

2013年中国网民信息安全状况研究报告

2013年9月



目录

摘要	5
第一章 研究设计	7
1. 研究背景	7
2. 研究方法	7
3. 术语定义	8
第二章 中国网民信息安全总体现状	9
1. 中国网民信息安全环境	9
2. 信息安全事件发生概率	10
2.1 信息安全事件发生类型及比例	10
2.2 信息安全事件造成的损失	12
2.3 中国网民信息安全状况分类	13
3. 信息安全防护及处理措施	14
3.1 信息安全防护	14
3.2 安全事件处理情况	15
第三章 中国网民电脑上网安全状况	16
1. 电脑上网安全状况概述	16
2. 电脑使用搜索引擎安全状况	16
2.1 搜索引擎安全事件类型及发生比例	16
2.2 搜索引擎安全事件发生后的处理情况	17
2.3 搜索引擎可信度现状	18
2.4 提升搜索引擎可信度的因素	19
3. 电脑网络购物安全状况	21
3.1 网络购物安全事件类型及发生比例	21
3.2 网络购物安全事件处理及防范情况	21
4. 电脑浏览网页安全状况	22
5. 电脑即时通信安全状况	23
5.1 即时通信安全事件类型及发生比例	23
5.2 即时通信安全事件防范情况	24
6. 电脑网上下载安全状况	24
6.1 网上下载安全事件类型及发生比例	24
6.2 网上下载安全事件防范情况	25
7. 电脑网络支付安全状况	26
7.1 网络支付安全事件类型及发生比例	26
7.2 网络支付安全事件防范情况	26
8. 电脑网络游戏安全状况	27
第四章 中国网民手机信息安全状况	28
1. 手机安全事件发生类型及比例	28
2. 手机安全事件发生情景	29
第五章 中国网民安全软件安装情况	30
1. 安装情况	30
2. 不安装原因	30
3. 手机安全软件使用情况	31

第六章 结论.....	33
版权声明.....	34
免责声明.....	34

图目录

图 1	过去半年中国网民信息安全问题整体发生率.....	10
图 2	过去半年中国网民各种安全问题的整体发生率.....	11
图 3	2012-2013 年中国网民各种安全问题发生率变化.....	12
图 4	因安全事件造成的各种损失.....	12
图 5	中国网民信息安全人群划分.....	13
图 6	中国网民信息安全人群划分矩阵图.....	14
图 7	发生安全事件的网民安全防护措施.....	15
图 8	发生安全事件后的处理情况.....	15
图 9	各种电脑上网情景安全事件发生率.....	16
图 10	电脑网上搜索发生的安全问题.....	17
图 11	使用搜索发生安全事件后处理情况.....	17
图 12	发生搜索安全事件的网民对搜索引擎信任度评价.....	18
图 13	发生搜索安全事件的网民对搜索广告信任度评价.....	18
图 14	提升搜索结果可信度的因素.....	19
图 15	提升搜索引擎可信度的因素.....	20
图 16	电脑网上购物发生的安全问题.....	21
图 17	电脑网上购物发生安全事件后的处理方式.....	22
图 18	发生网购安全事件人群的防范措施.....	22
图 19	电脑浏览网页发生的安全问题.....	23
图 20	电脑即时通信发生的安全问题.....	24
图 21	发生即时通信安全事件人群的防范措施.....	24
图 22	电脑网上下载发生的安全问题.....	25
图 23	发生网上下载安全事件的人群防范措施.....	25
图 24	电脑网上支付发生的安全问题.....	26
图 25	发生网络支付安全事件人群的防范措施.....	27
图 26	电脑网络游戏发生的安全问题.....	27
图 27	中国手机信息安全问题的类型及比例.....	28
图 28	手机安全事件的发生情景.....	29
图 29	安全软件安装普及情况.....	30
图 30	不安装安全软件的原因.....	31
图 31	网民在手机上使用安全软件的功能.....	32

摘要

一. 中国网民信息安全总现状

- ◇ 整体上,我国信息安全环境不容乐观,有 74.1%的网民在过去半年内遇到过信息安全问题,总人数达 4.38 亿。
- ◇ 手机垃圾短信/骚扰短信、骚扰电话发生比例仍然较高,在整体网民中发生比例分别达 59.2%、49.0%;其次为手机欺诈/诱骗信息,发生比例为 36.3%;再次为手机恶意软件,发生比例达 23.9%;其它方面,假冒网站/诈骗网站发生比例为 21.6%,中病毒或木马发生比例为 17.6%,个人信息泄露发生比例为 13.4%,账号或密码被盗发生比例为 8.9%。
- ◇ 信息安全事件对人们的影响较大。遭受安全事件的人群中,50.4%的人认为“花费时间和精力”,有 28.2%的人学习或工作受到了影响,13.1%的人重要资料或联系人信息丢失,还有 8.8%的人经济受到了损失。
- ◇ 在遭受经济损失的人群中,平均每人损失了 509.2 元,过去半年全国因信息安全遭受的经济损失达到了 196.3 亿元。
- ◇ 根据安全事件发生种类数以及遭受损失的数量来划分用户群体,重度受害人群占 16.2%,轻度受害人群占 28.3%,风险人群占 29.6%,安全人群占 25.9%。

二. 中国网民电脑上网安全状况

- ◇ **电脑搜索引擎:**截止 2013 年 9 月的过去半年因电脑搜索遇到安全事故的网民数占整体电脑端网民的 6.0%,影响人口达 3004.6 万人。使用搜索引擎发生安全事件的人群中,遇到诈骗信息、诈骗网站、网页附带木马或病毒的比例较高,分别为 72.7%、71.9%、67.2%。
- ◇ **电脑购物:**过去半年因电脑网上购物发生安全问题的网民数占整体电脑端网民的 4.0%,影响人口达 2010.6 万人。因电脑购物发生安全事故人群中,发生较多的是遇到欺诈信息,发生比例达 75.0%;其次为假冒网站/诈骗网站,比例为 60.7%;其它方面,个人信息泄露和账号密码被盗分别为 42.9%、23.8%,中病毒或木马的情况为 22.6%。
- ◇ **电脑浏览网页:**过去半年有 13.0%的网民浏览网页时候发生过安全事件。在浏览网页发

生安全事件的网民中，接触欺诈诱骗信息的比例达 72.7%，遇到病毒或木马的比例达 70.9%，浏览假冒网站/诈骗网站的比例为 63.0%，账号密码被盗的比例为 18.3%。

- ✧ **电脑即时通信：**过去半年有 11.5%的网民使用即时通信时发生过安全事件。因使用即时通信发生安全事件的人群中，63.5%的人接收到了欺诈信息，53.0%的人接收到了假冒/诈骗网站，还有 52.6%的人账号或密码被盗，40.6%的人电脑中病毒或者木马。
- ✧ **电脑网上下载：**过去半年有 13.3%的网民电脑下载时发生过安全事件。因网上下载发生安全事件的人群中，有 86.1%的人遇到了数据包加载木马/病毒等情况，53.8%的人遇到过欺诈、诱骗信息，还有 48.6%的人遇到过假冒网站/诈骗网站。
- ✧ **电脑网络支付：**过去半年有 1.5%的网民电脑网上支付时发生过安全事件。在发生网络支付安全事件的人群中，遇到假冒网站/诈骗网站的比例达 57.1%，遇到个人信息泄露的比例为 39.3%，资金被盗、被骗和账号密码被盗的比例达 32.1%。
- ✧ **电脑网络游戏：**过去半年网络游戏安全事件在电脑网民中的发生比例为 4.2%。发生最多的是游戏被盗号/装备被卖，占因玩网络游戏发生安全事件的网民的 56.0%。其它常见的安全事件为中病毒或木马、账号密码被盗、游戏中欺诈信息、个人信息泄露等，发生比例分别为 52.7%、51.6%、51.6%、22.0%。

三. 中国网民手机信息安全状况

- ✧ 智能手机上网用户群中，接收到手机垃圾短信/骚扰短信、骚扰电话的比例较高，分别达 68.6%和 57.2%，遇到恶意软件的比例也达到了 33.2%。
- ✧ 发生手机安全的人群中，除了骚扰电话和骚扰短信外，发生概率最多的是手机浏览网页，比例达 16.8%；其次为手机游戏，发生比例达 13.8%；再次为手机聊天工具和手机下载文件，发生比例在 12%左右；手机搜索、手机购物、手机支付等也可能导致安全事件。

四. 中国网民安全软件安装及使用情况

- ✧ 96.5%的网民在电脑上安装了安全软件，远高于智能手机的 70.0%。
- ✧ 网民之所以不安装安全软件，“没发生过安全事件，不需要”是主要原因，还有 15%左右的人担心安装后设备运行或上网速度变慢。此外，安装知识欠缺、对安全软件不信任，也是网民不安装安全软件的原因。

第一章 研究设计

1. 研究背景

2013 年网络诈骗、信息泄露等事件频繁发生，影响了网民的上网体验，也阻碍了互联网产业的健康发展。

良好的信息安全环境是整个互联网产业发展的前提，其中网络安全软件扮演了重要的角色，网民安全意识也非常重要。为反映当前中国网民信息安全现状和网民安全意识，以及安全软件的安装使用情况，CNNIC 开展了“2013 年中国网民信息安全状况研究”，从网民角度评估我国互联网安全中存在的风险，了解网民在信息安全上遇到的问题和需求。

2. 研究方法

✧ 调查样本分布

调查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 11 个、三级城市 9 个。调查最终获得有效样本量 2503 个，由以下两部分组成：

1. 固话样本：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 1248 个。

2. 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 1255 个。

✧ 调查时间

从 2013 年 8 月 15 日至 2013 年 9 月 2 日。

✧ 调查方式

通过计算机辅助电话访问系统（CATI）进行调查。

3. 术语定义

◇ 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、手机收到垃圾短信、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。

◇ 安全软件

是指包括杀毒软件、防火墙软件、查杀木马插件等安全辅助软件等各种类型安全软件的集合。

◇ 安全套装软件

是指出自同一个安全软件厂商，打包对外销售，至少包括杀毒软件及防火墙软件这两种类型的安全软件，有些安全套装软件甚至包括除以上两种类型外，其他更多功能。

◇ 杀毒软件

也称反病毒软件或防毒软件，是用于消除电脑病毒、特洛伊木马和恶意软件的一类软件。杀毒软件通常集成监控识别、病毒扫描和清除和自动升级等功能，有的杀毒软件还带有数据恢复等功能，是计算机防御系统（含杀毒软件，防火墙，特洛伊木马和其他恶意软件的查杀程序，入侵预防系统等）的重要组成部分。

◇ 防火墙软件

是一个位于计算机和它所连接的网络之间的软件。该计算机流入流出的所有网络通信均要经过此防火墙。该软件可协助确保信息安全，其会依照特定的规则，允许或是限制数据通过。

第二章 中国网民信息安全总体现状

1. 中国网民信息安全环境

近年来随着网民信息安全意识逐渐提高，维护安全的工具性能提升，中国网民大规模遭受同一安全事件的概率降低。但近年来各种恶意程序的变种产生速度不断加快，每天都有海量新生的恶意程序威胁着普通用户的上网设备（包括电脑、智能手机等），而且除恶意程序之外的其它安全问题也层出不穷，网民面临的信息安全环境仍然复杂。当前主要信息安全类型如下：

