网络安全防卫
与互联网安全

front porch

Piers Project (Piers企划)
工具盒和资源指引 (2019年版)

Front Porch Center for Innovation and Wellbeing之倡议

协力贊助商

California Lutheran Homes

Front Porch，为一服务民众的非营利机构，其特色是根据个别人士因步入老年而引发的不断改变的需要而设计创新的社群和计划。机构获代表昔日退休社群居民Ellie Piers家属慷慨赠于一笔款项。

Ellie Piers

这赠予有助 Front Porch Center for Innovation and Wellbeing (FPCIW) 一直致力使用科技来促进耆老康泰的使命。Piers曾住在位于加州卡尔斯巴德(Carlsbad)名为 Carlsbad By The Sea的 Front Porch一处退休社区。她的贡献让CIW可通过知讯科技来开发应对长者安全防卫的问题，不单于大圣地亚哥地区制定与长者上网安全相关的措施，也让各地域的社群能一同通过跨越地域的互联网来使用。

对于科技，Piers有求知和冒险的精神，且相信科技能帮助长者安居乐业。她抓紧利用科技来与朋友和家人联系的机会，但也意识到用这些科技时会同时出现的安全防卫问题。Piers 对使用科技带来的危险有敏锐的触角，每次勇闯网络世界前都习惯仔细提问，让她都能达成每个「上网浏览」的目的。 为赞扬Piers 的助人精神，FPCIW 成立**Piers Project**，通过下面的策略来解决长者上网安全防卫问题和提高他们对此的意识：

- 实验有关长者上网安全的新科技并研发跟长者上网安全的内容；
- 接触大圣地亚哥地区内在这方面有专门知识的各团体来建立合作社运用捐款，提高有关长者上网安全防卫的关注和影响；
- 寻找可提升住在大圣地亚哥地区的长者有关改善生活的科技的意识的媒体；和
- 缔造一网上和社交媒体运动，来赞扬Piers对改革长者的优质生活这一重要范畴的殷切和馈赠。

这个由FPCIW创建的工具盒可用作为一本指引帮助各位更了解网上世界存在的一些风险 ，并在享受互联网优势的同时可主动和自信地避免这些风险。

目录

你知道吗…

- 2016年，在美国65及以上的人中有百分之67 (67%)在用互联网[1]。
- 在 24 起耆老受虐的案件中，只有一起有举报[2]。
- 2017年，耆老因财务上受虐，损失了17亿美元之多[3]。
- 有百分之45 (45%)财務上受虐是从使用互联网开始[4]。
- 有百分之59 (59%)的人说他们不肯定他们在转播媒体看到的资讯是真的还是假的[5]。

今天，科技已成为我们日常生活中不可或缺的工具。我们通过互联网与親人交谈，进行网上理财和网上购物，在脸书（Facebook) 或推特 (Twitter) 等社交平台上聊天和搜寻一些我们有兴趣的主题。互联网有许多的裨益，可是，我们如何安全地享用这浩大的数码世界呢？

作为数码社会的活跃成员，我们实践良好的互联网卫生非常重要。我们需要洞察有些人会用不合宜的伎俩来滥用我们的个人资料，可能导致我们个人的、社交上的、和/或钱财的损失。正如任何有用的技能，重要的是要采取有助于减低风险的预防措施，可让你舒适地、安稳地和安心地享用互联网的好处：我们的力量和控制权来自我们的知识和能与人分享我们的经验。

设计这工具盒是要它成为长者安心使用电脑的资源指南。这工具盒内的课程内容都基于三个简单却重要，关于凑效而又安全的上网经历的规则。

1) 查究你在网上看到的内容，
2) 查证其可信性和真实性，和
3) 查找你的朋友、邻居或同事来帮忙，并教导你周围的人。

网络安全防卫和长者成为诈骗目标

网络安全防卫是指一般性互联网的安全防卫，专注于储存在电脑内的或可通过互联网取得的资讯的防卫。利用各种科技方式（包括电脑或互联网）进行的诈骗层出不穷。

任何使用互联网的人都有可能成为网路罪犯的目标，但为何大多数犯罪目标都是长者呢？长者多半是经济较为稳健，多半不会举报诈骗或许是不知道怎样或往哪举报这些事故。长者也可能投资大量金钱于一些伪称可促进记忆力、长寿或强健体魄的产品。

因着感到丢脸和害怕，长者倾向于少去举报犯罪行为，从而助长了这类牵涉钱财的罪行，伤害更多的受害人[9]。若你过往曾是网路罪行的受害人，你要知道**你并不是唯一的受害人**，许多人也有相同的遭遇。

更重要的是，对消费技术不熟悉的人都会学习积极避免网络诈骗的伎俩。Piers Project 工具盒的目的是要防止长者遭网上的欺凌和使他们有能力在进行安全的上网活动的同时能获取资讯科技的许多好处。

该相信谁？识别冒名顶替的人！

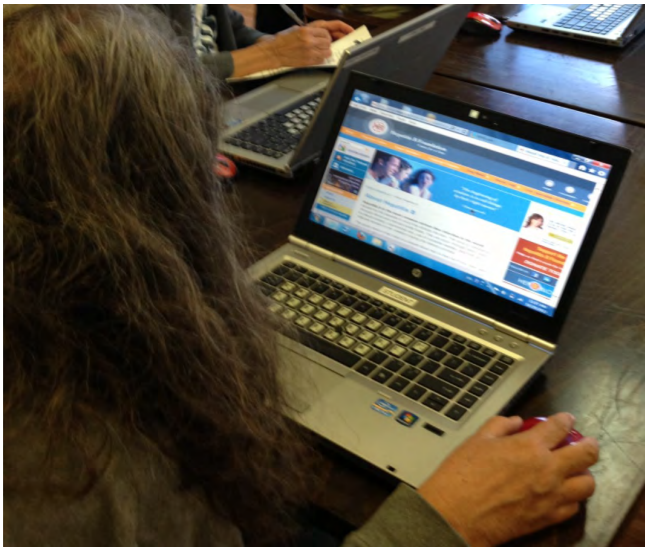
互联网众多好处之一是让我们能在这平台上处理日常生活的多个范畴：这包括健康、税务或财务。我们能易于搜寻所需的资讯，在需要协助时也能瞬间马上跟适当的人连上。在使用互联网时，能辨识和筛出骗局和撞骗的人是很重要的。

