中国网民权益保护调查报告2016

中国互联网协会
Internet Society of China
2016年6月

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。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，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、钓鱼邮件，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，也是对网民获取真实信息权益的侵犯。

知情权和选择权，指的是网民对自身接收、发出的信息具有知情权和选择权。比如，网民对上网设备上的软件，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。

个人信息保护的权利，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。网民发觉个人信息泄露之后具有主张的权利，即被遗忘权。

报告摘要

1、 网民受到骚扰的情况。近半年，网民平均每周收到垃圾邮件 18.9 封[1]、垃圾短信 20.6 条[2]、骚扰电话 21.3 个。“骚扰电话”是网民最反感的骚扰来源，“电脑广告弹窗”和“APP 推送信息”紧随其后。

2、 网民收到诈骗信息的情况。76%的网民遇到过“冒充银行、互联网公司、电视台等进行中奖诈骗的网站”，排在诈骗信息的第一位；其次是“冒充 10086、95533 等伪基站短信息”，有 66%的网民曾经收到；55%的网民收到过“冒充公安、卫生局、社保局等公众机构进行电话诈骗”的诈骗信息；收到过“冒充苹果、腾讯等公司进行钓鱼、盗取账号的电子邮件”的网民也有一半以上，占 51%；还有 47%的网民遇到过在“社交软件上冒充亲朋好友进行诈骗”的情况。**37%的网民因收到上述各类诈骗信息而遭受到钱财损失。**

3、 网民个人信息泄露情况。54%的网民认为个人信息泄露严重，其中 21%的网民认为非常严重。84%的网民亲身感受到了由于个人信息泄露带来的不良影响。

4、 网民知情权和选择权被侵犯情况。“诱导用户点击”是侵犯网民知情权和选择权的主要现象；其次是“预装软件无法卸载”。“APP 获取个人信息，用户并不知情”的现象排在第三位。其他侵犯网民知情权和选择权的现象依次为“手机、电脑中有些软件不知怎么来的”、“浏览器首页被绑架”、“无法拒收的商业短信”和“无法拒收的商业邮件”等。

5、 近一年估算网民权益被侵犯所造成的经济损失达 915 亿元。近一年，我国网民[3]因为垃圾信息、诈骗信息、个人信息泄露等遭受的经济损失为人均 133 元，比去年增加 9 元，总体经济损失约 915 亿元（我国网民数量 6.88 亿╳网民平均经济损失 133 元=915 亿元）。其中，9%的网民由于各类权益侵害造成的经济损失在 1000 元以上。

6、 保护网民权益优秀创新&实践案例。近一年，我国互联网企业积极履行社会责任，在保护网民权益方面开展了大量的探索和实践，其中取得较好成果的有：互联网金融一站式电子数据保全解决方案——无忧存证；腾讯守护者计划；华为 Mate8/P9 手机基于麒麟 950/955 芯片的防伪基站功能；百度与最高人民法院合作上线失信被执行人查询平台 一键查“老赖”名单；锋尚 MAX 双系统；爱路由；域名不良应用治理——净化网络环境、保护网民权益；网络安全战车；联合 58 同城“打击虚假兼职，黑职介”；电信运营商联手互联网企业防范骚扰诈骗电话。

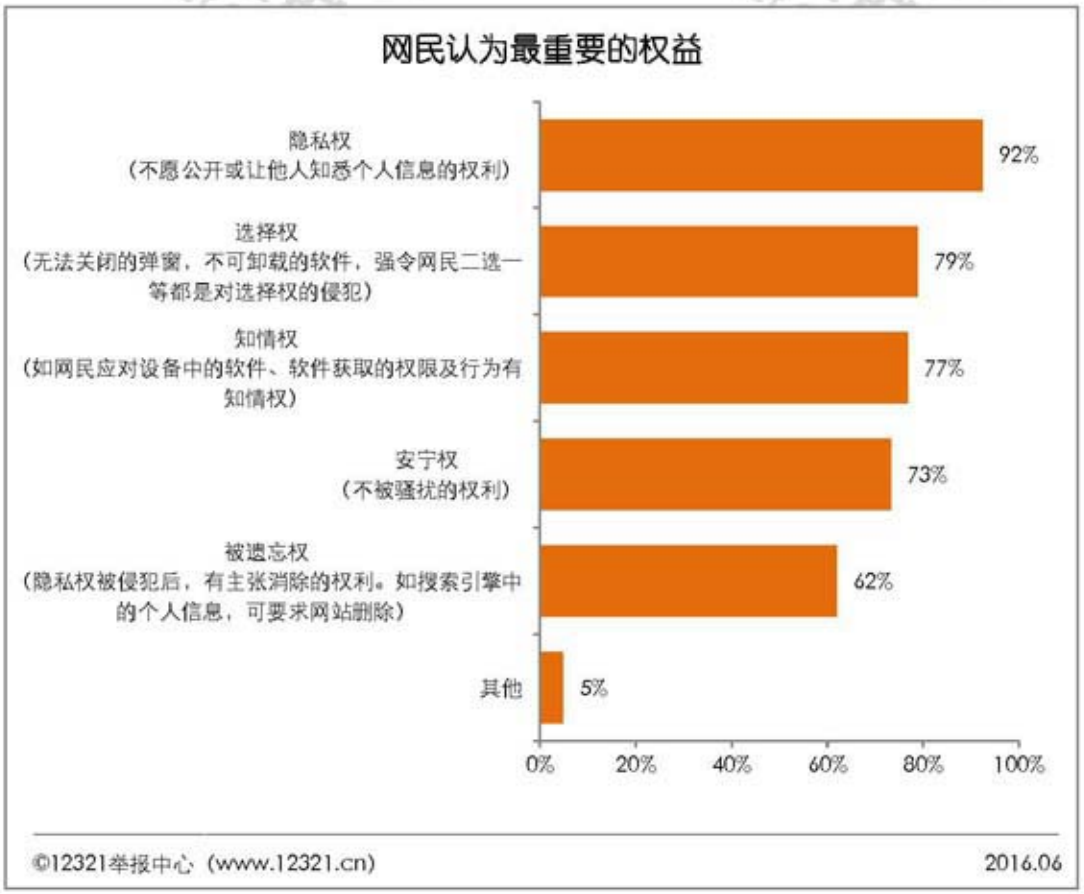
---

[1]2015 年下半年邮箱用户平均每周接收到的垃圾邮件数量为 17.0 封。
[2]2015 下半年调查显示，手机用户平均每周收到的垃圾短信息数量为 16.0 条。
[3]根据 CNNIC 发布的第 37 次《中国互联网络发展状况统计报告》，截至 2015 年 12 月，我国网民规模达 6.88 亿。

第一章 网民权益认知

1. 网民认为最重要的权益

本次调查显示：92%的网民认为“隐私权”是最重要的网民权益；其次是“选择权”和“知情权”，分别有 79%和 77%的网民选择。“隐私权”越来越受到网民的重视，说明广大网民已经认识到个人信息保护的重要性。“隐私权”能否得到有效的保护，对“安宁权”等其他网民权益的保护也起到至关重要的作用。



2. 安宁权

对网民安宁权方面的调查显示：“骚扰电话”成为网民最反感的骚扰来源，有 40%的网民选择。“电脑广告弹窗”和“APP 推送信息”紧随其后，占比分别为 25%和 13%。

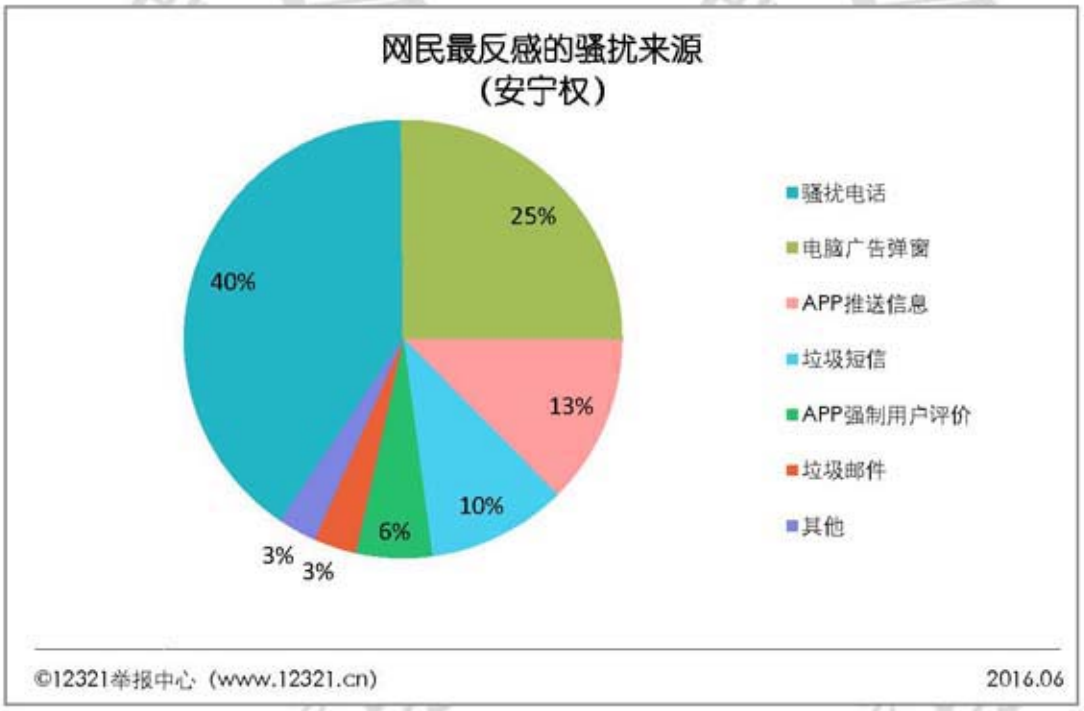
2015 年 6 月 30 日《通信短信息服务管理规定》出台后，短信息服务市场得到了进一步的规范，垃圾短信的治理取得了一定的成效。根据 12321 的举报数据显示，近一年基础运营商点对点垃圾短信举报量减少了 25%，垃圾短信泛滥的势头有所遏制。目前垃圾短信的治理难点主要是伪基站和虚拟运营商。

【提示】

（1）手机中的“APP 推送信息”可以通过设置关闭消息推送功能或设置防打扰时段来有效减少对网民的干扰。

（2）手机用户可以下载安装手机安全软件，屏蔽骚扰电话、垃圾短信的骚扰。

（3）部分手机用户可以设置勿扰模式，选择在特定时间只接收特定联系人的来电。



【法规原文】

（1）《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。

（2）新《消费者权益保护法》第二十九条规定：在经营者未经消费者同意或者请求，或者消费者明确表示拒绝的情况下，经营者不得向消费者发送商业性信息。

3. 知情权和选择权

调查显示：“诱导用户点击”是侵犯网民知情权和选择权的主要现象，有 80%的网民选择。

其次是“预装软件无法卸载”，占 68%。如何既方便用户体验又不伤害用户利益，合理的为用户提供选择，让用户自己决定要不要安装和卸载，是考验终端制造商的一个命题。

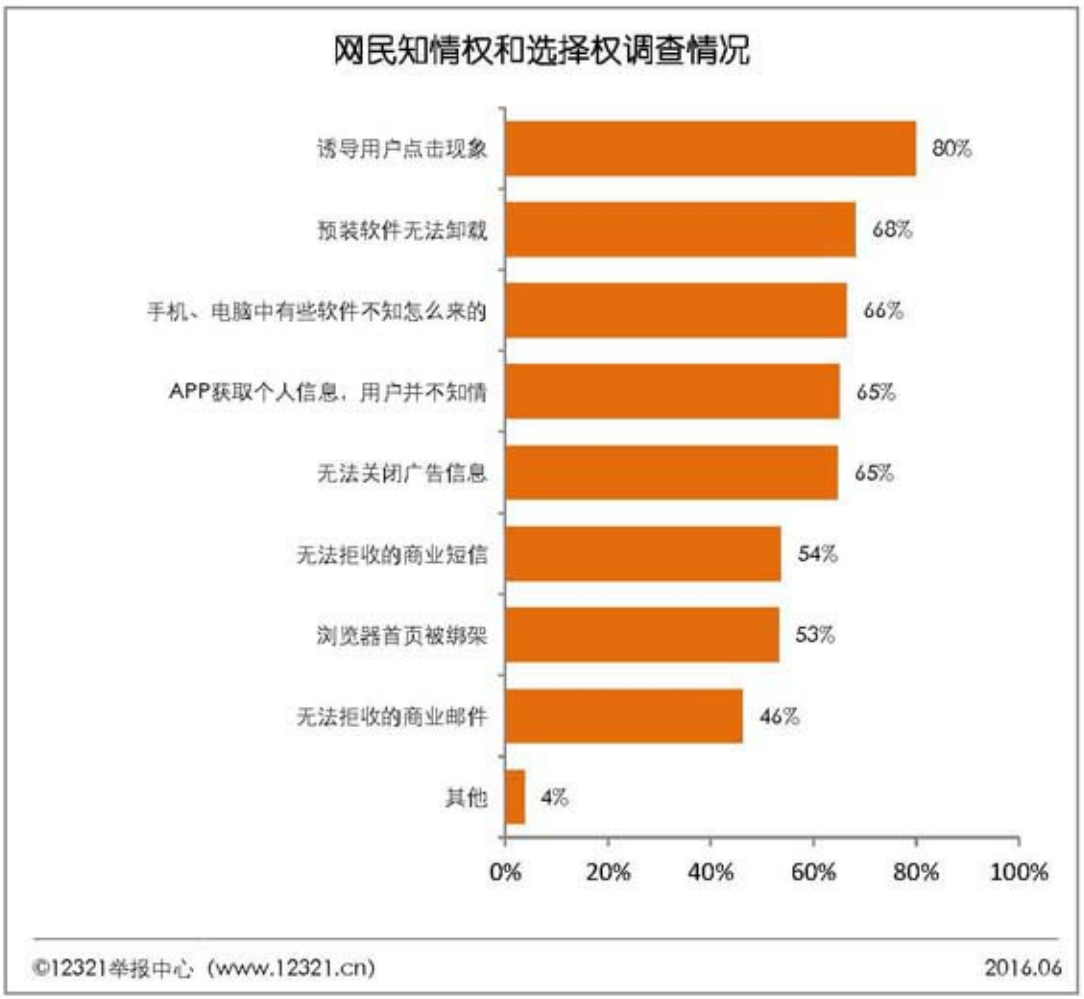
“手机、电脑中有些软件不知怎么来的”占比 66%。此类软件往往具有较大的安全隐患，

建议对其提高警惕，及时清理。

“APP 获取个人信息，用户并不知情”的现象占 65%。根据 12321 举报中心对 APP 敏感权限（安卓系统）进行的分析，2016 年第 1 季度 APP 获取用户信息排名前五位的是：获取用户网络状态、WiFi 状态、访问网络、手机地理位置和读取电话状态这五项权限；另外还有开机自动启动、读取系统日志、读取联系人、修改联系人信息及读取短信内容也是安卓系统获取用户手机敏感权限的主要行为。

“无法关闭广告信息”占 65%，“浏览器首页被绑架”占 53%。这些行为往往伴随着恶意代码或病毒，存在较大的风险，同时侵犯了网民的选择权。

“无法拒收的商业短信”占 54%，“无法拒收的商业邮件”占 46%。《通信短信息服务管理规定》和《电子邮件服务管理办法》均明确规定：未经用户同意，不得向用户发送商业性信息。用户明确表示拒绝接收的，应当停止发送。



【法规原文】

（1）《通信短信息服务管理规定》第二十条：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。

（2）《电子邮件服务管理办法》第十四条：互联网电子邮件接收者明确同意接收包含商业广告内容的互联网电子邮件后，拒绝继续接收的，互联网电子邮件发送者应当停止发送。双方另有约定的除外。互联网电子邮件服务发送者发送包含商业广告内容的互联网电子邮件，应当向接收者提供拒绝继续接收的联系方式，包括发送者的电子邮件地址，并保证所提供的联系方式在30日内有效。

4. 接收真实信息的权利

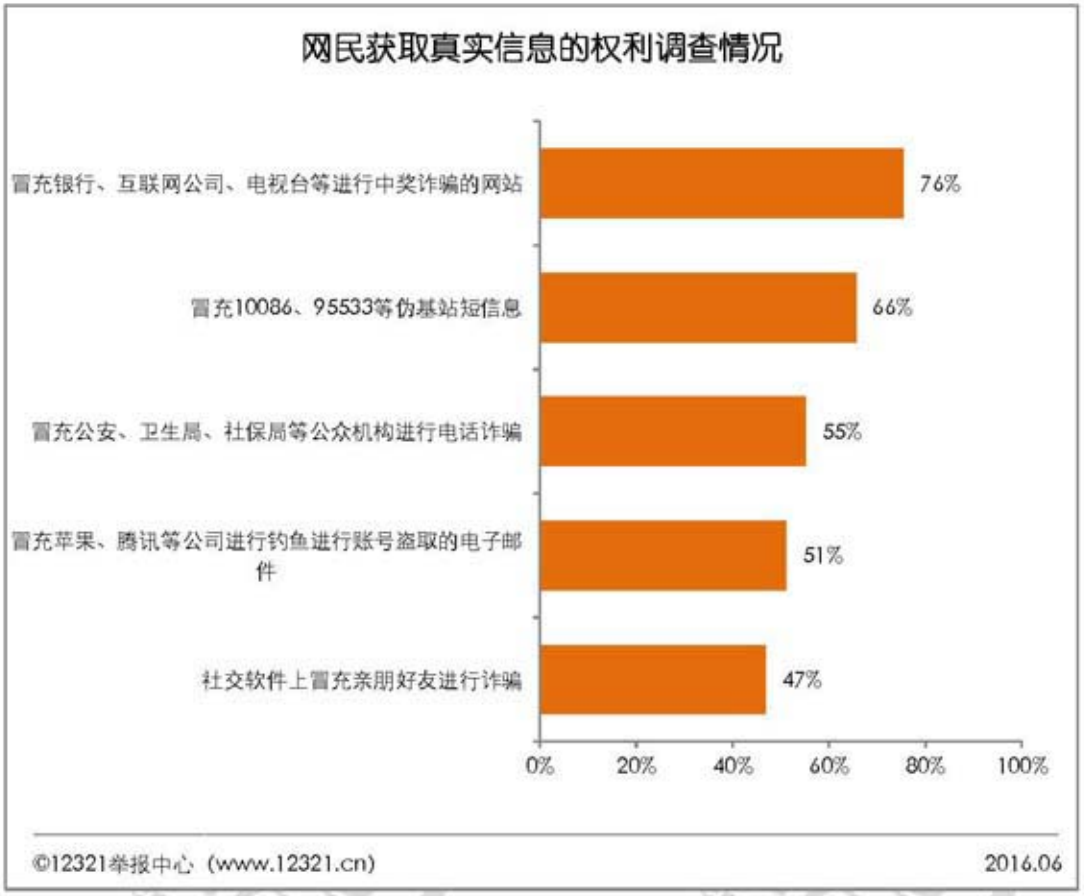
获取真实信息，是网民最基本的权利。本次调查列举了五种最常见的诈骗现象，其中“冒充银行、互联网公司、电视台等进行中奖诈骗的网站”的现象最严重，有76%的网民遇到过。其次是“冒充10086、95533等伪基站短信息”，占66%。“冒充公安、卫生局、社保局等公众机构进行电话诈骗”的占55%。“冒充苹果、腾讯等公司进行钓鱼、盗取账号的电子邮件”占51%。在“社交软件上冒充亲朋好友进行诈骗”的占47%。

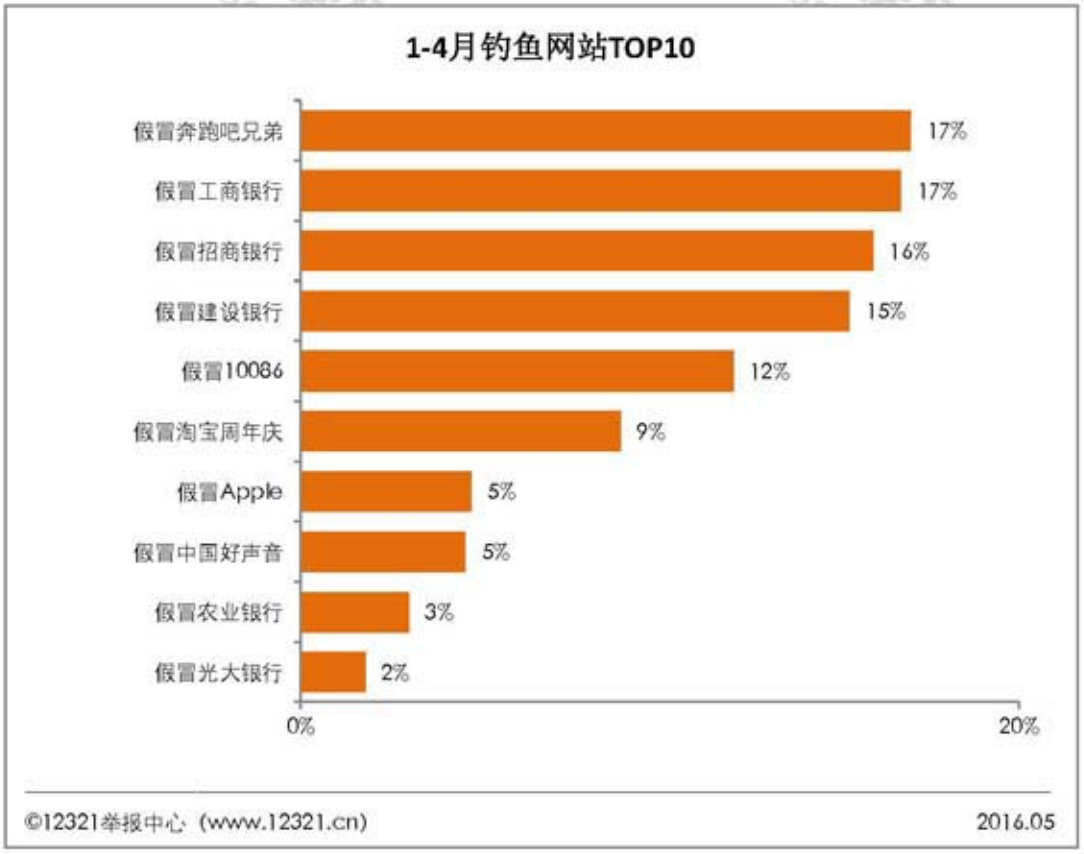
调查还显示：37%的网民因收到下图中的诈骗信息而遭受钱财损失。

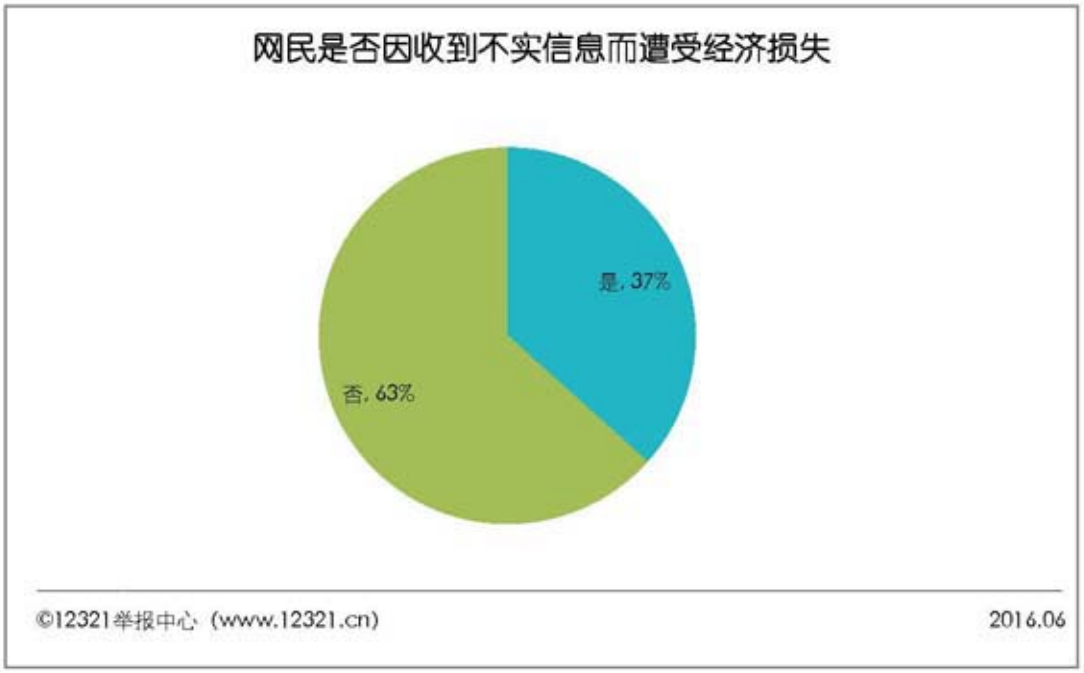
【专项整治】

（1）在2016年1至5月期间，12321举报中心、各基础电信运营、互联网企业多方配合，对改号软件采取专项治理工作，打击网络诈骗。各方共同完善改号软件关键词屏蔽库，累计屏蔽搜索结果超过1亿条、删除下载和链接信息14462条；12321举报中心联动“安全百店”成员单位（应用分发平台）配合工信部累计下架改号APP 657个；联合电商平台发现并下架问题产品293个、处理商户152户。

（2）2016年3至5月，根据网民举报，12321举报中心向安全联盟共享了46541条恶意短信数据，通过对这些信息进行提取与人工审核，已将16091条欺诈网址录入恶意网址库，并同步至搜索引擎、浏览器、网络安全软件、社交软件等各互联网企业，向网民提供了1.83亿次风险提醒，避免造成财产损失。

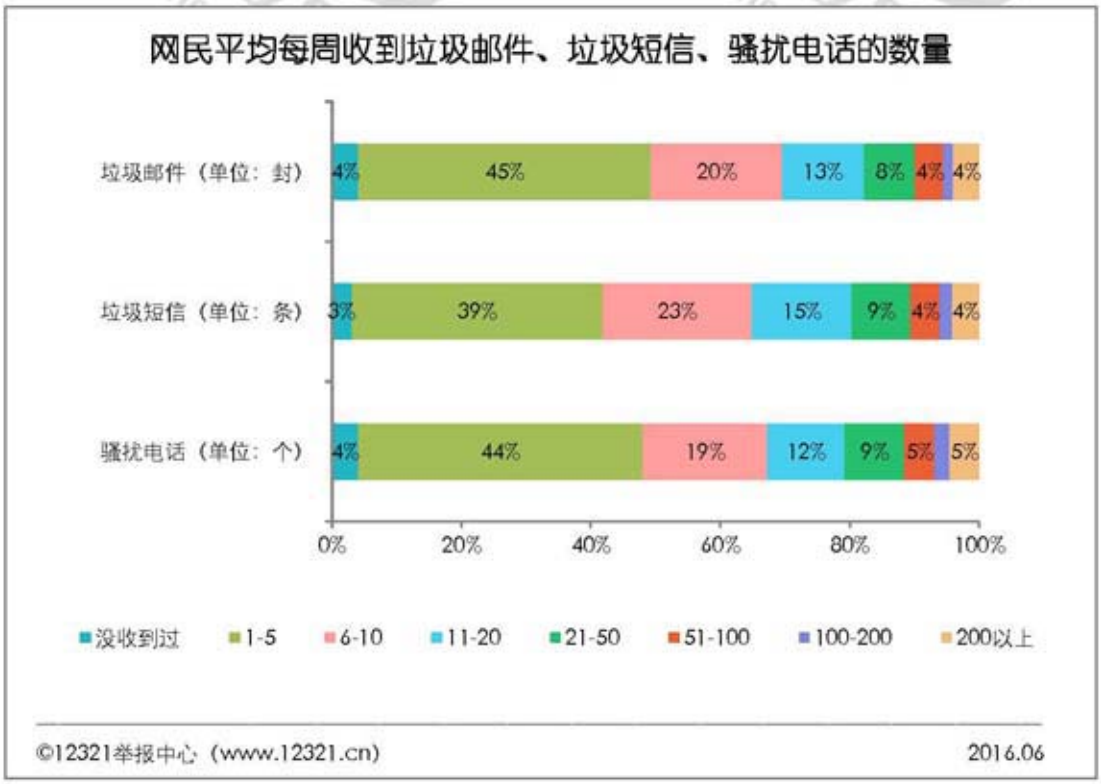

网民获取真实信息的权利调查情况
冒充银行、互联网公司、电视台等进行中奖诈骗的网站
76%
冒充10086、95533等伪基站短信息
66%
冒充公安、卫生局、社保局等公众机构进行电话诈骗
55%
冒充苹果、腾讯等公司进行钓鱼进行账号盗取的电子邮件
51%
社交软件上冒充亲朋好友进行诈骗
47%
0%
20%
40%
60%
80%
100%
©12321举报中心（www.12321.cn）
2016.06


1-4月钓鱼网站TOP10
假冒奔跑吧兄弟
17%
假冒工商银行
17%
假冒招商银行
16%
假冒建设银行
15%
假冒10086
12%
假冒淘宝周年庆
9%
假冒Apple
5%
假冒中国好声音
5%
假冒农业银行
3%
假冒光大银行
2%
0%
20%
©12321举报中心（www.12321.cn）
2016.05



5. 每周收到垃圾邮件、垃圾短信和骚扰电话的数量

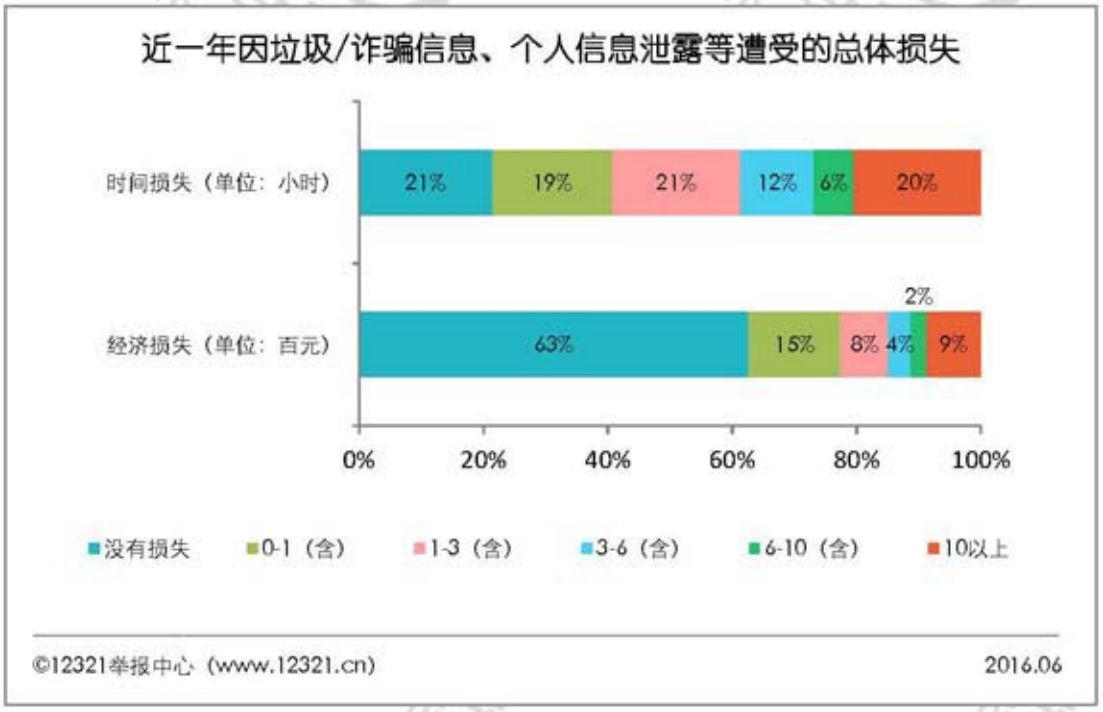
近半年网民平均每周收到垃圾邮件 18.9 封[4]、垃圾短信 20.6 条[5]、骚扰电话 21.3 个。



