臺東林區管理處政風室
111年 10月號

公務機密
資訊安全維護

網路詐騙層出不窮，切勿輕信，如有任何疑問，可撥打165反詐騙諮詢專線即時查證。

牢記三不&三要原則

(一)不聽信電話通知，要保持冷靜。

(二)不告知個人資料，要立即查證。

(三)不依據所留電話查證，要報警處理。

資安時事案例

詐騙手法新招 釣魚簡訊騙取「認證碼」

避免駭客入侵 資安專家傳授三撇步

個人資料保護法

什麼是個人資料的國際傳輸？

生活中的資安

你的 Gmail 也被入侵了嗎？分辨釣魚信件的 5 大技巧！

數位學習

107年資安動畫金像獎 行動支付駭起來
https://www.youtube.com/watch?v=eWqiwAXTNVw

詐騙手法新招 釣魚簡訊騙取「認證碼」

周刊王CTWANT |中國時報陳鴻偉、胡欣男 2022年9月12日

[周刊王CTWANT] 詐騙手法繼續推陳出新，用1支手機搞定一切的「悠遊付」，也被不法集團盯上，陸續傳出多起捷運族遭騙。歹徒用釣魚簡訊或話術騙取民眾「認證碼」，再將錢包金額提領一空，北市7月起陸續發生8起案件。刑事局指出，近期民眾悠遊付或街口支付遭詐，起源多是從iPhone的iMessage收到釣魚簡訊，建議開啟「過濾未知的寄件人」功能，或直接關閉此功能。

悠遊卡電子支付的「悠遊付」，功能包括儲值提領、掃碼轉帳付款和繳費，此外還能「嗶」乘車，也能購買1280定期票，透過智慧手機下載悠遊付App，完全取代悠遊卡。

然而，近幾個月來，詐團透過iMessage亂槍打鳥的假投資、偽造衛福部防疫紓困補貼網址的詐騙釣魚簡訊氾濫。刑事局表，歹徒取得認證碼後，除網路銀行遭盜轉款項占2成，個資也遭綁定電子支付詐財情形占8成，其中以悠遊付、街口等2家為主。

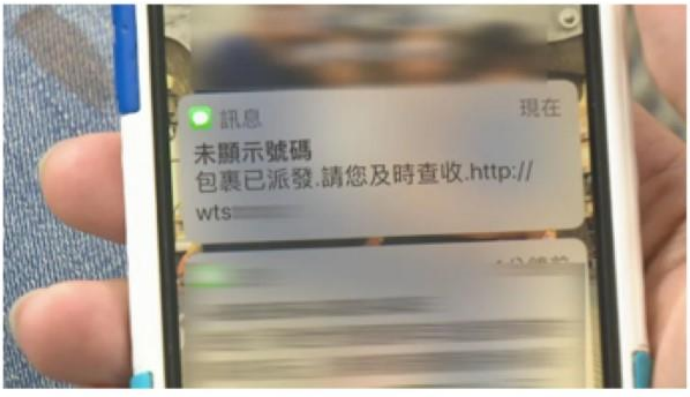
除釣魚簡訊，北市1名粉領族則是用悠遊付消費後，接到自稱網購業者來電，表示系統出錯，造成重複訂購，藉此騙取認證碼，將悠遊付裡的5000多元領光。

另一名6旬婦人，則是接到「勞保局」來電，誆稱要辦理健保退費，從中騙到婦人雙證件個資，接著再偷偷拿去申辦悠遊付，從中詐走1萬多元。

避免駭客入侵 資安專家傳授三撇步

民視新聞網
網路駭客手法，推陳出新，不外乎透過各種方式，要你點選網址，藉此「導入」看起來像是真的「假網站」，詐騙個資，資安專家就建議，手機軟體除了不定時更新，不要破解自己的手機，更重要的是，不要點選不明網址，導入網銀系統，而是要回到原本銀行的網銀系統登錄，避免詐騙。

