2012 年中国网民信息安全状况研究报告

中国互联网络信息中心

目录

图目录

报告摘要

网民总体信息安全状况

- 网民普遍知道要重视信息安全，但对其原因认识并不清晰。90.3%的网民知道要重视信息安全，但知道信息安全事件会给自己、给其他人带来不良影响的网民分别仅占 57.2%、41.4%。
- 网龄越长的网民，对信息安全事件的危害越了解。4 年以上网龄的网民，知道信息安全事件会给自己、给其他人带来不良影响的网民分别占 62.0%、45.4%，1-4 年网龄的网民则分别为 47.3%、33.7%，1 年以内网龄的网民分别为 43.8%、28.6%。
- 学历越高的网民，对信息安全事件的危害越了解。知道信息安全事件会给自己、给其他人带来不良影响的网民比例，从小学及以下的 42%、24%，逐渐提高到硕士及以上的 78%、66%。
- 96.2%的网民都会采取信息安全保护措施，平均每个网民采取 5.3 种措施。
- 87.3%的网民安装安全防护软件保护信息安全，网民不安装安全防护软件，主要是因为“没发生过安全事件，不需要”，“不会安装”，分别占不安装的网民的 46.1%、26.2%。
- 有 84.8%的网民遇到过信息安全事件，总人数为 4.56 亿。平均每人遇到 2.4 类信息安全事件。
- 垃圾短信和手机骚扰电话发生比例最高，分别有 68.3%和 56.5%的网民遇到过，其它事件比例分别为：欺诈诱骗信息（38.2%）、中病毒或木马（23.1%）、假冒网站（17.6%）、账号或密码被盗（13.8%）、手机恶意软件（10.6%）、个人信息泄露（7.1%）。
- 在遇到信息安全事件的网民中，77.7%的网民都遭受了不同形式的损失。发生经济损失的网民，人均损失额为 553.1 元，损失总额为 194 亿元。
- 在遇到信息安全事件的网民中，高达 47.5%的网民不做任何处理。

各类信息安全事件状况

- 网络活动是导致中病毒或木马的最重要情境。浏览网页、下载文件而中病毒或木马的网民比例分别为 55.3%、45.4%。中病毒或木马后，网民采用最多的处理方式是使用安全防护软件查杀、重装系统，分别占 76.0%、48.5%。
- 在被盗的网络账号中，最多的是聊天工具账号和网络游戏账号，被盗这两类账号的网民比

例分别为 83.8%、22.6%。账号或密码被盗后，网民的处理方式较为多样分散，使用最多的四种方式被网民采取的比例都在 33%-40%之间，有 13.6%的网民不再使用该网站或软件。

- 泄露的信息类型中，有过个人联系方式泄露的网民占 79.8%，个人属性信息泄露的占 47.2%。个人信息泄露后，88.2%的网民没有任何办法处理。
- 在有手机的网民中，16.3%的网民发布过当前位置信息。其中，年轻、男性、城镇网民更喜欢发布当前位置信息。在发布过的网民中，7.3%的网民后悔这一行为。
- 在遇到假冒网站的网民中，遇到假冒购物网站、知名节目的网站、金融类网站的比例最高，都超过了 30%。7.8%的网民上过假冒网站的当。
- 在遇到欺诈诱骗信息的网民中，遇到虚假的中奖信息、转账汇款信息的网民最多，分别占 80.9%、64.1%。有 3.3%的网民上过当。
- 在网民遇到的手机恶意软件的危害行为中，恶意扣费最多，占 37.4%；其次分别是偷偷联网（23.0%）、很难删掉或根本删不掉（22.6%）。
- 在收到过垃圾短信的网民中，46.2%的网民偶尔收到（每月不足一次），22.1%的网民每天至少收到一次垃圾短信。垃圾短信的内容以广告和代开发票、诈骗、股票推荐类居多。
- 在收到过手机骚扰电话的网民中，43.7%的网民偶尔收到（每月不足一次），每周至少收到一次的网民占 42.0%。

安全防护软件安装状况

- 总体网民中，83.6%的网民电脑上安装了安全防护软件，用户数为 4.5 亿。在这些网民里，平均每个网民电脑上安装了 1.9 个安全防护软件，其中安装 2 个软件的网民最多，占 51.0%。
- 网民电脑上最多只安装 1 个单一功能软件，但可能安装多个套装软件。安装了单一功能软件的网民占 69.2%，安装了套装软件的网民占 88.4%。
- 在有手机的网民中，41.1%的网民手机上安装了安全防护软件，用户数为 2.16 亿。在这些网民里，平均每个网民手机上安装了 1.1 个安全防护软件，其中安装 1 个软件的网民最多，占 88.4%。
- 更换了新智能手机、对手机病毒危害性的认识是引起用户安装手机安全防护软件的最主要的触发因素，分别占 42.2%、33.8%。

调查介绍

1 调查方法

本报告数据主要来源于中国互联网络信息中心（CNNIC） 开展的“2012 年中国网民信息安全状况调查”。

1.1 调查样本分布

调查的目标总体是中国大陆（除港、澳、台三地）网民。CNNIC 随机抽取华北、东北、华东、华南、华中、西北、西南 7 大区域内的一级城市 4 个、二级城市 5 个、三级城市 7 个、四级城市 8 个、五级城市 5 个。调查最终获得样本量 2492 个，由以下两部分组成：

一、固定电话样本。根据城市所有固定电话局号，通过随机生成电话号码的方式，形成固定电话样本，抽取用户进行访问。最终样本量为 1246 个。

二、手机样本。根据城市所有手机局号，生成一定数量的四位随机数，形成手机样本，抽取用户进行访问。最终样本量为 1246 个。

1.2 调查时间

从 2012 年 9 月 7 日到 2012 年 9 月 27 日。

1.3 调查方式

通过计算机辅助电话访问系统（CATI）进行调查。

2 术语界定

- **信息安全事件：**是指通过电脑、手机，以及其它可上网设备进行的导致用户信息系统受损、信息内容泄露、个人活动受到不良干扰的事件。在本调查中，特指中病毒或木马、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、手机被安装恶意软件、收

到垃圾短信、手机收到骚扰电话等。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。

- **安全防护软件：**是指保护用户电脑、手机的设备安全、内容安全、系统设置安全，避免发生或协助处理信息安全事件的软件。部分安全防护软件可能还有系统清理优化、软件下载等功能；但单纯的系统或软件管理、不具备安全保护功能的软件不列入安全防护软件范畴。

第二章 中国网民总体信息安全状况

1 信息安全意识

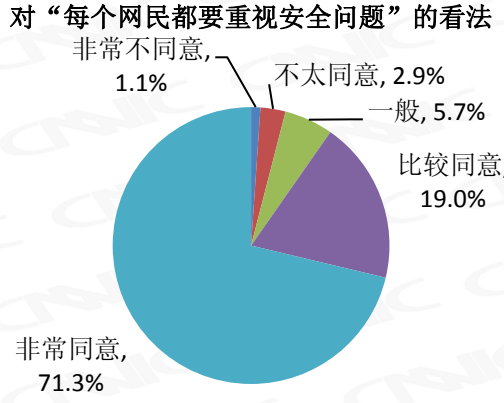
1.1 总体网民的信息安全意识

总体来看，目前中国网民只是简单地被灌输了要“重视信息安全”，但其实对其的原因认识并不清晰，形象地说，中国网民的信息安全意识处于“知其然，不知其所以然”的阶段。表现在以下两个方面：

第一，经过各种媒体的广泛宣传，中国网民普遍都知道要重视信息安全问题。同意（含比较同意和非常同意）“每个网民都要重视安全问题”看法的网民占总体网民的 90.3%，特别是，非常同意的占 71.3%。

第二，有较大部分的中国网民对信息安全事件的危害并不清楚。在总体网民中，同意“如果我的上网设备发生了安全事件，会给我造成不良影响”看法的用户占 57.2%，同意“如果我的上网设备发生了安全事件，会给其他人造成不良影响”看法的用户占 41.4%。

上述两个方面的比例存在着很大的差距，说明了很多网民知道要“重视信息安全”，但并不知道为什么要重视。



（a）

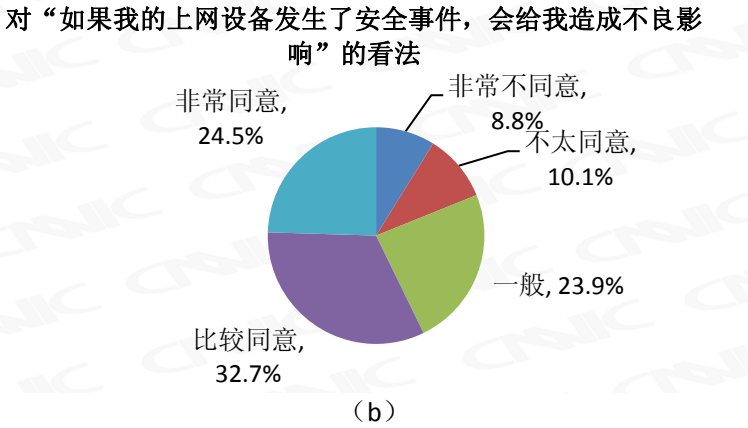
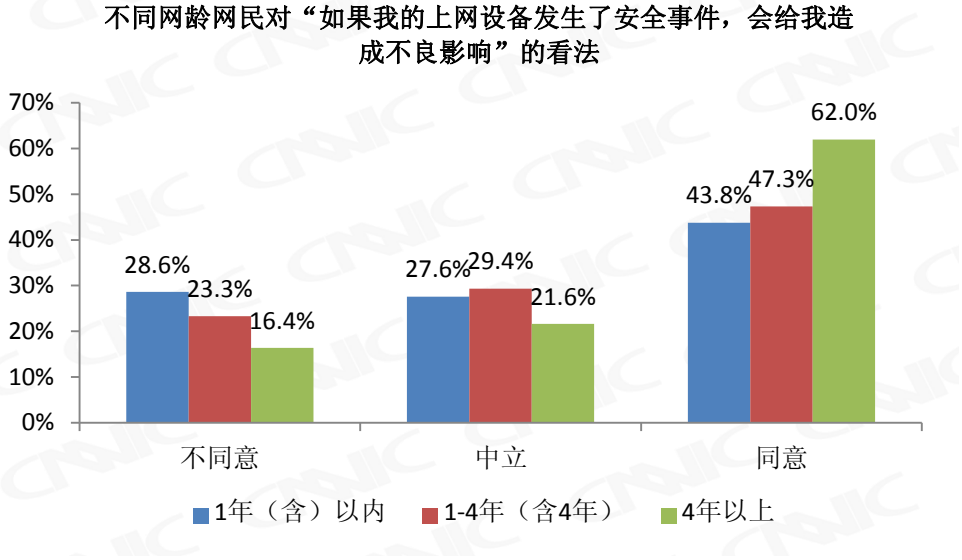


