冒充10086非法盗取近200万元

——手机网络安全漏洞调查

只因为点击了显示为“10086”发来的“积分兑换现金”的链接，浙江省湖州市民钱先生的银行卡里近8000元就被盗取了。近日，浙江警方破获的多起案例显示，通过短信等多种方式植入手机的木马程序和钓鱼链接，正威胁着用户的个人隐私和财产安全。

“新华视点”记者调查发现，随着移动互联网的发展，手机网络安全事件正呈高发状态，除了冒充“10086”等伪基站短信发的链接，类似“测一测你的前世”等一些有趣的应用链接，也可能藏有盗取用户个人信息的木马程序。

利用钓鱼链接获利数百万元

浙江市民钱先生的手机不久前收到一条显示为“10086”的号码发来的信息：“你的手机积分可以换取270元钱，可以上网提现”，并附有网址链接。“点进去之后觉得页面很正规，就按提示输入了姓名、电话、农业银行卡号和密码，但提交之后就再无音信了。”钱先生随后去农业银行查询，发现卡里的7948元已全部被提走。

据浙江警方介绍，钱先生的遭遇并非个案。在浙江警方查明的这起系列案件中，犯罪嫌疑人冒充中国移动客服10086，在浙江、重庆、江西、湖南、广西等多地通过伪基站向手机用户发送“10086积分兑换现金”活动的链接，非法盗取近200万元。在浙江警方破获的另外一起案件中，犯罪嫌疑人在不到一年多的时间里，利用短信等方式向受害人发送木马程序链接，尽管每位受害者的损失折合人民币仅约1000元，但案件数量众多，犯罪嫌疑人总计诈骗或窃取至少250万元。

浙江省公安厅网警总队总工程师蔡林介绍，利用钓鱼网站、木马APK程序侵害用户财产安全的案件不断发生。这类木马APK程序往往是通过短信链接、手机APP嵌入等方式进入手机系统。奇虎360旗下第三方漏洞响应平台“补天”公布的某手机钓鱼网站的后台里，有500多名受骗人的银行账号、手机号、姓名等个人信息，而且每天都以20至30条的速度更新。

还有一类木马程序仅以骚扰用户为目的。北京某事业单位的刘先生告诉记者，他的手机总是收到一些奇奇怪怪的链接，要求他安装各类APK应用程序，有时还推送包含不健康内容的视频或图片，“删掉了又来”，严重影响手机的正常使用。在不得已更换新手机后的第一个月，刘先生又发现话费骤然增加，致电运营商客服才发现，他的手机号莫名开通了包括多款手机报在内的增值服务，加起来达100余元。

专业人士表示，刘先生后来遇到的这种情况，很可能就是通常所说的“恶意吸费软件”，这也是目前最为普遍的移动安全问题之一。数据显示，在安卓智能手机终端快速增长的2013年，我国平均每天有27万人的安卓手机被恶意程序所感染，其中资费消耗和恶意扣费类程序的感染量最高，分别占到总量的52%和24%。“近年来，这类手机安全事件更是呈现高发态势。”蔡林说。

查分APP、“测测前世”等竟是钓鱼链接

记者调查发现，利用手机和移动互联网应用程序的漏洞，盗取用户信息乃至获利的案件，其手法也在不断翻新。

——利用热点事件，集中发送钓鱼网站链接。比如，在高考结束后的一段时期，多地考生及家长收到了包含“高考查分APP”的短信链接；在A股市场备受关注的情况下，“查看明日涨停股”等信息频频出现在一些用户手机上。近期还有不法分子将木马程序植入“优衣库”视频在网络上传播。

奇虎360手机安全研究团队负责人宋申雷告诉记者，很多这类APP实际就是一个木马，只要用户点击下载安装，它就会在手机后台“安营扎寨”，“这就好比在手机里安装了一双眼睛，你在手机上的操作几乎一览无余，短信验证通知、银行卡密码、支付宝密码等都有可能被窃取。”

——利用用户猎奇心理，暗中盗取个人信息。有着5亿用户的微信，被用户认为相对安全私密。然而随着各种嵌入到微信平台中的应用程序越来越多，一些潜藏信息泄露风险的应用也逐渐增多。比如，“测测你的前世是什么人”等小应用程序就通过微信平台广泛传播。

上海市微信用户郑先生说，出于好奇点开链接，测出自己前世是“老鸨”，觉得蛮好玩，还在微信朋友圈里面分享了。“尽管在登录页面时要求授权认证，当时也有些担心，但觉得微信上的应用应该没什么问题。”

蔡林等专家认为，正是利用用户的猎奇心理和对平台的信任，一些包含木马的钓鱼网页才会具有强大的传播力，一些用户的信息正是通过所谓的授权认证而泄露。记者近日再点开类似链接发现，部分已经显示为“恶意链接”，被腾讯技术团队拦截。

