

(上接 A26 版)

►随着 WIFI 无线上网的普及,其安全问题也日益引起用户、业界、网络运营商等的关注。图为香港某 WIFI 安全论坛的宣传海报,图中的“802.11”是 WIFI 的技术代号。



无线上网易泄密 黑客分分钟在下套

有人的地方就有江湖,有网络的地方就存在隐患。跟有线上网相比,由于 WIFI 是散发在空中的信号,更容易被黑客突破,若被盯上不仅电脑上的资料容易被盗、还可能被传播病毒。

著名的写手韩寒曾在电视节目上透露,他经常深夜才更新博客,因为那时他可以蹭邻居的无线信号来上传文章。尽管经常传着传着就会断线,但他还是乐在其中。

上文提到的陆先生也告诉记者,他在无线上网的过程中,经常会发现陌生账户连接到自己的无线网络。假如对方只是看看网页还无所谓,并不影响自己的使用;但有的邻居居然在上面玩起网游,严重影响他上网的流畅。

据业内人士介绍,陆先生的情况,是由于他使用的无线路由器上网没有设置密码,相当于在整栋楼里开通了无线局域网,他的邻居只要有无线上网设备就能蹭上他的网络。

据了解,无线上网却不注意加密的 WIFI 用户大有人在。一位网络高手告诉记者,无线网络虽然方便,安全性也相对减弱了。如果无线网络的主人不注意防范,被他人成功蹭网,资料信息被盗走、电脑被灌入病毒、木马都是比较容易出现的事情;甚至可能因帐号被盗而承受经济损失。

专家解读:无线比有线危险

对于 WIFI 无线网络的安全防范问题,记者还采访了北京大学通信与信息安全实验室(深圳)主任、博士生导师、信息安全专家朱跃生教授。

朱教授告诉记者,WIFI 技术的确存在一定的安全隐患,因为连上同一热点的用户处于同一局域网中,如果不采取必要的安全措施,就可能受到攻击。尤其是公共场所的无线网络,由于成员都是动态匿名的,安全问题更为突出。

也就是说,在公共场所使用 WIFI 无线上网,与自己处于同一局域网的用户都是陌生人,比起在单位等有线的局域网,用户大都是同事这样相对熟悉的人,安全性自然不可比。因此,就更要保护自己的隐私。

蹭上无线网络偷窥别人电脑资料有多容易?记者请教网络高手吴先生,见证了“偷窥”的全过程。

记者见证:“偷窥”其实很简单

首先,吴先生下载并安装了软件“局域网超级工具”,并进行一些简单的设置。这样他轻易地从扫描到的热点中,搜索到有“共享文件”的用户;然后从中选取感兴趣的文件,直接打开就可以看到了。

“偷窥真的这么简单?”面对记者的惊讶,吴先生很平静地说,“操作其实很简单,只要你有心偷窥,只要不是对电脑一窍不通,从网上下载这一类软件,稍微学习一下就可以了。看完我的演示,现在你也应该学会了。”

吴先生告诉记者,被偷窥是最常见的安全隐患。除此以外,更危险的是被窃取个人密码、甚至被传播病毒。他告诉记者,破解密码的软件在网上有很多,有了这些工具就能轻易利用无线上网连接,对其他用户进行攻击。记者看到吴先生利用破解软件,轻松连接到加密的无线局域网中,这时吴先生就获取对方电脑的各种机密信息、电子邮件等,“我们还可以删除这个人的私密的文件、邮件,甚至传播电脑病毒,这些都很容易操作。而且利用他的账户进行话费充值,甚至进行犯罪活动都是可以实现的。”吴先生告诉记者。这个过程,吴先生只用了十分钟。“虽然这种偷窥在有线网络也能实现,但相比而言,无线网络中更容易。”

安全习惯很重要

在公共场合使用无线,应该怎样保证自己的安全呢?朱教授建议我们首先要有很好的安全风险意识,养成良好的计算机安全习惯。比如,和别人共享的内容要即时关闭,不要将自己的文档暴露在局域网中;还要及时更新系统补丁和防病毒、防木马软件。

此外,对于垂手可得的免费热点,朱教授提醒大家,即使发现不明的免费无线网络,不要贪小便宜,因为这也可能是温柔的陷阱,有可能是有人诱惑你上钩,从而窃取你的资料。

朱教授提醒,有些黑客会在公共场合设置一个伪装的无线存取设备,吸引使用者上钩,从而截取上钩者输入的各类密码,或将病毒输入上钩者的电脑。因此,在公共场合中,运营商提供的热点会相对更安全。

电信专家告诉记者,随着时代进步,比如安全保密性更强的无线上网标准 WAPI 很可能会在不久将被全面采用。届时,我们就可以进一步享受到快乐、安全的无线上网。

无线上网安全小贴士

如何杜绝蹭网?



许多安装无线路由器的用户,都不注意对自己的热点设置登陆密码。图中所列的热点,都是“未设置安全机制的无线网络”,是别人随时随地“蹭网”的最好对象。

安装了无线路由器,要怎样才能防止不明用户“蹭网”呢?其实设置起来也不太难,以目前使用最多的无线路由器为例:

- 1、在 IE 地址栏输入“192.168.1.1”(不同的品牌型号的路由器,输入的 IP 地址可能会有所不同,具体查阅产品说明);
- 2、进入路由器控制面板,一般来说路由器登录时密码默认为空,这就是无线上网的最大漏洞。
- 3、进入“修改登录密码”选项,填入密码,就可以杜绝大多数人的蹭网行为了。考虑到可能有网络高手会进行破解,密码要设置得尽可能复杂;
- 4、一般无线路由器都会提供“允许 SSID 广播”功能,如果不希望自己的无线网络被别人搜索到,可以通过设置“禁止 SSID 广播”,这样自己的无线网络仍然可用,只是不会出现在其他人所搜索到的可用网络列表中;
- 5、还可以设置网卡的 MAC 地址绑定,设定只有自己电脑的无线网卡才能使用该无线网络,这样就基本能做到万无一失了。

怎样查出是否被蹭?

大多数路由控制面板带有流量统计的界面,可以直观地看到已连接网络的电脑终端的 IP 地址和流量情况。如果发现异常情况,可以通过路由控制面板直接关闭可疑的 IP 地址连接。

如何避免信息泄漏?

- 1、安装一定的防病毒、防木马和防火墙软件;
- 2、保持电脑操作系统以及杀毒软件等的更新,并定期利用这些软件扫描计算机,查杀病毒、木马、垃圾软件等;
- 3、定期更新微软等操作系统的补丁;
- 4、关闭共享的文件,如果必须共享应在共享结束后及时关闭共享;
- 5、以加密方式传输重要资料也是比较安全的方法,比如在网址开头是“Https”的网站所使用的资料都是经过加密处理的,比起一般的“Http”网址的网站安全。一般来说,电子银行或网上交易网站都会使用这种技术。
- 6、为避免连上可疑的无线热点,导致个人资料被盗,要牢记只可用信任的无线热点,在咖啡店等消费场所上网前应先店员确认热点的网络名称,以免上错黑客伪造的名称相近的热点;
- 7、在使用公共开放无线网络时,应避免读取私人电子邮件、使用网上银行服务或进行网上交易等操作。



朱跃生教授提醒,公共场所使用不明 WIFI 上网,危险性最大,尤其要注意保护隐私。