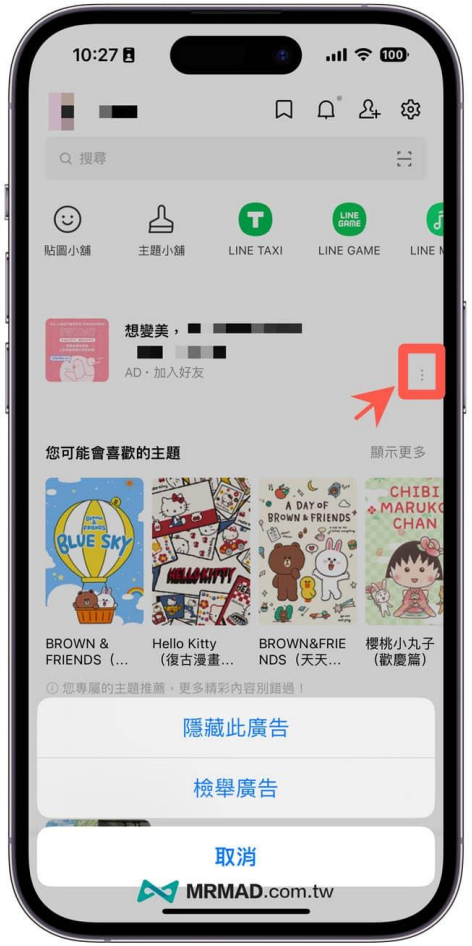
方法 1. 停用 LINE 隱私「關閉個人化廣告」追蹤

- 點選「**廣告相關設定**」
- 將「**使用網路活動紀錄接收個人化廣告**」與「**使用LINE內部識別碼接收個人化廣告**」都關閉。

LINE廣告關閉教學(4/8)

方法 2. 隱藏 LINE 首頁廣告

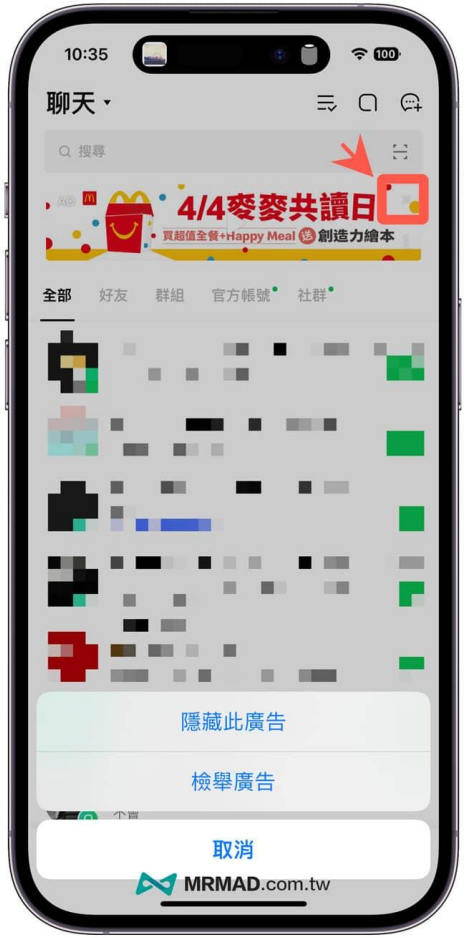
當你打開 LINE 主頁面後，會在 LINE 服務區塊下看見 LINE 廣告欄位，可以點擊廣告右下角「**三個點⋯**」圖示選單，就能選擇「**隱藏式廣告**」和「**檢舉廣告**」，不管選哪一個，只要選擇為什麼要隱藏/檢舉廣告的理由，送出後就能將 LINE 廣告關閉。



LINE廣告關閉教學(5/8)

方法 3. 關閉LINE聊天室廣告方法

每個 LINE 聊天室分類頂部都會自動被加入 LINE 廣告，如果想關閉置頂LINE廣告，可以點擊右上角「**關閉**」按鈕，同樣會出現「**隱藏式廣告**」和「**檢舉廣告**」選單，選擇其中一個回答就能關閉 LINE 聊天室分類廣告顯示。



LINE廣告關閉教學(6/8)

方法 4. LINE社群廣告關閉封鎖方法

連同 LINE 社群內也都會看見廣告，而且位置非常明顯，會直接顯示在聊天室頂部，要是想要將 LINE 社群廣告關閉，可以直接點擊右上角「**多功能鍵**」選單，選擇隱藏或關閉廣告，就能一鍵關閉 LINE 社群聊天室廣告。

LINE廣告關閉教學(7/8)

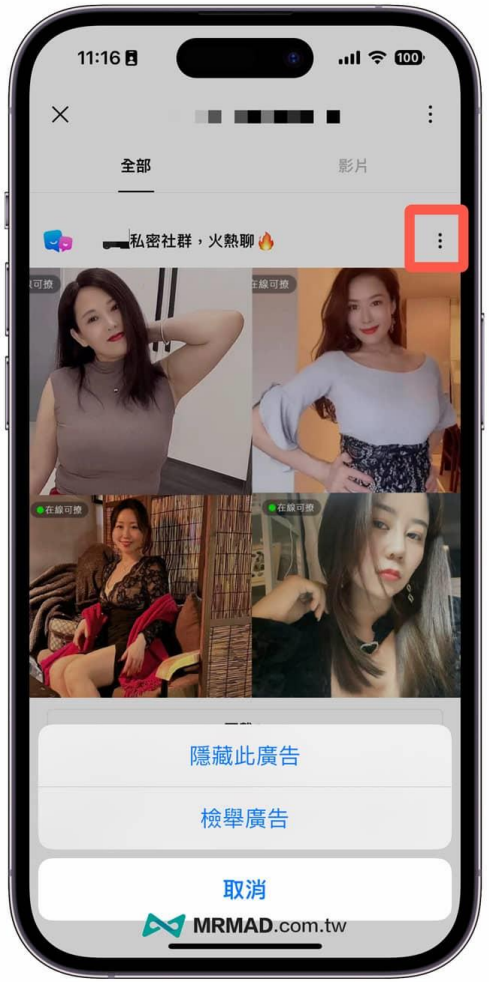
方法 4. LINE社群廣告關閉封鎖方法

最後可以看看 LINE 社團廣告關閉前後差異，聊天室頂部就不會被煩人的廣告佔據。

LINE廣告關閉教學(8/8)

方法 5. LINE貼文串廣告關閉

自從 LINE貼文串改為 LINE VOOM 後，每次瀏覽 LINE 朋友的動態，都會看見奇怪情色的視訊廣告，例如單身阿姨要找另一半，想要關閉 LINE貼文串廣告，只要點擊右上角「**三個點…**」按鈕，選擇「**檢舉廣告**」就能夠隱藏這類型LINE廣告。



令人迷失的網路世界

網路交友

惡意連結網路威脅(網路交友)

操作手段:

- **情感詐騙：**
  攻擊者在交友網站或應用上建立假冒個人資料，與受害者建立情感關係，一旦獲得信任，他們會引誘受害者點擊帶有惡意軟件的連結，或前往釣魚網站。
- **黑郵與勒索：**
  攻擊者可能要求用戶點擊一個看似無害的連結來查看某個私密照片或訊息，一旦點擊，就下載勒索軟體或木馬，這些軟體可以鎖定設備或竊取敏感資料，然後要求支付贖金。
- **欺詐性連結與網站：**
  1. 攻擊者偽裝成交友對象，並邀請受害者訪問特定的網站，這些網站要求用戶填寫個人資料，這些資料隨後會被用於身份盜用。
  2. 誘騙受害者購買禮物卡或轉賬給所謂的網路愛人，以此騙取金錢。

惡意連結網路威脅(網路交友)

戀愛腦暈船險遭詐？

網路交友詐騙新聞案例

兩台女遭網戀詐騙15萬USDT，刑事局罕見回覆「DYOR」

by luc: — 2023-04-17 in 台灣, 犯罪 AA

https://www.chinatimes.com/realtimenews/20230416002388-260402?chdtv

兩女遭網戀詐騙15萬USDT

時間	2023年7月間
案情	➢ 一名女子在假交友的陷阱中投入新台幣270萬購買泰達幣，結果資金蒸發，蒙受巨大經濟損失。 ➢ 透過社交網站LinkedIn認識的假投資顧問，通過LINE建立信任並介紹高收益投資，最終導致女子巨額財產損失。 ➢ 詐騙手法涉及建立日常溝通並培養感情，逐步引導受害者到註冊於詐騙者控制的假冒交易平台進行投資。 ➢ 刑事局警示公眾，詐騙集團常以假交友手法結合投資詐騙，利用假的高回報承諾誘騙受害人投資虛擬貨幣。
影響	● 受害者面臨重大經濟損失，影響個人及家庭財務安全。 ● 社交平台的信任度下降，用戶對於網路交友變得謹慎。 ● 加劇法律與執法機構的壓力，需要更多資源打擊網路犯罪。

網路交友威脅預防方法(1/2)

預防方法：

- **保持警惕：**在交友網站或應用上與他人互動時，對於提供個人資訊或點擊未知連結保持警覺，建立關係需要時間，若對方急於要求個人或財務資訊，應保持警惕。

- **驗證身份：**若在線上建立了情感連接，可透過視訊通話等方式驗證對方的真實性，欺詐者通常會找藉口避免面對面的互動。

- **使用安全的網路行為：**不要點擊未經驗證的連結，安裝並更新防毒軟體，以防止惡意軟體和勒索軟體的侵害。

- **進行背景檢查：**若在線上遇到某人，而此人提議將關係進一步發展或進行金錢交易，進行簡單的網路搜尋或背景檢查可能揭示重要的資訊。

網路交友威脅預防方法(2/2)

預防方法：

- **不進行金錢交易：**絕不向網路上的人轉賬或購買禮物卡，即使對方聲稱有緊急情況也不應提供財務援助。
- **保持隱私：**不分享私密照片或資訊，以防被用作未來的勒索材料。
- **學習辨識騙局：**熟悉常見的網路詐騙手法，例如過於完美的個人資料、不合邏輯的故事或其他引起疑慮的行為。
- **採取正式渠道：**只透過官方和有信譽的交友平台尋找交友對象，並使用其內建的通訊工具而非私下通訊。

臉書交友邀請關閉教學(1/4)

FB臉書交友邀請功能如何關閉？一鍵設定避免陌生人亂加好友

步驟 1. 打開 Facebook 臉書 ，點選右下角「**功能表**」，將「**設定和隱私**」功能展開後，按下「**隱私捷徑**」。

https://mrmad.com.tw/facebook-closes-friend-invitation

臉書交友邀請關閉教學(2/4)

步驟 2. 在FB隱私設定頁面內，點選「**查看更多隱私設定**」。

臉書交友邀請關閉教學(3/4)

步驟 3. 找到**其他人如何尋找和聯絡你**區塊，會看見「**誰可以傳送交友邀請給你？**」點入改為「**朋友的朋友**」即可，後續其他陌生人或假帳號就沒辦法再傳送交友邀請給你。

