# 社交媒體工具你要識

# 第三堂 保安設定

# 視像文字稿

保安設定

這個單元裡，我們會介紹社交媒體及即時通訊軟件的保安設定。

社交媒體與即時通訊軟件的保安

社交媒體及即時通訊軟件為我們日常生活帶來很多便利，可以讓我們隨時隨地聯繫親友和分享自己的見聞，但我們同時亦會在這些工具內，留下不少數碼腳印甚至個人資料。我們用這些工具的時候，一定要提高警覺，採取防禦措施，才能夠避免帳戶被人盜用，或洩漏個人資料，不讓不法分子有機可乘。

保障個人帳戶安全

首先，記住、記住、記住，千萬不要打開一些覺得可疑的網頁連結及附件檔案。第二就是要使用安全度高的密碼，至於怎樣才是安全度高的密碼？例如不要用你的手提電話號碼、生日日期、身份證號碼，又或者容易讓人猜到的密碼，都應避免用。最好不要用與其他網站或者服務一樣的密碼。究竟為何呢？因為如果在其中一個平台的密碼洩漏了，就很容易會讓人登入其他平台的帳戶，而且千萬不要與人分享你個人帳戶的登入資料。最後還要記著更新瀏覽器至最新版本，而且要定時更新防毒軟件。把瀏覽器更新到最新的版本可以堵塞漏洞，防止黑客入侵你的裝置，而定時更新防毒軟件，可以令到你的防毒軟件有最新的病毒資料，預防電腦病毒的入侵。

一般社交媒體的注意事項

接著與大家講講用社交媒體的時候要注意的事項。首先，不要接受陌生人的交友邀請，因為陌生人一旦成為你社交媒體上的朋友，就有機會拿到你的個人檔案、照片、社交活動記錄等等的資料，這些資料就可能會作非法的用途，例如假冒你的身份四處騙人。另外，不要在個人檔案入面披露過多或者敏感的個人資料，好像：地址、電話、身份證號碼、信用卡號碼等等，記住，在個人檔案披露越多資料，這些資料洩露予陌生人的風險就會越高。

雙重驗證

雙重驗證是指在登入帳戶的時候，除了需要輸入原有密碼之外，還需要輸入另外的驗證碼來驗證身份。如果啟用雙重驗證，在輸入密碼之後，系統會自動產生驗證碼，這個驗證碼會傳送到指定的地方，例如你的電子郵箱、SMS 短訊等等，打開這個訊息後，再輸入訊息中的驗證碼就可以成功登入。

雙重驗證的驗證碼在一段時間後，就會失效。所以，即使不法分子取得你原本的密碼，都會因為沒有有效的驗證碼而無法登入。如果你正在用的社交媒體及即時通訊軟件，有提供雙重驗證的功能，就應該開啟。同一時間，你們都要小心現在常見的認證碼詐騙，如果不是在登入的時候，突然收到驗證碼訊息，就代表很有可能有不法分子正在嘗試登入你的帳號，這個時候就千萬不要提供驗證碼給任何人了。

關於社交媒體及即時通訊軟件的保安設定介紹就來到這裡，多謝大家收看。再見！
本教材由屯輝長者學苑提供內容及製作。