[4]2015 年下半年邮箱用户平均每周接收到的垃圾邮件数量为 17.0 封。
[5]2015 下半年调查显示，用户平均每周收到的垃圾短信息数量为 16.0 条。

6. 总体经济和时间损失

近一年，我国网民[6]因为垃圾信息、诈骗信息、个人信息泄露等遭受的经济损失人均 133 元，总体经济损失约 915 亿元（我国网民数量 6.88 亿×网民平均经济损失 133 元=915 亿元）。9%的网民近一年由于各类权益侵害造成的经济损失在 1000 元以上。每个网民平均时间损失 3.6 小时。



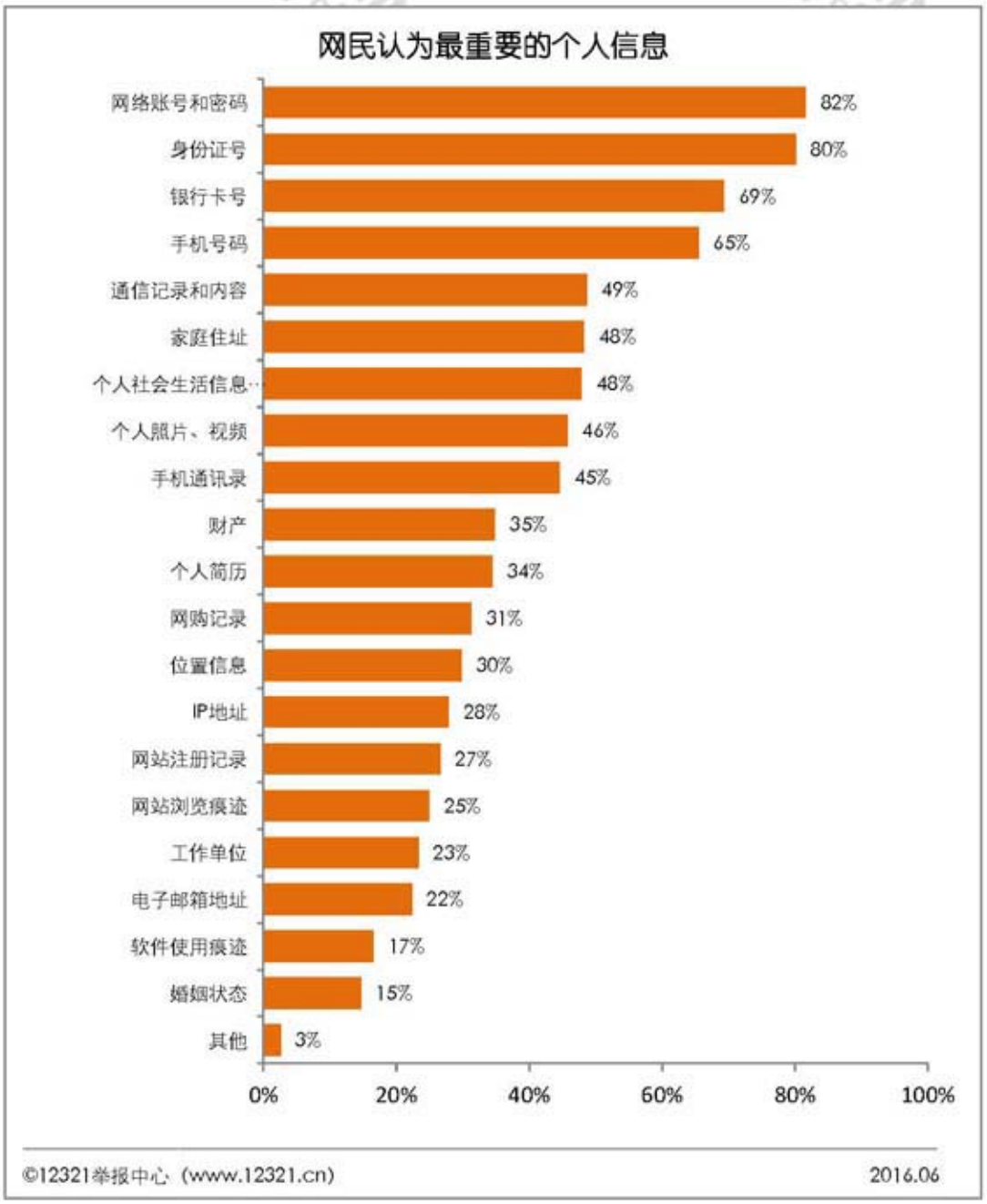
[6]根据 CNNIC 发布的第 37 次《中国互联网络发展状况统计报告》，截至 2015 年 12 月，我国网民规模达 6.88 亿。

第二章 个人信息保护

1. 网民认为最重要的个人信息

在本次调查罗列的二十项个人信息中，网民认为最重要的个人信息是“网络账号和密码”、“身份证号”、“银行卡号”和“手机号码”，占比都超过半数，分别为82%、80%、69%和65%。

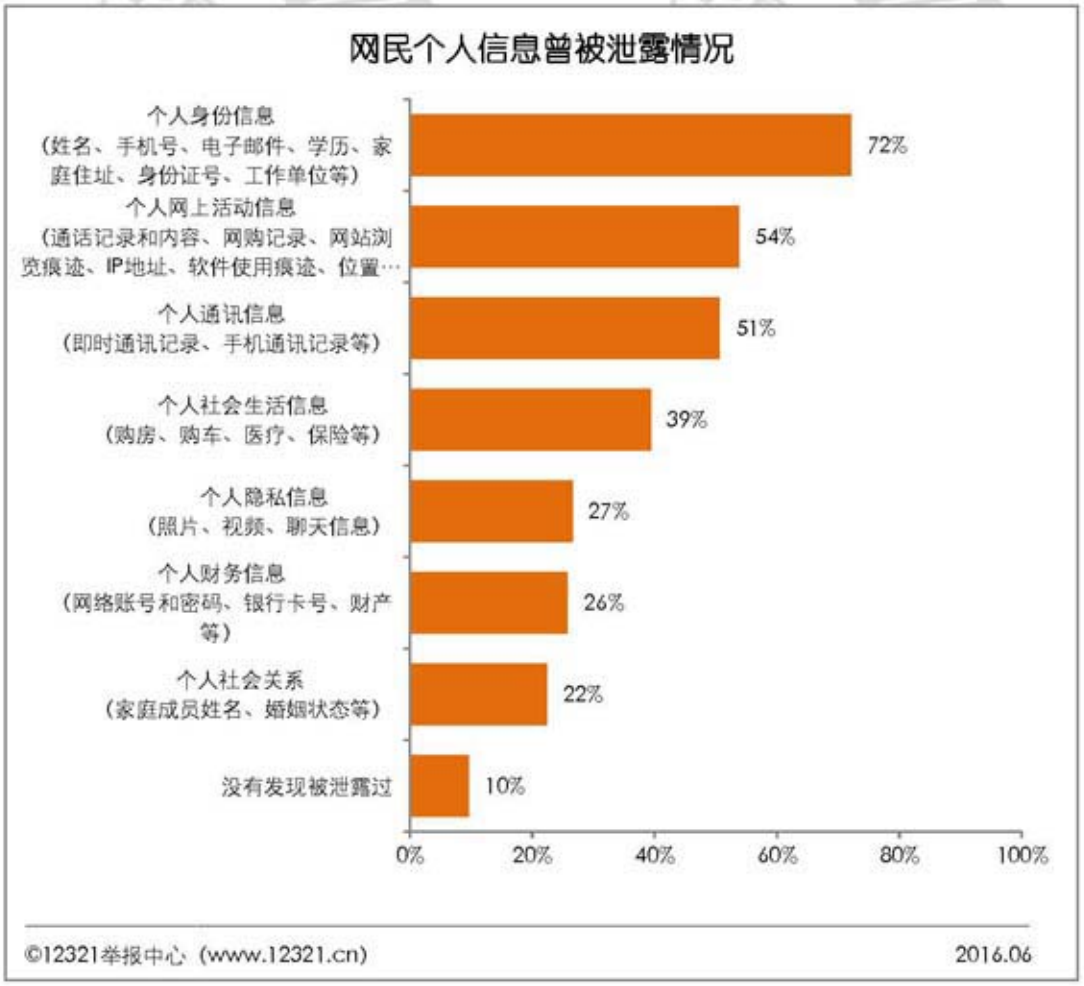
事实上，随着互联网和移动网的发展，网民的“网购记录”（占31%）、“位置信息”（30%）、“IP地址”（占28%）、“网站注册记录”（占27%）、“网站浏览痕迹”（占25%）、“软件使用痕迹”（占17%）也是很重要的个人信息，应值得网民重视。



2. 个人信息泄露状况调查

在调查中，网民“个人身份信息”泄露情况最严重，有72%的调查者选择。包括网民的姓名、手机号、电子邮件、学历、住址、身份证号码等信息。

其次是个人网上活动信息，占 54%。包括通话记录和内容、网购记录、网站浏览痕迹、IP 地址、位置信息等内容。



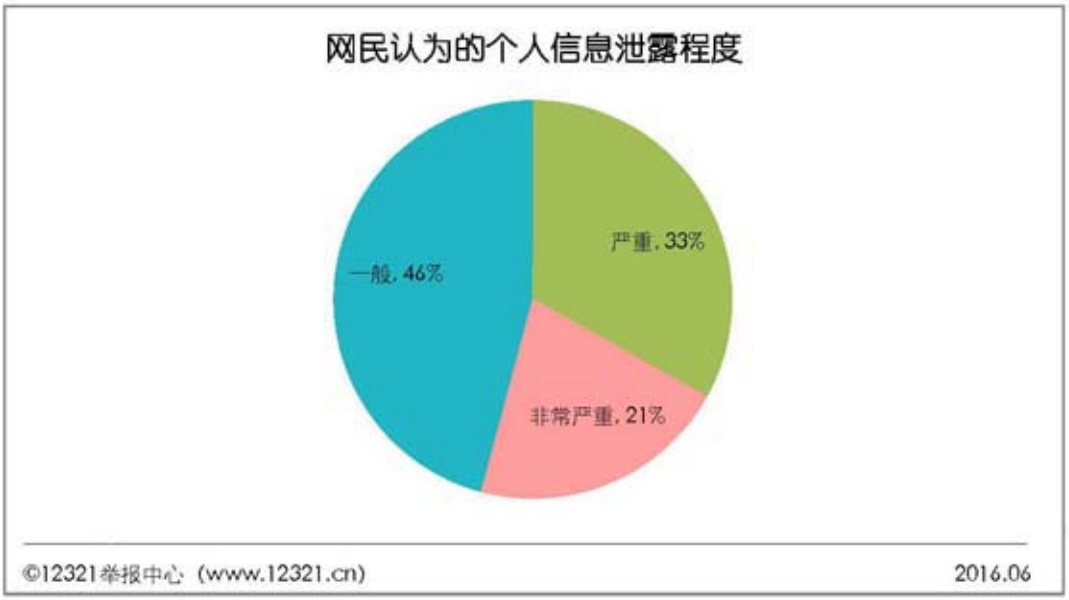
目前我国网络个人信息泄露呈现多样化的特点，泄露的类型有通过黑客破解数据库、恶意代码等技术手段窃取，也有通过 APP、社交软件等程序非法收集，通过线上和线下举办活动收集，甚至有些信息可以通过网络公开购买、查询、下载，还有些个人信息是由于商场、医院、教育机构、金融机构、物流环节等疏于管理而被泄露。

根据 12321 的举报数据分析，2016 年 1 至 6 月网民举报的个人信息泄露主要情况及数量见下表：

2016 年 1 至 6 月网民举报个人信息泄露主要情况及数量	
1、原因不明的个人信息泄露，来电就知道网友姓名等个人信息	9453 件次
2、个人隐私信息在搜索引擎中泄露	4437 件次
3、手机号泄露，遭遇电话炸弹或短信炸弹。（短时间内收到大量电话或短信）	2026 件次
4、日常生活信息（购租房、考试、购车、车险、升学、生子、去世等）泄露后遭遇特定骚扰或诈骗	1894 件次
5、个人邮箱、即时通信工具、微博、苹果 ID 等各类网络帐号密码被盗	1779 件次
6、在二手交易网站留下个人电话后，持续遭遇各类骚扰	1426 件次
7、网购信息泄露，收到相关交易异常诈骗信息	1418 件次
8、在钓鱼网站填写个人信息后收到冒充公检法机构的诈骗、恐吓信息	1415 件次
9、收到针对网友本人的银行卡、信用卡系统升级、额度提升等诈骗信息	1367 件次
10、批量个人信息（各类账号、卡号、身份证号、特定人群手机号等）贩卖	1338 件次
11、购买机票后遭遇航班异常诈骗信息	1251 件次
12、个人信息被某网站公布了	942 件次
13、接到调查类电话，感觉是骗取个人信息的	919 件次
14、注册金融类 APP 后收到大量理财、股票类骚扰电话或短信	425 件次

3. 网民对个人信息泄露程度的主观感受

54%的网民认为个人信息泄露严重。其中 21%的网民认为非常严重，33%的网民认为严重，46%的网民觉得一般。



4. 个人信息泄露带来的不良影响

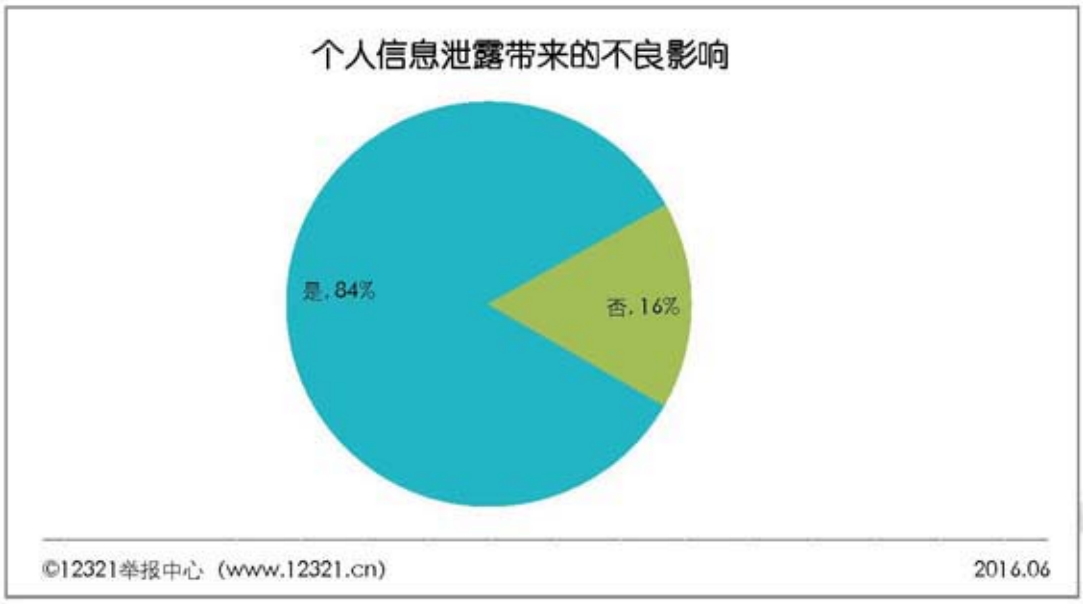
84%的网民亲身感受到了个人信息泄露带来的不良影响，16%的网民无明显感受。

个人信息泄露有可能给网民带来以下不良影响：

（1）**个人信息泄露导致垃圾信息泛滥。**不少网民反映，一些从未接触过的商家向其发送垃圾短信和垃圾邮件，这些网民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网民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。在12321接到举报中，遭受骚扰的案例占比达到59.6%，少数网民遭遇短信炸弹，生活遭受严重干扰。

（2）**个人信息泄露导致非法诈骗猖獗。**根据12321的举报数据，网民明确表示遇到骗子、欺骗行为或者事后意识到被骗的情况占网民举报总量的16.2%。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。



第三章 典型应用的侵权现象及防护措施

1. 电子邮件

- **网民使用电子邮件的过程中遇到的侵权现象**

“收到不良内容（病毒、欺诈、违法等）的邮件”是邮箱使用过程中遇到的最严重的侵权现象，有 71%的网民遇到过。

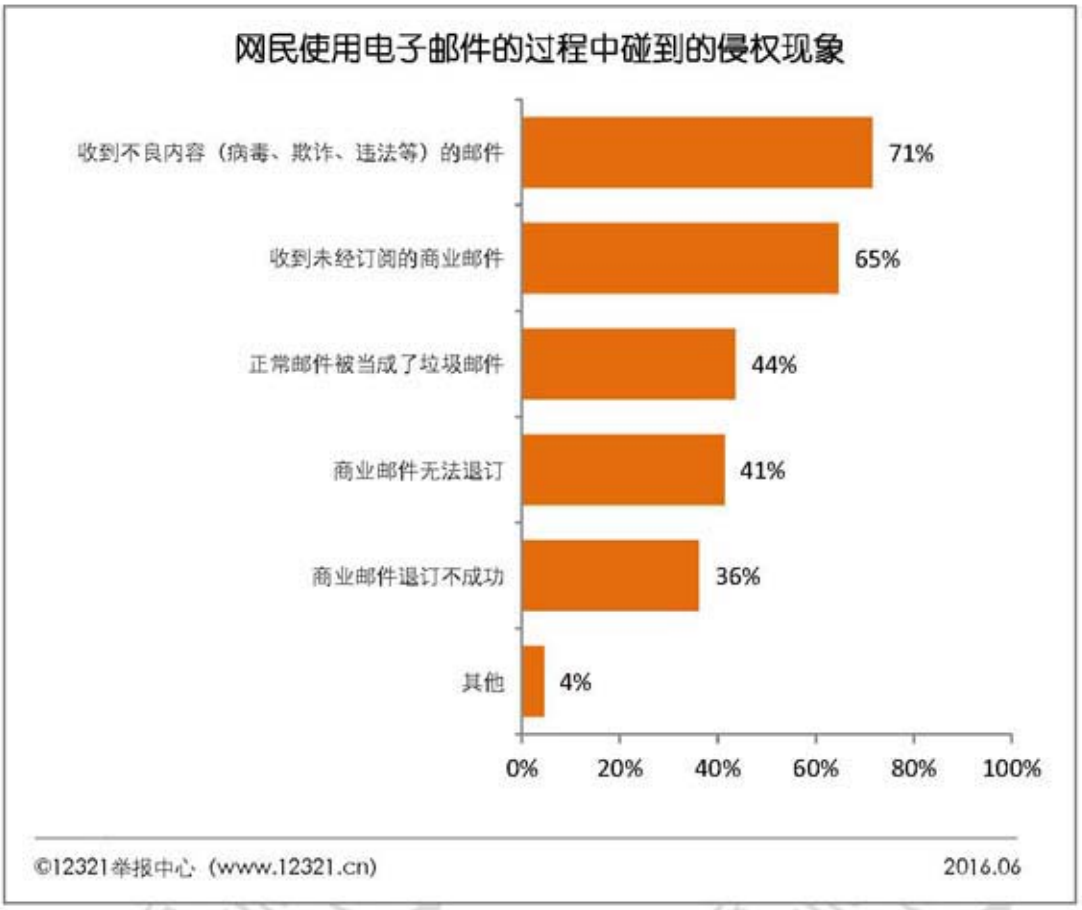
“收到未经订阅的商业邮件”（占 65%）和“商业邮件无法退订”（占 41%）、“商业邮件退订不成功”（占 36%）等不规范的商业邮件发送行为仍然经常在电子邮件使用过程中遇到。

“正常邮件被当成垃圾邮件”过滤掉的，占 44%。

【提示】

（1）建议网民定期浏览垃圾邮件箱中的邮件，以免由于正常邮件被误判为垃圾邮件，从而对工作和生活造成影响。有网友向 12321 举报中心反映过，有面试通知邮件、甚至国外学校录取通知邮件被误拦导致用户耽误了面试、入学的情况。

（2）对于邮箱中的垃圾邮件，建议不要轻易点击查看，以免被垃圾邮件发送者当作活跃用户，继续受到垃圾邮件的骚扰。

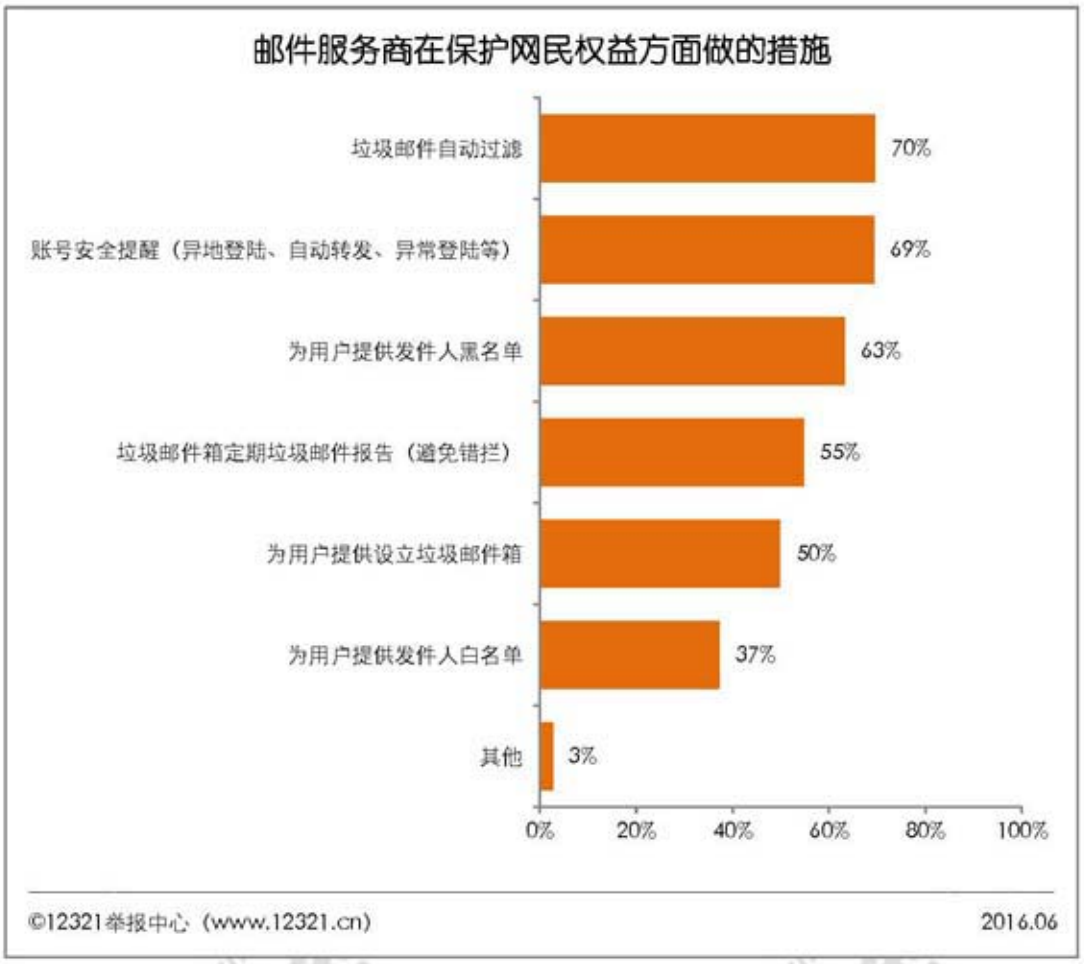


- **邮件服务提供商保护网民权益的措施**

“垃圾邮件自动过滤”和“账号安全提醒”两项措施的认可度较高，分别占 70%和 69%。

“为用户提供发件人黑名单”占 63%。该项措施虽然认可度较高，但由于垃圾邮件发件人的邮箱地址极易伪造，因此实际效果并不明显。

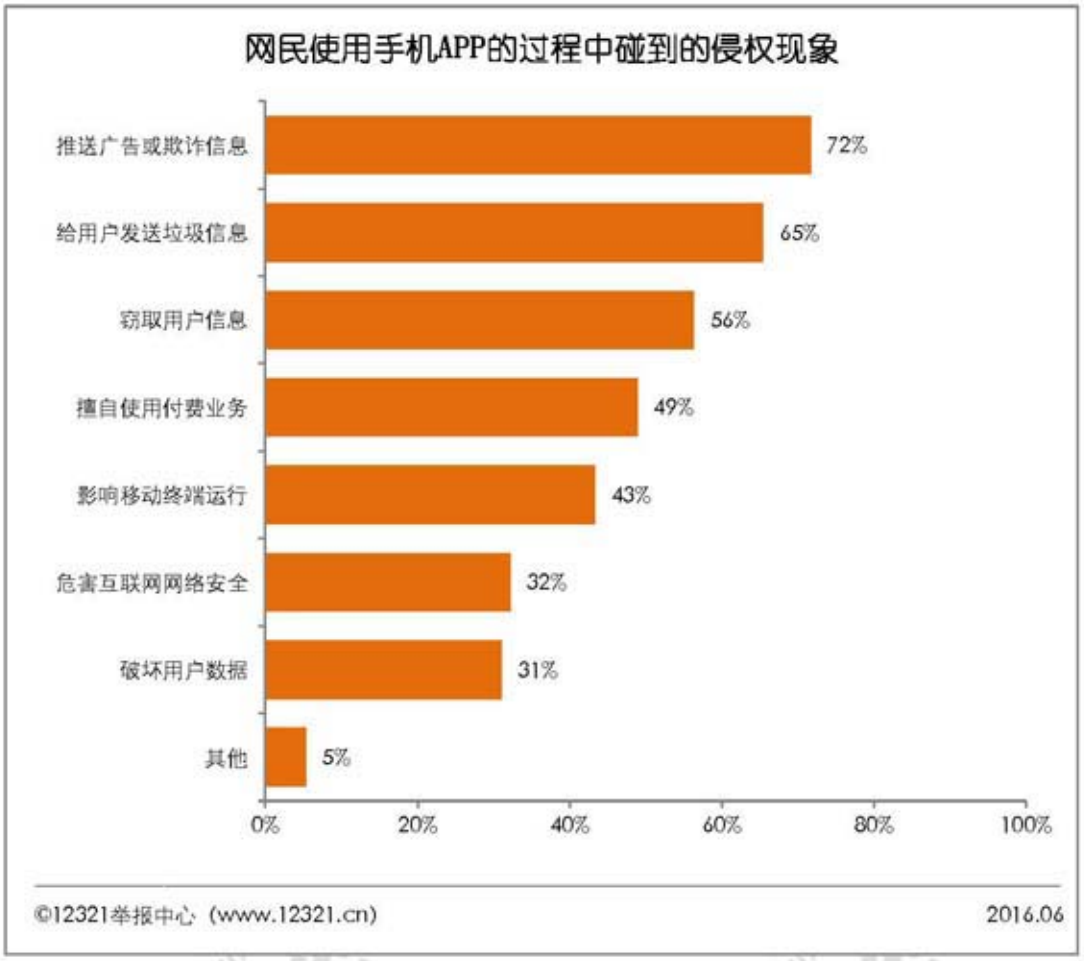
“垃圾邮件箱定期提供垃圾邮件报告（避免错拦）”占 55%。该措施可以帮助网民纠正正常邮件被错拦的情况，与网民的工作生活相关性较大，建议邮件服务提供商普及该项措施。



2. 手机 APP

- **使用手机 APP 的过程中遇到的侵权现象**

“推送广告或欺诈信息”和“给用户发送垃圾信息”是手机 APP 在使用过程中最常见的侵权现象，占 72%和 65%。其次是“窃取用户信息”和“擅自使用付费业务”占 56%和 49%。



- **防范恶意 APP 的保障措施**

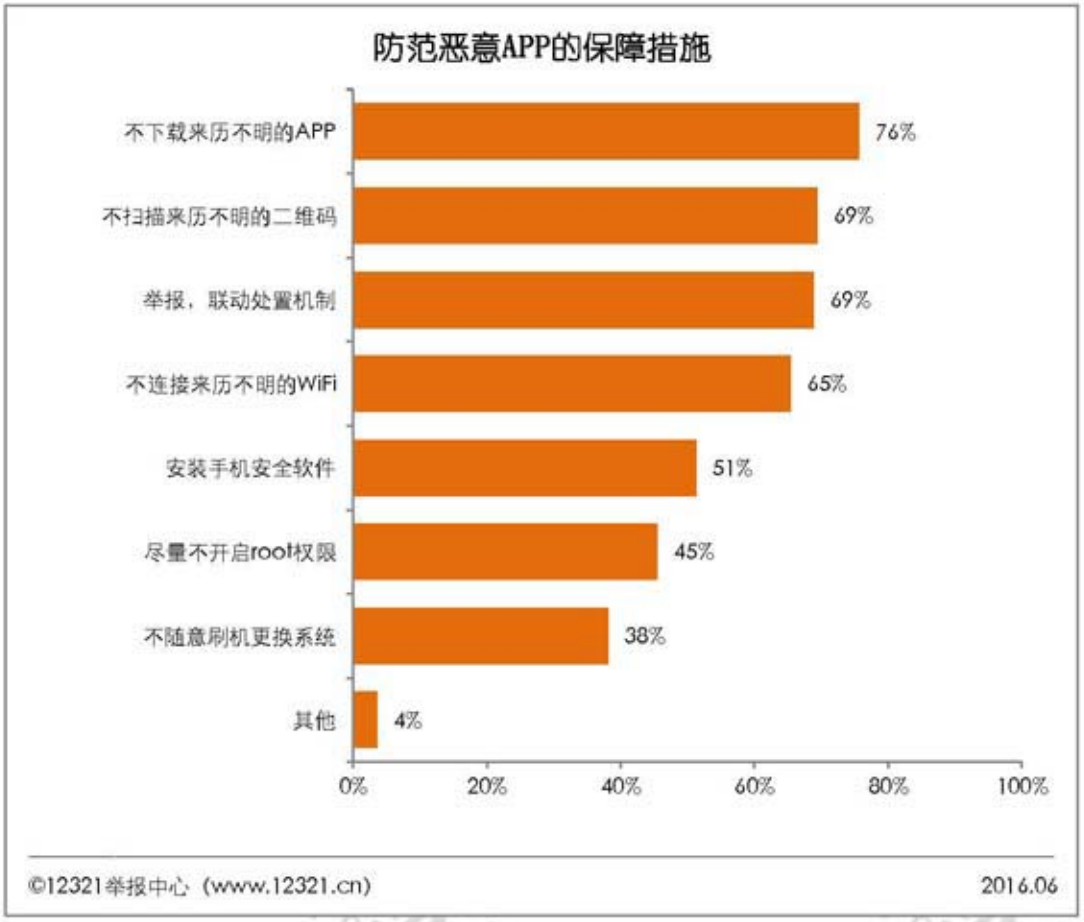
在防范恶意 APP 的措施中，76%的网民认为“不下载来历不明的 APP”是最有效的防范措施。“不扫描来历不明的二维码”占 69%。“不连接来历不明的 WiFi”占 65%。“尽量不开启 root 权限”占 45%。“不随意刷机更换系统”占 38%。除了网民养成良好的使用习惯外，加强“举报、联动处置机制”也很重要，占 69%。另外 51%的网民认为“安装手机安全软件”比较有效。

