信息泄露、垃圾短信泛滥、暗藏扣费陷阱

小心！别让手机暴露了你的隐私

本报记者 **叶薇**

查天气、找美食、玩游戏、买电影票、网上购物……安装APP(应用程序),手机变成“百事通”。不过，享受便利的同时,你可能把位置信息、通讯录名单、朋友圈、上网记录全都暴露在外。你的手机其实一直在“裸奔”。

智能手机越来越“聪明”,也越来越不安全。在今年全国两会上,多名互联网领域的代表委员均提出,智能手机比电脑泄密更严重。昨晚，央视“3·15”晚会曝光了多款APP调取用户隐私信息的案例,垃圾短信泛滥、恶意插件扣除话费等问题频频发生。

图 IC

【相关链接】

消费者须提升隐私保护意识

智能手机拥有强大的扩展性能与丰富的第三方软件资源。然而,应用软件是把双刃剑,既可能成为造福人类的“天使”,也可能成为危害社会的“怪兽”。在移动互联网时代,全世界都面临着手机安全监管难题。

一名从事安卓游戏海外代理发行业务的业内人士介绍,国外用户下载APP以“Google Play”市场为主,里面也有大量的盗版和垃圾APP,开发者随便找张信用卡，付20美元就可以在市场里创建账号并上传应用。但是,国外用户对于应用权限要求的防范意识非常高,尤其是对短信权限异常敏感。他们会仔细查看每项权限的解释说明,即使看了说明后,也有可能拒绝安装。目前,国外加大对安卓平台的监管和整顿。一些欧美国家已有明确的立法规范,并公布了实施细则。

面对手机中可能正存在的APP应用,用户应尽快提升对手机安全的防护意识。

■提高警惕,通过正规渠道下载APP

■安装程序时,根据程序的功能,严控系统权限的授予

■采用专业杀毒软件,并注意升级和定时查杀

■仔细查看财务对账单或交易明细及时发现任何异常情况

本报记者 **曹刚**

“越轨”行为 抓取用户个人数据

“手机下载了几款软件之后,状态栏频繁弹出广告窗口,不断收到垃圾短信。按‘清除’没用,必须要点击‘观看’。”李先生逐一卸载手机软件,最后发现是一款名为《爆破小鸟》的APP作怪,卸载后就清静了。

在智能手机和移动互联网普及的今天,当你安装热门应用软件时,是否会留意安装前的授权确认？比如,这款《爆破小鸟》除了要求知晓你的位置信息外,还会提出“读取/删除SD卡”“读取通讯录”等要求,如果不同意,则无法继续安装。于是,很多消费者点击“确认”,APP迅速安装成功,同时也为手机小偷隔空窃取你的隐私打开了方便之门。

为什么授权会泄露隐私?复旦大学计算机系统与安全专家杨珉介绍,智能手机采用基于权限的安全管理机制。例如安卓系统采用约130个权限管控系统资源,其中就有打开手机麦克风或摄像头、收集短消息、邮件、账号、通讯录、通话记录及位置等信息。有些软件开发者,申请权限超出正常需要,多数普通用户并不会留意,结果拇指一动,“家门”洞开。杨珉举例,不少手机输入法为增强用户体验,可能会申请读取通讯录和自动联网的权限,前者方便输入名字,后者可建立在线个人词库。可一旦两功能叠加并被不怀好意者利用,千万用户的通讯录便唾手可得。

DCCI互联网数据中心最近针对中国各类安卓市场下载量前1400位的APP所进行的安全测评显示:66.9%的智能手机移动应用在抓取用户隐私数据，而其中高达34.5%的移动应用有“隐私越轨”行为。通话记录、短信记录、通讯录是用户隐私信息泄露的三个高危地带。

消耗资费 扣钱不和你商量

“太坑人了!在手机上装了一款‘植物大战僵尸’的游戏,玩的时候没注意,结果今天上网查话费才知道,这几天被多扣了180元短信费。”网友“悠悠金光”抱怨说，自从手机安装了这款游戏后,在毫无察觉的情况下屡次被扣费,经过查询才发现,是游戏软件“热情”地帮机主订制了多条增值业务短信。

网友“牛牛过河”发帖倾诉:手机一天没响,结果一拨号,居然欠费停机了,平时每月话费最多50元,这才月初为何就欠费了?原因是他下载了一款名为“超级酒保”的免费APP,被植入了多款广告插件,内置广告通过联网下载和刷新,闷声不响“吃流量”。这条信息跟帖众多,不少网友都纷纷吐槽:“什么都没干,流量就没了”。

这些用户遭遇的，正是智能手机面临的第二大安全问题——消耗资费，包括流量和话费。

“许多用户下载的热门应用软件,其实已经被动过手脚了,软件里被重新打包了一些恶意代码。”杨珉分析道,这种代码可以让手机在用户未授权的情况下,通过发短信或者链接指定的扣费网站,为机主订购不同类型的手机业务。它最厉害的地方在于,可以屏蔽扣费业务反馈给用户的确认扣费短信。

“询问是否订购业务、服务器反馈、最终确认扣费,手机短信正常扣费的3个步骤,消费者一个也收不到,遭受了经济损失,却还完全蒙在鼓里。”杨珉说。

商业利益链 环环相扣瓜分利润

网上应用商城中，大量软件靠个人上传,门槛较低,商城自身检测水平、核查机制良莠不齐,为不法分子提供了可乘之机。杨珉认为,移动广告商、恶意扣费、移动网银支付、用户信息交易等均是商业利益链上的环节。

