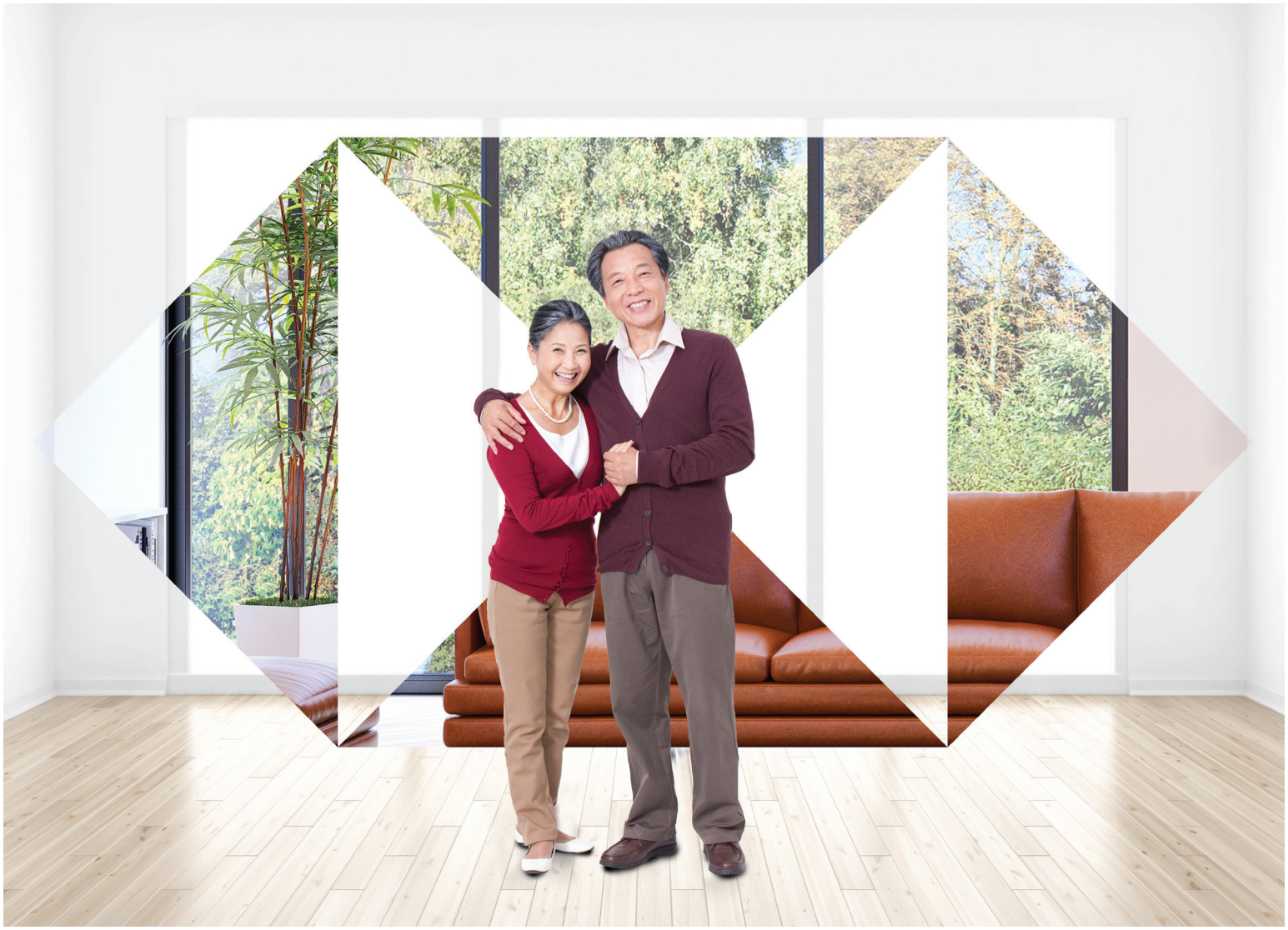


你的钱是重要的
身份盗窃

汇丰
银行

我们一起茁壮成长

内容

什么是身份盗窃? 2

盗贼如何利用你的信息 2

身份盗窃是如何发生的 3

保护你的身份 11

你是身份被盗的受害者吗? 14

如何发生在你的身上，如何去恢复 15

身份盗窃和保护你的法律 17

监控你的信用以防止你成为受害者 18

你的下一步是什么 20

关键词列表 21

记录 22

汇丰银行提供的“你的钱是重要的”这项计划可以提供帮助！联系我们的合作伙伴绿色通道金融健康。 拨打电话 **866.692.2659** 与金融健康专家做一对一的谈话，访问网站 **us.hsbc.com/yourmoneycounts & greenpath.org**。

什么是身份盗窃?

