網上安全

www.aoema.org

感到網上世界
不安全?

這本指引可助你
提升「網上安全」。

內容包括:

做做兩分鐘
「網上安全」測驗,
防患未然。

特別刊載dot.com詐騙、
網上黑客、特洛伊木馬及
其他互聯網陷阱等
重要資料。

網上安全

目錄

互聯網現已成為廿一世紀的重要溝通工具。目前全球網民超過三億人，互聯網可說掀起了一場通訊革命。它改變了人與人之間的關係，也改變了我們周遭的環境。現在，我們可以接觸到過去遙不可及的人物、地方及資訊。企業及政府精簡運作、祖父母與身在地球另一面的孫兒保持聯繫、學生與遠在外太空的太空人溝通 — 這些目標全部透過互聯網逐一實現。互聯網已經無處不在，充分滲透了生活各個層面。互聯網確實在改變我們的生活模式。

不過，對於網上這個新領域，你可能有些擔心。我們時常聽到病毒、特洛伊木馬、侵犯私隱、客戶保障不足、「dot.com詐騙」，甚至一些叫「網上臭蟲」的東西 — 這些問題不禁令人擔憂。可是，這就是未來的發展大勢，要完全漠視網上世界越來越困難。對付這些潛在問題的最好方法，就是學會怎樣**防止**這些問題發生。

這本小冊子是為初學者及經驗豐富的互聯網用戶而編寫的實用指引，旨在幫助大家加強「網上安全」意識，以免誤墮網上欺詐的陷阱。凡事都有風險，世上沒有百分百安全的事。只要我們花一點點時間，了解這些網上「壞蛋」有甚麼技倆，然後做好預防措施，就可以大大減低網上交易的風險。上網可以很富趣味，只要你按照這本小冊子的簡單指示，自可**防患未然**。

簡介

基本上我們要考慮四個問題：

怎樣才能確保我的電腦安全呢？

怎樣才可以保護我的個人資料呢？

我怎樣才能信賴網上交易呢？

我怎樣才可避開網上的煩擾、陷阱和詐騙呢？

這本小冊子旨在以簡明方法解答這些重要問題，內容不會過於專門，或者糾纏於繁瑣的細節，以免你越看越困惑。本小冊子共分24個課題，按照所針對的問題編排，包含一系列值得注意的保安問題。每個課題都會先說明潛在問題，然後闡述建議的預防步驟，並且提供參考網站，方便你得到進一步援助或更深入探討有關課題。

如欲了解所有課題的進一步資料及最新內容，包括亞太經合組織(Asia-Pacific Economic Cooperation (APEC))個別經濟體系的特定參考資料，請參閱**www.aoema.org/safetynet**。

4

兩分鐘「網上安全」測驗

	是	否	
你的系統是否已安裝抗電腦病毒軟件?	☐	☐	參閱第32頁
你是否知道你擁有的抗電腦病毒軟件是最新版本?	☐	☐	參閱第32頁
你是否已選擇「自動更新」病毒定義檔?	☐	☐	參閱第32頁
在過去七日內,你是否已下載新的病毒定義檔?	☐	☐	參閱第32頁
你的系統是否已安裝個人防火牆?	☐	☐	參閱第12頁
你是否擁有最新版本的防火牆軟件程式?	☐	☐	參閱第12頁
當你沒有上網的時候,是否會「中斷」網絡連線?	☐	☐	參閱第12頁
你的密碼是否由數字、大寫及小寫字母組成?	☐	☐	參閱第23頁
在過去30日內,你是否曾經更改密碼?	☐	☐	參閱第23頁
不用紙筆寫下來的話,你是否可以記住自己的密碼?	☐	☐	參閱第23頁
你所用的操作系統軟件、瀏覽器、電郵及所有應用系統程式是否都是最新版本?	☐	☐	參閱第27頁
你是否已在所有有提供「自動更新」選項的程式中選擇自動更新?	☐	☐	參閱第27頁
你是否知道自己的瀏覽器用了甚麼Cookies程式設定?	☐	☐	參閱第10頁

做做這個兩分鐘「網上安全」測驗,防患未然。

暫時沒有遇到問題?一切事情都在你掌握之中?很有可能是這樣,但我們還是建議你至少做做這個兩分鐘「網上安全」測驗,看看你是否已經採取所有重要的保安措施。

對於上述任何一個問題,如果你的答案是「否」的話,我們十分建議你參閱表內提及的頁數,加深對有關課題的認識。

網上安全

課題及建議行動

怎樣才能確保我的電腦安全呢？	參閱：
我怎樣阻止黑客進入我的電腦系統？	防火牆 第12頁
我怎樣保護孩子免受色情物品及仇恨網站的危害？	監測 第19頁
使用我家小狗的名字作密碼有甚麼不妥？它很容易記啊。	密碼 第23頁
為甚麼我不需要那些電腦軟件的新功能，還要將它們更新至最新版本呢？	軟件 第27頁
是不是真的可以透過把程式裝進我的系統，來破壞我的電腦或者給其他人帶來麻煩呢？	特洛伊木馬 第31頁
我怎樣阻止病毒入侵我的電腦？	病毒 第32頁

答案在哪裏

怎樣才可以保護我的個人資料呢？	參閱：
我怎樣阻止網站取得我電腦內的個人資料呢？	Cookies程式 第10頁
在聊天室交朋友及交換資訊安全嗎？	聊天室 第14頁
我怎樣阻止商業機構擅自使用我的個人資料？	私隱 第24頁
當我在圖書館或網吧等公眾地方上網時應該怎樣保護自己？	公用接入 第25頁
我非常討厭垃圾郵件。它們真的會危害安全嗎？	濫發電郵 第28頁
是不是真的有可以潛入電腦的「間諜」程式？	間諜軟件 第30頁

參閱：

我怎樣才能信賴網上交易呢？

參閱：

我怎樣才可避開網上的煩擾、陷阱和詐騙呢？

8

消費者的保護 (Consumer Protection)

消費者的保護

專業騙徒可謂無處不在。因此，消費者在購物時必須時刻警惕留神。不論親身或在網上購物，均應該緊記「買者自負」這句古老的拉丁文警語。由於大多數人還未試過在網上購物，因此對於未知之數或多或少會感到害怕。正如在現實世界購物一樣，消費者應該小心謹慎，具備應有的常識。

參考以下的建議行動，在網上購物前做好準備。

如需協助或獲取更多資料，請瀏覽：

www.econsumer.gov

www.bbbonline.org

建議行動

- 尋找並閱讀網站上的政策聲明，包括網站上刊載有關個人資料私隱、消費者滿意程度及退貨程序，以及金融交易安全性的聲明。
- 確保網上表格是安全可靠的。
- 拒絕不必要的Cookies程式。
- 使用安全的瀏覽器，並確保它是來自製造商的最新版本。
- 確保自己清楚了解有關公司的付運及退款政策。
- 如果網站有「常見問題」部分，最好先看一遍，以便了解有關公司如何與消費者進行交易。
- 除了完成交易所需的資料外，切勿透露其他個人資料。除非你滿意網站刊載的政策及程序，以及肯定你的個人資料將會透過安全的連結傳送，否則不要向網站提供任何個人資料。
- 切勿透過互聯網或電話向任何人透露密碼。
- 切記保留網上交易記錄。如果你質疑信用卡月結單上的收費，便可能需要查看這些資料。
- 檢查信用卡及銀行月結單，看看是否有錯誤或有人未經授權購物。有問題的話，應立即通知適當的金融機構。
- 如果你認為任何公司所作出的聲稱很難令人相信，就要小心提防。它多半不是聲譽良好的公司。
- 設法了解你所接觸的公司。老實的公司做生意向來「光明磊落」：他們會清楚說明如何與你進行交易；如果你透過電郵向他們提出有關政策聲明或常見問題部分未有涵蓋的問題，他們一般都會樂意解答。
- 確保網站清楚列明購物條款及條件，包括有沒有存貨、付運方法、價格、可能由消費者承擔的額外費用、退貨及退款政策、保證及擔保。
- 要用信用卡，不要使用銀行扣賬卡。使用後者時，會立即從你的銀行戶口中扣除金額，以致很難處理有爭議的支出。
- 小心那些消費者評級的網站，因為它們很多都不老實。
- 最重要的是查明你所在地實施的消費者保障法例，以便了解你的消費者權利。不同地區的消費者保障法例之間會有很大差別。

如果碰到問題的話：

- 聯絡有關公司，討論怎樣解決問題。
- 如果無法達成協議，則聯絡你所在地的消費者團體。
- 如果有關公司參加像BBBOnline之類的認可計劃，則聯絡計劃的管理人。
- 諮詢你的信用卡公司。