广告商和广告平台私自收集个人信息,已是业内默认规则。信息处理方式通常有两种。一是卖给短信群发平台等渠道,立即套现;如果不急着套现,广告商和平台可以对这些信息做数据分析和短信推送,通过短信渠道向用户发送广告信息,反复骚扰,实现精确广告投放。“更可怕之处在于,通过获得用户的隐私信息,便可掌握其所在方位、社会关系网络、单位组织构成等,甚至能侵入并远程控制用户的智能手机等移动设备,实施窃听、跟踪与监视。胁迫或欺诈、发送垃圾广告、套取专业领域机密等违法犯罪行为都成为可能。”杨珉说。

不过,与暗扣费APP制作方相比,广告手段只能算小巫见大巫。业内人士透露,有些公司会盗版和仿冒下载量较高的游戏和应用，比如在《捕鱼达人》等游戏中内置扣费插件，二次打包后,以汉化版、破解版等名义推向第三方市场(应用商城)。用户下载后,插件就会暗中扣费。这些公司再和APP开发者甚至第三方市场合作,瓜分利润。

“广告利润较低,但加入‘暗扣代码’做APP,最快一周就能回本,月收入轻松过万。”业内人士透露,做暗扣业务一本万利,而且内置扣费插件还可用更改签名等方式,绕开手机安全软件的查杀。

安全大门 仅靠自律很难防守

记者调查发现,目前市面上已经推出多款安全软件,比如“安全管家”“手机卫士”等,具备了相应的权限管理功能，用户可以通过这些软件,有针对性地关闭APP的部分权限，而且部分系统还能做到按实际需要有选择地授权。

但是，在杨珉看来，这种方式治标不治本。“用安全软件就必须‘root’你的手机,也就是完全开放系统权限,这意味着你把手机的最高权限交给了这些安全软件,相当于把家里的钥匙交给了保安,安全与否完全依赖于保安是否自律。”杨珉透露,其实有不少安全软件本身就在窃取用户隐私。他还介绍,有些智能手机出厂时,系统就自带不少软件,其中很有可能内藏“小偷”。

“守住手机安全大门，不能仅靠安全软件、APP开发者、手机生产商自律,应有相应的监管机制。”杨珉认为,一要有标准,移动终端隐私数据分级、应用程序收集和使用隐私数据应有标准;二要有相应的技术检测手段,智能手机应用程序发布、审核等方面应有国家安全技术标准和测评机制,三要有追惩机制,制定相应的法律法规与管理办法,明确告知开发者和运营商,能做什么和不能做什么,比如要求应用程序显示声明对用户隐私数据的收集行为,并要求收集者承担对这些数据的保护和不扩散的责任。

记者了解到，工信部正在建立评估体系,对智能手机应用程序、内置软件进行评估和抽查,将第三方平台纳入管理,逐步完善备案、审核、监督、抽查等管理环节,督促服务提供商和内容提供商加大自我清查,整治恶意APP暗扣费等现象。

“苹果”自说自话 “神药”自吹自擂

—一批品牌被央视“3·15”晚会点名

昨晚,中央电视台“3·15”晚会成为全国消费者的关注焦点,多行业的多个企业被曝光。无论是“神医”广告忽悠人、金饰品以“铱”充好,或是苹果售后服务涉嫌歧视,还是一些手机安卓软件暗暗窃取用户信息等,都是时下消费者关心的热门话题,在网络和市民中引发广泛议论。

我国移动电话商品修理退还责任规定明确了移动电话商品换货后,三包期重新计算。然而苹果旗下的手机、电脑和iPad等多款产品却拒不执行。苹果公司对这些产品自有一套规定：整机更换回来的手机不重新计算保修期，最多只向后延90天,理由是手机“后盖没换”。央视记者调查发现,苹果为了逃避相关三包规定,在对出现故障的手机进行维修时,故意不更换后盖,即使其他部件全部更换,但“新手机”使用的仍然是原机的旧后盖,除非另外付钱才能换新盖。另据调查,英国、澳大利亚、韩国的苹果用户如发现自己的手机出现故障,只要在保修期一年内,苹果公司就会给用户免费整体更换一部新手机,根本不存在后盖不换的说法。

昨天,还有一些被央视3·15晚会曝光的案例:

■ 神药！不看疗效看广告

高老太降糖贴、慕容氏糖贴、丁三怪拔喘膏、平老太降压贴等大量虚假广告产品,通过包装神医、虚假广告,向消费者兜售。

■ 扒开黄金“内铱”

个别商家的所谓“千足金”都没达标,而是添加了价格只是黄金五分之一到十分之一的另一种元素,叫做“铱”。周大生等品牌均涉及。

■ 江淮同悦被曝“生锈钢板”,安全存隐忧

江淮同悦轿车为了节约成本,采用价格相对便宜的普通钢板代替防腐性能较好的镀锌板,造成钢板生锈,给车主带来极大安全隐患。

■ 网易等公司追踪用户cookie收集用户隐私

有的浏览器可以通过设置“阻止第三方cookie”,或者清理浏览器历史痕迹的方式,来保护用户隐私,避免上网行为被跟踪。但易传媒集团相关人士告诉央视记者,他们早已突破这些防护措施。

本报记者 **陈杰**