網路安全防衛與互聯網安全

front porch

Piers Project (Piers企劃)

工具盒和資源指引 (2019年版)

Front Porch Center for Innovation and Wellbeing之倡議

協力贊助商

California Lutheran Homes

Front Porch, 為一服務民眾的非營利機構，其特色是根據個別人士因步入老年而引發的不斷改變的需要而設計創新的社群和計畫。機構獲代表昔日退休社群居民Ellie Piers家屬慷慨贈于一筆款項。

Ellie Piers

這贈予有助 Front Porch Center for Innovation and Wellbeing (FPCIW) 一直致力使用科技來促進耆老康泰的使命。Piers曾住在位於加州卡爾斯巴德(Carlsbad)名為 Carlsbad By The Sea的 Front Porch一處退休社區。她的貢獻讓CIW可通過知訊科技來開發應對長者安全防衛的問題，不單于大聖地牙哥地區制定與長者上網安全相關的措施，也讓各地域的社群能一同通過跨越地域的互聯網來使用。

對於科技，Piers有求知和冒險的精神且相信科技能説明長者安居樂業。她抓緊利用科技來與朋友和家人聯繫的機會，但也意識到用這些科技時會同時出現的安全防衛問題。Piers 對使用科技帶來的危險有敏銳的觸角，每次勇闖網路世界前都習慣仔細提問讓她都能達成每個「上網流覽」的目的。為讚揚Piers 的助人精神，FPCIW 成立Piers Project，通過下面的策略來解決長者上網安全防衛問題和提高他們對此的意識：

- 實驗有關長者上網安全的新科技並研發跟長者上網安全的內容，
- 接觸大聖地牙哥地區內在這方面有專門知識的各團體來建立合作社運用捐款提高有關長者上網安全防衛的關注和影響；
- 尋找可提升住在大聖地牙哥地區的長者有關改善生活的科技的意識的媒體，和
- 締造一網上和社交媒體運動來讚揚Piers對改革長者的優質生活這一重要範疇的殷切和饋贈。

這個由FPCIW創建的工具盒可用作為一本指引幫助各位更瞭解網上世界存在的一些風險，並在享受互聯網優勢的同時可主動和自信地避免這些風險。

目錄

你知道嗎…

- 2016年， 在美國65及以上的人中有百分之67 (67%)在用互聯網[1]。
- 在 24 樁耆老受虐的案件中，只有一樁有舉報[2]。
- 2017年，耆老因財務上受虐，損失了17億美元之多[3]。
- 有百分之45 (45%)財務上受虐是從使用互聯網開始[4]。
- 有百分之 59 (59%)的人說他們不肯定他們在傳播媒體看到的資訊的真假[5]。

今天，科技已成為我們日常生活中不可或缺的工具。我們通過互聯網與親人交談，進行網上理財和網上購物。在臉書(Facebook) 或推特(Twitter) 等社交平臺上聊天和搜尋一些我們有興趣的主題。互聯網有許多的裨益，可是，我們如何安全地享用這浩大的數碼世界呢？

作為數碼社會的活躍成員，我們實踐良好的互聯網衛生非常重要。我們需要洞察有些人會用不合宜的伎倆來濫用我們的個人資料，可能導致我們個人的、社交上的，和/ 或錢財的損失。正如任何有用的技能，重要的是，要採取有助於減低風險的預防措施，可讓你舒適地、安穩地和安心地享用互聯網的好處。我們的力量和控制權來自我們的知識和能與人分享我們的經驗。

設計這工具盒是要它成為長者安心使用電腦的資源指南這工具盒內的課程內容都基於三個簡單卻重要，關於湊效而又安全的上網經歷的規則。

1) 查究你在網上見到的內容，
2) 查證其可信性和真實性，和
3) 查問你的朋友、鄰居或同事來幫忙，並教導你週遭的人。

網絡安全防衛及長者成為詐騙目標

網路安全防衛是指一般性互聯網的安全防衛，專注于儲存在電腦內的或可通過互聯網取得的資訊的防衛。利用各種科技方式（包括電腦或互聯網）進行的詐騙層出不窮。

任何使用互聯網的人都有可能成為網路罪犯的目標，但為何大多數犯罪目標都是長者呢？長者多半是經濟較為穩健，多半不會舉報詐騙；或許是不知道怎樣或往哪舉報這些事故。長者也可能投資大量金錢于一些偽稱可促進記憶力、長壽或強健體魄的產品。

因著感到丟臉和害怕，長者傾向于少去舉報犯罪行為，從而助長了這類牽涉錢財的罪行傷害更多的受害人[9]。若你過往曾是網路罪行的受害人，**你要知道你並不是唯一的受害人**，許多人也有相同的遭遇。

更重要的是，所有可能使用消費者技術不熟悉的人都會學習積極避免網路詐騙的伎倆。Piers Project 工具盒的目的是要防止長者遭網上的欺淩和使他們有能力在進行安全的上網活動的同時能獲取資訊科技的許多好處。

該相信誰? 識別冒名頂替的人!

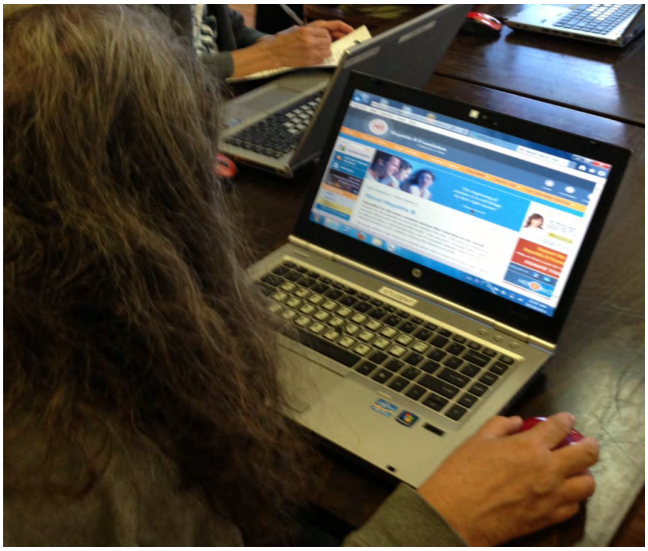
互聯網眾多好處之一是讓我們能在這平臺上處理日常生活的多個範疇：這包括健康、稅務或財務。我們能易於搜尋所需的資訊，在需要協助時也能瞬間即可跟適當的人連上。在使用互聯網時，能辨識和篩選騙局及撞騙的人是很重要的。

當有人未得你本人許可或同意而取得或使用你的個人資料即做成身份盜用。這資料將可用作訂購/購買東西、領取社安退休福利、盜竊你的個人錢財或進行其他犯罪行為。身份盜用的受害者可招致各種虧損的後果。曾出現的案例有非法複製護照、信用減少或聯邦醫療保險/州政府醫療援助詐騙。下列是需要警覺的常見的騙局的清單及你應如何採取防衛措施來穩妥地上網。