——入侵具有信誉的‘安全APP’，获取用户信息。拥有数千万甚至超过1亿活跃用户的搜狗手机输入法、UC浏览器等手机应用，也会因为程序漏洞遭到恶意代码入侵。

据专家介绍，用户在不安全的网络环境下点击“更新应用程序”，或者看到好看的“输入法皮肤”点击下载时，恶意木马就有可能趁机植入正常程序当中，不仅可以获取用户保存的个人资料，还可以通过提取用户敲击键盘的数据读取交易密码。“还有一些用户反映，手机某些应用会在不经用户允许、没有任何提示的情况下自动进行后台更新，这也留下了较为严重的安全隐患。”宋申雷说。

移动APP存监测盲区，网络案件立案难

上海二三四五网络科技有限公司董事长庞东升认为，在“互联网+”的时代，个人在网络世界的曝光度越来越高，也给了不法分子可乘之机，移动端的钓鱼、木马植入等问题频发，正在加剧用户信息泄露等安全隐患。宋申雷认为，现在人们的日常生活越来越依赖于手机等移动设备，移动网络安全隐患的影响并不比传统的网站小，应当引起更多的重视。

据业内人士透露，尽管各类移动APP后台漏洞不断暴露，用户信息泄露、财产被窃取的案例也频频发生，但是由于网络空间没有地域概念，移动APP存在监测盲区，很多案件立案难。

比如，在浙江警方破获的案件中，犯罪嫌疑人的作案地点遍及多个省市，嫌疑人团伙分布在吉林延边、福建龙岩、浙江金华等多地，作案对象甚至包括我国台湾地区的手机用户。“对此，还应进一步发挥国家信息安全漏洞共享平台的作用，强化第三方漏洞监测和公众监督机制，保证用户的个人信息和财产安全。”宋申雷说。

专家认为，对于近5亿多移动互联网用户来说，首先还应提高辨别能力，避免被恶意链接欺诈。“比如，要养成从正规网站登录的习惯，遇到要求输入手机号甚至银行卡等个人信息的手机网页时，需要提高警惕，对于需要用户‘授权并登录’的跳转页面，应多留一个心眼。”宋申雷说。

蔡林表示，因流量不足而到处寻觅“免费WIFI”的手机用户，也要避免接入无需验证的公共WIFI。“黑客能够制造假冒的公共WIFI，监视并记录用户所有的操作信息，特别是盗取用户隐私信息及网银账户密码。普通用户很难区分接入网络的真假，但一旦连入‘黑网’，就有可能因信息泄露而蒙受巨大损失。”

业内人士提醒，手机丢失后，应第一时间冻结与移动支付相关联的银行卡账号、支付宝账号等，“此外，也不要将自己的身份证扫描件存在移动终端上，以免被不法分子利用。”蔡林说。

（据新华社）

2016年我国将建成世界最大单口径射电望远镜

正在贵州黔南安装建设的500米口径球面射电望远镜（英文简称：FAST），是目前世界上在建的口径最大、最具威力的单天线射电望远镜。中国FAST工程办公室称，这一超级望远镜有望在2016年建成，建成后将成为世界级射电天文研究中心。

■超级望远镜有多大？

FAST口径有500米，有近30个足球场大的接收面积。其主反射面的面积达25万平方米，由近460000块三角形单元拼接而成。它的圈梁被50根6米到50米高低不等的钢柱支在半空，周长约1.6公里，绕走一圈约要40分钟。

■性能如何？

与号称“地面最大机器”的德国波恩100米望远镜相比，FAST的灵敏度提高约10倍；与被评为人类20世纪10大工程之首的美国Arecibo300米望远镜相比，FAST的综合性能提高约10倍。作为世界最大的单口径望远镜，FAST将在未来20至30年保持世界一流设备的地位。

■有何独到之处？

全新的设计思路加之得天独厚的台址优势，使FAST突破了射电望远镜的百米极限，开创了建造巨型射电望远镜的新模式。首先，它利用贵州天然的喀斯特洼坑作为台址；其次，洼坑内铺设数千块单元组成500米球冠状主动反射面，球冠反射面在射电电源方向形成300米口径瞬时抛物面，使望远镜接收机能与传统抛物面天线一样处在焦点上；第三，采用轻型索拖动机构和并联机器人，实现接收机的高精度定位。

■如何诞生的？

FAST工程的预研究历时13年，由中科院国家天文台主持，全国20余所大学和研究所的百余位科技骨干参加此项工作。2007年7月FAST项目正式立项。2011年3月25日，FAST工程正式开工建设。 **（据新华社）**

我国网民数量已达6.68亿人

中国互联网络信息中心（CNNIC）昨日在京发布了第36次全国互联网发展统计报告。报告显示，上半年我国共新增网民1894万人；截至2015年6月，互联网普及率为48.8%，我国网民总数已达6.68亿人。

报告数据显示，截至2015年6月，中国手机网民规模达5.94亿，较2014年底增加3679万人。中国网民通过台式电脑和笔记本电脑接入互联网比例分别为68.4%和42.5%；网民中使用手机上网人群占比由2014年底的85.8%提升至88.9%；平板电脑上网比例为33.7%，较2014年底下降了1.1个百分点；网络电视使用率为16.0%。

报告显示，2015年上半年网络金融服务类应用蓬勃发展，网上炒股网民的规模显著提升。截至今年6月，我国网上炒股用户规模已达5628万，同比增长47.4%。 **（据新华社）**