資訊保安常見問題–家長篇

1. 我的子女在上網時，會遇到什麼危險呢？

以下是孩子在上網時會遇到的一些危險:

接觸到不良的資訊

互聯網上的資訊也許並不是全部適合他們的，例如一些有關色情、暴力、賭博、 違法活動 或毒品的網站等。

透露私人資料

有些孩子或許會在瀏覽網站時透露私人資料，例如在網上填寫表格和參加網上遊戲時透露信用咭資料、密碼、個人或家人資料等。這些網站會把收集得來的資料用在違法的活動上，如用作網上購物，再將費用轉收我們。

網上聊天

在互聯網上,任何人都可以隱瞞真正身份，假裝其他人或事物。例如，孩子在聊天室或許會遇到一些變童癖者，他們會嘗試成為你子女的朋

友，再向他們收集個人資料，更可能安排與孩子會面。

網上騷擾

你的子女可能會受到網友的騷擾，如收到無禮的或帶恐嚇性的電郵或網上訊息。

入侵者和病毒

在互聯網上，有些人是熱衷於入侵他人電腦作破壞或散播電腦病毒。然而，很多小朋友並不小心或沒有適當地保護他們的電腦，這樣會增加入侵者成功入侵的機會。

觸犯電腦罪行

電腦罪行包括在未經授權下進入他人的電腦系統、撰寫和散播電腦病毒來攻擊他人的電腦及侵犯版權等。小孩子很容易受到入侵電腦時的挑戰和刺激感所吸引。

2. 有沒有提示或指引可以給我教導子女適當地使用互聯網？

以下提供一些適當使用互聯網的指引以作參考:

- 不要完全相信網上的事或人。在網上所得到的資訊,不一定是對的;而於網上所認識的朋友亦可以是假裝的。
- 要視在網上認識的新朋友為陌生人。
- 不要單獨或在沒有監護人的陪同下,與網上朋友約會。
- 不要透露個人資料,如聯絡電話、住址、信用咭資料或家庭詳情等。
- 不要與任何人透露或分享密碼,即使是好朋友也不例外。
- 不要花太多時間在互聯網上。
- 不要回覆濫發郵件、帶騷擾、恐嚇性的電郵或網上訊息。最簡單有效的方法就是不加埋會,並將它們刪掉。
- 不要下載任何盜版軟件、音樂或視像檔案。
- 不要在網站內接受不清楚的條款。
- 如子女需要在網上訂購東西,必先要得到你的批准。此外,如你可親自替他們訂購會更好; 切記於可信的和有保護的網站訂購。
- 當子女在網上遇到一些奇怪的或令他們感到氣憤或不安的東西時,鼓勵他們與你討論。

- 尊重及親切地對待網上朋友。
- 確保電腦的操作系統及軟件已安裝和執行最新的版本及修正檔案。
- 先用防毒軟件掃描所有從互聯網下載的檔案，才開啟使用。
- 不要參與網上賭博。

此外，這裏有些關於互聯網安全守則的例子，以供參考:

- 學生承諾

  (http://cesy.qed.hkedcity.net/chit/intro_students.php?t=3)
- 家庭互聯網安全約章

  (http://www.icra.org/_zh-hk/kids/familycontract/)
- The Safe-Surfing Contract - Using the Internet （英文版）

  (http://www.wiredkids.org/documents/safesurf_agreement.html)

3. 我的子女經常整天對著電腦，究竟他們是在做什麼呢？

互聯網可以說是一個大型的圖書館，你可找到很多不同種類的資料及

訊息。你應該鼓勵子女在互聯網找尋有用的資料去幫助學業及增進他們的知識。同時，互聯網也是一個提供娛樂的地方，他們可以在互聯網觀看電影、收聽音樂及參與遊戲等。

你應教導他們不要盡信在互聯網找到的東西及訊息，因不是所有的也是正確或真實的。他們應學習如何分辨真偽，及判斷資料及網站的可信性，例如從網站的主旨及網主的身份背景等。如可以的話，與子女一同上網和教導他們如何適當地使用互聯網。

此外，你也要確保你的子女不要過份沉迷在電腦及互聯網上。除了在電腦中可得到樂趣外，孩子亦需要有其他活動及興趣，例如運動、家庭和朋友。

你也要提醒他們在上網、網上購物、電郵通訊和結識網上新朋友時要提高警覺，避免披露個人資料，小心入侵者和病毒入侵，與及不要參與違法的活動。

4. 什麼是ICQ？我的子女用 ICQ 有什麼危險呢？

ICQ 是一種即時通訊的應用程式，兩個用戶可通過互聯網進行即時對話。透過 ICQ，你的子女可與朋友聊天，傳送文字訊息、檔案及電子賀卡給他們的朋友。

可是， ICQ 的設計比較簡單，並不是十分安全。黑客可利用 ICQ 進行攻擊、偷取資料及散播病毒。

以下是一些使用ICQ 的安全貼示:

