2019 年中国手机安全状况报告

2020 年 02 月 04 日

前言

360 手机卫士通过在移动端多年的技术积累，依托 AI 模型和安全大脑的分析能力，针对电信诈骗、钓鱼网址和恶意程序的攻防、传播和识别进行了有效的防护；在 2019 年 360 手机卫士共为全国用户拦截各类钓鱼网站攻击约 22.8 亿次，为全国用户拦截恶意程序攻击约 9.5 亿次；拦截骚扰电话约 260.9 亿次，拦截垃圾短信约 95.3 亿条。

随着电信诈骗的发展，诈骗手段趋于专业化、多样化，不法分子利用电话、短信、URL 等方式进行违法犯罪、通信诈骗等行为，严重影响了社会稳定，威胁到了广大人民群众的财产安全。鉴于此，需要在公安专网、运营商内网建立针对诈骗电话、诈骗短信的，有效的拦截系统。为此 360 集团开发了针对诈骗电话、诈骗短信、诈骗彩信以及涉诈 URL 为主要数据源的综合反诈平台——应龙综合反诈平台，被工信部、信通院连同公安部联名评选为““众智护网”2019 防范治理电信网络诈骗创新示范项目”；

应龙综合反诈平台是业界首家部署在运营商网络中进行实时预警、拦截的系统。面对频发的通信诈骗案件和巨额的经济损失，运营商、公安和 360 重新审视现有的通信反诈机制，并对其采取优化和升级。依靠卓越的业务基础、智能的数据算法，有效规避了通信诈骗案件数量。在配合公安部在打击“杀猪盘”电信诈骗专项、冒充公检法、套路贷和贷款诈骗专项治理行动中，依靠应龙系统自身的大数据分析预警能力，对一系列的诈骗进行预警、溯源打击。

摘要

恶意程序：

- 2019 年全年，360 安全大脑共截获移动端新增恶意程序样本约 180.9 万个，平均每天截获新增手机恶意程序样本约 0.5 万个。新增恶意程序类型主要为资费消耗，占比 46.8%；其次为隐私窃取（41.9%）、远程控制（5.0%）、流氓行为（4.6%）、恶意扣费（1.5%）、欺诈软件（0.1%）。
- 2019 年全年，在 360 安全大脑的支撑下，360 手机卫士累计为全国手机用户拦截恶意程序攻击约 9.5 亿次，平均每天拦截手机恶意程序攻击约 259.2 万次。
- 从省级分布来看，2019 年全年遭受手机恶意程序攻击最多的地区为广东省，占全国拦截量的 9.8%；其次为山东（7.7%）、江苏（7.3%）、河南（6.9%）、浙江（5.8%）等。
- 从城市分布来看，2019 年全年遭受手机恶意程序攻击最多的城市为北京市，占全国拦截量的 2.2%；其次为重庆（2.0%）、上海（1.9%）、广州（1.9%）、成都（1.8%）等。

钓鱼网站：

- 2019 年全年，360 安全大脑在 PC 端与移动端共为全国用户拦截钓鱼网站攻击约 800.2 亿次。其中，PC 端拦截量约为 777.5 亿次，占总拦截量的 97.2%，平均每日拦截量约 2.1 亿次；移动端拦截量约为 22.8 亿次，占总拦截量的 2.8%，平均每日拦截量约 623.9 万次。
- 2019 年全年，移动端拦截钓鱼网站类型主要为境外彩票，占比高达 74.7%；其次为网站被黑（17.8%）、假药（2.9%）、虚假购物（1.4%）、虚假中奖（1.2%）、金融证券（1.1%）等。
- 从省级分布来看，2019 年全年移动端拦截钓鱼网站最多的地区为广东省，占全国拦截量的 26.3%；其次为广西（10.0%）、山东（6.5%）、福建（4.1%）、四川（4.1%）等。
- 从城市分布来看，2019 年全年移动端拦截钓鱼网站最多的城市为广州市，占全国拦截量的 4.4%；其次为深圳（3.4%）、北京（3.1%）、东莞（2.8%）、泉州（2.4%）等。
- 2019 年全年，360 安全大脑共截获各类新增钓鱼网站 2431.0 万个，平均每天新增 6.7 万个。观察钓鱼网站新增类型，境外彩票类占据首位，占比 77.7%，属于新增钓鱼网站中的重点打击类型。其次为金融证券类，占比 11.2%。
- 从新增钓鱼网站的服务器地域分布看，77.7%的钓鱼网站服务器位于国外，22.3%的钓鱼网站服务器位于国内。其中，国内服务器位于香港的占比为 25.9%，居于首位；其次为

广东（12.8%）、北京（10.0%）、台湾（9.5%）、浙江（6.7%）等。

骚扰电话：

- 2019 全年，360 安全大脑收获用户主动标记各类骚扰号码（包括 360 手机卫士自动检出的响一声电话）约 0.62 亿个，平均每天标记约 17.0 万个。
- 结合 360 安全大脑骚扰电话基础数据，360 手机卫士共为全国用户识别和拦截各类骚扰电话约 260.9 亿次，平均每天识别和拦截骚扰电话约 0.7 亿次。
- 从骚扰电话标记类型来看，响一声以 58.7%的比例位居首位；其次为广告推销（14.1%）、骚扰电话（8.3%）、疑似欺诈（7.3%）、房产中介（5.1%）、保险理财（4.1%）、招聘猎头（2.1%）、诈骗电话（0.2%）。
- 从骚扰电话拦截类型来看，广告推销以 46.0%的比例位居首位；其次为骚扰电话（27.0%）、疑似欺诈（16.3%）、房产中介（7.6%）、响一声（1.7%）、保险理财（1.1%）招聘猎头（0.2%）与教育培训（0.1%）。
- 2019 年全年，从骚扰电话拦截号码的号源分布看，被拦截的固定电话最多，占比高达 30.0%；其次为运营商为中国移动的个人手机号（20.1%）、95/96 开头号段（17.9%）、运营商为中国联通的个人手机号（16.2%）、运营商为中国电信的个人手机号（9.1%）、虚拟运营商（6.1%）与 400/800 开头号段（0.6%）。
- 从省级分布来看，2019 年全年广东省用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的 11.3%；其次是山东（6.8%）、河南（6.2%）、江苏（6.2%）、四川（5.3%）。
- 从城市分布来看，2019 年全年北京市用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的 4.8%；其次是广州（3.3%）、上海（3.2%）、深圳（2.2%）、重庆（2.1%）
- 从省级分布来看， 2019 年全年广东省用户接到骚扰电话最多，占全国骚扰电话拦截量的 11.7%；其次是江苏（7.3%）、浙江（6.3%）、山东（6.3%）、北京（6.2%）等。
- 从城市分布来看，2019 年全年北京市用户接到的骚扰电话最多，占全国骚扰电话拦截量的 5.9%；其次是广州（4.1%）、上海（3.7%）、杭州（2.6%）、深圳（2.6%）等。

垃圾短信：

- 2019 年全年，在 360 安全大脑的支撑下，360 手机卫士共为全国用户拦截各类垃圾短信约 95.3 亿条。
- 2019 年全年，垃圾短信的类型分布中广告推销短信最多，占比为 95.0%；诈骗短信占比 4.4%；违法短信占比 0.6%。

✧ 2019 年全年，短信平台 1065/1069 号段发送垃圾短信占比高达 94.8%，已成为垃圾短信主要传播渠道。

除短信平台 1065/1069 号段发送垃圾短信外，从其他发送者号码个数分布看，运营商为中国联通的个人手机号发送垃圾短信的最多，占比 25.5%；其次是运营商为中国电信的个人手机号（23.7%）、95/96 号段（22.4%）、运营商为中国移动的个人手机号（20.4%）、虚拟运营商（5.2%）、14 物联网卡（2.6%）。

✧ 从省级分布来看，2019 年全年广东省用户收到的垃圾短信最多，占全国垃圾短信拦截量的 16.9%；其次是山东（7.3%）、浙江（6.9%）、江苏（6.7%）、河南（6.4%）等。

✧ 从城市分布来看，2019 年全年广州市用户收到的垃圾短信最多，占全国垃圾短信拦截量的 8.2%；其次是北京（5.7%）、深圳（4.4%）、南京（3.7%）、上海（3.3%）等。

网络诈骗：

✧ 2019 年 360 手机先赔共接到手机诈骗举报 3924 起。其中诈骗申请为 1930 起，涉案总金额高达 1546.5 万元，人均损失 8013 元。

✧ 在所有诈骗申请中，金融理财占比最高，为 25.3%；其次是赌博博彩（18.4%）、虚假兼职（13.7%）、身份冒充（12.8%）、网游交易（5.1%）等。

✧ 从涉案总金额来看，同样是金融理财类诈骗总金额最高，达 499.2 万元，占比 32.3%；其次是赌博博彩诈骗，涉案总金额 486.2 万元，占比 31.4%；身份冒充诈骗排第三，涉案总金额为 271.5 万元，占比 17.6%。

✧ 从人均损失来看，赌博博彩诈骗人均损失最高，为 13658 元；其次是身份冒充诈骗为 10947 元，金融理财诈骗为 10208 元。

✧ 从举报用户的性别差异来看，男性受害者占 66.3%，女性占 33.7%，男性受害者占比高于女性。从人均损失来看，男性为 7639 元，女性为 10338 元。

✧ 从被骗网民的年龄段上看，90 后的手机诈骗受害者占所有受害者总数的 38.0%；其次是 80 后占比为 27.0%；00 后占比为 20.6%；70 后占比为 9.5%；其他年龄段占比为 4.8%。

✧ 从用户举报情况来看，2019 年全年广东（12.8%）、广西（6.3%）、山东（6.1%）、河北（5.4%）、河南（5.2%）这 5 个地区的被骗用户最多。

✧ 从用户举报情况来看，2019 年全年广州（2.2%）、东莞（2.2%）、北京（2.0%）、成都（1.8%）、重庆（1.8%）这 5 个城市的被骗用户最多。

关键词：恶意程序、钓鱼网站、骚扰电话、垃圾短信、网络诈骗

目录

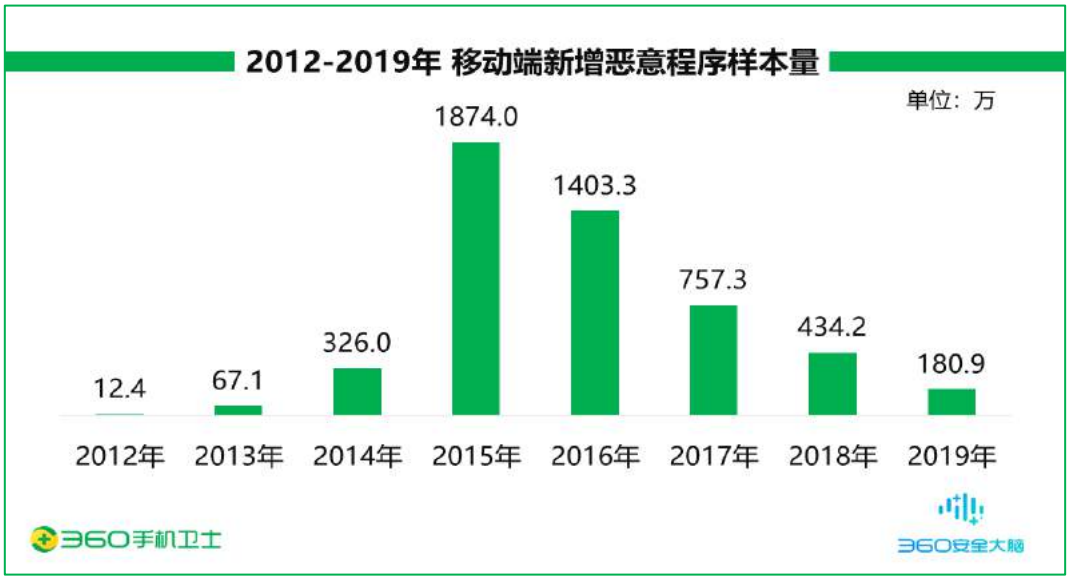
第一章　恶意程序

随着互联网及智能便携设备的普及，移动互联网迅速崛起，移动端的各类应用程序越来越丰富，给予大众便利的同时，出现了大量互联网恶意程序，严重危害网民的个人信息安全与财产安全。

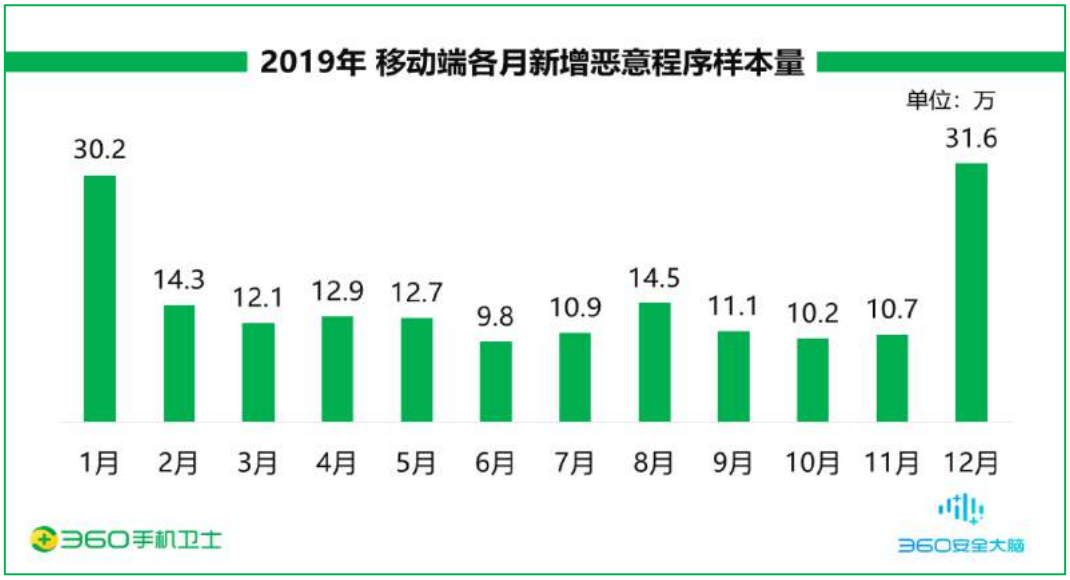
恶意程序是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行，侵犯用户合法权益的应用程序。一般存在以下一种或多种恶意行为，包括资费消耗、隐私窃取、远程控制、流氓行为、恶意扣费、欺诈软件、系统破坏等。为有效防护移动互联网安全，360 安全大脑持续加强对移动互联网恶意程序的识别和拦截力度，以保障移动互联网健康有序发展。

一、 恶意程序新增样本量与类型分布

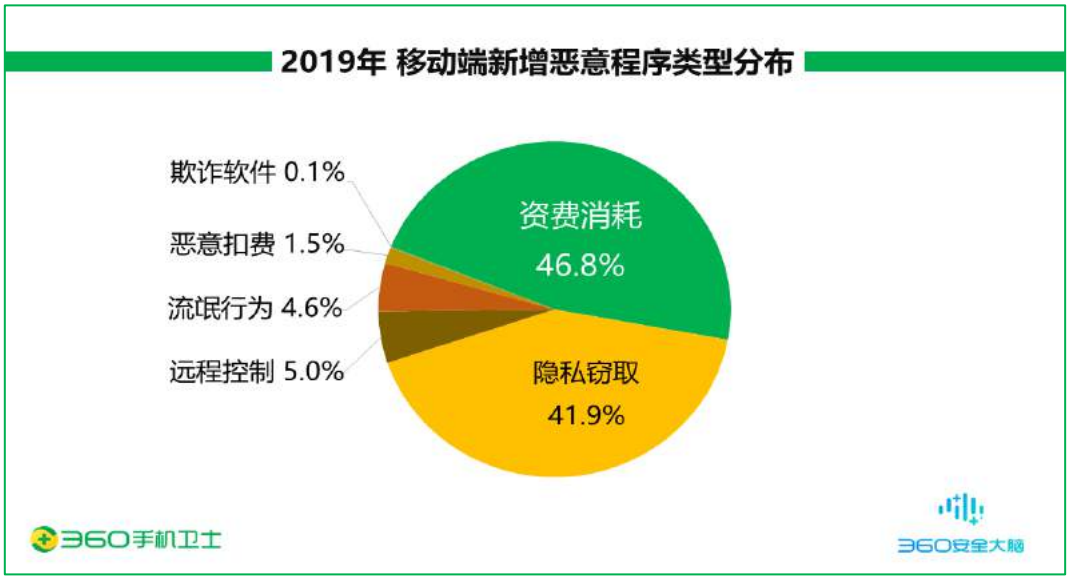
2019 年全年，360 安全大脑共截获移动端新增恶意程序样本约 180.9 万个，环比 2018 年（434.2 万个）下降了 58.3%，平均每天截获新增手机恶意程序样本约 0.5 万个。自 2015 年起，恶意程序新增样本呈逐年下降趋势。下图给出了 2012 年-2019 年移动端新增恶意程序样本量统计：



在 2019 年 1 月与 12 月出现新增样本量峰值，期间月份新增样本趋势较平稳。观察新增样本类型，主要体现在恶意扣费、资费消耗、隐私窃取。由于春节假期前后，大众的社交娱乐活动增多，棋牌游戏、抢红包已成为大众假期娱乐必选项。不法分子正是利用这一敏感时间段，大肆传播恶意程序，实现不良获利。具体分布如下图所示：

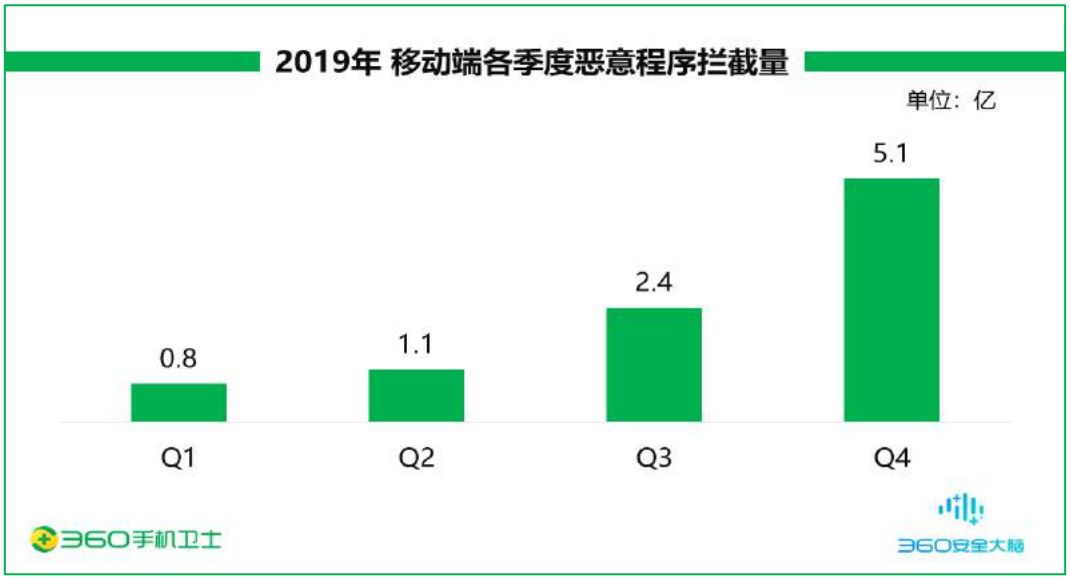


2019 年全年移动端新增恶意程序类型主要为资费消耗，占比 46.8%；其次为隐私窃取（41.9%）、远程控制（5.0%）、流氓行为（4.6%）、恶意扣费（1.5%）、欺诈软件（0.1%）。



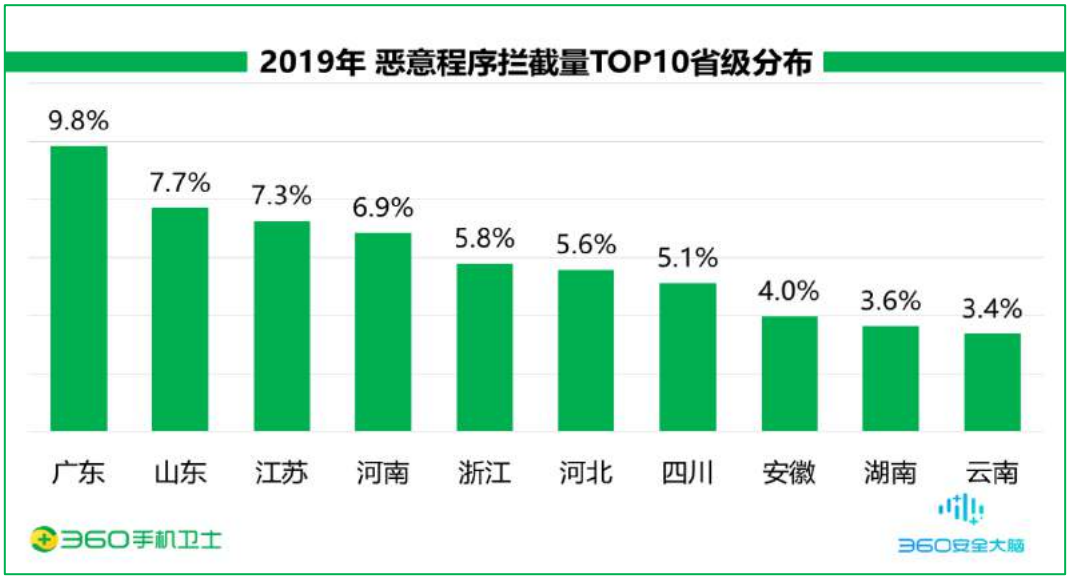
二、 恶意程序拦截量

2019 年全年，在 360 安全大脑的支撑下，360 手机卫士累计为全国手机用户拦截恶意程序攻击约 9.5 亿次，平均每天拦截手机恶意程序攻击约 259.2 万次。通过统计 2019 年 Q4 季度样本数量 TOP500 的恶意程序发现，赌博棋牌与色情视频类程序呈现增长态势，致使拦截量直线上升。下图给出了 2019 年移动端各季度恶意程序拦截量统计：



三、 恶意程序拦截量地域分布

2019 年全年，从省级分布来看，遭受手机恶意程序攻击最多的地区为广东省，占全国拦截量的 9.8%；其次为山东（7.7%）、江苏（7.3%）、河南（6.9%）、浙江（5.8%），此外河北、四川、安徽、湖南、云南的恶意程序拦截量也排在前列。



从城市分布来看，遭受手机恶意程序攻击最多的城市为北京市，占全国拦截量的 2.2%；其次为重庆（2.0%）、上海（1.9%）、广州（1.9%）、成都（1.8%），此外深圳、郑州、苏州、东莞、西安的恶意程序拦截量也排在前列。


2019年 恶意程序拦截量TOP10城市分布
2.2%
2.0%
1.9%
1.9%
1.8%
1.5%
1.3%
1.2%
1.2%
1.2%
北京
重庆
上海
广州
成都
深圳
郑州
苏州
东莞
西安
360手机卫士
360安全大脑

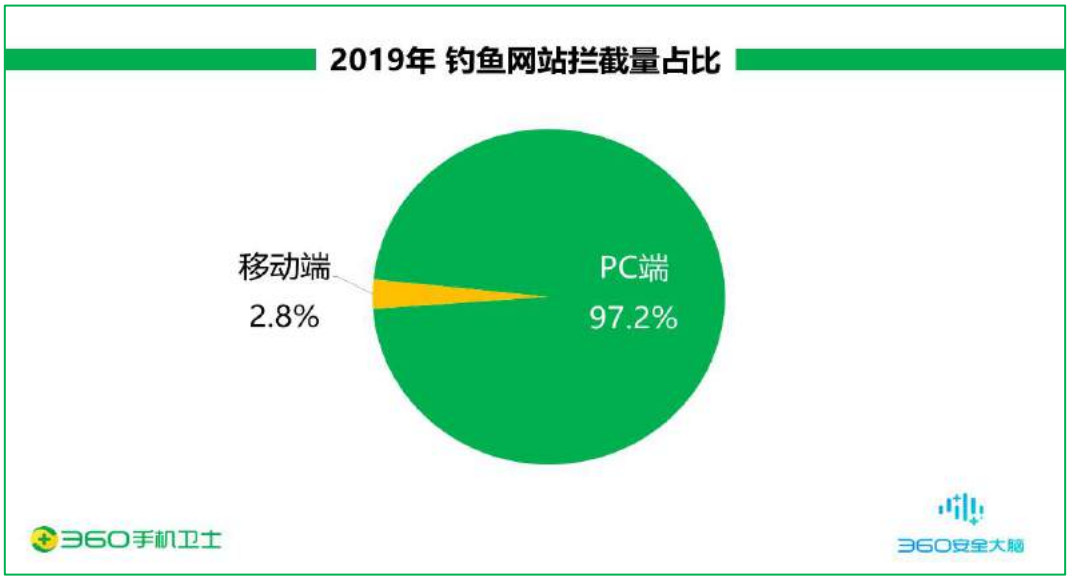
第二章　钓鱼网站

如今，移动互联网内充斥着各种虚假信息，在大众日常浏览网站的过程中，容易遭受“钓鱼网站”侵害。所谓“钓鱼网站”是一种网络欺诈行为，指不法分子利用各种手段，仿冒真实网站的 URL 地址以及页面内容，以此来骗取用户银行或信用卡账号、密码等私人资料。“钓鱼网站”的频繁出现，严重地影响了在线金融服务、电子商务的发展危害公众利益，影响公众应用互联网的信心。