Cookies 程式

COOKIES程式

Cookies程式的主要目的是識別用戶，以便為消費者度身訂做符合他們需求的網頁。有些網站會問你一些特定的問題，然後透過網絡瀏覽器將你的答案儲存在「Cookies程式」中，以備日後使用。而有些網站則會直接記錄你在網站上的一舉一動，並建立一個反映你上網及購物習慣的Cookies程式。當你下次再瀏覽這個網站時，它會查看你電腦上的Cookies程式，並利用裏面的資料為你建立個人化的網頁。例如，你的名字可能會出現在歡迎畫面上，而網站亦可能會翻查你的購物記錄，找出你可能有興趣的產品，並且提供折扣優惠。一般來說，Cookies程式能夠增添上網樂趣，你亦不必擔心信譽良好的公司使用Cookies程式。可是，有些公司卻利用所謂的「第三方Cookies程式」，這一點就不得不防了。

「第三方Cookies程式」並非來自你瀏覽的網站，而是來自一班廣告商。他們往往希望了解你的興趣及喜好，從而找出最適合你的廣告。這些廣告公司喜歡在你每次瀏覽網站時展示新廣告，而Cookies程式則有助它們取得你的瀏覽記錄。這類Cookies程式在未經許可的情況下強裝至你的瀏覽器上，帶來許多自動彈出的廣告畫面。這些廣告都是不請自來，你亦多半不會對它們感興趣。雖然「第三方Cookies程式」不會損害你的系統，但它卻會造成侵擾，也著實令人討厭。

建議行動

現時，Cookies程式是可以控制的。你可以免費下載程式來解決這個麻煩問題。請參考下文所列的網站。

要查出一家公司是否在利用Cookies程式，以及它怎樣使用從Cookies程式中收集得到的資料，最簡單的方法是查看他們網站上的政策聲明。今時今日，信譽良好的網上業務公司會誠實地向消費者說明他們如何使用Cookies程式，以及發表政策聲明解釋他們的用意。如果他們在網站上沒有披露這類資料，你在跟這業務實體進行交易前就必須三思。

記得檢查瀏覽器內的Cookies程式設定。以微軟Internet Explorer為例，方法是進入「工具」選項單，再選擇「網際網路選項」，然後在「隱私」一欄內選擇最符合你需求的設定。

此外，亦要定期刪除網際網路暫存檔(temporary Internet files)(參考瀏覽器上的「說明」選項單)。

如需協助或獲取更多資料，請瀏覽：

www.cookiecentral.com

www.lavasoft.de

數碼簽署 (Digital Signatures)

數碼簽署

對於寫在紙張上的文件，我們能夠利用手寫簽署表示同意、接納或承諾。許多人擔心在電子世界沒有那麼方便。不過，數碼簽署不但可以做到這一點，更能夠帶來更多好處。

不要把「數碼簽署」與「電子簽署 (electronic signature)」及「數碼化簽署 (digitized signature)」混淆了。「電子簽署」包含多種形式，最簡單的就是在電郵結尾打上姓名。「數碼化簽署」其實是你手寫簽署的電子圖像，即是在紙張上簽名後再掃描入電腦。雖然它看起來像你的簽署，但在電子文件中並不具有法律約束力。

數碼簽署是由複雜的數學公式產生，秘訣在於所謂的「配對密碼匙(key pair)」。「配對密碼匙」的一部分是私人的，用於以數碼方式進行簽署。這個密碼匙絕對不可以向任何人透露。「配對密碼匙」的另一部分是公開的，用於核實某個人或實體的簽署。公開密碼匙可以從網上資料庫獲取，或透過電郵寄給有關方。

但你會問，如何知道私人密碼匙確實屬於該使用人？

密碼匙會由受信任的第三方核實。該第三方會在密碼匙上加簽，以示信納密碼匙的確屬於有關人士。這個過程稱為核證 (certification)。公開密碼匙附有一份證書 (certificate)。當一組受信任的第三方共同核實多個身份時，則稱為公開密碼匙基礎建設 (Public Key Infrastructure) 或公匙基建 (PKI)。

為方便理解，我們試舉護照作為例子。當申請護照時，你必須提供一張相片及超過一份文件以核實你的身份。你的政府然後核實相中人是否與你是同一人，而且是有效的。然後，你會獲發一本可以證明你身份的護照（證書）。其他政府相信你的政府已經做了核實工作，因此接納你的身份。護照可以偽造，證書亦同樣可以偽冒。不過，由於發生機會甚低，你不大可能遇到這種問題。

發送私人信息前，你必須用接收者的公開密碼匙加密。公開密碼匙與私人密碼匙配對在一起，收件者才可以解密及閱讀信息。運用「配對密碼匙」方法，除非擁有私人密碼匙，否則無人可以閱讀加密信息。因此，保護你的私人密碼匙極為重要。

數碼簽署其實很複雜，這裡僅作基本介紹。如果想了解更多詳情及相關技術，請參考下列網站。

請勿向任何人透露你的私人密碼匙。

如需協助或獲取更多資料，請瀏覽：

www.apectelwg.org/apecdata/telwg/eaTG/crypto.html

http://searchsecurity.techtarget.com

防火牆 (Firewalls)

防火牆

利用「個人防火牆」，你可以保護電腦免受黑客及不想要的程式入侵。

你可能覺得你的電腦沒有甚麼好窺探或偷取的，因此毋需使用防火牆。然而，黑客入侵你的電腦的理由可能有很多，例如：

破壞 (VANDALISM)— 獲取你的重要檔案，並可能破壞你的系統；

盜竊 (THEFT)— 盜取你的賬戶資料及密碼，或者出動「間諜軟件」冒充你的身份；

操縱 (MANIPULATION)— 使用你的電腦向其他電腦發動攻擊或濫發郵件。

黑客不用知道你的系統或密碼。他們可以用軟件任意掃描互聯網，尋找進入電腦的開放「埠」或缺口。如果你的電腦由於任何原因存在開放的埠，黑客便可以獲取你電腦上的數據，或從你的電腦向其他電腦濫發郵件，令你的互聯網地址受到堵截。防火牆可以保護你免受上述威脅，並確保系統在連接互聯網時運作暢順。防火牆還可以阻擋無用的cookies程式及彈出式廣告，防止他人在你不知情時把程式植入你的電腦。

防火牆有兩類。一類是硬體式防火牆，最適合內部網絡（家用或商用電腦網絡）。而另一類防火牆則透過在一個獨立的電腦上安裝軟件而建立，可監測所有進出互聯網的信號。

不用上網時，最好「中斷」互聯網連線（對寬頻用戶來說尤其重要）。

建議行動

現今，所有接達互聯網的電腦都應該使用防火牆。防火牆並非可有可無，亦跟使用互聯網的頻密程度無關。不論你是偶然或整天上網，同樣有機會被黑客用任意掃描的方式選中。既然互聯網上有多個有效的免費程式可供下載，就沒有藉口不安裝防火牆。下列網站提供這類防火牆軟件，以及有關防火牆技術的其他資訊。

如需協助或獲取更多資料，請瀏覽：

www.zonelabs.com

www.symantec.com

www.sygate.com

身份盜竊

身份盜竊及身份詐騙(identity fraud)是指非法獲取及使用他人的個人資料，而又在某程度上涉及詐騙或欺詐的各種罪行。這些罪行通常以獲取經濟利益為目的。雖然這類罪行在現實生活及網上都會發生，但由於人們越來越多在網上收集、保存及獲取個人資料，令人不禁擔心更容易受到這類罪行的侵害。

身份盜竊 (Identity Theft)

身份盜竊足以對受害人造成可怕的後果，因此應該加以正視。如果有人冒充你的身份，就可以破壞你的信用記錄，以及因未經授權使用你的信用卡而令你負債累累，甚至令你被控犯下與你無關的罪行。身份盜竊不但會破壞你的良好聲譽，你還要花費大量時間及金錢彌補損失。鑒於這類問題後果嚴重，最好及早採取預防措施，否則待問題發生時才處理便為時已晚。

建議行動

既然無論在現實或網上世界中都會發生這類罪行，就應該隨時採取下列預防措施：

1 從安全角度而言，某些個人資料比其他資料更為重要。例如，在美國，社會安全福利號碼(Social Security Number (SSN))普遍用於證明個人身份，而且在進入安全網站或用電話向銀行或其他金融機構查詢賬戶資料時，第一樣要提供的資料便是社會安全福利號碼。其他重要的資料包括母親的本姓、駕駛執照號碼，以及任何被視為最私人也最安全的其他身份證明。

2 在網上及現實世界中，都要注意保護銀行賬戶資料及銀行月結單。

3 盡可能保護你的信用卡賬戶。當你將信用卡交給他人處理時，應保持警惕。如果你打算使用信用卡在網上購物，應事先檢查有關網站有否充足的安全保障以進行財務交易。取消過去六個月內未動用的賬戶亦是明智之舉，因為罪犯往往以開設後而不使用的賬戶為目標。

4 在使用提款卡時應保持警惕，慎防身旁的人看到你的個人密碼。

5 確保所有賬戶均有不易破解的密碼，並且經常更換密碼。

6 經常檢查你的銀行及信用卡月結單，留意是否有任何不尋常的活動。

如需協助或獲取更多資料，請瀏覽：

www.idtheftcenter.org
www.privacyrights.org/identity.htm
www.consumer.gov/idtheft/

即時通訊、聊天室(CHAT ROOMS)及檔案共用

在互聯網上進行實時溝通或「聊天」有多種方式。透過網站聊天是最簡單的方式，所需的只是一個瀏覽器。而如果要使用互聯網線上聊天系統 (Instant Relay Chat (IRC))，你就需要購買或下載一個特定的套裝軟件，讓你可以加入已經建立的「聊天頻道(chat channels)」或討論組。利用即時通訊，你可以建立一個朋友或同事名單，讓你知道誰在上網。如果名單上的人與你同時在上網，你可以向對方發送信息，而對方亦會即時收到。

直接經由檔案擁有人的電腦提取檔案，從而實現檔案共用。這類應用程式的風險包括：

- 檔案共用軟件配置不當，令互聯網上任何人都可以接達你的電腦；
- 違反版權法例。為避免侵犯版權，必須取得版權擁有人的許可。

14

即時通訊等 (Instant Messaging, etc.)

