

免费WiFi有“鬼” 手机“裸奔”易受攻击

　　随着WiFi网络和移动支付的普及，每到一地必连WiFi已成了许多手机用户的使用习惯，不过，这些随手可连的免费公共WiFi真的安全吗？当你在手机上购物、炒股、收发邮件、银行转账时，你有意识到，你的账号密码会有被盗取的风险吗？  
　　日前，记者跟随杭州安恒信息技术有限公司的资深安全顾问范毅，走入锦里、新南门客车站等人群密集地，现场演示公共WiFi如何让手机裸奔以及如何更好地进行自我防护。  
  
**电脑+路由器3分钟搭建免费WiFi环境**

　　演示之前，范毅只准备了一台笔记本电脑和一个常见的路由器。首先将电脑连接互联网，然后将电脑与路由器连接，再通过笔记本电脑的网络分享制造出一个无密码的免费WiFi环境，手机用户可以自由连接。  
　　记者看到，整个准备过程非常简单，不到3分钟，演示环境已设置完成。  
  
**保护意识太弱20台设备接上免费WiFi**　　很快，范毅的电脑屏幕上出现了一些用户名，他解释说，这些是已经连接上WiFi的手机、电脑名称。接着，越来越多的移动终端设备连接上了WiFi设备。记者数了数，短短10分钟，已经有7台手机和电脑连接上范毅设置的免费WiFi。范毅说，这7台手机和电脑，他都可以任意入侵。  
　　事实上，在整个实验过程中，先后有20台设备接入到这个免费WiFi中，“这说明用户的自我保护意识还非常弱。”  
  
**现场演示“黑客”轻松盗取账号密码**

　　**演示1：**几分钟实现“中间人攻击”  
　　第一个演示叫“中间人攻击”。范毅说，“黑客和一个普通网民连入的是同一个WiFi，普通网民进行一个上网的操作，例如逛个人微博，上QQ、QQ空间，黑客都可以监听到，可以看出对方在做什么，也可以很方便地查看对方的隐私。”  
　　范毅向记者模拟了用户遭遇黑客攻击的全过程。首先记者用手机打开QQ空间，范毅打开黑客攻击软件后，记者的手机IP地址被扫描发现。“选择这个需要‘劫持’的设备，然后会话‘劫持’，再点击‘开始’，这个攻击软件就已经对对方的手机进行一个‘劫持’攻击了。”范毅边演示边介绍。不到3分钟，黑客软件成功检测到记者使用手机所浏览网页的全部记录。虽然记者的QQ空间里私密相册设置了浏览权限，却还是被偷窥到了，范毅的手机中实时显示出记者QQ空间内的照片。不仅如此，范毅说，如果愿意，他甚至可以让记者手机上植入任意他想显示的图片。  
　　接着，记者登录百度网站，并输入百度账号和密码，结果，账号和密码全部出现在范毅笔记本电脑的软件中。范毅介绍，此时一般黑客就会将记者“踢”出网络，代替记者在网络上进行操作。“当你的账号转载和发布了你并不知晓的议论和图片时，你的电脑就被黑客攻击了。”  
  
　　**演示2：**几分钟植入木马盗取密码  
　　银行卡在未离身的情况下，还是被盗刷，这种情况黑客是如何实现的呢？范毅向记者介绍，除专门设置钓鱼WiFi外，还有2种方式就能实现。  
　　第一种方式，是通过向用户手机植入木马，即当用户和黑客同属于同一WiFi状态下，黑客向用户实施了“中间人攻击”后，就能向用户手机发放任意链接、数据包，从而轻松向用户手机植入木马。这种情况用户是无法察觉的；第二种方式，是采用“钓鱼网站”方式，黑客可以用软件设计一个假想的“钓鱼网站”，几分钟就能获取记者的账号和密码。专家表示，一般的黑客会设计出与银行、购物等网站相同的界面，用户登录该界面时很难察觉，一旦使用支付功能，银行卡内的钱就会神不知鬼不觉地跳转至黑客的账户。  
  
**消费提醒：通信运营商的网络安全性最高**　　免费WiFi有风险，那么如何保护自己隐私的安全呢？记者电话采访了上海贝尔杰出工程师卢振陶。  
　　据卢振陶介绍，首先要尽量不使用不明来源的WiFi，尤其是不需要密码的开放式WiFi。如果使用商家提供的免费WiFi网络，最好主动向商家询问wifi的具体名称，以免不小心连接黑客搭建的钓鱼WiFi。二是开启防火墙、安全软件和禁用网络发现等功能，防止其他人利用公共网络对个人设备进行非法访问。三是最好关闭WiFi自动连接的功能。

　　另外，卢振陶强调，不要轻易在WiFi网络环境下进行支付等敏感信息操作，如果需要支付，最好是使用运营商提供的4G等安全网络进行支付操作。“其实，现在随着运营商大力推动的4G网络建设，在公共场合已经能够提供较快的4G网络服务，”卢振陶介绍，“4G网络能够提供更高的上网安全保障。”  
　　如果在4G信号覆盖情况不好，或要使用较大的数据流量，如视频或音频的访问，需要使用WiFi网络时，也要尽量选择相对安全的网络，如运营商提供的公共无线网络。运营商的4G网络和无线网络使用了安全性较好的认证方式和加密手段，攻击者不容易进入这样的网络进行监听或注入攻击，从而为用户的安全提供了较好的防护。