身份盗窃是指利用他人的个人信息、信用记录或者其他身份特征进行购买、借款、就业或者取得法律文件的犯罪行为。不幸的是，大多数人直到成为受害者后才去考虑身份盗窃的影响。每年都有数以百万计的美国人受到影响，这种情况可以以多种不同形式出现。

我们可以很轻易的假定我们的个人信息是安全的，但是每分钟就有19人成为身份盗窃的受害者。这是一个可怕的数字，但你不应该惊慌，因为你可以采取措施来保护你的身份。

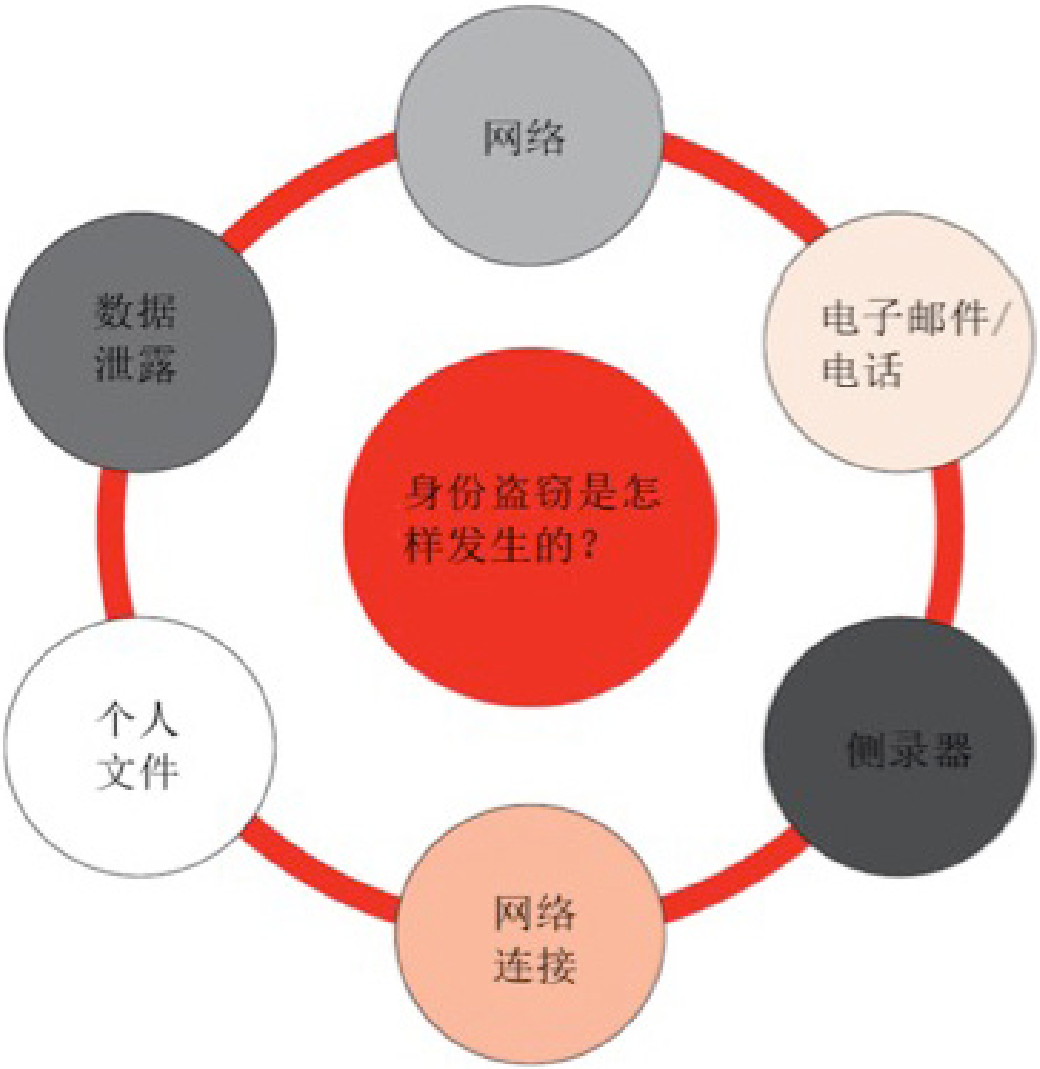
身份盗贼如何利用你的信息

盗贼会用几个不用的方式去利用你的个人信息。 盗贼会:

- 利用你现有的信用和信用卡号码去购买商品。
- 开设新的信用账户。他们使用帐户后可能不支付账单，导致拖欠帐户出现在您的信用报告上。或者，他们可能会按时支付账单的最低额度，以保持信用额度的开通和活跃。
- 用你的名字去开通电话或无线服务。
- 开设银行账户，开出不良支票。
- 以你的名义贷款，购买消费品。
- 获取护照、就业、医疗保险、法律文件、驾照等。

身份盗窃是怎样发生的

身份盗贼在你不知情的情况下获取你的一些个人信息，并利用它进行欺诈或盗窃。盗贼获取您的信息的一些例子如下:



网络

虚假网站（Pharming）

虚假网站是发生在互联网上的身份盗窃的一种形式，有人(法老)引导用户进入欺诈性的商业网站并捕获用户输入的个人数据。 您可能是通过电子邮件直接联接到这些欺诈性网站。

请看下面的网站示例。一开始你可能不会注意到任何不同之处。然而，如果你仔细看，第二个网站有什么问题吗？这个网站很可疑。如果你查看文本，你会发现它不是facebook.com。它看起来非常相似，但是，它并不以.com结尾，而且它也不是一个安全的网站(没有锁符号或https://).)如果您将电子邮件和密码输入到第二个站点，您输入的信息可能会被身份盗贼存储和使用，从而使您面临风险。所以要小心！确保检查在网站地址前面是否有一个安全锁图标或https：，并去读取网站地址，以确保您所在地方正是您想要在的网站上。

