2015 年中国手机网民网络安全状况报告

（2016 年 9 月）

内容简介

近年来，智能手机在网民生活中扮演的角色日益重要，其安全问题受到社会各界高度重视，CNNIC 针对各种手机网络安全问题和网民网络安全意识进行调查。报告主要内容包括 2015 年国内手机信息安全环境、手机信息安全整体概况、用户手机安全风险认知情况、用户手机安全软件使用情况等，并针对当前重点手机安全问题提出建议。

本报告中关于网民手机上网安全问题的被动监测数据得到国家互联网应急中心和腾讯手机管家的大力支持，特此鸣谢！

版权说明

欢迎扫描二维码，关注 CNNIC 互联网发展研究官方微信。

报告下载：http://research.cnnic.cn/

互联网报告.中国

报告咨询

联系方式：喻先生 010-58813459

孟女士 010-58813326

联系邮箱：cnnic-survey@cnnic.cn

中国互联网络信息中心（CNNIC）

2016 年 9 月

目 录

第一章 调查介绍 1
一、 调查对象与调查内容 1
二、 调查样本规模与生成方式 1
三、 调查方式 1
四、 被动监测数据来源 1
五、 调查随机性和准确性控制方法 1
六、 术语定义 2
第二章 报告摘要 3
一、 基础数据 3
二、 国内手机网络安全趋势 4
第三章 手机信息安全环境 5
一、 政策环境 5
二、 社会环境 5
三、 技术环境 6
第四章 各类手机信息安全事件概况 7
一、 手机信息安全事件主要类型 7
二、 骚扰诈骗类手机信息安全事件 7
三、 信息泄露类手机信息安全事件 8
四、 恶意软件类手机信息安全事件 9
五、 病毒木马类手机信息安全事件 10
第五章 手机信息安全事件对用户的影响 12
一、 用户对各类手机信息安全事件的感知 12
二、 手机信息安全事件造成的损失 13
三、 手机信息安全事件的处理方式 14

四、 手机应用权限管理情况 15
五、 手机操作系统使用情况 16
第六章 用户手机安全风险认知情况 18
一、 手机网民信息安全态度 18
二、 手机网民信息安全事件关注状况 19
三、 公共 Wi-Fi 风险认知 20
四、 二维码风险认知 21
五、 伪基站风险认知 22
第七章 手机安全软件概况 23
一、 手机安全软件安装情况 23
(一) 手机安全软件用户规模 23
(二) 手机安全软件用户分布区域 23
(三) 手机安全软件安装方式 24
(四) 手机安全软件未安装原因 24
二、 手机安全软件使用情况 25
(一) 手机安全软件使用频率 25
(二) 手机安全软件常用功能 26
(三) 手机安全软件信任程度 27
三、 手机安全软件品牌 28
(一) 手机安全软件首选率 28
(二) 手机安全软件选择因素 29
第八章 趋势与建议 30
一、 移动网络服务快速发展，手机信息安全环境更加复杂 30
二、 骚扰类信息安全事件频发，窃取用户信息的手段趋于隐蔽 30
三、 用户对各类手机安全风险认知仍需加强 31
四、 手机安全软件渗透率较高，防护功能齐全是用户首选因素 31
五、 完善法规与加强协作是未来网络安全大势所趋 32
版权声明 33

免责声明 33

图目录

图 1 全国骚扰、诈骗电话发生情况.....8
图 2 2015 年移动互联网恶意程序类型占比.....9
图 3 2015 年手机病毒类型比例.....10
图 4 手机病毒传播渠道占比.....11
图 5 手机病毒感染人次.....11
图 6 用户对各类手机信息安全事件的感知.....13
图 7 各类手机信息安全事件造成损失.....14
图 8 手机信息安全事件处理方式.....15
图 9 手机网民应用权限管理情况.....16
图 10 手机网民操作系统占比.....17
图 11 手机网民信息安全态度.....19
图 12 用户对 Xcode、WormHole 等信息安全事件关注情况 19
图 13 手机应用漏洞出现后的反应.....20
图 14 手机网民公共 Wi-Fi 安全认知 20
图 15 手机网民二维码风险认知.....21
图 16 手机网民伪基站风险认知.....22
图 17 手机网民手机安全软件安装情况.....23
图 18 不同区域手机安全软件使用率.....24
图 19 手机网民手机安全软件安装方式.....24
图 20 手机网民未使用手机安全软件原因.....25
图 21 手机网民手机安全软件使用频率.....26
图 22 手机网民手机安全软件各功能使用率.....27
图 23 手机网民手机安全软件信任程度.....28
图 24 手机安全软件首选率.....28
图 25 手机网民手机安全软件选择因素.....29

第一章 调查介绍

一、 调查对象与调查内容

调查对象：过去半年居住在国内且使用手机上过网的 6 岁及以上手机用户。

调查内容：各类手机安全事件发生情况、影响范围，以及手机网民的手机上网安全意识与信息保护行为。

二、 调查样本规模与生成方式

本次调查的电话样本共 4,000 个，样本覆盖中国大陆一至五线城市。CNNIC 根据各地区的移动电话号段，按照 1:100 的比例随机生成电话号码后四位，完成生成之后，采用乱序表将生成的电话号码打乱顺序，由访问员随机拨打。

三、 调查方式

通过计算机辅助电话访问系统（CATI）进行调查。

四、 被动监测数据来源

本报告中关于网民手机上网安全问题的被动监测数据来自国家互联网应急中心发布的《2015 年中国互联网网络安全报告》和腾讯手机管家的《腾讯移动安全实验室 2015 年手机安全报告》、《2015 年度互联网安全报告》。

五、 调查随机性和准确性控制方法

- ✧ 拨打号码的随机生成由 CNNIC 研究人员完成，以保障抽取样本的随机性。完成调查后，电话调查公司须提供所有电话的拨打明细情况给 CNNIC 进行抽查。
- ✧ 为避免接通率对随机性的影响，对号码无法接通的情况，采取至少拨打三遍的方式。
- ✧ 为避免访问员个人观点对访问造成的影响，规定不需要读出的选项一律不加以任何提示，并追问到位。

✧ 电话调查结束后对数据进行了预处理、核对了变量的取值和变量之间的逻辑关系等，对于不合格样本予以整体删除处理。

六、 术语定义

✧ **手机安全事件：**指用户通过手机在接入互联网的过程中导致用户信息系统受损、信息内容泄露或个人活动受到不良干扰的事件。在本调查中，特指用户账号或密码被盗、个人信息泄露、遇到假冒网站、遇到欺诈诱骗信息、手机中病毒或木马、手机被安装恶意软件、手机收到垃圾短信、手机收到骚扰电话等问题。这些事件之间可能互有包容，本调查并不严格要求事件的互斥性。

✧ **手机安全防护软件：**指保护用户手机设备安全、内容安全、系统设置安全，避免发生或协助处理手机安全事件的软件。部分手机安全防护软件可能还有系统清理优化、软件下载等功能；但不具备安全保护功能的系统管理软件不列入安全防护软件范畴。

✧ **安装率：**指被访问的手机网民中最近半年内安装了手机安全软件的用户比例，安装率 = 回答最近半年内安装过某手机安全软件的手机网民 /手机网民样本总数。

✧ **使用率：**指被访问的手机网民中最近半年内使用过手机安全软件的用户比例，使用率 = 回答最近半年内使用过某手机安全软件的手机网民 /手机网民样本总数。

✧ **手机恶意程序：**指用户不知情或未授权的情况下，在手机系统安装、运行过程中违反了国家相关法规行为的可执行文件、程序模块或程序片段。

✧ **伪基站：**通过短信群发器、短信发信机等相关设备搜取以其为中心、一定半径范围内的手机卡信息并伪装成运营商的基站，通常冒用他人手机号码强行向用户手机发送诈骗、广告推销等短信息。

✧ **二维码：**按照一定规律分布在平面上的黑白相间的几何图形符号，具有记录数据信息的功能。

第二章报告摘要

一、 基础数据

- ✧ 截至 2015 年 12 月，国内手机网民规模达 6.2 亿，手机网民已经占到整体网民的 90.1%。
- ✧ 95.9%的手机网民在 2015 年遇到过手机信息安全事件，在所有遇到过手机信息安全事件的用户中，52.7%的用户认为自己没有因此造成损失；由于个人信息泄露影响正常工作生活和由于手机安全问题花费时间和精力解决的用户占比分别为 26.4%和 26.1%；造成用户话费、流量丢失或者账户资金丢失等直接经济损失的比例为 8.9%。
- ✧ 使用手机安全软件进行查杀病毒和恶意程序已经成为当前手机网民的首选处理方式，且用户占比高达 48.6%；通过社交媒体公布安全事件、向相关部门举报投诉以及向安全联盟反应问题的占比分别为 10.7%、10.1%和 8.1%；26.4%的用户在遭遇手机信息安全事件后不会采取任何措施进行处理。
- ✧ 截至 2015 年底，手机网民中会主动查看手机软件隐私权限的用户仅占 35.8%；只有 8%的用户会通过手机安全软件的提示留意手机应用的隐私权限；高达 56.2%的用户完全没有注意过手机应用的隐私权限问题。
- ✧ 38%的手机网民认为目前使用手机上网非常安全或比较安全，而认为使用手机上网比较不安全或很不安全的比例仅为 12.8%。
- ✧ 55.4%的手机网民在过去半年中曾经使用过公共场所的免费 Wi-Fi 或手机软件提供的免费 Wi-Fi，其中 44.7%的用户会在不确认公共 Wi-Fi 是否安全的情况下直接连接。
- ✧ 67.5%的手机网民认为扫描二维码可能存在风险，并会在扫描二维码时进行有意识的鉴别；仍有 29.4%的用户认为不会有风险或没有想过此类问题。
- ✧ 58.9%的手机网民没有听说过伪基站，另外 15.8%的用户虽然听说过伪基站但对其带来的危害并不了解，仅有 25.2%的用户听说过伪基站也了解其可能带来的危害。
- ✧ 截至 2015 年 12 月，国内手机安全软件用户规模达到 4.5 亿，占整体手机网民的 72.6%。
- ✧ 手机垃圾清理、手机内存清理、扫描杀毒、骚扰电话拦截和流量监控是目前手机网民最为常用的五项功能，使用率均在 60%以上。

二、 国内手机网络安全趋势

移动网络服务快速发展，手机信息安全环境更加复杂

截至 2015 年底，国内手机网民规模已达 6.2 亿，随着移动 4G 网络的普及，O2O 服务、手机购物和移动支付等业务快速发展，越来越多的用户信息通过互联网上传给各类应用服务商，网民的手机信息安全环境日趋复杂。按照不同手机信息安全事件的类型进行区分可以发现，手机安全风险向手机应用产业链上下游延伸的趋势明显。

骚扰类信息安全事件频发，窃取用户信息的手段趋于隐蔽

2015 年国内手机信息安全事件的发生呈两极化趋势，且信息安全事件数量显著增长。一方面，不会对用户构成直接经济损失的骚扰类安全事件的用户覆盖率很高；另一方面，通过手机病毒、恶意软件窃取用户信息的手段则越来越隐蔽。不容忽视的是，手机病毒和恶意软件在 2015 年影响群体的规模显著增长，但很少有用户对此有所察觉。

用户对各类手机安全风险认知仍需加强

智能手机功能的不断发展使得其可以在越来越多的场景下为用户提供便捷服务，但随之而来的各类风险也逐渐增多，公共 Wi-Fi、二维码、伪基站等安全问题也更易发生。调查发现，目前国内仍有近半数手机网民对于公共 Wi-Fi、二维码等各类手机安全风险缺乏基本的安全防范意识，加强对手机网民在各种应用场景下手机信息安全知识的普及宣传仍十分必要。

手机安全软件渗透率较高，防护功能齐全是用户首选因素

根据第 37 次中国互联网络发展状况统计调查数据，截至 2015 年 12 月，国内手机安全软件用户规模达到 4.5 亿，占整体手机网民的 72.6%。通过对不同地区手机网民的手机安全软件使用率进行分析可以发现，城市发展水平越高，其手机安全软件的使用率反而越低。从选择因素来看，功能齐全是用户选择手机安全软件的首要因素。