醫療保健騙局 這類騙局可以不同的形式出現：包括與事實不符的電視宣傳，訛稱因新法例而產生的新醫療卡或來電者承諾醫保的大折扣。

1) **查究**你在網上見到的內容，
2) **查證**其可信性和真實性，和
3) **查問**你的朋友、鄰居或同事來幫忙，並教導你週遭的人。

其他騙局包括有冒稱的詐騙，他們訛稱為政府公職人員需要你的聯邦醫療卡號來辦理新發的客戶卡。



你可以這樣做！

- ✓ **留意時事** 騙徒經常利用聯邦醫療保險及其他醫療計劃的改制及轉接期間，媒體亦在廣泛報導的時候出擊[註 6]。臨屆聯邦醫療保險接受辦理更調期間應謹慎和有所防範。由 2018 年 4 月起，因應刪除社會安全號的倡議[Social Security Number Removal Initiative (SSNRI)] 聯邦醫療保險及州政府醫療援助服務中心已開始改發和郵寄新聯邦醫療保險客戶卡來取締以社會安全號為編號的舊聯邦醫療保險卡。
- ✓ **勘查確定賬單是否真確** 提交你的個人資料前，應先聯絡聯邦醫療保險服務中心 (1-800-633-4227) 以防萬一 。你要明白聯邦醫療保險服務中心從來都不會給你打電話的，故此，若你接到電話，**切勿**提供你個人的任何資料。

稅務相關的詐騙 近日，訛稱填報W-2 的網絡釣魚電子郵件成為網絡安全的一大關注。騙徒正在尋找不同的方法發送看來像是來自雇主的首席或其他的行政人員的假電郵，要求雇員提供 W-2稅務資料。網絡罪犯隨即用獲取的W-2內的資料申報假的報稅表並偷取受害人的身份[7]。

你可以這樣做！

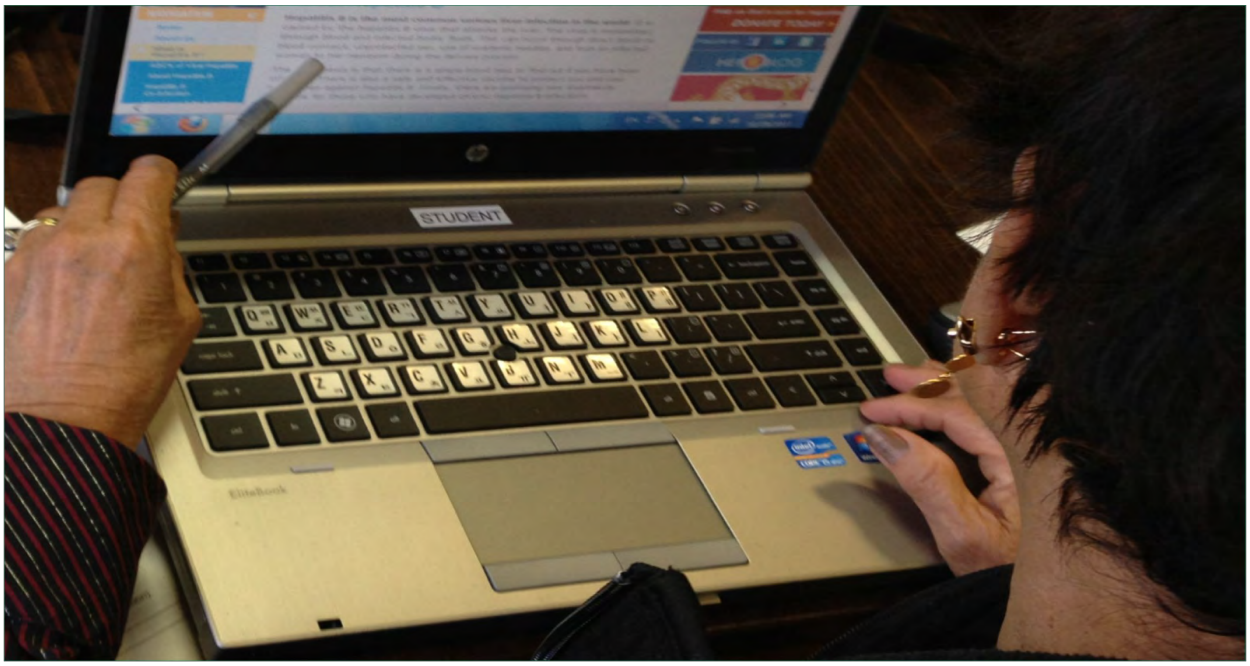
- ✓ **打通電話** 你若收到任何索取 W-2 稅表資料的電子郵件，請在發送任何資料之前致電貴公司核實該請求。
- ✓ **盡早報稅** 你愈早報稅，你將能夠堵塞網絡罪犯趁機冒你的名提交偽造的報稅表來襲擊你的漏洞。
- ✓ **定期查閱你的信用報告** 你可使用 AnnualCreditReport.com 提供一年一次的免費信用報告來免費查詢你的信用評分。發現任何可疑的活動時可立刻凍結該賬號。

彩票詐騙 這類非法行為包括偽稱你的彩票中獎了，而你須先付手續費才開始領取彩金。彩票詐騙騙徒常訛稱為某一實在的彩票機構或其他實在的機構來發出電子郵件。不要急，慢慢小心搜查資料來確定，電郵所述若顯得好得令人難以置信時，大概不會是真的啊。

投資詐騙 這些查詢涉及對你新開或現有的資金的投資 。可能亦有建議你投資不同的項目，如採礦、石油、氣油或一些新科技公司。“Prime Bank” (主要銀關)詐騙即為一典型例子。推銷員聲稱投資人的資金將用作購入及買賣一官方機關如聯邦儲備局保證的“Prime Bank” (主要銀關)發行的貨幣。他們更聲稱，此格式的投資機會僅通過獨家邀請，僅限於一組精選客戶。[8] 此外，由於國內的法規和監管，應對海外投資進行極度謹慎查核。

你可以這樣做！

- ✓**不要單憑外表來對一家公司作出評價** 有些網站可能看來繪聲繪影和正當，但這並不總是意味著它們值得信賴。
- ✓**咨詢合約的細節和條款** 我們建議要仔細審閱合約，因為人們常會忽略那些重要的細節。
- ✓**切勿輕信巨額的承諾** 這是誘餌電子郵件收件人的常用技倆。



電子郵件

電子郵件是在互聯網上的一主要溝通模式。可是，你怎知道哪一封是可以安心打**開**和哪一封**應刪除**？有**甚麼線索**可**隨**？以下是一些你**應認識**的**詞彙**和你如何**認**別你的收件箱內**潛**在的危**險**。

網絡釣魚(Phishing) **當騙子使用虛假的電郵或短訊誘騙你提供重要的個人資料，這即為「網絡釣魚」**(phishing)**。猶如「釣魚」，騙子試圖通過偽裝成合法安全網站的鏈接或虛假網站來誘導受害者。這是他們收集密碼、社會安全號、銀行**戶口資料等的方**式。**

垃圾郵件(Spam) **這是屬於不請自來的、漁翁撒網式的電子郵件用來進行多種網上詐騙。大多數的垃圾郵件是無傷大雅的或令人厭煩的廣告，但有一些卻能在未經許可下一面傳送病毒一面切入電腦和侍服器中。這種形式的詐騙亦能非法取得並出售你的隱私資料。**

