資訊安全案例宣導

案例一：武功極界—無影手 VS.麥擱騙啦—有影沒

社團法人台灣 E 化資安分析管理協會、逢甲大學資訊工程系李榮三主任／教授

資料來源：清流雙月刊 112 年 3 月號

由臺灣警政署與美國網路犯罪投訴中心（Internet Crime Complaint Center, IC3）統計的網路犯罪資訊，可發現近年來國內外的網路攻擊、詐騙等犯罪事件數量居高不下。

據臺灣警政署統計，自 2017 至 2021 年間，平均 1 年發生 1 萬 3 千例以上。雖近年來的犯罪統計稍有下降趨勢，但受害者仍成千論萬。況且，這些統計數量僅計算已通報的案件，未通報的案件更是不計 其數。美國則更甚，IC3 的報告中指出每年平均有 55 萬例，且數量有顯著提升，2017 至 2021 年的通報案數量已暴增 2.8 倍。甚至網路犯罪受害者損失的金額平均每年高達 370 億美金，由此可見，網路犯罪所帶來的威脅不可估量。其中，最常見的手法即為「網路釣魚攻擊」。網路釣魚如同真實世界釣魚，釣客即為隱匿於網路背後的駭客，常見的公務通訊軟體、社群媒體等則是作為駭客的釣場，駭客透過散播魚餌誘使民眾點擊上鉤。

個人案例與防範策略

一、周杰倫無聊猿 NFT 被偷損失上百萬

2022 年 4 月，明星周杰倫在社群網站公布其「無聊猿」非同質化代幣（Nonfungible Token, NTF）被釣魚網站偷走的消息。所謂「無聊猿」是由無聊猿遊艇俱樂部（Bored Ape Yacht Club, BAYC）推出 的 1 萬隻各有獨特表情的猿猴 NFT 作品，當時每隻價格約在 100 枚以太幣（約 26 萬美金）。這類事件的起因就是駭客在官方社群網站放上釣魚網址來誘騙被害人。使用者在社群媒體上看見 NFT 的預購訊息，以為可以用較便宜的方式來購買新的 NFT；誘使使用者點擊鏈結後會進入釣魚網站，便可選擇

金額開始進行交易手續。然而釣魚網站的交易內容並非預購 NFT 作品，實際上是受害者被鏈結的文章所吸引，毫無警覺內容的真偽，導致駭客成功騙取授權交易。

二、FB Messenger 點擊網址詐騙達高峰

亦有受害者 2020 年在 Messenger 收到名為「我不敢相信是你」的假 YouTube 影片鏈結，想觀看者必須先輸入 Facebook 帳號密碼，一旦使用者於假網站中登入，駭客便成功盜用使用者帳號密碼，隨後再將鏈結散播給該帳號的好友，讓被害人淪為散播惡意鏈結的工具。根據國外資安廠商 Pixm 發布的最新研究報告，推估全球臉書至少有數百萬位用戶遭誘騙導致個資外洩。

三、個人防範策略

在網路資訊發達的年代，駭客偽裝成一般使用者來散播惡意鏈結進行釣魚已是常態，因此資安意識對於民眾而言已是必修課題之一。

防範作為有：

（一）提升潛在威脅警覺性：當收到陌生訊息、開啟未知網址、下載非官方軟體時，人們其實難以辨別其中是否夾帶惡意行為或攻擊，應提高警覺性，避免落入駭客陷阱。

（二）陌生訊息：當使用者瀏覽社群媒體上陌生人所發布的訊息時，應時刻保持懷疑的態度，在進入網址前要先查證訊息的正確性。如 NFT 遭盜取事件中，在社群網站看到 NFT 鏈結時，應先去向官方求證，而不是相信社群網站的訊息。只要使用者對內容產生懷疑並查證，就可以有效避免釣魚事件發生。

（三）未知網址：收到朋友傳遞的未知網址時，使用者應先確定該消息為本人傳遞，才點擊鏈結。如案例 FB Messenger 點擊網址詐騙中，使用者在收到可疑鏈結後，可透過打電話的方式來確認朋友身分的真偽，避免朋友的個人帳號遭到駭客利用而不自知。

（四）使用威脅檢測軟體：使用檢測軟體可以有效偵測惡意鏈結和惡

意程式，大幅降低使用者被釣魚的風險。當使用者遇到必須點擊陌生鏈結或執行來歷不明檔案的情況時，可以利用 Virustotal 檢測軟體，使用者將鏈結或檔案上傳後，該軟體會自動偵測其是否被資安廠商認證為惡意鏈結或檔案，並產出相應的報告。使用者可自行評估該檔案所伴隨的風險。基於安全考量，倘若有任一廠商對該鏈結報有疑慮，建議使用者不要點擊。

有別於個人案例，駭客對於企業的攻擊更具威脅性，其會針對企業的特色、員工 的素質、工作內容進行釣魚郵件的客製化，進而達成各種攻擊目的。這種持續針對特定組織發起的網路攻擊我們稱之為進階持續性滲透攻擊（Advanced Persistent Threat, APT）。

無論是一般民眾或是政府企業，都會收到來自駭客的釣魚攻擊，手法層出不窮且越加高明。除了依靠系統提供的自動防禦偵測機制外，全民應提升對於釣魚訊息 的警覺性以及基本認知，才能計出萬全，去危就安。

案例二：公務郵件帳密資料外洩案例

資料來源:摘錄自中國時報 109 年 4 月 30 日疾管署人員被駭嚴控防疫資訊外 流新聞內容。

一、資安事件

新冠肺炎疫情嚴峻之際，近期傳出衛福部疾病管制署人員帳密個資，疑遭駭客入侵竊取的資安事件，據了解，國安局指示調查局資安工作站立案調查後，檢調懷疑駭客透過歐洲等地 IP 作為跳板入侵，先在電腦主機植入後門程式，再竊取帳密個資，不排除是歐洲或大陸駭客所為。KPMG 數位科技安全服務執行副總謝昀澤表示，初步分析應為公務員使用公務帳號，在如電子商務等外部網站註冊，導致大規模帳密外洩。

疾管署官員指出，於接獲國家資通安全會報通報發生公務電子郵

件帳密資料外洩事件計 68 筆，隨即進行清查，發現其中 65 筆資料為 2018 年、2019 年曾經通報的歷史資料，僅 3 筆為今年首次出現且非屬現在的有效帳號，該署於清查後，除確認沒有跟使用中的帳密相符外，並均已將相關帳號予以停用。

二、預防及策進作為

身在數位時代，電腦與網路是辦公的得力助手，但也可能成為公務機密維護的漏洞。建議機關同仁處理私人事務，應以私人信箱帳號為主，請勿使用公務信箱帳號進行外部服務註冊，更不要於外部網站設定與公務帳號相同的密碼，避免外部網站主機一但被入侵，使用者所擁有的公務信箱、公務資料、個人金融帳密等，都將一起曝險。

保護自己也保護機關公務機密安全，人人有責。