完善法规与加强协作是未来网络安全保护大势所趋

要真正改善手机网民的信息安全环境，不能仅依靠政府与相关部门的执法行动，必须明确各方责任，汇聚手机信息安全产业生态中的各方力量进行深度合作，才能够对信息安全相关的违法犯罪行为进行有效打击。这一过程不仅需要政府完善与执行相关法律法规，还包括手机信息安全企业对用户安全产品的改进，以及用户安全防范意识的提升和对手机信息安全问题的积极反馈。在完善安全相关法律法规的同时加强手机网络安全生态建设，将成为未来网络安全治理的大势所趋。

第三章手机信息安全环境

一、 政策环境

网络安全问题逐渐得到政府的高度重视，并被上升到国家战略层面。习近平总书记提出：“没有网络安全就没有国家安全”，并出任中央网络安全和信息化领导小组组长，体现了国家最高层领导对保障网络安全、维护国家利益、推动信息化发展的决心。

在十八届四中全会上决定完善网络安全保护方面的法律法规后，于 2015 年 6 月召开的第十二届全国人大常委会第十五次会议初审通过了《中华人民共和国网络安全法（草案）》，针对网络主权、网络产品和服务安全、网络运行安全、网络数据安全、网络信息安全等方面进行了具体的制度设计，同时建立了网络安全监督管理体制和监测预警与应急处理机制。7 月，《中华人民共和国国家安全法》颁布并实行，将“建设网络与信息安全保障体系，提升网络与信息安全保护能力”作为维护国家安全的重要职责。由于移动互联网逐渐取代 PC 端互联网的趋势已经形成，未来以手机信息安全为核心的网络安全相关政策将更加完善，对手机信息安全的违法侵权行为将有更加清晰明确的界定，令用户享有更加全面可靠的法律保护。

二、 社会环境

网络违法犯罪行为得到社会各界关注，并受到相关部门的严厉打击。根据国家互联网应急中心（CNCERT/CC）发布的《2015 年中国互联网网络安全报告》的数据，截至 2015 年底，CNCERT/CC 共接到网民举报的网络安全事件 54937 起。而据公安部统计数据显示，2015 年我国公安机关共侦办网络违法犯罪案件 173 万起，抓获犯罪嫌疑人 29.8 万人。

手机网民规模不断增长、应用场景日趋多样，使得用户手机网络安全环境也更加复杂，逐渐增多的手机信息安全事件已经引起全社会的关注。根据《第 37 次中国互联网络发展状况统计报告》的数据，截至 2015 年 12 月，国内手机网民规模已达 6.2 亿，手机网民渗透率为 90.1%。而随着 4G 移动宽带网络的普及，手机端在线购物、支付、O2O 等业务高速增长，手机在日常生活中的应用场景大幅拓宽，且与用户财产的联系日益密切，造成网民面临的手机信息安全环境更加复杂。用户隐私信息泄露与手机应用安全漏洞等移动互联网信息安全问

题逐渐成为社会关注的新焦点，但另一方面仍有很多用户忽视手机信息安全问题、缺乏基本的手机信息安全意识，并因而造成了不必要的损失。与此同时，电话短信诈骗、骚扰等事件依旧频繁发生，影响了用户的日常生活，也阻碍了移动互联网产业的健康发展，使得手机信息安全问题更加不容忽视。

三、 技术环境

虽然 2015 年政府陆续推出多项政策加快建设网络强国，同时开展多项针对手机信息安全违法行为的专项行动，但仍然难以避免伴随技术发展而来的诸多信息安全新隐患。互联网基础设施、域名系统、终端设备、应用程序等产业链各环节仍然面临着较大安全风险，网络安全事件多有发生。木马和僵尸网络、移动互联网恶意程序、拒绝服务攻击、智能硬件安全漏洞、网页仿冒篡改等网络安全事件表现出新的特点：利用分布式拒绝服务攻击和网页篡改获得经济利益现象普遍；个人信息泄露引发的精准网络诈骗和勒索事件增多；智能终端漏洞风险增大；移动互联网恶意程序的传播渠道开始向网盘和广告平台转移。整体来说，技术水平的发展虽然推动了我国网络信息安全环境的提升，但也由此产生了很多新问题，未来网络安全攻守双方将以新型技术漏洞为核心进行长期博弈。

第四章 各类手机信息安全事件概况

一、 手机信息安全事件主要类型

本报告按照手机信息安全事件造成的影响进行区分，将用户遇到的手机信息安全事件分为以下四种类型：

1. **各类骚扰短信、电话：**通过电话或手机短信等方式，发布各种垃圾广告或诈骗信息，骗取用户钱财或非法牟利。此类事件常因用户上网时信息泄露造成，与用户手机信息安全息息相关，因此也列入本次调查范围。

2. **信息泄露问题：**移动社交网络、O2O 服务、互联网金融等新业务在为用户提供服务的同时，用户的个人信息也面临着越来越多的潜在风险。由于互联网应用程序暴露安全漏洞造成用户姓名、住址、电话、身份证号、消费记录等重要个人信息被泄露的问题在 2015 年时有发生。

3. **恶意软件问题：**恶意软件指在用户不知情或未授权的情况下安装、运行的程序，可能出现恶意扣费、信息盗取、传播垃圾信息、远程控制、资源消耗、诱骗欺诈等违法或流氓行为。手机端的此类问题多发生于手机应用渠道审核机制不够严格且下载渠道分散的安卓手机用户群体中。

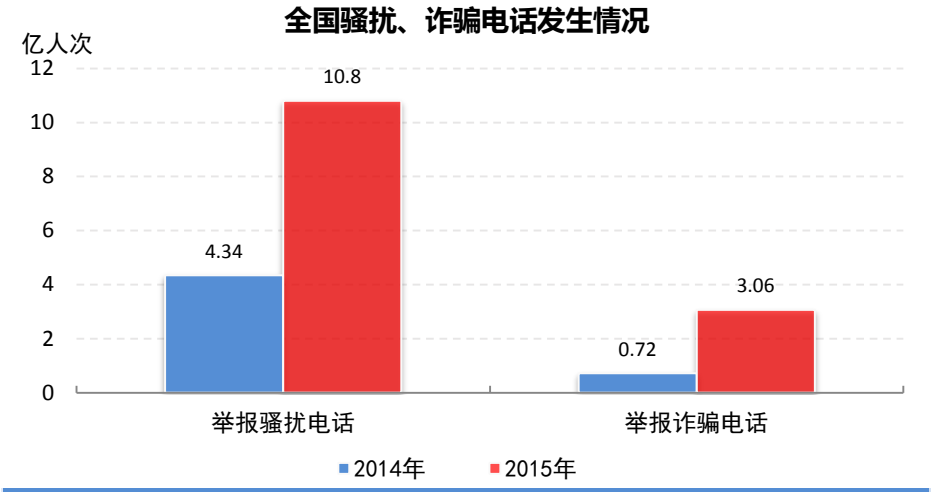
4. **病毒木马问题：**不法分子通过钓鱼网站或二维码等手段给用户手机植入病毒木马窃取用户银行账户密码或消耗用户手机资费，直接给用户造成重大经济损失。病毒木马等信息安全问题的解决不仅需要在技术和管理上进行完善，培养网民正确的手机安全使用习惯也同样重要。

二、 骚扰诈骗类手机信息安全事件

2015 年国内骚扰类手机安全事件数量呈明显上升趋势，未来将成为手机安全治理的重点方向。根据腾讯手机管家监测的数据，2015 年全年国内用户标记举报骚扰电话达到 10.8 亿次，是 2014 年的 2.48 倍；诈骗电话举报达到 3.06 亿次，是 2014 年的 4.25 倍；用户举报的垃圾短信总数达到 6.6 亿条，其中广告类短信达到 5.5 亿条，诈骗短信 7943 万条。造成骚

扰诈骗类手机信息安全事件数量爆发式增长的重要原因在于，自动拨号、智能语音系统和伪基站设备在近年来逐渐普及，大幅降低了骚扰电话和短信的执行成本。

2015 年 6 月国务院批准建立了由公安部、工信部、中宣部、中国人民银行等 23 个部门和单位组成的打击治理电信网络新型违法犯罪工作部际联席会议制度，加强对全国打击治理工作的组织领导和统筹协调。10 月 9 日，国务院打击治理电信网络新型违法犯罪工作部际联席会议第一次会议在北京召开。10 月 30 日，部际联席会议办公室在京召开电视电话会议，部署自 11 月 1 日起开展为期半年的打击电信网络新型违法犯罪专项行动。截至 2016 年 3 月，该行动已经取得一定成效，共破获电信诈骗案件 2.7 万起，抓获犯罪嫌疑人 9432 名。



来源 ：腾讯手机管家

图 1 全国骚扰、诈骗电话发生情况

三、 信息泄露类手机信息安全事件

信息泄露类手机信息安全事件的发生存在多种成因，包括：由于用户主动在社交类应用上公开自己信息后被不法分子窃取；由于手机平台存在安全漏洞造成用户个人信息被不法分子窃取；由于应用服务商被黑客攻击造成用户数据泄露等。个人信息泄露并不会给用户带来直接影响，但不法分子可能在了解用户个人信息后冒充同学、好友、同事、亲属对用户实施精准诈骗。

2015 年，由于手机系统漏洞问题造成用户数据泄露的事件时有发生，且影响规模极大：

2015 年 8 月，乌云漏洞平台披露通过分析红包外挂时发现一起越狱 iPhone 手机真实窃密案例，国内一些 iOS 应用/插件开发团队正在盗取越狱用户的 iCloud 账号与明文密码，并记录在远程服务器。据了解，已有超过 22 万 iCloud 账号密码等信息被多款内置后门的 iOS

插件窃取。经验证，这些被盗的 iCloud 账号可以随意登录，造成用户邮件、照片等信息全部泄露。

9 月，国家互联网应急中心（CNCERT/CC）在官网针对 XCodeGhost 开发环境漏洞发布了预警公告，指出被植入恶意程序的苹果手机应用可以在 AppStore 正常下载并安装使用，恶意代码具有信息窃取行为，并进行远程控制的功能，这意味着感染病毒的手机随时随地具有被恶意遥控的风险。据统计，在 App Store 上的 Top500 应用有 76 款被感染，受此病毒影响的用户数超过一亿。虽然苹果 iOS 系统一向以“封闭而安全”著称，但该事件的发生表明 iOS 系统安全漏洞问题仍需得到用户和厂商的重视。

10 月，乌云报告安卓 APP 存在一个叫做“WormHole (虫洞)”的安全漏洞，只要安卓设备连接网络，无论是否 Root，黑客都可以远程控制手机，甚至还可以上传隐私短信和照片，弹出对话框显示广告或钓鱼链接等，受影响用户预计将达三亿。

四、 恶意软件类手机信息安全事件

移动互联网恶意程序数量仍大幅增长。2015 年，CNCERT/CC 通过自主捕获和厂商交换获得移动互联网恶意程序数量近 148 万个，较 2014 年增长 55.3%。恶意程序主要出现于应用下载渠道分散且不易管理的安卓平台，占比达 99.6%以上。按恶意行为进行分类，排名前三位的恶意行为分别是恶意扣费类、流氓行为类和远程控制类，占比分别为 23.6%、22.2%和 15.1%。恶意程序传播次数达 8384 万余次，较 2014 年增长了 9.8%。

