免费蹭WiFi 小心被黑

- 只要是遭遇钓鱼WiFi,用户上网过程中个人信息和密码就都有可能被别有用心的黑客获取
- 一想到有可能连网银的账号和密码都泄露，就不敢再用，在专业人士眼中,这种担忧有些过虑
- 造成用户信息泄露并非WiFi设备惹祸,而是用户贪便宜的心理和浏览器网络传输协议有漏洞
- 普通商家自行搭建的WiFi热点大多使用民用级设备,有的甚至连密码都没有,给黑客留下机会

坐在星巴克的落地窗边,杜瑞强没有如常打开iPhone的WiFi开关,虽然每天下午来星巴克喝杯咖啡、顺便蹭蹭网早已成为他的习惯。但就像窗外广州阴霾的天气一样,此时他的心情正在为天涯论坛上一篇网帖而备感纠结。

这篇名为《有图有真相,你还敢用UC上网吗?》的帖子说,“在星巴克、麦当劳,黑客只要用一台笔记本、一套无线热点和一个叫做Wireshark的软件，最少只要15分钟,就能获取通过临时无线网络上网者的账号和密码。”

“虽然不知是真是假，但是听起来真有点恐怖。”杜瑞强担忧地说。

有着同样忧虑的不止杜瑞强一人，自从上述网帖发布后,网络上关于使用公共场所免费WiFi上网究竟是否安全的讨论激增。公共免费WiFi,上还是不上,一串串有关安全的追问随之而来。

□据《南方日报》

制图 李荣荣

疑问1 钓鱼WiFi窃取用户密码?

从技术角度来说,只要使用免费WiFi上网,手机或者电脑都有可能被钓鱼

在那篇网帖中,名为“妖妃娘娘”的楼主详细演示了如何用“Win7系统电脑、无线热点和Wireshark软件”窃取使用UC浏览器用户个人信息和密码的全过程。

“妖妃娘娘”称,按照该教程,即使是初级黑客也只需要两个小时,就能掌握如何在公共场所设置免费WiFi来进行钓鱼，熟练后甚至仅需15分钟就能够轻松搞定使用UC浏览器上网用户的密码。而这其中的关键在于,UC浏览器本身存在安全漏洞,其所谓的“云加速”服务在传输用户信息时使用了明文传输密码,让泄密成为了可能。

对于这份“钓鱼WiFi”的详细教程，很快就有热心网友进行了亲身验证，结果证明在iPhone上使用版本号为8.2.1.132的UC浏览器，果真可以通过Wireshark软件截取到登录Gmail账户时输入的账号和密码信息。然而,这还不是让公共WiFi安全性问题被彻底引爆的关键,在“妖妃娘娘”的网帖和随后网友实证帖被广泛传开后,有关“钓鱼WiFi”窃取他人信息和密码的强大能力被越传越神,“网银密码也能轻松搞定”等说法更是引起了众多网友的强烈不安。

作为UC浏览器开发厂商——UC优视公司对于这个问题并没有太多回避。该公司CEO俞永福直承,在前期某个版本的iPhone用UC浏览器上的确存在漏洞，但很快就推出了新版本的软件加以改进。不过他同时也表示,只要是遭遇“钓鱼WiFi”,用户上网过程中个人信息和密码就都有可能被别有用心的黑客获取,并非只有使用UC浏览器的用户才会有这个风险。“最大的问题其实是在我们目前网站建设上普遍采用的HTTP(超文本传输)协议本身的安全性较低。”俞永福的说法获得了金山网络安全专家李铁军的支持。

李铁军称,从技术角度来说“妖妃娘娘”介绍的钓鱼方法是可行的,只要使用免费WiFi上网，手机或者电脑都有可能被钓鱼。李铁军进一步解释，如果用户使用黑客设置的钓鱼WiFi上网，那么黑客使用相关软件监视并记录用户在网上进行的所有操作信息，从中窃取有价值资料,比如QQ聊天记录、邮件内容等,“获取网银账户密码的可能性较小,但也并不是完全没有可能”。

疑问2 用户资料泄露漏洞在哪?

WiFi设备并没有出现安全方面的问题，是人们怎样使用WiFi上出了问题

虽然专家证明“钓鱼WiFi”的确有可能导致用户的个人信息泄露,但这究竟是WiFi网络本身的问题还是其他方面的因素导致，这种泄露的后果究竟又会有多严重呢?

贝尔金公司技术工程师梁汉明认为,钓鱼WiFi引发的公共场所WiFi的安全性问题和WiFi本身的安全性问题，在本质上是两回事,前者更多的是人的问题,后者则只是较为单纯的设备问题。

“首先我们需要承认WiFi设备是有一定技术漏洞，这种情况在各种高科技产品和服务中都存在,就像Windows系统市场多次爆出安全漏洞，美国五角大楼也曾经被黑客攻破一样，网络设备和服务安全性虽然一直都在提升中,但谁也不敢保证万无一失。”梁汉明说,2011年WiFi设备就曾经爆出过WPS（WiFi保护设置）协议的漏洞，黑客只要用密码穷举法（使用计算能力强大的设备将所有有可能性的密码排列组合都尝试一遍)暴力破解,能够攻破WiFi设备的安全防护。“但这样做不仅需要专业的设备，还需要精通相关安全协议的知识，并非一般黑客能做到的,即使能做到,也往往要花上几天的时间。”

