聰明看穿電子郵件詐騙手法（下篇）

在上篇文章中，已介紹四種常見的電子郵件詐騙手法，接下來還有哪些電子詐騙手法需要注意呢？

強調優惠或好康訊息的郵件

像是服務升級、各式好康、優惠通知的郵件內容，千萬不要隨意點開信中連結與檔案，攻擊者時常會挑戰人性的貪婪，若是警覺心不夠，很容易被帶到假冒的釣魚網站，例如：儘管郵件內文的某電信服務電話完全正確，寄件者名稱也取名也是該電信公司的名字，但其實內文中所附的連結網址卻已經偷偷動過手腳，最後並不是導向你所以為的官方網站。

偽造的系統通知信（一般使用者無法完全判別，建議使用網路工具輔助）

別看到系統的通知信，就不疑有他而打開。現在這類告知帳號有問題或通知系統升級的假冒電子郵件越來越常見，加上網路社群與資訊平臺已經廣泛受到使用，人們早已經不完全記得曾經註冊過哪些網站服務或系統。因此，有關此類信件若想去確認，網路上已經有輔助工具，在收到此類信件的時候，可以第一時間主動透過工具去判斷是否可疑，或者直接以第二管道打電話去店家客服進行詢問。

看似正常的假冒重要郵件、長官郵件、客戶與廠商往來郵件（較難判別，建議使用網路工具輔助）

這類信件是最容易攻擊成功的手法，攻擊者通常會利用收件人擔心錯失重要信件心理，像是偽裝成生意上的通知信件，例如信件標題帶有訂單（Order）、發票（Invoice）、運輸（UPS、Fedex、Amazon）或是報告（Report）等，這類詐騙電子郵件欺騙使用者得逞機會很高，讓他們相信這是工作上溝通的信件，或是有重要、緊急的訊息，降低使用者警戒心。收件人若要開啟這類郵件中時，最好還是找到第二種管道，也就是與對方確認過後再開啟，也因為難以自行判別，同樣也可以利用網路工具協助做判斷。

以上的例子都是 BEC（Business Email Compromise 商務電子郵件入侵）實際常見案例，造成的損失堪比木馬程式與惡意病毒，防範的不二法門即是收件當下的判斷，除了主動自行尋求第二管道查證確認外，也要謹記電子郵件中的陌生網址或附件都不要隨意亂點選、下載，多一些懷疑，就讓自己的個資與電腦受到更多的保護。