

除了网速变慢,还有安全风险

你的私人 Wi-Fi 被共享了吗?

○记者张惠婷

近年来,共享经济对各个行业产生了重大的影响,互联网行业也不例外,以 Wi-Fi 共享为核心服务功能的 Wi-Fi 分享软件日益盛行,无论是身处普通居民小区、商业机构,还是政府机关、金融机构,打开手机中的 Wi-Fi 分享软件,无需密码就能免费蹭网。殊不知,用户在享受蹭网便利的同时,自己的 Wi-Fi 也可能不知不觉中被共享。当私人 Wi-Fi 变成公共网络,除了导致网速变慢,还将造成用户信息泄露的安全风险。

手机来浏览网页、观看视频等,流量不够用成为很多人的困扰,Wi-Fi 分享软件正是抓住人们这一心理吸引了大批用户。有了流量,就可以大量推送广告,或为商户导航。

让人细思极恐的是,支撑 Wi-Fi 分享软件提供核心服务功能的,是其所收集和掌握的用户个人信息。

腾讯 Wi-Fi 管家的用户服务协议,指出了它可能需要使用的必要信息:用户使用本机号码登录,将允许软件获取本机手机号码;为了帮用户找到附近可能存在的 Wi-Fi,软件会识别用户的地理位置;在用户启用网络测速功能时,会识别用户的网络运营商信息以及网络速度;为了实现 Wi-Fi 安全检测等功能,会识别用户所连接 Wi-Fi 的详细信息,如 IP 地址等;在用户使用 Wi-Fi 开放平台时,则需要输入 Wi-Fi 数据及密码。

可以说,在 Wi-Fi 分享软件面前,用户隐私如同“裸奔”。Wi-Fi 被共享,对用户来说,最大的问题不是流量,而是安全。

极大的安全风险

当一个训练有素的黑客面对一台已经共享 Wi-Fi 密码的路由器,他能干些什么?

有网友写了一篇在攻破隔壁女神家的路由器之后的故事。他将获取到的信息加以组合,掌握了女神的微博、微信、QQ、手机号等各种社交资料。通过数据监听和劫持,还可以用女神的微博账号发布微博,甚至远程控制女神家的电视盒子播放电影。

信息安全从业人员谢明江很早就开始关注 Wi-Fi 共享领域。他告诉记者,由于 Wi-Fi 网络的开放性和基于明文的网络协议,用户数据很容易被监听和伪造。监听的危害主要体现在隐私安全上,让所有登录过的网站、下载的文件、输入的密码暴露在黑客面前。而数据伪造的危害更可怕。“比如你登录支付宝官网,黑客可以通过技术欺骗将网页跳转到假支付宝网站,诱导你下载病毒木马,严重威胁你的财产安全。”

当然,这不全是 Wi-Fi 分享软件造成的,用户安全意识不强是主要原因。但如果没有 Wi-Fi 分享软件共享这些密码,路由器被蹭网的几率将大大降低。

多款 Wi-Fi 分享软件宣称,它们不自行创造内容,所有数据内容均由用户上传。但实际上,Wi-Fi 主人对 Wi-Fi 密码的共享行为并非完全主动。谢明江说,不少 Wi-Fi 分享软件的分享功能设置隐蔽,没有给予用户相应的选择权,也没有充分告知可能存在的风险。但凡人得知了 Wi-Fi 主人的热点密码,并通过 Wi-Fi 分享软件进行过连接,该热点就会在主人不知道的情况下被共享出去。

谢明江认为,不是说“共享 Wi-Fi”这个模式行不通,而是不能不考虑 Wi-Fi 主人的感受随意分享,可以在主人同意的情况下进行有偿共享,提升闲置 Wi-Fi 资源的使用率,这也是一种共享经济。

在多款 Wi-Fi 分享软件中,Wi-Fi 主人可以通过快捷渠道取消热点分享。但记者发现,主人热点的“被分享”远远比取消分享容易。比如取消 Wi-Fi 万能钥匙的热点分享,必须填写

热点 SSID 名称、热点密码、路由器 MAC 地址,最后提交申请等待客服审核。“许多用户连手机上的 Wi-Fi 设置都玩不转,更别提这么繁琐的技术操作了。”谢明江说。

是共享还是侵权?

