2019 年第一季度

中国手机安全状况报告

360 安全大脑

360互联网安全中心

2019 年 4 月 30 日

摘　要

恶意程序：

- 2019年第一季度，360互联网安全中心共截获安卓平台新增恶意程序样本约56.6万个，平均每天截获新增样本约0.6万个；360手机卫士累计为全国手机用户拦截恶意程序攻击约8480.8万次，平均每天拦截手机恶意程序攻击约95.2万次。
- 2019年第一季度安卓平台新增恶意程序类型主要为隐私窃取，占比高达81.0%；其次为资费消耗（15.6%）、流氓行为（2.1%）、恶意扣费（0.7%）、欺诈软件（0.4%）等。
- 从省级分布来看，2019 年第一季度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9.6%；其次为山东（8.1%）、河南（7.3%）、江苏（6.2%）、河北（5.7%）等。
- 从城市分布来看，2019 年第一季度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2.0%；其次为重庆（1.7%）、广州（1.7%）、上海（1.3%）、成都（1.3%）等。

钓鱼网站：

- 2019年第一季度，360互联网安全中心在PC端与移动端共为全国用户拦截钓鱼网站攻击约73.6亿次，其中，PC端拦截量约为66.6亿次，占总拦截量的90.5%，平均每日拦截约0.7亿次；移动端拦截量约7.0亿次，占总拦截量的9.5%。
- 2019年第一季度移动端拦截钓鱼网站类型中，境外彩票类比重最高，为72.2%；其他占比较高的类型包括网址被黑（25.2%）、虚假购物（0.9%）、虚假招聘（0.3%）、模仿登陆（0.3%）、金融证券（0.3%）等。
- 从省级分布来看，2019 年第一季度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21.6%；其次为广西（9.4%）、福建（7.2%）、山东（5.8%）、湖南（4.8%）等。
- 从城市分布来看，2019 年第一季度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 3.9%；其次为北京（3.1%）、天津（2.6%）、上海（2.3%）、重庆（2.1%）等。
- 2019年第一季度，360互联网安全中心共截获各类新增钓鱼网站502.1万个，平均每天新增5.6万个。观察钓鱼网站新增类型，境外彩票类占比最高，属于新增钓鱼网站中的重点打击类型，近几年由于打击力度的加大，这一类钓鱼网站数量大幅降低。
- 从新增钓鱼网站的服务器地域分布来看，86.1%的钓鱼网站服务器位于国外，13.9%位于国内。其中，国内服务器位于香港的占比为86.4%，居于首位，其次为广东（3.6%）、北京（1.9%）、河南（1.6%）、台湾（1.1%）等。

骚扰电话：

- 2019年第一季度，用户通过360手机卫士标记各类骚扰号码约1649.1万个，平均每天标记约 18.5 万个。从拦截量上看，360 手机卫士共为全国用户识别和拦截各类骚扰电话约52.3亿次，平均每天识别和拦截骚扰电话约0.6亿次。
- 综合360互联网安全中心2019年第一季度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59.3%的比例位居首位；其次为广告推销（13.3%）、骚扰电话（8.4%）、疑似欺诈（7.1%）、房产中介（5.0%）、保险理财（4.4%）、招聘猎头（2.5%）。

- ✧ 从骚扰电话拦截类型来看，广告推销以 52.7%的比例位居首位，其次为骚扰电话（23.9%）、疑似欺诈（12.3%）、房产中介（6.6%）、响一声（3.1%）、保险理财（1.2%）、招聘猎头（0.3%）。

- ✧ 从用户标记的骚扰电话归属运营商来看，被标记的中国移动的手机号码最多，占比高达 41.6%；其次为固定电话、中国电信、中国联通与虚拟运营商（170 号段）的电话号码，分别占比 16.7%、16.6%、14.5%与 10.5%，400/800 号码最少，占比 0.1%。

- ✧ 从骚扰电话号码拦截个数看，同样为中国移动的手机号最多，占比达 32.8%，其次为固定电话、中国电信与中国联通，分别占比 27.0%、20.4%与 19.8%。

- ✧ 2019 年第一季度，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个数最多，占全国骚扰电话标记个数的 10.8%，其次是山东（7.1%）、河南（6.1%）、江苏（5.9%）、四川（5.5%）等。

- ✧ 从城市分布来看，北京市用户标记骚扰电话个数最多，占全国骚扰电话标记个数的 3.7%，其次是广州（2.6%）、重庆（2.3%）、上海（2.3%）、成都（2.2%）等。

- ✧ 2019 年第一季度，从各地骚扰电话的拦截量上分析，广东省用户接到的骚扰电话最多，占全国骚扰电话拦截量的 11.9%，其次是浙江（7.7%）、江苏（7.1%）、山东（6.9%）、北京（6.8%）等。

- ✧ 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 6.8%，其次是广州（6.4%）、杭州（4.2%）、南京（3.7%）、济南（3.5%）等。

