

請上鎖

如何保障個人互聯網隱私



互聯網可以讓個人和家庭隨時隨地使用電腦或是移動設備的來進行社交、購物、理財、工作及娛樂。利用互聯網將會令你受惠良多，而且在多數情況下，上網是安全的。因為幾乎所有公司都十分重視保護用戶的隱私及安全，而且會使用最新科技保障消費者的網上安全。

網上安全及隱私是大家的共同責任。要達到一定程度的隱私和安全性，各位電腦及移動設備用戶就應該運用相關常識並善加利用各種保安工具來保護自己，包括使用大公司如谷歌(Google)和微軟(Microsoft)所提供的免費網絡安全工具。如果你能積極參與維護網絡安全，就有可能安然無恙地享受數碼生活。

鎖好你的帳號

科技在不斷地進步，不斷為你提供好方法去阻止他人進入你的帳戶盜取你的資料。從網上理財到社交網站，許多需要處理個人敏感資料的網站均提供各種安全措施來保障用戶資料安全及避免遭人窺視。採用一個強而有力的密碼對於保護個人資料安全是很有幫助的，而使用雙重認證的方式來驗證用戶身分就更加理想。

密碼保護：密碼是第一道安全保護線，也是保障帳戶安全最為廣泛使用的方法。以下幾點提示你應該怎樣做才可以有效地保障你帳戶的安全。

◆ 設定一個至少有八個字符，而且以字母、數字以及符號隨意混搭組合的密碼。學習如何設定強而有力的密碼，



可瀏覽這幾個網頁：谷歌(bit.ly/1MoNVfk)，微軟(bit.ly/1JnLHbp)或 ConnectSafely (bit.ly/1Kyu2i2)。有的網站還能幫你創造一個密碼，例如 PasswordsGenerator.net 就能提供類似協助。

◆ 妥善收藏好你的密碼。與其要把所有的密碼寫下來，不如用一個密碼儲存工具收錄起所有的密碼，這樣的話你就只需要記住一個密碼就行。學習如何管理個人密碼，請至：PCMag.com (bit.ly/10tbirr) 和 Lifehacker (bit.ly/1QXEc1b)。

◆ 你如有多個帳戶，應給每個帳戶設定不同密碼。有必要時就要更換密碼，例如，當有人已經了解你的密碼時或者當市面上出現大量個人資料被他人洩露時（即資料爆光或是大量用戶的資料被盜）。

◆ 在選擇安全問答題時，應選用那些只有你才知道答案的問題。注意不要選用他人容易發現答案的問題，例如“你母親的原來姓氏是什麼？”或“你家中寵物叫什麼名？”（當你忘記密碼，或是用你帳戶無法識別的電腦和移動設備去登入帳戶時，某些帳戶可能會要求你回答預設的安全問題以確認你的身分）。

◆ 當你完成之後，要記得退出帳戶(log out)。如果你與他人共用一台電腦的話，千萬不要把你的登入密碼資料儲存在瀏覽器裡。（當瀏覽器提示你留存密碼，你應選擇不要，即點擊“Not Now”，“Never for this site”等類似選項。也可以在瀏覽器設置或選項中，取選適合的安全度和密碼，取消同步及自動填表等選項）。

◆ 啟動或喚醒你的電腦時必須使用密碼。這樣設置提供更多一層保護，防止其他人用你的電腦進入你的網上帳戶。想了解蘋果電腦的相關設置可上網查閱(apple.co/1V9p5Yt)，如使用PC電腦可瀏覽(abt.cm/1Wiy72s)。（你也應在自己的移動設備上，設定要求用密碼、個人代號“PIN”或是拇指指紋來開啟）。

雙重認證(2FA)：這比只使用一個密碼的保護程度更強。它需要兩種驗證才能有登錄進入帳戶（例如，使用密碼並認證屏幕顯示的圖片是你的設置所選用的圖片，或者一個密碼外加指紋掃描，或是一個密碼外加一個通過短訊或電郵發送給你的驗證號碼），這就像你在雜貨店刷記賬卡時還需要鍵入個人驗證碼PIN一樣。如想查詢更多雙重認證資訊，請瀏覽 Stop.Think.Connect 網站(bit.ly/1DQlzpY)。