臉書交友邀請關閉教學(4/4)

如何隱藏朋友名單、防止Email、電話搜尋？

透過 FB臉書「**功能表**」>「**設定和隱私**」>「**隱私捷徑**」>「**查看更多隱私設定**」可以設定「**誰可以查看你的朋友名單？**」、「**誰可以使用你所提供的電子郵件地址找到你？**」、「**誰可以使用你所提供的電話號碼找到你？**」。

很多人想要確保自己FB帳號有隱私權，避免對外公開，
建議可以根據底下設定：

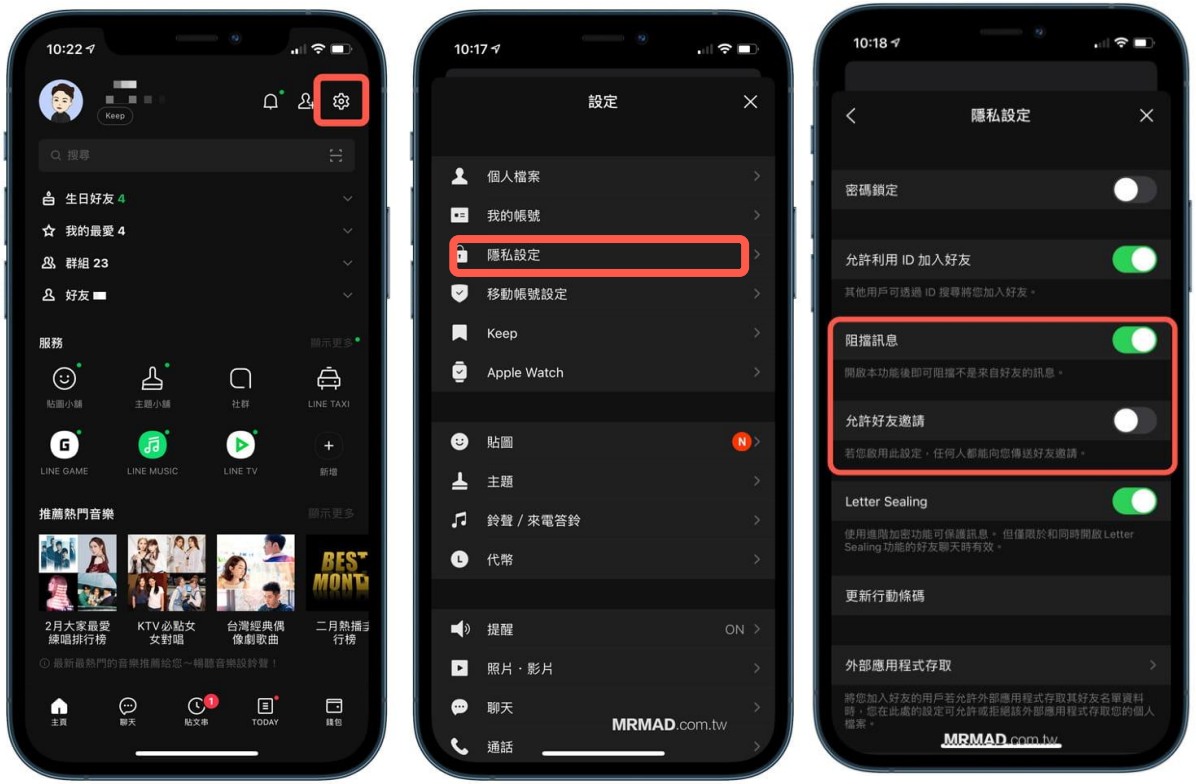
- 誰可以查看你的朋友名單？改為「**只限本人**」
- 誰可以使用你所提供的電子郵件地址找到你？改為「**朋友**」
- 誰可以使用你所提供的電話號碼找到你？改為「**朋友**」

10招提升LINE安全設定技巧(1/12)

1. 加強LINE隱私設定：防止陌生人亂傳亂加

打開 LINE App ，點選右上角「設定」圖示，進入 LINE 設定頁面，後續可依照教學近一步調整 LINE 隱私。

首先，先點選擇「**隱私設定**」，將「阻擋訊息」開啟，能避免會收到陌生訊息，並且將「永許好友邀請」關閉，能避免陌生人會直接透過群組或公開貼文點開個人檔案，不會出現加好友按鈕，就能防止稍擾訊息。

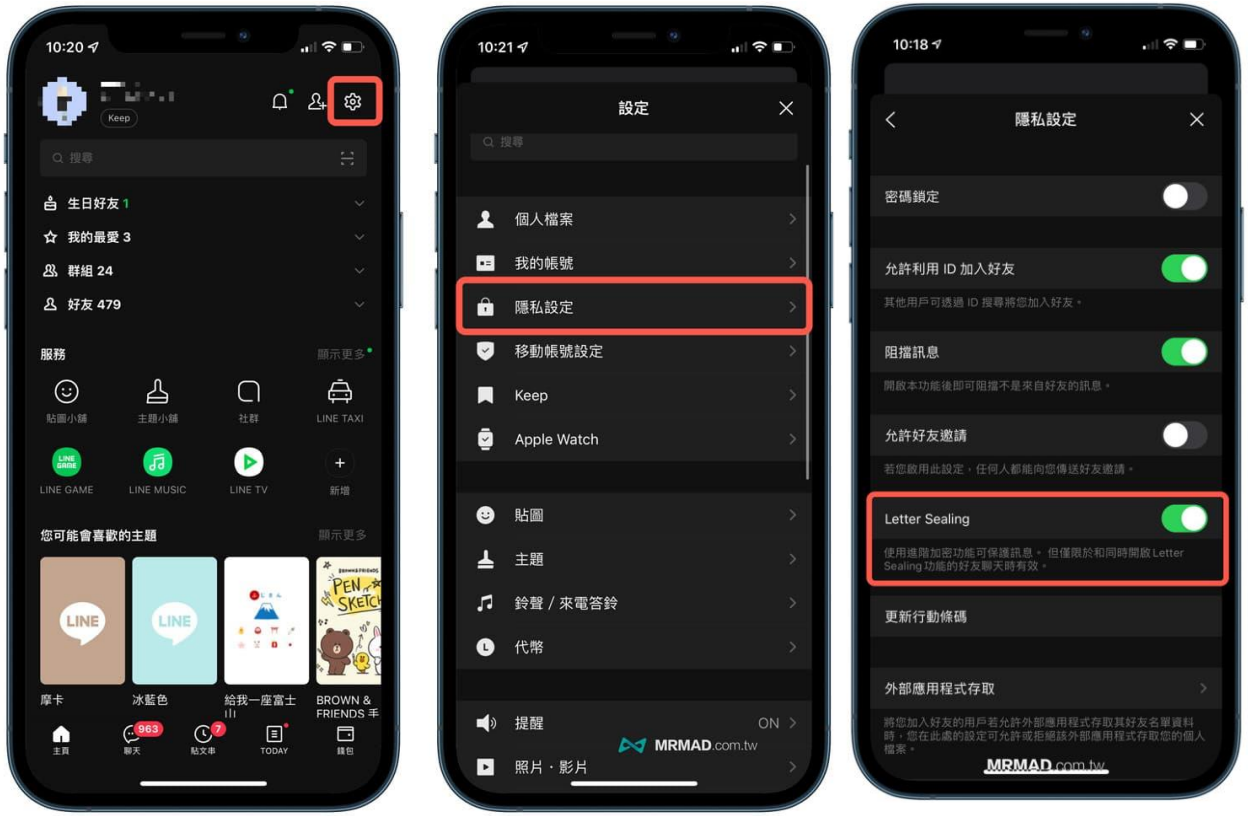


https://mrmad.com.tw/line-security-settings

10招提升LINE安全設定技巧(2/12)

2. 開啟點對點訊息保護（Letter Sealing）

LINE的Letter sealing(訊息保護)，是採用全球主流的AES演算法進行點對點加密，不僅是文字訊息，內容也支援語音通話的加密。而點對點加密的優勢，在於加解密使用的金鑰，皆由使用者手機自動產生，並存放於手機上，可以避免對話內容被第三方側錄而破解。



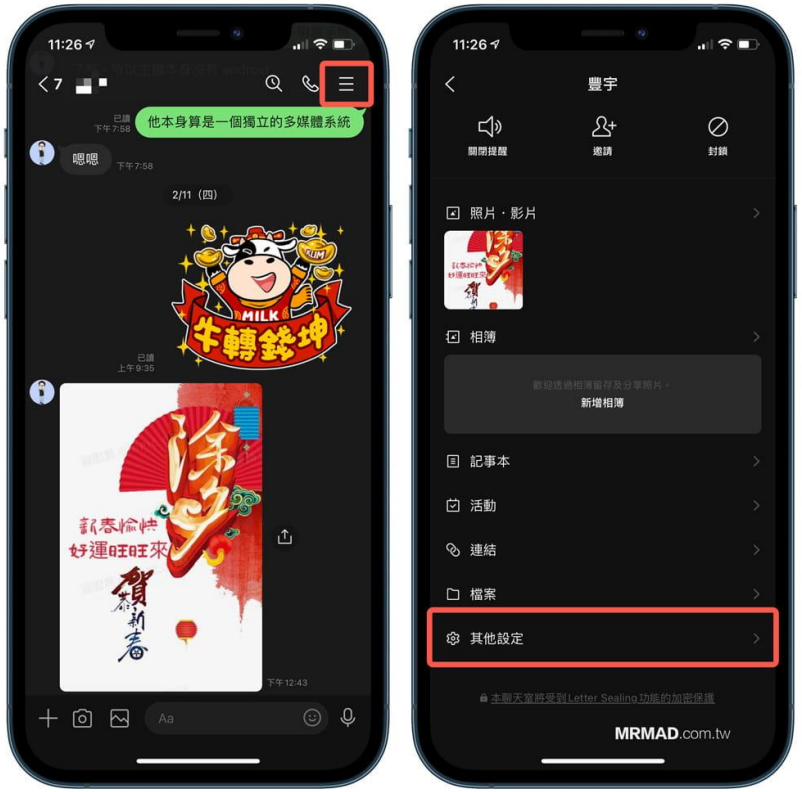
LINE App 預設會開啟，如想要確認，可以到「**隱私設定**」內將「**Letter Sealing**」開啟即可，這功能不建議關閉。

開啟手機版 LINE App 後，點選主頁右上角「**設定**」，再點「**隱私設定**」。

10招提升LINE安全設定技巧(3/12)

2. 開啟點對點訊息保護（Letter Sealing）

如果想要確定 LINE 聊天室有沒有啟用「**訊息保護（Letter Sealing）**」，可以打開 LINE 對話視窗後，點擊右上角「**三**」選擇「**其他設定**」。



10招提升LINE安全設定技巧(4/12)

2. 開啟點對點訊息保護（Letter Sealing）

會看見「**加密金鑰**」選項，就代表雙方都有打開 Letter Sealing 加密保護，甚至還可以看見加密金鑰細節，如果沒有就代表對方沒有開啟 Letter Sealing ，如果是聊比較機密對話，就可以先提醒對方要打開。