1. 恶意程序或病毒：此类恶意程序利用人们访问网页、下载文件或网络聊天等上网行为，潜伏到人们的电脑或者手机中，通过删除文件、破坏用户设备系统、盗取网民资料、窃取账号密码、恶意刷网页或广告流量，损害他人利益或为自己谋利。

2. 假冒网站或诈骗网站：也称为钓鱼网站，通过模仿银行、购物网站以及其它权威网站的网页设计，骗取网络用户的钱财或盗取密码等信息。一方面，通过设立虚假网站骗取用户登录，进而获取用户账号密码；另一方面，通过虚假抽奖页面，造成用户中奖的假象，骗取用户钱财；其它方式还有通过虚假购物、虚假医药销售等方式来非法牟利。此类网站往往通过手机短信、即时通信工具发送网址，或者通过木马强制弹出或转移用户访问其页面，以达到其非法目的。

3. 垃圾/诈骗短信或电话：通过电话或手机短信等方式，发布各种诈骗信息或大量垃圾广告，骗取用户钱财或者非法牟利，常用方式有：通过语音和短信告知用户中大奖、或者以熟人身份向用户“借”钱，以达到骗取用户钱财的目的；拨打用户电话，接通之后便挂掉，让用户回拨以收取高价通信费等方式骗取钱财；或发送大量广告信息，让用户深受困扰。此类事件常因手机信息网上泄露而产生，而且与信息安全息息相关，因此也列入本次研究的范围。

4. 网络其它诈骗：通过在论坛、通信工具以及正常网页上发布招聘、购物等信息，一步一步引导网民陷入其编制的诈骗圈套中，让用户受害。

当前，针对上述安全问题而开发的安全软件也较多，常见的有安全卫士/电脑管家/手机管家、杀毒软件以及防火墙等等。尽管这些安全软件功能已经较为完备，但由于针对信息安

全的诈骗和攻击手段变化多端, 仅仅安装这些安全软件并不能完全使用户免遭信息安全问题。

2. 信息安全事件发生概率

2.1 信息安全事件发生类型及比例

整体上来讲, 我国信息安全环境仍不容乐观, 有 74.1% 的网民在过去半年内遇到过安全事件, 总人数达 4.38 亿¹。

近年来, 虽然安全软件逐渐普及、防范能力不断加强, 但新的病毒、诈骗手段和骚扰手段不断涌现, 安全软件防范难度加大, 安全事件发生概率仍然较高。

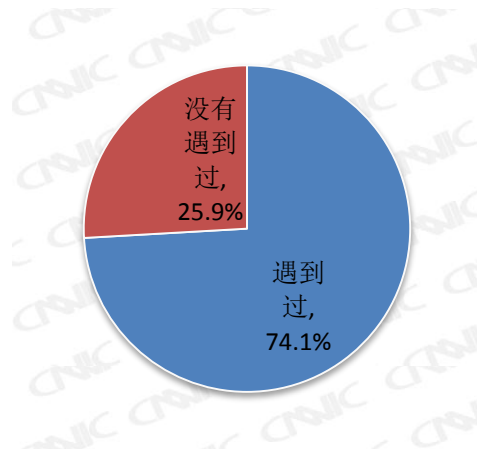


图 1 过去半年中国网民信息安全问题整体发生率

整体上看, 手机垃圾/骚扰短信、骚扰电话发生比例较高, 分别达 59.2% 和 49.0%; 网上欺诈和诱骗现象仍未改善, 钓鱼网站/假冒网站仍旧泛滥, 过去半年有 36.3% 的网民遇到过欺诈和诱骗信息, 21.6% 的网民遇到过钓鱼网站/假冒网站; 手机恶意软件越来越猖獗, 过去半年有 23.9% 的网民遇到过手机恶意软件, 这些软件主要以骗取流量、乱发广告、乱扣费为主, 严重影响了手机网民的使用体验。

个人信息泄露和账号密码被盗的发生比例分别为 13.4% 和 8.9%, 虽然表面上看比例较小, 但此类事件发生后给用户带来的损失非常大, 也不容忽视。创造一个良好的网络安全环境, 保护个人信息和账号密码刻不容缓。

¹根据 CNNIC 的《第 32 次中国互联网络发展状况统计报告》显示, 截至 2013 年 6 月底, 我国网民数为 5.91 亿。遇到信息安全事件的总人数=网民数 (5.91 亿) × 遇到过安全问题的网民比例 (74.1%)。

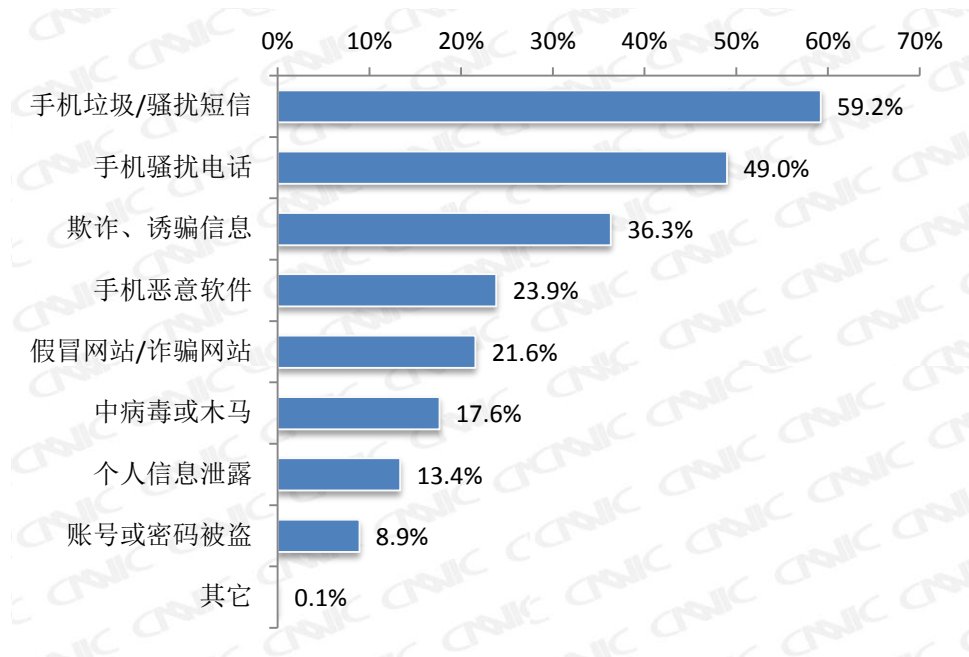


图 2 过去半年中国网民各种安全问题的整体发生率

与 2012 年相比，网民遇到手机垃圾短信和骚扰电话、中病毒或木马、账号或密码被盗的比例都有较大幅度下降，其中收到手机垃圾短信的比例下降了 9.1 个百分点，接到骚扰电话的比例下降了 7.5 个百分点，中病毒或木马的比例下降了 5.4 个百分点，账号密码被盗的比例下降了 4.9 个百分点。但新的问题也在不断出现，网民遇到手机恶意软件、假冒网站/诈骗网站、个人信息泄露的比例都有较大幅度上升，其中遇到手机恶意软件的比例上升了 13.2 个百分点，遇到假冒网站/诈骗网站的比例上升了 4.0 个百分点，遇到个人信息泄露的比例上升了 6.2 个百分点。

近年来手机安全软件不断改善，已能自动屏蔽常规的骚扰电话和垃圾短信，网民接收到垃圾短信和骚扰电话比例下降，但由于分辨骚扰电话和垃圾短信的规则单一，常常存在误杀和遗漏的现象。

当前安全软件对病毒或木马的捕获力度有所加强，使得网民遇到病毒或木马的比例降低，账号或密码被盗的风险下降。但网络诈骗手段千变万化，目前各种假冒网站/诈骗网站层出不穷，安全软件很难在其一出现即识别，网民接收到假冒网站/诈骗网站概率增加。近年来随着手机网民迅速增加，网民遇到手机恶意软件的比例也快速增加，今后识别和处理手机恶意软件，将是一大难题。

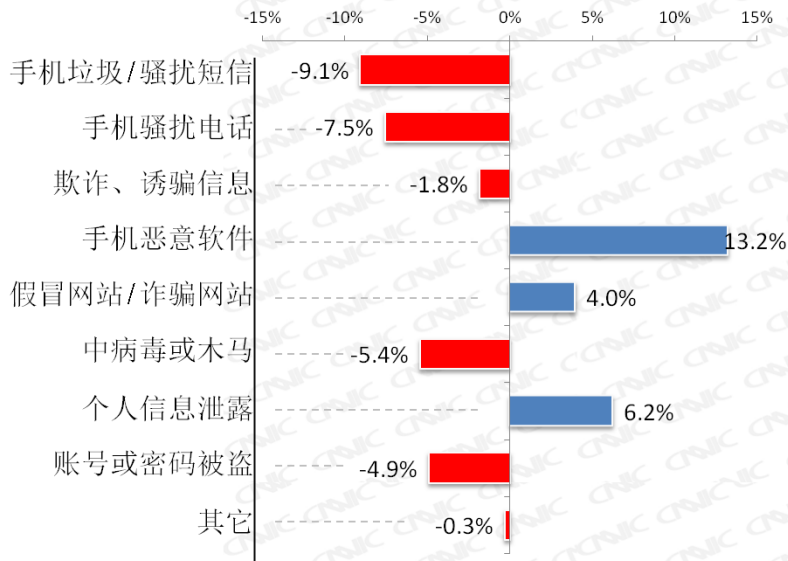


图 3 2012-2013 年中国网民各种安全问题发生率变化
(2013 年的发生比例-2012 年的发生比例)

2.2 信息安全事件造成的损失

信息安全事件发生后，带给人们的影响较大，其中 50.4% 的人认为“花费时间和精力”，有 28.2% 的人学习或工作受到了影响，13.1% 的人重要资料或联系人信息丢失，还有 8.8% 的人经济受到了损失。只有 39.9% 的网民认为没有损失。

