瑞报实验室

网传“没有密码的Wi-Fi不要随便连接，否则个人隐私会被泄露”，记者通过实验证实，在公共场所随意连接来源不明的Wi-Fi确实存在较大风险，而使用运营商4G网络更安全。

手机蹭网有风险需谨慎

《瑞报实验室》证实：公共Wi-Fi看似馅饼实则陷阱 用4G网络更安全

■记者 欧苗苗

“本景区Wi-Fi已开通”“本店无线已覆盖”“免费无线上网”……在很多公共场所的醒目位置都会贴着这样的标志，然而近期一则“在公共场所，没有密码的Wi-Fi不要随便连接，不然小心个人隐私被泄露”的警示信息在网上热传，并引起网友们的热烈讨论。那么，在公共场所连接来源不明的Wi-Fi网络是不是真的存在安全隐患？

为了验证该传言是否真实，日前，记者邀请我市一家电子信息技术有限公司的安全顾问褚核，分别在市区车站、餐馆、景点等人员密集的场所进行了实地测试。测试结果显示：在公共场所随意连接来源不明的Wi-Fi确实存在较大风险，而使用运营商4G网络更安全。

[调查] 公共场所无线Wi-Fi受市民青睐

“现在开店，没有Wi-Fi根本不行，要聚集人气，一定要有Wi-Fi，而且Wi-Fi能给我们省很多事。”市区某餐饮店的工作人员一边为给记者点菜一边说，以前顾客总是催着点菜、上菜，有时候，服务员稍慢一点，不少顾客还会生气，甚至起身走掉。但自从开了Wi-Fi后，点菜期间，顾客就会上网玩手机，催菜的顾客明显少了许多。

对于公共场所开通免费Wi-Fi一事，市民张海洋表示双手赞成。他笑着说：“免费Wi-Fi简直是男士的福音，就拿我来说吧，陪女朋友逛街买衣服实在是件头疼的事，陪着吧，自己不爱逛街；不陪吧，对方要生气。但有了Wi-Fi后，她在商店挑选衣服，我就在店里用Wi-Fi玩手机、打游戏，自娱自乐。”

“在用公共场所提供的免费Wi-Fi时，你们有没有考虑过安全性？”记者随机采访了20位市民，有九成表示没有考虑过。“有可以连接的免费Wi-Fi，我都会连接，没有考虑其安全性。”市民王小姐接受记者采访时说。

很多市民和王小姐有着同样想法。市民张先生也是手机不离手的人，到哪儿都问有没有Wi-Fi，他说：“有Wi-Fi用就可以了，哪还考虑那么多。”

[实验] 公共场所的无线Wi-Fi能轻易‘截获’个人信息

为验证公共场所无线Wi-Fi所欢迎程度，上周六傍晚，记者和褚核来到瑞安广场测试。由于是周末，瑞安广场上的人比平时多了很多。褚核在广场边缘的椅子上坐下，从包里掏出了一台笔记本电脑、一个无线路由器、一张上网卡，以及几台手机，开始测试。

几分钟之后，褚核就建起了一个名叫“kanrui”的无线网络，但没有设置密码。“我在这台手机上安装了一个软件，可以实时监测到有哪些人加入到我的Wi-Fi网络。”褚核说，从“kanrui”开通之后仅仅15分钟之内，很快就有约20个人加了进来，“大家已经习惯了，看到免费Wi-Fi，大多会在第一时间去加，甚至有的手机还设置了自动加入没有密码的Wi-Fi，很少有手机用户愿意去辨别这个Wi-Fi网络是否安全。”褚核说。

那么，加入这个Wi-Fi网络的用户隐私信息是如何泄露的呢？“简单来说，通过我手机和电脑上的软件，一个手机用户在连接我的Wi-Fi后，他在网上的所有行为，我都能看得到。”褚核告诉记者。