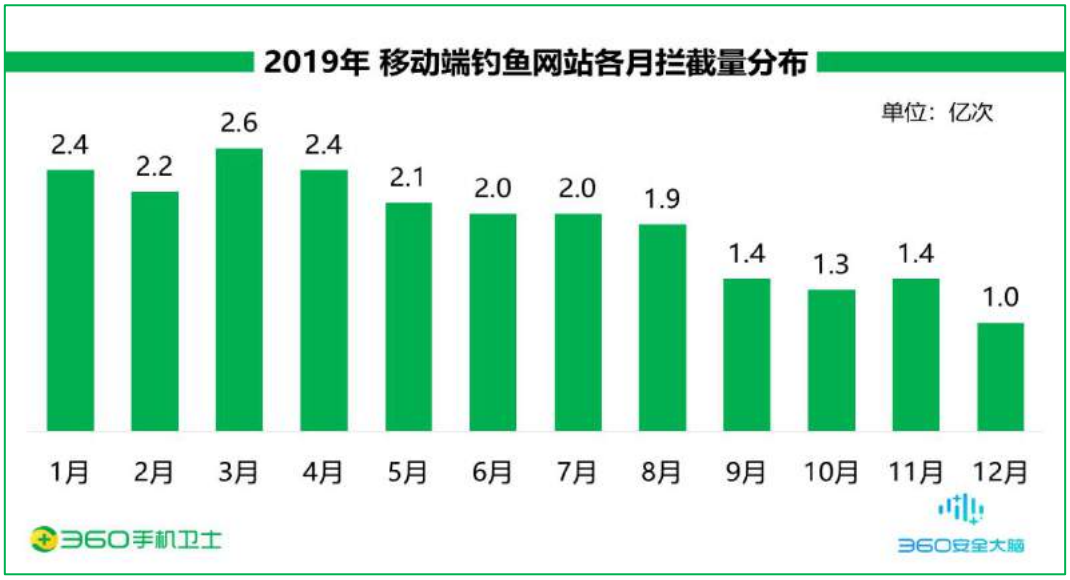
面对层出不穷的“钓鱼网站”，国内于 2008 年成立“中国反钓鱼网站联盟”。于此同时，360 安全大脑积极预设钓鱼网站识别规则，建立模型样本库等，实时进行钓鱼网站拦截，及时遏制其带来的危害，肃清移动互联网。

一、 移动端钓鱼网站拦截量

2019 年全年，360 安全大脑在 PC 端与移动端共为全国用户拦截钓鱼网站攻击约 800.2 亿次，环比 2018 年（369.3 亿次）上升了 53.8%。其中，PC 端拦截量约为 777.5 亿次，占总拦截量的 97.2%，平均每日拦截量约 2.1 亿次；移动端拦截量约为 22.8 亿次，占总拦截量的 2.8%，平均每日拦截量约 623.9 万次。下图给出了 2019 年钓鱼网站拦截量占比分布：

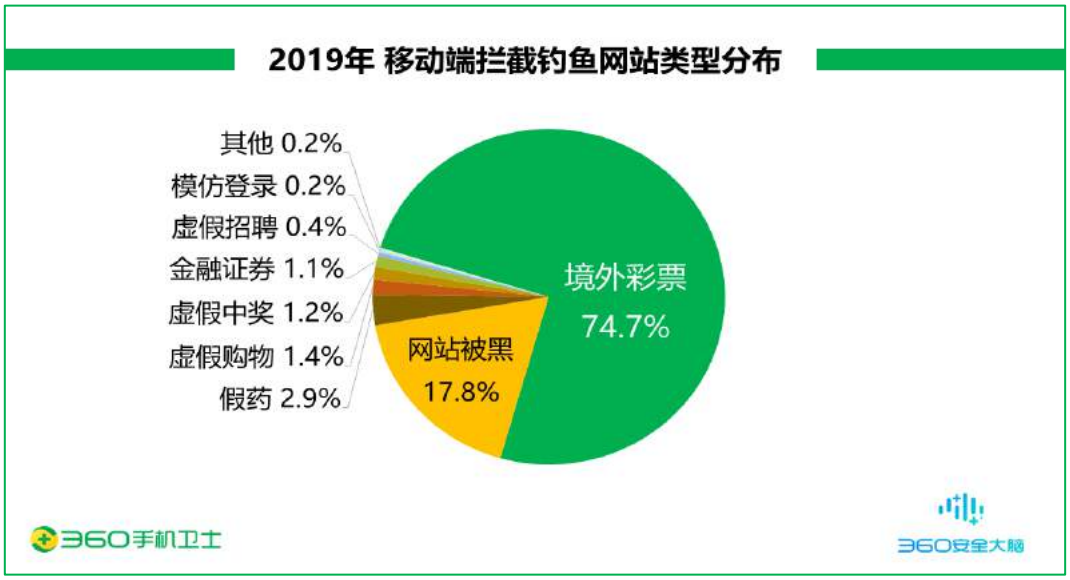


从下图 2019 年移动端钓鱼网站各月拦截量分布看，前半年钓鱼网站拦截量无较大起伏，自 8 月份起，拦截量呈下降趋势。



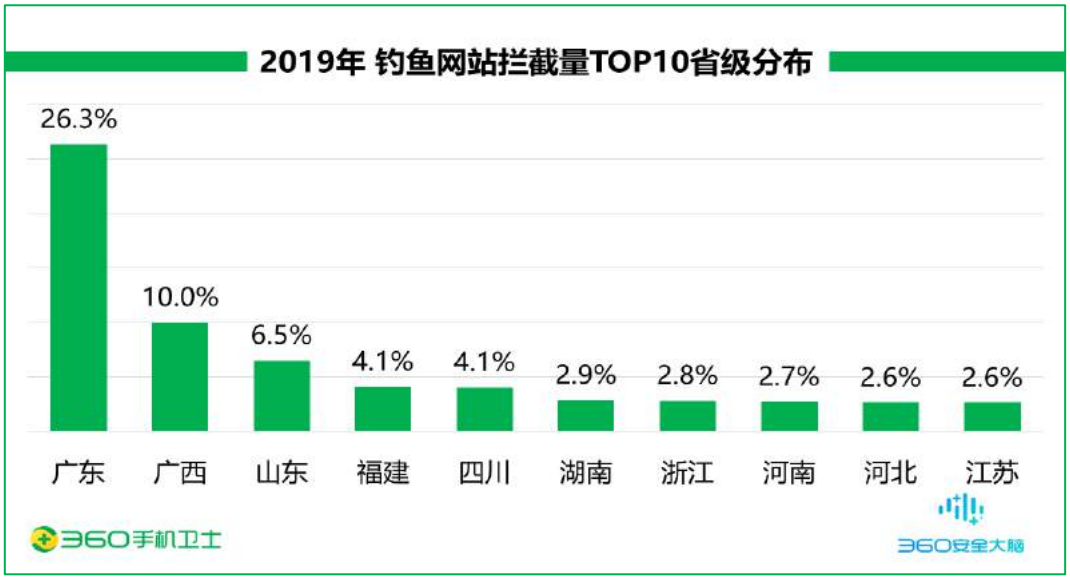
二、 移动端钓鱼网站类型分布

2019 年全年，移动端拦截钓鱼网站类型主要为境外彩票，占比高达 74.7%；其次为网站被黑（17.8%）、假药（2.9%）、虚假购物（1.4%）、虚假中奖（1.2%）、金融证券（1.1%）等。

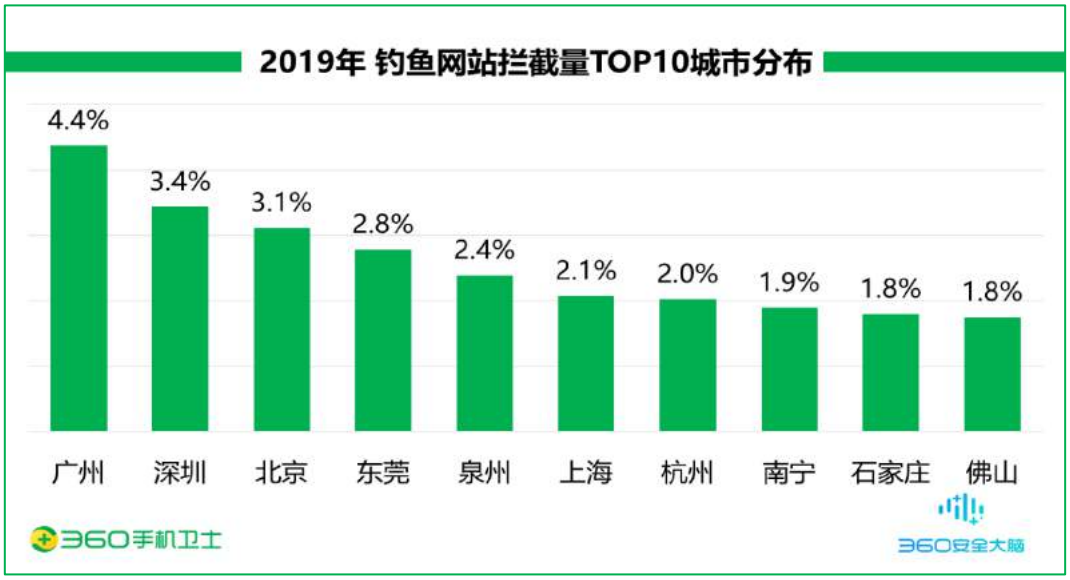


三、 移动端钓鱼网站拦截量地域分布

2019 年全年，从省级分布来看，移动端拦截钓鱼网站最多的地区为广东省，占全国拦截量的 26.3%；其次为广西（10.0%）、山东（6.5%）、福建（4.1%）、四川（4.1%），此外湖南、浙江、河南、河北、江苏的钓鱼网站拦截量也排在前列。

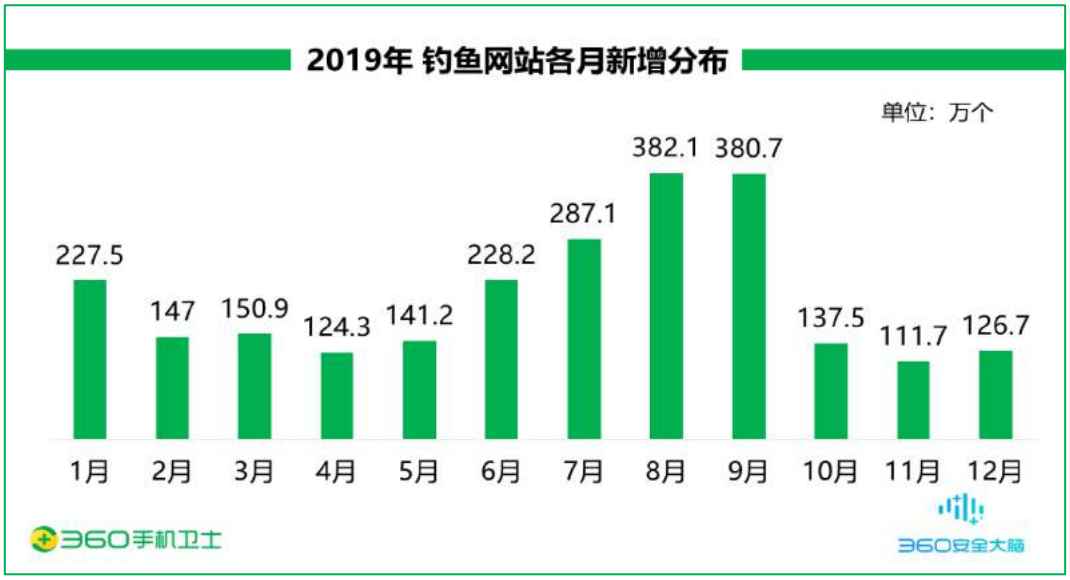


从城市分布来看，移动端拦截钓鱼网站最多的城市为广州市，占全国拦截量的 4.4%；其次为深圳（3.4%）、北京（3.1%）、东莞（2.8%）、泉州（2.4%），此外上海、杭州、南宁、石家庄、佛山的钓鱼网站拦截量也排在前列。

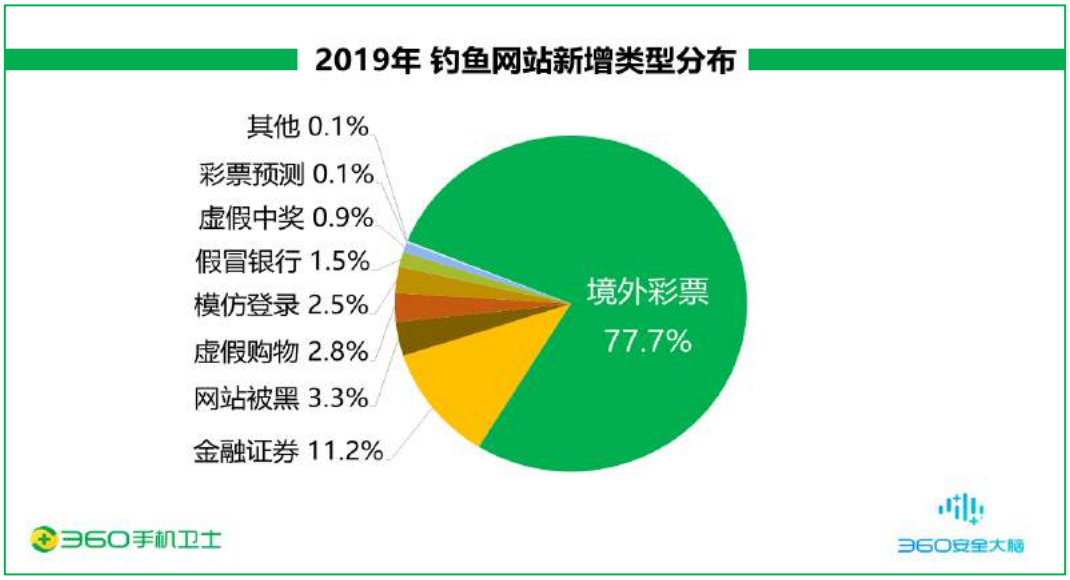


四、 钓鱼网站新增量与服务器地域分布

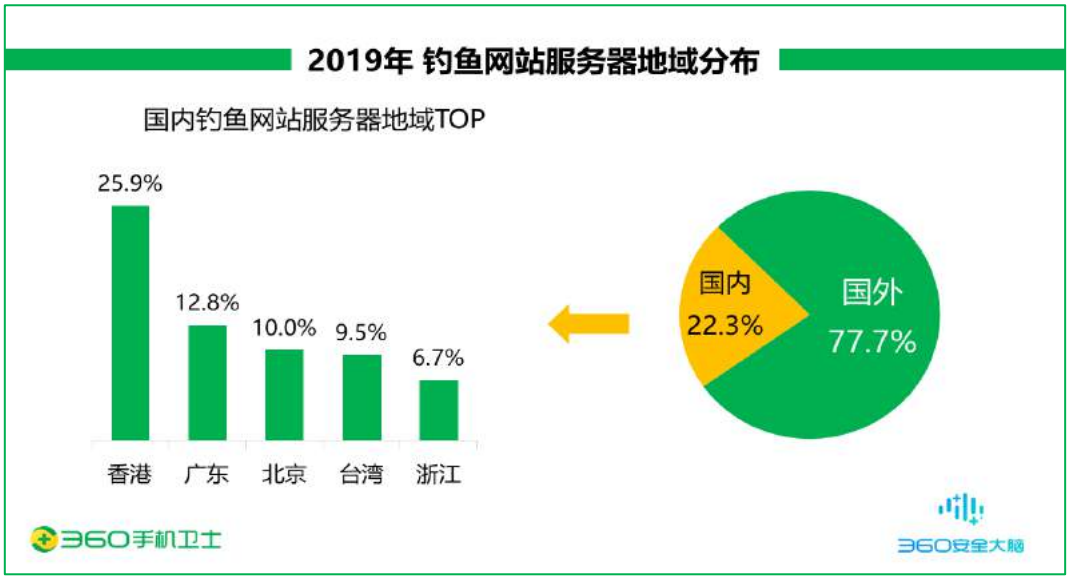
2019 年全年，360 安全大脑共截获各类新增钓鱼网站 2431.0 万个，平均每天新增 6.7 万个，新增量激增突出在 2019 年第三季度。



观察钓鱼网站新增类型，境外彩票类占据首位，占比 77.7%，属于新增钓鱼网站中的重点打击类型。其次为金融证券类，占比 11.2%。



从新增钓鱼网站的服务器地域分布看，77.7%的钓鱼网站服务器位于国外，22.3%的钓鱼网站服务器位于国内。其中，国内服务器位于香港的占比为 25.9%，居于首位；其次为广东（12.8%）、北京（10.0%）、台湾（9.5%）、浙江（6.7%）等。


2019年 钓鱼网站服务器地域分布
国内钓鱼网站服务器地域TOP
25.9%
12.8%
10.0%
9.5%
6.7%
香港
广东
北京
台湾
浙江
国内
22.3%
国外
77.7%
360手机卫士
360安全大脑

第三章　骚扰电话

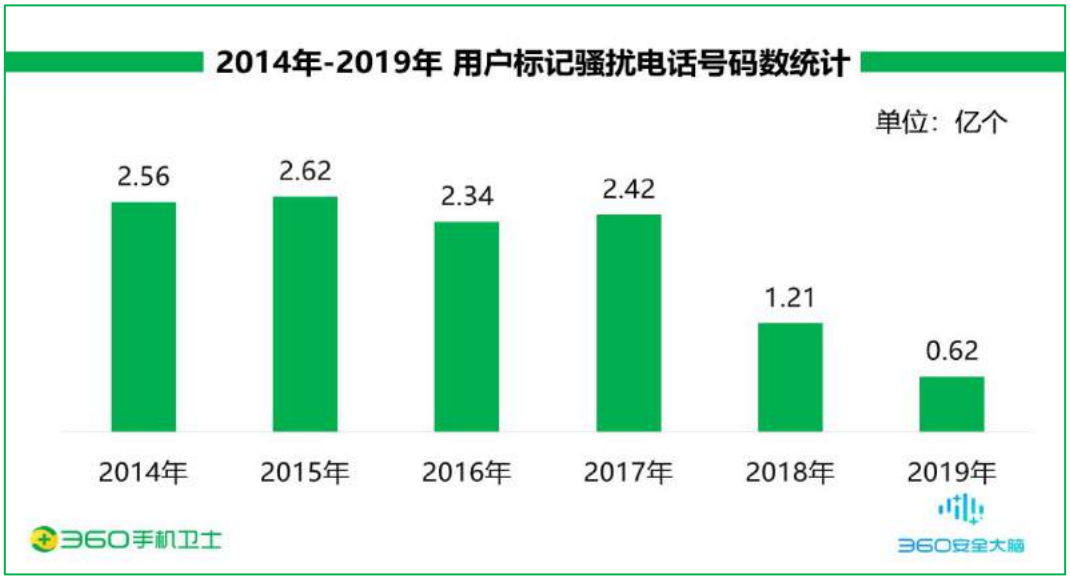
在大众日常生活中，经常接到多通骚扰电话，从保险推销、商家推广甚至上升为冒充身份、网络诈骗。究其根源，实际为用户个人敏感信息泄露所导致。个人信息犯罪案件屡禁不止，已成为社会关注的焦点。

如今大数据信息时代，公民个人信息泄露渠道增多，并呈现多样化态势，骚扰电话治理迫在眉睫。随着技术手段的不断升级，骚扰电话扰民方式更加多变。利用个人手机号发展到利用多号段、虚拟号码、自动外呼系统等，让人防不胜防。

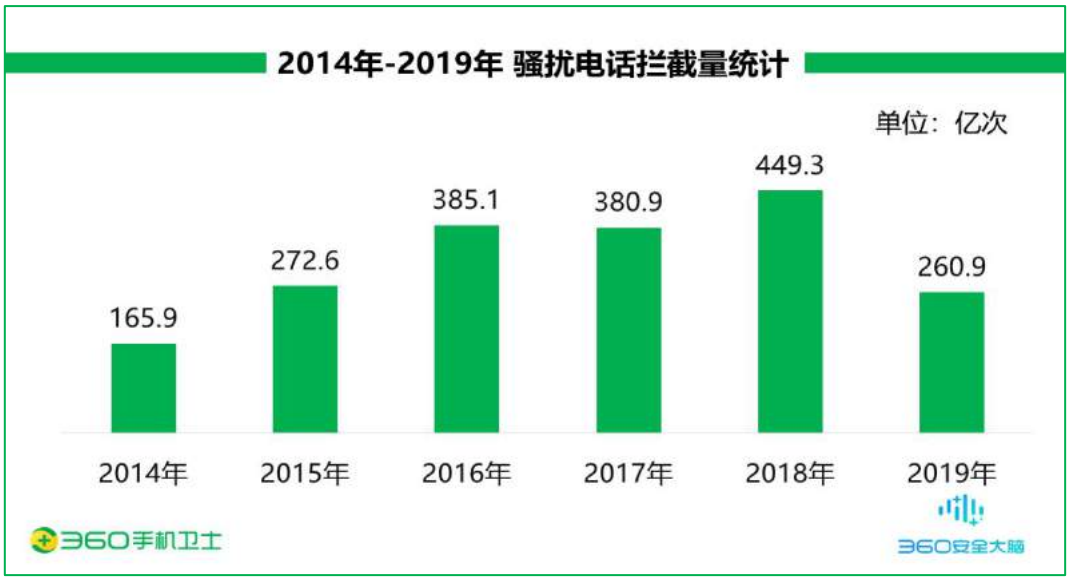
骚扰电话治理目前已开展专项活动，秉承《综合整治骚扰电话专项行动方案》，360 安全大脑利用自身大数据、人工智能等技术手段协助治理骚扰电话乱象，重点整治商业营销类、恶意骚扰类和违法犯罪类骚扰电话。

一、 骚扰电话标记数与拦截量

2019 全年，360 安全大脑收获用户主动标记各类骚扰号码（包括 360 手机卫士自动检出的响一声电话）约 0.62 亿个，平均每天标记约 17.0 万个。从标记号码总量上看，环比 2018（1.21 亿个）下降了 46.3%。下图给出了 2014 年-2019 年用户标记骚扰电话号码数统计：



结合 360 安全大脑骚扰电话基础数据，360 手机卫士共为全国用户识别和拦截各类骚扰电话约 260.9 亿次，平均每天识别和拦截骚扰电话约 0.7 亿次。环比 2018 年（449.3 亿次）下降了 41.9%。具体分布如下图所示：



据统计数据所示，用户标记骚扰电话号码数呈逐年降低趋势；于此同时，骚扰电话拦截量于 2019 年同样呈降低趋势，分析其降低原因主要存在以下几点：

1） 工信部政策实施，从根源上遏制骚扰

2018 年 7 月，工信部联合十三部门印发《综合整治骚扰电话专项行动方案》的通知，着力整治骚扰电话扰民问题，切实净化通信服务环境，决定在全国范围内组织开展为期一年半的综合整治骚扰电话专项行动。

自十三部门综合整治骚扰电话专项行动开展以来，互联网企业、基础电信运营企业充分利用技术手段，积极配合联合治理骚扰电话。2019 年 5 月，工信部针对垃圾信息严重扰民问题，集中约谈 20 家呼叫中心企业和 10 家移动转售企业；同年 11 月，再次约谈 18 家移动转售企业，明确要求被约谈企业端正态度、吸取教训、务实整改，确保短期内取得实效。加强企业内部管理和渠道管控，建立健全长效机制，促进移动转售行业持续健康发展。

2） 运营商整治骚扰电话，上线骚扰拦截系统

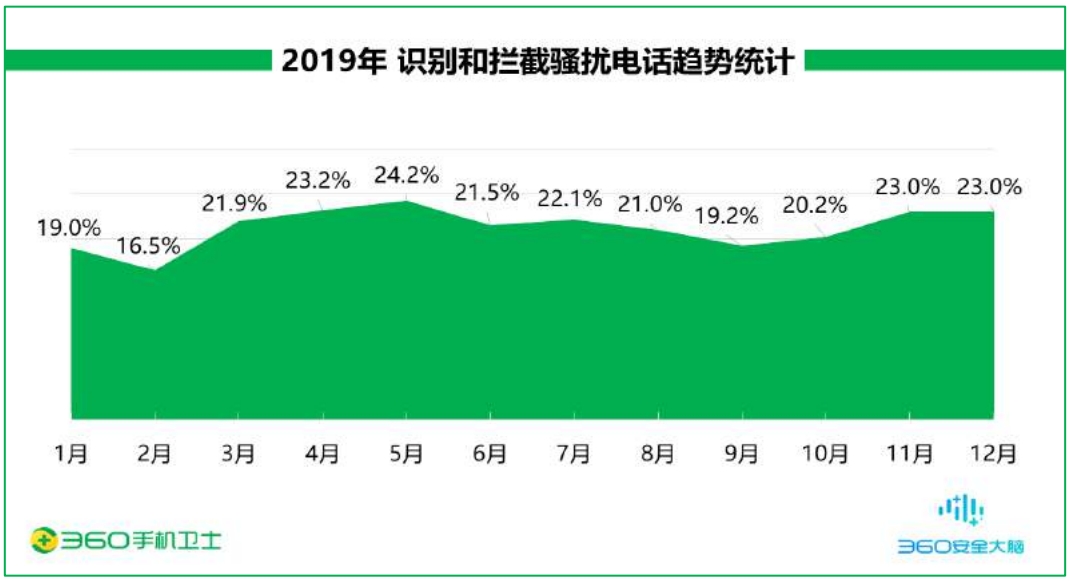
三大运营商全国上线骚扰拦截系统，针对客户提供骚扰、营销及自定义号码拦截服务，用户可针对个人需求免费开通服务，屏蔽各类骚扰电话。

3） 行业内多方企业联合整顿，效果显著

互联网企业联合基础电信运营企业充分利用技术手段，积极配合联合治理骚扰电话。开展数据共享及交换机制的探索，通过大数据、人工智能等新技术提高对不良号码的分析、处理和共享能力，实现骚扰电话的高效拦截。