10招提升LINE安全設定技巧(5/12)

3. 帳號安全基本設定

設定位置是在 LINE「**設定**」>「**我的帳號**」內，如果都還沒有設定建議全部都綁定好，避免後續 LINE 帳號忘記密碼或登入不了，都要透過這些資料來認證。

如果是 iPhone 就建議打開「**同步綁定Apple ID 帳號**」功能，未來只要換設備或重裝 LINE 就能透過 Apple ID 直接立即登入，另外 LINE 也提供 Face ID 同步功能也可以考慮打開。

10招提升LINE安全設定技巧(6/12)

4. 聊天對話定期備份

很多人都會用 LINE 聊公事，所以 LINE 對話紀錄就會非常重要，比較建議打開「**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**」內，詳細進階備份技巧也可以參考底下教學：

10招提升LINE安全設定技巧(7/12)

5. 開啟 LINE 密碼鎖定 避免被偷看

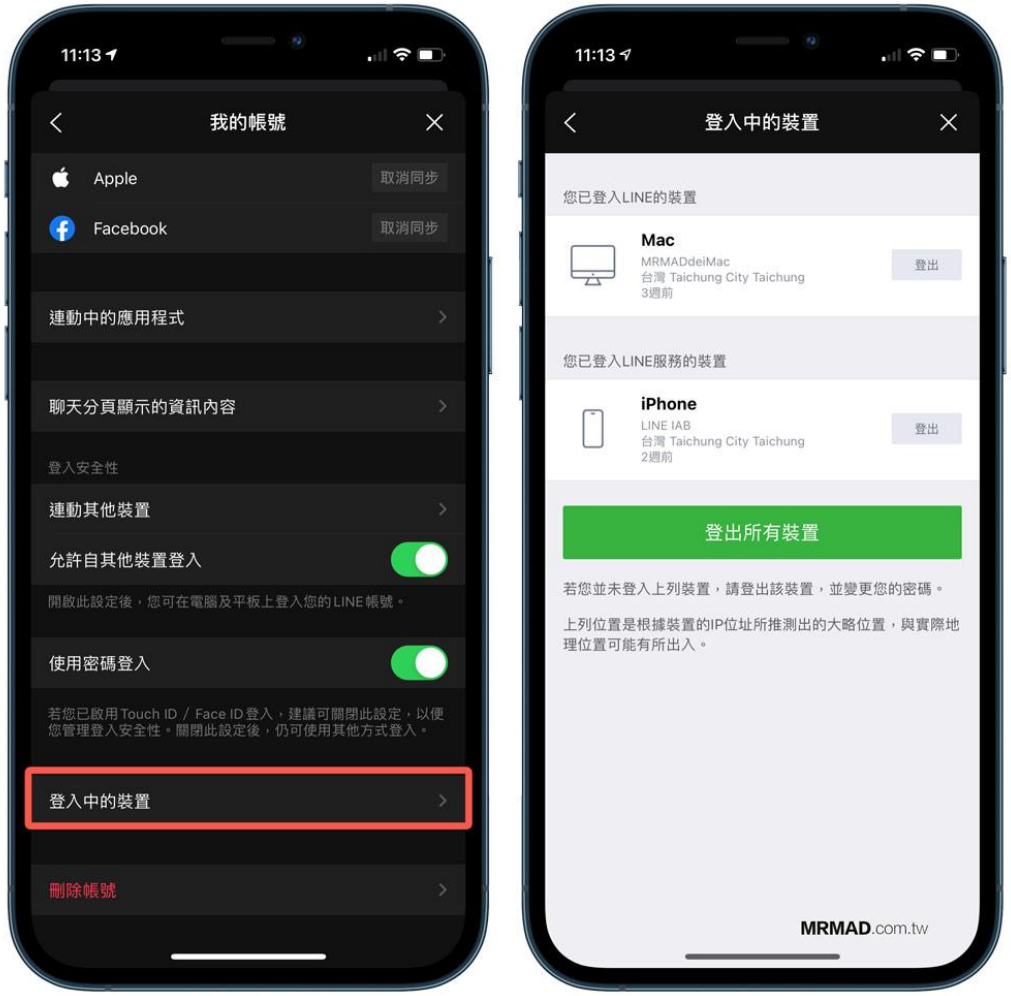
日常生活中，有些時候總是手機沒有帶在身邊，像是上班時間要去上廁所或裝水，剛好手機還沒上鎖狀態下，會造成有心人士就可能會偷看你 LINE 對話紀錄和聯絡人，所以要防止 LINE 隱私，就建議要打開 LINE 密碼鎖功能，只要對方點開 LINE App就會要求輸入密碼才可進入。

至於 LINE 密碼鎖設定，可以透過 LINE「**設定**」>「**隱私設定**」開啟「**密碼鎖定**」，就會要求自訂一組鎖定密碼。(特別注意這與 LINE 帳號密碼是完全不同)

10招提升LINE安全設定技巧(8/12)

6. 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。



10招提升LINE安全設定技巧(9/12)

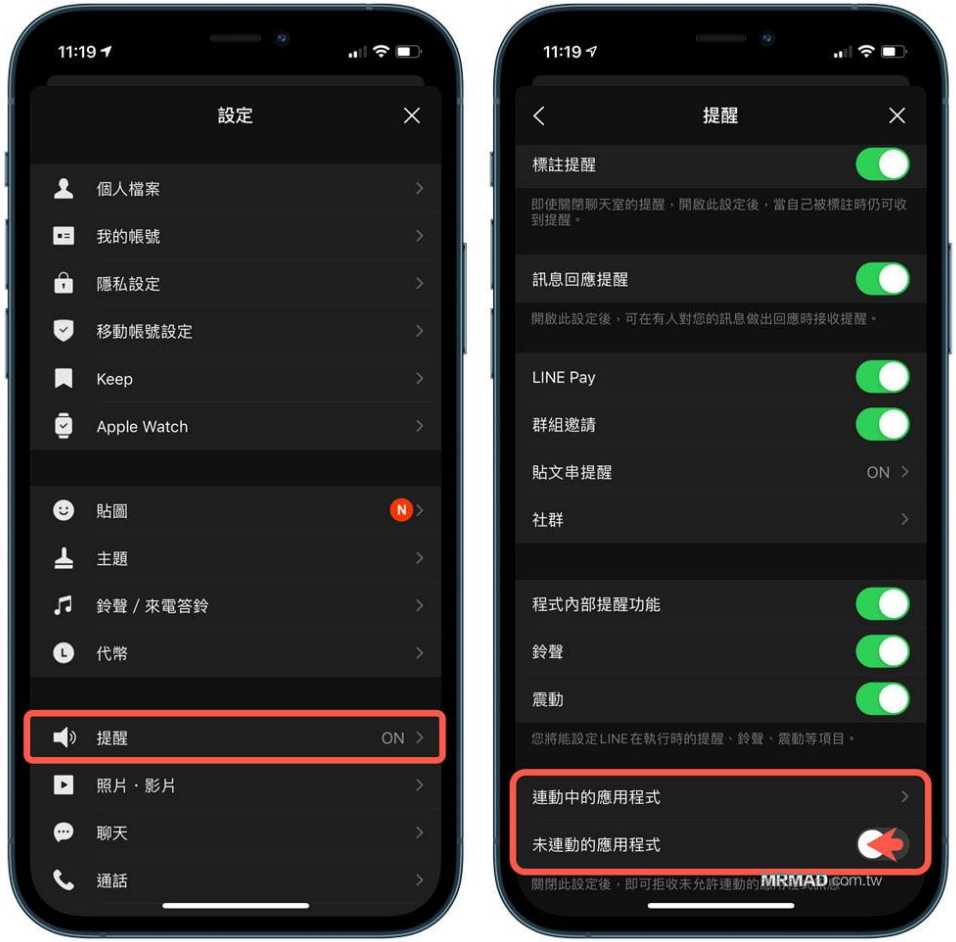
7. 防止其他裝置登入

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。

10招提升LINE安全設定技巧(10/12)

8. 關閉未使用連動的應用程式

有時候 LINE 免費貼圖活動，都會需要下載相關 LINE 推出的 App 或遊戲，連動後才能夠取的，但是這會導致朋友如果有在玩 LINE 遊戲，對方的活動進度就會不定時的發送通知，如果你感覺很煩，又或者是想取消所有和 LINE 連動的應用程式，以提升帳號安全，可以透過LINE「**設定**」>「**提醒**」，將「**為連動的應用程式**」關閉，並且點入「連動中的應用程式」清單中取消連動。



10招提升LINE安全設定技巧(11/12)

9. 防止不熟朋友掌握你動態消息

現在大家可能見面後，就會互相留下LINE ，甚至連同事、客戶和主管可能也都會加入，只是單純在工作上有來往，又不想將自己日常生活動態更新讓對方知道，這時候就可以到 LINE「**設定**」>「**貼文串**」，將「**自動向新好友公開**」關閉。

另外在點入「**追蹤設定**」內，可以將「**允許追蹤**」和「**公開追蹤資訊**」兩項功能關閉。

10招提升LINE安全設定技巧(12/12)

10. 公用電腦改用 LINE 行動條碼登入

如果是在公用場合或公用電腦要登入 LINE 帳號，我們很難確定電腦會不會有木馬，或是偷安裝鍵盤側錄軟體，如果直接輸入 LINE 帳號密碼，同等於就被盜取，所以最安全作法就是，非個人電腦都改用 LINE 行動條碼登入。

只要開啟 LINE 電腦版，右側會顯示行動條碼登入，打開手機 LINE App ，點選搜尋框右側「**掃描按鈕**」。

對準電腦 LINE 行動條碼掃描，就會跳出要登入 LINE 嗎？點擊「**登入**」即可免輸入帳密，就可以直接登入 LINE 帳號。

過度的授權將隱私拱手送人

權限開放不當，個資外洩

定義	權限開放不當是指在資料管理中未適當限制存取權限，導致未經授權的人員能夠存取或查看敏感個人信息，從而造成個人資料的非預期外洩和安全風險。
影響	➢ 受害者個人資料外洩可能導致隱私被侵犯，包括聯絡方式、金融信息等敏感數據。 ➢ 外洩的個資可能被不法分子用於身份盜用，進行詐騙或其他非法活動。 ➢ 個資泄露後，受害者可能經歷焦慮和不安，擔心個人信息被濫用的後果。
造成原因	➢ 過度寬鬆的數據存取權限，允許未經授權人員輕易訪問敏感信息。 ➢ 缺乏使用者身份驗證和授權機制，使得數據庫對所有人開放。 ➢ 未實施數據加密，使得存儲或傳輸中的個人信息易於被攔截。 ➢ 管理不善的系統權限設置，未及時更新或撤銷前員工的存取權限。