越來越多的公司將即時通訊用於內部及外部通訊。現在，兩名或以上的員工可以在網上舉行會議。許多公司亦採用即時通訊與供應商及客戶進行有效的溝通。即時通訊已經成為大小企業的有效通訊工具。而另一方面，聊天室似乎變成了青年人的天地。如果不採取預防措施保護你的電腦及個人資料，兩種網上實時通訊方式都有潛在的保安風險。因此，請採納本節的建議，以及重溫載於聯機滋擾、監測、防火牆及病毒各部分的建議措施。

「檔案共用」是現時另一種在互聯網上廣泛使用的應用程式。不同的檔案共用方式存在不同的保安風險，但都有可能無意中暴露電腦內部分或全部的檔案，令網上黑客有機可乘。忽視這些保安風險的話，便會危害你的個人或財務資料，亦會導致電腦遭受破壞。「點對點檔案共用(Peer-to-peer File Sharing)」是今時今日非常普遍的一種檔案共享方式。透過Kazaa、Morpheus及LimeWire等程式，人們可以

建議行動

- 經常更新防毒系統，並確保已安裝防火牆。
- 小心安裝檔案共用軟件。除了自己願意分享的檔案外，不要把其他檔案設為共用。
- 千萬不要在聊天室內透露個人資料。
- 注意共用檔案所牽涉的版權問題。
- 請留意，在互聯網上，這個領域是公開的，而且經常受到監察。

如需協助或獲取更多資料，請瀏覽：

www.icq.com/support/security/

www.cert.org

知識產權

世上充滿人類的創意及發明。我們吃飯用的餐盤、掛在牆上欣賞的畫、腳下人手製作的地毯、雪櫃、電話、我們聆聽的音樂、以致我們閱讀的書籍，都是人類所創造，而且全部都被視為知識產權。

要好好理解知識產權這個概念，你只須打開雪櫃。你會發現各種牌子的食品，每款都一定有熟悉的生產商「商標(trademark)」或標誌(logo)。受市場推廣手法及廣告影響，公司商標已經司空見慣，它們往往影響我們的購物習慣。

由於商標的市場推廣能力強大，各間公司都會盡可能保護其品牌，並防止商標侵權行為。如果我們再打開雪櫃，看看各式各樣的容器及特別包裝（例如罐頭、真空包裝、紙盒及密封包裝），我們會發現各項容器外形的註冊設計，以及包裝生產、品牌商標及

標誌的專利。雪櫃本身就有多項專利，包括冷凍機組、擱物架及其他部件。甚至連說明書都受版權保護，因為它是原創的文本。

由於互聯網已經在主流社會中大行其道，越來越多人關注到在網上未經授權散播知識產權的行為（包括電影、藝術形式、音樂、相片、書籍及軟件）。作為網上資料的用戶或提供者，你有責任了解這些問題，知道所有國家的適用知識產權法律，以及對國際知識產權公約有一般了解。

在把你的網站與其他網站連接前，應該尋求有關方面的許可，以避免侵犯其他網站的商標或版權。一些經常引發糾紛的地方包括：濫用meta標籤、廣告橫額、視框及未經授權深層連結。

知識產權 (Intellectual Property Rights)

建議行動

請注意，侵犯他人或公司知識產權的行為會受到**嚴厲**懲處。侵犯版權行為包括未經許可使用圖片、剽竊他人的作品及點對點共用音樂檔案等。鑑於了解問題的重要性，請務必參考下列網站。

如需協助或獲取更多資料，請瀏覽：

www.wipo.int
www.apecipeg.org

互聯網誘騙轉接（或脅持調解器(MODEM HIJACKING)）

甚麼叫互聯網誘騙轉接？互聯網誘騙轉接在世界各地有不同的叫法，是指你電腦裏的某個程式切斷原有的網絡連接，改撥另一個號碼（例如國際長途號碼或「收費服務」號碼）。受害人往往並不知情，直至在電話賬單上發現莫名其妙的收費時，才知道被人「誘騙轉接」了。

建議行動

要避免誤墮這類詐騙行為：

- 留意孩子或員工（任何可能使用你電腦的人）的活動，確保他們並沒有同意這類網站上的條款及條件。
- 調高調解器的音量，以便在電腦重新撥號時，可以聽到重撥訊號。

16

互聯網誘騙轉接 (Internet Dumping)

互聯網誘騙轉接是如何發生的呢？在互聯網上有些缺德的公司，其中大部分是「成人」網站，這些網站會設法誘騙用戶同意改用另一個號碼瀏覽其網站，而這個號碼其實是要額外收費的。網站會指示新用戶下載一個叫「瀏覽器(viewer)」的特別軟件，用作瀏覽有關網站，而下載前用戶必須接受一系列的條款，當中包括同意透過另一個電話號碼接達該網站。這些條款及條件往往用特別方法顯示，令你無法完全了解所有條件，更不知道會轉用另一個號碼。此外，所謂「瀏覽器」其實是經過特別設計的程式，專門用來改撥收費號碼，令你被徵收驚人的電話費。

可惜，許多人就這樣糊里糊塗地墮入騙局。由於他們在下載軟件時已明確同意網站提出的條款及條件，故必須支付不合理的電話費。受害人往往追討費用不果，唯有乖乖掏腰包。

- 長時間保留瀏覽器中的「記錄」，以便追查可能引致問題的網站。
- 你可以聯絡電訊供應商，禁止透過你的數據線撥打國際長途號碼或「1-900」等「收費」號碼。
- 如果你有意進入「成人」網站，在點擊「OK」或「YES」之前，請小心閱讀及了解所有同意事項。

如需協助或獲取更多資料，請瀏覽：

www.tio.com.au/FAQ/int_dumping.htm

10 條款寬鬆的擔保貸款或信貸 — 透過濫發電郵提供無抵押房屋貸款及信用卡。事實上，正當的金融機構都不會用這種方式經營業務。

11 修補信用 — 宣稱可以刪除負面信用記錄，讓你有資格申請信用卡、貸款或工作。如果你遵循當中的建議，便會觸犯詐騙罪。

12 旅遊大獎宣傳 —「你剛剛贏得精彩的旅遊大獎」或「你已獲選參加精彩的旅遊套餐計劃」。你會發現事實並非如你想像，又或者必須支付先前並無提及的額外費用。

互聯網詐騙

現時，互聯網上不幸地出現許多詐騙行為。根據美國消費者提交的投訴，聯邦貿易專員公署(Federal Trade Commission)舉出下列12種值得警惕的最常見詐騙：

1 商機 — 毋須辛勤工作或投資大量資金，便可賺取巨額收入。它們大部分屬非法金字塔計劃 (pyramid schemes)。

2 大量電郵 — 提供長長的電郵地址清單，讓你宣傳自己的產品或服務。其實大部分互聯網服務供應商都不允許用戶發送大量電郵或濫發郵件，而你的電郵地址亦會因此被關閉。

3 連鎖信(Chain Letters) — 你向清單上的四至五位人士各自寄出一筆小額款項，並以自己姓名代替其中一位人士。連鎖信作法由來已久，但透過電郵或郵政局寄發則屬違法行為。

4 在家工作計劃(Work-at-home Schemes) — 輕鬆工作，穩定收入。例如，「摺好一本小冊子再裝入信封，每次可賺取兩美元」。可是，當你交了初期費用及按要求完成工作後，卻永遠不會獲得承諾的款項。

5 健康及節食詐騙 — 現今許多詐騙透過電郵傳播，氾濫電郵信箱，最常見的有藥丸、草藥配方、性無能及脫髮療法等。這些行騙伎倆所推銷的物品根本並無什麼效用，只會令你白白浪費金錢。