当有人没有得到你本人许可或同意而取得或使用你的个人资料这即构成身份盗用。这资料将可用作订购/购买东西、领取社会退休福利、盗窃你的个人钱财或进行其他犯罪行为。身份盗用的受害人可招致各种亏损的后果。曾出现的案例有非法复制护照、信用减少或联邦医疗/州政府医疗援助诈骗。下面是需要警觉的常见的骗局的清单和你应如何采取防卫措施来稳妥地上网。

医疗保健骗局 这类骗局可以不同的形式出现：包括与事实不符的电视宣传，讹称因新法律而产生的新医疗卡或来电者承诺大折扣的医保。

1) 查究你在网上看到的内容，
2) 查证其可信性和真实性，和
3) 查问你的朋友、邻居或同事来帮忙，并教导你周遭的人。

其他骗局包括有冒称的诈骗，他们讹称为政府公职人员，需要你的联邦医疗卡来办理新的客户卡。



你可以这样做！

- ✓ **留意时事** 骗徒经常利用联邦医疗保险和其他医疗计划的改制和转接期，媒体也在广泛报导的时候出击[6]。临近联邦医疗保险接受办理更调期间应谨慎和有所防范。由2018年4月起，因应删除社会安全号的倡议[Social Security Number Removal Initiative (SSNRI)] 联邦医疗保险和州政府医疗援助中心已开始改发和邮寄新联邦医疗保险客户卡来取缔以社会安全号为编号的旧联邦医疗保险卡。

- ✓ **查询确认账单是否真实** 在提交你的个人资料前，应先联络联邦医疗保险服务中心(1-800-633-4227) 以防万一。你要明白联邦医疗保险服务中心从来不会给你打电话的，故此，若你接到电话，切勿提供你个人的任何资料。

税务相关的诈骗 近日，讹称填报W-2 的网络钓鱼电子邮件成为网络安全的一大关注。骗徒正在寻找不同的方法发送看似来自雇主的首席或其他的行政人员的假电邮，要求雇员提供 W-2税务资料。网络罪犯随即用拿到手的W-2内的资料申报假的报税表并偷取受害人的身份[7]。

你可以这样做！

- ✓ **打电话** 你若收到任何索取W-2税表资料的电子邮件，请在发送任何资料前致电该公司核实该请求。

- ✓ **尽早报税** 你愈早报税，你将能够堵塞网络罪犯趁机冒你的名提交伪造的报税表来袭击你的漏洞。

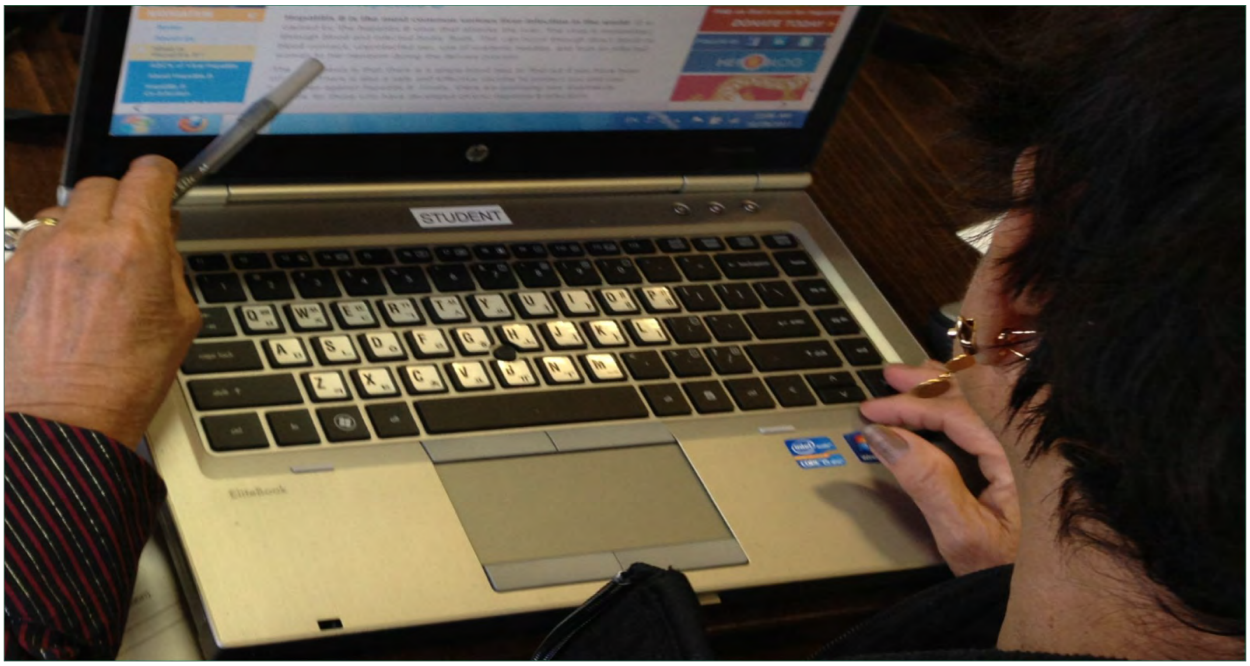
- ✓ **定期查阅你的信用报告** 你可使用AnnualCreditReport.com提供的免费一年一次的信用报告来免费查询你的信用评分。发现任何可疑的活动时可立刻冻结该帐号。

彩票诈骗 这类非法行为包括伪称您的彩票中奖了，而你须先付手续费才能领取奖金。彩票诈骗常讹称为某一存在的彩票机构或其他存在的机构来发来电子邮件。不要急，慢慢小心搜查资料来确定，电邮所述若显得好得令人难以置信时，多半是假的。

投资诈骗 这些查询涉及你新开或现有的投资。也可能建议你投资不同的项目，如采矿、石油、汽油或一些新科技公司。“Prime Bank” (主要银行) 诈骗即为一典型例子。推销员声称投资人的资金将用作购入买卖一官方机关如联邦储备局保证的“Prime Bank” (主要银行) 发行的货币。他们更声称，此格式的投资机会仅通过独家邀请，仅限于一组精选客户。[8] 此外，由于国内的法规和监管，应对海外投资进行极度谨慎查核。