图 1 总体网民的信息安全意识

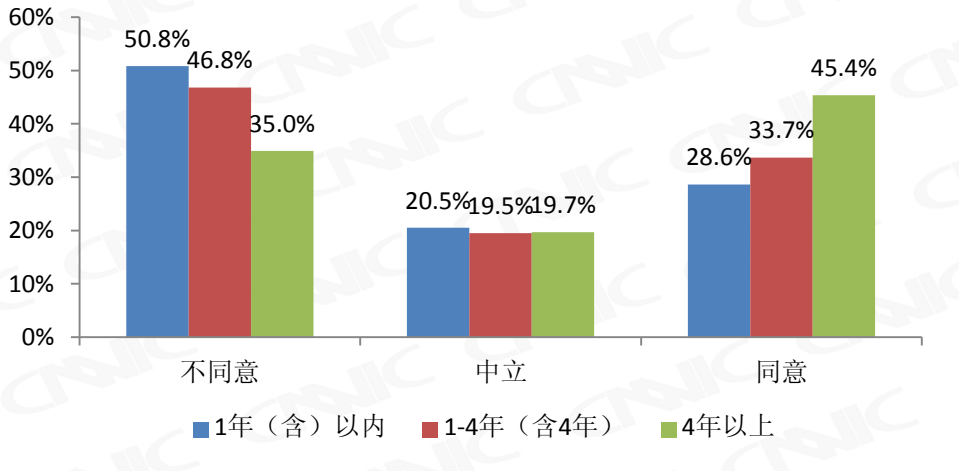
1.2 不同网民的信息安全意识

（1）网龄

网龄越长，网民对信息安全事件的危害越了解。4 年以上网龄的网民中，同意“如果我的上网设备发生了安全事件，会给我造成不良影响”和“如果我的上网设备发生了安全事件，会给其他人造成不良影响”看法的分别占 62.0%和 45.4%，1-4 年网龄的网民则分别为 47.3%和 33.7%，1 年以内网龄的网民分别为 43.8%和 28.6%。网龄越长，了解到或亲身遇到信息安全事件的情况越多，对信息安全事件的危害也更有体会。



（a）

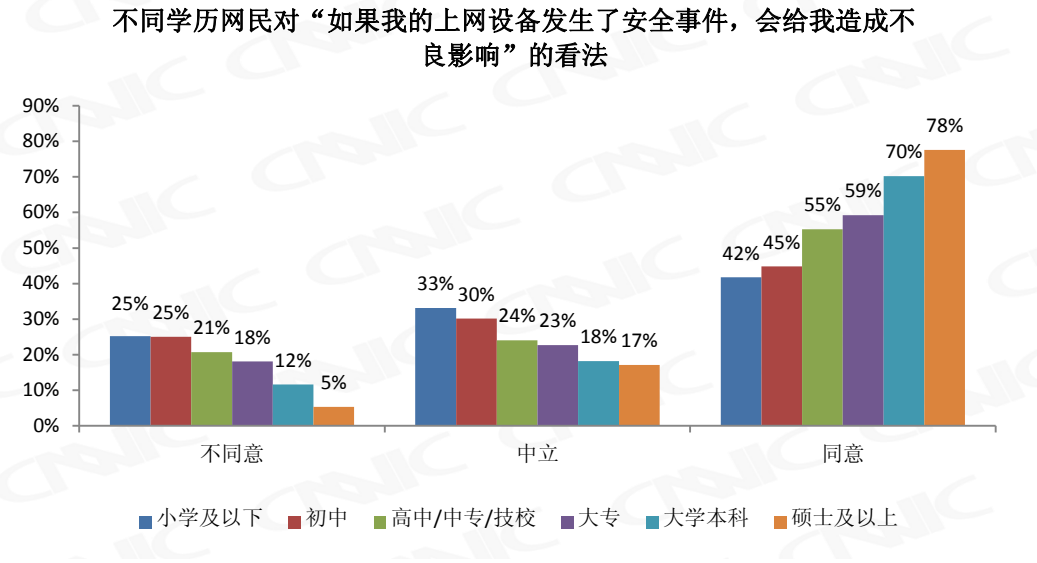


（b）

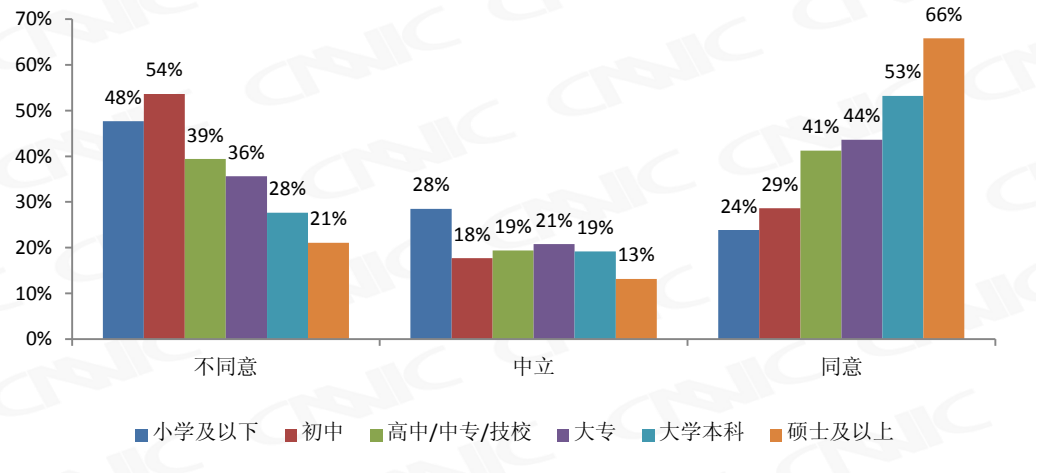
图 2 不同网龄网民的信息安全意识

（2）学历

学历越高，网民对信息安全事件的危害越了解。同意“如果我的上网设备发生了安全事件，会给我造成不良影响”和“如果我的上网设备发生了安全事件，会给其他人造成不良影响”看法的网民占相应学历网民的比例，随着学历的提高，呈现显著递增趋势，从小学及以下的 42%和 24%，逐渐提高到硕士及以上的 78%和 66%。学历越高，所接受的信息安全知识越多，对信息安全事件的危害也更为了解。



（a）



（b）

图 3 不同学历网民的信息安全意识

2 信息安全保护

2.1 信息安全保护措施数量

绝大多数网民都会采取措施保护信息安全。在总体网民中，只有 3.8%的网民不采取信息安全保护措施。在采取保护措施的网民中，平均每个网民采取 5.3 种，其中 47.9%的网民采取 4-6

种措施。考虑到本次调查的措施都是非常常见的信息安全保护措施，这一数字仍需继续提高。

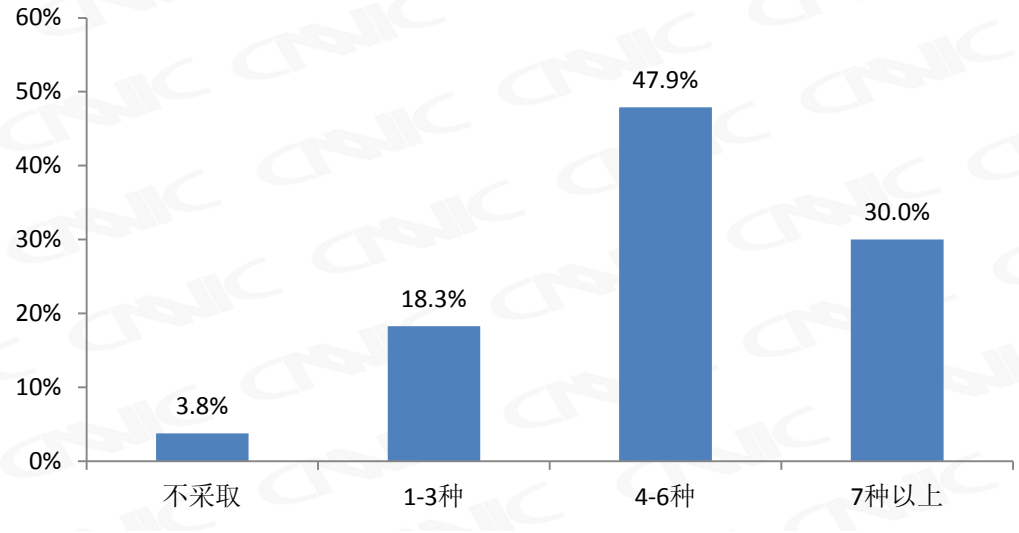


图 4 采取的信息安全保护措施数量

2.2 信息安全保护措施类型

采用最多的信息安全保护措施是安装安全防护软件，有 87.3%的网民安装，用户数为 4.7 亿。超过 70%的网民采用的保护措施还有“不安装来历不明的软件”、“除非网站有强制要求、否则不在网上透露真实的个人信息”。