6 不勞而獲 — 這些所謂的快速致富計劃(get-rich-quick schemes) 都不可行。

7 免費商品 — 先是繳交一筆小額入會費加入俱樂部，再招募其他人士加入以獲取贈品。可是你繳費後卻永遠不會收到贈品。

8 投資機會 — 承諾高回報，零風險。通常，這類計劃由於缺乏妥當的資金來源，根本無法支付任何類型的投資回報。其聲明及統計數字大部分都是謊言。

9 有線電視解碼器零件(Cable De-scrambler Kits) — 花少許金錢購買一套零件，讓你裝配一部有線電視解碼器，免費收看有線電視。這些玩意都無法運作。即使能夠運作，使用它們亦屬違法行為。

互聯網詐騙 (Internet Scams)

建議行動

天下沒有免費的午餐。凡事如果聽來好得令人不敢相信，那就千萬不要信以為真。切勿被花巧的廣告所蒙騙，並切記許多這類詐騙最終可能會令你遭受刑事檢控。聯邦貿易專員公署網站及其他類似網站致力讓消費者了解互聯網上最新的詐騙手法，請熟讀這些網站的內容。

如需協助或獲取更多資料，請瀏覽：

www.ftc.gov

www.crimes-of-persuasion.com

法律問題

互聯網屬全球性資源，但各國有關互聯網活動的監管法律卻各不相同。部分行為在全球均屬違法，例如兒童色情或黑客入侵電腦等。而其他行為，例如賭博或仇恨網站，則只在部分地區允許。

止。同時切記，現實世界的商業監管法律，例如合約法、產品責任及廣告等，也適用於網上世界。互聯網正逐步成為正式的商貿場所，故此應遵照實行多年的法律及慣例。互聯網並非「西部荒野」，亦非「毫無法紀的邊疆」。你應該了解網上的法律限制，並且加以遵守。

法律問題 (Legal Issues)

以下行為在全球許多地區均屬違法：

- 賭博；
- 購買軍火；
- 買賣藥物（包括配方藥物及違禁藥物）及其他醫療物資；
- 針對特定種族、宗教及少數民族等的仇恨網站；
- 各種色情內容；
- 為信息加密，以致政府在需要／必要時無法解讀；
- 黑客入侵；
- 盜版軟件；
- 編寫及散播病毒軟件；
- 「拒絕服務」攻擊，令他人無法接達某些網站；
- 截取通訊；
- 惡意作出關於自己的失實陳述，以取得經濟利益（包括身份盜竊）；
- 金字塔及邦斯計劃(Pyramid and Ponzi Schemes)。

首先要記得的是，凡是在現實世界違法或禁止的行為，在網上世界也同樣違法或禁

建議行動

在互聯網上出售貨品前，請向你所在地政府的國際貿易部門查詢，確保你打算出售的貨品並無受到限制。

在國際網站上購物前，可事先向有關政府部門查詢，確保並無違反任何限制或規例。

如需協助或獲取更多資料，請瀏覽：

www.eclip.org

www.bmck.com/ecommerce/

www.gipiproject.org/

www.ilpf.org

www.uncitral.org

www.cybercrime.gov

監測互聯網的使用

監測僱員使用互聯網：互聯網已成為當今工作場所中非常有用的商業工具，同時也容易分散工作注意力。監測僱員如何使用互聯網，已成為管理人員工作不可或缺的一部分。為了維持工作效率，及保障公司避免不必要的法律訴訟，應該了解今時今日不同業務所面對的大小問題，並制訂主動的策略。

監測家人使用互聯網：互聯網為家庭成員提供許多學習機會及富建設性的娛樂節目。此外，更有助個人成長。然而，亦有家長擔心孩子進入那些他們認為不良的網站。雖然互聯網基本上對兒童大有裨益，但網上有些地方仍然是兒童不宜，正如幾乎每個城市都有不適合兒童的場所。此外，互聯網上的某些活動可能對成人來說是恰當，但對兒童則不然。而有些地方則只適合部分兒童。

監測互聯網的使用 (Monitor Internet Usage)

建議行動

商用：在制訂政策及相關指引時，應涵蓋下列各項：

- 制訂書面政策，禁止僱員利用公司電腦寄發個人電郵或瀏覽不良網站。
- 清楚說明公司的電腦資源不容浪費，只限用於許可的商業用途。
- 加入關於電郵措詞及內容的指引。
- 使用監測軟件來規管互聯網政策有否確實執行。
- 僱員透過持續進修來執行互聯網政策。

家用：家長所面對的難題，是除了自己學習如何安全使用互聯網之餘，更要教導兒童有關知識。家長可以利用審查及過濾軟件來監測兒童使用互聯網的情況。以下是一些入門網站。

如需協助或獲取更多資料，請瀏覽：

商用	家用
www.email-policy.com	www.getnetwise.org/
www.epolicyinstitute.com	www.wiredpatrol.org/
www.fatline.com	www.childnet-int.org/

建議行動

如果你本人或公司遭遇網上誹謗：

- 保持冷靜，不要灰心。
- 聯絡作出誹謗的一方，冷靜討論問題。提議對方撤回誹謗言論。
- 如未能取得預期結果，聯絡熟悉誹謗訴訟的律師。
- 向你的互聯網服務供應商報告有關侵犯行為。

20

網上誹謗 (Online Defamation)

網上誹謗

每個人都應該對網上誹謗有所了解。數十年來，提交法庭的誹謗訴訟屢見不鮮。因此報章、雜誌及書籍出版商等傳統媒體，都會在付印前仔細檢查資料來源。然而近年的法庭裁決清楚顯示，即使在互聯網上發表資訊，亦可以被控誹謗。「發表(Publishing)」一詞現包括電郵、郵遞伺服器、聊天室及網站。我們都要對自己的言論負責，以及確保並無有意或無意地散播有關個人或公司的虛假或不利資訊。

如需協助或獲取更多資料，請瀏覽：

www.onlinepolicy.org/defamation.shtml

www.wiredpatrol.org/law/freespeech/defamation.html

www.spawn.org/marketing/slander.htm

www.cyberlaw.com

要避免捲入訴訟：

- 確保你所作出的任何聲明或評論，均有無可爭議的事實為依據，而並非只憑意見或感情用事。
- 請緊記，電郵一旦寄出，收件人就會看到，到時才想收回便為時已晚。
- 小心你在電郵、郵遞伺服器、聊天室及即時通訊中的言論，對在網站上發表的內容尤須慎重。
- 為免法律訴訟，務必教導家人及僱員在網上發表資訊所涉及的潛在問題。
- 在網上發表負面言論前，先評估一下其中目的及可獲取的利益。通常你會發現不值得冒這種風險。

聯機爭議處理

日常生活難免出現爭議，互聯網亦不例外。但是，如果根本不曾與對方見面，就更不容易解決。歐洲聯盟(European Union)現正試行名為電子消費爭議處理(Electronic Consumer Dispute Resolution (ECODIR))的計劃，旨在協助消費者和網上業務解決各類由互聯網交易引起的爭議。

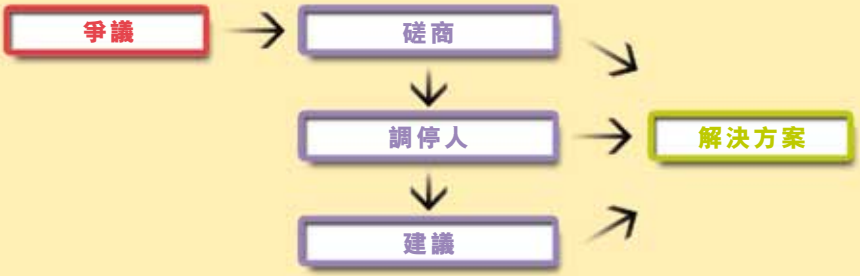
倘若各方磋商後未能同意和解方法，將會委任一名中立第三方（調停人）居中斡旋。調停人須簽署「公正聲明書」，而調停過程則屬保密及自願性質，各方有權隨時退出調停過程，改用法律程序提出申索。

整個概念在於透過聯機爭議處理解決互聯網上產生的衝突。隨著更多經營者在互聯網設立「網上商店(store front)」，這項計劃將會是不久將來必備的商業工具，提供符合成本效益和具備效率的解決方案，應付所有源自網上銷售交易的小額爭議。

電子消費爭議處理計劃由歐洲及北美各地政府、私營企業和學術機構多方參與。欲知更多此項計劃或其他同類計劃的資料，請瀏覽以下的網站。

聯機爭議處理 (Online Dispute Resolution)

電子消費爭議處理是結合安全網絡科技的網上程序，共分三個階段：



如需協助或獲取更多資料，請瀏覽：

www.ecodir.org
www.adr.org

聯機滋擾 (Online Stalking)