在遭受经济损失的人群中，平均每人损失了 509.2 元，过去半年全国因信息安全遭受的经济损失达到了 196.3 亿²。

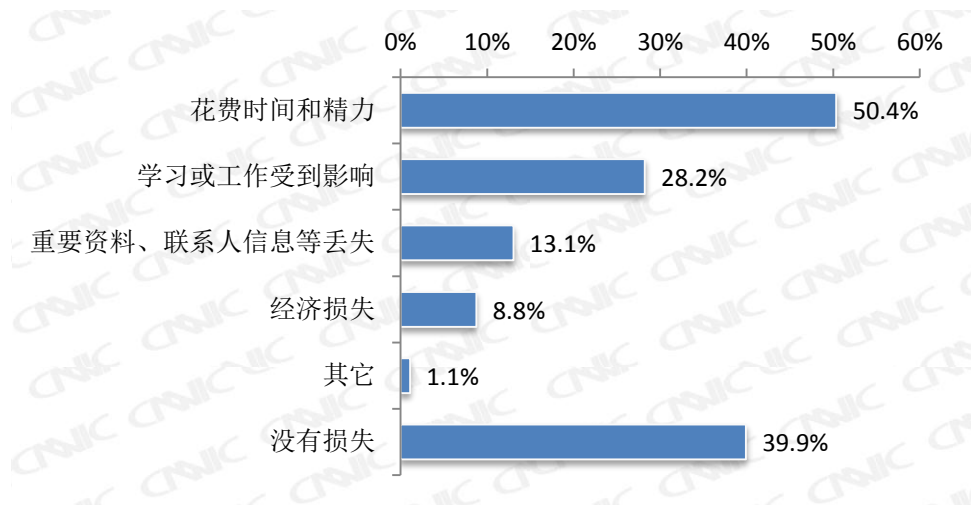


图 4 因安全事件造成的各种损失

²推算过程: 全国因信息安全问题遭受的经济损失=网民数 (5.91 亿) × 遇到过安全问题的网民比例 (74.1%) × 因安全问题遭受到经济损失的比例 (8.8%) × 因安全问题遭受的平均经济损失 (509.25 元) = 196.3 亿。此损失仅计算个人损失，未包括企业等非个人主体因安全事件产生的损失。

2.3 中国网民信息安全状况分类

根据网民遇到上述安全问题和遭受损失的种类多少，把中国网民分成四类：

1. **安全人群**：过去半年未遇到信息安全问题，而且也未因此遭受损失的网民。
2. **风险人群**：过去半年遇到过信息安全问题，但未产生任何损失的网民。
3. **轻度受害人群**：过去半年遇到 1-4 种安全问题，且遭受上述 1-2 种损失的网民。
4. **重度受害人群**：过去半年遇到了 5 种及以上安全问题，且遭受了损失的网民；或过去半年遭受了 3 种及以上损失的网民。

根据以上分类，中国整体网民中，大部分网民处于风险状态或受损状态，绝对安全的人员比重较小，整体互联网网民信息安全问题仍不容乐观。

整体网民中，因信息安全问题而受损的人群占 44.5%，其中重度受害人群占 16.2%，轻度受害人群占了 28.3%；遇到安全问题但未发生损失的风险人群占了 29.6%，这部分人群暂未受到危害，但仍不能掉以轻心；绝对安全的人员仅占 25.9%，比例较小。

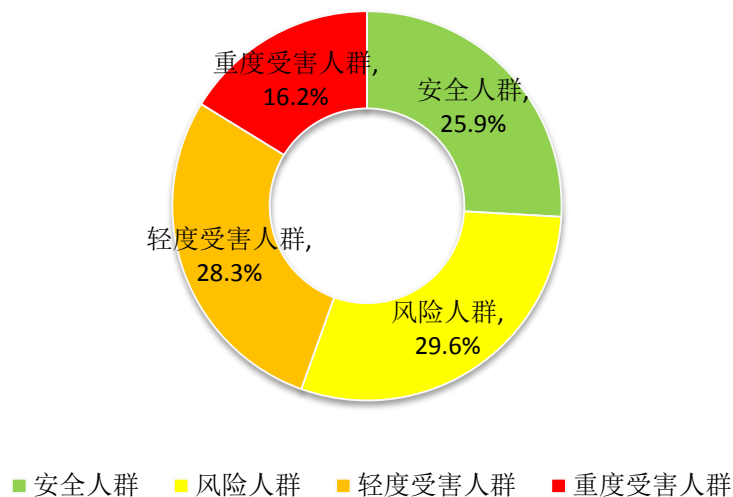


图 5 中国网民信息安全人群划分

具体划分区间以及各区间网民占比如下：

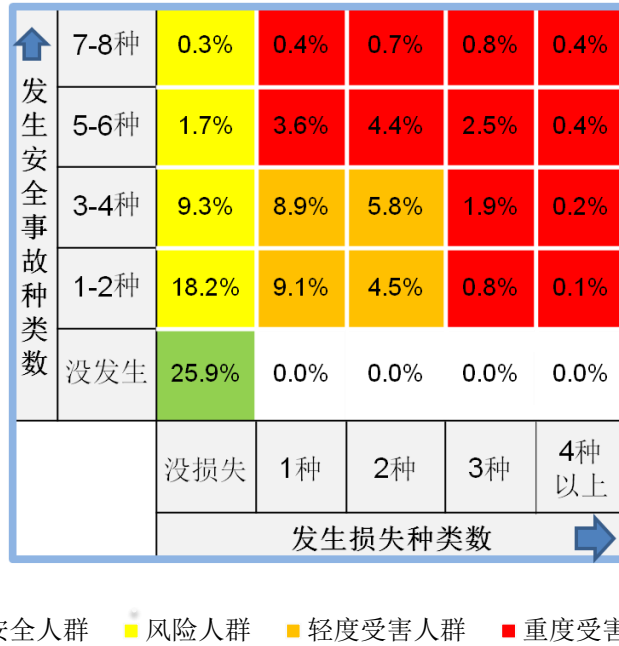


图 6 中国网民信息安全人群划分矩阵图

从上图可知，发生安全事故的种类越多，造成损失的概率也越大。但发生 1-2 种安全事故即造成损失的占比高达 14.5%，为此应对每一个安全事故予以充分重视。

3. 信息安全防护及处理措施

3.1 信息安全防护

在发生安全事件的网民中，信息安全防范意识有待提高。虽然有 93.3% 的人安装了安全软件，85.9% 的人不安装来历不明的软件，85.4% 的人不轻易在网上透露个人真实信息，83.8% 的人不随便点击可疑的链接，但仅有 75.2% 的人使用系统自动更新/打补丁，只有 67.3% 的人设置复杂密码，只有一半的人在不同网站设置不同账号或者密码，以上常见的个人安全防范措施尚未完全普及，是信息安全事件频发的重要原因。

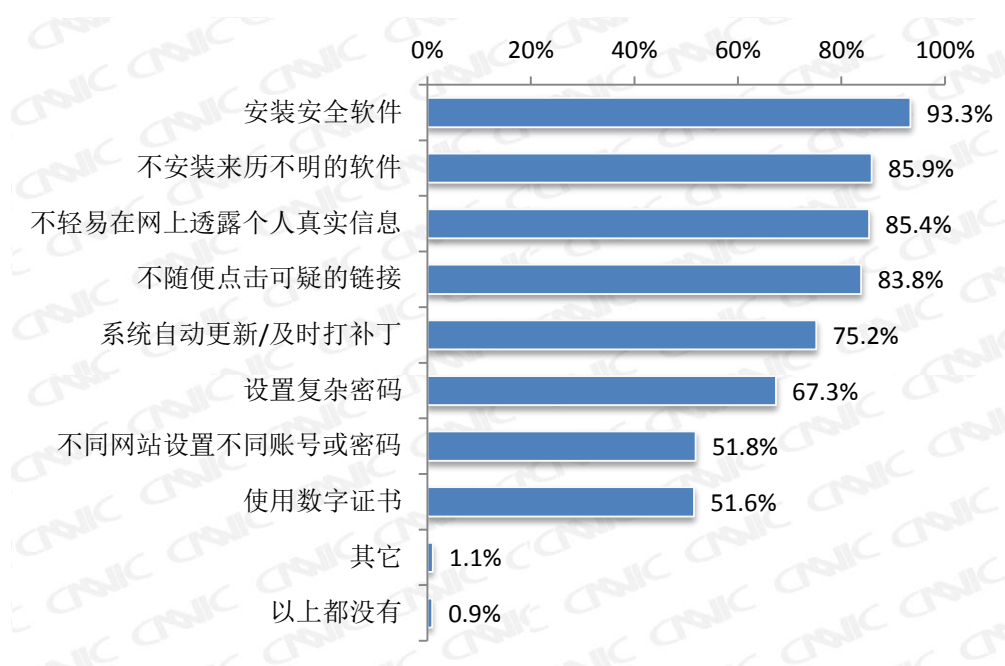


图 7 发生安全事故的网民安全防护措施

3.2 安全事件处理情况

对于发生安全事件以后的处理措施中，有 80.8% 的人会杀毒，四成左右的人会重新安装软件、重装系统或者屏蔽网站，除此之外采取其它措施的比例较小。

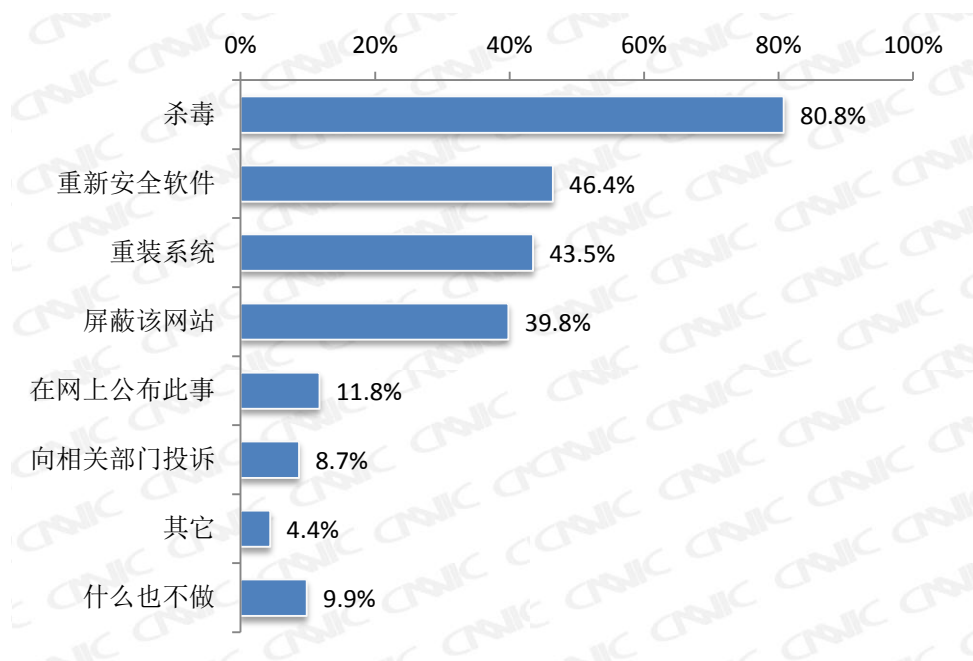


图 8 发生安全事件后的处理情况

第三章 中国网民电脑上网安全状况

1. 电脑上网安全状况概述

电脑上网人群中，浏览网页、即时通信以及下载软件是最容易遇到安全问题的三项网上活动，发生比例在 10% 以上；其次为使用搜索引擎，发生安全事件的比例在 6% 左右；最后为网络游戏、网上购物和网上支付，虽然发生比例较小，但发生后损失较大，也不容忽视。

