免責聲明：本小冊子所載的保安建議及有關產品或軟件的使用，並不構成對該等產品或軟件的任何形式推介。任何人士須審慎考慮個別需要，因使用該等產品或軟件而造成的一切損失或損害，個人資料私隱專員(「專員」)一概不負任何責任，亦不影響專員行使其條例賦予的所有職能及權力。

鳴謝：葛珮帆博士(互聯網專業協會創辦人及前會長)

香港個人資料私隱專員公署
查詢熱線：(852)2827 2827
傳真：(852)2877 7026
地址：香港灣仔皇后大道東248號12樓
網址：www.pcpd.org.hk
電郵：enquiry@pcpd.org.hk
二零零八年八月

電腦安全你要知

個人資料你話事

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

《個人資料(私隱)條例》六項保障資料原則

第1原則 - 收集個人資料的目的及方式

個人資料的收集必須與資料使用者的職能和活動有關，而收集的資料適量便可；及以合法及公平的手法收集，並須告知收集的目的及資料的用途。

第2原則 - 個人資料的準確性及保留期間

須採取切實可行的步驟確保個人資料的準確性，並在完成資料的使用目的後，刪除資料。

第3原則 - 個人資料的使用

限制個人資料使用於當初收集的目的或直接有關的用途上，否則必須先獲得資料當事人的同意。

第4原則 - 個人資料的保安

須採取切實可行的步驟確保個人資料的保安，免受未獲授權或意外的查閱，處理或刪除。

第5原則 - 資訊須在一般情況下可提供

制定及提供個人資料的政策及實務。

第6原則 - 查閱個人資料

個人有權查閱及更改個人資料。

電腦安全你要知
個人資料你話事

電腦安全你要知
個人資料你話事

目錄

個人資料私隱專員公署及你的私隱權利

個人資料私隱專員公署是一個獨立的法定機構，負責監管《個人資料(私隱)條例》(「條例」)的執行，條例於1996年12月20日正式生效，目的是保障市民在個人資料方面的私隱權利。

根據條例，市民可享有個人資料私隱的權利包括：公平收集個人資料；獲告知資料的用途；只需提供所需個人資料；要得到同意下，才可更改個人資料的用途；要求個人資料準確；要求個人資料保存期間不超過實際需要；要求採取個人資料保安措施；查閱及改正個人資料；以及要求機構公開私隱政策。

根據條例中有關個人資料保安的保障資料原則規定，資料使用者須採取所有切實可行的保安步驟，確保所持有的個人資料不受未獲准許或意外的查閱、處理或刪除，尤其須考慮資料的種類及如發生該等事情所造成的損害等因素。因此，如未採取適當措施保障個人資料，或不當棄置電腦而引致個人資料洩漏，則可能有違該原則的規定。

