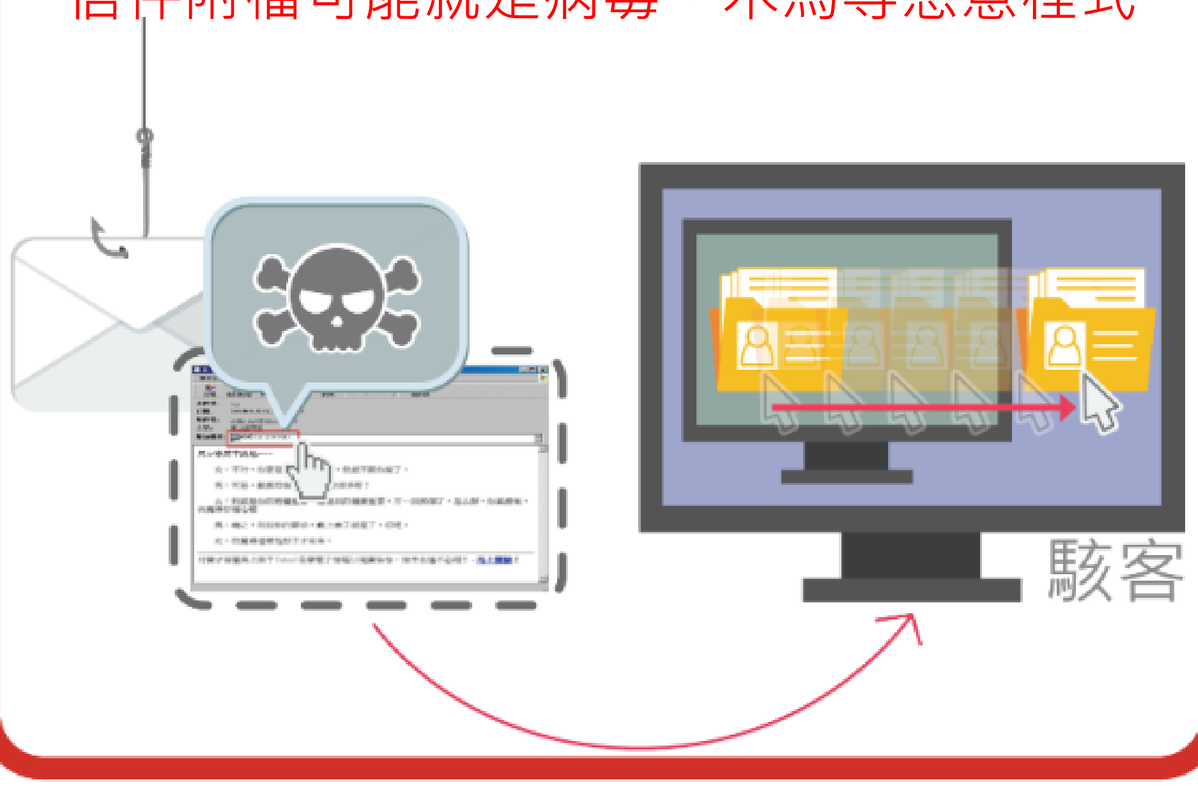
社交工程要警覺

教育部每年4月~11月都會實施社交工程演練，目的是為了模擬駭客寄送各類詐騙信件的手法，測試教職員點選各類誘騙信的比率，以強化教育機構教職員對資安等社交工程的警覺意識。