只要有可能，你應盡可能選用有雙重驗證。雖然不是所有網站都有這種保障設置，但已有很多公司網站包括Google,Apple,Facebook,Twitter和Paypal等都有這種服務。你可上網至bit.ly/1JpGz6w查看他們所列出的許多提供2FA服務或不提供2FA服務的公司名單。（如果你使用的網站不提供2FA雙重驗證，你可以要求他們提供）。每個網站都各有其說明，教你怎樣啟動其2FA雙重驗證。你應先在設置選項(Settings)里查找一下，如果無法找到，可聯絡該網站的技術部門。

保障網上交易及移動設備交易的安全

網上購物和網上理財可以讓你省錢又省時，這是讓你參與數字化理財和消費的兩個最主要的原因。只要採取一些簡單而有效的預防措施，就可以保障你自己帳戶的安全，就像你保護自己的錢包一樣。請放心，有很多強而有力的安全工具已經可以供你使用。

資訊加密：這是一種資訊科技，將通過網絡空間傳送出去的電子信息進行混淆（加密），從而使得黑客很難追蹤他人的活動或者盜取你傳出的資訊。

若想確定你所瀏覽的網站是否在你和網站之間互動時，有加密服務保護個人資料安全，可先查看網址(URL)上有沒有一個代表安全(Secure)的“s”字母(是https://而不是http://)。有時你也可能會見到一把鎖的標誌，或見到網址一欄轉成綠色，這都表示你進入了安全的網站。在進行任何網上購物、網上理財或交易之前，一定先看清楚該網站有沒有顯示出上面所談到的一兩個安全標誌。

請注意,有些常用電郵或短訊是沒有任何加密設施的，所以不要通過電郵或短信發送你的帳戶號碼、社安卡號或其他切身重要敏感資訊。

如果你家中有設定無線上網(Wi-Fi)，你會有一個無限網絡的路由器(router)。當你通過無線網絡進入互聯網時，為了防止附近有人能進入你的網絡盜取你的資訊，你必須先啟動路由器的加密功能（一般路由器是沒有啟動其加密功能的）。同時給路由器設定一個強而有力的網路密碼（含有至少14個雜亂混合的字母及符號），以防止網路入侵者在你Wi-Fi訊號範圍內進入你的無線網路。OnGuardOnline.gov為你提供如何保護個人無線網路安全資料，請瀏覽(1.usa.gov/1G2Eiya)。

因為你很難保證外面的網絡有加密措施，所以出門在外時做網上購物或理財，最安全的方法就是使用你的無線運營商(wireless carrier)的上網服務，而非公共場所的無線網絡。如果你需要使用他人的電腦或通訊設備上網，一旦完成網上購物或理財就一定要記得退出(log out)帳戶以免有人在你離開後進入你的戶口。聯邦交易委員會(FTC)提供公共無線網路安全使用詳情，可至(1.usa.gov/1L62Nlr)。

防火牆：大多數電腦操作系統都有預置一道防火牆，這是一道在你的電腦和外界之間的安全屏障。可是這道預置的

防火牆功能常常沒被「啟用」。你應查看你電腦的安全設置選項(通常列在Preferences)以確定防火牆已被啟用。如果你實在無法找到你電腦的安全設置，可以上網尋找相關指示，用firewall（即防火牆）和你電腦操作系統名這兩個字作網上搜索。

移動設備的安全

智能手機或平板電腦可以讓你隨時隨地上互聯網，並享受其所有的功能。雖然移動設備攜帶輕便四處能用，給用戶提供十足便利，但在隱私及安全方面它們卻有其獨特隱患。這不是說你要放棄享用移動設備，只是在使用時多加一些不同的步驟就可以保障你的隱私和你的個人資料了。

保護你的移動設備：由於它們可隨身攜帶，移動設備比電腦更容宜被丟或被盜，故風險較高。除了要好好看緊自己的隨身設備，你也可以利用相關的高科技工具來保障移動設備及其內含資料的安全。