你可以这样做！

- ✓ **不要单凭外表来对一家公司作出评价。**有些网站可能看来绘声绘形和正当，但这并不总是意味着他们值得信赖。
- ✓ **咨询合约的细节和条款。**我们建议要仔细审阅合约，因为人们常会忽略那些重要的细节。
- ✓ **切勿轻信巨额的承诺。**这是诱饵电子邮件收件人的常用伎俩。



电子邮件

电子邮件是在互联网上的一主要沟通模式。可是，你怎知道哪一封是可以安心打开和哪一封应摈除？有什么线索可随？以下是一些你应认识的词汇和你如何识别你的收件箱内潜在的危险。

网络钓鱼(Phishing) 当骗子使用虚假的电邮或短讯诱骗你提供重要的个人资料，这即为「网络钓鱼」(phishing)。犹如「钓鱼」，骗子试图通过伪装成合法安全网站的链接或虚假网站来诱导受害者。这是他们收集密码、社会安全号、银行户口资料等的方式。

垃圾邮件(Spam) 这是属于不请自来的、渔翁撒网式的电子邮件用来进行多种网上诈骗。大多数的垃圾邮件是无伤大雅的或令人厌烦的广告，但有一些却能在未经许可下，一面传送病毒，一面切入电脑和侍服器中。这种形式的诈骗也能非法取得并出售你的隐私资料。

骇客(Hacking) 一个未经你许可，遥远地切入你的电脑或个人账户就是骇客（hacker)。任何利用电脑系统内的弱点进行任何形式的骇客均属非法和刑事犯罪活动。

奈日利亚信件骗局(Nigerian Letter Fraud / 419 Fraud) 这种行骗又称为预付费诈骗(Advance Fee Fraud)，通过电邮索取你个人或有关你的银行资料，声称发件人为一外地政府官员或一位需要经济援助的外国人。这些邮件的收件人被怂恿将印有信头的空白的公文纸，连同他们的银行名称和户口号码并其他私隐的资料等资料发给写信人，也可通过传真号(信中有提供)方式取得。[9] 看到从外国发来的电子邮件要提高警觉。他们都会请求你把大笔款额存到一家设于外国的银行来帮忙。这类骗徒常是提出紧急的请求和催促你马上提供经济援助。同时，对美国政府发来的电子邮件也要提高警觉。 例如，遇到有人声称从社会安全局办公室发出讯息向你索取你的社会安全号是要小心注意。要三思！一般而言，这类机关是不会通过互联网来向你索取你的个人资料的。

仔细看看

网路钓鱼的垃圾邮件并不只限于来至奈日利亚： 对那些寻求以转移大额金钱来帮忙的电子邮件要持怀疑的态度，这包括了看似是由你的朋友或家人发出的一个可疑的危急状况。

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

这个例子里你会察觉到这似是由所谓是你的家人发出一紧急要求的电邮有点怪异。注意其他不对劲的蛛丝马迹并当心你熟识的人的电邮地址可能已经被骇客进入了。 经常**查究**真确性，并跟另一位双方都认识的家属或朋友通电话来求证。

你可以这样做！

- ✓ **注意电邮内文的并字和文法** 查核统一资源定位符(URLs)、电子邮件地址和电子邮件的内容的并写。网络钓鱼电邮常存在你可以察觉的不明显的并写错误。当你看着发件人名字时 ，多看清楚发送该讯息的实际电邮地址。另外，若你将滑鼠指针悬停在该链接上，你可能发现它实在引进到一可疑的网站而并非讯息内所承诺要引进的网站。

- ✓ **切勿打开不明来历的电子邮件** 若一电子邮件、短讯或社交媒体的讯息是由一不熟识的人发出的，应删除或不理它。对声称你需要申领金钱、礼物或度假优惠的电子邮件也应同样地谨慎：这讯息很可能会引你进入另一网站，在那里你可会容易接到恶意软件或电脑病毒。遇有可疑，丢掉它！

- ✓ **对电子邮件或短讯内的网站链接要有戒备的心**。若你接获你认识的人发出的电子邮件，而其内容只载有一个网站链接，**切勿**点击该链接。这常是显示该电邮的主人可能已被骇客入侵了。遇到这情况，致电或用其他方式通知此人并删除该电邮。

- ✓ **切勿通过电子邮件提供你的银行帐号或个人资料**。 你要明白银行和保险公司等正规的公司绝不会通过电邮索取你的个人资料的。直接登入公司设有保安系统的网站才登入你的个人帐号来查阅通告和讯息。

1) 查究你在网上看到的内容，
2) 查证其可信性和真实性，和
3) 查问你的朋友、邻居或同事来帮忙，并教导你周遭的人。

仔细看看

骗徒常盗用民众熟识的公司名号来发送电子邮件令你觉得放心点击附带的链接网站。请读下述的电子邮件。 请看以下这封看似来自百度推广中心的邮件，你能辨识出这是一封「网络钓鱼」邮件 吗？

若你不能肯定某公司发放的电子邮件内附带的链接网址是否安全，最安全的做法是另外开启一新的浏览界面，直接进入该公司的网站，再登入你的帐号。若有关于你帐号的重要通告或讯息，这些通常会显示在公司设有保安防卫的网站内属于你的帐户内。

发件人：邮件管理（由[redacted]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

保护你的钱财

使用互联网理财是有许多好处的：网上购物的方便、安排支付账目、即时资金转账。线上行销金钱诈骗以多种形式出现，而最常见的诈骗牵涉使用信用卡和银行账户资料，这些资料通常被用于购物、投资和税务的问题。这些阴谋可通过伪装的网站或电子邮件来获取有关的资料。

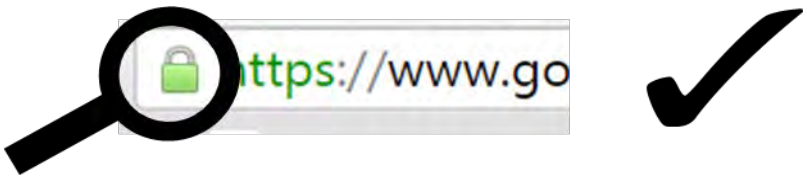
网上购物诈骗行为 包括提款卡或信用卡的使用。这可通过盗取该卡或非法地获取持卡人的帐号、卡号、卡上的保安密码、卡主的姓名和住址等个人资料进行。