Wi-Fi 共享,是方便还是侵权,在目前的法律条文中还不是特别清晰。对于被共享的用户个人信息,你认为是隐私,他认为是信息;于你而言强调保护,于他而言强调分享——这似乎是一种难以调和的矛盾。

但是,非法获取企业存储、处理和传输的 Wi-Fi 数据是有可能构成侵权的。有这样一个案例:被告人郭某与刘某开发了 Wi-Fi 万能通、Wi-Fi 万能助手两款手机 APP,但其无共享 Wi-Fi 密码数据资源,两人便通过反向编译获取了 Wi-Fi 万能钥匙数据库中的共享 Wi-Fi 热点密码数据,供自己的软件客户使用。两人被判非法获取计算机信息系统数据罪。

随着争议声日益增多,Wi-Fi 安全问题已经引起各方高度重视。今年3月底,央视做深度报道聚焦 Wi-Fi 万能钥匙带来的各种安全隐患。工信部随后在官网发布关于“蹭网”类移动应用程序的通报,要求有关单位依法对此类程序进行处理。公安部也集中约谈了境内 Wi-Fi 分享类网络应用服务企业,要求其切实加强公民个人信息保护。

迫于压力,Wi-Fi 万能钥匙等 Wi-Fi 分享软件纷纷修改部分侵权设置,完善“Wi-Fi 安全险”等功能,但由于这类软件经过长期积淀,用户群体巨大,仍不能避免地存在安全问题。

记者了解到,不仅是 Wi-Fi 分享软件,当前我国软件市场上各类软件对于用户个人信息的收集和保存,均不同程度地存在不规范行为。例如,一些地图软件自动开启记录行踪信息的功能,一些 APP 会收集与提供的服务完全无关的用户信息等。

要遏制这种乱象,网络安全建设迫在眉睫,国家已经祭出相关法律重器:首部网络安全的专门性综合性法律《中华人民共和国网络安全法》于去年6月实施,规定“网络产品、服务具有收集用户信息功能的,其提供者应当向用户明示并取得同意”。《信息安全技术个人信息安全规范》也于今年5月正式实施,规范了开展收集、保存、使用、共享、转让、公开披露等个人信息处理活动应遵循的原则和安全要求。

“遵纪守法是任何技术发展的前提。”江西南南律师事务所律师刘毅接受记者采访时说,Wi-Fi 分享软件应加强自律,充分尊重消费者知情权,提供清晰易懂的用户协议和隐私条款;杜绝非法收集、滥用、泄露个人信息等行为,将用户数据隐私权置于商业利益之上。

同时,互联网用户也应切实提高自我保护意识。Wi-Fi 主人应谨慎共享自己的 Wi-Fi 网络,并定期更换 Wi-Fi 密码;有一定网络知识的用户,可以通过添加无线设备过滤以及隐藏无线网络的方式,来降低被蹭网的几率。Wi-Fi 使用者应增强安全上网意识,拒绝来源不明的 Wi-Fi,在用手机登录掌上银行或支付宝等金融服务类网站时,最好使用手机自带的网络。

(本报原创稿件未经授权不得转载)



(资料图片)

无需密码连 Wi-Fi

最近,市民曾丽英发现家里的 Wi-Fi 连接速度变慢了,怀疑是被人蹭网所致。但她的 Wi-Fi 密码设置比较复杂,对方是怎么掌握密码的,曾丽英百思不得其解。后来她才想起来,上个月家里来了客人,客人连接 Wi-Fi 的时候,用的是手机上装的一款叫 Wi-Fi 万能钥匙的 APP。

Wi-Fi 万能钥匙是一款 Wi-Fi 分享软件,在各应用市场的下载量十分靠前。通过无线路由器后台系统,曾丽英看到有 5 台陌生设备接入了自己的 Wi-Fi,也就是说,有 5 个人借助 Wi-Fi 万能钥匙共享了她的 Wi-Fi 密码。

为了测试这款“蹭网神器”有多厉害,6月21日,记者来到万盛购物中心,在手机上打开 Wi-Fi 万能钥匙,软件界面自动显示出周边的 10 多个 Wi-Fi 热点。选取其中有钥匙图标热点,无需输入密码,顺利连上网络。

记者又来到邮政储蓄银行一家门店,同样用 Wi-Fi 万能钥匙成功蹭网,还不是银行营业厅对外开放的公共 Wi-Fi,而是银行内部办公部门的网络。在一些政府机构门口,记者也毫不费力地蹭上了 Wi-Fi。

这样强大的“黑科技”究竟是如何实现的?根据 Wi-Fi 万能钥匙软件服务协议,它是利用热点主人分享的闲置 Wi-Fi 资源来提供上网服务的。其工作原理可以理解为:用户 A 通过软件登录某 Wi-Fi 并输入密码,软件便存储该 Wi-Fi 的 IP 和密码到自己的数据库。当软件另一用户 B 搜索到该 Wi-Fi 时,软件通过调用数据库内保存的密码信息,帮助用户 B 免费连网。

随着移动互联网的发展,我们常常会使用