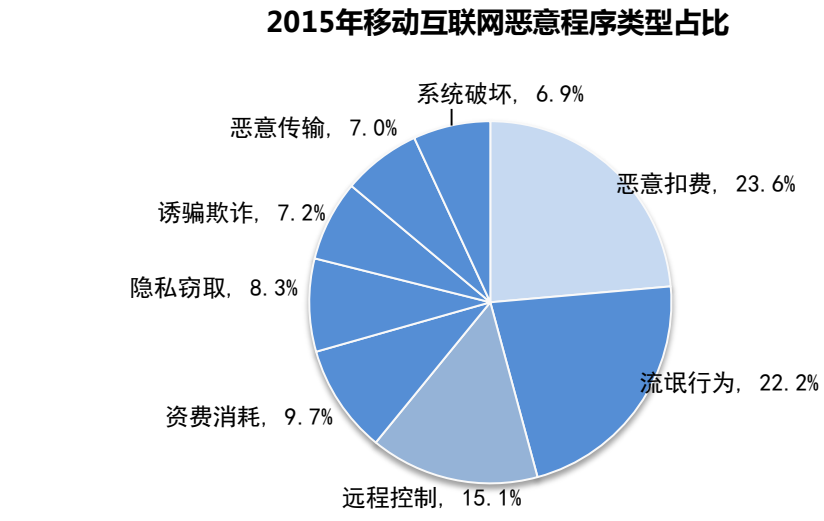


图 2 2015 年移动互联网恶意程序类型占比

主流移动应用商店安全状况明显好转，大量移动恶意程序的传播渠道转移到网盘或广告平台等网站。在工业和信息化部的指导下，经过连续三年的治理，国内主流应用商店积极落实安全责任，不断完善安全检测、安全审核、社会监督举报、恶意程序下架等制度，积极参与处置响应与反馈，恶意 APP 下架数量连续保持下降趋势，2015 年较 2014 年下降了 57.3%。根据 CNCERT/CC 的数据，按各平台接到通报的数量来看，排名前 6 的平台接到的通报次数占全年总通报次数的 50.2%。经确认发现，这 6 家主要是提供云盘、网盘、广告宣传等业务的网站，反映出大量的恶意程序传播源已发生转移。

五、 病毒木马类手机信息安全事件

根据腾讯手机管家提供的数据，2015 年国内 Android 病毒包数量迅猛增长，全年新增病毒包 1670.4 万。其中资费消耗类病毒占比最高，达到 74.22%，为 1239.5 万个，其次为诱骗欺诈类、流氓行为类和隐私窃取类病毒，占比分别为 9.75%、8.13%和 5.33%。其他类型手机病毒占比均在 2%以下。

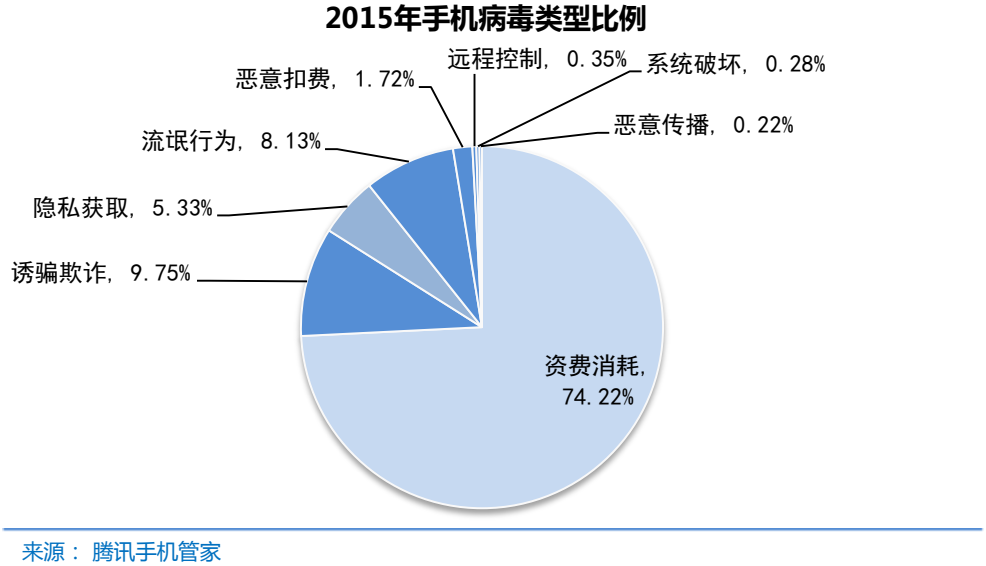
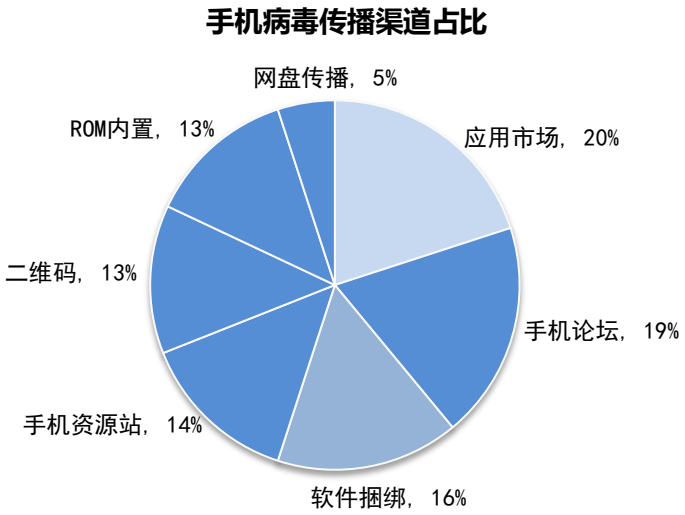


图 3 2015 年手机病毒类型比例

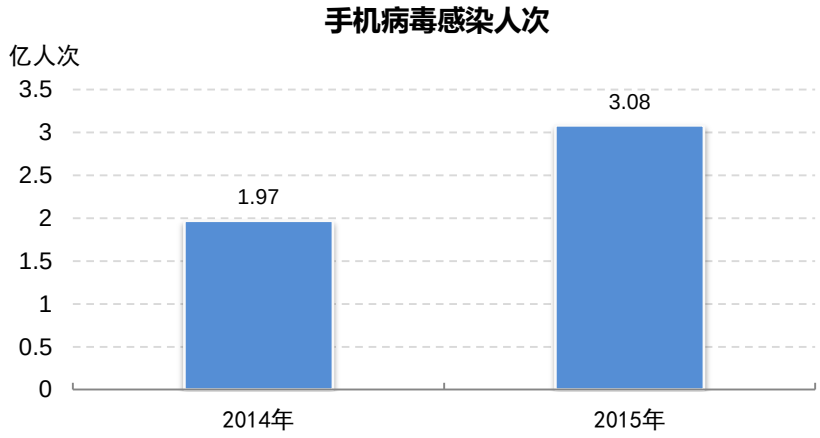
从手机病毒的传播渠道来看，由于国内应用市场下载渠道分散，且各渠道审核标准高低不同，造成应用市场仍是手机病毒传播的最主要渠道，占比达到 20%。此外，手机论坛也一直是恶意软件开发者的传播重地，其作为手机病毒传播渠道的占比达到 19%。由于国内手机论坛一直缺乏恶意程序的监管与鉴别机制，使得在热门游戏应用或者视频类软件中植入广告或恶意代码成为论坛黑客二次打包应用的常见手段。



来源： 腾讯手机管家

图 4 手机病毒传播渠道占比

随着手机网民规模的不断增长，遭受手机病毒侵害的用户群体也在逐渐扩大，但由于手机病毒具备不易被用户察觉的特性，导致大多数用户即便遭受手机病毒侵害也毫不知情。根据腾讯手机管家监测的数据，2015 年国内仅安卓用户的手机病毒感染人次就达到 3.08 亿人次，相比 2014 年增长 56.5%。且从整体增长趋势上看，手机病毒感染人次呈现每月爬坡式增长态势，12 月达到增长高峰。可以预期未来手机病毒安全问题形势将更加严峻。



来源：腾讯手机管家

图 5 手机病毒感染人次

第五章手机信息安全事件对用户的影响

一、 用户对各类手机信息安全事件的感知

整体来看，当前国内手机信息安全事件的发生呈两极化趋势。一方面不会对用户构成经济损失的骚扰、广告类安全事件发生频率很高；另一方面通过窃取用户信息给用户带来直接或间接经济损失的安全问题越来越隐蔽。比如通过手机病毒盗取用户账号密码、话费或流量等安全事件，大多数用户在遭受这类不法侵害后难以感知，等到发现经济损失后再采取应对措施则为时已晚。

截至 2015 年底，95.9%的手机网民认为自己曾遇到过手机信息安全事件。通过对手机安全事件类型进行区分可以发现，由于骚扰广告、违法诈骗类手机安全问题多处于法律监管的灰色地带，并且缺乏行之有效的打击手段，造成这类安全问题的发生最为频繁。

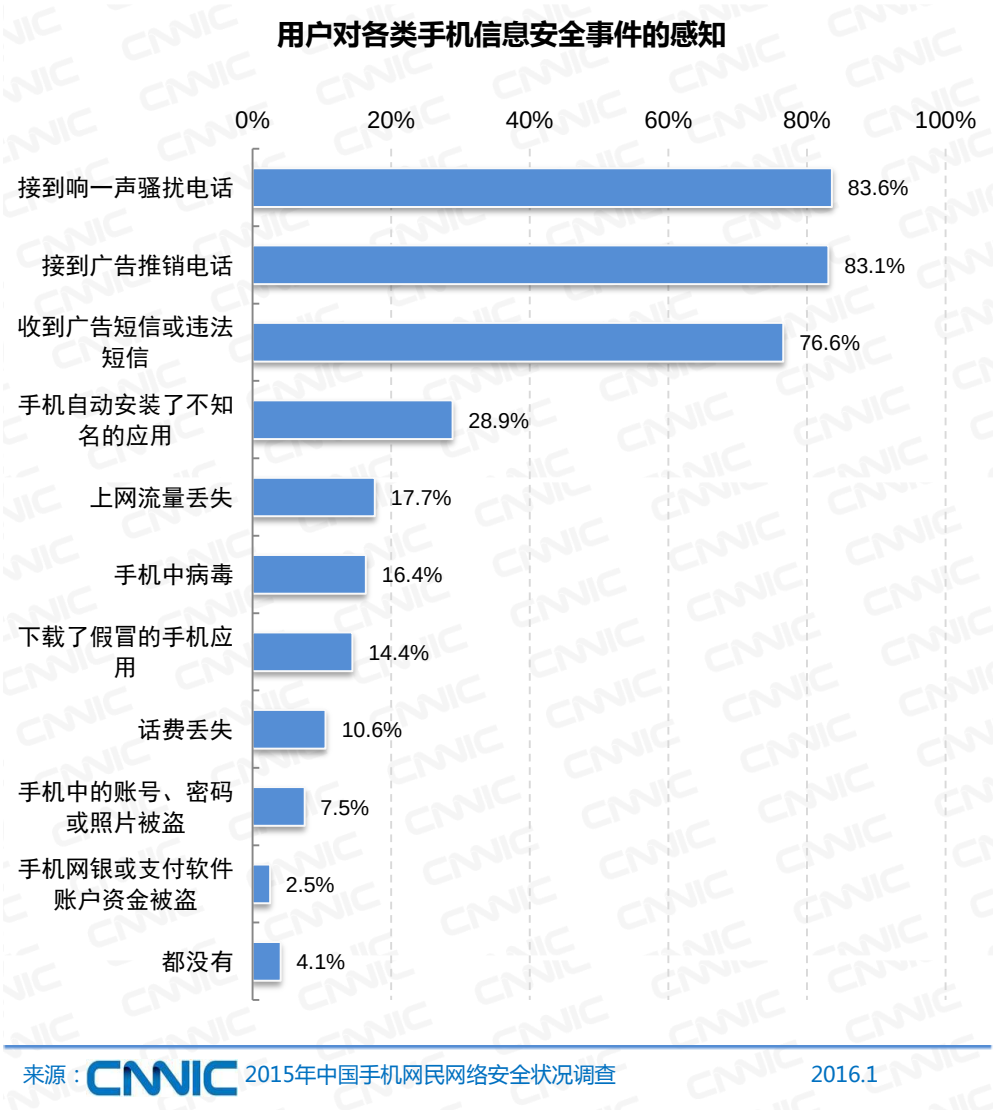


图 6 用户对各类手机信息安全事件的感知

二、 手机信息安全事件造成的损失

通过对手机信息安全事件给用户造成的损失进行分析可以发现，超过半数用户并未认为手机信息安全事件给自己造成了损失。其原因在于，一方面由于绝大多数用户遇到的是骚扰类手机信息安全事件，且这类问题往往不会对用户的日常工作和生活构成实质性影响，因此在过去半年所有遇到过手机信息安全事件的用户中，52.7%的用户认为自己没有因此造成损失；另一方面，对于察觉到手机信息安全事件给自己造成损失的用户来说，大多数手机信息安全事件带给用户的并非直接经济损失，而是由于用户隐私泄露对日常生活造成的影响。数据显示，由于个人信息泄露影响正常工作生活和花费时间和精力解决手机安全问题的用户占比分别为 26.4%和 26.1%。因手机信息安全问题造成用户话费、流量丢失或者账户资金丢失

