2013—2014 年中国手机支付安全报告

随着智能手机和移动互联网越来越多地渗入到人们生活的方方面面，手机支付从 2013 年开始也获得了爆发式地增长。一系列被冠以“XX 宝”的手机支付产品引发热潮不断。阿里巴巴加大了支付宝钱包的推广力度，余额宝上线 4 个月用户规模突破 3000 万；微信支付通过嘀嘀打车和微信红包短短几个月用户就达到了千万量级。

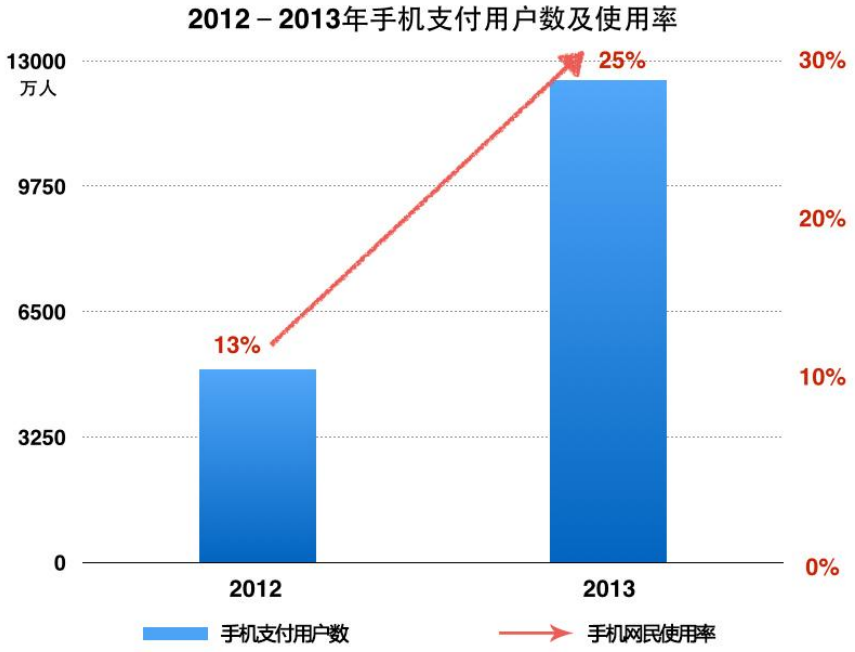
人们通过手机购物、转账、还信用卡、订车票、话费充值，变得日益普遍。统计显示，2013 年中国第三方手机支付市场规模已经超过 12000 亿元。未来十年是移动支付行业的黄金十年，已基本成为行业共识。

手机支付带来更多便捷的同时，也面临着越来越多的安全风险。金山毒霸安全中心分析发现，从 2013 年初至 2014 年 2 月份，手机支付相关的病毒、木马等风险因素急剧增长了 312%，成为威胁网民资产非常重要的原因。

一、中国手机支付市场规模

手机网民的高速增长，以及移动电子商务相关产业链的日趋成熟，使得网上支付和手机支付的用户数量快速扩大。

统计显示，截至 2013 年 12 月，我国使用网上支付的用户规模达到 2.6 亿，使用率达到 42.1%。2013 年手机在线支付增长更为迅速，用户规模达到 1.25 亿，使用率超过 25%，较 2012 年底提升了 11.9 个百分点。



从支付金额来看，统计数据显示，2013 年中国第三方互联网支付市场交易规模超过 53000 亿元，同比增长 46.8%，整体市场持续高速增长。2013 年中国第三方手机支付市场交易规模也超过 12000 亿元，同比增速超过 700%。

在国内的移动支付市场中，支付宝钱包、各大银行网银客户端、拉卡拉、微信支付形成

了第一军团，占据了超过 90%的市场份额。其中，支付宝钱包仍然遥遥领先，占据约 60%的市场。腾讯的微信支付则蓄势待发，增长最为迅猛，成为冲击支付宝钱包地位的最有力竞争者。

