中国网民权益保护调查报告2015

中国互联网协会
Internet Society of China

目录

关于网民权益

网民权益的初步定义：网民因使用互联网产品、服务及相关设备而应该享有的权益。

网民权益与网络安全、净化互联网环境、消费者权益等概念有相似、重合部分，但又都有明显的区别。

网民权益主要包括：

安宁权，即避免骚扰的权利。未经用户请求或许可，不得发送商业性信息，包括电子邮件、短信、电话等。非请自来的广告信息，侵犯了网民的安宁权，对网民形成了骚扰和侵害。对于各类商业性信息，网民有拒绝的权利，相关产品和服务应该设置便捷有效的拒绝方式，任何人和机构不得为网民的拒绝设置障碍。

接收真实信息的权利，即避免遭受不实信息诈骗的权利。假冒网站、钓鱼网站，冒充公众机构的诈骗电话、伪基站短信等，均向网民传递虚假信息，对网民获取真实信息的权利形成了侵害。网站上的下载量、销售量及网友点评情况造假，也是对网民权益的侵犯。

知情权和选择权。比如，网民对自身上网设备上的软件，在安装、卸载、获取、上传信息等情况具有知情权和选择权。“我的手机我做主”，任何人不得代替用户进行选择。静默安装、新手机预装、无法卸载等行为均在一定程度侵害了网民的选择权。

信息保护的权利，即避免个人信息泄露的权利。任何组织和个人不得窃取或者以其他非法方式获取公民个人电子信息，不得出售或者非法向他人提供公民个人电子信息。收集、使用公民个人电子信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意，不得违反法律、法规的规定和双方的约定收集、使用信息。网民发觉个人信息泄露之后具有主张的权利，即被遗忘权，相关互联网企业应予以配合。

报告主要观点

1. 在对网民权益认知情况的调查中，网民对隐私权的认可度最高。其次是选择权、知情权和安宁权。
2. 在有关安宁权的调查中，恶意软件是网民最反感的骚扰来源，其次是骚扰电话和网络弹窗。相比前三者，网民对垃圾短信和垃圾邮件的反感程度较低。
3. 七成左右的网民认为“诱导用户点击”、“无法关闭广告信息”、“手机、电脑中的软件不知道怎么来的”、“预装软件无法卸载”是侵犯网民知情权和选择权的主要问题。
4. 网络诈骗侵犯了网民获取真实信息的权利，本次调查中罗列了五类诈骗现象，其中最严重的是“冒充银行、互联网公司、电视台等进行中奖诈骗的网站”，占比达 76.3%；其次是“冒充 10086、95533 等伪基站短信”，占比为 55.3%；收到“冒充公安机关、卫生局、社保局等公众机构进行电话诈骗”的也超过半数，占 50.8%。
5. 近一年网民因为垃圾信息、诈骗信息和个人信息泄露等现象，导致遭受的经济损失人均 124 元，总体损失约 805 亿元（我国网民数量 6.49 亿 x 网民平均经济损失 124 元=804.76 亿元）。
6. 高达 7%的网民（估算约 4500 万）近一年由于各类权益侵害造成的经济损失在 1000 元以上。
7. 网民最关心的个人信息依次是：网络账号和密码（85.8%）、身份证号（79.0%）、银行卡号（70.8%）和手机号（61.6%）。而对网购记录、通话记录、网站注册记录、网站浏览痕迹、软件使用痕迹这类网上活动记录的关注度较低，占比仅为 33.8%、33.4%、26.7%、24.8%和 13.6%。此类信息的隐蔽性较强，往往不被认识到其重要性，对它的认知和保护还需要加强。
8. 网上活动记录作为网民重要的个人信息，调查结果显示其泄露情况非常严重，应引起重视。七成左右的网民个人身份信息和个人网上活动信息均遭到泄露。78.2%的网民个人身份信息（姓名、学历、家庭住址、身份证号及工作单位等）被泄露；63.4%的网民个人网上活动信息（通话记录、网购记录、网站浏览痕迹、IP 地址、软件使用痕迹及地理位置等）被泄露。近半数的网民个人通讯信息（即时通讯记录、手机短信等）被泄露。
9. 82.3%的网民亲身感受到了由于个人信息泄露对日常生活造成的影响。几乎半数（49.7%）的网民认为个人信息泄露情况严重或非常严重。

10. 网民使用搜索引擎时遭遇的最严重侵权现象是“搜到假冒网站/诈骗网站”（62.6%）和“搜索结果不是我想要的”（61.7%）。网民认为搜索引擎企业所做的保护措施最为有效的是“网站标识”（例如：加“V”、“官网”等认证），占 31.2%。其次是“提供个人信息保护服务，应网友请求可对个人信息进行删除”，占 22.3%；“提示风险网站”占 15.7%。
11. “网络水军/虚假评价”是网民在网购过程中遇到的最严重侵权现象，达 72.7%。由于网络水军刷销量、刷好评等现象向网民展示了虚假的信息，侵害了网民获取真实信息的权利。有 80.6%的网民认为“不明来源的购物 APP”是网购中风险最大的购物渠道。
12. 网民防范恶意 APP 的主要措施包括：“开发者第三方认证”（30.6%）；35.6%的网民认为应该通过提高自身安全意识来防范；22.1%的用户表示“举报、联动处置机制”能够有效防范恶意 APP。
13. 网民在使用网络社交工具的过程中遇到的侵权现象排名前三的是：“广告信息多”（70.8%）；“交友对象信息虚假”（49.2%）和“打色情擦边球”的现象严重（47.4%）。网民认为网络社交工具在保护网民权益方面做的最有效措施是“实名认证”，占 41.6%；其次是“建立对网站上传信息的审查机制”，占比 23.0%；认为“不良信用记录共享”比较有效的占 19.8%；认为“投诉举报机制”有效的占 13.3%。

调查背景

网民是互联网的主人。全国 6.49 亿网民的智慧和力量，是互联网这个新引擎的动力之源，维护网民的正当权益，就是维护互联网行业高速发展和繁荣兴旺的基础。但是，作为互联网主人的网民却在遭受各类不良信息和不良行为的骚扰和侵害。中国互联网协会 12321 网络不良与垃圾信息举报受理中心每天都接到上千件次的网民举报和投诉，对广大网民遭受的各种“疾苦”感同身受。

中国互联网协会作为沟通网民和互联网企业的桥梁，在网民权益保护工作方面责无旁贷。从 2013 年起，中国互联网协会开始尝试开展系统的中国网民权益保护调查工作，形成了我国第一份关于网民权益保护领域的调查报告：《中国网民权益保护调查报告（2014）》。该报告发布后，得到了媒体的广泛报道，引起了一定的社会反响，取得了良好的社会效果。一方面，引发了全社会对网民权益保护工作的进一步关注；另一方面，引导互联网企业发挥保护网民权益的主体作用，履行企业社会责任。

为了加强网民权益保护知识的普及，继续唤醒并提升网民自身权益保护的意识，中国互联网协会在以往的工作基础上，继续开展了网民权益保护问卷调查，并尝试性地启动了保护网民权益创新&优秀实践案例的征集、评选工作，目的是展示互联网企业在网民权益保护方面的努力与成果，加强对网民权益保护相关工作的推广与宣传，使保护网民权益理念更加地深入人心。

调查内容和目的

1. 了解网民对网民权益的认知情况，进一步唤醒网民权益保护意识；
2. 了解网民权益损失状况，明确权益保护工作的重点；
3. 对当前侵犯网民权益的热点问题进行专项调查；
4. 总结典型网络应用场景侵权现象；
5. 对部分典型应用场景的具体保护措施进行探索。

调查方式

网民权益保护调查采用定性和定量调查相结合的方法。

定性部分，主要依靠桌面研究的方式；定量部分，主要采用在线问卷调查的方式进行，问卷名称为《2015 中国网民权益保护调查问卷》（以下简称“问卷”），辅以第 16 次中国反垃圾短信半年度调查、第 37 次、第 38 次中国反垃圾邮件季度调查、2014 年 7 月至 2015 年 6 月期间网民向 12321 网络不良与垃圾信息举报受理中心（下称 12321 举报中心）投诉的数据。

问卷调查对象为中国大陆网民。通过在中国互联网协会网站、12321 举报中心网站，以及部分中国互联网协会会员企业网站挂载问卷链接的方式，由网民主动参与填写问卷的方式，获得样本。

问卷调查时间：5 月 15 日~6 月 15 日。

整个问卷调查历时一个月，获得答卷 16925 份。

第一部分 网民权益的认知

1.1 最重要的网民权益

说明：网民权益指的是网民因使用互联网产品、服务及相关设备而应该享有的权益。

本次调查共 16925 名网民参与，90.5%的网民认为隐私权是其最重要的权益；其次是选择权和知情权，占比分别为 74.8%和 67.5%。

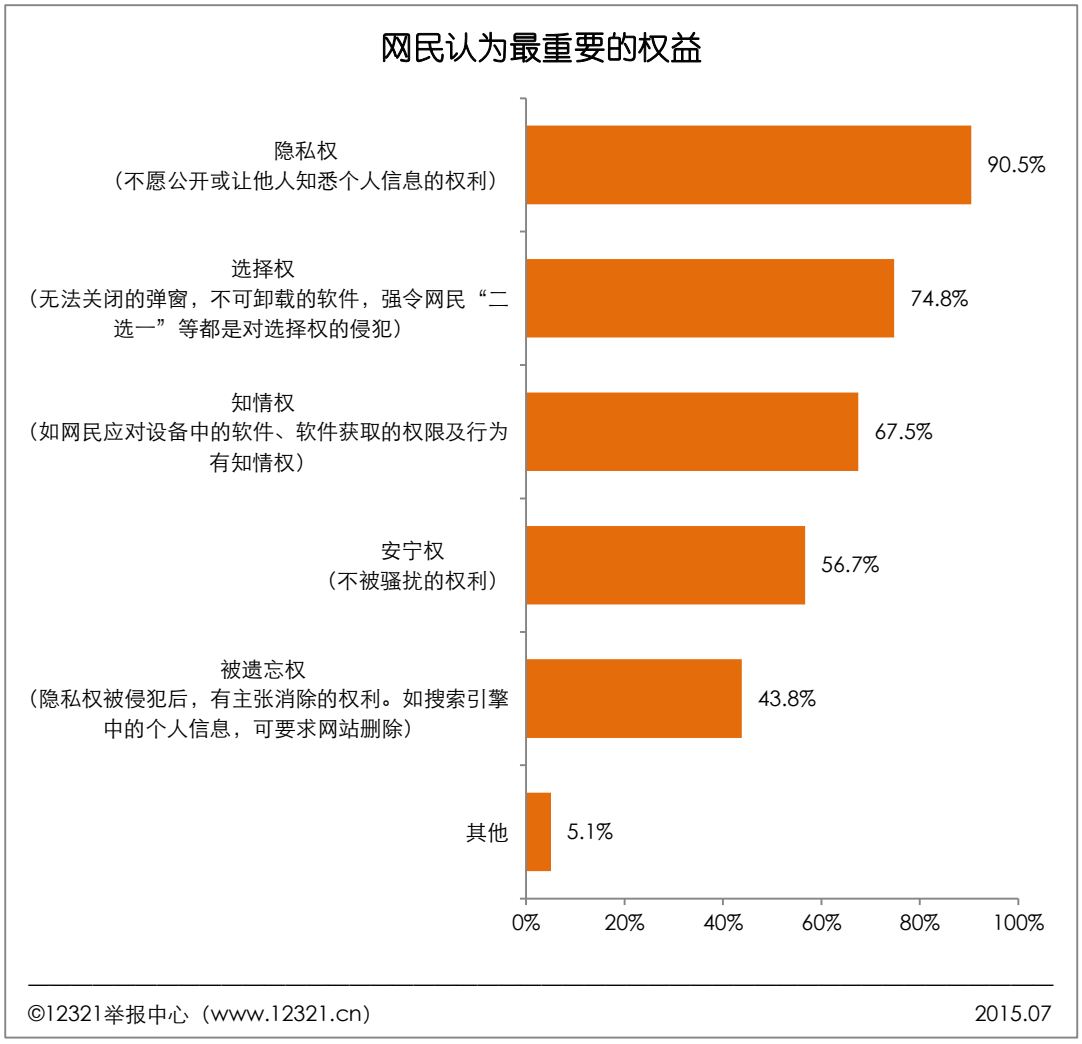


图 1

1.2 安宁权

对网民安宁权的调查结果，如图 2 所示，网民在上网和日常生活中，36.3%的网民最反感受到恶意软件的骚扰；29.0%的网民最反感来自骚扰电话的骚扰；24.2%的网民选择最反感网络弹窗的骚扰；来自垃圾短信和垃圾邮件的骚扰仅占 8.9%和 1.3%。

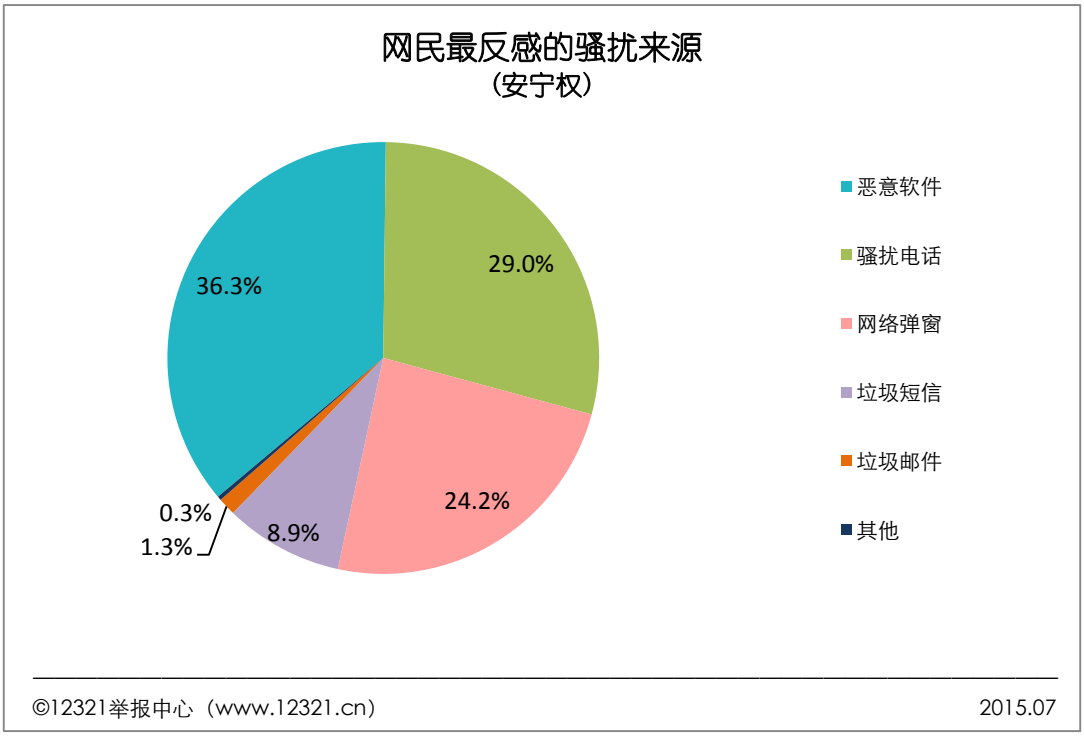


图 2

【法规原文】《全国人民代表大会常务委员会关于加强网络信息保护的决定》第七条：任何组织和个人未经电子信息接收者同意或者请求，或者电子信息接收者明确表示拒绝的，不得向其固定电话、移动电话或者个人电子邮箱发送商业性电子信息。

1.3 选择权和知情权

对网民选择权和知情权的调查结果，如图 3 所示，在网民上网的过程中，

“诱导用户点击”这一现象最为严重，85.5%的用户遇到过；

73.3%的网民“无法关闭广告信息”；

其次是“手机、电脑中有些软件不知怎么来的”严重侵犯了网民的知情权，占 69.6%；“预装软件无法卸载”（69.3%）；“浏览器首页被绑架”（52.0%）；“无法拒收商业短信”（51.4%）；“无法退订商业邮件”（32.9%）；

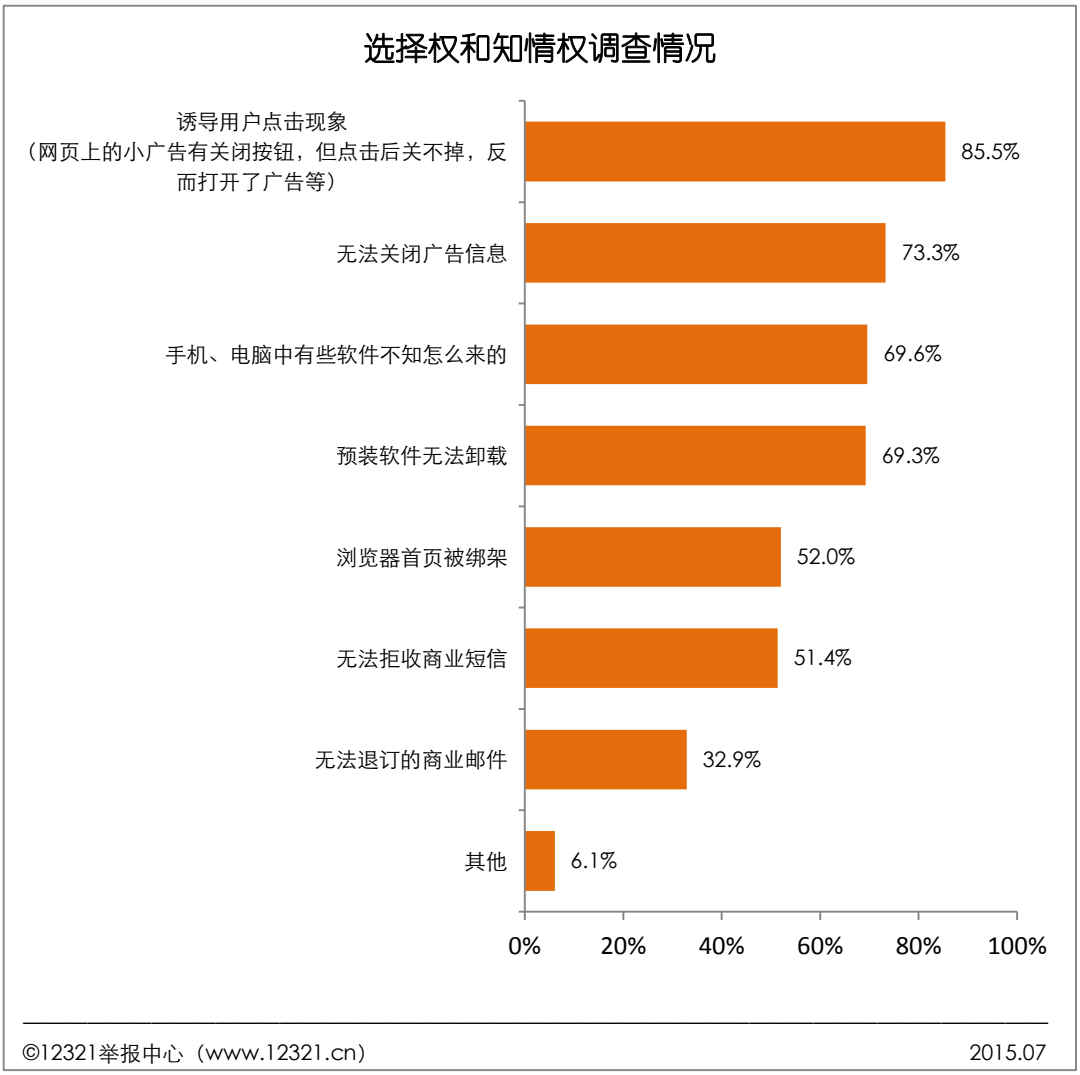


图 3

1.4 诈骗信息

网民具有接收真实信息的权利，但各类不实、诈骗信息充斥着用户的手机和电脑。其中遇到最多的诈骗现象是冒充银行、互联网公司、电视台等进行中奖诈骗的网站，占比达 76.3%；其次是冒充 10086、95533 等伪基站短信，占比为 55.3%；收到冒充公安机关、卫生局、社保局等公众机构进行电话诈骗的也超过半数，占 50.8%。

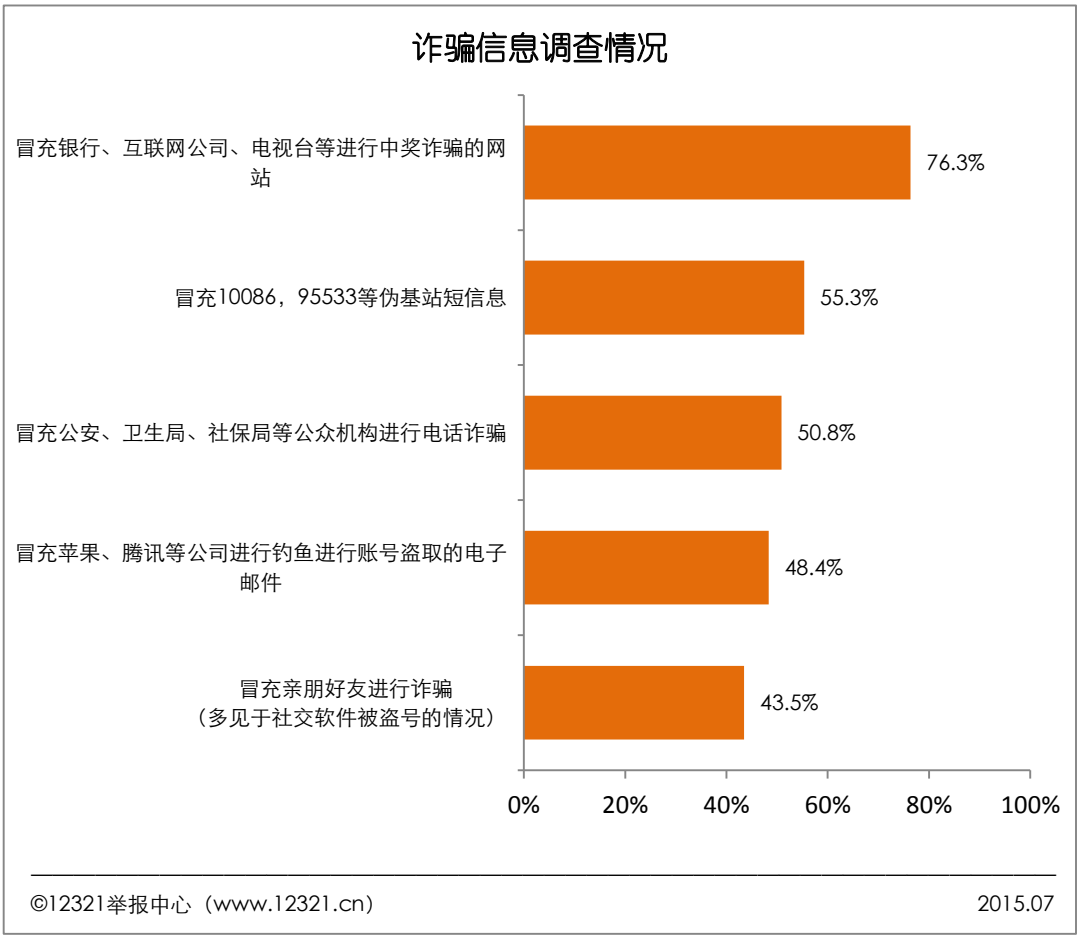


图 4

【提醒】12321 发布关于假冒运营商的伪基站诈骗提醒

“尊敬的用户，您的积分已经到账，请您尽快登录移动商城 10086.cn5ef.pw 兑换 249.36 元现金，以免积分过期失效”，这是一条典型的由伪基站发送的诈骗短信。点击进入该网站就会发现，领取积分需要提供银行卡号、身份证号、姓名、手机等各种重要的个人信息。不法分子利用伪基站，在一定范围内干扰正常手机信号，冒充任意号码向用户手机发送短信。这种“伪基站”信息不容易被用户识破，主要原因是该短信的确显示发自于某些常见的客服号码，用户见到熟悉的客服号码会放松警惕，容易上当受骗。短信中显示的钓鱼网站与真实的网站网址十分相似，也会让很多用户信以为真。此类诈骗在岁末年初尤其高发。12321 举报中心近十天接到此类钓鱼诈骗信息 80 多件次。

12321 举报中心通过网友举报的信息发现，此类短信主要分为两类诈骗手法：一类是向用户手机发送钓鱼网站链接，通过系统故障、升级、优惠、中奖、积分兑换活动等诱导用户登录钓鱼网站、获取用户个人信息；另一类是利用扣费、消费提醒、银行卡逾期等话题引诱

用户回拨电话并进一步实施电话诈骗。

12321 举报中心提醒，广大网友遇到此类短信要做到：不要轻易泄露银行卡账号、密码及个人信息；不轻信任何转账要求；不透露短信验证码。遇到网银升级、网银失效、积分兑换、短信扣费、银行卡逾期等诈骗短信时，要第一时间拨打官方电话进行核实或向 12321 举报中心咨询、举报。

【提醒】谨防假冒“奔跑吧兄弟”中奖钓鱼诈骗

近日浙江卫视《奔跑吧兄弟》节目热播，一些不法分子随即采用中奖短信和仿冒网站等手段进行诈骗和套取个人信息。12321 举报中心接到所谓“奔跑吧兄弟”的中奖诈骗信息也在逐渐增多。其诈骗短信样本如下：

登录“中奖”钓鱼网址后，按照网站系统提示输入兑奖的验证码后，网站弹出一个系统提示，内容为“恭喜您！验证通过，您已被系统确认为浙江卫视《奔跑吧兄弟》活动二等奖幸运用户！请您详细浏览阅读活动、按照网站提示进行领取奖项！”奖金及奖品的安全转账及运输风险抵押金共 4600 元，请 1 小时之内在 ATM 机转账办理保险抵押金。系统还显示，如不按时交取手续费，系统将自动把所填写的资料提交到您当地的法院起诉，要求违约用户按照法律和合同的规定承担赔偿违约金。不法分子借此来威胁用户，让其尽快汇款。为了让用户信以为真，骗子甚至还在中奖信息下方附上虚假的客服联系方式和公正信息。

12321 举报中心提醒广大网友注意：

第一、不法分子依托热点电视节目，炮制逼真的山寨网站对广大用户实施中奖钓鱼诈骗，是一种常见诈骗伎俩。用户如果访问这些钓鱼网站，并按照网站提示填写真实信息，将导致

个人信息的被盗，或被对方以所得税、手续费等骗取钱财，进而蒙受经济损失。

第二、《奔跑吧兄弟》的官方网站上已公布提醒：有关《奔跑吧兄弟》的相关中奖大家不要轻易相信，金额巨大的都是假的，另外官方的活动不会向你索要手续费等费用。

12321 举报中心提醒：收到此类中奖诈骗信息后，不要轻易打开短信中的网址链接，更不要泄露自己的个人信息，应尽快向“奔跑吧兄弟”咨询或向 12321 举报中心举报。

1.5 网民权益损失

根据调查，近一年网民因为垃圾信息、个人信息泄露或网络诈骗等现象，导致遭受的经济和时间上的损失，如图 5 所示。

我国网民数量 6.49 亿[1]，估算经济损失约 805 亿元。具体情况如下：

大部分网民没有遭受经济损失。68%的网民没有损失；13%的网民损失在 1 到 100 元之间；10%的网民损失在 100 到 600 元之间。

网民平均经济损失 124 元。32%的有损失的网民，平均经济损失 180 元。

少部分网民经济损失较大。高达 7%的网民近一年遭受的经济损失在 1000 元以上。

调查显示，三分之一的网民在时间上没有损失；14%的网民遭受的时间损失在 10 小时（不含 10 小时）以上，网民平均时间损失达 2.54 小时。

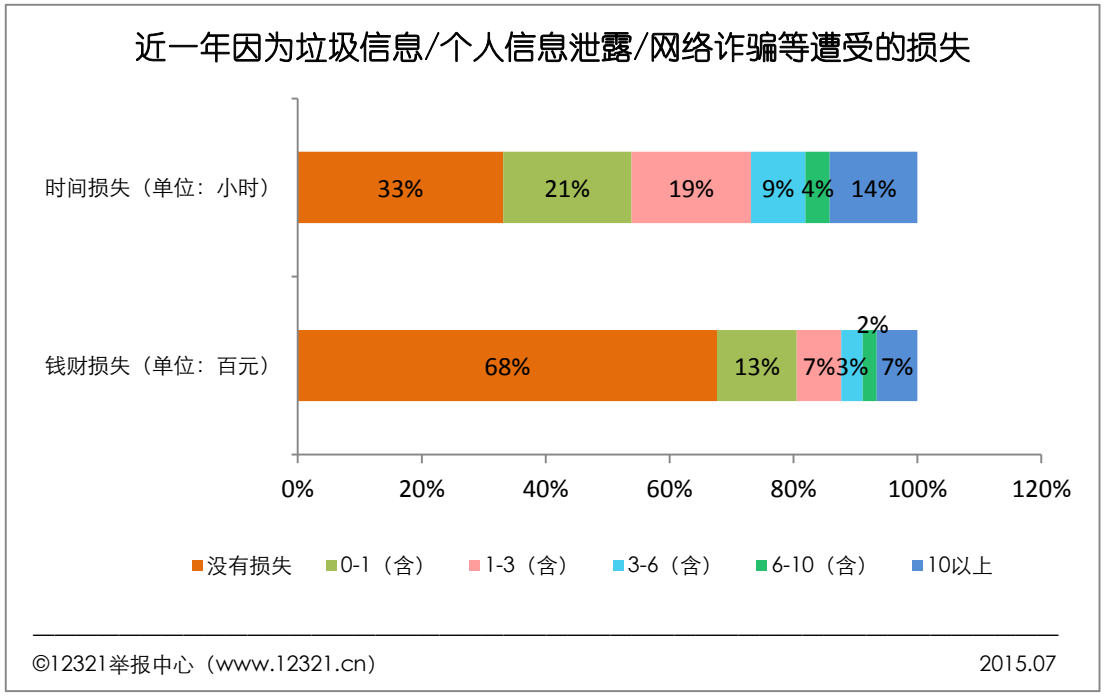


图 5

[1]根据 CNNIC 发布的《第 35 次中国互联网络发展状况统计报告》，截至 2014 年 12 月，我国网民规模达 6.49 亿。

第二部分 个人信息保护

2.1 个人信息的认知

个人信息是网民权益的重要组成部分，个人信息泄露也是网民权益遭受侵害最重要的领域。本次问卷共列出了 23 种个人信息供网民随机选择。

从调查结果看，与网民在上网过程中关系最为密切的网络账号和密码是网民认为最重要的个人信息，占比达 85.8%；

其次是身份证号、银行卡号和手机号，认知度也较高，均超过半数，分别为 79.0%、70.8%、61.6%；

而网民对网购记录、通话记录、网站注册记录、网站浏览痕迹、软件使用痕迹这类网上活动记录的关注度较低，占比仅为 33.8%、33.4%、26.7%、24.8%和 13.6%。此类信息泄露的隐蔽性更强，往往不被认识到其重要性，对它的保护还需要加强。

