三招破五網絡私隱陷阱

講者：林景昇先生
國際信息系統審計（中國香港分會）會員服務理事（項目和活動）、國際演講會中國區市場副總監

日期: 2011 年 8 月 6 日

今天，我會從工作經驗中，總結互聯網上須多加警惕的地方。本講座題為「三招破五網絡私隱陷阱」，將先介紹五個網絡私隱陷阱，再教授三招避險技巧，皆是人人都可做到，可避免成為受害者。

陷阱一：虛假訊息

個案：「急性盲搶鹽」

日本爆發核輻射事件後，香港出現「食鹽可抗輻射」、「海水受污染，未來無食鹽」等傳言，導致大批市民搶購食鹽。從新聞所見，當天在深水埗買鹽要排隊，更有店鋪坐地起價，原價一、兩元的一斤裝食鹽竟加價至二、三十元。有水貨客甚至一次購買百多斤食鹽。

專家表示謠言毫不正確：製鹽需要海水，而海水佔全球總水量四分之三，因此鹽的供應量不會受影響。他們亦呼籲市民要有常識和分析能力，了解輻射如何影響身體，不應該受流言影響，亦不應該讓散播流言的投機分子從中取利。

香港「盲搶鹽」一事已成為國際新聞。不久前，加拿大華僑朋友回港，與我見面時表示此事在加拿大也廣受關注。有關「盲搶鹽」的流言，明顯是經網絡散播的。提起「電腦陷阱」，大多數人可能想到電腦病毒，但陷阱並不限於病毒。今時今日，網絡覆蓋率極高，香港差不多每家每戶都可上網，於是網絡成為散播假訊息的最快途徑，也成為「虛假訊息陷阱」最多的地方。

「盲搶鹽」當天，不知道大家有否收到以下的短訊：「BBC 最新消息：核輻射已擴散到菲律賓。請轉發予亞洲各地朋友。」說得真嚴重！當天，我收到這短訊的英文、繁體中文和簡體中文版，分別來自香港和內地的朋友。除了核輻射短訊，相信大家平時也收到不少主題不同，但形式相近的短訊或電郵：發生了某事件，請儘快轉發消息，以示支持某某活動（可能是扶貧或環保），或避免生日當天遭逢厄運。

以前寄信要買郵票，寄十封就要 14 元。現在，即使寄信給 100 萬人，也只需按一下鍵盤，費用全免。因此，雖然連鎖信不是甚麼新鮮事兒，卻在互聯網出現後威力加倍。如果我們不仔細分析，隨便相信連鎖信的內容，便很容易誤中圈套。

如何分辨訊息真偽？方法很簡單，就是先認定訊息是假的。如果消息是真的，以後一定還有機會知道，因此我們不必一收到消息就急著相信。另外，假消息連鎖信通常有三大特徵：

1. 聲稱消息來自權威（例如英國廣播電台 BBC 或微軟），卻不提供核實資料來源的途徑（例如 BBC 或微軟的網址）。
2. 要求你馬上轉發消息，聲稱不這樣做便後果堪虞，例如很多人會因此遭殃。
3. 聲稱你轉發消息後會走運，或者得到人格上的昇華等等。

真實的訊息，通常不會聲稱轉發或不轉發會帶來後果，而且來自較權威的來源，也會提供核實資料的方法。

「盲搶鹽」事件翌日，BBC 便澄清短訊是假冒的，純屬惡作劇。然而，惡作劇也可以極速蔓延，可見網絡的威力。希望大家不要輕易被假訊息騙倒，墜入「虛假訊息陷阱」。

個案：《明報》報道香港成為沙士疫埠？

2003 年 4 月 1 日，有人盜用《明報》網頁，刊登香港成為沙士疫埠的消息，使人以為這是《明報》新聞，馬上一傳十、十傳百，導致全城恐慌。原來始作俑者只是一個少年，他最後因為傳播虛假消息而被檢控。