有信誉的网站登陆要求是安全的。欺骗网站将捕获您的登录信息，并有可能窃取您的数据。

避开虚假网站的建议：

- 注意你在互联网上的位置。你是在你以为的那个网站上吗？
- 不要把你的个人信息或财务信息发送到你无法确认的电子邮件里，也不要把这些信息输入你无法确认的网站上。
- 确保你在一个安全、加密的网站上。安全站点通常由url指定，以“https”开头，“s”代表安全。它还可能显示锁图标:

电子邮件

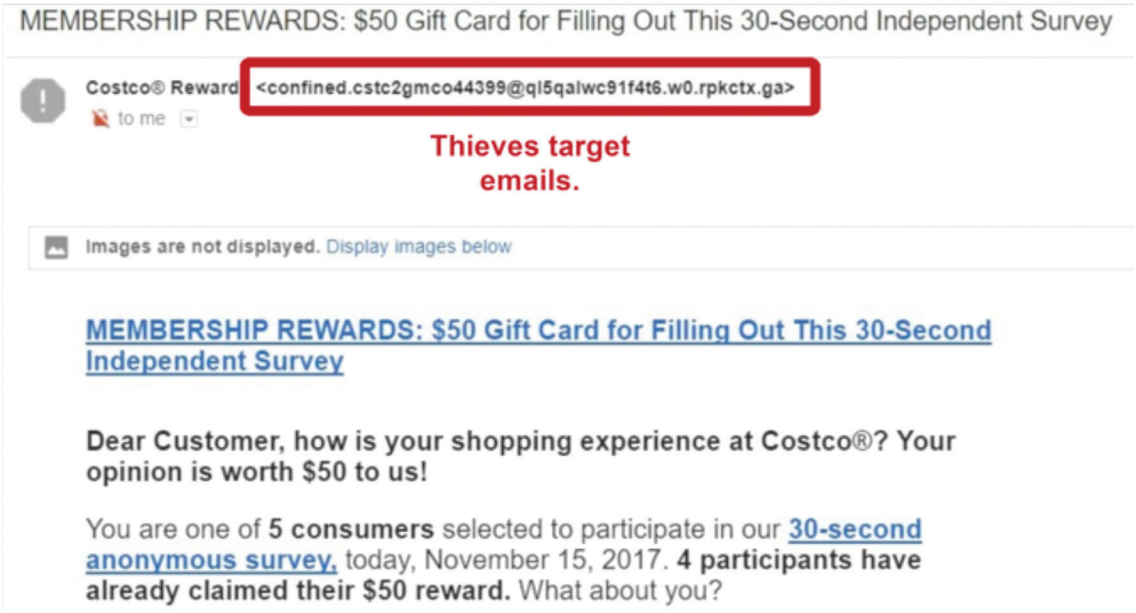
电子邮件钓鱼欺诈(Phishing)

电子邮件钓鱼欺诈是利用电子邮件来“钓鱼”试图获得密码和财务数据一种技俩。欺诈者建立一个假网站，并发送数千封带有假网站链接的网络钓鱼电子邮件。受害者点击电子邮件中的链接，相以为这是合法的网站。然后，网站会提示他们输入个人信息。欺诈者汇编被盗的个人信息，并在网上出售或自己使用。

请看下面的电子邮件示例。这封邮件有什么不对？你会点击这封电子邮件中的链接吗？

这是一个垃圾邮件的例子，身份窃贼正在“钓鱼”你的个人信息。该邮件地址里的字母和符号是随机选取的，而不是传统的@Costco.com或类似的公司电子邮件地址。如果你在这封电子邮件中点击一个链接，你可能会被引导到一个可疑的网站，在那里窃贼正在等待盗取你的用户名和密码。

你可能会收到过似乎来自你的银行的电子邮件。汇丰银行永远不会给你发送电子邮件通知，要求你在电子邮件中中提供你的个人资料，其他银行也不会。你应该以同样的谨慎和逻辑来辨别这类电子邮件的有效性。如果你不确定，不要点击！



避免被钓鱼的建议:

- 删除未知的电子邮件，不要下载附件，不要点击电子邮件中包含的链接。
- 不要为了贪图方便而忽视安全。不要点击你没有预期的或你不确定是谁发送的电子邮件的链接。
- 通过电话联系公司或个人，确认邮件的有效性。不要回复电子邮件。

电话

电话欺诈（Vishing）

语音钓鱼（也叫Vishing）是一种通过电话进行的攻击。欺诈者通过打电话试图操纵人们行动或让人们为他们提供信息。欺诈者可能通过提问问题来获取家庭成员或受害人的个人生活的信息，这最终导致受害者在不知情的情况下信息，这些信息可能会被罪犯拿来利用。欺诈者也可能会使用恐吓手段，例如告诉你你的家庭成员有麻烦，他们需要你寄钱帮助他们。欺诈者可能会假装他们是来自你的金融机构，并试图让你提供密码或信用卡号码，以便他们可以访问你的金融帐户。