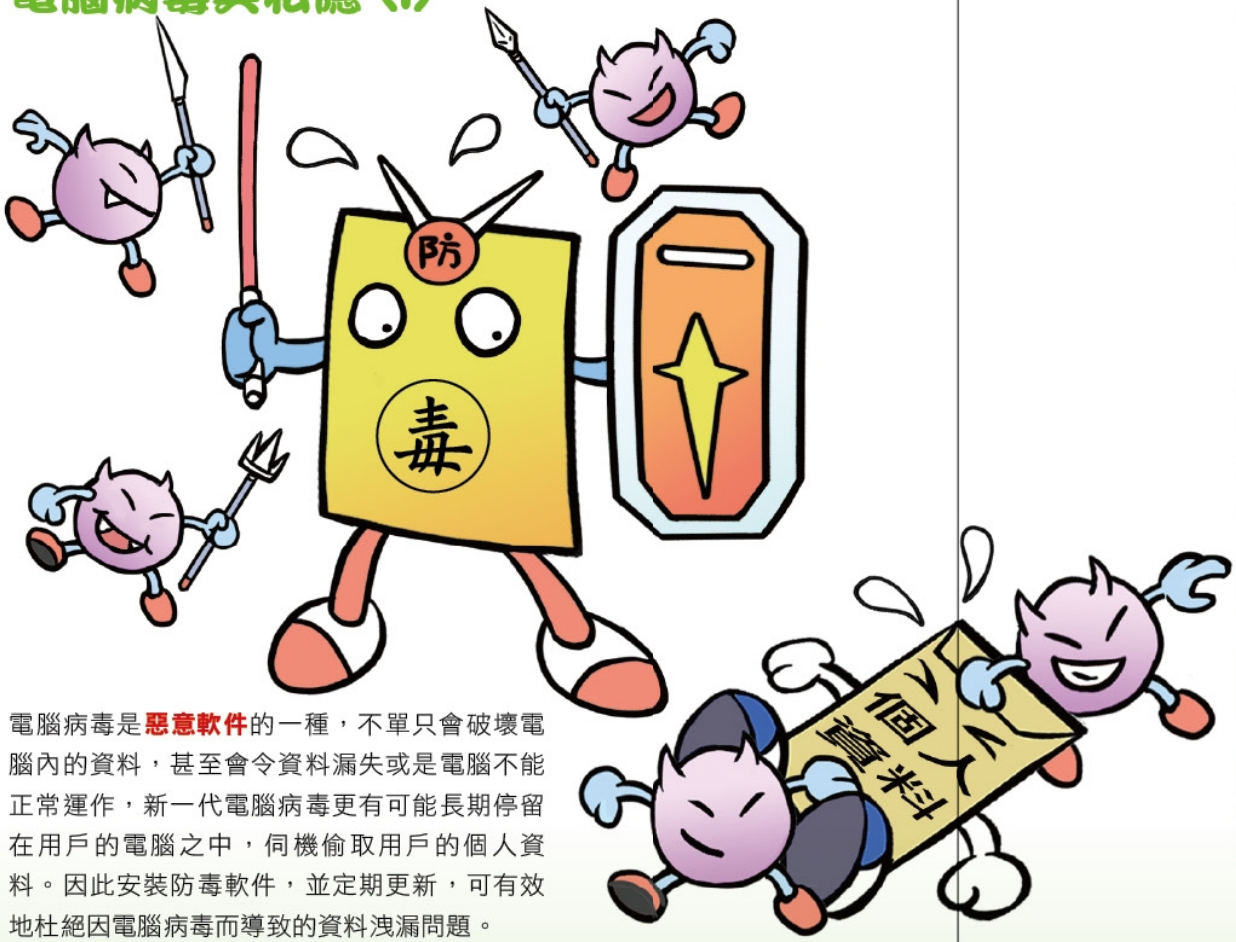
電腦安全你要知

近日連番發生的個人資料洩漏事件，大部分都與電腦有關。以往電腦的功能簡單，網絡功能亦未算完善，但隨著電腦技術，尤其是互聯網以驚人的速度發展，我們在享受著電腦所帶來方便的同時，也要留意隨之而來的各種風險，當中最嚴重的，莫過於個人資料洩漏。

現在電腦除了可以做一般的文書處理外，還可以讓用戶寫Blog、玩MSN Messenger、網上理財等，萬一你的電郵密碼甚至網上理財密碼被盜用，所引發出來的問題可真的難以想像。

電腦安全你要知
個人資料你話事

電腦病毒與私隱 (I)



電腦病毒是**惡意軟件**的一種，不單只會破壞電腦內的資料，甚至會令資料漏失或是電腦不能正常運作，新一代電腦病毒更有可能長期停留在用戶的電腦之中，伺機偷取用戶的個人資料。因此安裝防毒軟件，並定期更新，可有效地杜絕因電腦病毒而導致的資料洩漏問題。

市場上防毒軟件種類繁多，除了收費軟件外，其實也有一些免費產品供用戶使用，雖然功能會較收費版本弱一些，但總比完全沒有安裝好，例如AVG Free、Avast! Home Edition及Avira AntiVir等。

惡意軟件　我們統稱電腦病毒、木馬程式、間諜軟件等軟件為惡意軟件，一般來說都是在用戶不知情的情況下安裝，並在系統中進行散播、破壞及搜尋/傳送資料等工作。

除了防毒軟件外，我們亦建議在電腦安裝個人防火牆軟件，除了操作系統內建的防火牆軟件外，亦可安裝由第三方軟件供應商所提供的防火牆軟件，以提升保安。防火牆像是一個網絡過濾器，以過濾網絡上各式各樣的危險資料。大部分保安軟件公司都會推出一些兼備防毒軟件連同防火牆的整合式Internet Security產品，方便用戶一次過得到全面的保障。此外，用戶亦可以選擇使用一些免費的防火牆軟件，例如Comodo(http://www.personalfirewall.comodo.com/index.html)，功能也相當不錯。

