保持安全的四个简单步骤

概述

以安全可靠的方式充分利用技术看似困难而复杂。但无论您使用哪种技术，或是怎样使用技术，您都可以遵循以下四个简单步骤，帮助确保您的安全。

1.保护好自己：首先，技术本身无法有效保护您的安全；您要对自己的安全负责。攻击者意识到，将您本人（而不是您的计算机或其他设备）作为攻击对象，是获得他们想要的东西的最简单办法。如果攻击者想获得您的密码、信用卡或控制您的计算机，那么他们就会通过营造紧迫感，尝试诱使您提供相关信息。例如，他们可能会伪装成 Microsoft 技术支持人员给您打电话，谎称您的计算机已被病毒感染，但实际上他们是网络罪犯，想要获得您计算机的访问权限。或者，他们可能会向您发送一封电子邮件，警告称您的邮件无法投递，要求您点击某个链接以确定邮寄地址，但其实他们只是想诱骗您访问包含病毒的网站，以便入侵您的计算机。最后，您本人才是抵御攻击者的最牢固防线。运用常识就可以发现和阻止很多攻击行为。

2.密文：在当今的计算速度下，旧的 8 位字符密码已经过时且容易被盗取。当网站要求您创建密码时，请创建安全强度高的唯一密文。密文也是一种密码，由一系列容易记住的词语组成，例如“bee honey bourbon rain”。密文越长，安全强度越高。唯一是指为要每台设备或每个在线帐号都设定各不相同的密文。这样一来，即使泄露了一个密文，所有其他帐号和设备仍然安全。记不住您所有的密文？使用密码管理器，这是一种专用程序，能将所有密文以加密格式安全存储（还提供众多其他强大功能）。

最后，启用两步验证机制（也称作两要素或多要素身份验证）。除了输入正确的密码外，还需要完成另一个步骤，例如输入由应用生成并发送到您智能手机的验证码。对保护在线帐号来说，启用两步验证机制可能是最重要的方法，并且操作起来比您想象的还要简单。

3.保持更新：确保您的电脑、移动设备、程序和应用都运行最新版本的软件。网络攻击者时时刻刻都在寻找您设备使用的软件的最新漏洞。当他们发现漏洞后，就会使用专用程序利用漏洞入侵您的设备。同时，软件公司会通过发布更新来努力修复这些漏洞。确保您的计算机和移动设备及时安装更新，可以将攻击者拒之门外。为此，只需尽可能启用自动更新模式。这条规则几乎适用于接入网络的任何技术，包括 Internet 互联电视、婴儿监控器、安保摄像头、家用路由器、游戏手柄，甚至您的汽车。

4.备份和恢复：有时，我们难以做到万无一失。在遭到入侵时，使用备份恢复所有个人信息通常是唯一办法。确保定期备份所有重要信息，核实您可以从中恢复数据。大多数操作系统和移动设备都支持自动备份，无论是备份到外部驱动器还是云端。

特邀编辑

SANS 认证讲师 Steve Anson 为全球各地的 IT 安全团队和政府部门提供指导，帮助他们改善安全状况。Steve 是即将出版的《Applied Incident Response》一书的作者，并通过 AppliedIncidentResponse.com 为 IT 安全从业人员提供免费资源。

资源

社会工程学： https://www.sans.org/u/Uz6
定制化诈骗行为： https://www.sans.org/u/Uzb
让密码变得简单： https://www.sans.org/u/Uzg
备用重要信息： https://www.sans.org/u/Uzl