除了連鎖信，虛假網站也是散播假消息的途徑，曾被偽冒的網站也不只一個。不少人都知道閱讀網址的重要性，知道只有一串數字的網極為可疑。然而，也有些像真度極高的網址，例如偽冒某銀行的網站，網址竟也是近似該銀行網站的網址！這網站經電郵廣發，聲稱該銀行推出新保安措施，而客戶若要保留戶口，必須立即登入並更改密碼。

然而，這個表面上是該銀行網址的網站，網址本來也是一串可疑的數字，只是網頁中放了一張以假亂真的網址列圖片，所謂近似該銀行網站的網址，其實只是圖片中的網址。它可能寄給了 100 萬人，當中總有 1 萬人用該銀行吧，他們就可能上當了。

如何避開假網站陷阱？新聞和金管局也經常呼籲：切勿胡亂點擊電郵裡的連結，應該自己鍵入網址。如果是常用網站，第一次鍵入網址後，便可以把網站加入「我的最愛」，作為瀏覽捷徑。各大銀行也不時澄清：不會要求客戶經電郵連結進入

網站。雖然自己輸入網址好像很麻煩，但與以往必須親身前往銀行相比，已經方便不少，同時也能保障私隱安全。

互聯網的內容不一定可信。以維基百科為例，其內容由網民撰寫，誰也可以提供資料。網民雖然不一定特意提供假資料，卻可能把未經核實的資料放到維基百科，因此我們也不應輕信當中的內容。

如果同一消息從不同途徑傳來，就連官方網站也發佈，該消息大概可信。如果只是從單一途徑收到消息，而內容又幾近天方夜譚，那麼作假的機會便比較大。我們必須謹慎過濾互聯網的資料。

陷阱二：粗疏密碼

Facebook 很多人都使用，也非常方便。然而，不知道大家有否聽過以下個案？

個案：Facebook 帳號被盜

在 Facebook 留言有兩個主要途徑。第一是張貼在塗鴉牆（wall）上，讓所有朋友或公眾（視乎個人 Facebook 的公開程度）都看見。第二就是寄送私人訊息，屬於單對單溝通，只有收發二人會看見。

有一天，一美國女子在 Facebook 塗鴉牆上發表了一段看似私人訊息的文字，向某男子表示非常享受昨晚「共歡」時光，內容非常露骨。留言面世後，有朋友問該美國女子是否不小心把塗鴉牆當作私人訊息，又有人恭喜該美國女子找到男友，「守得雲開見月明」。

數小時後，該美國女子的妹妹表示姐姐的帳號被黑客入侵，而該段露骨留言是黑客發表的。

入侵 Facebook 容易嗎？Facebook 是全球最大社交網絡，入侵它就像打劫匯豐銀行一樣，並不容易，因為 Facebook 必會投放大量資源於保安，以免流失用戶，被競爭者後來居上。

然而，入侵個別 Facebook 帳戶的難度，卻要視乎該戶口的密碼而定。如果密碼很容易被猜中，那麼 Facebook 的保安系統再森嚴也無補於事。我們設定密碼的時候，應該盡量挑選難以被人猜中的密碼，不要使用生日、手機號碼等人所共知的數字。不過，該美國女子的密碼其實尚算安全，為甚麼帳戶仍然被人入侵呢？

設定密碼後，網站通常還會請你設定保安問題，以便用戶忘記密碼後可以方便地重設密碼。常見問題包括母親的名字或結婚前的姓氏，或者寵物的名字，而該美國女子便選擇了寵物名字作為保安問題。然而，Facebook 用戶常常分享個人生活點滴，公告天下，而該美國女子亦曾經提及自己某天與寵物一起散步，還公開了寵物的名字。於是，黑客假冒該美國女子，謊稱自己忘記密碼，然後正確回答保安問題，順利控制該美國女子的帳號。

保安問題不再保安，實在諷刺。個人資料以往非常私密，現在卻可能是公開資訊。在 Facebook 上，你的資料可能不只朋友看得見，就連朋友的朋友也看得見。如果那朋友的朋友剛好是記者，或者覺得你的發言很有趣，努力揭秘，可能明天報章頭條就是你！因此，我們必須小心，不要輕易公開所有個人資料。這也可以說是陷阱，我們必須避免。