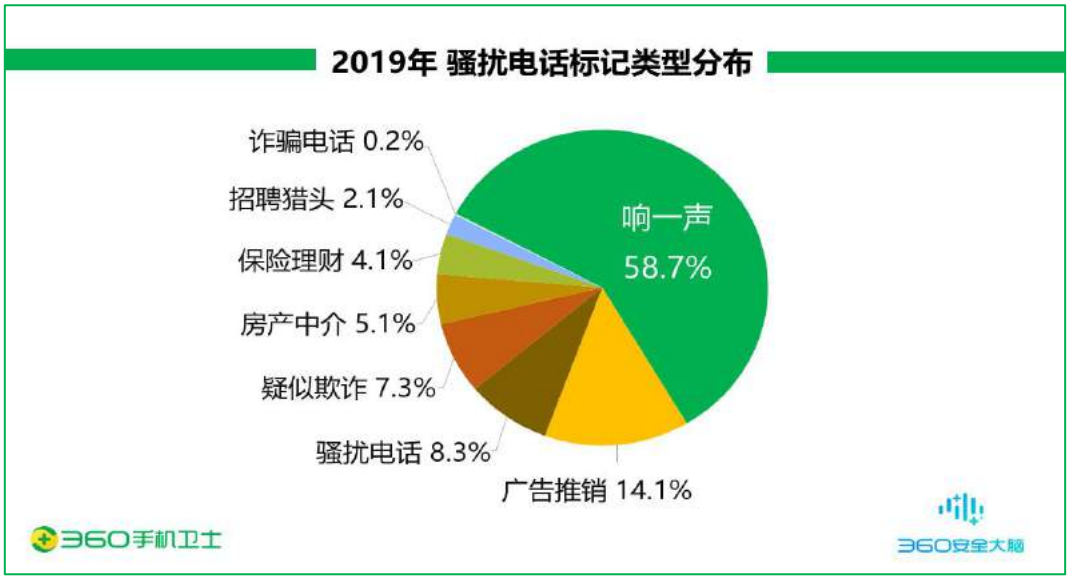
分析 2019 年 360 手机卫士识别和拦截骚扰电话趋势可见，骚扰电话呼入量受到节假日、电商节等特殊时段影响，波动性较为明显。

根据各月骚扰电话呼入占比分析：2019 年 2 月份期间正值春节假期，骚扰电话拦截量最低。通过往年趋势可知，在春节期间，从事拨打骚扰电话的人员减少，从而导致骚扰电话的呼入量降低。2019 年 3 月份起，骚扰电话拦截量回升，并呈持续小幅增长态势。自 2019 年 6 月份起，骚扰电话拦截量回落，并持续呈下降趋势。并在年终时有涨幅态势。具体分布如下图所示：

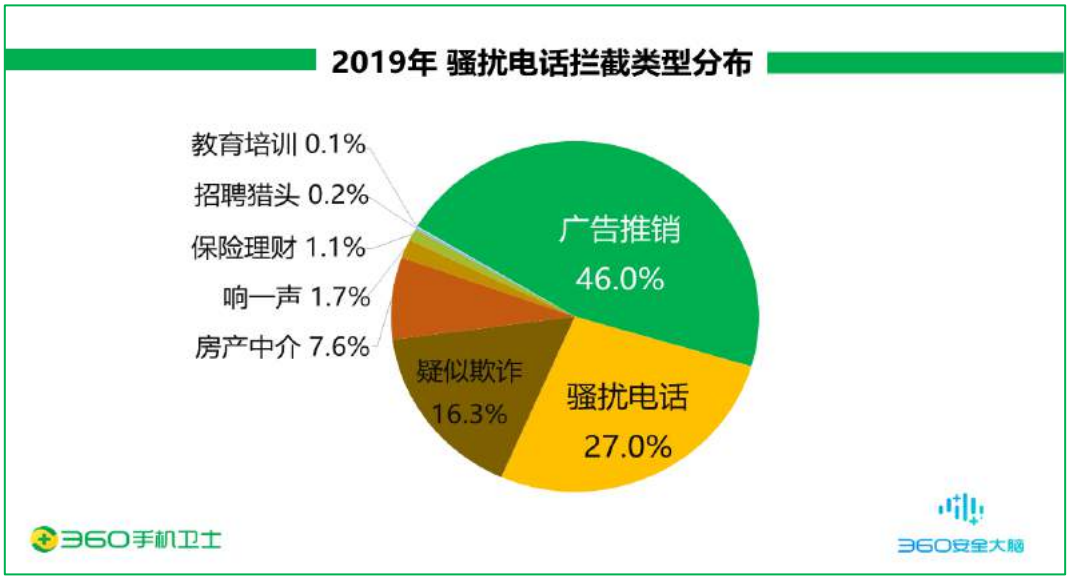


二、 骚扰电话类型分布

2019 年全年，综合 360 安全大脑的拦截监测情况及用户调研分析，从骚扰电话标记类型来看，响一声以 58.7%的比例位居首位；其次为广告推销（14.1%）、骚扰电话（8.3%）、疑似欺诈（7.3%）、房产中介（5.1%）、保险理财（4.1%）、招聘猎头（2.1%）、诈骗电话（0.2%）。具体分布如下图所示：

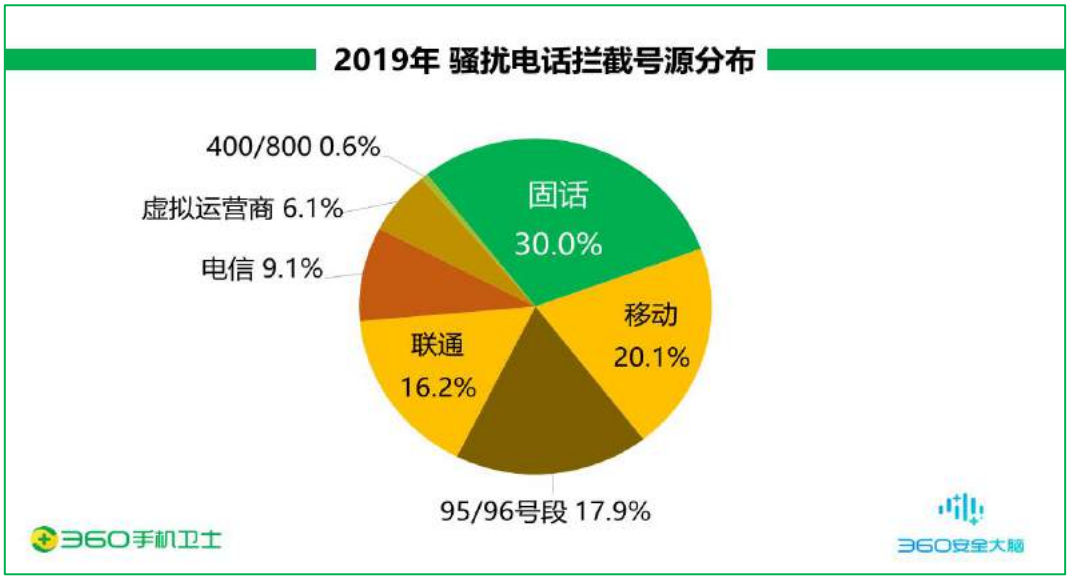


从骚扰电话拦截类型来看，广告推销以 46.0%的比例位居首位；其次为骚扰电话（27.0%）、疑似欺诈（16.3%）、房产中介（7.6%）、响一声（1.7%）、保险理财（1.1%）招聘猎头（0.2%）与教育培训（0.1%）。具体分布如下图所示：

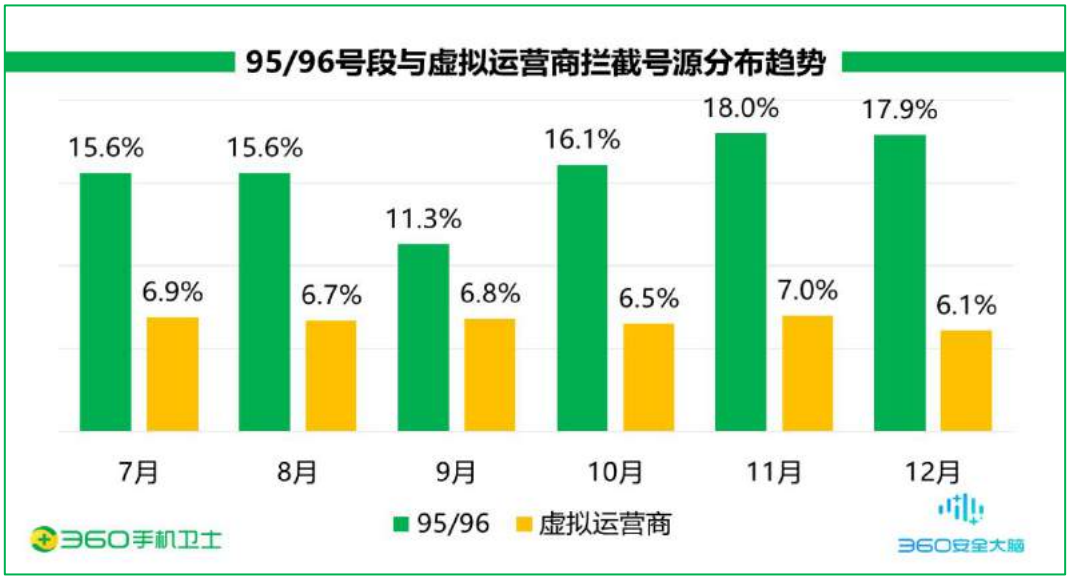


三、 骚扰电话拦截号源分布

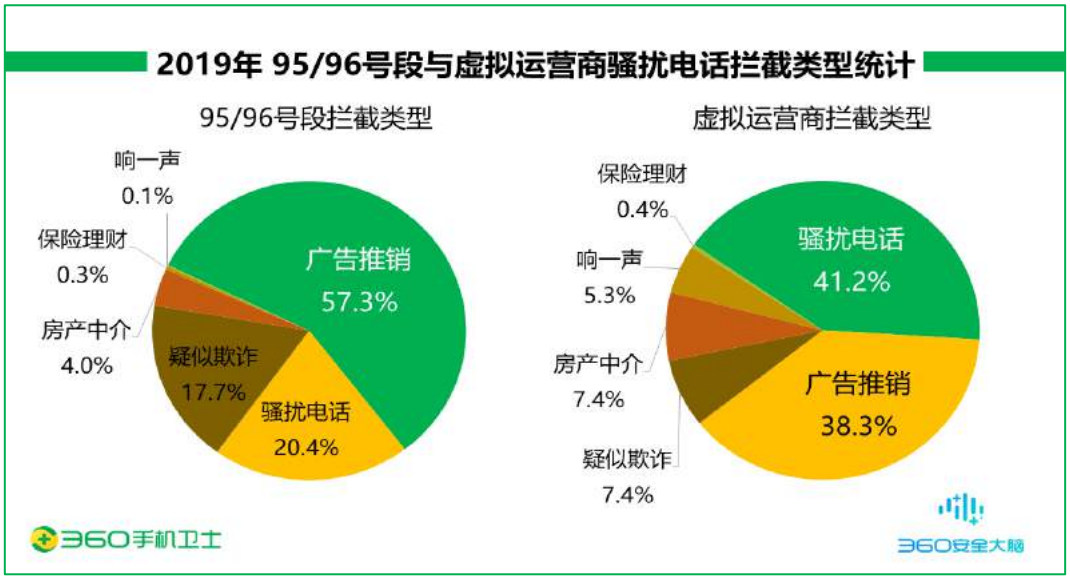
2019 年全年，从骚扰电话拦截号码个数分布看，被拦截的固定电话最多，占比高达 30.0%；其次为运营商为中国移动的个人手机号（20.1%）、95/96 开头号段（17.9%）、运营商为中国联通的个人手机号（16.2%）、运营商为中国电信的个人手机号（9.1%）、虚拟运营商（6.1%）与 400/800 开头号段（0.6%）。



近几年，“手机用户实名登记制度”的实施，从源头上遏制了骚扰、诈骗等通信犯罪的实施，增加了不法从业者实施手法的成本。通过对骚扰电话号源分布的统计，发现不法从业者利用 96/96 号段与虚拟运营商号码从事非法行径的数量激增，频频爆出诈骗成功案件。根据下图 95/96 号段与虚拟运营商拦截号源分布趋势，95/96 号段接近年底有涨幅趋势，而虚拟运营商号段趋势较平稳。

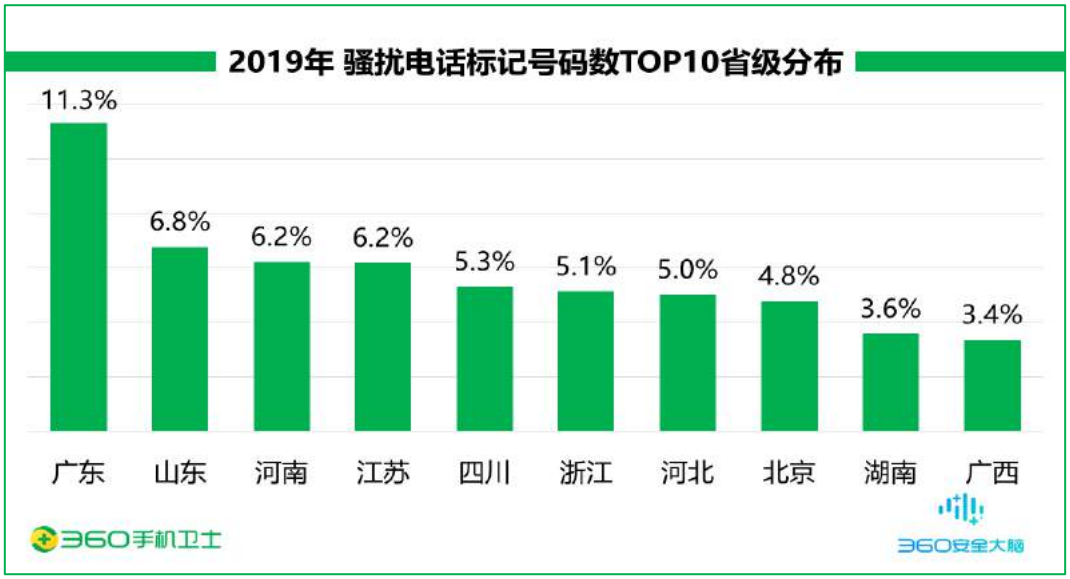


观察 95/96 号段与虚拟运营商骚扰电话拦截类型，95/96 号段广告推销类占据首位，占比 57.3%；虚拟运营商骚扰电话类占据首位，占比 41.2%。而疑似欺诈类分别占比 17.7%与 7.4%，类型比例占据前列。可见 95/96 号段与虚拟运营商号码遭不法分子利用，成为从事非法行径的主要号源之一，后续需加强针对以下号段的拦截与识别，防范非法行为的成功实施。

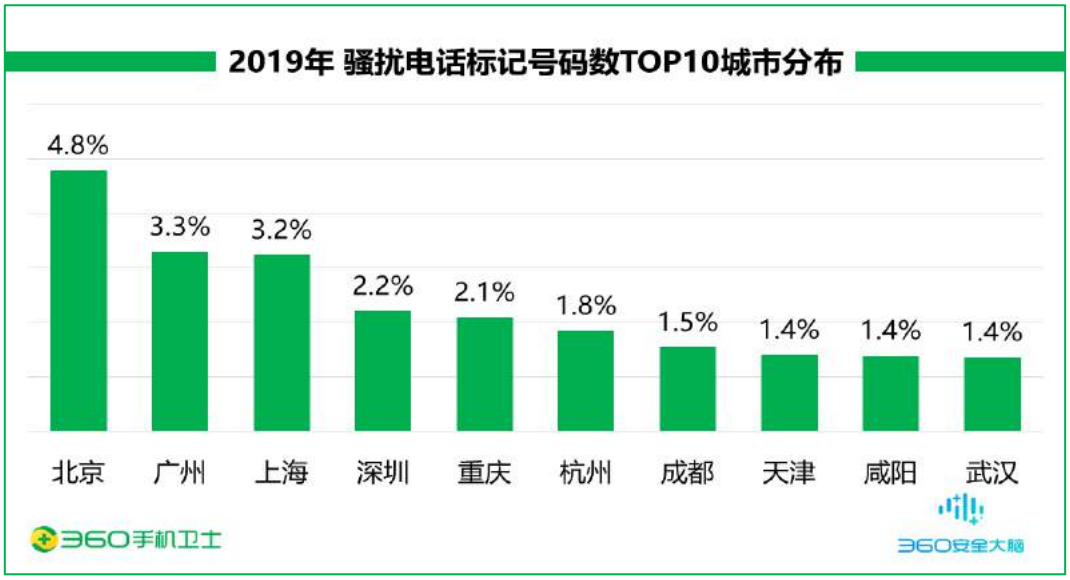


四、 骚扰电话归属地分布

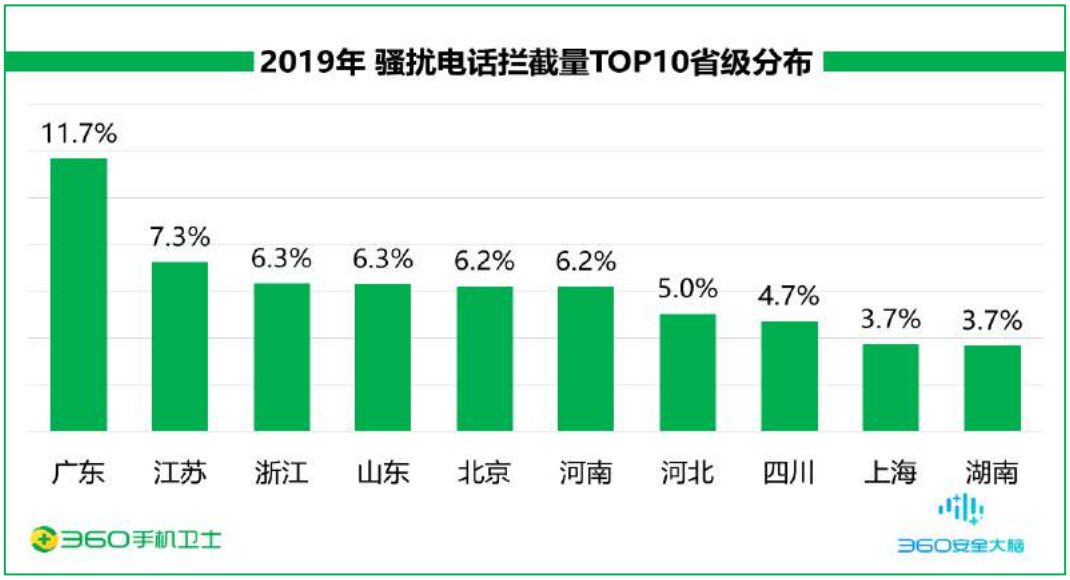
2019 年全年，从各地骚扰电话标记号码个数上分析，广东省用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的 11.3%；其次是山东（6.8%）、河南（6.2%）、江苏（6.2%）、四川（5.3%），此外浙江、河北、北京、湖南、广西的骚扰电话标记号码个数也排在前列。



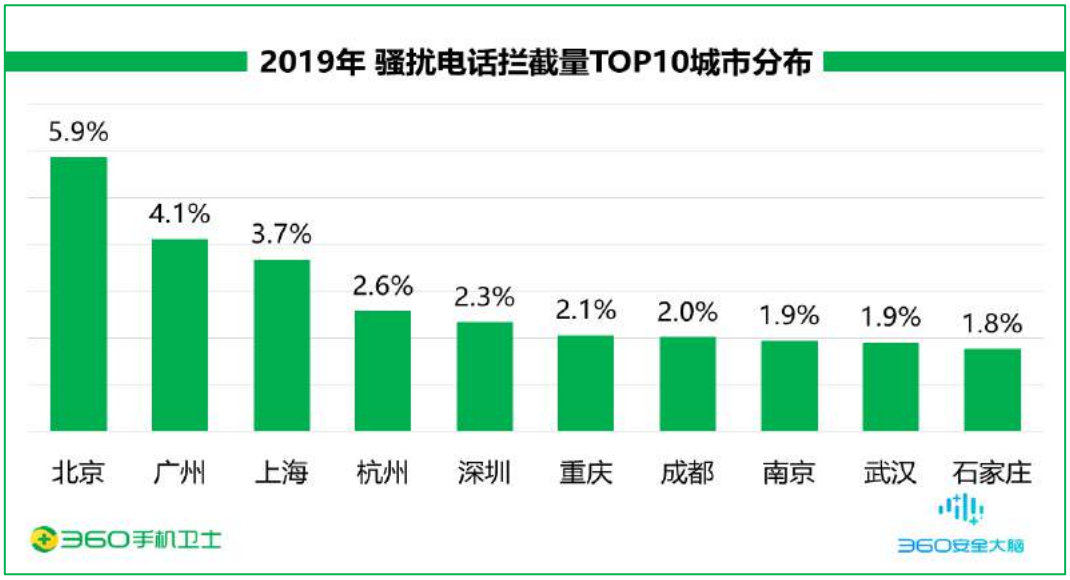
从城市分布来看，北京市用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的 4.8%；其次是广州（3.3%）、上海（3.2%）、深圳（2.2%）、重庆（2.1%），此外杭州、成都、天津、咸阳、武汉的骚扰电话标记号码个数也排在前列。



2019 年全年，从各地骚扰电话的拦截量上分析，广东省用户接到骚扰电话最多，占全国骚扰电话拦截量的 11.7%；其次是江苏（7.3%）、浙江（6.3%）、山东（6.3%）、北京（6.2%），此外河南、河北、四川、上海、湖南的骚扰电话拦截量也排在前列。



从城市分布来看，北京市用户接到的骚扰电话最多，占全国骚扰电话拦截量的 5.9%；其次是广州（4.1%）、上海（3.7%）、杭州（2.6%）、深圳（2.6%），此外重庆、成都、南京、武汉、石家庄的骚扰电话拦截量也排在前列。


2019年 骚扰电话拦截量TOP10城市分布
5.9%
4.1%
3.7%
2.6%
2.3%
2.1%
2.0%
1.9%
1.9%
1.8%
北京
广州
上海
杭州
深圳
重庆
成都
南京
武汉
石家庄
360手机卫士
360安全大脑

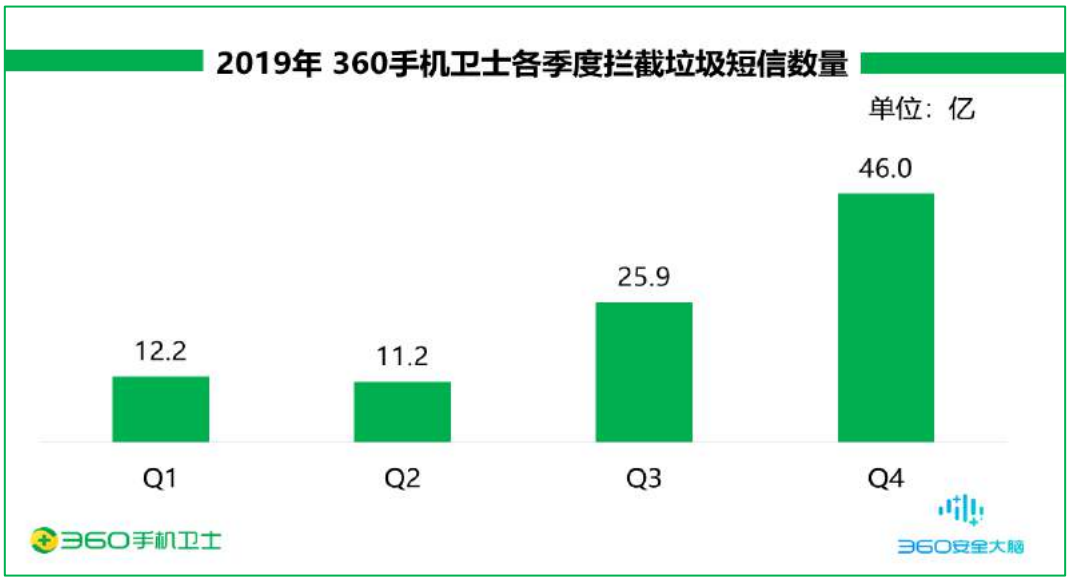
第四章　垃圾短信

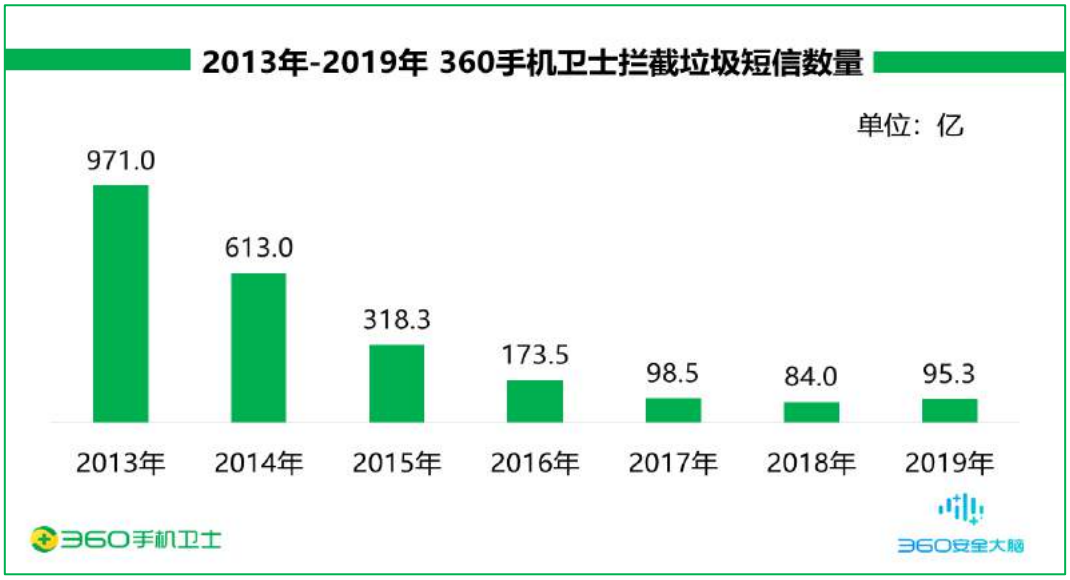
近几年社交 APP 的广泛使用，我们生活中的通讯习惯也在悄然发生变化。短信在我们日常沟通中使用的频次越来越低，而逐渐转变成身份验证、支付校验的重要方式。系统收件箱渐渐成为了短信“垃圾箱”，充斥着各类商业类、广告类，甚至违法诈骗类的短信息。垃圾短信的泛滥，已经严重影响到人们正常生活、运营商形象乃至社会稳定。

