

# 保障網上私隱須知 — 互聯網個人用戶指引

目錄

引言

第一步 - 準備在網上瀏覽

第二步 - 上網前先作系統設定

第三步 - 網上瀏覽時應注意的事項

第四步 - 網上瀏覽後應採取的措施

## 引言

國際電腦聯網(Internet)(下稱互聯網)發展一日千里,讓網上用戶輕易取得大量的資訊。隨著網絡資訊容量與日俱增,公眾人士也可享有愈來愈多的服務及資訊。毫無疑問,互聯網將不斷改善通訊、教育、商業、政府服務以至現代生活的每個環節,並開創煥然一新的局面。但創新網上科技帶來了顯著的個人私隱問題,這包括用戶在網上消閒尋樂、搜尋資料、購買貨品或訂購服務時,他們在個人資料的收集、使用及保安方面所面對的問題。用戶特別關注到其個人資料在他們不知情的情況下被收集,或是被網上闖入者截取,並使用這些資料進行欺詐活動等違背用戶意願的用途,例如編製個人檔案,可能對個人資料私隱構成威脅。由於我們在使用網絡服務前,或在透過當中載有機密資料的電子郵件與對方通訊時,往往需提供個人資料,因此,上述有關個人私隱方面的問題也隨之而生。

在香港的機構方面,《個人資料(私隱)條例》(下稱條例)賦予公眾人士可享有以下的私隱權:

確保他人以合法及公平的方式收集你的個人資料,並需通知你有關資料的使用目的;

在你的同意下方可更改資料的用途;

確保對方所保留的資料是準確和最新的,並且用穩妥的方法保存而保留期間亦不得超乎實際需要;

可向資料使用者索取你的個人資料複本,並有權要求對方更改不正確的個人資料;

確實資料使用者的個人資料政策及使用方法。

這份指引旨在加強網上個人用戶對保障個人資料的意識,並藉著提醒用戶採取預防措施,以助保障個人私隱。

## 第一步 - 準備在網上瀏覽

### 檢查項目

你的互聯網服務供應商(ISP)關注你的私隱權嗎?

### 建議

=> 查詢互聯網服務供應商在處理個人資料方面所採取的政策及方法。你所選擇的互聯網服務供應商應以積極的態度保障個人資料私隱。當你詢問有關其保障私隱的政策及方法時,它應提供詳盡的資料。你可在滿意後才選用該互聯網服務供應商。

你已清楚互聯網服務供應商使用「用戶瀏覽紀錄」(clicktrails)的政策嗎?

### 建議

=> 詢問你的互聯網服務供應商如何使用你的「用戶瀏覽紀錄」資料。互聯網服務供應商可藉著查閱其服務器的電腦紀錄檔案(log files),以得悉你曾到訪的網頁。這些資料稱為「用戶瀏覽紀錄」,一般只作系統保養及故障檢修方面的用途。互聯網服務供應商不得使用這些資料作其他用途,例如在未得你的同意下把資料作市場調查用途。

你是否採用最新的瀏覽器(browser)?

### 建議

=> 使用最新的正版瀏覽器軟件。現今瀏覽器軟件的保安科技不斷改良,你應使用最新的版

本，務求享用最新的保障科技，確保私隱及個人資料得到保障。

## 第二步 - 上網前先作系統設定

### 檢查項目

你的私人密碼(password)安全嗎？

#### 建議

- ⇒ 選用較難猜度的密碼。上網及電子郵件(下稱電郵)系統的密碼是個人私隱的第一道防線。用戶應使用沒跡可尋的密碼，一個可取的做法是採用由數字及大小階英文字母混合而成的密碼。
- => 經常更改私人密碼。要求互聯網服務供應商在初次開立帳戶後更改密碼，並於日後經常更改密碼。
- => 設定不會自動輸入私人密碼的電郵程式。當別人取得你的密碼後便很容易偽造郵件。為了避免這情況發生，應設定不會自動輸入私人密碼的電郵程式。

你是否設定瀏覽器接受「曲奇」(cookies)檔案前徵求你的同意？

#### 建議

- => 在瀏覽器設定接收「曲奇」(cookies)檔案的功能選項(option)，讓系統每次均需徵詢你的同意，才可接收「曲奇」檔案。「曲奇」是你每次到訪網頁時可能會儲進電腦的小檔案，讓你再次到訪同一網頁時毋須再次登記。不過，這功能也可用以記錄你感關注的事項。如你曾填寫網上表格，你的個人興趣便可連同你的名字記錄在案，並可能被編成你的個人檔案(profile)，假以時日其仔細程度可教人驚訝。
- =>使用「無名氏曲奇」軟件。你可用「曲奇」(cookies)一詞在網絡上尋找有關軟件，其用途是可避免你的電腦儲存任何「曲奇」檔案或避免他人取閱你的「曲奇」檔案，從而保障你的私隱。