駭客(Hacking) **一個未經你許可，遙遠地切入你的電腦或個人帳**戶就是駭客(hacker)。**任何利用電腦系統**內的弱點進行任何形式的駭客均屬非法和刑事犯罪活動。

奈及利亞信件騙局(Nigerian Letter Fraud / 419 Fraud) 這種行騙又稱為預付費詐騙(Advance Fee Fraud)，通過電郵索取你個人或有關你的銀行資料，聲稱發件人為一外地政府官員或一位需要經濟援助的外國人。這些郵件的收件人被慫恿將印有信頭的空白的公文紙，連同他們的銀行名稱和戶口號碼並其他隱私的資料等資料發給寫信人，亦可通過傳真號 (信中有提供)方式取得。[9] 看到從外國政府發來的電子郵件要提高警覺。他們都會請求你把大筆款額存到一家設於外國的銀行來幫忙。這類騙徒常是提出緊急的請求和催促你馬上提供經濟援助。同時，對美國政府發來的電子郵件也要提高警覺。例如，遇到有人聲稱從社會安全局辦公室發出訊息向你索取你的社會安全號時要小心注意。要三思！一般而言，這類機關是不會通過互聯網來向你索取你的個人資料的。

仔細看一下

網絡釣魚的垃圾郵件並不只限於來至奈及利亞： 對那些尋求以轉移大額金錢來幫忙的電子郵件要持懷疑的態度，這包括了看似是由你的朋友或家人發出的一個可疑的危急狀況。

David 你好！

我正哭着给你写邮件。我来伦敦度假，但不幸的是昨天晚上我在酒店附近被持枪抢劫了。我身上所有的现金，信用卡和手机都被劫匪抢走了。

我已经去大使馆和警察局报案了，但是他们并不帮助我。我的航班再过 8 小时就起飞了，但我没有钱付给酒店。酒店的经理说如果不付清账单就不放我走。我现在十分需要你的经济救援。我需要 1500 美金，我回去之后还给你。

你会帮我的对吗？我现在非常地慌乱无助。

Casey

這個例子裡你會察覺到這似是由所謂是你的家人發出一緊急要求的電郵有點怪異。注意其他不對勁的蛛絲馬跡並當心你熟識的人的電郵地址可能已經被駭客進入了。經常查究真確性，並跟另一位雙方都認識的家屬或朋友通電話來求證。

你可以這樣做！

✓ **注意電郵**內文的併字和文法 查核統一資源定位符(URLs)、電子郵件地址和電子郵件的內容的併寫。網路釣魚電郵常存在你可以察覺的不明顯的併寫錯誤。當你看著發件人名字時，多看清楚發送該訊息的實際電郵地址。另外，若你將滑鼠指針懸停在該鏈接上，你可能發現它實在引進到一可疑的網站而並非訊息內所承諾要引進的網站。

✓ **切勿打開那些不明來歷的電子郵件** 若一電子郵件、短訊或社交媒體的訊息是由一不熟識的人發出的，應刪除或不理它。對聲稱你需要申領金錢、禮物或度假優惠的電子郵件亦應同樣地謹慎：這訊息很可能會引你進入另一網站，在那裡你可會容易接到惡意軟件或電腦病毒。遇有可疑，丟掉它！

✓ **對電子郵件或短訊**內的網站鏈接要有戒備的心 若你接獲你認識的人發出的電子郵件，而其內容只載有一個網站鏈接，**切勿**點擊該鏈接。這常是顯示該電郵的主人可能已被駭客入侵了。遇到這情況，致電或用其他方式通知此人並刪除該電郵。

✓ **切勿通過電子郵件提供你的銀行賬號或個人資料** 你要明白銀行和保險公司等正規的公司絕不會通過電郵索取你的個人資料的。直接登入公司設有保安系統的網站才登入你的個人賬號來查閱通告和訊息。

1) **查究**你在網上見到的內容，

2) **查證**其可信性和真實性，和

3) **查問**你的朋友、鄰居或同事來幫忙，並教導你週遭的人。

仔細看一下

騙徒常盜用民眾熟識的公司名號來發送電子郵件令你覺得放心點擊附帶的連結網站。請讀下述的電子郵件。 請看以下這封看似來自百度推廣中心的郵件，你能辨識出這是一封「網路釣魚」**郵**件**嗎？**

若你不肯定點擊某公司發放的電子郵件內附帶的連接網址是否安全，最安**全的做法是另外開**啟一新的瀏覽器框頁，直接進入該公司的網站，再登入**你的賬號。若有關於你賬**戶的重要通告或訊息，這些通常會顯示在公司設**有保安防衛的網站**內屬於你的賬戶內。

发件人：邮件管理（由[illegible]代发）
时　间：2012-11-05 21:00
主　题：百度营销

推广中心于今天早上8点进行维护，
升级系统，为了不影响您的帐户正常推
广请点击《进入》首页查看您的帐户是
否正常生效，如帐户有异常请立即联系
推广顾问解决。

给您带来不变，敬请谅解！谢谢

百度推广中心

2012/11/4

保護你的錢財

使用互聯網理財是有許多好處的：網上購物的方便、安排支付帳目、即時資金轉帳。線上行銷金錢詐騙以多種形式出現，而最常見的詐騙牽涉使用信用卡和銀行賬戶資料，這些資料通常被用於購物、投資和稅務的問題。這些陰謀可通過偽裝的網站或電子郵件來獲取有關的資料。

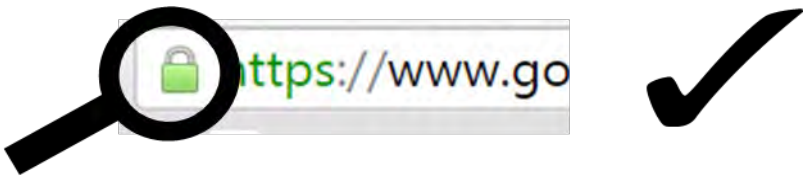
網上購物 詐騙行為包括提款卡或信用卡的使用。這可通過盜取該卡或非法地獲取持卡人的賬號、卡號、卡上的保安號碼、卡主的姓名和住址等個人資料進行。

你可以這樣做！

- ✓ **盡可能使用別的付款方法** 取代通過該網站直接付款，改用 PayPal、Amazon 和 Google Check Out 等設有多重保安防衛功能的付款服務機制 [註 10] 。可以的話，你亦可以用「賓客」的身份來結賬和選擇不貯存你的卡號在賬號內。
- ✓ **注意銀行月結單** 妥為整理你手上有效的信用卡清單並定期查看銀行月結單。若察覺任何錯誤或不尋常的賬目，應馬上通知發卡的機關。
- ✓ **儘可能採用信用卡** 使用信用卡一般較提款卡安全，因若遇上貨品沒有送出或貨不對板時，信用卡客戶是可以討回款項的[11]。
- ✓ **採用辨識能力最強的工具** 你可以採用辨認能力最強的工具，如生物辨識、保險鎖、或在你行動器材內裝置的應用程式採用獨特的一次性代碼來保護你網上購物賬戶[11]。

