尊敬的纽约人：

您的身份信息遭遇威胁。无论是通过网络、电话甚至面对面交流，相比过去，今天的诈骗者更容易窃取您的个人信息并将其用于诈骗目的。

身份信息失窃每年对数百万人造成影响。诈骗者会使用您的信息申请信用卡、医疗福利甚至利用您的社保号码进行税务欺诈，损害您的信用状况，导致您需要花费时间和金钱修复信用。

只需多加留心，您就能够保护您的个人信息，防止大多数形式的身份盗窃，我们将帮助您学习如何做到这一点。

欲了解有关如何确保自己身份信息安全的更多信息，或者了解在认为自己身份信息被盗的情况下应当采取什么措施，请登录我们的网站：ag.ny.gov。

此致，

Letitia James

纽约总检察长
Letitia James

资源

纽约州检察长办公室反消费者欺诈局
报告诈骗或提出投诉。
(800) 771-7755 / ag.ny.gov

美国联邦交易委员会
报告诈骗或身份盗窃。
877- 382-4357 / ftc.gov

年度信用报告
核验或冻结您的信用报告。
877-322-8228 / annualcreditreport.com

大型信用报告机构

Experian:
(888) 397-3742 / experian.com

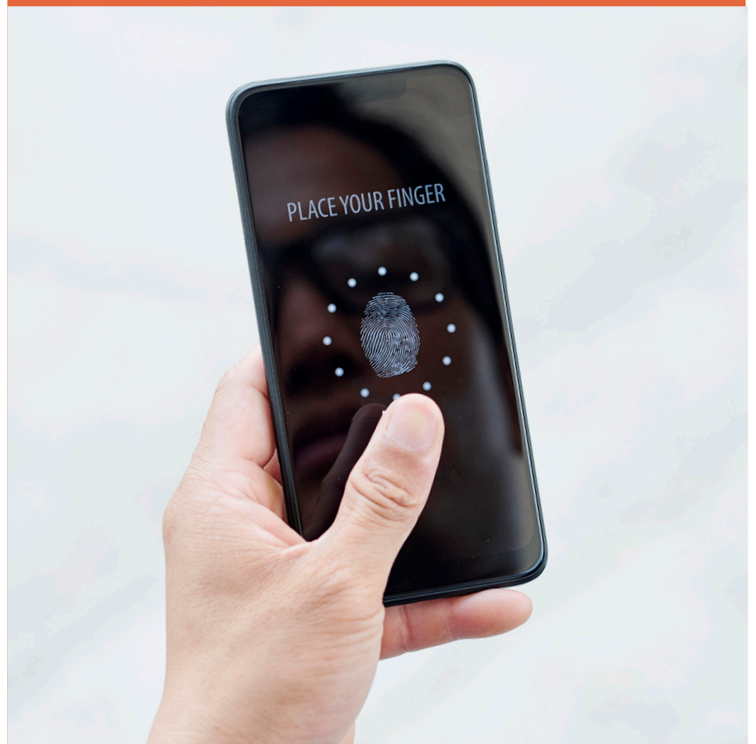
TransUnion:
(800) 888-4213 / transunion.com

Equifax
(800) 685-1111 / equifax.com

Innovis
innovis.com

保护您的身份信息

保护您身份信息安全的小贴士



纽约州总检察长
Letitia James
的办公室

保护您的个人信息

一般来说，向他人提供姓名或电话号码是安全的，但是告诉他人您的出生日期、社保号或任何帐号可能会导致您的身份被盗。您还应该避免泄露您用作在忘记密码时从网站“找回密码”问题的任何信息。

绝不要将您的个人信息透露给贸然联系您的人；除非您曾联系过对方，否则您很可能遭遇“钓鱼”。

“钓鱼”指的是企图让受害人提供个人信息，如他们的用户名、密码或信用卡号的行为。 骗子可能会通过短信、电话或电子邮件联系您，他们经常伪装成政府机构、银行或知名公司。他们会要求您提供个人信息以解决一些问题或紧急情况，或者假称他们只是需要“确认您的信息”，以便于向您提供某样东西。