垃圾短信：

- ✧ 2019 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 12.2 亿条，较 2018 年第四季度（19.1 亿条）环比下降了 36.1%，平均每天拦截垃圾短信约 1367.4 万条。

- ✧ 2019 年第一季度垃圾短信的类型分布中，广告短信最多，占比为 98.0%，诈骗短信占比 1.7%，违法短信占比 0.3%。

- ✧ 2019 年第一季度，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 15.8%，其次是河南（7.4%）、浙江（6.5%）、江苏（6.5%）、山东（6.3%）等。

- ✧ 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 7.6%，其次是北京（5.4%）、深圳（4.0%）、南京（3.3%）、上海（3.2%）等。

网络诈骗：

- ✧ 2019 年第一季度 360 手机先赔共接到手机诈骗举报 1391 起，其中诈骗申请为 571 起，涉案总金额高达 306.1 万元，人均损失 5360 元。

- ✧ 在所有诈骗申请中，赌博博彩占比最高，为 20.3%；其次是金融理财（19.3%）、虚假兼职（11.6%）、身份冒充（8.8%）和网游交易（7.0%）。

- ✧ 从涉案总金额来看，赌博博彩类诈骗总金额最高，达 131.8 万元，占比 43.1%；其次是金融理财诈骗，涉案总金额为 74.8 万元，占比 24.5%；身份冒充诈骗排第三，涉案总金额为 33.2 万元，占比 10.9%。

- ✧ 从人均损失来看，赌博博彩诈骗人均损失最高，为 11359 元；其次是信用卡诈骗为 9355 元，金融理财诈骗为 6804 元。
- ✧ 从举报用户的性别差异来看，男性受害者占 75.9%，女性占 24.1%，男性受害者占比高于女性。从人均损失来看，男性为 5532 元，女性为 4880 元，男性受害者人均损失同样高于女性。
- ✧ 从被骗网民的年龄段分析，90 后的手机诈骗受害者占所有受害者总数的 36.4%，位居第一；其次是 00 后占比 27.1%，80 后占比 23.8%，70 后占比 7.7%，60 后占比 3.5%，其他年龄段占 1.4%。
- ✧ 而从具体年龄上来看，16 岁至 20 岁的人群依然是手机诈骗受害者最为集中的年龄段，占所有手机诈骗受害者的 21.7%。
- ✧ 2019 年第一季度，从用户举报情况来看，广东（13.3%）、广西（7.0%）、河南（5.6%）、湖南（5.6%）、河北（5.3%）这 5 个省级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 36.8%。
- ✧ 从各城市手机诈骗的举报情况来看，广州（2.3%）、东莞（2.1%）、重庆（1.9%）、成都（1.8%）、武汉（1.6%）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 9.6%。