你可以这样做！

- ✓ **尽可能使用别的付款方法。**取代通过该网站直接付款，改用 PayPal、Amazon 和 Google Check Out 等设有多重保安防卫功能的付款服务机制[10]。可能的话，你也可以用「宾客」的身份来结账和选择不贮存你的卡号在帐号内。
- ü **注意银行月结单 妥為整理你手上有效的信用卡清单並定期查看銀行月結單。**若察觉任何錯誤或不寻常的账目，应马上通知发卡的机关。
- ü **尽可能使用信用卡**使用信用卡一般较提款卡安全，因若遇上货品没有送出或货不对版时，信用卡客户是可以讨回款项的[11]。
- ✓ **采用辨识能力强的工具**你可以采用辨识能力最强的工具，如生物辨识、保险锁、或在你行动器材内装置的应用程式采用独特的一次性代码来保护你网上购物账户[11]。

仔细看看

查核挂锁标志 当你进入一网站时，一个小挂锁出现在网址栏上，表示这网站是使用*较高*保安度的机制来传送资料数据。虽然这标志代表着某种保护，这不能保证百分百的保障！



查证链接网址的网站链接看似可靠但仍可能并非真实，故此必须万分小心地看清楚该链接。举个例子，该链接或许显示“bankofamericacard.com”或“B-of-America”—带有 “bank”或“America”等字样可使这些网站显得真确，然而，它并非该公司网站的真确链接。

请查阅联邦贸易委员会网站 **www.ftc.gov** 来了解更多消费者的心得和提示！

网上理财 当你稳妥地连上你银行设有保安防卫的网站或应用程式时，你将可以安心进行网上理财。当你进行网上购物时，注意同样的保安防卫标志(绿色的挂锁、“https”和统一资源定位符 (URL)的拼写是否正确。以下是更多安全地进行 网上理财的心得。

你可以这样做！

- ✓ **使用你个人的无线上网机制(Wi-Fi)来进行网上理财** 切勿使用免费或公众的无线上网机制来进行任何牵涉敏感资料的事宜。
- ✓ **经常查阅你的银行月结单** 看清月结单上你所购买的东西，确定都是你熟知的。若发现你帐号内有任何可疑的活动，务必马上跟你的银行联系。
- ✓ **离开你的银行的网站或应用程式前必须登出网站或引用程式** 你甚或可在登出后把浏览器关闭。
- ✓ **了解你银行的保险规条** 遇上被电脑罪犯盗取你的银行资料时，那么你能提前知道你银行在处理发生在你身上的诈骗事故而须报销给你的条例和程序，如申报的期限有多长和你能获得多少的保障等。

1) 查究你在网上看到的内容，
2) 查证其可信性和真实性，和
3) 查问你的朋友、邻居或同事来帮忙，并教导你周遭的人。

恶意软件(Malware)

我们如何知道哪些网页的链接是可以安心点击、哪些不可？ 你希望能够从可信赖的来源接收真正为你准备的讯息，故此这些是你应了解的一些重要事项。

Clickbait (标题党/钓鱼标题)指互联网上的内容，旨在吸引注意力并让访客点击通往特定网页的链接。有些标题或广告或许会真正带你通往一份有趣的文章或一所你可能想要购物的网上商店。然而，若网站采用很多标题党的钓鱼标题，这些多半是带有恶意软件的。

恶意软件(Malware) 恶意软件(Malware，malicious software 的缩写)是一种旨在对一电脑系统造成破坏或令它无法运作的程序。使用行动器材时同时要谨慎，因这些器材也免不了受恶意软件和电脑病毒的袭击。据维基百科(wikipedia.org)阐释：「恶意软件可以是鬼祟的，意图盗窃资讯或在电脑使用者不知情下进行一段长时间的偷窥」。 恶意软件有多种类别：

勒索软件(Ransomware) 这是‘*ransom*’(赎金)和‘*software*’(软件) 两个字的组合。勒索软件指任何能遥控地锁住你的电脑，继而提取贮存于电脑内的资料或提出需退还你被盗的失款而索取金钱上补偿的软件。发放这些恶意软件的人可能讹称自己是某官方人士，如警察等。这些勒索软件的有害攻击也可能会针对智能手机和平板电脑设备。

病毒存于人类中的病毒跟电脑中的病相类似。从技术而言，病毒用电

脑成为它们存在的主体。如此进行时，病毒即能继续倍增并在你的电脑中作出自我调整来达成它们的任务，在袭击时也进一步散布这恶意软件到其他领域。

防毒程式(Vaccine programs) Vaccines(防毒疫苗)也称为「防毒软件」(“anti-virus software”)是用作预防或反击恶意软件的攻击工具。 确定你的电脑最少有一个有效的防毒程式 (或Windows FireWall，即视窗防火墙)来预防恶意软件的攻击。若你近期曾出现运作速度大幅度减慢的情况，这程式即尤为须要。

坊间有多种防毒程式可用，它们的防毒功能和售价不一。以下为一些常见的品牌：

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

反恶意软件程式(Anti-Malware Program) 视窗作业系统防火墙的作用为基本针对恶意软件的防卫，也可以内置到微软视窗程式中。若是Apple Mac (苹果麦金塔) 用户，要紧的是要确定从Apple的操作选项内启动了软件更新。此外，Apple 用户必须在「系统优先选项」中允许设立定期更新检查。如uBlock Origin 等的浏览器扩充程式会屏闭追踪你在电脑上的活动和装置恶意软件的广告。