你是否設定了瀏覽器，提示你已進入保安範圍？

#### 建議

- => 在瀏覽器上設定功能選項(option)，在你每次進入及離開保安範圍時發出提示。名為「sniffers」的特別程式可監察網上的訊息傳遞，並可辨認有機會被記錄或濫用的特別數字組合，例如信用咭號碼。瀏覽器可發出提示，讓你決定在當時的情況下是否透過互聯網傳送敏感的資料。
- => 檢查瀏覽器視窗是否設有保密連接符號。大部分負責任的網址在索取保密資料時均會自動將資料加密(encryption)。例如瀏覽器視窗上端的位址的開端出現https://而非http://，或於瀏覽器屏幕底部出現完整的鑰匙或已關閉的鎖，則所有傳送至該網址的訊息均會經過編碼處理。經編碼後的訊息較難辨認，因此可加強保密程度。你只應在信用咭號碼及其他敏感性個人資料會用編碼的形式發送的情況下傳送你的信用咭號碼及其他敏感性資料。

## 第三步 - 網上瀏覽時應注意的事項

## 檢查項目

對方是否要求你在網上提供你的個人資料？

### 建議

=> 如要透過網上表格或電子郵件傳送個人資料，應於按下「呈交」(submit) 按鈕前採取以下行動：

你了解索取你的個人資料一方的身分嗎？

### 建議

=> 瞭解網址的詳細背景。一些網址可能會虛報電郵地址，用戶應到訪「機構資料」(About the Organisation) 網頁，瞭解其背景資料，例如名稱、公司地址及聯絡電話 / 傳真號碼。

=> 瞭解網址的保障私隱政策。向對方提供個人資料前，應先了解對方處理這些資料的政策，以策安全。條例規定所有在香港的機構均須公開其處理個人資料的政策及方法。

你知道自己的個人資料會用於甚麼目的嗎？

### 建議

=> 在網址內尋找「收集個人資料聲明」告示。「收集個人資料聲明」告示是用來告知用戶其個人資料會用於甚麼用途、個人資料可能被移轉給其他人士的身分、用戶可索取個人資料複本及更正資料的權利，以及尋求上述服務的聯絡人的名字。根據條例的規定，香港的機構在收集個人資料時或收集資料之前，必須提供以上資料。

對方有否要求你提供與收集目的無關的個人資料？

### 建議

=> 避免提供與收集目的無關的過多個人資料。檢查要求提供個人資料的網上表格，分辨必要及非必要的填報項目。在網上填寫求職、抽獎、徵友、賭博、網上信用咭及其他服務等申請表時，如發現對方索取過多的個人資料，必須提高警覺。當你登記進入某個網址時，如對方要求提供不相關的個人資料，也應加倍小心。不妨考慮以公司地址代替住址，或於地址欄上註明有關資料僅可用於指定用途等。

你所提供的資料屬信用咭號碼或身分證號碼等敏感性資料嗎？

### 建議

=> 視網上通訊並非私人通訊。除非你採取預防措施，否則互聯網上的保安能力是非常薄弱的。你應確定網頁已採用安全的傳輸方式，才考慮傳送敏感的個人資料，你可設定瀏覽器提示何時進入或離開保安通訊範圍。(請參閱上一節「上網前先作系統設定」)

=> 在網上使用信用咭付帳時應採取預防措施。你的信用咭號碼是敏感性的個人資料。你在網提供信用咭號碼購物前，可考慮使用現金或支票等傳統付款方式，以及考慮賣方有否提供一個安全的環境讓你傳輸你的信用咭號碼，例如在傳輸時將信用咭號碼加密，以減少可能在保安方面出現的問題。另一做法是使用商業中介人服務，授權中介人從你的信用咭帳戶付帳，從而避免在網上傳輸你的信用咭號碼。如欲查閱有關服務的詳情，你可使用關鍵詞「網

上信用咭付款」(INTERNET CREDIT CARD PAYMENT)在互聯網上搜尋有關資料。

=> 切勿輕易把身分證號碼告訴別人。很多機構往往要求進入其網頁的用戶提供身分證號碼，例如當你登記使用其服務時。然而，卻非所有機構均有提出這種要求的合理或合法依據。

你的電子郵件是否載有你或他人的敏感性個人資料？

#### *建議*

=> 考慮使用私隱保障軟件替電子郵件加密。未經加密的一般電子郵件可輕易被人截取或竊讀。加密程式可把訊息或檔案編成密碼，除了擁有解碼軟件的接收人外，任何人包括截取者都難以閱讀電郵內容。如有需要保障郵件的完整性，不妨採用用戶身分核實技術。你可使用關鍵詞「網上加密」(INTERNET ENCRYPTION)在互聯網上搜尋進一步資料。