【专项整治】

为治理恶意手机应用软件，发挥 12321 举报中心的公众监督职能，从下载源头开展对恶意 APP 进行治理的探索与实践，规范 APP 及其下载服务。12321 举报中心发起“安全百店”行动，通过联合广大手机应用商店，建立“一键举报、百家联动”的公众监督和治理机制。

12321 举报中心受理网民举报不良 APP，对网民举报并经核查存在问题的不良 APP 予以问题告知、约谈、下架、提交至相关部门四种处理方式；约谈的 APP 企业要根据自身的责任情况进行整改，在限期内提交整改报告并完成整改，完成整改的 APP 将恢复上架。对于无法联系或不进行有效整改工作的，12321 举报中心联动“安全百店”成员单位（移动应用分发

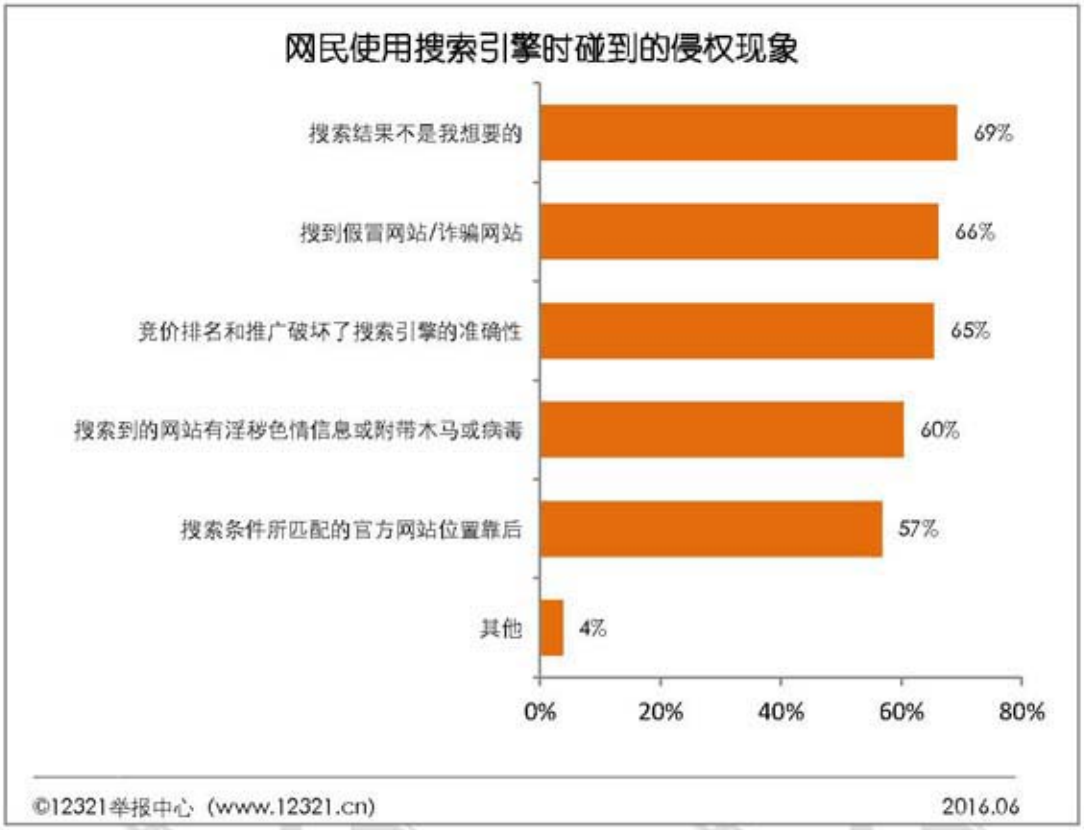
平台）对涉及 APP 予以下架处理。2016 年 1 至 5 月，12321 举报中心共接到手机应用软件（APP）举报 320605 件次，下架 APP 1166 款。



3. 搜索引擎

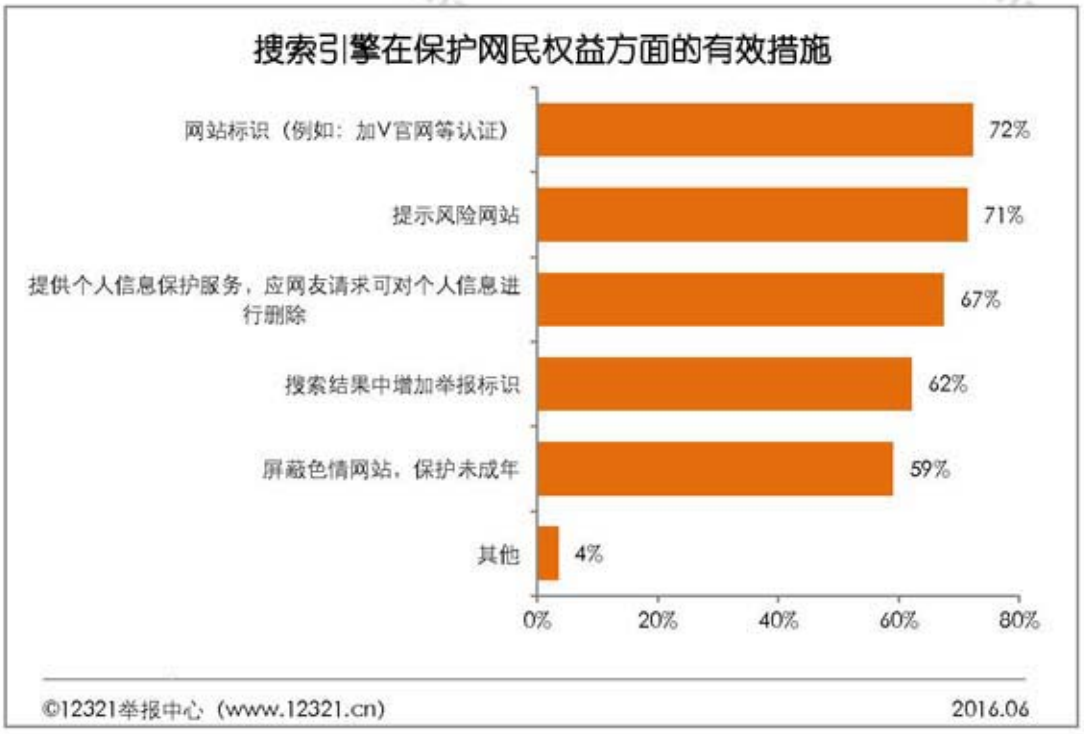
- **使用搜索引擎时遇到的侵权现象**

网民使用搜索引擎时，“搜索结果不是我想要的”（占 69%）的侵权现象排在第一位，略高于“搜到假冒网站/诈骗网站”（占 66%）和“竞价排名和推广破坏了搜索引擎的准确性”（占 65%）。“搜到的网站有淫秽色情信息或附带木马病毒”占 60%。“搜索条件所匹配的官方网站位置靠后”占 57%。



- **搜索引擎在保护网民权益上所做的最有效的保护措施**

网民认为搜索引擎给网站增加“网站标识”是保护网民权益最有效的措施，占 72%；其次是“提示风险网站”，占 71%；“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 67%。“搜索结果中增加举报标识”占 62%。“屏蔽色情网站，保护未成年人”占 59%。

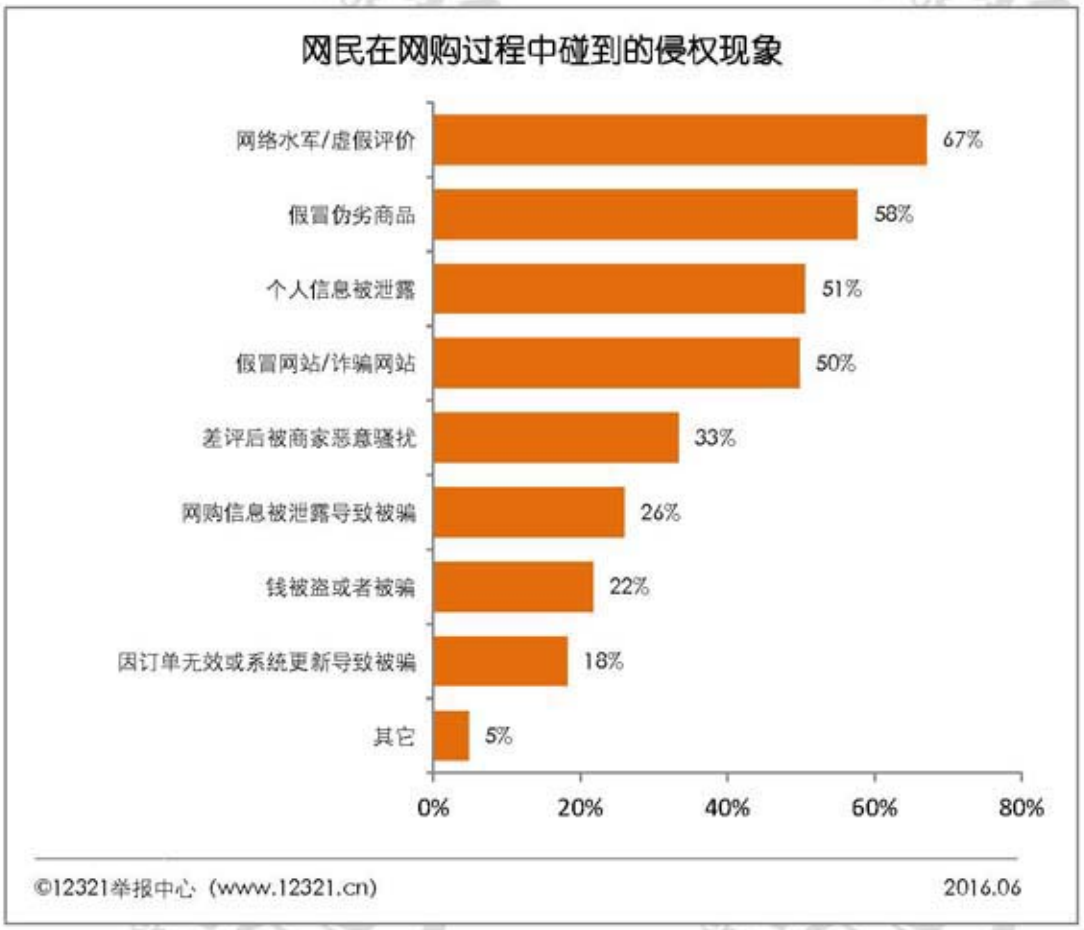


4. 网络购物

- **网民在网络购物的时候遇到的侵权现象**

“网络水军/虚假评价”是网民在网购过程遇到的最严重的侵权现象，调查显示占比 67%。其次是网购买到“假冒伪劣商品”的现象占 58%。“个人信息被泄露”和“假冒网站/诈骗网站”分别占 51%和 50%。

“差评后被商家恶意骚扰”占 33%，排第五位。虽然该项占比不高，但对网民的侵害程度强，危害极大，严重影响了网民的正常生活。另外，由于网民频遭恶意骚扰，导致网购之后不愿、不敢打差评，影响了网购的总体评价环境，对其他网民的知情权也是一种损害。



- **网购渠道存在的风险**

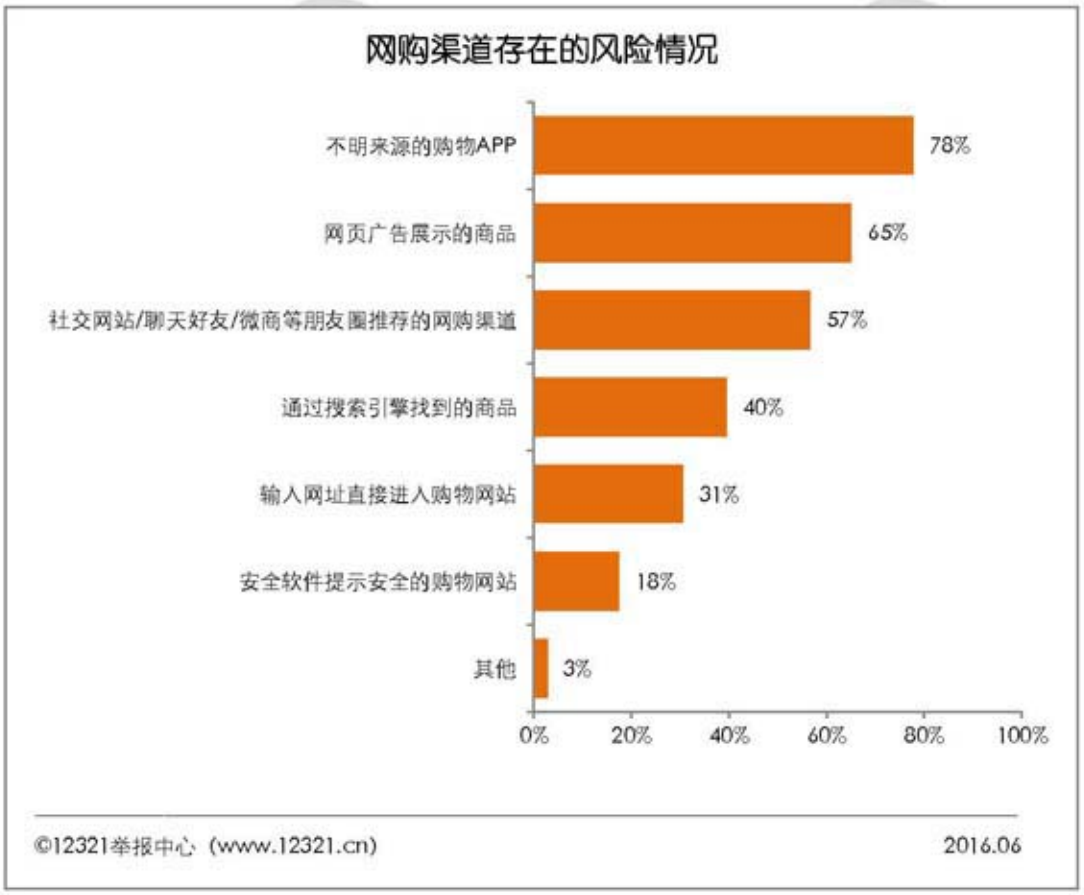
78%的网民认为“不明来源的购物 APP”是风险最大的购物渠道。其次是“网页广告展示的商品”，占 65%。“社交网站/聊天好友/微商等朋友圈推荐的网购渠道”排在第三位，占 57%。

【提示】

（1）“不明来源的购物 APP”往往是钓鱼网站窃取用户信息的工具，隐藏着极大的风

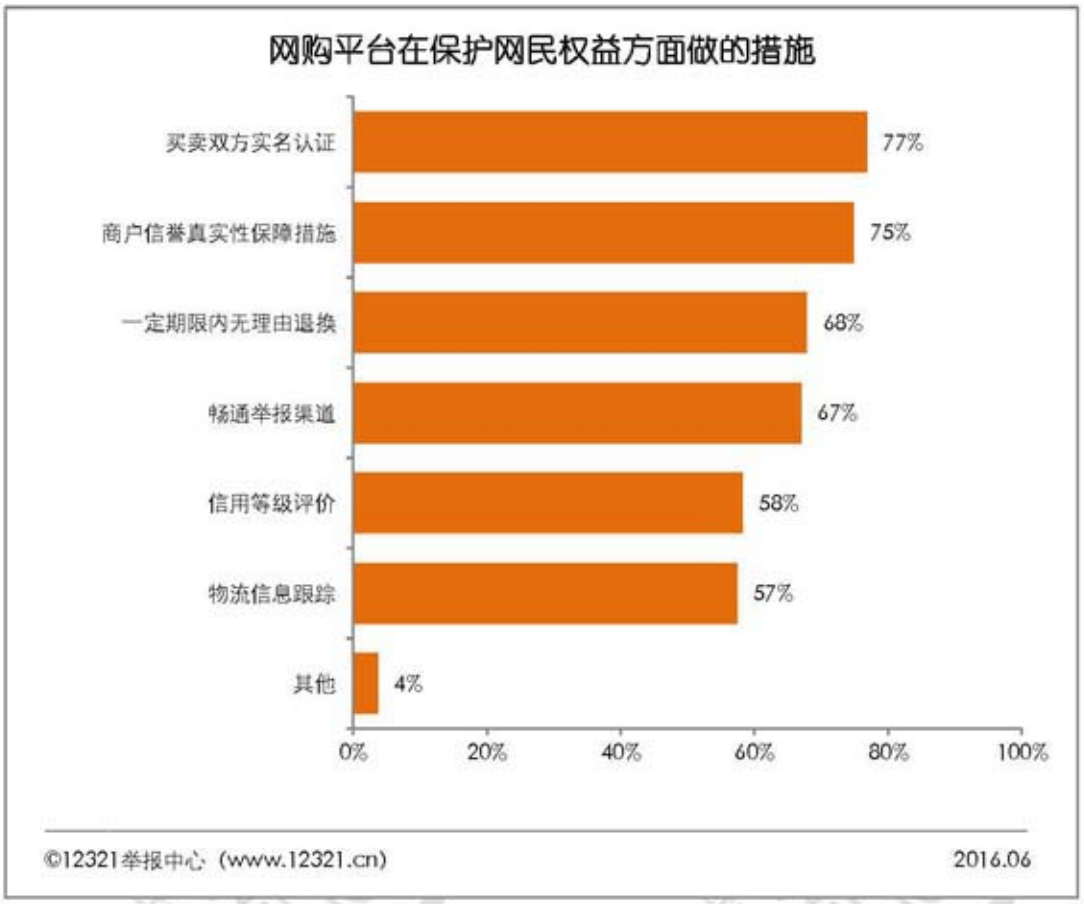
险。建议网民通过正规渠道、在正规的应用商店下载购物 APP。

（2）通过微博、微信等渠道购买商品很多都是“熟人交易”，并无相关营业资质，网民要足够谨慎，不要轻易盲目下单。



- **网购平台在保护网民权益上所做的措施**

在网购平台保护网民权益的措施上，“买卖双方实名认证”和“商户信息真实性保障措施”的占比比较接近，分别为 77%和 75%。其次是“一定期限内无理由退换”和“畅通举报渠道”占 68%和 67%。“信用等级评价”和“物流跟踪”占 58%和 57%。



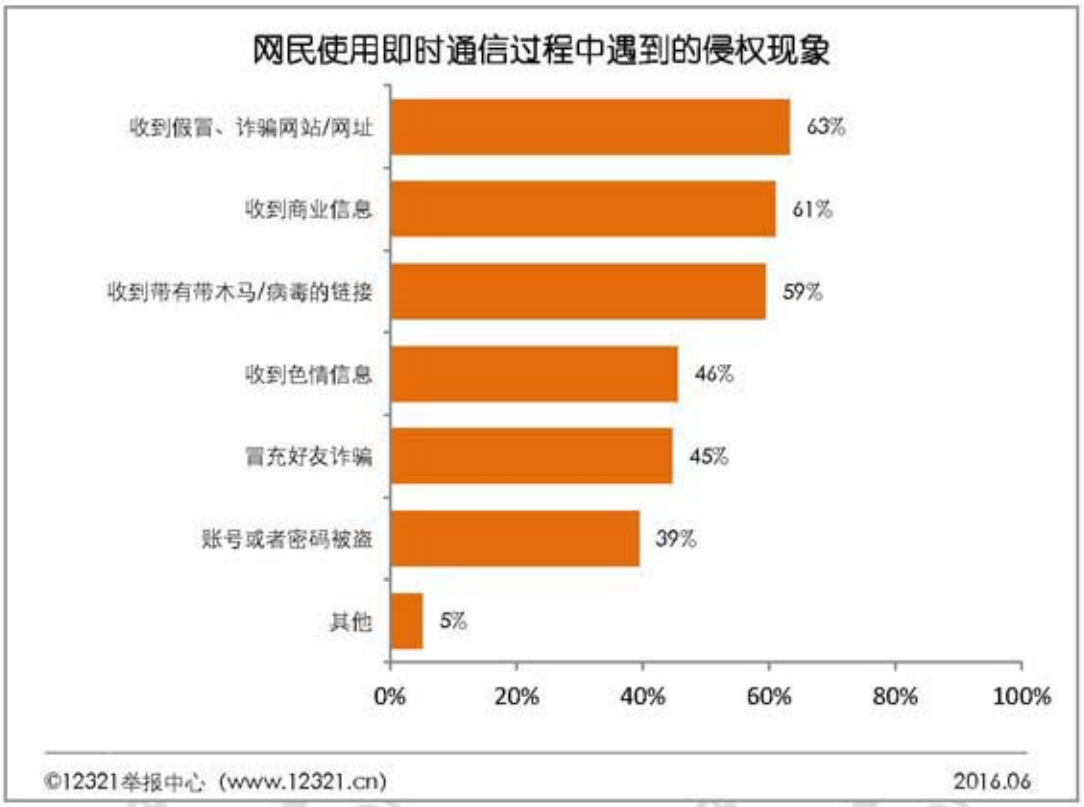
5. 即时通信

- **网民使用即时通信过程中遇到的侵权现象**

即时通信作为基础的互联网应用，已与网民的日常生活密不可分。而在使用的过程中，63%的网民会遇到“收到假冒、诈骗网站/网址”的现象；61%的网民会“收到商业信息”；59%网民遇到过“收到带有木马/病毒的链接”。“冒充好友诈骗”占 45%。“账号或密码被盗”占 39%。

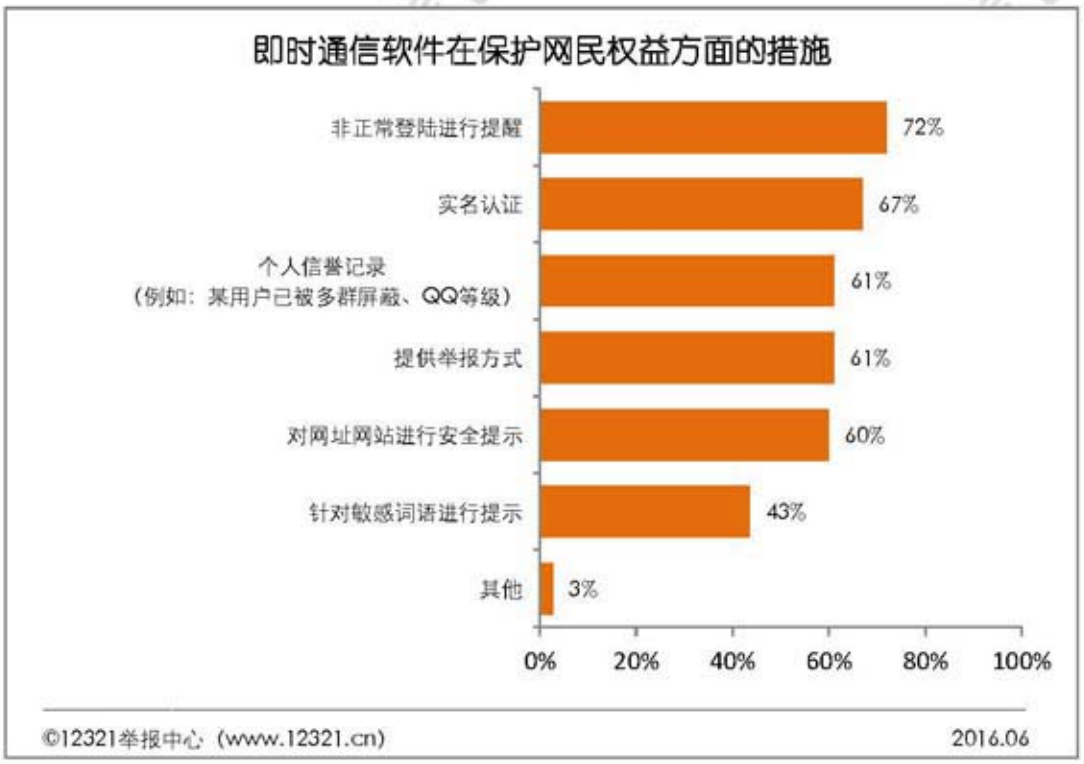
【提示】

QQ、微信等即时通信工具成为被不法分子利用进行诈骗的重要渠道，因此不建议点击陌生人发来的链接或压缩包等信息。即使是好友发送的信息，也要谨慎判断，避免因好友账号被盗而遭受损失。



- **即时通信在保护网民权益方面做的措施**

即时通信目前所做的保障网民权益的措施中，“非正常登陆提醒”的认可度最高，占 72%。其次是“实名认证”，占 67%。“个人信誉记录”（61%）、“提供举报方式”（61%）和“对网址网站进行安全提示”（60%）紧随其后，认可度均超过 60%。



6. 网络游戏

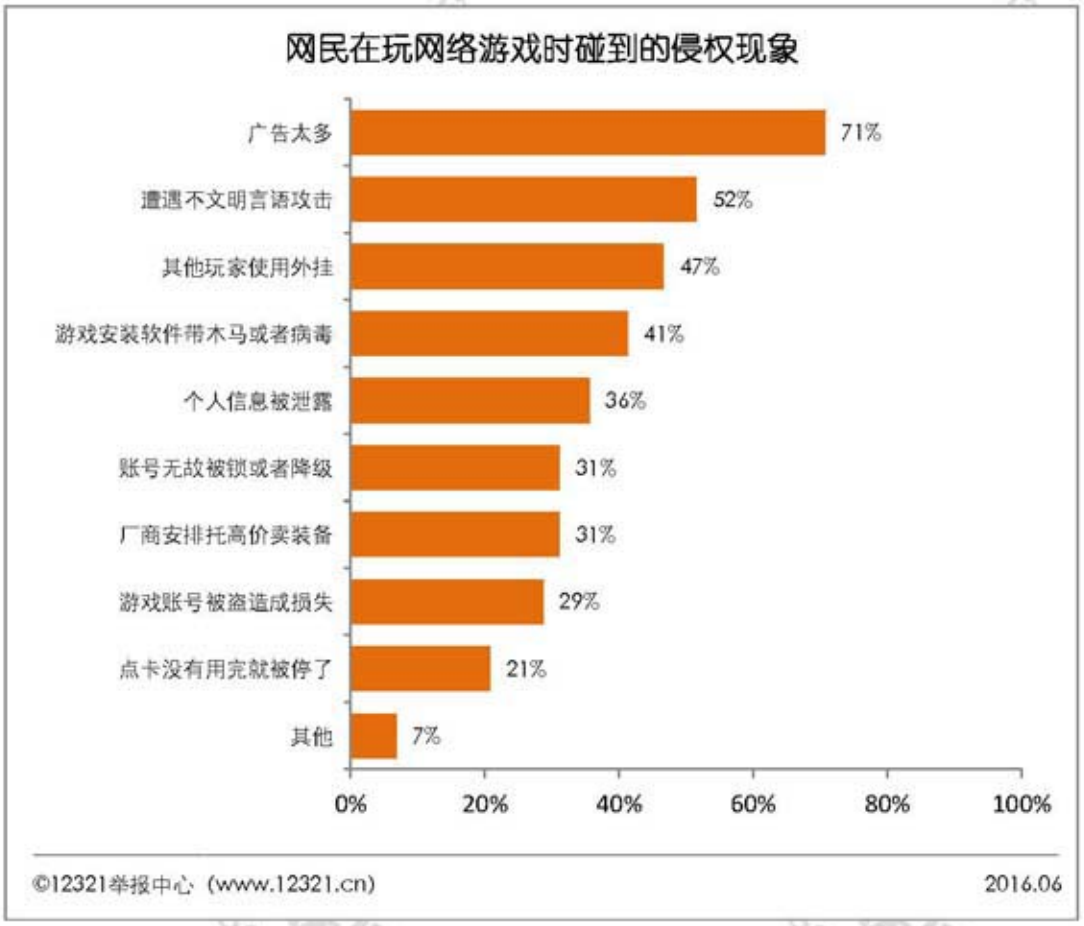
- **网民玩游戏的过程中碰到的侵权现象**

“广告太多”远超其他侵权现象，占 71%。其次是“遭遇不文明言语攻击”，占 52%。

其他的侵权现象可以归为两类：玩家待遇不公平和玩家信息不安全。

“其他玩家使用外挂”（占比 47%）、“厂商安排托高价卖装备”（占比 31%）、“账号无故被锁或者降级”（31%）、“点卡没有用完就被停了”（占 21%）是在玩游戏的时候遇到的不公平现象。

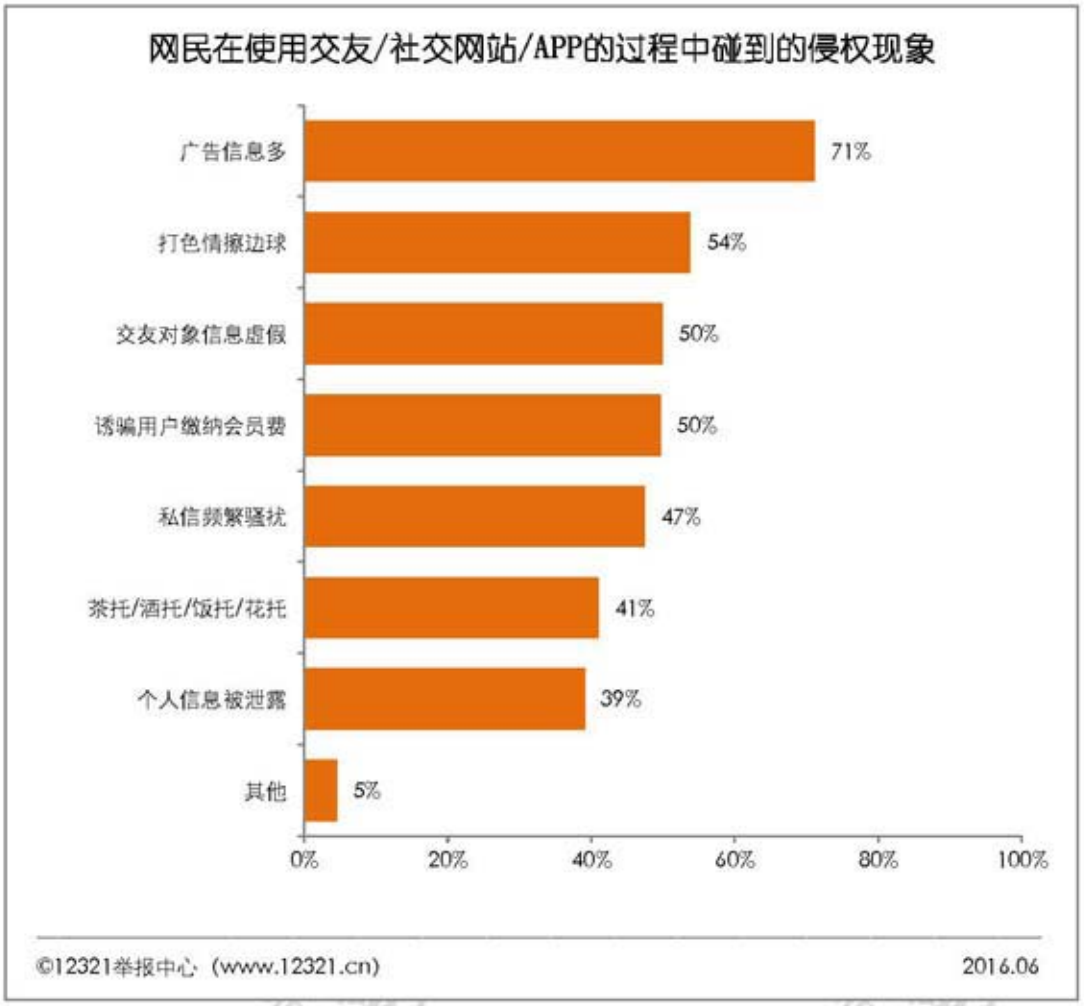
“个人信息被泄露”（占 36%）、“游戏账号被盗造成损失”（占 29%）、“游戏安装软件带有木马或病毒”（占 41%）是在玩游戏的时候存在的不安全现象。