聯機滋擾

我們先要了解「滋擾」是甚麼，才可以替「聯機滋擾」下定義。儘管不同定義互有出入，但都有兩項共通點：

1. 以重覆和令人討厭的行為嘗試接觸他人，及
2. 令受害者感到威脅、恐懼或擔憂的行為。

因此，聯機滋擾就是透過電郵、互聯網聊天室和即時通訊騷擾別人。

這些行為會令被滋擾者感到非常困擾。有些政府已經立法或修改現行法例涵蓋聯機滋擾在內，而在個別情況下更可以發出禁制令。

如果沒有跟隨本小冊子建議的安全預防措施，滋擾行為更有可能進一步破壞電腦系統。雖然有辦法制止這些滋擾者，最好還是預先加以防範。

如需協助或獲取更多資料，請瀏覽：

www.cyber-stalking.net

www.wiredpatrol.org/stalking/

www.privacy.net

建議行動：

如果被滋擾：

- 刪除在聊天室和即時通訊系統設立的所有身份。
- 馬上更改電郵地址，改用中性的稱呼。
- 考慮改用匿名轉交郵件人。
- 聯絡互聯網服務供應商或聊天室管理人，並且提供遭到騷擾的證據。

為減低聯機滋擾的風險，應：

- 確保選用的「別名」或「屏幕名稱」不會暴露自己的性別。
- 確保自己的個人資料不會在互聯網上唾手可得。
- 利用更難破解的密碼。如果想知道更多建議，請參考本小冊子密碼一節。
- 不要設立網上個人資料表，如已設立，應馬上刪除。
- 最重要是緊隨本小冊子提供的保安建議，這就是最好的保護措施，能夠助你防患未然。
- 切勿在聊天室或即時通訊中出言侮辱他人。
- 欲知更多建議，請參考指引一節。

密碼

一天你離家外出，卻粗心忘了鎖門，結果有個陌生人進來，看了看，倒沒有拿走甚麼。即使沒有損失，但是知道陌生人翻看自己的私人物品，你又會作何感想？同樣，如果不好好自我保護，別人也能夠「窺視(snooping)」你的電腦。只有「不易破解(strong)」的密碼才是防備的屏障，跟家居正門的鎖匙同樣重要，也應該像門鎖那樣精挑細選。

黑客使用「密碼破解軟體」，可以在短短一小時內拆解簡單的密碼。相反，要破解「不易破解」的密碼，也許要花上十年以至二十年的時間。

建議行動：

看見這些數據，編定密碼時就值得多花時間跟隨這些簡單「要」或「不要」的指引：

- 不要使用任何字典（所有語言）內出現的詞彙（包括科學詞彙）。
- 不要使用任何字典（所有語言）內詞彙的倒寫。
- 不要使用任何與自己有關的詞彙，例如地址、電話號碼、出生日期、寵物名字、綽號、喜歡的運動或興趣。
- 不要使用連續的字母或數字，例如「abcdefg」或「234567」。
- 不要使用鍵盤上相鄰的字母，例如「qwerty」。
- 密碼應該簡單易記，毋須筆錄。
- 任意組合字母、數字和特殊字符。
- 使用大小寫和特殊字符(* @ #)。
- 密碼最少應有六個字母，越長越好。

密碼 (Passwords)

下一步就要保護你的密碼：

- 切勿把它寫在任何地方。
- 無論如何，切勿向任何人透露你的密碼。
- 瀏覽網站時不要剔選「記住我的密碼」選項，同時關閉瀏覽器內這項功能。
- 不要永遠用同一個密碼 —— 非關鍵活動應該使用一個密碼，而敏感或關鍵的活動則另設密碼。（緊記，登入電腦已經屬於關鍵活動）。

個人資料私隱 (Privacy of Personal Information)

個人資料私隱

無論自覺與否，我們每天其實慣常與他人共享個人資料：在繳交賬單、安排外遊、在商店食肆使用信用卡等時候，已經向陌生人公開了個人資料，然而我們卻無從判斷他們是否可靠。基於某些原由，不少人偏向認為網上世界較現實世界風險來得較高，因而對互聯網敬而遠之。

我們固然需要著緊怎樣保障個人資料，但也不必過份憂慮，只要跟隨本小冊子內的簡單建議即可。電子世界與現實世界其實並無不同，重要的是先認識網上世界特有的問題，並且學會防避的方法。跟以前的信用卡一樣，多年來人們對信用卡收據的用處一無所知。然而，我們一旦知道收據上的資料能夠用於採購詐騙，就馬上學會在丟棄前先撕成碎片。這就需要教育的過程。

財務資料並非消費者唯一需要注意的範疇。別人怎樣了解我們的消費喜好、網站瀏覽喜好、網上醫療記錄、信貸記錄等都同樣重要，必須加以正視。為保障你的私隱和個人資料，請遵照本小冊子建議的所有保安步驟，並養成採取以下行動的習慣。

建議行動：

管理個人資訊，首先要知道部分網站利用了蒐集個人資料的技術，而且你未必同意這些資料的用途。

既然明白了這個漏洞，下一步便是到每個瀏覽的網站（特別是與你有商業聯繫的網站），查看其私隱聲明及使用閣下個人資料的方法。私隱聲明內有兩項要點務須留意：

- 該公司怎樣處理你的電郵地址 —— 會否出售或交換電郵地址？
- 該公司會否蒐集個人資料，並在未經知會或取得你同意的情況下使用有關資料？

如需協助或獲取更多資料，請瀏覽：

www.privacyfoundation.org
www.oecd.org
http://epic.org
www.privacy.net

公用接入點

世上許多人未必擁有自己的電腦，但都會希望接達互聯網；度假人士不一定攜帶膝上電腦，卻會使用互聯網跟親友和業務夥伴保持聯絡；外訪的商務旅客即使不愛攜帶膝上電腦，也需要上網收發電郵和交換重要業務文件。因此，人們有需要在公用接入點連接互聯網。現時普遍的公用接入點包括互聯網咖啡室、機場資訊亭、以及酒店和圖書館的公用電腦系統等。

公用接入點對不少人而言既可行又方便，但必須小心使用。緊記，這些系統屬於公開性質，只要小心跟隨以下的建議，就能夠在公眾場所安全地接達互聯網。

建議行動

- 留心坐在或站到你附近的人 — 他們可能在你背後看見你輸入的登入名稱、密碼或個人資料等。
- 倘若定期使用公用接入點，應該不時更換密碼。
- 離開時清除瀏覽器的「快取記憶」，有助降低被他人取得個人資料的機會。
- 清除瀏覽器的「記錄設定」。
- 離開前關閉所有開啟的瀏覽器。
- 切勿讓電腦「記住密碼」— 緊記解除這個選項。
- 切勿在公用接入點的電腦輸入私人或敏感的資料。

公用接入點 (Public Access Points)

安全網頁 (Secure Web Pages)

安全網頁

如果你想在互聯網上購物，網上商店便會向你索取信用卡號碼及個人資料。在確實進行網上購物之前，你當然要用盡一切辦法衡量與你進行交易的網站是否從事合法業務，以及有否奉行本小冊子列出的電子貿易最佳實務政策。

比如說，你正準備與一家值得信賴的企業進行交易，並且對此事充滿信心。在快將遞交個人資料及信用卡號碼的時候，你要核實這些資料會否以保密方式傳送。下文列出一些簡單測試的建議，你可以在提交個人資料前先進行這些測試。

建議行動

有一個簡單測試可以助你衡量一個網頁是否安全：在微軟視窗系統上，當指標停留在網頁任何一處空白位置時，點擊滑鼠右鍵，選取「內容」。屏幕便會出現關於該網頁的資訊。點擊「憑證(certificates)」。如果該網頁並非安全網頁，電腦會讓你知道該網頁沒有安全性憑證。然而，如果該網頁為安全網頁，電腦會告訴你該網頁的「密碼匙的長度」。理論上，最理想的密碼匙長度是128數元。這裏僅對這個既複雜又涉及高科技的課題略作簡單解釋。不過，這個簡單測試卻能夠讓你知道你的敏感資料會透過安全的途徑傳送。

此外，還有兩個方法可以用來衡量網頁是否安全，但它們不及第一個方法可靠。一個是檢查瀏覽器上方「網址(address)」一欄是否出現「https」字樣，而非一般的「http」。「https」顯示網頁**是否**安全，但卻不能告訴你**有多**安全（例如是否128數元）。

另一個方法，亦是最常建議新用戶的方法，是查看瀏覽器下方有否出現提示你正在安全網頁的圖示（例如關上的鎖、關上的安全鎖或完整的鑰匙）。這個方法亦不能告知你該網頁**有多**保密，而且若干類別的網頁（即框式網頁）並沒有顯示這些圖示。

如需協助或獲取更多資料，請瀏覽：

尋找更多關於憑證、
安全網站，以及
使用安全網頁、
查看瀏覽器的小幫手。

軟件更新

如果你沒有定期更新電腦上運行的軟件，這些軟件可能會構成保安問題。當使用某程式一段時間後，這程式會出現一些小問題，生產商便需要製作「更新 (updates)」或「修補 (patches)」程式來修理有關程式。此外，信譽良好的軟件生產商一直致力令用戶進行網上活動時更安全，你大可以放心每個新版本軟件都有引入新保安措施，尤其是視窗、Mac、Linux等操作系統軟件。為了自己著想，最好使用最新版本的操作系統及定期更新程式。應用軟件亦應不斷更新。