用戶亦應該將**保安軟件**的自動更新啟動，以防禦最新型的威脅。政府設立的「資訊安全網」(http://www.infosec.gov.hk)中，可以下載常見的防火牆、防毒軟件、和各大製造商的安全漏洞修復程式。

免費防毒軟件的相關網站：

AVG Free
網址： http://free.grisoft.com
簡介：支援Windows　XP及Vista操作系統的免費防毒及防間諜軟件，家庭用戶可免費使用。

Avast! Home Edition
網址：http://www.avast.com/eng/free_software.html
簡介：登記過後可免費使用的防毒軟件，除了電腦病毒及間諜軟件外，Avast!更支援偵測日漸流行的Rootkit軟件、P2P檔案傳送及IM(如MSN Messenger)的防毒功能，備中文版供用戶使用。

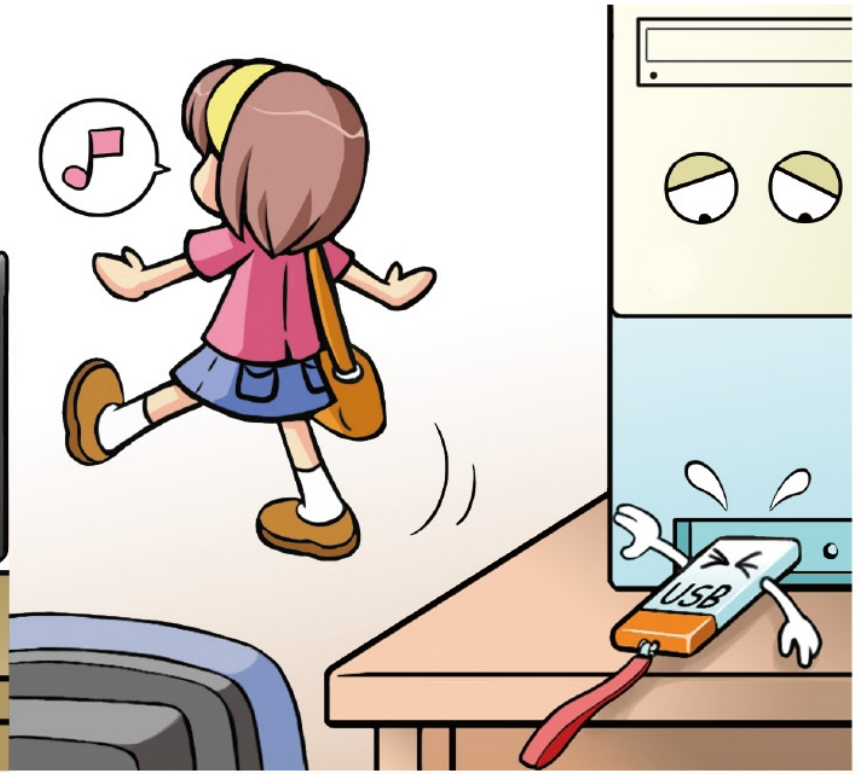
Avira AntiVir
網址：http://www.free-av.com/
簡介：除防止電腦病毒、蠕蟲、木馬程式外，亦能偵測Rootkit及釣魚網站，同樣容許家庭用戶單一電腦使用。

保安軟件　保安軟件就是針對這些惡意軟件而設，當中包括防毒軟件、防間諜軟件及防火牆等。近年流行將這些功能整合，成為Internet Security Suite，為系統作出全面保護。

電腦病毒與私隱 (II)

