**2018国家网络安全宣传周系列动漫① WiFi安全篇**

如今，随着移动终端的兴起和互联网技术的不断进步，那些古老的盗窃、诈骗、骚扰手段也换了新颜。不知道大家有没有意识到，大家每天使用的WiFi，其实并不安全。

是的，你没看错，使用WiFi上网时，我们的个人信息安全或许面临着巨大的风险。

比如，黑客自己搭建一个“山寨WiFi”，取一个与附近WiFi相似的名字，不设登录密码诱导人们连接。使用时，传输的数据就会被黑客监控，个人隐私、账号名和密码等信息，也可以轻易被盗取。其实，不仅是蹭WiFi，不少人还喜欢随时开着手机无线网自动连接功能，这样风险就更大了。

不信？看看下面这几幅漫画，这些危险场景，或许你都曾经置身其中。

* **免费WiFi接入**

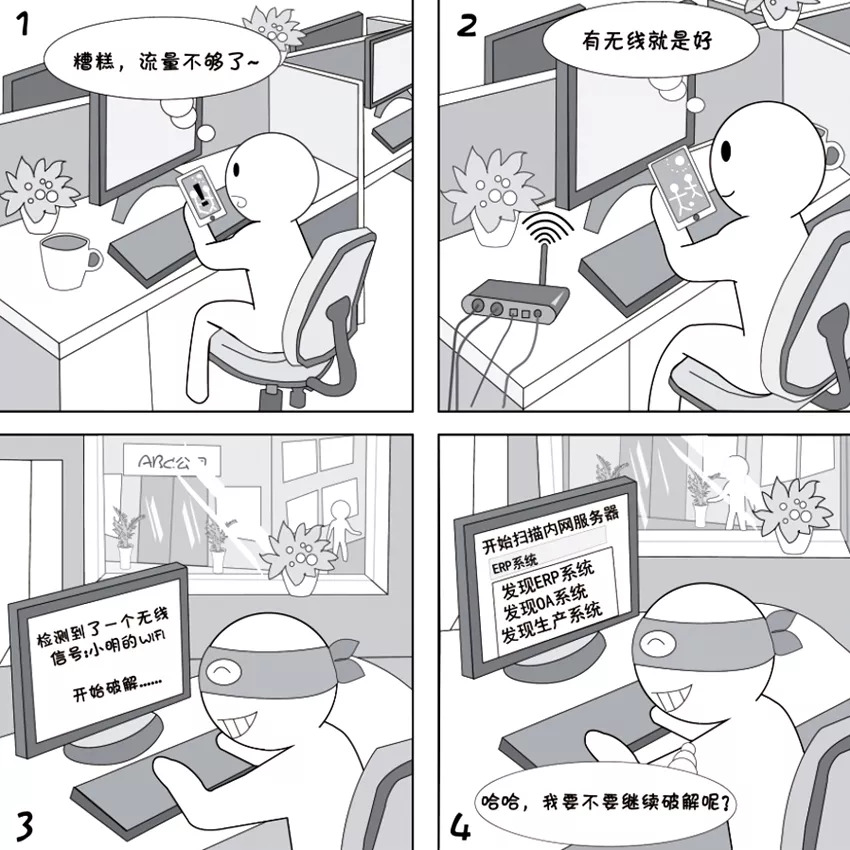


【危险】

不法分子搭建与常用WiFi相同或相近的WiFi，设置空密码或者相同密码吸引公众连接，然后在WiFi路由器上劫持DNS(域名系统)，将用户引入到钓鱼网站获取

【提示】

* 公共场合连接WiFi时请同商家确认好WiFi名称
* 没有密码的公共WiFi慎用
* 使用支付APP时，尽量使用运营商的4G网络
* **私搭WiFi热点**