老年人往往是这类欺诈的目标。一定要提醒你的父母、祖父母和年长的邻居，让他们知道保护自己。如果你不认识来电者，不要透露任何个人信息或敏感信息！

短信欺诈（SMShing）

SMShing或Smisching(一个相当新的网络术语)是用移动设备操作的类似网络钓鱼的行为。当您的手机上收到一条声称来自一个来源是有信誉的短信(文本)，要求您提供个人信息，这就是短信欺诈。

避免被电话欺诈和短信欺诈的建议:

1. 不要通过电话或短信提供敏感信息。金融机构永远不会要求提供口令或密码。
2. 如果你不确定来电者或发短信者是他们声称的人，建议你终止通话，并直接与该机构联系。
3. 把你的电话号码加到全国不打电话（Do Not Call）名单上，这可以把你从大多数的电话推销员的名单上删除。登记网址：www.donotcall.gov。

   • 请记住，合法组织遵守“不打电话”名单。欺诈者不遵守这一法律。

侧录器

侧录器是一种小型仪器，用在合法的信用卡或借记卡交易中以窃取信用卡或借记卡信息。当信用卡或借记卡通过侧录器时，设备会捕获并存储卡磁条中存储的所有详细信息。侧录器最常见于ATM（自动提款机）和燃气泵上。

避免侧录器的建议：

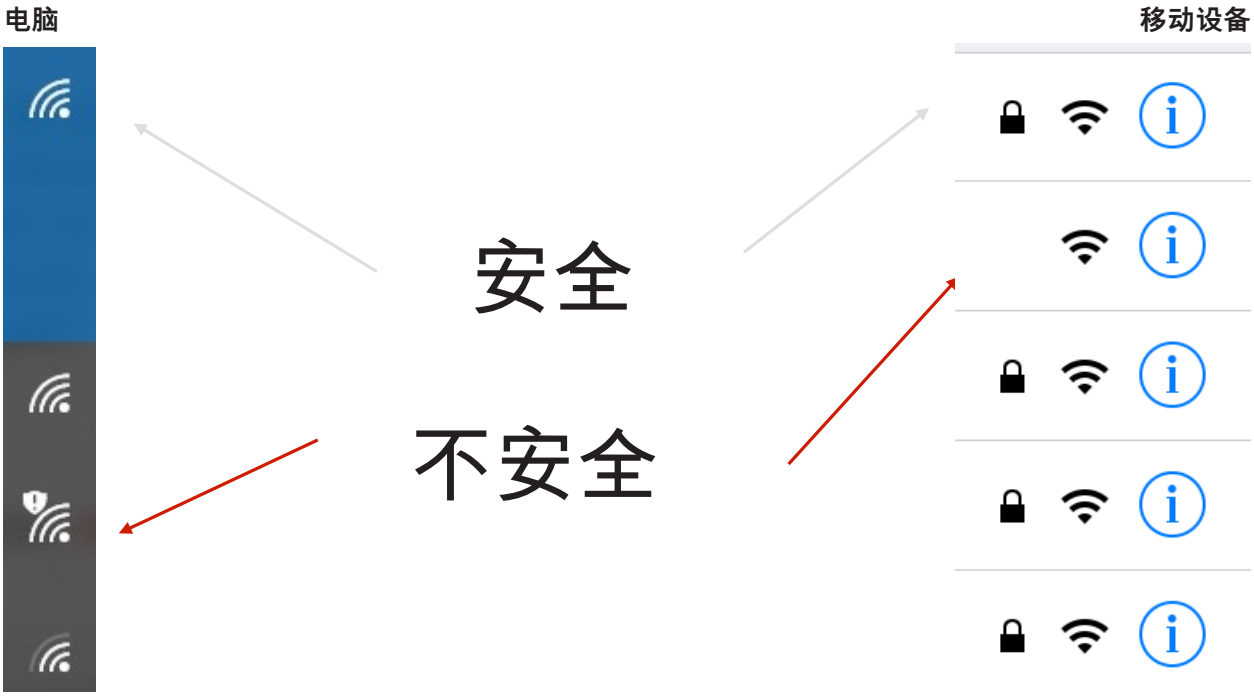
- 使用加油站服务员视野内的加油泵加油。
- 尽可能使用你的金融机构内的ATM（自动取款机）。

网络连接

身份窃贼获取信息的一种常见方式是通过不安全的网络连接。因此，在使用移动设备或计算机时，使用安全的Wi-Fi连接是很重要的。

查看下面的连接图片。如何知道你的电脑或移动设备连接的网络是安全的？当你把电脑和Wi-Fi连接时，不安全的网络连接将有一个带有黑色感叹号的符号，并且不需要密码。安全网络需要输入密码。