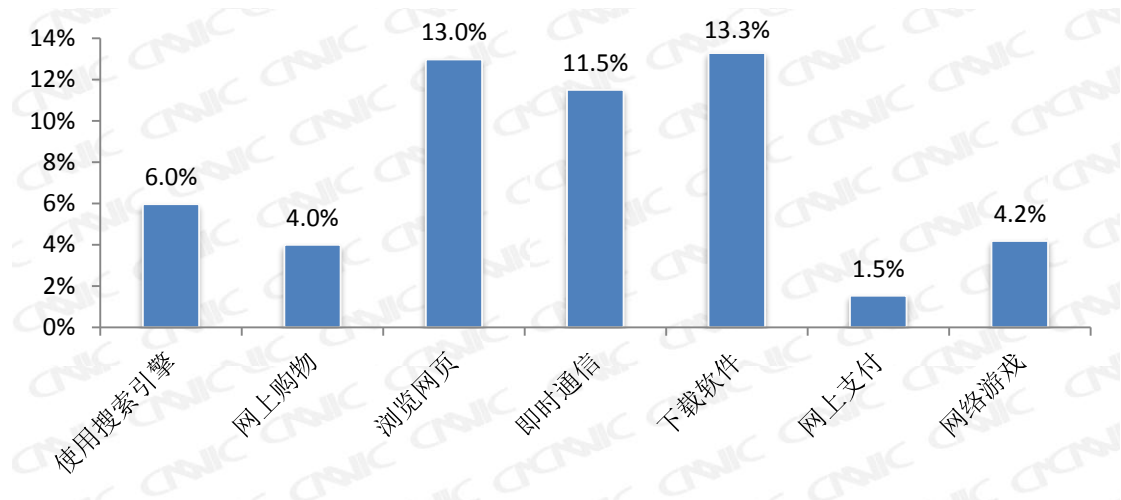


图 9 各种电脑上网情景安全事件发生率

2. 电脑使用搜索引擎安全状况

2.1 搜索引擎安全事件类型及发生比例

因电脑搜索发生安全问题的网民数占整体电脑上网人数的 6.0%，影响人口达 3004.6 万人³。虽然发生问题的比例不是非常高，但由于网民基数大，影响人口总数也较大。

使用搜索引擎发生安全事件的人群中，遇到诈骗信息、诈骗网站、网页附带木马或病毒的比例非常高，分别为 72.7%、71.9%、67.2%。搜索结果出来后，用户不小心就会点击进入一些网站（分类网站、论坛、贴吧等）发布的诈骗信息，稍有不慎就会被骗。近期钓鱼网站/假冒网站发生概率也较大，常模仿正常的网站页面，以中奖、彩票、领取礼品等方式骗取

³推算过程：网民数（5.91 亿）× 电脑使用比例（85.09%）× 因使用搜索引擎发生安全问题的比例（6.0%）= 3004.6 万（人）

用户金钱和个人信息。搜索结果中鱼目混杂，很多不良网站上附带木马或病毒，也会导致用户发生安全事件。虽然部分搜索引擎加大了非法网站过滤力度，并采用认证的方式引导用户点击安全网站，但仍不能完全杜绝此类事件发生。

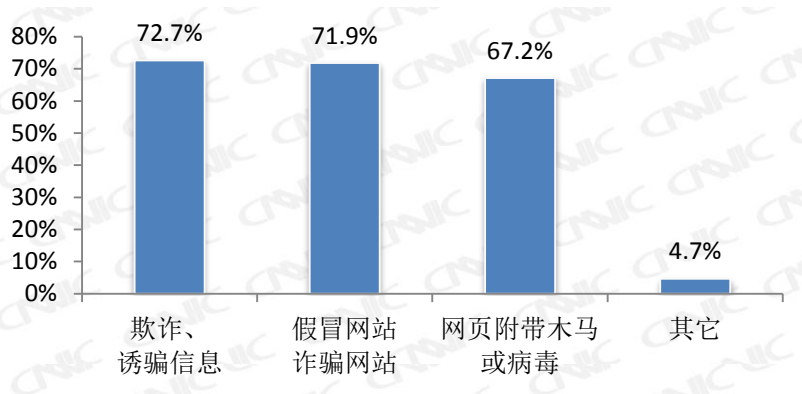


图 10 电脑上搜索发生的安全问题

2.2 搜索引擎安全事件发生后的处理情况

使用搜索引擎发生安全事件后，82.8%的人会选择屏蔽发生安全事件的网站，还有 60.9%的人会选择减少使用当前的搜索引擎，也有 10%左右的人会在网上公布此事件、向搜索引擎企业申诉或者向相关部门投诉。

使用搜索引擎发生安全事件后，用户会降低对当前使用的搜索引擎的信任度，减少使用该搜索引擎，这对搜索引擎吸引和留住用户产生了较大的负面作用。

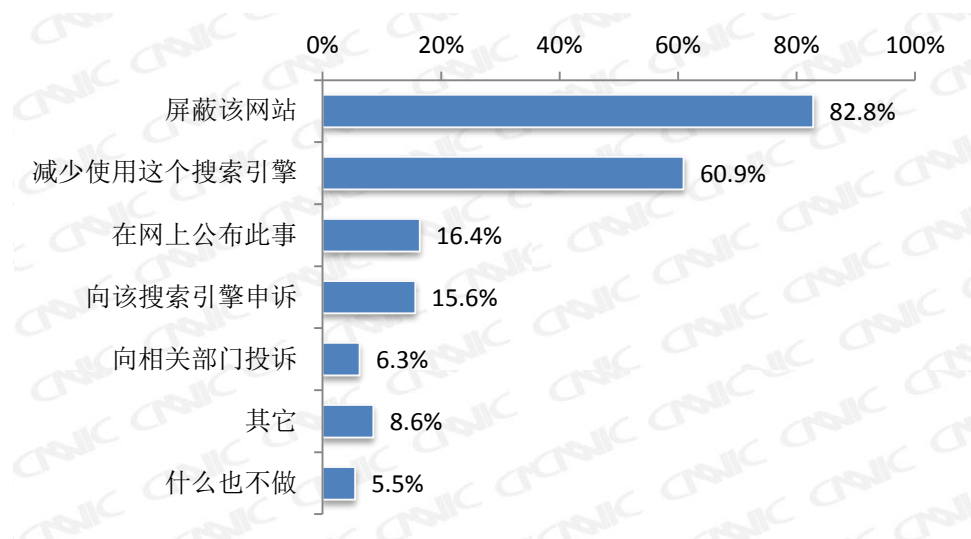


图 11 使用搜索发生安全事件后处理情况

2.3 搜索引擎可信度现状

因为部分网民在使用搜索引擎时发生了安全事件，加上媒体对此广泛报道，直接导致对搜索引擎的信任度不高。发生搜索安全事件后，5.3%的人认为搜索引擎完全不可信，10.5%的人认为有些不可信，二者之和达到了15.8%。此外，有34.6%的网民对搜索引擎评价保持中立，仅有45.9%的网民认为搜索引擎完全可信或有些可信。

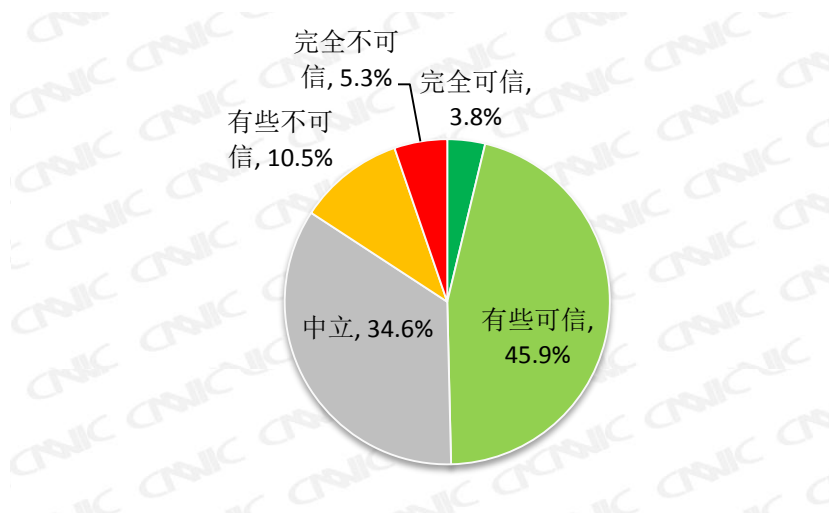


图 12 发生搜索安全事件的网民对搜索引擎信任度评价

安全事件发生后对搜索广告的信任度评价影响更大，在发生搜索安全事件的人群中，高达34.9%的人认为搜索广告完全不可信，29.4%的人认为搜索广告有些不可信，二者之和达到了64.3%。搜索广告是搜索引擎商业收入的主要来源，网民对搜索广告的信任度直接关系到搜索引擎企业的生存和发展，因此提升搜索广告的信任度尤其重要。

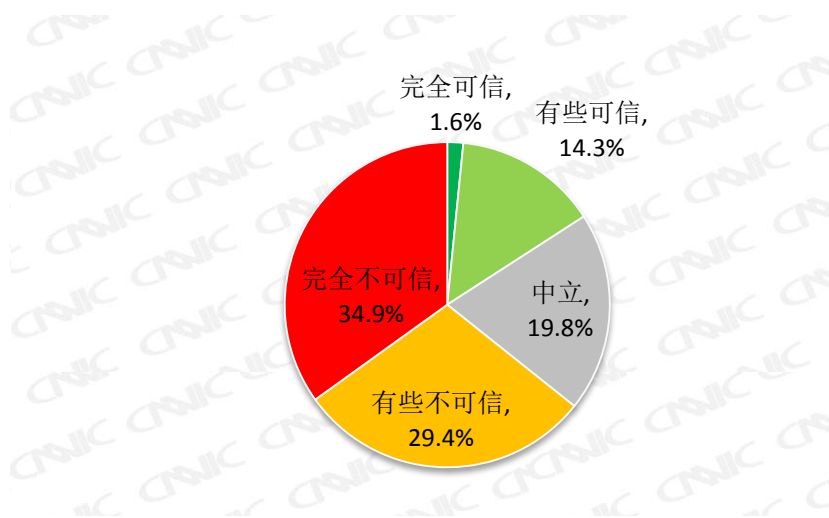


图 13 发生搜索安全事件的网民对搜索广告信任度评价

2.4 提升搜索引擎可信度的因素

搜索引擎的认证和搜索结果网站自身建设都能提升搜索结果的可信度。网民对于搜索结果可信度的判断上，有 79.2% 的人认为搜索出来的网站品牌权威性很重要，73.8% 的人认为搜索结果后面带有认证标识很重要，有 58.5% 的人认为搜索出来的网站联系方式齐全很重要，还有 41.0% 的人认为搜索出来的网站设计很重要。