個資外洩案例

https://news.tvbs.com.tw/life/2068208

某高中通報3級個資外洩事件

時間	2023年11月間
案情	➢ 2023年11月11日某高中通報，該校誤設定Google表單，開啟填寫摘要功能，導致已填寫該表單之同學，其姓名、學號、座號、個人電話、電子郵件、通過英檢等級、檢定證照照片等個資外洩。 ➢ 遭外洩之學生個資，可能導致學生的權益受損或個資遭不法利用。
影響	● 學生個資泄露可能遭不法分子利用，影響學生隱私和安全。 ● 個資外洩事件可能損害學校信譽，引起家長和學生不滿。

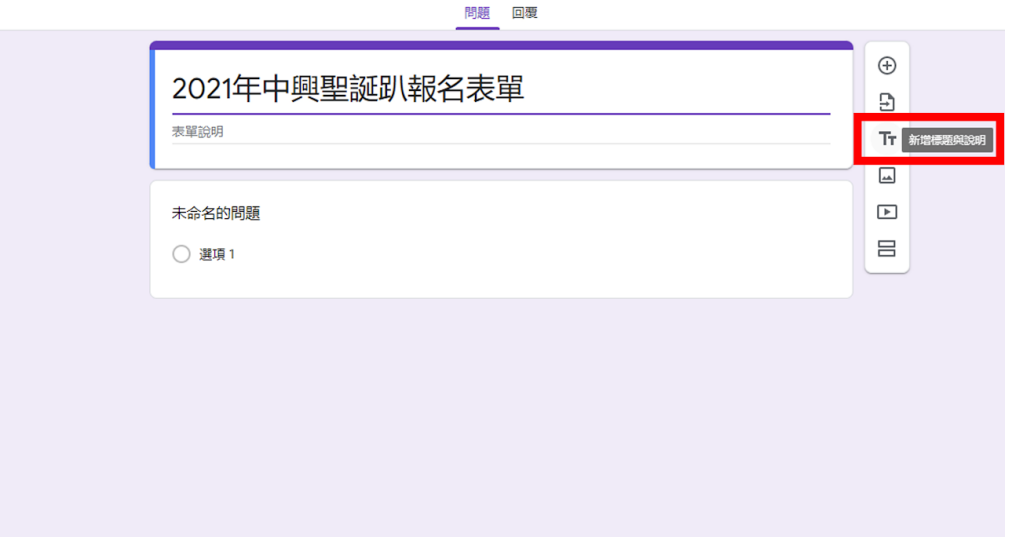
Google表單個資使用原則(1/9)

Google表單個資使用原則(2/9)

1.「個人資料蒐集聲明」的處理方式

使用Google表單蒐集個人資料時，需於表單一開始明確告知個人資料蒐集、處理及利用方式。

開啟Google表單右排工具列選擇「**新增標題與說明**」，
在「**標題**」及「**說明**」內輸入相關資訊。



https://sites.google.com/email.nchu.edu.tw/g-form/%E9%A6%96%E9%A0%81?authuser=1#h.7g0p3uqwc1cc

Google表單個資使用原則(3/9)

2. 落實「資料最少蒐集原則」

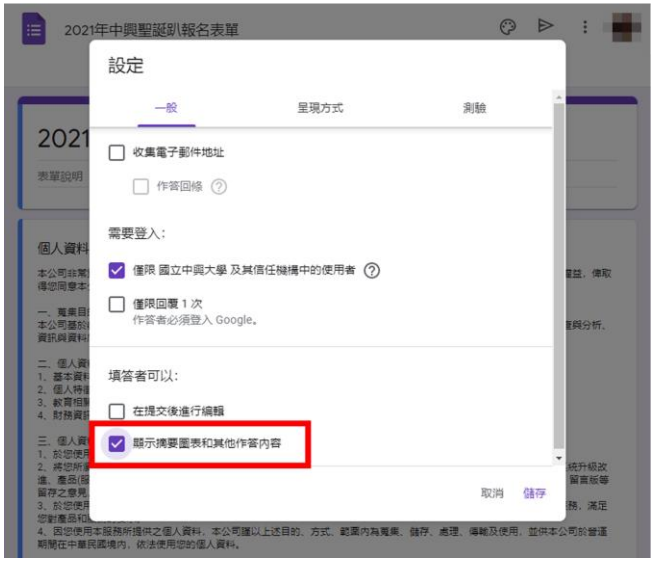
只需要蒐集必須的資訊，不過度的蒐集個人資訊，減少資料保管負擔。

舉例來說，一般報名時常見需填寫手機號碼，但是如果已要求報名者填寫email，並且以email 聯絡已可滿足作業需求，並無必要使報名者額外填寫手機號碼，徒增資料保管風險。

Google表單個資使用原則(4/9)

3. 避免不小心公開作答內容

在設定中看到「**顯示摘要圖表和其他作答內容**」，可能會認為勾選起來才方便讓填答者看到自己的填答內容，但其實這樣做是很危險的!!!
如果真的勾選該項設定，就會讓**"所有"**填答者都能看到其他所有人填寫的內容，也就是表單中只要有個資欄位就會造成個資洩漏，導致非常嚴重的後果，因此要特別注意這項不能勾選起來。

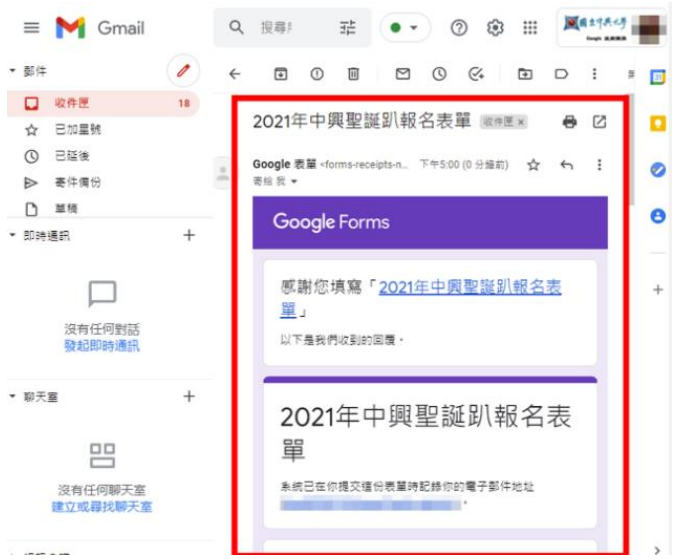


為了防止讓人看到所有人填寫的作答內容，**必須確認「顯示摘要圖表和其他作答內容」沒有勾選，如此才不會在填寫完表單後出現這個「查看先前的回應」連結。**

Google表單個資使用原則(5/9)

3. 避免不小心公開作答內容

若需要讓填答者可以存查自己的作答內容則可以使用「**收集電子郵件地址**」中的「**作答回條**」讓作答者自己可以存查自己的作答內容。
將「**作答回條**」內的「**一律**」勾選之後，每位填答者都可以在填寫完問卷後收到信件留存自己填寫的內容，使用此功能不會造成作答內容被公開外洩的問題。



Google表單個資使用原則(6/9)

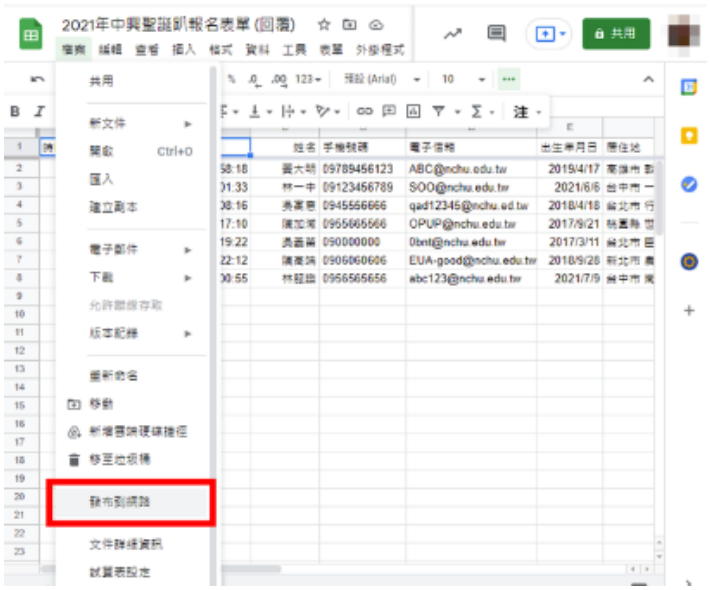
4. 不應執行「發布到網路」功能

Google表單管理者若想要更方便取用填答內容時，通常會再建立試算表，填答資料就會連動記錄在這個試算表。
所以，這個試算表也要保護好，尤其**千萬不可執行「發布到網路」功能**，以避免將資料公開到網路上。

Google表單個資使用原則(7/9)

4. 不應執行「發布到網路」功能

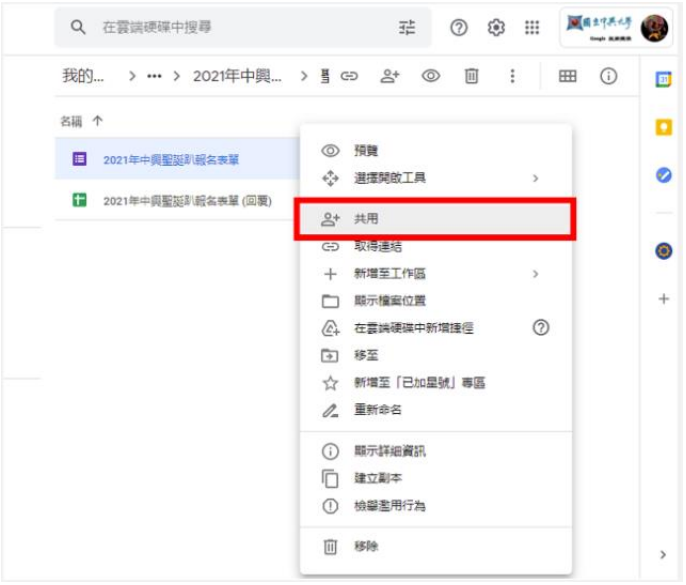
建立試算表後檔案內有一個功能是「**發布到網路**」，會將內容以HTML網頁形式公開，任何人只要知道網址都可以直接觀看你的試算表內容，且無須登入Google信箱也可觀看，所以**千萬不可執行「發布到網路」這項功能。**