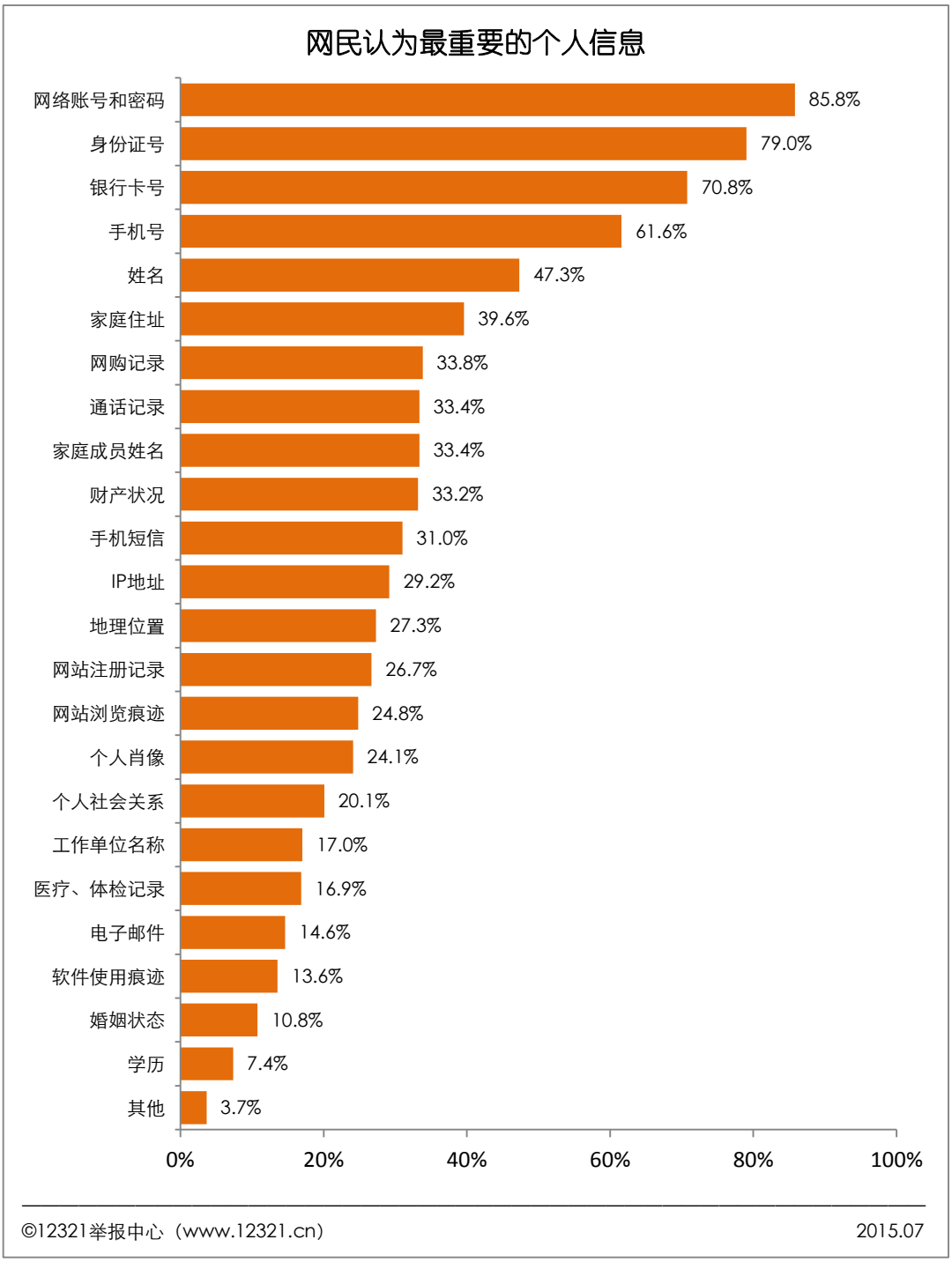


图 6

2.2 个人信息保护

网民个人信息泄露情况如图 7 所示：

超过半数的网民个人身份信息和个人网上活动信息均遭到泄露。

受利益驱动，手机号码、电子邮箱作为网民生活中必备的通信信息被一些不法分子贩卖，因此泄露情况最为严重。78.2%的网民个人身份信息被泄露过，包括网民的姓名、学历、家

庭住址、身份证号及工作单位等等。

随着 O2O、电子商务、精准营销及精准定位的发展，网民的个人网上活动在不知不觉中被自动抓取。63.4%的网民个人网上活动信息被泄露过，包括通话记录、网购记录、网站浏览痕迹、IP 地址、软件使用痕迹及地理位置等。

另外 49.9%的网民个人通讯信息（即时通讯记录、手机短信等）被泄露过。

12321 根据网民在举报中的描述，网民被泄露的个人信息包括姓名、身份证号、手机号码、家庭住址、社会关系、开房信息、邮箱、邮箱密码、网购订单信息、生育情况、购车、购房情况、工作职位、医疗体检记录等，涵盖的范围非常广泛。

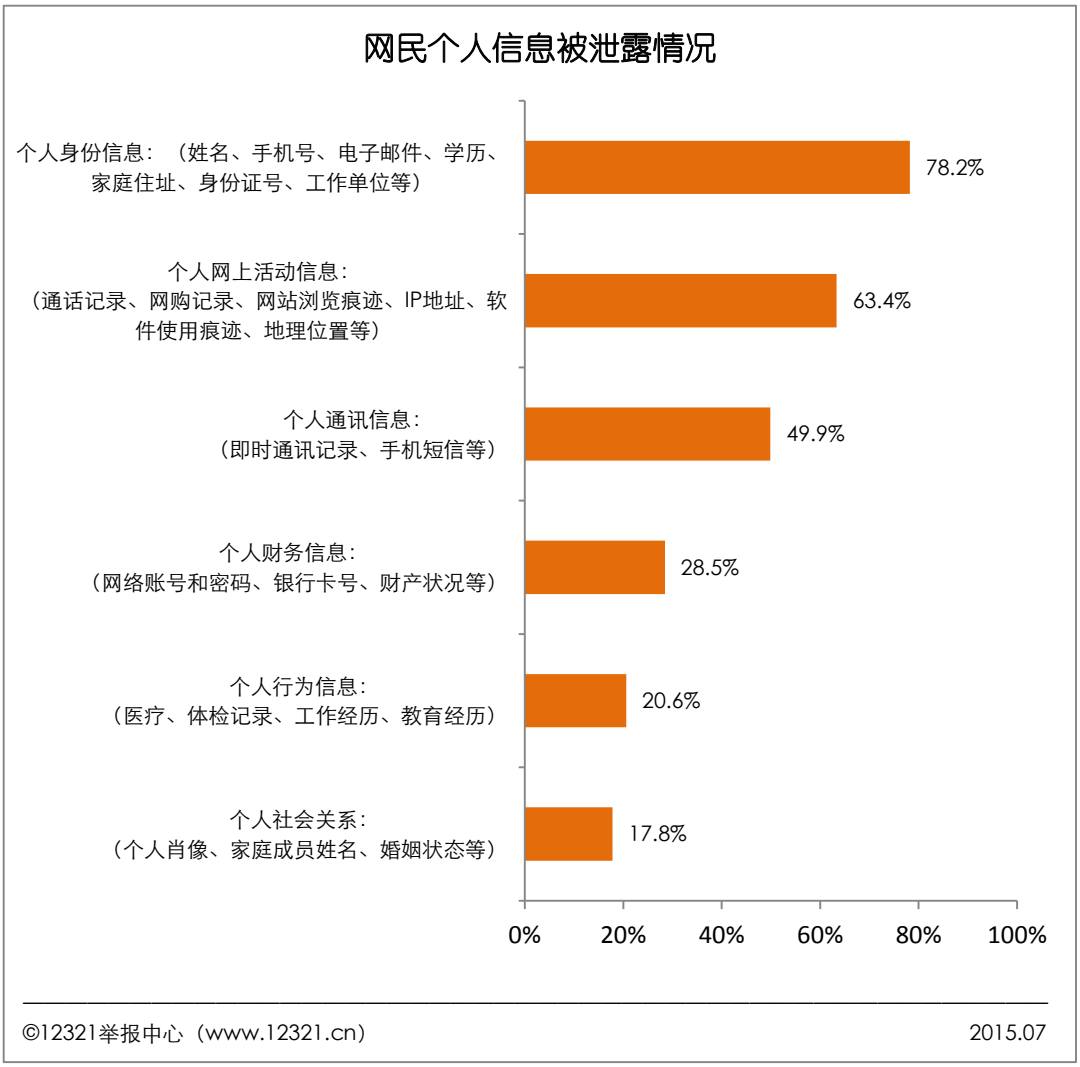


图 7

2.3 个人信息泄露程度

近两成的网民认为个人信息泄露非常严重。

本次调查中，50.3%的网民认为个人信息泄露一般；31.5%的网民认为个人信息泄露严重；18.2%的网民认为个人信息泄露非常严重。

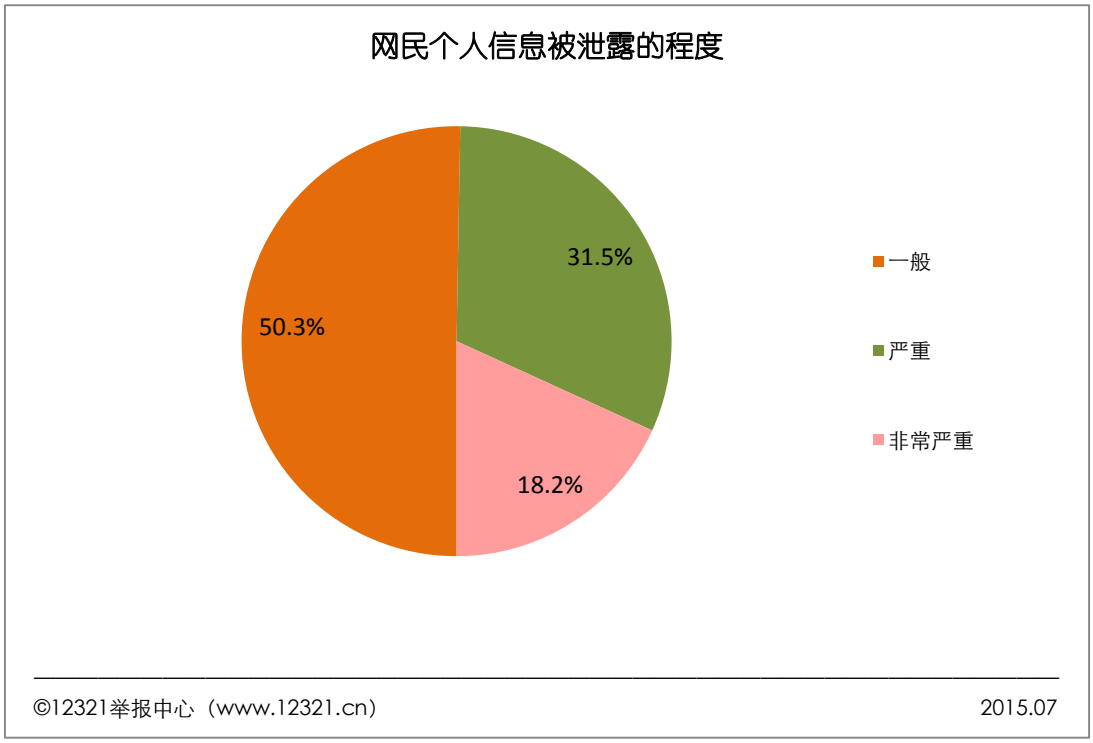


图 8

2.4 个人信息泄露带来的不良影响

82.3%的网民亲身感受到了由于个人信息泄露对日常生活造成的影响；17.7%的网民没有明显感受。

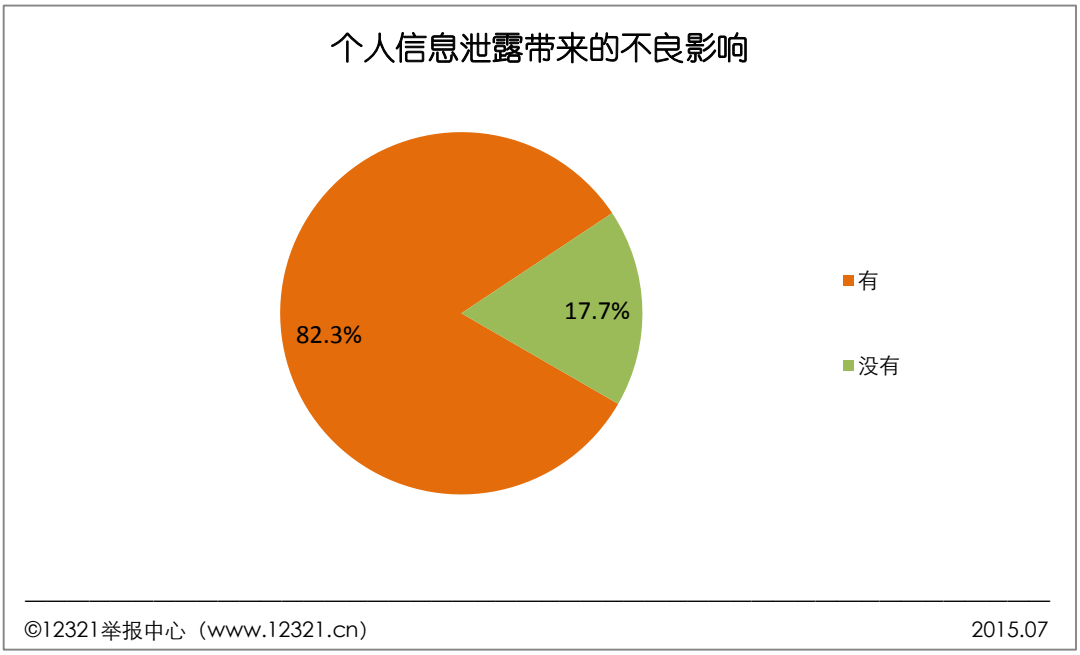


图 9

【分析】12321 据网民举报情况分析，个人信息泄露造成的危害有以下几点：

1、个人信息泄露导致垃圾信息泛滥

不少网友反映，一些从未接触过的商家向其发送垃圾短信和垃圾邮件，这些网友的个人信息可能已被泄露。而一些商家通过非法渠道获得大量用户的电话号码和电子邮件地址，并向其推送广告信息，甚至拨打电话进行营销，甚至部分信息被利用实施电信诈骗、敲诈勒索、恐吓威胁等违法犯罪行为。少数网民遭遇短信、邮件炸弹，生活遭受严重干扰。

2、个人信息泄露导致非法诈骗猖獗

个人信息泄露严重，是网络诈骗得以猖獗的重要原因。在网民举报当中，特别是虚假中奖、退款诈骗、游戏交易、虚假票务、钓鱼盗号等形式网络诈骗，都或多或少与受害者个人信息泄露相关。一些骗子在实施诈骗时，对受骗人的个人信息了如指掌，从而有针对性的设计精准的骗局，令人难以察觉和防范。

3、个人信息泄露造成的损失难以挽回

个人信息泄露之后，可能会被多次倒卖转移，使信息所有者受到进一步的骚扰和侵害，其造成的后果难以撤销，带来的损失难以挽回。实际上，网络的开放性使信息的监管成本大幅增加，而一些跨境犯罪行为的信息更加难以追踪。

【治理建议】根据个人信息泄露的情况，12321 提出 3 点治理建议：

1、强化举报处理机制，提高公众的安全意识。

对于网络上存在的个人信息泄露情况，一方面应鼓励网民举报，及时发现信息泄露线索，充分发挥公众监督的作用；另一方面应及时对网民举报的信息进行处理，减少信息泄露造成的影响和危害。同时应加强宣传，提高公众的自我保护意识，尽量避免出现个人信息泄露的情况。

2、严厉打击泄露个人信息的行为。

对含有泄露个人信息内容的网站，应参照钓鱼网站的处理模式，及时采取封堵关停等处置措施；对涉及个人信息交易的信息，应及时删除，并追究相关责任人的法律责任。

3、严格规范网站公示的个人信息。

应禁止在网络上公布个人的身份证号码、手机号码、电子邮件地址等个人信息。对在网站上公示的姓名、地址、相应联系方式等信息应予以规范。如，中奖手机号码公布时应遮蔽中间四位；学校公布的学生信息不得完全公开，应采取必要的加密保护措施等。对不符合要求的网站应立即通知其进行整改。

第三部分 典型应用场景侵权现象及防范措施

3.1 搜索引擎

- **使用搜索引擎时碰到的侵权现象**

搜索引擎作为网民重要的上网场景，用户在使用时遭遇到的侵权现象依次为“搜到假冒网站/诈骗网站”，占搜索引擎使用者的 62.6%；“搜索结果不是我想要的”有 61.7%；“搜索到的网站有淫秽色情信息或附带木马或病毒”的有 58.0%；认为“竞价排名和推广破坏了搜索引擎的准确性”的有 56.6%；“搜索条件所匹配的官方网站位置靠后”的占 45.9%。

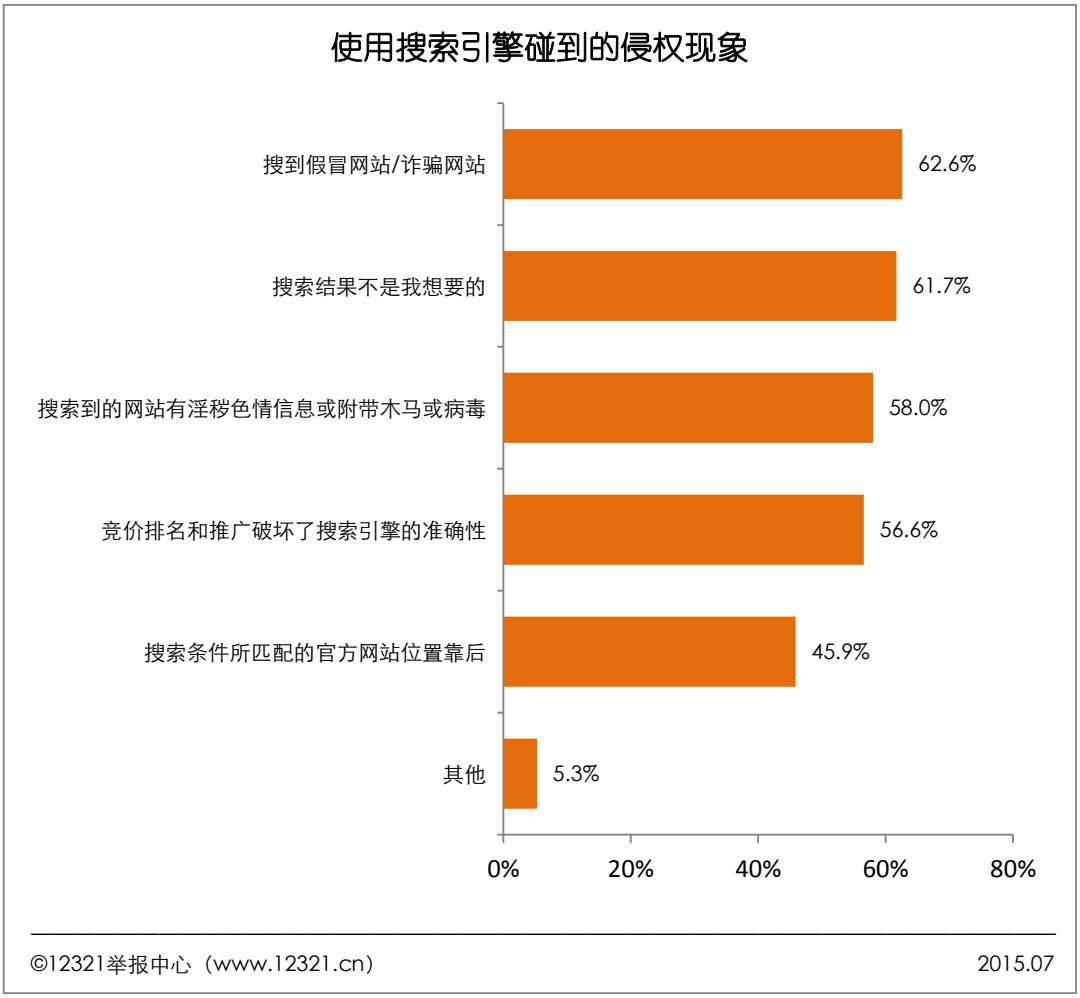


图 10

- **搜索引擎在保护网民权益上所做的最有效的保护措施**

针对搜索引擎中的各类侵权现象，网民认为企业所做的保护措施最为有效的是“网站标识（例如：加‘V’、‘官网’等认证）”，占 31.2%；其次是“提供个人信息保护服务，应网友请求可对个人信息进行删除”，占 22.3%；“提示风险网站”占 15.7%；14.9%的用户认为

“搜索结果中增加举报标识”的措施最为有效；14.7%的用户认为“屏蔽色情网站，保护未成年人”的措施做的较好。

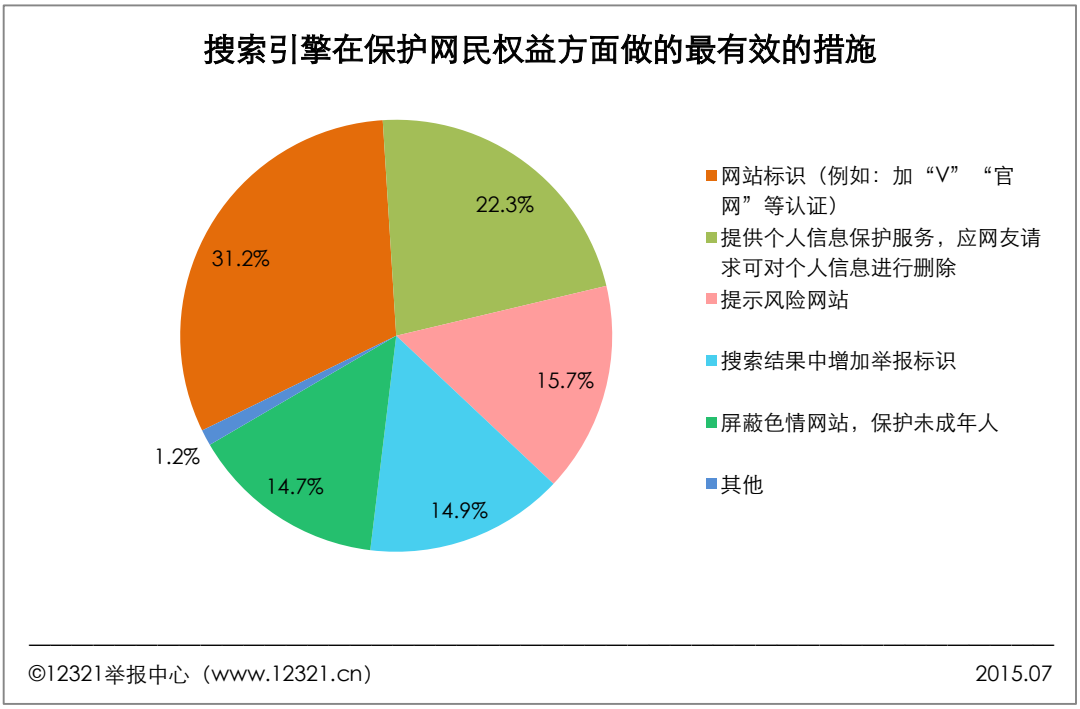


图 11

3.2 网络购物

- **网购中碰到的侵权现象**

网民在网购的过程中遇到的侵权现象如下：“网络水军/虚假评价”的现象最严重，达72.7%;“假冒网站/诈骗网站”、“个人信息被泄露”的现象也均超过半数，占比分别为 53.9%、52.4%；“网购信息被泄露”的占 41.5%；“钱被盗或被骗”的占 17.4%。

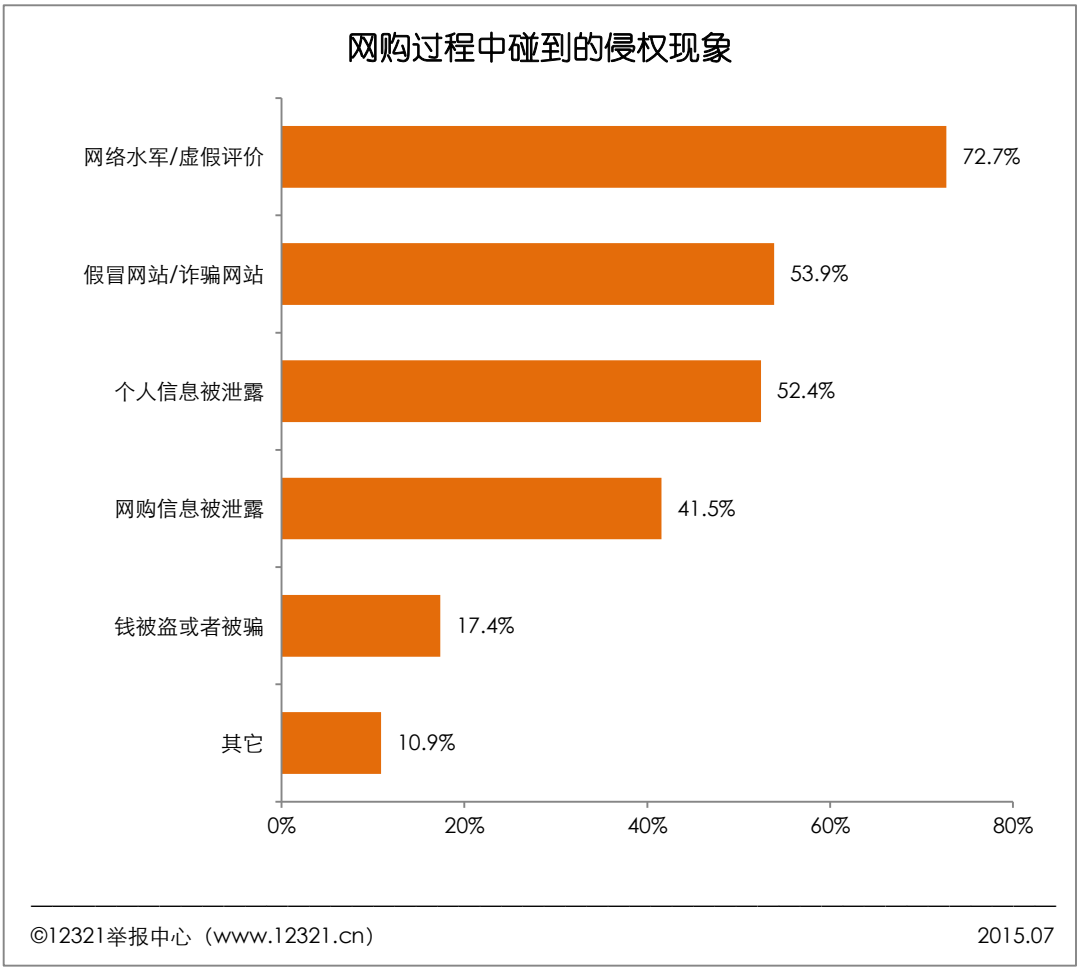


图 12

【法规原文】《网络交易管理办法》第三十六条规定：为网络商品交易提供信用评价服务的有关服务经营者，应当通过合法途径采集信用信息，坚持中立、公正、客观原则，不得任意调整用户的信用级别或者相关信息，不得将收集的信用信息用于任何非法用途。

【提醒】谨防假冒支付宝订单处理退款中心诈骗

4 月以来，12321 举报中心接到有关“假冒支付宝订单处理退款中心”的诈骗举报数量就达到了 20 余件次。不法分子利用木马病毒盗取网民支付宝信息，制作虚假退款页面让网民填写有关银行卡账号及密码信息，进一步盗取用户的账户存款。12321 举报中心特别提醒广大网民朋友，谨防假冒支付宝订单处理退款中心的诈骗。