1. 以電郵作為通訊工具會比使用ICQ 較為安全；
2. 小心保護ICQ 密碼，不要將密碼儲存在電腦內，以及要定期更換密碼；
3. 不要披露個人資料，如電話、照片及地址等，尤其是陌生人；
4. 只接受認識的朋友所發放的訊息及檔案；
5. 開啟檔案前先用防毒軟件掃描一次;
6. 定期執行電腦病毒掃描及更新病毒碼檔案；
7. 其它人需要你子女的授權才可將你的子女加到他們的通訊列內；
8. 盡量隱藏IP 位址，以防止針對IP 位址的攻擊;

9. 使用最新版本的ICQ軟件(只在可靠的ICQ網站下載)；

10. 不要跟在ICQ認識的新朋友會面，除非有父母或監護人的陪同(至少在初次會面時)；

11. 不要花太多時間於ICQ上。

5. 我已在孩子的電腦上安裝了防毒軟件，我是否可以從此安心，免受病毒的入侵呢？

這是不足夠的!沒有最新的病毒碼，你的電腦是可以受到新病毒的入侵的。你應教導你的子女定期更新病毒碼，大約每星期一次或當有新病毒碼推出時。此外，你亦應定期掃描病毒及啟動防毒軟件的自動保護/即時進行掃描的功能。

6. 假若我子女的電腦受病毒感染，我應該怎辦？

如果不幸發現有電腦感染了病毒，請不要慌張!你要暫停受感染電腦正在運行的程式，並用防毒軟件的清洗病毒功能，或根據防毒產品/服務供應商提供的方法進行病毒清洗。當病毒已被消除，你可從備份中復原檔案。

其實，對付電腦病毒的最好方法是預防感染。你應該確保所有電腦都

裝上防毒軟件，並使用最新版本的病毒碼檔案。同時，你亦應該提醒你的子女在開啟電子郵件附件、從互聯網下載的檔案及磁碟前，先掃描檔案才開啟使用。此外，你們必須預備重要程式及數據的備份；當受到病毒感染時，最有效的復原方法是從備份中取回檔案。

按此(http://www.infosec.gov.hk/tc_chi/virus/virus.html)看更多有關電腦病毒的資料，包括最新病毒警告、病毒種類及預防電腦病毒的指引等。

7. 我收到一些關於電腦病毒警告的電郵，要求我將這封電郵轉寄給所有我認識的人。其他人對我說電郵內的訊息有可能並不是真的，我應該怎樣分辨呢？

有些人會發出虛假的電腦病毒警告的電郵，並利用互聯網散發給其他人。我們通常會稱這類電郵為“惡作劇電子郵件”。你們可以按此(http://www.infosec.gov.hk/tc_chi/virus/types_om.html)看有關惡作劇電子郵件的資料和辨認方法。

8. 有些報導指出一些仿冒網頁或騙案郵件騙取他人的帳戶和信用卡資料。我如何教導子女避免這事情發生在他們的身上?

有些仿冒網站會偽裝其他網站來套取你的信用卡或其他個人資料。另外，有些騙案郵件，內容帶有行騙及欺詐的成份；更有些電郵會誘使收件人按超連結進入仿冒網站，套取個人及銀行資料，例如帳戶密碼、信用咭號碼等。

以下有一些貼示供你的子女參考:

1. 不要從不可信的網站或電郵的超連結進入網站；
2. 要確保你所瀏覽的網站是你要去的，最安全的方法是自己打下網址或從瀏覽器的書籤中選取；
3. 如需要在網上購物，應該選擇可靠及有保護的網站，例如使用 SSL 及 SET；
4. 要小心處理個人或銀行資料，銀行是很少會經電郵要求這些資料的；
5. 確保你的電腦已安裝最新版本的修正檔案及防毒軟件。

此外，你亦可於以下的地方找到更多有關這方面的資料:

- 瀏覽網頁及網上購物須知

(http://www.infosec.gov.hk/tc_chi/yourself/surfing.html)

- 電台節目: 提防網上陷阱 (Real 格式)

  (http://www.infosec.gov.hk/tc_chi/youngsters/files/infosecfamily_02.mp3)

- 網上銀行 - 安全理財

  (http://www.hkab.org.hk/PDF/customer_info/ebanking_c.pdf)

9. 我聽說一些青少年攻擊他人的電腦，請問這是犯上電腦罪行嗎？

青少年很容易受到入侵電腦時的挑戰和刺激感所吸引。攻擊他人的電腦是犯上電腦罪行，後果嚴重。你必須要知道現存的電腦罪行的相關條例或法律，再警告你的子女觸犯罪行的嚴重後果。你可以瀏覽以下網頁獲得更多相關的資料，如罪行種類、有關法例及電腦罪行真實個案等。

- 電腦相關罪行

  (http://www.infosec.gov.hk/tc_chi/crime/crime.html)

- 相關條例

  (http://www.infosec.gov.hk/tc_chi/ordinances/ordinances.html)

10. 我的子女想和網上認識的新朋友會面，我應該准許他們嗎？

在互聯網上，一個人可以偽裝成任何人或事；他們對你的子女友好或許是另有目的。固此，你應該教導你的子女要視在網上認識的新朋友如陌生人一樣。你不應讓他們在沒有你或長輩的陪同下，跟網上的新朋友會面(至少在初次見面時)。