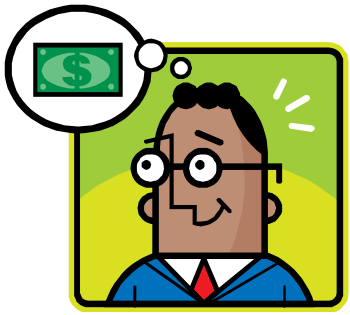
什麼是釣魚網站



§ 前言
網路釣魚擅偽裝，真假難分要提防

現代人的生活與網路密不可分，連帶提昇了個人資料在網路上的多元價值。相對的，利用個人資料進行網路犯罪的情況也日益猖獗，「網路釣魚」(phishing)即為透過網路來騙取個人資料的方式之一。網路釣魚通常會透過電子郵件假冒知名銀行、信用卡公司或其他聲譽良好的商家，從信件中引導連結至真偽難分的網頁（多為金融、付款等活動），博取使用者信任，誘使其提供個人資料，像是帳號、密碼、財務資訊等，最終目的就是竊盜身分取財。

本手冊先剖析網路釣魚的常見手法，再進一步舉列多項判斷網路釣魚的防範撇步，提供大家於使用網路時可加強警惕及更懂得保護自己，最後則介紹目前國內專門受理網路釣魚案件的通報機構，當使用者遇到網路釣魚時可以直接向該單位檢舉通報。

手冊內容

1. 網路釣魚的常見手法

網路釣魚主要是利用人類信任或好奇的心理，以誘導受害者掉入詐騙圈套。以下舉列 3 種常見的手法：

手法 1. 使用與官網相似的網址與頁面

網路釣客常仿冒知名公司網站，架設以假亂真的山寨網頁或使用變形的網址(例如 www.yahoo.com.tw 可能變成 www.yhaoo.com.tw)，再用電子郵件或即時通訊軟體發送主旨為緊急通知的 email，要求使用者按下 E-mail 中的連結，來更改帳戶、密碼或信用卡密碼等資料。一旦使用者按下此連結轉至假網站的同時，很可能會自動下載惡意軟體，且開始記錄您的登入帳戶資訊並立即回傳給釣客利用來獲取不當利益。

手法 2.網路抽獎廣告連結

您是否曾收到過促銷的 DM，或者點選過網路上精美且吸引人的廣告訊息?許多網路上看似合法的活動，一旦您點選後可能嫁接至另外需要輸入個人資料的頁面，這時千萬要三思而後行。詐騙集團或行銷公司就是看中網路使用者喜歡撿好康的人性弱點，一旦您上當洩漏個人重要資訊，接踵而來的可能就是莫名的電話要求支付相關費用，或是每個月的手機帳單突然多出了高額的簡訊傳送費用，那就得不償失囉！

網路釣魚的目的就是為了「錢財」而來！使用者進行每項網路行為皆需謹慎三思所接收及提交資訊的正確性與安全性！

手法 3.裝熟套交情的訊息

利用即時通或社群平台(例如 Msn 或 Facebook 等網路媒介)向受害者傳遞「問候」和「請求幫忙」的詐騙訊息亦層出不窮。歹徒通常會將蒐集到的帳號被盜者個資背景進行瞭解研究，甚至模擬其生活模式和打字語氣。而偽裝身分傳訊給親友的交談過程毫無異樣，等到受害者卸下心防，在無戒心的情況下一步步掉入陷阱。大家除了需謹慎保護自身帳號安全，對來自網路上各方親友突然的請求訊息也請務必先行冷靜確認。

2. 網路釣魚的防範撇步

通常釣魚電子郵件中所提供的超連結，其網址會與你實際所前往的網站不同。乍看下為知名公司網址，但其中的字母可能經過增減或更換，例如：www.google.com 可能變成 www.gooogle.com，受騙的民眾輕則帳號被盜用，重則因個人金融資料外洩而損失慘重。以下針對網路釣魚提供相關的基本防範措施：

（1）對於詢問您個人資料的信件提高警覺

當收到詢問相關敏感資訊（例如：使用者名稱、帳號、密碼等）的信件要提高警覺，尤其含對外超連結的內容。通常一般大型企業、銀行，都不會透過 e-mail 的方式詢問使用者個人資訊。

（2）不要隨意點選信件中的網址連結及開啟附件

建議可將經常使用的網站加入「我的最愛」書籤，直接透過書籤連結至正確網站，或可開啟新的瀏覽器視窗手動輸入網址，除可避免誤連詐騙歹徒設立的假網頁，亦可經由正確網站查看相關訊息是否為真，或撥打官方服務電話或郵件地址確認。

（3）勿貪小便宜點選好康連結

天下沒有白吃的午餐，對於「免費優惠」、「好康大放送」 .....等吸引人的好康廣告文案，常會引導使用者輸入敏感資料來換取優惠或利益，請務必留意此網站的真實性，並詳知所同意留下的資料之用途及造成的影響。

