# 十大威胁，你的手机中招了吗？

如今，越来越多人依赖手机完成生活和工作中的各项事宜，比如收发邮件、查询美食信息、网购生活用品等。之前只能依靠电脑操作的众多事情，大多可以安心交给手机来完成。然而，与之相关的安全问题也受到了前所未有的挑战。据CNNIC最新统计，国内手机网民规模在2013年达到3.88亿，超越PC成为最大的上网终端。与此同时，手机用户面临的黑客攻击也愈演愈烈。由于手机直接关联着话费、短信、通讯录等用户财产和私密信息，手机中招后果相比PC也更加严重。根据黑客攻击的影响范围和危害程度，360手机卫士发布了“十大手机安全威胁榜”，全面盘点伪基站、恶意二维码、安卓木马、GSM短信漏洞等新兴威胁，警示网民提升移动上网安全意识，注意防范潜伏在身边的手机安全威胁。尽管这只是一家安全厂商的数据，但非常有代表意义，因此，我们还是对此进行详细的介绍，希望大家能够对隐藏在自己身边的安全问题进行关注。

**●伪基站**

**恶劣行径：克隆银行号码发诈骗短信**

2013年，一种名为伪基站的强发垃圾短信和诈骗短信的攻击方式泛滥。据不法商家宣称，其一个月卖出伪基站上百台，而一台伪基站每小时最多可发3万条短信。不法分子将其放入车中，在人群密集的街道和小区自动搜索附近手机卡信息，发送广告或诈骗短信，甚至冒充95588等银行号码诱骗中招者访问虚假网银，盗刷银行账户资金。保守估计，2013年国内由伪基站发出的短信达到上百亿条规模。

**●不良应用市场**

**恶劣行径：存高危级“签名”漏洞**

安卓平台的开放性，决定了手机下载会像PC一样危机四伏，一些不良的应用市场尤其成为手机木马重灾区。特别是在2013年以来，安卓连续曝出三个高危级别的系统“签名”漏洞，黑客可在不破坏数字签名的情况下，将木马植入正常应用，从而混入应用市场进行传播，实现偷账号、窃隐私、窃听、打电话或发短信等多种恶意行为。对此，安卓用户除了注意定期对手机进行安全检测以外，更要加强安全下载意识。

**●短信拦截木马**

**恶劣行径：瞄准短信验证码，威胁支付安全**

短信拦截和窃取类手机木马迅速泛滥，最典型的是名为“隐身大盗”的安卓木马家族。此类木马运行后会监视受害者短信，将银行、支付平台等发来的短信拦截掉，然后联网上传或转发到黑客手中。黑客利用此木马配合受害者身份信息，可重置受害者支付账户，国内已出现多起“隐身大盗”侵害案例，有受害者损失高达十余万元。

目前有网站以1000元的价格公开售卖短信拦截类木马，智能手机用户应安装手机安全软件并保持更新，以防手机安装应用时不慎感染木马。

**●恶意二维码**

**恶劣行径：为手机木马打开入侵通道**

二维码有风险，见码就扫易破财。随着安卓智能的手机普及，恶意二维码成为黑客定向发送手机木马的途径。据360网购先赔用户反馈，不法分子往往针对网店卖家，以“购物清单”等名义发送恶意二维码。卖家扫描后会下载手机木马，一旦安装就中招，导致手机号、短信等信息泄露，甚至危及网银和支付账户资金，安卓用户应予以警惕。

**●虚假中奖短信**

**恶劣行径：利用《爸爸去哪儿》诈骗**

利用热门电视节目发送虚假中奖短信，是很老套的诈骗方法，但随着湖南卫视《爸爸去哪儿》节目的热播，骗子们也盯上了这个新节目。2013年，以《爸爸去哪儿》名义发送的虚假中奖短信泛滥，根据相关数据显示，每天由用户举报的此类中奖诈骗短信高达上万条。

除了使用手机卫士拦截诈骗短信以外，电视观众尤其是中老年人还应提升安全意识，切不可重蹈被中奖短信连骗30万元还执迷不悟的“大妈”覆辙。

**●山寨手机预装木马**

**恶劣行径：暗中吸费**

新买的手机没用多久，话费就噌噌被扣光了？当心买到预装吸费木马的手机，这种现象在一些山寨机和水货手机中并不少见。其中，有些是山寨厂商自己预装了手机木马，有些则是经过经销商二次刷机或“白卡”解锁的水货手机被刷入固件木马。据介绍，手机预装木马相比普通木马更加顽固，而且还会破坏手机安全软件。

**●“挂马”漏洞**

**恶劣行径：利用可疑链接被黑客控制**

只要点一下链接，手机就会被他人控制发短信或安装恶意应用。2013年年9月，安卓系统WebView开发接口引发的挂马漏洞曝光，国内大批热门应用和手机浏览器中招。

黑客通过受漏洞影响的应用或短信、聊天消息发送一个网址，安卓手机用户一旦点击网址，手机就会自动执行黑客指令，出现被安装恶意扣费软件、向好友发送欺诈短信、通讯录和短信被窃取等严重后果。目前该漏洞已被各大应用升级修补，智能手机打补丁也将成为惯例。

