如何提防網上詐騙

普遍常識

大多數的網絡罪犯祇是普通的騙子，他們專門利用人類的貪婪野心,或盲目的信任順從,又或是孤獨的恐懼心態。如果有人給你一個難已置信的價格做買賣，這可能真的是不可相信。如果察覺到有些事情似乎不太尋常或大不可能,這或者真的是一個騙局。

選擇強而有力的密碼

不同的賬戶(account)用不同的身份 (ID = Identification) 和密碼 (Password) 的組合，盡可能避免寫在隨處放置的零散紙張,容易遺失,可以考慮用手機內可幫你保存多個密碼的軟件。將大小字母、數字和特殊符號混合,組成複雜的密碼，並要定期更改,如一年兩次,與春未及初秋更改夏令時間之際同步並進。

保衛您的電腦

引用你的防火牆 (Firewall) 作為網絡入侵防禦的前線，這軟件會阻止不明來歷或虛假網站的連接，也可將某些類型的病毒和黑客拒之門外。使用抗病毒軟件(Anti-Virus)如 AVG, AVAST,及抗惡意程式 (Anti-Malware)如 IObit Maleware Fighter, Malwarebytes Anti-Malware,他們可防止病毒通過安裝來侵蝕您的電腦，並會定期更新殺毒軟件。

阻止間諜軟件 (Spyware) 的刺探

安裝和更新反間諜軟件如 Malwarebytes Anti-Malware,IObit Maleware Fighter, 勿讓它入侵您的電腦。

入社交媒體及網絡時必須提高警覺

確保您的社交網絡個人資料（如 FaceBook 臉書，Twitter 嘰喳網，YouTube 遊視頻）的設置列為「私人」(set to “Private”)。請檢查您的安全設置,小心你在網上發佈的信,一旦你將資料放上社交網絡,就是永遠都會存在。

保護您的各樣手提電子工具（手機、手提電腦、平板電腦等）

您的手提電子工具是很容易受到病毒和黑客的攻擊。祇選擇有良好信譽的網址來下載須要的應用程序式。盡量不要用機內的環球定位(GPS = Global Positioning System)功能，以防你曾經到過的地方位置自動被地理標記 (geotag) 每一張照片,將你的行踪暴露給所有人,包括歹徒。

安裝最新的操作系統更新

保持更新您的應用程式和操作系統(在 Windows 微軟視窗,Mac 萍菓,Linux 騏驎)。開啟自動更新設置功能。

如何提防網上詐騙

保護您家中的數據

將您最敏感的文件加密 (encryption)，如納稅申報，對重要的數據作定期備份(regular backup)，並將其存儲在其他安全的地方。

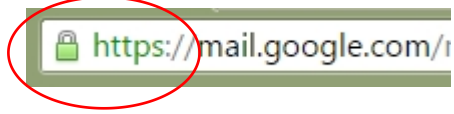
保護您的無線網絡

如果沒有適當的安全設施，家庭 Wi-Fi 無線網絡將會很容易受到入侵。應查看和修改默認設置(Default Setup)。公眾地方公開的 Wi-Fi Hotspot "熱點" 多數不設防衛,應避免在這些網絡上進行敏感的交易。

保護您的電子身份

在網上購物，當你要交出你的姓名、地址、電話號碼、財務信息、出生日期等私穩資料時,千萬要特別小心,確保此交易網站是安全的（請看下圖)。當你使用社交網絡時,要確足你已啟用了隱私設置 (Privacy setting)。

安全網站顯示在地址欄為:



避免被騙

在點擊來歷不明的鏈接或文件之前一定要想清楚,不要屈服於電郵的壓力下而行差踏錯。檢查電郵來源和堅持要驗證。千萬不要點擊任何連接或回覆那些要求您確認您個人信息或確認用戶身份 ID 和密碼的電子郵件。

請到「加拿大反詐騙中心」網站或致電舉報有關詐騙的信息。
www.antifraudcentre.ca
1-888-495-8501

有關「網上欺凌」Cyberbullying 的更多信息，如何保護自己，如何保護您的公司,請到這網頁查詢: www.getcybersafe.ca

請求合適的人幫忙

如果你是一位受害者，或在互聯網上遇到非法內容（如剝削兒童），或你懷疑有某人用電腦作奸犯科、身份盜竊 (Identity Theft)或商業騙局等等，請將此情況報告給當地警方。

- 本文大部份從點城警察局反網絡罪行小組發佈的資料中翻譯 -