社交工程是利用人性的弱點進行詐騙，最常利用電子郵件等方式進行。往往駭客最常在這類的信件中藏惡意的軟體或連結，使用者稍不注意點擊或開啟就會讓駭客有機可趁。

駭客會弄個假冒網站來騙取你的帳號密碼

信件附檔可能就是病毒、木馬等惡意程式



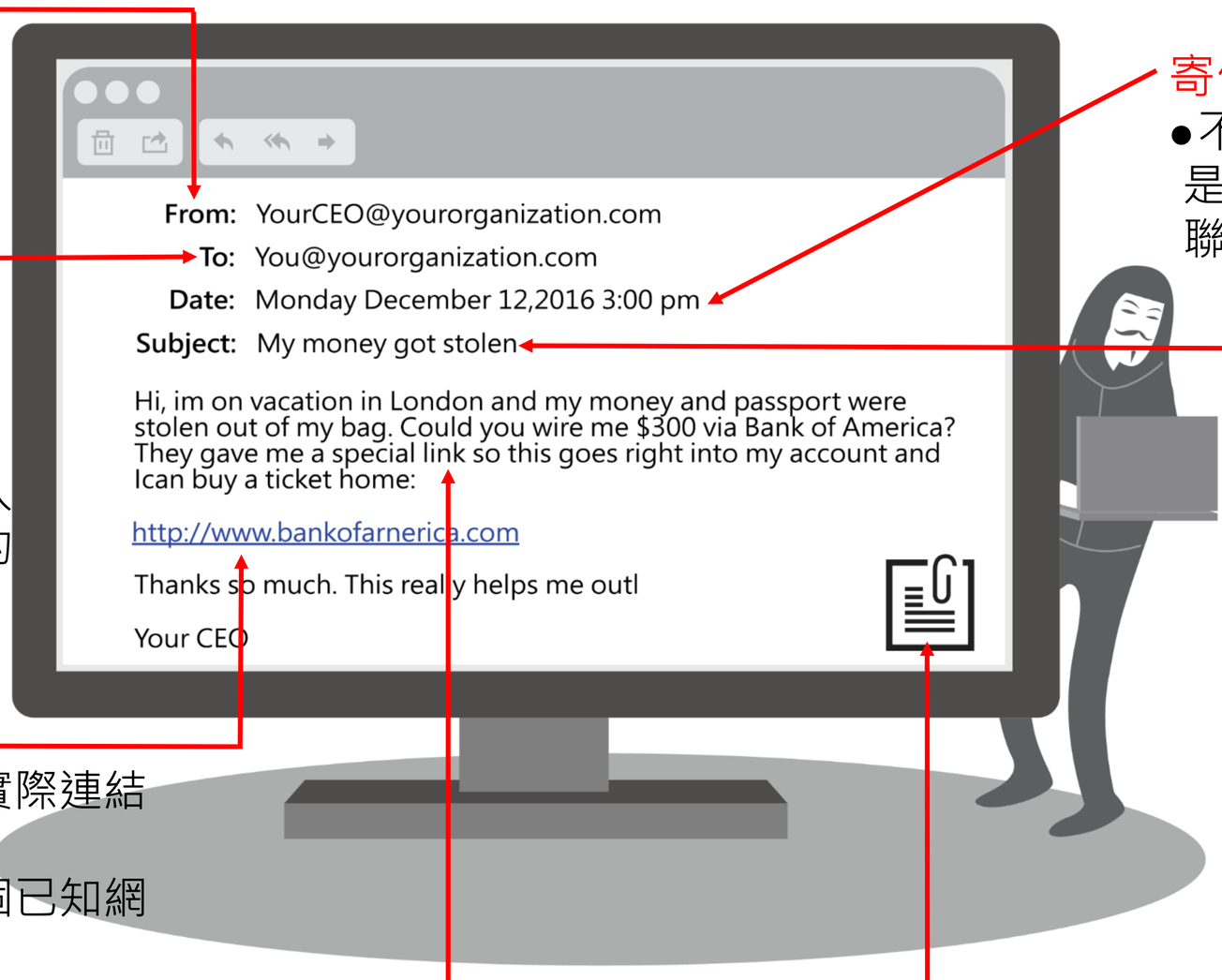
收信時必須要注意寄件者的信箱、寄件時間以及信件的主旨還有附加檔案等等...，發現這些疑點有可能是釣魚郵件就應避免開啟信件附件或點擊信件內的超連結。

寄件人信箱若是.....

- 不認得的人
- 沒有業務往來的人
- 署名某人但他應該不會跟我聯絡的信箱網域名稱蠻可疑的(像某單位的網域又有點不像、或是免費信箱)

收件人群組若是.....

- 還有其他一些不認識收件人
- 看來像是從網站把同頁面的通訊錄都納入收件人名單中



寄件時間若是.....

- 不太正常的寄件時間，像是半夜3點怎麼有人會寄信聯繫業務呢?

信件主旨若是.....

- 主旨看來跟自己無關的
- 主旨與信件內容不相關
- 主旨是回覆什麼，但之前並未寫信去問過什麼啊!

信件內的超連結若是.....

- 滑鼠移到超連結上可看到實際連結的網址與表面上的網址不同
- 超連結網址看得出來是某個已知網站但中間有些微拼錯字的
- 超長的超連結網址就要特別小心

附加檔案若是.....

- 檔案名稱看起來不應該寄給我的
- 檔案名稱與信件內容不相關
- 署名某人來信，但應該不會寄這種檔案給自己啊!
- 除了副檔名.txt，任何檔案都有可能包藏惡意程式在內，有懷疑的話就開啟前先用防毒軟體掃描較保險。

信件內容若是.....

- 不合常理
- 提到為了避免什麼不好的後果
- 提到你中獎了或你獲得什麼好處
- 提到別人或自己可能發生桃色事件或不雅照片等八卦消息
- 內容明顯文法錯誤或錯字不少，不像是一般人會嚴謹擬訂字句。
- 強調快點擊超連結或開啟附加檔案