以便攜式電子裝置儲存機密資料宜三思

政府資訊科技總監辦公室
資訊科技保安小組

■ 便攜式電子裝置的使用現已非常普及，因掉失這些裝置以致資料遺失的事件也時有所聞。由於資料可能會因而外泄，因此，保護儲存於裝置內的資料，與保護裝置的實體同樣重要。此外，在很多情況下，例如未獲授權的接達，資料也可能會外泄。使用這些裝置的用戶必須重視資訊保安。

實體保安

嚴密監察是實體保安的基本策略。儲存了機密資料的便攜式電子裝置，如沒有人看管，便應存放於安全的地方，最好是把裝置鎖起來。存放裝置的文件櫃或辦公室的安全也不可忽略。

實體保安對於那些細小及流動的物品，例如手提電腦、流動電話及外置磁碟機等，更爲重要。爲防遺失，可以爲這些物品編訂索引，並貼上標籤，以便識別和進行定期存貨檢查。這樣，如有遺失，也可馬上察覺。

未獲授權的接達

任由他人使用電腦裝置，即使只是短暫的使用，也可以產生很嚴重的後果，例如資料給複製或重要的保安設定遭更改。舉例來說，把智能電話借予他人使用一陣子，便有可能讓對方以短訊或電郵方式把電話內的重要檔案傳送。要防範這些風險，通常要靠接達上的限制，例如安裝設有密碼保護的熒幕保護裝置，也可使用較先進的生物特徵識別技術，例如指紋鑑定。

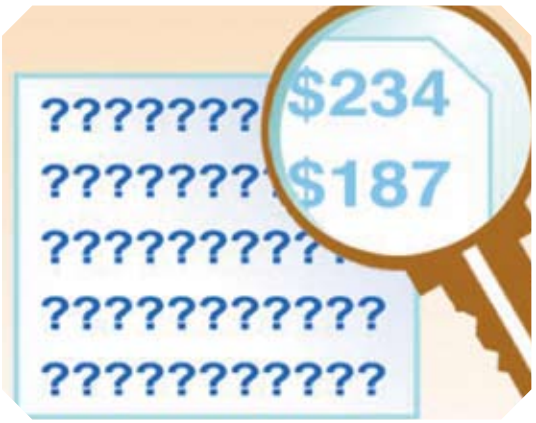
未獲授權的接達也可來自網絡，這種情況在便攜式無線網絡裝置尤其常見。電腦病毒、間諜軟件及木馬程式的破壞力無人不知，它們所造成的破壞有時相當巨大，有時更是不可補救。要防範這些問題，必定要妥善安裝防病毒軟件等的保護軟件。

清除資料

印有敏感資料的文件，在丟棄前須先行碎掉。同樣地，把便攜式裝置棄掉或給予他人前，也必須先行清除內裏的資料。用戶應建立良好的習慣，當便攜式裝置內的資料無須再使用時，便立即把資料清除。利用便攜式裝置作資料備份更需要有適當的實體保護作配合。

加密內容

資料加密，是利用加密匙把文件轉換成一種不能解讀的形式儲存，是保護資料的有效措施。萬一已加密的資料意外地遺失，如沒有解密匙，任何人都無法讀取儲存的資料。加密匙愈長，保護能力便愈強。



就儲存於便攜式電子裝置內的機密資料，要確保加密保護有效，一定要使用足夠長度的加密匙。加密匙一定要保密，且必須由資料擁有者持有。加密匙很多時候是儲存於安全裝置內，例如附有密碼保護的智能卡。

結語

總括來說，用戶應知道使用便攜式電子裝置有一定的安全風險。用戶必須評估風險，並採取適當的保護措施。如果經過評估後，確定存有高風險，而用戶對保護措施是否足夠存疑，便應放棄使用這些裝置。