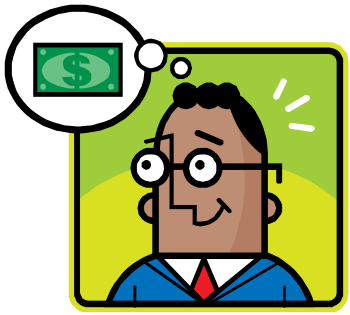
什麼是釣魚網站



§ 前言
網路釣魚真可怕，真假難分要小心

我們都很喜歡使用方便的網路，因此常常會在網路上輸入許多的個人資料，然而各種網路犯罪手法也越來越多元，「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公司或網路商家，在信件中放入真假難辨的網頁（如網路遊戲點數登入畫面），取得使用者的信任後，在假網頁中輸入個人重要資料，像是帳號、密碼、財務資訊等，最終目的就是盜用使用者身分取財。

本手冊先說明網路釣魚的常見手法，再進一步列舉多項判斷網路釣魚的防範方法，讓大家在使用網路時可以加強警惕並更懂得保護自己，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，以誘騙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（假網頁）

網路釣客常會仿冒知名公司網站，製作類似的假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連結，通知你需要登入網站與修改資料等訊息，一旦按下此連結連到該假網站的同時，你的電腦可能就會自動下載並安裝惡意軟體，且開始記錄你的登入資訊並回傳給釣客，用來獲取不當利益。

手法 2.網路抽獎廣告連結

網路上常有一些很炫的廣告頁面，會用「免費」或「限時限量」的字句吸引你（常以抽獎為名義，跳出視窗告訴網路使用者獲得大獎、送手機或遊戲點數卡，甚至是出國機票），假冒的網頁與真的網頁幾乎一模一樣，但當你點選進入後便要求你輸入個人資料，這時千萬要三思而後行。詐騙集團就是看中網路使用者喜歡撿好康的人性弱點，一旦你洩漏了個人的重要資訊，接著可能就會收到莫名的繳費帳單，那可就得不償失囉！

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

有時歹徒會利用即時通或 MSN、Facebook 向你傳遞「問候」並「請求幫忙」的詐騙訊息。歹徒通常會使用騙來的帳號，偽裝身分傳訊息給帳號中的親友，讓你在毫無戒心的情況下一步一步掉入陷阱，要求你幫忙買遊戲點數或借手機號碼進行小額付款。這種利用朋友關係下手詐騙錢財的成功率相當高，尤其是傳送的訊息中如果包含緊急金錢需求或危及生命安全的劇情時，更容易讓你受騙而急著將大筆金錢奉上！各位同學除了要謹慎保護自身帳號安全之外，對於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，例如你可以詢問對方只有你們兩人才知道的私事，以確認對方的身分，避免受騙。

2. 網路釣魚的防範方法

通常釣魚電子郵件中所提供的網址會與真正的網站不同，例如其中的字母可能經過增減或更換，像 www.google.com 可能變成 www.gooogle.com，如果沒有仔細觀察很容易就會受騙，造成帳號被盜用或是個人資料外洩。以下針對網路釣魚提供相關的基本防範措施：

（1）對於詢問你個人資料的信件要提高警覺

當你收到詢問相關重要資訊（例如：使用者名稱、帳號、密碼.....等）的信件或訊息時都要提高警覺，尤其包含對外超連結的內容。通常一般大型企業都不會透過 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」，直接透過「我的最愛」連結到正確網站，或者開啟新的瀏覽器視窗手動輸入網址，除了可以避免誤連詐騙歹徒設立的假網頁，也可以經由正確網站查看收到的訊息是不是真的。

（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，常會引導使用者輸入敏感資料來換取優惠或利益，請小心留意這些網站的真實性，輸入個人重要資料的用途及可能造成的影響。

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

對於重要的個人常用網站，例如：電子郵件信箱、網路遊戲……等，需時常注意登入的時間、位置、或電信業者的小額付款等紀錄，是否有不正常的登入或消費紀錄，如果有疑問應儘速撥打該公司的客服電話查詢。

（5）透過加密的網頁功能傳送個人資料

如果網站要求你輸入任何重要資料，要注意網址是否為 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，不同的瀏覽器顯示的方式及位置可能會有不同），這些方法並不是百分之百安全，但至少可以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，各位同學除了本身需要具備充足的資訊安全觀念，建議你可以安裝防護軟體並且隨時更新，更加提昇安全性。

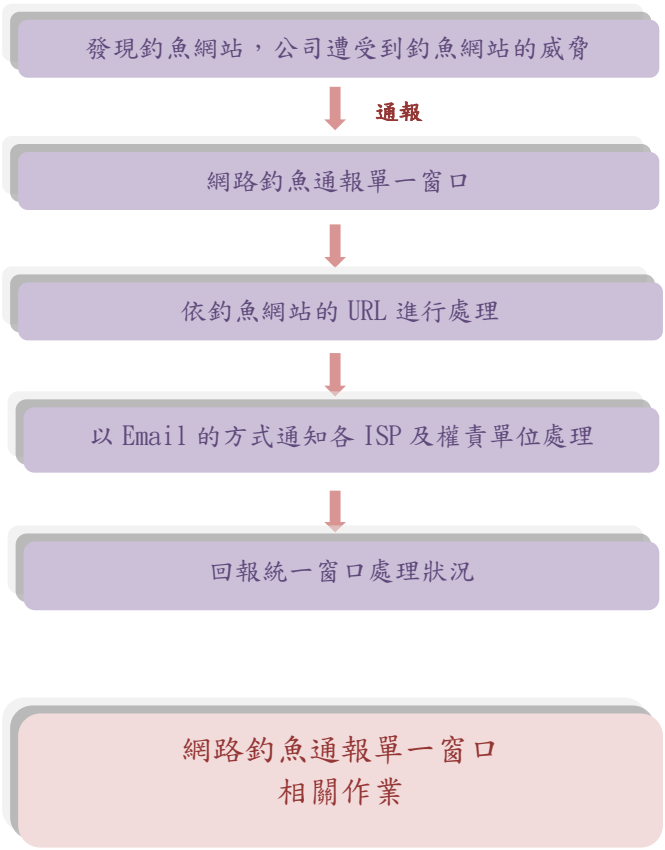
（7）主動回報釣魚網站資訊

一旦發現自己遭遇網路釣魚時，為了防止受害範圍擴大，建議你可以將案例通報到專責單位進行記錄及後續處理追蹤。相關作法請參考下一節「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（但不受理惡意程式或其他網路攻擊事件），透過這個平台可以協助企業、電信網路業者及警政單位以自動化的方式加快釣魚網站追蹤處理的流程，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，讓相關單位可以儘速追蹤處理，降低網路釣魚帶來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/）

當你進入通報平台後，可以在首頁中依據案件類型（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，將這個資訊立即轉告其他相關機構，提早揭露與預防歹徒網路犯罪的手法！

社群網站日益盛行，網路釣客也會趁機入侵，利用聳動或有趣的訊息內容（例如：偶像明星的八卦）引誘使用者點入連結或執行外掛程式，個資即可能馬上洩漏，甚至成為釣魚陷阱的犯罪跳板。釣魚手法日新月異，身為網路使用者的你我，都應共同為安全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
潤稿人員　鄧達鈞　桃園縣祥安國民小學教師
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。