公共 Wi-Fi 安全使用小贴士

坏人可以在网上利用您。如果您需要使用公共 Wi-Fi，请阅读下面的一些建议。

为了应对冠状病毒的爆发以及企业和图书馆的关闭，我们中的许多人正在花更多的时间上网。因此我们可能需要使用公共 Wi-Fi 来连接互联网。如果您确实需要使用公共 Wi-Fi，请考虑州 Chief Privacy Officer（首席隐私办公室） 的以下建议以帮助保护您的数据：

1. 确认您有正确的网络。

请确保连接到正确的网络。坏人可能会创建一个基于他们的名字看起来无害的网络，但实际上是在引导你连接一个网络设置来查看您的上网情况。这意味着如果您输入登录凭证或密码进入网站，黑客将能够窃取您的信息。为了防止此类情况发生，请仔细查看网络名称，如果可能请询问员工或检查企业标识以确保网络合法。

诸如大家熟悉的咖啡馆等众所周知的网络很少受怀疑，因为该公司是将网络作为一种服务与他们的业务一起运营。已知的网络通常比可能在公共场所出现在您手机上的随机免费 Wi-Fi 网络更安全。

2. 关闭自动连接。

许多设备（智能手机、笔记本电脑和平板电脑）都有自动连接设置。此设置允许您的设备方便地连接到附近的网络。这对于受信任的网络是可以的，但它也可能将您的设备连接到可能不安全的网络。您可以通过设备上的“设置”功能禁用此功能。保持关闭这些设置，特别是当您要去不熟悉的地方旅行时。作为额外的预防措施，您可以在使用公共 Wi-Fi 后勾选“忘记网络”。

在公共场所，您也应该监视您的 Bluetooth（蓝牙）。Bluetooth 连接允许各种设备相互通信，黑客可以寻找开放的 Bluetooth 信号来访问您的设备。当您在一个不熟悉的地方时，保持关闭手机和其他设备上的此功能。

3. 关闭分享。

确保连接公共 Wi-Fi 时关闭文件共享选项。根据您的操作系统，您可以从 “系统首选项” 或 “控制面板” 关闭文件共享。例如您需要关闭共享文件功能 AirDrop。有些操作系统，如 Windows/PC，在第一次连接到新的公共网络时会通过选择 “公共” 选项来关闭文件共享。

关闭文件共享的步骤

在 PC 上：

1. 转至 “网络” 和 “共享中心”。
2. 更改高级共享设置。
3. 关闭文件和打印机共享。

在 Macs 上：

1. 转至 “系统首选项”。
2. 选择 “共享”。
3. 取消选择所有。
4. 在“查找器”中点击 AirDrop，选择 允许我被：没有人发现。

在 iOS 上，只需在 “控制中心” 找到 AirDrop 并将其关闭。

4. 使用 VPN。

考虑在设备上安装 VPN（虚拟专用网络）VPN 是公共 Wi-Fi 上最安全的数字隐私选项。当您的数据进出您的设备时会被加密，并充当一个保护性的 “隧道”，这样您的数据在通过网络时就不可见了。

5. FBI 有关加密网站的警告 – HTTPS。

FBI 对地址以 “https.” 开头的网站发出警告。“https” 和锁图标的出现应该表明网页流量是加密的，访问者可以安全地共享数据。然而网络犯罪分子现在依靠公众的信任，诱使人们进入恶意网站，这些网站包含 https，并在不安全的情况下显得安全。

FBI 的建议：

- 不切勿简单地相信电子邮件上的名字：质疑电子邮件内容的意图。
- 如果收到来自已知联系人的带有链接的可疑电子邮件，请致电或发送电子邮件给该联系人以确认该邮件是合法的。不要直接回复可疑电子邮件。
- 检查链接中是否有拼写错误或错误的域（例如，如果一个应该以 “.gov” 结尾的地址以 “.com” 结尾）。
- 切勿仅仅因为某个网站在浏览器地址栏中有锁定图标或 “https” 就信任它。

6. 不建议访问敏感信息。

即使您有一个 VPN，仍然不建议访问个人银行帐户，或类似敏感的个人数据，如在不安全的公共网络上的社会安全号码。即使是公共安全网络也可能存在风险。如果您必须通过公共 Wi-Fi 访问这些帐户，请基于您的最佳判断。对于金融交易来说，使用您的智能手机的热点功能可能会更好。

7. 安全型与不安全型。

公共 Wi-Fi 网络基本上有两种情况：安全型与不安全型。

尽可能连接到安全的公共网络。不需要任何类型的安全功能（如密码或登录）就可以连接到不安全的网络。安全的网络通常要求用户在连接到网络之前同意条款和条件，注册帐户或键入密码。

8. 保持启用防火墙

如果您使用的是笔记本电脑，请在使用公共 Wi-Fi 时保持防火墙启用。防火墙充当屏障，保护您的设备免受恶意软件的威胁。用户可能会因为弹出窗口和通知而禁用 Windows 防火墙，然后忘记将其启用。如果你想在 PC 上重启它，则转至“控制面板”，“系统和安全”，选择“Windows 防火墙”。如果您是 Mac 用户，转至“系统首选项”，选择“安全和隐私”，然后启用“防火墙”项。

9. 使用防毒软件。

还要确保在您的笔记本电脑上安装最新版本的防病毒程序。防病毒程序可以在您使用公共 Wi-Fi 时帮助保护您的系统，检测可能通过公共网络进入您的系统的恶意软件。如果已知的病毒被加载到您的设备上，或者有任何可疑的活动、攻击，或者恶意软件进入您的系统，将有警报提示您。

10. 使用双重或多充身份验证。

使用您的个人信息登录网站时使用多重身份验证（MFA）。这意味着您有了第二个验证码（发短信给您的手机，或者通过应用程序或物理密钥提供）以进一步保护您的信息安全。因此即使黑客得到了您的用户名和密码，他们也不能在没有身份验证码的情况下访问您的帐户。

11. 跟踪您的个人设备。

切勿 将笔记本电脑、平板电脑或智能手机无人看管地放在公共场所或车辆中。即使您在 Wi-Fi 网络上采取了预防措施，也不能阻止有人偷走您的财产或偷看您的信息。注意您周围的环境，留心您周围的人。

12. 其它网络安全小贴士。

以下是一些保持上网安全的小贴士，特别是当你使用公共 Wi-Fi 连接时：

- 使用强密码。
- 加密您的设备。
- 谨防钓鱼电子邮件。
- 留意您在社交媒体上发布的内容。太多的个人细节可以帮助黑客猜测密码。

- 删除您不再需要的历史信息。
- 如果网络询问您安装任何额外的软件或浏览器扩展，切勿连接。
- 确保您的设备上安装了最新的补丁和软件更新以预防已知的问题。