与移动设备连接时，锁符号表示网络是安全的，并需要密码才能连接。如果你没有看到锁符号，并且不需要输入密码，则表示网络是敞开的或不安全的。



避免连接到不安全的网络的建议:
把计算机和移动设备上自动连接到打开的网络的设置关闭起来。

个人文件

身份盗用的另一种方式是个人信息的丢失。如果朋友、亲戚、雇员或陌生人窃取你的数据或你的个人信息在因某种原因被泄露。盗用身份的人通常会偷走信件、搜查垃圾，或者拿走你的钱包、提包或手机来获取你的个人信息。他们也可以在你做事的时候偷窥，或是在你没有锁上你的电脑就走的时候把你的信息拿走。

避免个人信息丢失的建议:
不要把密码写下来，不要把密码和卡放在一起，也不要把它放在别人容易看见的地方。

从第11页开始，您可以找到更多主动保护您的个人信息和文档的办法。

数据泄露

一个人在自己曾经发生过业务往来的地方个人档案被盗时，就会发生数据泄露。例如，您可能听说过一家大型零售商的信用卡/借记卡号码被盗。

避免受到数据泄露影响的建议：
要积极主动。如果您了解到可能受到数据泄漏的影响，请更改与已泄漏帐户相关联的密码。

数据泄露示例：标题

- “Delta 数据泄露2018：你的付款信息被暴露了吗?
- “Target(目标折扣店)的数据泄露正在变成恶梦”
- “Yahoo(雅虎)称有5亿个账号被盗“

2017年艾可飞泄露

2017年，有1.44亿美国人受到Equifax（艾可飞）数据泄露的影响。Equifax（艾可飞）是三大信用局之一。由于这一漏洞，Equifax（艾可飞）向所有受到影响并提出要求的人提供一年的免费信用监测。每四个月检查你的信用报告的准确性是非常重要的。而以这个为例，则应该对可能影响到你的数据泄露立刻跟进。你若要获得免费信用报告，请访问 ***annualcreditreport.com***.

保护你的身份

几乎每个人都很容易被盗用身份，因为外面有太多的个人信息如果你曾经申请过信用卡、信用额度或贷款，上过大学或有过工作，有过储蓄账户或支票账户，或者在雇主那里有过医疗保险，那么你将面临风险。

你可以通过积极地管理你的个人信息和不断地提高意识来降低你的风险。保护你的身份不被盗用有很多的方法:

社会安全号码 (SSN)

- 只有在绝对必要的情况下才给出你的SSN（社会安全号码）(如雇主需要你的号码来报告工资和税收)。
- 不要把社会安全卡带在身上。把社会安全卡存放在安全的地方，比如家里这样安全的地方。
- 任何时候都不要把SSN（社会安全号码）写在你的支票上。
- 如果有人向你询问你的SSN（社会安全号码），提出以下几个问题：(你获得的答案将有助于确定你是否想要继续与他们有业务往来)。
    - 你为什么需要?
    - 你怎样去防范号码被盗?
    - 用来做什么?
    - 如果我不给你会有什么后果?
- 每年检查你的社会安全收入记录和福利对账单以确定没有欺诈发生。

密码

- 设定复杂的密码，密码包含大小写字母、数字和特殊符号。
    - 不要用容易识别的信息如：母亲未婚时的姓、地址、出生日期或你的电话号码。
    - 设定新密码时，使新的密码明显有别于原来用过的密码。
- 如果你很难记住你的密码，那就写下一些有助于帮助你记起来的线索，但是线索不能让别人容易猜到，记得把线索藏在安全的地方。
- 不同的账户设定不用的密码。
- 不要把密码保存在与他人共享的手提电脑里，也不要保存在手机里。
- 如果你认为他人知道了你的密码或者别人能够进入你的账户，应立刻改变你的密码。
- 不要把你的密码告诉任何人，也不要写下来或带在身上。

个人文件/信息

在家里

- 撕碎所有敏感材料，如账单、预先批准的信用优惠以及其他带有个人信息的文件。
- 不要把你的密码写下来带在身上。
- 不要把个人信息放在室友、亲戚或外援人员可以看到的地方。
- 控制好你的财务状况，尤其是账单到期日期。
- 如果你接到电话，你向对方要求给对方回电话。除非你知道你在和谁说话，否则不要透露信息。
- 你的账单上出现任何可疑的费用及时报告。
- 在你用邮件支付账单时，不要把你的信用卡号或账号写在支票上。
- 立即签署和激活新的信用卡。把过期的信用卡剪碎或撕碎后扔掉。
- 如果你住的地方外寄的信件由邮递员收取，请你多付出一点努力，把要寄出的信件送到邮局，并且把垃圾桶放在安全的地方。
- 把金融、个人和保险卡及身份证复印一份放在你携带的钱包里。把这些东西放在家里安全的地方。
- 每年向三大信用机构各订购一份信用报告，登陆 *annualcreditreport.com*.

