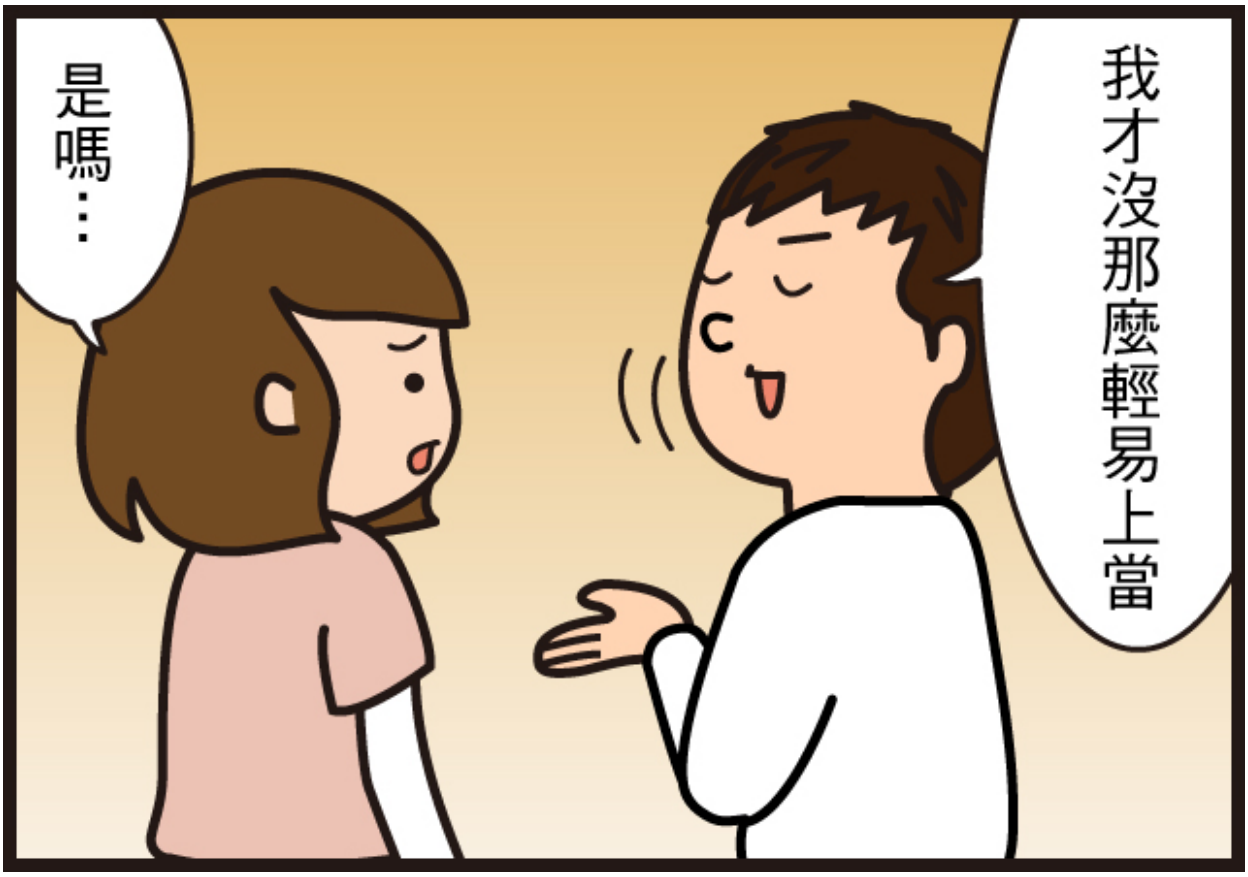