仔細看一下

查核掛鎖標誌 當你進入一網站時，一個小掛鎖出現在網址欄上，表示這網站是使用*較高*保安度的機制來傳送資料數據。雖然這標誌代表著某種保護，這也不能保證百分百的保障！



查證連接網站的網址 網站的鏈接表面看來真確的仍有可能並非真實的，故此必須萬分小心地看清該鏈接。舉個例子，該鏈接或許顯示“ bankofamericacard.com”或“ B-of-America”，帶有“ bank”或“ America”等字樣可使這些網站顯得真確，然而，它並非該公司網站的真確鏈接。

請查閱聯邦貿易委員會網站 www.ftc.gov 來瞭解更多消費者的心得和提示！

網上理財 當你穩妥地接連到你銀行設有保安防衛的網站或應用程式時，你將可以 安心進行網上理財。當你進行網上購物時，注意同樣的保安防衛標誌(綠色的掛鎖、“ https”和統一資源定位符(URL)的拼寫是否正確。以下是更多安全地進行網上 理財的心得。

你可以這樣做！

- ✓ **使用你個人的無線上網機制(Wi-Fi)來進行網上理財** 切勿使用免費或公眾的無線上網機制來進行任何牽涉敏感資料的事宜。
- ✓ **經常**查閱你的銀行月結單 看清月結單上你所購買的東西，確定都是你熟知的。若發現你賬號內有任何可疑的活動，務必馬上跟你的銀行聯繫。
- ✓ **離開你的銀行的網站或應用程式前必須先登出網站或應用程式** 你甚或可在登出後把瀏覽器關閉。
- ✓ **瞭解你銀行的保險規條** 遇上被電腦罪犯盜取你的銀行資料時，那麼你能提前知道你銀行在處理發生在你身上的詐騙事故而需報銷給你的條例和程序是很好的。申報的期限有多長及你能獲得多少的保障？

1) **查究**你在網上見到的內容，

2) **查證**其可信性和真實性，和

3) **查問**你的朋友、鄰居或同事來幫忙，並教導你週遭的人。

惡意軟件(Malware)

我們如何知道那些是可以安心點擊和那些不可？ 你希望能夠從可信賴的來源接收真正為你準備的訊息，故此這些是你應瞭解的一些重要事項。

Clickbait (**標題黨/釣魚標題**)指互聯網上的內容, **旨在吸引注意力並讓訪客點擊通往特定網頁的鏈接。有些標題或廣告或許會真正帶你通往一份有趣的文章或一所你可能想要購物的網上商店。然而，若網站採用很多標題黨的釣魚標題，這些多半是帶有惡意軟件的。**

惡意軟件(Malware) 惡意軟件(Malware，malicious software 的縮寫) 是一種旨在對一電腦系統造成破壞或令它無法運作的程序。使用行動器材時同樣要謹慎，因這些器材也免受不了惡意軟件和電腦病毒的襲擊。據維基百科(wikipedia.org)闡釋：「惡意軟件可以是鬼祟的，意圖盜竊資訊或在電腦使用者不知情下進行一段長時間的偷窺」。 惡意軟件有多種軟件類別：

勒索軟件(Ransomware) 這是 '*ransom*' (贖金)和 '*software*'(軟件) 兩字的組合。勒索軟件指任何能遙控地鎖住你的電腦，繼而提取貯存於電腦內的資料或提出需退還你被盜的失款而索取金錢上補償的軟件。發放這些惡意軟件的人可能訛稱自己是某官方人士，如警察等。勒索軟件的這些有害攻擊也可能針對智能手機和平板電腦設備。

病毒 存於人類中的病毒跟電腦中的病毒相類似。從技術性而言，病毒用電腦成為它們存在的主體。如此進行時，病毒即能繼續倍增並在你的電腦中作出自我調整來達成它們的任務，在襲擊時亦進一步散佈這惡意軟件到其他領域。

防毒程式(Vaccine programs) Vaccines(防毒疫苗)亦稱為「防毒軟件」(“ anti-virus software”)是用作預防或反擊惡意軟件的攻擊的工具。 確定你的電腦最少有一個有效運作的防毒程式(或 Windows FireWall，即視窗防火牆)來預防惡意軟件的攻擊。若你近期曾出現運作速度大幅減慢的情況，這些程式即尤為須要。

坊間有多種防毒程式，它們各有不同的防毒功能和售價。以下為一些常見的品牌：

- Avast
- AVG
- Bitdefender Antivirus
- Kaspersky Anti-Virus
- McAfee AntiVirus
- Norton Security

反惡意軟件程式(Anti-Malware Program) 視窗作業系統防火牆的作用為最基本針對惡意軟件的防衛，也可以內置到微軟視窗程式中。若是 Apple Mac (蘋果麥金塔) 用戶，要緊的是要確定從 Apple 的操作選項內啟用了軟件更新。此外，Apple 用戶必須在「系統優先選項」中允許設立定期更新檢查。如 uBlock Origin 等的瀏覽器擴充程式會屏閉追蹤你在電腦上的活動和裝置惡意軟件的廣告。