**【危险】**

无线路由器有较多的安全隐患，比如，之前的WEP认证能很轻易破解。个人架设无线路由器，如果配备不当会导致蹭网或个人资料泄露，在公司使用可能导

**【提示】**

* 在办公网络架设无线路由器必须经过公司批准并进行安全安装
* 认证方式使用安全的WPA2
* 建议隐藏SSID(服务集标识)，绑定接入设备的MAC地址
* WiFi密码必须八位数以上，包含大小写、数字和标点符号，定期修改密码
* **WiFi自动连接**

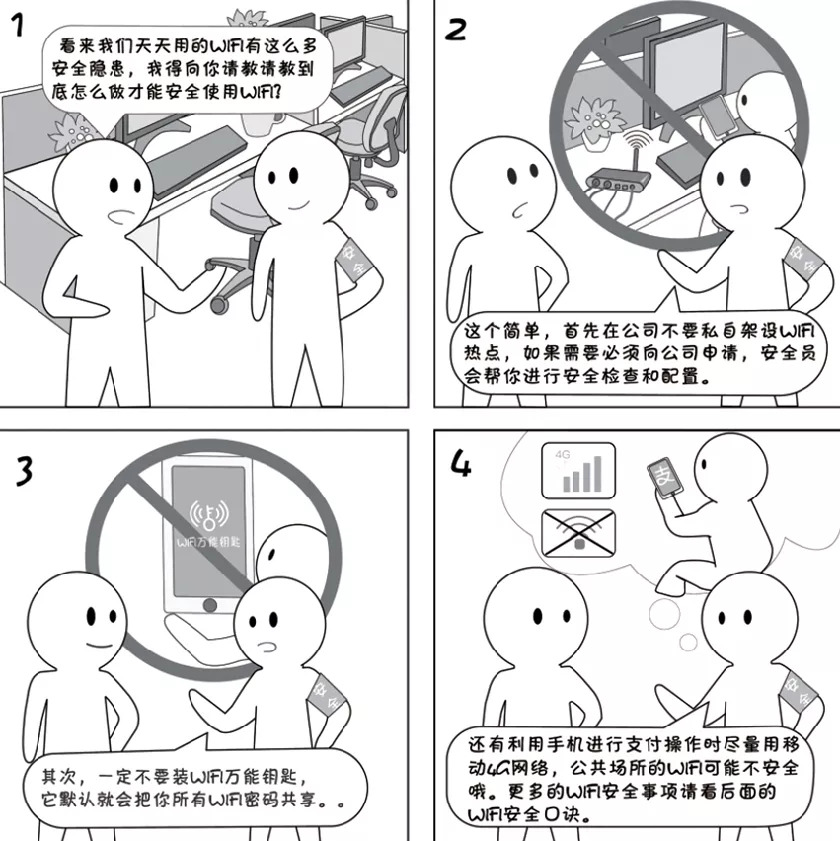


**【危险】**

一些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，这就给黑客以可乘之机。

**【提示】**

* 日常不用WiFi时关闭手机和笔记本电脑的无线局域网功能，以防自动连接恶意WiFi
* 当手机和笔记本连上WiFi后，留意连接到的WiFi热点名称
* **WiFi安全总结**



**<WiFi安全口诀>**

公共场合接WiFi，名称一定确认好

无密WiFi不要连，安全支付用4G

私搭路由要审批，安全设置莫忘记

WiFi不用要关闭，万能钥匙请回避

**【后记】**

万物互联时代，蹭WiFi似乎成为了一项基本“生存技能”，但在享受WiFi带来便利的同时，由于人们普遍缺乏WiFi上网的安全防范意识，逐渐成了各种网络陷阱、钓鱼诈骗的重灾区。WiFi风险主要有两种形式：一是正常WiFi被不法分子入侵，二是不法分子建设假冒可信热点。

为防范这些安全问题，无线网都需要增加基本安全认证和加密功能。包括：

* 1、用户身份认证，防止未经授权访问网络资源；
* 2、数据加密以保护数据完整性和数据传输私密性；
* 3、平时使用要注意固件升级，有漏洞的无线路由器一定要及时打补丁；
* 4、手机端、电脑端都应安装安全软件。