一位周姓网民朋友向 12321 举报中心举报称，4 月 17 日，她在帮助朋友购买衣服时候，刚刚从天猫上拍下一件价值 139 元的连衣裙，可是刚刚下完订单 5 分钟后，周女士接到一个自称是支付宝订单处理退款中心的电话，对方称您是不是在天猫上购买了某品牌的衣服，抱歉您的订单出现异常，发不了货，需要您重拍。周女士一想，我们的钱都付过了，怎么办？

对方立刻解释，钱可以退的，随即以所谓淘宝客服形式发一个链接过来，周女士心有提防有点犹豫，电话中对方说，您也可以直接从自己的淘宝账号登陆退款，这下周女士没有防备，就登陆自己的淘宝账号，对方让周女士点击账户的头像，随后提醒说在订单号前是不是看见一个灰色小旗帜？周女士果然发现了自己的订单号前有小旗帜，周女士将鼠标放在小旗帜位置立刻显示一个网页地址，于是周女士打开了这个网页，进入了所谓的“支付宝订单处理中心”页面，此刻周女士已经完全相信电话中的人，于是按照相应提示输入了身份证、银行卡、手机号、支付密码等信息。此刻，电话另一端的人还问周女士是否有网银或信用卡，周女士回复没有后，等了一会不但没有收到退款，反而是收到银行提醒自己的卡上被划走了 3000 元钱。

经核查分析，该类诈骗主要有四个特点：一是锁定淘宝、天猫等高端网络购物群体；二是通过木马病毒盗取用户淘宝账号及密码，并且在用户的头像上植入虚假淘宝订单异常处理中心的页面地址；三是以所谓订单号前插入灰色小旗帜方式迅速获得用户信任；四是以电话诱骗用户输入有关身份证号码、银行卡号、手机号及密码。

12321 举报中心提醒广大网民注意四个“不要”

第一、不要轻易相信购物过程中所谓“订单处理异常”、“网络故障”等理由的退款；

第二、不要用对方发来的网址登陆并付款，切不可下载或安装不明链接下的文件；

第三、不要随便使用公用的电脑进行购物、支付等操作；

第四、不要轻易地将自己的购物账号、信用卡账号和密码泄露给陌生人。

此外，网民朋友如果发现有网站发布不良、违法信息及涉嫌诈骗的，可向 12321 举报中心进行举报。

【提醒】“双十一”临近，网民谨防网购诈骗

网络购物凭借价格低廉、商品繁多、方便快捷等优势已经成为很多消费者的购物方式，随着“双十一”购物狂欢的日渐临近，网络购物进入一个新的旺季，同时网络购物诈骗的信息也逐渐增多。刚进入 11 月，12321 举报中心接到有关“双十一”的短信举报数量就达到了 500 余件次。

经核查分析，该类诈骗主要有三个特点：一是模仿知名的购物网站建立钓鱼网站或虚假交易平台；二是采取以低价诱惑、巨额奖品、多种赠品、大幅折扣等为诱饵，发布虚假信息，诱导消费者前来注册，在客户下单后以收取运费、定金、保证金、押金等方式骗取消费者钱财；三是以升级 VIP 客户等名义诱骗他人向平台充值和往指定银行账户汇款。

12321 举报中心结合用户举报情况，总结出典型的 6 大购物陷阱:

陷阱 1 钓鱼网站：有些买家会收到一些陌生的卖家发来“推荐”链接，“亲，双十一点击这个可以给您优惠，发链接给您看看。”而事实上，这个链接是一个木马链接，也就是俗称的钓鱼网站。买家如果点击这个链接，填入的账号密码等个人信息就会被窃取。

陷阱 2 “秒杀”骗局：网店上时不时推出“限时秒杀”，平时几十元甚至上百元的东西，仅售一元、10 元，买家疯狂刷屏抢购。而有时候，秒杀也有陷阱，比如一元抢下来的商品，却发现运费要 50 元，远远超标；或者秒杀结束后，店铺不发货，然后店铺关闭。

陷阱 3 要求汇款到个人账户：有些骗子会找各种理由，不使用支付宝交易，比如说支付宝系统暂时坏了等理由，继而要求你直接汇款到对方账户上，以避开第三方平台的保护机制实施诈骗。

陷阱 4 盲目夸大宣传效果：一些商家选择性地在商品标题、宣传页面中夸大甚至虚构部分产品功效或性能，这些描述往往是消费者在选购产品时看重的参考依据，从而误导消费者购买不符合预期需求的商品。

陷阱 5 仿冒知名品牌商品：一些电商宣称以超低折扣销售知名品牌商品，实际贩卖的是仿冒产品，这些不良商贩混杂在打折促销的活动中，利用“双十一”的机会大肆宣传，欺骗消费者。

陷阱 6 传播虚假电子优惠券：“看上去很美”的电子优惠券有时也会暗藏“玄机”，一些电商制作和传播大量电子优惠券，但在客户消费的时候以各种理由不予兑现，比如限制优惠券的适用范围，或者以商品价格虚高予以抵消。

12321 举报中心提醒广大网民注意：

第一、在网购时需要谨慎，不要贪图一时之利而被冲昏头脑，要仔细考察店铺信誉;

第二、尽量利用第三方交易平台，不要轻易用对方发来的网址登陆并付款，切不可下载或安装不明链接下的文件;

第三、注意保存交易记录、有关单据，收货时，要注意验货;

第四、尽量不要使用公用的电脑进行购物、支付等操作，更不要轻易地将自己的网络账号、信用卡账号和密码泄露给陌生人。

此外，网民朋友如果发现有网站发布不良、违法信息及涉嫌诈骗的，可向 12321 举报中心进行咨询、举报。

● 网购渠道的风险

随着移动互联网的崛起，网民的网购渠道也不断的扩展到移动端。

本次共调查了六种网购渠道，网民对各种渠道的风险认知如下：

认为“不明来源的购物 APP”风险最大的占 80.6%；

近七成的用户认为“网页广告展示的商品”风险较大，占 69.2%；

认为“社交网站/聊天好友/朋友圈推荐的网购渠道”存在风险的占 57.6%。

“通过搜索引擎找到的商品”、“输入网址直接进入购物网站”和“安全软件提示安全的购物网站”，这三种网购渠道风险较低，占比分别为 29.4%、25.2%和 11.9%，成为用户认为较为安全的网购渠道。

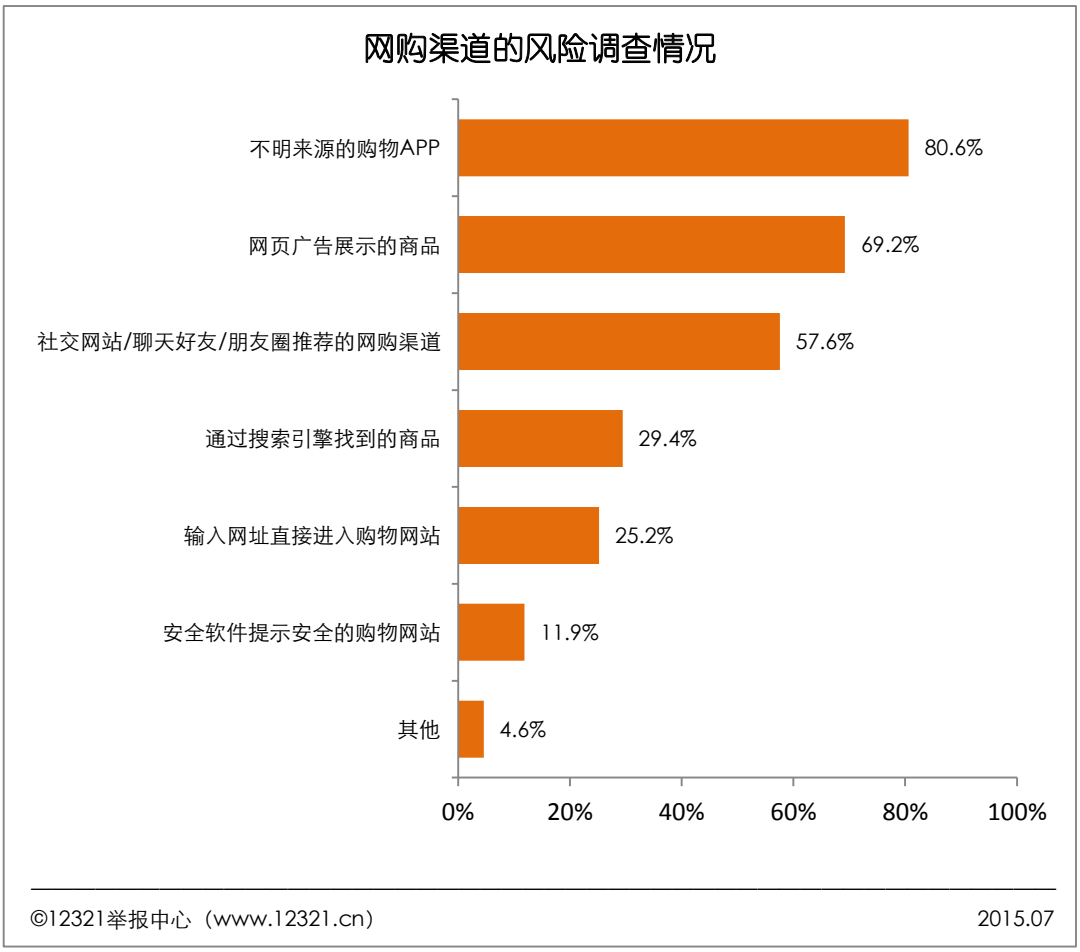


图 13

【技巧】八招识别网购诈骗陷阱

近来网购诈骗案件多发，普通网民存在网络防范意识不强、缺乏相关维权知识等问题。针对网购诈骗案件，滨州市工商局提醒消费者在网购过程中要做到以下几个方面。

第一，要对所购物品有一定的了解，在网上购物也要做到“货比三家”。不光要比价格，

也要对比物品的质量等。对于出价过低的物品，消费者需谨慎选购。

第二，注意商家网站域名和红盾标志。一般而言，有规律、越好记的域名价值越高，找知名的大型网站购物比较安全。同时要核实该网站是否已经备案，在工商部门备案过的网站，出现购物纠纷比较容易找到投诉对象。

第三，仔细甄别网络卖家留下的联系方式及相关信息。假如该卖家的联系方式只有 QQ、E-mail、手机，而没有具体的固定地址和固定电话，或者卖家拒绝使用具有防“钓鱼”功能的即时通讯工具，消费者就要提高警惕。

第四，利用网上搜索引擎，查询供货者的信息中留下的联系电话、联系人、公司名称以及银行账号等关键信息是否一致。

第五，查看产品信息和消费者反馈。制作和维护一个商品丰富、产品信息齐备的网站需要付出不低的成本，骗子网站一般不愿意在这方面多下功夫。

第六，尽量去大型、知名、有信用制度和安全保障的购物网站购买所需的物品，这些网站大多采用安全性较高的支付工具作为“第三方交易中介”，或是实行先到货后付款等保护消费者的购物方式。

第七，不要轻易将自己的网络账号、信用卡账户和密码泄露给陌生人，尽量不要使用公用的电脑进行购物、支付等。

第八，如发现有网站发布不良、违法信息及涉嫌诈骗的，应及时向公安机关举报。

- **电商在保护网民权益方面所做的最有效措施**

对电商在保护网民权益方面做的措施的梳理中，网民认为效果最好的措施前三位是：“商户信誉真实性保障措施”、“买卖双方实名认证”和“一定期限内无理由退货”，共占到 77.3%。“畅通举报渠道”占比 13.4%。

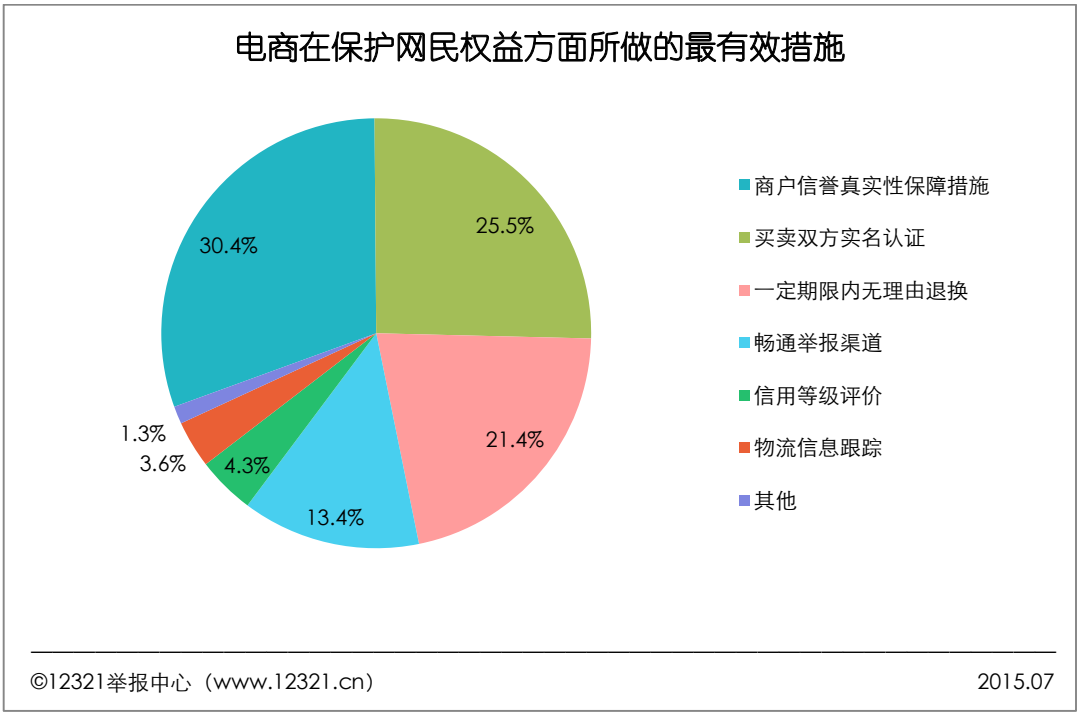


图 14

【资料】盘点 2014—2015 年度十大电商法律关键词

近日，中国电子商务研究中心发布《2014—2015 年度电子商务法律报告》。报告显示，电商立法、“微商”营销机制、电商征税、信息泄露、电商售假、商标抢注、不正当竞争、网络实名制、虚假交易、P2P 跑路成为了“2014-2015 年度十大电商法律关键词”。

关键词 1：电商立法。发展电子商务的落脚点应该是消费者权益的保护，电子商务立法则要以消费者权益的保护为出发点。2015 年两会期间，电商界大佬纷纷提出完善电子商务监管的提案，与此同时，电子商务立法正在紧罗密布的制定过程中。但是，眼下我国电子商务正如一匹疾驰的骏马，立法如何既给骏马上“辔头”，又不让马儿放缓脚步，无疑成了考验立法的难题。律师认为，得民心者得天下，得消费者之心得市场，把增加消费者信任及保护消费者权益作为发展电子商务要解决的重要问题，是电子商务立法的重中之重。

关键词 2：“微商”营销机制。微信的广泛使用，使得“微商”这一网购模式逐渐进入公众视野，相比于传统电商，微商有着门槛低、成本小、传播广等优势，非常适合个体创业者，同时容纳就业的前景也非常广阔；但另一方面，微商市场假冒伪劣产品多，价格混乱，售后服务不完善等现象也很多，实际上现阶段的微商处于国家的“监管盲区”。律师认为，要解决这个问题，一方面电商平台要负起责任，加强自律和内部的监管，微信电商模式要健康发展，应让规范的营销机制先行。而对于监管部门来说，这种类似个人账户的网上营销行为应当尽快纳入到法治的框架中。

关键词 3：电商征税。

关键词 4：信息泄露。2014 年 3 月 22 日，国内知名漏洞报告平台乌云指出携程网站的技术漏洞导致部分用户银行账户信息泄露；5 月 13 日，小米论坛约有 800 万小米社区用户数据遭泄漏；临近年末，乌云报告显示铁路购票网站 12306 的漏洞危险等级为“高”，漏洞类型则是“用户资料大量泄漏”，这意味着将有可能导致所有 12306 注册用户的账号、密码、身份证、邮箱等敏感信息泄露。因为我国没有一部统一的关于互联网信息保护方面的法律规范，律师认为当务之急是我国的立法机关和拥有权限的行政主体应当尽快推进、进行此方面的立法工作，明确经营者信息安全法律规范及责任，为信息安全提供法律上的权利保障、救济途径。

关键词 5：电商售假。2014 年下半年，国家工商总局、中国消费者协会两次对网络交易平台上销售的商品进行的质量检测，抽查的 9 个电商平台中 7 个在卖假冒或质量不合格商品，问题率约为 77.8%。律师建议，第三方交易平台应当承担起电商售假的法律、社会责任，对于商户资质、商品发布审核，同时应当通过技术创制，健全制度体系加以严格筛选。另一方面，立法者应当通过法律法规对避风港原则的适用予以必要的限制；市场监督管理机构则可以将第三方平台之间的黑名单商户进行信息共享，避免商户打一枪换一炮的规避行为。

关键词 6：商标抢注。

关键词 7：不正当竞争。

关键词 8：网络实名制。国家互联网信息办公室发布《互联网用户账号名称管理规定》，明确提出网上昵称不准违反法律、危害国家安全、破坏民族团结、侮辱诽谤他人等“九不准”，并就互联网用户账号名称的管理，对互联网信息服务提供者、使用者的服务和使用行为进行规范，规定自 2015 年 3 月 1 日起施行。律师认为，网络实名制监管，应充分考虑我国互联网发展的现状，在此背景下，网络服务提供者、网络监管者除提高服务及监管水平之外，还应提高保护网民个人信息安全、保护网民权益的意识。

关键词 9：虚假交易。电商平台上的店铺刷单早已经成为行业公开的秘密之一。在电商平台上，商品可以通过销量进行排名，更大的销量意味着被展示在靠前位置的概率更高，也意味着获得更多的流量，因此刷单成为不少网店的提升销量的捷径。如今各式各样的刷单，在电商产品和服务销售过程中出现。有雇人刷单升级的，有以刷单为诱行骗的，有组织刷单不正当竞争的。律师认为，刷单的根源在于网络的虚拟性和隐蔽性，如果现实中的交易，刷单就会变成无聊的人做的无聊的事情，因此其关键还是电商形成的评价体系，给诚信卖家带来了优势地位，而不诚信的人意图反扑，利用规则进行不正当竞争或者欺诈。

关键词 10：P2P 跑路。据中国电子商务研究中心监测数据显示，截至 2014 年 6 月初，全国共有 P2P 平台 1275 家，其中今年前 5 个月共上线 220 家。而今年跑路 P2P 平台已有 45 家。律师建议应由政府部门牵头，尽快对 P2P 平台进行核查、考评，鼓励合法、优质的 P2P 平台规范经营，打击不法、低劣的平台并采取有效措施予以处理，还投资者一个安全、合法的投资环境。

3.3 即时通信工具

- **使用即时通信工具时碰到的侵权现象**

网民在使用即时通信工具中碰到的侵权现象主要集中在下面四类：

（1）收到病毒信息。60.7%的用户表示“收到带有木马/病毒的链接”；35.3%的用户碰到过“账号或密码被盗”的情况。因如被病毒侵入，其所有信息可能会被拦截，且银行卡、密码、身份证号等个人信息会被盗。因此对于陌生链接不要轻易点开。

（2）收到“钓鱼”信息。60.5%的用户“收到假冒、诈骗网站/网址”；37.3%的用户收到“冒充好友诈骗”；

（3）收到商业信息。52.0%的用户“收到商业信息”。商业信息是即时通信工具获得收益的重要渠道，但含有虚假信息或夸大宣传内容，将会损害用户的正当权益。

（4）收到色情信息。34.6%的用户“收到过色情信息”。根据 12321 举报中心的举报数据显示，即时通信工具已成为色情信息传播的一个重要渠道，需加以治理。

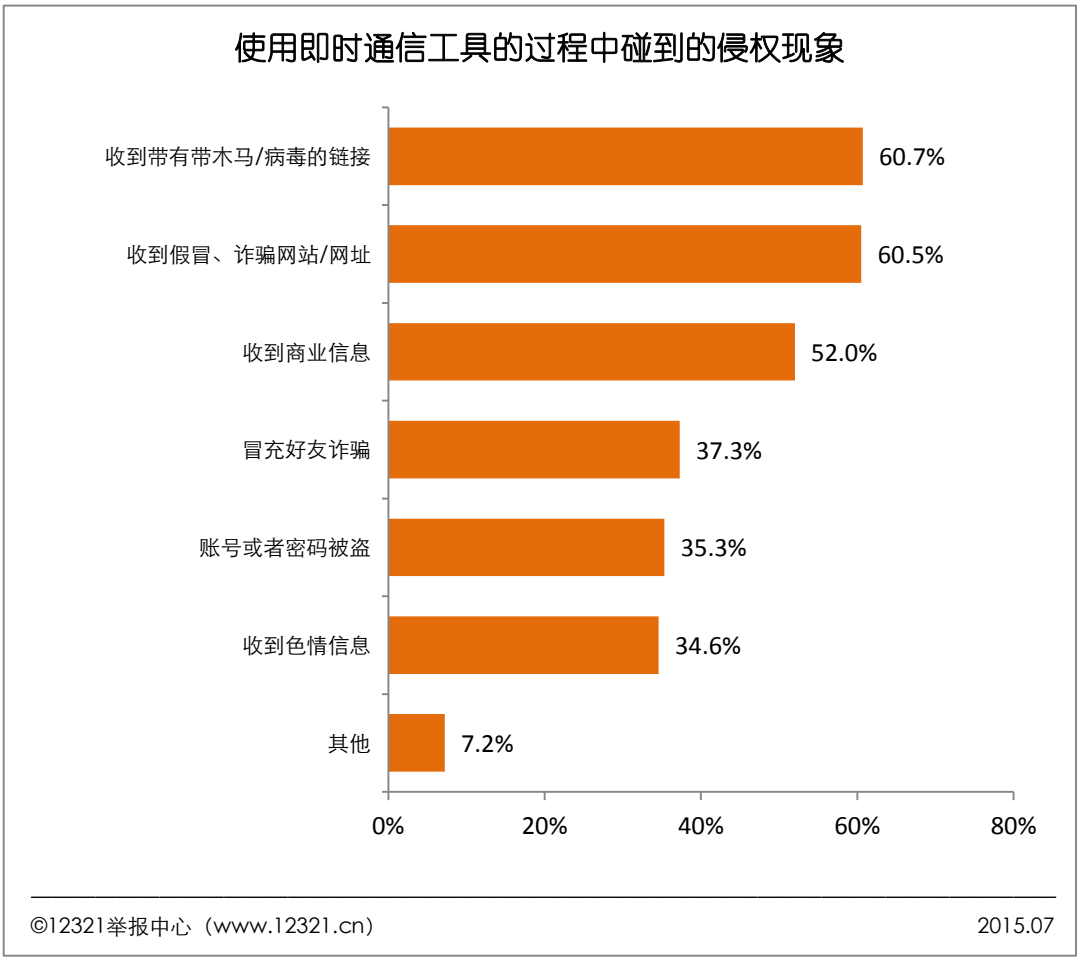


图 15

【提醒】手机病毒“XX 神器”变种再袭 12321 提示：慎点不明链接

“赖总看看你做了什么光彩事，哈哈，自己下载看看吧 http://feish******uan.com/12.apk”。近期，不少手机用户都收到了这样一种病毒短信。如果点开该链接，下载并安装其中的程序，手机就可能被感染病毒，植入木马，并被远程控制，自动将此短信群发给通讯录中的亲朋好友。12321 举报中心短时间内接到网友举报的此类诱骗下载安全病毒程序的短信 70 多件次，其短信样本如下：

此手机短信是一种新型诱骗短信，骗子在病毒程序链接前一般加上一句话，诱导你点开网址链接并下载安装，诸如“你下流的一段被我拍到”、“看你干的好事，自己点击”、“你最近的事被传到网上了”等等，都是以引起本人的好奇心为切入点，让接收方在不知不觉中随手点开病毒链接。这种手机木马病毒危害极大，手机一旦感染了此种病毒，将自动向手机通讯录好友群发短信，使通讯录中的好友成为新的受害者。如果手机上绑定了网银或者支付宝等，还可能被盗取密码等个人信息，造成财产损失。

针对此类短信，12321 举报中心提醒广大网友注意：

1、建议用户不要轻易打开陌生（包括熟人发来的短信）短信中带有的链接地址，更不要下载安装其中的应用程序。

2、建议在智能手机中安装并开启安全软件，及时发现含有木马病毒的应用程序，防止手机中毒。

3、若是不慎点击安装了恶意程序，可以采取两种方法应对：第一种方法是使用安全软件查杀，并完全卸载这个病毒；第二种方法是重新安装干净的操作系统。

- **即时通信工具提供的最有效的权益保障方式**

网民依旧认为“实名认证”是即时通信工具提供的最为有效的权益保障方式，占比 32.3%。

“非正常登陆进行提醒”得到了 27.0%的用户的认同；这种措施有助于用户第一时间了解账号的状态，及时做出反应避免账号被盗。

“对网址、网站进行安全标识”得到 20.0%的认同。如建立行业共享黑名单，则将更快速有效的进行安全提示。

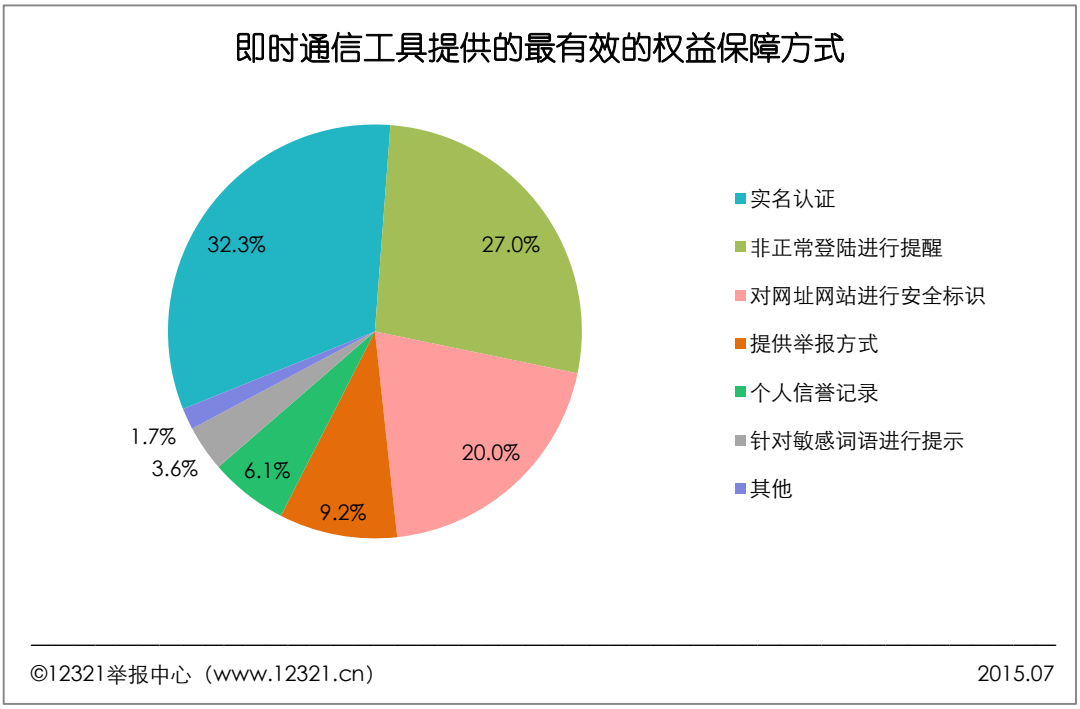


图 16

【提醒】微信朋友圈要认清 6 招诈骗陷阱

微信作为时下时尚的交流方式，受到越来越多网民朋友的追捧。但随之而来的各种诈骗手段也是五花八门，让不少网友因此吃了苦头。12321 举报中心总结出六大微信诈骗手段，提醒大家“朋友圈”中危机四伏，使用微信时需多长个心眼，防盗防骗。

骗术 1：利用代购诈骗。诈骗者声称可以“打折代购”，在你付款之后，再以“商品被海关扣下，要加缴关税”为由，要求你“加付关税”，税款付了货品却永远不会收到。

12321 提醒：到正规网站或实体店购物，别只顾着捡便宜。

骗术 2：二维码诈骗。诈骗者以商品为诱饵，称给消费者返利或者便宜，发送的二维码，实则是木马病毒。一旦安装，木马就会盗取应用账号、密码等个人信息。

12321 提醒：手机不要随便安装不明程序，贪小便宜可能吃大亏。

骗术 3：盗号诈骗。此种诈骗与盗用 QQ 号诈骗类似，冒充家人跟您联系，并以各种理由向您要钱。

12321 提醒：打个电话联系，听听声音，就可以发现真相了。

骗术 4：身份伪装诈骗。诈骗者伪装成“高富帅”或“白富美”搭讪，骗取信任后，再以资金紧张、手术等为由骗取钱财。

12321 提醒：无论什么途径认识的朋友，都要牢记“交友需谨慎”，少做“白日梦”。

骗术 5：“点赞”诈骗意在套取个人信息。目前，这种诈骗方法最多。一种诈骗由头是“集满多少个赞就可获礼品或优惠”，等集满“赞”去兑换时，发现拿到手的奖励“缩水”了。另一种是商家发布“点赞”信息时，就留了“后手”，并不透露商家具体位置，而是要求参与者将自己的电话和姓名发到微信平台，一旦所征集的信息数量够多了，这种“皮包”网站就会自动消失，目的是套取更多的真实个人信息。