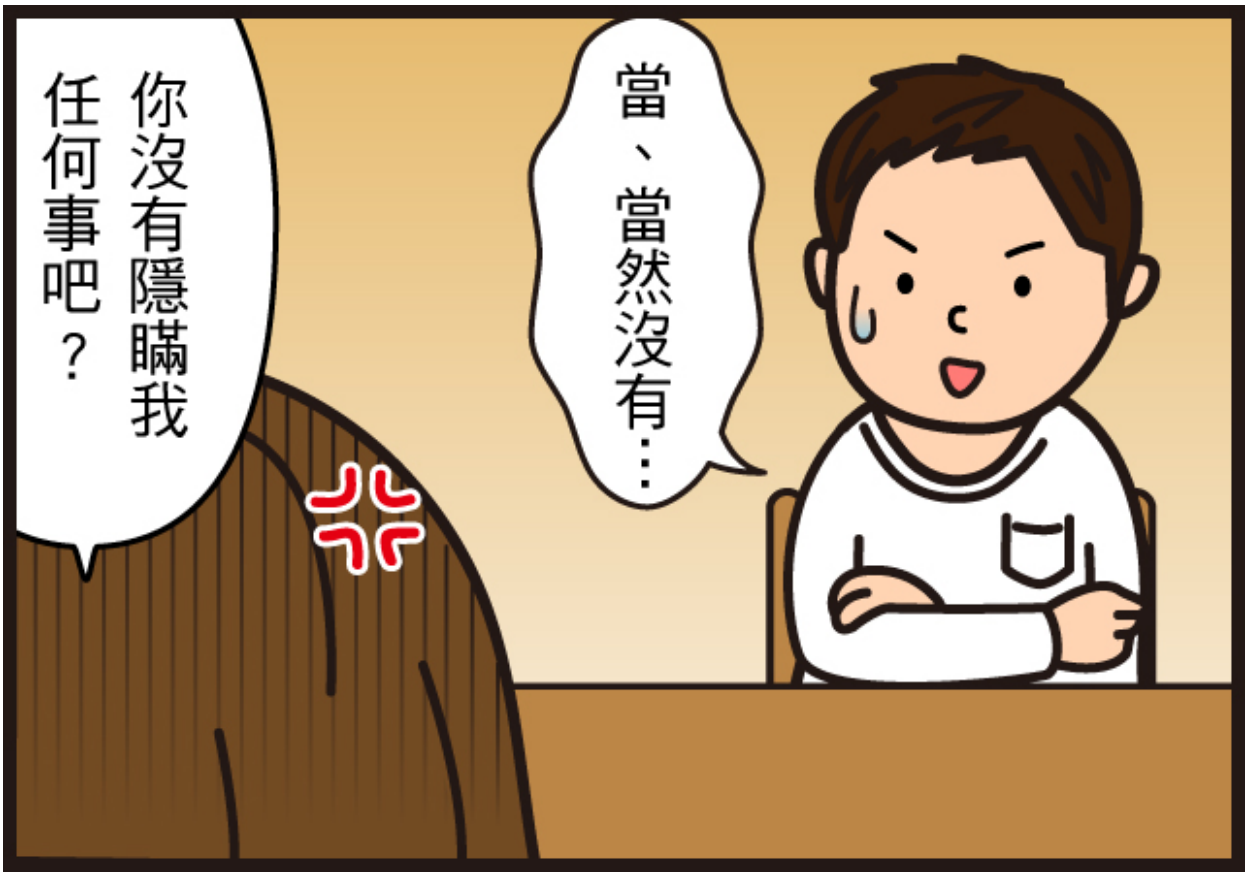
什麼是社交工程（social engineering ）陷阱/詐騙?