首先，設定一個密碼或個人代碼來鎖上自己的設備（有的型號可用指紋認證作密碼）。設定移動設備閒置數分鐘後就自動上鎖的功能。同時，註冊加入對移動設備遙控的服務，這類科技可遠程定位你的設備並上鎖刪除內含資料，例如蘋果機的Find My iPhone或是安卓機的Android Device Manager。這樣可以在你忘記了將它放在哪裡時，用該服務幫你找回它，或是在遺失被盜時，用該服務遙控上鎖或刪除其中個人資料。

在你出售、捐贈或丟棄你的移動設備時，不要忘記“洗淨”設備里的所有資料，這樣就不會有人能拿到你的個人資料了。CTIA無線通訊設備聯盟的網站bit.ly/1jeEDZN為大家提供了多種提示，針對每一種移動設備解釋應如何清除其中的所有資料。

要了解更多有關如何保障你手機的網路安全，可至AARP網站(bit.ly/1FfksoF)。

應用程式(Apps)：這是一種特別為移動設備而設計的應用軟件。許多智能手機及平板電腦的各項功能均來源於下載的應用程式，它們可以讓你追蹤個人健身情況，分享自拍照，通告朋友們你正在哪裡用餐，監控你投資的走勢，玩網上遊戲等等。你應確保這些功能強大的軟件時時為你服務，而不是和你對抗。

◆ 篩選你的應用程式。只從有信譽的機構下載各類應用程式。詳讀用戶們的評語，在下載前確認軟件設計者的合法性的。



◆ 將應用程式的隱私設置選項定在你認可的範圍內。很多應用程式的功能完全依賴於收集並分發用戶的個人資料，例如地址本內親朋的聯繫資料，用戶日曆里的日程安排以及用戶目前身在何處。如想控制某應用程式對你的資料收集和分享，就要檢查並適當設定該應用程式的設置（而非移動設備的設置）。如果該應用程式想收集的資料遠超出你覺得舒適的範圍，請不要下載它。如果該應用程式有隱私政策，你應先研讀核實。如果它沒有隱私政策，就應考慮選用其他的應用程式。

◆ 應避免使用公布個人所在地點的應用程式，或關閉該功能（在有可能時）。與陌生人分享自己目前身在何方，可能造成家中被打劫的風險或是使得個人安全及隱私受到連累。（有些應用程式，例如地圖和指路的程式，它們是以你的定位來提供服務，但不會向外界公布你的行蹤）。

◆ 軟件一旦有升級版就需要立即更新，以確保你常用最新版本的應用程式。

◆ 仔細閱讀應用程式的使用或隱私政策更改通知，如果它的用戶資料收集分享計劃超過你所能接受的範圍，你可以將它刪除。取決於每個應用程式內部規定或是否有較大的升級，你有可能會收到直接通知（通常是來自電郵或從應用程式本身發出的推送通知）。而在其他情況下，你唯一可能發現規定改變的方法就是重新瀏覽應用程式的說明欄目或到其相關網站查看。

安全無慮使用社交媒體

對很多人來說，使用社交媒體是日常生活的一部分。分享可以是一件好事，如果你只和自己選擇的網友分享你希望公布的信息內容。在你上網貼文、推文甚至是發布個人資料之前，一定要深思，才可避免可能過度分享的後果，也可以使用一些配備的工具來控制他人的能見範圍。

保留個人隱私：使用社交媒體的人並非全部都是心存善念的。如能做一個聰明的選擇，決定你想分享什麼以及和誰分享，這是非常重要的，如此你的個人資料就不會被用在意料之外的地方了。

首先調整社交媒體的隱私範圍設定，以配合自己感覺舒適的程度：從不與任何人分享開始，到只與自己選擇的朋友分享，直到與全民大眾分享。做法是，先登錄進入你的帳戶，然後找尋類似以下這些字標去更改分享設定：Privacy（隱私）Privacy Controls（隱私控制）Privacy Settings（隱私設置）Account Settings（帳戶設置）或 Preferences（設置選項）。如果你無法找到這些設置標誌，可以到“Help”功能求助，或是電郵給該網站的技術支持人員。