說回密碼。黑客有不少攻破密碼的方法，所以光是設定密碼，仍不能完全防止帳號被入侵。不過，假如帳號真的被入侵，更換密碼始終是終結問題的最有效方法。假設我的電郵密碼被他人知道了，那個人未必會有大動作，卻不時偷看我的電郵，今天看情信，明天看月結單，後天可能翻看我更改其他帳戶密碼的紀錄！不過，只要我定期更換密碼，便可以阻止那個人繼續翻看我的電郵，終結損失。

一般提倡每三個月至半年更換密碼，不過聽從的人大概寥寥無幾。互聯網服務眾多，每人可能有十多個密碼，如果每個都要經常更換，的確頗為麻煩。我們可以只挑選重要而常用的帳號，例如電郵、網上銀行和常用社交網站，定期更改其密碼，在安全和方便之間取得平衡，避免連續性損失。個人來說，對手提電話的密碼，我甚至不到三個月就轉一次。

另外，大家會使用同一密碼登入不同服務嗎？這其實是相當危險的做法！

個案：某大銀行戶口被接連入侵

多年前，某銀行的客戶接二連三地被入侵戶口，盜用款項，但那是全球規模數一數二的大銀行，齊備各種最新的保安工具，為甚麼這麼容易便被入侵？銀行懷疑是客戶選擇的密碼不安全，調查後卻發現不是這麼回事。

真正的原因，原來是一個與銀行完全無關的討論區被黑客入侵。這個討論區的保安並不嚴密，黑客得以取走所有用戶的帳號和密碼。

討論區的內容本是公開的，即使用戶密碼被盜，事態本也不算嚴重。但是黑客很聰明，沒有使用該批密碼登入討論區，而是登入銀行戶口，成功率竟達百分

之二十，即是說兩成用戶在討論區和網上銀行使用同一密碼！

我曾在另一講座分享此個案，話音甫落，幾百個參加者之中突然有百多人離座，可能是去更改密碼呢！到了可以使用手機上網的年代，我分享個案後也有不少人拿出手機，按個不停。如果大家在不同網站使用同一密碼，可能也要馬上拿出手機，更改密碼了。

在不同網站使用同一密碼的風險，就是可能要承受一連串損失，只要其中一個帳號被入侵，就會引發骨牌效應。因此，我們不但要經常更換密碼，也要把密碼分類。當然，最安全的做法是每個網站都採用不同密碼，但我們的帳號實在太多，所以這做法並不實際。建議大家在使用重要服務（電郵、網上銀行和常用社交網站）的時候，一定要採用不重複的密碼。

此外，有些人使用雲端電腦，把所有密碼都儲存在網上，風險亦非常高。奉勸各位，如果使用雲端服務儲存資料，雲端帳號的密碼必須設定得非常安全，並經常更換。

除了網上服務外，電腦本身也可以設定密碼。但是，設定了密碼真的安全嗎？電腦設定了密碼，就好像房間鎖上了門，雖然不能輕易進出，但如果有人用力踢門，還是可能闖進去。同理，有些人也懂得跳過密碼的關卡，獲取電腦裡的資料——只要取出電腦硬碟，把硬碟連接至另一部電腦，就可以閱讀硬碟資料而毋須輸入任何密碼。即使不取出你的硬碟，黑客也可以用程式猜中你的密碼。

因此，只設定密碼絕不足夠，我們還須加密電腦資料。「加密」並非「加設密碼」的意思，而是打亂資料的次序，讓賊人踢門闖入之後，看到的只是一片混亂景象，一無所獲。無論我們使用的是桌上電腦、手提電腦還是智能手機，進行資料加密都是基本要求。