**●山寨客户端**

**恶劣行径：将热门应用作为“寄主”吸费**

铁路12306手机客户端刚刚推出，大量山寨版就在网上涌现，打着查询、抢火车票旗号传播手机木马。这些手机木马带有窃取用户12306账号密码、偷流量、吸费等危害。在整个2013年，木马将热门应用作为“寄主”的情况也非常普遍。安全专家提醒，用户要从官方渠道或安全市场下载应用，切莫轻信手机搜索上的推广链接。

**●GSM漏洞**

**恶劣行径：可致短信被黑客监听**

通信层面的安全漏洞造成的威胁，往往是最难以防范的。2013年，360安全中心首家发布红色警报，由于国内运营商对部分地区的GSM制式的数据通信没有加密，黑客可以监听自己所在基站覆盖范围内所有GSM制式手机（移动、联通的2G用户）的通信内容。一旦手机短信内容被黑客获取，手机号码所绑定的网上支付、电子邮箱、聊天账号等重要账户将全部面临被盗风险。

对此安全专家建议，GSM手机用户收到各种短信验证内容时应提高警惕，一旦发现不是由自己发起的网上支付或“找回密码”短信，应立即联系银行和支付平台客服求助。此外，网民应注意对个人信息严格保密，以免身份证号等重要信息泄露。

**●阿拉伯字符**

**恶劣行径：让iPhone应用闪退崩溃**

即便是封闭的苹果iOS系统，也可能因为漏洞攻击而变得脆弱。2013年8月，短短一条阿拉伯语字符串在网上走红，只要通过短信、微信消息、朋友圈、微博等方式把字符串发送给iPhone手机用户，就会造成对方应用闪退崩溃。

事实上，iOS上的漏洞数量并不亚于Android、WP等其他系统，其中不少漏洞可以利用远程攻击，iOS漏洞价值在国外黑客交易市场也居高不下，吸引了更多黑客火力。而对于iPhone用户来说，及时更新系统，谨慎点击可疑消息，是防范威胁最好的办法。

（叶丹）

# 苏宁云商“零钱宝”打响2014年余额理财市场第一枪

1月13日晚，苏宁云商发布公告称，旗下的南京苏宁易付宝网络科技有限公司（以下简称“易付宝”）推出的余额理财产品“零钱宝”，将于1月15日正式上线（licai.suning.com），备受市场关注的“零钱宝”终于揭开神秘面纱。作为2014年第一款上市的互联网金融产品，1月12日，苏宁的“零钱宝”的七日年化收益率为6.9910%，远超同业收益水平。

去年10月上旬，苏宁易付宝获得证监会关于基金销售支付结算的许可，随后又与广发基金、汇添富基金进行产品开发、测试，再到新产品“零钱宝”的上线，投入了大量的资源，这也充分体现了苏宁进军互联网金融的决心。

据苏宁金融事业部相关负责人介绍，“零钱宝”实际上是将基金公司的基金直销系统内置到易付宝中，易付宝和基金公司通过系统的对接，为用户完成基金开户、基金购买等一站式的服务，打破了很多基金业的传统模式，整个流程非常简单。

据Wind资讯统计显示，苏宁“零钱宝”接入的两家货币基金的七日年化收益率，一直稳定在6%以上的较高水平。相关数据统计显示，2013年12月份整月“零钱宝”平均年化收益率为6.32%，与同期0.35%的银行活期存款利率相比，苏宁“零钱宝”达到银行活期存款利率的18倍。2014年1月12日，零钱宝的七日年化收益率6.9910%，万份收益为1.8410元，同期华夏现金增利货币A七日年化收益率为5.8330%，天弘增利宝七日年化收益率为6.7030%。相较而言，“零钱宝”的收益远超市场同类产品收益，且一直处于稳健的态势。

不同于目前市场现有的一些理财产品，用户存入“零钱宝”的资金可以实现“7*24小时”、随时随地“T+0”快速提现到银行卡或者易付宝账户。用户还可直接使用“零钱宝”资金在苏宁易购购物支付、缴费、充话费、还信用卡。“零钱宝”实际上是为普通客户提供了一个从理财、增值到日常消费花钱的整体解决方案，让用户真正实现理财、购物两不误。

“和原先动辄几万元的理财产品高门槛相比，‘零钱宝’提供的这种1元起存、0手续费和稳健的资金收益的理财方式，为许多普通消费者提供了碎片化理财的机会和乐趣。”苏宁金融相关负责人告诉记者，这也是苏宁将余额理财产品命名为“零钱宝”的缘由，“在基金公司的稳健收益背景下，转入‘零钱宝’的资金将不只是零钱了。”

苏宁金融事业部相关负责人表示，苏宁推出“零钱宝”余额理财业务，旨在培育用户良好的理财习惯，优先保障用户权益，将老百姓的“零钱”汇集起来，通过合作基金公司专业的投研经验与投资能力，为用户实现增值。该负责人强调，在帮客户实现安全稳健投资的同时，苏宁将为用户提供更多消费应用场景，全力打造一个安全、稳定、灵活、便捷的集理财消费于一体的账户体系。相信在“零钱宝”推出后，苏宁将进一步加快在互联网金融方面产品的研发速度，为消费者提供更多样化的选择。

分析人士指出，苏宁“零钱宝”的上线，正式打响了2014年互联网金融市场竞争的第一枪。随着各大商业巨头布局互联网金融领域，今年将会有更多的互联网金融理财产品面市，这将大大满足普通消费者个性化、多样化的理财需求。

（田松平）