短信平台已成为垃圾短信的主要传播手段，其泛滥的主要原因是部分卡商企业未严格管控短信群发主体，致使垃圾短信产业链形成完整闭环。为此，360 与运营商、手机厂商达成合作，借助 360 安全大脑的云端拦截规则与本地算法能力，为用户防御垃圾短信保驾护航。

一、 垃圾短信拦截量

2019 年全年，在 360 安全大脑的支撑下，360 手机卫士共为全国用户拦截各类垃圾短信约 95.3 亿条，同比 2018 年（84.0 亿条）上升了 11.9%，平均每日拦截垃圾短信约 2610.3 万条。对比 2019 年各季度拦截垃圾短信数量，呈持续上升趋势，第四季度垃圾短信拦截量达 46.0 亿，有可能与年底各电商购物营销活动有关。

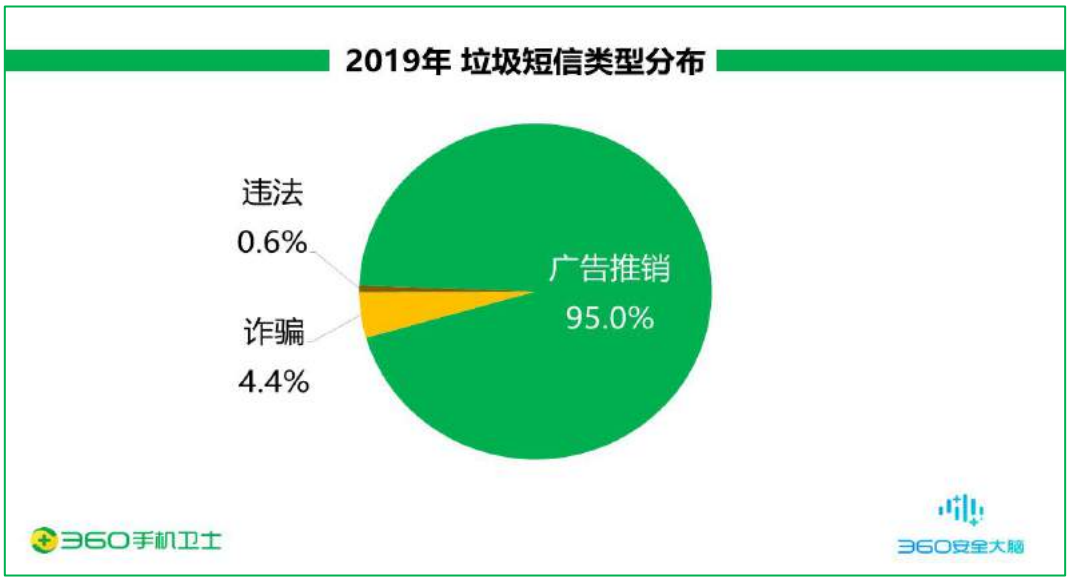




随着垃圾短信治理力度的不断加大，垃圾短信数量逐年降低，治理成效显著。近年来，垃圾短信不断出现新趋势，利用短信发送平台发送各类推销、诈骗、违法短信，同时攻防手段升级，在非法短信中不断迭代变体字，以增加运营商及安全厂商的垃圾短信识别难度。同时利用虚拟号段、95/96 号段、物联网卡、霸屏短信等手段实现垃圾短信的传播。在 2019 年垃圾短信拦截量有所提升，垃圾短信治理依然是一场“攻坚战”。

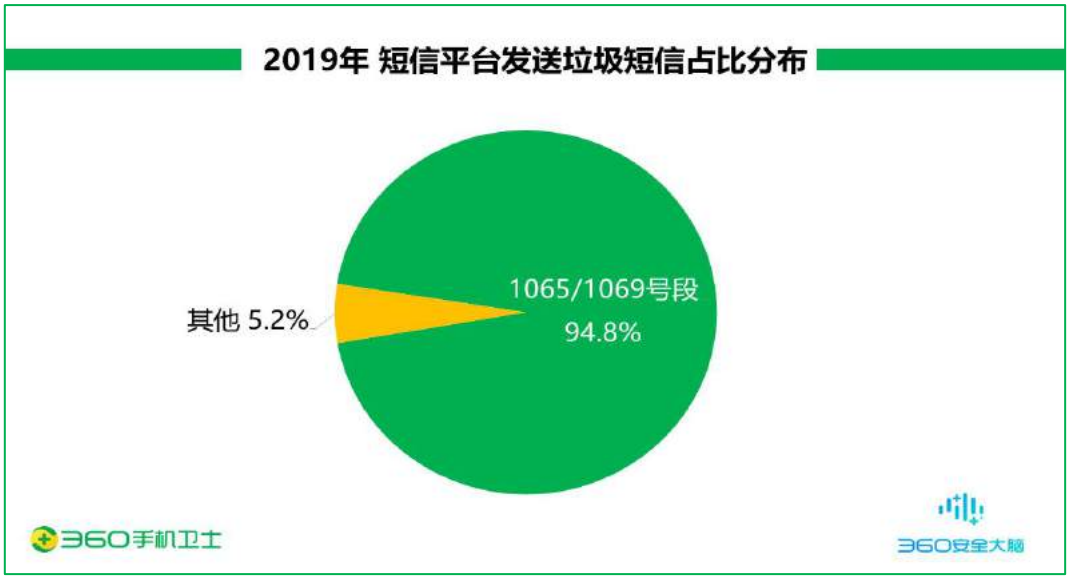
二、 垃圾短信类型分析

2019 年全年，垃圾短信的类型分布中广告推销短信最多，占比为 95.0%；诈骗短信占比 4.4%；违法短信占比 0.6%。

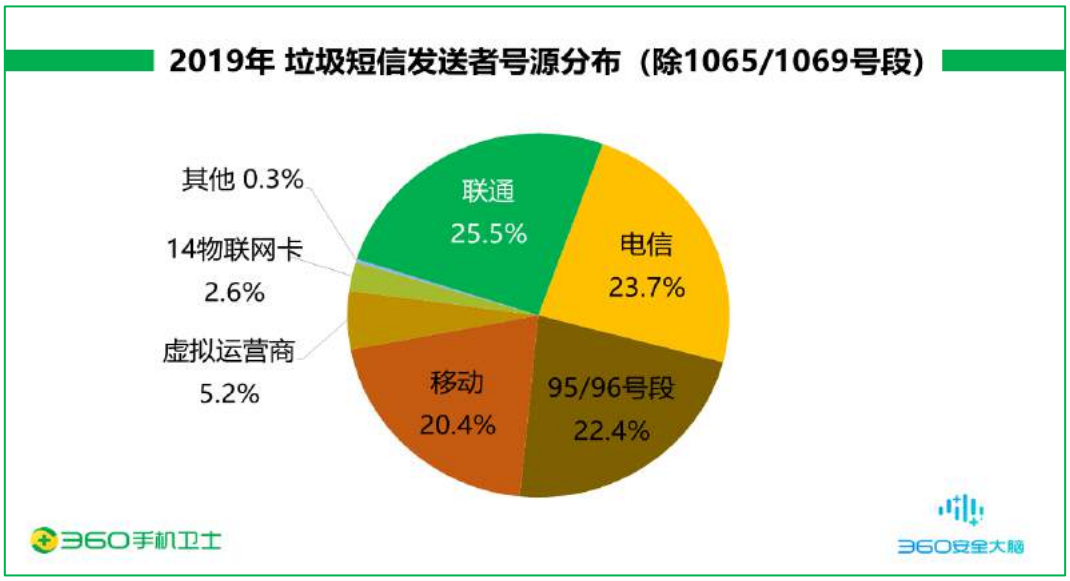


三、 垃圾短信运营商号源分布

2019 年全年，短信平台 1065/1069 号段发送垃圾短信占比高达 94.8%，已成为垃圾短信主要传播渠道。对比其他号源发送的短信，短信平台号段的号码整齐、格式统一，发送成本低，因此各大型购物、社交平台也会经常申请通过该号段发送各种平台促销或者招聘、金融广告等内容。同时，越来越多的垃圾短信甚至违法、诈骗类内容也会趁机通过该短信通道进行传播。

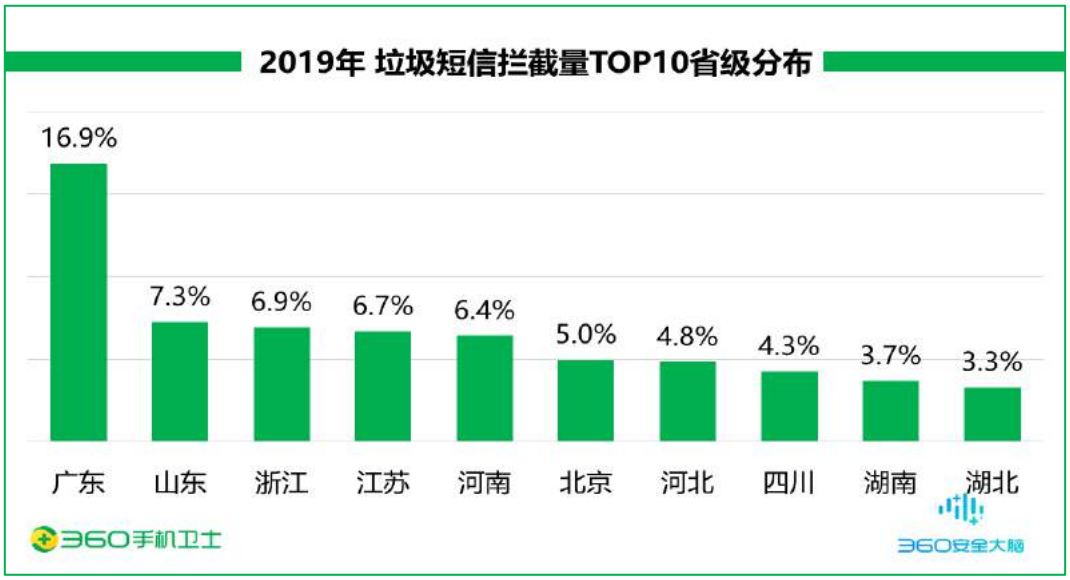


2019 年全年，除短信平台 1065/1069 号段发送垃圾短信外，从其他发送者号码个数分布看，运营商为中国联通的个人手机号发送垃圾短信的最多，占比 25.5%；其次是运营商为中国电信的个人手机号（23.7%）、95/96 号段（22.4%）、运营商为中国移动的个人手机号（20.4%）、虚拟运营商（5.2%）、14 物联网卡（2.6%）。

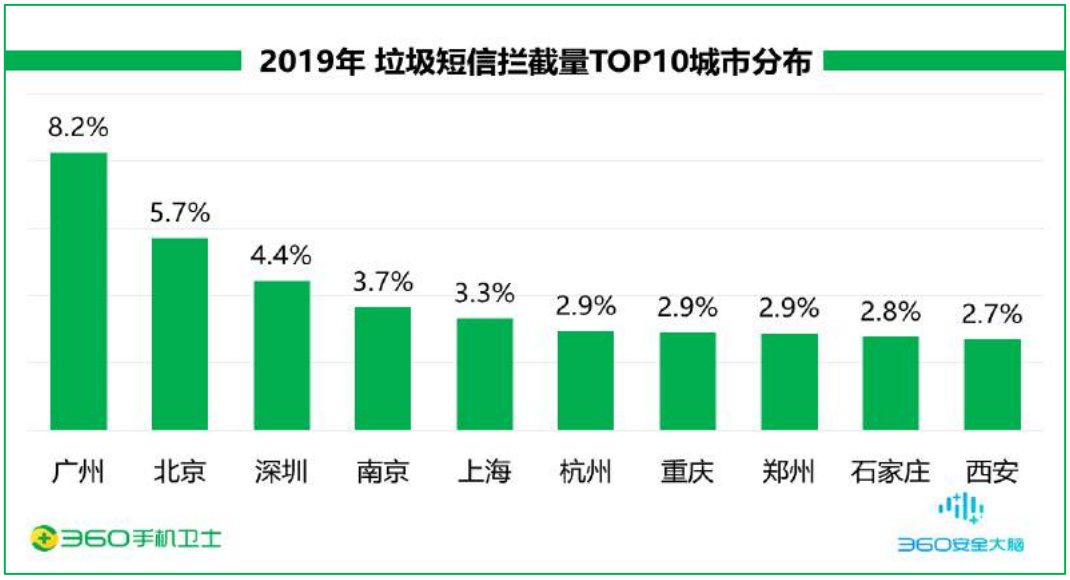


四、 垃圾短信拦截量地域分析

2019 年全年，从各地垃圾短信的拦截量上分析，广东省用户收到的垃圾短信最多，占全国垃圾短信拦截量的 16.9%；其次是山东（7.3%）、浙江（6.9%）、江苏（6.7%）、河南（6.4%），此外北京、河北、四川、湖南、湖北的垃圾短信拦截量也排在前列。



从城市分布来看，广州市用户收到的垃圾短信最多，占全国垃圾短信拦截量的 8.2%；其次是北京（5.7%）、深圳（4.4%）、南京（3.7%）、上海（3.3%），此外杭州、重庆、郑州、石家庄、西安的垃圾短信拦截量也排在前列。



第五章　2019 年手机诈骗现状

一、 报案数量与类型

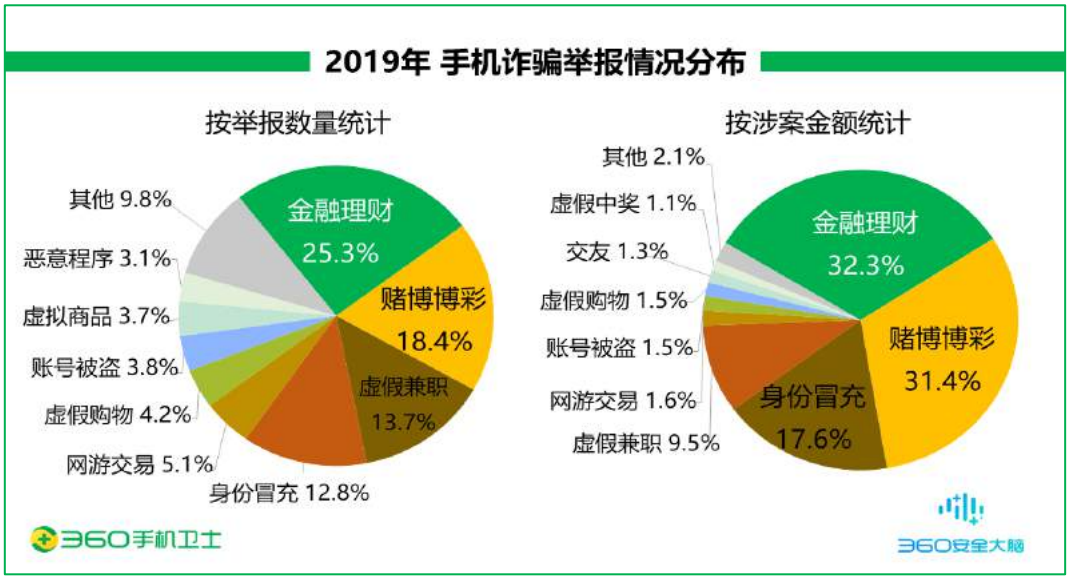
2019 年 360 手机先赔共接到手机诈骗举报 3924 起。其中诈骗申请为 1930 起，涉案总金额高达 1546.5 万元，人均损失 8013 元。

在所有诈骗申请中，金融理财占比最高，为 25.3%；其次是赌博博彩（18.4%）、虚假兼职（13.7%）、身份冒充（12.8%）、网游交易（5.1%）等。

从涉案总金额来看，同样是金融理财类诈骗总金额最高，达 499.2 万元，占比 32.3%；其次是赌博博彩诈骗，涉案总金额 486.2 万元，占比 31.4%；身份冒充诈骗排第三，涉案总金额为 271.5 万元，占比 17.6%。

从人均损失来看，赌博博彩诈骗人均损失最高，为 13658 元；其次是身份冒充诈骗为 10947 元，金融理财诈骗为 10208 元。

下图给出了主要手机诈骗类型的举报量和涉案总金额分布情况：



2019 年，手机诈骗中赌博博彩、身份冒充、金融理财属于高危诈骗类型，受害人数较多且人均损失高；信用卡、虚假兼职属于中危诈骗类型。信用卡类型虽受害人数少，但人均损失较高；虚假兼职虽人均损失偏低，但受害人数较多。

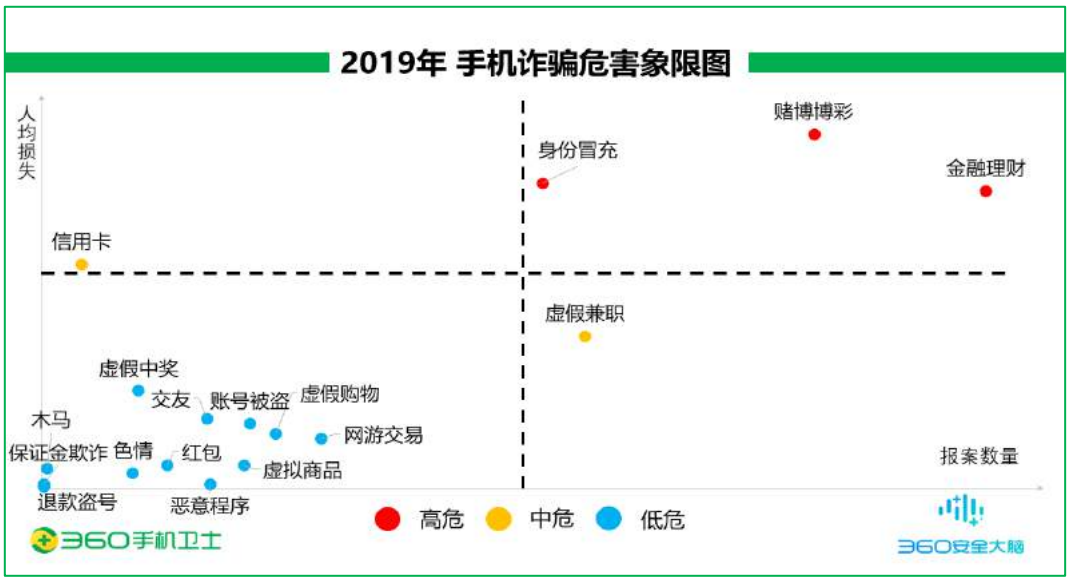
1） 赌博博彩类型主要为设立非法赌博平台、组织非法赌博游戏等，诱导用户充值进行娱乐。

2） 身份冒充类型主要以冒充亲友与冒充银行手法居多。其中，冒充亲友即为冒充亲戚朋友对用户社交账户中联系人进行钱财诈骗的行为；冒充银行则是通过伪基站发送诈骗短信，诱导用户访问钓鱼网址进行账户盗刷，或短信内容中以信用卡违规、账户冻结、卡扣除年费等虚假借口，引导用户主动联系短信内号码，实施下一步诈骗的行为；

3） 金融理财类型主要为贷款诈骗。其中，利用手续费、合同费、保证金等虚假借口引导用户进行转账的情况居多；而整个诈骗流程中运用虚假借贷 APP 的情况也较为常见，通过技术手段在 APP 内显示用户可贷款额度，在用户申请下款时，页面显示需缴纳验证费用或账户冻结，以此引导用户在 APP 进行支付，但最终不予下款。

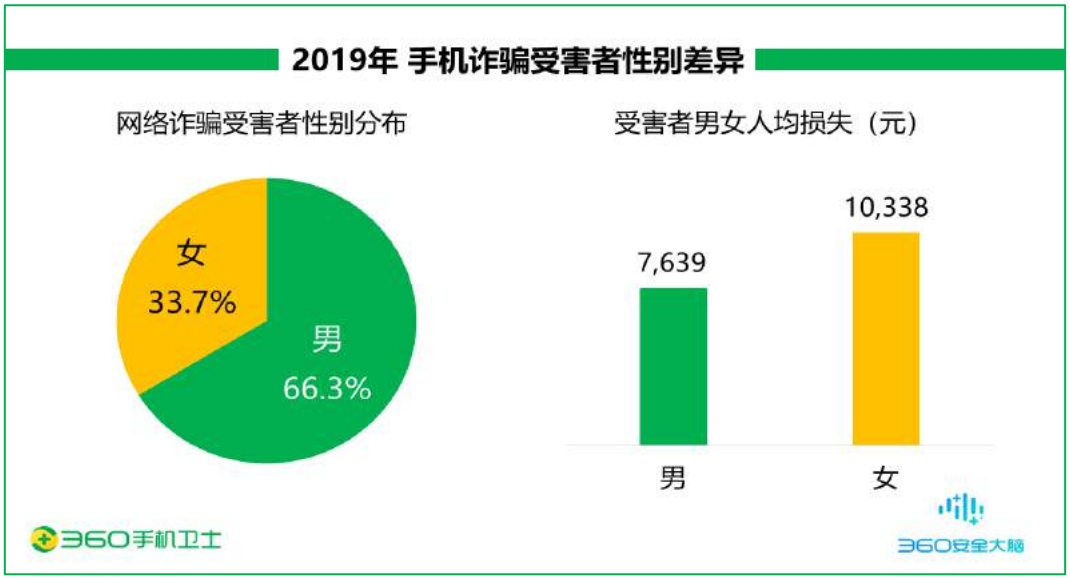
4） 信用卡类型主要利用个人信息泄露发起的定向诈骗，危害性较高。不法分子声称可对用户进行包装，增加发卡成功率。后续有可能利用合同费、手续费、工本费等虚假借口对用户实施多次诈骗。一般情况下，遭遇信用卡诈骗时损失金额均较高。

5） 虚假兼职类型主要以兼职缴纳会费的手法居多，会费金额一般在 200 元以下。但由于不法分子通常利用社交平台发布兼职广告，吸引众多用户进行兼职任务，导致遭受兼职诈骗的用户较多。具体分布如下图所示：

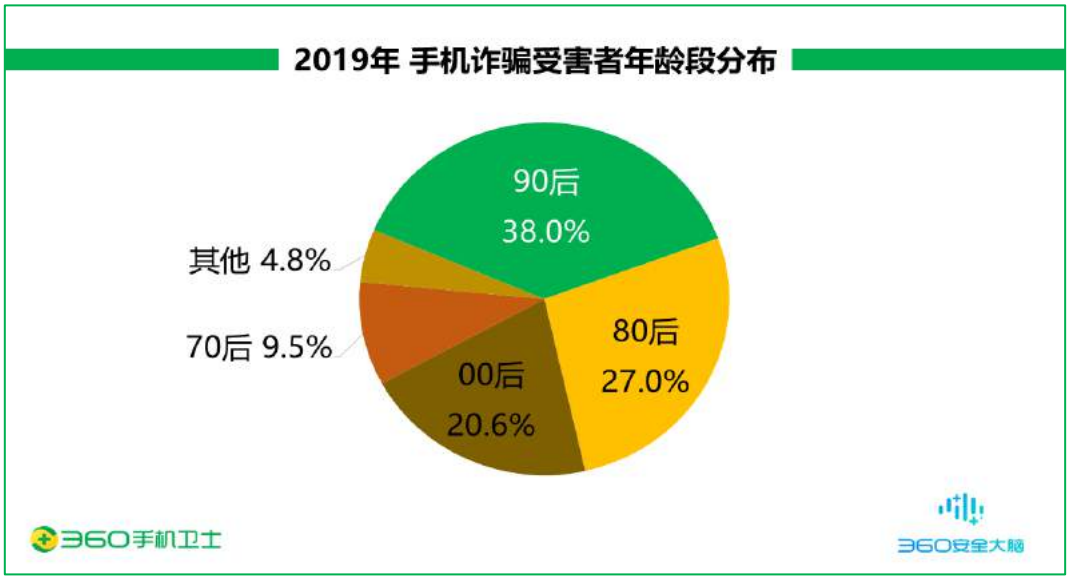


二、 受害者性别与年龄

从举报用户的性别差异来看，男性受害者占 66.3%，女性占 33.7%，男性受害者占比高于女性。从人均损失来看，男性为 7639 元，女性为 10338 元，男性受害者人数虽高于女性，但人均损失低于女性。



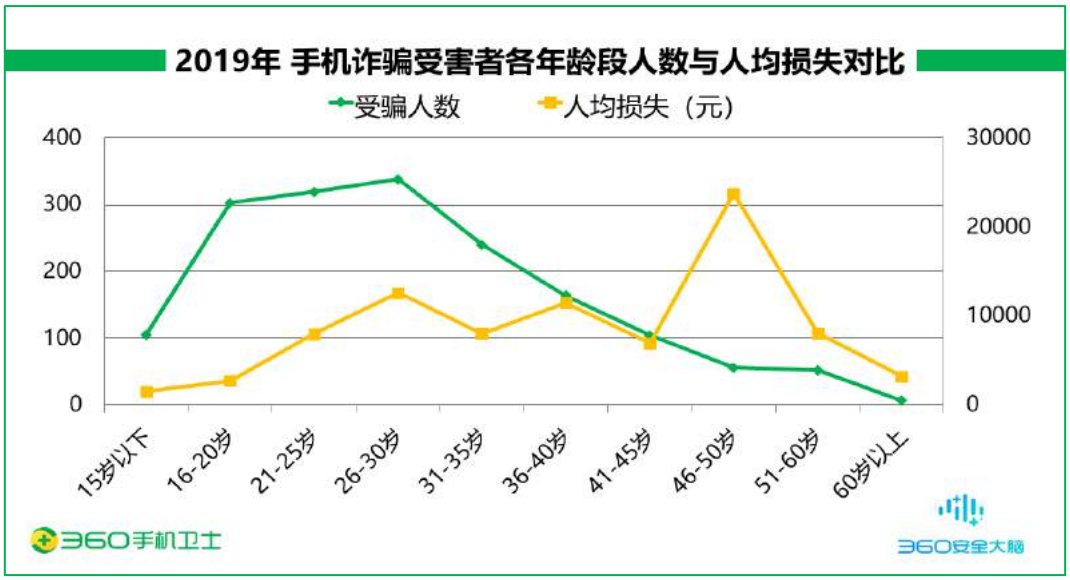
从被骗网民的年龄段上看，90 后的手机诈骗受害者占所有受害者总数的 38.0%；其次是 80 后占比为 27.0%；00 后占比为 20.6%；70 后占比为 9.5%；其他年龄段占比为 4.8%。如下图所示，2019 年 90 后为手机诈骗主要针对人群。