即使安裝了防毒及防火牆等保安軟件，也不等於可以掉以輕心，因為網絡上的攻擊和陷阱不斷演化，保安軟件亦不一定可即時追上所有最新的網絡攻擊發展，單靠保安軟件實在不能完全避免受到網絡攻擊而導致的個人資料洩漏。**要保障自己，用戶的使用習慣才是最重要的一環。**例如不要隨便在網上下載不明來歷的檔案、不要開啟可疑的電郵附件、不要輕易將個人資料（包括用戶名稱、密碼、出生日期、身份證號碼等）輸入到網站等等，否則安裝了多厲害的保安軟件都是徒然。

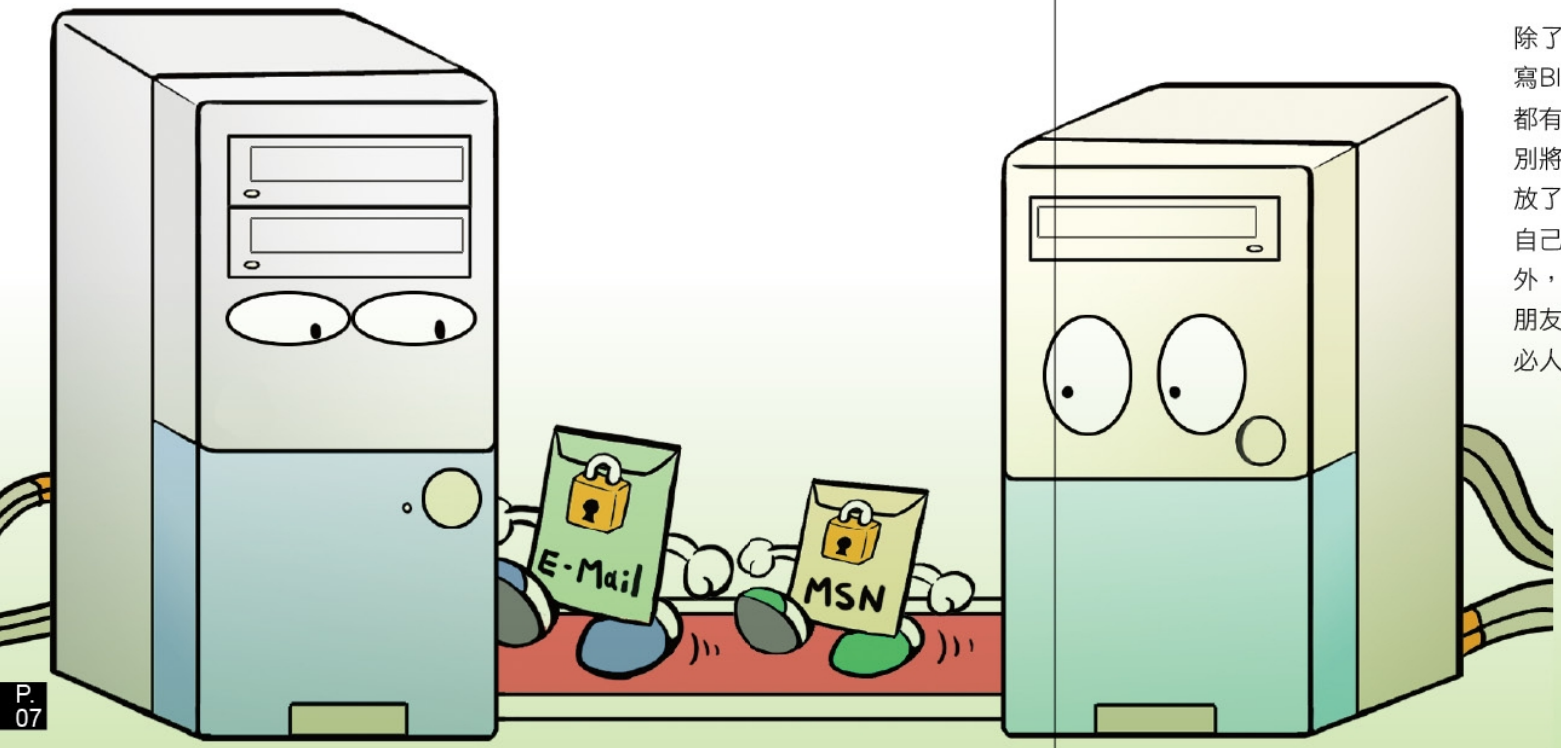
USB手指的保安



USB手指，即USB Flash Memory，它方便攜帶之餘，儲存的容量亦越來越高，不少年青人都會將學校的功課甚至個人的相片儲存在USB手指上。正因USB手指體積細小，因此亦相當容易遺失，導致個人資料洩漏。其實，用戶可以使用有加密功能的USB手指，或使用加密軟件，例如True-Crypt程式（http://www.truecrypt.org/），將沒有內建加密功能的USB手指進行加密便可。加密了USB手指，用戶必需先輸入密碼才可以進行任何存取，否則便不能讀取其內容，確保用戶的資料不易洩漏。

