網路平臺安全使用學習手冊

本手冊將帶領你

認識常用的
網路服務平臺

瞭解使用網路平臺時
可能遭遇到哪些風險

學習如何避免網路
平臺所帶來的風險

手冊大綱

一、 小故事

詩詩是一位高中生，星期六的早上她打開電腦，收件匣裡有一封來自作業小組長的電子郵件：「想要我的素材嗎？想要的話可以全部給你，去找吧！我把所有的素材都放在雲端了。」詩詩啞然失笑：「這是誰想的台詞呀！」

她打開雲端硬碟下載了所有檔案，想要早點做完作業，下午就能和好閨蜜一起逛街，於是詩詩打開手機裡的通訊軟體，透過訊息約定見面的地點。

下午兩點，詩詩拿著手機開著地圖導航，走到新開幕的厚鬆餅店前和閨蜜阿姿會合，排隊等著進店的時候，她們滑著手機看短影片，查看最新的時尚流行，一頓悠閒的美食過後，詩詩心滿意足地在網路地圖上給店家留下了五星好評。

走在繁華的潮服一條街，兩人頻繁地進出幾間店家，不停試穿並且相互評論，終於詩詩找到了一件令她眼睛為之一亮的洋裝，她買下之後直接換穿，自拍一張照片發到社群網站上，並且留下一句話：「我找到了我的one piece!」收穫了無數的讚與愛心。

請你想一想，在詩詩的一天中，她用到了哪些網路服務平臺？

雲端硬碟

雲端硬碟是一種線上同步儲存服務，具有線上的檔案儲存空間可以透過任何裝置存取、備份，同時也是一個檔案共用平臺，使用者可以利用安全的個人雲端儲存空間與其他人共用內容。

地圖導航

地圖導航是結合線上地圖與街景圖像的一項網路服務，使用座標來辨識地理位置，能夠即時計算出發地與目的地之間的距離與交通時間，並且提供即時路況、路線安排、交通方式等資訊。

二、 概述

現代人的學習、工作、交際、娛樂都離不開電腦，再加上網路發達，各種相關內容都直接透過網路接收與交流，生活的面貌很自然地就變成了網路的形狀，人人都是各種網路服務平臺的重度使用者，當網路把全世界展示在你面前的同時，你也把自己公開在網路世界上了，在享受便利的同時，其實風險也伴隨而來，如何保護自己，就成了現代人必須具備的基本網路素養。

現代人常用的網路平臺，最基本的還是交換訊息與資料用的電子郵件，收集查閱資料的網頁服務和搜尋引擎，接著是日常聯絡的即時通訊軟體，還有大方秀出自我的社群網站平臺。

而使用這些平臺的安全考量重點，其一是不讓惡意的內容隨之流入你的電腦或手機，二是不讓你的隱私和個人資料流出到網上。

個人在任何網路平臺上所有行為，都應該以確保這兩個重點為前提而行，以下會分別介紹一些該關注的要點。

三、 電子信箱平臺安全使用

電子郵件信箱地址（E-mail Address)就像是住家的門牌號碼，任何人都可以根據這個門牌號碼寄信給你，即時通訊軟體則須雙方都是好友才能彼此傳送訊息與通訊，電子郵件是任何陌生人都可以寄送給你的，所以當然會有許多不請自來的廣告信件和惡意信件，這並不是它的缺點，電子郵件的用途本來就是用來和外人交流用的，但是就像你不會隨便給陌生人你的手機號碼一樣，你也不應該隨便給陌生人你的電子郵件信箱地址。

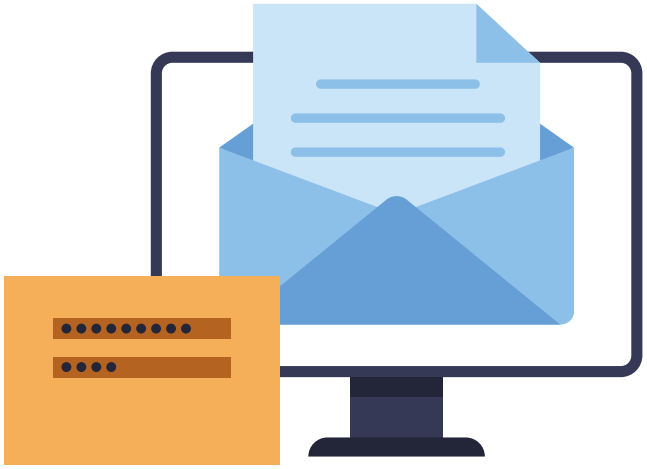
安全地使用電子郵件平臺的第一個要點

就是不要隨意流傳你的電子郵件信箱地址。

在網路上常有許多「填上電子郵件就抽獎或送贈品」的活動，也有許多必須填上電子郵件註冊帳號以後才能夠使用的網站，你在填上你的電子郵件之前，需確認這個活動或網站的主辦方，是不是一個資訊透明、有商譽、可以信任的廠商，否則貿然填上電子郵件，等於是把你的信箱奉送給可疑份子。