請勿分享個人資料，例如你的全名、地址、電話號碼、母親姓氏或是出生年月，這些資料可用來認證你的身分（或盜用你的身分）。同時不要公布你目前所在地點和你的旅行計劃，這可能會為你本人或你的財產帶來傷害和風險。

一個好的做法是，不接受任何不認識人士的邀請或“加我為友”請求。

消費者行動的社區教育刊物Privacy and Control for Social Media Users（社交媒體用戶的隱私和控制）里提供了更多的相關詳情，請瀏覽 (bit.ly/1xPC8PO)。

保護你的網上信譽：你和他人分享的所有相片、視頻、活動、見解，都能顯示你的為人。善加管理並保護你的電子口碑與形像才能使你免於難堪，同時避免由於一時忽略做錯而留下不良後果。以下是一些“良策”可以幫你避免社交媒體的不佳後果。

◆ 每當你和他人分享時，應考慮你的雇主、招聘人員、大學招生部、貸款公司、房東、顧客客戶、政府機構、保險公司或者其他做決定的人會不會因此對你有看法。你要明白，很多不認識你的人將會去社交媒體里去打聽了解你。

◆ 請小心，一個所謂網上的“朋友”是可以將你以為只分給少數自選網友的資料重新貼文、推文或做其他爆光動作的。而且，你若是在他人的帳戶牆面貼文，你就無法掌控誰會看到你的貼文了。

◆ 如有必要，可撤下已分享的內容。有些社交網站可以讓
你刪除貼文、清除相片、改換可看此文的
網友等等，這樣你以前所分享的一些內容
就不會讓以後的觀望者看到了。（當然，
對那些已經看到了你所分享的事情，你就
無法去改正了。）

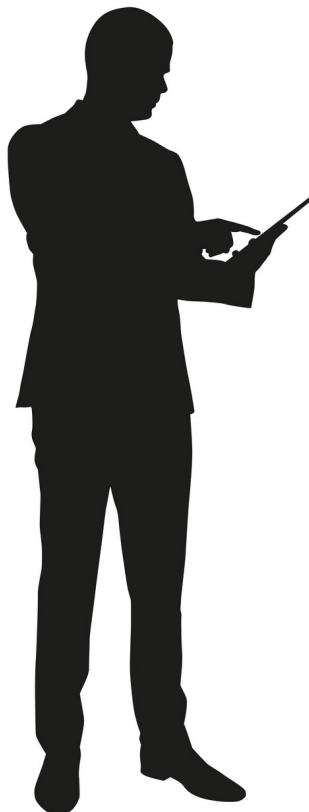
◆ 你可以用Google谷歌去查一下，看看自己的名下有何網上記錄。如有不好的網上記載，可請求貼文者刪除那些有你在內的不良相片、視頻或貼文。

◆ 你應確保你網上各帳戶的安全，防止他人侵入你的帳戶並用其中內容去傷害你。

如需查詢更多有關如何善加處理個人網上信譽資料，可至谷歌安全中心網站 (bit.ly/1FunANI)。

親子型網站

互聯網不僅向成年人，同時也為各個年齡的孩子提供豐富及高品質的網上資料。為了能確保你全家可以好好享用互聯網的最佳服務，同時又能避免任何不受歡迎的內容，以下這些保護措施和告誡提醒可幫你採取行動保障安全。



阻止不適當的內容：網上有許多很好的適宜兒童年齡的網站和內容。但也有一些兒童不宜的內容。許多內容分發公司，包括寬頻服務公司和各種社交媒體網站，都讓家長在各方面能對子女做出安全限制，例如限制上網時間，可瀏覽的網站，能觀看的視頻，可參加的留言板和聊天室等等。