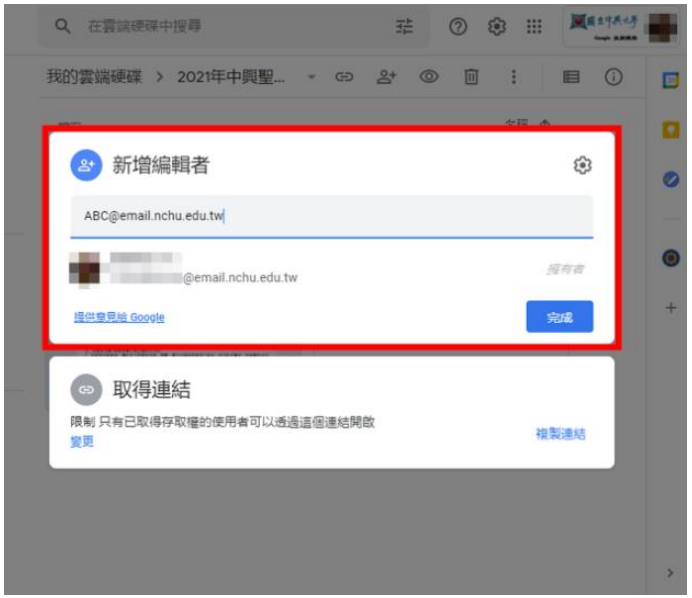


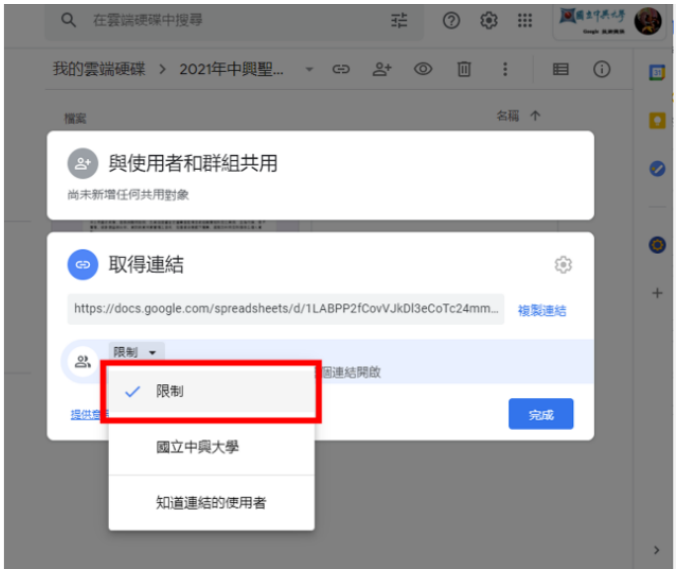
Google表單個資使用原則(8/9)

5. 不應開放給不相關人員存取權限

Google雲端硬碟的表單與試算表檔案，應確認有無將檔案開放給不相關的人員存取權限，如有共同作業之需求，應使用新增共同編輯者。
最後**「取得連結」一樣禁止開放成「知道連結的使用者」能編輯或檢視**，以避免連結網址外洩而可能導致資料洩漏。



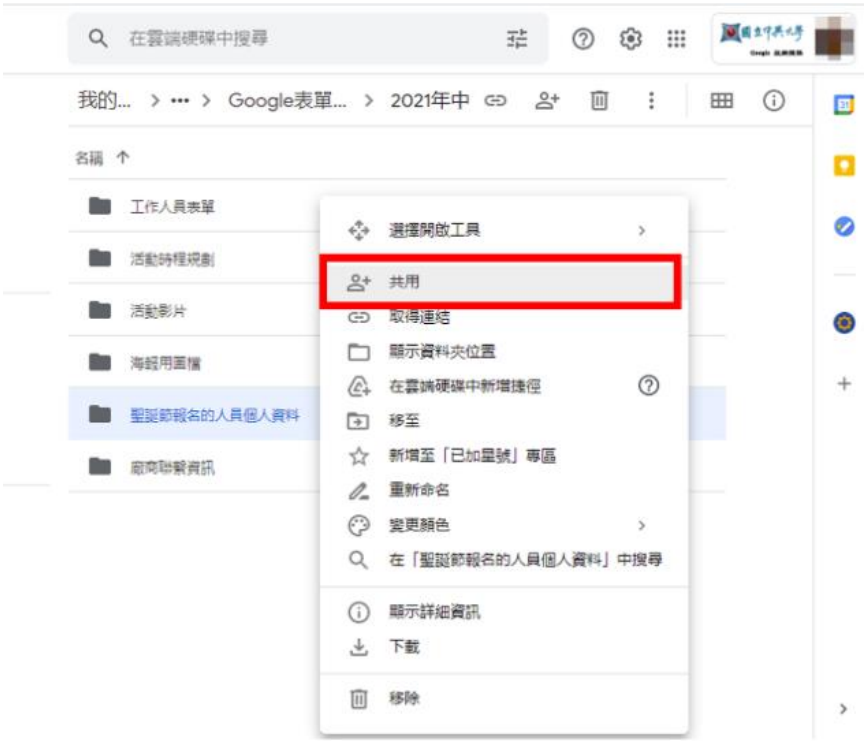


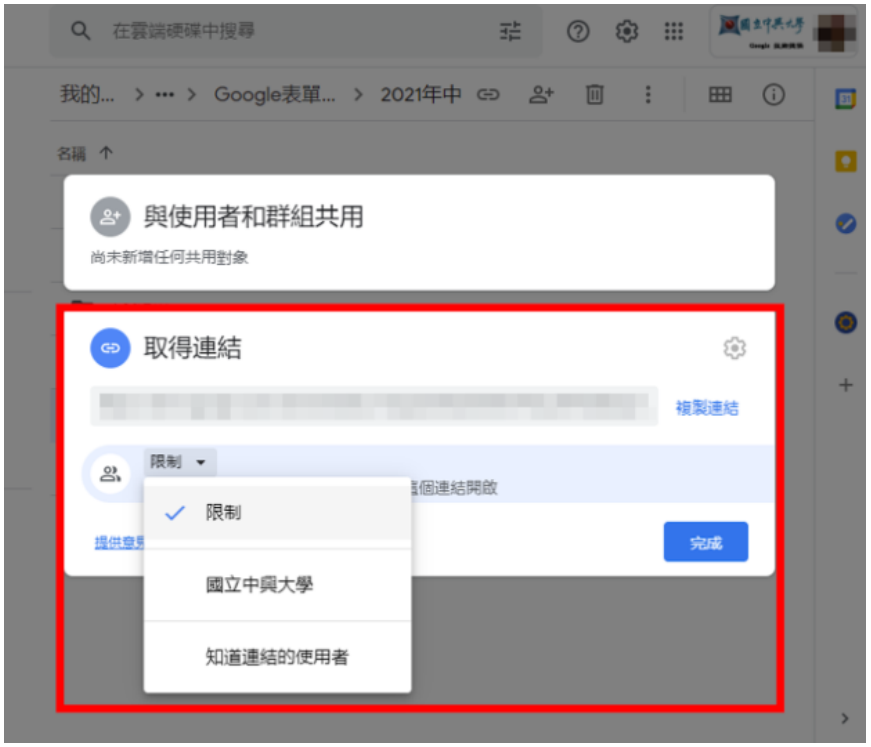


Google表單個資使用原則(9/9)

6. 雲端檔案切勿放置在共用資料夾

為了防止資料洩漏，除了檔案本身不要開啟共用外，資料所放置的「資料夾」本身也不要開啟共用。





猝不及防的勒索軟體攻擊

勒索軟體

定義	勒索軟體，又稱勒索病毒，是一種特殊的惡意軟體，又被歸類為「阻斷存取式攻擊」，其與其他病毒最大的不同在於目的。
症狀	➢ 將受害者的電腦鎖起來，使其無法運作。 ➢ 加密受害者電腦硬碟上的檔案。
目的	➢ 取得電腦控制權要求支付贖金以解除控制。 ➢ 要求支付贖金以讓受害者取回解密檔案的金鑰。
傳播形式與途徑	➢ 偽裝成看似無害的檔案，以木馬病毒的形式傳播。 ➢ 以一般電子郵件的途徑欺騙受害者點擊連結下載。 ➢ 透過USB等移動式儲存設備或軟體本身的漏洞在聯網的電腦間傳播。 ➢ 新趨勢：網路釣魚(群發郵件、網紅發連結) 。

勒索軟體科普

https://www.youtube.com/watch?v=5TKqxtzj8cM

勒索軟體攻擊新聞案例

這些網站別亂點！　小遊戲、心理測驗恐遭木馬程式入侵

記者 劉俐均 / 攝影 陳宥翔 報導
發佈時間：2023/03/14 23:13
最後更新時間：2023/03/14 23:13

小 中 大

這些網站別亂點！ 小遊戲、心理測驗恐遭木馬程式入侵

劉俐均 陳宥翔
更新時間： 2023年3月15日

個資外洩的狀況頻頻發生，除了企業大規模的洩漏狀況，還有零星案件像是民眾誤點釣魚網站，最常見就是心理測驗、填寫陌生問券、小遊戲等等，現在政府也擬提高個資法罰則，希望能遏止亂象。

圖 / TVBS

https://news.tvbs.com.tw/life/2068208

網站別亂點! 心理測驗有木馬程式!

時間	2023年3月間
案情	➢ 企業和政府資料庫大規模外洩普遍，常因安全漏洞或員工疏忽導致敏感信息公開。 ➢ 民眾常透過點擊釣魚網站、參與社群心理測驗等活動，不知不覺中洩露個人資料。 ➢ 台灣在檔案加密和勒索病毒方面的攻擊比國外高2到3倍，顯示資安防禦觀念需加強。 ➢ 台灣有超過1000萬人手機號碼被洩漏，最容易外洩三大個資包含「登入密碼」、「電話號碼」以及「姓名」。
影響	● 個人隱私外洩可能導致身份被盜用，網路安全受威脅。 ● 企業若洩漏資料可能面臨信譽損失及客戶流失。 ● 經濟上直接受損，需支付恢復系統和資料的額外費用。 ● 法律責任加重，違反資料保護法可能遭受嚴厲處罰。