随后，褚核做了现场演示。他从围观的市民中随机拿了一台苹果6手机，连接到他搭建的名为“kanrui”的Wi-Fi网络中。手机很快上网。

随后，褚核请该市民用手机查看私密照片。很快，这位游客在手机上看过的照片全部在褚核的电脑上显示，个人隐私一览无遗。惊得该市民连连说：“以后再也不会链接没有密码的Wi-Fi了。”

“照片泄露只是一个方面。”褚核说，如果在连接有“陷阱”的Wi-Fi时，无论苹果手机或安卓手机登录了邮箱，或者其他需要输入密码的各种账号，那么用户名和密码都有可能被黑客全部窃取，然后被黑客随意更改。尤其是一些涉及资金交易的账户通过不安全的Wi-Fi网络被黑客窃取的话，将给用户带来不可估量的财产损失。

随后，褚核还分别在瑞安客运中心、公园等人员密集区域进行了测试。对于测试结果，褚核表示非常吃惊：“大部分手机用户对于Wi-Fi安全性的意识非常淡薄，为了省流量，他们都会主动寻找各种免费的Wi-Fi网络，尤其是不设密码的Wi-Fi网络最受欢迎，这种行为相当危险。”褚核说。

[结论] 公共场所上网 用4G网络更安全

随着智能手机的快速普及，以及伴随着移动互联网而来的各种新应用层出不穷，越来越多的人习惯在手机上完成各种事务，甚至衣食住行都可以用一台手机来解决。也正因如此，手机网络的安全性也变得越来越重要。而因为手机使用不当而引发的银行卡被盗刷等新闻近年来也常常见诸报端。尽管如此，仍有很多手机用户没有意识到，自己常常使用的各种免费Wi-Fi是个人信息泄露的“源头”。

“事实上，除了未加密的Wi-Fi网络，如果黑客有心要窃取你的信息，那么在公共场所即使连接有密码的Wi-Fi，也同样是存在安全隐患。”褚核说。

对此，温州金蚂蚁科技网络有限公司工程师冯硕表示，在公共场所需要上网，一定要有安全意识，不要使用不熟悉的无线Wi-Fi，尤其是在网上操作一些关键信息时，最安全的方式还是直接连接运营商提供的4G网络。“因为运营商对其网络采取了严格的加密措施，很难被黑客破解，所以安全性更高，不要因为节省流量而造成不必要的损失。”冯硕说。

[小贴士] 手机用户 该如何保护自己的隐私？

冯硕建议，用户不要链接不用密码的WiFi网络，转而多使用有密码的WiFi网络以及多用移动数据网络。如何能够更安全地使用免费Wi-Fi，可以注意以下几个方面：

拒绝来源不明的Wi-Fi

设置钓鱼WiFi陷阱的黑客大多利用的是用户想要免费蹭网的占便宜心理。因此要想避免堕入类似陷阱，首先要做到的就是尽量不要使用来源不明的WiFi，尤其是免费又不需密码的WiFi。

关闭Wi-Fi自动连接功能

用户在日常使用电子设备时最好关闭“WiFi自动连接”功能。因为如果这项功能打开的话，手机在进入有WiFi网络的区域就会自动扫描并连接上不设密码的WiFi网络，这会大大增加用户误连钓鱼Wi-Fi的几率。

另外，用户在使用智能手机登录手机银行或者支付宝、财付通等金融服务类网站时，最好使用手机自带的3G、4G网络，另外最好不要直接通过手机浏览器进行，请优先考虑使用银行或者第三方支付公司推出的专用应用程序，这些程序的安全性要比开放的手机浏览器高不少。

及时更新升级浏览器

和传统有线网络相比，Wi-Fi网络环境下，用户信息的安全性挑战更多。用户在使用非加密的WiFi网络或者陌生的WiFi网络时，最好提前在笔记本电脑或智能手机中安装一些安全防范软件以作提防。

更换路由器初始密码

除了要谨慎使用公共场所的免费Wi-Fi，家里使用的路由器管理后台的用户名、密码，不要使用默认的admin，密码最好更改为数字+字母的高强度密码，同时设置的WiFi密码选择WPA2加密认证方式，相对复杂的密码可大大提高黑客破解难度。

求证新闻