7. 交友/社交网站/APP

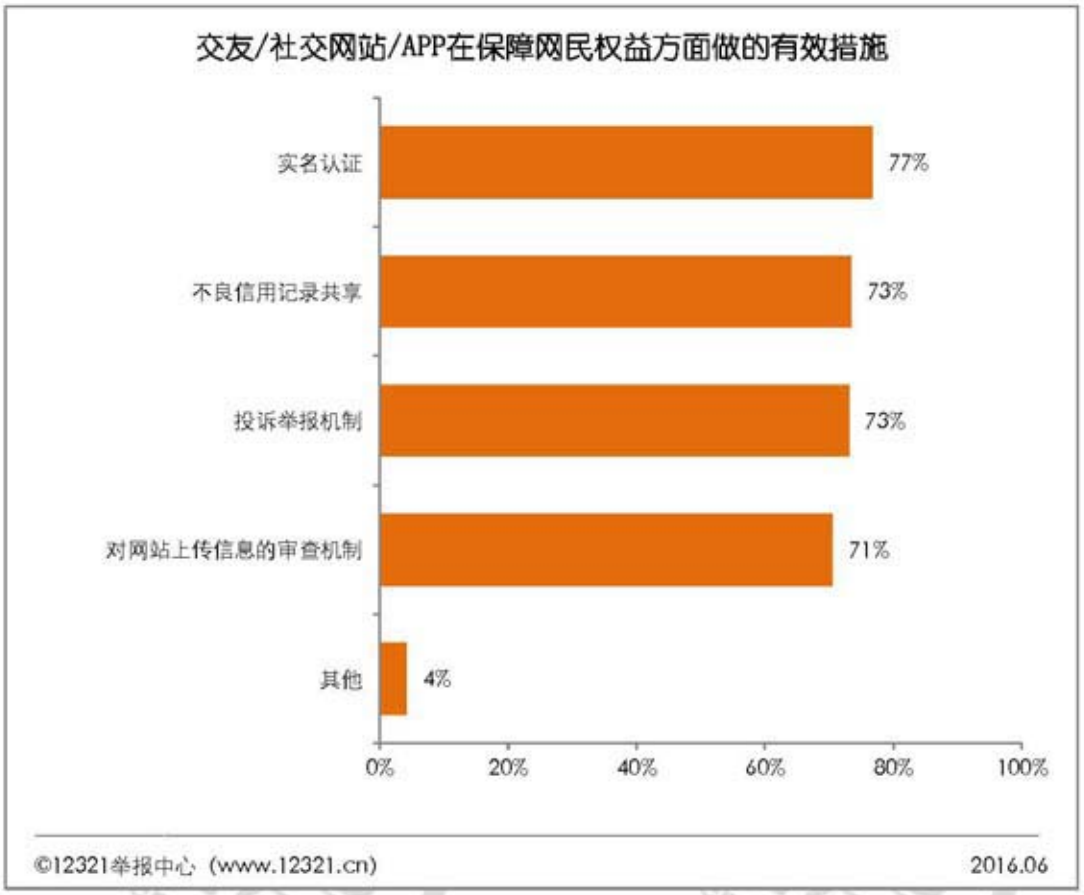
- **网民在交友/社交网站/APP 的使用过程中遇到的侵权现象**

在交友/社交网站/APP 使用中的侵权现象排名前三位的是：“广告信息多”占 71%；“打色情擦边球”占 54%；“交友对象信息虚假”、“诱骗用户缴纳会员费”并列第三，占 50%。



- **交友/社交网站/APP 保障网民权益的措施**

交友/社交网站/APP 所做的保障网民权益的措施，认可度都比较高，所占比例比较接近。排名依次为："实名认证"（占 77%）、"不良信用记录共享"（占 73%）、"投诉举报机制"（占 73%）、"对网站上传信息的审查机制"（占 71%）。



关于调查的情况说明

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 17 次中国反垃圾短信半年度调查、第 39 次中国反垃圾邮件季度调查、2016 年 1 月至 2016 年 4 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）举报的数据。

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、微信和微博，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：4 月 15 日~5 月 15 日。

整个问卷调查历时一个月，获得答卷 2856 份。

第四章 保护网民权益优秀实践案例汇编

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，中国互联网协会再次发起了保护网民权益创新&优秀实践案例征集活动。共收集案例 55 份。来自工信部、公安部、国家互联网信息办公室、国家互联网应急中心等政府和机构的领导、法律专家及新闻媒体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、保护网民权益方面的效果、公益性、创新性、社会影响等。经过评选，专家组认为，这些案例展现了互联网企业在保护网民权益方面的努力和举措，各具特色，均具有一定程度的推广普及价值。前 10 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。

案例 1：互联网金融一站式电子数据保全解决方案——无忧存证

A. 保护网民权益创新&优秀实践总体情况简介

无忧存证是安存科技旗下的互联网金融一站式电子数据保全解决方案，于 2015 年 2 月上线。

背景介绍：我国已经进入“全民互联网金融”时代，市场规模已达 10 万亿，用户数量达 4.89 亿，网民渗透率 71.91%。

但与此同时，跑路、非法集资、兑付危机等乱象丛生，2014 年，我国的 P2P 问题平台数量为 275 家，2015 年，问题平台数量飙升至 896 家。1 年的时间，问题平台增幅竟高达 226%。这些乱象大大损害了网民的合法权益，打击了网民的投资信心，网民在投资过程中遇到纠纷，维权难、成本高，谈互联网金融色变。

产品简介

无忧存证首创“金融安全级全数据生命周期电子数据保全体系”。

实时保全：交易各方产生的电子数据（电子合同、支付凭证、标的信息等）在产生的那一刻就通过无忧存证被保全下来。第一时间进行固化。

云端存储：保全的电子数据，会被同步传输至云端。确保电子数据不被篡改。

公证处出公证：全国 28 个省（市、区）200 多个地区的公证处将依法出具公证书。使得虚拟的电子数据可直观呈现。

B. 实践效果

无忧存证不仅有效保全了虚拟的电子数据，而且经无忧存证保全的电子数据是合法的、真实的，可作为呈堂证供，还原事实真相。

其彻底改变了此前互联网金融纠纷“取证难、确权难、维权难”的现状，被网民和媒体誉为“保障虚拟世界里的真金白银”。

仅 1 年时间，已经有近 200 家平台接入，4000 多万网民的权益得到有效保障。

保障消费者的合法权益：此前，消费者手中缺乏可直观呈现的、有效的凭证。无忧存证有效固化电子数据，生成保全证书，明确各方权利和义务。

降低维权难度和成本：互联网金融纠纷具有发生频率高、涉及范围广、处理相对复杂等特点，传统的事后维权取证成本高、维权难度大、维权效果差。无忧存证作为一种事前防范，大大降低了维权难度和成本。

提供多元化纠纷解决机制：无忧存证与公证处、法院、仲裁机构的合作，可为消费者提供多元化的纠纷解决机制，更高效、快捷、低成本地解决各类纠纷。

C. 网民反应

微贷网创始人姚宏：互联网金融的本质还是金融，风险的防范至关重要。携手无忧存证，为每一个投资者的交易过程做实时保全，是微贷网“打造诚信交易生态”的最佳实践。

汉金所 CEO 曾庆群：接入无忧存证可以让投资者更安心，更好地保障他们的权益。这对平台和投资者来说，是一个双赢的事情。

善金网总裁左云：善金网与无忧存证的合作，让网络借贷过程变得可追踪、可证明。无忧存证是互联网金融风控迈出的一大步，对互联网金融行业具有里程碑式的意义。

钱江晚报：无忧存证不仅能够证明投资者投资了多少钱，还能监督这个钱直接进入了政府项目账户，而并不是被平台截留。对于融资平台来说，自设资金池，投资者看不见投资方向往往是最可怕的地方。无忧存证会将整个交易过程数据实时同步至安存金融级数据保全云，所保全数据可在必要时依法申请出具公证书。也就是说，用户在入驻了“无忧存证”的互联网金融平台上发生交易行为之后，可以在该互联网金融后台查看电子数据保全证书。如果平台违约，投资者可以通过该后台选择公证处提交公证申请，向公证处预约出具公证书。

口贷网：口贷网此次与安存的合作将进一步强化对口贷网投资人权益的保护，不仅有助于防范和化解金融风险，同时也对提升投资人信心、维护 P2P 网贷行业安全与稳定具有积极意义！

网友：通过无忧存证，不管你在哪里，你都能实时了解到每笔投融资过程，不管任何时候，你都可以还原事实真相，不再担心口说无凭。无忧存证，保障的是投资者的权益，也是平台方的权益，它让投资者投的放心，让平台方因为第三方的介入，变得更具公信力。泥沙俱流的互联网金融行业，无忧存证看似一粒微小的明矾，却起到了滤清行业的作用。

D. 推荐理由

在互联网金融冰火两重天的背景下，无忧存证以中立的、第三方的身份保全交易过程中的电子数据，解决了电子数据“易变性、易改无痕性和不易呈现归档性”等固有缺陷，明确各方权利与义务，让虚拟的电子数据变得可追溯、可证明、可信赖。

无忧存证既保障了消费者的合法权益，又维护了整个行业的交易秩序，是互联网金融诚信生态不可或缺的一环。

公司简介

安存科技创立于 2008 年，公司以“打造诚信信息世界”为愿景，主营业务为“电子数据保全”。

安存首创“金融安全级全数据生命周期电子数据保全体系”，让虚拟的电子数据变得可追溯、可证明、可信赖。旗下八大产品系（语音保全系、邮件保全系、凭证保全系、合同保全系、版权保全系、电子政务保全系、医疗数据保全系、即时通讯保全系）深受用户喜爱。

2014 年，公司荣获 A 轮一亿元融资。

专家点评：

电子取证首当其冲，任何网络痕迹都可转化为呈堂公证，彻底解决网民取证难、难取证的问题。

案例 2：腾讯守护者计划

A. 保护网民权益创新&优秀实践总体情况简介

“腾讯守护者计划”是 2015 年腾讯公司成立的一个针对反电信网络诈骗的联合开放品牌。基于腾讯天下无贼反信息诈骗联盟丰富的实践经验，联合公安部全面升级。腾讯守护者计划将联动腾讯公司资源，包括 QQ、微信、腾讯安全云库、腾讯手机管家、腾讯安全平台部、腾讯安全管理部等相关产品或力量，发挥腾讯在大数据技术以及海量用户的优势，联合包括公安部、工信部在内的政府部门，与银行、运营商、互联网企业等对当前愈演愈烈的电信网络诈骗重拳出击。建立集用户教育、技术创新、行业联合、大数据共享在内的反电信网络诈骗体系，以实现构建移动互联网生态安全体系，保护网民权益的目的。

腾讯守护者计划涵盖三大部分，包括协助公安部进行犯罪打击的安全管理部门、国内首个反电信网络诈骗联合实验室、基于反信息诈骗联盟的行业联盟交流平台。2016 年 4 月，反电信网络诈骗联合实验室正式成立反电信网络诈骗专家智库，邀请行业专家组织联合智囊团为反诈骗献计献策。同时，推出了首个“诈骗热度指数”，基于大数据量化当前诈骗发生状况，以方便百姓预防。而反诈骗联合实验室首款大数据运用产品鹰眼智能反电话诈骗盒子，在深圳某运营商试用一年以来，帮助该运营商仿冒公检法类诈骗的损失金额下降 80%。

腾讯守护者计划三大特点：

1、海量用户资源，实现优质高效的用户教育，防范于未然。

腾讯拥有最大的亿级的互联网产品 QQ 微信，是国内实用最多影响和覆盖人群最广泛的互联网公司。通过打通腾讯内部的海量用户资源，具有将信息传达到相关的用户手中的先天优势。而反信息诈骗最关键的就是对用户教育，提升网民安全意识。腾讯可以通过相关渠道，建立最广泛的反诈骗教育平台，通过各种新颖的形式和及时的沟通防止用户在各种场景中被诈骗。

2、海量大数据加先进技术，实现用户行为的精准预判；

腾讯具有海量大数据运营经验，领先的大数据运营和分析技术，腾讯手机管家率先推出用户举报和标记功能，具有强大的大数据基础。基于此腾讯推出的诈骗电话检测系统，能够精准识别出正在遭受诈骗的用户，然后通过相关单位进行精准的提醒，有效阻止诈骗的发生。

除此之外，腾讯安全云库是全球最大的安全数据库，其能力在反诈骗上具有广泛的运用。包括，在诈骗 URL 识别拦截上，能够将能力输出给腾讯电脑管家、腾讯手机管家、手机 QQ、微信、以及各合作伙伴的浏览器、路由器等对恶意 URL 进行识别拦截；同时，能够帮助腾讯手机管家以及使用了手机管家拦截 SDK 的合作伙伴，提供诈骗短信识别的拦截、诈骗电话来电提醒和标记功能、诈骗木马的拦截和查杀。

3、行业联合，促进反信息诈骗产业合作

腾讯守护者计划联合公安、银行、运营商、各大互联网企业，推动反信息诈骗产业合作，将各自能力互通，资源数据共享，职能互补，实现在反诈骗上合作的创新，促进反信息诈骗的联动，协助有关部门重拳打击电信网络诈骗。同时，利用先进的科技手段和大数据技术，实现在技术上的解决方案，并且做出有触达性的反信息诈骗宣传教育，打造具有影响力的反信息诈骗生态环境。

腾讯守护者计划反电信网络诈骗手段：

1、鹰眼智能反电话诈骗盒子

腾讯基于大数据分析的精准识别系统，通过与运营商的合作，能够对正在遭受诈骗的用户进行识别，并且进行三级提醒。避免遭受诈骗损失。该系统在与深圳某运营商开展合作以来，该运营商仿冒公检法诈骗金额下降 80%。

2、反电信网络诈骗数据库

以腾讯安全所运营的“安全云库”为基础。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、诈骗短信样本库、诈骗木马库，以及全国首个恶意诈骗银行账号黑名单数据库，以“大数据”的方式增强对信息诈骗的防御能力。

以该安全数据库为基础，将能力应用于包括腾讯手机管家、腾讯电脑管家以及其他进行了能力合作的客户端产品内，能够有效对诈骗短信、客户端诈骗电话、诈骗木马、诈骗 URL 进行识别和拦截。

3、反电信网络诈骗联合实验室专家智库

面对这种新的反诈骗形势，腾讯守护者计划旗下的反诈骗联合实验室成立反电信网络诈骗专家智库，共同打造一个能够全面掌握信息诈骗形势，精确看清未来信息诈骗打击发展方向，有能力推动整个产业链合作的反诈骗智囊团。

反诈骗专家智库将集合互联网技术专家、公安专家、运营商合作伙伴专家、银行支付服务风控专家、警方一线反诈骗专家等，具有资深反诈骗经验或技术的专家团队构成。将为反诈骗的技术开发、情势预判、打击方式、法律建言等提供全面策略帮助。

4、诈骗热度指数

2016 年 4 月 1 日，腾讯守护者计划通过腾讯安全大数据平台所掌握的当期社会“诈骗行为”全流程的数据热度，通过综合评估诈骗行为流程中的多项因素（如诈骗分子数量、带来的信息与财产损失、用户主动举报等），进行综合计算后得出总体指数——“诈骗热度指数”。用以反映社会诈骗行为影响的严重程度，为广大从业者、用户提供一个实时的预警与风向标，提升行业与市场对诈骗行为的掌握程度。

5、标记和拦截诈骗电话号码

基于腾讯手机管家超过 8 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，对可以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。

6、反信息诈骗查询

基于腾讯安全平台部、安全云库的反信息诈骗数据库，民众可以快速获得对信息或数据的查询，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，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。同时，腾讯新闻客户端民生页面以及手机 QQ 城市服务 80 余座城市也可以看到这一功能，覆盖 3 亿人。

7、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，腾讯守护者计划与公安部刑侦局开展紧密合作，警企互动联手打击信息诈骗罪案。

8、反诈骗公益品牌宣传

腾讯拥有众多亿级用户产品，尤其是 QQ 微信是使用最多的软件之一。QQ 微信不仅提供着大数据的支持，同时也能够传导反诈骗用户教育。增强社会民众对信息诈骗的识别能力和防御能力，这同时也是守护者计划的社会使命。腾讯守护者计划将联合社区、公安等线下资源，QQ、微信、腾讯手机管家等线上资源，通过大数据报告、互动小游戏、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。

B. 实践效果

腾讯守护者计划成立了反诈骗联合实验室，首次推出大数据技术——鹰眼智能反电话诈骗盒子的运用。在深圳某运营商上使用，使改运营商的特定诈骗类型金额下降 80%。

警企民联动模式继续发挥作用，截止 2015 年 12 月 31 日，仅在深圳地区共接听市民来电 132 万余人次，咨询员直接劝阻 2.2 万余人避免被骗汇款，涉及金额达 1.8 亿余元，帮助 2.14 万名事主快速拦阻被骗资金 3.54 亿余元。避免、挽回群众损失合计近 5.34 亿元。

2015 年 9 月，腾讯守护者计划与深圳市公安局反诈办联合，在打击信息诈骗专项整治行动中，提供技术支持，协助深圳警方破信息诈骗案 91 宗，抓获犯罪嫌疑人 87 人，打掉犯罪团伙 10 个。2015 年 11 月-2016 年 1 月，在广东省公安厅破获“飓风 1 号”特大跨国电信网络诈骗案，腾讯守护者计划联动机制提供了技术支持，协助摧毁跨国电信网络新型犯罪窝点 5 个、制售伪基站窝点 4 个。2016 年 3 月，在深圳市公安局伪基站整治专项行动中，一个月协助打击伪基站团伙 8 个。

此外，在 2015 年 10 月，腾讯“反诈骗查询”功能在腾讯新闻客户端民生页面和手 Q 城市服务 30 个城市上线。民众同样可以通过该页面进行对诈骗信息的鉴别和举报。同年 12 月该功能已陆续上线至 80 余座城市，覆盖 3 亿人。全国联防的局面初步形成，查询举报通道的覆盖面覆盖也进一步加强了市民的安全防范意识。

C. 网民反应

网友评论：“腾讯守护者能够让我们感觉到安全。手机管家的拦截，QQ 微信的安全提醒，都能够帮助我们过滤到更多有害信息。”

网络安全专家评论：“腾讯公司整合了大数据资源，并且将自身产品的属性都带上反诈骗的功能，集合 QQ、微信、腾讯手机管家、腾讯电脑管家、安全云库等在内的各种产品，通过提醒、教育、拦截、标记等功能，不断强化网民安全意识，实时保护于无形。”

D. 推荐理由

腾讯守护者计划通过发挥互联网公司的技术和数据优势，通过与警方、银行、运营商建立合作平台，建立了包括犯罪打击、用户教育、技术创新等在内的新型反诈骗平台。从政策和平台创新上，促进了反电信网络诈骗的执行落地，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。

公司简介

腾讯是中国最大的互联网综合服务提供商之一，也是中国服务用户最多的互联网企业之一。腾讯安全拥有 16 年能力积累及 8 亿用户海量大数据运营经验，是中国最为领先的互联网安全产品、安全服务提供者，为中国互联网用户提供全方位的安全保障服务。本着“开放、联合、共享”的理念，腾讯安全将多年积累的能力和数据共享给合作伙伴，并且始终致力于互联网安全开放平台建设，提升互联网安全产业链安全能力，提升用户安全意识，共同推进中国互联网安全环境的建设，为洁净中国互联网环境而努力。

专家点评：

大企业占了较大市场份额，掌握先进的技术与大量数据，与其他各平台合作，必然会产生很大的影响力。

案例 3：华为 Mate8/P9 手机基于麒麟 950/955 芯片的防伪基站功能

A. 保护网民权益创新&优秀实践总体情况简介

近几年，骚扰短信越来越成为手机用户深恶痛绝的首要烦恼，更严重的是通过伪基站发送的诈骗短信特别具有欺骗性，导致造成用户经济损失的事情层出不穷。为了解决这个痼疾，华为利用其麒麟 95x 芯片解决方案的技术优势，推出了协议级防伪基站功能，并在 HuaweiMate8、P9 等手机上搭载。该功能可以在手机侧有效识别伪基站的场景，确保手机不会驻留在伪基站上，从源头上杜绝从伪基站来源的垃圾短信、诈骗短信，确保用户的隐私数据不被侵犯，避免发生不必要的损失。

B. 实践效果

华为 Mate8、P9 等机型上市后，其芯片协议级防伪基站的功能得到了用户的一致好评，有效杜绝了来自伪基站的垃圾短信，使用户获得了一个更加干净的手机使用环境，而那些伪装成银行、运营商的诈骗短信更加不会出现在用户手机上，确保了网民的隐私和金融安全。

C. 网民反应

使用 HuaweiMate8\P9 等手机后，再也没有标榜着运营商、银行等号码的垃圾短信的骚扰了，手机使用起来更加放心舒心。

D. 推荐理由

防伪基站功能从芯片层面识别出伪基站，并通过技术手段确保移动终端不会驻留到伪基站上面，将诈骗源头的垃圾短信拒之门外，从根本上切断了犯罪分子利用伪基站进行诈骗的途径，是移动终端领域的技术创新。在终端侧对伪基站的杜绝起到了相当重要的作用，也值得业界进行推广学习。

公司简介

关于华为消费者业务：华为的产品和服务遍及 170 多个国家，服务于全球 1/3 人口，其 2015 年的全球智能手机出货量位列第三，在美国、德国、瑞典、俄罗斯、印度及中国等地设立了 16 个研发中心。消费者业务是华为三大业务之一，产品全面覆盖手机、个人电脑和平板电脑、可穿戴设备、移动宽带终端、家庭终端和终端云。基于华为二十多年通讯行业的深厚沉淀，凭借自身的全球化网络优势、全球化运营能力和全球化合作伙伴，华为消费者业务致力于将最新的科技带给消费者，让世界各地更多的人享受到技术进步的喜悦，以行践言，实现梦想。

专家点评：

此做法为一个底层性的创新，在芯片技术方面有很大突破，保护了网民权益、维护了网络安全。我国网络安全问题的解决确实需要有大的民族企业的参与进来。

案例 4：百度与最高人民法院合作上线失信被执行人查询平台 一键查“老赖”名单

A. 保护网民权益创新&优秀实践总体情况简介

随着互联网的快速发展，因信用而产生的问题也日益突出。百度全面接入最高人民法院的失信被执行人数据，上线“全国失信被执行人名单”信息查询平台，网友可通过百度一键查询包括自然人、法人或其他组织在内的 3 万余例失信被执行人的详细信息。这是业内首个接入最高人民法院数据的互联网信用监督平台，使信用信息更加透明化的同时，也进一步促进了互联网诚信体系的建设。

B. 实践效果

网友直接在百度搜索自然人的名称，如果存在失信行为，页面右侧会出现百度的提醒，网友也可点击查看详情，或查看详细的“全国失信被执行人名单”；网友也可输入法人或其他组织的名称，如果有失信情况，会在结果页最上方显示百度的提醒“XXX 公司由于失信已被列入国家失信被执行人名单”。对于与陌生企业有生意往来的商家，可通过此办法一键查询合作伙伴是否为“老赖”。

据悉，自百度“全国失信被执行人名单”信息查询平台开通后，企业查询平均点击率达 38%。数据显示，企业名单数量上周开始有明显的下降趋势，一些企业发现自己位于名单之上，已经主动向金融机构偿还所拖欠资金或贷款。一旦企业履行了相关义务后，其企业名称会跟随最高人民法院一并下线。

图示：

C. 网民反应

失信被执行人名单制度，是对失信被执行人的信用惩戒。百度上线查询平台将政务信息公开、透明化，有效借助了互联网的全民监督优势，促进政务工作更高效地进行。

D. 推荐理由

这项举措在积极推动失信被执行人依法履行义务的同时，也促进了整个行业的诚信体系建设。

公司简介

百度公司于 2000 年成立于北京中关村，经过十六年时间的发展，现已成为全球最大的中文搜索引擎和中文网站。百度公司业绩增长迅猛：2015 年公司营收超 663.82 亿元，同比增长 35.3%。目前公司员工近五万人，其中工程师占比超过三分之一。

百度公司利用自身的平台优势，以技术创新为驱动力，在促进产业转型升级、扶持中小企业发展、引领核心科技进步、消弭知识传播鸿沟等方面发挥着越来越重要的作用。百度未来的发展目标是：到 2020 年，发展成为世界互联网的创新中心；将百度打造成在全球一半以上互联网市场中家喻户晓的品牌；代表中国企业在全球经济中发挥影响力。

专家点评：

因最高法具有一定的公信力，与最高法合作，网民的信任能力将会大大增加。此举具有一定的推广示范效应，若最高法与所有的搜索引擎企业合作，将会取得更好的效果。

案例 5：锋尚 MAX 双系统

A. 保护网民权益创新&优秀实践总体情况简介

安全双系统作为酷派的一项具有里程碑意义的技术，不仅将手机的安全性能提升至前所未有的高度，也从根本上解决了用户信息安全的使用痛点。私人空间属于完全独立、封闭的安全系统，保障用户的私隐信息不被泄露，用户可在这个空间放心进行金融方面的操作。同时，进入安全系统需要验证指纹或者密码，既确保了财产安全，又保障了安全系统免于病毒侵害。用户信息安全、隐私安全就得到更好的保证。

B. 实践效果

可在私密的安全空间进行支付等金钱交易，防止被恶意盗刷，财产更安全；一部手机两个微信号，信息资料放在安全空间，防止他人窃取，保护个人隐私；安全空间的 APP 都是通过官方安全认证，安全杜绝第三方软件侵入，保障资金信息安全。

C. 网民反应

双微信：一个手机两个账号，互不干扰，工作和生活分开，保护个人隐私

支付安全：在安全空间进行交易支付，防止恶意盗刷，更放心

下载软件：不明链接根本无法下载，安全空间下载软件均为官方安全认证，从根本上杜绝第三方软件侵入

D. 推荐理由

酷派锋尚 MAX 在 2016 年 1 月的美国 CES 展上荣获“2015 全球智能手机信息安全金奖”

公司简介

酷派(Coolpad)是宇龙通信公司的手机品牌。宇龙通信公司全称"宇龙计算机通信科技(深圳)有限公司"，创立于 1993 年 4 月。

系酷派集团有限公司(香港主板上市公司，股票代码 2369)的全资附属子公司，是中国专业的智能手机终端、移动数据平台系统、增值业务运营一体化解决方案提供商，专注于以智能手机为核心的无线数据一体化解决方案，并致力发展成为智能手机领导者与无线数据行业应用专家。

专家点评：

双系统对网民来讲较好，此系统对支付、个人隐私等均有一定的保护作用。

案例 6：爱路由

A. 保护网民权益创新&优秀实践总体情况简介

1、保护网民权益的创新：儿童上网专用的路由器，做到了管理孩子规律上网，手机远程管理网上内容，做到 7*24 小时安全陪护。

2、总体情况：现在 00 后的孩子，上网、打游戏，变成了他们生活中不可分割的一部分。家长在担心孩子上网过度，会导致学习下降、近视、驼背等外，更担心孩子受到上网色情、赌博、诈骗等不安全因素的影响，我们公司推出这款产品，内置安全联盟，屏蔽色情、暴力、赌博、诈骗、钓鱼网站，时刻守护家庭网络安全。

B. 实践效果

的确可以了解到孩子的上网习惯，行为记录。通过这些来了解、管理孩子。外加安全联盟卫士。真正做到了 24 小时完美关怀。

C. 网民反应

我们 80 后，每家每户都是独生子女。孩子就一个，家里四位老人宠着，想干什么干什么；孩子没有树立自己的识别能力；很担心他现在狂妄自大的心态，会被网上不好的信息所影响。如果能知道孩子在网上浏览什么、玩什么类型的游戏、有没有早恋倾向等，我可以更好的了解他，管理他。

D. 推荐理由

触云做爱路由不是为了监控，而是呵护；我们设计的方案是让爸妈了解小孩，关爱小孩，每天父母都很忙，没有时间去了解孩子；强化了解通道，不是强加管理的通道；了解更多的时候，父母给出关爱。我们会提供更多的措施让小孩子在网上安全学习、娱乐。

公司简介

深圳触云科技有限公司成立于 2014 年 10 月，是国内首家专注于智能路由 OS 生态，提供个人数字画像的大数据服务公司。触云智能路由器 OS 及云端服务解决方案，助力合作伙伴加速产品智能化进程，融入智能生活生态圈。应用大数据支撑智能网络管理与应用，获取更多的业务价值。提供网络系统安全保障，为 IoT 智能家居设备提供稳定安全联网服务。

专家点评：

儿童上网专用路由器，管理儿童上网，屏蔽色情、暴力等不良内容。对网民尤其是家长，可以了解孩子上网情况、规避其所担心的问题。

案例 7：域名不良应用治理——净化网络环境、保护网民权益

A. 保护网民权益创新&优秀实践总体情况简介

中国互联网络信息中心（以下简称 CNNIC）发挥长期积累的国家域名注册管理经验，多头并举开展域名不良应用治理工作，通过停止域名解析等治理手段实现净化网络环境，保护网民权益的目的。

2008 年 7 月 18 日 CNNIC 牵头成立中国反钓鱼网站联盟（以下简称 APAC），由国内银行证券机构、电子商务网站、网络安全企业、域名注册管理机构、域名注册服务机构、专家学者等共同组成，是国内唯一为解决钓鱼网站问题而成立的公益性协调组织，目前拥有会员单位 500 多家。

2009 年 12 月以来，CNNIC 结合国家深入整治互联网和手机淫秽色情及低俗信息专项行动，开展国家域名注册信息核验专项行动，从注册源头遏制不良域名的产生。同时建立域名不良应用公众举报及外延合作处理机制，结合自主研发的域名不良监测技术平台，实现权威高效处置域名不良应用信息，有力维护互联网的健康环境，实现保障网民权益的目的。

B. 实践效果

APAC 自成立以来累计认定并处理钓鱼网站 278,693 个，仅 2015 年认定并处理的钓鱼网站达 58,660 个，其中涉及 CN 域名的钓鱼网站有 2,317 个，占钓鱼网站处理总量的 3.95%。钓鱼网站的主要钓鱼对象包括淘宝网、工商银行、建设银行、平安集团、Paypal 等各大电子商务和金融服务平台以及浙江卫视、湖南卫视等媒体传播平台。通过 APAC 的协作共治，极大限度的保护了网民利益，成为国内打击网络钓鱼欺诈的中坚力量。

