SANS SECURITY AWARENESS

给大家的安全意识通讯月刊

虚拟私人网络 (VPN)

概述

当您出门在外时，比如前往当地的餐厅或咖啡厅，旅游期间入住酒店或在机场候机，您可能会发现自己需要使用公共 Wi-Fi 来访问互联网。但这些公共网络是否安全，您的上网行为是否被监控或记录？也许，就连在家时，您都不信任自己的 ISP（互联网服务提供商），并且想要确保他们不会监控您在网络上的一举一动。不妨使用 VPN（虚拟私人网络）来保护您的在线活动和隐私。VPN 这种技术可以为您的在线活动创建私人加密渠道，大大增加他人观看或监控您的在线行为的难度。此外，VPN 还可以帮助您隐藏自己的位置，使您所访问的网站更难以确定您所在的位置。

它是如何工作的？

VPN 的原理是建立一条私人加密通道通向您所选择的 VPN 提供商。您的所有在线活动都会经由该通道离开 VPN 提供商的网络，然后进入您的预期目的地。例如，如果您身在美国佛罗里达州坦帕市，但您接入位于德国慕尼黑的 VPN 服务器，那么您所浏览的任何网站都会判定您是从德国慕尼黑进行访问的。VPN 使用起来很简单。第一步是找到值得信赖的 VPN 提供商，然后创建账号（通常需要购买他们的服务）。拥有账号以后，您需要下载、安装和配置 VPN 软件。软件安装和配置完毕后，照常接入互联网。VPN 软件会默默地在后台为您创建加密通道，并且开始保护您的隐私，甚至连您自己都意识不到。

选择 VPN 提供商

您的在线活动是否安全和私密，取决于您的 VPN 提供商。务必选择您信赖的 VPN 提供商。以下是选择 VPN 服务提供商的要点。

日志：寻找不保留任何日志并专注于保护隐私的服务。如果您的 VPN 服务提供商不收集任何日志，那么要通过查看记录来了解您的在线行为就会难上加难。

公司所在地：不同 VPN 提供商位于不同国家。务必从实行严格隐私法律的国家选择 VPN 提供商。一些国家的隐私法律不健全或不完善，这些国家的 VPN 提供商可能会被迫提供他们收集的关于您的信息。

服务器：寻找服务器位于您所需国家或城市的 VPN 服务。一些 VPN 提供商在全球各地分布着上千台服务器和运营地点。您是否需要伪装成来自某个特定国家的访问者，您的 VPN 提供商在该国家是否设立了服务器？

兼容性：寻找可以在不同计算机和移动设备上运行的服务。例如，您可能会使用 Windows 笔记本和平板以及 iPhone。您需要在所有这些设备上都能运行的 VPN 服务。

避开“免费”陷阱：对“免费”VPN 服务提高警惕，他们如何盈利并维持运营？免费服务可能收集和出售您的信息。

VPN 是帮助保护在线隐私的最好方式之一。不过，VPN 并不能保护您的电脑、设备或在线账号。所以，即使您使用 VPN，也要始终遵循基本安全步骤，包括更新设备，使用锁屏，为所有账号设定单独的复杂密码。

特邀编辑

Phil Johnsey（@peakreflections）是位于 Palm Beach County 的 IT 专业人员，在安全、取证和审计方面拥有丰富经验。他获得了 SANS 数字取证和安全基础认证，是 OUCH 社区审查委员会成员。他热衷于为他人提供简单的安全措施。 Why

资源

个性化攻击: https://www.sans.org/u/Sd8
保护您的移动设备: https://www.sans.org/u/Sdd
停止此恶意软件: https://www.sans.org/u/Sdi