=> 考慮使用私隱保障技術隱匿身分。你可以使用「匿名轉交郵件人」(ANONYMOUS RE-MAILER)，以匿名者的身分在互聯網上收發電子郵件。這「匿名轉交郵件人」擔當中介人的角色，讓通訊雙方在交換郵件時隱匿真正的電郵地址。如你信任「匿名轉交郵件人」，這是一種保障私隱的重要方法。如你需要以完全匿名的方式傳輸資料，則可使用多重轉交郵件服務。你可使用關鍵詞「網上匿名」(INTERNET ANONYMITY)，在互聯網上搜尋這些保障技術的進一步資料。

你會在搜尋網址 (search sites)、新聞組(newsgroups) 或網上論壇(chat areas) 上提供個人資料嗎？

#### *建議*

=> 提供個人資料時應三思而行。當你採用常用搜尋器及登記自己的姓名時，應考慮到每次搜尋資料時所查詢的內容均可能被記錄在你的個人興趣名單之內，並逐步將你的姓名、聯絡資料、特別愛好等資料累積成你的個人檔案。

=> 揭露他人的個人資料前應先考慮別人的私隱。新聞組(newsgroups)與網上論壇(chat areas)均可讓多名網上用戶即時對話。但參與這類公開討論時，你所提供的個人或他人資料均會被公開並且長時間可讓所有參與者參閱。此外，其他人亦可藉著這些互聯網址提供的服務，搜尋及顯示你在新聞組上的訊息。根據條例的規定，你有責任不向第三者披露別人的個人資料(透過新聞組或網上論壇)，除非你是因有關使用目的而獲提供該等資料，或當事人事先已自動給予明確同意。

你會讓子女瀏覽網頁嗎？

#### *建議*

⇒ 指導子女正確使用互聯網。兒童在網上特別容易被侵犯私隱。他們可能以為是直接跟網址上的卡通人物談話。這些網上卡通人物往往以誘人的獎品向兒童取得有關其個人及家庭方面的資料，令你可能會收到促銷郵件或電郵廣告，甚至出現更糟的濫用情況。你應教導子女在未經你的准許前切勿向他人提供個人資料；此外，也應確保他們對保障私隱方面有所認識，並於最初幾次網上瀏覽時從旁督導。

你對於寄給你的直銷郵件感到厭煩嗎？

### **建議**

=> 要求直銷商停止向你寄發宣傳郵件。根據條例的規定，向你進行直接促銷的本港機構有責任讓你作出拒絕服務選擇，以後不再與該等機構有直接接觸。此規定讓你有權要求直銷商停止滋擾你。

=> 採取預防措施，以免收到自來的宣傳用途的電子郵件。為減低自己成為促銷對象的機會，你應該避免申請免費電郵服務「白頁」或電郵目錄服務。假如你採用載有簽署檔案(signature file)的電子郵件，該檔案不應載有無關的個人資料，以免被直銷商取得有關資料，令你成為促銷對象。

## **第四步 - 網上瀏覽後應採取的措施**

### **檢查項目**

你是否與別人共用電腦？

### **建議**

=> 立刻中斷網絡接駁。如別人可使用你的電腦、你的密碼易被猜中，或是你在網上瀏覽後而沒有中斷線路的情況下將電腦置之不理，他人便可輕易利用你的電郵地址而假冒你的身分。

=> 清理電郵文件夾(folders)。電子郵件不僅在傳送期間容易被截取，它們還會長時間留在收發的地點。如別人可使用你的電腦，你應養成經常清理電郵文件夾的習慣，並隨即清理「垃圾」(Trash)文件夾，因為這些文件夾跟其他未經保護的個人資料一樣容易被竊讀。

你是否知道及擔心自己的電腦會記錄你的網上瀏覽活動？

### **建議**

⇒ 避免在你的電腦留下上網痕跡。上網時電腦不僅可短暫記錄你曾到訪的網頁，更可記錄網頁的內容。如認為此舉可威脅你的個人私隱，你可使用瀏覽器軟件的功能選項清除電腦的暫存資料，包括「高速緩衝存儲器」(cache)、「瀏覽路徑」(followed links)及「歷史」(history)等，也可經常刪除這些區域內的無用資料。

## **總結**

=> 網上保安能力是十分薄弱的。用戶每次使用網絡時均須提高警覺，保障個人私隱。

=> 每次在網絡上消閒尋樂、搜尋資料、購買貨品或享用服務時，若對方要求你提供個人資料，應在按下「呈交」按鈕或傳輸訊息前先考慮其對個人私隱所造成的潛在威脅。

=> 在香港的機構方面，《個人資料(私隱)條例》保障你的個人資料私隱。不過，為本身的利益著想，你也應採取適當及「實際可行」的預防措施，在這些機構及在與你透過互聯網互有往來的海外機構方面，盡量減少對個人資料私隱造成的威脅。

=> 若你對《個人資料(私隱)條例》所賦予的私隱權利有任何疑問，請向個人資料私隱專員公署查詢詳情。

*(本指引所載的資料只作一般參考用途，並未就《個人資料(私隱)條例》的應用提供詳盡指引。讀者如欲得知*

條例的詳細內容，請直接參閱條例。]