等直接经济损失的比例占到所有遭遇过手机信息安全问题用户的 8.9%。

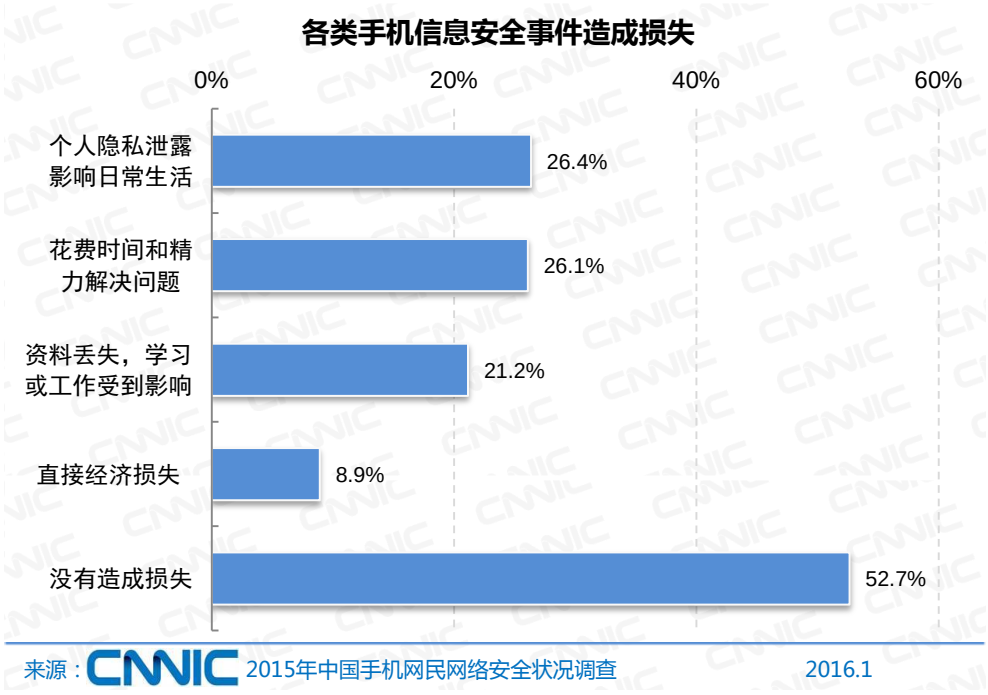


图 7 各类手机信息安全事件造成损失

三、 手机信息安全事件的处理方式

通过对遇到手机信息安全问题用户的处理方式进行调查可以发现以下三点：

第一，使用手机安全软件处理手机信息安全问题已经成为当前用户的首选方式，用户占比高达 48.6%。这表明手机安全软件在过去几年经过厂商的大力推广已经逐渐得到用户认可，且未来仍有提升空间。

第二，用户在遭遇手机信息安全问题后进行举报或问题反馈的积极性较差。数据显示，通过社交媒体公布安全事件、向相关部门举报投诉以及向安全联盟反应问题的占比分别为 10.7%、10.1%和 8.1%。造成用户反馈安全问题积极性不高的原因主要在于，向相关部门反馈手机信息安全问题的流程往往相对复杂导致操作成本较高，且即便反馈成功也并不会为用户带来任何短期利益。

第三，超过四分之一的用户在遭遇手机信息安全事件后不会采取任何措施进行处理。造成这种情况的原因在于大多数用户对自己遭遇的手机信息安全事件没有感知，或遇到的只是骚扰类手机信息安全事件且并未造成明显损失。此外，部分用户由于手机信息安全意识较差，且不具备手机信息安全事件的处理经验，因此在遭遇手机信息安全事件后不知道采取何种应对措施。

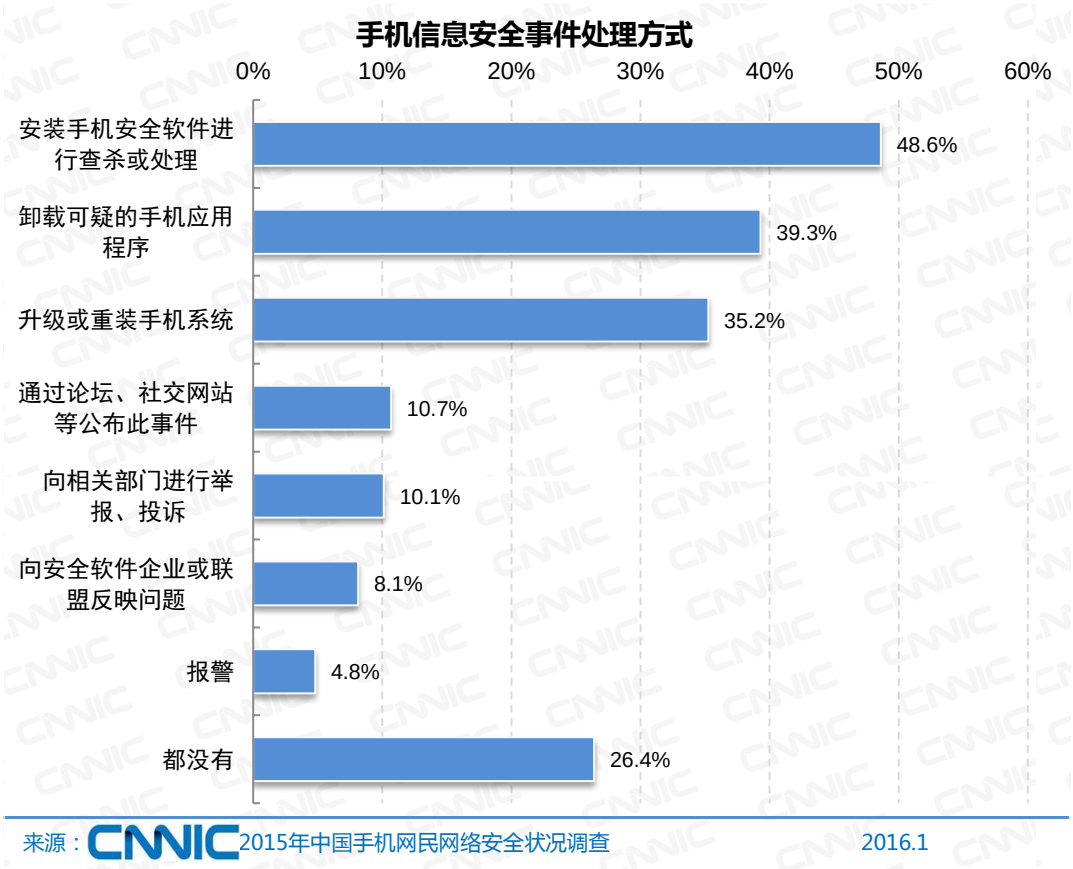


图 8 手机信息安全事件处理方式

四、 手机应用权限管理情况

很多恶意手机应用在获取用户通讯录信息时并非通过私下盗取，而是先向用户申请授权，由于用户并不具备风险鉴别能力，盲目对手机应用程序进行授权，导致自己的隐私信息泄露。调查发现，截至 2015 年底国内手机网民中会主动查看手机软件隐私权限的用户仅占整体手机网民的 35.8%；只有 8%的用户会通过手机安全软件的提示留意手机应用的隐私权限；高达 56.2%的用户完全没有注意过手机应用的隐私权限问题。

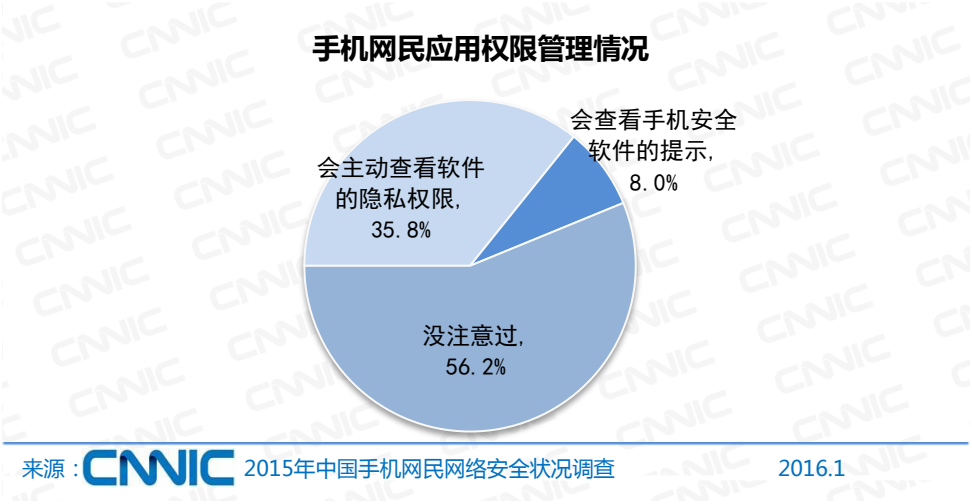


图 9 手机网民应用权限管理情况

五、 手机操作系统使用情况

由于安卓应用程序的分发渠道分散，且不正规的中小应用发布渠道较多，造成该平台是移动互联网恶意程序传播的主要平台。CNCERT 数据显示，2015 年捕获的安卓平台移动互联网恶意程序占比在 99.6%以上。而 iOS 平台应用主要通过官方渠道 App Store 进行分发，厂商可以从发行端对可能存在风险的恶意应用进行筛选和治理，因此其恶意应用数量较少。但是 2014 年 iOS 平台出现“Wirelurker”等恶意程序后，2015 年该平台出现了感染范围更广的恶意程序“XcodeGhost”，标志着 iOS 平台恶意程序的制作和传播链条趋于成熟。

根据调查，手机网民中使用没有 Root[1]过的安卓类手机系统最多，占比达到 53.1%，其次为未越狱[2]的苹果 iOS 系统，占比为 27.1%。值得注意的是，当苹果手机越狱后其封闭环境即被破坏，安全性完全丧失，因此越狱 iOS 系统的安全风险极高，这部分用户占比为 3.1%；此外，经过 Root 的安卓类手机系统由于权限完全开放，恶意程序可以在不通知用户的情况下静默安装任意应用，因此其安全风险也高于未 Root 的安卓系统，这部分用户占比为 14.3%。