2019 年，手机诈骗受害者中 20 岁以下的用户，被骗的人数虽多，但由于这个年龄段用户经济能力有限，被骗平均金额相对较少。21 岁-30 岁之间的用户是 2019 年举报受骗的主要人群，这个年龄段用户有一定经济实力，人均受骗金额也较高。

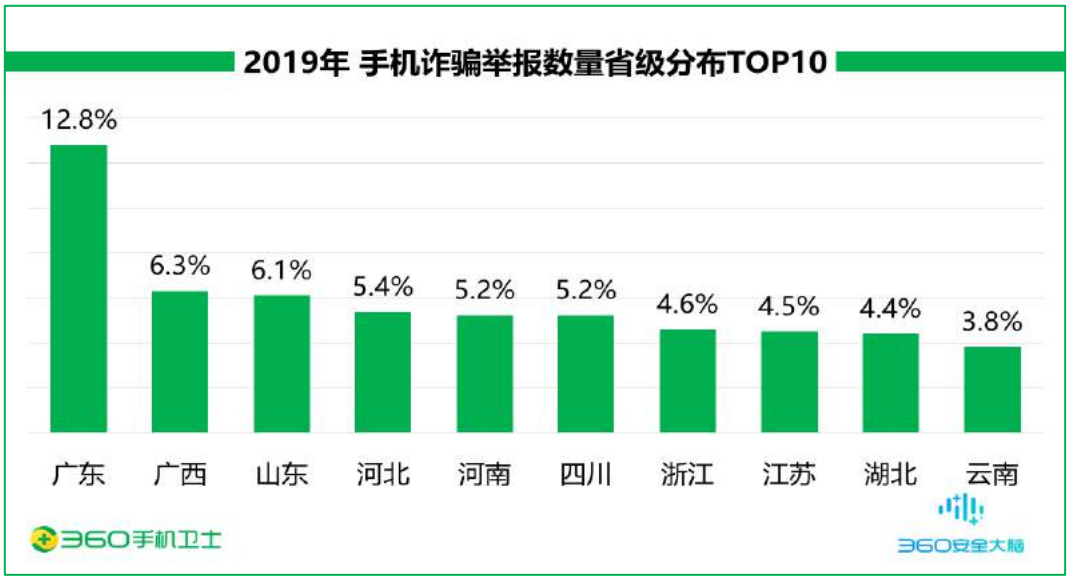
46-50 岁之间的用户，虽然已经不是上网的主力人群，但人均损失突破 2 万元。观察这个年龄段的用户，投资理财被骗的反馈较多。可见，投资理财在中年人群体中比较受欢迎，希望通过网络投资变现的投资人不断增多，但很多投资人并不明确行业市场大环境及其走向。很多人存在“跟投”、“盲投”的现象，同时缺乏投资理财方面的知识，投资风险较高，

极易遭受财产损失。具体分布如下图所示：

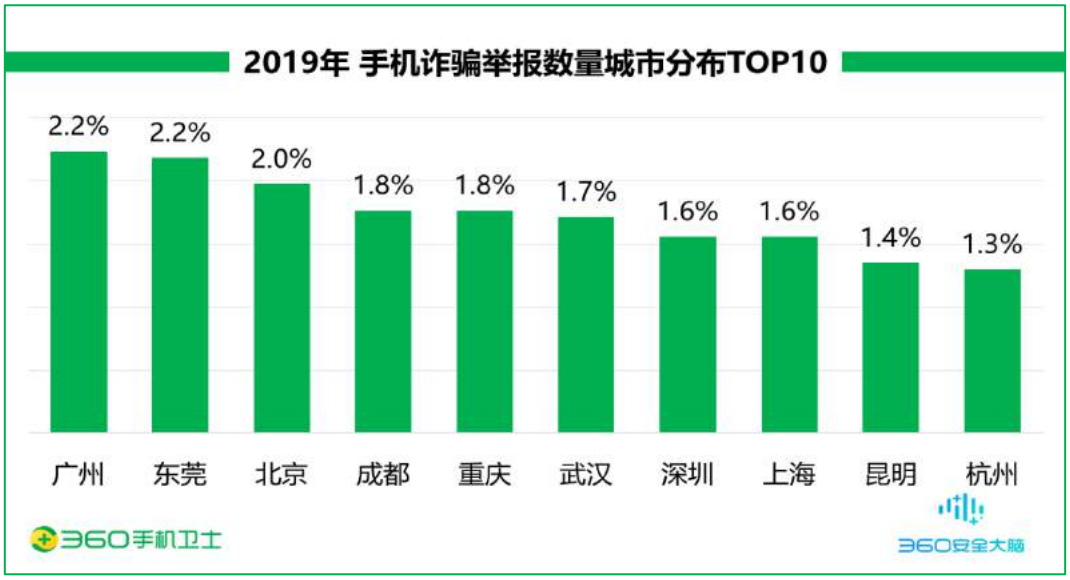


三、 受害者地域分布

2019 年全年，从各地区手机诈骗的举报情况来看，广东（12.8%）、广西（6.3%）、山东（6.1%）、河北（5.4%）、河南（5.2%）这 5 个地区的被骗用户最多，举报数量约占到了全国用户举报总量的 35.9%。下图给出了 2019 年手机诈骗举报数量最多的 10 个省份：



从各城市手机诈骗的举报情况来看，广州（2.2%）、东莞（2.2%）、北京（2.0%）、成都（1.8%）、重庆（1.8%）这 5 个城市的被骗用户最多，举报数量约占到了全国用户举报总量的 9.9%。下图给出了 2019 年手机诈骗举报数量最多的 10 个城市：


2019年 手机诈骗举报数量城市分布TOP10
2.2%
2.2%
2.0%
1.8%
1.8%
1.7%
1.6%
1.6%
1.4%
1.3%
广州
东莞
北京
成都
重庆
武汉
深圳
上海
昆明
杭州
360手机卫士
360安全大脑

第六章 2019 年移动安全重点趋势分析

一、 通信技术发达时代，骚扰治理形势严峻

互联网的萌发，技术能力的演进，对于互联网用户而言，本是一件便捷生活的好事。短信、电话作为生活中必不可少的一部分，拓宽了社交渠道，增加了信息来源。但随着黑灰产业的介入，信息爬取、新型短信、电话骚扰技术成为了困扰正常生活的绊脚石。以下通过对被黑灰产业介入并利用的短信及电话行业所产生的黑灰原理及手法进行分析：

1、 “闪信”成为黑灰产业从事非法行径的新“渠道”

1) “闪信”功能现状

短信作为功能机时代的必须品，进入智能机时代后，变得更加重要。平台注册，交易信息校验，用户无时无刻都在与短信打交道。2019 年 8 月多个用户在互联网反馈收到“闪信”短信，寻求科普。

“闪信”，又称霸信、屏信、0 级短信、弹屏消息、免提短信、来电名片，是一种在屏幕上即时显示的特殊文本信息。通俗来说，收到“闪信”的用户，信息内容直接显示在手机屏幕上。“闪信”本意是帮助政府和运营商，发送紧急信息，如极端天气、自然灾害、防诈骗的提醒。随着短信技术的发展，运营商根据时代需求，推出利用新技术达到和“闪信”相似可以在手机屏幕显示的功能，用来提示用户，如运营商帮用户拦截骚扰电话提示功能。此种技术的应用，意味着屏幕直显短信技术商业化。

（以下附图来自互联网）

2) “闪信”的两种显号方式，发送者显示号码与不显示号码

根据“闪信”类营销人员介绍，目前此种短信售卖渠道，存在多种发送通道，显示效果不同。有的渠道屏幕直显短信显示发送者号码和有的渠道则不显示。部分渠道发送的屏幕直显短信，在某些手机上可实现保存。显示发送者号码的短信平台，对发送的内容范围无限制，可以发送棋牌、博彩、贷款、兼职、理财等类型短信。此类短信价格每条约 6-8 分，量大甚至还可以获得批发价。不显示发送者号码的短信推送平台，发送的短信内容会有相应的限制，限制为地产、金融（贷款）等合法的营销内容。事前发送短信的语料需要审核，且审核周期较长。此类短信通道中，由于显示发送者号码的闪信，发送的内容基本无限制。此种类型的“闪信”被黑灰产业利用的可能性较大。

下图为两种不同效果的界面，及保存到手机中的效果：

3) “闪信”被黑灰产业利用，传播违法违规信息

屏幕直显文本技术的成熟，商业化的推进，带动了相关黑灰产业链的完善。短信渠道商通过搜索引擎、社交软件等渠道毫不隐晦的推广屏幕直显短信，部分渠道商在售卖此类通道时并不关心发送的内容是否违规违法，只关心发送的量级。短信渠道需求方，如违法小额贷、博彩、虚假广告，依托强大的短信直显技术推广自己的产品，以求达到近乎 100%的短信达到率。下图为闪信渠道交流群发送的广告，其中 BC、6h、QP、JZ、WD 分别为博彩、六合 、棋牌、兼职、网贷的简称。

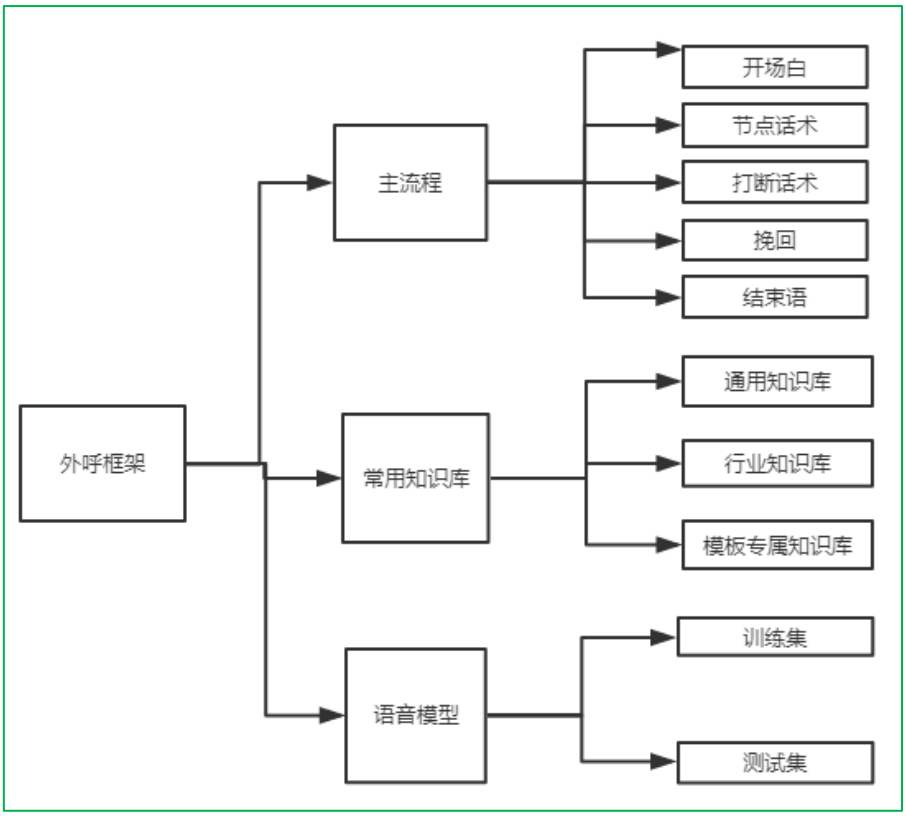
屏幕直显短信技术成为了一种黑灰的商业交易，用这种无法屏蔽的信息，打造出了效果近乎 100%广告投递效果。对于手机用户而言，这远比传统意义上的营销短信伤害大。目前主流安全厂商对于利用此类屏幕直显文本技术推广的黑灰短信，已可进行内容识别，并进行安全提示，降低了黑灰产业对此行业的恶意影响。

2、 骚扰程序化，外呼机器人被广泛应用

伴随着短信技术的发展，电话技术也进行了快速演进，进入了智能语音时代，模拟人工客服的外呼机器人应运而生。传统的销售行业，往往是通过人工拨打电话并筛选海量用户号码。此种人工客服群拨电话的方式，往往挂断率居高不下，筛选意向客户花费时间多，无法实施跟踪记录，调整获客方案。随着语音识别技术与人工智能技术的发展与成熟，集合拨打、回答、采集、推销于一身的外呼机器人出现，并在 2019 年呈现爆发增长趋势，各种电话机器人集成商打包提供服务。智能外呼机器人似乎成为了企业电话营销的利器，但作为接电话的一方，它的负面影响也很巨大。以下通过原理、产业链、应对方式等多个维度对外呼机器人行业进行解读分析：

1) 外呼机器人外呼电话实现流程自动化

外呼机器人的框架包含 3 个部分，主流程、常用知识库、语音模型。主流程为拨打电话的流程，包含开场白（电话开始的语音）、节点话术（在进行下一步时的场景转换语音）、打断话术、挽回话术（对已无意向的用户进行深度挖掘）。常用知识库为电话行业及所在行业的术语，包含通用知识库（电话技巧）、行业知识库。语音模型为外呼机器人的语料库，帮助外呼机器人了解语音类型，识别语音、识别语义，包含训练集和测试集。



外呼机器人的工作流程，拨出电话→接听→通话→挂断→标签分类→云端存储。外呼机器人通过呼叫中心拨打电话，利用语音识别、语义理解等技术方式识别接入方的语音。通过电话场景模板，了解接电话方的语义意图，进行正确的电话回复操作。对接听情况进行分析，判断没有接听到是由于网络原因、关机、挂断还是正在通话中，将此些信息进行标签分类。如意向用户，无意向用户，可进行转化用户。随着拨打电话次数的增加，借助增加的语料，增强对外呼机器人的学习能力，交互能力。筛选完之后会再根据标签来进行二次沟通。达到客户的筛选、沟通和分析的目的。

如下图展示的某外呼机器人平台的外呼话术流程。对外呼机器人的外呼话术、外呼节点进行了规定，帮助外呼机器人更好的疏通外呼流程：

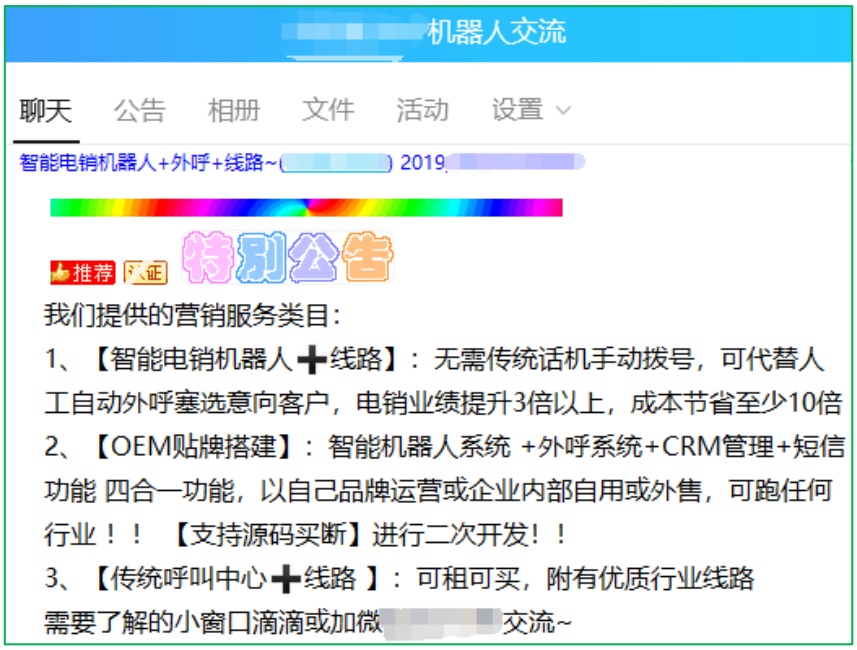
2) 外呼机器人通过 AI 技术可实现与真人无阻对话

“你需要买房吗？”、“你最近在做股票吗？”、“你需要投资吗”，不想被陌生电话打扰成为一种奢望。很多人接到骚扰电话后，出于礼貌总是会让对方先表明来意，如不需要再委婉拒绝。随着时间的推移，忽然发现，以前那套委婉拒绝，无法产生效果。无论怎么回答，对方总是像“老师”一样耐心开导“你”。原因在于电话背后的，并不是真人，而是外呼机器人。

3) 智能外呼系统搭建难度低、成本低，平台售卖渠道广

外呼机器人行业借助计算机算法技术的成熟、语音识别能力 SDK 集成化在 2019 年迅猛发展。智能外呼系统搭建包含四个部分，运营商线路、呼叫中心、AI 能力、服务平台。运营商线路提供通讯能力，呼叫中心提供集中化呼叫服务，AI 能力提供外呼机器人的语音、语义等识别技术能力，服务平台提供外呼机器人运营操作平台。组成外呼系统的四个部分，随着技术的发展，已经可以集成打包。在部分云服务器厂商平台就可能接入这种能力，搭建成本和难度进一步降低。

目前大多数的外呼机器人平台已将平台运营接口话，根据需求方输出在线或本地版的入口。需要外呼业务的人员，只需登录外呼网站后台，导入话术及需拨打号码，即可开始引导外呼机器人执行号码任务，一台机器每日可拨打上千个号码。但同时也意味着电话骚扰的严重。目前外呼机器人市场鱼龙混杂，各种渠道都可以发现他们的踪影，如搜索引擎，社交软件。



此些外呼机器人售卖渠道一般不会审核接入方资质及拨打的内容，企业是否有营业执照都不会过于审核。由于渠道商的放任，各类营销、欺诈电话蜂拥而至，带来了严重的骚扰。

在外呼机器人的语音、语义日益增强的情况下，接听电话的一方，在接听到外呼机器人电话时，无法察觉对方是真实还是虚拟的电话，轻则随着机器人的话术进行下一步，重则被对方套取多个角度的语音进行画像分析，后续源源不断的进行电话骚扰。虽然外呼机器人行业较火，但对于接听电话的一方则较为陌生，未接听过此类电话，或者接听电话后也无法识别此类电话，呈现出一种无奈的状态。

4） 通话场景下，外呼机器人仍存在语义障碍、语速过低等缺陷

外呼机器人虽然宣称强大，但仍存在不少缺陷，对于接听电话的一方可以通过以下的方式进行识别。接听陌生电话时不主动说话，尝试让对方先发生，根据对方第一句话的语义话术和停顿时间判断，人在接打电话时，说话的语速和话术会随着场景产生不顺畅性，不会像外呼机器人那样一次性完整毫无停歇的表达出语义。根据对方语速的流畅性，初步怀疑对方是外呼机器人后，可尝试表示不明白，打断对方的说话。查看对方的停顿周期，或在对方说完话后，不说话，停顿几秒。后续可能会发现外呼机器人已经无法准确对话。通过此种方式打破外呼机器人的常见认知、常见场景，让自身无法准确回复下一步话术。

5） 网络安全行业已实现技术拦截外呼骚扰电话

企业希望通过技术实现业务流程效率。对于企业而言，外呼机器人降低了运营成本，增加了获客率。企业希望外呼机器人能够不断提高自然语言处理的准确性，更加的智能化。对于用户而言，高频的营销电话影响了人们的正常生活。面对频繁的骚扰电话，用户想拒接陌生来电又有可能错过重要信息。用户希望通过技术避免自身遭受的电话骚扰问题。鉴于此种情况，网络安全行业借助 AI 的力量与骚扰电话行业进行了一场 AI 与 AI 对抗的比赛。

网络安全行业通过预防与识别两种手段增加对骚扰、欺诈电话的识别率，事前借助大数据实现对各种骚扰、欺诈电话号码的标记，在用户来电时对用户提示此为骚扰、欺诈电话。事中充当用户电话助理，帮助用户接听电话，通过语音、语义等技术识别来电方的意图行为，帮助标记并记录来电者的语音内容和意图，通过移动设备的通知栏、短信、社交软件推送电话信息。通过事前预防与事后识别两种方式，帮助用户阻挡电话骚扰。

3、 呼吁技术企业严谨自律，行业内加强管控，推进设立相关法律法规

在大数据和云计算的帮助下，各种新型的计算机技术运用到了现实生活，企业获取了互联网发展的红利，用户改善了生活方式，但技术一旦被滥用，甚至用于非法用途，将来带来社会问题，如短信、电话技术的骚扰、欺诈场景。对于技术提供方而言，可以通过几个维度降低这种“不良效应”产生的影响。对于技术提供方而言，进行行业限制，审核使用方的资质，避免骚扰类、欺诈类接入方使用该产品。进行场景限制，避免此类短信、电话技术被盗用于骚扰、欺诈。对于安全类产品而言，借力打力，顺应时代推出反制产品，如结合号码标记+语音语义识别的安全大脑，帮助用户识别，解决用户痛点与烦恼。

二、 山寨应用泛滥，打击其背后产业链刻不容缓

随着互联网快速发展，移动支付的便捷，人们对于移动端预约、处理交通事宜，有了迫切的需求。于是中国铁路客户服务中心网站（12306.cn）和 12123 公安部互联网交通安全综合服务管理平台正式上线。前者为用户提供客货运输业务和公共信息查询服务，后者为用户提供机动车/驾驶证/违法处理等业务预约、受理和办理等服务。出于名称的简约和对应用的信任，12306 和 12123 成为了平台的代名词，买车票用 12306，缴违章使用 12123。由于名称的“简约”性，黑灰产业开始利用相似名称，进行仿冒应用推广。此类应用由于是非“官方”应用，存在众多的陷进，套取用户隐私、诱导扣费，甚至推荐或直接售卖虚假产品。

1. 正规应用遭不法分子利用，山寨 APP 套路多、危害大

由于 12306 和 12123 的便利性和实操性，此类应用成为生活的必需品，也应运成为了国民级应用。从某应用商店的数据可以看出 12306 和 12123 下载量都已达千万级（数据采集时间截止 2019 年 1 月 6 日）。面对如此火热的产品，黑灰产业也想分一杯羹，于是开始了各种“借名”骗钱套路。

套路一：仿冒知名应用名称、描述，下载应用时需练就“火眼金睛”

用户下载应用时，一般使用手机应用商店或知名第三方应用商店下载应用。通过搜索“关键词”+描述内含“官方”字样判断应用是否为官方出品应用。如搜索 12306，应用描述为中国铁路总公司官方手机购票客户端，含“中国铁路总公司官方”字样；搜索 12123，应用描述为“交管 12123”是公安部官方互联网交通安全综合服务管理平台的唯一手机客户端应用软件，含“公安部官方”字样。针对以上的用户下载应用习惯，黑灰产业开始了自己的套路之旅：

1） 山寨 APP 名称功能性比官方应用更强，更具迷惑性

如 12123 查违章，12306 买火车票。这些应用虽带有 12306、12123 字样，但非政府部门出品的 12306、12123 官方应用。

2) 应用描述偷换官方二字概念

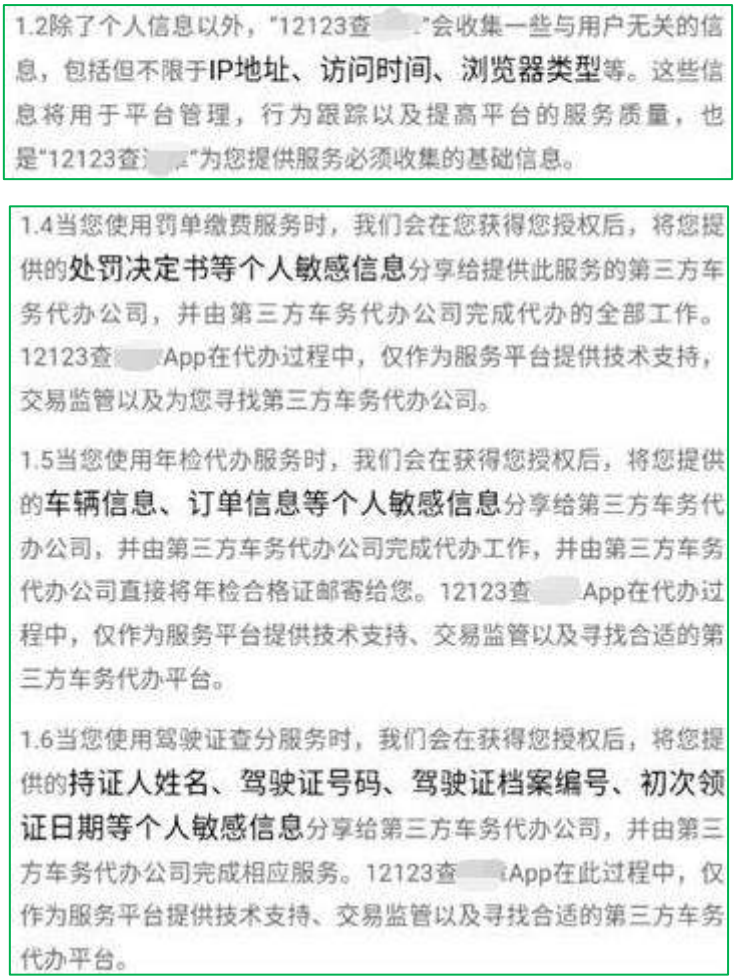
名称含 12123，12306，概述描述“官方出品”，让用户很容易以为这就是心中所想的哪个官方应用，但实际上应用描述的官方二字含义为自己运营平台对应的官方应用。如 12123 查*，为*3.com 的官方应用，其背后对应的平台运营方为某网络技术有限公司，非公安部。12306 买*，其背后运营公司为某信息技术有限公司，非铁道部。

