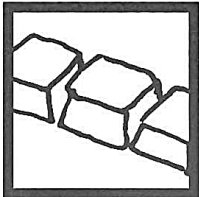
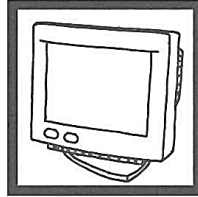


網上私隱十大自保攻略

科技令人們的生活得以改善，科技的潮流只會一路向前邁進，而步伐越來越快，電腦和互聯網被喻為上世紀的最偉大發明之一。互聯網開創了廣闊平台，將知識和數據分享，在任何角落發生的事物，跨越地域界限，打破時空限制，呈現在眼前。可是，一小撮害群之馬，破壞了原意和秩序，製造麻煩。

記得三年前的寒冬，突然在網上傳出大量女藝人艷照，成為各大傳媒的頭條，很多人在網上搜尋和互傳這些影像，喚醒了大眾對資訊保安的關注，這好像是個別事件，但電腦如此普及的情況下，這隨時會發生在自己身上，這絕不是危言聳聽。



當的設定，加強互聯網保安，免遭不必要的損失。

1. 瀏覽器的選擇

瀏覽器是進入互聯網世界的軟件之一，其重要性常被忽略，市面上有五種流行的瀏覽器，分別是微軟的IE、Firefox（火狐）、谷歌的Chrome、蘋果的Safari和Opera。很多用戶和香港特區政府仍用IE6，微軟早已停止支援，有潛在風險。最近的功能測試顯示，Chrome 10 測試版排名第一，Opera 10.63 緊隨其後，火狐排第三，儘管IE9在多方面進行了改進，它卻排在最後一位。雖然可用測試分數定優劣，對於用戶來說，選擇一款快捷、易用和安全的瀏覽器

是最重要的。Chrome和火狐運行速度比IE9快，在保安方面，微軟的ActiveX功能，容易被駭客利用，將有害程式隱藏。Chrome和火狐不支持ActiveX插件，有效防止不良程式和攔截彈跳新頁，較安全，Chrome和火狐比IE快很多，下載大檔案更明顯，而且越來越流行。不講不知，在一台電腦可安裝多款瀏覽器，不會干擾或影響電腦運作。為了安全，最好盡快轉用火狐或Chrome，可從以下網站免費下載。<http://www.mozillaonline.com/>，<http://www.google.com/chrome/>

2. 電子郵件

電子郵件是常用的軟件，也是通訊的主要渠道。電子郵件分為兩大類，POP及 web mail（網上郵箱）。POP需要安裝用戶端，例如：微軟的Outlook Express, Thunderbird（雷鳥），Lotus Notes等等。相信很多人採用Outlook Express，但微軟早在2004停止更新和支援，有漏洞和隱患存在，風險高，萬一電腦有任何故障，或者舊電腦退役，新電腦不支援Outlook Express，多年的電郵紀錄和地址簿可能盡失，應盡快升級或改用其他安全的用戶端。雷鳥是開放源碼的郵件用戶端，2005年面世，不斷改良和堵塞漏洞，非常易用和穩定，安裝時可

資訊保安，人人有責

近月網站「維基解密」不斷公開各國的國防及外交機密檔案，造成極大震撼和尷尬，香港政府已制訂全面的資訊保安規例和指引給各部門，政府資訊科技總監辦公室上月已提醒各部門保持警覺，一部份用戶也成為驚弓之鳥，對互聯網、雲端運算等，望而生畏。

實際上，使用電腦及互聯網其實可以十分安全，否則網上銀行及關鍵性服務早就關閉。現在銀行、政府和商業機構都鼓勵網上交易和網上服務，從而降低交易成本。互聯網的發展只會持續，不會停滯或倒退，請勿因噎忘食。各國政府制訂資訊保安規例和指引，這只能減少人為疏忽，若在技術層面多加防範，就更有效。要維持互聯網上秩序，單靠警察捉賊是不足夠的，若全民皆兵，不良份子就無所遁形。

學會自保免煩惱

很多人對電腦和互聯網的認識不夠深入，警覺性低，出事後損失慘重，悔之已晚。坐以待斃不如自學和自保，以下有十點簡易方法，讓互聯網用戶對網上保安加深理解。筆者所推介的大部份是開源的免費軟件和在軟件作出適

自動將Outlook, Outlook Express的郵件，地址簿等遷移入新軟件，有垃圾郵件過濾器，讓你收發信件更快、更安全，也更簡單。下載連結是<http://www.mozilla.com/en-US/>

網上郵箱有Gmail, Yahoo Mail, Hotmail等免費郵箱，無需下載，無需安裝，隨時隨地，任何電腦可使用，這些郵箱都有強大的防電腦病毒功能，十分方便易用，越來越普及。Gmail有提供郵件備份功能，讓用戶將郵件儲存。

3. 加密USB記憶棒

醫管局曾多次遺失存有病人紀錄的USB記憶棒，洩露病人私隱，惹來很多指責。若預先將數據加密，才存放在USB記憶棒，即使遺失了，病人紀錄也不致外洩。網上也有很多加密軟件，而限於安裝了軟件的某台電腦，使用時不方便。市面上的USB記憶棒，較優質的上千元，平價的靠不住。筆者發現香港郵局推出了新的加密USB記憶棒，4GB儲存容量，內附加加密軟件，和個人電子證書，隨時隨地加密、解密，十分安全兼方便，只售\$100，是政府部門、工商界和市民的恩物，詳情可訪問這網站或往附近郵局洽購。<http://www.ecerts.hk/hk/>