看到一封陌生簡訊，強調包裹已派發，要你及時查收，一貫的詐騙伎倆，小心對方透過假網站，要騙取你的個資。



現在銀行大都有設有網路銀行的服務，除了提供電腦版，也有手機版APP可以下載，這回網路駭客，疑似先入侵銀行網銀系統後，寄發給不特定用戶查收包裹簡訊，裏頭附上網址，而這個詐騙的IP位址，通常設在國外，引導進入假的銀行網銀系統，看起來就跟真的沒兩樣，只要你輸入帳號密碼，駭客就成功把你帳密騙到手。
台科大資安中心主任查士朝表示，「他其實是沒辦法利用其他程式去做一些事情，我們不要隨便相信簡訊裡面提供進來的網址，可能它看起來像網銀，但是實際上可能是所謂釣魚的網頁。」

一般來說，手機分成Android以及iOS系統，Android允許不明程式安裝，如果要防止駭客入侵，務必進行關閉，至於iOS則有主動防禦機制，但如果隨意進行手機破解，恐怕就會出現資安漏洞。
查士朝更說，「手機如果有一些版本更新的時候要記得去做更新，第三個來講就是說，如果你點擊一個連結或點擊一個簡訊，它要你輸入什麼帳號密碼等等，都不要相信這樣事情。」

專家提醒，要進入網路銀行，還是循正常管道，進到原始的網銀系統，避免透過點選不明網址方式「導入」登錄，多一分警覺，才能少一分被詐騙的風險。

（民視新聞／綜合報導）

什麼是個人資料的國際傳輸？

依本法第2 條第6 款規定，國際傳輸係指將個人資料作跨國（境）之處理或利用。

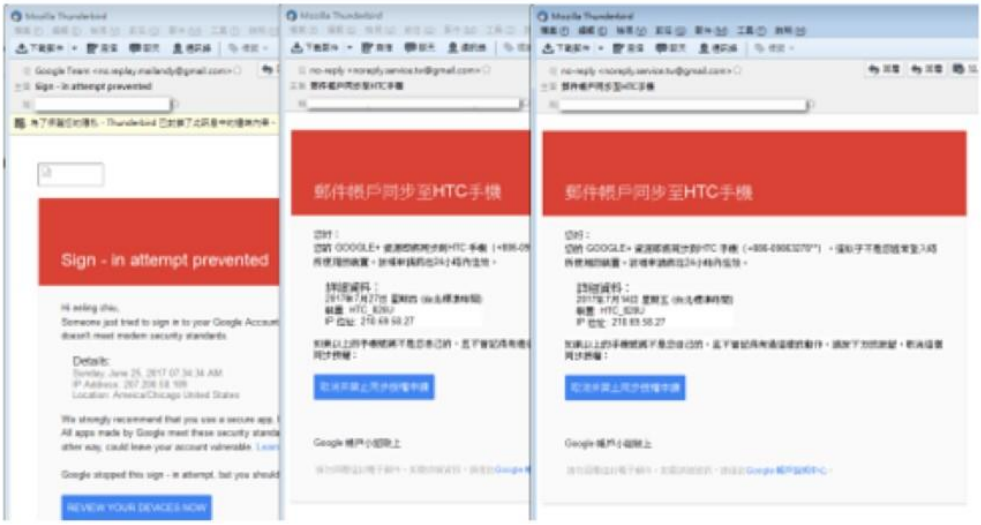
例如：

(1) 總公司將資料傳送給國外（境外）分公司或國外其他公司、機關（構）等。

(2) 公務機關將資料傳送給國外（境外）辦事處或國外其他公務機關（構）、公司等。

【節錄自法務部102年8月編印之－個人資料保護法規及參考資料彙編】

你的 Gmail 也被入侵了嗎？分辨釣魚信件的 5 大技巧！



文／林雨蒼　民間司改基金會執行祕書

近日，臺灣 NGOs 持續關切中國諾貝爾和平獎得主劉曉波於服刑期間逝世的議題，並聲援遭中國拘禁的我國非政府組織工作者李明哲。在人權團體鍥而不捨大力奔走的努力下，聲援行動受到聯合國與歐盟的支持與關注。然而，除了獲得國際間的關注之外，這些 NGOs 成員似乎也受到另類的「關注」。