采用“系统自动更新、及时打补丁”的网民仅占 66.5%，这与国内较多用户使用盗版操作系统有关，同时也反映出安全防护软件提供“打补丁”的功能极为必要。

采用“设置复杂密码”的网民仅占 57.2%，为保障用户密码安全，网站可强制进行密码复杂度检查和要求。

采用“数字证书”的网民达到了 39.1%，这与越来越多的网民参与网上交易活动，银行近年来加大“U 盾”、“口令卡”等宣传和推广力度有关，但比例仍较低，还需要继续加强。

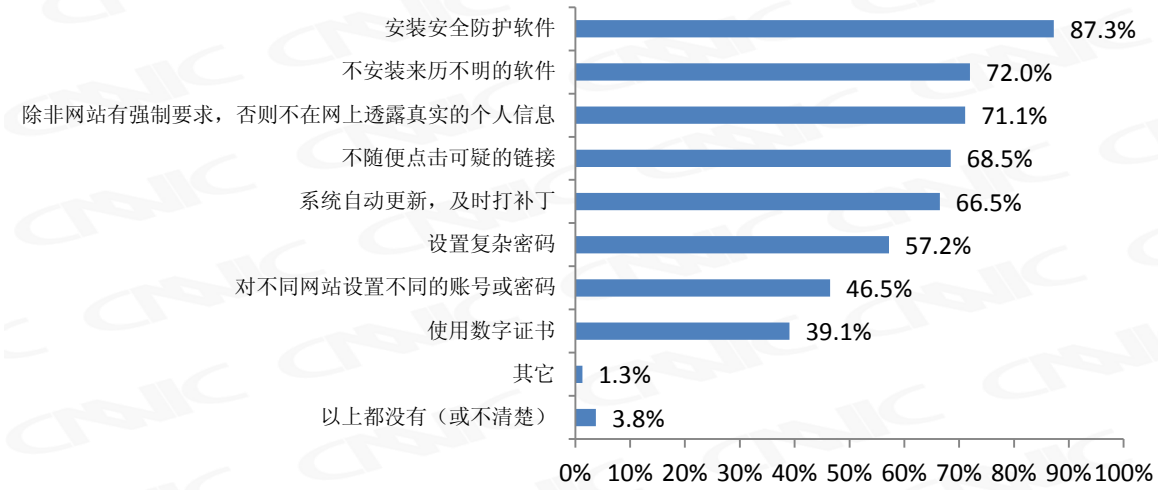


图 5 中国网民信息安全保护措施

2.3 不安装安全防护软件的原因

网民不安装安全防护软件，主要是因为“没发生过安全事件，不需要”，“不会安装”。这来自于两个更深层的原因：第一，信息安全事件的发生，很多是隐蔽进行的，网民并不总是能发现，因此容易产生麻痹大意心理；第二，安全防护软件的安装虽然已尽可能简便化，但仍未达到足够的“傻瓜化”，今后在这方面还需加强。

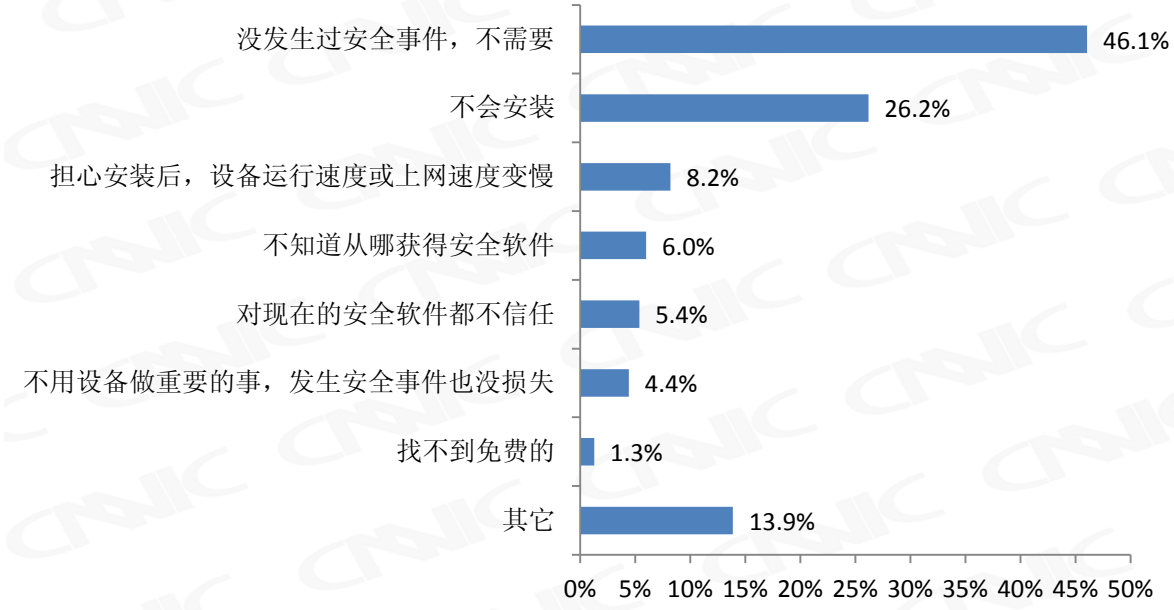


图 6 不安装安全防护软件的原因

3 信息安全事件

3.1 信息安全事件发生状况

在总体网民中，有 84.8%的网民遇到过信息安全事件，总人数为 4.56 亿[1]，在这些网民中，平均每人遇到 2.4 类信息安全事件。我国的信息安全状况不容乐观。

在信息安全事件中，垃圾短信和手机骚扰电话发生比例最高，分别有 68.3%和 56.5%的网民遇到过。这是因为：对网民来说，这两种事件完全是被动发生的，非智能手机网民无法事先采取任何保护措施（智能手机网民可安装手机安全防护软件自动拦截）。其它事件，网民都可在不同程度上采取一定的预防保护措施。因此，在目前仍有大量非智能手机网民的情况下，对于垃圾短信和手机骚扰电话的治理，需要继续加强，治理重点是源头。

新型信息安全事件愈发严重，甚至超过了部分传统信息安全事件。一般说来，“欺诈诱骗信息”、“假冒网站”近几年才逐渐产生，还属于新型信息安全事件。总体网民中，38.2%的网民遇到过“欺诈诱骗信息”，这一比例甚至比传统的“中病毒或木马”的网民比例高出 15.1 个百分点。遇到“假冒网站”的网民比例也达到了 17.6%。从这个意义上来说，对待这些广泛发生的新型信息安全事件，应像对待传统信息安全事件一样，纳入常态化治理范围。

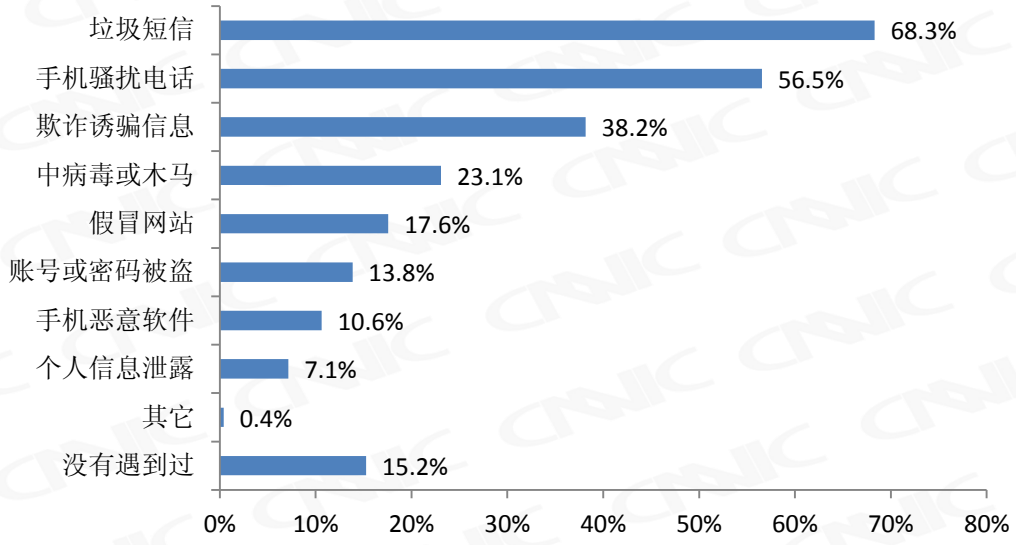


图 7 总体网民遇到的信息安全事件

[1] 根据 CNNIC 的《第 30 次中国互联网络发展状况统计报告》显示，截至 2012 年 6 月底，我国网民数为 5.38 亿。遇到信息安全事件的总人数=网民数（5.38 亿）*遇到过的网民比例（84.8%）。

3.2 信息安全事件导致的损失

在遇到信息安全事件的网民中，77.7%的网民都遭受了不同形式的损失。其中，“花费时间和精力”的网民最多，占 38.6%；发生“经济损失”的占 7.7%，人均损失额为 553.1 元，损失总额为 194 亿元[2]。

