常見電子郵件詐騙手法

電子郵件的便利性，使其成為駭客攻擊的最佳管道，依據內政部警政署刑事警察局 165 反詐騙諮詢專線的統計，從 2016 年起，臺灣商務電郵詐騙已逾百起，企業損失超過 1 億新臺幣，近年來此類詐騙數量仍在急遽成長，在 2018 年因商務電郵詐騙引起的損失金額更高達 2 億元。以下列出 2018 年主要的五大電子郵件詐騙手法，提供各界參考。

一、偽造系統通知信

舉凡密碼過期、授權不足或郵件空間已滿等相關的通知信類型都可能成為詐騙攻擊的前奏。這類偽造信與真正的系統通知信相似度極高，且信中帶有 URL 連結，當使用者點擊信中連結，會導到偽造的釣魚網站騙取使用者的帳號密碼，此外信件中的回覆地址（Reply-To）與寄件地址（From）往往不同。

正確處理方式：

- 確認信件中連結是否為官方網站。
- 勿輸入任何帳密資訊。
- 只透過官方電話與客服人員確認相關服務。

二、跨國貿易詐騙信

國際貿易的詐騙信大部分以英文語系為主，有時也會自動翻譯成簡體中文，主要攻擊對象鎖定在跨國貿易公司，其詐騙情境為運送之貨櫃被國外海關扣留，必須支付一筆為數可觀的關稅。信件會附上完整的匯款資訊、物流編號與國際物流公司網站連結。使用者點擊後會導到製作精美的網站，且有完整機制可供查詢，目的在於取信收件者，實際上是一場精心策劃的詐騙攻擊，值得注意的是此類網站通常沒有安全憑證，且網域建立的日期很新。

正確處理方式：

- 確認該網站是否有安全連線憑證，若無憑證很有可能就是釣魚網站。
- 在未查證之前，絕不輕易匯款。

三、勒索信件

此類信件中多會提供被害人曾使用過的帳號密碼或聯絡方式，攻擊者宣稱「透過惡意程式側錄了你的密碼」，並利用網路攝影機錄製了隱私畫面，被害人需於 48 小時內透過比特幣支付贖金。若未支付贖金，就會向受害者的家人、朋友、同事或社群網站的聯絡人散布隱私照片或影片。

正確處理方式 ：

- 遮蔽網路攝影機鏡頭，避免遭到有心人士側錄。
- 電腦軟體應安裝修補程式，避免產生漏洞。

四、中獎通知信或一頁式購物詐騙

這類詐騙主要透過電子郵件 EDM、facebook 及 LINE 等方式傳播，其特徵是銷售網站為一頁式網站、免運費、七天鑑賞期、價格遠低於市場行情，為了取信消費者也會標榜「貨到付款」，但下單後實際收到的商品卻與網站上有極大落差，若打電話給客服要求退貨通常求助無門。

正確處理方式：

- 可參照官方網站查證是否有促銷活動。
- 可向 165 反詐騙專線查證。

五、以匯款為標題的惡意程式攻擊

屬於典型的病毒信，其內容多是請收件者確認匯款收據等相關資訊，附檔為 ZIP 或 RAR 壓縮檔，若為 Office 檔案類型格式，通常帶有惡意巨集程式，若為 PDF 檔其中可能含有 JavaScript 攻擊腳本，有些附檔內則含有病毒或木馬程式等執行檔。

正確處理方式：

- 對來路不明的信件提高警覺。
- 勿輕易開啟未知附檔。

※ 本文轉載於全民資安素養網

基隆監獄政風室 關心您