在你外出的时候

- 只携带你实际需要的信息。钱包里不要装任何你不需要的其他身份资料。
- 确保自动柜员机(ATM)卡、个人识别码(PIN)和自动取款机收据的安全。

在工作中–安全练习和质疑一切

- 每次你离开的时候都要把笔记本电脑锁上。如果你在酒店中使用笔记本电脑，在你离开房间前把电脑关上放好。
- 不要把个人信息扔进垃圾中。
- 在笔记本电脑上安装一个隐私屏幕，以避免坐在你旁边的人窥探。
- 不使用的时候，一定要关掉笔记本电脑上的无线网络。

科技品

- 使用安全的浏览器来保护在线交易的隐私。
- 启用移动设备上的密码选项。
- 定期更新家用电脑的防毒软件。
- 在线支付账单。在网上支付账单，身份被盗用的机率要比通过邮件支付的要低。
- 仔细阅读隐私政策。
- 不要从陌生人那里下载文件，也不要从你不认识的人那里点击超链接。
- 如果你收到一封朋友的电子邮件，上面只有一个链接，或者有些东西看起来很奇怪，那么在点击任何东西之前，先联系一下你的朋友。
- 避免使用为在线服务提供的自动登录功能。

减少在线风险

我们今天所做的许多事情都是在网上完成的，因此我们必须尽可能地减少我们的风险。以下是一些在线保护自己的额外提示。

- 反病毒程序　反病毒程序是检测、预防和清除计算机病毒的软件程序.确保在所有技术设备上使用有信誉的防病毒程序，并定期更新程序。 一些不错的选择包括BitDefender（比特梵　），Norton（诺盾），Kaspersky Lab（卡巴斯基　　室）和McAfee（迈克菲）。

- 清除cookies（小甜饼）　　网页小甜饼（Webcookie）是网站用来跟踪各种用户活动的特殊文件。您应该定期从网页浏览器中清除cookie（小甜饼），方法是进入设置并按照要删除的指示进行操作。大多数网络浏览器cookie（小甜饼）设置都在“选项”或“设置”菜单中。在线查询如何删除首选浏览器的cookie（小甜饼）。您也可以使用匿名浏览或非公开浏览。你可以通过右键点击你的互联网图标，然后选择私密或隐秘的浏览。这允许您在不附加历史记录或cookie（小甜饼）的情况下进行搜索。

- 谨慎对待你在社交媒体上分享的内容　身份盗贼在许多地方寻找你的信息，如果你不小心，社交媒体可以很容易把你的个人信息拼凑在一起。不要分享身份证件的图片、账单、旅行确认信息或活动门票。

- 使用 Apps（应用程序）　你允许访问什么？在使用应用程序时如果被要求允许访问你的数据或位置时要小心。允许应用程序访问通讯录或“通过Facebook登录”既是允许第三方应用程序可以访问您的数据。

总之，尽可能把你可以控制的东西保护好。小心身份盗窃，注意检查你的信息，发现可疑的活动立即报告。

你是身份盗用的受害者吗?

有时候，你会在最不合适的时候才发现自己是身份盗窃的受害者。如：去工作机会、贷款被拒绝，甚至被逮捕，也许这些事情的发生才给你敲起警钟。

了解自己是否是受害者的一些最常见的方法包括:

- 在你的支票账户或储蓄账户上出现不明原因的费用或取款。
- 未能收到每月账单。
- 收到您没有订的信用卡。
- 信贷无缘无故地被拒绝。
- 债权人和收债人的账单催缴电话，而这些账单并不是你的。
- 你的信用报告上出现非人为错误引起的不准确报告。

如何恢复？

如果你是身份盗窃的受害者，你要知道你有那些记录已经失密，你可能要去提交一份警察报告。你的一些记录的位置可能比另外一些更常见。比较常见的数据库包括：信用机构、地方和州警察局以及机动车管理部门。因为身份窃贼的犯罪活动、欺诈性的银行活动或与你的社会保险号码有关联的未知地址，你的个人信息也有可能出现在联邦监视名单上。

如果你成为身份盗用的受害者，请迅速采取行动，恢复你的良好声誉。访问IdentityTheft.gov 获取良好的资源为你提供帮助，指导你逐步恢复你的声誉。

根据已发生的身份盗窃的类型，采取的步骤可能不同，这个网站将引导你采用恰当的步骤。一般情况下，你要考虑以下几点:

第一步: 给欺诈发生的公司电话。	• 要求联系欺诈部门 • 关闭或冻结账户 • 按照程序对不准确之处提出异议。 • 设定新的个人识别码（PIN）、密码等。
第二步: 联系信用机构设定欺诈警报，并获取你的信用报告。	• 在三家机构-艾可飞、益博睿和环联在你的信用报告中设定欺诈警报。 • 小心核对你的信用报告（你可以在Annualcreditreport.com申请获得免费的信用报告。).
第三步: 向联邦贸易委员会和其他相关机构报告身份盗窃。	• 通过FTC www.ftc.gov 提交投诉。 • 你可以在身份盗窃发生的地方向当地的警察局做一份警察报告。要冻结你的账户，一份警察报告是必需的。 • 如果有人使用你的社会安全号码，联系社会安全局（SSA），访问www.ssa.gov. • 如果您的邮件被篡改，请与美国邮政部门联系。
下一步怎么办: 对受损的部分做好修复跟踪并维护好未受损的信息。（对你的行动做好记录，并有书面确认。）	• 关闭已经打开的账户。申请要一份书面确认。 • 要求删除被盗用的交易。 • 与信用报告机构跟进，纠正你的信用报告中的不准确之处。在几个月后再要一份你的报告，以核实所有的更正。 • 考虑在90天后延长欺诈警报，或考虑应用信贷冻结。