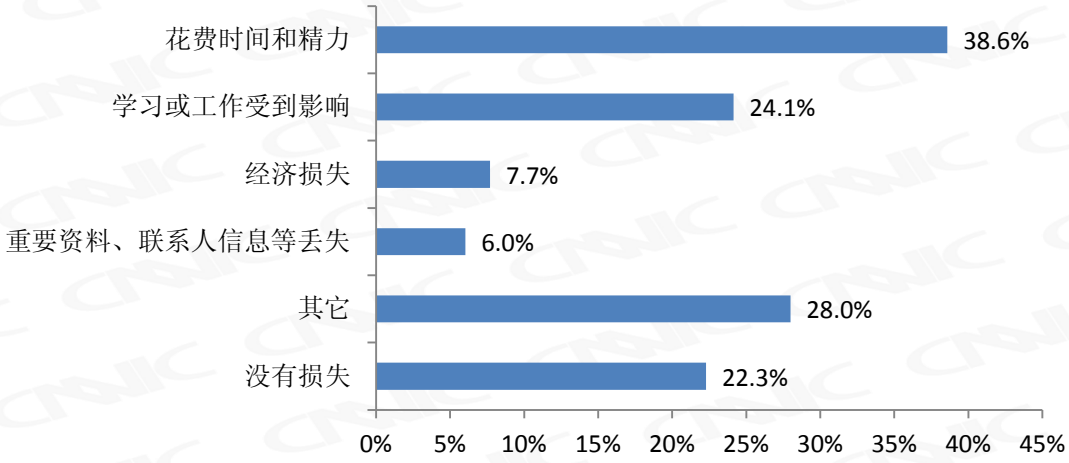


图 8 信息安全事件导致的损失

3.3 处理信息安全事件的方式

在遇到信息安全事件的网民中，高达 47.5%的网民不做任何处理，这也再次反映出网民对信息安全事件的危害并不了解或不在意；15.3%的网民会请别人帮忙解决，信息安全事件处理服务可能具有一定的市场潜力；只有 2.1%的网民会向媒体、政府、法院投诉，绝大多数网民不会采取如此强烈的手段，这也是整体信息安全状况严重的重要因素之一，为建设良好的信息安全环境，媒体、政府等有关部门有必要主动介入，而不应坐等网民投诉。

[2] 损失总额=遇到信息安全事件的网民总数（4.56 亿）*发生经济损失的网民比例（7.7%）*人均损失额（553.1 元）

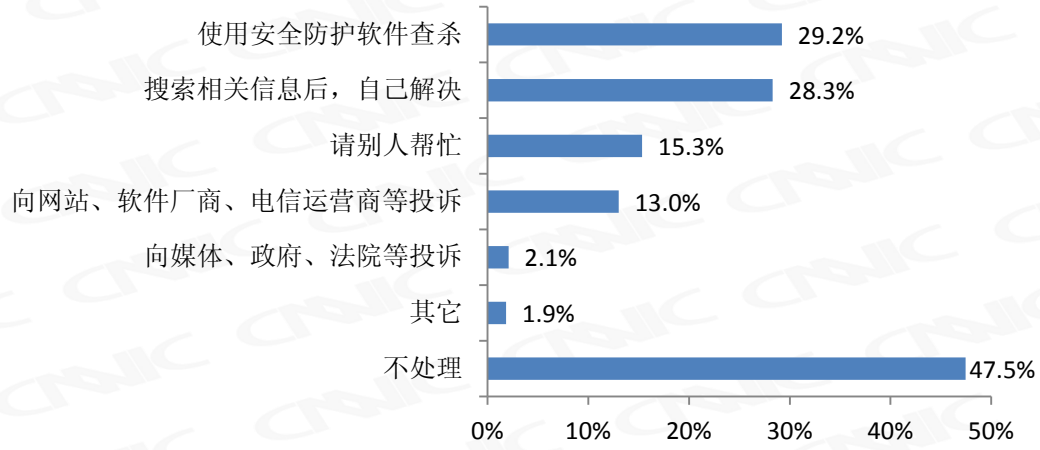


图 9 处理信息安全事件的方式

第三章 各类信息安全事件状况

1 中病毒或木马

1.1 中病毒或木马的情境

当前，病毒和木马已经广泛存在于各类计算机和网络载体中，在多种情境下，网民的电脑和手机都可能中病毒或木马。最多的是浏览网页时，在中过病毒或木马的网民中，有 55.3%的网民在浏览网页时发生过；其次是下载文件时，为 45.4%。为此，需要大力加强网上的 Web 页面和文件的安全检测。另外，对于 U 盘、程序等离线载体也需要继续加强检测。

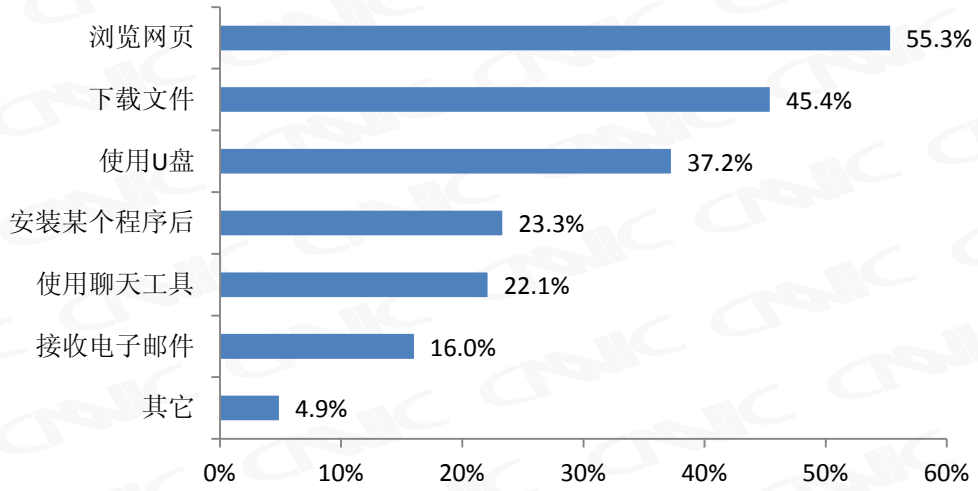


图 10 中病毒或木马的情境

1.2 处理方式

在中病毒或木马的网民中，97.7%的网民都会采取行动处理，远高于总体信息安全事件的处理比例（见第二章 3.3），这主要是因为中病毒、木马是传统信息安全事件，网民对其相对较为重视。但是，处理此类事件并不简单，网民需要结合各种方式进行，平均每个网民采用过 2.8 种方式。

使用安全防护软件查杀是被最多网民采取的处理方式，超过 3/4 的网民采用（76.0%）。

重装系统作为最有效、最彻底的解决方案，且通常不需要了解中病毒或木马的原因、技术

原理等，得到了很多人的欢迎，不过由于重装系统要求一定的计算机操作能力，以及所需总时间较长（包括操作系统和应用软件安装、设置时间），限制了网民的使用，通常作为最后的解决方案，采取该方式的网民比例为 48.5%，排在第二位。如此高的比例，说明了在软件、其他人、信息的辅助下网民还难以清除病毒木马，病毒木马的自我保护能力极强。在这种情况下，安全防护软件要不断提高杀毒杀木马能力，重装系统全过程也应更加简便化、快速化。

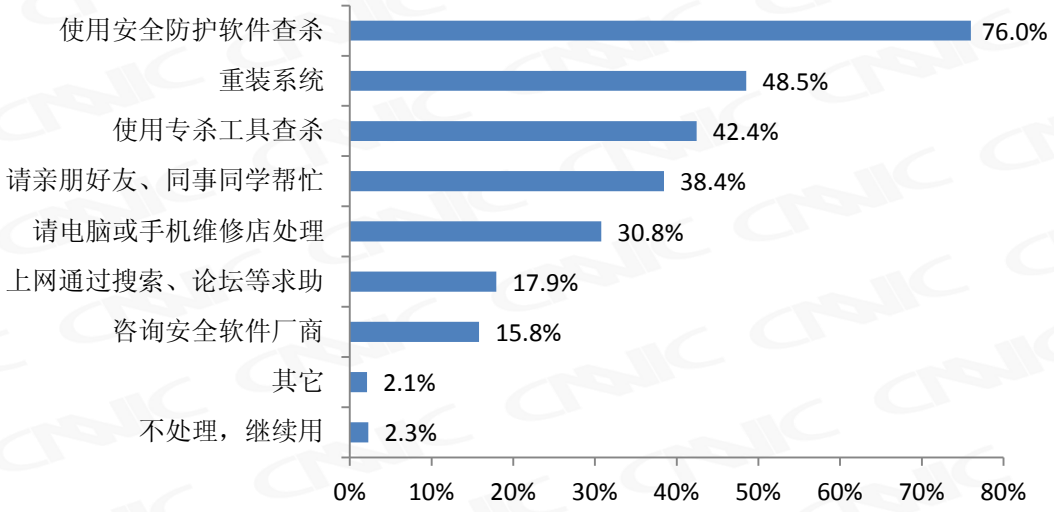


图 11 处理中病毒或木马事件的方式

2 账号或密码被盗

2.1 被盗的账号类型

在被盗的网络账号中，最多的是聊天工具账号和网络游戏账号，尤其是聊天工具账号。被盗过的网民中，83.8%的网民聊天工具账号被盗过，比排在第二的网络游戏账号高出 61.2 个百分点。除了聊天工具和网络游戏账号，其它账号被盗的网民比例均低于 10%。这主要是由两个原因共同影响的：第一，聊天工具和网络游戏的用户较多；第二，当前的盗号以获取经济利益为主，盗取聊天工具和网络游戏账号可能带来更多的经济利益。加强聊天工具和网络游戏账号安全性的手段应继续强化。