仔细看看

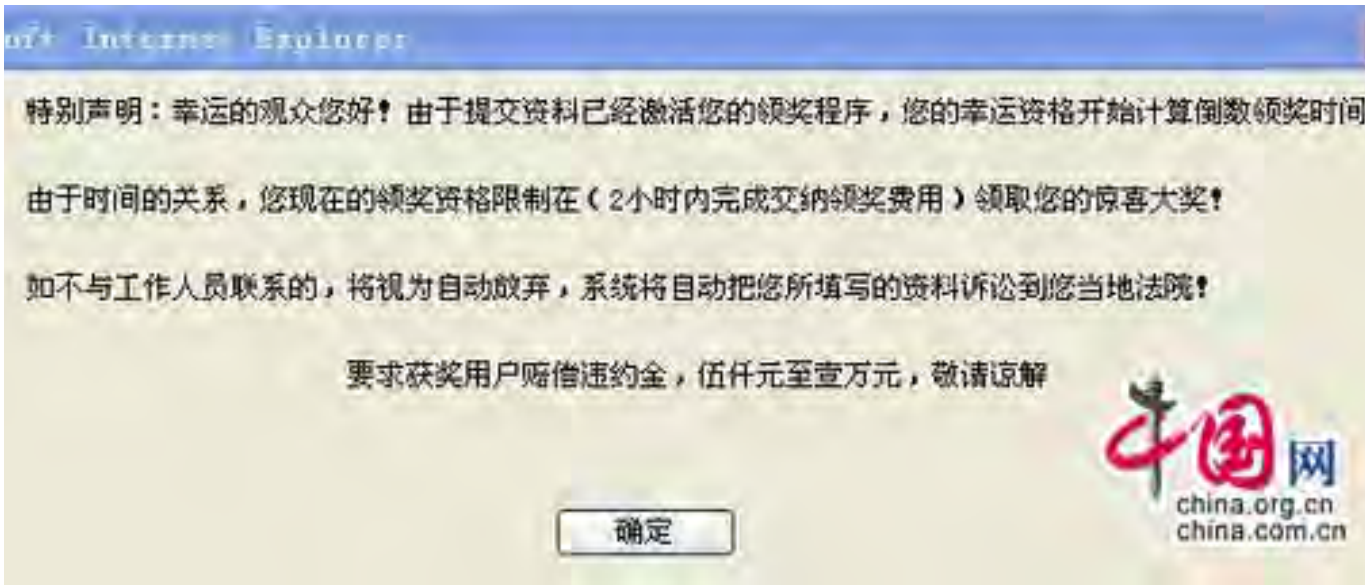
这些你要在电脑内注意的红旗警告讯号：

- 电脑停止运作或工序慢下来
- 不停弹出通告讯息
- 会消失的数据
- 发出异常的声音或哔哔声
- 讨厌的图像

定期查核你已装置的防毒软件的更新—再而进行全面彻底的扫描过滤来确定其运作[12]。别忘记每年续订这些防毒软件以确保你的电脑更新来防卫新的软件攻击。

你可以这样做！

- ✓ **马上关闭** 若遇有看来草率的自动跳出的广告或网站，随即点击右上角载有「X」的方格来关闭该视窗。若你的浏览器或防毒程式对某一网站的安全提出质疑，切勿进入该网站站[11]。
- ✓ **切勿下载**任何东西，除非你完全知晓那是什么和那是出自一安全的来源的。
- ✓ **广告和跳出的视窗**常会有看似一项系统测验的警告讯息或声称你已中奖。切勿点击它们。马上关闭这些视窗并为电脑或器材进行一次一般的防毒扫描。下列跳出的视窗是一些你应避免的。



密码的安全保障

我们应视我们的个人资料如钱财—我们应重视和保护它。密码安全保障是极为关键的，因为它是提供获取你重要的个人资料的门径—看密码如同你家的门匙。保护我们自己重要的一环是创造一些别人难于猜测的密码。

造出一个强而有力的密码

✓ 造长的密码。超过 6 个字符即算理想。
✓ 不要每个帐号都使用相同的密码。
✓ 来个英文字母、数字和符号的大混合。
✓ 不要用如儿女的名字、出生日期、年龄、住址等 的个人资料。
✓ 定期更改你的密码。专家建议每 6 个月最少更改一次。

密码管理员 密码管理的程式能助你在多个帐号用同一个密码。它们可在你已预先注册的网站自动为你填上你登入网站的资料。请对这类程式进行个别的查考其利与弊，看哪一个程式最适合你。下列为一些免费的程式，这些也有提供其他收费的服务：

- LastPass
- Keeper
- Dashlane

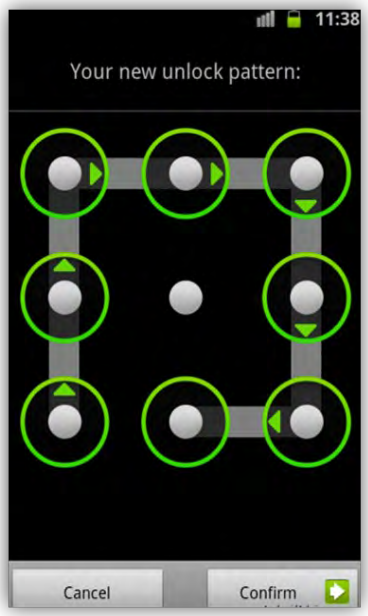
你的密码在名单内吗?

骇客通过猜测我们的密码来偷进我们的账号。故此，切勿选用易于被人想到的密码。务必切勿使用下列的密码：

这些是 2018 年 25 个常被使用**的密碼**、因而常会被骇客入侵*

排名	密码
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

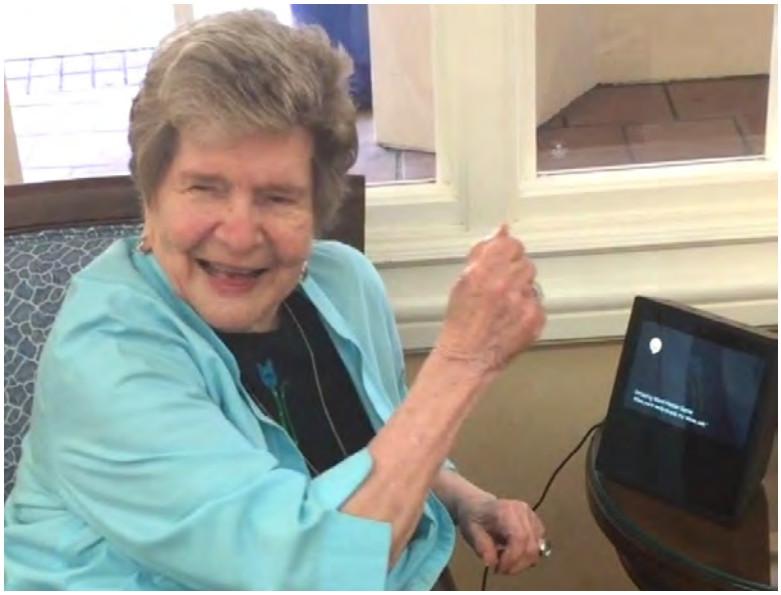
**SplashData, 2018*



请务必锁上你的器材 无论是电脑、笔记本电脑、平板电脑或智能手机。 你的器材均能让你设立密码以至只有你才能使用该器材。

Two-Factor Authentication(双重辨识) 启动双重辨识(2FA)增加多一度保安防线以阻挡别人试图偷入你的账号中。这是说就是某些人能猜中你的密码，它们仍需拿到你手上的电话才能偷进你的账号中。双重辨识是这样达成的：一些你知到的东西(你的密码)加上一些你手上拿着的东西（你的手机)[13]。辨识工具也可以是某种生物特征辨识、保险匙或通过你的行动器材上的应用程式采睇的独特的一次性代码[14]。