如需協助或獲取更多資料，請瀏覽：

http://windowsupdate.microsoft.com/

www.apple.com/swupdates/

建議行動

- 如果使用視窗XP或視窗2000，指定「NTFS」檔案系統較「FAT32」系統為佳。這樣會加強電腦的保安，以及提供加密處理磁碟上的敏感數據的功能，以達到保密的效果。
- 確保你的操作系統（例如視窗2000、視窗XP、Mac X作業系統）為最新版本。
- 確保瀏覽器軟件為最新版本（例如Internet Explorer 6、Netscape 6.2）。
- 由於辦公室應用軟件（例如文字處理器、試算表、數據庫、行事曆）製造的檔案經常透過電郵、軟磁碟及檔案共用來與其他人分享或分發，故這些軟件是很重要的。
- 由於你會定期使用電郵與認識的人甚至陌生人溝通，故此電郵軟件非常重要。你需要最新的保安措施。（例如Outlook Express、Netscape Mail及Eudora電郵軟件）。
- 確保你擁有最新版本的抗電腦病毒軟件（例如Symantec、McAfee）。最重要是定期更新病毒定義檔。
- 為令防火牆全面保護你的電腦，故此亦須不斷更新防火牆（例如ZoneAlarm、Black Ice Defender、Symantec）。
- 而最重要的建議是，上述大部分軟件產品都設有「自動更新」選項。這是管理所有軟件產品更新程序的最佳方法。

軟件更新 (Software Updates)

濫發電郵 (Spam)

濫發電郵

我們大部分人都會收到垃圾郵件。我們的郵箱往往擠滿不請自來的廣告，甚至連看也沒看便扔掉。電子郵件或「電郵」現在亦出現這種情景。我們的電子郵箱差不多每天都收到不請自來的郵件，實在令人生厭。

實際上，濫發電郵較垃圾郵件隱含更多問題。即使你可以輕而易舉地「刪除」濫發電郵，你亦應該細想一下濫發電郵的深遠問題。垃圾郵件的成本全部由寄件者支付，即那些公司出錢印製及郵寄宣傳刊物。而濫發電郵方面，則需要所有收件者付出代價來接收這些電郵。不論收件人是一個還是一百萬個，寄件者都是付出同樣的金錢。濫發電郵會損耗個人及公司的時間與金錢，原因如下：

- 在大部分情況下，你必須把所有信息下載到電子郵箱，不能只下載有興趣閱讀的信息。
- 很多用戶按上網時數繳費，如果你下載大量濫發電郵，就必然會花費更多金錢。
- 篩選電郵很花時間，而時間就是金錢。
- 濫發電郵阻塞全球的電郵伺服器，導致成本上漲，接駁速度減慢。

我們不能完全阻止濫發電郵，唯有希望透過以下建議行動來減少發生。

建議行動

1 永遠不要回覆濫發電郵。當你回覆濫發電郵時，實際上亦同時確認你的電郵地址，令你成為目標。

2 不要把日常電郵地址加到訂閱、新聞通訊及通訊錄等名單上。這個地址應該專門用於定期聯絡的人，例如商業聯繫人士、朋友及家人。至於其他用途，則可以開設獨立電郵地址。換句話說，使用一個私人地址及一個公眾地址。

3 千萬別選購任何濫發電郵推廣的產品。這只會鼓勵寄件者繼續使用這種銷售伎倆。

4 使用濫發電郵過濾器。市面上有多種這類過濾器，你可以選擇最適合你的電郵需要的過濾器。

5 向反濫發電郵網站及政府消費者機關舉報「濫發電郵者」。

6 切記檢查所有你曾到過的網站的私隱聲明，查看他們會如何使用你的電郵地址。

如需協助或獲取更多資料，請瀏覽：

http://spam.abuse.net

www.cauce.org

仿冒

「仿冒」分為兩大類。第一類發生於技術溝通層面，稱為「互聯網規約仿冒(IP Spoofing)」。優質互聯網服務供應商會保護其用戶免受這類威脅，因此大部分家庭及小型商業用戶不用為此而擔憂。然而，假如你以路由器操作網絡，請跟器材供應商討論如何自我保護。

另一類仿冒為「電郵仿冒(email spoofing)」。這種仿冒可以不同形式發生，其結果是用戶收到的電郵表面上看似來自某個來源，實際上卻另有出處。電郵仿冒的目的往往是誘使用戶作出損害性的聲明，或發放敏感資料（例如密碼或個人資料）。

建議行動

- 你可能會從電郵收件者或調查「退回電郵」錯誤訊息中察覺到「電郵仿冒」。如是的話，務必盡力收集關於問題訊息的資料，然後將有關詳情轉交互聯網服務供應商作進一步調查。
- 如果你擔心收到的電郵是否來自已知的來源，可以考慮使用數碼簽署，以確保所有訊息都經過認證。如欲獲取更多資料，請參閱「數碼簽署」一節。

仿冒 (Spoofing)

- 網上有形形色色的欺騙手法，用來誘騙用戶披露密碼等敏感資料。這些騙人的手法可以是「仿冒」電郵、網站的互動區、電話，甚至郵寄的函件。若遇到別人向你索取密碼或其他個人資料，你先要核實該要求是否從已知及經認證的來源發出。以下的電腦緊急應變小組(CERT)網站收錄了一些這類騙案的例子。這個組織接收來自世界各地的「仿冒」事件報告。

如需協助或獲取更多資料，請瀏覽：

www.cert.org/tech_tips/email_spoofing.html

間諜軟件 (Spyware)

間諜軟件

間諜軟件在沒有知會你或取得你的同意下，利用你的電腦及互聯網連線，把你的個人資料發送給個人或機構。間諜軟件以軟件病毒的姿態從你瀏覽的網頁或電郵進入你的電腦。

間諜軟件可以是「第三方cookies程式」（見「Cookies程式」一節），亦可以是入侵程式，專門向軟件生產商報告你如何使用他們的程式。這種情況在由互聯網下載的軟件中特別常見。生產商總希望進一步知道用戶的喜好，好讓他們修改現有的程式，以及有助日後開發新程式。然而，顧客一般都反對這種監視行為（因為這樣不但造成侵擾，更干犯他人私隱）。不少人已對採用這種方式的公司提出訴訟。因此，大部分這類程式都已被修改，停止這種侵擾性的數據收集行為。

然而，仍有部分公司繼續秘密收集個人資料。為審慎起見，在下載時請仔細閱讀所有提供的資料。很多情況下，你可以「選擇不接受」這些「功能」，但你要非常小心地閱讀，才能夠發現對方是在問你是否准許把有關資料向生產商回報。部分決心收集個人資料的公司，更會盡力掩飾，不讓人知道他們在你的電腦安裝「間諜軟件」。

另一種「間諜軟件」叫「網上臭蟲」。這小小的程式通常是附在網頁或HTML格式電郵的細小圖像檔案。在大多數情況下，這些「網上臭蟲」是隱形的，無法察覺。但它們會與「Cookies程式」串通一氣，收集你瀏覽習慣的資料。對付這些「網上臭蟲」的最佳方法，是按自己需要盡量選取較安全的「Cookies程式」喜好設定。

建議行動

- 檢查瀏覽器的「Cookies程式」設定。
- 下載「間諜阻截(spy check)」軟件，例如「Ad-aware」(www.lavasoft.de)。
- 就所有接觸的網站，查看及閱讀所有有關使用個人資料，以及會否使用間諜軟件收集資料的政策及聲明。
- 確保你已安裝防火牆軟件，並且不斷更新。

如需協助或獲取更多資料，請瀏覽：

www.bugnosis.org

http://grc.com/optout.htm

www.spychecker.com

特洛伊木馬程式

「特洛伊木馬程式」往往在你不知情時入侵你的電腦系統，並在背後悄悄運作，令人難以察覺。特洛伊木馬程式通常「依附」在其他程式，就像古希臘神話中的特洛伊木馬一樣，在平實的外表下暗藏侵害，因此這種程式被稱為「特洛伊木馬」。特洛伊木馬程式可依附在以電郵傳送的檔案、在聊天室交換的共享軟件(shareware)，以及軟磁碟內的檔案、盜版軟件，又或循其他不正當的方法感染電腦檔案。