使用IM/ Email/ Blog/ Facebook的保安措施

IM (Instant messaging或即時通訊)是一個實時通訊系統，允許兩人或多人使用網路作即時的文字訊息、檔案、語音與視訊交流。經常使用的IM軟件，如MSN Messenger，傳送檔案倒沒有太大的風險，用戶只要安裝好防毒軟件，加上避免安裝不知名軟件的話，應該能避免大部分的問題。需要比較留心的反而是用戶不應隨意將個人資料向其他聯絡人透露，因為大部分IM軟件都有資料記錄功能（History），萬一該記錄被他人取得，後果難以想像。另外，部份IM軟件設有「資料夾分享」功能，用戶應小心設定，以免個人資料被不當分享出去。



近日亦有愈來愈多人透過MSN Messenger傳送帶有電腦病毒的網站連結。別以為朋友傳送給你的訊息就一定沒有問題，因為此類網站感染了病毒之後，會自動再將帶有病毒的網站連結傳送到你的Messenger朋友，一按上網即會中毒，繼而再傳送給你朋友的朋友，因此除了安裝防毒軟件外，用戶最好在開啟朋友送來的網址前，先問一下朋友傳送來的是甚麼，會比較安全一些。

至於電郵(Email)方面，應該避免隨便按下網絡連結及開啟附件。若要大量寄發同一電郵時，便應使用「密件抄送」(「bcc」)，以免收件者的電郵地址洩露或受病毒襲擊。

除了MSN Messenger外，相信不少人都有寫Blog及上Facebook習慣。雖然這些服務都有基本的安全保護，不過用戶要留意千萬別將個人資料放在網上，因為這些資料一旦放了上網，就可能讓全世界人看到，為保障自己，還是小心選擇放在網上的資料好。另外，如果你打算在Blog或社交網站中分享與朋友的合照，最好還是先知會朋友，因為未必人人都想隨時「亮相」呀！

在Facebook上，你可以設定不同用戶對你的個人資料存取權限。簡單來說，如果是好友的話，可以看到你更多的資料，而其他較不相干的人則怎樣也不可瀏覽有關你的私人資料，以保障個人資料。