12321 提醒：这一类的所谓优惠活动建议少参加。必要时，先打电话查证，可把咨询答复录下来，或者截屏保留证据，防止商家“赖账”，也可实地查看，眼见为实。

骗术 6：微信假公众账号诈骗。诈骗者喜好在微信平台上取类似于“交通违章查询”这样的公众账号名称，让您误以为这是官方的微信发布账号，然后再进行诈骗。

12321 提醒：对于各类公众账号要提高警惕，擦亮双眼，多方求证真伪，尤其不要随意进行网上交易。

3.4 电子邮箱

- **使用电子邮箱时碰到的侵权现象**

用户在使用电子邮箱的过程中，罗列出常见的侵权现象如图 17 所示：

（1）“收到含有欺诈内容的邮件”这一现象最为严重，占 61.8%。

（2）收到商业邮件。58.5%的用户表示“收到过未经订阅的商业邮件”；33.2%的用户表示“商业邮件无法退订”。

（3）收到不良内容邮件。45.0%的用户“收到含有病毒的邮件”；31.4%的用户“收到含有违法内容的邮件”。

（4）邮件拦截有误。31.8%的用户曾遇到过“正常邮件被当成垃圾邮件”的现象。

12321 提醒网友定期去电子邮箱中的垃圾箱看一看，或设置垃圾邮件提醒信息，防止重要邮件被误拦。

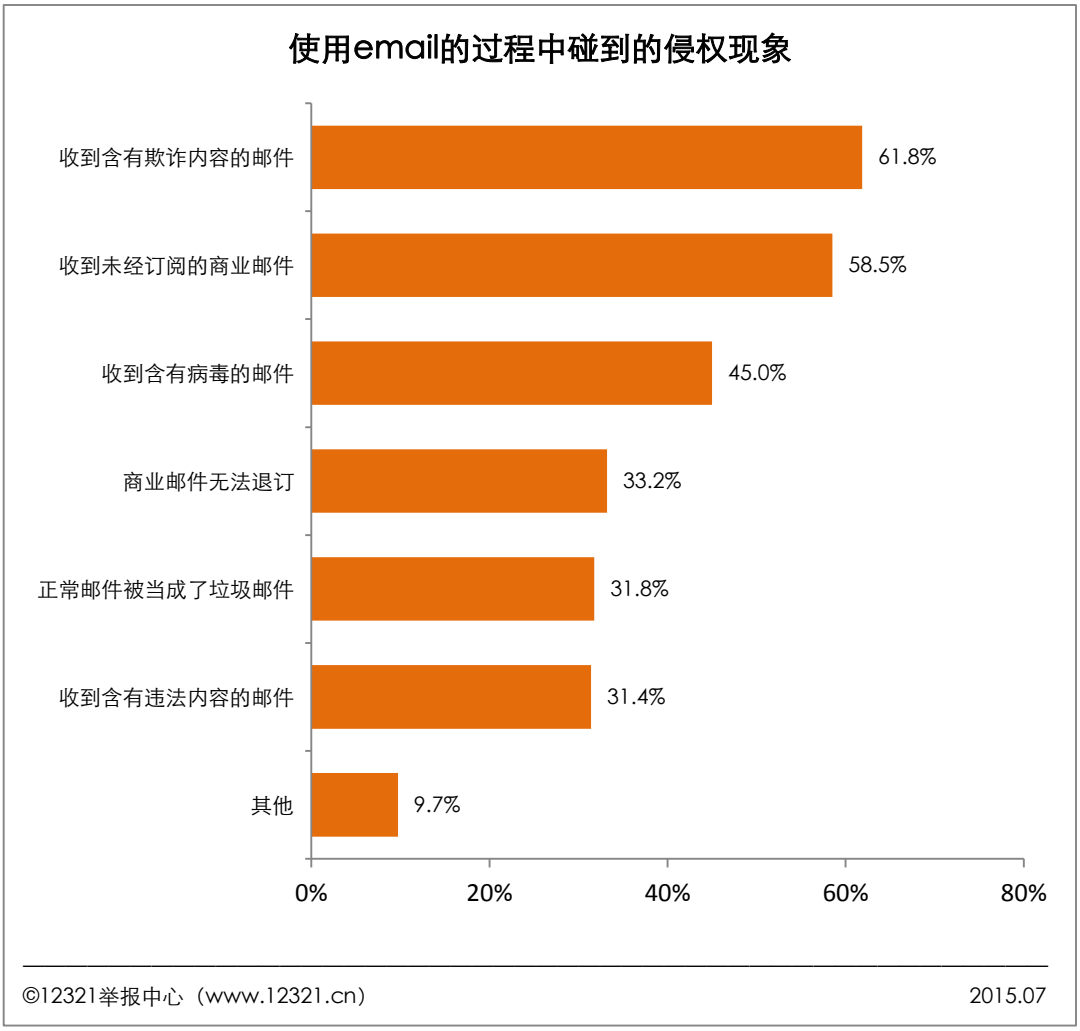


图 17

【技巧】12321：九个方法告别垃圾邮件

几乎可以这样说，如果你有免费电子邮箱，你收到垃圾邮件的机会将会很高。对付垃圾邮件除了各方共同努力外，对于普通用户来讲，注意以下几点是可以防范垃圾邮件的：

①不要响应不请自来的电子邮件或者垃圾邮件，绝对不要回复垃圾邮件，如果你回复甚至警告他们不要再发，这无疑也相当于告诉对方你的邮件地址实际存在，今后你可能会收到更多的垃圾邮件。所以，即使垃圾邮件上写有“如果不需要此邮件的话请回信告知”等句子，也决不要回复，这一点非常重要。

②不要试图点击垃圾邮件中的任何链接，某些垃圾邮件发送者会自动收集点击者的信息，事实上当你点击链接进入相应网站时就无疑高速对方这个电子邮件地址是存在的（不然谁会去点击？）。

③不要把您的邮件地址在网上到处登记，如果经常用某个邮件地址在网上大量注册（很多论坛都要求填写 email 地址然后给你发送密码），相信你今后收到垃圾邮件的次数会越来

越多，那怎么办呢？告诉你一个方法：由于网络上收集电子邮件地址通常是用软件进行，而目前的电子邮箱表示法中都会包含“@”这个符号，所以当你注册成功后不妨再次进入论坛，将电子邮箱中的“@”改为其他符号如“#”，这样其他用户查看时会知道你的 email 的，但对付那些软件就有效多了；不过有些网站，检测地址的合法性，所以此法肯定行不通，那也有办法——将电邮地址修改为其他的字符组合，比如增加字符长度等。

④不要登陆并注册那些许诺在垃圾邮件列表中删除你名字的站点。

⑤保管好自己的邮件地址，不要把它告诉给你不信任的人。

⑥不订阅不健康的电子杂志，以防止被垃圾邮件收集者收集。

⑦谨慎使用邮箱的“自动回复”功能。为了体现互联网高效、快捷的特点，很多网站和邮件收发工具中都设置了“自动回复”功能，这虽然方便，但是如果两个联系人之间都设置了“自动回复”，想想看有何后果？恐怕双方的邮箱中都是一些“自动回复”的垃圾信件。换句话说，此功能使用不当，人人都会变成垃圾邮件发送者。

⑧发现收集或出售电子邮件地址的网站或消息，请告诉相应的主页提供商或主页管理员，将您删除，以避免邮件地址被他们利用。

⑨用专门的邮箱进行私人通信，而用其他邮箱订阅电子杂志。

- **邮件服务商在保护网民权益方面做的最有效措施**

邮件服务提供商在保护网民权益方面所做的保障措施中，“垃圾邮件自动过滤”措施得到的认知度最高，达 34.3%；“异地登陆提醒”、“垃圾邮件箱定期垃圾邮件报告（避免错拦）”、“发件人黑名单”分别占比 17.9%、17.2%和 17.0%。

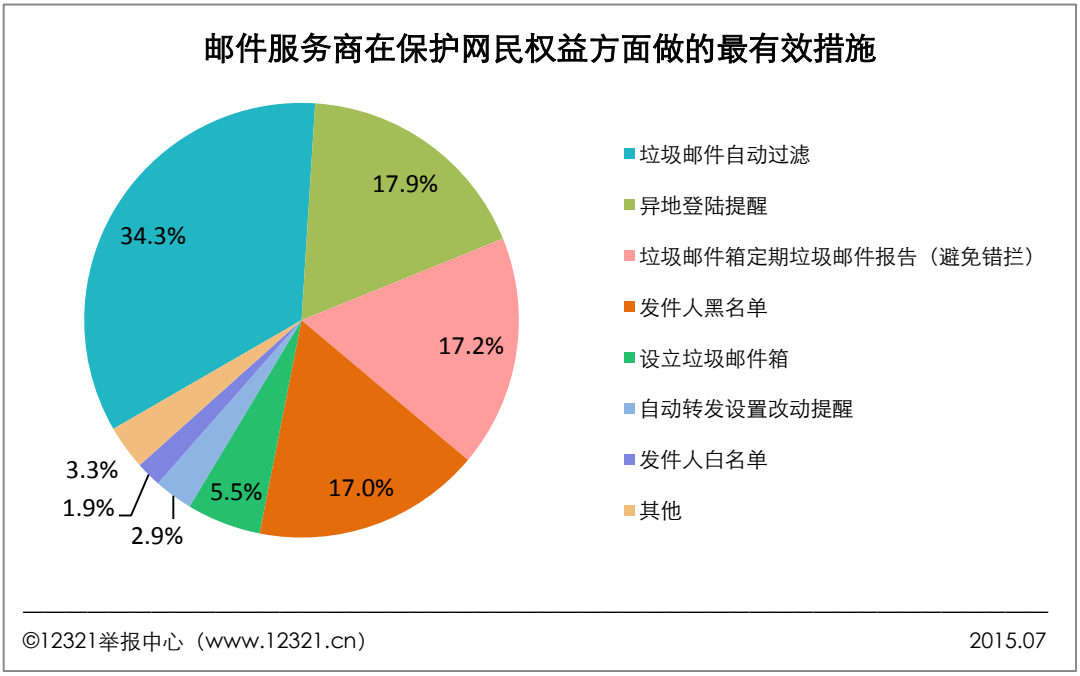


图 18

3.5 APP

- **防止恶意 APP 侵权的最有效措施**

为防止恶意 APP 的侵犯，APP 开发企业所做的最有效措施调查结果如下：

（1）30.6%的用户主要依赖“开发者第三方认证”；9.6%的用户选择“安装手机安全软件”；

（2）22.2%的用户不下载来历不明的 APP；6.4%的用户“尽量不开启 root 权限”；4.2%的用户不扫描来历不明的二维码；2.8%的用户“不随意刷机”；以上举措均说明网民已有一定的安全意识；

（3）22.1%的用户表示“举报、联动处置机制”

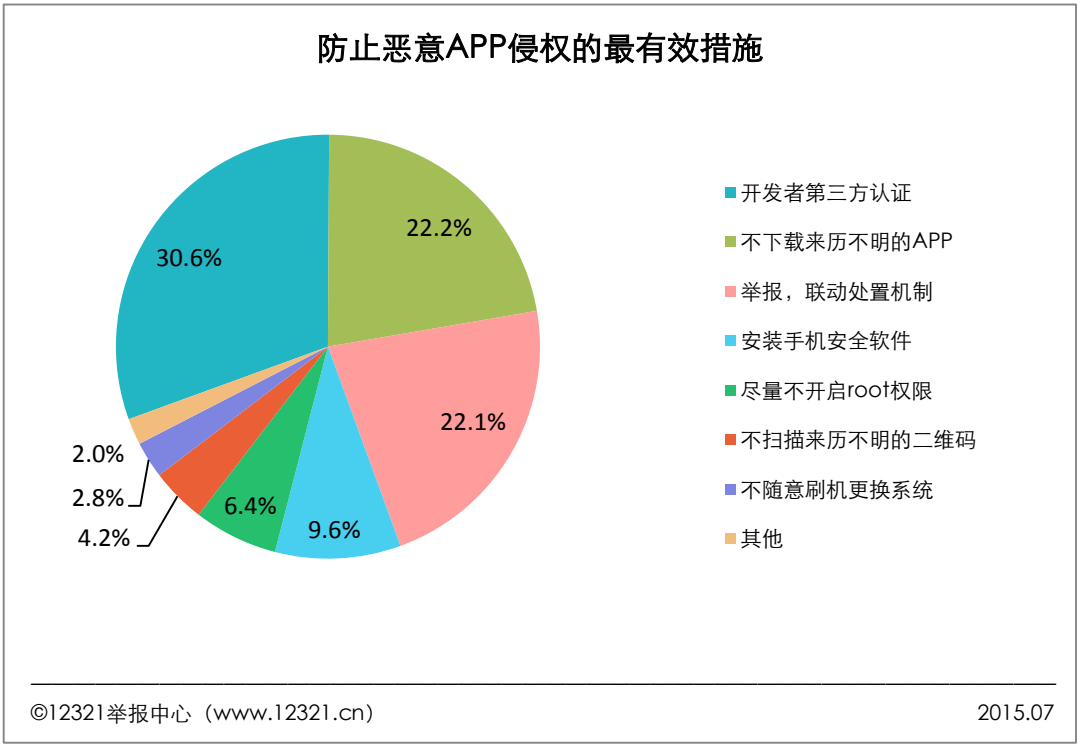


图 19

【提醒】谨防恶意 APP 九大陷阱

随着智能手机的普及，移动互联网发展迅猛。各种移动应用也层出不穷，一些 APP 在给我们带来便利或者乐趣的同时，也会产生各种烦恼。一些恶意应用利用智能手机的推送功能，频繁推送各种广告信息。更有甚者，滥用系统权限窃取用户的个人隐私信息；还有后台短信秘密发送，私扣手机费用；应用被私自升级，暗扣手机流量等恶意行为。近期，12321 举报中心接到举报恶意 APP 呈不断上升之势。

12321 举报中心根据举报情况分析，总结出恶意 APP 九大陷阱:

陷阱 1 无限时不限量乱弹广告。用户在下载一款 APP 后，在使用过程中，会不定时推送一些与应用无关的广告内容，影响用户的正常手机应用。很多 APP 都有自动弹出广告的问题，在应用的某个位置有专门的广告滚动条，不停地滚动，推送广告，甚至不定期的弹出广告窗，对用户造成干扰。

陷阱 2 虚假宣传。一些 APP 在使用时可通过获取积分换取一些软件的特殊功能，如道具、关卡解锁等。有些 APP 设置虚假的积分体系以达到宣传效果，在用户获取足够积分并用积分换取软件功能时，相应的功能却没有兑现。

陷阱 3 未经用户同意窃取用户信息。用户下载此类型流氓 APP 后，该软件会在用户不知情的情况下，获取软件自身功能外的权限，去私自扫描获取用户个人信息。

陷阱 4 滥用增值服务。用户在下载这类 APP 后，该软件将会在毫无预示，用户不知情的情况下，自动联网，对该软件进行自动更新，安装插件或订阅其他业务。这造成用户流量飞速流失同时，也安装了具有潜在危险的插件。

陷阱 5 无提示自动下载应用。在用户下载某款 APP 后，软件会在无提示，用户不知道的情况下，私自下载其他应用，安装恶意病毒。大部分被私自下载的软件都是用户不了解的软件，它们可能会后台发送信息浪费用户手机费；也可能是病毒，偷偷窃取用户信息，卖给其他商家。

陷阱 6 无法正常卸载。当你发现所下载的 APP 是流氓软件，对其进行卸载时，发现卸载不成功或者还有残留的文件。这些文件依然能对你的手机进行各种流氓行为，干扰你的工作和生活。

陷阱 7 远程控制。下载此类 APP 后，用户手机 IMEI、IMSI、SIM 卡序列号、设备序号等手机硬件信息将被窃取，同时该恶意软件允许远程控制修改用户手机中的书签地址，浏览器主页等流氓行为。

陷阱 8 伪造短信。此类 APP 内含恶意广告插件，该插件会伪造短信推送垃圾广告，使得用户频繁接收垃圾短信，同时该插件存在伪造欺诈短信风险。

陷阱 9 山寨知名软件。此类 APP 假冒知名 APP，图标、名称和内容等模仿非常逼真，用户很难对其进行区分，从而来盗取用户的银行账号和密码等信息。

针对以上恶意陷阱，12321 举报中心提醒大家要做到:

1.不要随意点击不明链接，尤其是短信链接，多数为恶意链接。

2.不要随便安装不明手机应用软件，在一些正规的手机应用商城中下载软件。

3.平时关闭手机 USB 调试功能，关闭允许安装未知来源功能，防止手机应用后台私自安装。

4.要提高自身的隐私保护意识，个人隐私不要存入手机内，防止手机后台上传资料。

5.只使用可信网络来源访问网络，避免接入不熟悉的 Wi-Fi 网络，防范被网络入侵。

6.对数据加密，即使信息落到他人手中也破解不了。

7.及时发现手机异常。如：收发短信异常，接听拨打电话异常等。

8.用户手机要及时安装手机安全软件，经常对手机进行检查，有效地提高手机的安全。

12321 举报中心提醒：遇到手机病毒及应用安全问题可点击手机应用商店相关应用下载页面的“一键举报”按键向 12321 举报中心举报，或采取其他举报方式向 12321 举报中心进行举报。

3.6 网络游戏

- **玩游戏时碰到的侵权现象**

网民在玩游戏的过程中，碰到的侵权现象分为三类：

（1）垃圾信息较多。65.5%的用户表示“广告太多”；50.6%的用户“遭遇不文明言语攻击”；

（2）不公平现象严重。分别为“其他玩家使用外挂”（46.5%），“厂商安排托高价卖装备”（26.6%），“账号无故被锁或者降级”（25.1%），“点卡没用完就被停了”（13.0%）；

（3）信息安全得不到保障。29.6%的用户“个人信息被泄露”，27.1%的用户“账号和密码被盗”，26.5%的用户“装备被盗”。

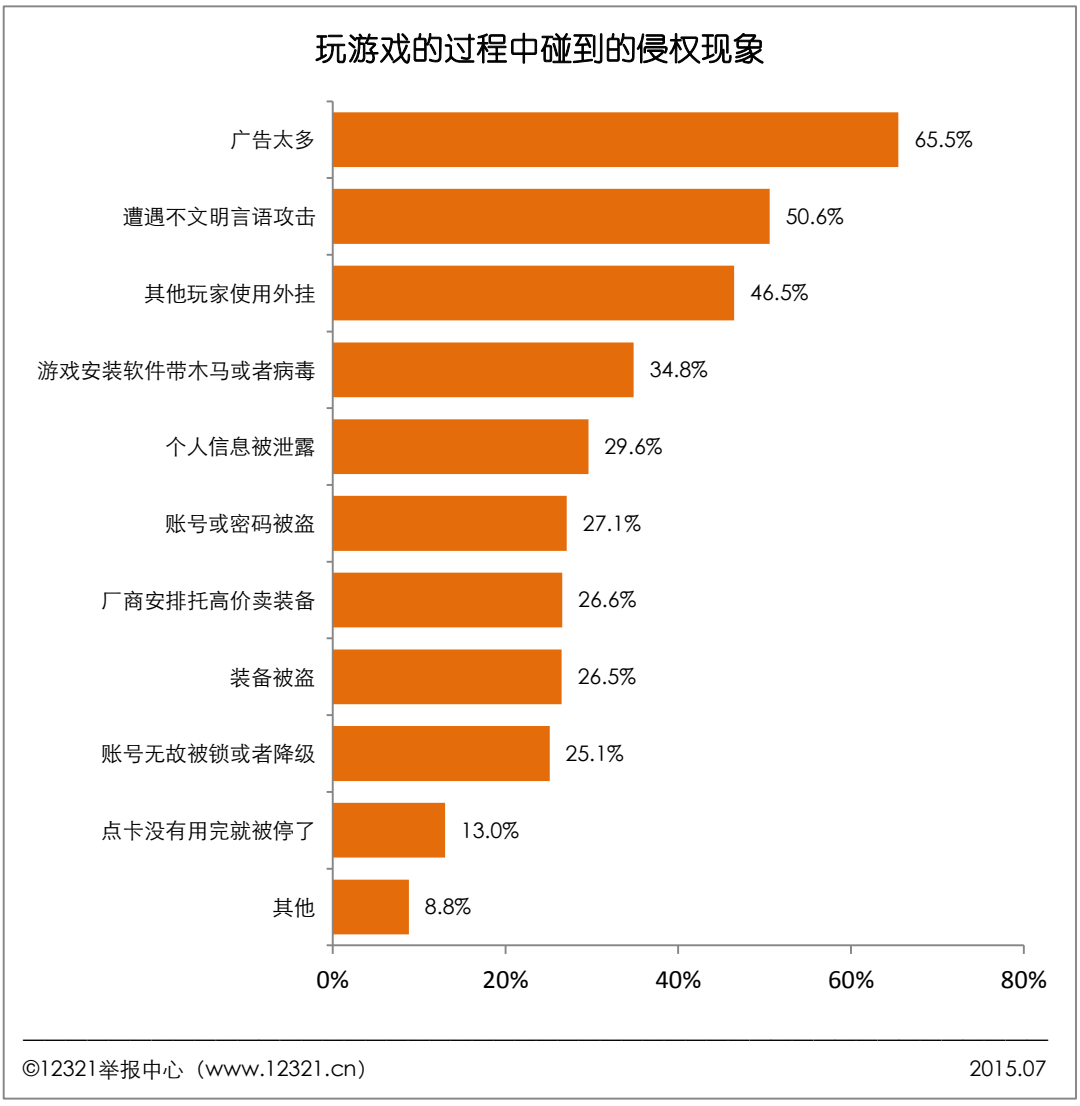


图 20

【案例】12321：盘点四大手机网游常见骗术

不论在哪款游戏中，都有这样一群人，他们热爱游戏，但却没有大量的时间投入到游戏中去。所以他们通过 RMB 来实现自身角色实力的突破。这些人往往都是游戏世界中的风云人物，对虚拟物品的需求强烈，数量惊人。他们就是我们所说的 RMB 玩家。

RMB 玩家的存在催生了游戏商人，两者之间的买卖关系保证了游戏的供需平衡。但游戏运营商是不希望这种贸易形势存在的，所以 RMB 玩家和游戏商人之间的买卖一般需要借助第三方平台。第三方平台的引用让心术不正的玩家看到了可乘之机。他们设下骗局骗取钱财或账号，受骗的不仅限于玩家，一些商人甚至也成为了骗子的猎物。今天我们就来盘点一下四大手机网游常见骗术。

骗术一：私下交易，被骗没商量。这是在网络游戏中出现最早的一种骗术。随着玩家警惕性的提高，这种骗术也进化的更为高明。很多骗子利用技术手段调取玩家账号密码，随后登录到游戏中给游戏好友发送借钱、借物一类的行骗信息。其它玩家一旦相信，便掉入了骗子的陷阱。骗完别人还不满足，索性将盗来账号内的游戏财富洗劫一空。对付这种骗子，我们需要多一份警惕，不要轻易相信游戏中的任何人。交易最好在正规的游戏平台进行，以免上当受骗。

骗术二：用密码和你开玩笑。在一些不正规的手游交易平台中，这是一种最为常见的骗术。骗子将一条真的账号信息发在交易平台上，并提供给交易平台正确的密码。当信息成功发布后，马上将密码修改。由于有第三方交易平台，所以玩家产生了盲目的信任心理。购买后，发现交易平台发给自己的游戏密码居然是错误的。当找到交易平台时，游戏平台无法验证是谁修改的密码，所以不会帮助买家解决问题。这种骗术主要是利用了交易平台不专业的特点，以及玩家对手游交易平台的信任。只要玩家能够选择正规的游戏平台，这一问题便可以迎刃而解。

骗术三：账号附带物品不对，死无对证。目前，一些手游交易平台对于账号信息的核对上存在一定的漏洞。一些玩家利用了这点，将自己账号的信息描述的与实际相差悬殊。一般描述信息不符主要体现在账号附带装备、宝石、物品等方面，账号基本情况都会如实描述。买家登录游戏账号后发现实际和描述相差很多时，第一时间想到的就是找交易平台理论，但是交易平台一般都不会理会这种投诉，毕竟交易已经成功，生米已经成熟饭。而且由于之前没有仔细核对信息，所以即使受理了这种投诉，卖方也可以说是买家在拿到账号后调换了账号中的物品。这种骗术和上面提到的骗术一样，也是利用了手游交易平台的不专业性。

骗术四：防不胜防的高招仲裁。这种骗术操作简单，成功率也比较高，所以玩家要尤其警惕。近期这种骗术应用的相当广泛，除了专业性较强的网站以外，其它网站中的卖家都有中招。这些骗子专门购买好的账号，在获得账号信息后，改动账号密码，同时申请仲裁，谎称收到的信息不对。当交易平台无法解决这一问题时，交易自然就被取消了。可是账号此时却已经归骗子所有，卖家不管找交易平台还是找游戏运营商，都已经无力回天了。

12321 提醒：广大游戏玩家会上当受骗，归根结底还是由于手游交易平台的不专业所导致的，一旦那些心怀不轨的玩家发现了其中新的空当，那么就会衍生出一种新的骗术。在漏洞百出的手游交易平台，骗术也自然五花八门。玩家在选择交易平台的过程中，其安全性、专业性都是必须要考虑的。

3.7 网络社交工具

- **使用网络社交工具时碰到的侵权现象**

网民在使用网络社交工具的过程中，遇到的侵权现象如下：

（1）垃圾信息较多。70.8%的用户认为“广告信息多”，40.6%的用户遇到“私信频繁骚扰”的现象；

（2）虚假信息严重。49.2%的用户遇到过“交友对象信息虚假”，36.4%的用户遇到了“茶托/酒托/饭托/花托”；

（3）色情信息严重。47.4%的用户遇到过“打色情擦边球”的现象；

（4）信息安全得不到保障。32.2%的用户“个人信息被泄露”。

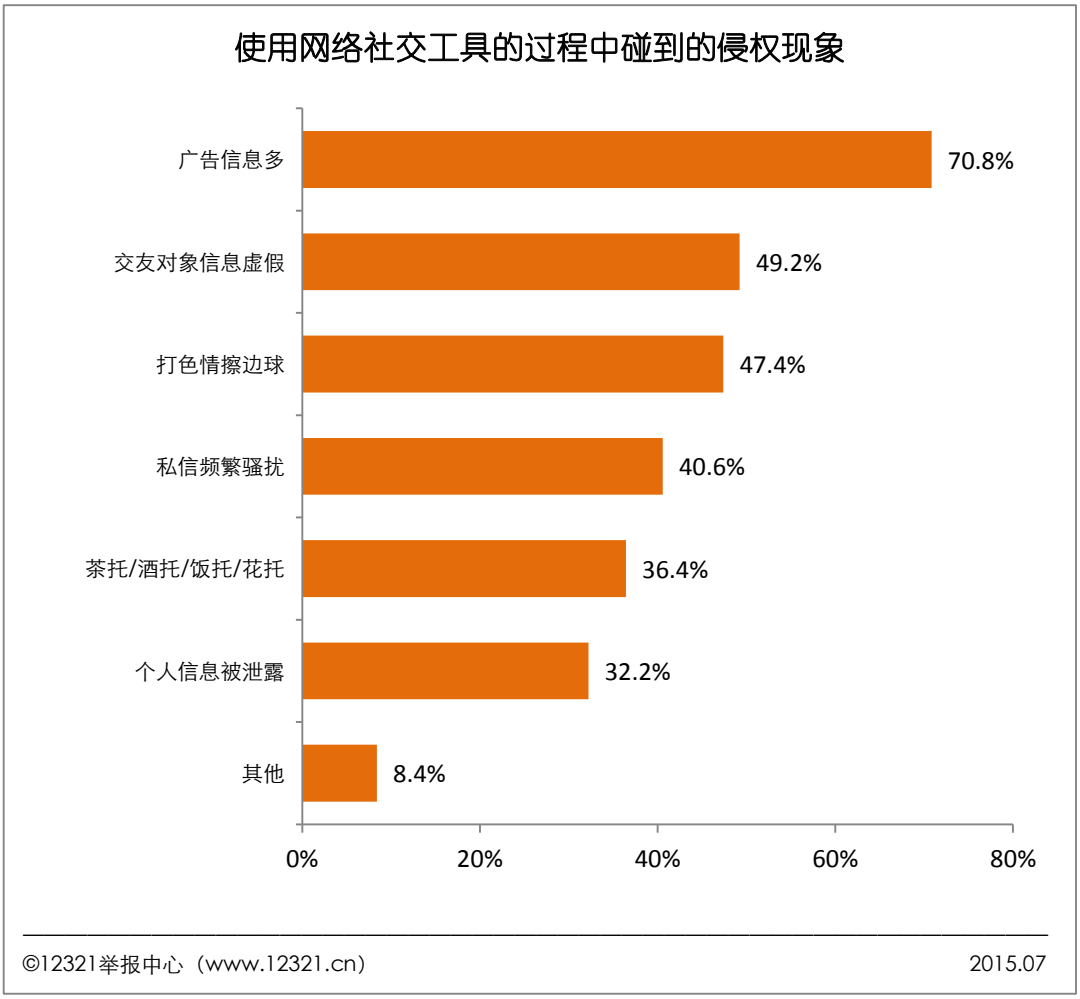


图 21

- **网络社交工具在保护网民权益方面做的最有效措施**

41.6%网民认为网络社交工具在保护网民权益方面做的最有效的措施是“实名认证”；其次是“对网站上传信息的审查机制”，占比 23.0%；认为“不良信用记录共享”比较有效的占 19.8%；认为“投诉举报机制”有效的占 13.3%。