陷阱三：網絡罪行

互聯網衍生不少罪行，其中之一是網上兜售毒品，就連特首也表示關注。在現實世界買賣毒品，很容易被拘捕，人贓俱獲。在網上兜售毒品，賣家卻甚至可能不在香港，而且貨品以郵遞交收，警方要與別國警方進行雙邊執法也很困難。另外，先不論毒品本身的禍害，網上購物常會貨不對辦，吸毒者收下的可能不是毒品，而是比毒品更毒的不明物質！面對網上的不道德交易，警方也已加勤執法，不時破解相關案件。

網上兜售毒品不是唯一問題。請聽以下案例：

個案：網上訛騙少年進行不道德交易

一名男子在 Facebook 上結交了一批年輕朋友，並以年輕美女的照片為頭像，又將更多美女圖片寄給年輕朋友，訛稱那是自己，邀請朋友「交換照片」。

後來，這位「年輕美女」寄出裸照，並希望對方也寄送自己的裸照。對方上當後，男子就公開自己的真正身分，並要脅對方必須與自己見面，否則便公開對方的裸照。

後來發生甚麼事，相信大家也想像得到。這些要求受害者進行不道德交易的勒索個案，牽涉到第一個陷阱：互聯網的內容未必可信。確認網上資料真偽之前，我們千萬不可做出有損自己私隱的事情，例如公開自己的私密照片。以上個案的犯案手法，不過新瓶舊酒。網上性罪行早在 ICQ 時代已經出現，只是現在的犯罪媒介變成 Facebook。要避免成為受害人，重要的還是核實網上「朋友」的真偽。

互聯網上的朋友與現實世界的朋友絕不一樣：我們在現實世界認識的是一個人，知道的資料往往較多，不像在網絡世界只能認識一個帳號。如果我們對待帳號如同對待真人一樣開放，便可能洩漏很多個人資料。

面對網絡罪行，最危險的其實不是不諳電腦的人，因為他們不使用電腦，並不會把個人資料上載。最危險的，是自以為已做足保安措施，但措施仍有漏洞的人。幾年前的「艷照門事件」中，事主把電腦拿去維修前，就是自以為已刪除所有不雅照片，殊不知照片仍可取回，釀成大禍。

陷阱四：侵犯版權

關於這陷阱，最經典的個案是「古惑天皇」事件，大家可能仍有印象。這是全球第一宗成功檢控點對點分享軟件（BT、Foxy 等）使用者的個案。

香港人喜歡使用點對點軟件分享電影、音樂，有時也會分享照片。分享這些資源，即使只是傳送給朋友，亦已侵犯版權條例。根據版權條例，只要你的行動損害版權持有人的利益，即屬違法。

陷阱五：流動裝置

不久前，一名藝人的床照傳遍坊間，而事件中的女主角聲稱是自己遺失手機之故。現在大家都愛用手機拍照，就連吃飯也要先拍下菜式的照片，離港前又要在

機場留影，還要在 Facebook 宣布消息，讓不法之徒知道你不在香港，乘虛而入——透過網上搜索，他不但知道你離開香港，還可以從你以往的留言（例如常在那裡吃飯）猜到你住哪一區，最後可能成功爆竊你的單位。

現時的流動裝置非常強大。智能手機除了比電腦小一些，功能根本與電腦無異，儲存的資料還可能更多。手機記錄了你的照片、影片、行蹤、朋友電話號碼、電郵等等，萬一遺失，可謂非常危險。

此外，以往我們使用網上銀行時，登入之後，銀行會發送一次性密碼至手機，那已是有風險。現在手機更為強大，我們可以使用手機登入網上銀行，也可以請手機記錄密碼，下次不用再輸入。於是，手機儲存了網上銀行戶口的登入密碼，如果落入不法之徒手上，銀行戶口便不攻自破。

如果大家使用 iPhone 或 iPad 等產品，應該聽過 iOS Jailbreaking（iOS 越獄），這是對蘋果公司便攜裝置作業系統 iOS 進行破解的一種技術手段，用戶可經此獲取 iOS 的最高權限，甚至可以解開蘋果公司對裝置的限制，例如安裝本來不相容的軟件。使用 Android 手機的，也應該知道「開放平台」。開放的流動裝置網絡，固然方便用家，但也製造風險。不少調查和推測都認為，手機將成為病毒攻擊的首要目標。