但钓鱼WiFi的情况显然完全不同,“妖妃娘娘”称最短只需要15分钟就能搞定用户的账号和密码。“这是因为其本身就是设置了一个人为的陷阱，其攻克的本来就不是WiFi设备的安全防护,而是网络浏览器的软件漏洞，或者说是网络传输协议的漏洞。”梁汉明解释道,“在这件事上WiFi设备并没有出现安全方面的问题,是人们怎样使用WiFi上出了问题。”

不过无论是哪个环节出了问题,遭遇钓鱼WiFi有可能导致用户信息泄露的风险却是真实存在,仅这一点,就足够让杜瑞强这样的网络用户忧心忡忡:“一想到有可能连网银的账号和密码都泄露,就不敢再用了！”但在专业人士眼中,这种担忧显得有些过虑。

广东发展银行陈捷表示,目前绝大部分网络银行都已经在页面上加入了安全控件的技术,而且登录页面也多是采用了HTTPS（超文本传输安全协议）技术，在终端和服务器之间进行数据传输时采用的是密文形式,使用WireShark之类的软件是无法截取的。

支付宝公司朱建称，目前网络第三方支付账户的登录和使用也大多采用手机账号绑定或者数字证书认证等技术，即使黑客通过“钓鱼WiFi”获得了账户和密码，在没有相关数字证书和绑定账号的手机短信认证的情况下,也是无法对账户资金进行调动的。

疑问3 免费公共WiFi还能用吗?

不少运营商都提供免费WiFi，市民在公共场所最好选择运营商提供的WiFi

钓鱼WiFi被曝光后,在引发人们对WiFi安全性再检讨的同时，也让不少人对于是否应该继续在公共场所接入WiFi网络产生了怀疑。

媒体人士潘少文平日经常在机场、酒店等公共场所利用免费WiFi工作,现在正考虑买一个3G上网卡。潘少文的顾虑并非杞人忧天。专门为中国移动提供WiFi设备专业建设和维护服务工作的夏侯宇表示，目前公共场所的WiFi主要分为两种,一种是有电信运营商提供的WiFi热点,另一种则是商家为招徕客户自行搭建的WiFi。

“这两种WiFi在技术上是有着很大差距的。运营商提供的公共WiFi网络无论是否免费,都是采用电信运营级的网络设备,性能稳定。运营商在WiFi组网时都会部署多种安全措施，例如连接上WiFi后要想上网还需要通过身份认证、或是要求使用专用的客户端软件等,在后台服务器端,运营商往往还会提供24小时的监控。”

夏侯宇称，普通商家自行搭建的WiFi热点则大多使用民用级WiFi设备,“其实就是家庭用户的普通无线路由器，而且后台也没有进行专门的安全性设置,有的甚至连密码都没有，这就给黑客留下了乘虚而入的机会。”

作为行业人士，夏侯宇个人建议，市民在公共场所最好优先选择运营商提供的WiFi。“目前不少运营商都针对其自身的用户提供免费的WiFi使用时长,充分利用这种优惠可以让用户在省钱的前提下享受到安全性更有保障的WiFi服务。”

名词解释

WiFi

WiFi是一种短程无线传输技术,能够在数百英尺范围内支持互联网接入的无线电信号。随着技术的发展，以及IEEE802.11a、802.11b、802.11g以及802.11n等标准的出现,现在IEEE802.11这个标准已被统称作WiFi。

如何防范钓鱼WiFi

天涯网帖的火爆传播,让钓鱼WiFi臭名远扬，也让不少对于技术不太精通的用户闻之生畏。有关专家指出，只要用户增强主动防范意识，并建立良好的WiFi使用习惯，就能够防止堕入钓鱼WiFi的陷阱。要想做到这一点,有些小技巧可以利用。

第1招 拒绝来源不明的WiFi

正如“妖妃娘娘”所披露的那样，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。如果是在星巴克、麦当劳这样有商家提供免费WiFi网络的地方，用户也要多留一个心眼,主动向商家询问其提供的WiFi的具体名称，以免在选择WiFi热点接入时不小心连接到黑客搭建的名称类似的钓鱼WiFi。

第2招 及时更新升级浏览器

和传统有线网络相比,WiFi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。

针对最容易泄露用户信息的浏览器软件,用户除了要在官方网站进行下载和安装之外,还要养成定时更新升级的好习惯。例如此前提到的UC浏览器，其最新的版本就加入了连接到无密码的WiFi网络自动提醒用户是否要断开的功能,这种功能升级对于用户防范钓鱼WiFi无疑会起到比较实用的效果。

使用浏览器登录网站时,如果碰到需要用户输入账户名和密码并弹出“是否记住密码”选项框的情况,最好不要选择“记住密码”,因为“记住密码”功能会将用户的账号信息存储到浏览器的缓存文件夹中,无形中方便了黑客进行窃取。

第3招 手机软件设置莫偷懒

针对智能手机用户尤其需要提醒的是,在日常使用时最好关闭WiFi自动连接这项功能。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,这无疑会大大增加用户误连钓鱼WiFi的几率，为了一时方便而留下安全隐患,未免有些得不偿失。

另外,用户在使用智能手机登录手机银行或者支付宝、财付通的金融服务类网站时,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上不少。