建议:

解决盗用身份的问题并不是一朝一夕的事。平均而言，修复身份盗窃需要6个月或200个小时的时间。它可能会对你的信用评分产生负面影响，并会影响你办事的能力，比如买房、租赁公寓、获得贷款或获得其他种类的信用。它甚至可能使开设新帐户(如煤气水电帐户或支票帐户)变得困难。因此，迅速采取适当措施加以纠正是非常重要的。

身份盗窃和保护你的法律

解决因身份盗窃而产生的信用问题可能会耗费时间，而且令人沮丧。对纠正信用报告和账单错误联邦法律提供有保护措施，这项联邦法律保护你免于被收债者向你索要不是你欠下的债。

此外，还通过了专门针对身份盗窃的联邦法律。

2003年《公平正义信用交易法》(FACT Act)

- 每一位消费者每年都有权免费获得他们的信用报告。
- 要求商家在商店收据上只能留下信用卡号码的最后五位数。
- 为消费者创建和成立国家欺诈检测和警报系统。
- 制定处置规则，规定所有以商业目的个人，不管此人是消费者信息的维护者或拥有的者，在处置这些信息前必须先做妥善的销毁。

1998年《身份盗窃和推定威慑法》

- 没有合法的理由去转移或使用他人的身份证明以实施犯罪意图，则构成联邦罪。

《身份盗窃罪加强刑罚法 》

- 加大对身份盗贼的惩罚力度。
- 造成“严重身份盗窃”罪，如果与其他重罪有关，最高可判处两年徒刑

《公平信贷账单法》

- 在处理帐单错误时，给予消费者特定的权利。

《电子资金转账法》

- 建立程序解决电子资金转移账户报表的错误。

《公平信用报告法》

- 旨在提高报告机构文件中每个消费者的信息的准确性、公正性和隐私，其中最常见的是信用报告局。

建议:

如果你遭遇身份盗窃后信用有问题，你想找人了解你的情况，有一些非营利的信用咨询机构可以帮助你。如果你想联系绿色通道财务健康，这是一家非盈利机构，已经帮助人们近60年。 你可以拨打电话免费咨询你的个人情况，电话号码*866.692.2659* 或访问*greenpath.org.*

监控你的信用以防止你成为受害者

监控您的信用应该是您个人财务计划中的一个关键部分。

无论你的财务状况如何，了解信用报告中的信息是很重要的。这些信息直接影响到你获得信用卡、买车或买房、租公寓、甚至找到新工作的能力。审查你的信用报告的两个最好的理由是：1)确保你的信用报告是准确的；2)保护你自己免受欺诈或身份盗窃。

你可以从*annualcreditreport.com*每四个月获得一份免费信用报告来创建自己的免费持续的监控系统.

比如:

1. 一月份，订要Experian（益博睿）的报告。

2. 五月份，订要TransUnion（环联）的报告。

3. 最后，九月份，订要Equifax（艾可飞）的报告，然后明年一月份又重新开始。

由于三家信用报告局的信息大多数相同，你可以在信用报告上的活动识别可疑的项目。如果发现有不准确的地方，你可以逐个向三家机构提出争议。联系信息如下:

信用报告局		
联系:	电话:	网站:
Experian（益博睿）	888-EXPERIAN	www.experian.com
TransUnion（环联）	800-916-8800	www.transunion.com
Equifax（艾可飞）	800-685-1111	www.equifax.com

儿童也可以成为身份盗窃的受害者。如果您有孩子，并怀疑他们是身份盗窃的受害者，您可以检查是否存在您的孩子的信用报告。每个信用报告机构的网站都有关于这方面操作的说明。

当涉及到你的个人信息时，小心谨慎是最重要的。

结论

盗用身份是犯罪行为。盗用身份每年都会影响到许多美国人。虽然没有办法可以保证完全避免，但你可以采取一些措施来保护自己。保护你的社保号码、查看你的信用报告、在购物时注意你的环境，特别是当你需要用到敏感信息的时候，你可以利用这些措施来保护自己。记住，如果你是身份盗窃的受害者，不要惊慌。与有关当局联系，并参阅本手册中介绍的办法。

（绿色通道财务健康）是一家全国性的非营利组织，提供财务咨询，教育和产品，让人们能够过上财务健康的生活。 通过与个人直接合作，以及通过与其他组织的合作，GreenPath（绿色通道）旨在帮助每个人去打造自己的美国梦。 总部位于密歇根州法明顿希尔斯的GreenPath（绿色通道）拥有近500名员工，在19个州经营着约60个分支机构。 GreenPath（绿色通道）是国家信用咨询基金会（NFCC）的成员，并获得了认证委员会（COA）的认证。 欲了解更多信息，请访问greenpath.org（绿色通道）或拨打电话866.692.2659与经过认证的金融健康专家进行一对一交谈。

你的下一步是什么?

