公務機密維護宣導 - 麥擱騙啦─有影沒

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。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。

FB Messenger 點擊網址詐騙

受害者在 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。

BEC 釣魚郵件

國外駭客經常使用像“office”、“president”、“chief”、“director”等高階職務名稱作為電子郵件帳號，透過偽造身分，來向員工索要機密檔案。或是會偽造一個與被冒充人非常相似的地址，包括將某些英文字母和數字互換以達到混淆的目的，像是英文 l (小寫 L) 與數字 1 (數字一)、英文 o 與數字 0 等，讓受害者難以在第一時間辨認出真偽。因此，使用者收到信件時，應多留意信件的來源地址是否正常，若有異常之處即可通報或忽略該信件。

個人防範策略

（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。可以先去向官方求證，而非逕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。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。

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。

資料來源：清流雙月刊 2023.3 月號