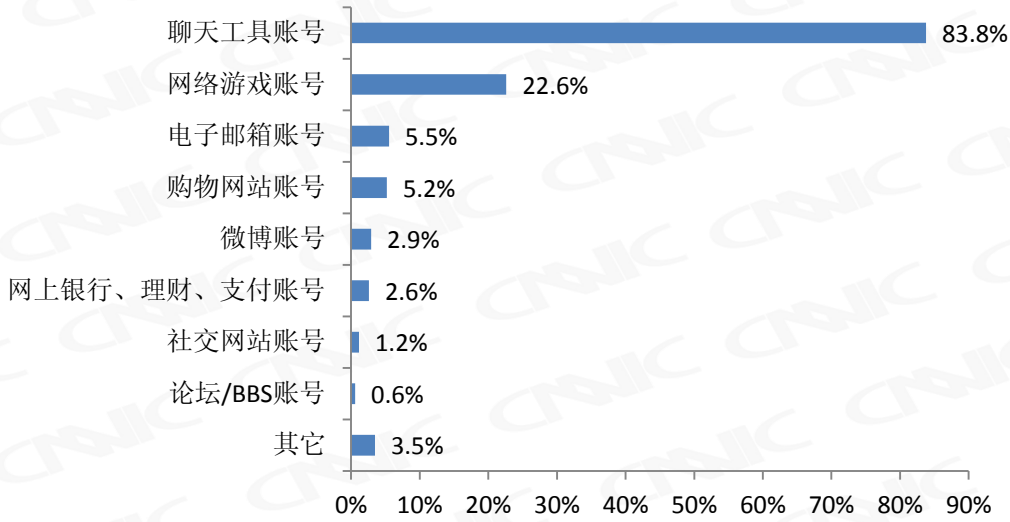


图 12 被盗过的账号类型

2.2 处理方式

在账号或密码被盗后，网民的处理方式较为多样分散。使用最多的四种方式被网民采取的比例都在 33%-40%之间。

受 2011 年底 CSDN 密码泄露事件的影响，很多人对在多个网站使用同一套账号和密码的安全性有所注意，账号或密码被盗后，修改其它网站的同一套账号密码成为最多网民采取的方式，有 39.7%的被盗网民采取。

账号或密码被盗后，有 13.6%的网民不再使用该网站或软件。网站或软件服务商应主动加强用户账号的安全性保障，避免因账号被盗而引起的用户流失。

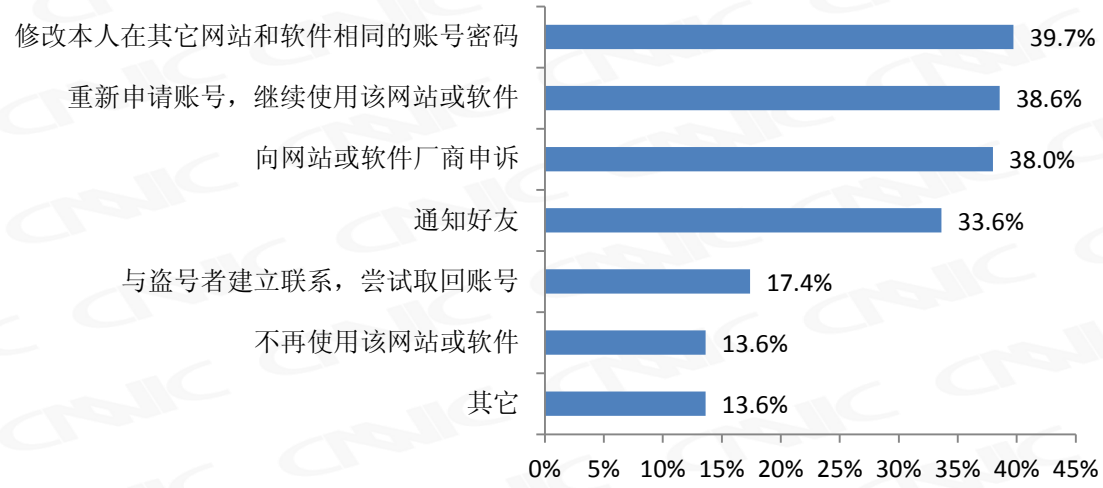


图 13 处理账号被盗事件的方式

3 个人信息泄露

3.1 泄露的信息类型

当前，泄露的信息类型已经丰富多样，有 6 类信息，其泄露的网民占所有被泄露网民的比例超过了 10%。最多的是个人联系方式，有 79.8%的网民泄露过；其次是个人属性信息，如姓名、年龄、性别等，占 47.2%。值得注意的是，极为隐私性的健康医疗信息、金融财产信息泄露比例分别达到了 11.2%和 7.3%。这说明，窃取个人信息的逐利性越来越强，已不满足于传统的个人联系方式、属性信息，而是追求更具营销精准性的住房、汽车、健康、医疗、金融财产信息等。

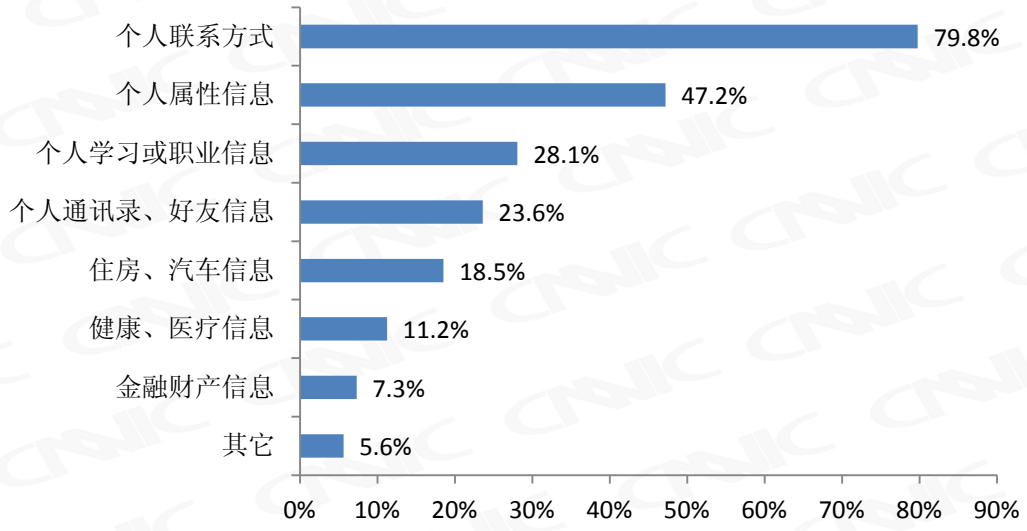


图 14 泄露的信息类型

3.2 处理方式

对于个人信息泄露，绝大多数网民处于无助的状态，这也是窃取个人信息日益严重的重要原因。88.2%的网民在信息泄露后没有任何办法处理，只有 6.7%的网民会向掌握信息的机构投诉，向政府部门、媒体投诉和到法院起诉的网民仅分别占 2.8%和 0.6%。保护个人隐私，还需法律、行政、司法、宣传等多渠道共同主动进行，加快个人隐私保护法的制定和出台，严厉打击非法出售用户信息的机构，鼓励网民主动投诉并提供便利条件。

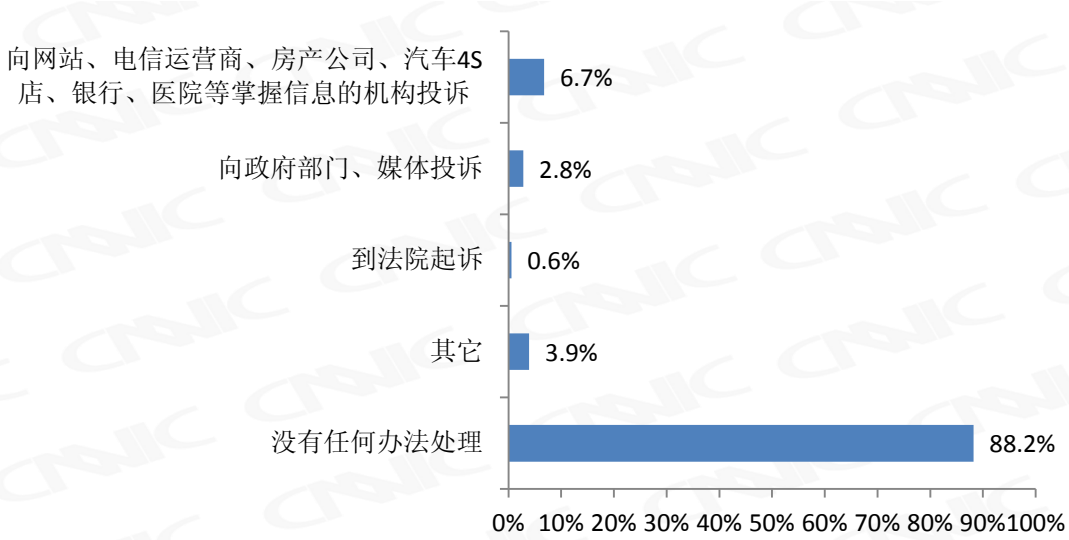


图 15 处理信息泄露事件的方式

3.3 手机发布当前位置信息

随着移动互联网的来临，具有发布当前位置信息功能的手机软件越来越多，原有的网站也逐渐开发了这一功能模块，发布过当前位置信息的网民日益增多。在有手机的网民中，16.3%的网民发布过当前位置信息。其中，年轻、男性、城镇网民更喜欢发布当前位置信息。发布当前位置信息也带来了个人信息的泄露问题。在发布过的网民中，7.3%的网民后悔这一行为。