趨勢科技 TrendMicro ⁝

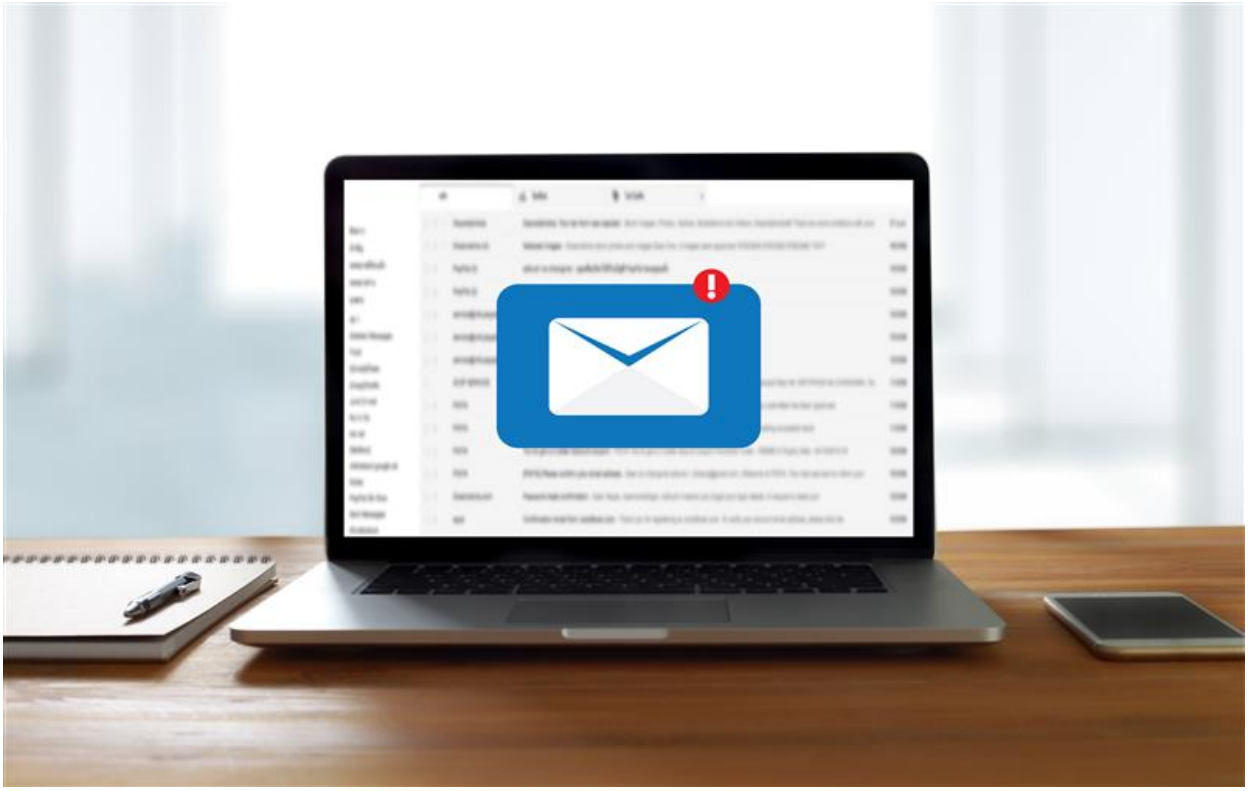
一封冒稱健保局的「二代健保補充保險費扣繳辦法說明」,導致萬筆中小企業個資遭竊;一封偽裝銀行交易紀錄信件,導致南韓爆發史上最大駭客攻擊;996 名公僕因為一封標題為「李宗瑞影片，趕快下載呦！」信件, 以上是因好奇心中了社交工程陷阱著名案例。


這就是時下流行的詐騙手段
如果不想個人隱私被公開，就得乖乖付費。


我才沒那麼輕易上當
是嗎…



你可以強化各種防禦措施，但人類的情感可能是整個安全防護體系中最脆弱的一個環節。正如趨勢科技資安威脅研究專案經理 Jamz Yaneza 所言，「您的許多連線可能都十分安全，唯有椅子和鍵盤之間的這個連線可能造成問題。」



社交工程技巧：操控人類心理的藝術

社交工程技巧涵蓋許多用以操控人類心理，使他們採取特定行動或透露機密資訊的技巧。「社交工程技巧」一詞指的通常是用以收集資訊或電腦系統存取權限的詭計。社交工程圈套利用目前備受矚目的重大事件與新聞作為誘餌，無論是政治、運動、娛樂性質，同時也不分全球性或地區性。此外，社交工程圈套也可能利用日常活動作為誘餌，例如線上理財、投資、帳單管理以及購物等等。