最近一段时间以来，腾讯与阿里巴巴在手机支付方面贴身厮杀，通过互联网理财产品、春节红包、手机打车软件等几场战役，竞争异常激烈。从整个手机支付市场来看，也正是这几场战役让网民对手机支付的认知度大大提高，对市场教育与行业格局都有积极意义。

二、手机支付安全风险分析

自 2013 年下半年以来，随着互联网金融概念的火热，越来越多的网民使用手机支付和手机理财，与之相随的是针对移动支付工具的恶意攻击表现极为突出，受害者损失普遍超过以往。

金山毒霸安全中心分析发现恶意攻击多呈现以下几种形式：

1、手机验证码大盗

该病毒的特点是：非常简单的低成本病毒，开发门槛很低，掌握一些社会工程学技巧，极易得手。

病毒的主要功能是拦截短信，有的拦截所有短信，稍用心的只拦截与验证码有关的短信，然后，病毒将拦截下来的短信通过电子邮件或短信转发传递给小偷。小偷用偷来的验证码，以及利用社会工程学欺骗从受害者处得到的身份证号、密保信息、银行卡号等个人信息，即可重置支付宝密码。

得到登录和支付权限之后，小偷可以立刻转出余额、消费（一般是买游戏点卡和手机充值卡）、通过快捷支付消费关联银行卡的活期存款、申请淘宝贷款，受害者损失可达数十万元。

2、网购退款钓鱼。

正常交易之后，骗子假冒网购卖家，谎称交易失败，联系买家退款。聊天过程中，发送钓鱼网站骗取受害者银行卡、身份证及验证码信息。得手后通过互联网支付工具迅速转移受害者网银资金。

类似案例大量出现，受害者除通过网络购买一般商品会上当外，一些预订机票的客户在起飞前被骗子拨通电话，骗子借口航班取消或改签，欺骗受害者退款，聊天过程中，让受害者通过网银或 ATM 转帐的。

3、假冒身份证补办手机 SIM 卡。

通过非法购买个人信息，伪造他人身份证，在一些管理不严的电信运营商营业厅补办手机卡。受害人的手机 SIM 卡失效，而另一张 SIM 卡却直接落入犯罪分子手中，其后的结果

和验证码大盗中毒完全一样，小偷可轻易通过重置密码来获得受害者资金的支配权。

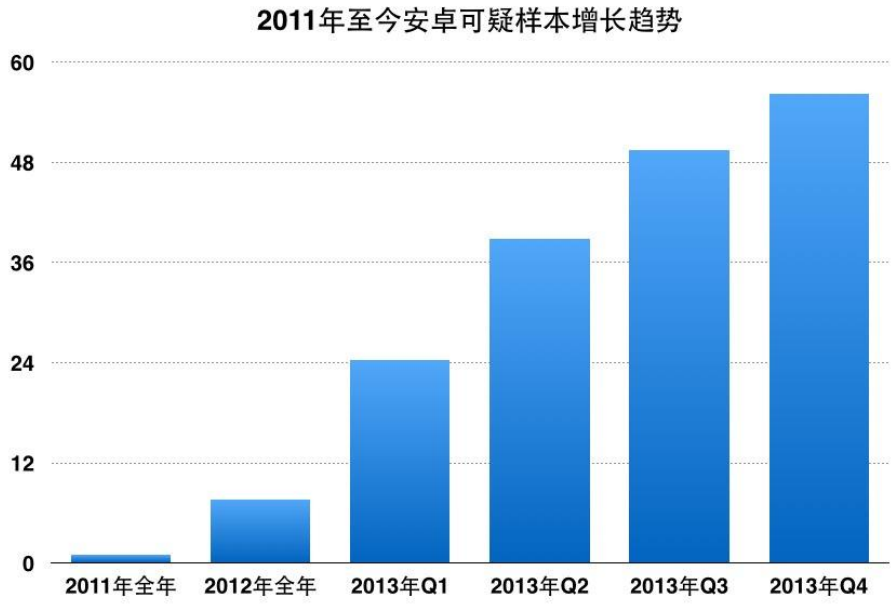
4、办理信用卡骗取个人详细信息

以办理大额信用卡为幌子，欺骗受害者提供详细个人信息，办理银行卡开户，将新储蓄卡关联小偷手机号，小偷迅速通过互联网支付工具，采用和前面类似的方法，使用移动支付工具将受害者新办储蓄卡里的所有资金转走。