又或者你擁有不只一個電子郵件信箱地址的話，就填上你最不常使用、或較不重要的電子信箱吧！

那麼萬一這個電子郵件信箱被廣告信淹沒了，至少不會影響到你日常學習與工作用的信箱。



安全地使用電子郵件平臺的第二個要點

就是不要點開來路不明的東西，包括郵件內夾帶的檔案或連結，檔案裡面可能包含惡意的電腦病毒或木馬程式，連結可能把你帶往詐騙的偽造網站。

所以，當你收到一封電子郵件的時候，首先注意寄件人的拼字和網域是否正確，其次注意當中夾帶的連結網址拼字是否正確，是否指向相似但不同的網域，又或者根本是亂七八糟的免洗網址。

許多惡意郵件會偽造成知名服務平台的客服信件，接著告知你中獎了、帳號出了問題、有包裹要收，然後要求你下載「驗證程式」或是引導你到某一個「驗證網站」，要求你填寫帳號密碼與個人資料，其實都是詐騙集團的把戲。

如果電子郵件中夾帶的是可以執行的檔案，包括副檔名是exe、vbs、lnk、scr、bat、js，以及vb的檔案，就要懷疑它是否可能夾帶電腦病毒或木馬程式，務必要使用防毒軟體掃描過後再開啟。

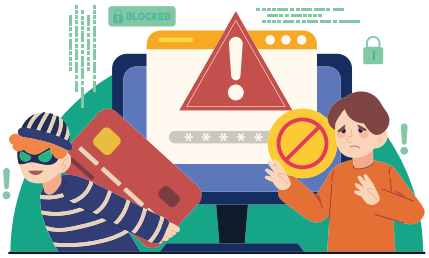
最後，如果你要把郵件轉寄給別人，請刪除無關人士的電子郵件信箱，以減少那些人的信箱外流之機會。

四、 即時通訊平臺安全使用

有別於電子郵件是陌生人之間的交流，即時通訊軟體幾乎都是親友間的聯絡，例如Line或Messenger，如果在即時通訊平臺上進行詐騙，取信程度和成功率都更高，所以即時通訊平臺上的主要風險在於被「盜帳號」上，歹徒會先想方設法加入你的好友圈，接著透過訊息拐騙你交出帳號，然後再使用你的帳號去詐騙你好友名單裡的人。

首先，歹徒會舉辦各種活動，甚至假冒名人與知名企業的名義，宣稱只要「加入好友」就可以抽獎、領贈品、獲得免費貼圖、或是查看特殊的內容，例如上映中的電影，如果你一時好奇或貪小便宜，將對方加為好友，就等於讓歹徒進入了好友圈，獲得了對你發送私人訊息的許可。

由於也確實會有名人或知名企業真的以「加好友送優惠」的方式累積會員，因此真假難辨，遇到這種情況的時候，請上該名人或企業的官方網站或客服專線查詢是否真的有舉辦這些活動。



進入你的好友圈以後，歹徒會把通訊軟體上顯示的名稱修改為其他人名，然後向你攀談。
由於即時通訊軟體在使用者遺忘登入密碼的時候，經常會使用手機驗證碼的方式確認身分，所以歹徒會藉口自己的手機遺失或損壞，請你幫忙接收驗證碼，如果你一時不察，把你的手機號碼和手機簡訊中收到的驗證碼數字告訴對方，你的帳號就這麼被盜走了。盜走了你的帳號以後，歹徒就可以使用你的帳號、假冒你的名義，向你好友名單中的其他人，故技重施再盜取其帳號，或是直接詐騙錢財。

所以當你在即時通訊軟體上收到任何向你詢問手機號碼或驗證碼的訊息，一定要提高警覺，就算是來自你熟識的親友也一樣，可能是他的帳號已經早一步被盜用了。收到這類訊息的時候，請以其他的方式向當事人查證，例如直接撥打電話而不是使用同樣的通訊軟體回訊。同樣地，如果收到訊息要求你提供信用卡資料或是代買儲值點數的話，也請先以其他方式向當事人查證。