家庭在線安全協會 (bit.ly/1L63Emf) 及 谷歌安全中心 (bit.ly/1G2F7XP) 均提供很多有關家長控制子女網絡安全提示。

監視網上交流：不是所有的網絡內容都適合兒童觀看，同樣，社交網站上的人們也不會都為你的子女著想。身為父母，你是自己子女在網絡社交互動中，最主要的把關者。

家長應和子女談談網上安全及責任。定下清楚規則，限制子女可以瀏覽哪些網站以及聯繫哪些人。在網上和自己的子女做“朋友”，確認你能看到他們在社交網站上與他人分享什麼，同時其他人又向你的子女分享什麼。一定要交代他們任何時候都不可以跟網上“相遇”的人單獨見面。還要承諾，在子女告訴你有不適當的網上交流時，不會處罰他們，也不會禁止他們上網。查詢相關小提示可至：OnGuardOnline.gov (<http://bit.ly/2eewAI>)。

向有關法制或管制部門舉報任何網上騷擾威脅掠奪等劣行，管制部門包括學校行政人員，當地警察或網絡報警站 CyberTipline (bit.ly/1NMIQDY 或電話 800-843-5678)。

避免煩人的市場推銷：許多網絡公司搜集用戶的個人資料。有些公司用那些資料來定製並增進用戶的網上經驗，例如根據愛好而建議用戶看什麼電影或書籍；有些公司則利用該資料來設計廣告推銷訊息以便吸引有相似興趣的客戶。同時還有另一些人，也叫數據經紀商，會收集客戶的資料然後銷售給第三方營銷公司或別的公司，用來做有針對性的目標廣告及促銷。有信譽的公司會採取公開透明的方式讓用戶知道他們將如何使用客戶的資料，同時他們也會讓用戶決定並選擇哪些資料公司可分享或哪些應為客戶保密隱私。

學習以下各項要點，了解你的資料可能會如何被使用，而你如何才能更好的掌控你的個人資料。

◆ 詳細閱讀網絡公司的Privacy Policy（隱私安全規定）或Data Use Policy（數據資料使用規定），了解他們是如何收集、使用及分發用戶個人資料的。如果你不滿意該公司的做法，可以另找一家為你提供更多控制權的網站。

◆ 如果家有幼童，教導他們不要在上網瀏覽時洩露任何敏感資料。兒童網絡隱私保護法(COPPA)規定每個網站在收集或使用13歲以下兒童的個人資料時必須得到家長同意。如有違規，可向聯邦交易委員會(FTC)舉報(www.ftccomplaintassistant.gov 或電話 1-877-382-4357)。

◆ 在需要時可以啟動瀏覽器上的 Private browsing（隱密瀏覽）功能，它可以使你在網上瀏覽時避免瀏覽器儲存記

住你看過哪些網站或網頁，你也可以使用彈出窗口阻止程序(pop-up blocker)來避免打開不受欢迎的廣告視窗。（不過要留意，這個阻止程序也有可能擋掉一些你想要的功能，例如零售網站會因此無法記住你的購物車Cart里加了什麼物品。）

◆ 你要考慮清楚是否應提供多一點資料。尤其是在沒有特別好的理由下，如果你被要求提供基本資料以外的個人資料（通常基本資料用星星記號注明）才可註冊或使用網站的服務。你應盡可能只給最基本的個人資料。

◆ 要明白，在任何時候你交出個人資料給未經審核的對方，哪怕只是回答一些看來不起眼合法的小問答或參加一個遊戲節目，你的個人資料都可能會意想不到的被他人使用。

高科技對不斷為人們在通訊、工作、學習、創造、分享和娛樂各方面提供日新月異的改進。你不能錯過，但要小心面對謹慎使用。大家共同努力來保護自己及家庭在網絡世界中平安無憂。■



關於消費者行動

www.consumer-action.org

消費者行動藉由多種語言消費者教育材料、社區外展及為特定時間的權益代言，多年來未全國弱勢消費者強化他們在商業市場上的權益及提升財務狀況。

消費者如有投訴，可致電消費者行動的建議及轉介熱線：（中文請按“2”）。網上投訴，請至：http://www.consumer-action.org/hotline/complaint_form or 415-777-9635。

熱線諮詢專員以中文、英文及西班牙文回電。

本刊物由消費者行動製作出版Google（谷歌）贊助發行

© Consumer Action 2015