任何病毒或特洛伊木馬程式，只有在執行或操作受感染的程式時，才會觸發病毒或特洛伊木馬的侵襲。開啟文字處理或試算表檔案時更千萬要小心，因為當中可能含有可執行的宏指令(macros)，而這些宏指令可能已在蓄意或無意中受到病毒或特洛伊木馬感染。既然特洛伊木馬程式如此狡詐，應當怎樣保護自己才好?很簡單，只要遵行下列的建議行動，做好預防措施，便是最佳的保護方法。雖然特洛伊木馬程式有別於一般的電腦病毒，不應將兩者混淆，但你仍可使用內設有特洛伊木馬偵察功能的抗電腦病毒軟件，為電腦執行關鍵的防護措施。

特洛伊木馬程式 (Trojan Programs)

特洛伊木馬程式造成的破壞可以相當嚴重，必須認真處理。特洛伊木馬程式基本上分為三種：

- 「遠程接達工具(Remote Access Tools (RATs))」—黑客可任意套取你電腦內的所有資料；
- 「鍵盤側錄程式(Key-loggers)」—記錄你輸入的所有鍵次，然後將收集到的資料檔案傳送給黑客；
- 「密碼檢索器(Password Retrievers)」—收集你的密碼檔案，傳送給黑客。

有一點必須注意，單單在電腦下載檔案並不會啟動

建議行動

- 安裝個人防火牆。
- 定期下載病毒定義檔，令抗電腦病毒軟件保持最佳功能。
- 每次安裝程式前，緊記使用抗電腦病毒軟件進行手動檢查。
- 每星期最少進行一次病毒掃描，掃描整個電腦系統。

以上預防措施能有效確保你的電腦不受特洛伊木馬軟件的侵襲。

如需協助或獲取更多資料，請瀏覽：

www.cert.org

病毒 (Viruses)

病毒

甚麼叫病毒?電腦病毒之所以稱為病毒,原因是這些病毒與生物病毒擁有一些相同的特性。電腦病毒可由一部電腦傳染至另一部電腦,正如生物病毒會人傳人一樣。在互聯網尚未普及前,電腦病毒主要經共用受感染的軟磁碟散播,所以較容易找出病毒的來源。但現時病毒的來源層出不窮,包括電郵、文字處理及其他應用檔案、電腦遊戲及從互聯網下載的各種軟件程式等。雖然現時病毒的數目遠較以前為多,幸好現時已研究出預防方法,防止病毒入侵我們的電腦系統。

病毒會對你的電腦造成甚麼損害?病毒是一種軟件程式,其實質的影響須視乎製造病毒的人所編寫的程式而定。有些病毒專門損害電腦系統裏的檔案,或者以某種方式干擾電腦的正常運作。所有病毒,即使是被視為「傷害性」較低的病毒,都有能力破壞或損害檔案,但卻不能損害硬件。不管坊間流傳的說法如何,事實上,病毒是無法破壞中央處理器,不能燒毀硬磁碟,更不會令顯示器爆炸。你可能會收到這類病毒警告,但那無非是惡作劇,不是真的。

此外,你可能曾收到朋友或生意夥伴寄出的電郵,提醒你防範某種危險的病毒。通常,這些電郵也不過是惡作劇電郵,誤導大家在一片善意下轉寄給朋友,所以請勿再轉寄這些電郵。這些垃圾郵件只會阻塞互聯網,令其「發佈者」得逞。只要你經常更新抗電腦病毒程式,根本不必理會此等郵件。

建議行動

- 確保你已安裝最新版本的抗電腦病毒軟件。
- 緊記每隔數天更新病毒定義檔一次,更應善用大部分抗電腦病毒軟件程式內置的「自動更新」功能,這樣你每次登入互聯網時,抗電腦病毒軟件便會自動檢查有沒有最新的病毒定義檔。

- 收到來歷不明的檔案時,除非你肯定其內容是甚麼、由誰人傳送及為甚麼傳送給你,否則切勿開啟這些檔案。切記檢查所有檔案,不能鬆懈。即使電郵的寄件者一欄是你好朋友的名字,但實情可能是他的電腦已被黑客入侵,黑客獲得你的電郵地址後,向你寄發電郵。如要知道怎樣防止黑客入侵,請參閱「防火牆」一節。開啟任何檔案前,應使用最新的抗電腦病毒軟件程式檢查。

如需協助或獲取更多資料,請瀏覽:

www.symantec.com

www.mcafee.com

www.europe.f-secure.com/news/hoax.htm

(以上網站載有更多關於惡作劇電郵的資料)

網上安全

指引類別:

- 若非已安裝硬件或軟件加密設備，你應假設互聯網上交流的所有信息都不安全。不適宜寫在明信片上的東西，亦不適宜寫在電郵裏！
- 如要轉寄或轉貼你收到的某個信息，不要更改信息內的任何字眼。如果那是別人寄給你的私人信息，在轉寄給另一人或一群人前，應先得到寄件者的同意。
- 切勿透過電子郵件寄發連鎖信，這種行為在互聯網上是嚴禁的，否則你在網絡上享有的權利可能會被取消。如收到任何連鎖信，請立即通知你的互聯網服務供應商。
- 信息應盡量簡潔，但又要避免予人草率的感覺。簡短生硬的信息會被視為無禮或憤怒的表現。
- 在主旨一欄，註明信息的內容。這樣，收件者便可輕鬆和有效地整理寄入電郵，優先處理要立刻回覆的重要信息，以及將郵件存檔，方便日後查閱。

電郵信息指引
(Guidelines for Email Messages)

- 寄發信息或回覆電郵時要特別小心，因為部分電郵的收件者一欄雖然顯示為某個別人士，但事實上卻會分發給一群收件者。
- 有些人每日須處理大量電郵，往往希望事先知道哪些電郵篇幅較長，需要較多時間去處理。一般來說，電郵內容如超過100行，便屬於篇幅較長的郵件，應當在主旨一欄註明，通知收件者。
- 寫電郵時，應善用大小楷字母。在日常書信中，全大楷的信息代表**責罵對方**。
- 有些人喜歡用「笑臉」符號表達語氣或態度。開心的符號是:-)，而憂愁的符號是:-(，這些都是由鍵盤上的符號組成的。如果真的要用這些符號來表達，最好盡量避免濫用，並須緊記其他國家文化的人未必明白這些符號的意思。
- 收到信息時，你未必有時間立刻仔細回覆，所以最好先寄出一封簡短的電郵，讓對方知道你已收到他的信息，稍後會再詳細答覆。
- 不請自來的電郵廣告往往不受歡迎，在某些情況下甚至是犯法的。
- 避免寄發太大的檔案。內含超過150千字節的檔案便屬過大。
- 不要建立過於冗長的收件者名單，要將信息同時寄發給許多人時，可用「特別副本送(blind carbon copy (BCC))」功能。

- 在加入任何通訊錄或新聞組前，應先花一至兩個月時間了解這個組別，否則不要發表任何信息。
- 雖然用戶的不正當行為與系統管理員無關，但系統管理員有責任採取行動，阻止任何違規行為。
- 一旦按下「傳送」鍵，便會無法取消已發出的信息。因此，發表信息前必須仔細考慮，以免後悔莫及。

- 萬一不小心將私人信息傳送給組別的所有人，應當立即向當事人及該組別道歉。
- 如對某人發表的信息有強烈感覺，應透過私人電郵表達。
- 不要捲入任何「筆戰 (flame wars)」中。切勿發表煽風點火的信息，也不要回覆這類信息。通訊錄管理員自會解決這些問題。
- 避免使用不標準的字型，因為這些字型在不同的系統上會有不同的顯示方式，令用戶難以閱讀。
- 如要加入及離開通訊錄，請將有關信息傳送至適當的電郵地址。

通訊錄指引
(Guidelines for Mailing Lists)

- 力求信息簡潔、貼題。
- 有些通訊錄歡迎用戶發表廣告，但也有些表明嚴禁發表廣告。
- 回覆或發表信息時，應確保你引述的原文足以交代事情的始末，否則對方未必明白你所述何事。
- 發表私人回覆時要小心。若只按下「回覆寄件者」的話，很可能整個通訊錄的人都收到你的回覆，有違你只想回覆某人的原意。

- 如果你有一段長時間無法檢查電郵，應考慮退出通訊錄或設定「不收取郵件」選項（如有）。
- 若向不止一個通訊錄發表信息，尤其是各通訊錄關係密切的話，應為重覆發放道歉。
- 切勿透露你的用戶名稱或密碼。即使是系統管理員需要你的賬戶資料，藉以進行維修或修正問題，他們也可隨時登入你的賬戶，毋須事先向你索取任何資料。
- 為免引起誤會，應用以下格式表示日期：11 Feb 2002。
- 縮略語可以減省用字，但若然信息裏有太多縮略語，便會令其難以理解，對讀者造成不便。以下是部分常用的縮略語：

  IMHO = 我認為
  FYI = 僅供參考
  BTW = 順帶一提

方便消費者使用的網站指引
(Guidelines for Consumer-friendly Websites)