CNNIC 设立社会监督举报热线，7×24 小时受理公众对于域名不良应用的举报，联合相关单位和广大网民一起全力封堵国家域名不良应用。自开展域名不良应用治理专项行动始，CNNIC 累计处理涉及淫秽色情、网络赌博、枪支弹药、毒品、爆炸物五大类国家域名不良应用 19,318 个，其中 2015 年认定并处理的国家域名不良应用 10,212 个。CNNIC 不良应用域名的处理时间从 6 个工作日降低到 2 个工作日，大幅提升了不良域名的处理效率，大大减少了不良域名的网络危害。CNNIC 开展的域名不良应用治理为保护未成年儿童健康绿色上网，保护国家网络安全，净化网络环境起到积极促进作用。

C. 网民反应

网民：淫秽色情网站严重侵害小孩子的身心健康，作为一名孩子的家长，我举双手赞同关停色情网站，给孩子创造一个健康上网环境。

举报用户李先生：凌晨上网发现一个赌博网站，抱着试试看的态度打电话给互联网中心举报，没想到竟然真有人接，最出乎意料的是网站今天竟然已经被关闭了。为互联网中心点赞！为接听电话的小妹点赞！

小文（网友）：遭遇钓鱼网站不可怕，一定要向 APAC 举报，分分钟搞定。让我们身边的爷爷奶奶、叔叔阿姨都不受网络诈骗的危害。

D. 推荐理由

在利益驱动下，不少网络平台都存在以“色情”、“暴力”等低俗内容吸引人气的现象，严重影响了未成年人的身心健康成长。同时钓鱼网站的频繁出现，也阻碍了在线金融服务、电子商务的发展，严重危害公众权益，影响公众应用互联网的信心。CNNIC 作为国家域名的注册管理机构，主动肩负起“净网”的庄严使命，积极承担社会责任和义务，不断深化“净网”专项工作开展，成效显著。

公司简介

中国互联网络信息中心（CNNIC）作为中国信息社会重要的基础设施建设者、运行者和管理者，在“国家公益、安全可信、规范高效、服务应用”方针的指导下，负责国家网络基础资源的运行管理和服务，承担国家网络基础资源的技术研发并保障安全，开展互联网发展研究并提供咨询，促进全球互联网开放合作和技术交流，不断追求成为“专业•责任•服务”的世界一流互联网络信息中心。

专家点评：

从注册源头遏制了不良域名的产生，通过停止域名解析等治理手段实现净化网络环境、保护网民权益的目的。

案例 8：网络安全战车

A.保护网民权益创新&优秀实践总体情况简介

网络安全战车是在网信办、教育部、团中央的指导下，360 公司为青少年精心打造的全国首个网络安全科普流动基地，同时集合了 AR、VR、4D 体感、语音识别、跨屏联动、大数据可视化等最新融合了各种网络安全知识，打造近 10 个互动体验项目，将寓教于乐做到极致！目前战车已申请 17 项国家专利！网络安全战车将最先进的高科技体验技术与网络安全知识相融合，通过这样一个好玩的互动体验形式，让孩子乐于主动去学习网络安全知识，提高自身网络安全意识。同时，配合网络安全战车也会举办青少年信息安全比赛，选拔网络安全人才。

B.实践效果

网络安全战车中国行于 2015 年 12 月 25 日正式启动，截至 2016 年 4 月 22 日已覆盖北京、河北、河南、山东、天津等 5 个省市，石家庄、衡水、郑州、济南、青岛等近 20 个城市；前来参观体验的学生覆盖 300 余所学校、30000 余人次。青少年网络安全教育工程为 100 所学校授予“网络安全教育示范基地”称号，并建立长期友好合作关系；累计培训 1000 余名辅导员。央视、各地方卫视等近百家媒体持续进行跟踪报道。

网络安全战车巡展期间还配合了国税安全周、网警爱民行等活动。429 首都网络安全日后，还将驶向江苏、上海、广东等近 10 个省市、100 多个市县进行巡展，惠及全国千所学校、上百万名青少年。

C.网民反应

网络安全战车上不仅拥有炫酷的外形，还可以自动变形，十分炫酷。车内也有 AR、VR、4D 体感游戏、语音识别等科技感十足的项目，能够与网络安全知识相融合，以这样以方式来向广大青少年传播网络安全知识，会有效的提高他们的自我防护能力。确实是一个靠谱的网络安全科普流动基地。

D.推荐理由

网络安全战车是在网信办、教育部、团中央的指导下，360 公司为青少年精心打造的全国首个网络安全科普流动基地，在 2016 年计划到全国 10 个城市进行巡演。因为流动性强，与各地的网络安全科普基地互补，就像流动的广告牌和基地，网络安全战车将最先进的高科技体验技术与网络安全知识相融合，通过这样一个好玩的互动体验形式，让孩子乐于主动去学习网络安全知识，提高自身网络安全意识。目前战车已申请 17 项国家专利，将寓教于乐做到极致！

公司简介

360 公司（美国纽约交易所：QIHU）是中国领先的个人电脑，移动终端和企业级安全产品及服务提供商。其首创的“免费安全”模式曾被西方媒体誉为互联网的“中国模式”。360 公司坚持颠覆式创新的企业文化和用户至上的价值观，不断通过产品技术创新、用户体验创新和商业模式创新改变市场格局，保护用户权益，推动市场进步。

专家点评：

全民参与，精心为青少年打造，将 AR、VR、4D、语音等于网络安全知识融合，将网络安全教育与网络安全知识的普及做到极致。

案例 9：联合 58 同城“打击虚假兼职，黑职介”

A. 保护网民权益创新&优秀实践总体情况简介

4.29 首都网络安全日，知道创宇运营的安全联盟联合 58 同城发起了“打击虚假兼职，黑职介”活动，双方共同设立了防骗举报专区，接受全民对于虚假招聘信息的举报，并对该类欺诈网址、QQ 号等进行拦截预警，全方位、多渠道地打击网络“黑招聘”，保护网民权益，规范网络求职环境。

B. 实践效果

活动开展仅一周，就接受网民各类举报 1386 条，日均举报 198 条，安全联盟迅速将发布虚假招聘信息的网址、QQ、微信列入安全联盟恶意数据库，同时同步给合作伙伴处理。并将这些数据同步到 QQ 浏览器、搜狗浏览器、YY 浏览器、腾讯 QQ 等互联网主流应用进行拦截预警，为网民建起防护屏障，重拳打击侵犯求职者利益的网络欺诈行为。

C. 网民反应

（1）自己着急找工作却误入了一个虚假招聘网站，被骗了不少钱。看到安全联盟这个举报专区后，我马上对这个网站进行了举报，之后我便发现此网站被 QQ 和 QQ 浏览器所拦截，想到自己被骗的经历能够通过这种方式来帮助其他人免受欺骗，心里安慰不少。

（2）我是个全职妈妈，在网上看到招聘打字员，每天只需在电脑上工作几小时就能日赚千元，自己头脑发热就相信了，损失了 3000 多元。看到安全联盟这个活动觉得非常好，马上就对发布信息的 QQ 和网站进行了举报，希望这个活动能够坚持下去，坚决打击这些可恶的骗子。

（3）我是一个大学生，在一个 QQ 群里看到了招聘刷单员的兼职，自己受高薪诱惑便进行了尝试，但刷了两单后我便感觉自己受骗了，于是便到活动举报专区对骗子的 QQ 号进行了举报，第二天我发现这个 QQ 号已经被清除掉了，感觉心理特别解恨，也觉得自己为网络安全贡献了一份小小的力量。

D. 推荐理由

（1）活动旨在解决当下的热点问题：目前，网络招聘的黑色产业链年产值已高达 1100 亿元，从业人数近 160 万人，已经成为极大的社会隐患，活动在解决这一社会热点问题上进行了全新尝试。

（2）活动形成了协作共赢的联防联控机制：安全联盟作为公益组织与生活服务平台 58 同城进行合作，共享反信息诈骗数据库，对侵犯求职者利益的欺诈行为起到了重拳打击效果。

公司简介

安全联盟（www.anquan.org）是国内最大的网络安全数据共享交换平台，致力于团结互联网企业及行业机构建立行业公认的互联网安全标准，构建有效的网络安全社会化治理体系。目前，安全联盟已建立起超过 8 亿条的恶意网址数据库，拥有腾讯、搜狗、百度、金山等合作伙伴 120 余家，每日与合作伙伴进行 5500 万次数据交换。通过将恶意网址共享同步至合作平台的各大互联网终端，以每天 30 亿以上的安全风险提醒，为广大网民避免了难以估计的巨额经济损失。

专家点评：

网上、网下联动，细分化做得较好，保护了网民权益，是一个较好的案例。

案例 10：电信运营商联手互联网企业防范骚扰诈骗电话

A. 保护网民权益创新&优秀实践总体情况简介

背景：近年来，通过电话进行诈骗的案件频发，有电话欠费诈骗、中奖诈骗、汽车退税诈骗、冒充熟人诈骗等等，诈骗分子还紧跟社会热点设计骗局，让广大网民防不胜防，带来生活上困扰和财产损失。

应对方案：百度等安全企业将骚扰诈骗号码的数据库分享给中国移动、中国联通、中国电信，用户在接收到骚扰、诈骗电话的来电时，电信运营商会通过闪信的方式进行弹窗提醒，提醒用户谨慎接听，从而有效降低用户被骗案件的发生。

B. 实践效果

百度安全与中国移动、联通开展合作以来，免费开通该服务的用户近 2 亿，每日为用户弹窗提醒 400+万次，月度提醒上亿次。据统计，电话诈骗的案发率下降 60%，有效遏制了电话诈骗案的高发势头，取得了显著的效果。

C. 网民反应

自从运营商开通防骚扰诈骗服务，每个人都是火眼金睛，再也不担心上当受骗，不论安卓用手机还是苹果手机都可以体验，感谢互联网企业与运营商背后做出的努力和付出，点个赞。

D. 推荐理由

互联网企业和运营商的强强联手，是从国内用户的实际痛点出发，以全新的功能服务解决了用户在移动端上的安全需求，并从根源上就切断了电信诈骗的通路，防止用户上当受骗。

专家点评：

大企业与运营商强强联合，充分发挥其价值，也是其责任的体现。此模式今后有可能成为常态。

案例 11：“联合全国 40 省市消协打击网络欺诈”实践活动

A. 保护网民权益创新&优秀实践总体情况简介

由知道创宇运营的安全联盟联合全国 40 省市消协（消委会、消保委）、中国消费者报社、中国消费网共同开展“打击网络欺诈，确保消费安全”活动，通过设立联合举报专区，对接双方举报平台，共享诈骗信息数据库，整合双方线上线下的能力，共同打击网络诈骗，为广大网民营造安全的网络消费环境。

B. 实践效果

从 2015 年 10 月份活动启动开始，截至到 2016 年 2 月底，联合举报专区共接收 85173 条举报，月均举报 21293 条，39039 条欺诈网址、电话等被列入安全联盟黑名单，通过同步到腾讯、搜狗、金山等互联网终端进行拦截预警，为广大消费者避免经济损失达 400 多万。

2016 年 3.15 期间活动方联合发布的《“打击网络欺诈，确保消费安全”分析报告》获数百家媒体发布转载，极大提高了网民的整体反欺诈意识。

C. 网民反应

（1）当我将欺诈网站举报后，很快就能看到它在 QQ 聊天窗被标记成红色风险网站，让自己有一种打击网络犯罪的成就感，也感觉在网上多了一分安全感。这种发动全民参与举报的活动形式，能够更好地打击网络欺诈行为，更好地保护我们的合法权益。

（2）自己平常喜欢网上购物。有一次，骗子冒充客服以商品缺货需要退款为由，让我点击一个链接填写信息进行退款。当我用搜狗浏览器打开链接时，浏览器提醒我这是一个钓鱼网站，这时我才反应过来可能是遇上了诈骗。幸好有安全联盟的风险提醒，才让我避免了损失。

（3）我曾经在网络购物时遭遇过诈骗，自己非常懊恼，并且这些欺诈网站始终没能被“消灭”，不断地还有更多人上当受骗。安全联盟的这个活动，形成了“多平台反网络欺诈

联动体系”，被举报并确认为欺诈网址的，都会被“全网拦截”，同时我们的举报还会汇集成有效情报供消协进行线下查处，的确为我们网民消费权益建立起了一道防护墙。

D. 推荐理由

（1）活动影响度大：联合了全国 40 省市消协，中国消费者报社、中国消费网，在全国各地都产生了较大影响力，出品的相关分析报告获数百家媒体发布转载；

（2）活动参与度高：来自全国各地的网民贡献了 8 万余条举报信息；

（3）活动效果良好：近 4 万条欺诈网址、电话等被列入安全联盟黑名单，并被国内数十家主流互联网应用平台所采用进行拦截预警，对保护网民权益起到了有力作用；

（4）活动实现了线上线下能力的有效整合：安全联盟对恶意网址的阻断能力在活动中得到了延伸，而消协则实现线下处置消费者投诉纠纷，线上维护消费者权益的有机整合，为“构建社会化的网络安全治理体系”摸索出了一条切实可行的道路。

案例 12：中国移动通讯信息诈骗治理实践

A. 保护网民权益创新&优秀实践总体情况简介

近年来，通讯信息诈骗层出不穷，已成为全社会关注的信息安全焦点问题。据公安部统计，2011 年以来，我国通讯信息诈骗案件年均增长 60%以上；2014 年，全国发案 50 余万起，造成损失 100 多亿元；2015 年，全国发案 59 万余起，造成经济损失月 222 亿元。

为维护广大人民的合法权益，在上级单位指导下，中国移动持续开展防范打击通讯信息诈骗相关工作。针对来自“国际、网间、网内”不同源头的诈骗电话，形成一整套治理方案。针对国际诈骗电话：提出“识别＋取证＋拦截”的治理思路，2014 年 9 月在浙江试点建设国际诈骗电话监控平台，目前已覆盖 31 省网间关口局和北京、上海国际关口局；针对网间虚假主叫和语音群呼类骚扰诈骗电话：一方面利用虚假主叫管控平台对网间虚假主叫进行拦截，另一方面利用骚扰电话集中管控平台开展全网监测，并利用人工回拨取证及投诉数据分析的方式开展集中研判，对确认违规号码实现一键加黑/关停；针对网内改号风险，一方面对语音专线开启主叫白名单功能，仅允许在白名单内的号码发起呼叫，定期开展基于计费错单的 PBX 白名单稽核工作，确保白名单的正确性和有效性，同时在关口局上开启主叫号码强制显示功能，防范隐藏主叫号码的违规呼叫；另一方面加强手段建设，在全国 31 省开展语音专线集中管控平台的建设，对语音专线实现集中管控。

B. 实践效果

截至 2016 年 3 月底，实现月均拦截国际诈骗电话 2600 余万次，全国 31 省用户周平均国际诈骗电话投诉量比拦截前下降超过 90%；月均拦截网间虚假主叫 4400 余万次；月均发现处置“响一声”电话月 19 万个，研判网间语音群呼类疑似骚扰诈骗号码 42 万余个，处置违规号码 8.8 万余个；同时，中国移动率先建设技术手段，向用户免费提供涉嫌通讯信息诈骗来电号码提示服务，目前已覆盖 18 个省的 4700 余万用户，后续将在全国范围内进一步推广。

C. 网民反应

中国移动开展防范打击通讯信息诈骗工作，切断了犯罪分子的诈骗渠道，保障正常通信秩序，营造清朗网络空间，有效遏制电信网络新型违法犯罪发展蔓延势头，切实维护人民群众财产安全和合法权益，切实维护社会和谐稳定。

D. 推荐理由

一是“打得快”。坚持第一时间开展全网动员与部署，在打击治理工作方面争锋多秒，始终“跑在前面”。二是“打得准”。坚持“突出重点、问题导向”，重点围绕业务安全以及骚扰诈骗电话、“伪基站”、“黑卡”、恶意软件等焦点、热点问题有的放矢地推进治理工作。同时，公司持续健全技术手段，针对不同源头的诈骗电话，初步形成了“国际拦截、

网间联动、网内严打”的打击治理流程。三是“打得狠”。始终保持高压态势，月均拦截国际改号诈骗电话约2600万次，研判网间语音群呼类疑似骚扰诈骗号码42万余个，处置违规号码8.8万余个，整体取得了较为显著的治理成效。四是“打得实”。坚持“建常态、抓长效”，将打击治理工作纳入省公司考核体系，并定期开展自查、抽查，力促相关工作的常态化与机制的长效化，确保问题不反弹。

中国移动作为负责任的国有企业，一直高度重视防范打击通讯信息诈骗工作，按照公安部、工信部等部门的工作部署，紧密围绕“突出重点、技管结合、落实责任、标本兼治”的总体思路，深入落实“打击治理电信网络新型违法犯罪”专项行动的各项工作，全力保障人民群众的合法权益。

公司简介

2011年11月，中国移动通信集团公司在原信息安全管理部的基础上成立了信息安全管理与运行中心，归口全集团信息安全管理与不良信息治理，负责开展不良信息集中治理与信息安全集中运营，实现了信息安全工作的“两归口、两集中”。中心自成立以来，在行业内开创了不良信息集中治理新模式，创造性实现了全国“一盘棋”的信息安全工作格局，治理对象涉及垃圾短彩信、手机淫秽色情信息、“响一声”电话、手机恶意软件、“伪基站”、电信诈骗等多个方面，工作范围覆盖内容安全、基础安全、业务安全、客户信息安全、终端安全等多个领域。

案例13：奇未安全桌面

A.保护网民权益创新&优秀实践总体情况简介

奇未安全桌面是针对低年龄的青少年开发，可以有效拦截黄、赌、毒、诈骗网站等不良信息，该功能基于360海量的DNS数据解析，保证精准拦截，是行业首创的创新性安全防护产品。同时，奇未安全桌面聚合了多家正版、独家、免费的全国顶尖教育资源，打造青少年同步学习平台。不仅与此，桌面还聚合多样的全国顶尖娱乐资源，将寓教于乐做到极致；并且，奇未安全桌面添加的人工智能操作系统，打造全新亲子上网陪护模式。是新一代的儿童上网生态平台。

B.实践效果

奇未安全桌面以360搜索提供数据库支持，500万条数据信息，实时更新含有黄色暴力内容的网址及DNS信息，通过360安全浏览器24小时保护孩子安全上网，实现对不良信息网站的实时、动态、精准查杀；还汇聚价值3000万元的新东方、学而思、简单学习网、未来网等免费、独家、正版的顶尖教育培训资源；青少年可以在奇未安全桌面根据自己的年级进行同步学习，同步课程教材覆盖人教版、苏教版等全国各地多种版本；在娱乐方面，桌面聚合了价值1500万元的网易云音乐、酷米网、未来网、4399游戏等精心挑选的优质儿童娱乐内容；定制化推出青少年专属的无广告、免费、独家、正版的电影、视频、动漫资源。从2016年1月上线至今已经已覆盖北京、河北、河南、山东、天津等5个省市，石家庄、衡水、郑州、济南、青岛等近20个城市，现在日活已经达到了30万，确实把寓教于乐做到极致。

C.网民反应

奇未安全桌面下载了可以保护孩子安全上网，把带有不良信息网站都给拦截掉；又集合了很多网站上的教育机构培训资源，人教版、苏教版等教材都可以用，使用起来特别人性化；同时还包括了很多儿童类的游戏、电影等资源。让孩子在娱乐的同时又学习到了知识，确实做到了让孩子“安全上网，健康成长”，是一个很有良心的保护孩子上网安全的软件。

D.推荐理由

奇未安全桌面集学习、社交、娱乐、购物一站式体验，寓教于乐，全新起航；同时涵盖了海量优质资源，学而思等多家网校入驻，轻松实现同步教学。通过家长设置密码，可查看孩子上网浏览记录对孩子上网时长进行设置，有效控制孩子上网时间；家长还能参与举报不良信息，为孩子搭建一片零污染的网络环境。是孩子安全上网的“守护神”

案例 14：AppleID 重要邮件来邮自动提醒

A. 保护网民权益创新&优秀实践总体情况简介

2015 年期间，国内发生了多起由于 appleID 被盗进而被黑客锁机勒索的事情，网民的经济利益受到了严重的侵犯。我们对黑客的手法进行了分析，发现黑客的其中一个手段是通过撞库的方式获得某些 appleID 对应邮箱的登录权，向 apple 发起修改密码申请，apple 会向用户的邮箱发一封含有修改 appleID 密码的邮件，然后黑客就是通过这封邮件修改了用户的 appleID 密码继而对用户进行锁机勒索行为。

得知这情况后，我们马上上线了响应的保护措施，当用户邮箱里面收到来自 apple 的跟帐号有关的邮件时候，我们会马上发送手机短信通知用户本人，用户可以马上获得消息。如果 appleID 的修复不是他本人操作的，他可以第一时间联系苹果客服申请进一步的保护措施，从而保护他的 appleID 不受侵犯，也有效地避免了之后被锁机勒索的事情发生。

B. 实践效果

从上线到现今，已经成功让超过 2100 万的网民第一时间获知 apple 有关帐号变动来邮信息，其中有被盗风险的用户大部分也第一时间联系 apple 申请了更高级别的帐户保护操作，避免了进一步的经济损失，所以这项措施也广受用户赞誉。

C. 网民反应

收到过短信通知的网友都对这项措施赞誉有加。有网友在论坛表示：“之前听说过苹果帐号被盗导致手机被锁的事情，所以就根据官方建议到苹果网站开启两步验证。操作过程中，苹果发送通知邮件到我的邮箱时，我同步收到了网易邮箱发来的短信，提示说我的帐号信息正在被修改。这真的很贴心啊，假设我的帐号是被黑客修改，我能够及时收到短信提示，及时给苹果打电话，应该就可以避免帐号被盗了。网易邮箱在这方面的工作做得还是挺细致的。

“我有几个朋友的 apple ID 也是被偷偷改了，我一直很担心，有天发现网易邮箱收入收到苹果的邮件，会手机通知我，我觉得放心很多”

“好险，原来有人在试我的 apple ID，幸亏网易会通知我，我马上打电话去苹果客服提高了我的帐号安全级别”

“什么叫贴心，什么叫智能化，网易这个安全提醒就是样板”

D. 推荐理由

网易邮箱是全国唯一一家针对 appleID 相关邮件提供主动提醒功能的邮件服务商，也是针对目前 appleID 被盗事件日益增多的情况下首先推出的相关安全措施。作为一家有社会责任感的企业，网易主动承担了下发短信的高额运营成本，有效地保护网民的 appleID 安全，使其经济利益不受侵犯。

公司简介

网易是中国领先的互联网技术公司，在开发互联网应用、服务及其它技术方面，网易始终保持国内业界的领先地位。网易对中国互联网的发展具有强烈的使命感，利用最先进的互联网技术，加强人与人之间信息的交流和共享，实现“网聚人的力量”。

电子邮件业务是网易公司最早开展的业务之一，经过-19 年来的持续投入，已经发展成为网易公司的核心战略平台，同时网易亦成为中国最大的邮件服务提供商。

案例 15：安全、绿色、高效的域名解析服务——SDNS 公共云服务

A. 保护网民权益创新&优秀实践总体情况简介

SDNS 公共云服务是一款面向公众的域名解析服务，旨在为互联网用户提供更加安全、绿色、高速的上网接入解析服务，服务地址为 1.2.4.8 和 210.2.4.8。

SDNS 公共云服务借助于域名安全评估引擎，使用多种基于域名的安全检测算法，智能检测用户访问的域名是否安全。如用户所要访问的域名经检测含有木马、僵尸、钓鱼以及涉黄等不安全风险，SDNS 能够第一时间为用户阻断上述访问或发出预警提示，保护网民权益。

B. 实践效果

SDNS 公共云服务是国内著名的非商业化运行的解析服务平台，作为一项互联网公益服务，SDNS 不但为普通网民提供安全、智能的解析服务，还能够保护用户不受域名劫持、网络攻击和网络欺诈行为的威胁，保护网民的每一次点击。

SDNS 公共云服务已为全国 1100 万用户提供了免费的解析服务，一年拦截恶意域名和钓鱼网站 2 亿次。SDNS 倡导并促进未成年人安全上网，并已在教育行业得到广泛应用。

C. 网民反应

我以前使用谷歌的 8.8.8.8，后来发现了国产的 1.2.4.8 这个 DNS 也很好记，使用之后觉得不错，比较稳定，速度也很快，以后懒得用改用其它的 DNS 了。——新浪微博网友@懒洋洋得意的笑

使用定制的公共云服务以后，有效的拦截了涉黄、涉暴等不良网站，很好的保护了我校同学在互联网里免受不良信息的毒害。——北大资源研修学院教导主任

我单位内网使用了 SDNS 公共云服务后，办公电脑中木马和病毒的情况明显减少了，看来它的安全防护功能确实是有作用的。——北京机械研究所网管员

D. 推荐理由

SDNS 公共云服务是中国互联网络信息中心(CNNIC)正式推出的面向公众的域名递归解析服务，该服务免费为广大网民提供安全、绿色、高速的上网接入服务。

CNNIC 为国家域名注册管理机构，拥有近二十年的域名研究实践与域名解析运行经验。SDNS 依托 CNNIC 自主研发的高性能解析软件系统、可靠的广域服务集群和专业的运行安全监测平台等技术优势，尤其针对学校，家庭，政府等特殊群体，为用户建立一个纯净安全的上网环境。

稳定高速：网络节点遍布全国，智能解析，全面提升上网速度；

无劫持：无恶意跳转和广告，减少和避免域名解析遭遇劫持；

安全防护：智能识别木马、钓鱼、涉黄等不安全域名，果断拦截或发出提示。

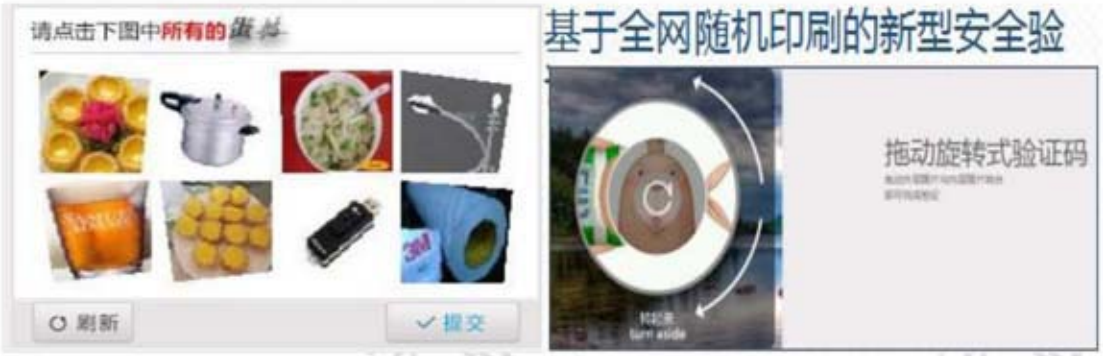
公司简介

中国互联网络信息中心（CNNIC）作为中国信息社会重要的基础设施建设者、运行者和管理者，在“国家公益、安全可信、规范高效、服务应用”方针的指导下，负责国家网络基础资源的运行管理和服务，承担国家网络基础资源的技术研发并保障安全，开展互联网发展研究并提供咨询，促进全球互联网开放合作和技术交流，不断追求成为“专业•责任•服务”的世界一流互联网络信息中心。

案例 16：点触云安全验证码

点触云安全验证码，下图为示例图：

A. 保护网民权益创新&优秀实践总体情况简介



点触验证码是基于行为大数据云的一套安全体系，主要作用是防止黑客恶意程序撞库行为，区分人和机器、区分是不是本人，防止网址信息泄露，为网民的信息安全做到全方位的保障。核心技术原理是机器学习算法以及行为大数据构建安全行为模型，系统具有自我更新更我学习的能力。

B. 实践效果

点触云安全验证码在 12306 购票系统的应用，很好的遏制了黄牛抢票和刷票行为；公有云服务的网站平台在注册登录、抢购秒杀等关键位置，屏蔽软件自动行为；使得各种非法软件失效，为普通网民提供一个公平的竞争环境。

C. 网民反应

点触验证码在安全性能方面得到了很好的验证，然而验证码的安全性和用户体验是个对立的矛盾统一体，安全性越高往往体验会降低；点触的云验证系统，采用机器学习的算法，按照用户识别难易度，进行验证图库的筛选和更新，系统自动抛弃，验证通过率较低的图组，以人为本，以人的行为作为基础模型，为网民提供信息安全服务、为平台保驾护航。

D. 推荐理由

北大密码学实验室汪定博士联合杭州微触科技合作产学研结合项目，积极推进科研成果转化。北大密码学实验室提供理论支持，杭州微触科技有限公司负责对学术性论文进行产品化开发。在人们忽视了网民信息安全的现在，对于保护网民用户信息安全具有重大意义。

公司简介

杭州微触科技有限公司从 2012 年起，开始研究基于行为技术的方法，研究和解决信息泄露和数据安全的问题. 点触验证码是的新一代互联网云安全验证方式；基于行为技术大数据的综合性解决方案；产品广泛应用于铁总 12306 售票系统、中国邮政集邮商城、discuz 等。我们致力于将点触行为安全技术发展成为新一代互联网行为安全技术的标准，为更多的用户提供基于行为大数据的信息安全保障服务。

案例 17：中国电信客服微信公众号防诈骗宣传案例

A. 保护网民权益创新&优秀实践情况介绍

随着互联网发展的深入，用户服务需求也由基本通信应用转向基于流量的丰富信息服务，其通讯网络诈骗问题日益突出，影响社会的和谐稳定。中国电信围绕“用户在哪里，服务在哪里”的服务使命，创建了“中国电信客服”微信、微博等公众账号，为广大客户提供便捷的业务办理、使用辅导、问题受理等服务，提升互联网服务水平，主要举措如下：

1、收集诈骗案例信息，制作符合互联网文化的、便于用户理解的漫画、视频等形式内容，通过“中国电信客服”微信、微博等公众账号定期发布，提高用户防范意识。

2、聚焦百姓常用的“余额查询、缴费充值、宽带报障”等功能，提供在线查询办理。

3、规范客户问题处理的闭环流程，7*24 小时受理在线客户的问题，当遇到举报诈骗问题时，第一时间将涉嫌诈骗号码和信息发送至当地公安机关、天翼安全中心的疑似诈骗库，积极协助处理。

B. 实践效果

“中国电信客服”微信、微博等公众账号运营以来，上线便民服务功能，策划发布防范诈骗专题信息 70 余期，有效地提高了用户防范意识，年处理 21 万客户问题，提升客户满意度和加强了用户的权益保障。

C. 网民反应

自 2012 年中国电信客服公众账号上线，截至 2015 年底，粉丝规模超 1 亿人，其中防诈骗专题信息被粉丝转载阅读超 4000 万次，得到了用户的高度认可。

D. 推荐理由

为保证广大用户的利益，中国电信建立客服微信、微博等公众账号，提升便民服务能力，宣传防诈骗知识，提高了防范意识和网民权益，取得了良好实践效果。

公司简介

中国电信股份有限公司增值业务运营中心设立于 2008 年 7 月 9 日，现有员工 353 人。主要承担中国电信全网集中运营的新媒体客服、互联网应用业务及增值业务的运营服务工作。2015 年，中国电信增值服务收入为 390.44 亿元人民币，较 2014 年增长 1.6%。

