

## 資訊保安動畫 - 仿冒詐騙 (旁白)

### 仿冒詐騙

仿冒詐騙 (Phishing)，又名網絡釣魚，是一種網絡詐騙形式。犯罪者利用仿冒電子郵件或欺詐網站，誤導毫無戒心的網絡用戶，輸入個人資料。

### 仿冒詐騙電郵

「仿冒詐騙電郵」，通常會涉及大量散播附有回郵地址、連結和品牌標記的欺詐性「偽冒」電郵，令電郵看似來自銀行、保險代理、零售商或信用卡公司。這類欺詐電郵的目的，是誘騙收件人相信電郵內容，跟從電郵內指示，登入仿冒詐騙網站，提供帳戶名稱、密碼、信用卡號碼及身份證號碼等個人資料，然後使用這些資料作其他非法活動。

### 仿冒詐騙網站

「仿冒詐騙網站」，即是使用與合法網站相似的域名 (Domain Name) 或子域名 (Sub-domain Name)、或複製合法網站的外表及真確內容，如圖像、文字或公司標記，以誘騙訪客輸入帳戶或財務資料。

仿冒詐騙電郵所設的連結，通常會誘導收件人連接到這類欺詐網站，而非網頁上所顯示的合法網站。

### 潛在威脅

如果你受到仿冒詐騙攻擊，你將會面對甚麼威脅？

由於這些電郵幾可亂真，有些收件人會作出回應，登入仿冒詐騙網站，結果是個人資料外泄、財務上受損失、身分被盜用/利用作其他欺詐活動。

### 防範措施

要防止被仿冒詐騙，我們在使用電腦時要注意什麼地方？

- 開啟電郵附件時要提高警覺，也不要按電郵內的連結進入網站。
- 不要登入可疑網站，或連接這類網站內的連結。
- 不要從搜尋器的結果連接到銀行或其他金融機構的網址，應以人手直接輸入 URL 網址或進入之前已加入書簽的連結。
- 進行網上銀行交易時，可使用雙重認證 (2-factor Authentication)，例如密碼加智能卡，來核實用戶身分。
- 在完成網上交易後，切記要打印、備存交易記錄或確認通知，以供日後查核。
- 提供個人或帳戶資料時，應保持警惕。銀行及金融機構絕少透過電郵要求客戶提供個人或帳戶資料。如有疑問，應向相關機構查詢。

- 定期登入網上戶口，檢查帳戶狀況及上次登入日期，確定是否有可疑活動。
- 收到信用卡或銀行結單後，應立即檢查是否有未經授權的交易或繳費。
- 另外，你必須為電腦採取基本保安措施，包括安裝反惡性程式碼軟件如防毒軟件，並須安裝防火牆和最新保安修補程式，每週最少全面掃描電腦一次，以及啟動相關軟件的「自動更新」功能。

### 考考你

請選擇正確的答案。

1. 仿冒詐騙是否指利用假冒電子郵件或欺詐網站進行詐騙？

- A) 是 (正確答案)
- B) 否

2. 以下哪一個是有效預防仿冒詐騙的方法？

- A) 在網吧的公用電腦進行網上銀行的交易
- B) 隨意打開副檔名是 ".pif", ".exe", ".bat", ".vbs" 的電郵附件
- C) 不要按電郵內的連結進入網站，而以人手輸入 URL 網址 (正確答案)

想知道更多有關資訊保安的資料，請瀏覽「資訊安全網」：

<http://www.infosec.gov.hk>