套路二：应用“见雀张罗”，设置索取个人信息陷阱

用户在使用应用时，为快速进入应用，对于应用提示的用户协议信息，一般会选择忽略，直接点击同意。正是存在此种用户习惯的特性，仿冒 APP 在应用的用户协议内设置了很多用户信息索取、分享免责条款，甚至索要了与软件不相关的信息。

如在 12123 查*的应用协议内，索要了用户的 IP 地址、访问时间、浏览器类型。一个代缴费类应用，却需要索要一些与应用本身不相关，却与用户隐私密切相关的信息。同时，该隐私协议，还描述平台可将用户隐私分享给第三方，在商业上的合理努力的前提下，平台并不就功能、软件、服务及其所包含内容的延误、不准确、错误、遗漏或由此产生的任何损害，以任何形式向用户或任何第三方承担任何责任。

正是由于此种条款的存在，用户在此类平台上传的个人信息，在被共享的过程中，就存在信息泄露的可能。



1.2除了个人信息以外，"12123查[redacted]"会收集一些与用户无关的信息，包括但不限于**IP地址、访问时间、浏览器类型**等。这些信息将用于平台管理，行为跟踪以及提高平台的服务质量，也是"12123查[redacted]"为您提供服务必须收集的基础信息。

1.4当您使用罚单缴费服务时，我们会在您获得您授权后，将您提供的**处罚决定书等个人敏感信息**分享给提供此服务的第三方车务代办公司，并由第三方车务代办公司完成代办的全部工作。12123查[redacted]App在代办过程中，仅作为服务平台提供技术支持，交易监管以及为您寻找第三方车务代办公司。

1.5当您使用年检代办服务时，我们会在获得您授权后，将您提供的**车辆信息、订单信息等个人敏感信息**分享给第三方车务代办公司，并由第三方车务代办公司完成代办工作，并由第三方车务代办公司直接将年检合格证邮寄给您。12123查[redacted]App在代办过程中，仅作为服务平台提供技术支持、交易监管以及寻找合适的第三方车务代办平台。

1.6当您使用驾驶证查分服务时，我们会在获得您授权后，将您提供的**持证人姓名、驾驶证号码、驾驶证档案编号、初次领证日期等个人敏感信息**分享给第三方车务代办公司，并由第三方车务代办公司完成相应服务。12123查[redacted]App在此过程中，仅作为服务平台提供技术支持、交易监管以及寻找合适的第三方车务代办平台。

套路三：应用服务“暗藏杀机”，引导支付服务费

此类 APP 一方面通过应用权限、用户协议获取使用者的个人信息，一方面通过此类 APP 诱导用户进行付费。在通过此类 APP 进行罚款缴费的过程中，需要缴纳一笔服务费，而在“交管”12123 是缴纳交通罚款、在 12306 购买火车票是无需缴纳服务费的。通过搜索引擎及应用商店评论，可以看到多位用户在此类平台被诱导缴纳了服务费。（缴费截图来源于互联网）

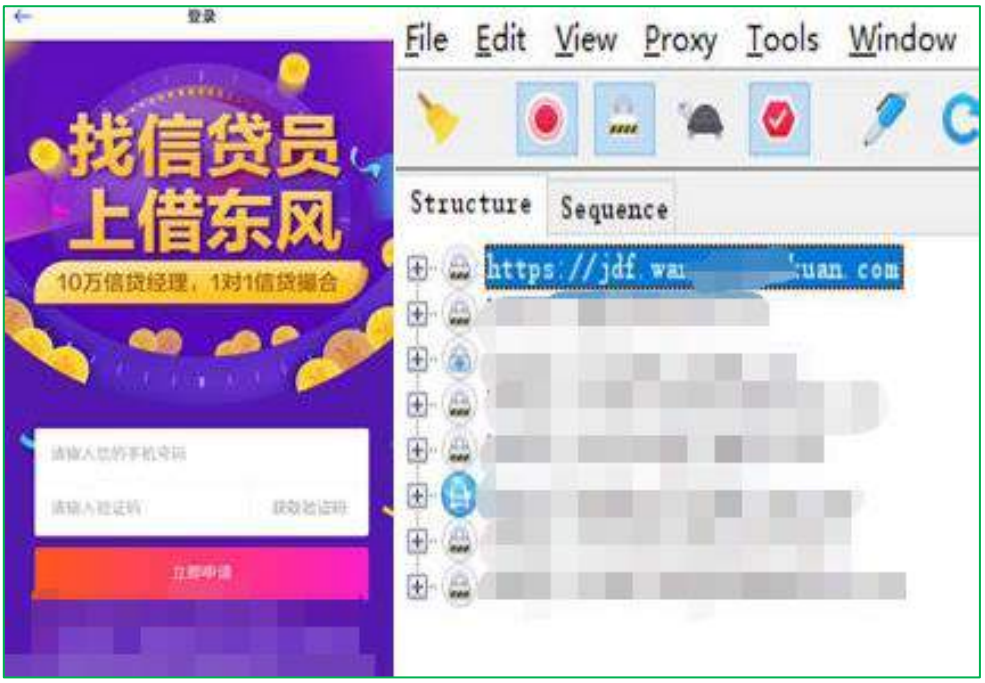
套路四：应用内广告“笑里藏刀”，推荐虚假产品

此类仿冒类应用，通过借名获得了大量用户及流量后，通过在平台内接入一些与应用无

关的广告，如贷款推荐、八字算命。但通过技术手段发现，这些广告源多为不具备经营资质的虚假平台。

如平台推荐的贷款平台，域名备案信息为某信息技术咨询有限公司，经营范围为信息技术咨

询服务；软件开发；数据处理和存储服务；数字内容服务；呼叫中心（不含需经许可审批的项目）；市场管理；信用服务（不含需经许可审批的项目），不具备开展金融贷款的资质。

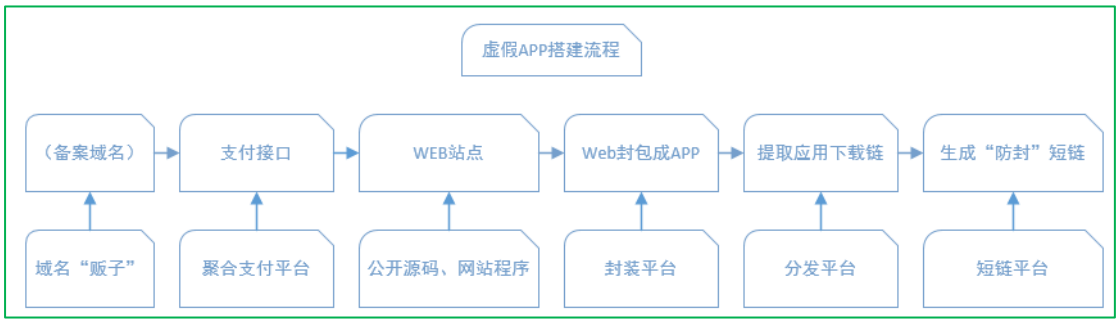


2. 山寨 APP 背后已形成搭建、推广、分成产业链

随着互联网 APP 行业的快速发展，“寄生”其上的黑灰产业规模和技术也在不断壮大和升级。APP 黑灰产业链条已十分完善和成熟，根据角色的不同，可分为产业链上游、中游和下游。上游提供 APP 搭建、中游负责各类接口对接，下游负责平台推广。

产业链上游提供 APP 搭建、上架服务

对自行搭建、推广，无需上架应用商店类的应用。 APP 搭建人员，从域名“贩子”手中买到大量（备案）域名，使用公开的源码或网站框架，接入支付接口搭建网站，通过一些 web 封装平台将网站封装成 APP，将 APP 上传至应用分发平台获得应用下载链（二维码或者 URL），在短链平台将应用下载链转换成短链接。如下图展示虚假 APP 制作过程、及搜索引擎中售卖虚假 APP 制作所需的资源网站。



安卓 APP 开发完如需上架应用商店，上游还会提供应用定制开发（原生类、HTM1 混合类）、计算机软件著作权登记证书代申请，帮助“虚假”类应用成功上架应用商店。

产业链中游提供 APP 开发所涉及到一些功能及支付接口

1） 开发 APP 需使用的身份查询、交通违章等接口

仿冒 APP 开发的过程中需要使用到一些查询接口，查询输入的数据否正确。如仿冒 12306 类应用需使用的 12306 车票查询及身份证实名认证接口；仿冒 12123 应用，需使用的全国交通违章查询接口；仿冒贷款应用，需使用的身份信息返照校验接口。如下图展示，在搜索引擎、数据提供商等渠道都可发现“他们”的踪影。

2） 开发 APP 需使用的支付接口

山寨的 APP 由于无法使用正规的支付接口，多采用第四方支付平台提供的接口。“第四方支付平台”指的是未获得国家支付结算许可，通过大量注册商户或个人账户，非法搭建的支付通道，非法对外提供支付结算服务。如下图展示第四方支付网站，提供的支付接口服务，如支付宝扫码、支付宝 H5、云闪付扫码、微信扫码。

产业链下游负责 APP“刷榜”、SEO、营销广告推送

仿冒类 APP 类完成定制后，为了吸引更多的人群使用，需要将 APP 进行包装推广，针对不同类型的应用，下游的推广商制定不同的方案。

1） 使用“刷榜”技术，推广应用商店的应用

用户使用应用商店搜索“不确定”应用时，一般会通过关键词的方式搜索，如搜索 12306；搜索 12123，根据搜索结果的排名，选择应用。鉴于此种用户使用习惯，下游 APP 推广提供商，提供一站式服务。如关键词优化、评论优化、关键词覆盖（产品分析、词汇分类、优化组合、迭代期优化）。下图展示的某些平台提供的应用“刷榜”一站式服务：

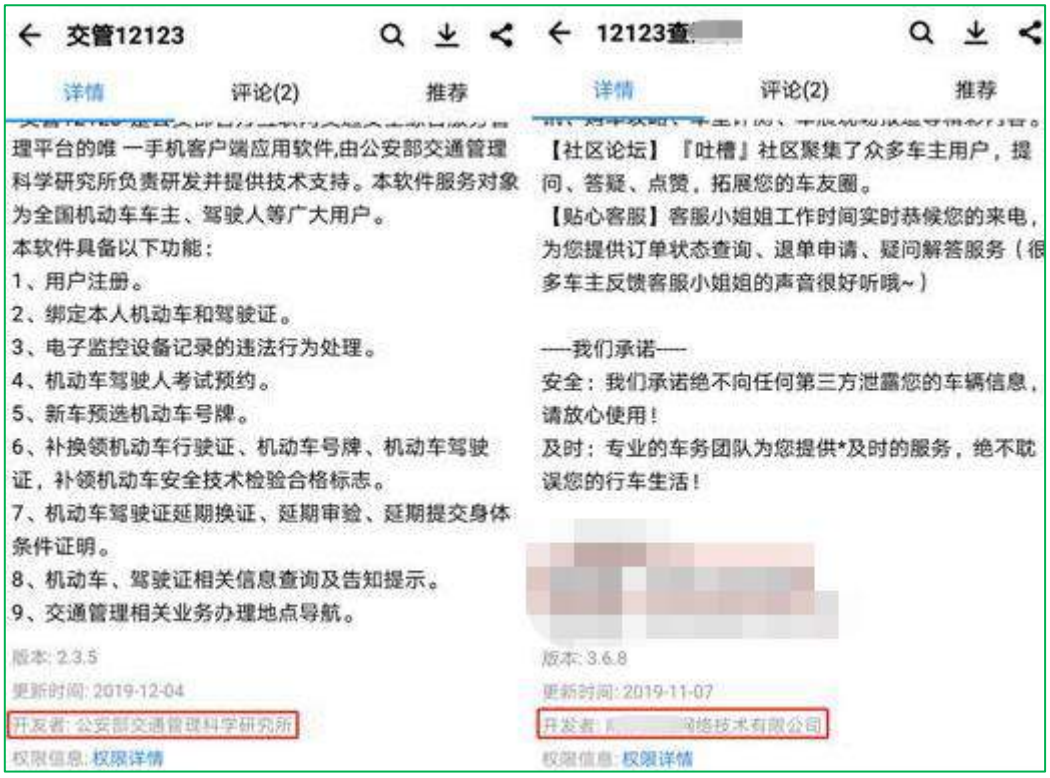
2) 使用黑帽 SEO、营销短信等方式推广应用

用户除通过应用商店下载应用外，还会通过其他渠道获取 APP。如搜索引擎、应用下载网站站（非常见应用商店）、好友推荐二维码（下载链）、营销短信（含下载链）、平台广告。针对搜索引擎，应用下载网站站（非常见应用商店），采用黑帽 SEO（搜索引擎禁止使用的作弊收录手段）优化方案，快速提升 APP 名称的收录排名；针对好友推荐二维码（下载链），采用社交群挂机平台，批量加社交群，在群内传播仿冒/虚假 APP；利用广告联盟，在联盟内通过高佣金，实现广告投放推广；利用卡池、伪基站、短信通道号平台群发短信。

3. 山寨应用泛滥，治理形势严峻

2019 年山寨类应用泛滥，究其原因，一方面是由于资源售卖渠道多、开源程序多、制作教程多，搭建成本低难度低，且接口技术平台方未对使用者信息进行二次校验；一方面是因为用户仍还处在依靠关键词+排名+评价的方式查找官方 APP。

针对山寨 APP 乱象，可以从加强虚假 APP 产业链打击和提高用户识别能力方两个角度进行。前者可以通过加强运营商、安全厂商的联合，实现资源互补，提升黑平台的识别能力。并从源头切断虚假 APP 的影响力。后者可以通过查看该应用的开发者，辅助判断应用是否为官方应用。与此同时，用户应养成使用杀毒软件查杀应用软件的习惯，做到事前预警，事中及时阻断。如下图展示，公安部出品的交通违章查询应用，交管 12123 的开发者为：公安部交通管理科学研究所，而高仿类应用，12123 查**的开发者为某网络技术有限公司。前者才是为公安部交通安全综合服务管理平台官方 APP。



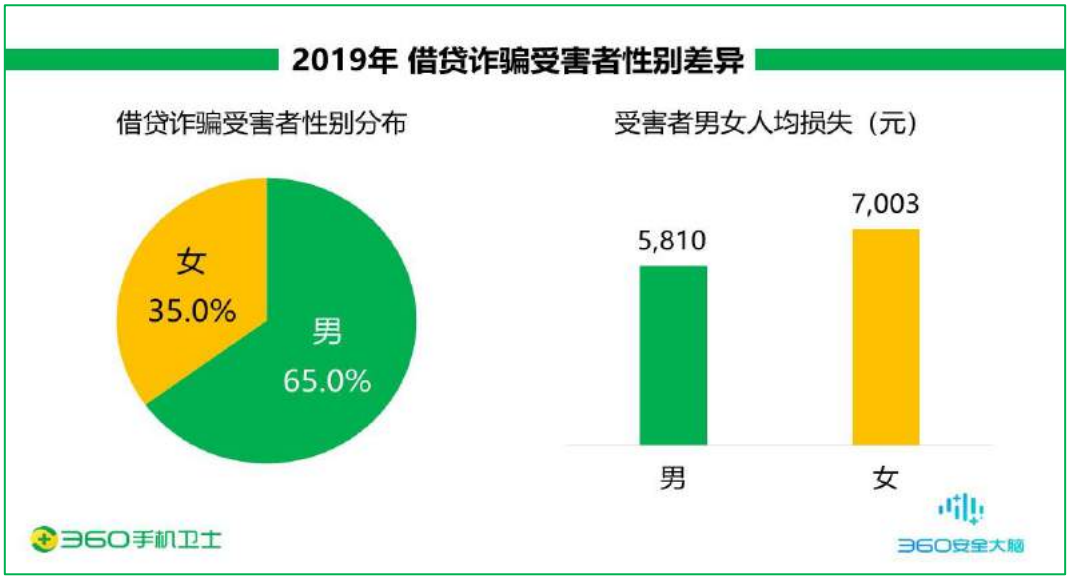
三、 虚假网贷已形成危害网络安全的产业链

随着中国经济结构和主力消费群体的变化，消费信贷市场逐渐迎来了蓬勃的发展。于此同时贷款也从早先的物质抵押，审核流程复杂，周期长，发展到使用金融 APP，动动手指，完成个人身份认证，便可获得所贷资金的演进。但现实却是用户一旦有了借贷需求，各种虚假信贷平台，如套路贷、贷款诈骗随之而来。本报告从“借贷欺诈手法”入手，通过分析借贷欺诈手法揭秘网贷黑灰产业链。

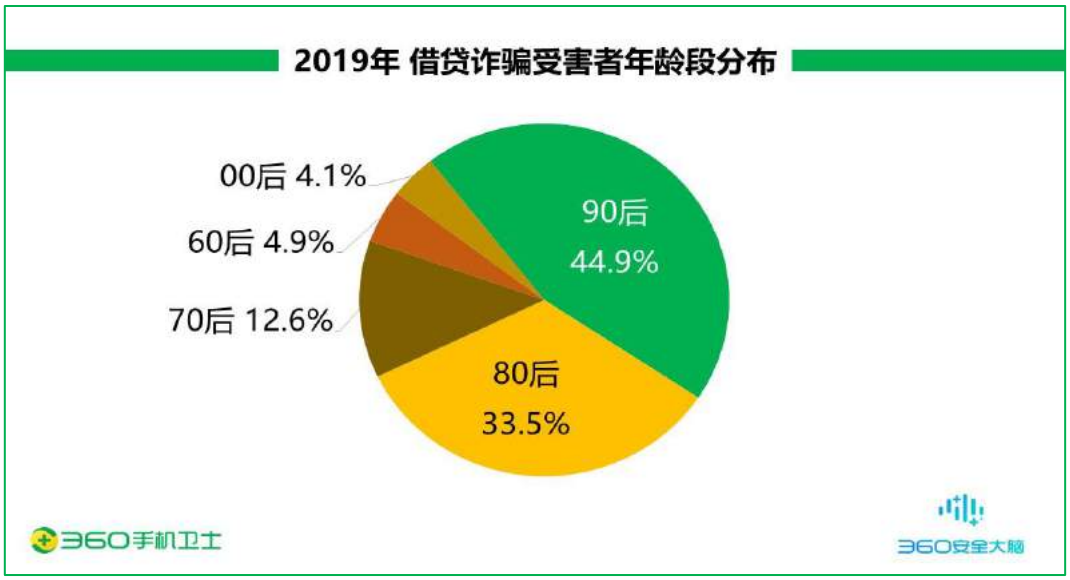
1. 2019 年金融借贷诈骗形势

2019 年 360 手机先赔共接到诈骗举报 3924 起。其中网络金融借贷诈骗申请为 363 起，涉案总金额高达 226 万元，人均损失 6227 元。

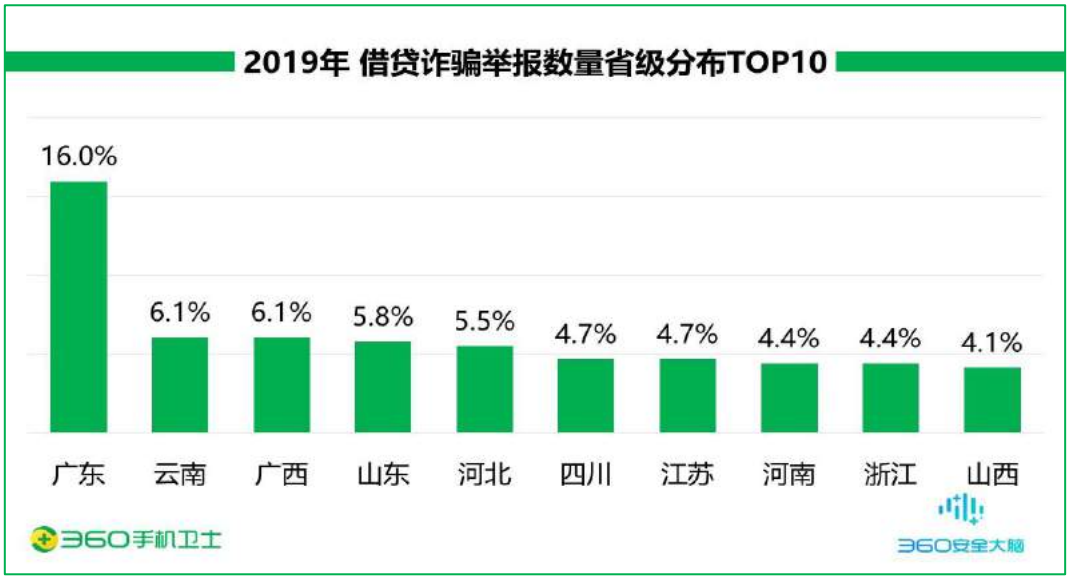
从举报用户的性别差异来看，男性受害者占 65%，女性占 35%，男性受害者占比高于女性。从人均损失来看，男性为 5810 元，女性为 7003 元，男性受害者人数虽高于女性，但人均损失低于女性。



从被骗网民的年龄段上看，90 后的网络借贷诈骗受害者占所有受害者总数的 44.9%；其次是 80 后占比为 33.5%；70 后占比为 12.6%；60 后占比为 4.9%；00 后占比为 4.1%。如图分布，2019 年 90 后为网络金融借贷诈骗主要针对人群。



2019 年全年，从各地区网络金融借贷诈骗的举报情况来看，广东（16.0%）、云南（6.1%）、广西（6.1%）、山东（5.8%）、河北（5.5%）这 5 个地区的被骗用户最多，举报数量约占到了全国用户举报总量的 39.5%。下图给出了 2019 年网络金融借贷诈骗举报数量最多的 10 个省份：



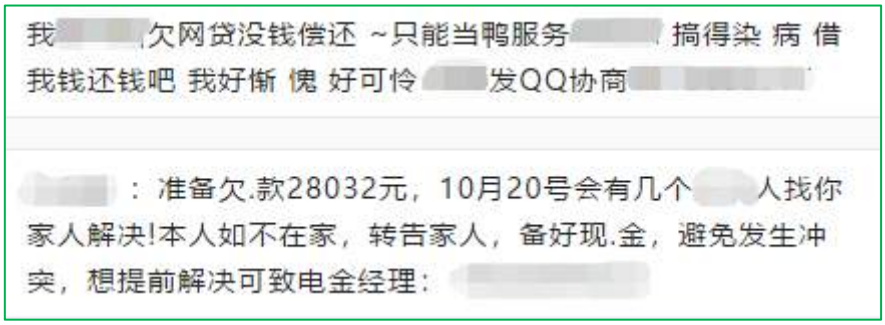
从各城市网络金融借贷诈骗的举报情况来看，北京（3.6%）、深圳（2.8%）、上海（2.5%）、广州（2.2%）、昆明（1.9%）这 5 个城市的被骗用户最多，举报数量约占到了全国用户举报总量的 13%。下图给出了 2019 年网络金融借贷诈骗举报数量最多的 10 个城市：

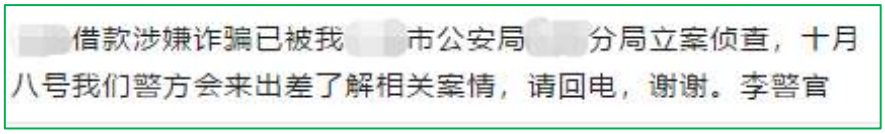
2. 网贷市场需求旺盛，传统 “高利贷”进军网贷行业

随着金融市场监管加强，不满足政策要求的网贷平台逐渐被“踢出”市场。网贷平台规模缩水，但网贷市场需求却没有缩减，于是传统 “高利贷”进军网贷行业。并催生出负责贷款推荐的“贷款超市”，负责贷款身份校验的审核平台，负责放款的套路贷（714 高炮）平台，负责逾期催收的“暴力”催债平台，以下对各个环节中出现的诈骗手法进行解读。

贷款超市是推荐贷款平台的应用，可以理解为应用商店，该应用商店内的应用都是借贷产品。使用“贷款超市”时，需上传个人身份信息及银行账号信息。开通贷款推荐服务时，会默认勾选一项“风险评估费”，一旦用户点了确认。无论后续用户借贷成功与否，此笔资金都会直接从用户在该平台绑定的银行账户内扣除。

套路贷俗称 714 高炮。借贷 1000 元到账几百元，须在 7 天或 14 天左右归还 1000 元，逾期会产生更高的利息费。不仅借贷利息高于国家规定的 36%，甚至会通过一些手段（还款当天还不上款）故意让用户产生逾期。当用户无力偿还时，还会引导用户去其他网贷借贷（同一放贷集团运作），让用户陷入借的平台越多，欠的资金越多的“魔咒”。当用户实在无力还钱时，群呼电话、短信等手段轮番上演。如下图展示，催收短信极尽侮辱之词，甚至冒充公检法给用户发送催收短信。



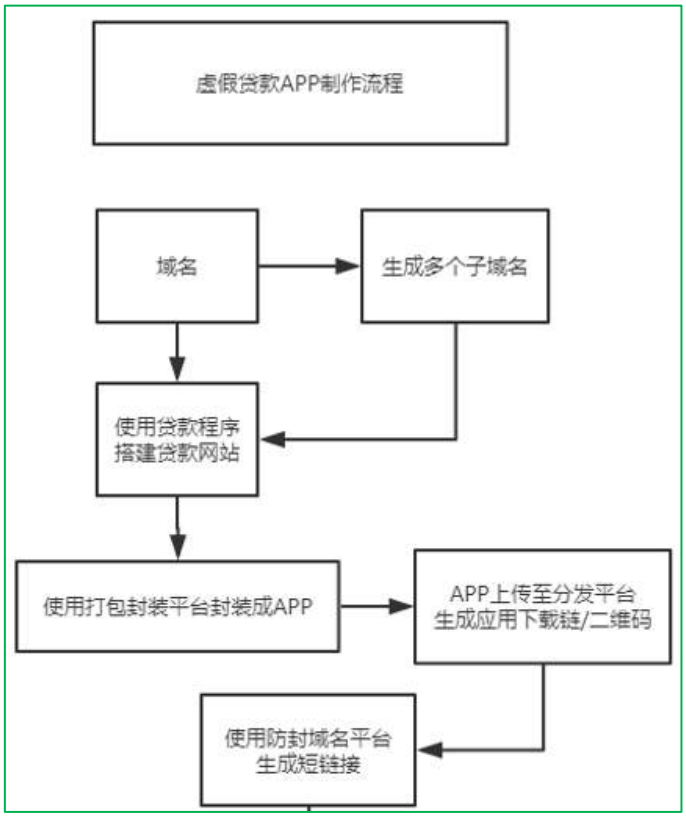


3. 虚假贷款平台背后已形成搭建、推广、分成产业链

随着互联网金融的快速发展，“寄生”其上的黑灰产规模和技术也在不断壮大和升级。网贷黑灰产链条已十分完善和成熟，根据角色的不同，可分为制作、推广、欺诈。

1） 制作方通过域名、开源程序等方式完成平台搭建

制作方通过域名售卖和抢注平台获取大量境内境外域名，利用境外服务器，使用贷款开源 WEB 程序，批量搭建 WEB 端网贷程序。完成虚假贷款平台搭建后，使用第三方封装平台将 WEB 平台批量封装成 APP，上架至应用分发平台，生成下载二维码，使用网址短链工具将二维码生成短链。