業務方面

你有沒有清楚描述你的業務性質？

你有沒有提供以下相關資料？

- 實際營業地址
- 可讓顧客直接聯絡你的電郵地址或電話號碼

處理資料方面

你有沒有清楚列明收集資料的作業實務？例如你收集甚麼資料？作何用途？會否與其他人共用資料？和誰共用？

你有沒有清楚列明可識別個人身份的資料會作何用途？會否與其他人共用？

你有沒有解釋採用了甚麼保安措施以保障在你網站內進行的交易？

你是否明白有關監管跨境傳送個人資料的法例？

宣傳及市場推廣

你在網站內有沒有提供準確而真實的產品和業務作業實務資料？

你能否證明你對貨品和服務所聲稱的任何或所有事項？

你有沒有在網站內公開所有廣告贊助商？

你有沒有尊重消費者不欲接收電郵廣告的決定？

向兒童宣傳時，有沒有特別小心處理？

銷售方面

你有沒有詳細列明產品的資料，讓消費者明白你售賣的是甚麼貨品和售賣條件？

你有沒有列明包括運費和手續費在內的收費總額，並標明所用的貨幣？

你有沒有清楚解釋買賣時可能適用的額外收費？

你有沒有列明任何買賣限制？

你有沒有提供買賣相關的保證或擔保的資料？

你有沒有列明買家大概多久才收到貨物？又或者有沒有提供跟進號碼及運輸公司的網址，讓買家查看運送情況？

你有沒有清楚說明付款方式？

消費者保障

你有沒有解釋公司的退貨政策，包括消費者如何退回貨品以取回退款、記賬或換貨的指示？

你是否已清楚說明退貨的所有條件？

你是否已提供所需的聯絡資料，讓消費者有投訴或問題時聯絡你？

你有沒有透過網站或隨後以電郵向顧客提供交易紀錄？

網站內有沒有就顧客的個人資料私隱提供清晰的政策條文？你有沒有讓顧客自行選擇是否參與電子通訊，或在未有要求的情況下收到其他商戶的電郵？

你有沒有列明會如何解決糾紛？你有沒有參與任何認可的聯機爭議處理計劃？

在互聯網上購物輕鬆方便，但同時消費者也必須確保交易安全可靠。在網上購物時，可使用以下指引保障自己。

- 確保與**值得信賴**的公司交易。朋友推介BBBOnline (www.bbbonline.org)這類網站或國際計劃，可以查證公司是否遵守網上的專業操守。
- 查看**商戶資料**，例如實際地址及電話號碼，確保有疑問或投訴時能聯絡商戶。
- 由於並非所有公司也接受退貨或退款，因此必須詳閱並確保自己接受商戶的**退款及退貨政策**。部分商戶只會允許日後購物時記賬，部分則會收取「回收費用」，而大部分則不會退回運費和保險費。如果網上商戶擁有實際營業地點，你或可以將產品退回最近的商店，以節省運費。
- 對於電子或翻新的電腦等產品，你必須細閱及理解**保養**的條款和條件。
- 確保以**不易破解的密碼**登入（參閱「密碼」一節）。千萬別向任何人士洩露密碼，最好取消任何網站內「記住密碼」的功能。
- 完成網上購物前，應小心**檢查購物詳情**，包括產品說明、大小、金額、形狀、顏色等等。確保已輸入正確的運貨及發送賬單地址，而所有計算均正確無誤，包括運費、手續費和稅項。好的購物網站會在完成交易前顯示將會收取的實際金額。

安全網上購物指引 (Guidelines for Safe Online Buying)

- 為保障你的私隱和防止個人資料被盜用，應閱讀和了解網站內的**私隱政策**。政策應披露網站將會收集的資料及資料用途。如果找不到私隱政策，應向網站寄發電郵或發送信息，查詢私隱政策，並要求於網站上刊載。許多公司也讓你選擇是否准許公司使用你的個人資料。你應該可以選擇拒絕或「選擇不接受」將你的電郵地址等個人資料用作市場推廣用途或與其他公司分享。
- 確保在**安全的網頁**內進行交易（參閱「安全網頁」一節）。
- 緊記**保留交易收據**，並列印有訂購號碼及訂購詳情的一頁。部分網站甚至會於某一步驟指示你列印，而其他網站則會表明你會透過電郵收到收據。如你在網站訂閱報紙、雜誌或申請通訊錄服務等，必須列印合約，並了解停止此項服務的手續。
- 好的購物網站會有**貨物追蹤**的功能，讓你知道貨物所在位置，以及預計送抵時間。其他網站則會提供查詢號碼及運輸公司的網址。如商戶並無提供以上任何一項，你可能需要透過電郵或電話聯絡商戶，查詢有關資料。

競投或購買貨品前：

- 確保自己清楚所競投的貨品是甚麼。細閱產品說明、付款條款、運費及手續費、保證及退款政策。如有任何不明白的地方或疑問，應發送電郵向賣家查詢。如果賣家不回覆電郵或回覆含糊，就要小心提防。
- 如果可以，透過互聯網或其他途徑尋找產品資料，盡量在競投前了解貨品的公平市價。

網上拍賣指引 (Guidelines for Online Auctions)

- 細看照片，了解貨品情況。
- 查閱賣家的意見紀錄（大部分拍賣網站也提供這項資料），並確保明白不同拍賣網站所用的評分制度。同時亦可查詢賣家於拍賣網站買賣的年期。如賣家初次參與網上拍賣，你應於競投前與賣家以電郵通訊，直接查詢。
- 閱讀所有載列的資料，包括網頁末段的資料，賣方通常會於頁尾列明他們的業務政策及銷售條件。
- 為免誤會，應協定確實的交收時間。
- 確保你所購買的貨品並非所屬司法權區列為危險或非法的物品。可到有關政府網站查詢詳情。
- 競投前，應為自己設下上限，以防後悔莫及，又或成功投得物件後卻發現無法支付買價。在拍賣網站競投時，你實際上已經訂立合約，可能必須履行法律責任付款。
- 如競投昂貴的貨品或你對交易有疑問，大部分拍賣網站也提供託管服務。詳情請參閱個別拍賣網站。
- 為方便往後與賣家聯絡，應習慣保留所有相關網頁及與拍賣有關的電郵。
- 如遇上懷疑詐騙的賣家，應立即向拍賣網站管理員報告。
- 與賣家通訊時，應慎防洩露個人資料。

Asia-Pacific Economic Cooperation

亞太經合組織電訊及資訊工作小組計劃
(An APEC Telecommunications and Information Working Group Project)
亞太經合組織刊物 #202-SO-01.1
www.apecsec.org.sg

由亞洲大洋洲電子市場協會編製
www.aoema.org

由多媒體交流協會(FMMC)(日本)資助
www.fmmc.or.jp

特別鳴謝

澳洲外交與貿易事務部(Australian Department of Foreign Affairs and Trade)及AusAID，於二零零一至二零零二年協助亞洲大洋洲電子市場協會在越南、菲律賓、印尼及中國舉辦亞太經合組織促進電子貿易研討會(APEC E-commerce Awareness Workshops)。本刊物專為回應工作坊內所確定的需要及優先處理事項而刊發。

www.dfat.gov.au

特別鳴謝

日本總務省(Ministry of Public Management, Home Affairs, Posts and Telecommunications)自一九九六年起一直支持AOEMA提高公眾意識講座活動，於十四個經濟體系舉辦研討會。本刊物專為回應工作坊內所確定的需要及優先處理事項而刊發，並以E-Japan論壇(E-Japan Forum (EJF))編製類似指引供日本使用的工作為基礎。

www.soumu.go.jp

二零零二年八月

消費者的保護

Cookies程式

數碼簽署

防火牆

身份盜竊

即時通訊、聊天室等

知識產權

互聯網誘騙轉接

互聯網詐騙

法律問題

監測互聯網的使用

網上誹謗

聯機爭議處理

聯機滋擾

密碼

個人資料私隱

公用接入

安全網頁

濫發電郵

軟件更新

仿冒

間諜軟件

特洛伊木馬程式

病毒

電郵信息指引

通訊錄指引

方便消費者使用的網站指引

安全網上購物指引

網上拍賣指引

本小冊子為 AOEMA 所出版的 SafetyNet 英文版的中文譯本；
SafetyNet 的英文原版刊載於網址：http://www.aoema.org/SafetyNet/index.htm。
香港特別行政區政府資訊科技總監辦公室獲AOEMA授權翻譯及出版本小冊子。
如對本中文譯本的內容有任何查詢，請電郵至 webmaster@infosec.gov.hk。
This booklet is a Chinese translation of SafetyNet published by AOEMA in English.
The original English version of SafetyNet can be found at http://www.aoema.org/SafetyNet/index.htm.
The Office of the Government Chief Information Officer of the Hong Kong Special Administrative Region Government has obtained the approval of AOEMA to translate and publish this booklet.
For enquiries about the contents of the translation, please email us at webmaster@infosec.gov.hk.

政府物流服務署印
（所用紙張取材自可再生林木）
Printed by the Government Logistics Department
(Printed on paper made from woodpulp derived from renewable forests)