五、社群平臺安全使用

現代人在社群平臺上記錄生活的點點滴滴並秀出自我，但是如果沒有妥善做好隱私方面的設定，這些公布在社群平臺上的資訊與內容，可能會成為跟蹤騷擾或網路霸凌的禍端。

人與人之間難免會有爭吵，就算再怎麼善意待人，網路上仍會有些單純想要造成別人困擾的酸民，或是心懷不軌的詐騙歹徒，此時你公布在社群平臺上的個人資訊，就是讓他們找到你、騷擾你，甚至騷擾你的家人的線索。

在社群平臺上的每一則貼文、照片、影片都可以設定分享的對象，只有你指定範圍內的分享對象才可以看到這些內容，大部分社群平臺的預設值都是「對所有人公開」，而大部分人也都不假思索就使用了預設值，於是就成了不肖之徒的騷擾或詐騙對象。

所以在社群平臺上發布任何一則內容時，請務必考量該則內容包含多少個人隱私資料。基本上包含個人姓名、長相、就讀學校、公共或居住地點的貼文，都不應該設為「公開」，應該設為「限好友」才可閱讀。如果你本身想要在社群上當個網紅，所以想要公開你的樣貌身材，那麼至少不要使用真實姓名，也不要暴露你的工作或居住地點資訊，例如在該地點拍照打卡，那麼至少有人想騷擾你的話，不會那麼容易找到你。

除此之外，當你發現在網路上發生爭吵或霸凌的時候，千萬不要參與霸凌別人的那一方，包括按讚或分享都不可以，以免自己也變成被報復或肉搜的目標。

謹守這些原則，讓你在大方秀自己的同時，也能保護自己的人身安全。

六、 動動腦時間

詩詩的信箱裡收到了一封這樣的郵件，告知她的G-mail信箱多次遭人試圖登入，請她立刻安裝指定的防護軟體，詩詩很驚慌，你會建議她怎麼做呢？

提示

直接忽略這樣的信件好嗎？直接安裝指定的軟體好嗎？

要怎麼查證這封信是否由Google發出的呢？

寄件人no-reply.accounts.google@wpereview.org真的是來自Google公司的網域google.com嗎？

七、 牛刀小試

問題一：

下列哪一種是網路上常見的釣魚詐騙？

A. 恭喜你是本站第999999位訪客，可獲得iPhone一支，請填寫資料。
B. 您的帳號發現安全性問題，即將被停權，請在此輸入帳號密碼進行處理。
C. 親友訊息：我的手機遺失了，用你的號碼幫我收一下驗證碼。
D.以上皆是。

問題二：

下列何種行為，有助於保護自己的帳號不被盜用？

A. 使用十幾個符號以上長密碼，並以數字、符號、大小寫英文字母等搭配。
B. 在多個網站使用都相同的帳號與密碼，以免忘記而無法登入。
C. 和家人共用帳號與密碼，以便互相救援。
D. 以上皆有助益。

你答對了嗎？

第一題的答案是 D
網站釣魚會偽裝成任何網站的頁面，通知受害人得獎了或是帳號有問題，此外，根據先前竊得的個資偽裝成親友，要求以受害人的手機代為接收通訊軟體的帳號驗證碼並告知，可奪取該通訊軟體帳號的使用權。

第二題的答案是 A
增加密碼的長度和符號種類都有助於提高密碼強度，其中加長密碼比增加符號種類更有效。在多個網站之間或與多人共用帳號密碼，非但沒有救援效果，還更容易被盜用，這些網站之中只要一個因為資安防護層級低而被入侵，就相當於你所有網站的帳號都會遭到盜用了。

八、 網路平臺安全使用六大撇步

1. 非必要不外流自己的電子郵件信箱地址（E-mail Address)。
2. 收到郵件先認明寄件人，不點開郵件內的不明連結與附件檔案。
3. 即時通訊軟體上不加來路不明的陌生帳號為好友。
4. 即時通訊軟體上收到關於詢問敏感資料、手機驗證碼、購買點數或匯款的請求，先以別的方式向當事人查證。
5. 妥善設定社群網站上每一則貼文的分享對象範圍，勿外流隱私予陌生人。
6. 不參與網路霸凌，以免成為報復或肉搜的對象。

參考資料

趨勢科技TrendMicro（2022，9月16日)。**「有人已取得您的帳戶密碼，請登入gmail重設密碼」收到Google重大安全警報是詐騙嗎？三步驟自我保護**。資安趨勢部落格。https://blog.trendmicro.com.tw/?p=74050