勒索軟體攻擊新聞案例

台積電驚傳遭駭客勒索7千萬美元？公司緊急回應了

16:20 2023/06/30 | 中時新聞網 | 吳美觀

台積電供應商傳遭駭客勒索7千萬美元 苦主回應事件始末

2023/07/03 08:04 文 | 鉅亨網

▲台積電供應商傳遭駭客勒索7千萬美元 苦主回應事件始末。（圖／鉅亨網）

https://www.wealth.com.tw/articles/9f54fe8d-2447-4f2a-ab26-635e319a4f32

台積電供應商遭勒索7千萬美元

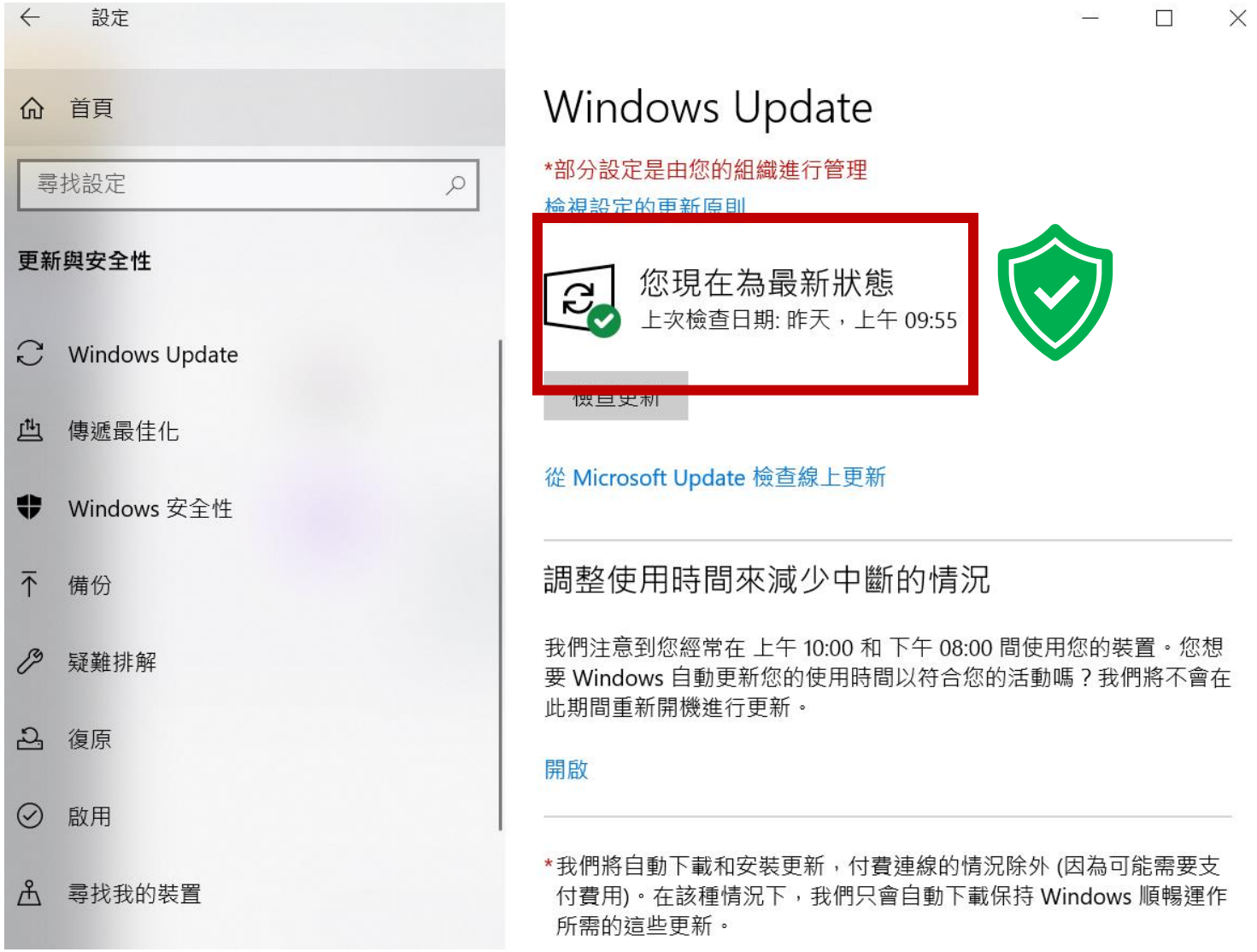
時間	2023年6月間
案情	➢ LockBit勒索軟體組織攻擊台積電供應商擎昊科技，竊取數據並索要7000萬美元勒索金。 ➢ 擎昊科技於6月29日發現遭網攻，立即通報客戶並啟動損害控管，聘請資安團隊評估影響。 ➢ 被竊數據包括工程測試區的設定檔等，目前無證據顯示客戶的機密資料或實際應用受到影響。 ➢ 擎昊科技關閉受影響系統，確認無重大運營損失，事件已進入刑事調查階段；如遇類似事態，可求助台灣電腦網路危機處理暨協調中心。
影響	● 擎昊科技遭LockBit勒索，引發供應鏈安全疑慮。 ● 台積電供應鏈可能面臨重大資安挑戰。 ● 擎昊科技客戶資料洩漏可能損害商譽。 ● 此事件可能促使業界加強網路安全防護措施。

預防勒索軟體牢記「三不三要」

重要檔案進行備份參考原則

- 至少備份三份。
- 使用兩種不同形式。
- 其中一份備份要存放異地。

強化防護措施 (檢查作業系統更新)



強化防護措施 (更新到系統最新版本)

Windows 11 目前版本

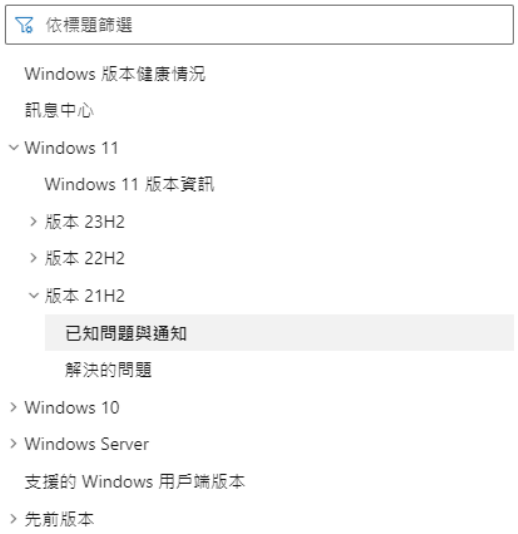
(所有日期都是以 ISO 8601 格式列出：YYYY-MM-DD)

維護通道

版本	服務選項	推出日期	最後修訂日期	最新組建	終止服務：家用版、專業版、專業教育版和工作站專業版	終止服務:企業版、教育版、IoT 企業版和企業多重工作階段版
23H2	正式版本通道	2023-10-31	2023-10-31	22631.2506	2025-11-11	2026-11-10
22H2	正式版本通道	2022-09-20	2023-10-26	22621.2506	2024-10-08	2025-10-14
21H2	正式版本通道	2021-10-04	2023-10-10	22000.2538	終止服務	2024-10-08

資料來源：微軟官網

強化防護措施 (停止使用不再支援的軟體)



Windows 11版本 21H2 已知問題和通知

發行項 • 2023/11/08 • 1 位參與者　　意見反應

本文內容

尋找已知問題和Windows 11版本 21H2 推出狀態的相關資訊。 如需 Windows 更新問題的立即協助，請使用 Windows 中的取得說明應用程式，或移至 support.microsoft.com。 請遵循 @WindowsUpdate X (先前的 Windows 版本健康情況更新 Twitter) 。

截至 2023 年 10 月 10 日目前的狀態

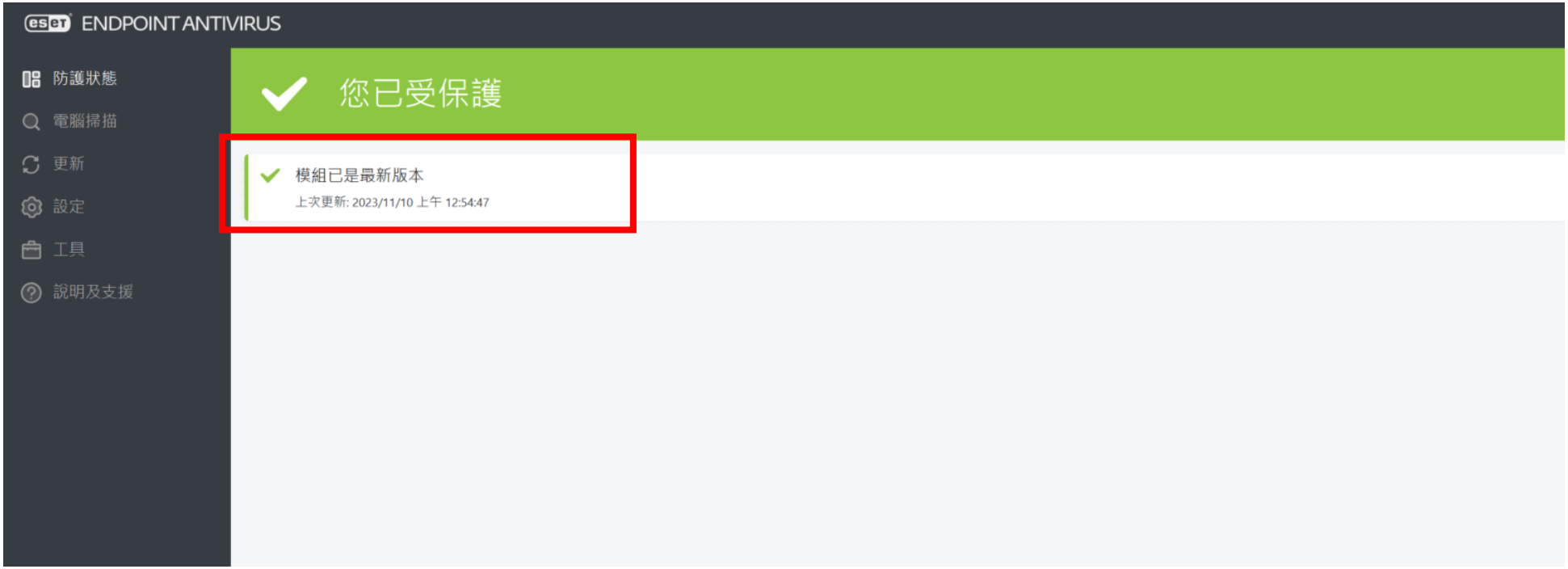
自 2023 年 10 月 10 日起，**21H2** 版的 Home 和 Pro 版本Windows 11已終止服務。 **2023 年 10 月** 10 日發行的 2023 年 10 月安全性更新是這些版本可用的最後一個更新。 在此日期之後，執行這些版本的裝置將不再收到每月安全性和預覽更新，其中包含來自最新安全性威脅的保護。 此版本的企業版、教育版、IoT 企業版和企業版多重會話版本將于 2024 年 10 月 8 日終止服務，屆時將會收到安全性更新。

為了協助您保持保護和生產力，Windows Update會自動起始Windows 11取用者裝置和非受控商務裝置的功能更新，這些裝置是在服務終止或在數個月內終止。 這可讓您的裝置持續受到支援，並接收對安全性和生態系統健康情況至關重要的每月更新。 針對這些裝置，您可以 **選擇方便** 裝置重新開機並完成更新的時間 。

一如往常，建議您將裝置更新 為最新版本 **的 Windows 11**。 如需詳細資訊，請參閱 **維護Windows 11 21H2 版結束 (家用 & 專業版)** 生命週期頁面。 如需維護時程表和生命週期的相關資訊，請參閱 **Windows 11版本資訊**、 **生命週期常見問題 - Windows**和 **Microsoft 生命週期原則搜尋工具**。

資料來源：微軟官網

強化防護措施 (檢查防毒軟體更新病毒碼)