您今天收到了哪些垃圾郵件？

您或許曾受吸引而去閱讀一些您收到的垃圾郵件的標題：

垃圾郵件是藉著博取收件者的信任感所設下的圈套。最近常見的手段即是偽裝成宅配業者寄出不在府通知郵件。例如：「您有包裹未取。詳情請點擊以下網址」等的文字記載 」或是讓很多 FB 用戶上當的「 12 小時內不驗證你的 Facebook 帳號,將被永久停權」 ,都在企圖誘導收件者進入不正當的網站，此手法近來頻頻可見。包誇近年大舉入侵全球的勒索病毒 Ransomware (勒索軟體/綁架病毒) 。

這些社交工程信件,常利用熱門政治新聞 、 宗教、文化、社會、環保以及科技活動相關議題，以及名名人八卦、慘劇、天災等等為散播主旨。
每年報稅期間'網路罪犯總會冒用稅務機關的標誌，試圖引誘納稅人中計。中國發生慘烈的大地震期間，風暴傀儡網路隨即散發中國再度遭地震襲擊的假新聞，垃圾郵件如洪水般湧入使用者的收件匣。這些垃圾郵件夾帶一個影片連結，一旦按下之後，便會下載一隻如蟲 (WORM_NUWAR.YH) 變更受害電腦設定，使之成為傀儡網路的成員。

無庸置疑：社交工程技巧極為有效

早在病毒問世之際，網路罪犯便開始使用社交工程技巧。雖然電腦威脅不斷進化，但有一個事實從未曾改變：社交工程技巧的有效性。社交工程技巧的成功可歸因於它利用人類先天具有的情感，例如同理心、同情心、好奇及心恐懼等。人們會對運動員的成就讚嘆不已，對病痛感到畏懼，對於遭受天災侵襲的景況心生悲憫。社交工程技巧操弄這些情感，藉此引誘人們採取網路罪犯所期待的行動，以便讓他們的惡毒詭計得逞。

社交工程技巧能夠奏效的原因在於它利用人類輕信他人的天性。輕信他人的天性導致許多人可能成為攻擊行動的受害者。目前已有許多軟硬體能有效防範各式各樣的網路威脅。然而，整個防護體系中最脆弱的一

個環節也是最可能遭受攻擊之處。就此而言，這個最脆弱的環節指的就是使用者。

社交工程技巧的演進

雖然社交工程技巧已經流傳多年，但仍一再被利用，並且不斷演進。各式各樣的資安威脅，都會使用社交工程技巧。社交工程技巧在目標式攻擊中使用的頻率愈來愈高。網路罪犯以往只會利用全球性事件或新聞 (例如世界盃足球賽或情人節等) 來引誘使用者。現在，蠕蟲、大量發信程式及其他資安威脅會整合社交工程技巧以鎖定世界上的某個區域或特定國家。網路罪犯可能使用各地的語言，利用各地的重大事件或新聞為誘餌，使特定國家的人產生興趣。這使得運用大規模社交工程技巧的網路罪犯得以躲避偵測，同時還能引發嚴重的災情。在擁有大量新的網際網路使用者上線的國家，這種方式可能特別有效。

什麼是社交工程惡意程式？

社交工程惡意程式專門假冒其他軟體和/或隱藏在其他軟體之內，引誘使用者下載並安裝該軟體，藉此趁機安裝惡意軟體。社交工程惡意程式不論對個人或對公司都會造成嚴重的風險，進而導致機密資訊遭盜用竊取、損毀或外流。

由於今日**經由網頁感染的惡意程式佔所有惡意程式的50% 以上**，因此這類威脅必須透過更精良的技術和資源來防範，而這也是桌上型電腦資訊安全產品目前努力的方向。

如何避免誤觸社交工程信件？

- 如果信件當中含有網站連結，**請將滑鼠移到連結上停一下**，看看其顯示的網址是否與電子郵件的來源相同。例如，發信的公司網域名稱與網址所顯示的網域可能不同。
- **仔細觀察訊息內容**，如果它一直在催促您盡快開啟某個附件檔案或點選某個連結，那很可能有詐。
- **先將附件檔案另存新檔，然後掃描**看看是否為惡意檔案，切勿貿然直接從電子郵件內開啟附件檔案。

延伸閱讀:

PC-cillin 雲端版整合 AI 人工智慧的多層式防護，精準預測即時抵禦未知威脅 》即刻免費下載試用