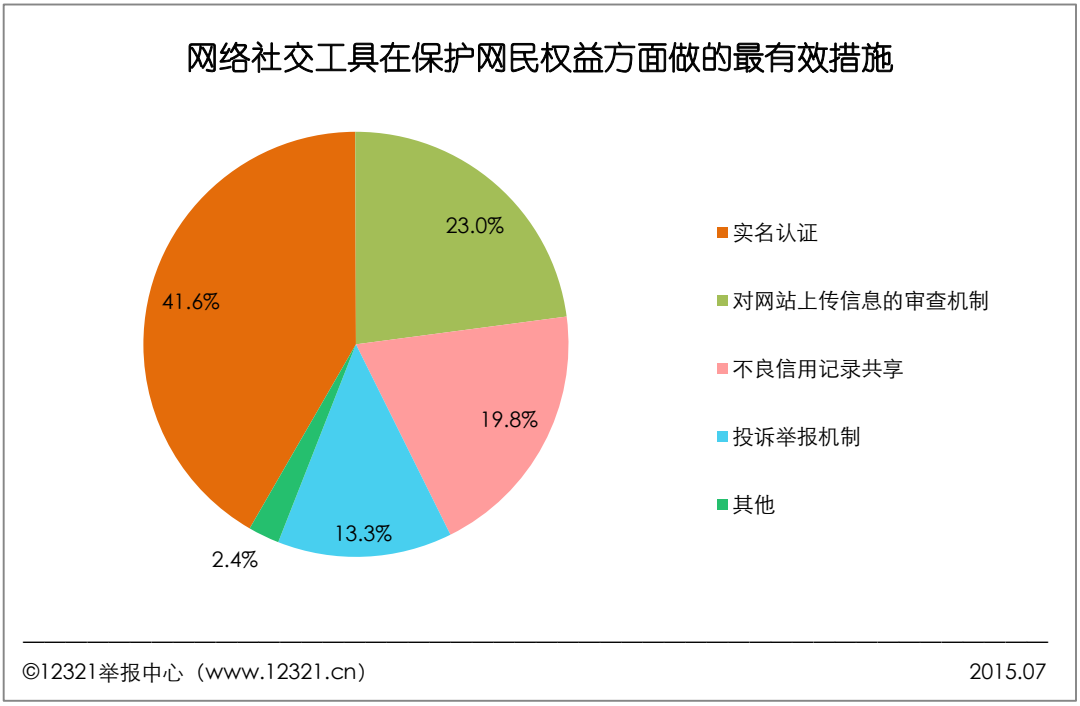


图 22

3.8 互联网金融

- **参与过的互联网金融模式**

调查显示：在互联网金融的快速发展下，第三方支付已成为城市消费场景中的主要支付工具。79.2%的用户参与过该互联网金融模式；依托互联网金融的平台，39.3%的用户参与过“网络理财”；13.3%的用户参与过“P2P 网贷”；9.6%的用户参与过“众筹”。

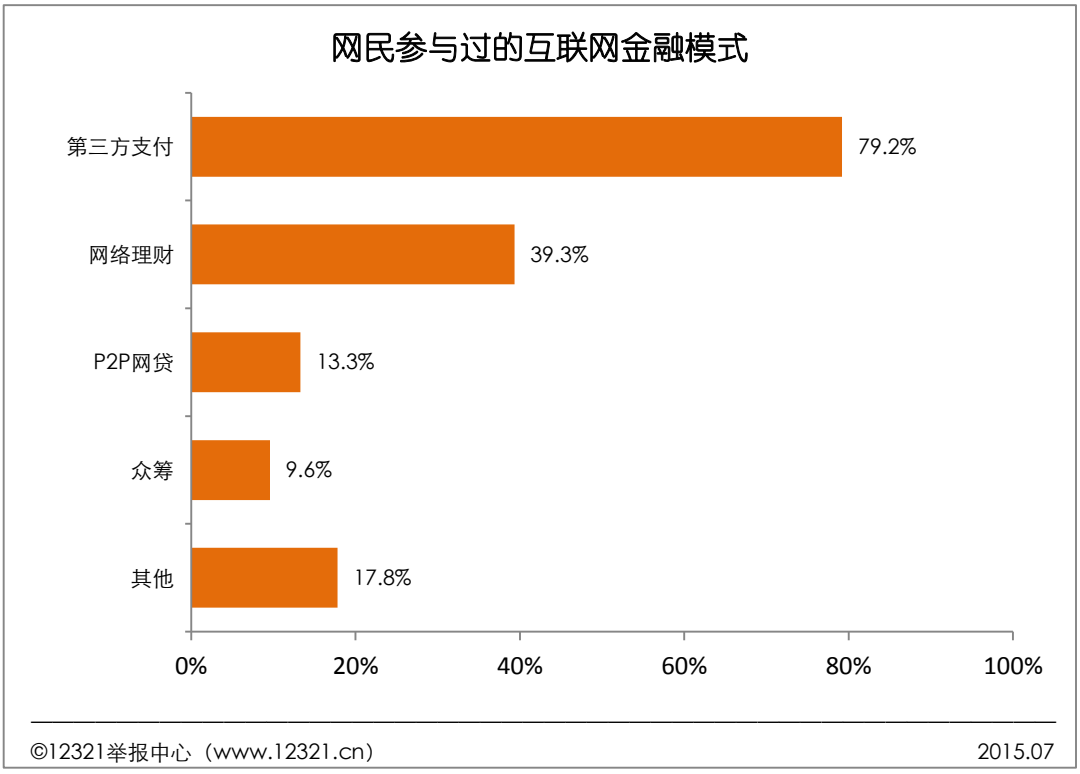


图 23

- **使用互联网金融产品时碰到的侵权现象**

互联网金融产品在使用过程中，遇到的侵权现象有：

（1）不诚信的现象普遍。57.4%的用户碰到过“夸大产品收益率”的现象；

（2）财产安全得不到保障。首先是“无法正常转账”，达 27.7%；其次是“账号密码被盗”（19.4%）；“银行卡被盗”（9.6%）；

（3）诈骗现象严重。26.5%的用户“遭遇木马钓鱼”；16.9%的用户“遭遇跑路、金融诈骗现象”。

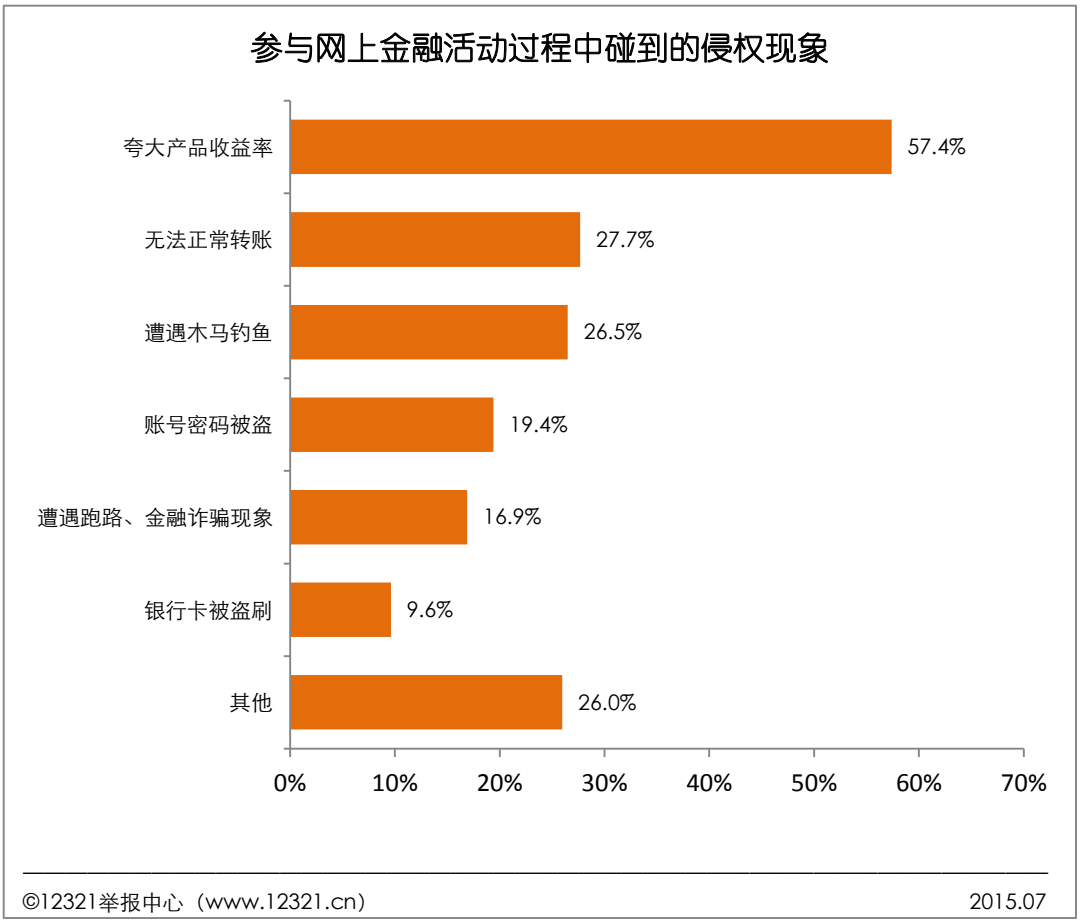


图 24

【提醒】假冒银行网银诈骗多发 警惕钓鱼网站

近期，12321 举报中心接到假冒官方银行以“电子密码器过期”为由的短信诈骗信息增多。经核查，不法分子冒充银行官方工作人员采用群发短信的方式，假称“电子密码器即将过期”，要求用户登录某网站进行安全升级，乘机盗取事主的账号、密码等信息。其短信样本如下：

用户进入仿冒的银行手机官网后，钓鱼网站会要求网友输入手机银行的账号密码，并逐步要求网友填写身份证号码及网银电子密码器上的动态密码。用户提交以后，该网址便会提示升级成功。此时，网友还误以为自己的电子密码器已经恢复正常使用，殊不知骗子已经将自己的个人身份信息盗走，并快速将银行账户洗劫一空。

12321 举报中心提醒用户注意冒充银行客服号码的短信，极有可能与真正的银行客服短信出现在手机短信界面的同一对话框内，极易导致群众上当受骗。另外，部分嫌疑人甚至还冒用手机用户名义，使用事主的手机号码发送短信，在其亲朋好友、同事等熟人中实施定向的诈骗。网民可以通过多种方式进行防范。

第一，“伪基站”发诈骗短信前，事主的手机可能会先失去信号，在此期间诈骗短信会进来，然后又恢复信号状态。如果遇到此种现象，就一定要小心了。

第二，要保管好自己的个人信息，包括身份证号、卡号、密码、电子密码器动态密码、短信验证码等，不要向他人提供。

第三，以不变应万变，收到什么短信都别轻信，也别怕麻烦，打个电话拨回官方的客服号码，银行也好，亲朋也罢，一沟通就知道真假。

第四，注意识别区分网站地址，不要点击他人发来的地址链接登录电子银行。

第五，绝不轻信任何套取信息的短信和电话，带有区号前缀的银行客服号码均为伪装号码。

第四部分 保护网民权益创新&优秀实践案例汇编

为了展示互联网企业在网民权益保护方面的努力与成果，加强对网民权益保护相关工作的推广与宣传，中国互联网协会 5 月发起了保护网民权益创新&优秀实践案例征集活动。征集活动历时 1 个月，截至 6 月 20 日，共收集案例 34 份。来自网信办、公安部、国家工商总局、工信部、国家互联网应急中心等政府和机构的领导以及 IT 界媒体和知名律师等相关业内人士共同组成的专家组对这些案例进行了评选。评选维度包括：用户的可感知度、保护网民权益的效果、公益性、原创性、社会影响等。经过评选，专家组认为，这些案例在展现了互联网企业在保护方面的努力和举措，都是在保护网民权益方面的优秀实践，各具特色，均具有一定程度的推广普及价值。有 11 个案例在评选中得票较高，尤其值得表彰。

在此向所有积极参加案例征集、评选的互联网企业和相关专家表示诚挚的感谢！部分专家对部分案例进行了简单的评价，一并附后。由于时间仓促，加之此次案例征集、评选工作尚属首次，纰漏在所难免，欢迎社会各界批评指正。

1、国家网络安全青少年科普基地

A.保护网民权益创新&优秀实践情况介绍

“国家网络安全青少年科普基地”是在中央网信办、国家教育部、国家科技部、中国科协和共青团中央的共同指导下，以“青少年网络安全教育工程”的网络安全教育经验为基础，结合 360 公司互联网安全中心的专业网络安全技术建立的专门面向青少年的网络安全科普体验基地。基地位于中国科学技术馆一层，占地面积 300 多平米。

基地定位于全面提升青少年的网络安全意识、普及网络安全知识。以 360 公司互联网安全中心提供的安全大数据可视化系统为核心，是国内第一个全设备入网，集合了云语音识别、多人体感互动、4D 场景体验、钓鱼 WIFI、黑客改号实景体验等先进技术的高科技智能体验基地。基地实现线上线下联动，可以通过 360 的全景技术进行线上参观体验，通过 360 智能摄像机进行实时同步直播。整个基地以互动体验的方式帮助青少年感知网络威胁、学习网络安全知识，进而提升网络安全意识。

B.实践效果

6 月 1 日，第二届国家网络安全周活动在科技馆举行，活动上中央网信办、国家教育部、

国家科技部、中国科协和共青团中央等相关领导和青少年代表为基地揭牌，并到基地参观体验。基地从 6 月 1 日正式揭牌到 6 月 7 日期间，累计参观人数约 35000 人，发放网络安全知识宣传单、网络安全漫画书、光盘等各 1000 余份，参观者反响热烈。与此同时，基地也吸引了大量的媒体关注，新闻联播、焦点访谈、新闻直播间、央视英文国际等频道均对基地进行了全面报道，此外，新华社、人民网、光明网、凤凰网、新浪、网易等 100 多家媒体也从不同角度对基地进行了深度报导。

C.网民反应

基地在线下吸引了 35000 多名参观者，线上覆盖了数百万名网民，参观者普遍表示，基地科技感十足，互动项目生动有趣，能够在游戏中轻松掌握网络安全知识和网络威胁的原理。

此外，基地每天都会举办网络安全知识讲座，由安全专家现场讲解安全知识。6 月 2 日，基地接待了来自全国 10 个省市自治区的参加第七届全国少代会的小代表 135 人，全体参与到了体验活动中。小代表们在接受媒体采访时表示，在基地学到了之前没有接触过的网络安全知识，回到家乡一定把自己学到的分享给身边的同学、小伙伴、老师及家长。其他来参观的青少年也反馈：“能在玩游戏中学习，感觉非常棒，轻轻松松的就学到了好多知识。”、“基地里最喜欢玩的就是这网络安全战车的游戏，答题通关对网络安全知识印象更深刻，而且非常有成就感。”等等。

D.推荐理由

“国家网络安全青少年科普基地”由中央网信办、国家教育部、国家科技部、中国科协和共青团中央共同指导，结合 360 公司专业的网络安全技术和创新意识，解构网络安全意识，重塑基地体验模式，将先进的体验互动技术与网络安全知识相结合，寓教于乐，用青少喜欢的方式传播了网络安全知识。

基地的建设一方面响应国家号召，加强青少年网络安全教育，另一方面从实际出发，运用互联网+的思维和先进的科学技术以互动体验的方式来传播知识，得到了政府、媒体及青少年的认可。

E.原创性声明（承诺书）

本公司承诺，“国家网络安全青少年科普基地”的内容策划、云语音识别技术、多人体感互动、4D 场景体验、钓鱼 WIFI 体验、黑客改号体验、危机地图等互动项目的技术等都为我方原创，依托于我公司安全技术和专业团队。

点评：

少年强则国强，青少年是互联网的原住民，更是中国网络安全的未来和希望。

“让我们共同携起手来，关爱青少年，服务青少年，引导青少年，培育造就新一代的‘中国好网民’，引领和开创网络空间更加美好的未来，培养和造就网络强国的建设者和接班人。”

2、天下无贼反信息诈骗联盟

A.保护网民权益创新&优秀实践情况介绍

“反信息诈骗联盟”是由深圳市公安局反信息诈骗中心、腾讯公司等发起的联盟组织，成立于 2013 年 12 月，现已壮大至上百个联盟单位，并得到公安部、深圳等各地网警、深圳市政法委、中国互联网协会、CFCA 中国金融认证中心等权威机构的认可和大力支持。作为中国首个实现“警、企、民”完整合作的网络反信息欺诈组织，其不断动员全社会力量，通过标记诈骗电话和短信、数据共享、案件侦破受理及安全防范教育等深度合作，向日益猖獗的信息诈骗产业链发起全面反击，唤起全民参与反信息诈骗。

联盟拥有以下反信息诈骗能力：

（1）反信息诈骗数据库

以腾讯安全所运营的“安全云库”为基础，“天下无贼”反信息诈骗联盟所有成员以反信息诈骗为目的，共建、共享反信息诈骗数据库。该数据库囊括了全球最大的风险 URL 网址数据库、全国最大的活跃电话号码库，以及全国首个恶意诈骗银行账号黑名单数据库。联盟内来自各行业、各领域的成员单位，也一起参与反信息诈骗数据库的建设和共享，以“大数据”的方式增强对信息诈骗的防御能力。

（2）警企联动打击诈骗罪案

基于对反信息诈骗联盟数据库的大数据分析能力，“天下无贼”反信息诈骗联盟与全国各级警方展开紧密合作，警企互动联手打击信息诈骗罪案。反信息诈骗联盟成立以来，先后协助深圳、广州等地警方，破获了包括“XXX 神奇”、“相册”病毒等多个信息诈骗典型案例。

（3）反诈骗公益品牌宣传

增强社会民众对信息诈骗的识别能力和防御能力，是“天下无贼”反信息诈骗联盟的社会使命。腾讯安全等联盟成员，与各地警方联手，通过大数据报告、互动小游戏、落地社区和校园宣传等多种形式，动员全社会关注信息诈骗，向民众普及反信息诈骗常识。

（4）标记和拦截诈骗电话号码

基于腾讯手机管家超过 7.3 亿累计用户量，庞大的用户群体参与到了反信息诈骗公益事业中——腾讯手机管家的用户，通过便捷的“一键标记”功能，对可疑的诈骗电话号码进行标记，把防御骗子的能力向社会大众接力传播。同时，通过腾讯手机管家，“天下无贼”反信息诈骗联盟也可以实现向海量用户提供无偿、实时的防诈骗提醒，保护联盟成员的用户免受信息诈骗之害。

“天下无贼”反信息诈骗联盟对外合作模式

（1）微信公众号便民查询服务

通过微信公众号，“天下无贼”反信息诈骗联盟合作伙伴可以快速获得对公众的反信息诈骗数据查询、举报等能力，让民众随时随地获得对诈骗信息的甄别和防御能力。通过统一开放的微信查询接口，合作伙伴可以在其微信公众号中实现对可疑电话号码、URL 网址、银行账号等信息的实时查询。

（2）数据共享与分析

“天下无贼”反信息诈骗联盟对合作伙伴开放反信息诈骗数据库，合作伙伴可以通过网站平台、数据接口获得反信息诈骗数据。借助腾讯安全的大数据分析能力，合作伙伴也可以分地域、诈骗类型等不同纬度的反诈骗数据分析报告，帮助合作伙伴提高对信息诈骗犯罪的打击和防御能力。

（3）公益宣传与教育

通过“天下无贼”反信息诈骗联盟成员海量的用户覆盖，以及广泛的社会传播资源，联盟与各级警方部门联手做好对社会大众的反信息诈骗公益宣传和教育工作，增强大众对信息诈骗的防御能力。

B.实践效果

联盟成立于 2013 年 12 月 26 日，成立之初只有十余家成员，如今这个数字翻了十倍，包括金山、搜狗、京东集团、拍拍网、唯品会、搜狐搜易贷、财付通、顺丰快递、珍爱网、微信支付、手机 QQ 钱包等互联网企业，工商银行、建设银行、农业银行、中国银行、招商银行、CFCA 等金融机构，以及全国三十余家电视台、网络媒体，十余家覆盖全国的商用 WiFi 厂商也都成为“天下无贼反信息诈骗联盟”的一员。

从成立至今，反信息诈骗联盟在全国取得了不错的成绩。数据显示，联盟共接群众来电 62 万人次，直接劝阻 1.84 万名群众避免转款达 1.56 亿元，为 9776 名受害人快速拦截被骗

资金 1.09 亿元（其中全额拦截 1597 宗 4820 万元）,避免、挽回群众损失合计近 2.65 亿元；“呼死”涉案诈骗电话 51641 个、帐号 25287 个，通报运营商关停及技术封堵违法电话 5017 个；处置违法网站 1390 个。2015 年 5 月，协助广州警方破获“10086”特大电信诈骗案。

C.网民反应

天下无贼的反诈骗能力通过腾讯手机管家获得了广泛的普及，通过与警方的联动，快速打击黑产和诈骗，获得了包括百姓、企业以及政府的认可和好评。

网友评论：“像拥有一道防护墙一样，将诈骗信息拒之门外，毫无遗漏。”

网络安全专家评论：“通过线上线下的资源共通，实现快速响应，举报体制的建立完成了从源头到过程再到结果的强力反诈骗体系。”

D.推荐理由

天下无贼反信息诈骗联盟通过“警、企、民”的联动和合作，为防止用户被网络各类不实信息诈骗，防止被垃圾电话、诈骗电话、骚扰电话骚扰，保护个人隐私，保障用户信息安全上，起了重要的作用，为 7.8 亿网民所使用，取得了良好的效果。

E.原创性声明（承诺书）

天下无贼反信息诈骗联盟属于腾讯原创，其中的案例和数据保证真实可信。

点评：

此案例体现出企业勇于承担社会责任的态度、勇气和胸怀。

3、360 骚扰电话弹幕吐槽

A.保护网民权益创新&优秀实践情况介绍

弹幕最早发源于视频动漫网站，因大量吐槽评论从屏幕飘过，看上去像是飞行射击游戏里的弹幕而得名。360 手机卫士的来电秀添加了弹幕吐槽功能，在手机用户接到陌生电话号码来电时，可展示其他用户对此陌生号码的多条动态点评，既真实又生动形象。

B.实践效果

用户在接到骚扰或诈骗电话后可对此电话号码进行标记，同时还可自由发挥输入 30 字节以内的吐槽文字，其他用户在接到此已被标记并弹幕吐槽的电话号码来电时，可了解到该电话号码有可能会进行推销、诈骗或骚扰等行为，从而对是否接听该通电话进行判断。

C.网民反应

弹幕吐槽功能给手机安全软件增加了互动性和趣味性，增强了对于防骚扰电话的知情权和参与感。如对骚扰电话号码评论“这货是机器人”、“你妹广告”、对广告推销电话号码则有评论“聊了 30 分钟，这货真能喷”、而房产中介电话号码还有评论“尼玛，你打过 3 遍了”、“请帮我付首付，谢谢”等等，在调侃骗子之余，也充斥着大家互助提醒防骚扰电话的主题。

D.推荐理由

通过这种倍受青年人喜爱的“弹幕吐槽”与骚扰拦截相结合的形式，既实现了 360 手机卫士安全软件的拦截功能，又增强了用户的互动参与性，同时也提升了骚扰及诈骗电话标记的准确性。

E.原创性声明（承诺书）

本公司承诺，360 手机卫士骚扰电话弹幕吐槽，为我公司原创。

点评：

一件事若无趣味，则不能长久。与网络各类不良信息的斗争，路漫漫其修远，需要一些有意思的事来点缀。此举调动了网友的兴趣，将一件枯燥但很重要的事情变得轻松。

360 手机卫士的防骚扰功能与弹幕的结合是工具类产品的一大创新，既能提示诈骗电话、骚扰电话的内容，让大家在接电话之前就看到电话内容，提高大家的防范意识，又很有趣味性。

4、新浪微博社区公约体系

A.保护网民权益创新&优秀实践情况介绍

新浪微博在 2012 年 3 月立项起草、5 月 28 日颁布实施《新浪微博社区公约》及一整套社区管理体系，该体系是国内首个微博社区公约，属于网络社区管理和自律机制，旨在规范和管理微博上的用户行为，维护和净化微博社区秩序。该公约明确了微博用户权利、用户行为规范及社区管理机制，并建立了公开透明的违规处理机制，有效维护了网民权益。

B.实践效果

微博社区公约上线两年时间，社区管理中心接到用户举报超过 2600 万次，其中处理了骚扰用户的垃圾广告 1900 多万次，淫秽色情危害信息 300 多万次，处理用户纠纷及不实信息 400 万次,超过 40 万人次被扣除信用积分；有效维护了微博社区秩序。在此期间，微博累

计处置不实信息案例 15384 个，处置用户纠纷类案例 711167 个。除此之外，新浪微博对违规行为的举报受理率始终维持在 99%以上，其中对“不实信息”的举报量已从上线时的日均 4000 条下降到日均 500 条，有效遏制了造谣传谣的不良行为。

C.网民反应

社区公约体系的社区委员会成员全部来自公开招募的微博网友，自社区公约上线的两年时间里，社区委员队伍逐步扩大，已经从最初的 5000 人扩大到 6.8 万人，为社区管理提供了有效支撑。通过社区公约惩罚制度，微博网民发布的有害信息与不良信息出现率不断减少，造谣、传谣的不良内容也被有效遏制，极大程度上净化了网络环境。

D.推荐理由

社区公约是一种网民自律的管理机制，其裁判机制参考借鉴了美国普通法系的陪审团制度，建立了独有的社区委员会制度。社区委员会参与违规行为的研判，决定具体行为是否违规，而社区委员会的成员则全部来自公开招募的微博网友，以此真正落实用户自律。具体而言，系统会随机抽取指定数量的委员会成员参与违规行为的研判，站方依照公约及管理规定，对委员会研判确认违规的行为执行处罚。专家委员成员则专门用于处理用户对研判结果不满提起的上诉，从而最大程度上实现公约实施的公开性和公正性，更好更快地维护了网民权益。

点评：

网上不良信息的判定是个大难题，管理机制和技术分析方面都有海量投入，但是效果并不如人意。新浪微博社区管理体系将这个难题交给了广大网友，取得了不错的效果，积累了经验。此案例说明，只要规范引导，安排得当，没有网友解决不了的网络问题。

5、北京网络安全反诈骗联盟

A.保护网民权益创新&优秀实践情况介绍

北京网络安全反诈骗联盟由北京市公安局网络安全保卫总队与 360 公司联合发起成立，旨在防范和打击日益猖獗的电信诈骗和网络诈骗犯罪行为。联盟是以北京网安的技术能力和 360 云安全防护体系为基础，面向企事业单位及社会组织提供的诈骗信息举报平台。任何企业、事业单位及社会组织均可通过联盟向北京网安和 360 互联网安全中心批量举报和推送诸如恶意网站、诈骗电话、诈骗 QQ 号码等网络诈骗信息。

B.实践效果

截至 2015 年第一季度，联盟合作伙伴已达 35 个，包括：商务部、支付安全联盟（中国银联）、淘宝网、中国人民银行、中国建设银行、顽石咨询和 Ebay 等，联盟共接到恶意网址举报 178503 条。

C.网民反应

有效减少了上当受骗的情况。

D.推荐理由

为企业与公安机关联手打击网络犯罪提供了更为有效便捷的新形式，同时也为企事业单位、组织机构等举报不良及诈骗信息提供了更为简单快捷的新途径。

E.原创性声明（承诺书）

本案例及相关描述为 360 公司原创。

点评：

发挥群策群力优势，扩大诈骗线索来源，提升信息响应速度，增强打击犯罪实效，更好地保护群众利益不受侵害。

北京网络安全反诈骗联盟开创了公安机关与互联网企业联合打击网络犯罪的新途径与新方法。联盟充分结合了北京网安的技术能力和 360 云安全防护体系，同时通过联盟合作伙伴的形式，为企业和社会组织积极参与打击网络诈骗的行动提供了有效的途径。

猎网平台，将反诈骗工作从公安机关和企业的合作参与，扩大到了全体网民的共同参与。为网民通过互联网方式举报和投诉各类网络诈骗开辟了新的，行之有效的方式方法。是互联网+安全执法的有益尝试。

6、阿里钱盾：智能手机真假鉴定

A.保护网民权益创新&优秀实践情况介绍

背景：针对当前市场上的智能手机存在以假乱真的现象，即低端机通过刷机换外壳等行为，制作成高端机型，继而再以高价卖出。导致了消费者正当权益受到严重的损害。另外，很多不法商家也将这样的手机放在互联网平台上进行售卖，极大的影响了电子商务的健康和发展。在打击假货，维护消费者利益和保障电商健康发展的道路上，阿里钱盾一直都在努力。创新方案：采用硬件指纹鉴真模型、手机造假木马专业查杀、真机串号查询三大手段为用户提供高精准的智能真机鉴定系统。