[1] Root：通过技术手段让用户获取安卓等手机系统的最高管理权限。

[2] 越狱：通过技术手段让用户可以避免 iOS 系统对用户施加的诸多限制，比如可以支持用户从第三方应用商店下载手机应用或对用户界面进行定制。

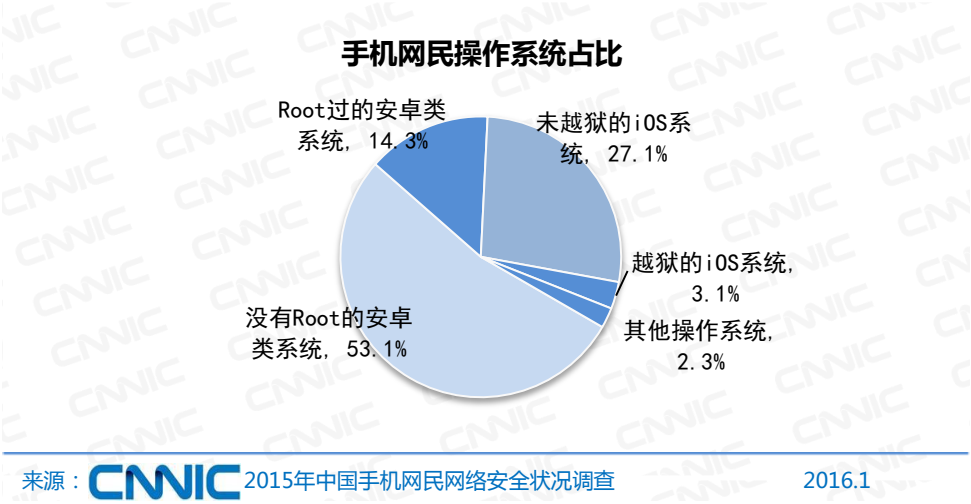


图 10 手机网民操作系统占比

第六章 用户手机安全风险认知情况

相比手机信息安全相关机构和企业对网民的被动保护而言，主动的手机信息安全意识更能够帮助用户避免该类事件的发生，因此加强手机信息安全知识普及、提高用户对于各类手机安全风险的认知是当务之急。调查发现，目前国内仍有近半数手机网民对于公共 Wi-Fi、二维码等各类手机安全风险缺乏基本的安全防范意识，加强对手机网民在各种应用场景下手机信息安全知识的普及宣传仍十分必要。

一、 手机网民信息安全态度

数据显示，38%的手机网民认为目前使用手机上网非常安全或比较安全，而认为使用手机上网比较不安全或很不安全的比例仅为 12.8%。多重因素共同促成当前手机网民网络安全感较强的情况：第一，2015 年政府相关部门对于伪基站、用户隐私数据盗取、电话短信诈骗犯罪等违法行为进行了有力打击，并收获了一定成效。第二，各手机安全企业积极推广自己的手机安全产品，并通过共享病毒库的方式提升了手机安全软件杀毒能力，从客观上推动了手机信息安全环境的改善。第三，随着媒体对手机信息安全问题的宣传，用户开始逐渐具备基本的手机信息安全防护知识，使得其规避手机信息安全问题的能力有所增强。

但同样不能忽视的是，49.3%的用户对目前手机信息安全持“一般”态度。这部分用户多为信息弱势群体，对信息安全风险缺乏清晰的认识，因此造成其往往对手机信息安全事件麻痹大意，是这类安全事件的高风险人群。

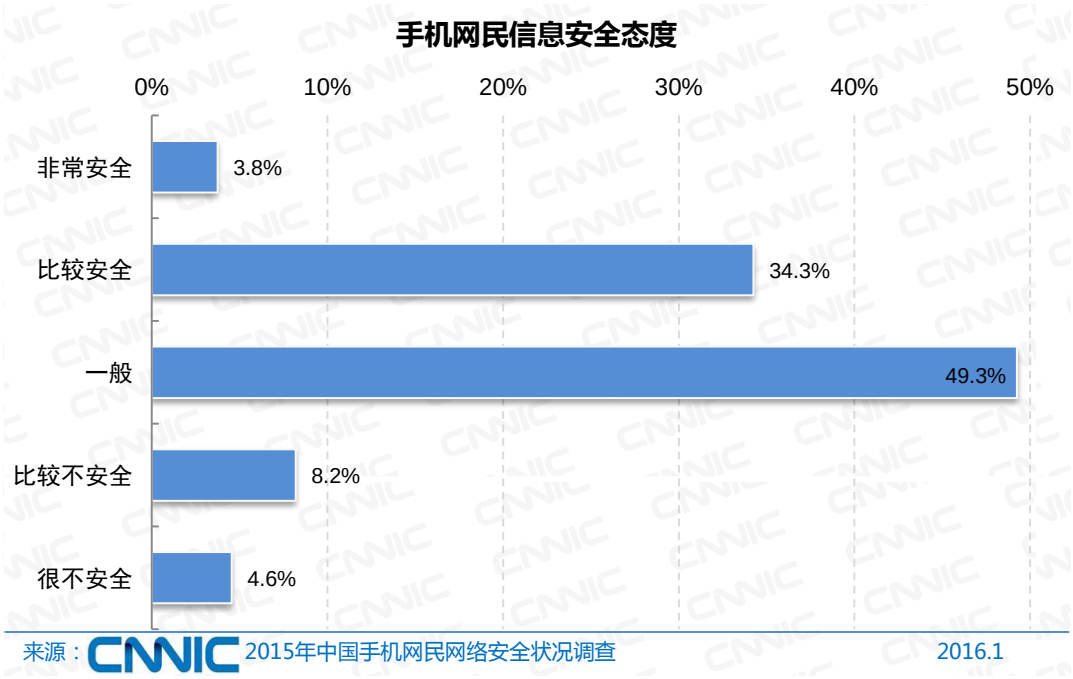


图 11 手机网民信息安全态度

二、 手机网民信息安全事件关注状况

2015 年手机应用程序出现安全漏洞的事件频繁发生，每次该类安全事件均可能造成数十万甚至上百万用户的个人信息泄露，但用户对此类事件的关注程度明显不足。根据调查，手机网民中曾经关注过苹果系统 Xcode 开发环境漏洞或安卓系统 WormHole 漏洞等重大事件的网民仅占整体的 40.3%，近六成用户对于此类可能直接影响到自己信息安全的事件没有关注或根本不知情。

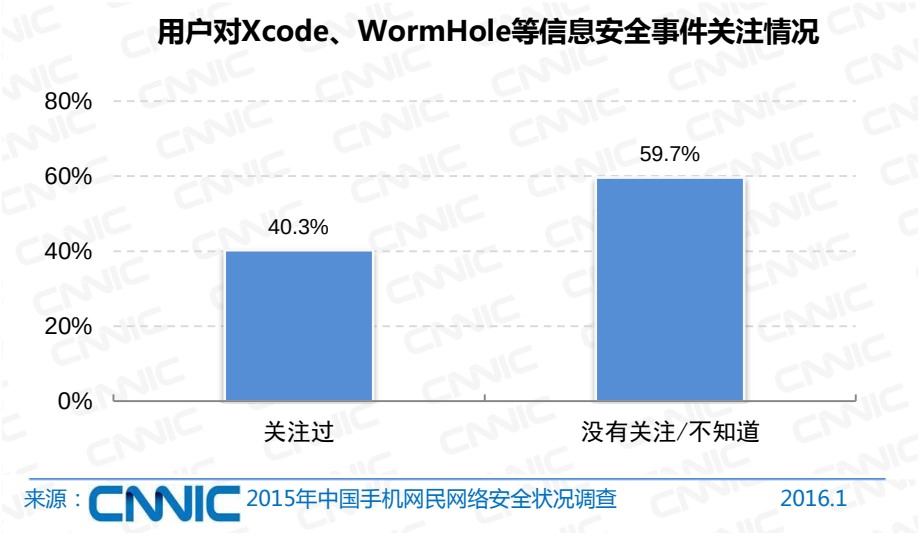


图 12 用户对 Xcode、WormHole 等信息安全事件关注情况

通过对关注上述手机应用程序漏洞的用户继续调查发现，虽然对手机应用漏洞事件有所了解，但仍有很多用户并未对此采取措施。数据显示， 39.7%的用户在了解到这类手机应用漏洞之后并未采取任何应对措施。

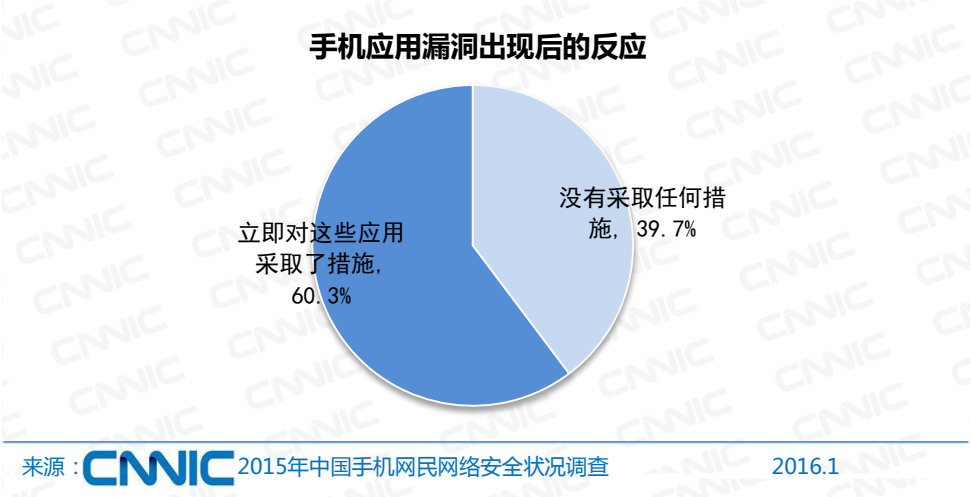


图 13 手机应用漏洞出现后的反应

三、 公共 Wi-Fi 风险认知

公共 Wi-Fi 随着移动互联网的发展已经在人们的日常生活逐渐普及，但很多用户对于接入不安全的 Wi-Fi 可能带来的危害却并不了解。一般来说，越是经济发达地区的公共场所，公共 Wi-Fi 的覆盖越完善。根据调查，国内手机网民中 55.4%的用户在过去半年中曾经使用过公共场所的免费 Wi-Fi 或手机软件（如 Wi-Fi 万能钥匙）提供的免费 Wi-Fi 。在连接过公共 Wi-Fi 的用户中，44.7%的用户会在不确认公共 Wi-Fi 是否安全的情况下直接连接，这部分用户很容易在上网过程中泄露自己的个人信息。

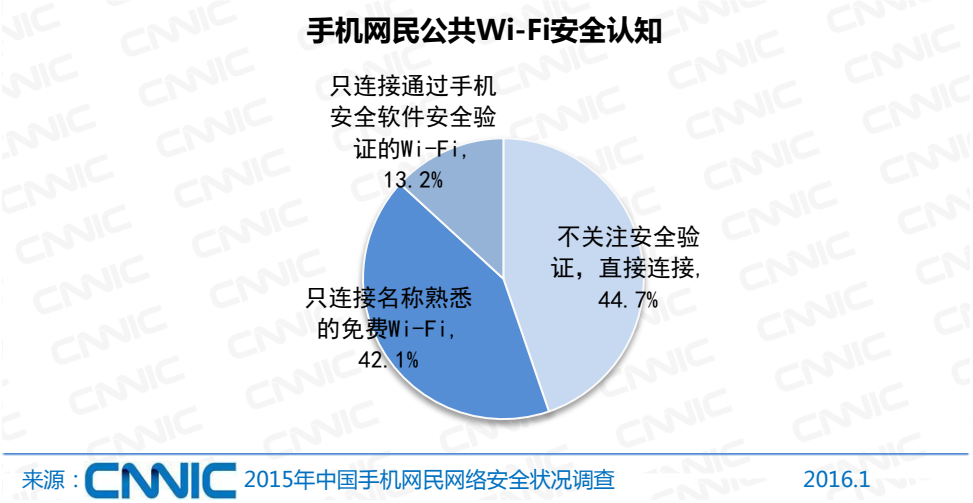


图 14 手机网民公共 Wi-Fi 安全认知

由于在连接公共 Wi-Fi 的过程中使用手机购物或进行支付可能存在支付密码被窃取的风险，因此应尽量避免在不可靠的公共 Wi-Fi 环境下使用手机支付功能。通过对连接过公共 Wi-Fi 的手机网民调查发现，绝大部分用户会在使用公共 Wi-Fi 时避免使用手机购物或支付。数据显示，在连接公共 Wi-Fi 的情况下使用手机购物或进行支付的用户占比仅为 19.6%。

四、 二维码风险认知

二维码自出现以来，其便捷性很快获得了大众的认可，但与此同时，借助二维码进行传播的手机病毒、恶意程序也日益增加。由于二维码技术已经相对成熟，任何人均可以通过网上的二维码转换软件轻易合成二维码，这大大降低了不法分子通过二维码进行各种非法操作的技术门槛。同时二维码从外观并不能辨别其安全性，因此很多用户即使因扫描恶意二维码导致手机被嵌入病毒，事后仍无从察觉。早在 2014 年央行就曾针对手机二维码支付存在的安全性问题紧急叫停过市场上的该类业务。