三、手机支付相关病毒数量统计

在移动支付平台未普及之前，金山毒霸安全中心观测发现针对支付的攻击主要是网购木马和钓鱼网站。攻击者在网民使用电脑网购时，将网购木马伪装成与商品有关的图片文件发给受害者双击，一旦中毒，网购木马可以在支付的一瞬间将网银资金抢走。网购木马被业界公认为有一定技术含量的木马，有较高的开发门槛。

在移动支付工具得到普及之后，特别是 2013 年下半年使用移动支付的网民人数迅速增长，许多人开始使用手机理财，手机里蕴藏的财富吸引了众多攻击者的注意。同时由于安卓的开放性，安卓病毒增长极为迅速。在安卓可疑文件中，病毒检出率高达 7%。

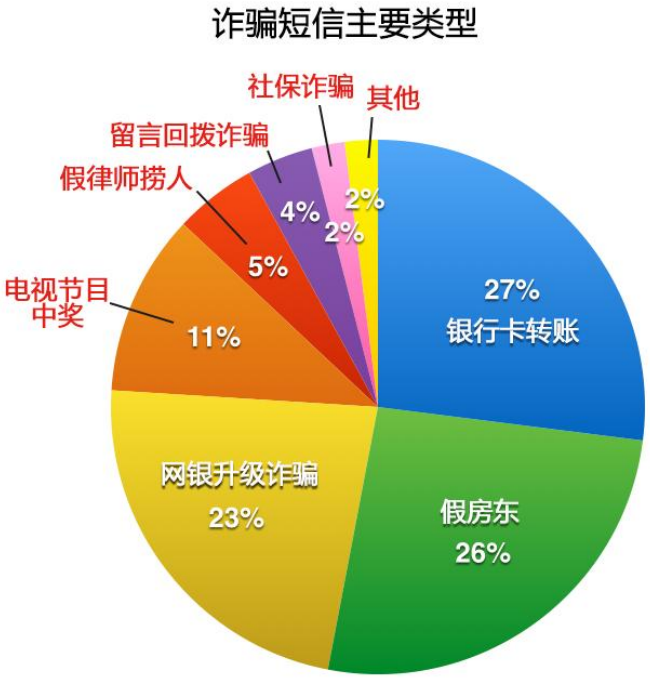


一部分攻击者很快发现，只需要简单的拦截安卓手机短信就可以获得大量财富。2013 年 7 月，金山毒霸安全中心截获了首例验证码大盗病毒，各地媒体不断报道网银资金莫名其妙被盗的案例。许多人无法理解银行卡、U 盾、密码都在自己手里，银行卡里的钱却不翼而飞。