为此，要增加搜索结果可信度，搜索引擎的认证较为重要，而搜索结果网站自身品牌建设以及网站设计也很重要。

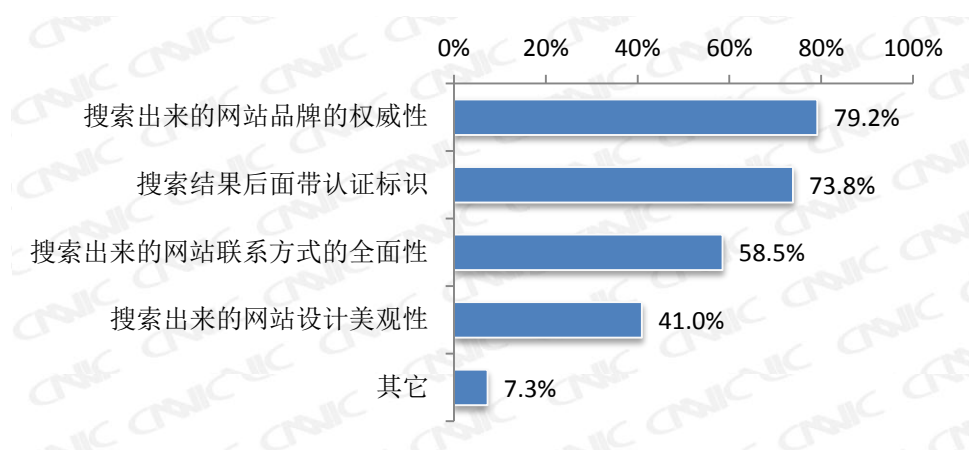


图 14 提升搜索结果可信度的因素

对于哪些因素可以提升搜索引擎的可信度，82.8% 的人选择了搜索引擎网站品牌知名度，这对于提升搜索引擎可信度较为关键；其次，搜索引擎本身的技术实力也很重要，80.3% 的人选择了“搜索技术实力和查出力度”。再次，搜索引擎认证和保障也很重要，73.7% 的人选择了“搜索引擎官方认证”，65.0% 的人选择了“第三方认证”，62.4% 的人选择了“企业官方授权”，45.8% 的人选择了“搜索引擎保障计划”。

整体来说，搜索引擎的品牌建设、使用率、技术实力提升、技术认证级后期保障对网民提升搜索引擎可信度都非常重要。

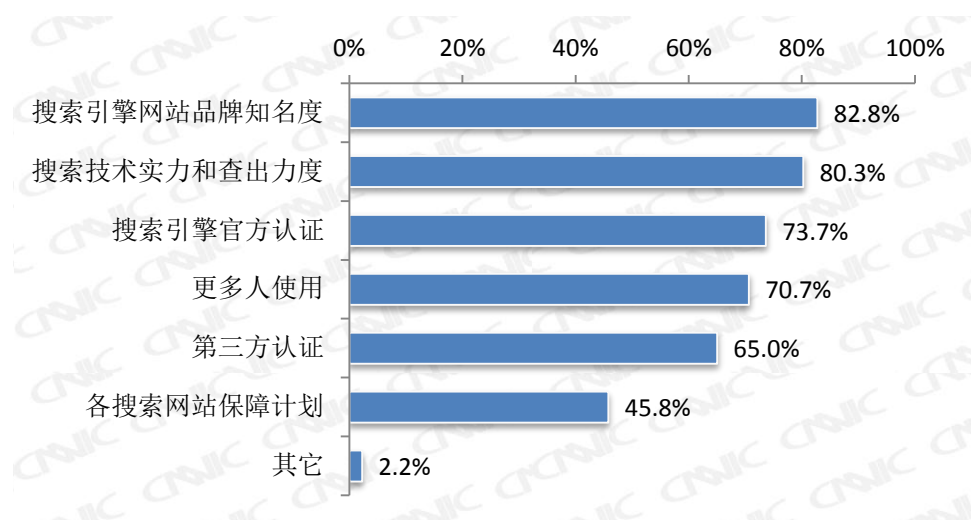


图 15 提升搜索引擎可信度的因素

当前部分搜索引擎已经推出了一系列行动来提升网民信任度，同时降低安全事件的发生率，保障网民的利益。例如，百度在 2010 年开展虚假网站专项打击行动“阳光行动”，之后推出了针对搜索结果的“官网认证”，针对广告的百度认证，针对搜索结果的第三方安全联盟认证，防止安全事件发生。2013 年，百度发布针对搜索推广和网盟网站链接的网民权益保障计划，出现的安全问题接受无时限申诉，保障搜索网民的利益。360 搜索也推出了不同的认证和保障计划，如“推广欺诈全赔计划”等，其它部分搜索品牌如搜狗等，也推出了部分认证。

认证和保障类别（截止 2013 年 9 月）			
品牌	百度	360 搜索	搜狗搜索
搜索引擎官方认证 (官网认证)	开通	开通	开通
搜索引擎官方认证 (针对广告)	开通	-	-
第三方认证	开通	开通	开通
搜索保障	开通	开通	-

当前各种认证和保障计划已经较为全面，如何提升这些措施在搜索网民中的认知度，进而提升搜索引擎的信任度，将是接下来的重要课题。

3. 电脑网络购物安全状况

3.1 网络购物安全事件类型及发生比例

因电脑网上购物发生安全问题的网民数占整体电脑上网人数的 4.0%，影响人口达 2010.6 万人⁴。

电脑网上购物发生安全事故较多的是遇到欺诈信息，在网购安全事故发生人群中的发生比例达 75.0%；其次为假冒网站/诈骗网站，比例为 60.7%；其它方面，个人信息泄露比例达 42.9%、账号密码被盗比例达 23.8%、中病毒和木马的情况为 22.6%。

网购时发生这些安全事件，给购物者造成损失的同时，也扰乱了网上购物秩序，影响网络购物行业的健康发展。

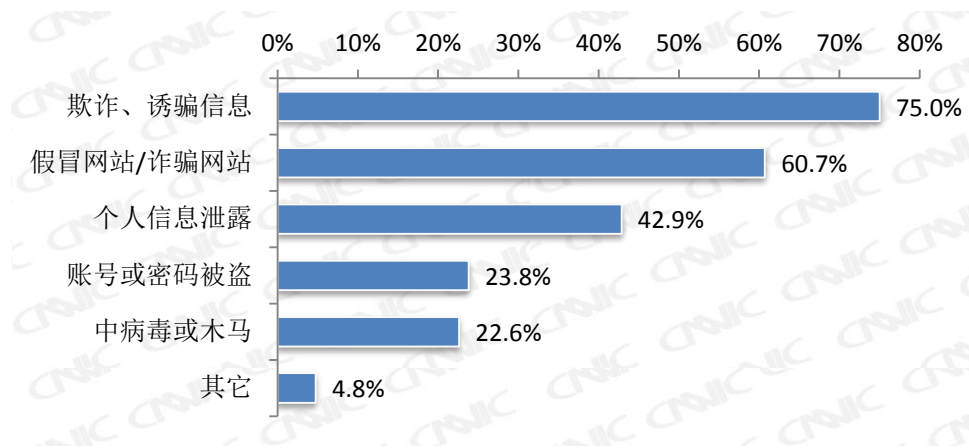


图 16 电脑网上购物发生的安全问题

3.2 网络购物安全事件处理及防范情况

电脑网购发生安全事件后，44.0%的人 would 向网购企业投诉，26.2%的人会在网上公布此事，还有 16.7%的人 would 向政府等主管部门投诉，但有三分之一的人选择什么也不做。

整体来说，网购发生安全事件后，网民申诉渠道还不太普及，维护自身利益的意识有待提升。

⁴推算过程：网民数（5.91 亿）× 电脑使用比例（85.09%）× 因使用搜索引擎发生安全问题的比例（4.0%）= 2010.6 万（人）

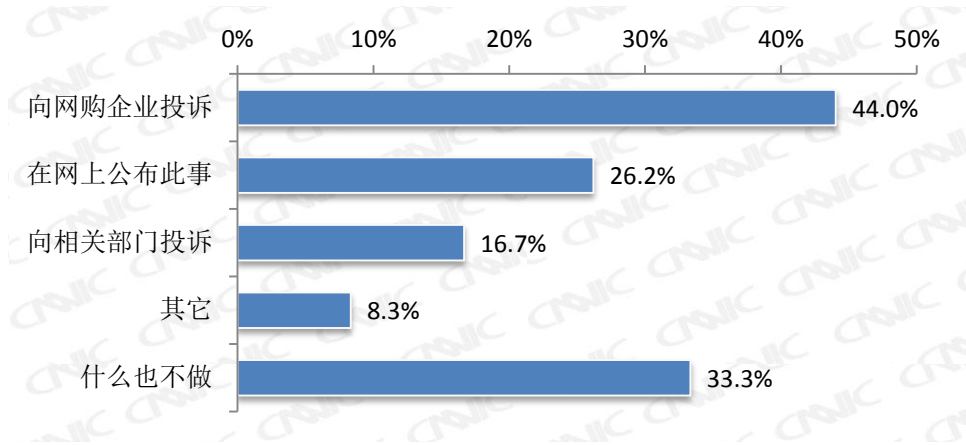


图 17 电脑网上购物发生安全事件后的处理方式

对于网购安全防范措施，部分受安全困扰的网民防范措施做得不太到位：虽然有 92.1% 的人会选择密码保护或修改密码，但仅有 86.5% 的人会仔细验证卖家信誉，85.4% 的人不去不知名的网站上购买货物，83.1% 的人申请账号验证。

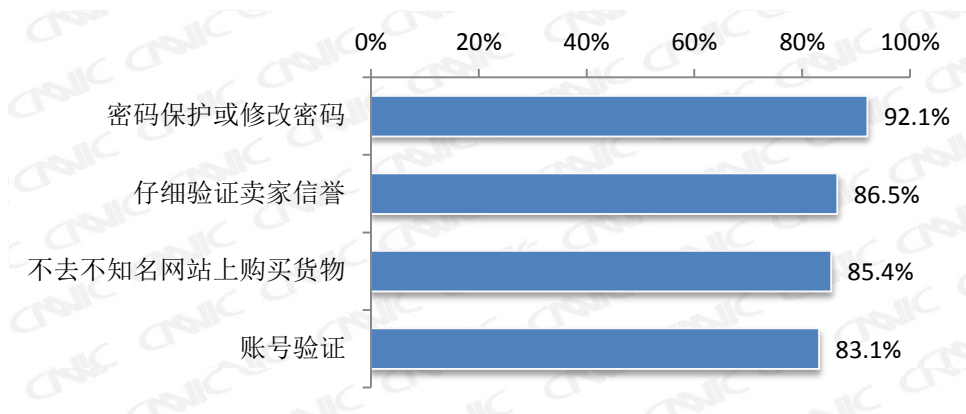


图 18 发生网购安全事件人群的防范措施

4. 电脑浏览网页安全状况

浏览网页是发生安全事件较为普遍的上网活动之一，过去半年有 13.0% 的电脑端网民浏览网页时候发生过安全事件。

在浏览网页时发生安全事件的网民中，接触欺诈诱骗信息的比例达 72.7%，遇到病毒或木马的比例达 70.9%，浏览到假冒网站/诈骗网站的比例为 63.0%，账号密码被盗的比例为 18.3%。当前尽管互联网监管措施日渐完善，但仍然无法避免一些诈骗信息和网站横行于互