事实上，正规机构不会以这种方式联系您索要重要信息。如果您不确定，拨打相关公司的电话（使用公开的号码）核实情况是否属实。一些企图实施网络钓鱼的手段是让您访问某个网站或打开某个附件。不要下载陌生人发送的附件或点击陌生人发送的链接。其中可能包含病毒，会感染您的电脑并窃取您的个人信息。

可疑信息：

即使发件人看起来是可信来源，如亲戚或熟悉的公司，它仍然可能是钓鱼行为：骗子可能已经盗取了这个帐户，或者用相似的名字创建了一个新帐户。如果您收到的信息语气反常，不像该发件人，只包含一个链接或附件，没有任何解释，或者在其他方面引起您的怀疑，请再次确认“发件人”字段，确保地址正确无误，或打电话给发件人确认情况是否属实。不只是电子邮件或短信，这种情况在社交媒体上也很容易发生，所以不要仅仅因为可疑信息来自于“朋友”，就选择相信它。

社保号

公司基本不需要向您询问社保号。如果有公司询问，一定要问清楚对方为什么需要，特别是当对方不是政府机构、雇主、银行或金融机构时。**再次强调，绝不要将它透露给不请自来的联络者。**

使用防火墙，更新操作系统

浏览网络可能会让您的电脑接触到病毒。保持更新操作系统和防病毒程序，并使您的防火墙保持运行，以保证安全。

创建强密码

如果您上网，您就需要强密码，并且需要好几个。强密码：

- 长度较长。应该至少为八个字符，越长越好。
- 不会被盯上您的坏人猜出，因此不要使用亲戚的生日或姓名。
- 应该是您可以记住的事物。这种情况下，使用长而不常见的单词（“batterystapler”）组合是个好办法。
- 只使用一次。如果您多次使用同一个密码，一旦别人获知，对方就可以访问您的所有帐户。

密码管理器

现在的浏览器有“密码管理器”功能，您可以安装它，用于记住密码：只要下载一个管理器，其他所有操作都会自动完成。一定要保护管理器的密码安全：如果骗子获得了它的访问权限，则他们就能访问您的所有帐户。

设置密码保护设备

像对待网站帐户一样对待手机和电脑帐户：设置唯一的强密码。

默认密码

有些设备，比如路由器或调制解调器，会有一个默认密码。默认密码基本不具有安全性，因此一定要立即修改。

定期修改密码

即使您按这条建议操作，您使用某个密码的时间越长，黑客获得密码的可能性也就越大：网站可能会遭到入侵。如果相关网站被入侵，一定要修改密码，并定期修改密码以确保安全。

安全连接

不安全的网站或Wi–Fi网络可能会泄露您的个人信息。绝不要通过公共网络操作个人或金融业务，在向网站提供任何敏感信息之前，一定要确保网站“安全”。安全站点以 **“https://”**开头。 而不是 **“http://”**

删除不需要的数据

对于任何个人信息记录，一旦不再需要，建议销毁。将收据、纳税申报单、财务或医疗记录等物理文档粉碎；删除或停用数字帐户并删除数字文件。请记住，即使是已删除的文件，仍然会保存在您的硬盘上，所以如果需要处理旧电脑，您需要特殊的安全软件删除所有的个人数据。

监控结单

仔细查看信用卡和银行结单上是否存在任何您并未授权的活动。

仔细检查医疗帐单和健康保险，确保您确实接受过上面描述的治疗。

信用报告

每个人都有权每年获得一份免费的个人信用报告，报告由各家大型信用报告机构提供。如果发现并非由自己发起或者自己不认识的帐户或查询，则可能说明其他人正在使用您的身份信息。您可以通过annualcreditreport.com或(877) 322-8228，安排在一年的不同时间段从不同机构获取报告，从而保证定时查看个人信用。

儿童身份信息失窃

儿童身份信息失窃最为常见，有时窃取信息的是信用评级糟糕的家人。像保护自己的个人信息那样保护您孩子的个人信息。如果他们接到他们名义下的账单缴费电话或者信贷邀约，因为其他人使用他们的号码而在福利方面遭到否决，或者收到IRS关于应缴税金的通知，请务必提出疑问并采取措施。