通过对网民使用手机扫描二维码的风险意识进行调查可以发现，目前手机网民中 67.5% 的用户认为扫描二维码可能存在风险，因此会在扫描二维码时进行有意识的鉴别；仍有 29.4% 的用户认为不会有风险或没有想过此类问题。可见对于二维码使用风险的宣传教育仍需持续推进。

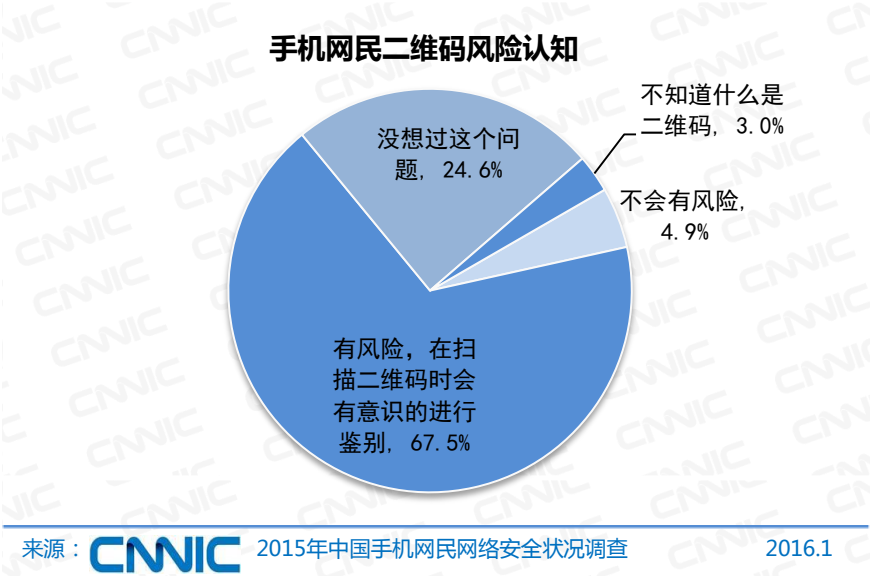


图 15 手机网民二维码风险认知

五、 伪基站风险认知

伪基站作为目前不法分子群发垃圾短信或违法短信的主要工具，自 2014 年开始就被各相关执法部门列为重点打击对象。2014 年 4 月 4 日，国家工商总局公布《禁止生产销售使用窃听窃照专用器材和“伪基站”设备的规定(征求意见稿)》。《规定》提出，对经公安机关认定的生产、销售窃听窃照专用器材、“伪基站”设备行为，由质量监督部门责令停止生产、销售，处以 3 万元以下罚款。此外，在后续出台的《中华人民共和国刑法修正案（九）》中规定：“违反国家规定，擅自设置、使用无线电台（站），或者擅自使用无线电频率，干扰无线电通讯秩序，情节严重的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。”围绕上述法规，2015 年国内各地警方纷纷开展针对伪基站问题的专项整治行动，对生产销售伪基站设备及使用伪基站的违法犯罪分子进行了有效打击。

虽然相关部门的打击行动能够减少伪基站设备数量，但还需手机网民提高自身对于伪基站工作原理的认知，从行动上避免点击伪基站推送的恶意链接，才能真正减少伪基站问题带来的损失。调查发现，2015 年国内手机网民对于伪基站的认知仍有很大不足，所有手机网民中 58.9%的用户没有听说过伪基站，另外 15.8%的用户虽然听说过伪基站但对其带来的危害并不了解，仅有 25.2%的用户听说过伪基站也了解其可能带来的危害。

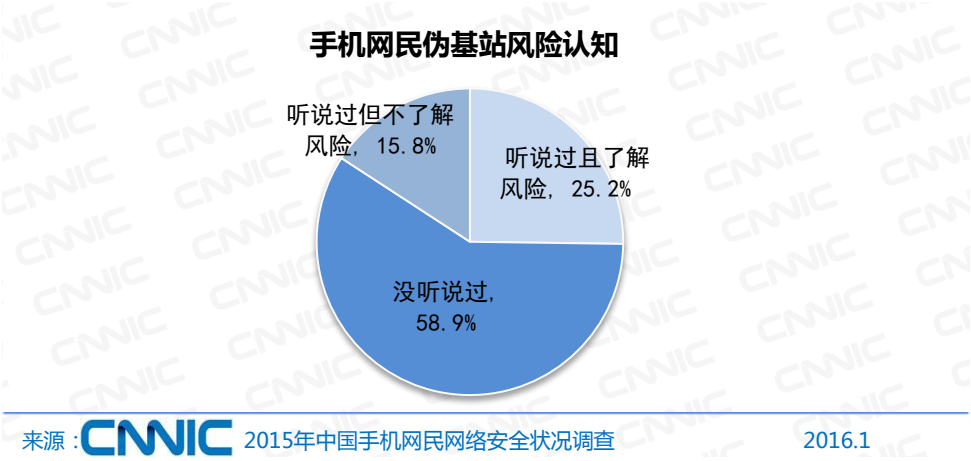


图 16 手机网民伪基站风险认知

第七章 手机安全软件概况

一、 手机安全软件安装情况

(一) 手机安全软件用户规模

随着对信息安全问题的逐渐重视，手机安全软件逐渐被广大手机网民所接受，且手机安全软件自身逐渐由基础的安全防范功能向外延伸，成为集病毒查杀、软件管理、隐私保护于一身的综合性手机管理工具。对于并不具备手机信息安全防范知识的用户来说，手机安全软件虽然不能完全杜绝手机安全事故的发生，但也从客观上为这类用户提供了一定安全保障。根据第 37 次中国互联网络发展状况统计调查数据，截至 2015 年 12 月，国内手机安全软件用户规模达到 4.5 亿，占整体手机网民的 72.6%。

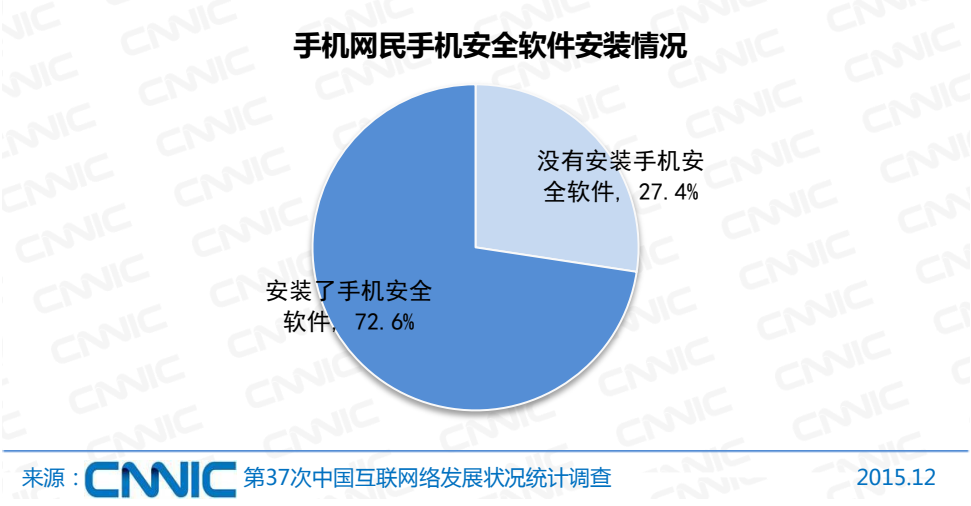


图 17 手机网民手机安全软件安装情况

(二) 手机安全软件用户分布区域

通过对不同地区手机网民的手机安全软件使用率进行分析可以发现，城市发展水平越高，其手机安全软件的使用率反而越低。这很大程度上是由于经济发达城市的用户 iOS 系统占比较高，而这部分用户对于手机安全软件需求不强造成的。数据显示，一线城市的手机安全软件使用率最低，为 65.7%；四五线城市的手机安全软件使用率最高，达到 74.7%。此外，手机安全软件在农村的使用率也达到 71%。

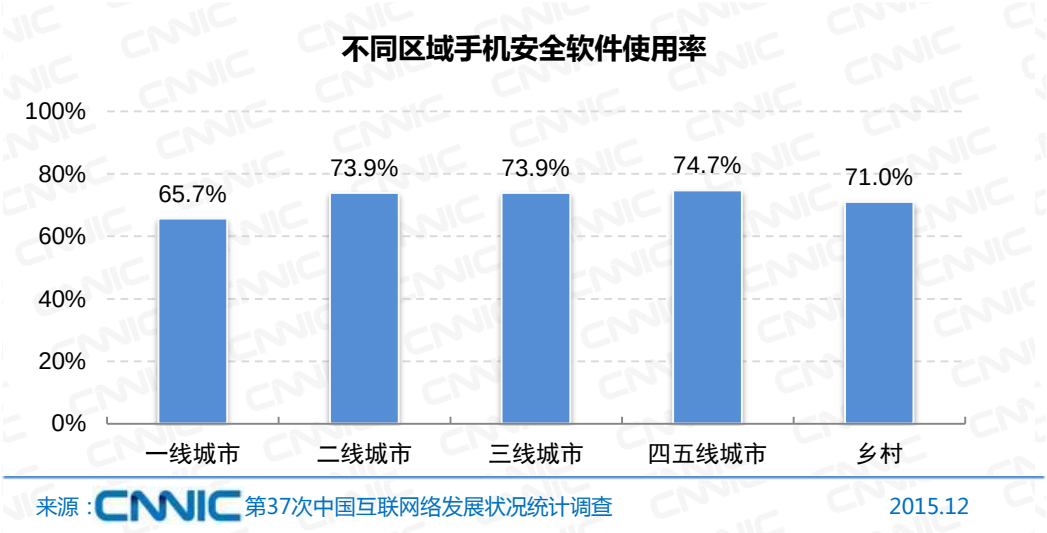


图 18 不同区域手机安全软件使用率

(三) 手机安全软件安装方式

通过对用户手机安全软件的安装方式进行调查可以发现，主动安装手机安全软件虽然已经成为主流，但手机出场系统预装仍是重要渠道。数据显示，主动安装或请别人帮忙安装手机安全软件的用户占比达到 70.8%；25.2%的用户手机安全软件是手机自带或系统预装的；4.1%的用户在无意中安装了手机安全软件或者对这类软件的安装完全没有意识。由于当前新网民逐渐向低学历、低收入等信息弱势群体渗透，而这类用户相比主动安装手机软件更易受到手机预装软件的影响，预计未来手机安全软件将更加依赖预装渠道。

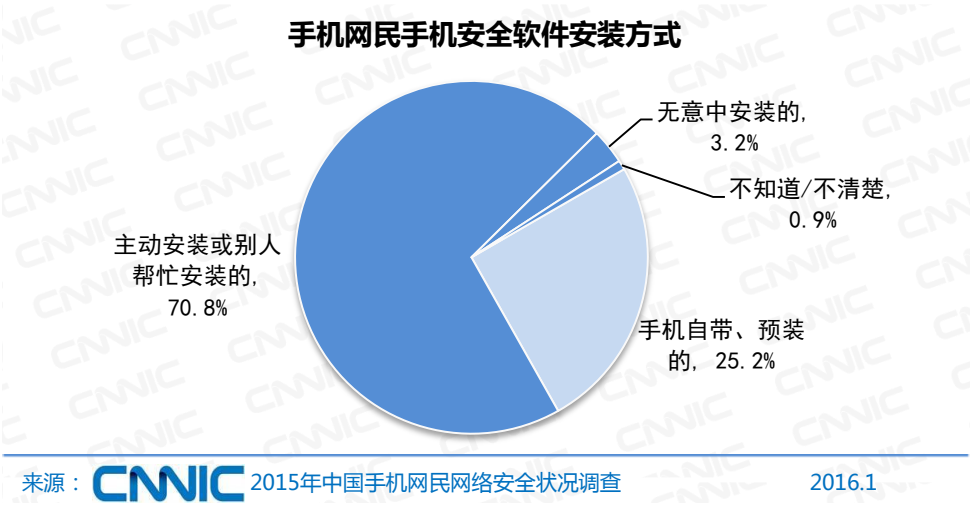


图 19 手机网民手机安全软件安装方式

(四) 手机安全软件未安装原因

通过对未使用手机安全软件的用户进行调查发现，三成用户认为手机安全软件对自己没

有明显帮助，超过两成用户则因为不知道/不会用这类软件而没有安装。随着手机安全软件厂商的推广和软件自身操作便捷化的发展，未来手机安全软件用户规模仍有较大提升空间。此外，46.6%的用户认为自己的手机很安全而没有安装这类软件，其原因在于苹果 iOS 系统用户的占比高达整体手机用户的 30.2%，且 iOS 系统天然的封闭环境导致其用户不易受到恶意手机应用的侵害，因此使得苹果手机用户对于手机安全软件的需求不强。