联网上。

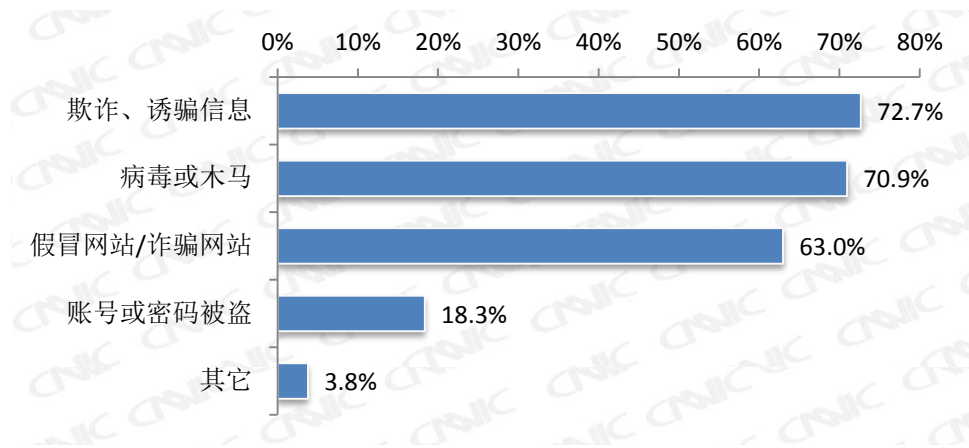


图 19 电脑浏览网页发生的安全问题

5. 电脑即时通信安全状况

5.1 即时通信安全事件类型及发生比例

即时通信也是发生安全事件较为普遍的活动之一，过去半年有 11.5% 的电脑网民发生过即时通信类的安全事件。

在使用即时通信时发生安全事件的人群中，63.5% 的人使用聊天工具时接收到了欺诈信息，53.0% 的人通过即时通信工具接触到了假冒网站或诈骗网站，还有 52.6% 的人账号或密码被盗，40.6% 的人中病毒或者木马，32.9% 的人个人信息遭到泄露。

当前很多即时通信工具都推出了识别链接或数据包安全性的工具，此类安全事件发生比例已经有所减少，但仍然不能完全识别所有通信工具上来往信息的真伪，造成部分用户利益受损。

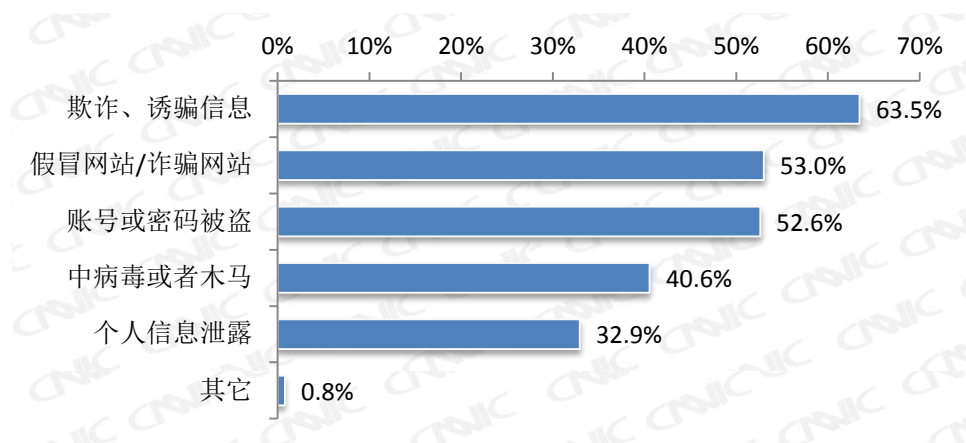


图 20 电脑即时通信发生的安全问题

5.2 即时通信安全事件防范情况

发生即时通信安全事故的人群中，即时通信时的安全防范意识不足。仅有 89.1% 的人不接受对方通信端的不明请求，84.0% 的人不点击来路不明的链接，77.3% 的人接受数据前会确认内容。

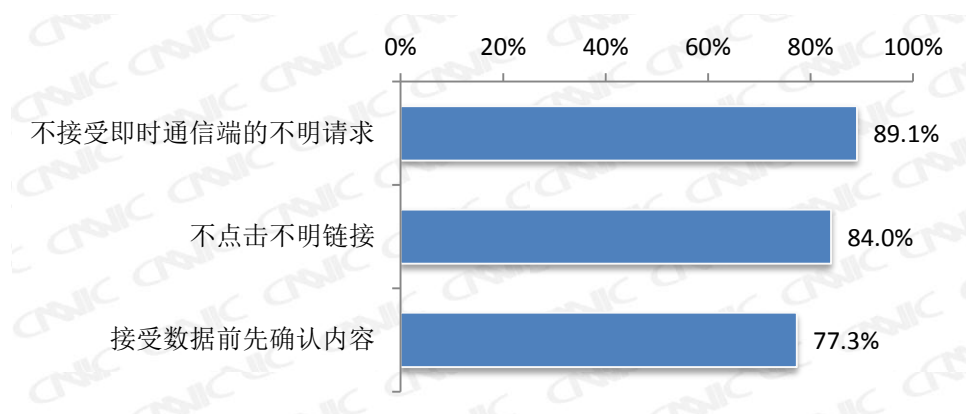


图 21 发生即时通信安全事件人群的防范措施

6. 电脑网上下载安全状况

6.1 网上下载安全事件类型及发生比例

网上下载是所有互联网应用中发生安全事件比例最高的应用，过去半年有 13.3% 的电脑网民下载时候发生过安全事件。

在因网上下下载发生安全事件的人群中，有 86.1% 的人遇到了数据包加载木马/病毒等情

况，53.8%的人遇到过网上发布的欺诈、诱骗信息，还有 48.6%的人遇到过假冒网站/诈骗网站。当前很多不知名的下载网站提供免费的文件下载，但常附带很多安装条件，且常伴随着木马病毒等恶意程序，用户下载后如不进行杀毒即运行，很容易遇到上述安全事件。

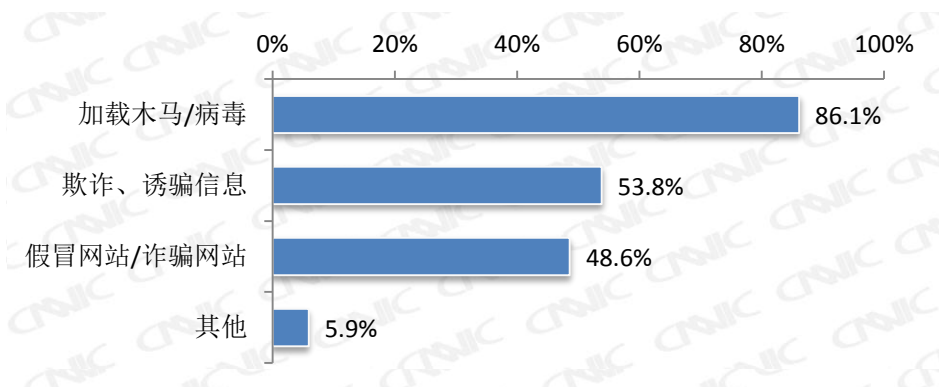


图 22 电脑网上下下载发生的安全问题

6.2 网上下下载安全事件防范情况

对于网上下下载遇到安全问题的人群中，只有 82.4%的受害者不安装软件捆绑附带的功能，82.1%的网民不点击运行不明工具，78.4%的人下载后先用杀毒工具杀毒再打开，76.7%的人从不去不知名的网站上下下载软件。部分网民网上下下载过程中，安全措施做得不到位，导致各种安全事件有了可乘之机。

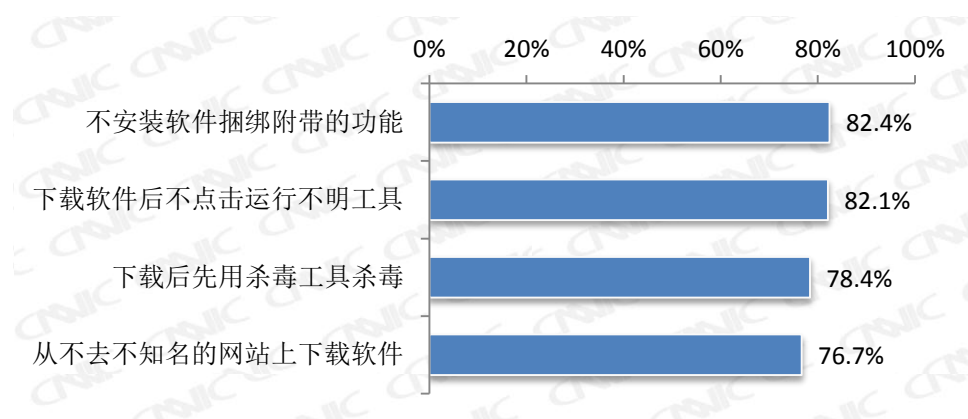


图 23 发生网上下下载安全事件的人群防范措施

7. 电脑网络支付安全状况

7.1 网络支付安全事件类型及发生比例

因电脑端网络支付发生安全事件的网民占整体电脑网民的 1.5%，虽然整体比例较小，但网络支付安全事件发生后危害严重，损失较大，也不容忽视。

在因网络支付发生安全事件的人群中，遇到假冒网站/诈骗网站的比例达 57.1%。近年来，假冒的钓鱼网站较为猖獗，已经成为互联网安全的主要危害之一。此外，遇到个人信息泄露的比例为 39.3%，资金被盗被骗和账号密码被盗的比例达 32.1%。

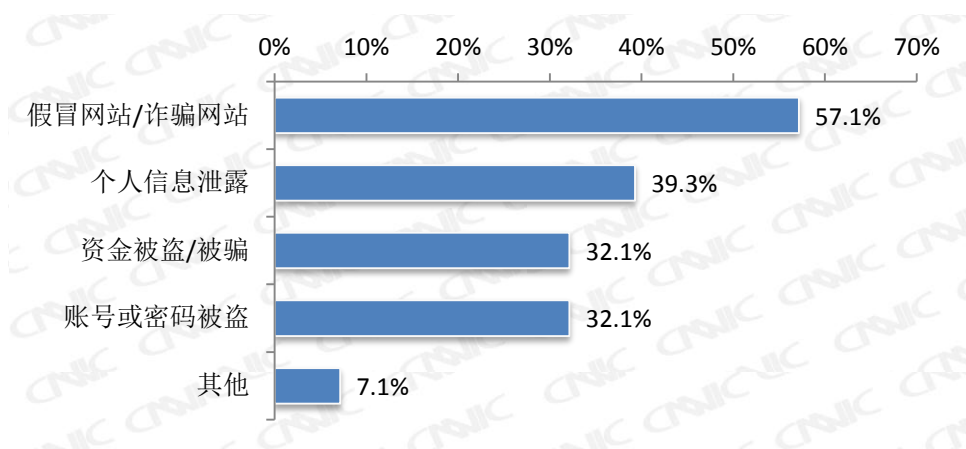


图 24 电脑网上支付发生的安全问题

7.2 网络支付安全事件防范情况

发生网络支付安全问题的人群中，针对网络支付的安全措施普及相对不到位，只有 82.4% 的人设置了强安全密码（数字字母大小写结合），更只有 79.4% 的人不随便登陆别人发的网站，仅有 67.6% 的人不在网吧等公共场所输入账号信息，安全防范意识不够普及，是网络支付遇到安全问题的主要原因。