仔細看一下

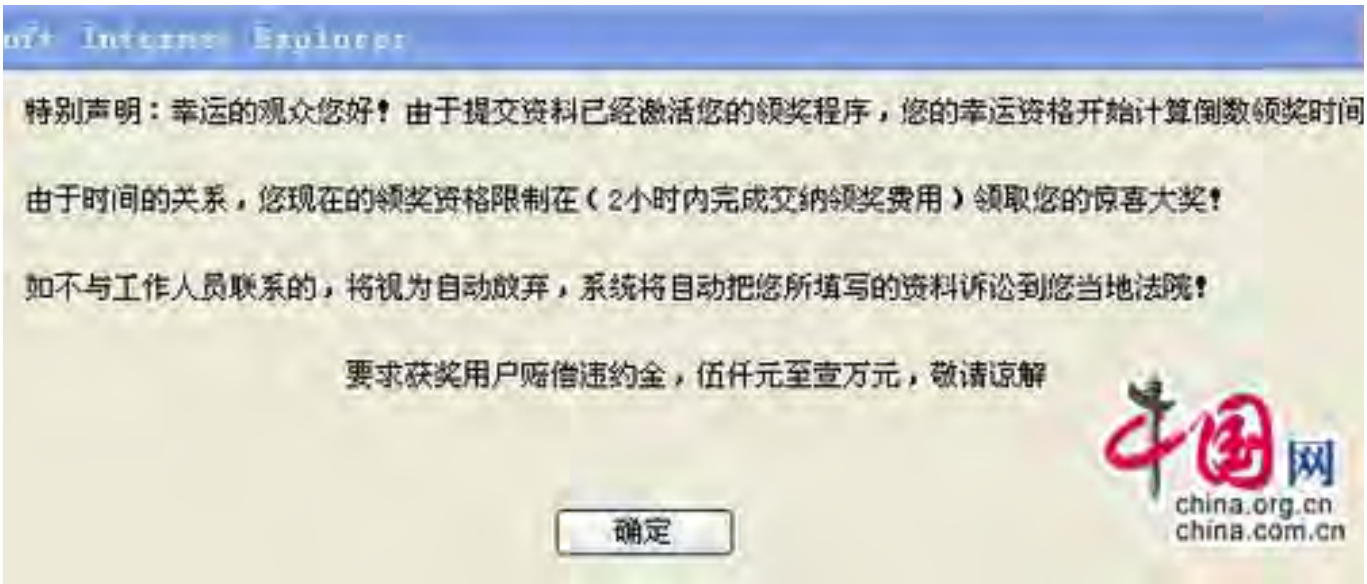
這些是你要在電腦內注意的紅旗警告訊號：

- 電腦停止運作或工序慢下來
- 發出異常的聲音或嗶嗶聲
- 不停彈出通告訊息
- 討厭的圖像
- 會消失的數據

定期查核你已裝置的防毒軟件的更新—再而進行全面徹底的掃描過濾來確定其運作[12]。別忘記每年續訂這些防毒軟件以確保你的電腦受更新的軟件防衛新的攻擊

你可以這樣做！

- ✓ **馬上關閉** 若遇有看來草率的自動跳出的廣告或網站，隨即點擊右上角載有「X」的方格來關閉該視窗。若你的瀏覽器或防毒程式對某一網站的安全提出質疑，切勿進入該網站[註 11]。
- ✓ **切勿下載**任何東西，除非你完全知悉那是甚麼及那是出自一安全的來源的。
- ✓ **廣告和跳出的視窗**常會看似一項系統的測驗警告訊息或聲稱你已中獎。切勿點擊它們。馬上關閉這些視窗並進行一次一般的電腦或器材的防毒掃描。下列是一些你應避開的常見的跳出的視窗。



密碼的安全保障

我們應將我們的個人資料如錢財—我們應重視和保護它。密碼安全保障是極為關鍵的，因為它是提供獲取你重要的個人資料的門徑—看密碼如同你家的門匙。保護我們自己重要的一環是創造一些別人難於猜測的密碼。

造出一個強而有力的密碼

- ✓ 造長的密碼。超過 6 個字符即算理想。
- ✓ 不要每個賬號都使用相同的密碼。
- ✓ 來個英文字母、數字及符號的大混合。
- ✓ 不要用如兒女的名字、出生日期、年齡、住址等的個人資料。
- ✓ 定期更改你的密碼。專家建議每 6 個月最少更改一次。

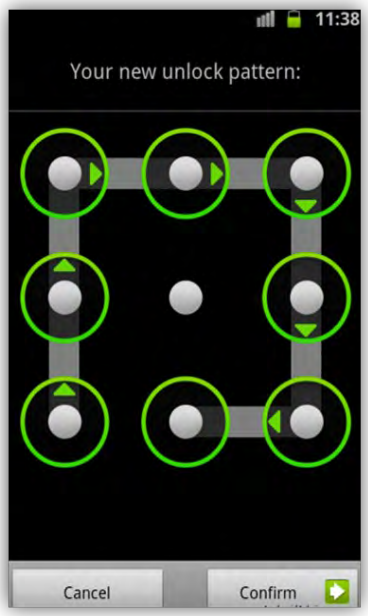
密碼管理員 密碼管理的程式能助你在多個賬號用同一個密碼。它們可在你已預先註冊的網站自動為你填上你登入網站的資料。請對這類程式進行個別的查考其利與弊，看那一個程式最適合你。下列為一些免費的程式，這些亦有提供收費的其他服務：

- LastPass
- Keeper
- Dashlane

你的密碼在名單內嗎?

駭客通過猜測我們的密碼來偷進入我們的賬號中。故此，切勿選用易於被別人想到的密碼。務必切勿使用下列的密碼：這些是 2018 年 25 最常使用的、因而是常被駭客入侵的密碼*

排名	密碼
1	123456
2	password
3	123456789
4	12345678
5	12345
6	111111
7	1234567
8	sunshine
9	qwerty
10	iloveyou
11	princess
12	admin
13	welcome
14	666666
15	abc123
16	football
17	123123
18	monkey
19	654321
20	!@#$%^&*
21	charlie
22	aa123456
23	donald
24	password1
25	qwerty123



請務必鎖上你的器材 無論是電腦、筆記本電腦、平板電腦或智能手機。 你的器材均能讓你設立密碼致使只有你才能使用該器材。

Two-Factor Authentication(**雙重辨識**) 啟動雙重辨識(2FA) **增加多一度保安防線以阻擋別人試圖**偷入你的賬號中。這是說就是某些人能猜中你的密碼，他們仍需拿到你手上的**電話才能**偷進你的賬號中。雙重辨識是這達成的：一些你知道的東西(**你的密碼**)**加上一些你手上拿著的東西(你的手機)**[13]。辨識工具也可以是某種生物特徵辨識、保險匙或通過你的行動器材上的應用程式采瞵的獨特的一次性代碼[14]。

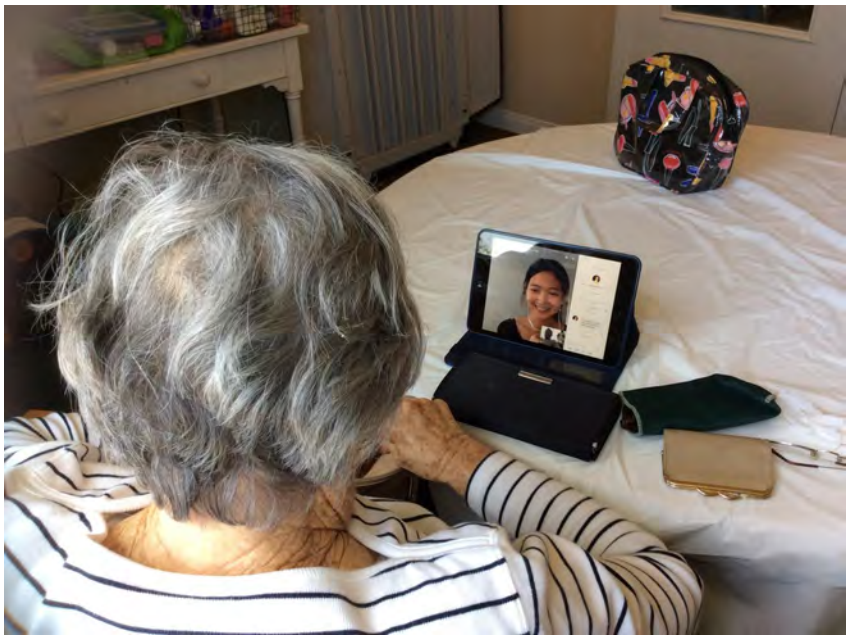
智能助理、智能家居和無線上網(Wi-Fi)