智能助理、智能家居和无线上网 (Wi-Fi)

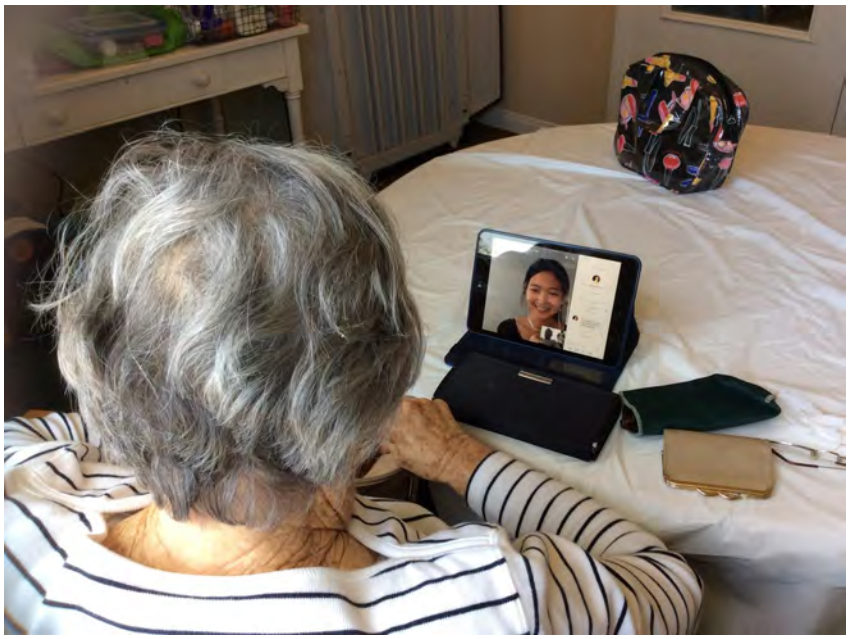


语音助理如 Amazon Alexa 在家居普及使用，要紧的是要明白有那些安全措施是你可以是用来守护你的隐私的。 **IoT** (又称「物联网」"The Internet of Things") 是指互联网的功能容让讯息可以通过物件和器材收发[15]。这包括任何智能家居器材、电器用品、扬声器、玩具、可配带的衣物等。常见的提问是：「Alexa 有在收录我所有的对话吗？」亚马逊网站说明此问题的答案是否定的。它解释该器材是设计来只侦测唤醒语 ("wake word" 即 Alexa) ，此乃通过原声结构来认出相配的唤醒语，故此没有任何其他的声音会被储存或发送到「云端」[16]。只要紧记当你使用任何与互联网相关的器材时，危机总是存在的：具有恶意的人可能会获得某些资料。然而，照惯常一样，紧记切勿在互联网上透露或存放任何敏感或私人的资料。

麦克风「静音」键和拔掉 语音首先设备，收音的器材是设有静音按钮的。当你启动这功能时，就是你说出唤醒语，那器材也不会有回应的。若你想确保那器材绝对不能听取或收录任何声音，你可以拔掉器材的插头或把电池拿掉。

无线上网(WiFi)路由器保护

无线路由器提供笔记本电脑和行动器材很大的自由度。但当你购买一部新的无线上网路由器时，它通常会带有某人可能查找或猜测的预设配置。务必更改那密码并重新命名那无线网络，好使你用于智能设备的互联网源头是安全的[11]。



社交媒体和假新闻

社交媒体网络在过去几年中变得非常流行。虽然它们容让你可以随时随地跟朋友和家人联系，若你在这平台上慎于你跟别人交流的内容，那就会较安全。

你可以这样做！

- ✓ **切勿接受您不认识的人向你发出的交友邀请** 你可能会接到不知名人士发出的讯息称赠送你礼物或门票，以此诱饵你点击链接或安排亲身会面。也要注意内容只在新消息发放宣传某些新产品或服务的帖文。永远不要点击可疑的链接，即使它们看似是来自认识的一位朋友或一家公司。
- ✓ **请注意你分享的信息量** 你在网上的背景资料可以分享大量有关你的个人资料。这包括你的住处、出生日期、你的喜好、家人等等。请注意你发布的帖文—你原是发给你的朋友，但由于你的私隐设定，骗徒也有可能看到。
- ✓ **尝试脸书私讯或电子邮件的替代品** 加密应用程式如 Signal、Whatsapp 及 ProntonMail 等可提供额外的保安防卫。

✓ **查核你的私隐设定** 在脸书等的社交媒体平台上，你是可以管理谁可以查看你的背景资料、你发布的帖子、你的活动、谁可以在你的时间轴上写帖子和谁可以在照片上标示你。 明智的做法是把你的设定提升至高度的限制，这样即可让你先审定你被标示在什么照片或帖文中，才让别人在你的版面上看到。

仔细看看

看似是 “Like(赞)”？脸书版面上看似是“Like(赞)” 按键或一个带有误导性图像的视频的屏幕截图可能会立刻吸引你的注意，这可能会不由自主地把你连接到你不需要的购物网站，甚至做成病毒和恶意软件的入侵。

要紧的是你能辨识在脸书帖文下方设置的真实「赞」按键标志的最初看起来类似但却是虚假的按键标志。「标题党」(Clickbaiting)令使用者对某些连接、照片、视像或文章感到好奇而点击观赏。有些此类虚假的故事或广告宣传只引领你到另一个网站，但有些是有破坏力的。然而，若因点击喜欢一个项目而沦为这些圈套的受害者的同时，你更会不知情地为这些诈骗的带有虚假的「赞」按键标志的视像或影像做宣传，可能使你网上的朋友也成为受害者。