手機病毒比電腦病毒更集中於取得個人資料，轉售圖利——在地下市場，一個有效的電郵地址可賣得數元美金。如果黑客可以轉售你整個電話簿的資料，收入幾可等同中了彩票。個人資料有價有市，所以黑客總是前仆後繼。新電腦產品面世後，會陸續出現免費下載的服務，但不少「服務」其實由黑客提供，目的是入侵裝置，我們必須小心提防。

小結：五大陷阱

五大陷阱總結如下：

1. 虛假訊息（包括釣魚電郵及假網站）
2. 粗疏密碼
3. 網絡罪行
4. 侵犯版權
5. 流動裝置

五大陷阱現已橫行網上世界，推測還會肆虐一段日子，怎麼辦呢？以下教大家三招，絕對足以應付五大陷阱。

招式一：認識電腦罪行

大家應該不會刻意犯罪，卻可能不知不覺地犯法。我們可能只想把有趣的檔案分享給朋友，卻無意中變成第二個「古惑天皇」，觸犯《版權條例》。因此，我們應該熟悉相關法例，才能確保自己不越雷池半步。

其中一條值得大家細閱的條文，是《刑事罪行條例》第 161 條「有犯罪或不誠實意圖而取用電腦」。名字聽來複雜，但內容簡單來說就是檢控黑客的一切行為。條文如下：

> 任何人有下述意圖或目的而取用電腦─
> (a) 意圖犯罪(不論是在取用電腦的同時或在日後任何時間)；
> (b) 不誠實地意圖欺騙(不論是在取用電腦的同時或在日後任何時間)；
> (c) 目的在於使其本人或他人不誠實地獲益(不論是在取用電腦的同時或在日後任何時間)；或
> (d) 不誠實地意圖導致他人蒙受損失(不論是在取用電腦的同時或在日後任何時間)，
> 即屬犯罪，一經循公訴程序定罪，可處監禁 5 年。
> ……（後略）

觸發法例者最高可被監禁五年，可見這是嚴重罪行。大家應該不會符合(a)、(b)兩個條件，但如果我們希望既不購買正版影音產品，又能欣賞影片或音樂，便屬於(c)的範疇。不購買正版而欣賞影音作品時，我們亦令版權持有人蒙受損失，亦符合(d)的條件。請注意，條文所說的「利益」，不一定指金錢利益，而包括一切「保有已有之物的獲益，以及取得未有之物的獲益」，範圍頗為廣泛。

要更清楚說明「利益」的定義，可參考以下案例。

> **個案：前高官醫療紀錄外洩**
> 某位前高官的醫療紀錄外洩，洩密人士本是醫院員工，有權瀏覽病人資料，但僅限於工作用途。他卻認為公眾對該前高官的健康狀況具有知情權，於是以「公義」為由，把資料寄給報館。
>
> 然而，終審法院裁定他不但侵犯私隱，更觸犯電腦罪行，因為他在事件中有所「得益」——他並非在工作期間獲取資料，因此本來不應該得悉該前高官的病情，而獲得某些資料，本身就是得益。

資料本身，就是一種益處。股價內幕消息便是好例子——如果我預先得知某股票的價格會飆升，我便可以趁早入市，大賺一筆了。以上個案之中，洩密人士有沒有把消息賣給報館並不重要，亦不涉及法律問題；他以不誠實手法獲取資料，這已值得詬病。由此可見，「得益」可以與金錢完全無關。

如果大家仍然認為法例過於複雜，難以明白，更簡單的做法是在分享某些資料前，嘗試向身邊的人解釋你要做的事，你會感到尷尬嗎？如果你感到尷尬，那上載資料大概會令他人受損，即是違法了。這就像商界一個叫 TV test 的概念：如果無法向傳媒公開解釋某種行為，即代表該行為有問題，不應落實。