語音助理如 Amazon Alexa 在家居普及使用，要緊的是要明白有那些安全措施是你可以是用來守護你的隱私的。 IoT (又稱「物聯網」" The Internet of Things") 是指互聯網的功能容讓訊息可以通過物件和器材收發[15]。這包括任何智慧家居器材、電器用品、揚聲器、玩具、可配帶的衣物等。**常見的提問是**：「Alexa **有在收錄我所有的對話嗎？」亞馬遜網站**說明此問題的答案是否定的。它解釋**該器材是設計來只偵測喚醒語**(" wake word" **即** Alexa)，**此乃通過原聲結構來認出相配的喚醒語，故此沒有任何其他的聲音會被貯存或發送到「雲端」**[16]**。只要緊記當你使用任何與互聯網相關的器材，總有存在危機：具有惡意意圖的人可能會獲得某些資料。然而，照慣常一樣，緊記切勿在互聯網上透露或貯存任何敏感或私人的資料。**

麥克風「靜音」鍵和拔掉 語音首先設備，收音的器材是設有靜音按鈕的。**當你**啟動這功能時，就是你說出喚醒語，**那器材也不會有回應的。若你欲確保那器材**絕對不能聽取或收錄任何聲音，你**可以拔掉器材的插頭或把電磁拿掉**

無線上網(WiFi)路由器保護

無線路由器提供筆記本電腦和行動器材很大的自由度。但當你購買一部新的無線上網路由器時，它通常會帶有某人可能查找或猜測的預設配置。**務必更改其密碼並重命名無線網絡，好使你用於智能設備的互聯網源頭是安全的**[11]。



社交媒体和假新闻

社交媒體網路在過去幾年中變得非常流行。雖然它們容讓你可以隨時隨地跟朋友和家人聯繫，若你在這平臺上慎于你跟別人交流的內容，那就會較安全。

你可以這樣做！

- ✓ **切勿接受你不認識的人向你發出的交友邀請** 你可能會接到不知名人士發出的訊息稱贈送你禮物或門票，以此誘餌你點擊鏈接或安排親身會面。也要注意內置在新消息發放的帖文宣傳某些產品或服務。永遠都不要點擊可疑的鏈接，即使它們看似是來自你認識的一位朋友或一家公司。
- ✓ **請注意您分享的信息量** 你在網上社交媒體的背景資料可以分享大量有關你的個人資料。這包括你的住處、出生日期、你的喜好、家人等等。請注意您發佈的帖文–你原意是發給你的朋友，但因應你的隱私設定，騙徒也可能看到的。
- ✓ **嘗試臉書私訊或電子郵件的替代品** 加密應用程式如 Signal、Whatsapp 及 ProntonMail 等可提供額外的保安防衛。

✓查核你的隱私設定 在如臉書等的社交媒體平台上，你是可以管理誰可以查看你的背景資料、你發佈的帖子、你的活動、誰可以在你的時間軸上寫帖子及誰可以在照片上標示你。 明智的做法把你的設定提升至高度的限制，這樣即可你先審查你被標示在甚麼照片或帖文中，才讓別人在你的版面上看到。

仔細看清楚

看似是“ Like(贊)” ？臉書版面上看似是“ Like(贊)” 的按鍵或一個帶有誤導性圖像的視頻的屏幕截圖可會立刻吸引你的注意，這可能會不由自主地把你連接到你不需要的的購物網站，甚至造成病毒和惡意軟件的入侵。

要緊的是你能辨別在臉書帖文下方設置的真實「贊」按鍵標誌和最初看起來類似但卻是虛假的按鍵標誌。「標題黨」(Clickbaiting)令使用者對某些鏈接、照片、視像或文章感到好奇而點擊觀賞。有些此類虛假的故事或廣告宣傳只引領你到另一個網站，但有些是有破壞力的。然而，若因點擊喜歡一個項目而淪為這些圈套的受害者的同時，你更會不知情地為這些詐騙的帶有虛假的「贊」按鍵標誌的視像或影像做宣傳，可能使你網上的朋友也成為受害者。

社交網路上有很多博眼球的標題党新聞 – 保持安全上網計畫的參考網站的連結，積極管理你在多個平臺的隱私設定。

網上交友約會網站 網上約會可以是一個結交跟你有類同興趣的新朋友的好工具，只要你對自己決定跟別人分享的內容保持謹慎和敏銳。注意在約會的應用程式內可能有虛假的背景內容，那些人欲試圖使你點擊一個鏈接引你到一些帶來損害的網站。

你可以這樣做！

- ✓ **注意在他們的背景資料中的紅旗警告訊號** 當你在社交媒體或約會的應用程式內與某人連繫時，要曉得一個帶著一大串數字的名字可能是虛構的背景的徵兆。那些標題和文句似在暗示對方只在尋求肉體的歡娛嗎？
- ✓ **切勿點擊任何他們發出來的鏈接**經過幾次訊息的來往後，而你亦感到跟對方有更多的認識，你或許對交換電話來親身會面感到安心。但若交流對話缺乏內容而對方只單單發你一個鏈接，這可能會帶引你到一個滿載惡意軟件和病毒的網站–避免點擊這類鏈接，另找朋友。

虛假新聞 在今天的新聞及媒體中，是難以解讀甚麼是真確的和甚麼是虛假的。現今跟過往相比，人們可有更多門路汲取資訊；然而，真相並非總是如此清晰的，因為任何人均能在互聯網上載任何的資訊而又聲稱是真實的。那麼，你怎麼可以斷定哪些是可靠的新聞來源？

