

資訊保安動畫 - 濫發電郵 II (旁白)

如何處理濫發電郵？

遇上來歷不明或可疑的電郵，切勿開啟或隨便回覆，應把它們刪除。如果你回覆這些電郵，你就會同時向寄件人證實你的電郵地址是一個有效的地址，結果可能收到更多濫發電郵。

檢查電郵戶口的寄件匣，留意是否有並非你發出的電郵。如有，你的電郵戶口可能已被濫發電郵者控制用來發送電郵。你應立即中斷網絡連線，並立即啟動防毒軟件，掃描你的電腦，以及重設電郵戶口密碼。

如果你的電郵戶口已嚴重充斥濫發電郵訊息，請考慮停用你目前電郵戶口，並轉用一個新設立的電郵戶口。

如有需要，你可考慮向你的互聯網服務供應商查詢或求助，並夾附濫發電郵的標題資料。視乎個別供應商的政策，濫發電郵者可能會被警告、暫停以致終止服務。

防範措施

防範措施包括保護電郵地址及個人資料，和保護你的電腦。

- 在網上提供個人資料時（如申請免費電郵帳戶時），要小心謹慎，仔細查閱網站或公司私隱政策聲明以及服務的使用條款。
- 不要在公開網站、聯絡人目錄、會員目錄或聊天室披露你的電郵地址。
- 盡量使用不同的電郵地址作不同用途。例如：使用兩個不同的電郵地址作聊天室和個人通訊用途。
- 避免使用字典裡簡單的字和通用的姓名作為電郵地址。濫發電郵者可以採用自動化軟件，串連一些字典內常用的詞彙、名稱、字母和數字，組成電郵地址來濫發電郵。
- 安裝過濾電郵軟件，自動過濾及刪除濫發電郵，減少接收的數量。雖然你不能以過濾電郵軟件阻止別人向你濫發電郵，但卻可阻止那些電郵在你的收件匣出現。
- 過濾電郵方法有很多種，一般都可根據寄件人的電郵地址、域名或電郵的標題、內容等來過濾電郵。例如，用戶可設定或使用一些黑名單 (Blacklist)（即拒絕接收電郵的地址名單）來過濾電郵。
- 另外，你必須在電腦上採取基本保安措施，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. 最簡單處理濫發電郵的方法，是否不開啟該電郵，並且將它刪除？

A) 是 (正確答案)

B) 否

2. 以下哪一個措施能預防電郵地址被濫發電郵者採集？

A) 不要在公開網站披露你的電郵地址。(正確答案)

B) 瀏覽可疑網站。

C) 回覆來歷不明或可疑電郵。

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>