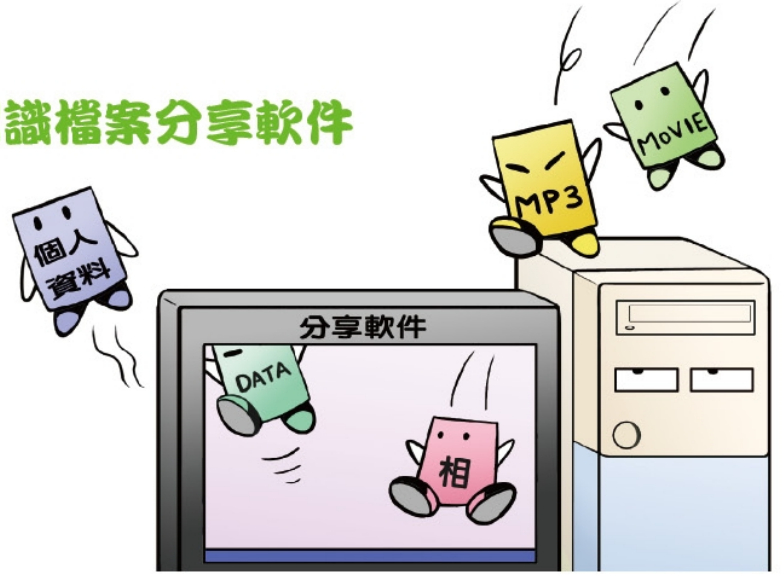
如何傳送及儲存重要的個人資料

如透過電郵方式傳送敏感的個人資料，可以將個別檔案加密再傳送，令對方要輸入密碼才能開啟，便可達致資料保安的效果。

另外，Microsoft Office已有設立密碼的功能，用戶可以為Word、Excel和Powerpoint等軟件的檔案設定密碼保護（一般方法是「檔案」→「另存新檔」→「工具」→「一般選項」→「保護密碼」）。除此以外，Winzip、WinRAR等壓縮軟件，也可以在壓縮檔案的同時，為檔案設立密碼。

若需要更有效的保護，可以使用 Entrust Entelligence、Drive Crypt等專業加密軟件，設定更高效能及更強的加密。

認識檔案分享軟件



Foxy軟件屬於**P2P**軟件，它的優點是檔案傳送非常高速，但由於P2P網絡往往充斥著不法軟件及檔案，用戶無法知道檔案是否安全，萬一被植入了木馬程式或電腦病毒，你的電腦就等同於中門大開，不單只電腦內的資料可任人存取，你的電腦更可能被操控，向其他電腦發出攻擊，無辜成為罪人。另外，部分P2P軟件需要用戶開啟大量網絡傳送埠，同樣有機會令電腦更容易受到網絡襲擊。

最近接連發生個人資料外洩事件，都是因為機構職員使用私人電腦工作時，忽略電腦安裝了檔案分享軟件，令個人資料外洩到網上也懵然不知。因此，用戶在使用Foxy軟件時，必須小心設定其「上載資料夾」，方法很簡單，在Foxy「共享資料夾」的設定版面上，剔走不想設定為共享的資料夾即可。

是否這樣就安全？還未可以，用戶亦需小心設定Foxy中「下載資料夾」的位置，因為Foxy亦會自動將「下載資料夾」中的所有資料分享到網上，給其他Foxy用戶搜尋及下載。因此，建議的設置是：「下載資料夾」的位置設定為一個純粹用作Foxy下載的空白資料夾，並經常清理其中不應被分享的資料／檔案。

點對點/P2P(「peer to peer」)技術 P2P是目前最流行的檔案傳送技術，每個傳送點會同時作出上載及下載活動，減輕需要一個中央伺服器去將資料傳送到多個客戶端的負荷，速度相當之快。

安全使用無線上網

無線網絡愈來愈流行，讓用戶可以更輕易地隨時隨地上網。不過由於無線網絡使用大氣電波作傳送，其他人要截取傳送的資料其實不難，因此使用時必須啟動加密系統，才能避免資料被他人非法截取。

大部份無線網絡系統都支援**WEP**或**WPA/WPA2**加密，當中以WPA2的加密設計最為安全，在可能的情況下，用戶應該採用WPA2加密。就以政府的WiFi通服務為例，它同時備有非加密及以WPA2加密的兩種連線方式，建議用戶使用設有加密的方式，可減低資料被截取及破解的風險。另外，在使用公眾無線網絡時，要注意不要設定將資料夾分享。

WEP 無線網絡加密技術之一，全名為Wired Equivalent Privacy，屬於舊式加密，採用靜態加密設定，已經不足以應付今天的要求。

WPA 無線網絡加密技術之一，全名為Wi-Fi Protected Access，透過動態加密設定，能有效減低無線傳送資料被破解的可能性。

電腦的維修及棄置

如果電腦壞了需要維修，我們如何才可以避免個人資料洩漏？首先，選定一間信譽良好、可以信任的維修公司，例如應瞭解公司的處理個人資料方面所採取的政策及方法，有否確保處理資料的人員有良好的操守及審慎的態度等。若果有必要連同硬碟一併維修，可以預先備份(backup)，然後再刪除私人檔案。假如用戶的電腦不要了，亦不應隨意棄置，以往有機構因隨意將不再使用的電腦棄置而導致資料洩漏。因此，建議先以專門的檔案刪除程式，例如WipeDrive、Inferno等軟件，把硬碟內資料刪除。或用硬碟廠提供的low level format（低層格式化）軟件將電腦格式化，便可徹底清除資料。