社交网络上有很多博眼球的标题党新闻 – 保持安全上网计划的参考网站的链接，积极管理你在多个平台的隐私设定。

网上交友约会网站 网上约会可以是一个结交跟你有类同兴趣的新朋友的好工具，只要你对自己决定跟别人分享的内容保持谨慎和敏锐。注意在约会的应用程式内可能有虚假的背景内容，那些人试 图使你点击一个链接引你到一些带来损害的网站。

你可以这样做！

- ✓ **注意在他们的背景资料中的红旗警告讯号** 当你在社交媒体或约会的应用程式内与某人联系时，要晓得一个带着一大串数字的名字可能是虚构的背景的征兆。那些标题和文句似在暗示对方只在寻求肉体的欢娱吗？
- ✓ **切勿点击任何它们发出来的链接** 经过几次讯息的来往后，而你也感到跟对方有更多的认识，你或许对交换电话来亲身会面感到安心。但若交流对话缺乏内容而对方只想方设法让你发红包，另找朋友吧。

虚假新闻 在今天的新闻和媒体中，很难解读什么是真确和什么是虚假的。现今跟过往相比，人们可以有更多渠道吸取资讯。然而，真相并非总是如此清晰的，因为任何人都能在互联网上载任何的资讯而又声称那是真相。那么，你怎么可以断定哪些是可靠的新闻来源？

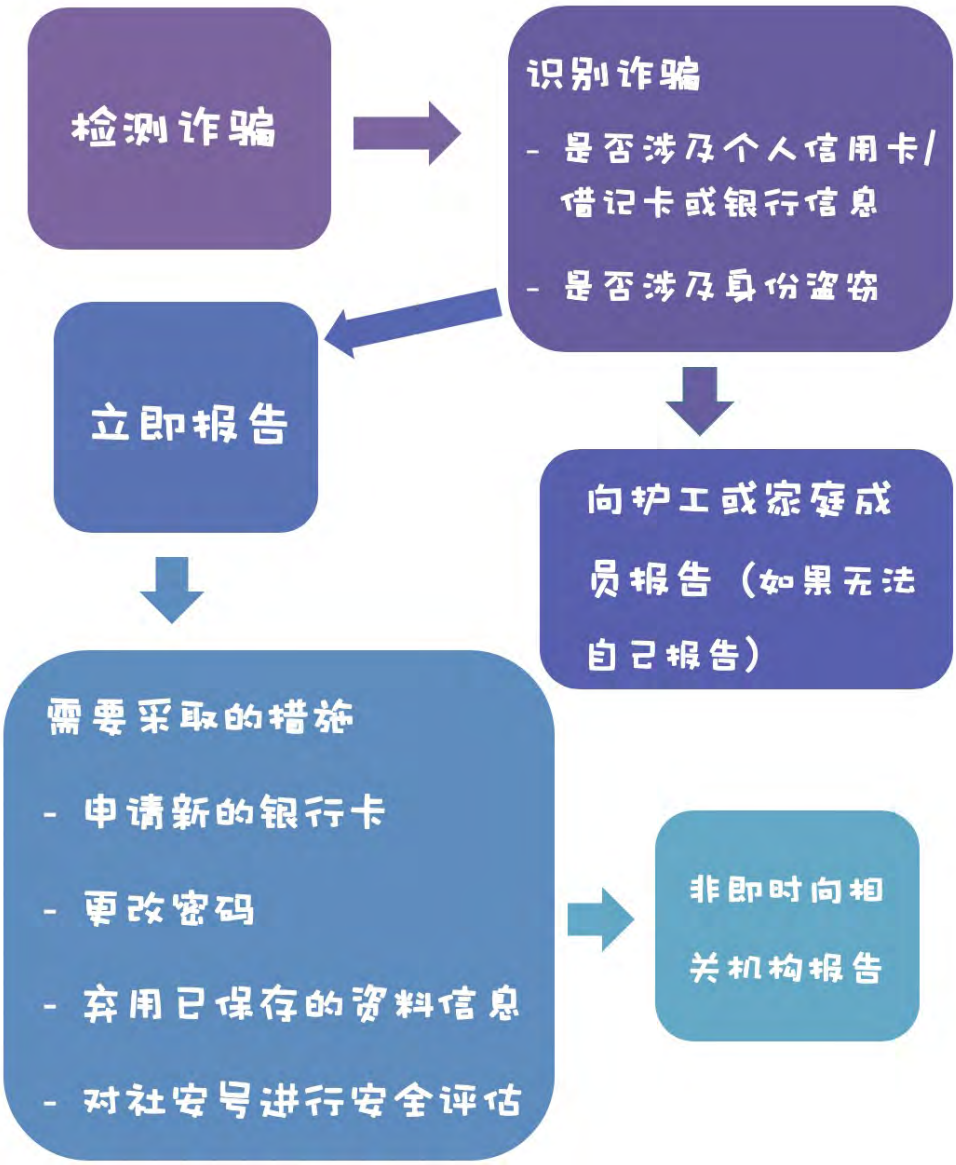
你可以这样做！

- ✓ **衡量该来源** 当你在网站上时，搜集有关该网址的资料。阅读「关于我们」一栏，是谁在主理这网站？他们为何制作该网站？谁负责网站的经费和他们有偏重某些赞助商吗？ 他们的资讯从何而来？你单单查看网站的统一资源定位符 (URL)末，你已能辨识不同级别的可信度。网站若是以「**.gov**」结尾，这表示这是以 政府部门的网站而通常须经过多重审查和品质确认查核才得以发表的。

网站若是以「.edu」结尾，这显示该网站是来自一所学校或四年制大学，通常遵照学术准则来发放材料。

- ✓ **查阅有关参考资料**若你浏览多个不同的、众所周知的、有声望的新闻资讯来源，虽然每个机构或有其偏向和立场，你可以从中辨识哪些事实的共同观点？哪些是怪异的或似是开玩笑的？其他来源有证实这些资讯属实吗？
- ✓ **多搜寻考证**查核资料发出的日期以确定其相对时事的适切性。可能的话，向专家查询事实考证的网站。

