做网络聪明：把你的“盾牌举起”

网上安全简单步骤

网络骗局已不是新事物了。每天，黑客和其他网络罪犯都在寻找最容易的网上目标。你认为自己不够有价值，不会成为网上掠食者的目标吗？再好好想想吧！

不管是你的身份信息、你的银行账户信息，还是单纯的你的电子邮件里的内容，你的信息都是有价值的，网上罪犯也会尽其所能来获取它。他们就仗着你不认为自己会是个目标呢。是时候把你的**盾牌举起**了，开始防范自己不会成为网络罪行的受害人。

让我们以基本的网络卫生开始——最简单也是最具常理的办法来在线上保护自己。以下是四个简单的步骤，你今天就可以开始，保证自己的网络安全：

- **在你所有的账户上都使用超过一种类型的身份验证。**一个密码并不足以保证你的网上安全。通过设置第二层的身份验证，比如确认短信、用身份验证软件生成代码、脸部或指纹识别，或安全钥匙，你会给你的银行、电子邮件供应商，或者其他你所登录的网站，一层额外的安全保障。多因素身份验证可以使你 99%更不会被黑客攻击或使自己的信息被盗！
- **更新你的软件。**黑客们会试图利用软件的缺陷和弱点。在你所有的设备上都更新系统软件，比如手机、平板电脑和笔记本电脑。切记也要定期为你的应用查询更新——尤其是网页浏览器——在你所有的设备上。直接打开你所有设备、应用、和操作系统的自动更新是最简单的办法了。
- **点击之前想一想。**超过 90%的成功的网络攻击开始于你在钓鱼邮件里点击了一个不熟悉的链接。一个钓鱼骗局是当一个链接或网页看起来是合法的，但是其实只是一个把戏，为了要让你揭示你的密码、信用卡卡号，和其他敏感信息。另外，钓鱼邮件也可能试图骗你运行恶意软件，也被称为恶意程序。如果你不认得一个链接，相信你的直觉，点击之前想一想。
- **使用强密码。**一个强密码应该由 8 位或更多数位，并由字母、数字和特殊符号混合组成。避免在不同账户上使用同一个密码。 理想上来说，个人也应当使用一个密码管理工具来生成或存储独特的密码。

我们的世界在不断地电子化，也在不断地联网，我们大家都有责任来真正保护我们都所依赖的电脑网络。做网络安全的冠军，分享这些窍门给你的朋友、家人和邻居。

欲了解更多信息，请访问：CISA’s Shields Up webpage.