B.实践效果

数据成果，产品上线之后，iPhone 验机神器使用率达到 75%，同时用户的检测数据显示 1000 台 iPhone 中有约 4.5 台为假冒 iPhone。Android 小米真假鉴定使用率达到 55%，100 台小米手机中就检测出约 1.7 台为假冒手机。此类假 iPhone，假小米不仅严重影响了消费者的权益，也侵害了 apple、小米等公司的利益。

C.网民反应

从超高的使用率来看，网民对此类创新功能是高度关注、非常感兴趣的，可见此类功能是切中了网民的要害，可以有效解决网民问题，保护网民的权益。

D.推荐理由

1.切实保护网民权益。

2.促进互联网购物健康发展。

E.原创性声明（承诺书）

承诺阿里钱盾-验机神器功能为阿里钱盾原创技术。

点评：

翻新手机层出不穷，这一招有效果！

7、公正邮

A.保护网民权益创新&优秀实践情况介绍

背景：电子邮件被网民广泛应用，国家法律规定电子邮件可作为法定证据。

现状：发生纠纷时，网民希望把电子邮件作为证据呈现，但取证难度大、成本高，效力低。

创新优秀实践：杭州安存网络科技有限公司推出公正邮，为 7.1 亿网民提供电子邮件存管证明服务。2014 年 7 月 8 日，安存科技联合中国第一大电子邮件服务商——网易推出了网易公正邮。

B.实践效果

网易公正邮为 7.1 亿网民解决了电子邮件取证成本高、难度大，电子邮件证据效力低的难题，大大节约了网民的时间、经济成本，对于净化网络环境、保障网民权益、打造诚信互联网生态圈起到了至关重要的作用。

以下是 7.1 亿网民中使用公正邮成功维权的代表之一：2014 年 10 月，张某通过网易公正邮，保全借款时间、数额等邮件内容，成功还原借款事实，挽回 10 万元经济损失。

C.网民反应

网民认为公正邮的出现是中国互联网法治史上里程碑式的事件，公正邮是一个互联网和司法跨界创新的好产品，可以有效解决电子邮件“易逝、易改、易变”的特性所带来的问题，前置性地解决了证据的法律效力问题，对于净化网络环境、保障网民权益、打造诚信互联网生态圈起到了至关重要的作用。可广泛应用于商务贸易、知识产权保护、劳动合同、律师服务、网络消费维权、客户服务等纠纷。

D.推荐理由

安存科技，以无利害关系的独立第三方身份，为 7.1 亿网民提供了公正邮这样一个电子邮件存管及公证解决方案，实现用户电子邮件取证的自主化，事前化和标准化。对于净化网络环境、保障网民权益、打造诚信互联网生态圈起到了至关重要的作用。

E.原创性声明（承诺书）

我公司郑重声明：“网易公正邮”安存电子邮件保全系统（方案）及其相关应用软件为杭州安存网络科技有限公司自主研发的成果。除邮件交互（发送、接收等）功能由网易邮箱系统实现外，不存在未经授权使用他人已经发表的研究成果等侵犯第三方知识产权的行为。若有不实之处，我公司承担相关法律责任。

点评：

当摊上事儿了，公正邮的好处就体现出来了。

8、媒体反欺诈举报平台

A.保护网民权益创新&优秀实践情况介绍

知道创宇运营的安全联盟（www.anquan.org）是国内最大的第三方网络安全数据共享平台，通过联合国内一线互联网及安全企业建立行业公认的互联网安全标准，进行恶意网址数据共享，目前已建立超过 5 亿条恶意网址 URL 的恶意网址数据库，每日与合作单位进行超过 5500 万次数据交换，每日对网民进行超过 10 亿次网络风险告警，有效提示网民远离坑蒙拐骗。

安全联盟成立了一个民间志愿者组织“民间万人鉴定团”，每日向安全联盟平台提交超

过 3000 条有效举报数据，目前“民间万人鉴定团”规模已经突破 4 千人。安全联盟“民间万人鉴定团”核心成员“小布”在第一届国家网络安全宣传周上被官方媒体采访报道（http://news.xinhuanet.com/politics/2014-11/28/c_1113447665.htm），在 2014 年 12 月 26 日“天下无贼·反信息诈骗联盟一周年发布会”上荣获反信息诈骗先进个人称号。

浙江卫视《中国好声音》节目火爆，导致被仿冒严重，信息诈骗分子制作中奖欺诈网站，诱骗网民，危害巨大。安全联盟与浙江卫视联合发起了“防骗举报专区”（http://www.anquan.org/zjtv/），利用浙江卫视强大的传播能力在《中国好声音》播出期间持续三个月不间断宣传举报平台，提醒网民防骗，并号召网民参与到举报中来。后安全联盟与湖南卫视、安徽卫视以及全国数十家媒体联合起来，建立媒体反欺诈举报平台（http://www.anquan.org/fqz/），并于 2014 年 12 月 26 日正式对外发布。因为在反信息诈骗领域的突出成就，安全联盟被授予“反信息诈骗先锋机构”荣誉。

B.实践效果

通过安全联盟与各大媒体的良性互动，以及合作单位如腾讯、百度、金山、搜狗等的配合，安全联盟媒体反欺诈举报平台通过各大公司及浙江卫视、湖南卫视等官微宣传曝光量超过 10 亿次；

2014 年帮助浙江卫视、湖南卫视、安徽卫视接受共 41874 次有效中奖欺诈网站举报，并有效拦截，共接受网民 34 万次举报。

通过对仿冒综艺娱乐节目的中奖欺诈网站的专项打击，令更多网民提升网络安全意识，并吸引网民参与安全联盟平台更多恶意网址数据的举报，一年内共收到网民和媒体的举报 737 万条，其中有效举报数达到 318 万条。

C.网民反应

由知道创宇拍摄，并选送首届国家网络安全宣传周公益视频《全民参与，网络更安全》，获得主办方一致好评，并推送至各大平台宣传周专题头条视频，最终被评选为国家网络安全宣传周优秀公益短片。

短片地址：http://v.youku.com/v_show/id_XODI4NDc4MDY4.html?from=s1.8-1-1.2

D.推荐理由

安全联盟“媒体反欺诈举报平台”是一次网络安全行业与媒体、娱乐行业跨界合作的经典案例。安全联盟通过恶意网址数据共享的形式，最终让相对独立的各大互联网平台连接为一体，以提供全网拦截坑蒙拐骗网站的能力；而通过与时事热点的结合，进行专项网络治理，

并号召全民参与，通过媒体力量的放大和宣传，最终形成全民效应。把网络安全平台的专业能力和媒体的影响力作结合，最终为网民提供了一套完整的解决方案。

E.原创性声明（承诺书）

我司承诺，相关选送案例真实且为原创，愿意接受真实性考察。

点评：

受骗的都是对网络不太熟悉的老年人，网络安全问题太重要了，真的不只是安全业界自身就能解决的。安全联盟“媒体反欺诈举报平台”是一次网络安全行业与媒体、娱乐行业跨界合作的经典案例。把网络安全平台的专业能力和媒体的影响力作结合，最终为网民提供了一套完整的解决方案。

通过联合业界力量、媒体力量、警方及社会各界力量组成的这样一个反信息诈骗平台，实现了“警、企、民”对信息诈骗的“社会化治理”，长远来看是必然的趋势，也是最有效的方式，应当受到提倡并大力推广。

9、河北联通：黑名单机制助力公共互联网网络安全环境治理

A.保护网民权益创新&优秀实践情况介绍

河北联通在开展公共互联网网络安全环境治理工作的过程中，引入了黑名单机制，以黑名单机制作为基础，通过限制滥用网络资源的客户的上网行为来积极保障其他网民的合法权益。

河北联通结合木马僵尸网络控制端和移动恶意程序控制端的被检出记录建立黑名单。将检测数据与客户资料进行对照，形成“客户恶意行为”关联数据库，可在行业内共享。该项机制结合了用户自律与行业自律两种机制，属于创新机制。

B.实践效果

黑名单机制有效的发挥了教育、惩戒、引导网络用户关注自身网络安全和维护网络安全环境的作用。使用较小的经济成本，获得了相对较大的社会效益，对于倡导文明上网、守法上网的社会理念也发挥了一定的作用。

根据 2014 年 7 月至 2015 年 5 月统计数据，河北联通累计处置木马僵尸网络控制端 IP 地址 440 个，累计检测到僵尸网络活动 4413.97 万次。累计涉案客户 276 个，其中固定 IP 地址客户 54 个，动态 IP 地址客户 222 个。累计被处置次数超过 10 次的客户（即应加入黑名单的客户）有 25 个，其中固定 IP 地址客户 8 个，动态 IP 地址客户 17 个。经劝诫后矫正行

为的客户 10 个，实际加入黑名单客户 15 个。根据监测到的僵尸网络控制端通信特点判断，黑名单机制预期可削弱或阻断木马僵尸网络 8 个，预期可减少僵尸网络活动约 1000 万次。

C.网民反应

使用河北联通线路接入互联网的广大客户，能够正面理解并积极配合河北联通在此黑名单机制建立、实施过程中的工作。大部分客户能够自觉自愿接受河北联通为开展互联网网络安全环境治理工作所采取的措施，未引发网民投诉，未发生负面舆情。

D.推荐理由

在网络安全上升为国家战略的社会环境之下，如何引导、规范广大互联网用户的行为，将成为重要的课题。由于互联网环境区别于传统社会环境但又越来越紧密的联系于社会日常生活，因此，开展网络安全环境治理的工作将发挥不可或缺的基础性社会治理功能。河北联通所实践的黑名单制度属于创新机制，为此提供了有益的尝试，能够以较小的经济成本带来广泛的社会综合效益。

E.原创性声明（承诺书）

本推荐案例的作者郑重承诺本案例所涉及内容均为原创。

点评：

在网络安全上升为国家战略的社会环境之下，如何引导、规范广大互联网用户的行为，将成为重要的课题。

10、百度手机卫士“安全支付保赔”

A.保护网民权益创新&优秀实践情况介绍

在通过安全软件保护用户安全的过程中，不出现技术上的纰漏是几乎不可能的。面对花样翻新的病毒，总有漏网之鱼在安全产品推出有效应对措施之前得逞。百度针对这一情况，提出了“安全支付保赔”的服务。当用户的权益受到恶意应用侵犯时，可以向百度申请赔付，以尽可能降低恶意攻击给用户带来的损失和不便。

B.实践效果

5 月 27 日，在上海从事建筑设计工作的张先生收到一条来自 10086 的短信，告知他的手机号码获得了中国移动 100 元现金红包奖励，同时附带着领取“红包”的网址链接 wap.10086hblq.com。张先生点开了短信中的链接，随即跳转到“中国移动掌上营业厅”的页

面，点击进入“登录领取红包”的提示，并填写了包括银行卡号、银行卡密码、手机号码在内的私人信息。资料填写完毕后，在网站提示下张先生又下载了“中国移动客户端”。

5 月 28 日凌晨，张先生发现自己的银行卡莫名多出了一笔 3400 元的支出，他意识到这可能与 27 日收到的来自“10086”的短信有关，立即向警方报案。随后张先生开启了百度手机卫士“安全支付保赔”功能，向百度手机卫士申请保赔 3000 元。一周后，张先生收到了保赔金。这是移动互联网业内用户遭遇移动金融陷阱后获得移动安全厂商保赔的第一起案例。

C.网民反应

接受采访时，张先生激动的对记者说：“案子还没破，就先收到保赔金了，庆幸自己当初多了份心，百度手机卫士这么靠谱有效率，这真是意外的保障和惊喜。”百度手机卫士不仅做出了“安全支付保赔”的承诺，而且在出现用户权益被恶意软件侵犯时高效率地进行了赔付。不难看出，百度手机卫士不仅通过技术上的不断进步保障用户的安全，更设法在技术范围之外减少用户的损失与不便。

D.推荐理由

面对花样翻新的病毒，安全软件难免有更新不及时难以有效查杀的情形出现。针对这一情况，百度安全卫士提出了“安全支付保赔”的服务。当用户的权益受到恶意应用侵犯时，可以向百度申请赔付，以尽可能降低恶意攻击给用户带来的损失和不便、百度手机卫士通过各种手段保障用户的财产安全，通过先行垫付用户损失的方式让用户的生活尽可能远离不法

侵犯的困扰。

点评：

敢于“保赔”，说明对自己产品的信任和对用户保护的勇气，这样的做法虽有商业考虑的意味，但是得实惠的是广大网友。希望这样的“保赔”理念被社会广泛接受。

11、广西联通整治宾阳县网络诈骗实践

A.保护网民权益创新&优秀实践情况介绍

宾阳县网络诈骗猖狂，据 2014 年《南宁晚报》报道，从 2009 年算起至 2014 年 10 月，宾阳警方已经协助外地警方抓获嫌犯 1050 名，破案 2200 多起，协助追缴赃款 1000 多万元。去年来，我公司为配合县政府打击网络诈骗，积极采取各项措施：（1）向各营业厅、代理商多次培训宣贯实名制管理文件，签订责任书；（2）做好存量用户梳理，完成了 29 个重点村屯排查工作；(3)对各网点配备了身份证鉴别仪，新用户开户要通过身份证鉴别仪才可开户；（4）营业员将新增用户信息每周一 12 点前传给固网部综合管理员,汇总交公安局作为证据保存；（5）严格规范宽带装、移机，装机员要对自己负责的片区负责，每天将装机工单打印出来，签字确认；（6）配合宾阳县委、县政府、公安局，在全县范围内开展墙体、横幅、电视台、报纸等多种形式的高压宣传。与政府部门成立网络实名制及 QQ 网络诈骗宣传车，轮流在重点诈骗村进行广播宣传。

B.实践效果

经过我公司在实名制上的层层严格把控，在新增用户方面，已尽力保证宾阳的新增宽带用户均为实名登记用户，至今为止没有发现新增用户涉嫌网络诈骗的情况。在存量用户方面，我公司对上万个老用户进行了逐一核查，截至 2015 年 5 月 31 日，已经关停 2416 户疑似诈骗用户的宽带账号。在政府与运营商的联合打击下，网络诈骗犯罪团伙已经渐渐外逃，出现离开宾阳到外地作案的趋势。

C.网民反应

我公司与县政府、公安局等多方合作，严厉打击网络诈骗，让天下无贼，还互联网一片蔚蓝天空，得到网民的普遍认可和欢迎。

D.推荐理由：

广西联通的工作得到了宾阳县委、县政府的充分肯定,在网民心中树立了通讯运营商的

正面形象

12、支付宝无线木马防控

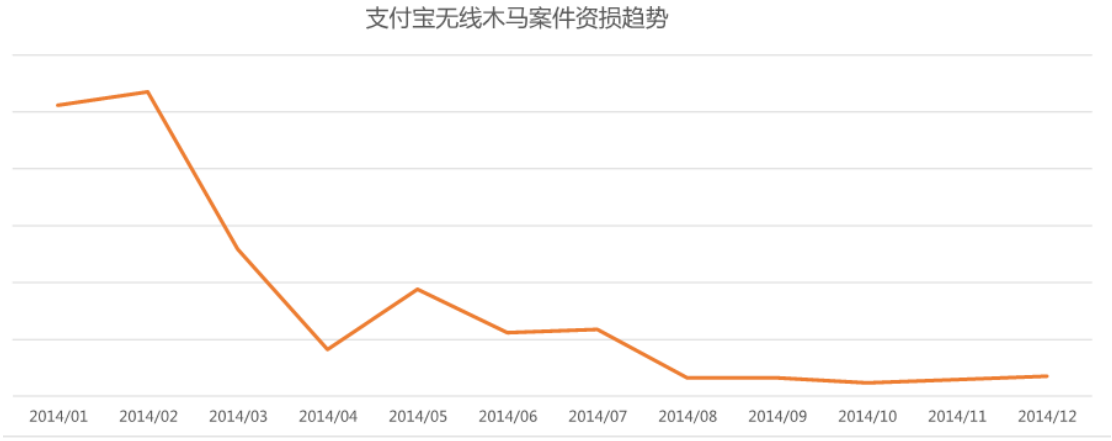
A.保护网民权益创新&优秀实践情况介绍

背景：根据第三方统计截至 2014 年 12 月，我国移动支付用户数从 2013 年的 1.26 亿，增长至 2.68 亿，同比增长 113%。权威第三方数据机构易观智库数据显示，2014 第三方移动支付的交易规模达到了 77660 亿元，环比增长近 500%。移动支付迅速成为中国手机用户的一种日常生活习惯，各种手机钱包和理财应用也成为了智能手机中必不可少的工具。然而，移动支付场景愈发丰富、用户规模迅速膨胀的情况下，必然会出现各种漏洞及各种攻击所带来的风险损失同样快速爆发。根据阿里移动安全研究，针对用户的欺诈，钓鱼很大一部分通过短信来完成。不法分子通过伪基站群发欺诈短信，使用钓鱼网站手机用户敏感信息，手机木马拦截转发验证码短信及通过网银或第三方支付平台盗取资金等一系列手段对用户进行诈骗，危害极大。支付宝通过实时防控策略，大范围降低了通过短信木马对用户带来的危害。

创新方案：通过聚安全提供的安全引擎识别高风险病毒及风险设备，来保护支付宝账户、身份证号码、银行卡号及手机号码，并通过支付宝提供的资金变动对交易风险进行综合评分，评选出高中低风险，联动执行各种安全操作，如直接拒绝交易冻结账户或通过安保问题检验来保护账户资金安全。

B.实践效果

2013 年大量支付宝用户受到伪基站短信木马的危害，案件量突增，阿里巴巴经过 2014 年在短信木马防控上的努力，目前案件量已经得到有效的控制。



C.网民反应

仅 2014 年第四季度阿里聚安全的查杀量就高达 371 万，确保超过 205 万用户的移动支付安全，无线木马安全资损率大幅降低，并长期持续维持在低水平趋势。

D.推荐理由

1.大幅度减少资金被盗案件，切实保护网民利益。

2.极大增加网民对移动支付的信心，进一步促进网络支付的发展

E.原创性声明（承诺书）

承诺聚安全提供的安全引擎识别高风险病毒，识别风险设备，来保护支付宝账户的功能为原创技术。

点评：

案件量得到控制说明此举取得了不错的成效。

13、浙江联通解决网站劫持案例

A.保护网名权益创新&优秀实践情况介绍

浙江宁波地区有用户反应，打开常见购物网站时有自动添加后缀的情况。由数据专业人员对宽带测试及网站访问测试中发现，访问苏宁等网站有异常跳转情况发生。在访问网站首页时，跳出弹窗广告的同时相关脚本进行了网站的重定向等操作。

针对此次网站劫持的现象，并不是简单的在页面中插入广告，而是在用户正常请求苏宁等电商主页后，通过推送脚本，在用户不知情的情况下，控制引导用户浏览器先进入链接，再重新打开首页。同时，此次问题处理中，推送后引导访问的 IP 不是联通本地 IP，对推送定位带来困难，即使专业用户也只能确认劫持情况的发生，却不能确认是哪方所为。因此，不仅影响了用户自有业务的正常使用，而且还会对用户的网络安全和隐私产生威胁，存在很大的安全风险。

B.实践效果

经浙江宁波分公司数据专业人员逐一关停测试后，确认是某业务合作项目违规推送造成，立即对相应的 IP 进行了封堵操作，同时通报相关市场部门，关停了该业务合作项目并进行相应处罚，有效解决解决网站劫持问题，保障了用户的网络安全和个人隐私，提升了客户感知。

C.网民反应

问题得到解决。

D.推荐理由：

目前在用户上网安全问题中，网站劫持是比较普遍的一种方式，一般的劫持方式有本地 ARP 劫持、路由器策略修改、安装客户端插件及服务器端控制等。现有的一些安全管理软件对于上述这些劫持均能及时发出警报，并引导用户处置。

而本次在日常工作中我们发现了一种相对隐蔽网站劫持事例，其利用正常的业务合作，通过连接跳转、重定向等操作，干扰了用户使用，并影响用户上网安全。发现该问题后，我们立即采取技术手段进行了业务封堵，并要求修订相应业务合作规范。从而保障用户使用安全，保护用户隐私。

14、淘宝活动防控

A.保护网民权益创新&优秀实践情况介绍

随着移动互联网的快速发展，为了提升用户的活跃度和满意度，同时增加用户的粘性，各家公司都将大量的营销资源投放到移动渠道上。通过各类活动，用户获取了实惠。但这也成为黑产眼中的香饽饽，不法分子通过自动化注册大量垃圾账户，利用垃圾账户和黑产工具来刷红包，获取优惠券，获取秒杀资源等，大量本该提供给用户的资源被黑产拿走，大大损害了用户的权益。通过阿里聚安全引擎中的设备指纹与后端大数据分析结合的防控技术，实现了实时高效的人机识别，打破了黑产流程中的自动化工作流，大幅度提升了黑产的成本，降低了黑产对活动的影响，将实惠还给用户。

B.实践效果

通过该防控技术，被不法分子占用的淘宝活动收益比例下降至 1/20，正常会员参加活动的机会得到有力保障，极大保护了客户的利益。

C.网民反应

用户的参与度，满意度大大提升，并从中真正获利。

D.推荐理由

1．保护了卖家营销资源不受侵害和用户获取实际实惠。

2．为了提升用户的活跃度和满意度，维护了整个商圈的生态利益。

E.原创性声明（承诺书）

承诺阿里聚安全引擎中的设备指纹与后端大数据分析结合的防控技术为原创技术。

专家点评：

网友最欢迎这样的案例了。虽然背后的技术实现机制网友可能不太懂，但是能抢到红包是最直接的实惠。

黑客产业化的运作模式值得业内警惕！

15、搜狗号码通 lite 版

A.保护网民权益创新&优秀实践情况介绍

搜狗号码通 Lite 版本，利用在通讯录里插入号码，首度在 iOS 上实现陌生电话防骚扰功能，搜狗号码通的 OCR 技术引用，进一步为苹果手机用户解决防骚扰问题。

B.实践效果

首度在苹果手机上为用户实现防骚扰功能，在 Appstore 可以直接下载。

C.网民反应

引起行业内专家用户的一致赞同，获得广大用户的喜爱，并在网络引发网民的一致好评。

D.推荐理由

iOS 首创、技术创新。

E.原创性声明（承诺书）

此功能为搜狗号码原创

点评：

苹果系统的封闭性导致苹果用户拿骚扰电话没办法。搜狗号码通的奇思妙想，使不可能成为可能，Lite 版本的效果和用户期望还有一定距离，识别率有待提高，但这份千方百计为用户着想的精神值得肯定。

16、腾讯手机管家

A.保护网民权益创新&优秀实践情况介绍

腾讯手机管家是腾讯旗下一款永久免费的手机安全与管理软件。功能包括病毒查杀、骚扰拦截、软件权限管理、手机防盗及安全防护，用户流量监控、空间清理、体检加速、软件管理等高端智能化功能。以成为“手机安全管理软件先锋”为使命，致力于为用户提供最可

靠的安全管理工具，目前已经拥有超过 7.8 亿用户，成为国民移动安全的标配软件。

其以成为“手机安全管理软件先锋”为使命，“玩得酷靠得住”为产品创新理念，成为 95 后年轻人的性格标签，完美贴合了“信息时代的优先体验者”90 后一代时尚新潮的追求。腾讯手机管家，不仅是安全专家，更是用户的贴心管家。

腾讯手机管家涵盖以下功能：

病毒查杀：独有杀毒引擎，自主研发云端查杀技术，国际测试全面认证，实现无缝安全保护；

骚扰拦截：业界领先云端智能拦截系统，精准拦截各类垃圾信息，屏蔽骚扰电话；

支付保护：首创移动支付“前、中、后”闭环保护，防钓鱼诈骗网站、防虚假二维码、防虚假 Wi-Fi 网络、防账号与密码被盗、防伪造支付软件；

广告拦截：全方位检测与拦截内嵌广告、弹窗广告，让用户远离广告骚扰；

权限管理：实时监控应用权限，滥用权限主动提醒，避免权限过度泄露隐私，保证用户信息安全；

隐私保护：对重要隐私信息进行深度加密，确保个人隐私不被暴露，实现全面隐私保护；

手机防盗：对手机的远程控制、定位被盗手机、远程清除手机隐私信息；

此外腾讯手机管家还支持强大的流量监控、垃圾清理、手机加速、手机瘦身、自启管理、软件管理等高端智能化功能。以“手机安全管理软件先锋”为使命，腾讯手机管家不仅是安全专家，更是用户的贴心管家。

腾讯手机管家依托全球最大的安全云库——腾讯安全云库，为用户提供强大的风险和信息识别功能，内容涵盖风险网址、诈骗电话、骚扰短信、银行账号黑名单、木马、APK 等丰富而且全面的网络安全数据,可以保障 99%网民的上网、搜索、网购、支付、通信等各层面的安全，其每日识别 8000 万电话号码、拦截 1200 万骚扰电话、拦截 500 万骚扰短信，检测出 3000 万恶意网址。同时，利用腾讯海量的计算和存储资源，每天可对上亿的用户行为和程序运行过程进行数据建模。并且在大数据的基础上，利用机器学习的算法，来识别物联网上的恶意数据。

B.实践效果

腾讯移动安全实验室监测数据显示，2014 年，腾讯手机管家查杀手机病毒次数达到 3.16 亿次，拦截 Android 病毒包达到 100.33 万，骚扰电话用户举报次数达到 4.34 亿次。此外，腾讯手机管家用户举报垃圾短信达到 6.2 亿。截止到 2014 年底，垃圾短信举报总数已达到

17.22 亿。如果将用户举报的垃圾短信用五号字串起来，长度可以从北京到广州往返 162 次。腾讯手机管家在提供移动安全产品服务的基础上，还积极与行业上下游建立紧密的安全合作关系，已经和 60 家电子市场、20 家安全厂商、23 家运营商与厂商、12 家手机应用等超过 100 家的企业或机构达成合作，通过整合行业安全的力量并进一步输送专业的安全检测服务，共同构建了更广泛的安全生态，使得产业链的合作伙伴们可以在网购、社交、游戏、支付、智能硬件等各种“连接”的场景中保护用户的安全。

截至 2015 年 6 月，腾讯手机管家用户数已超过 8 亿，已成为广大用户最喜欢的手机安全管理软件。2014 年知名调研机构易观智库发布研究报告显示，腾讯手机管家已经成为用户手机支付安全首选品牌。另据国内最大的独立第三方数据服务提供商 TalkingData 发布的《2014 移动互联网数据报告》显示，腾讯手机管家用户覆盖比例位居前列。

此外，腾讯手机管家的安全实力获得了世界的认可。腾讯手机管家连续多次以优异的成绩通过 AVTEST 国际测试，其中病毒查杀率、误报率等数据比肩国际手机安全厂商。英国西海岸实验室&赛可达实验室授予腾讯手机管家“手机安全唯一优秀产品推荐奖”。此外，手机管家还获得在 PCSL 2015 年 1 月的检测第一名；赛可达实验室 2014 年中文手机安全软件横评第一名等众多国际奖项认证。而手机管家的 WiFi 开放平台已经是国内最大的“免费安全 WiFi 开放平台”。

第三，依托于背后全球拥有最全数据的腾讯安全云库，每天对过亿网址进行安全监测，拦截千万次的欺诈骚扰电话，检测出百万量级的病毒木马，每年避免网民损失近百亿元。最后，腾讯手机管家已经多次协助警方成功破案。去年 8 月腾讯手机管家配合警方仅用 9 个小时就抓获了轰动全国的“XX 神器”手机木马案犯罪嫌疑人；2015 年 3 月，又配合广州警方抓获“相册”新型手机木马病毒制作者何某，缴获用于作案的笔记本电脑、短信群发器等一批工具。

C.网民反应

手机管家的技术能力以及强烈社会责任感不仅受到社会各界的广泛点赞。

网友评论：“手机管家功能强大，能够全方位保障手机安全，真是装机必备！”

网络安全专家评价：“依托强大的大数据积累和运营能力，腾讯手机管家将安全与用户的多种场景连结，并且具备鲜明的品牌个性，贴合互联网精神，普及率高，是可靠的个性的安全软件。”

D.推荐理由

作为腾讯旗下一款永久免费的手机安全与管理软件，其核心的病毒查杀，骚扰拦截，支付保护，隐私保护等功能，为全面保障用户的手机安全做出了巨大努力和贡献，践行了其“手机安全管理软件先锋”为使命，证明了腾讯手机管家不仅是安全专家，更是用户的贴心管家。结合安全云库的能力，反馈、收集、整理、分析，并且最终输出，不断增强自我防护升级，更及时保护用户移动信息安全。

E.原创性声明（承诺书）

腾讯手机管家系腾讯旗移动端重要安全产品，我们承诺其中的案例和数据保证真实可信。

17、微电影的原创保护

A.保护网民权益创新&优秀实践情况介绍

《我们眼中的你》视频拥有者“草根东方一号”是一位视频专业制作人（PGC 用户），2014 年 2 月，为了进一步提高其拍摄视频的热度，该用户与我网（第一视频）洽谈合作，签署授权协议，其所拍视频我网（第一视频）拥有独家播放权，而我网（第一视频）则保证其电影不作商业用途。

2014 年 12 月，我网（第一视频）为了进一步优化改革，与众多视频制作专业用户（PGC 用户）商谈合作，提高我网内容的质量以及专业度。而《一方水土》制作者“精彩源于原创”与我网（第一视频）于 2014 年 12 月 28 日签署协议，其定期制作的微电影将在我网（第一视频）微电影专栏定期推送，观影者付费观看。