2) 推广方多通过买卖个人信息，实现平台“广告”推送

推广方通过卡商（贩卖手机卡）、号商（贩卖互联网账号）、社工库（互联网泄露数据库）获取大量个人信息、社交账号、电商平台账号。一方面使用卡池、伪基站、短信通道号平台群发借贷推广短信，使用外呼平台给借贷人员批量拨打电话，引导用户联系小贷平台客服或直接使用借款平台借贷。一方面利用 SEO、社交软件、网贷论坛假借知名贷款平台放贷，引导用户使用虚假贷款应用申贷。如下图展示的各类个人信息售卖论坛及虚假贷款短信。

3) 欺诈方利用多个诈骗“剧本”，利用违法工具，实现非法敛财

欺诈方通过短信、电话、社交软件等方式联系用户并取得用户信任后，引导用户安装虚假贷款 APP，待用户在平台上传完个人信息后，给用户推送资质审核短信，引导用户在平台提现。当用户在平台提现时，平台则显示用户征信不足、提现银行错误，账户被解冻，要求用户缴费解冻，甚至设置平台提现密码，索要提现密码费。即使用户按照要求向对方转账，对方也不会给予用户放款。

冒充知名贷款平台，电话联系用户，表示用户在大学期间有借贷记录，由于国家政策，严禁在校大学生在借款平台上有任何账号，否则会影响个人征信，要求受害者把之前的贷款平台账户注销。注销的流程为在各大贷款平台借贷，并将借贷资金转给对方。用户转账后，对方失联。

冒充贷款平台联系用户，表示用户贷款逾期，如果不能按时还款，会联系用户家人朋友强制催收。此类欺诈，由于对方掌握了用户的基本信息，用户容易相信对方，向对方转账。

3. 公民个人信息保护立法须加快推进

消费信贷市场的蓬勃发展，不仅促进了金融市场的发展，也吸引了网贷黑灰产业的进场。网贷黑灰产业的发展与升级，不仅影响了金融产业的良性发展，更给正常信贷用户带来了资金损失。针对网贷黑灰产业的肆虐，可以从以下几个角度进行治理。

1) 个人建立信息保护意识、企业建立客户隐私保护机制

从信息泄露的来源来看，一方面来源于用户的主动性泄露，一方面来源于企业的被动性泄露，黑客入侵企业服务器，获取企业的用户信息。对于用户的主动性泄露，用户需要养成个人信息保护的安全意识，不轻易上传包含个人信息的照片。对于手机、电脑等存在个人信息的设备，丢失后进行远程擦除。设备在二手平台出售前，通过专业软件消除保留的个人资料或去除存储媒介后售卖。对于企业的被动性泄露，企业建立业务逻辑测试模型，挖掘出业务可能存在的漏洞与不足，并及时修补。同时时刻关注行业风险动向，及时调整自身的云端风险监控模型与机制。防止自己基础数据被黑灰入侵，发生信息泄露事件。

2) 加强企业内部管理和渠道管控，促进移动转售行业持续健康发展

针对卡号商贩的违规办卡，违规收卡。运营商可以加强办卡过程中的身份认证，防止黑

灰产从业人员假借他人身份办法或利用空卡公司大量办卡。针对违规信贷欺诈短信，一方面运营商加强短信通道号发送内容审核，防止短信通道号被利用，一方面，网络安全厂商、手机厂商、运营商通过短信关键词、短信语义，短信画像等方式提升虚假借贷短信识别的能力。

3) 全行业加强技术管控、遏制虚假网贷蓬勃发展趋势

2019 年假冒借贷类应用泛滥，究其原因，一方面是由于资源售卖渠道多、开源程序多、制作教程多，搭建成本低难度低。另一方面是由于第三方技术平台对于封装上架应用未进行有效审核，对于缩短域名未进行安全认证校验。加强运营商、安全厂商的联合，实现资源互补，提升黑平台的识别能力。安全厂商通过客户端提示用户平台的虚假性，运营商从端口直接拦截虚假平台。

第七章 2019 年典型诈骗“剧本”TOP

一、 敛财手段新趋势，利用云闪付 APP 盗刷资金

案例回顾

2019 年 1 月王先生在微信朋友圈看到了微信好友发送的信用卡提额广告，添加了该广告内的客服微信。客服表示可以帮助用户信用卡进行包装，提升信用卡额度，其中农行，平安，广发支持空卡提额，其他银行需要存入信用卡额度 10%才可提额，每提升 1 万元，收费 100 元。王先生按照客服的要求，向对方提供了姓名、身份证号码、银行卡号用于查询审核信用卡综合评分。之后客服以需在注册平台做虚假交易，提供信用卡额度为由，索要了王先生的收到的云闪付注册及支付短信验证码。事后王先生发现银行资金发生损失，得知受骗。

专家解读

云闪付 APP 类似于银行快捷支付功能，使用任意手机号、姓名、银行账号即可完成注册，注册后可在银行账号的资金日限范围内进行消费及支付。此案例中不法分子通过用户对云闪付功能的不了解，引导用户在信用卡内存入资金，套取用户的身份信息、银行账号信息、云闪付注册验证码、支付验证码，再使用用户的此些信息完成云闪付注册及资金盗刷。

防骗提示

由于手机验证码内容较多，手机厂商为方便用户，往往此类验证码短信通过通知栏显示时，只突出显示验证码，而隐蔽正文内容，不法分子正利用此特点，通过急迫的语速索要用户收到的支付验证码，用户往往被骗之后才发现验证码是支付验证码。在别人索要短信验证码时，切记查看验证码短信的完整内容。

二、 博彩可刷单挣钱，“兼职”娱乐两不误

案例回顾

用户在 2019 年 5 月通过社交群了解到兼职赚钱信息，添加了兼职信息内所含工作人员的微信。该工作人员表示该兼职活动是做“套利”的。使用指定的*彩国际 APP，在平台购买指定的投注项目（*庆时时彩），可获取收益。在兼职活动期间，会给用户提供平台体验金和提现账号。在按照规定操作在平台盈利后，将收益资金提现至指定的银行账户，将给予用户兼职佣金。

用户在平台注册后，平台账号收到了对方充值的体验金。按照对方提供的购买项目教程投注，均获取了盈利。用户将盈利资金提现至对方指定的银行账户后，获得了兼职佣金。后续体验金周期结束后，用户在平台绑定了自己的银行账户，充值 2000 元，按照对方提供的操作教程，盈利后但无法提现，得知受骗。

专家解读

1) 博彩平台欺诈手法多变，早先使用博彩必赢计划，吸引用户在平台投注，使用前期盈利，后期亏损的方式骗取用户资金。现阶段使用平台提现陷阱的方式，骗取资金。使用对方的银行账户“代刷”时可提现，使用用户自己银行账户时则无法提现。

2) 此种骗局是利用刷单赚佣金降低用户的心理防线，获取用户的信任。一旦“上钩”，就会通过各种平台规则限制提现，想要解除限制，就需要投入更多的资金，被骗资金越来

越多，无法及时抽身。

防骗建议

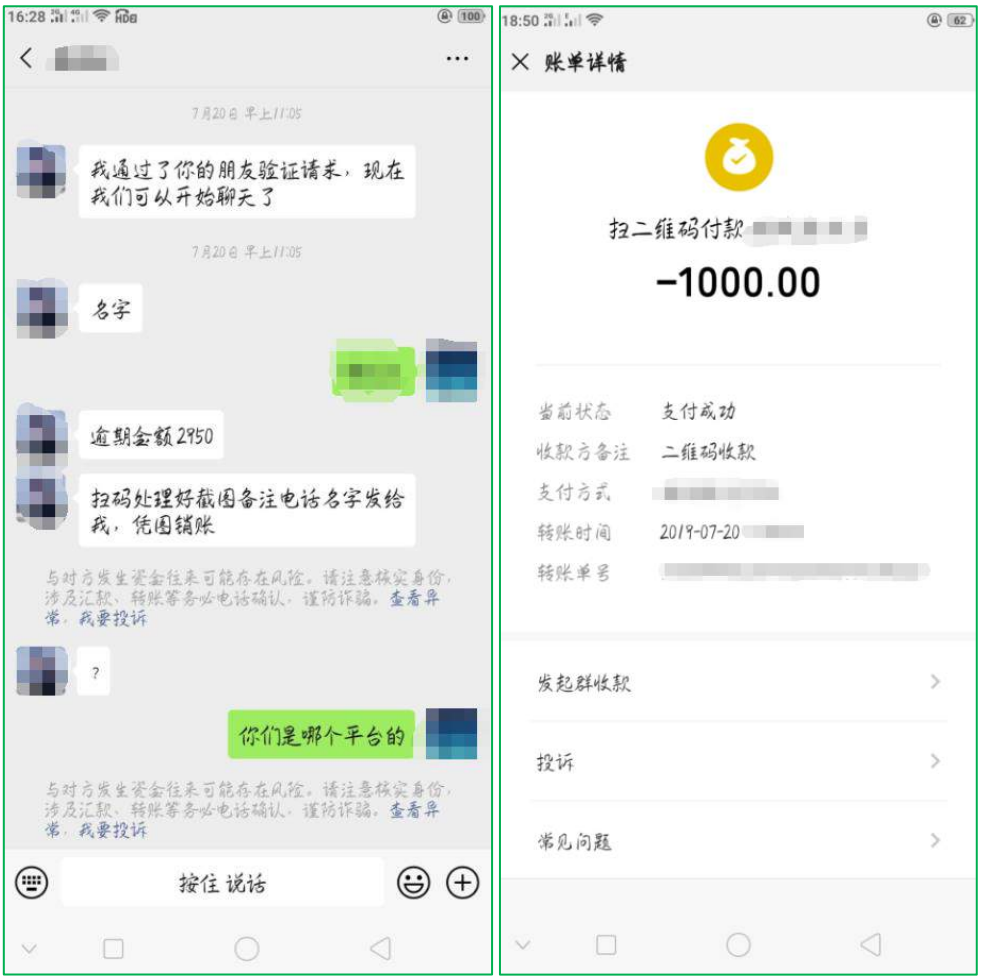
1) 在线博彩平台大多使用控制概率程序，对方通过控制输赢，造成博彩平台易赚钱的假象。教你轻松赚钱的人他其实在轻松赚你的钱，切勿因小失大。

2) 网络博彩属于违法行为，切勿向陌生人转账交易，保护好自身财产安全。

三、 冒充贷款平台催收：“你有贷款预期，加微信销账”

案例回顾

用户于 2019 年在多个小额贷款平台申请过贷款。在 2019 年 7 月，用户收到贷款催收平台电话，确认用户姓名后，表示用户贷款存在逾期情况。如果不能按时还款，则会联系用户父母强制催收，在用户及时还款后会给予销账回执单。随后，平台客服通过手机彩信的方式给用户发送收款二维码，并引导用户添加还款客服微信。在用户成功添加客服微信后，分多次向对方账号转账用于还款，共计 3350 元。但事后用户没有收到还款凭证，也无法联系上对方，得知受骗。



专家解读

1) 小额贷款平台的兴起，满足了人们超前消费的心理。但由于各种原因，存在着贷款逾期的现象，不法分子正是利用此种现象，冒充贷款平台进行催债。

2) 不法分子利用催促、恐吓的语气阐述逾期还款的严重后果，攻克用户的心里防线，获取到用户的信任。当用户轻信不法分子描述的种种后果后，不法分子则顺势引导用户通过转账的方式缴纳逾期贷款。

防骗建议

1) 不管从什么平台借款，一定要通过官方渠道及时还款，切勿轻信任何对私还款。还款之前，一定要明确自己是从哪个平台借款。

2) 如果接到此类电话请提高警惕，第一时间联系平台客服确认，是否欠款有逾期、逾期金额是多少，切勿被对方的言语迷惑。

四、 扫码领会员，全网 VIP 视频免费看？

案例回顾

影视行业火热，各家影视平台都有自家的独播资源，用户往往需要开通多个视频平台的会员账号才能实现全网资源播放。影视盗版产业正是借助此特点，开发了盗播各大视频平台资源的聚合类应用“全网 VIP 影视”。此类平台声称缴纳很低的会员费可以播放各大平台的 VIP 资源，浏览广告还能赚取广告费，邀请他人购买会员还可获得分成。随着各大影视平台加大对影视资源的版权保护，此类平台的“生存空间”越来越小，用户刚刚缴纳高额费用成为平台合伙人，准备实施赚钱大计一展拳脚时，平台已经圈钱跑路。

专家解读

此类平台利用盗播各大影视平台片源，通过“传销式收徒”模式，发展平台“合伙人”，套取用户资金，后期一旦影视平台升级接口限制盗播，此类平台就会陷入视频无法播放的境地，甚至圈钱跑路。

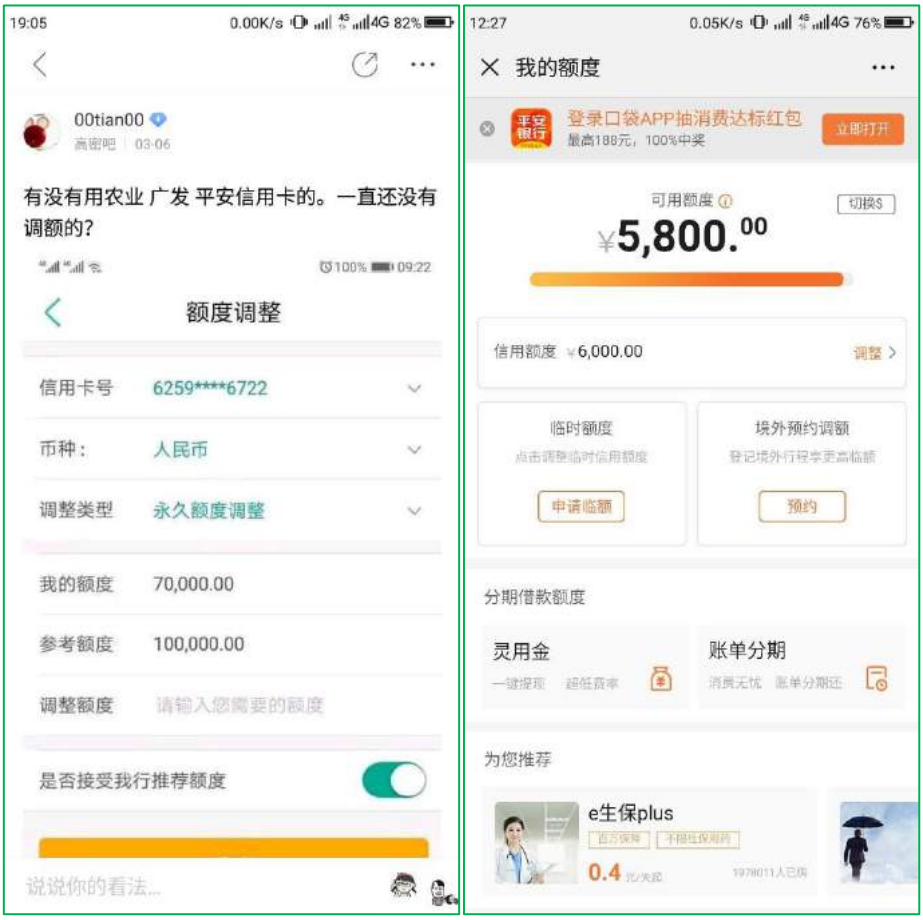
防骗提示

影视行业盗版、盗播屡禁不止，以兜售资源为由头，不断拉人入资源群赚取“代理费”的模式存在风险。用户对此要做好预警和判断，尽量选择正规的影视平台。

五、 信用卡“隐形额度”可以透支刷，9102 年了别说你不知道？

案例回顾

2019 年 3 月张先生在网上查看到信用卡提额的帖子，并添加了对方的微信。对方表示可以帮助张先生信用卡进行提额，同时索要张先生的信用卡额度截图(6000 元)，并要求张先生找朋友先将信用卡额度刷取至总金额的 1/3，张先生遵循步骤后，信用卡额度剩余 3800 元。对方以信用卡提额需要刷银行流水为由，要求张先生通过指定的提额二维码刷一笔支付失败的订单，用于银行验证，支付金额为 4397 元。同时对方表示，由于张先生的信用卡现在无法支付金额高于剩余额度的订单，所以不会支付成功，一定会支付失败，告知张先生无需担心。但是银行验证的过程有时间限制，需要张先生抓紧时间操作。于是，张先生听信对方的叙述迅速完成了扫码支付，意外的是，订单却支付成功了。等到张先生再次联系对方询问订单情况时，发现好友已被对方删除，这才得知受骗。



专家解读

信用卡提额诈骗针对的目标人群是：日常生活中频繁使用信用卡进行透支消费，但现有额度无法支撑日常消费需求的人群。利用持卡人急于提升信用卡额度的心理，同时利用信用卡透支盲点，诱导其进行订单支付，达到欺诈目的并盗刷用户账户。

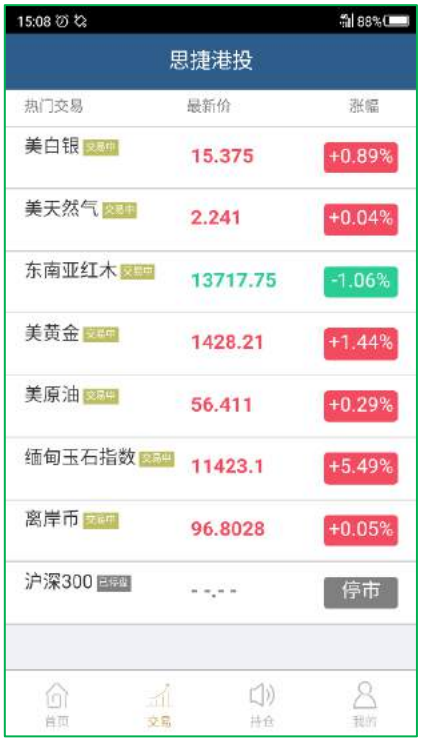
防骗提示

在持卡人有提额需求时，可以通过正规渠道联系银行进行提额申请，由银行对持卡人进行信用评估后，做出账户是否可以提额的判定。案例中以刷流水为借口诱导用户支付问题订单的形式，在用户详细考虑后，都可意识到其中蕴藏的猫腻。但不法分子以支付过程有时间限制为理由要求用户迅速支付，不给用户详细思考的时间，这种情况下，当用户听信不法分子的说法进行支付时，极易掉入不法分子设置的陷阱中。对于信用卡用户而言，应保持良好的信用卡消费习惯，增强防范信用卡防骗意识。

六、 一夜之间深陷投资“陷阱”，“杀猪盘”解密

案例回顾

2019 年 6 月王先生收到微信好友的添加请求，通过后，与该微信好友交谈工作情况、恋爱情况以及对爱情伴侣的要求。对方在与王先生聊天的过程中，时而会告诉王先生某天又赚了几千元钱，吸引王先生的追问。王先生追问后，顺势给王先生介绍期货平台（思捷港投）软件，教导王先生在期货平台购买“缅甸玉石指数” 、“东南亚红木”等项目。王先生前期在对方的指导下，获得了收益，后期购买的项目出现价格波动，加上王先生自身资金紧张，不想再投入资金。对方就以王先生“大惊小怪”为由，催促投资，王先生出于“面子”问题，增加了投入，投入的资金后期基本亏损完，得知受骗。



专家解读

不法分子，从获客，用户管理，人设制造，情感经营，套路流程，转战取财再到资金转移，“杀猪盘”团伙打造了一套非常完整的“诈骗工作体系”。先以交友为幌子，通过“撩友”的话术，让用户沉迷其中。再诱骗用户在虚假理财平台投钱。通过多变的“语言”透露自己对用户不投钱的不满。最终用户处于不投钱怕“心上人”不理自己，投钱又怕上当受骗的矛盾心理，最终即使自己没钱也要借钱投进去。

防骗提示

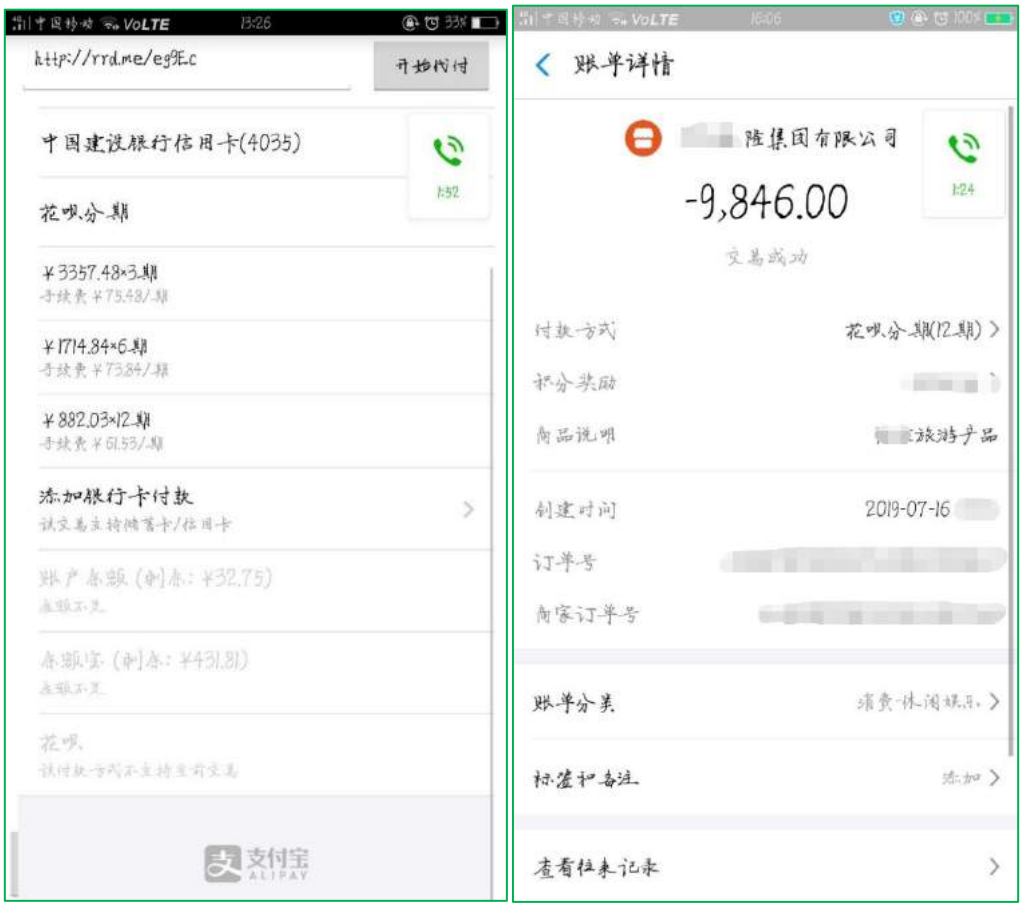
这些“养猪”的屠夫，其实离我们并不遥远，每一个突然找上门的“陌生人”，都有可能是骗子。网络交友千万条，绝不掏钱第一条！

七、 明明付款“0 元”，怎么就背上了千元贷款？

案例回顾

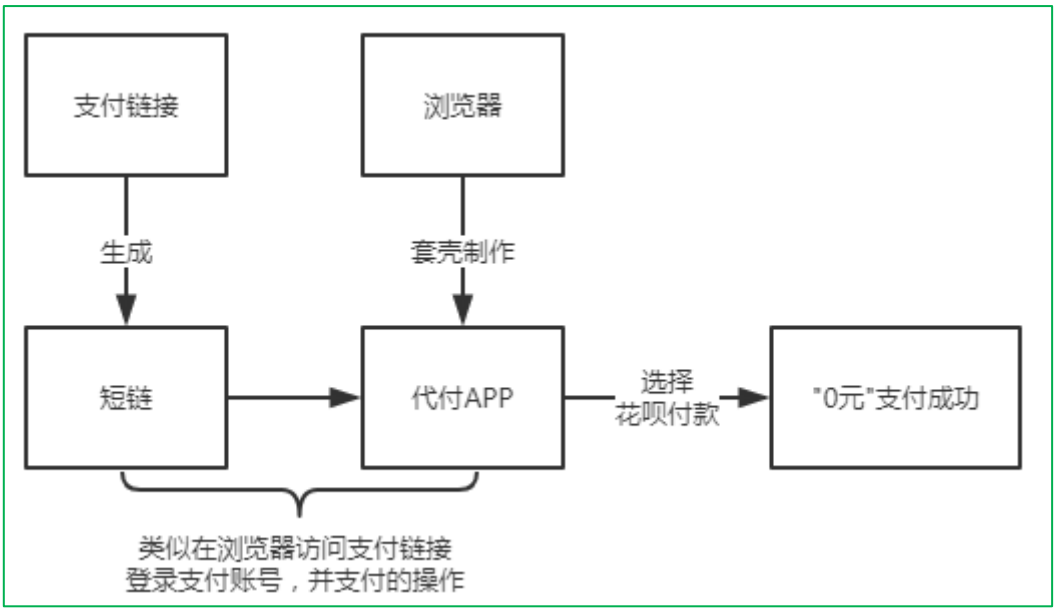
2019 年 7 月李女士在微信群了解到兼职活动，联系对方后，对方表示该兼职活动为电商刷单，费用由商家代付，无需用户付款，用户帮忙刷单后，根据金额不同，会获得不同金额的佣金，在得到李女士确认刷单的回复后，以刷单需验证刷手资质为由，索要了李女士的淘宝淘气值及花呗首页截图。