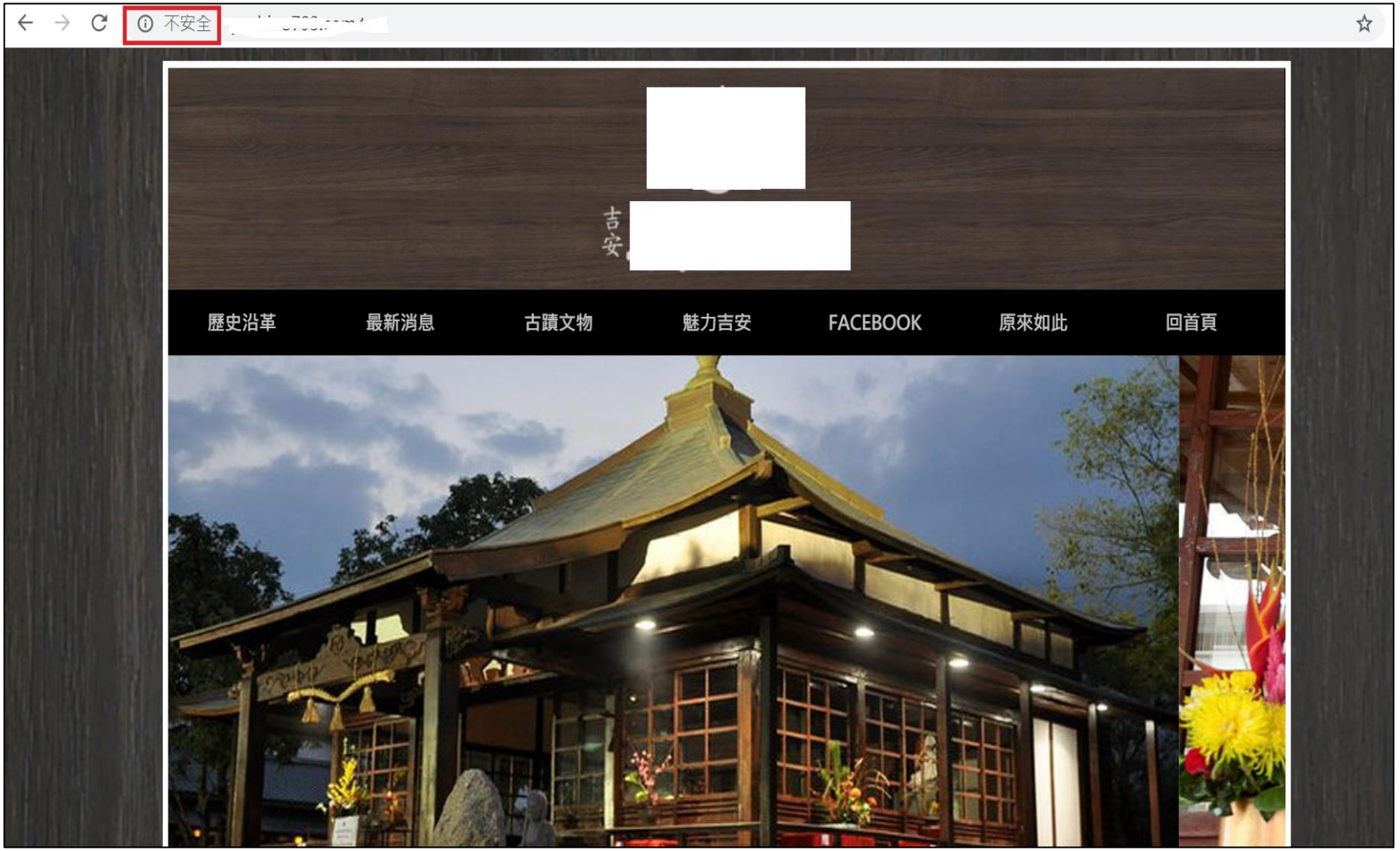
強化防護措施 (定期掃描)

強化防護措施 (關閉遠端桌面功能)

強化使用者安全性防護措施

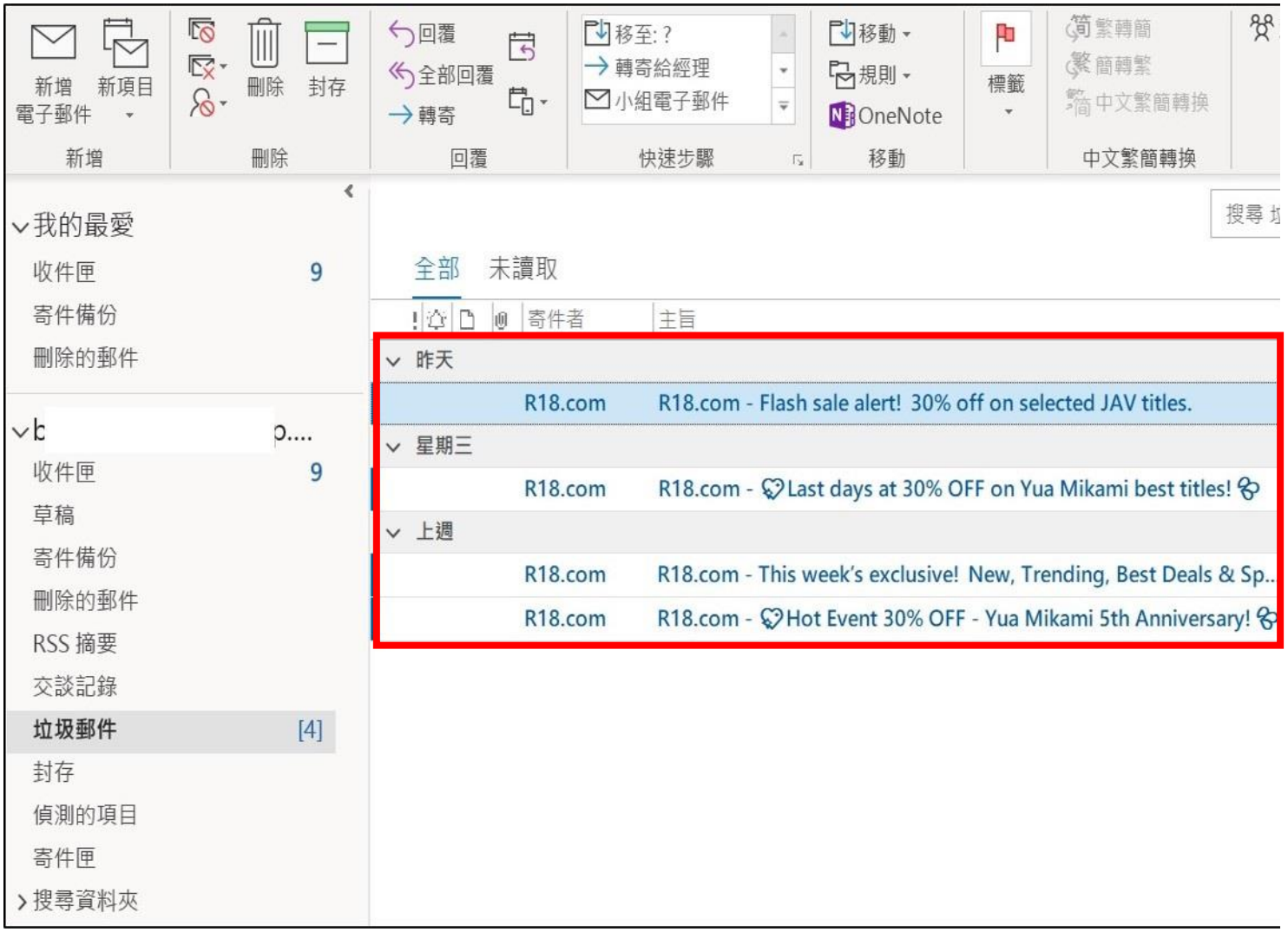
- 保持作業系統與應用程式的修補更新。
- 避免使用已不再維護更新的系統與軟體。
- 安裝並執行防毒軟體。
- 更新病毒碼與定期掃描。
- 第三方防毒軟體掃描。
- 保留防毒程式隔離區的紀錄以備追查求償之用。
- 關閉遠端桌面功能。
- 建立良好的資安意識。

改變作業習慣 (留意網頁是否安全)