自成立以来，中心始终围绕集团公司战略转型、经营发展及重点业务等工作，以信息安全管理、新媒体客服运营管理为重点，逐步形成了完善的中国电信不良信息处理体系、新媒体客户服务体系，清除网络不良信息，策划发布系列防范网络诈骗专题信息，有效地提高了防范意识和网民权益。

案例 18：残疾人互联网上实现居家就业梦--互联网专业鉴黄师（仅开放残疾人）

A. 保护网民权益创新&优秀实践情况介绍

背景：为了保护青少年身心健康，维护互联网绿色空间，同时为残疾朋友提供居家就业的机会，互联网安全志愿者联盟与杭州市残联合作，选拔 20 多名符合条件、自愿报名的残疾朋友，经过专业培训加入“专业鉴黄师”志愿者小组。这个小组为淘宝平台等阿里平台排查商品黄图、论坛答疑做出了突出贡献。这也是志愿者团队中唯一一支有报酬的团队。联盟中的其他志愿者小组都是公益行为，仅有公益证书和积分奖励，以及年终评选优秀志愿者的机会。

鉴黄师的背景：自 1980 年代后期，制作、复制、贩卖、传播淫秽物品量刑细化，鉴黄师这一岗位首先在公安系统内产生。他们负责审看办案单位送来的书、录像带、VCD、DVD，开具鉴定结论。这些结论会影响案件的定性、犯罪嫌疑人的量刑和处理。

【创新方案】：通过在互联网上提供安全类型岗位，无论何时何地何种方式（pc 或手机）端操作举报不良信息。

B. 实践效果

2013 年 5 月，杭州市残联、团市委、市志愿者协会与阿里巴巴集团联合启动了“鉴黄师”助残项目。该志愿服务项目面向的是全国有电脑操作基础的残障人员。目前项目以杭州市残疾人康复职业培训中心为试点基地，招募残疾人“鉴黄师”开展图片审核员培训，项目打造了一套可持续、可复制的日常化公益模式，让更多残疾人实现了更大的人生价值。项目自启动以来，志愿者们累计审核图片两亿五千一百二十七万九千三百张，为净化网络环境做出了巨大贡献。项目共有工作人员 20 名，包括志愿者运营专员两名，志愿者培训师三名，

并配有专业财务人员。项目最大的特点就是将志愿服务搬上了网络，满足残疾人反哺社会的愿望，帮助残疾人实现了居家公益梦。

2016 年，助残项目还在继续推进中，今年预计会有更多残疾人士加入到网络鉴黄的队伍中来。此项工作具有网络办公、可复制性、日常化。在线网络办公，帮助残疾人实现居家就业，满足残疾人的就业愿景；同时项目可复制性强，并且将公益发展成为日常化工作。

C. 网民反应

事迹人物：赵凯（脑瘫）

事迹简介：在每一次标注项目启动开始，赵凯同学会主动联系每一个志愿者，进行任务、时间等情况的确认，帮助小二完成项目启动的准备工作，并且在项目中主动负责维护群内秩序，做了大量辅助性工作。而且在每次项目中都能做到标注错误率最低，标注量最高，赵凯同学从标注开始至今，共标注了图片量为：952W 准确率为：99.53%，参与了全部标注项目。

D. 推荐理由

1，净化网络安全环境，争做互联网安全志愿者；

2，提供居家就业岗位，提供残疾人在网络上更大化的作用及就业岗位，受到中国残联。

公司简介

【互联网安全志愿者联盟】目前中国网络安全领域最专业、有梦想、有情怀、肯付出的民间志愿者精英联盟。团队隶属阿里巴巴集团安全部，2007 年 9 月成立，当年注册名“杭州市网络反欺诈志愿服务队”。9 年来累计举报网上各类违规、违法信息高达 15 亿人次。2016 年 1 月 11 日，在中央综治办、中央网信办、公安部和团中央的大力支持下，这支团队升级为“互联网安全志愿者联盟”，联盟成员遍布全国 29 个省市自治区直辖市，由全国 276 所高校在校生、全国诚信商盟，以及各行各业热爱公益、关注网络安全的社会人士组成，包括残联的残疾朋友，日常在线活跃人数 5000+。团队的梦想：“志愿守护净土，共创网络安全。”

案例 19：SP 监控模块助力垃圾短信治理

A. 保护网民权益创新&优秀实践总体情况简介

在短信中心和 LSTP 之间的所有信令链路上部署 MPM 设备，并启用 SP 监控模块。利用消息处理机（MPM）可以实时发现、实时拦截垃圾短信的特点，可以对 SP 大量群发短信，透支费用的行为进行监控和制止。此方案的特点是：在各 LSTP 到短信中心之间的七号信令链路上以无信令点方式接入 MPM，对流经的消息进行鉴别和转发。当 SP 群发短信时，MPM 会实时发现，并把该号码加入黑名单，对该号码产生的短信进行实时拦截。

B. 实践效果

1、通过短信群发频次、关键字匹配频次和关键字结合等拦截策略的运用，SP 短号码的月拦截量约 80 余件，便于及时发现处置违规 SP，从而加强对 SP 的约束考核。

2、根据集团公司垃圾短信治理情况通报数据，我公司端口类垃圾短信全年累计 1-2 件，投诉量极少。

C. 网民反应

谈到垃圾短信，现在经过国家强制性的监管和控制，垃圾短信得到了有效地控制。运营商在治理的道路上功不可没，尤其是实施实名制登记制度以来，收到垃圾短信的数量明显减少，以前一天大概 10 条，现在一个月大概 10 来条的样子。该案例从端口管控着手，势必会减少端口类垃圾短信，为垃圾短信治理添力。

D. 推荐理由

该案例是我公司垃圾短信治理过程中的实际情况，同意推荐参加 2016 保护网民权益创新&优秀实践案例评选。

公司简介

中国联通内蒙古分公司是中国联通在内蒙古自治区的分支机构，正式成立于 1997 年 10 月 22 日，负责中国联通在内蒙古地区的电信建设和业务发展。目前。公司已经在全区 12 个盟市分设立了分支机构，其经营范围包括移动通信业务，数据通信业务、互联网业务和 IP 电话业务，国际、国内长途电话业务，无线寻呼业务及其他电信增值业务。

中国联通内蒙古分公司成立来，在自治区政府和社会各界的关心和支持下，经过全体员工的奋力拼搏，在网络建设、用户发展、业务创新、提升服务等各方面努力拼搏，积极进取，取得了令人瞩目的业绩。

案例 20：触云 OS（智能路由器操作系统）

A. 保护网民权益创新&优秀实践总体情况简介

1、保护网民权益的创新：触云智能路由器 OS 操作系统就是一种将云计算与本地运算整合的智能网络管理平台。很好的解决了智能网络管理中大数据的获取与应用。触云智能路由器 OS 操作系统中的安全防护引擎的安全防护。触云智能路由器 OS 系统，目前有 100 万的路由器激活量，同时在以日均 5000 的激活量稳步增长。

2、总体情况：智能化的大潮，应用于以家为中心的智能家居，消费者能够便捷控制家庭中的各种终端设备，从而提升家庭生活的舒适性、便利性和安全性。

B. 实践效果

1、安全防护：实时监控每天拦截：钓鱼木马类数量 5715256、仿冒假冒类数量 3646420、欺诈虚假类数量 2258012、非法违规类数量 1488717、色情赌博类数量 301233。

2、实惠：保证用户的个人信息、流量安全。未来会发展到保障整个智能家居系统提供完整、可用的安全保障。

C. 网民反应

现在时代发展的那么快，手机还没玩明白，就开始推广智能家居、IoT；把家里的设备全部变成智能化，联网。那我们的信息安全谁来保护啊，信息泄露怎么办，黑客入侵怎么办。但是想想，还是要跟上时代，至少这些发明，让我们在家里生活的更舒适、便捷了。只要能保证好，我们的信息安全，接收这样的产品，也不是什么难事。

D. 推荐理由

触云重新定义智能路由操作系统，将智能路由 OS 与云端结合。实现了智能路由器操作系统的技术创新。把智能路由功能的 80%在云端完成，20%由本地路由完成。既降低了路由器的成本，又通过云端升级赋予了智能路由器无限的应用开发前景。将网络管理和云端应用与服务由业务驱动转变为数据驱动。

大数据正快速发展，对数量巨大、来源分散、格式多样的数据进行采集、存储和关联分析，从中发现新知识、创造新价值、提升新能力的新一代信息技术和服务业态。大数据的应用能够揭示传统技术方式难以展现的关联关系，建立“用数据说话、用数据决策、用数据管理、用数据创新”的新的管理机制。触云依托自身在大数据应用和云计算方面的优势和特长，观察智能家居的安全热点，指引安全体系建设方向。

公司简介

深圳触云科技有限公司成立于 2014 年 10 月，是国内首家专注于智能路由 OS 生态，提供个人数字画像的大数据服务公司。触云智能路由器 OS 及云端服务解决方案，助力合作伙伴加速产品智能化进程，融入智能生活生态圈。应用大数据支撑智能网络管理与应用，获取更多的业务价值。提供网络系统安全保障，为 IoT 智能家居设备提供稳定安全联网服务。

案例 21：中国移动伪基站治理实践

A. 保护网民权益创新&优秀实践总体情况简介

“伪基站”伪装成运营商的基站，利用局部功率大的优势，干扰屏蔽运营商通讯信号，强行将其信号覆盖范围内的手机劫持到伪基站上，以达到“获取手机信息、发送垃圾短信”的目的，俗称“圈地式短信群发器”。伪基站严重干扰通信，骚扰用户，并带给社会严重的危害。

我公司早在 2013 年底自主研发了基于信令的“伪基站”监测治理系统，试点了“伪基站”打击机制和工作流程，建立健全了集团—省公司两级联动机制，形成《伪基站治理经验汇编》并在全国范围内推广，主导《移动伪基站网络侧监测技术要求》作为行业标准立项，推动中央九部委在全国范围内开展“打击整治伪基站专项行动”，实现了“伪基站”治理有手段、有机制、有成果。

B. 实践效果

一是严厉打击不法分子。截至 2016 年 3 月底，我公司共配合执法机关侦破“伪基站”案件 5270 例，缴获设备 5853 套，抓获犯罪嫌疑人 7329 名。二是切实维护客户权益。“伪基站”危害程度大幅降低，在工信部通报的 2016 年 3 月垃圾短信投诉中，我公司涉及“伪基站”发送导致的投诉占比为 38.05%，较 2013 年 12 月的 70%大幅度下降。

C. 网民反应

不法分子利用伪基站滥发垃圾短信、诈骗短信，给用户带来极大骚扰，用户财产安全受到一定的威胁。中国移动深入开展伪基站治理，利用先进的技术手段监测、发现伪基站，配合公安等执法机关对伪基站进行收缴，使得不法分子难以利用伪基站向用户发送垃圾短信、诈骗短信，进而无法实施后续诈骗，切实保障了用户的合法权益。

D. 推荐理由

伪基站不仅骚扰用户，也给运营商带来严重的负面影响，运营商也是受害者。伪基站发送垃圾短信并不经过运营商的网络，如何监测伪基站是全行业共同面临的难题。同时，运营商无权对“伪基站”违法犯罪分子进行查处，对“伪基站”的抓捕、惩处工作需由政府执法部门完成。但我公司仍积极履行企业社会责任，在各地配合打击过程中，多次发生移动公司车辆被撞坏，员工被犯罪分子打伤甚至被黑社会威胁的情况，但这并未动摇我们打击伪基站的决心。

中国移动迎难而上，立足自主研发，率先研发“伪基站监测治理系统”，提出“伪基站综合治理体系”，全力配合公安机关等上级单位开展伪基站打击整治工作，取得了显著成效。2014 年 1 月，中央网信办、工信部、公安部、安全部在我公司召开伪基站治理现场会，为后续“打击整治伪基站专项行动”奠定基础；同时，我中心被中央网信办评为“打击整治伪基站先进集体”。中国移动伪基站治理工作始终走在全行业前列。

案例 22：可信号码信息服务联盟

A. 保护网民权益创新&优秀实践总体情况简介

可信号码信息服务联盟由新华网，中国电信号码百事通（114），号码服务专家电话邦三家理事单位共同发起，联合运营商、手机终端、安全厂商以及号码信息安全服务相关企业、事业单位和社会团体自愿组成的具有鲜明行业特征的非营利性行业组织。

联盟通过整合协调产业资源，推动中国可信号码信息服务生态系统建设，搭建号码信息认证和服务平台，推进号码信息服务规范化；建立官方可信的企事业单位基础号码信息数据库，推进企事业单位信用体系的建立；优化号码信息安全相关的服务，预防垃圾短信和电话诈骗，维护互联网安全，增强社会公众对号码信息服务的认知。

B. 实践效果

在联盟推动下，可信号码信息服务被各地政府、企事业单位所认可。目前联盟号码数据已经覆盖全国所有 34 个省级行政区、333 个地级行政区、2856 个县级行政区；拥有超过 6500 万商业机构的号码，基本覆盖三大运营商用户，终端用户覆盖超过 7 亿。

2015 年 6 月 23 日，可信号码信息服务联盟特别受邀亮相广东省第二届网络安全宣传周，并参与公众体验展开馆仪式。

2016 年 3 月 2 日，在北京隆重举行的“云上贵州•大数据招商引智推介会”上，可信号码信息服务联盟正式签约落地贵州铜仁，助力铜仁市建立企业信用大数据平台，打造“信用铜仁”。

C. 网民反应

评论一：现在社会上骚扰诈骗电话太多了，彰显出可信号码的重要性，对诈骗分子也是一种震慑；

评论二：可信号码联盟通过政企结合，充分发挥了各自的优势，对推动可信号码服务有一定积极作用；

评论三：个人号码实名制现在执行力度比较大，企业号码实名制还需要联盟大力推动。

D. 推荐理由

联盟推进了公众对可信号码服务的认知，对于净化通讯环境、保障网民知情权益、打造可信号码生态服务起到了至关重要的作用。

公司简介

北京羽乐创新科技有限公司成立于 2012 年，电话邦是其主营品牌。国内数据现已收录 6500 万商业机构的 8500 万个电话号码，有 12 亿+的数据总量，号码覆盖 370 多个城市，海外数据覆盖印度、东南亚、美国等国家和地区，是最全最准的电话号码库。

电话邦与 30 余家终端达成深度合作，覆盖超过 7 亿用户，日活跃用户达 1.32 亿，致力于联合入口方、生活服务提供方构建基于电话号码的生态圈，与各方协力共生、生态互赢，为更多中小企业提供可信号码生态服务。

案例 23：中国电信建立不良信息处理体系

A. 保护网民权益创新&优秀实践情况介绍

为有力地净化了互联网环境，按照中国集团公司的工作要求，通过组织架构、防范体系、整章建制、系统建设、重点保障等创新实践，建立了一套常态化、规范化、专业化运作的不良信息处理体系，形成了有效的信息安全风险防范机制，具体做法如下：

1、组建专职机构。2010 年 3 月，设立中国电信不良信息处理中心，从根本上改变了信息安全“战役式”工作方式，建立了信息安全工作接口人联络队伍，确保突发事件第一时间处理，推动工作的闭环管理，实现了信息安全工作的常态化、规范化。

2、打造防范体系。从“三个阶段十个方面”建立了事前事中事后风险防控体系，一是从建章立制、内容预审、重点保障、培训交流四个方面建立风险事前预防体系；二是从拨测监控、业务巡检、举报受理三个方面建立风险事中控制体系；三是从违规处理、应急处理、信息通报三个方面建立风险事后处理体系。

3、制定流程制度。先后制定了不良信息应急处理预案、监控及拨测问题处理流程等，通过实施上述规章制度和工作流程，建立了不良信息处理长效管理机制，缩短了信息安全问题处理时间，大幅提高了工作效率。

4、推进系统建设。建设不良信息内容检测平台，实现网站不良信息自动检测，大大提升信息安全问题发现的及时性和准确性，提高运营中心监控工作的范围和效率；建设中国电信防不良短信全国管理平台，集中受理用户投诉，实现垃圾短信联动处理，提升治理效率。

5、强化重点保障。完成“净网、净屏”等45余次信息安全保障和专项工作。

B.实践效果

建立中国电信不良信息处理体系以来，通过健全组织架构，形成上下联动的信息安全工作局面，有效清除网络不良信息912件，处理垃圾短信62.3万件，净化网络环境，促进和谐网络发展。

C.网民反应

引起行业内专家用户的一致赞同，网民反应效果良好。

D.推荐理由

中国电信不良信息处理体系的创新，建立了一套常态化、规范化、专业化运作的信息安全管理体系，形成了有效的信息安全风险防范机制，清除网络不良信息，促进和谐网络发展，取得了良好实践效果。

公司简介

中国电信股份有限公司增值业务运营中心设立于2008年7月9日，现有员工353人。主要承担中国电信全网集中运营的新媒体客服、互联网应用业务及增值业务的运营服务工作。2015年，中国电信增值服务收入为390.44亿元人民币，较2014年增长1.6%。

自成立以来，中心始终围绕集团公司战略转型、经营发展及重点业务等工作，以信息安全管理、新媒体客服运营管理为重点，逐步形成了完善的中国电信不良信息处理体系、新媒体客户服务体系，清除网络不良信息，策划发布系列防范网络诈骗专题信息，有效地提高了防范意识和网民权益。

案例24：全信通移动支付系统

A.保护网民权益创新&优秀实践总体情况简介

全信通移动支付系统以手机APP结合外置刷卡器（读取银行卡磁条或芯片信息），刷卡器通过音频接口/蓝牙与手机APP进行数据传输，IOS与Android全系统覆盖的智能移动系统平台，系统以拥有独立第三方便民服务平台为创新特色，刷卡终端设备与智能移动设备无缝集成，通过移动APP与云端支付大数据平台高效、精准、安全数据通信，并利用智能移动设备的轻便、易操作性为用户提供24小时随身银行服务，打造移动金融新体验，支付方便，随时随地，即插即用。

全信通移动支付系统只需使用IOS或Android智能移动系统手机一部、任意银行银联卡，使用WIFI/2G/3G/4G或无线网络即可实现信用卡还款、个贷还款、转账汇款、公共缴费（水电煤气）、手机充值、支付宝充值、个人付款、手机号提款、预付卡包（管理多张银行卡）、余额查询等功能。一站式提供便民服务，轻松实现快捷支付。

B.实践效果

全信通移动支付系统顺应移动互联网科技发展、专注于智能移动设备研发的划时代移动云支付创新产品，为使用者提供金融服务与便利生活全新技术体验。通过采用三重密码保护、初始化键盘服务、按键无状态模式及密码输入后非对称加密传输、彻底杜绝交易风险。通过数据加密，保障交易安全可靠。

C.网民反应

全信通移动支付系统使得支付资金携带更加方便，消费过程更加便捷简单，消除了支付障碍之后，可以更好的尝试许多新的消费模式；支付资金的安全性相对传统方式有大幅提高。

D.推荐理由

收款交易短信实时提醒，外接加密键盘，确保资金安全无忧。

公司简介

山东浚嘉移通信息技术有限公司隶属于即富金服控股集团，位于山东省济南市高新区，注册资本 1.28 亿，，是目前国内及山东省领先的电信增值、金融支付、电子商务、智慧医疗行业标杆企业；公司资金实力雄厚、人才汇聚、品牌知名，拥有工业与信息化部、中国人民银行颁发的电信增值业务及第三方金融机构支付牌照，以全国性运营团队、专业化的研发团队面向市场提供电信增值、便民支付、电商交易平台服务，是集研发、生产、销售、孵化、培训、服务、大数据整合为一体的高新技术企业。

案例 25：她社区联合百度律师团队为社区用户提供法律援助

A.保护网民权益创新&优秀实践总体情况简介

她社区和百度律师团队进行了平台跨界的合作，旨在为她社区用户提供无偿一对一的法律援助，以及向大众进行普法的知识教育。百度团队配合她社区在社区内部开展了圈子文化活动，在“法律小常识”进行大量的义务普法，并实时开通了法律问题在线提交功能，实现了快速有效的对话渠道。

B.实践效果

目前“法律小常识”的圈子内现有帖子近万篇，以案例模式从各个维度来阐述当下婚姻生活中出现的法律问题，为她社区用户实现了深度普法。一对一在线对话环节，成功帮助接近两千人实现了咨询，其中 24%的人获得了一对一对话服务和电话服务，解决了发生在自己身上的婚姻生活中的法律问题，提高了夫妻二人婚姻生活质量，也为全民懂法起到了重要作用。

C.网民反应

1、她社区用户“你转身我经过”：“刚刚遭遇了婚姻中出现小三的问题，我的老公和小三一直住在外面，我的儿子也被老公带走不让我见面，我们的婚姻形同虚设，协议离婚也成为了一句空谈，在她社区的帮助下，我终于知道如何解决自己的问题，感谢她社区”

2、她社区用户“温柔的姑娘“：“和老公结婚后，发现之前老公欠了不少的钱，让我们本就刚解决温饱的家庭出现了重大变故，因为我和他是相亲认识并闪婚的，现在的情况让我很难去维持我们的婚姻，而债主认为我们既然是夫妻，那么我老公的钱就应该由我来偿还，感谢她社区带来的法律援助，现在我已经诉诸法律解决了我的问题。”

3、她社区用户“大蚂蚁”：“在她社区很久了，自动开建了法律小常识这个圈子，我也一直浏览着上面的内容，对于法律有了深刻的了解，对生活中的诸多问题也对照获得了很大的帮助，很喜欢她社区的内容，让我可以学习收获更多”

D.推荐理由

她社区这一次与百度的合作，让目前中国的移动女性用户可以更直接有效的通过法律的武器来保护自己，让自己可以在享受合法权益的前提下幸福的生活，作为中国最大的移动女性社区她社区也致力于为年轻女性用户打造一个和谐良好的移动互联网氛围，塑造成熟独立的人格，这对某些程度上有点浮躁的移动互联网来说，可以说是降了一定的温度，起到了传递正能量的作用，因此我们在这里自荐，将此案例做为保护网民权益创新的优秀实践案例上报。

公司简介

浪淘金是周杰在美国 Google 回国后创立的互联网科技公司，目前公司主营女性社交社区“她社区”，周杰毕业于清华大学计算机本科后到美国耶鲁深造获得硕士学位并加入美国 Google 成为华人界最年轻的 Google 总监，在 4 年的美国硅谷历练后加入中国 Google 任技术负责人，并一手打造了 Google 地图，随后到来的创业浪潮里离开了 Google 着手开始自己的创业项目，她社区是一款纯女性社区社交应用，为女性交友提供了良好的氛围，多次获得业界大奖。

案例 26：新闻无人机航拍

A. 保护网民权益创新&优秀实践总体情况简介

为了适应媒体融合发展的要求，为网民提供更丰富的报道视角和浏览体验，新华网不断创新新闻报道模式，以“让新闻离你更近”为理念，率先进军无人机新闻报道领域。2015 年 6 月 15 日，新华网成功组建国内首个新闻无人机队，超前布局国内无人机新闻报道领域，以多维视角采集新闻，建立起重大突发事件的无人机新闻采集和传播机制。

通过半年多的探索和实践，新华网新闻无人机队已具备了全天候、多地形、全媒体的新闻航拍和内容输出能力，在天津滨海新区爆炸、深圳滑坡事故等突发事件中从现场为海内外受众提供权威、独家、视角独特的“高附加值”全媒体航拍新闻内容。

B. 实践效果

无人机用于新闻报道网民受益良多。首先，无人机的速度优势无可比拟，可以第一时间赶往新闻现场开展作业，为网民提供时效性高的新闻产品。此外，无人机居高临下，拍摄具有高清晰、大比例尺、高现势的优点，为网民提供全局视野的拍摄角度，大幅改善浏览体验。最后，对于危险的新闻现场，无人机可以深入险境，用最小代价拍摄到极具新闻价值的图片和视频，有效保证了网民对于突发事件现场情况的知情权。

C. 网民反应

网民表示，新华网的新闻无人机队拍摄的天津滨海新区爆炸和深圳滑坡事故的内容太震撼了，在事故现场进行全地形、全媒体进行新闻航拍，处处都是新闻现场的即视感，不仅给用户带来了完全不同视角的浏览体验，更保证了网民对新闻现场的知情权。为新华网无人机队点赞。

D. 推荐理由

新华网在中央重点新闻网站中率先成立新闻无人机队，以多维视角采集新闻，建立重大突发事件的无人机新闻采集和传播机制。这不仅是新华网适应媒体融合发展的转型布局，更是新华网贴近网民需求，提升网民新闻浏览体验，保障网民重大社会性突发事件知情权的创新手段，有力践行了新华网“让新闻离你更近”的传播理念，受到广大网民和用户的高度评价。

公司简介

新华网是国家通讯社新华社主办的综合新闻信息服务门户网站，是中国最具影响力的网络媒体和具有全球影响力的中文网站。依托新华社遍及全球的强大采编力量和权威内容发布，新华网 24 小时为全球网民提供最权威最及时的新闻信息服务，用户遍及 200 多个国家和地区，桌面端日均页面浏览量超过 1.2 亿，移动端日均覆盖人群超过 1.3 亿，重大新闻首发率和转载率遥遥领先国内其他网络媒体。

据全球权威网站排名机构 Alex 数据显示，2015 年，新华网在全球 7 亿多个网站中综合排名第 70 位，大幅领先美联社、路透社、法新社等通讯社主办的网站。在中央网信办主管的《网络传播》杂志发布的中央重点新闻网站传播力榜单中，10 月、11 月综合传播力排名首位，远超同类网站。

案例 27：域名城邮箱举报系统

A. 保护网民权益创新&优秀实践总体情况简介

易介集团北京有限公司作为域名行业的领军者，旗下域名城网站注册会员 22 万以上，是世界第一大域名论坛，处于行业领军地位。为了让行业内众多网友免受群发、垃圾、钓鱼邮件的骚扰，确保域名相关服务的正常运行。域名城网站特开设国内首家域名垃圾邮件黑名单系统。规则：用户需要登录状态，针对一个邮箱一个用户只能举报一次，当某个邮箱被举

报>=50 次，将会进入黑名单列表公示，同时，用户可以点击下载 TXT 并导入至自己的邮箱客户端下的黑名单列表。

不满足 50 次者，则进入即将公示列表，不提供下载功能；

如您的邮箱被人恶意举报，可以点击页面的“申诉”按钮提交相应请求，工作人员核实无误后便可将您的邮箱记录删除。同时系统可提供 TXT 文本下载，以便在各类邮箱中方便设置黑名单列表。

B. 实践效果

确保行业内网民更为安全的收发邮件，免受群发、垃圾、钓鱼邮件的骚扰，保证域名行业内相关服务平台的正常运行。

C. 网民反应

发表于 2015-9-1108:48 支持这个举报系统，功能强大，实用性很强，下载 TXT 加入邮箱黑名单后，垃圾、群发、钓鱼邮件明显减少。

发表于 2015-10-10 9:20 切身维护了我们的利益，再也不用担心钓鱼邮件的入侵啦

发表于 2015-11-2 12：50 易介集团的这个系统给我们米农带来了福音

发表于 2015-11-5 15:29 大赞一个，真正的解决了我的苦恼，还能下载黑名单，太棒了

发表于 2016-1-3 8:12 举报了一个钓鱼邮件，希望为米农们做点贡献，希望越来越多的人加入到域名城的邮箱举报系统

发表于 2016-2-3 19:00 好用，赞一个，我们域名行业的网民安全就靠你们了，希望这个系统越做越好。

发表于 2016-2-9 13:01 大力支持，持续关注

发表于 2016-03-02 2:22 系统不错，值得推广，让更多的米农受益。

D. 推荐理由

域名城的邮箱举报系统维护了行业内邮件安全，通过曝光网络上的群发、垃圾、钓鱼邮箱，告诫同在一个行业的不法分子，起到净化网络的作用，切实维护用户的利益，是值得推介，实用性很强的一套系统。（姓名：窦伟伟职务：前 shejiao.com 创始人颜文字创始人、域名行业，网络安全业内专）

公司简介

易介集团是一家专注于互联网信息服务的综合性企业，经国家相关部门批准注册，是中国专业的域名增值服务商，中国互联网络信息中心（CNNIC）及世界互联网名称与数字地址分配机构（ICANN）认证的顶级域名注册服务机构。集团在国内首次推出“网络品牌=域名+商标”理念。作为中国领先的专业网络资产增值服务提供商，公司现有业务划分为五大品牌：易介网（www.yijie.com）、域名城（www.domain.cn）、中付通（www.zft.com）、易域网（www.yiyu.com）、中华知识产权网（www.ipchina.com）。

案例 28：买家保护提醒

A. 保护网民权益创新&优秀实践情况介绍

创新方案：在案例一中提到实时监控并发现疑似正在发生信息泄漏事件的基础之上，自动对此次疑似泄漏事件所影响的买家消费者进行语音外呼或文本短信防骗提醒，以此来提升买家对诈骗行为的防范意识。同时结合多纬度的数据对买家进行易骗人群的分析，以此来提升防骗提醒的效果及用户体验。

B. 实践效果

通过及时对买家防骗保护提醒，有效降低了买家被骗的几率。从 2015 年 4 月开始，截止 2016 年 3 月底，累计语音外呼提醒量 5280.4 万次，累计短信提醒发送量 7374.6 万次。

C. 网民反应

买家在及时收到防骗保护提醒后，对阿里巴巴在防范电商交易类电信诈骗的工作表示认可。

D. 推荐理由

及时、精确对买家进行保护提醒，提升买家防骗意识，以此来降低不法分子的诈骗成功率。

公司简介

阿里巴巴集团经营多元化的互联网业务，致力为全球所有人创造便捷的交易渠道。自成立以来，阿里巴巴集团建立了领先的消费者电子商务、网上支付、B2B 网上交易市场及云计算业务，近几年更积极开拓无线应用、手机操作系统和互联网电视等领域。集团以促进一个开放、协同、繁荣的电子商务生态系统为目标，旨在对消费者、商家以及经济发展做出贡献。

案例 29：工作虫蓝领猎头服务

A. 保护网民权益创新&优秀实践总体情况简介

工作虫招聘平台在国内率先推出蓝领猎头招聘服务，为服务行业求职者提供一对一就业推荐，从面试邀约到录用上岗全程就业指导，确保招聘供需双方信息精准匹配，平台提供在线工资结算功能，商家通过平台支付工资，求职者可以快速在平台进行工资提现，平台还专门提供求职受骗赔付基金，最大限度保证求职者权益。

B. 实践效果

工作虫蓝领猎头服务目前已经累计为超过 10000 名求职者成功推荐工作，求职者找工作更加放心高效。

C. 网民反应

求职者江燕：工作虫平台为我推荐了联合利华促销员工作，招聘顾问服务态度很好。

求职者高爱云：工作虫平台为我推荐了保洁工作，上岗速度很快，工资发放比较放心。

求职者史咏梅：工作虫平台为我推荐了白家大院的职位，让我找工作非常放心。

D. 推荐理由

工作虫平台作为国内首家针对蓝领提供猎头服务的招聘平台，让蓝领行业求职更加放心、高效，有效提升了服务行业招聘和就业效率。

公司简介

工作虫是北京人人优活公司旗下专注服务行业招聘的移动互联网平台，致力于成为中国服务行业综合人力资源服务领导者。提供包括兼职、全职、自由职业的招聘及培训服务。专门为餐饮、零售、美容美发、快速消费品等行业提供快捷招聘服务。