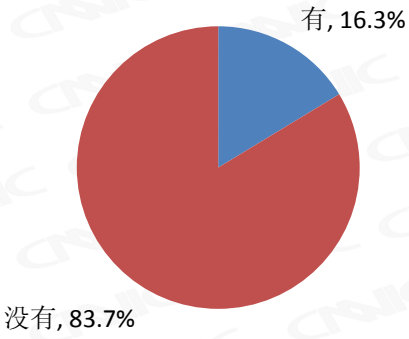


图 16 有手机的网民是否发布当前位置信息

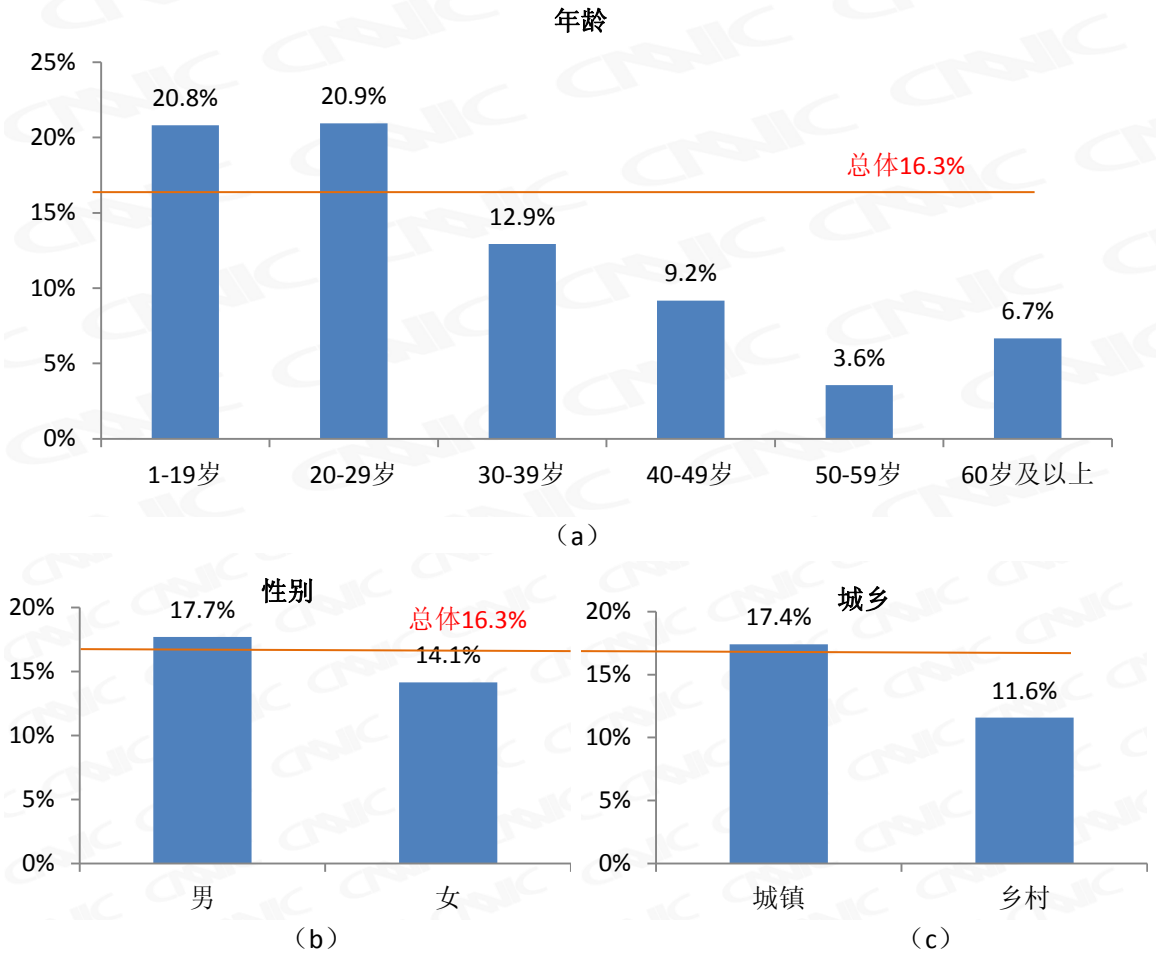


图 17 不同属性的有手机的网民发布当前位置信息的比例

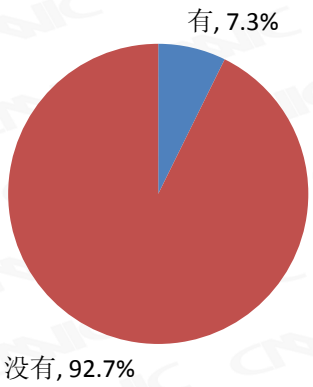


图 18 是否后悔发布当前位置信息

4 假冒网站

当前，假冒网站（钓鱼网站）日益严重，有 7 类假冒网站，其被遇到过的网民占所有遇到过的网民的比例超过了 10%。其中，假冒购物网站、知名节目的网站、金融类网站的比例最高，都超过了 30%。部分网民曾受骗上当，7.8%的网民上过假冒网站的当。

假冒网站带有很明显的经济利益，近年来对其的防范措施不断升级。安全防护软件厂商采用云安全的方式搜集假冒网站网址，并在事前保护的基础上增加了事后赔付措施，从技术上、经济上保障网民利益。比如，部分安全防护软件、浏览器对于用户访问购物、金融类等重要网站时，都会有真假性验证和提示，甚至提出了网购被骗赔付的保障手段。

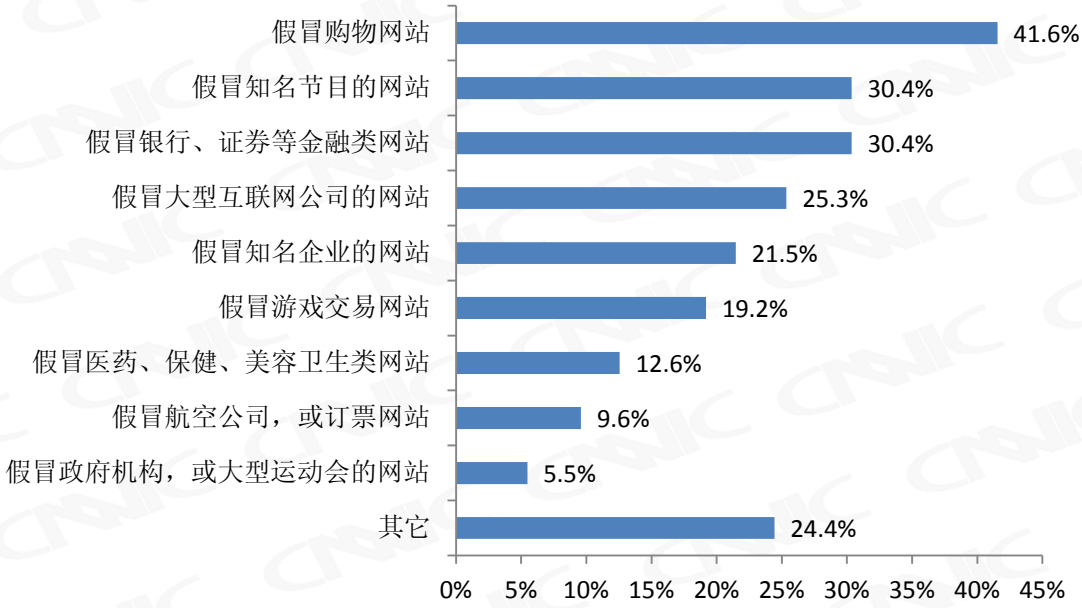


图 19 遇到的假冒网站类型

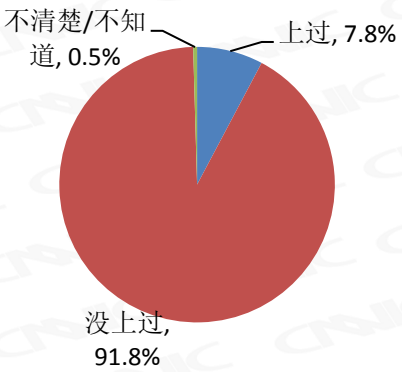


图 20 是否上假冒网站的当

5 欺诈诱骗信息

利用用户心理、知识等方面的弱点进行欺诈诱骗的事件越来越多。有 8 类欺诈诱骗信息，其被遇到过的网民占所有遇到过的网民的比例超过了 10%。其中，虚假的中奖信息最多，高达 80.9%，超过 50%的还有虚假的转账汇款信息（64.1%）。在遇到欺诈诱骗信息的网民中，有 3.3%的网民上过当。

治理欺诈诱骗信息，除了靠媒体宣传教育、电信运营商和安全软件厂商技术防范以外，更重要的是网民要抱有警惕心理，特别是在涉及财务交易时，通过搜索引擎、打电话、访问官方网站等方式确认信息的真实性。

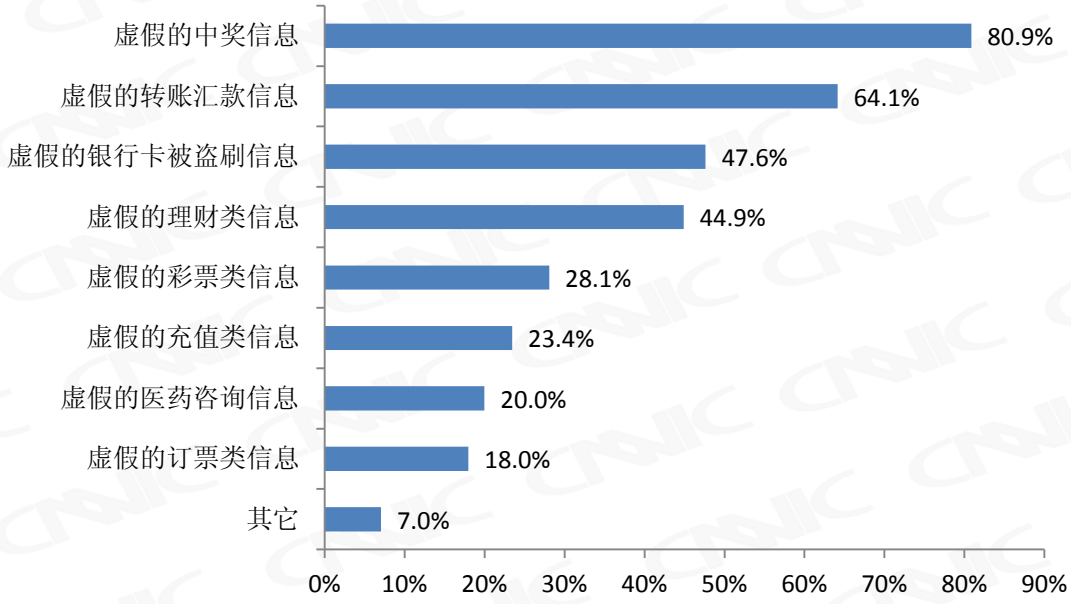


图 21 遇到的欺诈诱骗信息类型

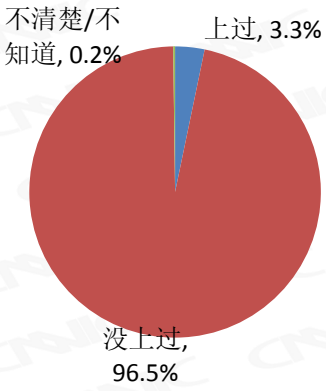


图 22 是否上欺诈诱骗信息的当

6 手机恶意软件

在网民遇到的手机恶意软件的危害行为中，恶意扣费最多，占 37.4%；其次分别是偷偷联网（23.0%）、很难删掉或根本删不掉（22.6%）。这些危害行为给用户带来了经济损失，降低了手机使用体验等。尤其是，手机作为私密性较强的工具，手机恶意软件的隐私窃取行为可能会给用户带来潜在的更大的损失。

