公務機密維護-

教你分辨釣魚網址分身術！

作者：高銘鍾

網路釣魚(Phishing)，多半利用 E-Mail、即時通訊軟體、社群網站等做為前奏，誘使收件者連往擬真的詐騙網站，再由詐騙網站入侵受害者的瀏覽器，或利用受害人一時不察登入詐騙網站，竊取受害人的機密資料。一般的資安宣導，都會建議大家不要連往可疑的網址，以便遭到詐騙網站的攻擊。但是，可疑的網址到底是如何可疑？為何可疑？如何防範，這卻是多數人不清楚的部份。接下來的文章我們就來談談這些可疑網址的一些特色及防範之道。

顯示位址與連往位址相異

網路釣魚多半會利用電子郵件做為攻擊的前奏，E-Mail 的內容通常會仿得極真，

早期遭到仿造的網站多半是一些金融或線上付費機制相關機構；近期則因為社群網站流行，故仿造的對象開始轉向各種社群網站的通知、確認信。只是，仍然換湯不換藥，在這些釣魚郵件中，經常會看到顯示位址與連往位址不一樣的情形，信中出現這樣的情況，幾乎百分之百可確定這是封釣魚郵件。

因此也建議各位保持一個良好的習慣，勿直接點選 E-Mail 上的超連結，而是將滑鼠游標移至該超連結位置上，檢視一下顯示位址與連往位址是否一樣，若不相同千萬別點擊，小小動作就可以避免您成為上鉤的魚兒。

圖 1、順手將滑鼠游標移至該超連結位置上，假造的 facebook 通知信，其中帶有顯示位址與連往位址不一樣的情形。

網址混淆技術

許多釣魚網站會在網址上加工，讓人難以分辨到底網址是否可信，例如：http://mail-google.com、http://www.goog1e.com，其實這些網址與 Google 並沒有關係，但這種以假亂真的網域名稱混淆，很容易讓人因為匆匆一瞥而錯信這是真實的網站。

另一種常見的做法，是將真正的網域名稱前面加上容易讓人信任的域名，例如：http://mail.google.com.xyznothisdomain.com，一般的申請自訂的網域名稱是在頂級域名(TLDs, Top-level domains, first-level domains)中的二級域名。頂級域名包括了國家代碼(.tw、.cn、.jp 等)、通用頂級域名(.com、.edu、.gov 等)，二級域名就是最靠近頂级域名左側的字段，擁有二級域名控制權限者，可以自訂更多的三級、四級域名，以前述的 http://mail.google.com.xyznothisdomain.com 例子來看，其實這個網址與 Google 並沒有關係，而是 xyznothisdomain 這個二級域名的擁有者自行製造出來的假象，透過這個網址所連往的地方是由這個二級域名的擁有者所指定的。

這類型的攻擊手法，防範之道是可以透過安裝防毒軟體、瀏覽器自身的保護功能，或裝設閘道端上網管理軟體，協助防止使用者瀏覽不當的網址。在使用習慣上，可將一些常用、重要的網址設置於「我的最愛」，當需要使用該網站功能時，一律由「我的最愛」連結；若是透過搜尋引擎尋找資料，也需留意搜尋引擎對搜尋結果的警告，對於可能會損害您電腦的網址，盡量不要瀏覽。

圖 2、Google Chrome 瀏覽器自身的防釣魚網址功能。Google Chrome 瀏覽器瀏覽危險的網址，即會出現畫面中的警告。

原文網址: 教你分辨釣魚網址分身術！,Information Security 資安人科技網
http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=6813#ixzz48y8aMja5

法務部廉政署　檢舉電話：0800-286-586
檢舉傳真電話：02-25621156
電子郵件信箱：gechief-p@mail.moj.gov.tw
新竹區監理所政風室　檢舉電話：03-5891935
檢舉傳真電話：03-5889820
電子郵件信箱：schtru07@ms33.hinet.net

新竹區監理所政風室
關心您

HMV
新竹區監理所
Hsinchu Motor Vehicles Office