4. 簽署和加密電郵

當收到一份電郵，只可憑發件人的電郵地址識別，不法之徒可假冒電郵地址，發出電郵行騙。香港政府已有指引，所有機密電郵，必要用電子證書簽署和加密，即使「維基解密」截取到電郵也無法破解密碼，避免洩密。

加密電郵不是政府專用，香港郵政署早於2003年成立公匙基建系統和香港郵政核證機關，讓廣大香港市民安心使用互聯網，大部份香港身份證都植入電子證書，若仍未裝或過期，三個步驟便可，這就可心安理得。

採用香港郵政核證機關的電子證書，在電郵簽署，讓你的商貿伙伴知道你的真正身份，無需猜疑，當人人都這樣做，不用電子證書可能是騙徒，這就天下太平，人人放心！<http://www.ecerts.hk/shop/>

5. 誠信網站

網頁提供大量資訊，近年網上商店越來越普及，令不法之徒



有機可乘，騙取金錢或毀約，而事後很難舉證，歹徒逍遙法外。產品有Q嘜，網站有無類似的核實標徵？香港郵政核證機關根據電子交易條例第553章獲認可的核證機關。香港郵政署根據電子交易條例及作業守則發出電子核證證書，確保安全電子商務。香港郵政電子核證（伺服器）SSL證書，以安全接層(SSL)訊息進行溝通，將所有數據加密。同時可以安裝誠信標徵，瀏覽者一眼就知這是誠信網站。最重要是萬一這些商戶有詐騙行為，這些交易紀錄可成為有力證據，將騙徒繩之於法。若採用其他SSL證書，未必能受香港電子交易條例保障。

6. 網上付款的漏洞

香港每年由於網上詐騙導致的直接損失達140萬港元。透過互聯網或電郵，偽裝成信譽的公司，騙得用戶姓名、密碼和信用卡等個人資料，作犯罪行為。這些電郵都聲稱（自己）來自於流行的社交網站（YouTube、Facebook）、拍賣網站（eBay）、網上銀行、電子支付網站（PayPal），以此來誘騙受害人的輕信。即使網站安全，若只靠帳號和固定密碼，因為這不能證明用戶的真正身份，容易被盜用，事後無法追究責任。若大家留意當登入網上銀行，網址自動轉為https，這代表採用加密方式傳遞數據和指令，在過數前會用二重核實身份(two-factor authentication)，是安全可靠的。

7. Facebook私隱設定

Facebook是全球流量之冠的社交網站，擁有五億用戶和他們的個人資料，一不小心，禍及朋友。希望安心用Facebook，請留意以下幾點：

7.1 Facebook是以你的電郵為帳號，密碼是自設，盡量不要貪方便，採用你原本的電郵密碼作為Facebook的密碼。

7.2 大部份忠實市民用實名註冊帳戶，有些心懷不軌之徒，可能用匿名，若收到交友邀請，先核實相片和資料，無照片或有懷疑就不應確認為朋友。

7.3 可在Facebook設定自己的私隱取向，你可讓所有人、朋友的朋友或只限於朋友，最安全是只限朋友分享，請參看下圖。



7.4 而你上載的相片也可限制那些人可以看，最安全是只限朋友分享。



7.5 有些Facebook內的程式，彈出授權請求，要小心閱讀及了解內容，若不肯定，不要隨便同意，最好是離開。



8. 超連結的陷阱

在2004年6月的一次調查中發現，500名美國西點軍校學員收到匿名電子郵件，有80%被騙並洩露個人資料。在郵件或網頁有問題的超連結，是近日常見的陷阱，不要急於按超連結，請將滑鼠移至超連結上，留意字面和連結，有懷疑就盡快離開並千萬不要繼續，寧殺錯也不要放過。

9. 自定安全密碼

網上的操作，大部份只靠用戶帳號和密碼，系統就認為操作者就是合法用戶。實際上，由於許多用戶為了避免忘記密碼，經常採用生日、電話號碼等有意義的字串作為密碼，這樣很容易被破解。為確保安全，密碼最小是8至12位，當中包括數目字、英文字母大小寫和符號，而每三個月轉換一次。

10. 善用公開密碼匙基礎建設，令大家更安心

公開密碼匙基礎建設技術類似銀行的保險箱，每個箱有兩條鎖匙，公共匙由銀行保管，另一條私匙自己保管，兩條匙才可打開保險箱。在數碼世界，公開密碼匙廣泛流傳，私人密碼匙祇有其擁有者才知。若使用密碼匙加密訊息，祇有使用與之相配的另一個密碼匙方能解密。電子證書加私人密碼，有四項功能，可證明身份、電子簽署、加密、解密等功能，可作網上交易、轉帳、簽署等。香港的電子交易條例第553章保障公開密碼匙基礎建設的法律效用。公開密碼匙在手，網上安全不用愁！詳情可參考香港郵政電子核證網 http://www.hongkongpost.gov.hk/support/faq/index_c.html#B1

以上是一些簡單技巧，容易掌握，希望大家使用互聯網時，不要掉以輕心，不要嫌麻煩，才對自己有保障，輕輕鬆鬆享受互聯網的優勢。

簡錦源
香港Linux商會主席