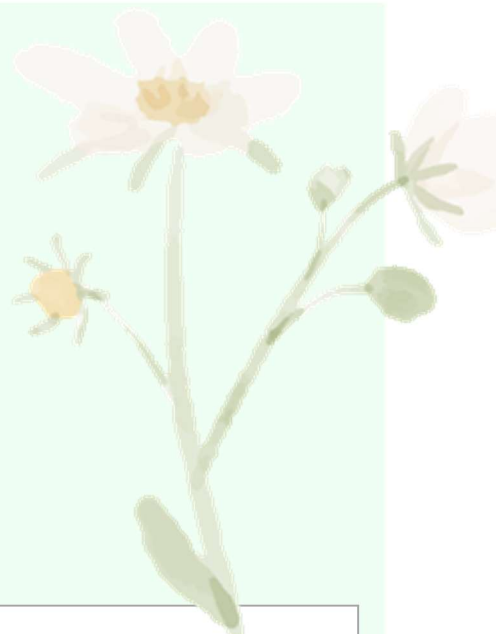


你连的 WiFi 安全吗？ | 关于校园网络安全，这些你应该知道

网络技术进步神速
在享受其便捷的同时
也应防范潜在的危险
有关网络安全
小伙伴们知道多少呢
大家一起来学习吧



背景

无线网络作为师生办公、学习的基础设施，在办公、学习场景中起着不可替代的作用，但是，日常生活中大家连接的 WiFi 真的安全吗？针对常见的网络安全问题，信息中心整理了以下常见的[网络安全问题及应对建议](#)，希望能更好地帮助大家安全使用网络。

具体情境

情境 1: 免费 WiFi 接入

不法分子搭建与用户常连接的 WiFi 热点[名称相同或相近](#)的 WiFi，设置[空密码或相同的密码](#)吸引公众连接，然后在 Wi-Fi 路由器上劫持 DNS（域名系统），将用户[引入到钓鱼网站获取用户的账号密码](#)，或者在路由器上[监听手机流量，获取明文密码](#)。部分手机在搜索到不是同一个 WiFi 热点但名称相同的 WiFi 时，也会自动使用保存的密码连接。



对应建议：

- 1.公共场合连接 WiFi 时请与提供 WiFi 的商家**确认好 Wi-Fi 的热点名称**；
- 2.**没有密码**的公共 WiFi 慎用，特别是**命名奇怪**的无线网络；
- 3.**使用支付 APP** 时尽量使用运营商的 **4G/5G 网络**；
- 4.不使用 WiFi 时关闭手机和笔记本电脑的无线局域网功能。

情境 2:私设 WiFi 路由器

根据《广州中医药大学网络安全管理办法》第十二条“**任何单位及个人不得擅自建设、更改、损毁和挪用校园网设施**”，私自增设路由器可能会破坏校园网络的整体布局，降低网络稳定性，影响其他师生的网络体验，如果**配置不当会导致信息泄露，网络攻击等安全隐患**，后果不堪设想。



对应建议：

- 1.不要在校内私自架设无线路由器；
- 2.对校园无线网**有特殊需求的部门**，可向信息中心**提出申请**，经中心评估后，根据实际情况进行部署。

情境 3:手机共享个人热点



打开个人热点后的设备将成为 WiFi 接入点，其他设备可以连接到该设备的网络。这可能会为黑客或恶意软件提供访问该设备和数据的途

径。**连接到热点的人可以访问该设备浏览的网站、发送的消息和下载的文件。**如果该设备上包含敏感信息，则可能会造成数据泄露。

对应建议：

- 1.仅在**需要使用个人热点时才将其打开**，并在**完成后立即将其关闭**；
- 2.**使用强密码**，确保热点密码安全且难以破解；
- 3.**限制连接设备**，仅允许受信任的设备连接热点，并**定期检查连接的设备列表**；
- 4.**定期检查可疑活动**，注意设备上或连接设备上的任何可疑活动，并采取相应措施。

WiFi 安全口诀

公共场合连 WiFi，名称一定要确认
无密 WiFi 不要连，安全支付用 5G（4G）
私搭路由不可取，安全设置莫忘记
WiFi 不用要关闭，万能钥匙请回避

网络安全建议

寒假马上到来，小伙伴们在享受寒假生活的同时，也要注意网络安全哦。下面是一些针对网络安全的温馨提示：

- 1.**保护个人信息**，谨慎分享；
- 2.**不要随意添加陌生人为好友**，以免给自己带来不必要的麻烦和危险；
- 3.识别网络谣言，**不造谣不信谣不传谣**；
- 4.**合理安排时间**，远离沉迷，多参加户外活动和体育锻炼，保持身心健康；
- 5.**不要随意点击不明链接或下载来历不明的软件**，警惕网络诈骗，守护财产安全；
- 6.尊重他人隐私，**文明上网**。

网络技术在发展
不法分子也并非原地踏步
小伙伴们要时刻保持警惕
文明上网的同时
保护好自己的个人隐私
寒假将至
预祝小伙伴们
假期快乐