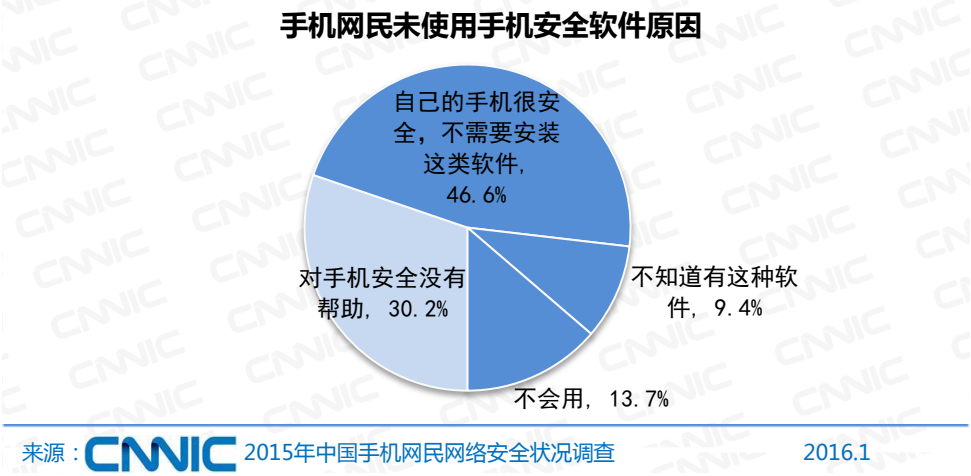


图 20 手机网民未使用手机安全软件原因

二、 手机安全软件使用情况

(一) 手机安全软件使用频率

由于手机安全软件的主要作用在于对手机信息的被动保护，因此用户每天主动打开这类应用的情况较少。数据显示，53.9%的用户每天打开手机安全软件的频率在 1 次以下，另外 40.5%的用户平均每天使用该类软件次数在 1-5 次。手机安全软件的使用频率较低，使得其很难如其他手机应用将广告作为主要盈利模式，同时由于国内手机安全软件基本对用户采取免费策略，造成目前手机安全软件行业整体缺乏有效的盈利模式。

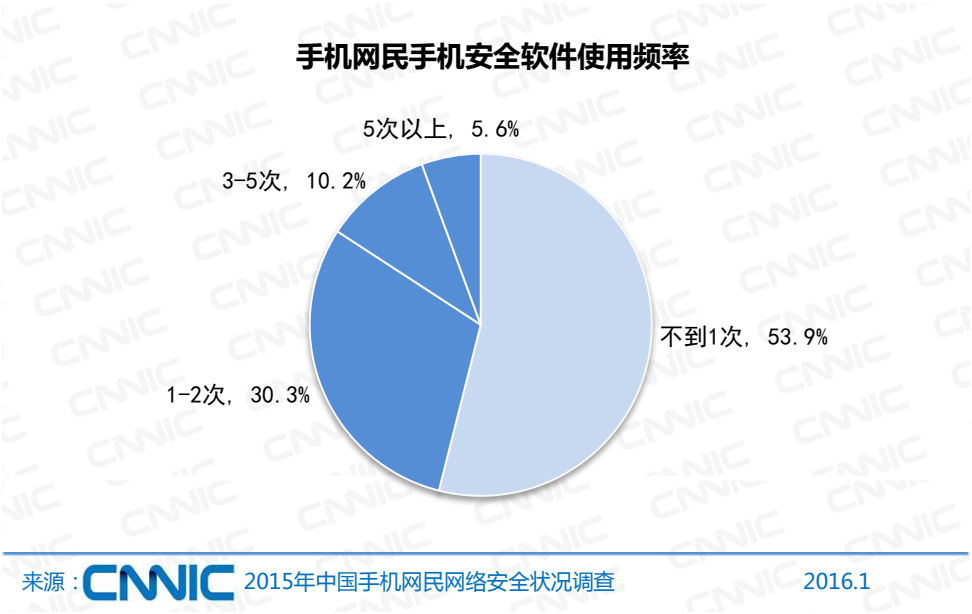


图 21 手机网民手机安全软件使用频率

(二) 手机安全软件常用功能

通过对手机安全软件各功能的使用率进行调查发现，手机垃圾清理、手机内存清理、扫描杀毒、骚扰电话拦截和流量监控是目前手机网民最为常用的五项功能，使用率均在 60%以上。另外值得注意的是，1.8%的手机安全软件用户虽然在手机上安装了手机安全软件，但没有使用过任何功能。

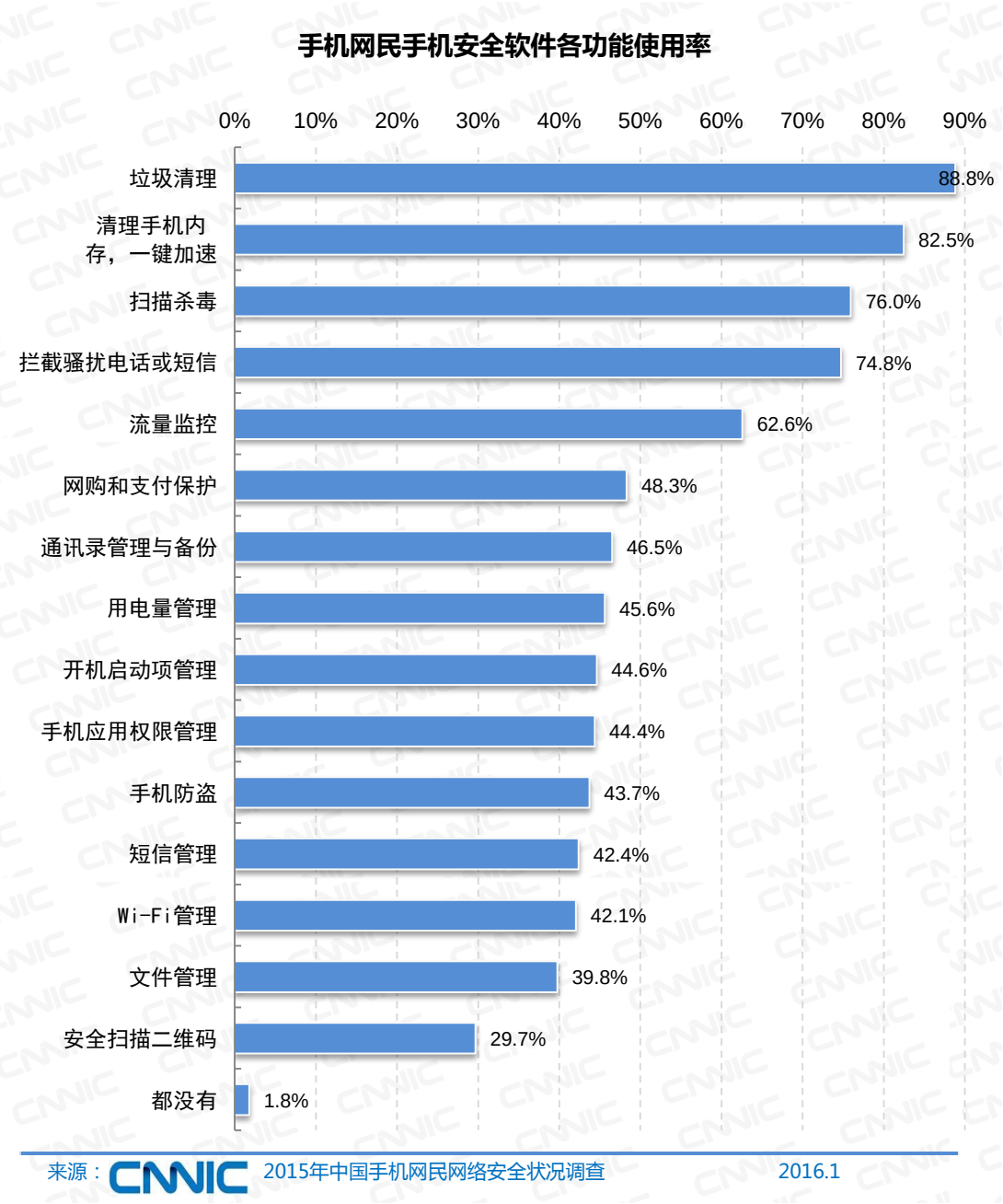


图 22 手机网民手机安全软件各功能使用率

(三) 手机安全软件信任程度

通过对安装了手机安全软件的用户进行调查发现，用户对于手机安全软件可能存在收集用户信息的行为普遍存在顾虑。数据显示，过去半年安装了手机安全软件的用户中，43.8%的用户认为手机安全软件在保护自己信息安全的同时也收集了自己的个人信息。而对于手机安全软件收集用户信息的行为，27.9%的用户表示信任，55.1%的用户存在顾虑。这很大程度上由于目前手机安全软件相关行业规范尚未完善，导致很多用户对手机安全软件的信任度

不高。因此未来应联合各方力量制定明确的行业标准，并推动落实，提高用户对该类软件的信任度。

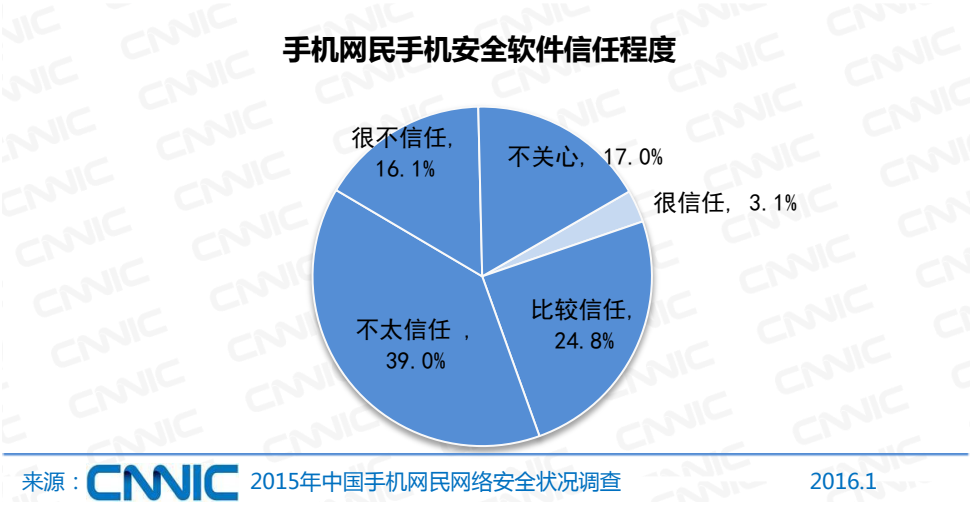


图 23 手机网民手机安全软件信任程度

三、 手机安全软件品牌

(一) 手机安全软件首选率

通过对手机安全软件用户进行调查发现，用户使用的手机安全软件品牌主要集中于 360 手机卫士、腾讯手机管家和百度手机卫士三家，其用户首选率之和达到 66.4%，市场集中度较高。此外，由于很多用户缺乏对手机安全软件品牌的分辨能力，27.6%的用户使用手机自带的不知名安全软件或不能分辨手机安全软件的品牌。