未来几年，智能手机逐渐普及，手机恶意软件将日益增多，政府、电信运营商、安全防护软件厂商应联合行动，从行政手段、技术手段加大监测和打击力度。

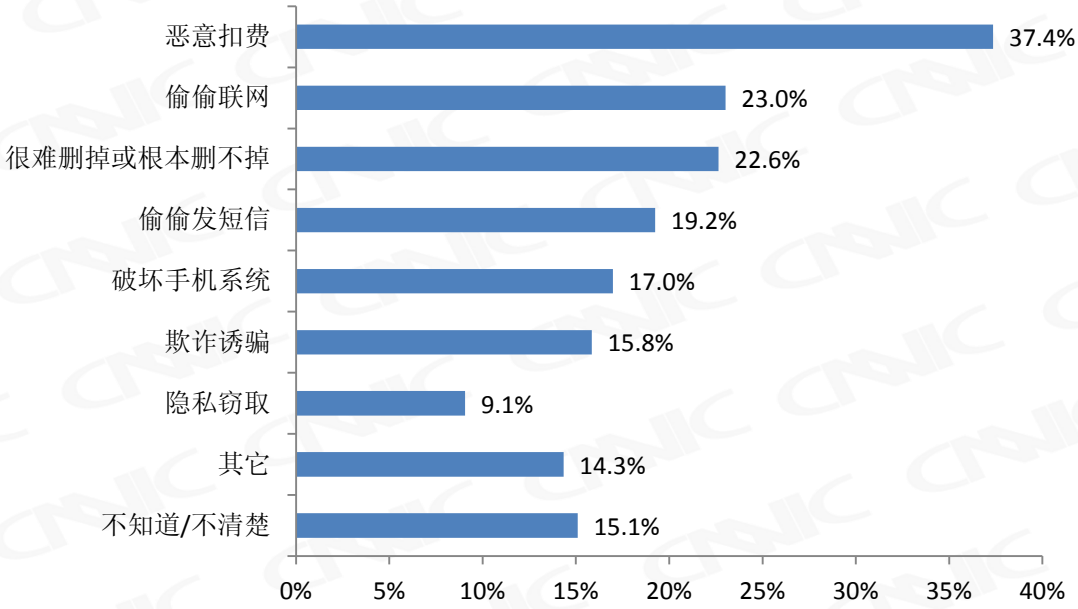


图 23 手机恶意软件的危害类型

7 垃圾短信

垃圾短信已成为一大公害。在收到过垃圾短信的网民中，收到频率两极分化，46.2%的网民偶尔收到（每月不足一次），22.1%的网民每天至少受到一次垃圾短信的困扰，从后者的受影响人群数量、频繁影响程度来看，治理垃圾短信需要加快、加大力度。

垃圾短信的内容以广告和代开发票、诈骗、股票推荐类居多。随着房地产交易和投资移民的频繁，这两类内容的垃圾短信也占据了不小的比例。

从垃圾短信的内容来看，治理垃圾短信要规范经营者行为和打击违法犯罪相结合。第一，

合法获得用户的手机号码的经营者，只能在用户明示同意的情况下向其发送指定类型的短信，不得未经允许随意发送，也不得发送其它类型的短信，尤其是广告类短信。第二，发送涉嫌违法内容的短信，监管部门应主动追查。

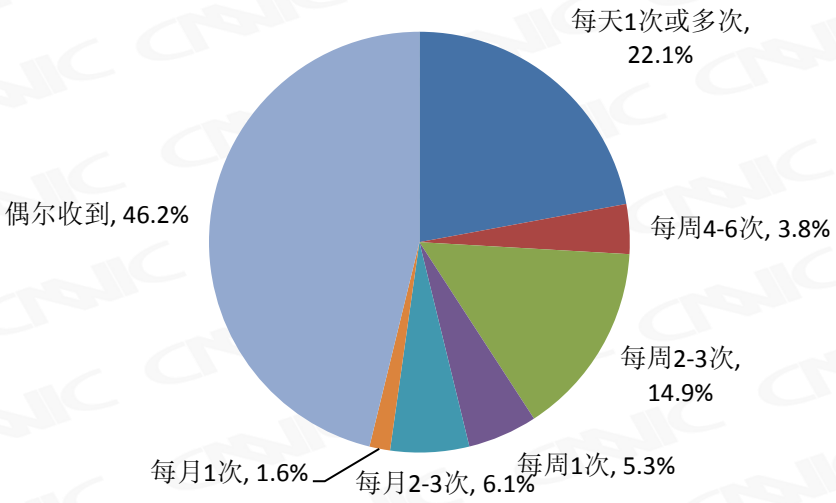


图 24 收到垃圾短信的频率

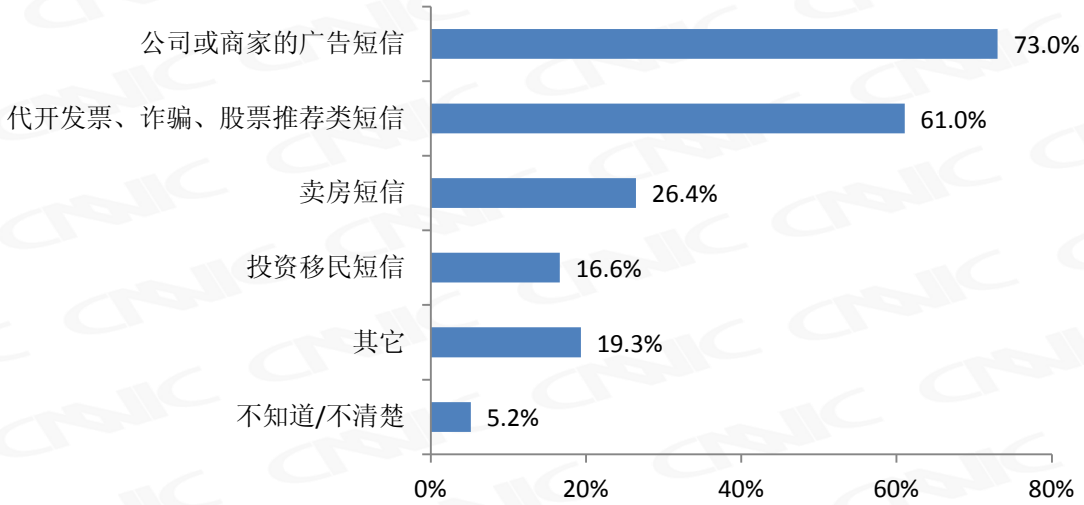


图 25 垃圾短信的内容

8 手机骚扰电话

手机骚扰电话也是当前社会的一大公害。在收到过手机骚扰电话的网民中，43.7%的网民偶尔收到（每月不足一次），但每周至少收到一次的网民占 42.0%。治理手机骚扰电话，除了打击

源头以外，还可通过在用户智能手机安装拦截工具被动地应对。

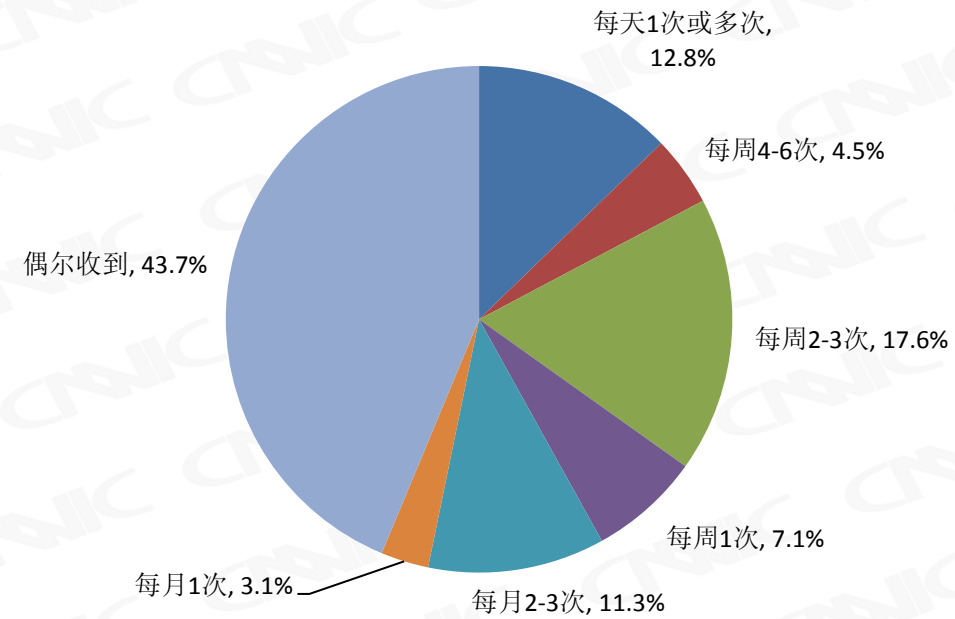


图 26 手机接到骚扰电话的频率

第四章 安全防护软件安装和使用状况

1 电脑安全防护软件

1.1 安装用户数与安装软件数

总体网民中，83.6%的网民电脑上安装了安全防护软件（不含 Windows 系统自带防火墙），用户数为 4.5 亿[3]。在这些网民里，平均每个网民电脑上安装了 1.9 个安全防护软件，其中安装 2 个软件的网民最多，占 51.0%；其次是只安装 1 个的网民，占 29.6%。

