

資訊保安你要知

網頁：www.infosec.gov.hk



常見的謬誤

- 「我的電腦已經安裝了抗禦病毒的軟件，不怕受到電腦病毒的攻擊了。」
- 「這並不足夠啊！要確保防毒保護經常有效，你必須定期更新抗禦病毒的檔案和對電腦進行病毒掃描。」
- 「我以自己的生日日期作為互聯網戶口密碼，會較為易記。」
- 「你要小心啊！電腦黑客也會很易測知這類密碼，盜用你的戶口，使你蒙受損失。」
- 「我接上了一個很有趣的網站，當中有很多遊戲和圖畫，不如把它們下載和朋友分享吧。」
- 「千萬不可！你是否確定這是一個可靠的網站？這些來歷不明的軟件可能帶有電腦病毒或黑客程式。把這些軟件隨便寄給別人，可能引致他們受到電腦病毒或黑客的攻擊。因此，切勿瀏覽有可疑的網站或從該等網站下載檔案。」
- 「我的電腦並無儲存有價值的資料，無須加以保護。」
- 「錯的！電腦黑客可輕易地以你的電腦作為踏腳石，對其他已接駁的電腦網絡展開攻擊。你的大意可能會為你的辦公室網絡和電腦系統帶來嚴重的保安危機。」
- 「我的辦公室已安裝了防火牆，所以大可放心瀏覽任何網站。」
- 「不對的！防火牆只可對付資訊保安上的某些攻擊。如果你的電腦沒有其他抗禦措施，或存在保安方面的漏洞，電腦病毒和黑客仍可趁機入侵你的電腦。」



注意事項

- 要**
- 要安裝並使用最新版本的抗禦病毒軟件及定期執行電腦病毒掃描。
- 要先用抗禦病毒軟件掃描所有電子郵件的附件、從互聯網下載的檔案、磁碟及光碟，才開啟使用。
- 要確保電腦的操作系統及軟件已安裝和執行最新的版本及修正檔案。
- 要選擇在已採用保安防護系統 (例如: SSL/SET) 及可靠的網站進行網上電子交易。
- 要選用不易被人猜破組成方式的密碼及要定時更新。
- 要啟動螢幕保護裝置及密碼保護功能。
- 要在不使用互聯網時立即終止連線。
- 不要**
- 不要瀏覽任何有可疑的網站。
- 不要從有可疑的來源下載檔案。
- 不要開啟或轉寄來歷不明的電子郵件及附件。
- 不要啟動電子郵件軟件所備有的自動處理電子郵件附件的功能。
- 不要隨便向別人披露或提供個人資料。
- 不要使用系統為新戶口設立的密碼。
- 不要把進入系統的密碼儲存在電腦內。
- 不要向任何人披露或共用互聯網的戶口及密碼。

詳情請瀏覽「資訊安全網」網頁：

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

其他有關的聯絡資料



警察防止科技罪案組
熱線：(852) 2528 3482 電子郵件：cpu-tcd@police.gov.hk
網址：<http://www.info.gov.hk/police/aa-home/chinese/cpb/comp/index.htm>



香港電腦保安事故協調中心
熱線：(852) 8105 6060 電子郵件：hkcert@hkcert.org
網址：<http://www.hkcert.org>