你可以這樣做！

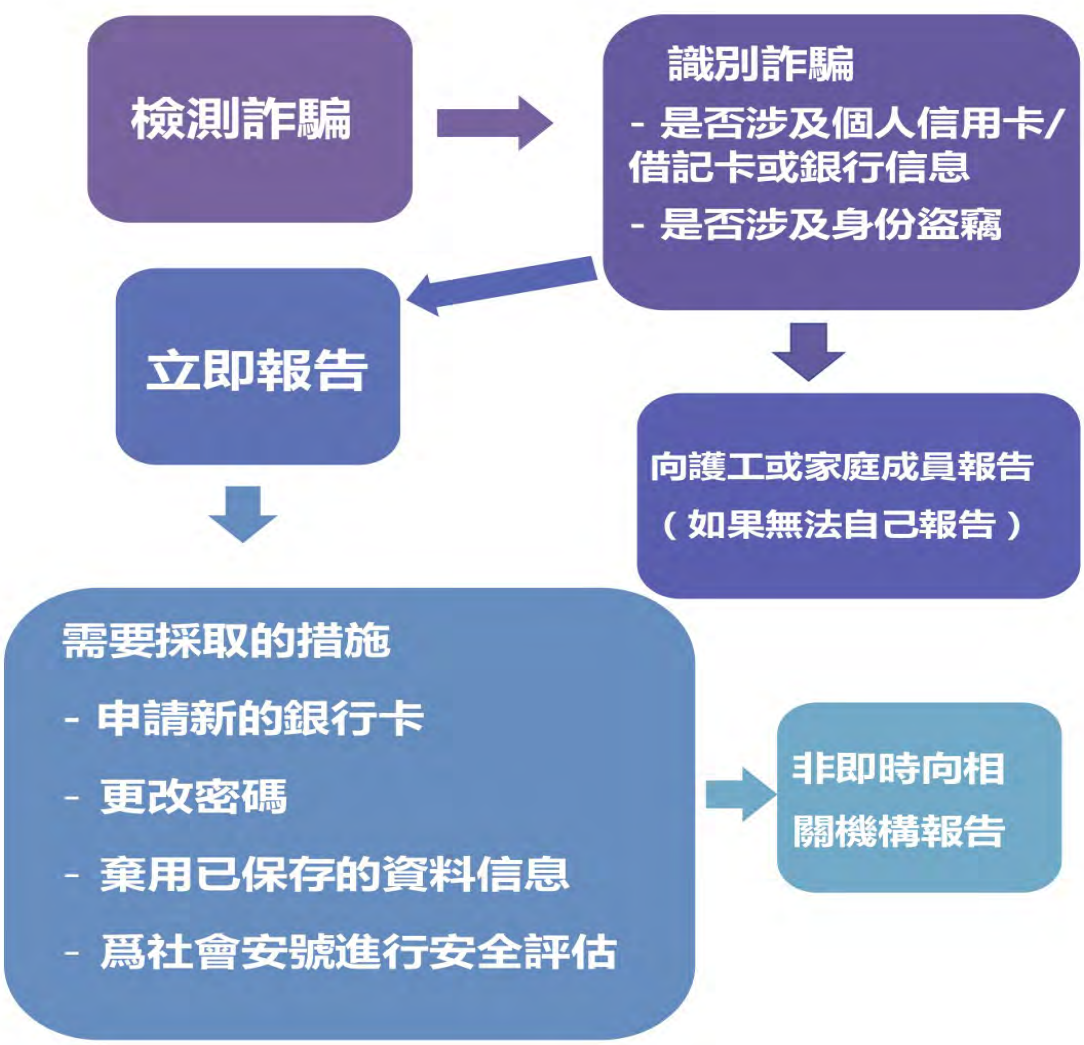
- ✓ **衡量該來源** 當你在網站上時，搜集有關該網站的資料。閱讀「關於我們」一欄，是誰在主理這網站？他們為何製作該網站？誰負責網站的經費及他們有偏重某些贊助商嗎？ 他們的資訊從何而來？你單查看網站的統一資源定位符(URL)末，你已能辨認不同級別的可信度。網站若是以「.gov」結尾，這表示這是一政府部門的網站而通常須經過多重審查及品質確認查核才得以發表的。

網站若是以「.edu」結尾，這顯示該網站是來自一所學校或四年大學，通常遵照學術準則來發放材料。

✓ 查閱有關參考資料若你瀏覽多個不同的、眾所周知的、有聲望的新聞資訊來源，雖然每個機構或有其偏向和立場，你可以從中辨識哪些事實均有其共通點？哪些是怪異的或似是開玩笑的？其他來源有證實這些資訊屬實嗎？

✓ **多搜尋考證** 查核資料發出的日期以確定其相對時事的適切性。可能的話向專家查詢或查閱事實考證的網站。

網絡詐騙應對程序



舉報機關

詐騙類別	舉報機關和聯絡方法
舉報一般的騙局(推薦)	**當地執法機關** 警方有責任協助你或轉介你到有關機構
舉報一般的騙局(推薦)	**Federal Trade Commission** 電話：1-877-382-4357 (電傳/TTY/TTD: 1-866-653-4261)
網路罪行和詐騙(推薦)	**Internet Crime Complaint Center** (IC3) 由 Federal Bureau of Investigation (FBI/联邦调查局) 和 National White Collar Crime Center (NW3C/全國白領犯罪中心) 合作組成。舉報互聯網上的罪行或詐騙。http://www.ic3.gov/default.aspx
举报医疗保险诈骗诈	**The Federal Trade Commission (FTC)** 電話：1-877-FTC-HELP (1-877-382-4357) 或電傳/TTY 1-866-653-4261 或流覽： ftc.gov/complaint
聯邦醫療保險詐騙	**Department of Health and Human Services** 電話： 1-800-633-4227 舉報聯邦醫療保險和州政府醫療保險**援助詐騙、揮霍和濫用** 電話： 1-877-808-2468 **Senior Medicare Patrol** www.smpresource.org **Office of the Inspector General** 電話：1-800-447-8477 或發送電郵至 spoof@oig.hhs.gov
身份盜窃罪行	**Identity Theft Resource Center** 電話： 1- 888-400-5530 http://www.idtheftcenter.org/knowledge-base/
針對西語人士與醫療相關的事故	**Su Familia: The National Hispanic Family Health Helpline** 周一至周五上午9时至下午6时（东岸时间） 電話： 1-866-Su-Familia (1-866-783-2645)
國稅局和與稅務相關的詐騙	**IRS's Identity Protection Specialized Unit** 電話： 1-800-908-4490 **Internal Revenue Service** 若你或你認識的人收到訛稱為國稅局發出的電郵索取個人或財務資料，請將該電郵轉發到國稅局：phishing@irs.gov.

詐騙類別	舉報機關和聯絡方法
国税局和与税务相关的诈骗	**IRS's Identity Protection Specialized Unit** 电话： 1-800-908-4490 **Internal Revenue Service（國稅局)** 若你或你认识的人收到讹称为国税局发出的电邮索取个人或财务资料，请将该电邮转发到国税局： phishing@irs.gov.
彩票骗局	**AARP Fraud Fight Call Center** 舉報任何外國彩票騙局 電話： 1-800 646-2283 **U.S. Postal Inspection Service** 舉報彩票或電子郵件詐騙 電話：1-877-876-2455
社会保障金诈骗	**Social Security Administration** 電話： 1-800-269-0271 (電傳/TTY: 1-866-501-2101) 10:00 am to 4:00 pm (東岸時間） http://oig.ssa.gov/report/
护照诈骗	**Department of the State** 聯絡 PassportVisaFraud@state.gov
商業詐騙	**Better Business Bureau** 登入其網站舉報 https://www.bbb.org/consumer-complaints/file-a-complaint/get-started
舉報網路釣魚電子郵件	**Department of Homeland Security, U.S. Computer Emergency Readiness Team** 電郵： phishing-report@us-cert.gov 或以電郵方式向Federal Trade Commission 申訴： spam@uce.gov 你可把網路釣魚的電郵轉發至 spam@uce.gov
舉報一般性的長者受虐	**Adult Protective Services** (成人保護服務)隸屬加州社會服務處。提供各項服務支援長者和需依賴別人的成年人士。可舉報疑為受虐的事故： 身體受虐、性受虐、自我疏忽、遺棄、財務受虐、心靈受虐和遭人疏忽等。詳情可流覽： http://www.cdss.ca.gov/Adult-Protective-Services 加州各個縣有當地的聯絡電話： http://www.cdss.ca.gov/inforesources/County-APS-Offices