招數二：先認證，後認真

為避過內容陷阱，我們收到任何消息後，應該先認證消息來源，確定消息屬實後，才認真處理，這樣便能篩除虛假消息。

如何認證消息來源呢？首先，我們可以善用 Google 等搜尋引擎。如果我收到一則聲稱來自英國廣播電台，而內容有關輻射的消息，可能我在 Google 搜尋一下「BBC」和「radiation（輻射）」等字眼，便找到 BBC 澄清輻射消息不實的聲明。第二，我們可以瀏覽一些羅列網上假消息的網站。例如 http://www.snopes.com，內容便非常齊全，而其用法接近搜尋器，方便我們找出各種各樣的謠言和假消息。

偽冒網站方面，著名防毒軟件 Norton（諾頓）可以核實網站的真假和安全程度。另一有名防毒軟件 McAfee，其 Site Adviser 配件也會為用家指出可疑的網站，包括「未知有問題」和「已知有問題」的網站，「已知有問題」的當然就不要冒險瀏覽了。大家可以同時安裝兩個防毒軟件，取得雙重保障。

順帶一提，某些網站會突然叫你安裝程式，可是那些程式幾乎肯定是帶有病毒的，大家千萬不要下載。

招數三：保密、密碼、加密

密碼必須安全並定期更換，而且不要所有網上服務都使用同一密碼，也不要設定容易回答的安全問題。但是，謹記密碼只是一扇門，黑客仍然可以將之一腳踢開，因此加密也必不可少。資料本身要保密，不要隨意公開，然後設定密碼，加密內容，三者缺一不可。

設定密碼後，我們可能也要設定保安問題，那怎樣的保安問題才算安全？我們最好把保安問題設得刁鑽一些。為求安全，你的問題甚至可以就是要求回答者再打

一次密碼，因為只有不知道密碼的黑客才會選擇回答保安問題。可以的話，我甚至不會設定保安問題，減少給人入侵的途徑。較新的網站不會在你答對保安問題後直接提供密碼，而會將之寄到用以登記帳號的電郵地址；這做法稍為安全，最少黑客要先攻破電郵才知道密碼。

另外，我們經常使用 USB 儲存資料，但這並不安全，報章也經常刊載因遺失 USB 而洩密的新聞。我工作的機構卻從未發生這種事故，因為我們習慣加密 USB 的內容，規定了只可於我們部門的電腦中顯示。我們不怕遺失 USB，因為黑客只會得物無所用。

不論工作還是身處家中，都應該想方法使機密的資料只可循特定途徑閱覽。經加密的 USB 操作較慢，也較麻煩，所以如果有其他選擇，部分員工可能寧願用較危險卻較方便的方法。我們一定要考慮周詳，不但要為裝置加密，也要確保身邊的人保護機密資料。有些公司採用了非常精密的保安措施，卻仍然容許風險較高的活動繼續進行，最後還是於事無補。

小結：三大招數

1. 認識電腦罪行
   若要簡單地避免犯法，我們可以想像：如果把我要從事的某種電腦活動放上 Youtube，我會感到尷尬嗎？如果答案是「會」，那麼該行為很可能有問題。記著，以不誠實手段使自己得益或令他人受損，皆屬違法。

2. 先認證後認真
   互聯網的資訊很多，大家應該先核實其真偽，之後才認真對待。舉例說，維基百科的內容非常豐富，我也經常從中蒐集資料。然而，得到資料後，我會再參考較權威的資料來源，核實內容真偽，才於日常工作裡應用。維基百科的作者不一定特意作弄你，但資料可能在過時後未有更新，因此「先認證後認真」非常重要。
   要驗證網站真假，可以使用 Norton 或 McAfee Site Adviser。至於傳言真假，則可求證於 Snopes。

3. 保密、密碼、加密
   我們要保密資料，也要設定密碼。密碼要定期更換，也不應以太易猜到的字眼構成。不要所有服務都使用同一密碼。之後，仍要加密內容，這樣黑客即使攻破了密碼一關，仍會一無所獲。