2015 年 3 月 16 日，“精彩源于原创”用户新拍摄的《一方水土》在我网推送上线，由于该微视频画面精美，且视频内容独特，上线三天内该视频获得了上千的点击，给用户以及我网（第一视频）都带来了一定的收益。我网在察看该视频投放情况是发现该视频的评论里涉及到一个名为《我们眼中的你》的微电影，该评论说《一方水土》与之前我网热搜的视频《我们眼中的你》无论在拍摄方式和内容构思上都极为相似。随即，我网（第一视频）相关工作人员查看相关视频，发现约一年前 2014 年 4 月“草根东方一号”用户上传的视频《我们眼中的你》与正在我网热播的微电影《一方水土》相似之处不少，且《我们眼中的你》视频最后拍摄者明确标明“原创精品，请勿抄袭”。

我网工作人员即刻与《我们眼中的你》的拥有者“草根东方一号”以及《一方水土》拍摄方取得联系，在得知双方拍摄该视频的一系列细节与用户的拍摄想法后，我网认为《一方水土》确实存在抄袭《我们眼中的你》的嫌疑。此前已与“草根东方一号”用户签署相关合

作协议，该用户在我网更新的视频只作宣传推广，不作商业用途。现今我网虽然未从《我们眼中的你》获取收益，但却从与其相似的视频《一方水土》获得一定的商业利益。这首先有违当初我网（第一视频）与“草根东方一号”的承诺，其次，《一方水土》的播放与我网（第一视频）的成立原则相违背，我网（第一视频）以来一直遵守国家相关法律，支持原创，维护版权。

事件发生的当天，经过一致的商讨后，我网立即下架《一方水土》的视频，不再将此视频在网站上进行任何的宣传和推广。同时针对他们此次的抄袭事件，我网对《一方水土》制作人进行了相应的处罚，不仅封禁他们的 PGC 账号，限制半年内不得再进行任何视频的上传，同时保留诉讼权。如果原创作者后续诉诸法律进行维权我网会全力支持并予以配合。针对此次产生的收入网站成立了支持原创的基金库，给予原创作者们制作上的支持，协助停止该视频在其他网站的侵权行为。为了防止此次的恶劣事件再次发生，我网对所有 PGC 及视频提供者进行了知识产权的培训，一方面警示 PGC 及视频提供者不要有这种不良和侥幸的行为，要尊重他人的版权，另一方面也引导 PGC 用户有版权保护意识，坚决打击抄袭的行为，支持原创，维护版权。

B.实践效果

通过我们的不断努力，以及各种举措，极大的提高了网民的原创热情及对第一视频的信任，吸引很多 PGC 用户（视频专业制作人）以第一视频作为他们原创视频的首发或者独家播出平台。

C.网民反应

在此事件发生以及处理后，广大网民通过评论、邮件、微博等不同形式表示了赞同。

D.推荐理由

此案例事情虽小，但是充分体现了第一视频在支持用户原创，打击剽窃上的决心，以及我们对构造一个绿色的、可发展的视频生态环境所做出的努力。

点评：

对原创版权的重视，其实是对网民的负责。

视频版权的侵权在最近几年一直是屡禁不止，视频拥有者对这方面的法律意识也较为淡薄。不过第一视频网对于这次事件的处理上很到位。不仅针对侵权方做了相应的处罚，同时也对 PGC 用户做了相应的培训，以此来杜绝此类事件的发生。这也是对整个视频行业的良

性发展做出了最大的支持和表率。

18、江苏电信：旺铺助手垃圾短信治理

A.保护网名权益创新&优秀实践情况介绍

为更好贯彻垃圾短信治理工作要求，江苏智恒在江苏电信的统一管理下，持续推进垃圾短信管理工作，确保业务持续、健康发展。

1、建立敏感词库：

旺铺根据国家公安机关提供的一系列关键词、敏感词，由旺铺（全国）垃圾短信监控小组进行汇总归纳；旺铺业务平台从互联渠道获取（360 互联网安全中心，百度互联网安全中心）；更新频次为每周（每周三更新敏感词库）。

2、明确旺铺平台拦截操作流程：

（1）旺铺助手业务平台对用户发送短信进行先期过滤，一旦发现短信中带有敏感的关键词，该短信无法送达接收方；

（2）旺铺业务平台对大批量的信息（超过 50 条）发送进行 24 小时不间断人工信息审核，对于有发送违规短信行为的用户坚决取消其接入号码；

3、细化敏感词类别：

（1）政治敏感及淫秽性违法违规类字眼。如：国家领导人姓名、民族、涉黄信息等等;

（2）通讯业敏感类字眼。如：运营商名称、中国银联等;

（3）商业广告营销宣传类的敏感字眼。如：大出血、楼价、热线、清仓、中奖等;

（4）特殊字眼。如：远志明、汪梦飞、点金、64 等。

（5）其他：根据国家、行业要求增补的相关字眼。

B.实践效果

2014 年旺铺助手产品有效拦截垃圾短信 30 万条，日均拦截 821 条，其中打折推销类占比高达 42%居首位，欺诈类居其次，占比为 32%，违法类占 26%。基本情况如下：

1）打折推销类垃圾短信：商场促销类以 21%，占据首席；房产中介类占 18%，位居其次，电商活动占 15%，居于第三。这前三类占比已超打折推销类短信的五成。此外，移民留学占 12%，餐饮优惠占 10%、银行业务推荐占 9%、旅游出行占 8%、证券信息占 7%。

2）欺诈类垃圾短信：38%为虚假“中奖”通知诱骗用户上钩；26%为假借亲友名义要求转账和回拨声讯电话；24%则为假借“公安”、“法院”名义传达通知，引导用户进入诈骗陷

阱；12%以提供所谓股票、债券内幕等实施诈骗。

3）违法类垃圾短信：42%提供“代开发票”业务；31%兜售手机窃听器、监控卡等，另有 27%散播违法信息等。

C.网民反应

通过一段时间的推进实践，调查反馈网民反馈满意度提升，网民评价：垃圾短信接到的少了，心情也不一样了。

D.推荐理由：

通过与互联网平台共享，具有实践创新性，相关举措也具有一定实效性。

点评：

电信公司与互联网企业相互合作，共享拦截关键词，是一种创新做法。期待电信运营商与互联网企业能够深入融合，发挥各自优势，共同合作双赢。

19、用户游戏道具被盗问题的解决

A.保护网民权益创新&优秀实践情况介绍

1.问题

公司旗下的 JJ 比赛游戏平台是广受玩家喜爱的游戏平台，迄今为止注册用户数量已经突破 2.2 亿。面对如此庞大的注册用户数据，数据库的安全成为了用户服务的重中之重。最近几年，接到用户数据被泄露的反馈越来越多，这一问题引起了公司的高度重视。经查，用户数据被泄露的原因多在于用户本身注册信息保管不善被人窃取及公司相关服务器遭受黑客攻击等。

2.解决方法

关于如何保护用户数据的安全这一问题，公司从内部人员管理和物理措施防范两方面入手维护注册用户数据的安全。在内部人员管理方面，公司建立了严密的层级管理制度，将用户数据划分为不同的机密等级，不同层级的管理人员有不同的权限，而有权限访问数据库的人员不论权限大小，人数控制在 5 人以内。此外，在员工的培训方面，公司也将保守机密信息作为培训的重点。用户数据事关用户的核心利益，用户的利益至上，本着诚信经营、认真负责的态度，公司从内部人员管理的层面最大限度地降低了注册用户数据的安全风险。另一方面，公司从技术防范的角度入手，将服务器与数据库的链接控制在最有限的范围内，数据库只针对有限的服务器开放，并且该服务器只能获取其对应权限内数据，这最大限度地保证

了数据库的安全。此外，公司也在官网和客户端的界面增加了风险提示，提醒用户保管好自己的账户信息，避免造成损失。

结合以上几个方面的措施，公司在保护注册用户数据安全的问题上采取了多种方法维护用户的利益，遵循了诚信经营的理念。

B.实践效果

在实践中，公司的上述措施取得了很好的实践效果，公司未发生注册用户数据大量泄露或被非法盗取的事件。数据库的安全风险相对较低。由于公司在用户数据安全方面措施到位，很好地保护了用户的数据安全，这使得用户在体验上有着更好的感触。公司越来越受用户的喜爱和推崇。

C.网民反应

公司注重对注册用户数据安全的保护。尽管保密措施是隐形的，用户不能直接触摸到，但是公司未发生注册用户数据大量泄露或被非法盗取的事件。这使得用户对公司的服务和信誉更加的肯定，JJ 比赛游戏平台的注册用户逐渐增加，用户认可度更高，相信这证明了公司的服务质量和安全措施的有效力度。一位网友更是在公司的论坛上做出了“JJ 比赛平台是值得玩家信赖的专业棋牌竞技平台”的评论。

D.推荐理由

竞技世界（北京）网络技术有限公司并非从事互联网安全领域的互联网公司，但身为互联网公司的一份子，公司充分认识到自己身上的责任和使命，那就是维护用户的利益。公司从管理和技术两方面进行创新很好地解决了用户游戏道具被盗的问题，极大地保障了用户的利益，用良好的信誉和态度筑起了安全的屏障。相信公司的创新、良好的信誉、认真负责的态度对于整个互联网行业的发展产生了积极的影响。

此案例叙述真实、详尽，体现了企业从实际着手解决问题的能力，也表现了企业诚信经营、用户利益至上的良好操守。

E.原创性声明（承诺书）

公司承诺表格所述的内容真实存在，并非抄袭和虚构。特此声明。

点评：

道具被偷其实是账号被偷，业内对游戏玩家的权益保护力度一直较弱。

此案例叙述真实、详尽，对于用户数据安全问题的解决办法具有很高的可操作性，值得

广大创业型互联网企业借鉴和推广。

20、公信手机卫士多重诈骗短信识别提示系统

A.保护网民权益创新&优秀实践情况介绍

公信手机卫士打造出多重诈骗短信识别提示系统，能够通过短信发送端口号码、短信内容、短信内 URL 及电话号码判断是否为诈骗短信，并对诈骗短信标示用户举报次数，用以提醒用户谨防诈骗风险。

第一道防线：诈骗短信发送端号码识别

公信手机卫士从事了近十年短信骚扰拦截与举报服务，积累了海量数据，在此基础上建立了诈骗短信发送端口号码黑名单库。

第二道防线：语义分析识别诈骗短信

公信手机卫士是最早通过语义分析实现骚扰拦截的安全服务商之一，针对大量诈骗短信数据分析，打造了一套全面、专业的知识库，包括词类词典、语法、语义规则知识库。依赖此知识库结合公信手机卫士智能分词方法、文本分析算法，使公信手机卫士引擎不仅能够对诈骗短信进行语义特征、结构特征、关键词特征进行分析，而且还具有一定的推理能力，能够对诈骗短信实现智能识别。

第三道防线：钓鱼网址 URL、诈骗电话号码识别

公信手机卫士通过多年积累，建立了短信钓鱼网址 URL、诈骗电话号码黑名单数据库。通过与其它相关安全企业数据合作，进一步丰富了黑名单涵盖范围。短信内容一旦出现黑名单 URL 或电话号码，即刻向用户做出风险提示。一旦新的诈骗短信钓鱼网址 URL、诈骗电话号码出现，通过用户举报或拦截引擎发现，在极短的时间内就会被纳入黑名单数据库，以最快的速度扼制诈骗危害的蔓延。

第四道防线：诈骗短信举报标记

针对已经被举报过的诈骗短信，用户一旦收到，系统会提示该短信被用户举报为诈骗短信，并同时标注该短信的用户举报次数。以数据的形式形象地向用户表明该条短信的危害性，以便用户通过举报数值大小判断该短信的风险程度。

B.实践效果

公信手机卫士打造了短信安全四道防线，通过我们测试，99%以上的诈骗短信能够被识别出来，以近期很猖獗的 10086 积分换现金的诈骗短信作为实例：

不法分子利用伪基站技术冒充移动公司，短信内容是一条积分兑换现金信息，短信中的网址链接弹出“中国移动-网上营业厅”的钓鱼网站，要求用户填写手机号码、银行卡号等个人信息，以盗取银行卡账户存款。

不法分子虽然通过伪基站技术，躲过了发送端号码识别第一道防线，但在内容上，通过语义分析，工程师已将这类结构判断为疑似诈。在第三道防线上，不法分子彻底露出马脚，提供的网址 URL 非但不在白名单库中，更是在黑名单库中出现。第四道防线，由于相同内容短信已被用户举报，举报次数更直接显示出这是一条被用户多次举报的诈骗短信。

点评：

专注于诈骗短信识别，深耕细作，值得肯定。

21、提升电信企业用户感知的垃圾短信“一体化闭环式体系建设”

A.保护网民权益创新&优秀实践情况介绍

近年来，垃圾短信严重干扰了消费者的正常工作和生活秩序，侵害了消费者的权益，增加了社会的不稳定因素，引起社会广泛关注和行业监管部门高度重视。社会对网民权益保护问题的关注度也在不断的攀升，如何在最短的时间内，降低垃圾短信给消费者带来的影响、提升用户感知，成为联通黑龙江省分公司的专项重点工作之一。面对严峻的形势，为有效遏制垃圾短信持续恶化的局面，提升垃圾短信治理的防控能力和水平，联通黑龙江省分公司从强化管理入手，改进治理方案，依托信息技术实行专业分工、条线管控与部门横向联动相结合的一体化管控体系。

B.实践效果

通过实施“一体化闭环式体系建设”，强化了垃圾短信综合治理各部门整体协同效应，促进了部门管理人员执行理念、管理方式的转变，增强了员工的创新意识和进取精神。垃圾短信投诉量大幅降低、垃圾短信拦截准确率显著提高、短信网间结算收入扭亏为盈、网间短信互通量比值趋于稳定、SP 类误封引发的投诉率趋于 0%、一次性解决成功率稳步提高。保护了用户的正当权益，为消费者营造绿色健康的短信服务消费环境，避免了由于垃圾短信的泛滥给用户带来的损失，取得了一定的社会效益。

C.网民反应

黑龙江省垃圾短信月均举报率为 11 件/千万户；2013 年至 2015 年 SP 类误封引发用户投诉率为 0%

D.推荐理由

所采用的“一体化闭环式体系建设”是通过多年来我省在垃圾短信治理上不断的摸索和创新而形成的比较成熟的管理体系建设，通过此体系的建设，我省在垃圾短信治理上取得了较为显著的成果，希望能和大家一起分享，一同将垃圾短信工作做到最好，为消费者营造绿色健康的短信服务消费环境，保护网民权益而努力。

E.原创性声明（承诺书）

垃圾短信“一体化闭环式体系建设”，为我省在治理垃圾短信多年以来不断的摸索和创新总结出来的经验而建设的体系。

22、基于短信综合特征识别技术的垃圾短信二次放通策略实践与应用

A.保护网民权益创新&优秀实践情况介绍

由于垃圾短信内容的多变和趋常，普通垃圾短信监控策略已不能适应垃圾短信的快速变化，导致大量正常短信被误拦截，给用户的使用带来不便的同时增加了短信的投诉量。我公司对现有垃圾短信平台进行优化，增加基于"短信自动审核技术"、"垃圾短信拦截策略滚动循环机制"等成熟的短信综合特征技术的智能分析模块，细化垃圾短信的监控识别，辅以人工仲裁，实现误拦截短信及时甄别和放通，有效的改善了用户短信业务体验，使误拦短信及时下发，直接提高短信收入。

B.实践效果

此项目功能自 2012 年 11 月上线以来，垃圾短信平台的监控效率得到显著提升，用户投诉率也有明显的下降。在确保用户业务正常使用下，更高效、准确完成垃圾短信的拦截工作，使误拦短信及时下发，直接提高了短信业务收入。此项目 2013 年为河北联通短信业务增收一百余万元，并将持续产生经济价值，有效解决了治理与收入保障之间的矛盾。

C.网民反应

此项目上线以后，卓有成效的降低了短信业务的投诉量：降低我省号码误处置及短信误拦截引发的用户投诉量约 50%以上，大大提升了用户的感知。

D.推荐理由

此项目以关键字自动反馈学习算法为依托、以用户行为特征数据为辅助，创新建立了垃圾短信智能分析模块及二次放通机制，有效提高了垃圾短信拦截准确度，降低了用户投诉率。

上线后，在确保用户业务正常使用下，更高效、准确完成垃圾短信的拦截工作，使误拦短信及时下发，直接提高了短信业务收入。此项功能每年为河北联通短信业务增收一百余万元，有效解决了治理与收入保障之间的矛盾，效果显著。

目前，河北联通垃圾短信治理工作在全国处于领先水平，垃圾短信投诉率一直相对较低。此项目中垃圾短信智能分析模块在国内处于领先水平，二次放通功能为国内首创（专利申请中），为垃圾短信治理工作开创了先河，具有同行业的借鉴意义。

E.原创性声明（承诺书）

承诺本应用系我公司原创。

本应用实现的功能在国内属于首次使用，基于"历史短信样本综合特征"的快速自动匹配方案为河北首创，此项技术是垃圾短信内容自动审核的基础。二次放通技术亦为国内首创，此次项技术有效的实现了短信业务营收的提高，当前此项技术正在专利申请的流程中。

23、山东联通宽带专家微信公众号用户信息安全保护案例

A.保护网民权益创新&优秀实践情况介绍

山东联通所属“山东联通宽带专家”微信公众号是按照客服部门改进客户服务、方便快捷、提升客户感知的需求而进行建设的。使用过程中，我公司发现在用户业务账号及身份证号码泄露的情况下，有存在被他人更改业务密码的可能性。

为了防止用户信息泄露，保护我公司宽带网民的权益，针对系统安全进行了以下改进：

（1）在查询接口中只查询并传输到前台所需必备信息，包括：宽带账号、带宽、产品类型、当前状态、开通日期等信息，即将所有和用户相关的信息去掉，只查询并展现产品的部分信息。

（2）对“账号信息查询”功能做必要限制，即只有权限绑定用户才可进行账号信息查询。

（3）在修改密码页面以添加验证码环节的方式进行动态验证。

（4）对于使用手机号码进行绑定的用户，在微信平台变更用户信息时，对该绑定手机号码（需为网内用户）发送信息变更通知短信。

通过以上改进方案的实施，我公司在方便用户使用的同时，有效地提升了对用户信息的保护，加强了宽带上网用户隐私和个人信息的保障。

B.实践效果

经过系统的改进和使用检验，在方便用户对宽带日常使用的情况下，提升了用户信息保护能力，加强了宽带上网用户的权益保障。

C.网民反应

网民反应效果良好。

D.推荐理由

山东联通宽带专家微信公众号用户信息安全保护案例，确实能够体现山东联通公司以客户为主导，为网民提供优质安全的服务，有效保障网民权益的努力是卓有成效的，因此进行推荐。

点评：

这是一项便民措施，便民措施也是保护网民权益的重要方面。

24、百度安全中心 URL 反钓鱼组

A.保护网民权益创新&优秀实践情况介绍

百度安全中心 URL 反钓鱼组致力于为广大网民提供，可靠、安全的网址防护功能。通过内置在百度杀毒当中的网页保护功能，确保用户点击到相关钓鱼网站时，百度杀毒会自动进行相关风险提示，告之用户网站风险。把用户被钓鱼、欺诈的风险降到最低。

B.实践效果

全面支持网民所用的主流浏览器，自动拦截虚假、欺诈、挂马网址，实现上网零风险！防护范围含盖：游戏网站、金融网站、购物交易网站、政府网站、旅游交易网站、博彩网站

等网民经常进行购物的网络平台。

日前，百度杀毒截获了一个伪造微信安全登陆的钓鱼网站。正是孙女士险些上当的亲身经历。

孙女士一直对各类测试兴趣颇浓，前不久她进入一个性格测试前授权了一家第三方平台。可是没想到，不久，她的邮箱就收到了一条“您的微信帐号存在安全风险”邮件，邮件详细说明了其风险原因，以及会对用户帐号进行部分功能限制，并且附上微信安全中心的链接，以供用户解除限制。

孙女士使用微信多年，但也是第一次遇见这种情况，她未多考虑便在网页中输入了自己的 QQ 帐号及密码，经过很简单的几步，便完成了解限过程。但却没有任何反应，几分钟之后，突然她微信显示下线，在别处登陆。正在她不解之时，接到了朋友的电话，朋友着急的问她：“你还好吗?没事吧?现在在哪了?”一番枪林弹雨式的问候让孙女士一头雾水，后来经

过朋友说明，原来是不法分子盗取了孙女士的微信帐号，利用其对朋友进行欺诈，向朋友借钱，好在其朋友电话及时，避免了这一起诈骗悲剧的发生。

很明显，孙女士从参与测试的第三方授权到登陆“解锁”网站，统统都是由不法分子预先安排好的。其实像这样的例子有很多，诈骗者凭借虚假的第三方平台授权获得用户的微信帐号，然后发送邮件至用户 QQ 邮箱，进行进一步引导，利用大家的粗心大意实施帐号信息骗取，百度安全提醒您，在输入个人帐号信息及密码之前务必反复核查网站的正确性。

对于如何正确防范钓鱼网站，百度安全专家表示，首先是安装专业电脑安全软件，专业杀毒软件的网页防护功能在遇到这些危险的网站时会自动拦截，保护你的上网安全。此外，谨慎打开通过聊天工具和不明邮箱传送的链接网站。或者百度一下正确的安全的网址，登陆官网确保信息安全。

C.网民反应

在互联网高速发展的今天，网络欺诈、钓鱼网站已成为危险网民权益的头等大事，为了更好的服务于网民，打击犯罪分子。百度安全中心 URL 反钓鱼实验室设立了可疑网站举报渠道。这一渠道的建立可以让网民自己亲身参与到网络安全防护的工作中，在避免自己被诈骗的同时，有效的为更多网民进行安全防护。

http://anquan.baidu.com/shadu/shadu_form.html#

D.推荐理由

随着网络购物进入到普通百姓的生活中，人们开始逐渐习惯在网上进行物品的查询及交易。但网络中鱼龙混杂，常有低价或不正规的宣传方式诱导普通用户进行点击，不法分子也正是利用大家图便宜、图方便的心理因素、采取低价陷阱、购物不成功需要二次支付等方式进行钱财诈骗。当网民被骗后，钱财很难被追回。在危险的环境下，虚假支付钓鱼陷阱大量涌现，一些网民频频中招。百度杀毒的网址防护功能能够很好的解决用户被何种类仿冒钓鱼网站进行欺诈的危险，从而保护网民的根本利益，净化网络空间。

点评：

安全网址的防护是保障网民权益的基本防线。

骗子使用各种方式及话术，迷惑受害者。致使受害者落入骗子事先设置好的陷阱。遇到此类情况，用户应该首先开启安全软件确保网站安全。然后再联系有认证的官方。进行最终确认。

25、百度手机卫士助力广东某市公安局速破伪基站诈骗案

A.保护网民权益创新&优秀实践情况介绍

“伪基站”即假基站，是一种高科技仪器，它通过短信群发器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，并将用户的手机信号强制连接到伪基站上，使用户无法连接到公用电信网络。伪基站通过伪装成运营商的基站，任意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，对用户进行骚扰，影响手机用户的正常手机使用。伪基站诈骗短信不仅严重影响了民众的日常生活，同时，也为人民群众带来了财产威胁和损失，而伪基站诈骗短信数量和犯罪团伙数量正在不断攀升，据《2014 中国移动安全报告》显示，2014 年伪基站短信数量为 11.9 亿，受其诈骗的案例数不胜数。伪基站已经引起了社会的广泛关注，以及公安机关等国家相关机构的高度重视。百度移动安全通过丰富的大数据资源以及伪基站定位监控技术不仅为用户提供骚扰短信识别拦截并提供了伪基站信息、数据获取和定位等技术的保障，为公安机关打击伪基站犯罪提供便利。

B.实践效果

6 月 25 日，犯罪嫌疑人谭某在某居住小区附近发送伪基站短信，该短信刚一发出，就被分局民警实时截获，并在百度移动安全部安全技术的帮助下准确的定位到犯罪嫌疑人具体位置，在分局民警的快速行动下，当场对谭姓男子进行了抓捕。警方在现场还一并起获一台伪基站主机、一个电池和三台手机等作案设备。据该犯罪嫌疑人交代，整个 6 月份利用伪基站设备在全国各地共发出了 12 万条诈骗短信。

C.网民反应

伪基站发出的诈骗短信基本都是伪装成“10086”、“95588”等运营商发出的短信，难以识别，很容易上当受骗，不少网友因此损失大量金钱，而且难以追讨。百度移动安全与警方合力打击伪基站诈骗，为广大网友解决了这个难题，让网友们可以更加安心的使用手机。

D.推荐理由

手机短信不管是青年人使用的智能机还是老年人使用的传统手机都是一个重要且常用的功能，伪基站诈骗短信影响范围大且难以防范。伪基站站点具有难识别、移动性高、难查处的特点，百度移动安全一方面通过用户手机上的百度手机卫士来帮用户识别拦截伪基站发来的诈骗短信，另一方面联合警方打击通过伪基站诈骗的犯罪团伙，依靠庞大的大数据资源以及过硬的技术能力为大家提供一个安全的网络环境。

26、阿里钱盾：信息泄露引起的欺诈防护

A.保护网民权益创新&优秀实践情况介绍

背景：随着网络的普及，信息泄露进而引起的网络欺诈增长也非常迅速，据此前中国证券网报道，2014 年以来，每年发生的网络诈骗案至少有 23 万起，报案的人均损失超 2 千元。为了保护这部分用户的资金和信息安全，阿里钱盾推出了欺诈防护功能。

创新方案：通过阿里全平台的大数据分析为每一个用户进行精细画像，为每一笔订单和每一步操作进行实时的安全监控，联合 12321、百度、腾讯等进行风险数据实时共享，结合钱盾自研的全方位安全分析模型，阿里钱盾能够及时的对风险用户、风险订单、风险操作，风险电话和短信进行提醒或拦截，帮助用户提升安全意识，防止其被骗。

B.实践效果

从 4 月份产品上线之后，钱盾为 1.8 万信息泄露风险用户推送了 4.1 万条风险提醒，钱盾的风险提醒使得用户被诈骗成功的概率下降了约 38%。

C.网民反应

阿里钱盾的提醒，引起了用户的警觉，有助于其安全意识提升，帮助其防范被骗。

D.推荐理由

1.与互联网安全的各大厂商和机构合作，结合阿里自有的大数据和钱盾自研的风险分析模型，为用户提供全面的安全防护。

2.根据数据监控，这一功能确实能够大幅度提升用户安全意识，防范其被骗。

E.原创性声明（承诺书）

承诺阿里钱盾-欺诈防范功能为阿里钱盾原创技术。

点评：

信息泄露的危害有直接危害（比如电话短信骚扰）和次生危害（如掌握个人信息之后的精准诈骗），而次生危害更加严重。通过多种举措避免因信息泄露造成的欺诈是相当长一段时间的难点和重点。

27、豌豆荚“安全认证”

A.保护网民权益创新&优秀实践情况介绍

早在 2012 年豌豆荚便推出了“安全认证”机制，对 Android 应用的安全性、是否包含广告插件、是否为正版、以及对敏感权限的调用等方面进行全方位检测，为用户提供最安全放心的应用下载体验。

豌豆荚“安全认证”包括：

无病毒标签：接入多家安全厂商引擎，针对手机病毒、扣费代码等风险进行全面扫描。

无广告标签：检测广告平台模块，针对通知栏广告和内嵌广告有明显提醒，帮助用户避免应用内广告造成的电量和流量损失、远离打扰。

信任权限标签：综合开发者认证情况和应用的权限调用情况，对于没有经过认证信任的应用调用敏感权限的情况进行警示，预防用户的通讯录等隐私信息的泄露。

Google 验证标签：检验应用签名与 Google Play 中是否一致，用做判断应用是否是官方版的参考、确保应用没有被第三方篡改，保护用户和开发者权益。

B.实践效果

豌豆荚“安全认证”从更全面的角度显示了一款应用的基础质量，豌豆荚的应用搜索和推荐算法也依据这些标签严格进行排序。安全性上被判为危险的应用会直接下架；判为可疑的、或者有通知栏广告的应用也绝不会出现在首页的各个推荐榜单；应用搜索的排名也会依据“安全认证”进行优化。

C.网民反应

用户在豌豆荚可以直观看到应用是否符合「安全认证」，方便用户随时做出放心的下载

决策。

凭借出色的用户体验，豌豆荚已从最初的个人信息管理工具成长为中国最具人气、活跃度最高的“应用搜索及发现平台”。目前，豌豆荚拥有 5 亿庞大安装量，可以让用户搜索到超过 230 万不重复的应用和游戏。

D.推荐理由

用户和开发者在享受 Android 的开放性所带来的繁荣和便利的同时，也不断遭遇各种问题的困扰：应用质量良莠难辨、仿冒和山寨应用层出不穷、第三方广告和敏感权限滥用难以规范、付费推广应用混杂在自然排名之中。