鉴于网络支付安全事件危害严重，针对网络支付而开发的一些安全措施也较多，比如绑定手机、账号实名制认证、设置强安全密码、办理动态密码或口令卡、安装数字证书等，上述很多方式是部分网络支付成功的必要步骤，但普及率仍有待提高。

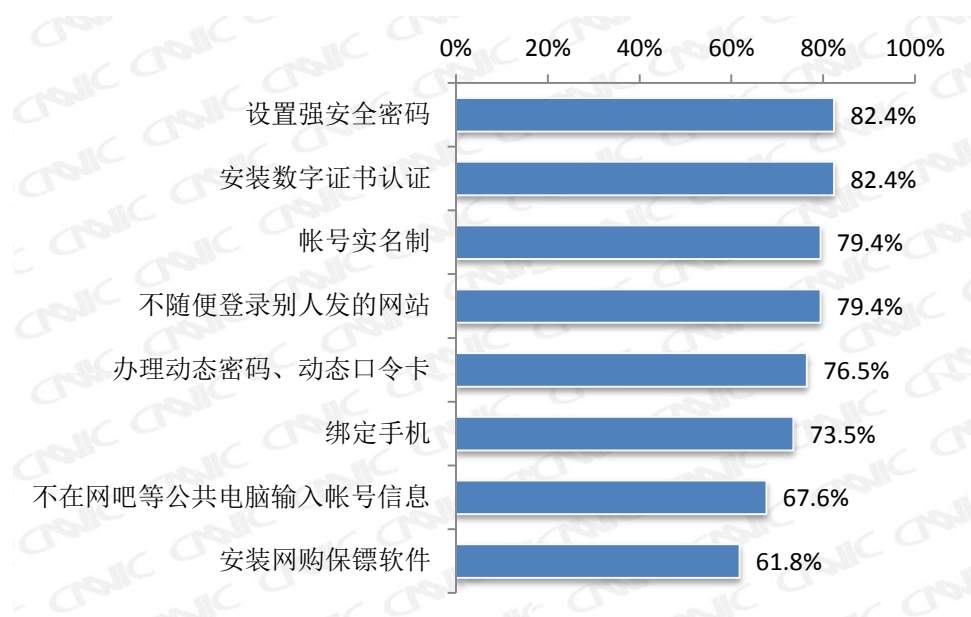


图 25 发生网络支付安全事件人群的防范措施

8. 电脑网络游戏安全状况

网络游戏安全事件在电脑网民中的发生比例为 4.2%，整体比例不是很高，但因为网络游戏安全事件常常是账号被盗、装备被卖等，此类安全事件对网民的影响较大。

网络游戏安全问题中，最常见的是游戏被盗号后装备被卖，占因玩网络游戏发生安全事件的网民的 56.0%，这也是职业盗号者的首要目的。其它常见的安全事件为中病毒或木马、账号密码被盗、游戏中欺诈信息、个人信息泄露等，发生比例分别为 52.7%、51.6%、51.6%、22.0%。

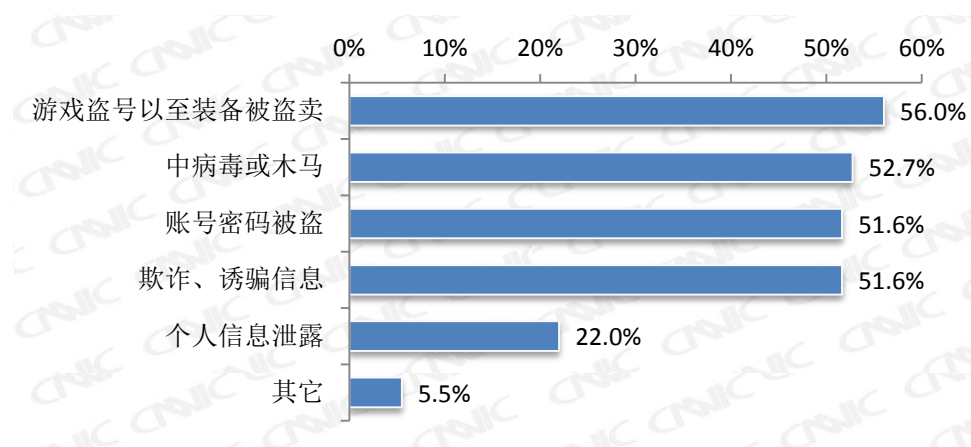


图 26 电脑网络游戏发生的安全问题

第四章 中国网民手机信息安全状况

1. 手机安全事件发生类型及比例

在智能手机上网用户群中，接收到手机垃圾短信/骚扰短信、骚扰电话的比例分别达 68.6% 和 57.2%，近年来随着手机安全软件屏蔽垃圾短信和骚扰电话的力度增加，此类事件的发生概率有所下降，但比例仍然较高。骚扰短信多以广告和推销为主，同时包含部分诈骗信息，而骚扰电话种类繁多，常见有两种：一种方式是拨一下即挂断，让用户回拨收取高昂的话费或者播放中奖等诈骗信息，不明真相的人则可能陷入其编制的一套骗局之中；另一方式是拨打接通后直接告诉用户中奖信息、或以熟人名义骗取钱财等。

值得一提的是，智能手机上网用户遇到恶意软件的比例达到了 33.2%，比例较高，很多软件以某种功能为载体供用户下载安装，之后频繁发送广告、或暗地刷流量或乱扣费，让用户遭受损失。

此外，手机上网也遇到诈骗网站、手机中毒或木马、手机联系方式泄露、账号密码被盗、手机地址簿被盗等问题。这些安全事件虽然发生的比例较小，但危害极大，应引起重视。

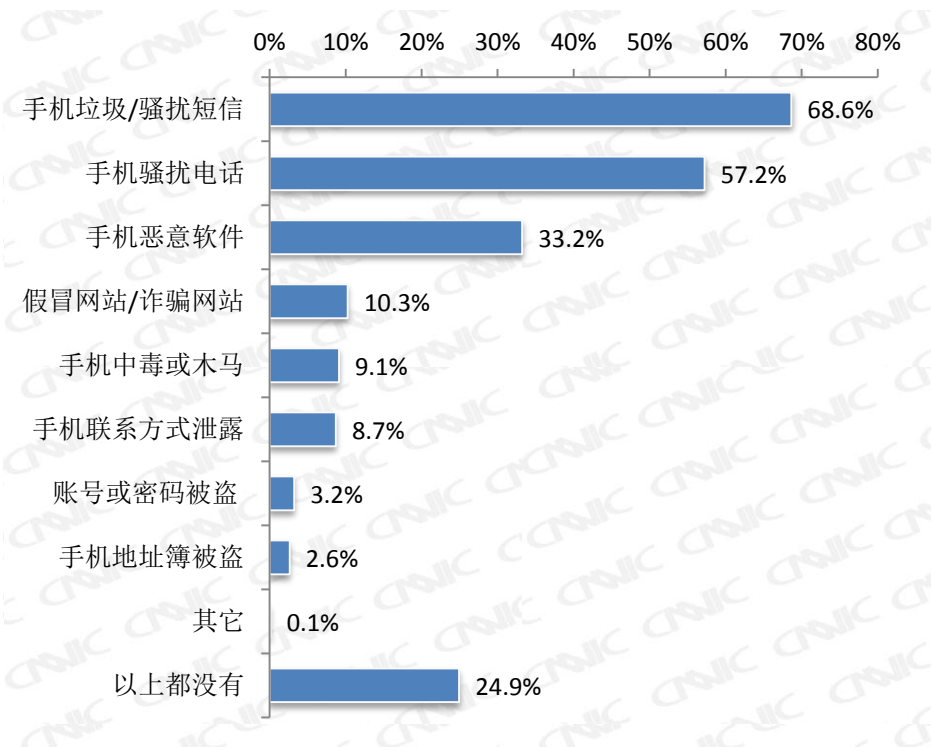


图 27 中国手机信息安全问题的类型及比例

2. 手机安全事件发生情景

在手机上网人群中，除了骚扰电话和垃圾短信外，发生安全事件概率最多的是手机浏览网页，发生比例达 16.8%；其次为手机游戏，发生比例达 13.8%；再次为手机聊天工具和手机下载文件，发生比例在 12%左右；其它方面，手机搜索引擎、手机购物、手机支付等也可能导致安全事件。