案例 30：信息泄漏实时发现与对抗

A. 保护网民权益创新&优秀实践情况介绍

创新方案：通过建立完善的交易订单数据流转的全链路日志，对全量的交易订单日志进行实时监控和分析，通过大数据技术的规则、模型主动发现正在产生交易订单泄漏的事件，并自动关联此类泄漏途径所对应的处置行为，大大降低了对已产生诈骗的交易订单信息的依赖，缩短了信息泄漏事件发现和处置的时间周期。

B. 实践效果

针对常见的信息泄漏途径，可以在半小时内发现疑似正在发生的泄漏风险事件，其中 70%的风险事件在接收到诈骗反馈之前就完成了风险处置。

C. 网民反应

在信息泄漏实时发现及对抗方案上线之后，从各个渠道搜集到收到诈骗电话的交易订单中，目前有 30%的订单其泄漏途径已经在最早接收到反馈之前发现并完成处置。

D. 推荐理由

1. 事中发现并处置，不依赖已产生诈骗的泄漏订单，极大缩短的信息泄漏问题处置的时间

公司简介

阿里巴巴集团经营多元化的互联网业务，致力为全球所有人创造便捷的交易渠道。自成立以来，阿里巴巴集团建立了领先的消费者电子商务、网上支付、B2B 网上交易市场及云计算业务，近几年更积极开拓无线应用、手机操作系统和互联网电视等领域。集团以促进一个开放、协同、繁荣的电子商务生态系统为目标，旨在对消费者、商家以及经济发展做出贡献。

案例 31：百度安全联合公安部门打击伪基站短信诈骗犯罪

A. 保护网民权益创新&优秀实践总体情况简介

背景：随着移动技术手段的不断更新，使用“伪基站”设备发送虚假广告、实施电信诈骗等违法犯罪活动日益猖獗，网民/用户稍不留神就会落入不法分子的圈套，造成隐私泄露及财产损失。

应对方案：百度安全借助安全技术与大数据分析能力，精准的识别伪基站发出的短信，定位伪基站位置信息。同时百度安全将识别的伪基站短信内容与定位信息同步给公安部门，公安部门进行抓捕，从源头打击伪基站诈骗犯罪，保护网民信息财产安全。

B. 实践效果

百度安全与公安部门开展合作以来，在全国范围内建立起合作交流平台，合作半年多来，协助广州、陕西、深圳、江西、四川等地公安破获伪基站诈骗案件 200 多起，缴获作案设备 500 多台，追回账款上千万，与陕西宝鸡市公安局的合作，20 天内成功打掉 13 个伪基站，查扣非法作案车辆 11 台，收缴伪基站设备 16 套 64 件，抓获犯罪嫌疑人 23 人。与江苏南京公安合作，破获一个以发伪基站诈骗信号小组、制作钓鱼网页技术小组、取钱小组以及联络小组组成的结构严密的犯罪团伙，横跨江苏、广东、北京、海南等多个省市。与去年同期相比，借助伪基站实施诈骗的案发率下降 40%，有效遏制了电信网络诈骗案的高发势头，取得了显著的效果。

C. 网民反应

接受到的骚扰诈骗短信明显减少，可以更加安心的享受互联网给生活带来的便利，感谢百度安全与公安部门背后做出的努力和付出。

D. 推荐理由

韩长青百度安全高级安全工程师表示：随着互联网的飞速发展，网民在享受快捷和便利的同时也面临着日益变化升级的安全挑战，完成维护网络安全，为用户提供安全可靠服务的重任也需要跨界合作，发挥各家优势，共同建立一个安全可靠的网络生态，百度安全事业部与公安部门合作打击伪基站诈骗犯罪，便是一个具有代表性的案例。

公司简介

百度公司于 2000 年成立于北京中关村，经过十六年时间的发展，现已成为全球最大的中文搜索引擎和中文网站。百度公司业绩增长迅猛：2015 年公司营收超 663.82 亿元，同比增长 35.3%。目前公司员工近五万人，其中工程师占比超过三分之一。

百度公司利用自身的平台优势，以技术创新为驱动力，在促进产业转型升级、扶持中小企业发展、引领核心科技进步、消弭知识传播鸿沟等方面发挥着越来越重要的作用。百度未来的发展目标是：到 2020 年，发展成为世界互联网的创新中心；将百度打造成在全球一半以上互联网市场中家喻户晓的品牌；代表中国企业在全球经济中发挥影响力。

案例 32：企业号码实名制展示

A.保护网民权益创新&优秀实践总体情况简介

2015 年 9 月 1 号工信部推出手机号码实名制，对象是手机个人用户，同时期电话邦推出了企业号码实名制，对象是企业号码。作为电话号码生态圈的构建者，电话邦推出企业号码实名制服务旨在帮助企业在移动互联网时代打造一个全新入口，真正意义上做到精准识别，实名展示。

当前展示渠道覆盖小米、OPPO、Nubia、美图、VIVO、金立、IUNI、PPTV、联通营业厅、TCL、百度手机卫士、腾讯手机管家等 16 大展示渠道，帮助企业号码实现价值最大化。

B.实践效果

电话邦为企业提供的号码实名认证服务，主要包含以下几点：1.来去电页面：来去电时通话瞬间即显企业名称、企业 logo、企业 slogan 等信息，让企业号码不再陌生，对企业品牌进行了有效曝光，很大程度上提高了用户接听体验；2.通话记录页：无论电话是否接通，一次拨号，即可将企业“名片”留存至客户手机内，相当于对企业的二次曝光；3.号码详情页：企业可在此页面进行官网外链、企业详情、快捷服务、一键导航等设置，全方位的展示企业信息，为企业打造了一个基于电话号码的全新入口。

目前电话邦企业号码服务覆盖了汽车、电商、房产、金融、旅游、医疗、家居、生活、航空等众多行业，与链家网、爱屋吉屋、捷豹中国、人人车、百度钱包、世纪佳缘、海南航空、途牛网等知名企业都已达成深度合作。

C.网民反应

电话邦的企业号码实名制展示对用户来说是一次全新体验，实际感受到移动互联新时代的变革，对企业来说，电话邦为企业打造移动互联网营销第一入口，构建一个全新的号码生态圈，从此企业号码再也不是一串冰冷陌生的数字，每一次接打都是一次最佳展示，让企业号码直接触达客户，实现通话价值最大化，所以得到了用户和客户的一致好评与肯定。

D.推荐理由

电话邦的企业号码实名展示服务有效的利用了企业号码资源，帮助企业在移动互联网时代的创新转型，让企业的每一通电话都能直接有效触达客户。

公司简介

北京羽乐创新科技有限公司成立于 2012 年，电话邦是其主营品牌。国内数据现已收录 6500 万商业机构的 8500 万个电话号码，有 12 亿+的数据总量，号码覆盖 370 多个城市，海外数据覆盖印度、东南亚、美国等国家和地区，是最全最准的电话号码库。

电话邦与 30 余家终端达成深度合作，覆盖超过 7 亿用户，日活跃用户达 1.32 亿，致力于联合入口方、生活服务提供方构建基于电话号码的生态圈，与各方协力共生、生态互赢，为更多中小企业提供可信号码生态服务。

案例 33：用户信息泄露预警中心

A.保护网民权益创新&优秀实践总体情况简介

用户信息泄露预警中心是杭州微触科技最新推出的一个平台，其目的是为普通网民提供一个已经泄露的信息的查询接口；每个网民都可以通过这个接口查询是否自己的敏感信息是否已经发生了泄露；查询结果关键字段已经进行了屏蔽，只有本人可以通过相似判断，这些信息是否属于自己的信息。

B.实践效果

网上存在很多之前已经发生泄漏的信息，往往网民本身不敏感，但是赤裸裸的看到自己的账户和密码，在网上摆着，才会刚到后怕；其实最可怕不是这个，而是很多人压根就不知道自己的账户密码发生了泄露，还在使用。

很多网民通过这个接口查询到信息泄露之后，马上就去采取措施，修改和更换账户和密码，防止进一步的伤害发生。

C. 网民反应

这种事情，文字和口头说，往往不太在意；只有看到了，经历了，才会切身体会；用过的网民都觉得这个查询很有必要、很有帮助。

D. 推荐理由

北大密码学实验室汪定博士联合杭州微触科技合作产学研结合项目，积极推进科研成果转化。北大密码学实验室提供理论支持，杭州微触科技有限公司负责对学术性论文进行产品化开发。在人们忽视了网民信息安全的现在，对于保护网民用户信息安全具有重大意义。

公司简介

杭州微触科技有限公司从 2012 年起,开始研究基于行为技术的方法，研究和解决信息泄露和数据安全的问题.点触验证码是的新一代互联网云安全验证方式；基于行为技术大数据的综合性解决方案；产品广泛应用于铁总 12306 售票系统、中国邮政集邮商城、discuz 等。我们致力于将点触行为安全技术发展成为新一代互联网行为安全技术的标准，为更多的用户提供基于行为大数据的信息安全保障服务。

案例 34：北京联通强力支撑北京市非法小广告专项治理行动

A. 保护网民权益创新&优秀实践总体情况简介

小广告号码治理停机，是北京市政府近年开展的综合治理非法小广告行动的重要举措。作为北京地区的主要通信运营商，市政府要求北京联通将治理非法小广告停机当作一项政治任务，高度重视，全力支撑。北京联通积极响应市政府要求，利用现有系统条件，短时间内，制定完成了针对小广告停机的业务支撑流程及管理办法，强力支撑北京市非法小广告专项治理行动。

B. 实践效果

从 2015 年 7 月到 2016 年 3 月，北京联通共收到城管部门发来的停机文件 246 批次，涉及北京联通号码 4573 个。此项工作开展以来，北京联通既保证停机操作 100%正确无差错，又保持高效的运行处置流程，当日接收的停机通知当日全部完成，并及时向城管部门反馈处理结果，助推北京市政府治理非法小广告工作的顺利进行。

C. 网民反应

配合政府治理非法小广告，净化公众用户通信环境，降低电信骚扰，阻断小广告违法行为，得到了广大公众用户的认可。

D. 推荐理由

具备畅通的流程，完备的机制，实施效果明显，具有实践性和示范性。

公司简介

中国联合网络通信有限公司北京市分公司（以下简称：北京联通）主要经营固定通信业务，移动通信业务，国内、国际通信设施服务业务，卫星国际专线业务、数据通信业务、网络接入业务和各类电信增值业务，与通信信息业务相关的系统集成业务等，是北京地区实力雄厚、品牌强劲的全业务电信运营商，广泛服务于国家和北京市党、政、军及企业客户，为广大公众用户提供基于固定通信网络和移动通信网络服务，服务面积 16800 平方公里。

案例 35：用户隐私保护系统

A.保护网民权益创新&优秀实践总体情况简介

随着互联网行业的快速发展，网民的个人隐私泄露问题变得越来越重要。为了保护去哪儿网用户的隐私安全，并结合公司的业务特点，在多个层面、多个维度对用户隐私进行了安全防护，具体措施为：

1、搭建数据加密系统，对去哪儿网的数据库系统、web 应用系统、服务系统、日志系统、HIVE 数据分析处理系统等所有系统中的用户敏感信息都进行了加密保护。保证黑客无法窃取用户信息。

2、保护用户在登录、支付、消费等重要操作过程中敏感信息和重要操作的安全性。数据安全方面，在互联网传输中使用 HTTPS 安全通道并且对传输的信息加密，实现了双层加密保护。业务安全方面分为业务安全 API 和风险控制两个部分，详细说明如下：

2.1 建立业务安全 API 保护用户登录安全：过对用户的登录、重要操作、信息来源等行为进行分析，判断是否正常的用户行为。其中业务安全 API（secapi）保护业务逻辑的安全，前端安全（secapife）保护业务接口的访问安全。通过这 2 个系统可以有效防止黑客利用网络上泄露的信息进行盗号、撞号、暴力破解用户账号等操作，保护用户账号安全。

2.2 建立风险控制系统，在应用层角度保护支付系统的安全，利用大数据分析用户登录、支付、消费等行为规律，从中识别出恶意用户和恶意的行为。有效防止恶意用户的盗卡、诈骗、非法支付等恶意行为，保护用户在支付和消费的安全。

3、建立 web 网络防火墙（WAF）系统，用于防御 XSS、SQL 注入、目录遍历、远程/本地命令执行等 web 应用程序的黑客攻击行为，有效保护用户的数据安全。

4、建立 QAegis 恶意行为拦截系统，通过分析 HTTP/HTTPS 的数据流量，识别并拦截恶意的攻击行为。可以有效阻止黑客利用自动化工具或恶意脚本等工具的攻击行为。阻止黑客进行批量刷票、洗号等恶意攻击。

5、建立网络层面的安全防护措施。在防火墙、交换机等网络出口设备上设置安全策略防御 DDOS 等网络流量攻击。同时我们和第三方安全服务提供商合作共同防御网络攻击行为，保证用户可以随时随地能够使用去哪儿网产品服务，保护用户权益。

6、搭建去哪儿网信息安全中心（Qics）系统，对数据库、中间件、web 服务器、运维系统、日志等系统进行定期安全检测，保证开发、测试、生产环境不存在安全漏洞间接保护了用户敏感信息和用护的合法权益。

B.实践效果

我们保护用户隐私的工作得到了同行的一致认可，并且公司通过了支付卡行业数据安全保护(PCI-DSS)、银联卡收单机构账户信息安全管理标准(ADSS)、塞班斯法案(SOX)等一系列行业安全规范。

用户可以放心使用去哪儿网的产品，在使用过程中，涉及到隐私信息的页面上会有部分提示信息，让用户知道我们是如何处理用户隐私信息。用户在使用过程中有疑问还可以和我们的客服联系，我们会耐心解答。

C.网民反应

评论 1：最近两年出去玩基本上都是在去哪儿上订的机票、酒店，界面简洁，操作起来很方便。不管是预订机票还是酒店，都有相当详细的介绍或者评论，价格也还是比较实惠的。付款比较方便，基本上都是刷信用卡或者银行卡，没有预付冻结一类的。

不过去哪儿网每次赠送的酒店红包这一类实在没什么太大用处，每次选的酒店都是豪华型的，用不了赠送的红包。

还是会继续使用去哪儿网的，用习惯了。

评论 2：去哪网算是名气很大的网站，比较放心。

评论 3：去哪儿网上的机票很便宜，经常可以买到折扣很高的机票，很值。虽然定的时候总要在别家注册，比较麻烦，不过能买到放心的特价机票还不是错的。

D. 推荐理由

去哪网作为上市公司，我们主动承担保护用户隐私的相应责任。我们将在每一个环节、每一个步骤都采取安全保护措施，通过技术手段、管理手段、让用户真正能够安全、放心的使用我们的旅游产品。为了回报用户对我们的信任，我们会继续努力去保护好用户的隐私信息。

公司简介

去哪儿网是中国领先的无线和在线旅游平台，成立于 2005 年 5 月，总部位于北京，业务覆盖机票、酒店、度假、会场等。凭借便捷、先进、人性的搜索技术，去哪儿网对网上机票、酒店、度假等信息进行整合，为用户提供及时的旅游产品信息比较服务。现在，去哪儿网的搜索范围覆盖全球 28 万余条国内及国际航线、约 103 万家酒店、85 万条度假线路、近万个旅游景点。未来去哪儿网将继续执行以投资回报率为核心的增长战略，帮助旅行者聪明地安排旅行。

案例 36：重要邮件加锁功能

A. 保护网民权益创新&优秀实践总体情况简介

【重要邮件加锁】功能是 2015 年底网易邮箱推出的重要安全功能。这个功能是系统通过发件人地址和邮件标题等关键字进行综合分析，对于用户重要的邮件进行加锁，用户在打开这些邮件的时候，需要输入手机收到的验证码才能打开邮件，最大限度保护用户的重要邮件不被他人窃看。

目前这项功能主要应用在 Apple 发来的帐号修复邮件上，也是应对目前 appleID 失窃日益严重情况的重要安全措施，所有的 apple 发过来的重要邮件我们都需要用户用手机解锁才能阅读，有效保护了网民的利益。我们计划这个功能逐步会开放给用户可以自定义自己的重要邮件并加以保护。

B. 实践效果

作为业内首创的专门针对苹果帐号的安全保护措施，重要邮件加锁功能从上线以来，一共保护了 2500 万封来自 apple 的重要邮件免受黑客侵犯，获得了用户的广泛点赞。

C. 网民反应

知乎网友主动发文称赞这个功能，并对其在安全性上的重要作用进行知识普及：“另外，有一些邮箱服务商比如网易邮箱针对 appleID 也推出了一个类似两步验证的保护措施，如果你使用网易邮箱，你会发现邮件不能直接看，而是这么一个提示……这等于给 APPLE ID 密码的邮件加了个锁。……这相当于是邮箱方面的两步验证。此类 APPLEID 盗窃都是大规模作业，虽然只是简单增加了一个手机验证操作，对于盗窃者来说，大规模的撞库破解这些都是通过程序实现的，如果需要手机验证就必须通过人工去完成，可操作性难度和风险都增加了很多，基本都会选择放弃。

“第一次碰到读邮件需要手机解锁开始还觉得有点麻烦，但细思恐极后，才发现网易这个做法实在太赞了！”

“我一直担心会不会被人通过邮件去修改我的 appleID，网易这个策略好让我放心了！”

“好像就只有网易邮箱想到通过这种策略保护用户 apple ID，虽然略嫌麻烦但还是很赞，有什么比安全更重要呢，我可不想我的手机变砖”

D. 推荐理由

网易邮箱是全国首家、也是唯一一家针对用户的重要邮件提供自动加锁保护服务的邮件服务商，在 appleID 失窃日益严重的背景下，此服务上线后即广受好评，虽然它会给企业增加大量的运营成本，但我们还是以网民安全和利益为首要考虑，第一时间推出这个功能，给用户带来更安全的保护。

案例 37：极致的反垃圾技术和成效

A. 保护网民权益创新&优秀实践总体情况简介

在 2015-2016 年里，网易邮箱在反垃圾领域投入了大量的人力物力，成为了国内为数不多的自主研发反垃圾平台的邮件运营商。基于海量数据和强大技术力量，网易邮箱的智能反垃圾系统对垃圾邮件的拦截率高达 98%，垃圾邮件误判率仅为十万分之一，优于国际十万分之三的业界标准，更优于国内大部分邮件服务商万分之一的标准。我们部署了一支专业的反垃圾队伍每天都在观察垃圾邮件的最新动态，并不断地调整反垃圾策略。过去的两年中，网易邮箱一共拦截了 338873417290（3389 亿）封垃圾邮件，对恶意用户进行禁用处理，一共禁用了 273011240（2.7 亿）个恶意用户，维护了全国电子邮箱邮箱的安全和通信的健康发展。

B. 实践效果

为了让广大用户得到洁净的电子邮件网络环境，网易坚决反对和抵制任何利用网易邮箱服务传输、分发或传送任何未经请求的大量邮件或商业电子邮件（垃圾邮件）。过去的两年中，网易邮箱一共拦截了 338873417290（3389 亿）封垃圾邮件，对恶意用户进行禁用处理，一共禁用了 273011240（2.7 亿）个恶意用户。

C. 网民反应

网友对于网易邮箱的反垃圾能力非常认可。网友评论说：“十几年里用了很多邮箱，网易邮箱是最清爽的，反垃圾技术非常成熟。比如，所有的垃圾邮件会被归类在垃圾邮箱的文件夹下，通过各个网站订阅的邮件都归类在订阅邮件夹，而且分类非常精准，很少出错。一些企业官方发来的邮件还会在邮件标题旁标注官方 LOGO，一眼就能识别。“我用了好多个不同的邮箱，网易邮箱的是最干净清爽的”

D. 推荐理由

网易作为中国互联网反垃圾邮件行业协会的发起人之一，同时也是电子邮件行业的排头兵和倡导者，深刻认识到垃圾邮件的毒害和影响，在反垃圾领域投入了大量的人力物力，成为了国内为数不多的自主研发反垃圾平台的邮件运营商。基于海量数据和强大技术力量，网易邮箱的智能反垃圾系统对垃圾邮件的拦截率高达 98%，垃圾邮件误判率仅为十万分之一，优于国际十万分之三的业界标准，更优于国内大部分邮件服务商万分之一的标准。

案例 38：建设点对点短信屏蔽功能，全力打造清朗网络空间

A. 保护网民权益创新&优秀实践总体情况简介

“是否想要接收”是用户判定垃圾短信的重要标准。运营商在整体治理的同时，应该兼顾用户的接收意愿，将特定号码的短信对拒收用户进行点对点屏蔽，满足用户在短信服务方面的个性化需求，全力打造清朗网络空间。

为保护客户权益，防范客户被同一号码反复骚扰，履行对客户投诉的垃圾信息采取必要的措施予以制止的义务，我公司建立了基于用户投诉的点对点短信屏蔽功能，对投诉与被投诉号码之间的短信进行屏蔽，确保客户投诉后不再收到被投诉客户发送的任何短信。

B. 实践效果

该功能实施以来，我公司已根据用户投诉情况，在 151 万余个客户间实施短信屏蔽功能，解决了用户被同一号码反复骚扰的问题。我公司受理用户点对点垃圾短信投诉量较实施前下降了 45.2%。

C. 网民反应

自从互联网越来越普及，普通人的手机号码就不再是个秘密。报复差评的淘宝卖家、聊过一次就天天纠缠的房屋中介、还有不知道从哪里得知我电话的推销员，这些人不断发来的短信对工作和生活造成了很大困扰，有了投诉后点对点屏蔽这个功能，我的短信箱终于可以由我做主，世界终于清静了。

D. 推荐理由

手机终端的普及使得“随时随地向任何人发送信息”的梦想成真。然而，越来越多的用户对于自己免受垃圾短信打扰的权利有了更高的要求。该功能从用户角度出发，基于用户投诉对特定号码的短信进行点对点屏蔽，实现了用户自主对通信底层规则的个性化定制，使用户不再依赖于第三方软件便可以实现对自身通信需求的自由控制，提高了用户在通信管理中的主动性。

案例 39：生物传感技术

A. 保护网民权益创新&优秀实践总体情况简介

新华网与荷兰国家数学计算机中心、英国诺丁汉大学、美国密苏里大学新闻学院等一流学术科研机构开展密切合作，共同研究开发生物传感技术，旨在开展广泛的用户行为研究。

新华网在北京总部建立中国首个用户体验传感实验室，运用生物传感技术深入研究用户感知行为。2015 年，新华网已在利用生理传感器进行用户体验研究方面取得重大突破与进展。“生理传感器研究用户反馈”项目可通过皮电传感与脑电传感获取用户无意识数据，经过模型分析得出体验评估报告，全面展现用户对媒体产品的体验与反馈过程，为提升用户体验提出科学依据。

B. 实践效果

2015 年，新华网推出国内第一代生物传感智能机器人“思达”（Star），打造用户生理数据和智能挖掘分析系统，在业界引起轰动。

新华网运用生物传感技术开展一系列大型实验并且进入实战应用领域。其中，新华网与国家话剧院合作开展英国经典舞台剧《战马》（中文版）的观众体验测试，通过皮电、脑电、心电、眼动、微表情等多种传感技术，监测用户兴奋度、专注度、心跳速率等一系列生理指标与情绪波动。获得极大成功。通过监测研究 150 名现场观众的观感体验，制作方充分了解了这部经典舞台剧会在观众中产生怎样的现场反应，究竟哪些瞬间、哪些细节最能打动观众的心灵，为将来剧目的制作和指明了方向。

C. 网民反应

网友表示，新华网的生物传感技术很有意思，能够监测和客观反映所有现场观众对于这部剧的体验，反馈结果。这在以前我们自己看表演时是完全无法实现的。这项技术也帮助我们客观的认识自己。

D. 推荐理由

新华网以生物传感技术在传媒领域应用为主线，强化在生物传感领域已经取得的特色，重新定义对于自身、对于生命的认知与感知需求，不断深化用户观感和用户行为的研究，实现不同分类用户分析，有利于打造“千人千面”的传媒产品，提升产品的个性化和定制化程度，大幅改善传媒产品的用户体验，有效满足用户需求。

公司简介

新华网是国家通讯社新华社主办的综合新闻信息服务门户网站，是中国最具影响力的网络媒体和具有全球影响力的中文网站。依托新华社遍及全球的强大采编力量和权威内容发布，新华网 24 小时为全球网民提供最权威最及时的新闻信息服务，用户遍及 200 多个国家和地区，桌面端日均页面浏览量超过 1.2 亿，移动端日均覆盖人群超过 1.3 亿，重大新闻首发率和转载率遥遥领先国内其他网络媒体。

据全球权威网站排名机构 Alex 数据显示，2015 年，新华网在全球 7 亿多个网站中综合排名第 70 位，大幅领先美联社、路透社、法新社等通讯社主办的网站。在中央网信办主管的《网络传播》杂志发布的中央重点新闻网站传播力榜单中，10 月、11 月综合传播力排名首位，远超同类网站。

案例 40：恶意搜索内容拦截

A. 保护网民权益创新&优秀实践总体情况简介

近几年出现的针对搜索引擎的恶意 SEO，在大型网站搜索非法恶意的内容，并通过搜索引擎传播非法内容、诈骗内容、恶意广告等。针对以上情况，我们基于机器学习开发了恶意搜索内容拦截系统，主要的工作是：

1、建立 QAccesslog 访问日志收集系统，收集统计访问去哪儿网的全部信息，提取并分析搜索引擎爬虫的日志内容。

2、开发基于机器学习的恶意搜索行为检测系统，如存在恶意搜索内容则自动拦截，利用贝叶斯算法进行分析学习，经过多次迭代学习后可以将恶意内容识别率成功率达到 98%。

3、开发 QAegis 恶意行为拦截系统，利用机器学习识别并拦截所有的恶意搜索内容。当系统检测到来自搜索引擎爬虫时，会自动调用机器学习的接口进行分析判断和拦截操作。

4、开发搜索内容黑/白/灰名单管理系统，将非法的搜索内容直接拦截掉。对于用户搜索的内容，利用黑/白/灰名单进行分析判断和拦截。

B. 实践效果

经过实践后的统计分析，我们可以将来自搜索引擎爬虫的恶意内容数量降低至 2%，有效拦截了非法内容、欺诈内容、恶意广告等，提升网站的安全性，保证用户能够安全有效使用去哪儿网服务。

C. 网民反应

评论 1：在去哪儿网上展示的产品都真实可靠，没有虚假诈骗的信息。

评论 2：很实用，每次想订机票首选就是上这个网站搜索，最终确定在哪儿订票。不过有很多不靠谱的网站，不敢随意订，之前订的几次碰巧最低价的票都是携程或者航空公司出票的，所以很放心的订了。总体感觉还是不错的～

D. 推荐理由

基于机器学习的恶意内容识别，可以自动、高效、精确拦截非法和恶意信息。

公司简介

去哪儿网是中国领先的无线和在线旅游平台，成立于 2005 年 5 月，总部位于北京，业务覆盖机票、酒店、度假、会场等。凭借便捷、先进、人性的搜索技术，去哪儿网对网上机票、酒店、度假等信息进行整合，为用户提供及时的旅游产品信息比较服务。现在，去哪儿网的搜索范围覆盖全球 28 万余条国内及国际航线、约 103 万家酒店、85 万条度假线路、近万个旅游景点。未来去哪儿网将继续执行以投资回报率为核心的增长战略，帮助旅行者聪明地安排旅行。

案例 41：多措并举，积极响应，打击电信诈骗

A. 保护网民权益创新&优秀实践总体情况简介

一、封堵恶意域名，肃清电信诈骗行为

北京联通近期根据管理局的统一部署，开展移动互联网电信诈骗专项行动，通过对涉嫌钓鱼的恶意网站进行封堵，达到保护最终用户的目的。北京联通收到任务后，积极组织，高度重视，组织相关部门梳理工作各项流程。目前，北京联通通过在 DNS（域名解析）平台进行操作，达到封堵的目的。工作过程中，克服了人员少，任务重等诸多困难，出色的完成了相关工作，得到了管理局的认可。经过一段时间的运行，达到了专项行动的预期。

钓鱼网站通常指伪装成银行及电子商务，窃取用户提交的银行帐号、密码等私密信息的网站。时下流行的网购也是钓鱼者的主要目标，假冒网上购物、在线支付网站往往能欺骗网民直接将钱打入黑客账户；恶意团购网站或购物网站也可能假借“限时抢购”、“秒杀”等噱头，骗取用户个人信息和银行账号；国内知名 C2C 商城淘宝网、B2C 网站京东商城，乃至第三方支付平台快钱等都曾经经受假冒钓鱼网站的侵害，钓鱼者已经明目张胆地将陷阱布置到了普通网民的脚下。

北京联通 DNS（域名解析）平台承载北京联通城域网、移动网域名解析服务。2016 年 3 月，北京联通 DNS 平台与北京市通信管理局联动，通过封堵域名解析的方式，达到关闭钓鱼网站的效果，阻止钓鱼网站的传播。目前系统累计封堵恶意域名超过 5000 多个域名。

B. 实践效果

一、封堵恶意域名

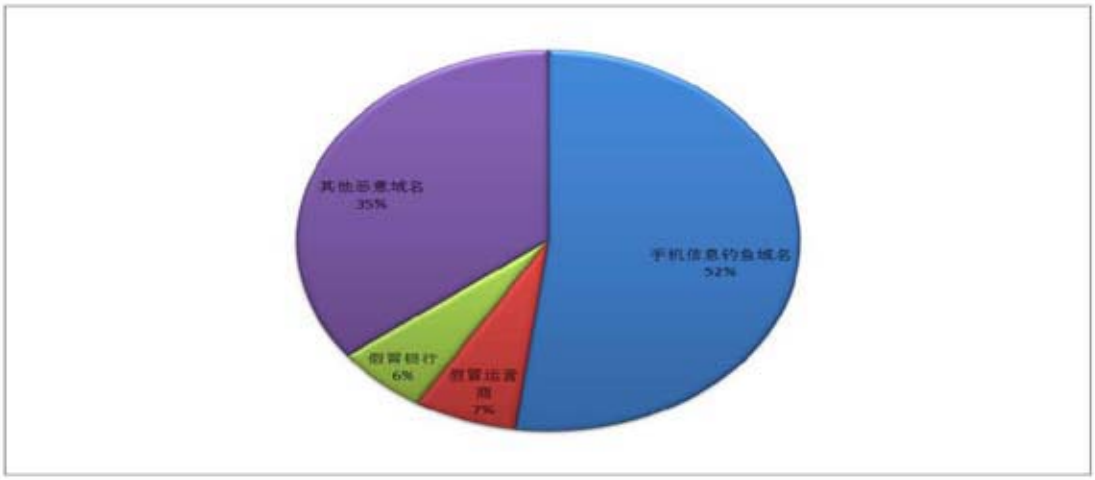
众所周知，钓鱼网站实际是一种网络欺诈行为，是不法分子利用各种手段仿照真实网站的网址及页面内容，或者利用真实网站服务器上的漏洞，在网站的某些页面中插入危险的 HTML 代码，以此来骗取用户银行和信用卡账号、密码等私人资料。钓鱼网站传播途径最主要为即时通讯工具和社交网络，这些钓鱼网站不仅页面制作精良，同正规官网相似度极高，而且惯用一些极易混淆的字符做域名。