網路上總是有許多含有誘人好康的廣告網頁，但在參加活動前務必確認網站的真實性和留下資料的實際用途與可能造成的影響！

（4）定期檢查交易紀錄與網站帳號

對於重要的個人交易網站，應經常檢查帳號和瀏覽交易紀錄，如收到信用卡和銀行帳戶的交易紀錄時，請確認是否有任何未經授權的收費。

（5）透過加密的網頁功能傳送個人資料

若網頁要求輸入任何敏感性資料，注意網址是否為 https（資訊加密協定）開頭、在瀏覽器頁面是否出現黃色鎖頭圖示、或 SSL 安全性警示視窗（請注意，各家網頁瀏覽器顯示的方式及位置可能會有不同），此方法並非萬無一失，但可強化訊息在傳輸過程中的安全性。

（6）使用安全有效的防護產品

確保個人電腦維持在安全的狀態，除自身需具備充足的資訊安全觀念，亦建議安裝防護軟體並隨時更新，更加提昇安全性。

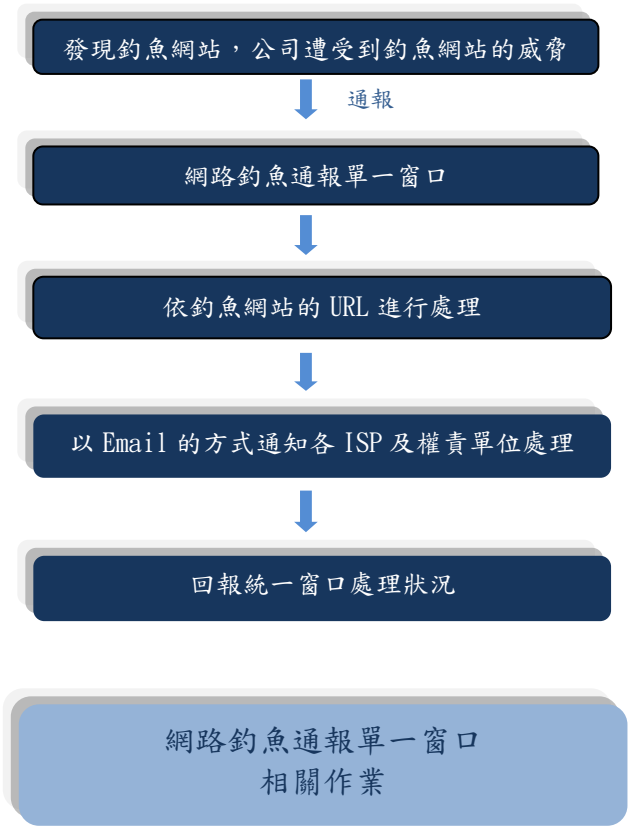
（7）主動回報釣魚網站資訊

一旦發現自己遭遇網路釣魚時，為防止受害範圍擴大，建議大家可將案例通報至專責單位進行記錄及後續處理追蹤。相關作法請詳見下一節「網路釣魚通報窗口」。

3. 網路釣魚通報窗口

由 TWCERT/CC（台灣電腦網路危機處理暨協調中心）成立的「網路釣魚通報單一窗口」http://www.apnow.tw/，負責處理網路釣魚的相關通報（不受理惡意程式或其他網路攻擊事件），藉由此平台可協助企業與 ISP 業者進行聯防，以自動化方式加快釣魚網站交由 ISP 業者與權責單位追蹤處理的流程，以降低釣魚網站造成的危害與損失。

若發現可疑的網站或親身遭遇網路釣魚時，可向「網路釣魚通報單一窗口」http://www.apnow.tw/ 檢舉立案，讓相關單位可儘速追蹤處理，降低網路釣魚對個人或企業造成的資安危害與金錢損失！



網路釣魚事件通報流程圖（圖像出處：http://www.apnow.tw/）

使用者進入通報平台後，可以在首頁中依據符合之案件類型（如發現網路釣魚網站、收到網路釣魚信件、網站被植入釣魚網頁等）進行通報，透過簡單的頁面，方便民眾檢舉，同時亦可直接將此資訊立即轉知其他相關機構，提早揭露與預防各式網路犯罪手法！

社群網站日益盛行，網路釣客也會趁機入侵，使用辛辣或趣味的訊息內容（例如：影星名人的八卦）引誘使用者點入連結或執行外掛元件，個資即可能馬上洩漏，甚至成為釣魚陷阱的跳板；釣魚手法日新月異，身為網路使用者的你我，皆應共同為乾淨的網路環境盡一份心力！

出 版 者　教育部
發 行 者　蔣偉寧　教育部部長
召 集 人　吳國維　財團法人中華民國國家資訊基本建設產業發展協進會執行長
　　梁理旋　財團法人中華民國國家資訊基本建設產業發展協進會協理
指導委員　何榮桂　教育部電算中心主任
　　韓善民　教育部電算中心副主任
　　楊文星　教育部電算中心高級管理師
　　苗宗忻　教育部電算中心資訊管理組組長
　　劉玉珍　教育部電算中心資訊管理組程式設計師
審查委員　林杏子　國立高雄大學資訊管理學系教授
撰稿人員　吳夢潔　財團法人中華民國國家資訊基本建設產業發展協進會管理師
承辦單位　財團法人中華民國國家資訊基本建設產業發展協進會
出版日期　民國 101 年 07 月

※此手冊內容係對特定議題所提供之學習教材，僅供各界參考，非本部相關政策。