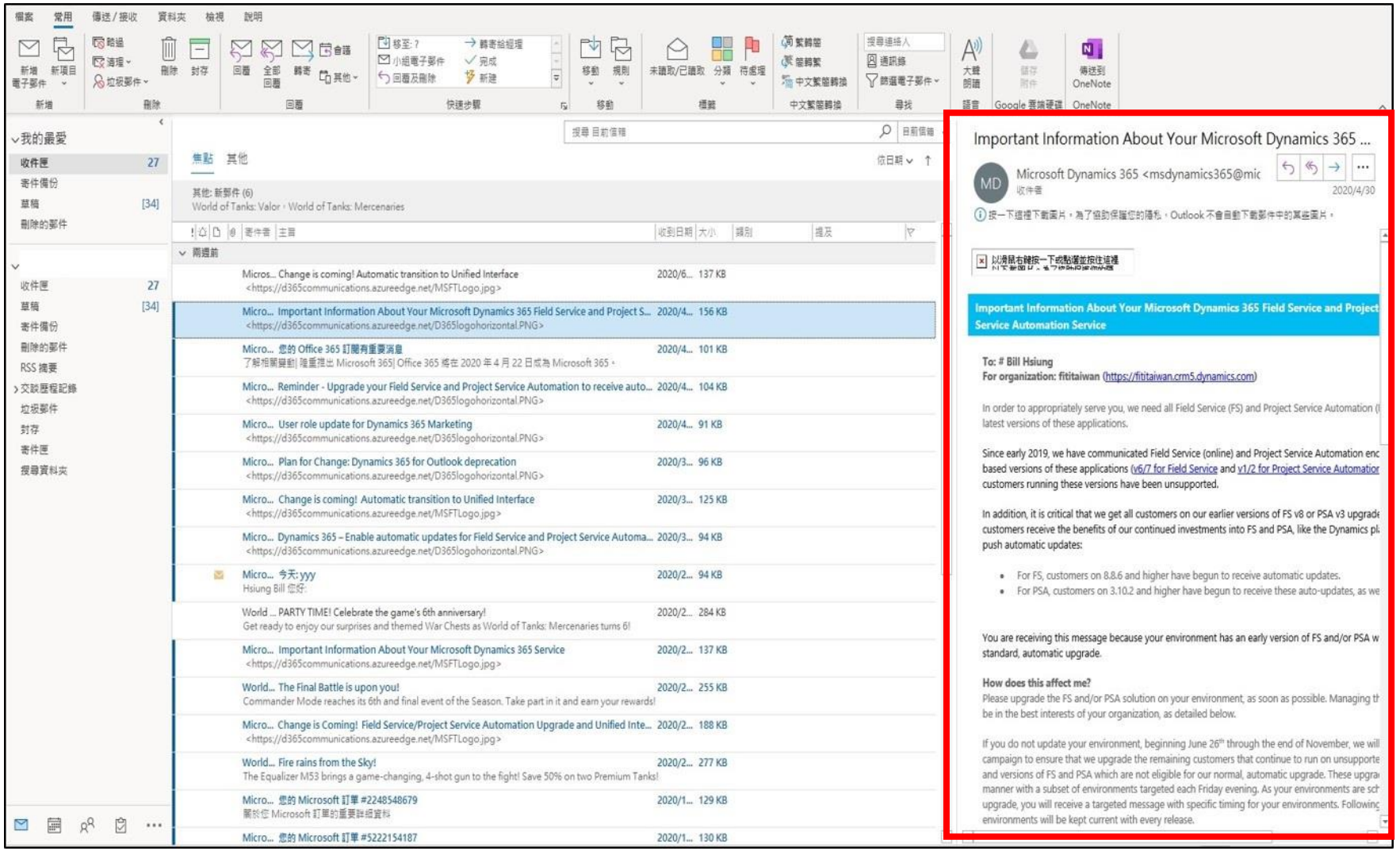


資料來源：網路

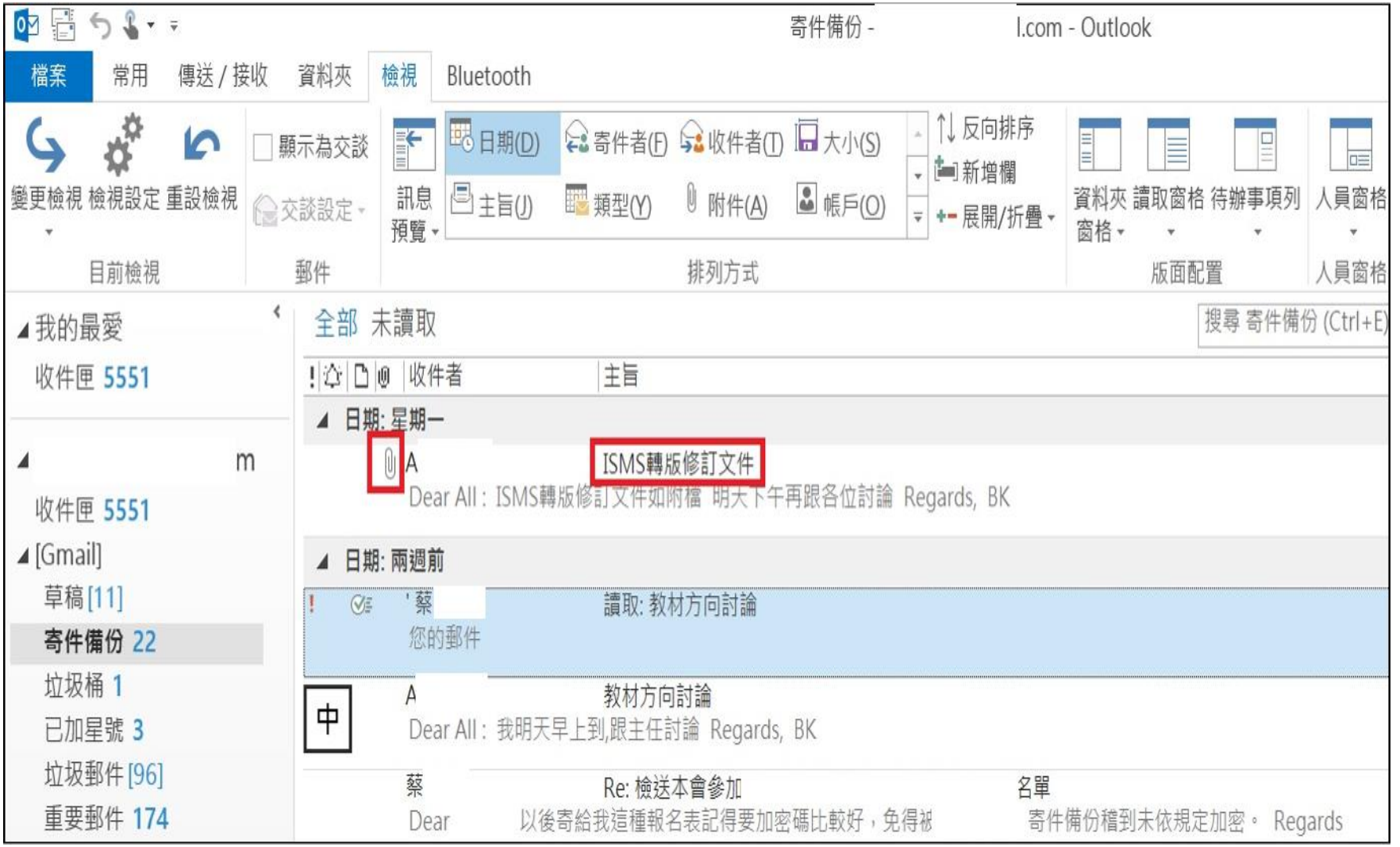
改變作業習慣 (不明來路的信件不要開啟)



改變作業習慣 (關閉信件預覽功能)

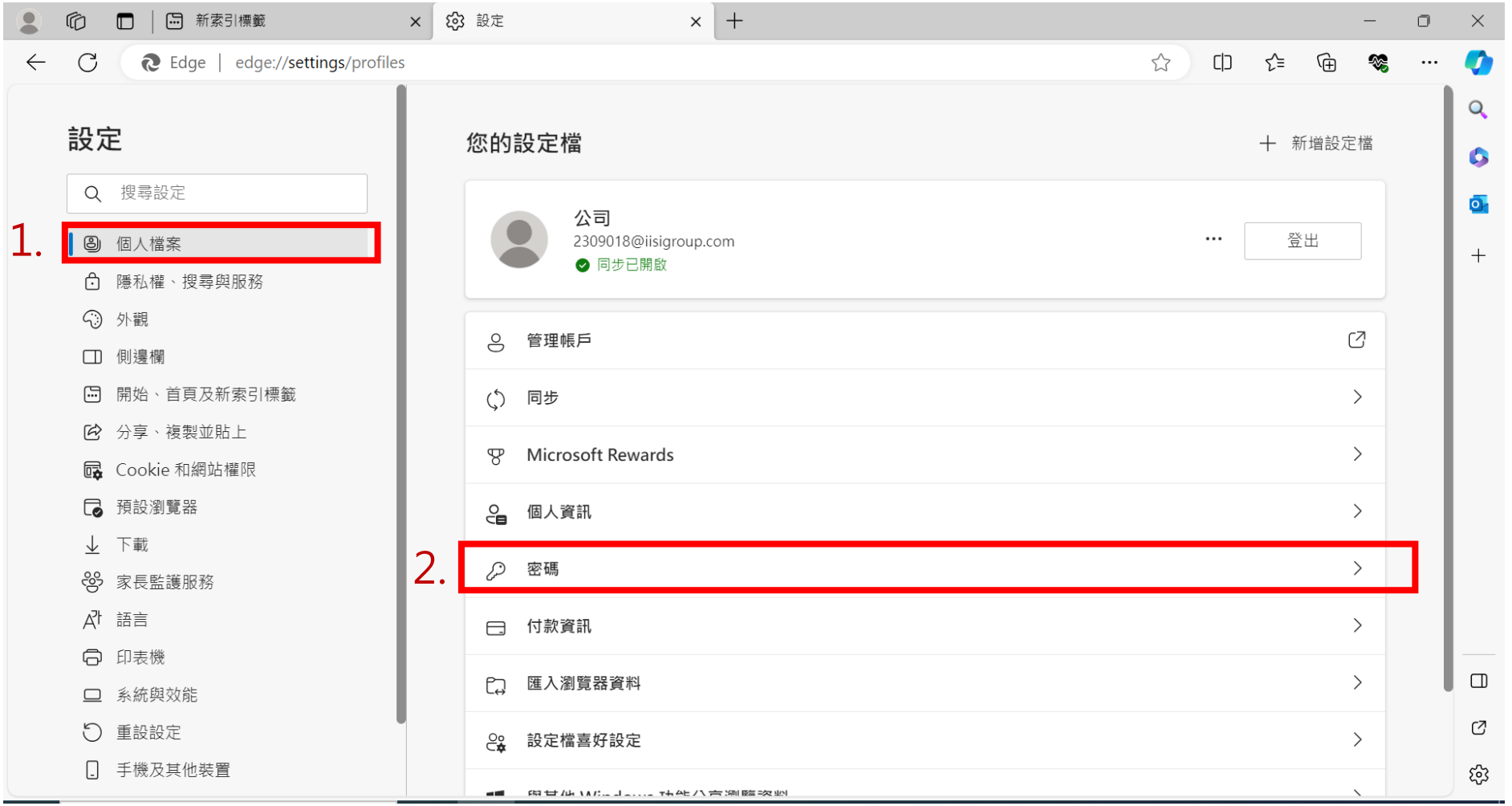


改變作業習慣 (外寄檔案加密)



改變作業習慣 (瀏覽器安全性設為平衡以上)

改變作業習慣 (瀏覽器取消自動記憶密碼1/2)



改變作業習慣 (瀏覽器取消自動記憶密碼2/2)

改變作業習慣 (設定螢幕保護程式)

改變習以為常的作業方式

- 勿瀏覽未受安全保護的網頁或下載不明來源檔案。
- 勿使用狀態不明的外接裝置 (USB、記憶卡等)。
- 勿點選不明的連結或開啟不明來路的信件。
- 勿使用郵件預覽功能。
- 瀏覽器安全性應設為中高或平衡 (Microsoft Edge) 以上。
- 瀏覽器不可設定自動記憶密碼。
- 外寄郵件如有附加機敏性檔案應加密處理。
- 設定螢幕保護程式，長時間離座關閉電源。

建立良好的資安意識 (1/2)

- 留意一些違反常理的優惠或抽獎活動。贏得競賽或免費獲得昂貴的版權內容，都可能是誘使您下載惡意軟體的伎倆。
- 留意發現病毒或告知裝置遭感染的相關警告。顯示這類警告的網站可能試圖引起您的恐慌，進而誘使您下載垃圾軟體。
- 務必只下載您確定沒有安全危害的檔案，或是只造訪您所信任的網站。

建立良好的資安意識 (2/2)

- 網路下載的檔案，應先使用防毒軟體進行掃毒，確認無虞才可執行、開啟使用。
- 如果畫面上出現可疑的彈出式視窗要您更新或下載程式，請勿點選該視窗，並改為前往官方網站下載程式。

遭受勒索軟體攻擊時之災害應變

- 立即拔掉網路線或無線網路裝置以避免災情擴散。
- 立即關機並通報資通安全相關單位請求協助。
- 如有必要通知有關單位進行全面清查。
- 謹慎復原受攻擊之設備避免二次攻擊。

面對攻擊事件的因應之道

本日總結

網路安全，人人有責

- 別輕信，網址先核信，防範網釣始於點擊前
- 防護如盾，防毒軟體護你安全
- WiFi公開，個資不公，隨時防範網路陷阱
- 資料貴重，嚴防網騙，謹慎分享，保護你我他
- 知識如劍，網安自強，時刻警惕網詐威脅

「鍊條的強度，取決於其最薄弱的環節」

（A chain is only as strong as its weakest link）

~18世紀英國哲學家托馬斯．里德（Thomas Reid）

- 感謝聆聽 -

資拓宏宇永遠與您一起創新前進

always innovative always IISI