随后李女士在对方指引下，安装了商家代付（小海代付）APP，将对方提供的需刷单商品链接输入小海代付 APP 内，根据页面提示登录了自己的支付宝账户，选择花呗付款，页面显示 0 元支付。李女士看到页面是 0 元支付，以为是对方所描述的费用由商家代付，于是输入支付宝支付密码进行了“0 元”支付。支付后，退款客服以李女士退款账号存在借款额度，要求李女士将支付宝借呗额度，网商贷额度转至支付宝，随后李女士表示退款怎么还需借款，在对方无法明确回答的情况下，李女士得知受骗。



专家解读

此类兼职刷单属于利用代付 APP 实施诈骗。不法分子先以兼职刷单由商家代付，无需用户付款为由放松用户警惕，再利用所谓的代付 APP，诱导用户支付商品费用。该代付 APP 可以理解为一个浏览器，用户在代付 APP 访问短链的过程，就相当于在浏览器访问支付链接的过程。随后使用话术引导用户输入支付平台的账号密码，选择花呗付款。商品由于选择了花呗付款，当前的支付金额就为 0 元。

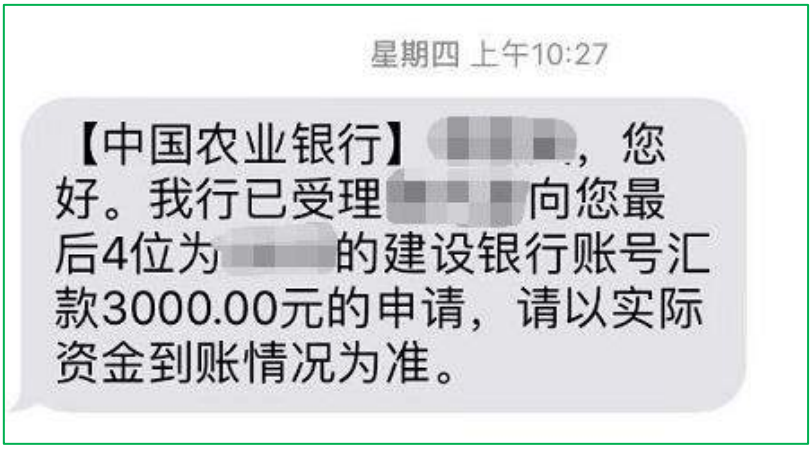


防骗提示

刷单是一种作弊行为，国家法律法规、淘宝等电商平台均明令禁止这种虚假交易。切莫相信低投入、高回报的幌子，通过正规渠道寻找兼职，确保付出得到回报。同时不要轻易点击或扫描陌生人发来的网页链接和二维码，增强互联网安全。

八、 转账给对方的钱，还能悄么声的拿回来

2019 年 11 月，360 用户反馈，表示自己在某电商平台售卖商品过程中遭受欺诈。用户在电商平台收到买家的商品咨询消息，买家假装与用户洽谈购买事宜，双方确认了尺寸、价格以及购买数量，此时，买家提出自己是帮助公司采购，想要赚取差价。商品总价 2000 元，自己上报财务 3000 元，由财务给用户转账。用户收到财务转账后，将资金全部转给自己，然后再通过店铺下单。随后用户收到银行的短信通知。出于账户资金安全考虑，用户在询问身边朋友后，发现此种方式可能是诈骗，后续并未向对方转账，避免了资金损失。



专家解读

其实，这种诈骗手段非常简单，就是钻了“银行到账时间差”的空子。使用网银转账的过程中，可以选择到账时间：实时到账、2 小时后到账、次日到账。在发卡行受理转账业务的有效时间内，可以向发卡行申请撤销转账转账。也就是说，银行的短信通知并不代表实际资金已经到账。

防骗提示

对于通过网络进行买卖的行为，警惕诈骗分子利用滞后到账这一办法，打“时间差”，空手套白狼。收到此类短信，一定要通过通过线上网银或线下银行查询资金到账情况。

第八章 2019 年热门安全事件 TOP

一、 新品种“虚拟货币”，垃圾分类能挣钱

2019 年上海实行“最严垃圾分类”，“你是什么垃圾？”成了上海人民每天都要面临的灵魂拷问。借助垃圾分类的推行，各家知名互联网公司纷纷推出垃圾分类识别产品，但随之而来的是各大黑灰产打着“垃圾分类”噱头的项目。2019 年 9 月多个黑灰产网站开始推广一款名为“EP 环境保护”，垃圾分类赚钱 APP，但此应用实际是虚拟货币炒币项目。

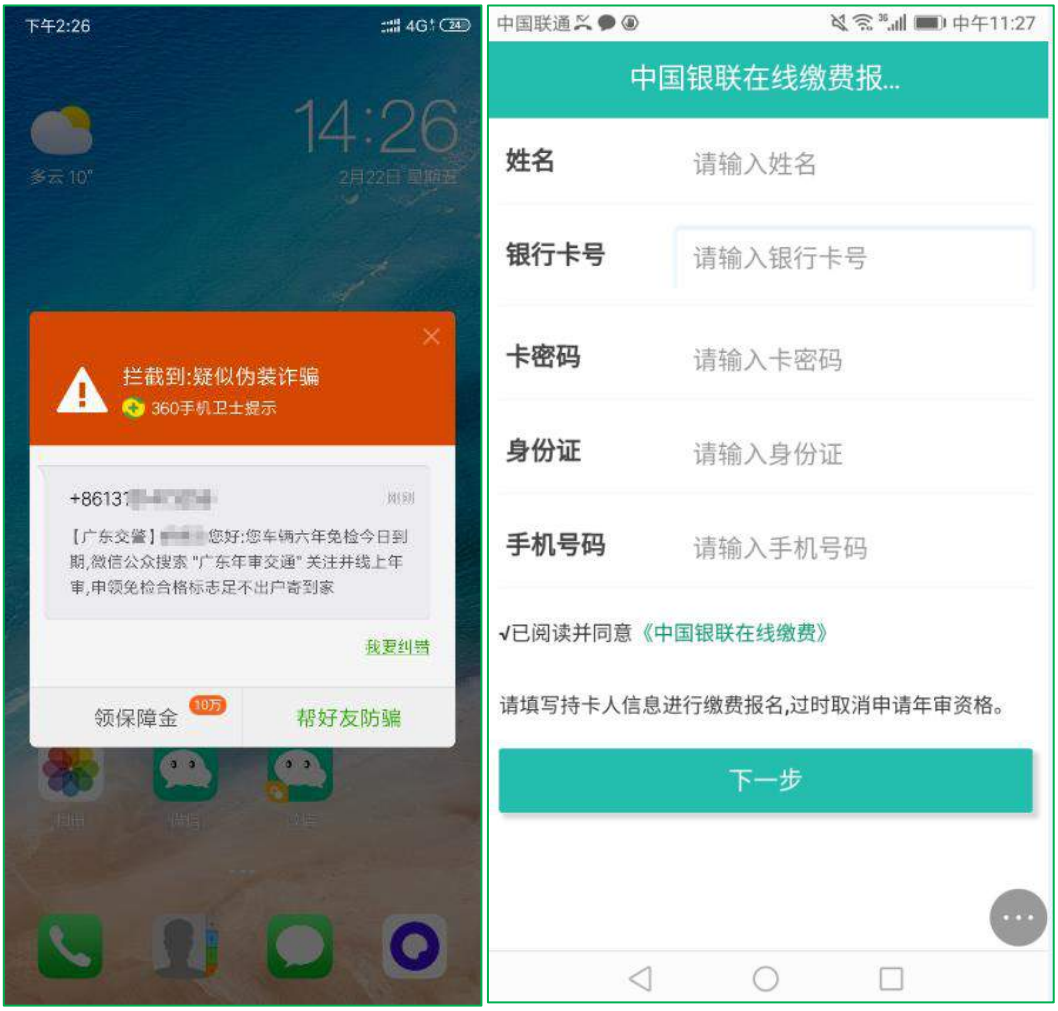
平台宣传发布有限的 EP(平台货币)，每天把平台界面内的“垃圾”拖到对应垃圾桶即可完成任务， 获得 0.37EP(平台货币)，达到 10 个 EP 后，可购买资源转换器，增加 EP 收益。如花费 10EP 购买微型资源转换器，每日可释放 0.37EP，锁仓周期 30 天，可获取 11 个 EP。同时成立自己的战队，邀请他人注册，可获取不同数量的 EP。获得的 EP 可在平台的交易商城进行交易。但投入资金和时间成本，换回来的可能仅仅是服务器中的一串数字。

专家解读

此类平台都是借助热点事件推广虚拟货币。宣传数字货币的数量有限，增加平台货币的价值。但实际上此类平台货币毫无价值可言，用户花了时间，投入了资金，换回来的可能仅仅是服务器中的一串数字。同时，用户在此类平台注册时需实名认证，甚至需上传个人手持身份证照片，存在信息泄露的情况。

二、 “车辆年审”电信诈骗，专骗“有车族”

2019 年 2 月，360 安全大脑监测到有不法分子冒充“广东交警”向车主发送“车辆年审”的诱骗短信，内容涉及关注名为“广东车辆核审”、“广东车辆查审”、“广东车辆极速核验”、“广东车辆急速验审”等迷惑性很强的虚假微信公众号，继而诱导车主点击钓鱼网站，通过后台实时套取银行卡信息并进行盗刷等操作。



专家解读

传播钓鱼链接的公众号自身进行了一些攻防操作，如利用与正规公众号相似的名称，公众号添加了身份认证信息，以此来增强公众号的迷惑性。同时通过微信访问钓鱼网站属于在微信内部操作，第三方安全软件没有相应的权限进行安全提示，绕过了第三方安全软件。所以许多不法分子开始通过短信、QQ 来引导大家关注微信公众号，再通过这些假冒的公众号来给用户发送欺诈信息、钓鱼链接，从而牟取不正当利益。

防骗提示

交警部门向车主发送的年检提示短信，不会附链接，也不会要求填写银行账户信息，同时车辆如果有年检业务需求，请按官方公布的正规渠道预约办理。若收到带有验证码的短信，要仔细阅读内容。因为有些支付渠道，输入验证码就能完成转账。

三、 为“爱豆”应援，流量造假属自愿？

走过 2018 的偶像元年，一茬又一茬的偶像新星们从节目中诞生偶像数量增长，各家粉丝为了打榜、轮博、集资、反黑粉更是忙的不可开交。追星 App 便是为粉丝提供高效追星服务的平台，帮助粉丝在错综复杂的环境中更加迅速的对偶像的一切动向了如指掌。某明星一亿微博转发量幕后推手“星援 APP”被查封，撕开了流量造假产业链的一角。

此类用户流量造假产业的明星应援类 APP，通过月租费或功能收费等方式收取费用，包含很多关注明星动态功能，如时刻提醒所关注明星的社交动态，一键查看明星行程动向。监控微博、贴吧平台上出现所关注明星的黑帖，实时生成举报链接。微博、贴吧、爱奇艺等平台实现一键签到，各种投票类榜单的一键投票打榜。

互联网科技公司或艺人经纪公司开发应援类 APP。粉丝自发或艺人经纪公司给粉丝安排刷榜任务，帮助粉丝组建刷量数据组，应援群。粉丝通过内部圈、微信公众号、应用商店等方式下载应援 APP。粉丝为完成各种任务（明星转发量，热搜），纷纷利用各种应援 APP，轮播，刷榜，帮助“心爱” 的明星刷出大量的虚假流量。为获得与所追明星见面或者获得粉丝周边的产品，利用各种应援 APP，抢占所追明星的热评。为帮助所追明星完成线上或线下的活动，在应援类应用充值开展众筹活动。

专家解读

从粉丝角度看，虽然这是一种粉丝自愿行为，但属于数据造假，违反了《中华人民共和国电信条例》和《北京市微博客发展管理若干规定》中关于实名制注册，不得以虚假身份办理入网手续，实施扰乱网络传播秩序的法律规定，应予以禁止。

从平台角度看：平台作为网络服务提供者，有审核及监督义务。“根据《侵权责任法》第三十六条规定，平台需在未履行网络服务提供者义务的情况下，承担侵权责任。”另外，根据《网络安全法》《电子商务法》相关规定，平台有义务核实应援项目真实性，监管资金去向，以保证网络安全，保障电子商务交易安全。

四、 “传销”又传新手法，“微信挂机”日日赚

随着微信用户群体数量的增加，很多黑灰产业都盯上了微信这块蛋糕。号称“每天挂着微信、加几个群就能赚钱，随便玩每天几块到几十块，稍微努力每天上千没问题，随时提现秒到账，真实可靠不收费”的微信挂机平台就是微信黑灰产里的一个“火爆”项目。

微信挂机平台，使用微信在此平台登录后，系统会向用户的微信群发送产品广告（博彩、色情等），全程只要挂机，无需用户手工发送，事后用户即可获得广告收益。同时邀请他人成为合伙人，也可获得对方的收益提成。此类微信挂机平台，版本多样，存在 APP 版本、网页版本，由于平台搭建难度低，成本低，被封后，往往很快改名重建。

专家解读

此类平台可能会泄露用户隐私。用户登录此类平台，相当于把微信的使用权限交给了此类平台。平台可能利用用户的微信号实施诈骗，甚至盗刷用户的资金。传播的广告存在国家禁止及限制的项目，如博彩平台，虚拟货币。用户成了变相主动传播违法违规内容的人员。

五、 走路就能赚钱的“趣步 APP”

“走路赚钱”在近期一跃成为大众热点话题，随着趣步 APP 的话题性日渐深入，区块链又一次进入大众视野。“立足运动健康领域，以区块链技术为支撑，开发并运营趣步及网络商城，鼓励全民关注自身健康，参与快乐运动的创新型科技公司”这是趣步的宣传口号，看似简单快捷的赚钱方式，实则是一家利用区块链实施诈骗的非法企业。

1. 以区块链的旗号吸引眼球

区块链，通俗来讲是由一组技术实现的大规模、去中心化的经济组织模式。对于区块链，人们通过比特币了解了这项技术，比特币作为最早的虚拟货币，在中国虽得到禁售，但比特币的价值也获得了人们的认可。无形中，一些运用区块链技术的企业得到了更多人的关注。

而趣步在运营期间声称有国家颁发的区块链牌照，这使更多用户相信平台的真实性，并放心大胆的进行投资。实际上，国家并没有任何部门颁发虚拟货币运营牌照，平台属于虚假宣传，利用国家认可的噱头获得更多曝光度。

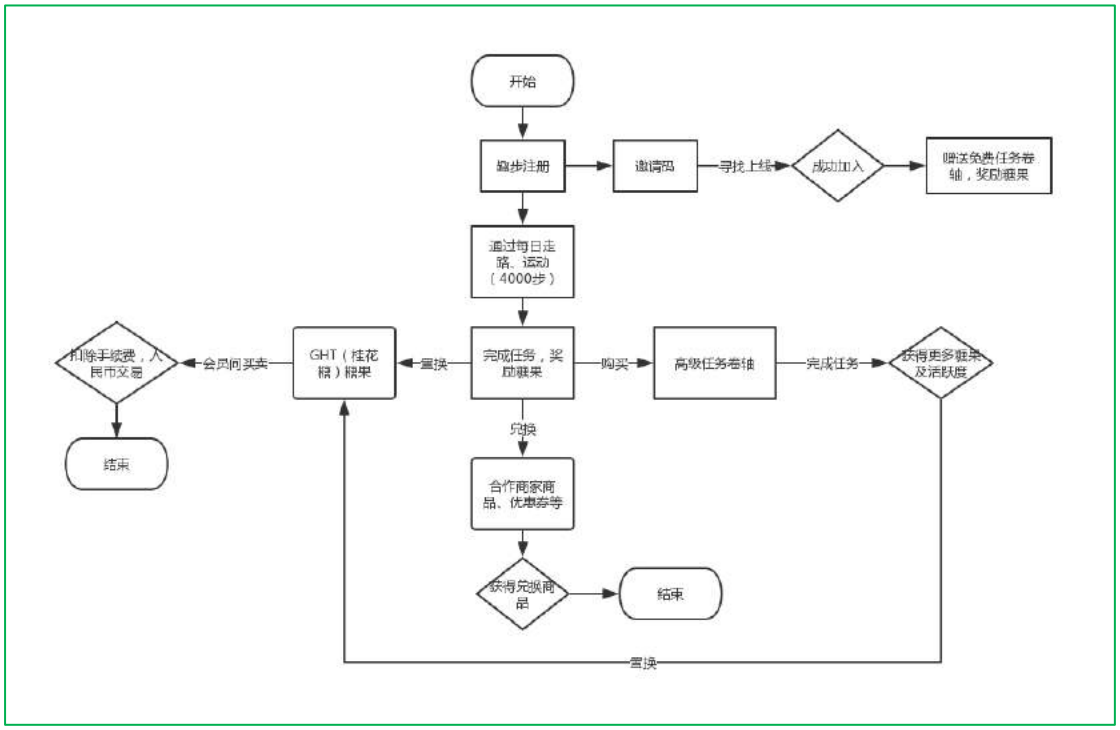
“用趣步每天走路 4000 步”=“月入十几万元”+“饭店、旅游、健身、宾馆甚至买房服务”“零投入，走路就赚钱，这样的好事是真的吗？”“趣步每天 4000 步，手机变成摇钱树！”。这些是趣步运营期间，网络上流传的宣传话语，走路赚钱确实是一种新鲜方式，再加上趣步洗脑式的宣传，更多的人愿意接受这一形式去进行尝试。

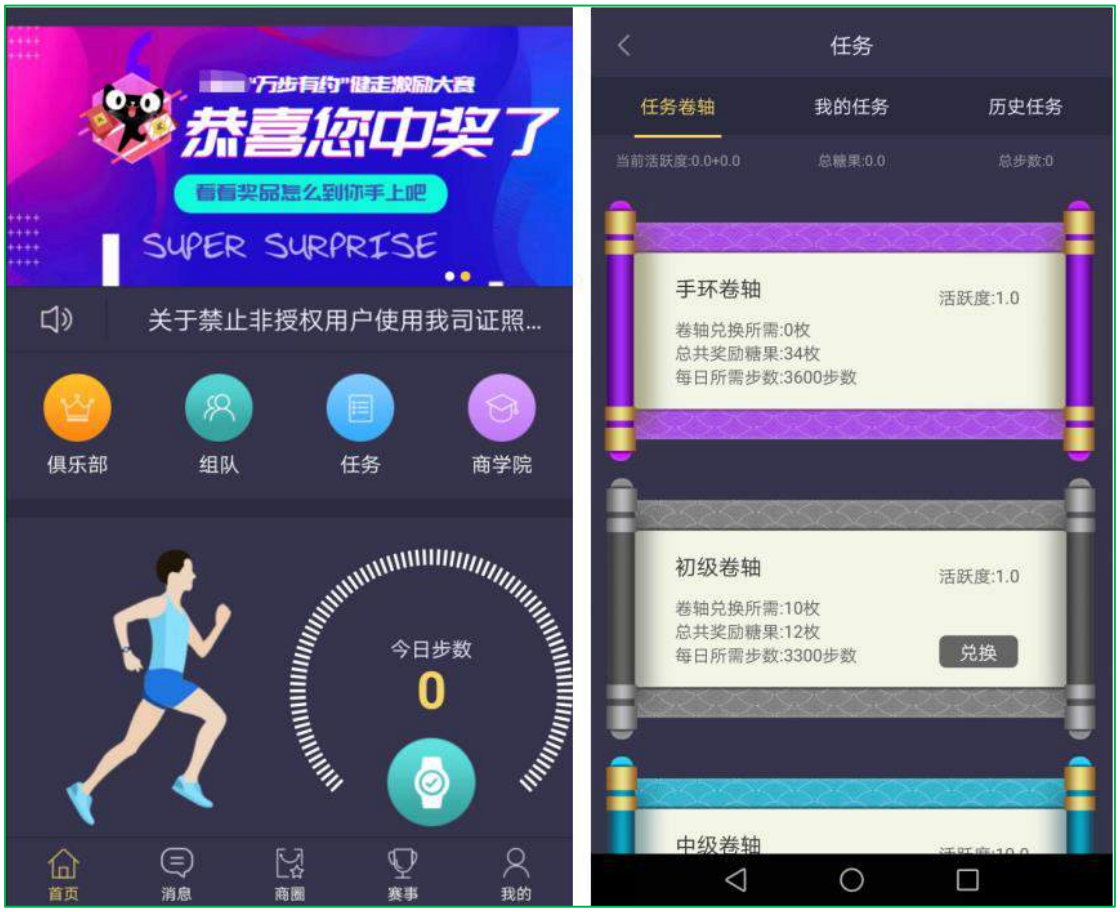
2. 趣步“传销式”的运营模式

在趣步平台流通的是一种叫做“糖果”的虚拟货币，平台声称利用“区块链”技术以人体运动计步来计算“糖果”的产量，参与者的每一步都能够产出“糖果”。号称不出售糖果，只能通过运动的方式获取，并且有数量上限，总量为 10 亿枚、永不增发，糖果不具备货币功能，只是为了奖励爱运动的人们，可以利用糖果在商城中兑换商品。但同时，趣步 APP 中又支持糖果兑换成 GHT（桂花糖），这种糖果支持用户间交易，而价格每日间有浮动。交易就需要扣除手续费，由平台收取。这种否认糖果价值又支持糖果交易的“双标”举动，可见其中蕴含猫腻。

在趣步中，通过每日任务可获得少数糖果。如果想要积攒更多的糖果，则需要购买任务卷轴，购买卷轴的同时，需要花费现有糖果。但后续完成卷轴任务后，每日可获得更多上限的糖果，每日步数要求也随之增长，并可获得活跃度。玩法简称，想获得更多的糖果，就需要完成更高级的任务。利用这种手法，带动更多的用户进行活动。

那么问题来了，要获得更多的糖果，需要用一定数量的糖果换卷轴，可换卷轴的钱从哪来？如果想依靠每日系统赠送的糖果，确实需要很长一段时间，于是，拉新成为一种主要方式。通过趣步内推荐码拉拢身边的人参与，即自己的下线。如果通过“直推”形成团队，成为星级达人，则给予更高的奖励。可获得全球手续费分红。前期想进入趣步，同样需要寻找上线，才可加入，高息返佣、发展下线，属于明显的“传销”手段。





3. 趣步“糖果”交易运用形式

在趣步注册期间，要求用户以个人真实信息绑定，并使用与支付宝类似的刷脸。此要求成为硬性要求，向用户表达了，趣步是一款正规化、流程化的可持续发展平台。在交易时，用户可在平台通过低价买入桂花糖，寻找机会高价卖出的方式达到获得收益的目的。但收益是需要建立在糖果有价值的基础上，通过以上分析可得知，如果用户花费资金“囤”糖果，只会造成资产亏空。这种形式，糖果为一种虚拟货币的现象就更加明显。官方承诺的 10 亿固定数量并没有在此得到体现，更像是要多少则有多少，趣步作为“资金盘”的特性越见明显。

由于趣步不承认糖果含有货币价值，建立了交易平台，但并不支持平台交易。用户间交易需要通过私下转账方式进行，交易完成再由糖果的卖方支付给买方糖果。再回头看，趣步用户间存在多个交流群，每个群都有领导者、运营者，并有人在群里喊话卖糖果。猜测这些卖方都是诈骗平台的非法人员，通过这种交易方式，用户将得不到任何担保，直接导致损失。

专家解读

趣步所依靠的区块链技术实际是一个噱头，并不真实存在。而“糖果”，是不法分子所运用的非法产物，可以人为地操控其数量、价格等信息。我国目前还没有任何机构承认虚拟币的合法性，已属于违法。分析其运营模式，是常见“传销”模式，通过高返佣、拉下线实现新用户的增长。同时建立多个非法组织群，群内不法分子对群内人员进行洗脑，诱导用户拉新，从中获利。

六、 “预测 2020 年你会遇到的几道坎”我猜你想知道

输入姓名、手机号、生日等个人信息后，随机系统会给出测试结果。这些测试类的小游戏，凭借简单操作和自身趣味性，在社交网络中火热传播。然而，很多人都没有意识到，在参与游戏测算的过程中，自己的个人信息可能已被系统完整的收集。

1. 商家常用的营销手段

一些个人/企业注册微信公众号，借助热点事件进行引流，同时转换为广告收益。通常，此类平台大多不具备测算功能，这是单纯的 H5 活动页面，测试结果随机生成。参与用户更多被活动趣味性吸引。

2. 虚假的付费测运势平台

虚假的测运势平台会通过微信公众号传播，用户扫码后打开形式可能有两种：

1) 微信小程序

测算过程中，用户会被要求授权微信昵称、头像、地区、姓名等个人信息。

2) “阅读原文”

部分扫码后跳转到微信文章，点击“阅读原文”后，会跳转到“鼠年运势预测”的站外链接，用户想了解测算结果，需要付款后查询。部分公众号备案为个人，并无认证标识。

专家解读

这些平台一般都需要微信登录认证，获取微信昵称、头像、地区、性别等权限，在平台参与活动的过程中又填写了个人信息，如果被不法分子掌握，很可能实施定向诈骗。测算网站表面上是免费，实际上，如果想查看预测结果时需要付费。此类免费测算网站无备案信息，缴费后很可能遭遇欺诈。从活动页面返回时，会多次跳转到色情小说、金融理财等界面。色情小说到关键情节，用户同样需要付费阅读；金融理财广告，目的就是骗取用户贷款或购买虚假理财产品。