資源

名稱	網站
AARP (American Association of Retired Persons) 提供有關針對長者的詐騙的最新資訊。	http://www.aarp.org/money/scams-fraud/ 經詐騙諮詢培訓的志願者可提供協助，請致電熱線電話1 (877) 908-3360。
CFTC (Commodity Futures Trading Commission) 教育消費者認識美國國內期貨的詐騙新聞。	http://www.cftc.gov/ConsumerProtection/Resources/index.htm
Consumer Financial Protection Bureau 提供有關金融詐騙和欺騙性金融產品的資訊。	http://www.consumerfinance.gov/
FBI (Federal Bureau of Investigations) 提供有關使用大眾行銷的詐騙手法來矇騙消費者的提示。	https://bit.ly/2rWBZOK
ElderCare.gov 可協助長者聯繫區內法律和財務方面的各項服務。	https://eldercare.acl.gov/Public/Index.aspx
Federal Trade Commission 提供有關新近和現有的詐騙手法的資訊，並載有各人可如何保護自己的小提示。	http://www.consumer.ftc.gov/scam-alerts 浏览FTC制作的网上骗局意识宣传内容：http://www.consumer.ftc.gov/features/feature-0030-pass-it-on
Federal Housing Finance Agency 載有各項提示說明消費者免受有關房屋的騙局：房貸救援騙局、破產騙局、逆向按揭詐騙等。	https://www.fhfa.gov/
U.S. Bureau of Consular Affairs 為受害于海外罪行的美國人提供資訊。	http://travel.state.gov/content/passports/english/go.html

名稱	網站
Internet Crime Complaint Center由聯邦調查局(FBI) 和/全國白領犯罪中心(National White Collar Crime Center)合作組成，並將刑事訴訟提交聯邦、州、地方或國際執法和/或監管機構	http://www.ic3.gov/crimeschemes.aspx
Oasis 促進長者學無止境課程和提供有關網路安全防衛的資源。	https://bit.ly/2RrFnQh
Elder Justice Initiative 提供從國家司法部製作有關長者遭虐和錢財被剝奪的受害者和其家人的資訊。	http://www.justice.gov/elderjustice/
Stay Safe Online by National Cyber Security Alliance 提供保護你自己的家人的心得和資源。	https://www.staysafeonline.org/stay-safe-online/resources/
GCF Global 提供互聯網安全防衛的資源。	https://edu.gcfglobal.org/en/internetsafety/
Medicare.gov提供有關如何護衛你的個人資料和避免遭聯邦醫療詐騙所害的資訊。	https://www.medicare.gov/forms-help-resources/help-fight-medicare-fraud

參考文獻

[1] Anderson, Monica and Andrew Perrin. “Technology Use Among Seniors.” *Pew Internet Center*, 17 May. 2017. Web. 31 Dec. 2018. http://www.pewinternet.org/2017/05/17/technology-use-among-seniors/

[2] New York State Office of Children and Family Services “Under the Radar: The New York State Elder Abuse Prevalence Study.” *Self Reported Prevalence and Documented Case Surveys Final Report* 2011. Web. 31 Dec. 2018. https://ocfs.ny.gov/main/reports/Under%20the%20Radar%2005%2012%2011%20final%20report.pdf

[3] Office of Financial Protection for Older Adults “Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends.” *Consumer Financial Protection Bureau*, February 2019. Web. 12 March 2019. https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_suspicious-activity-reports-elder-financial-exploitation_report.pdf

[4] Baig, Mehroz. “Elder Abuse and Technology.” *The Commonwealth Blog*, 6 Jun. 2013. Web. 4 Jan. 2016. http://www.commonwealthclub.org/blog/2013-06-06/elder-abuse-and-technology

[5] VanDeVelde, Amy. “Oasis YouTube video provides great guidance on how to navigate and trust what you hear on the news.” *Oasis Blog*, 14 March 2018. Web. 31 Dec. 2018. https://www.oasisnet.org/Blog/is-it-fake-news-find-out-how-to-know-for-sure-151661?utm_source=Center+0&utm_medium=email&utm_campaign=7585+March+2018+Discoveries&utm_term=620598

[6] Federal Trade Commission. "Health Care Scams." *Pass It On Resource Guide*, 2014. Web. 31 Dec. 2018. https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0183-health-care-scams.pdf

[7] Sjouwerman, Stu. “Scam Of The Week: New FBI and IRS Alerts Against W-2 Phishing.” *KnowB4 Security Awareness Training Blog*, 18 March. Web. 31 Dec. 2018. https://blog.knowbe4.com/scam-of-the-week-new-fbi-and-irs-alerts-against-w-2-phishing

[8] The Office of Investor Education and Advocacy (OIEA). “Investor Alert: Prime Bank Investments Are Scams.” U.S. Securities and Exchange Commission, 5 Feb. 2015. Web. 4 Jan. 2016. http://www.sec.gov/oiea/investor-alerts-bulletins/ia_primebankscam.html

[9] The Federal Bureau of Investigation. “Common Fraud Schemes.” *Scams & Safety*, 2010. Web. 4 Jan. 2016. https://www.fbi.gov/scams-safety/fraud

[10] AARP. “Prevention, Not Just Awareness, Key to Cyber Security.” Web. 31 Dec. 2018. https://states.aarp.org/prevention-awareness-cyber-security/

[11] Stay Safe Online. “Shopping Online.” *Online Safety Basics*. Web. 31 Dec. 2018. https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/

[12] Kirchheimer, Sid. "Is Your Computer Infected." *AARP*, 9 Jan. 2012. Web. 31 Dec. 2018. https://www.aarp.org/money/scams-fraud/info-01-2012/computer-infected-scam-alert.html

[13] VanDeVelde, Amy. “Two factor authentication adds an essential layer of security.” *Oasis Blog*, 17 October 2017. Web. 31 Dec. 2018. https://www.oasisnet.org/Blog/want-more-protection-for-your-email-and-facebook-accounts-135523

[14] National Cyber Security Alliance. “Cheers to Safe Cybershopping!” *Stay Safe Online*. Web flyer. 31 Dec. 2018. https://staysafeonline.org/wp-content/uploads/2018/11/Online-shopping-tip-sheet-1118.pdf

https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230&pop-up=1

[15] “IOT.” *Merriam-Webster Dictionary*. https://www.merriam-webster.com/dictionary/Internet%20of%20Things

[16] Amazon.com. “Alexa and Alexa Device FAQS” Web. Feb. 2019. https://www.merriam-webster.com/dictionary/Internet%20of%20Things

我們的使命： 發掘創新使用科技的方法來幫助各式各人生活豐富，特別是隨著年齡增長時增強他們的安康和獨立能力。

我們的遠景： 科技的創新對於各人能在自己認定為家的地方，增強他們欲「按自己所想來生活」的能力方面發揮著重要作用。我們的目標利用支持和增強福祉的技術解決方案， 好讓我們每個人在思想，身體和精神上都能豐富和旺盛。

我們的企劃：我們的倡議在於研發多元化的科技及創新項目，重點在強化社交聯繫、促進豐富的人際關係、全人的成長及康泰、積極主導掌控個人體能的康泰、拓展有關活動能力、視力、聽力和認知能力的輔助，在危急或嚴重事故發生前作出預防，讓照顧長者的人士得到力量和支持，促進環境的健康、安全、易於進出及妥善的環境。

要獲取更多資料，請瀏覽 www.fpciw.org.

front porch

CENTER FOR INNOVATION AND WELLBEING