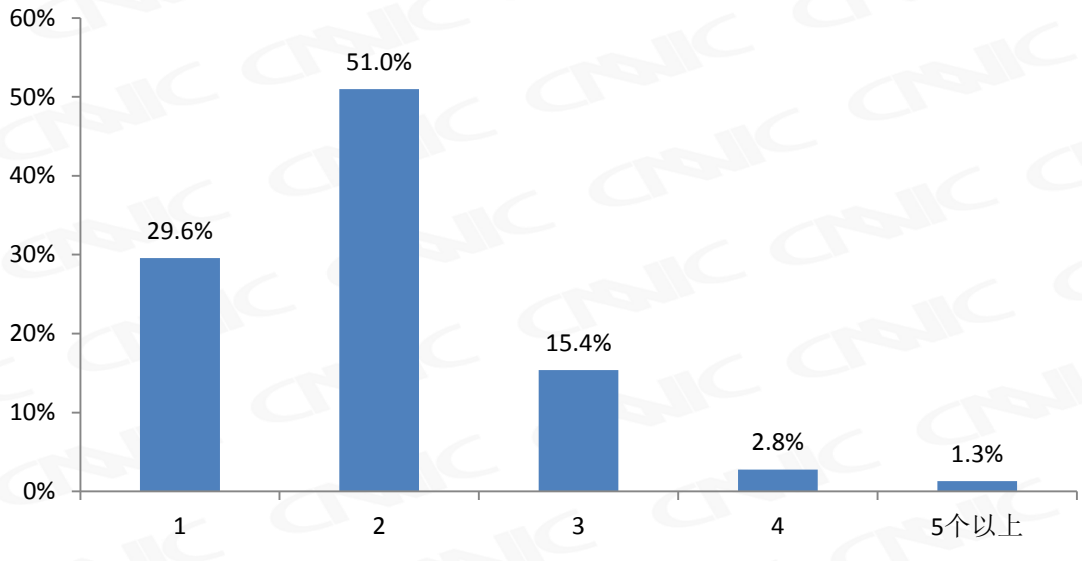


图 27 网民电脑上安装的安全防护软件数量

1.2 软件搭配模式

按照安全防护软件主要功能的多寡，可粗略划分为单一功能软件和套装软件，前者通常只能完成杀毒杀木马或（和）防火墙的功能（如以“杀毒”、“防火墙”为名称后缀的软件），后者通常还能完成系统清理优化等功能（如以“管家”、“卫士”、“套装”为名称后缀的软件）。

本调查显示，网民电脑上最多只安装 1 个单一功能软件，但可能安装多个套装软件。安装

[3] 电脑安全防护软件用户数=网民总数（5.38 亿）*安装的网民比例（83.6%）

了单一功能软件的网民占 69.2%，安装了套装软件的网民占 88.4%。

在只安装 1 个安全防护软件的网民中，74.0%的网民选择安装套装软件，26.0%的网民选择安装单一功能软件；在安装 2 个软件的网民中，89.3%的网民选择“1 个单一功能软件+1 个套装软件”的模式，10.7%的网民选择 2 个套装软件；在安装 3 个软件的网民中，97.7%的网民选择“1 个单一功能软件+2 个套装软件”的模式，2.3%的网民选择 3 个套装软件。

2 手机安全防护软件

2.1 安装用户数与安装软件数

在有手机的网民中，41.1%的网民手机上安装了安全防护软件，用户数为 2.16 亿[4]。在这些网民里，平均每个网民手机上安装了 1.1 个安全防护软件，其中安装 1 个软件的网民最多，占 88.4%；其次是安装 2 个的网民，占 10.7%。

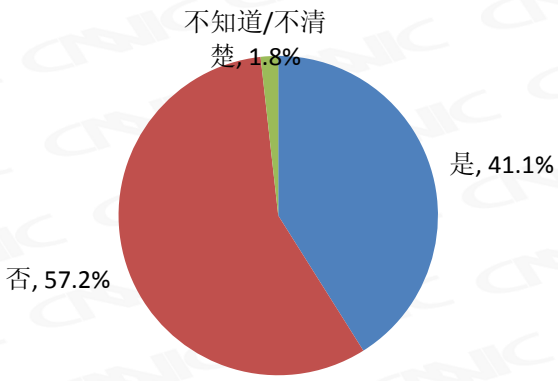


图 28 手机上安装安全防护软件的比例

[4] 手机安全防护软件用户数=网民数（5.38 亿）*有手机的网民比例（97.55%）*安装的网民比例（41.1%）。本调查对网民中的手机使用率进行了调查，结果显示，97.55%的网民拥有或使用过手机。

2.2 安装原因

用户安装手机安全防护软件的原因中，更换了新智能手机是最大的触发因素，由于这一原因的网民占 42.2%。对手机病毒危害性的认识，也是引起用户安装的重要因素，由于这一原因的网民占 33.8%。因此，借助销售智能手机的机会引导和加强手机病毒的宣传，有助于提高手机安全防护软件的安装率。

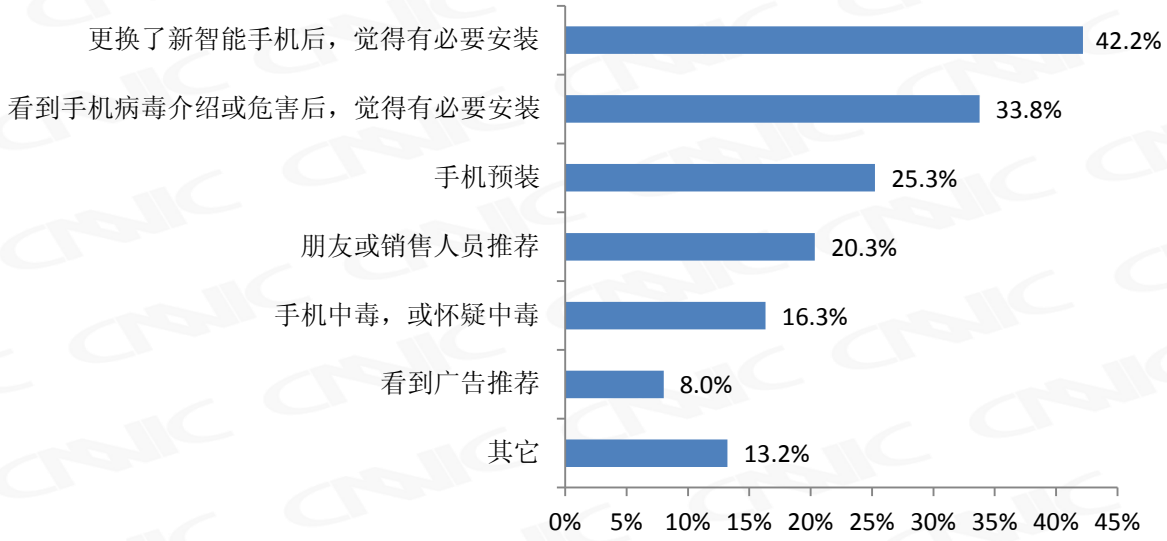


图 29 手机上安装安全防护软件的原因

第五章 总结

调查显示，2012 年中国网民信息安全领域呈现以下特点：

一、信息安全状况极为严重

多年来，我国不断加强网民的信息安全治理，但仍然极为严重。第一，新型的信息安全事件不断出现，且迅速向更多网民蔓延；第二，导致信息安全事件的情境日益多样复杂化，令网民防不胜防；第三，信息安全所引起的直接经济损失已达到很大规模，接近 200 亿元；第四，发起信息安全事件的因素已从此前的好奇心理升级为明显的逐利性，经济利益链条已然形成；第五，信息安全事件中所涉及的信息类型、危害类型越来越多，且日益深入涉及网民的隐私，潜在的后果更严重。

继续加快、加大对信息安全的重视和治理，始终是一个常抓不懈的重要任务，并且应根据现实信息安全状况的新变化，及时调整治理重点和治理思路。

二、网民对信息安全的知识较为欠缺

总体来说，网民缺乏关于信息安全的知识。第一，网民对信息安全的危害性并不清晰；第二，网民采取的信息安全保护措施还未达到较好的水平；第三，很多网民并不具备处理信息安全事件的能力；第四，部分网民对信息安全事件还存在麻痹大意的心理，在不导致明显可见的负面后果的情况下，并不去着手处理。

未来应不断加强对网民的信息安全教育和培训，从认识、技术、心理等各方面武装网民，提高网民的自我信息安全预防和处置能力，特别是对新网民、学历较低的网民。

三、全社会的信息安全保障环境还不令人满意

信息安全保障环境应是法律、政策、执法、媒体、商家、技术、用户等共同组成的体系。目前，这一保障体系还不令人满意。第一，部分掌握用户信息的机构的经营行为规范性不足，造成了用户信息的外泄和对用户的随意干扰；第二，鼓励网民自我维护信息安全的制度环境还未能很好地建立起来，网民遭遇信息安全事件后，难以进行维权；第三，技术上保障信息安全还存在很大难度，安全防护软件还需继续提高技术水平。

当前，应加快有关个人信息使用规范的法律法规的制订和出台，政府、司法、媒体等应主动介入信息安全事件处理，并为网民维权提供便利和支持，继续研究信息安全技术，不断探索新的保障模式。

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。所以，本报告只提供给个人或单位作为市场参考资料，本中心不承担因使用本报告而产生的法律责任。

中国互联网络信息中心

China Internet Network Information Center（CNNIC）

2012 年 10 月