豌豆荚“安全认证”从多重角度评估应用质量，为用户提供全面的决策信息，还用户一个安全、洁净的手机使用环境。

点评：

在治理不良和恶意移动应用方面，应用商店是关键的一环。采取措施得力，保障到位，是赢得用户的关键。

28、豌豆荚“人工审核”体系

A.保护网民权益创新&优秀实践情况介绍

由于使用 Android 系统的手机来自不同厂商，许多应用会出现适配异常，以及不良开发者利用 Rom 漏洞进行破坏等问题。

豌豆荚“人工审核”通过技术手段实现了应用在不同 Rom 上的真机实测，对于应用是否存在异常状态，以及有无包含恶意内容进行筛查。

通过人工观察和测试，豌豆荚判断应用所属的类型并将结果进行标注，类型包括“正常”、“不推荐”、“需下线”，并依照类型判断结果进行上架或下线等处理。

如对于应用本身不稳定，或包含淫秽色情内容等无法通过技术手段检查的情况，均会被人工测试发现，并会被豌豆荚拒绝收录。

经过豌豆荚“安全认证”和“人工审核”的应用将获得可信认证，“可信应用”在豌豆荚 Android 端、Windows 客户端、网页端都有着明显的标识，有机会得到豌豆荚内部各个栏目得到更多的推荐机会，对于潜心打磨优质应用的开发者也是一种鼓励和支持。

B.实践效果

在豌豆荚上架的应用得到了更加系统的梳理，杜绝了恶意应用的存在。

C.网民反应

网民在使用豌豆荚时能够找到安全、稳定的应用，避免了下载到存在病毒威胁、恶意广告和盗版山寨等问题应用所造成的影响，用户因此更加信赖豌豆荚。

D.推荐理由

豌豆荚“人工审核”是国内首家通过技术配合人工实测来保证应用的安全监测体系，由于实施此项监测需要有对应用技术和人力成本双重投入，目前行业内尚无其他企业推出类似机制。

点评：

人工审核费时费力，认认真真做好的商店不多。

29、百度卫士、百度杀毒

A.保护网民权益创新&优秀实践情况介绍

随着智能手机的普及，手机木马病毒日益猖獗，不法分子把它们包装成不同的花样来诱导用户上当受骗。面对花样翻新的病毒和恶意软件，百度手机卫士快速反应，全面查杀，有效保护用户的安全。

近日，百度安全实验室便截获一款“伪成绩单”恶意病毒，该病毒被伪装成“成绩单”通过短信进行扩散，并诱骗广大家长下载安装。目前，百度手机卫士已率先截获，并全面查杀该病毒。从百度安全实验室截获的病毒信息来看，“伪成绩单”病毒扩散很快，许多家长已经收到此类短信，其中一些家长因点击短信内连接，其个人信息已遭到窃取。

B.实践效果

在“伪成绩单”病毒传播过程中家长会收到如下短信：

百度安全专家表示，当用户收到带有病毒的短信并点击链接时，病毒程序就会立即被下

载。

病毒程序运行后首先会让用户激活设备管理器，不断提示用户使用“成绩单 A”作为默认短信应用（Android4.4.2 以后，只有被设置为默认短信应用的程序才能读写操作），直到用户确定。最后，用户会发现提示安装错误，点击“确定”之后，程序消失了。实际上，该程序却在后台偷偷运行，将用户的联系人及短信等隐私发送到不法分子的邮箱。

目前，百度手机卫士已对“伪成绩单”病毒进行了全面查杀。6.0 版本的百度手机卫士升级了病毒查杀功能和技术，能够及时的发现手机后台运行的“伪成绩单”病毒，并可以直接破解加密程序和“保护壳”，实现彻底查杀。另外，百度手机卫士为用户提供“快速扫描”

和“全面扫描”两种扫描方式，帮助用户随时随地的对手机安装包和应用程序进行扫描，及时发现病毒。

监测数据显示，“伪成绩单”病毒近期迅速扩散，百度安全专家提醒广大用户，遇到诸如此类附有链接的短信，切记不要点击。可以下载百度手机卫士等手机安全软件，定时给手机彻底扫描杀毒，防患于未然。

C.网民反应

百度手机卫士以较快的反应速度对于恶意应用进行分析和查杀，尽最大可能阻止恶意应用的传播和破坏。有效保护了用户的隐私、财产安全等权益。

D.推荐理由

据百度安全实验室安全专家介绍，该病毒之所以能够肆意猖獗，一方面主要抓住家长关心孩子学习的心理；另一方面，这款“伪成绩单”病毒程序较复杂，病毒作者作了加壳处理，以阻止安全研究人员破解分析，增加了查杀难度，变得极为顽固。在百度安全实验室发现该病毒后，百度安全专家和技术人员加大力度对其进行破解，最终通过脱壳得到了真正的病毒代码，对其进行了查杀，并帮助受害者了解该病毒“作威作福”的过程。

30、百度手机卫士有效应对顽固威胁

A.保护网民权益创新&优秀实践情况介绍

一直以来，百度手机卫士不断强化技术水平。在面对一些其它安全软件难以处理的恶意应用、病毒时，百度手机卫士的技术优势使得其可以有效地进行处理。在以下事例中，用户手机中安装的安全软件虽然检测出漏洞却无法有效处置，最终还是通过百度手机卫士使手机恢复正常。

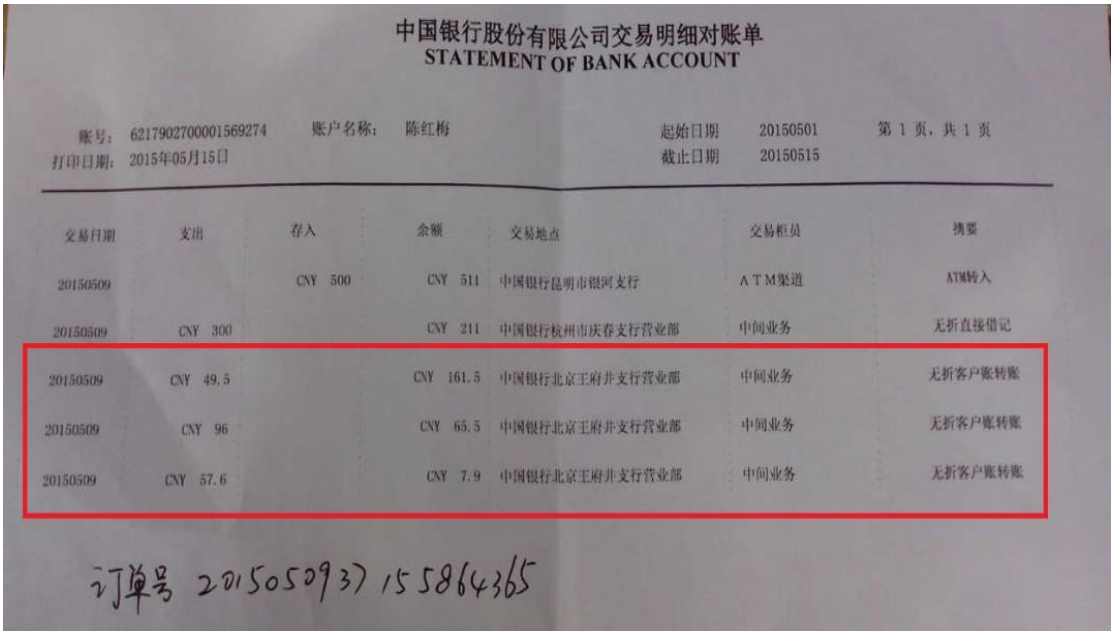
B.实践效果

5 月 9 日，陈女士老公给其中国银行的账户转了 500 元，随后陈女士通过支付宝给平安银行的信用卡进行 300 元的还款。之后收到一条来自“10086”的短信，内容如下：

“尊敬的用户:您的话费积分足已兑换 288 元现金，请登录:www.cy-l0086.com 根据提示激活领取，过期失效。【中国移动】”

陈女士点击链接后页面显示下载的进程，此时联想手机自带的杀毒系统“乐安全”弹出一条消息，内容为“高危漏洞、恶性”等描述，建议卸载这个软件。陈女士选择“取消下载”按钮，但无法卸载，导致手机也无法收发短信。

5 月 14 日，陈女士去中国银行取剩下的 200 元，发现余额不足，才知道自己银行卡中的钱不翼而飞了，查询的银行记录显示有支付宝订单号为：2015050937155864365，但是陈女士登录自己的支付宝账户未找到这一项。同事帮陈女士下载了百度手机卫士，成功查到病毒项，且将该软件卸载，随后手机收发短信正常。



中国银行股份有限公司交易明细对账单
STATEMENT OF BANK ACCOUNT

账号：621790270000156927 4　账户名称：陈红梅　起始日期 20150501　第 1 页，共 1 页
打印日期：2015年05月15日　截止日期 20150515

交易日期	支出	存入	余额	交易地点	交易柜员	摘要
20150509		CNY 500	CNY 511	中国银行昆明市银河支行	ATM渠道	ATM转入
20150509	CNY 300		CNY 211	中国银行杭州市庆春支行营业部	中间业务	无折直接借记
20150509	CNY 49.5		CNY 161.5	中国银行北京王府井支行营业部	中间业务	无折客户账转账
20150509	CNY 96		CNY 65.5	中国银行北京王府井支行营业部	中间业务	无折客户账转账
20150509	CNY 57.6		CNY 7.9	中国银行北京王府井支行营业部	中间业务	无折客户账转账

订单号 2015050937155864365

C.网民反应

百度手机卫士的技术水平可以有效应对各类恶意应用、病毒等威胁，有效地保护了用户的隐私和财产安全，是简单、可依赖的手机安全软件。

D.推荐理由

百度手机卫士通过不断强化技术水平，在面对一些其它安全软件难以处理的恶意应用、病毒时，百度手机卫士却可以有效进行处理。这充分说明了百度手机卫士在行业内的领先地位以及在安全技术领域的不懈努力。

31、云南联通“移动互联网应用个人信息及权益保护工作”

A.保护网民权益创新&优秀实践情况介绍

2015 年云南联通联合北京中创信测科技股份有限公司在昆明金牛营业厅开展恶意软件检测试点工作。对到厅用户介绍软件检测，对自愿参与检测的用户，免费为其终端进行检测。

B.实践效果

恶意软件检测试点工作，共有 32 部手机参与检测，检测应用 574 款，发现 4 部手机感

染 3 款恶意应用，恶意应用比例：6.97‰，用户感染比例：12.5%。对发现恶意应用的手机在经用户同意后，为用户删除相关应用保障了用户权益。

C.推荐理由：

随着移动互联网的普及，不少恶意软件也侵入用户手机，盗取用户信息，侵犯用户权益。为推进云南移动互联网应用个人信息及权益保护工作的开展、加强移动互联网应用安全管理、维护人民群众合法权益，创造安全的移动互联网信息消费环境。云南联通多方位，采取多种形式维护用户的权益。2015 年联合北京中创信测科技股份有限公司在营业厅对用户终端进行检测，发现并为用户移除各类恶意软件。

点评：

在营业厅为网民检测手机安全问题，做法新颖，值得推广。

32、北京联通垃圾短信综合治理

A.保护网民权益创新&优秀实践情况介绍

在工信部、联通集团公司及相关部门的监督和指导下，北京联通进一步明确垃圾短信快速响应及处置流程，形成长效治理机制。

在日常治理工作中，北京联通的主要举措如下：

（一）加强制度管理与考核

2013 年底，联通集团再次提出《垃圾短信综合治理第二阶段方案》，重点针对行业端口垃圾短信等问题，加大考核力度。在此基础上，北京联通更新制定 2014 年公司内部垃圾短信考核标准，加强考核手段，对各相关销售线及维护部门纳入业绩考核范畴，严格执行罚扣制度，做到收入扣罚和 KPI 扣罚双管齐下，进一步规范销售源头。

（二）加强端口类短信管理

针对行业用户，加大违约惩罚力度。以每个自然月为单位，对投诉量超过两个的行业端口进行关停处置。

为使行业端口垃圾短信得到有效控制，提升用户感知，降低公众用户投诉，北京公司 2014 年启动用户自助屏蔽行业短信服务系统功能，用户可自行通过发送“0000”和“1111”进行短信的退订和恢复，既方便了用户又降低了用户投诉。

（三）落实用户实名制

从 2013 年 9 月 1 日开始，按照工信部要求，联通公司全面实行入网实名登记，这一举

措能有效减少以往非实名制用户发送垃圾短信的现象，降低垃圾短信的发送量。同时对垃圾短信及违规行为用户可进行溯源，有效遏制违法违规行为。同时也为执法部门清查工作提供有效依据。

（四）健全技术拦截手段

北京联通完善垃圾短信智能分析拦截平台，针对用户投诉、举报以及垃圾短信传播的新趋势，通过智能化算法实时动态优化拦截策略，配合关键字、频次、离散度等指标，实现了对垃圾短信的收端、发端双向拦截及黑名单自动拦截。

（五）畅通举报途径

北京联通向用户提供了热线、短信、微博、手机营业厅等多种垃圾短信举报渠道，并承接了来自 12321 网络不良与垃圾信息举报受理中心的垃圾短信受理任务。进一步梳理投诉处理流程，加快垃圾短信处置响应速度。

B.实践效果

近年来，垃圾短信严重干扰了人们的日常生活，甚至有些违法有害信息严重危害社会安全。多年来相关政府部门、电信运营商作了很大的努力加以治理垃圾短信。中国联通北京市分公司（以下简称北京联通）采取了多种治理举措，也取得了一定治理成效。

C.网民反应

近年来，北京联通倾注了大量的人力、物力用于治理垃圾短信，2014 年北京联通公司进一步加大垃圾短信治理力度，全年短信发送总量约为 56 亿，而拦截到的垃圾短信为 1 亿，拦截占比在 1.7%左右。而垃圾短信用户投诉量也较去年大幅度减少，垃圾短信举报率从 638 件/千万户下降到 64 件/千万户，社会反响也呈降低趋势。

D.推荐理由：

作为电信运营商，北京联通对垃圾短信治理做了很大努力，通过管理和技术等多种手段遏制垃圾短信产生，然而对于垃圾短信整体治理工作来说，需要公安、工商等多个执法部门协调行动，提升整体治理能效。

为保证广大用户的利益，需要营造防范与打击垃圾短信、有害信息的良好氛围；商务用户应遵守法律法规，健康而有序地开展业务；公众用户应理解并支持实名制，抵制有害短信的传播，及时举报垃圾短信，与运营商一道共同打造诚信、健康的通信环境。

33、迅雷打击淘宝市场非法会员：涉案人员被判刑

A.保护网民权益创新&优秀实践情况介绍

2013 年 8 月，迅雷工作人员发现网络上有众多非法销售未经迅雷授权商品的店铺，而其所销售的迅雷会员多是不法分子通过一些非法刷迅雷会员的软件或者被弃用但未被注销的手机卡注册所得的，这些不法分子在盗刷迅雷会员后，就会通过店铺商以各种非法手段将其出售给用户，而用户在购买之后才会意识到上当受骗。迅雷与各地公安部门合作，在河南淮阳、辽宁大连、江苏苏州、河北石家庄、湖南长沙、广东深圳、福建福州、安徽、江西宜春、浙江杭州、湖北襄樊等地做了深入调查，共抓获多地涉案人员多名并依法进行了处置。

B.实践效果

迅雷是一家坚持以用户体验为导向的公司，任何侵害用户体验的违法行为都将遭到严厉打击，而此次与公安部门的合作只是一个开始，未来双方还将加大合作力度，此次将这一违法行为斩草除根，还迅雷用户一个纯净的体验环境。

C.网民反应

通过此次行动，网民纷纷表示迅雷在保护用户权益方面做得非常周到全面，给用户足够的安全感，并表示今后消费一定通过正规的途径以免受骗上当。

34、迅雷与美电影协会签约：打击非法下载

A.保护网民权益创新&优秀实践情况介绍

迅雷在 2014 年与美国电影协会(Motion Picture Association of America, MPAA)签署协议，共同促进互联网上影视节目的合法获取，打击美剧与电影的非法下载。

美国电影协会及其成员公司和迅雷已达成全面协议，用以保护互联网上的影视内容，并教育用户以最佳途径获取正版的影视节目。依据该内容保护协议，迅雷采取一系列综合措施，防止非法下载和获取。这其中，迅雷将建立内容识别技术系统，以确保通过迅雷下载的影视作品版权是由美国电影协会成员公司合法授权的。

迅雷和美国电影协会将相互协作，以确保这些内容保护措施能持续地发挥作用。双方将合作确保这些内容保护措施的落实，并开展宣传教育，帮助用户了解未经许可上传和下载创意内容所造成的损害。

迅雷推出一整套监管措施，阻止用户下载到各大影视公司未经授权的影视资源。这些措施中包括建立一套内容识别系统，确保迅雷各项服务只能接触到已经获得授权的那部分影视

资源。其实这并非版权监测系统的首次曝光，上月网易科技曾经报道，迅雷与首都版权产业联盟近日宣布将在互联网版权保护领域展开技术合作，共同推动中国网络视听内容正版化。

B.实践效果

协议签署初期没有明显效果，甚至失去了部分用户，但不到一个月的时间用户数恢复并且不断上涨

C.网民反应

网民起初表示不解迅雷为何要自断生路，因为这是下载平台最核心的营收来源，但为了保护正版以及保障网民观看正版的权益，迅雷冒着丢失部分用户及付费会员的风险依然坚持履行协议，结果反而出乎意料的博得了用户的好评，网民普遍反感盗版及非法内容对自身的侵害，电脑经常被非法内容染上病毒，迅雷的此行为另网民表示非常钦佩！

【参考资料：新政策解读】通信短信息服务管理规定：发垃圾短信最高罚 3 万

5 月 28 日，工信部对外公布了已获通过的《通信短信息服务管理规定》，其中明确要求短信息服务提供者、短信息内容提供者未经用户同意或请求，不得向其发送商业性短信息。该规定将自 2015 年 6 月 30 日起正式施行。

针对商业性短信息，《规定》特别提出，未经用户同意或者请求，不得向其发送商业性短信息。用户同意后又明确表示拒绝接收商业性短信息的，应当停止向其发送。短信息服务提供者、短信息内容提供者向用户发送商业性短信息，应当提供便捷和有效的拒绝接收方式并随短信息告知用户，不得以任何形式对用户拒绝接收短信息设置障碍。

《规定》还要求，经营短信息服务的，应当依法取得电信业务经营许可。短信息服务需向用户收费的，事先要明确告知用户服务内容、资费标准、收费方式和退订方式等。短信息服务提供者发送短信息，应当将发送端电话号码或代码一并发送，不得发送含有虚假、冒用的发送端电话号码或者代码的短信息。基础电信业务经营者、短信息服务（内容）提供者如违反上述规定，将由电信管理机构处以 1 万-3 万元罚款。

工信部要求短信息服务提供者建立投诉处理机制，公布有效、便捷的联系方式，接受与短信息服务有关的投诉，并委托 12321 网络不良与垃圾信息举报受理中心受理短信息服务举报。

该规定中特别说明，短信息服务是指利用电信网向移动电话、固定电话等通信终端用户，

提供有限长度的文字、数据、声音、图像等信息的电信业务。按照这一规定，短信息指的并不仅仅是手机短信，也包括微信、微博等新型社交媒体方式，都可以被纳入此管理范围中。

有业内人士表示，这是我国第一次明确为商业短信息制定有针对性的管理办法，治理垃圾短信也有了相应的政策依据。不过该政策真正实施起来还是存在难题，如对历史存量短信如何管理、电信管理部门怎么克服执法难的问题等。

【参考资料：新法规解读】新广告法：互联网广告不能“一键关闭”将受罚

【互联网广告不能“一键关闭”将受罚】2015 年 4 月 24 日下午，广告法修订草案三审稿在全国人大常委会十四次会议表决通过。表决稿新增规定，利用互联网发布广告，未显著标明关闭标志，确保一键关闭的，将处五千元以上三万元以下的罚款。

【未经同意不得发送电子邮件广告】新广告法明确，任何单位或者个人未经当事人同意或者请求，不得向其住宅、交通工具等发送广告，也不得以电子信息方式向其发送广告。在互联网页面以弹出等形式发布的广告，应显著标明关闭标志，确保一键关闭。违者将被处五千元以上三万元以下罚款。

相关法律条款:

第四十三条 任何单位或者个人未经当事人同意或者请求，不得向其住宅、交通工具等发送广告，也不得以电子信息方式向其发送广告。

以电子信息方式发送广告的，应当明示发送者的真实身份和联系方式，并向接收者提供拒绝继续接收的方式。

第四十四条 利用互联网从事广告活动，适用本法的各项规定。

利用互联网发布、发送广告，不得影响用户正常使用网络。在互联网页面以弹出等形式发布的广告，应当显著标明关闭标志，确保一键关闭。

第六十三条 违反本法第四十三条规定发送广告的，由有关部门责令停止违法行为，对广告主处五千元以上三万元以下的罚款。

违反本法第四十四条第二款规定，利用互联网发布广告，未显著标明关闭标志，确保一键关闭的，由工商行政管理部门责令改正，对广告主处五千元以上三万元以下的罚款。

【参考资料】网民权益保护需要动真格

网民权益保护随信息化发展而递进

随着互联网的发展，人们在上网行为中各类权益遭受侵害的情况在不断增加，网民权益保护概念逐渐进入公众视野。网民权益保护与维护网络安全、净化互联网环境、保护消费者权益等领域皆有交叉，但与这些概念又有着明显的不同：

网络和信息安全是事关国家安全和发展、事关广大人民群众工作生活的重大战略问题，没有网络安全保障，网民权益保护将无从谈起。值得注意的是，在强调网络安全对国家安全的重大战略意义的同时，不应忽略网络安全与广大人民群众工作生活的紧密关系；

净化网络环境是保障网民权益的一个重要方面，但不是全部。净化网络环境主要是指保护网民避免遭受各类不良与垃圾信息侵扰，对于网民个人信息泄露、网民的知情权与选择权被侵害等情形则覆盖不到；

消费者权益保护从消费行为角度出发，而网民权益保护则从更大范围地“使用互联网”角度出发，网民在网上进行消费行为，作为一名消费者，网民权益与消费者权益是重合，但是网上的行为范围远远不止消费，还有通信、社交、娱乐、获取信息等等，消费者权益保护的范畴要远小于网民权益保护。

大体来说，网民权益，是从个人作为信息主体的角度出发，天然具有的相关权益。在信息社会逐步发达的条件下，主要和“信息”相关，在一定程度上，也可以称之为公民信息权益。中国互联网协会发布的首份《中国网民权益保护调查报告》中，将网民权益解释为：网民因使用互联网产品、服务及相关设备而应该享有的权益。相信随着互联网不断发展，网民权益保护意识的不断觉醒，网民权益保护概念也将不断演变、完善。

网民权益受损现状

中国互联网协会 12321 网络不良与垃圾信息举报受理中心作为公众举报机构，自 2008 年成立以来累计接受各类网民举报超过 2500 万件次，多数都于网民权益受损有关。通过对网民举报信息的梳理分类，网民权益遭受侵害较为严重的情形大致包括如下几个方面：

（一）安宁权：即，网民拥有不被骚扰的权利。骚扰电话、垃圾电子邮件、垃圾短信等，是骚扰的主要来源。据中国互联网协会的调查统计，电子邮件用户平均每周接收垃圾邮件 12.8 封，占全部电子邮件的 1/3；我国手机用户平均每周接收垃圾短信 12.0 条；而骚扰电话的总量更是达到百亿量级。这些“不请自来”而又不能拒绝的信息侵犯了网民的“安宁权”，对网民形成了严重的骚扰，侵害了网民的合法权益。伴随着网民被骚扰的加剧，业内也出现

了一些保护网民避免被骚扰的积极实践。现在不少互联网企业，都在防骚扰方面下了大力气，根据来电的时间不同（工作日或非工作日、白天或者晚上）、来电号码与机主本人的关系（VIP号码或者联系人号码，或陌生号码）以及来电行为（如响一声识别、重复呼叫等），有不同的提醒级别，比如有无响铃、震动等。行业内还发起了黑名单、白名单（商户号码备案）等策略。但是对于固定电话、非智能手机，安宁权的保障仍须加强。

（二）接收真实信息的权利。互联网的高技术性为骗子利用虚假信息欺诈网民带来了一定的便利。伪基站信息（修改短信息号码），改号软件拨打的电话、假冒他人或者相关机构，比如公安、法院、银行社保局等进行诈骗、各类网络钓鱼、中奖诈骗、盗取社交网站账号冒充好友诈骗等各类网络诈骗横行，皆侵害了网民获取真实信息的权利，给网民带来了骚扰的同时，破坏了网络诚信，“网上消息不可信”几乎成了人们的共识，不少网民还遭受了经济损失，危害巨大。

（三）知情权与选择权：网民应该对自己上网设备的软件有选择权，未经网民的允许，不得预装、静默安装不必要的软件；软件的安装与卸载权利，应该掌握在设备持有人手中。随着移动互联网的发展，尤其是 android 系统的普及，侵犯网民知情权和选择权的情形逐渐高发。移动应用静默安装、无法卸载、获取不必要的权限等问题突出，不少网民感觉，自己的手机，自己做不了主。在不知情的情况下，偷传通信录、通信记录、个人隐私信息等问题严重。

（四）个人信息保护：网民的个人信息受到保护，不得违规采集、使用、贩卖、传播网民的个人信息，网民发现自己个人信息泄露时，向网络服务提供者主张，应该予以删除。目前个人信息泄露情况非常严重。网络黑客大量盗取、网站对个人信息保护意识和能力不足、android 系统上不良 APP 泛滥是造成个人信息泄露日益严重的几个因素。个人信息泄露具有两个特性。一个是危害无法预估，轻则遭遇骚扰电话、垃圾短信、垃圾邮件的骚扰，重则遭遇诈骗及其他严重后果。近期高发的“航班异常”诈骗及网购“交易异常”诈骗，就是诈骗分子在获取了网民个人信息后实施的精准型诈骗，成功率高，危害大。在大数据时代，通过对信息的比对、深入分析和挖掘，能够将网民的个人信息了解的比本人都清楚，网民在网上成了“透明人”。从前的那则名言是，在互联网上没有人知道你是一条狗，现在则变成了，在互联网上不仅知道你是条狗，连每根狗毛都看的清楚。二是泄露的过程不可逆，泄露之后就几乎不可能再回到未泄露的状态，不可挽回。个人信息的存储和流通成本极低，为以后的不法活动提供了条件，成了“不定时炸弹”，随时可以引爆。

加强网民权益保护面临的挑战

（一）法律法规挑战。我国现有涉及网民权益保护的法律规定，不仅过于原则、缺乏可操作性，而且比较零散、缺乏系统性，同时还存在保护范围狭窄等不足。今年的全国“两会”上，《个人信息保护法》呼声很高，建议加快立法进度。对于涉及网民权益保护的《广告法》、《消费者权益保护法》、《电信和互联网用户个人信息保护规定》等，加大执法力度，明确企业责任，加大对侵害网民权益行为的打击力度。

（二）技术挑战。随着大数据和云计算的普及，大量的数据收集和分析成为可能，政府和企业的决策越来越依赖大量的数据收集和分析。在这种情况下，数据挖掘、分析技术使数据被利用的可能性增加，数据被非法收集、使用的风险增大。对于利用高技术进行侵害网民权益的行为，也要利用相关技术采取反制措施，“魔高一尺道高一丈”，增大诈骗分子的难度和成本，提高治理效果。

（三）行政监管挑战。目前我国的互联网管理处于内容管理、行业管理、安全管理分割状态，还没有专门的保护网民权益的相关部门和机构。但从长期发展来看，建立专门机构有利于明确监管主体责任，落实相关法律法规，有利于为网民提供维权申诉一站式服务，提升网民权益保护整体水平。

（四）社会力量有待于进一步加强。网民权益保护离不开网民自身的觉醒。需要加强公众监督，因为网民举报、标记信息是治理网络不良与垃圾信息的重要依据和证据；需要行业组织加强行业自律，督促互联网企业履行社会责任；需要法律维权组织，帮助网民维权，发起公益诉讼；需要网民志愿者组织，加强网民权益保护力量，共同维护自身权益等。总之，网民权益保护任重道远，它不是简单的法律问题、技术问题、管理问题，需要社会各界把保护网民权益作为制定法律法规、开展行政监管及互联网产品设计、互联网市场竞争等诸多领域的出发点和归宿。

今年的 7 月 22 日，中国互联网大会上将举办 2015 中国网民权益保护论坛，欢迎有志之士前来共商网民权益保护大计，共同开创网民权益保护的新局面。

作者简介：郝智超，中国互联网协会 12321 网络不良与垃圾信息举报受理中心副主任，中国互联网协会反垃圾信息工作委员会秘书长，首份《中国网民权益保护调查报告》及首届“中国网民权益保护论坛（2014）”发起人。

（本文刊登于《中国信息安全》2015 年第 4 期）

第五部分 鸣谢

本次调研活动得到广大网民的大力支持，同时非常感谢中国电信、UC 浏览器、百度、腾讯、新浪、公信卫士、二六三邮箱、悠悠村、网易、彩讯科技、小米、奇虎 360、安全管家、金农网、节约网、鸿联九五对本次活动的配合，从而使得调查问卷的数据收集工作得以顺利进行，在此深表感谢！

第六部分 法律声明

本报告中发布的调研数据部分采用网络调查问卷获得，其数据受到样本结构的影响及数量的影响。部分数据未能够准确反映真实市场情况。所以，本报告只提供给使用者作为参考资料，报告制作方对因使用该报告产生的任何后果不承担法律责任。

第七部分 联系方式

地址：北京市复兴门南大街 2-乙号天银大厦 A 东座 10 层 1001 室

邮编：100031

电话：(010) 66414321

传真：(010) 66414320

邮箱：info@12321.cn

网站：www.12321.cn