北京联通 DNS 平台利用黑名单机制，在北京市通信管理局统一行动中，对恶意域名予以封堵，保障北京联通网络、移动用户免受电信诈骗网站的影响，保护了用户隐私信息、资产安全。

封堵的域名分类：

二、认真分析，建立打击诈骗的长效机制

北京联通在积极组织进行封堵的同时，加强了对钓鱼网站的多维度分析，希望从中发现某些重要规律，为打击工作提出更加有效的意见与建议，尽快建立打击工作的长效机制。



从网站域名的注册环节入手，通过互联网查询等公共信息获取渠道，对各类网站进行分类汇总，发现非法网站的某些共性的信息。例如，犯罪团伙通过几个账号，通过国内的域名

注册代理机构，注册了大量的域名。通过这些线索的掌握，在一定程度上可以从根源上增加犯罪团伙的犯罪难度。

多措并举，共同打击电信诈骗。经过一段时间的工作，北京联通已经对钓鱼网站封堵积累的一定的经验同时，将不断晚上各类技术手段的应用。包括尝试使用技术手段，对移动互联网用户对不法网站链接进行干预、对涉嫌诈骗的 IP 地址进行封堵等工作。同时，加大伪基站的打击力度，从根本上杜绝此类诈骗行为的发生。

不断完善、建立长效机制。目前采用域名的封堵的方式，对公安部门认定的钓鱼网站进行有针对性的封堵。经过一段时间的磨合，下一步北京联通将不断优化流程，将目前十分钟之内处置完毕的时间继续保持下去。同时，与公安、管局等多部门，共同商讨，逐步延长封堵网站的封堵期限，最终实现，一次确认，长时间封堵的目的。

C. 网民反应

一说起电信诈骗，从事 IT 行业的白领 X 先生一脸的无奈，“说真的，现在各种推销电话、短信满天飞，真假掺杂，我真的不懂该怎么分辨哪些是真，哪些是假了。”是的，我们已经不能再相信任何一个来电或者短信，哪怕它来自至亲、好友、大型企业或是公众服务机构，电信诈骗问世仅十多年时间，却正在摧毁了我们用一生建立的信任。北京联通正积极配合公安部门打击电信诈骗行为，即使用户不小心点击了不安全的链接或网站，由于恶意域名已遭到封堵，诈骗内容也无法显示，犯罪分子的阴谋无法得逞。

D. 推荐理由

具备畅通的流程，完备的机制，实施效果明显，有效地保护网民权益，具有实践性和示范性。

公司简介

中国联合网络通信有限公司北京市分公司隶属于中国联合网络通信有限公司，是北京地区实力雄厚、品牌强劲的全业务电信运营商，长期致力于北京市信息化基础设施建设，在全市范围内为公众客户、商企客户和政府机构等客户提供包括固定电话、移动电话、数据传输、互联网、宽带接入等基础电信业务和增值电信业务，以及与上述业务相关的行业应用、系统集成、技术开发、技术服务、信息咨询、工程设计施工等相关服务。

案例 42：手机通信卫士

A. 保护网民权益创新&优秀实践总体情况简介

本产品打造手机安全的新高度，将整个移动核心网络升级为用户的“通信卫士”，能够面向所有手机用户提供普遍服务而与手机型号、操作系统能够无关；并可将安全范畴拓展到泛安全领域，通过流量提醒、提供安全认证的应用软件下载平台，为用户和移动通信网络打造一个安全绿色的手机使用环境。

B. 实践效果

1、用户无需安装任何手机安全软件，无需具备专业知识，就可以享用到智能网络管道所提供的全方位安全防护—发现病毒并及时处置、发现诈骗电话并及时提醒、实时拦截垃圾短信和骚扰电话、用户速率感知提示、伪基站短信拦截等。

2、用户在访问页面时，页面的顶部、中部、底部按照用户兴趣图谱和行为路径，展示基于用户喜好的个性化内容和安全上网提醒服务，插入页面不影响用户正常浏览上网。

3、用户可以及时收到网络侧监控到用户手机的病毒发作的告警短信。

C. 网民反应

装了通信卫士产品后，少了很多不必要的垃圾信息骚扰。一些广告类、促销类的垃圾短信直接到了垃圾箱，骚扰电话直接屏蔽过滤。另外，还提高了对诈骗等垃圾短信的警惕，减少了上当受骗等经济损失。

D. 推荐理由

我公司通信卫士产品，率先在面向最终用户的安全服务上采用移动互联网主动防御理念应对病毒及安全问题，改变了传统依靠终端侧软件或者用户投诉解决用户安全问题的被动局面。用户无需安装任何手机安全软件，无需具备专业知识，只要在使用移动互联网络就可以享用到运营商智能网络管道所提供的全方位安全防护—发现病毒并及时处置。推荐作为保护网民权益创新案例产品。

公司简介

恒安嘉新（北京）科技有限公司（下称“恒安嘉新”）成立于 2008 年 8 月，是国内领先的网络与信息安全解决方案提供商。公司是国家级高新技术企业、北京市软件企业和中关村高新技术企业，核心业务定位于移动互联网和互联网网络与信息安全服务、产品及增值业务，拥有“云-管-端”一体化的解决方案。

案例 43：号码标识联盟

A. 保护网民权益创新&优秀实践总体情况简介

当前社会信息泛滥、骚扰诈骗电话高发，陌生号码标记识别功能已成为大部分智能手机、安全类软件的标配，但孤立的号码标记信息有很大的局限性，很难做到有价值的标记信息为社会所共享。为消除标记信息孤岛，让标记数据可以在云端自由充分流通，电话邦联合业内企业发起成立号码标识联盟，致力于通过大数据技术，人人标、人人识，不断净化通讯环境。

B. 实践效果

号码标识联盟通过人人标，人人识的方式帮助大家预防诈骗，用户在接到陌生电话后可按照通话性质进行标记，这样其他用户在接到相同电话时就能提前知晓对方的身份，很大程度上帮助用户避免了骚扰、诈骗等电话的侵袭，减少了财产损失。

截至目前，联盟成员覆盖小米、腾讯、百度、阿里、联想、中国移动、中国联通、华为、中兴、OPPO、VIVO、努比亚、金立、美图、乐蛙、蜗牛移动、公信卫士、LBE 安全大师、安医生等三十余家。

据号码标识联盟统计，2015 年手机用户在平台标记骚扰诈骗电话共计 1708 万个，平均每天有 8000 万次骚扰诈骗电话呼出，年呼出约 290 亿次；假设每通电话时长 5 秒，通话时长累计可达 12.7 年。

C. 网民反应

网民认为这种人人标、人人识的方式可以让大家都参与其中，互相帮助，减少陌生电话带来的恐慌感，在标记的同时自己也受益，感觉自己对骚扰诈骗电话的标记更有意义了，有一种神圣的责任感，同时减少了财产损失，很大程度上避免了电信诈骗，有效减少了上当受骗的现象。

D. 推荐理由

联盟充分利用号码大数据分析处理技术，激发每个手机用户的主观能动性，标记身边的骚扰诈骗电话，避免了更多人上当受骗、蒙受损失，同时为通讯环境的净化做出了一定贡献。

公司简介

北京羽乐创新科技有限公司成立于 2012 年，电话邦是其主营品牌。国内数据现已收录 6500 万商业机构的 8500 万个电话号码，有 12 亿+的数据总量，号码覆盖 370 多个城市，海外数据覆盖印度、东南亚、美国等国家和地区，是最全最准的电话号码库。

电话邦与 30 余家终端达成深度合作，覆盖超过 7 亿用户，日活跃用户达 1.32 亿，致力于联合入口方、生活服务提供方构建基于电话号码的生态圈，与各方协力共生、生态互赢，为更多中小企业提供可信号码生态服务。

案例 44：360 手机卫士骚扰电话拦截

A. 保护网民权益创新&优秀实践总体情况简介

360 手机卫士骚扰拦截可以通过本地以及云端数据对电话号码进行识别并且拦截，重点识别疑似欺诈、广告推销以及骚扰电话等，帮助网民第一时间获取电话信息并且提高警惕，让骚扰电话没有施展的空间。同时，根据亿万卫士用户的标记行为和服务端对号码行为的判断识别进行实时更新标记号码库，提高了卫士对骚扰电话判断的准确率和覆盖度。此外，网民还可以根据自身使用习惯设置个性化号码拦截规则，可以针对特定号码类型、号码标记次数、时间以及特定号码进行拦截，增强了骚扰拦截功能的灵活性和定制化。

360 手机卫士电话拦截通过与外部合作，对整个行业治理骚扰诈骗电话起到了积极的促进作用。近年来，卫士一直与 12321 在网民号码标记方面保持密切的合作关系，通过数据的提供与比对，有效提升 12321 工作的准确性：依托举报信息，建立行业内诈骗信息的通报机制，点出问题、特点和趋势，作为对运营商（含虚拟运营商）的排名、考核等参考；依托用户举报，建立涉嫌诈骗电话号码的核查、处置机制。本次合作对用户举报信息的后续处理有很大价值。

B. 实践效果

2016 年第一季度，360 手机卫士共为全国用户识别和拦截各类骚扰电话 48.0 亿次，平均每天识别和拦截骚扰电话 5270.6 万次。在电话来电的第一时间用户可以看到该号码的标记信息和类型，并根据用户个性化设置挂断骚扰电话，防止疑似诈骗、骚扰电话、广告推销等电话给网民造成经济损失。

C. 网民反应

360 手机卫士电话拦截功能得到了用户广泛好评，以下评论摘自用户反馈后台、各大应用市场以及微博微信等公众评论："骚扰拦截功能是我最常使用的功能，能够帮我识别诈骗电话，直接拦截…"

"以前总是被各种骚扰电话打扰，安了 360 手机卫士这些问题都解决了…"

"安了 360 卫士，接电话的时候就能看到这是个骚扰电话，还能调戏骗子呢…"

D. 推荐理由

之前，骚扰电话已经对网民造成极大的困扰，网民被电话诈骗高达数十万元的案例层出不穷，被广告推销电话骚扰令人头疼却无能为力。360 手机卫士作为一款安全类软件，对于保障网民的财产安全、通话安全责无旁贷，通过强大的电话数据信息实现了对诈骗电话、骚扰电话以及广告推销的识别能力，能够帮助网民在第一时间识别号码的真正面目，并通过亿万网友的标记行为和自身专业的技术能力不断扩充和精准标记号码库，实现了在行业内的领先水平，为广大网友的电话安全提供了强有力的保障。

公司简介

奇虎 360 科技有限公司创立于 2005 年 9 月，是中国领先的互联网和手机安全产品及服务供应商。致力于提供高品质的免费安全服务，360 公司的使命是利用互联网安全技术，依托于大数据和云计算，为中国数以亿计的用户提供具有极至体验的软硬件产品，守护儿童安全、家居安全、出行安全和数据安全，让每个人都有安全感。

案例 45：猎网平台

A. 保护网民权益创新&优秀实践总体情况简介

猎网平台是由北京市公安局网络安全保卫总队与 360 公司联合发起成立的一个警、企、民联动的网络诈骗全民举报平台，面向全国网民征集网络诈骗举报线索。网民通过猎网平台

举报的每一条网络诈骗犯罪信息，都将通过平台的大数据分析系统进行关联分析和线索综合，为公安机关提供迅速、全面、有效的破案线索和证据链。

B.实践效果

2015年，猎网平台共收到全国用户提交的网络诈骗举报24886例，举报总金额1.27亿余元。

1）地域关联

在猎网平台上，网络诈骗的受害者将不再是孤立无援的。被同一个网络诈骗团伙诈骗，但分散在全国不同地区的受害者的举报信息将会被进行自动的关联分析，从而复原出这个犯罪团伙在全国各地犯罪活动的全貌，为公安机关跨地域打击网络犯罪的提供有力的支撑。

2）金额汇聚

也许一位受害者仅仅被骗100元，根本达不到立案标准。但通过猎网平台，我们在全国各地找到另外29为有相同遭遇的受害者，这样一来，经过串并案分析，犯罪分子的涉案金额就达到了3000元的立案标准，公安机关就可以正式立案并据此抓捕犯罪分子。而且一旦犯罪分子被抓，每一位用户的举报信息都将成为加重对犯罪分子量刑的砝码！

3）线索串并

网络诈骗犯罪过程中会使用到多种作案工具，如木马病毒、钓鱼网站、电话号码、QQ号码、诈骗短信等。猎网平台通过讲用户的举报信息与360既有的恶意网址库，恶意程序库、恶意号码库、恶意短信库等信息进行深度关联分析，就能够全面掌握犯罪分子使用作案工具的情况及其相互关联性，并进而迅速的形成一条完整的、结构化的证据链，为公安机关迅速梳理破案线索，迅速侦破网络诈骗案件提供有力的技术支持。

并且，猎网平台每季度发布网络诈骗趋势报告，报告中不仅分析了当前最新的网络诈骗类型，人均损失，受害者分布等情况，把握诈骗最前沿动态，并且总结时下最流行的案例，还原整个诈骗过程以及诈骗犯罪分子的作案手段，应用的技术方法。从而帮助警方及普通用户更加具体的了解诈骗过程，提示防骗信息。

并拍摄了50余部网络防骗视频提供给广大网民，帮助其增加防骗技巧和意识。仅春节前期，拍摄的“哎呀回家”三部系列防骗短剧，在春节前一周的收看量达到600万次以上。与网安联合拍摄的网络安全剧《老马家那点事儿》在北京科教频道现场说法中播出，取得了较高的收视率。

C、网民反映

猎网平台不仅可以举报网络诈骗，其微博、微信的公共号还能提供防骗小知识，分析最新热点诈骗案例，提醒我们谨防上当；

猎网平台的网络诈骗小视频，轻松幽默，在观看的同时还能告诉我们诈骗案例，从而提高了防骗意识；

在猎网平台举报，工作人员还会给电话回访，详细记录诈骗的过程，其实有些时候自己也说不清楚，但经过工作人员的梳理，明白了被骗的全过程，同时也增强了自己的防骗意识。

D.推荐理由

网络诈骗往往具有异地作案，小额多发，取证困难等特点。

1）异地作案

网络诈骗过程中，骗子们与受害者往往不在一个城市，不仅受害者可能遍布全国各地，甚至诈骗产业链上下游的犯罪分子们也可能是来自全国各地。这就为公安机关获取破案线索造成了很大的难度。

2）小额多发

尽管也时有被骗几十万，上百万的受害者出现，但绝大多数网络诈骗犯罪造成的单笔损失都在几百元到3000元以下，而一般情况下，涉案金额低于3000元，公安机关是无法立案

的。这就使得很多犯罪分子尽管骗了几百人、几千人，但由于单笔诈骗金额都很小，所以得不到法律的制裁。

3）抓捕困难

侦破网络诈骗案件，获取犯罪嫌疑人的行迹信息，往往需要对多种来源，多种纬度的情报信息进行综合性的关联分析。但各地用户的零星报案，往往难以汇聚在一起，难以形成情报的有效汇聚和结构化分析。

而网络诈骗犯罪近年来呈现持续高发的状态。按照最保守的估计，当前专门从事网络诈骗的犯罪分子人数超过 180 万，涉案金额超过 1000 亿元，而且已经形成了分工明确，组织严密的产业链。面对有组织，成规模的网络诈骗犯罪，传统的打击与防范体系已经很难奏效，我们需要一个全国联网的，全民举报的。警、企、民联动的新型反诈骗工作体系。而这正是猎网平台的目标、价值与意义。

案例 46：国内最专业的网络安全志愿者

A. 保护网民权益创新&优秀实践情况介绍

背景：2016 年 1 月 11 日，在中央综治办、中央网信办、公安部和团中央的大力支持下，“互联网安全志愿者联盟”在杭州召开成立大会。联盟成员遍布全国 29 个省市自治区直辖市，由全国 276 所高校在校生、全国诚信商盟，以及各行各业热爱公益、关注网络安全的社会人士组成，包括残联的残疾朋友，日常在线活跃人数 5000+。团队的梦想：“志愿守护净土，共创网络安全。”

B. 实践效果

9 年以来，互联网安全志愿者联盟总计举报 15 亿人次，团队成员遍布全国 29 各省市自治区直辖市。安全业务覆盖了互联网禁限售、假货、欺诈等 10 多条业务线的违法违规信息举报，并在线解答会员安全疑问。例如互联网安全志愿者联盟-诚信商盟的志愿者们，因为长期在互联网上从事举报违禁商品（枪支弹药黄赌毒等），同时对网络交易欺诈抓骗子等工作，了解网上骗子行为及特征，串联关系一同举报。此外对大数据侦查假货工作，专业志愿者们有自己的操作模式，较大量的举报网上售假商品。例如互联网安全志愿者联盟-高校联盟的志愿者们，对网络灰产举报较为擅长，对学校周边代写论文，带上课等网上违禁售卖的服务举报精准。专业的志愿者们在自己擅长的领域，每天每小时举报着违规信息。

C. 网民反应

1、“互联网安全”上升为“国家安全”，只有安全的网络环境才能切实维护网民权益。

2、全国政法类院校积极参与这支专业网络安全志愿者团队，仅 2016 年 3 月 1 日在中国刑警学院的一场专场招募活动，就有 2700 多师生报名参加。

3、清华大学多名博士和硕士生加入这支志愿者团队，在危险化学品举报方面做出积极贡献。

D. 推荐理由

1. 大幅度减少网络安全欺诈案件，切实保护网民利益。

2. 极大增加网民对互联网网购的信心，进一步促进网络安全的发展。

公司简介

【互联网安全志愿者联盟】

目前中国网络安全领域最专业、有梦想、有情怀、肯付出的民间志愿者精英联盟。团队隶属阿里巴巴集团安全部，2007 年 9 月成立，当年注册名“杭州市网络反欺诈志愿服务队”。9 年来累计举报网上各类违规、违法信息高达 15 亿人次。2016 年 1 月 11 日，在中央综治办、中央网信办、公安部和团中央的大力支持下，这支团队升级为“互联网安全志愿者联盟”，联盟成员遍布全国 29 个省市自治区直辖市，由全国 276 所高校在校生、全国诚信商盟，以及各行各业热爱公益、关注网络安全的社会人士组成，包括残联的残疾朋友，日常在线活跃人数 5000+。团队的梦想：“志愿守护净土，共创网络安全。”

案例 47：泄漏订单自动溯源

A. 保护网民权益创新&优秀实践情况介绍

背景：在开展治理电商交易订单在电子商务生态中的信息泄漏问题工作中，信息泄漏的溯源和定位是最基础并且最核心的环节，而电子商务生态中与交易订单有关的角色、系统错综复杂，无疑又极大地增加了信息泄漏溯源的难度。阿里巴巴生态安全团队结合大量信息泄漏治理的工作积累和大数据分析技术，总结经验并建立了一套完整的已泄漏的交易订单在电子商务生态中自动溯源的产品。

创新方案：通过建立整个电子商务生态中交易订单数据流转的全链路日志，其中包括但不限于电子商务平台自身、第三方软件系统、核心物流商处理交易订单的全链路日志，并借助大数据分析对每一笔存在诈骗行为反馈的交易订单进行全链路、全方位的分析，最终自动产出造成交易订单的泄漏途径。

B. 实践效果

截止 2016 年 3 月，搜集汇总的所有泄漏订单中 75%的泄漏订单可以通过自动分析产出泄漏途径，其中泄漏途径涵盖平台、商家、第三方软件提供商、物流四个大类，具体子类多大二十余种。

人工排查平均所需时间为 2-3 天，而自动分析最快可以在接受到外部反馈后 1 小时便能定位泄漏途径，极大的缩短信息泄漏事件的持续时间。

C. 网民反应

商家、第三方软件服务商以及物流商对于自动分析产出的结果给予的极大的认可。

D. 推荐理由

1. 极大的提升了交易订单泄漏的溯源效率。

2. 极大增加第三方软件提供商以及商家对信息泄漏治理的信心，进一步促进电子商务生态的发展

公司简介

阿里巴巴集团经营多元化的互联网业务，致力为全球所有人创造便捷的交易渠道。自成立以来，阿里巴巴集团建立了领先的消费者电子商务、网上支付、B2B 网上交易市场及云计算业务，近几年更积极开拓无线应用、手机操作系统和互联网电视等领域。集团以促进一个开放、协同、繁荣的电子商务生态系统为目标，旨在对消费者、商家以及经济发展做出贡献。

案例 48：垃圾短信拦截

A. 保护网民权益创新&优秀实践总体情况简介

360 手机卫士短信拦截功能，是根据大数据分析并建立了一系列的诈骗及骚扰短信模型，配合其他识别规则在用户收到短信时进行智能匹配是否属于骚扰或诈骗短信。

若分析识别为诈骗短信时将直接弹窗提示用户此条短信有高危风险请不要点击/回复，极大的降低了用户受到诈骗的概率，保护了用户的财产安全。若识别为骚扰短信时将把骚扰短信收录到 360 手机卫士的『骚扰短信』模块，将打扰用户的频次降到极低，还用户一个清爽干净的短信箱。

B. 实践效果

2016 年第一季度，360 手机卫士共为全国用户拦截各类垃圾短信约 49.8 亿条，较 2015 年第一季度的 96.9 亿条同比大幅下降了 48.5%；平均每天拦截垃圾短信 5484 万条，其中垃圾短信中广告推销最多，占比为 93.8%，其次是诈骗短信（2.0%）和违法信息（1.2%），对诈骗短信作进一步分类，其中身份冒充银行类诈骗短信占比最高，为 73.1%，其次是冒充电信运营商（11.4%）、打款短信（3.3%）以及其他诈骗短信（12.2%）。

即每天为用户报出诈骗短信 110 万条，根据统计用户平均受骗金额为 6140，相当于挽救了十亿级人民币级的潜在财产风险。

C. 网民反应

“现在信息泄露太严重了，我之前收到过一条短信，还知道我名字，让我帮忙点击短信里的网址给他孩子投个票，如果不是 360 提醒我是诈骗短信的话我可能真就点击上当了”赵女士接受反馈时表示，360 手机卫士不仅能够拦截垃圾短信还能提醒诈骗，很大程度避免了广大用户上当受骗。

D. 推荐理由

智能手机越来越普遍，大家注册使用的 APP 也越来越多，当你用手机号注册的时候就相当于要接受众多服务号的短信打扰，并且还存在号码被泄露的风险的，随着移动设备智能化越来越普遍用户收到骚扰和诈骗短信的几率不但不会降低反而会大大增加。360 手机卫士基于大量的数据进行分析构建了识别能力极强的拦截模型，在非常大的程度上保护了用户不受垃圾短信的打扰以及诈骗短信欺骗，于此同时还主动保护用户支付类短信，防止被窃取，可谓全方位的防护用户的短信安全。

公司简介

奇虎 360 科技有限公司创立于 2005 年 9 月，是中国领先的互联网和手机安全产品及服务供应商。致力于提供高品质的免费安全服务，360 公司的使命是利用互联网安全技术，依托于大数据和云计算，为中国数以亿计的用户提供具有极至体验的软硬件产品，守护儿童安全、家居安全、出行安全和数据安全，让每个人都有安全感。

案例 49：360 手机卫士手机先赔险

A. 保护网民权益创新&优秀实践总体情况简介

360 手机卫士的手机先赔功能，对用户在进行手机支付、网址访问或者在接收短信时，自动识别钓鱼网址和木马，有效的保护用户的个人隐私安全；并且如果开启手机先赔功能的

用户因为收到钓鱼网址或者木马短信诈骗遭受损失，能通过 360 手机卫士来申请理赔，符合理赔条件的用户会获得相应的赔付金，将用户损失降低到最小，同时提升产品的防护能力。

B. 实践效果

目前手机先赔有 6500 万用户使用，每天有 300 例理赔用户申请，反馈的诈骗案例有伪基站、网购钓鱼、个人隐私盗号诈骗等当前最流行的网络诈骗手法，通过对用户反馈的理赔进行审核，对一部分符赔付的用户给予赔付，同时将用户的这些举报案例提供给网络警察，配合警方来打击此类诈骗团伙；并且通过媒体传播让更多人知道、预防这些网络诈骗。

C. 网民反应

“本来想在网上买手机，结果刚买完客服就给我打电话说要退款，我加他 QQ 之后在一个网址填了信息，结果银行卡里的钱就没了。幸亏有 360 手机卫士，我之前开通了先赔险，还拿到了一部分赔偿。”网友小赵收到赔付时表示。360 手机卫士不仅在技术上保护手机安全，还通过先赔保障尽量减少用户损失。

D. 推荐理由

智能手机支付越来越普及，针对手机支付的陷阱也层出不穷。通过 360 手机卫士不仅可以帮助用户辨别和拦截钓鱼网站、诈骗短信、诈骗电话，还可以免费开启 360 手机卫士先赔险，遇到手机诈骗造成财产损失，也可获得相应赔偿，挽回损失。

案例 50：360 手机卫士程序锁

A. 保护网民权益创新&优秀实践总体情况简介

360 手机卫士的程序锁是将用户需要保护的手机应用设置上密码，就能成功将应用锁住。无论谁要进入这些加锁应用都需要输入密码，可以有效的保护用户的隐私与信息的安全。基于加锁的基本功能，还提供给用户输错密码就给偷窥者拍照，人脸解锁以及指纹解锁等更多趣味功能。

B. 实践效果

360 手机卫士的程序锁目前平均每天有超过 800 万用户使用，使用人脸解锁的用户达 200 万，抓拍偷窥者超过 7000 万次。

C. 网民反应

360 手机卫士程序锁功能上线一个月就被用户评为最喜欢的新功能，被用户评为手机界的“锁哥”。网友评价程序锁“既能保护隐私，又好玩，是个有意思的功能。”程序锁功能专门用于守护用户手机中的各种 APP，在全面保护用户隐私信息的基础上，更增加了科技感强的刷脸解锁和指纹解锁。

D. 推荐理由

360 手机卫士一直以来重视对用户隐私的守护，程序锁功能很好的守护手机中的隐私信息。用户可以自行选择为每个应用上锁，任何不想让别人随意打开的应用只需加个锁。此外，还为这些应用定制个性化解锁程序，用户甚至可以选择计算器样式的解锁界面；独家的人脸解锁，不但安全便捷，而且提供了炫酷的科技感体验；不仅有效保护用户手机隐私安全，顺便还可以偷拍“偷窥者”。

案例 51：北京联通配合公安部《打击治理电信网络新型违法犯罪专项行动》

A. 保护网民权益创新&优秀实践总体情况简介

北京联通为配合公安部《打击治理电信网络新型违法犯罪专项行动》，严厉打击电信网络新型违法犯罪，从 2015 年 11 月，开展为期半年的打击治理专项行动。公安部在此期间 7*24 小时向违法号码所属的运营商提供关停号码。北京联通积极响应公安部要求，利用现有系统条件，短时间内，制定完成了相关业务支撑流程及管理办法，负责关停所属违法号码。

B. 实践效果

从 2015 年 11 月到 2016 年 3 月，北京联通共收到公安部发来的停机文件 56 批次，涉及北京联通号码 1518 个。同时，通过技术手段，拓展查询到违法号码的关联号码 4368 个，提供给公安部作为参考；根据公安部门涉及境外通信诈骗的案件特点，对国内受害方事主，实施保护性通话阻断和短期停机，自 2015 年 8 月至 2016 年 3 月底，北京联通对涉及通讯诈骗的受害方采取保护性通话中断并停机的用户达 292 户。此项工作开展以来，北京联通既保证停机操作 100%正确无差错，又保持着停机处置的工作效率，建立快速处理通道，当日接收的停机通知当日全部完成，并及时向公安部反馈处理结果，对于保护性停机用户实现随时关停的工作能力，助推公安部打击电信网络新型违法犯罪工作的顺利进行。

C. 网民反应

配合政府开展打击治理电信网络新型违法犯罪，有效防范用户遭受电信诈骗的风险，实现电信诈骗案件、群众损失明显下降；据公安部门情况反馈，国内涉及诈骗的事主，由于北京联通及时有效的通话阻断措施，最高挽回用户达百万元损失。

D. 推荐理由

与政府建立联动机制，多举措并行，保护网民权益效果显著。

公司简介

中国联合网络通信有限公司北京市分公司（以下简称：北京联通）主要经营固定通信业务，移动通信业务，国内、国际通信设施服务业务，卫星国际专线业务、数据通信业务、网络接入业务和各类电信增值业务，与通信信息业务相关的系统集成业务等，是北京地区实力雄厚、品牌强劲的全业务电信运营商，广泛服务于国家和北京市党、政、军及企业客户，为广大公众用户提供基于固定通信网络和移动通信网络服务，服务面积 16800 平方公里。

案例 52：中国移动整治钓鱼诈骗网站实践

A. 保护网民权益创新&优秀实践总体情况简介

钓鱼网站通常指仿冒银行、运营商、网上商城等官方网站的 URL 网址以及页面内容，以此来窃取用户提交的姓名、身份证、银行账号及密码等个人信息。不法分子利用窃取的个人信息，进行网上支付账号的恶意盗刷，给消费者造成巨额损失，严重侵害了客户的合法权益。

为维护网民的合法权益，在上级单位指导下，针对假冒中国移动的钓鱼网站，依托不良信息集中管控平台，与国家互联网应急中心（CNCERT）、中国互联网络信息中心（CNNIC）开展联动治理，建立了钓鱼网站集中治理工作体系：对于系统拨测、客户举报、联动监测发现的疑似钓鱼网站，开展了 7*24 小时的不间断高效处理流程，对确认违规的钓鱼网站进行一键封堵和下线处置。

B. 实践效果

截至 2016 年 3 月底，累计主动监测处置假冒中国移动的钓鱼诈骗网站信息 23.8 万余件，核实封堵违规网站 3.5 万余个。累计阻断钓鱼网站连接访问达 929 万余次，有力保护了客户利益。

C. 网民反应

中国移动开展钓鱼诈骗网站集中治理，对钓鱼网站进行封堵，使钓鱼网站链接无法打开访问，用户手机不会被感染病毒，避免了钱财被不法分子窃取，有力保护了网民的合法权益。

D. 推荐理由

钓鱼网站问题已成为社会公害，对广大客户造成经济损失，严重侵害了客户的合法权益；中国移动作为一个负责任的通信运营企业，针对钓鱼诈骗网站，创新建立了钓鱼网站集中治理工作体系，对发现的假冒中国移动的钓鱼网站进行一键封堵，使钓鱼网站无法访问，有力保护了客户利益。

鸣谢

以下单位对本次调查的在线问卷投放和数据收集给予了大力支持，此表示衷心的感谢！（排序不分先后）

360
新浪
阿里
189 邮箱
139 邮箱
百度
搜狐邮箱
网易邮箱
263
蜗牛移动
天音移动

法律声明

联系方式

地址：北京市西城区复兴门南大街 2-乙天银大厦 A 东座 10 层
邮编：100031
网站：www.12321.cn