公務機密

資訊安全維護

簡訊通常都會夾帶不明連結，當使用者點入之後，就會導致手機中毒、遭植入木馬，除了個資洩露外，還可能成為散播詐騙簡訊的工具。Whoscall也公布釣魚網址前三名，分別是「OOO.duckdns.org」、「OOO.xyz」、「OOO.club」。

資安時事案例

假冒國泰世華釣魚簡訊 3天21人被騙300萬

軟體更新邀請竟是釣魚郵件？小心駭客這樣偷走你個資

個人資料保護法

個資法Q&A

生活中的資安

通訊軟體用在公務上好不好

數位學習

100年資安動畫金像獎
資安小紅帽

假冒國泰世華釣魚簡訊 3天21人被騙300萬

TVBS 李采穎 陳弘毅 2021年1月30日 週六 下午10:27

小心，這是詐騙簡訊！最近不少民眾收到署名國泰世華的簡訊，其實是詐騙集團發出的釣魚簡訊，點入連結網址，輸入了個資，可能被盜用，短短三天21人被騙，詐騙金額300萬。

記者李采穎：「你有收過這樣的簡訊嗎？假冒國泰銀行的釣魚網站，只要你點進去，輸入帳號密碼，就有可能會變盜用，成為人頭帳戶。」

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。

軟體業界資料工程師Gavin：「注意看它的網域的名字，假的網站中間有一槓，有一條這個，因為它做得很像，那真的網站是沒有的。」

專業人士說，通常這一類釣魚網站，嫌犯會先在國外網頁，購買和正版網址名字相似的網域，一年大約是15元美金，但是一般人收到這樣的簡訊，該如何避免受騙呢？

軟體業界資料工程師Gavin：「你可以去google，比如說你google國泰世華，這樣子真的國泰世華的網銀會排在最上面，通常會是在廣告的下面，它就會是真的那個網站，因為假的網站它沒辦法，比較難做到把它的(網路)排名往前拉。」

不太會使用網路的長輩則打電話給客服做確認，或是專業一點，可以直接對比網域是否有一致。

最近也有網友在臉書po文，詢問是否是FB詐騙簡訊。

軟體業界資料工程師Gavin：「一個就是兩階段驗證，很多情況會收到兩階段驗證，第一個就是你用陌生裝置登入的時候，情況有兩種，第一種就是你換手機、電腦，第二種就是你的帳號被人家嘗試登入。」

專家建議，不管是收到哪種類型簡訊，其實還是搜尋官方網頁或是聯繫客服，是最安全最保障的方式。

軟體更新邀請竟是釣魚郵件？
小心駭客這樣偷走你個資

匯流新聞網記者王佐銘／綜合報導 2021年2月14日
勒索軟體無孔不入！駭客攻擊愈發頻繁，網路安全公司日前發現，Windows 10系統月發布更新版本後，遭惡意人士盜用，發送假冒微軟名義的「更新版本邀請函」，郵件中藏有惡意勒索的病毒程式，一但勘起假冒的復健檔案，就會遭鎖定加密，需支付贖金才能解鎖。

Trustwave分析，這種網路釣魚信件主旨是「立即執行安裝最新版本的微軟Microsoft Windows Update」，郵件內夾帶會使電腦設備感染Cyborg勒索軟體的執行檔，一旦收件人打開檔案後，就會自動下載一個名為bitcoingenerator.exe的檔案，將用戶電腦中所有文件加密鎖定，並要求用戶支付價值500美元(約新台幣1.5萬元)的比特幣贖金。

Trustwave進一步透露，數據庫中已發現三個被植入Cyborg開發程式碼的惡意勒索軟體，意味這支病毒不僅會透過釣魚郵件形式散播，還連帶將Cyborg開發程式碼散播出去，若遭有心人利用，將可能迅速擴大勒索軟體感染範圍與變種版本。

據了解，這類檔案大小大約是28KB，並且假冒.jpg格事當作附檔名稱，騙過郵件安全防護，Trustwave表示，所幸目前並未有大規模攻擊的跡象，Windows 10用戶在安裝更新系統時，千萬不要打開此類假冒微軟名義的病毒郵件，建議使用系統內建工具下載更新最安全。

新聞照來源： unsplash

個資法Q&A

- 網路暱稱或Email屬於個資法規範的個人資料嗎？
- 由於網路暱稱不易識別出其代表的個人，所以原則上不會受到個資法規範(但若達到得以直接或間接方式識別該個人的程度，則將受個資法規範)。至於Email則有可能識別出個人，法務部會請主管機關NCC提供認定標準。