吸收你所学的知识并付诸行动是很重要的。积极主动是防止身份盗窃的最好办法。完成以下行动计划，并使用校对清单以确保您继续朝着你的目标前进。设置完成目标的日期，并在完成操作项时在对应的方框做标志。

行动计划:

- ☐ 1 **我会:** 上网的时候小心，对我不认识的电子邮件也要小心。
- ☐ 2 **我会:** 我在ATM（自动提款机）和其他地方使用卡的时候要小心侧录器。
- ☐ 3 **我会:** 只使用安全的网络连接，把我电脑上和移动设备的自动连接功能关闭。
- ☐ 4 **我会:** 保护我的文件和资料，包括社会安全号码、密码，个人识别码（PIN）和敏感资料。我会设定复杂的密码，撕毁敏感文件，小心使用高科技品以保护我的个人信息。
- ☐ 5 **我会:** 注意有关数据泄露的新闻。我会积极主动应对的对可能影响到我的数据泄露。
- ☐ 6 **我会:** 为了降低我的在线风险，我会使用和更新防病毒程序、在互联网上清除cookie、不在社交媒体上分享个人信息以及不允许应用程序（APP）访问我的个人信息。
- ☐ 7 **我会:** 如果我成为身份盗窃的受害者，我会按照identitytheft.gov上的步骤操作。我将持续监测我每年的信用报告的准确性，如果我需要专家的额外指导，我将拨打866.692.2659联系GreenPath（绿色通道）财务健康获得帮助。

补充记录和目标: _____

_____

我会做好准备!

关键词

防毒程序 – 一种检测、预防和清除计算机病毒的软件程序。

应用软件 – 用在移动设备上下载的应用程序或程序。

Cookies（小甜　） – 网站用于跟踪各种用户活动的特殊文件。您应该定期从网页浏览器中清除cookie（小甜饼），方法是进入设置并按照要删除的指示进行操作。

信贷冻结 – 消费者可以对其信用报告进行信贷冻结以锁定报告，新的信用帐户将无法打开。信贷冻结后，将一直保留在你的报告里直到你删除它。（在一些州，7年后到期。）根据国家法律，信贷冻结可能涉及费用。在大多数州，对身份盗窃的受害者是免费的。对于其他人来说，每次消费者冻结或解冻他们在每个信用报告机构的账户时，费用大约5到10美元。

信用报告 – 一种财务报告卡，用来评估你的信用价值和计算你的信用分数。信用报告包含关于个人信用记录的详细信息，包括个人识别信息、信用账户和贷款的信息(包括付款记录)、公共记录和查询。

数据泄露 – 个人档案在曾经发生过业务往来的地方被盗。

加密 – 将信息或数据转换成代码的过程，尤指防止未经授权的访问。

欺诈警报 – 消费者可以在他们的信用报告中设置欺诈警报，这就要求企业/贷款人在发放新的信贷之前要验证消费者的身份，这使得身份窃贼难以你的名义开立更多账户，欺诈警报是免费的，通常情况下，设定后如果没有延期，警报会信用报告保留90天。

身份盗窃 – 用他人的个人信息、信用记录或者其他身份特征进行购买、借款、就业或者取得法律文件的犯罪行为。

密码 – 一种秘密的词或短语，用来做一种身份验证。强密码应该是复杂的，包含大小写字母、数字和特殊字符。

个人识别码 (PIN) – 在许多电子金融交易中使用的数字或α-数字代码，用于对系统的用户进行身份验证。例如，您必须输入您的个人识别码密码才能从ATM机上从您的帐户取钱。

个人信息/文件 – 包含个人识别信息的文件，如社会保险号码、出生日期、地址等，盗贼窃取这些信息，然后在你不知情的情况下利用这些数据进行欺诈。

虚假网站(Pharming) – 一种在互联网上发生的身份盗窃形式，有人(法老)引导用户进入欺诈性的商业网站并捕获用户输入的个人数据。

电子邮件钓鱼欺诈（Phishing） – 电子邮件钓鱼欺诈是利用电子邮件来“钓鱼”试图获得密码和财务数据一种技俩。欺诈者建立一个假网站，并发送数千封带有假网站链接的网络钓鱼电子邮件。受害者点击电子邮件中的链接，相以为这是合法的网站。然后，网站会提示他们输入个人信息。欺诈者汇编被盗的个人信息，并在网上出售或自己使用。

安全网络连接 – 一种由一个或多个安全协议加密以确保数据流安全的连接。建立安全连接需要密码。

侧录器（Skimmer） – 侧录器是一种小型仪器，用在合法的信用卡或借记卡交易中以窃取信用卡或借记卡信息。当信用卡或借记卡通过侧录器时，设备会捕获并存储卡磁条中存储的所有详细信息。

短信欺诈（SMShing） – SMShing 或 SMiShing是类似与Phishing（电子邮件欺诈）的一种欺诈行为。当您的手机上收到一条声称来自一个来源是有信誉的短信(文本)，要求您提供个人信息，这就是短信欺诈。

不安全网络连接 – 无需密码即可访问且未加密的网络连接。这些网络向公众开放。

电话欺诈（Vishing） – 语音钓鱼（也叫Vishing）是一种通过电话进行的攻击。欺诈者通过打电话试图通过操纵人们行动或让人们提供他们想要的信息。

记录