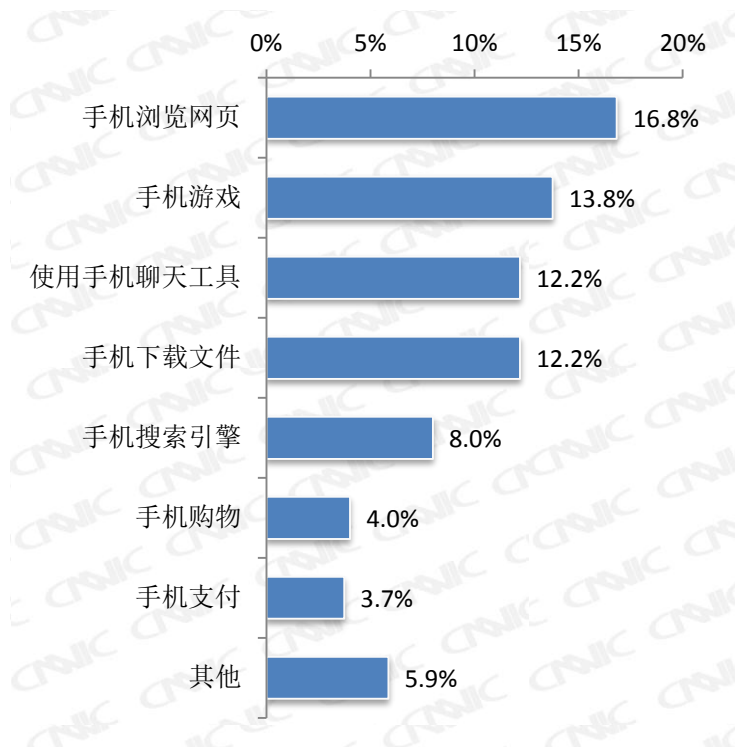


图 28 手机安全事件的发生情景

第五章 中国网民安全软件安装情况

1. 安装情况

96.5%的电脑上网用户安装了安全软件，远高于智能手机上网用户的 70.0%。电脑上安装安全软件已经较为普及，但手机上普及率还不够。

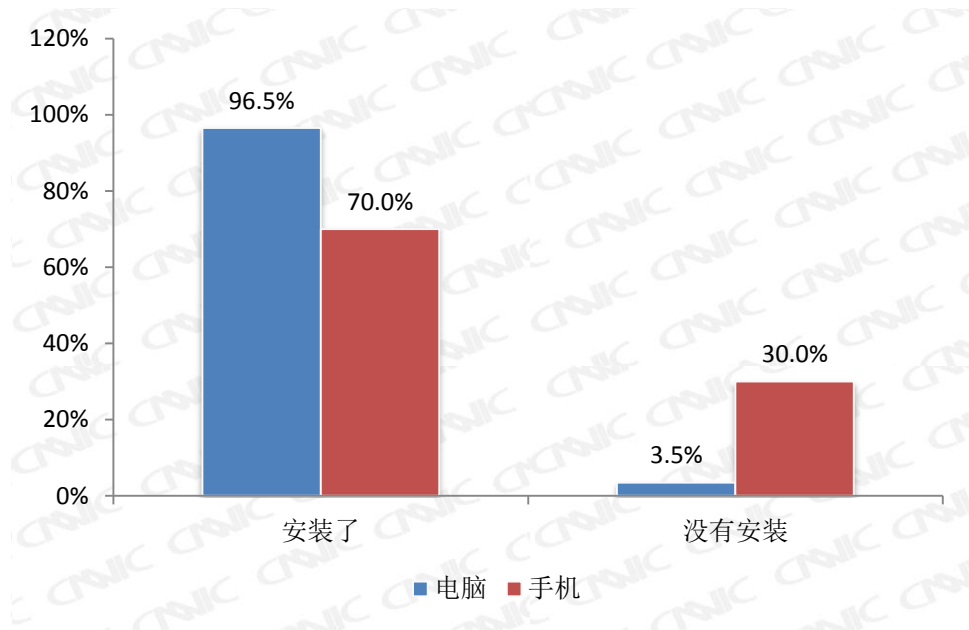


图 29 安全软件安装普及情况

2. 不安装原因

之所以不安装安全软件，“没发生过安全事件，不需要”是主要原因，电脑端上网网民选择比例为 46.2%，手机端网民选择比例达 68.7%，这部分网民因为没有发生过安全事故，信息安全的危机意识不足。

此外，15%左右电脑/手机端未安装安全软件的网民都担心安装后，设备运行或上网速度变慢，是网民不安装安全软件的第二大原因。此外，对安装知识欠缺，对安全软件不信任，也是网民不安装安全软件的原因。

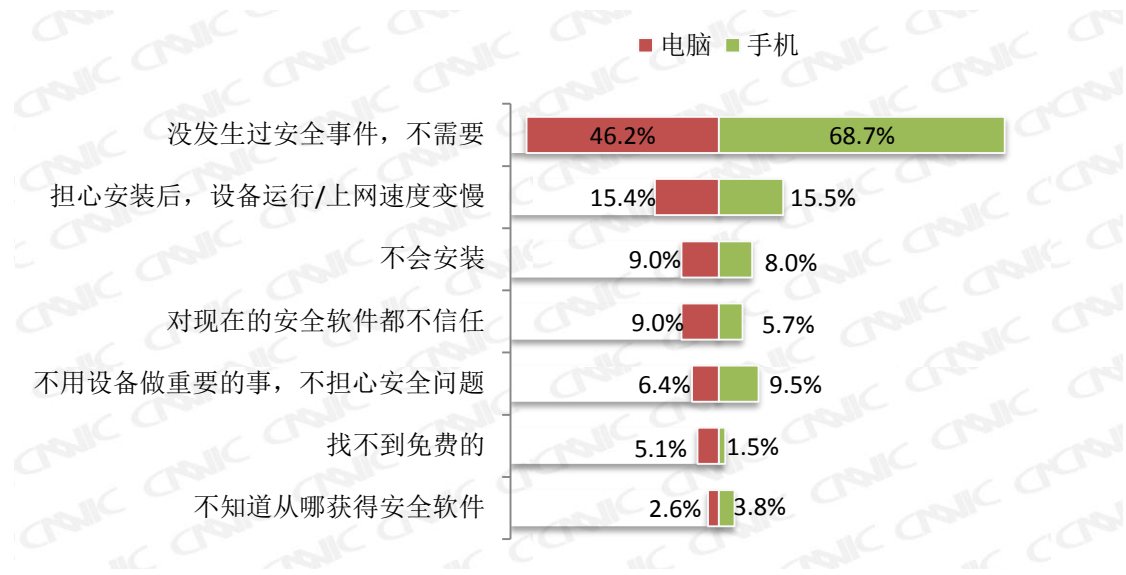


图 30 不安装安全软件的原因

3. 手机安全软件使用情况

手机安全软件有手机管理和安全防范两大功能：其中手机管理包括清理手机内存、延长待机时间、管理开机启动项、管理短信以及管理电话号码等业务，其目的是让手机使用更流畅、提高设备的使用效率；手机安全防范包括流量监控、屏蔽骚扰电话、定期扫描、定期杀毒等业务，目的是让手机远离安全威胁。总体来说，当前手机安全软件对智能机上网起到了非常重要的作用。

手机上网用户安装手机安全软件后，使用最多的是清理手机内存，使用比例达到了 86.6%，其次为流量监控，使用比例为 79.0%，第三为屏蔽骚扰电话，使用比例为 77.1%。手机内存有限，而用户手机里的应用越来越多，内存占用较大，是手机上网用户经常使用安全软件清理内存的主要原因。而当前手机上网大多采取包流量的形式，手机用户必须随时知道自己的流量耗费情况，因此流量监控使用比例也很高。

其它业务应用上，定期杀毒、开机自动启动、定期扫描、延长待机时间、管理开机启动项、管理短信和电话号码的比重都在 50%以上，也是人们使用手机安全软件的重要内容。

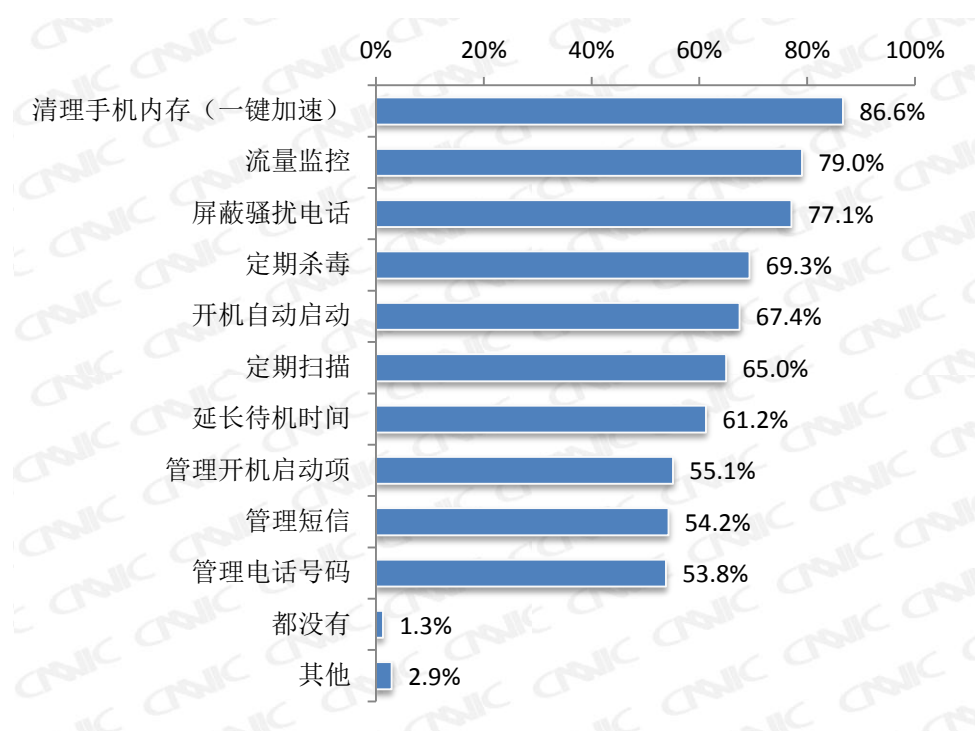


图 31 网民在手机上使用安全软件的功能

第六章 结论

1. 中国网民信息安全状况不容乐观

中国网民信息受到信息安全困扰比例仍然很大，74.1%的网民在过去半年内遇到过安全问题，总人数达 4.38 亿，其中因使用搜索引擎遇到过安全问题的网民达 3004.6 万人，因网上购物遇到过安全问题的网民达 2010.6 万人。信息安全影响网民的时间之长、规模之大前所未有。发生信息安全后，网民受到影响比例仍然很大，有 60.1%的人认为造成了影响。信息安全的影响体现在多方面，第一点是让网民花费时间和精力来应付这些事情，第二点让网民的学习或生活受影响，第三点是让网民的重要资料或信息丢失，最后是让网民直接遭受经济损失，过去半年网民因信息安全事件而造成的个人经济损失达到了 196.3 亿元。

信息安全带来的危害不仅体现在网民方面，更进一步破坏了互联网秩序，加重了人们在虚拟世界中的不信任度，对互联网经济带来严重的打击，提升中国网民信息安全刻不容缓。

2. 中国网民信息安全防范意识不足

在发生安全事件的网民中，信息安全防范意识还有待提高。虽然有 93.3%的人安装了安全软件，85.9%的人不安装来历不明的软件，85.4%的人不轻易在网上透露个人真实信息，83.8%的人不随便点击可疑的链接，但仅有 75.2%的人使用系统自动更新/打补丁，只有 67.3%的人设置复杂密码，只有一半的人在不同网站设置不同账号或者密码，以上常见的个人安全防范措施还没有完全普及，是信息安全事件发生的主要原因。对于发生安全事件以后的处理措施中，有 80.8%的人会杀毒，四成左右的人会重新安装软件、重装系统、屏蔽网站，采取其它措施的比例较小。

3. 智能手机安全措施做得不到位

智能手机上安装安全软件的用户仅为 70%，有三成智能手机用户都没有安装安全软件，其中一半人认为“没有发生安全事故，不需要”，但近年来针对手机而出现的恶意软件和病毒木马越来越多，乱扣费和骗流量的软件会对手机用户直接造成经济损失，其危害程度不亚于电脑端同类安全问题。

网民手机端安全防范意识不足，给大量手机恶意软件和病毒有机可乘，使这些手机用户直接面临着信息安全威胁。加大手机安全意识的普及，是今后相关企业和部门的任务之一。

版权声明

本报告由中国互联网络信息中心（CNNIC）制作，报告中所有的文字、图片、表格均受到中国知识产权法律法规的保护。引用本报告文字或图片，需注明出处为 CNNIC。

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)

2013 年 9 月



CNNIC

中国互联网络信息中心

China Internet Network Information Center (CNNIC)