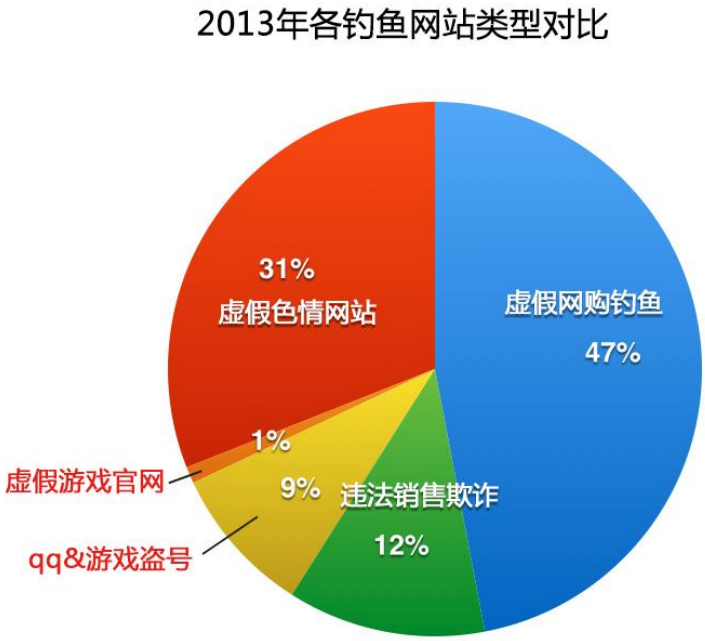
金山毒霸安全中心对验证码大盗类手机病毒的感染情况做过专门统计，截止目前，共拦

截验证码大盗病毒样本 2959 个，每天被验证码大盗病毒感染的不同型号安卓手机达 2800 余部，受害者损失难以估计。

除手机病毒之外，用户还会被各种诈骗短信欺骗、骚扰。犯罪分子利用短信群发器发送大量含诈骗内容的短信，直接欺骗网民登录假银行钓鱼网站骗取网银资金，通过短信、电话欺骗网民通过 ATM 机或网上银行转帐。



钓鱼网站对手机网民同样影响很大，金山毒霸安全中心统计到假网购钓鱼网站占到钓鱼网站总量的 47%。手机上网的用户由于受手机界面的限制，比电脑上网更难区分网站真假。一旦上当，将个人信息提交到钓鱼网站，很难避免经济损失。



随着各种“宝类”理财工具的火热，与之相关的各种假投资理财网站增长迅猛，其主要类型为：1.小额贷款办理，2.信用卡办理，3.投资理财诈骗。其中投资理财类钓鱼为单笔诈骗金额最高的钓鱼类型，单笔诈骗金额达到 1500 元以上。

四、专家建议及解决方案

与手机支付安全相关的案件发生有两个基本条件：第一，各种原因导致的个人信息泄露；第二，各种原因导致移动支付依赖的手机验证码信息到达犯罪分子手中。

阻止这两个基本条件同时满足，即可阻止网络犯罪发生。具体建议如下：

1、 网民需要认识到密码管理的重要性。

重要的、关键的网络服务（比如常用邮箱、B2C 网站帐号、QQ、微博等），必须确保不重复使用密码。重复使用密码就如同一把钥匙开所有的门，只要任意一个网站被黑客入侵，就会危及所有关键网络服务的安全。

网民可以选择在自己的电脑上使用密码管理软件，生成复杂密码，再将生成的密码加密存储在本地计算机，注意定期更换重要服务密码。

2、 相关企业、单位协作做好公民个人信息保护

掌管用户个人信息的企业、单位、国家机关，加强信息系统安全管理，防止黑客入侵；

司法机关加强对非法倒卖个人信息犯罪的查处，依法打击黑客非法入侵；
安全厂商、媒体、银行等机构对网民进行持续性的安全常识教育，让网民逐步养成自觉保护个人信息的习惯。

3、使用安全软件拦截手机应用软件普遍存在的权限滥用问题，阻止手机软件非法收集个人信息

4、金山手机毒霸针对验证码大盗的特殊作案手法，抢先一步，将含有验证码、银行、支付等关键字的机密短信内容加密，阻止任何第三方可疑程序读取。令验证码大盗手机病毒拦截短信的企图完全落空，即使遇到无法检测出来的新验证码大盗病毒，一样不能获得关键短信内容。从而阻止网银被盗案件发生。

5、金山毒霸反钓鱼系统拦截骗子小偷发送的钓鱼网址链，防止用户在不安全的网站提交银行卡号、密码、身份证、手机号等关键信息。

6、提供网购敢赔服务，在攻击者突破金山毒霸防御时，为用户提供每年最高 8000 元的敢赔服务。敢赔服务可以有效地帮助捕捉最新的病毒攻击和钓鱼网站攻击。