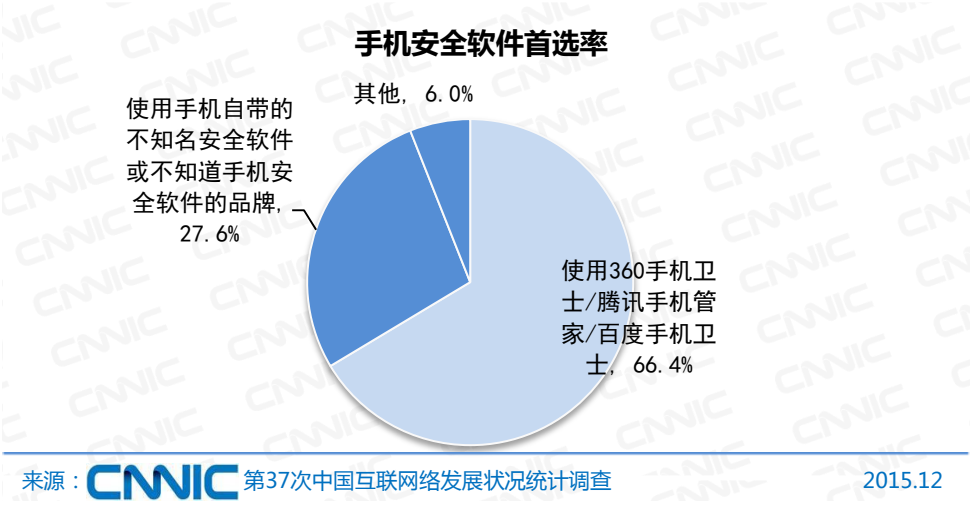


图 24 手机安全软件首选率

(二) 手机安全软件选择因素

通过对使用手机安全软件的用户进行调查发现，手机信息安全保护功能齐全是用户选择手机安全软件的首要因素，64.5%的用户会根据这一因素选择手机安全软件品牌。此外，产品安全性、操作便捷性和品牌知名度也受到用户重视，超过半数用户会在选择手机安全软件时考虑这三项因素。

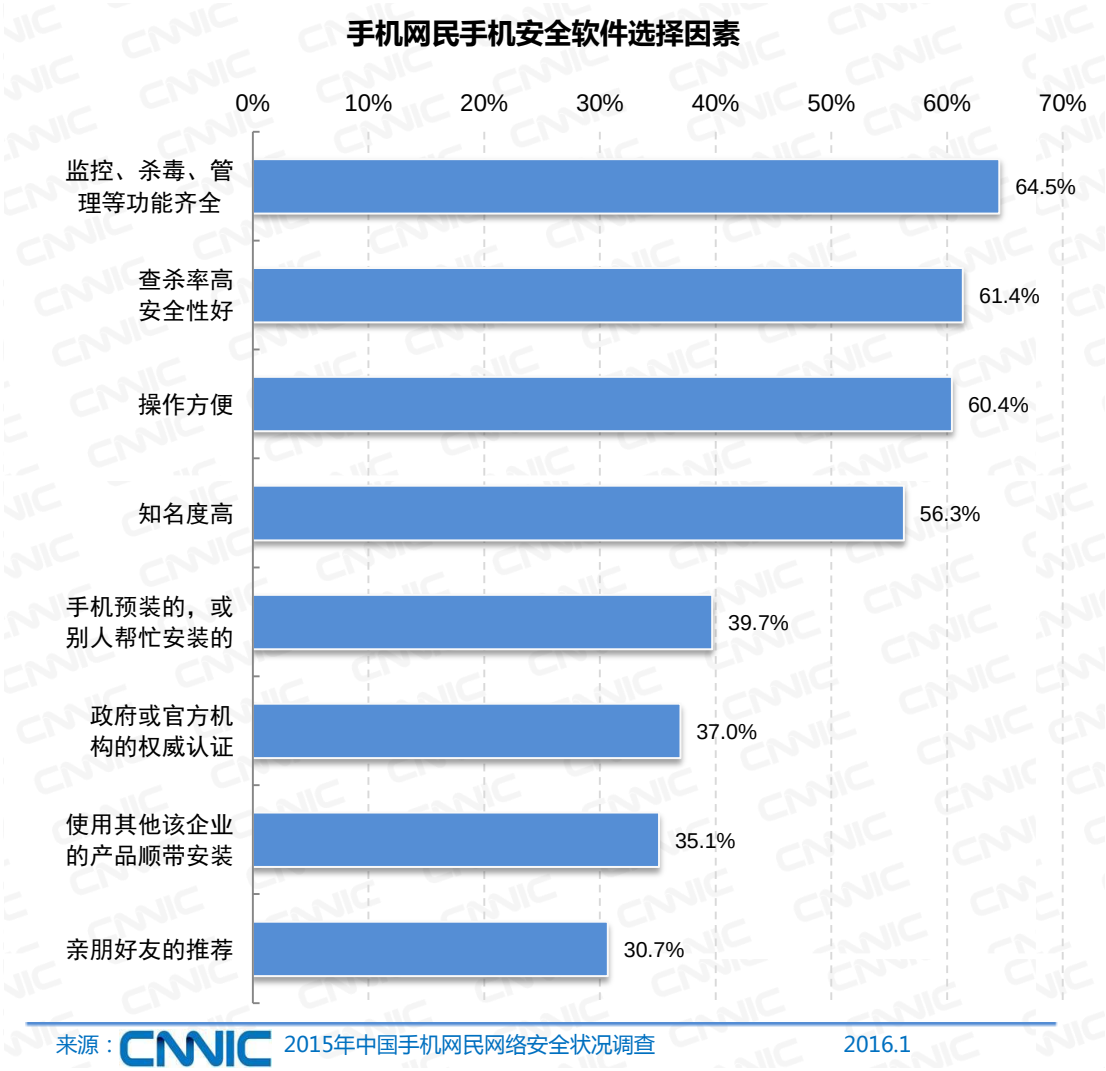


图 25 手机网民手机安全软件选择因素

第八章 趋势与建议

一、 移动网络服务快速发展，手机信息安全环境更加复杂

截至 2015 年底，国内手机网民规模已达 6.2 亿，随着移动 4G 网络的普及，O2O 服务、手机购物和移动支付等业务快速发展，越来越多的用户个人信息通过互联网上传给各类应用服务商，网民的手机信息安全环境日趋复杂。按照不同手机信息安全事件的类型进行区分可以发现，手机安全风险向手机应用产业链上下游延伸的趋势明显。在产业链上游，越来越多的黑客开始利用移动网络硬件或系统漏洞对用户信息安全造成不法侵害。在硬件端，如路由器、交换机等硬件设备安全风险依然较大；而在软件端，如“XcodeGhost”病毒，在应用程序的开发过程中就可以在开发者不知情的情况下对 App 注入第三方代码，从而窃取用户数据。这种恶意行为不仅普通用户无法感知，甚至连应用开发者也难以察觉，而且影响范围极大。在产业链中游，黑客将恶意程序伪装成正常应用，通过钓鱼短信、自制网页、社交平台等渠道散播，欺骗用户安装后窃取个人信息，进而实施精准网络诈骗。在产业链下游，以骚扰、广告、诈骗电话为代表的信息安全问题依然严峻，不仅影响了网民的日常生活，也阻碍了移动互联网产业的健康发展。

二、 骚扰类信息安全事件频发，窃取用户信息的手段趋于隐蔽

从手机安全事件的用户覆盖率来看，2015 年国内手机信息安全事件的发生呈两极化趋势，且信息安全事件数量显著增长。一方面，不会对用户构成直接经济损失的骚扰类安全事件的用户覆盖率很高，骚扰、广告电话和广告违法短信的用户覆盖率均在 75%以上；另一方面，通过手机病毒、恶意软件窃取用户信息的手段越来越隐蔽，大多数用户被盗取了个人信息之后很难察觉，其用户覆盖率均未达到 20%。不容忽视的是，虽然用户察觉到的比例较低，但手机病毒和恶意软件在 2015 年影响群体不减反增。根据腾讯手机管家提供的数据显示，2015 年安卓病毒感染人次达到 3.08 亿人次，相比 2014 年增长 56.5%；新发现的手机病毒数为 1670.37 万个，约为 2014 年的 17 倍，全年每月手机病毒感染终端数量呈现逐步增

长趋势。

三、 用户对各类手机安全风险认知仍需加强

智能手机功能的不断拓展使得其可以在越来越多的场景下为用户提供服务，但随之而来的各类风险也逐渐增多。伴随各地经济的发展，移动上网基础设施不断普及，公共 Wi-Fi、二维码、伪基站等安全问题更加易于发生，使得不具备手机安全风险防范意识的用户更可能遭受经济损失。由于诈骗电话、钓鱼短信、应用隐私授权等手机安全问题完全可以依靠用户自身防范意识进行避免，因此提高用户对于各类安全风险的认知并建立防范意识是当务之急。调查发现，目前国内仍有近半数手机网民对于公共 Wi-Fi、二维码等各类手机安全风险缺乏基本的安全防范意识，加强对手机网民在各种应用场景下手机信息安全知识的普及宣传仍十分必要。与此同时，对于伪基站、不法公共 Wi-Fi 等问题的打击也将成为各相关部门未来工作的重点。

四、 手机安全软件渗透率较高，防护功能齐全是用户首选因素

随着智能手机的普及，手机安全软件逐渐被广大手机网民所接受。尤其对于并不了解手机信息安全防范知识的用户来说，手机安全软件虽然不能完全杜绝手机安全事故的发生，但也从客观上为这类用户提供了一定安全保障。根据第 37 次中国互联网络发展状况统计调查数据，截至 2015 年 12 月，国内手机安全软件用户规模达到 4.5 亿，占整体手机网民的 72.6%。通过对使用手机安全软件的用户进行调查发现，手机安全功能齐全是用户选择手机安全软件的首要因素，此外产品安全性和操作便捷性也受到用户重视，超过 60%的用户会根据这三项因素选择手机安全软件品牌。从安装方式来看，超过四分之一用户使用的手机安全软件是手机自带或系统预装的，表明应用预装依然是手机安全软件厂商推广产品的重要渠道。另外值得注意的是，大多数用户对于手机安全软件收集用户信息的行为存在顾虑。这很大程度上由于目前手机安全软件相关行业规范尚未完善，导致很多用户对手机安全软件的信任度不高。因此未来应联合各方力量制定明确的行业标准，并推动落实，提高用户对该类软件的信任度。

五、 完善法规与加强协作是未来网络安全大势所趋

2015 年 6 月，第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法（草案）》，从保障网络产品和服务安全、保障网络运行安全、保障网络数据安全、保障网络信息安全等方面进行具体的制度设计。但要真正改善手机网民的信息安全环境，不能仅依靠政府与相关部门的执法行动，必须明确各方责任，汇聚手机信息安全产业生态中的各方力量进行深度合作，才能够对信息安全相关的违法犯罪行为进行有效打击。这一过程不仅需要政府完善与执行相关法律法规，还包括手机信息安全企业对用户安全产品的改进，以及用户安全防范意识的提升和对手机信息安全问题的积极反馈。目前国内已经形成了“安全联盟”等公益性手机信息安全保护联盟，以及旨在协同运营商、公安局、手机安全企业、手机应用网站，实现“警、企、民”全面合作的“天下无贼”反信息诈骗联盟等。但调查发现，手机网民在遭遇手机信息安全事件后选择向各类信息安全联盟进行反馈的用户占比仅 8.1%，因此如何进一步加强各方合作，形成高效、良性的信息安全反馈体系，为更多用户提供信息安全保护将是未来提升国内手机信息安全环境的主要方向。

版权声明

免责声明

本报告中的调研数据均采用样本调研方法获得，其数据结果受到样本的影响，部分数据未必能够完全反映真实市场情况。本报告仅供参考，本中心不为依据本报告所作决策产生的任何损失承担责任。

中国互联网络信息中心

China Internet Network Information Center（CNNIC）

2016 年 9 月