許多 NGOs 工作者最近收到了貌似來自 Google 的安全通知信件，聲稱其帳號受到多次嘗試登入，並且帳戶已因此遭到鎖定。除此之外，信件內容更要求收件者點選連結以重新登入帳戶，或進行安全設定檢查來確保帳戶的安全性。收到此信件的許多工作者因而感到非常擔心，懷疑是否自己設定的 Gmail 二階段驗證登入機制失效，或帳戶已受到駭客掌控。

然而，將此信件轉交專業資安研究人員鑑定後，研究人員判定這些疑似來自 Google 的安全通知信件，事實上是來自駭客的釣魚信件。

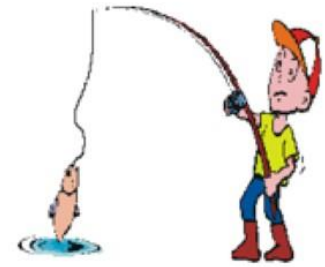
看似安全通知信，原來是釣魚信

此釣魚信件的目的是利用當事人恐慌的心理狀態，誘騙當事人點選信件中的連結以騙取其電子郵件的帳號密碼。一旦收件者受騙上當並輸入帳號密碼後，駭客極有可能會利用這組帳號密碼嘗試入侵其他相關系統，達成進一步的入侵。

在資安研究的領域中，這種透過當事人各種心理狀態進行誘騙，達到攻擊目的的攻擊方式被稱為「社交工程」。使用社交工程的攻擊方式不僅能大幅提高攻擊的成功率，更能降低攻擊者的攻擊成本。因此，這是一種在網路攻擊行動中被廣泛使用的攻擊手法。

身為一般電子郵件使用者的我們，該如何自行判斷這封信件是否正常呢？首先，不只生活中充斥著各種詐騙，電子世界中也是。因此，不論收到任何主題與內容的電子郵件，收件者都務必保持冷靜，並仔細觀察信件內容，以找出任何可疑的蛛絲馬跡。

判斷釣魚信件的 5 個技巧



以此封釣魚信件為例，我們可以透過以下方式來進行判斷：

1. 標題

此封信件的標題為「登入告警：嘗試登入達到認證上限」，其中「登入告警」很明顯為中國用語，在繁體中文的環境下，正常應會被寫作「登入警告」，而不會使用「告警」。

2. 寄件者

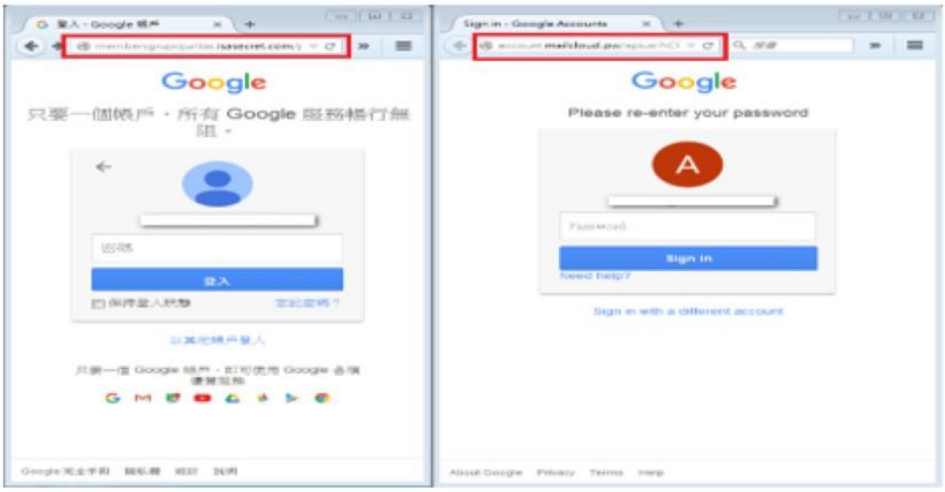
為避免冒用，Google 不會使用 gmail.com 結尾的電子信箱來寄送任何 Google 系統信件，因為 gmail.com 任何人都能註冊，這封信的結尾卻使用了 gmail.com。Google官方的 email 結尾應該是 google.com（內部員工才能拿到的 email位址）。