网络诈骗应对程序



举报机关

诈骗类别	举报机关和联络方法
举报一般的骗局(推荐)	**当地执法机关** 警方有责任协助你或转介你到有关机构
举报一般的骗局(推荐)	**Federal Trade Commission** 电话：1-877-382-4357 (电传/TTY/TTD: 1-866-653-4261)
网络罪行和诈骗(推荐)	**Internet Crime Complaint Center** (IC3) 由 Federal Bureau of Investigation (FBI/联邦调查局) 和 National White Collar Crime Center (NW3C/全国白领犯罪中心) 合作组成。举报互联网上的罪行或诈骗。http://www.ic3.gov/default.aspx
举报医疗保险诈骗诈	**The Federal Trade Commission (FTC)** 电话：1-877-FTC-HELP (1-877-382-4357) 或电传/TTY 1-866-653-4261 或浏览： ftc.gov/complaint
联邦医疗保险诈骗	**Department of Health and Human Services** 电话： 1-800-633-4227 举报联邦医疗保险和州政府医疗保险**援助诈骗、挥霍和滥用** 电话： 1-877-808-2468 **Senior Medicare Patrol** www.smpresource.org **Office of the Inspector General** 电话：1-800-447-8477 或发送电邮至 spoof@oig.hhs.gov
身份盗窃罪行	**Identity Theft Resource Center** 电话： 1- 888-400-5530 http://www.idtheftcenter.org/knowledge-base/
针对西语人士与医疗相关的事故	**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） 电话： 1-866-Su-Familia (1-866-783-2645)
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** 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.

诈骗类别	举报机关和联络方法
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** 举报任何外国彩票骗局 电话： 1-800 646-2283 **U.S. Postal Inspection Service** 举报彩票或电子邮件诈骗 电话：1-877-876-2455
社会保障金诈骗	**Social Security Administration** 电话： 1-800-269-0271 (电传/TTY: 1-866-501-2101) 10:00 am to 4:00 pm (东岸时间） http://oig.ssa.gov/report/
护照诈骗	**Department of the State** 联络 PassportVisaFraud@state.gov
商业诈骗	**Better Business Bureau** 登入其网站举报 https://www.bbb.org/consumer-complaints/file-a-complaint/get-started
举报网络钓鱼电子邮件	**Department of Homeland Security, U.S. Computer Emergency Readiness Team** 电邮： phishing-report@us-cert.gov 或以电邮方式向Federal Trade Commission 申诉： spam@uce.gov 你可把网络钓鱼的电邮转发至 spam@uce.gov
举报一般性的长者受虐	**Adult Protective Services** (成人保护服务)棣属加州社会服务处。提供各项服务支持长者和需依赖别人的成年人士。可举报疑为受虐的事故： 身体受虐、性受虐、自我疏忽、遗弃、财务受虐、心灵受虐和遭人疏忽等。详情可浏览： http://www.cdss.ca.gov/Adult-Protective-Services 加州各个县有当地的联络电话： http://www.cdss.ca.gov/inforesources/County-APS-Offices

资源

如果你有兴趣了解更多信息，或甚至在网上安全方面向别人讲解，下面的资源是可以帮助你的。

名称	网站
AARP (American Association of Retired Persons) 提供有关针对长者的诈骗的最新资讯。	http://www.aarp.org/money/scams-fraud/ 经诈骗咨询培训的志愿者可提供协助，请致电热线电话1 (877) 908-3360。
CFTC (Commodity Futures Trading Commission) 教育消费者认识美国国内期货的诈骗新闻。	http://www.cftc.gov/ConsumerProtection/Resources/index.htm
Consumer Financial Protection Bureau 提供有关金融诈骗和欺骗性金融产品的信息。	http://www.consumerfinance.gov/
FBI (Federal Bureau of Investigations) 提供有关使用大众营销的诈骗手法来蒙骗消费者的提示。	https://bit.ly/2rWBZOK
ElderCare.gov 可协助长者联系区内法律和财务方面的各项服务。	https://eldercare.acl.gov/Public/Index.aspx
Federal Trade Commission 提供有关新近和现有的诈骗手法的资讯，并载有各人可如何保护自己的小提示。	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 载有各项提示帮助消费者免受有关房屋的骗局：房贷救援骗局、破产骗局、逆向按揭诈骗等。	https://www.fhfa.gov/
U.S. Bureau of Consular Affairs 为受害于海外罪行的美国人提供资讯。	http://travel.state.gov/content/passports/english/go.html

名称	网站
Internet Crime Complaint Center 由联邦调查局 (FBI) 和/全国白领犯罪中心 (National White Collar Crime Center)合作组成，并将刑事诉讼提交联邦、州、地方或国际执法和/或监管机构处理。	http://www.ic3.gov/crimeschemes.aspx
Oasis 促进长者学无止境课程和提供有关网络安全防卫的资源。	https://bit.ly/2RrFnQh
Elder Justice Initiative 提供从国家司法部制作有关长者遭虐和钱财被剥夺的受害者和其家人的资讯。	http://www.justice.gov/elderjustice/
Stay Safe Online by National Cyber Security Alliance 提供保护你自己的家人的心得和资源。	https://www.staysafeonline.org/stay-safe-online/resources/
GCF Global 提供互联网安全防卫的资源。	https://edu.gcfglobal.org/en/internetsafety/
Medicare.gov 提供有关如何护卫你的个人资料和避免遭联邦医疗诈骗所害的信息。	https://www.medicare.gov/forms-help-resources/help-fight-medicare-fraud

参考文献

[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

我们的使命: 发掘创新使用科技的方法来帮助各式各人生活丰富，特别是随着年龄增长时增强他们的安康和独立能力。

我们的远景 : 科技的创新对于各人能在自己认定为家的地方，增强他们想「按自己所想来生活」的能力方面发挥着重要的作用。我们的目标是利用支持和增强福祉的技术解决方案 ，好让我们每个人在思想、身体和精神上能丰富和旺盛。

我们的企划: 我们的倡议在于研发多元化的科技和创新项目，重点在强化社交联系、促进丰富的人际关系、全人的成长和康泰、积极主导掌控个人体能的康泰、扩展有关活动能力、视力、听力和认知能力的辅助，在危急或严重事故发生前作出预防，让照顾长者的人得到力量和支持，促进环境的健康、安全、易于进出和妥善的环境。

要获取更多资料，请浏览 www.fpciw.org.

front porch | CENTER FOR INNOVATION AND WELLBEING