資料來源:清流雙月刊／蔡鎮戎

現在的人，幾乎沒有人生活中可以離開電腦、手機，而 Google瀏覽器及其相關附屬軟體則是必須裝備；我們使用的通訊軟體也多需要 Google 的支援才能使用，而其曝露出來的隱私問題，政府應該以嚴謹的態度視之，以避免國家相關資料被竊取。

數年前，早在社交通訊網站剛盛行時，銓敘部就發文各機關學校，禁止公務員利用公務電腦連結臉書（Facebook）、噗浪（Plurk）、推特（Twitter）、Tumblr、Flickr等社交通訊網站，擔心該等網站存在「不可預期的風險」：例如散播病毒以癱瘓政府機關網站的正常運作，或藉以竊取、竄改政府機關的重要文件。這與當前政府雷厲風行推動的嚴打假訊息、假新聞，似乎有著不謀而合的相同目標，目的都是在維護國家的資訊安全、穩定國家安全的正常運作。然而，在大勢所趨下，我政府也不得不承認，雖然這些社交通訊網站有著「不可預期的風險」，但是在越來越多民眾倚賴從這些社交通訊網站來獲得資訊，政府為了符合時代潮流、接地氣、讓民眾獲得正確的訊息，也不得不有條件開放使用；而當大門一開，各機關學校即蜂擁而上，紛紛成立自己的社交通訊網站、提供資訊予民眾或民眾在互動平臺上提供基資，這讓資訊安全在此際更顯得格外重要！

為了順應時代潮流，讓民眾獲得正確訊息，公家單位紛紛成立官方社交通訊網站及帳號，即時提供資訊並透過平臺與民眾互動。圖為臺北市政府臉書粉絲專頁與LINE官方帳號。（圖片來源：臺北市政府，https://www.facebook.com/humansoftaipei；https://line.me/R/ti/p/%40taipei）

Line可以說是近年來在臺灣最受歡迎的社交通訊軟體，用戶高達2,100萬戶，Line所具備的功能也持續在增加中。各機關學校也都組成各式各樣的工作群組，以方便工作上的即時聯絡。然而，其負面效應正一一呈現出來，最值得注意的有兩方面：一、雖然它提供了工作上即時互通的便利性，但是它缺乏加密保護的功能，所以各機關學校在工作上的資料隨時可能外洩，目前政府的資安工作在這方面並無法防範，輕者僅為公事上的交流瑣事，重者一旦夾帶機密檔案，難保不會被有心人士藉機取走，對國安將是一大警訊；二、由於Line的便利性及免費性，許多主管便不自覺地把它用來作為交付工作的工具，而且是無時無刻、不分平假日、想到什麼就Line一下，造成部屬極大的困擾與壓力、影響到員工的身心健康。2016年，美國總統大選前夕爆發「希拉蕊電子郵件事件」，美國對於資訊安全的防護工作，一直以來是極盡所能、做到滴水不漏，尚且出現如此重大外洩事件，可見只要是駭客有興趣的內容，不管什麼樣的電子通訊資料都有可能被駭。網路巨擘Google於2019年7月11日坦承，其承包商可以定期聽取和檢 查「Google語言助理」(「Google

Assistant」，即「OK Google」功能）的使用者與該系統所講內容的錄音。該公司表示，此舉主要是在協助「Google語言助理」可以更多瞭解不同國家的語言、口音，以開發「Google語言助理」更多功能。無獨有偶的是，2019年4月，亞馬遜（Amazon）也被爆出將民眾隱私外洩問題：Amazon內部的Alexa團隊工作人員每天每人需收聽上千個語音片段。Amazon發言人表示，此舉目的亦為了提升Alexa的語音辨識能力。此2個事件，足以證明人們在使用手機進行對話時，其內容均能被有心的手機開發商竊取及運用。綜上所述，隨著越來越多、也越便捷的通訊軟體出現，我政府機關在資安工作上尚未能做到有效防範之前，宜謹慎並有限制範圍性地使用，才能避免國家重要資訊不會輕易外洩、也才能夠確保國家的安全。同時也要教育各機關學校人員（特別是主管），應避免在非上班時間發布工作訊息、造成部屬的心理壓力，如此，才能算是將社交通訊軟體物盡其用、公務機密維護妥當。