3. 信件內容

信件內有附圖片，將滑鼠滑過去，左下角會出現圖片網址，將網址放到 WHOIS 上驗證，卻發現網址的持有者不是 Google（亦即放圖片的 server 不是 Google 的 server）。Google 系統通知信內，所附的圖片不使用 Google 旗下的伺服器或網站，這就是一個非常可疑的疑點。

4. 連結或者附件內容

雖然頁面長得跟 Google 登入畫面一模一樣，但要求帳戶安全檢查頁面的連結網址，其持有人卻不是 Google。如下圖紅框處，要求重設密碼的頁面，其網址本應顯示有 google.com 的字樣才對。



5. 交叉確認

Google 帳戶的安全警告除了利用 Email 通知，Google 通常會另行顯示在帳戶內的其他地方，例如會顯示在我的帳戶 → 裝置活動與通知 → 近期安全事件。使用者可以利用這個功能確認 Email 所描述的安全事件是否真的存在。

綜合以上描述，我們可以合理懷疑這封信大有問題。裡面的連結恐怕是惡意連結，非常可能是釣魚信件。
提升 Gmail 帳號安全性，從日常做起

其實，除了在收到信件時可以利用以上方法來進行確認，建議使用者平時也需對帳戶安全性多加注意，利用以下方法來加強安全防護──
1. 打開 Google 2 階段驗證

設定帳戶 2 階段驗證完成，使用者輸入登入帳戶密碼之後，系統會透過簡訊或其他方式寄送驗證碼到使用者的行動裝置上，或是透過 App 自動產生驗證碼，使用者需要再次輸入收到的驗證碼才能完成登入。此驗證方法的目的在於利用使用者的行動裝置再次確認登入者的身分，多一個確認步驟，即可增加駭客入侵的難度。
2. 從 Google 的研究功能中打開 Gmail 的驗證功能

啟用 Gmail 驗證功能後，Gmail 會在寄件者的地址旁邊提示使用者是否通過身分認證。因此開啟此功能後，真正的 Google 系統郵件旁邊會額外顯示鑰匙圖示。

最後，假設我們真的收到了釣魚信件時該怎麼辦呢？如同案發現場，在發現攻擊事件時最重要的是先保留證據，無論是使用瀏覽器登入使用 Gmail，或是使用 Outlook 等軟體收發郵件，都要記得透過擷取畫面的方式保留當下所看見的信件畫面。除此之外，保留原始信件也非常重要，在 Gmail 上，可以在信件右方點選「顯示原始郵件」來下載原始郵件。

在保留信件畫面與原始內容後，可以將這些資料交由資安研究人員進行分析，以利進行進一步的追查。

如果信箱真的遭到入侵，可能會被做什麼事？

首先，攻擊者可能會先設定「篩選器」功能，設定將郵件轉寄至攻擊者可以控制的信箱，進一步分析這個帳戶的來往郵件與撰寫習慣；接下來，攻擊者可能會透過信箱發送特定的釣魚信，謊稱是當事人並特別攻擊某位認識的朋友，看是不是可以取得更多資料，或是誘騙被入侵者點擊連結，進而取得被入侵者電腦的控制權，存取更多機密資料。

很多人會說：「我的信箱或電腦中又沒有什麼資料，我不擔心會被入侵」。

但事實上，對方要的可能不是你信箱中的郵件，而是透過你的信箱、電腦，偽裝成你（被入侵者）以接觸到你周圍的朋友或同事，進而從他們身上竊取資料；或是控制電腦後，以該電腦發起攻擊，如此一來警方追查時可能就只會追到被入侵者，而無法揪出真正在背後發動攻擊的攻擊者。

因此，不要以為自己沒有什麼重要的資訊就不會被入侵，你可能會變成有意人士攻擊別人的節點。

資訊安全不是只有換換密碼而已，有機會可以多多參與資安相關的研討會，了解最新的攻擊技術與防禦技巧，在現實生活中也要多方查證，才不會不小心讓自己成為攻擊他人的節點。