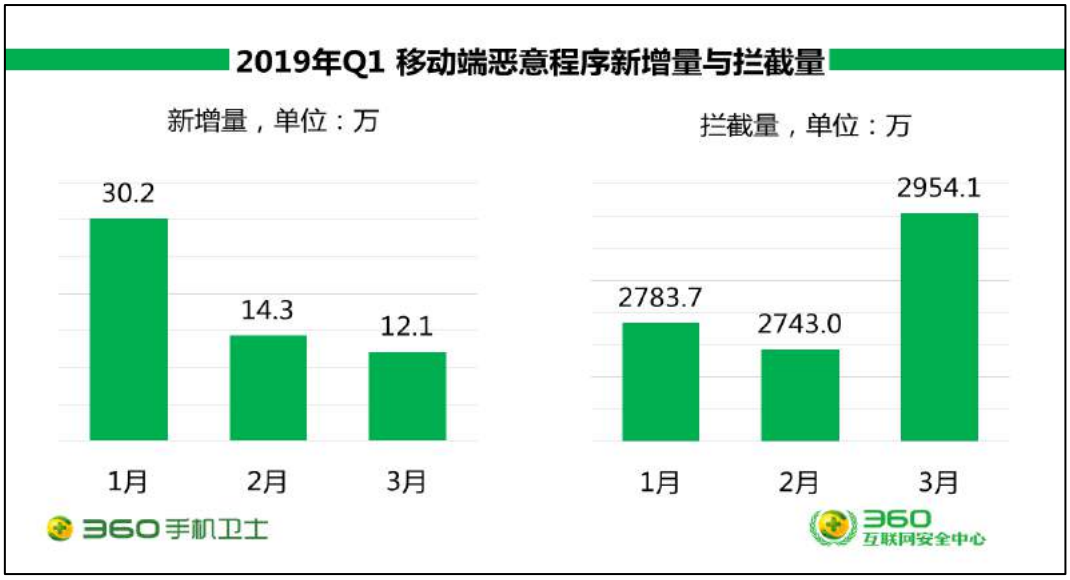
关键词：恶意程序、钓鱼网站、骚扰电话、垃圾短信、网络诈骗

目录

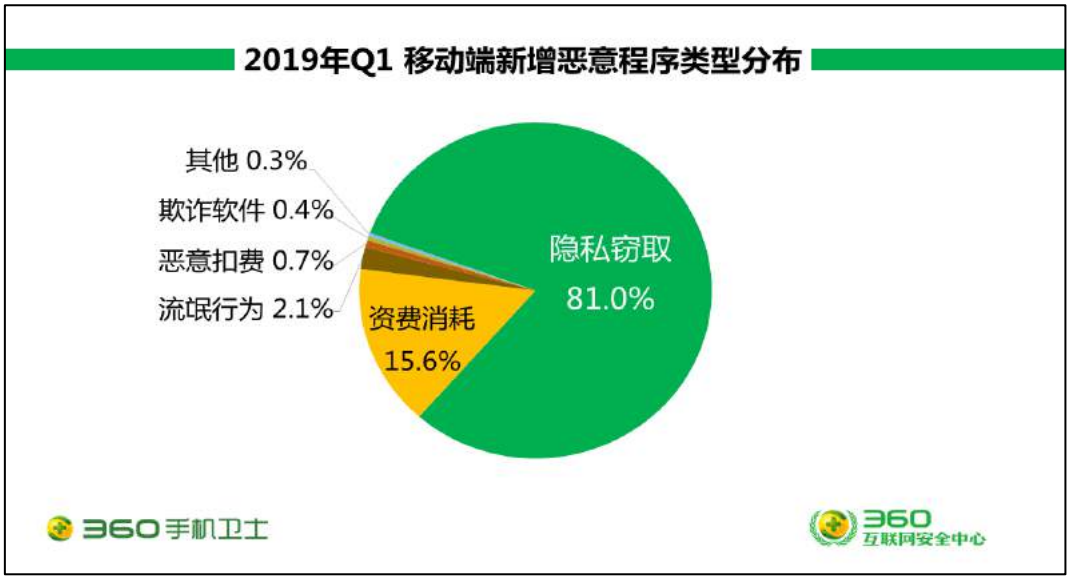
第一章　恶意程序

一、　恶意程序新增样本量与类型分布

2019年第一季度，360互联网安全中心共截获安卓平台新增恶意程序样本约56.6万个，比2018年第一季度（141.5万个）减少了84.9万个，平均每天截获新增手机恶意程序样本约0.6万个。360手机卫士累计为全国手机用户拦截恶意程序攻击约8480.8万次，平均每天拦截手机恶意程序攻击约95.2万次。下图给出了2019年第一季度移动端恶意程序新增量与拦截量统计：

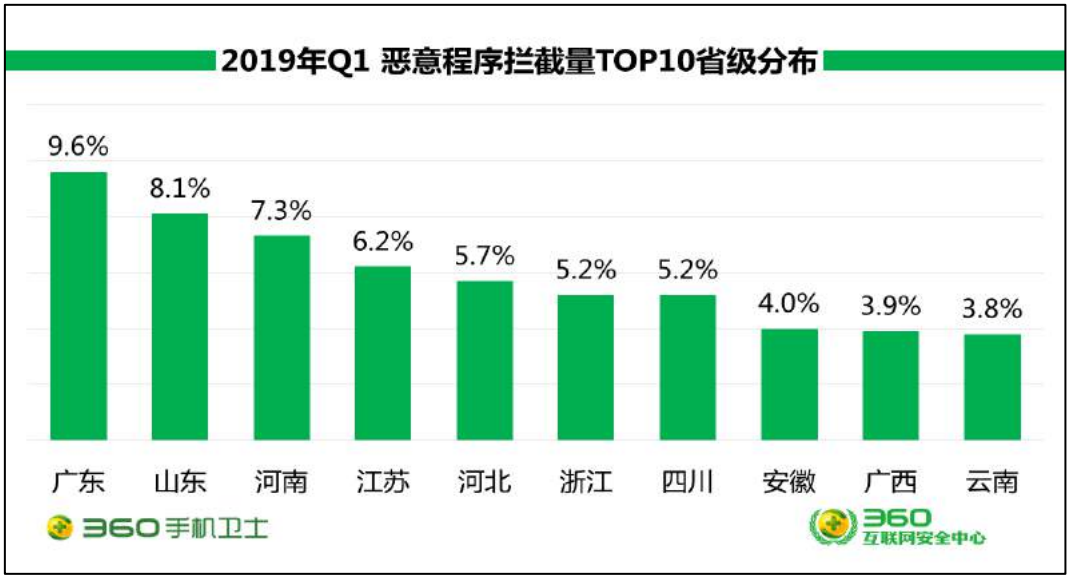


2019年第一季度安卓平台新增恶意程序类型主要为隐私窃取，占比高达81.0%；其次为资费消耗（15.6%）、流氓行为（2.1%）、恶意扣费（0.7%）、欺诈软件（0.4%）等。具体分布如下图所示：

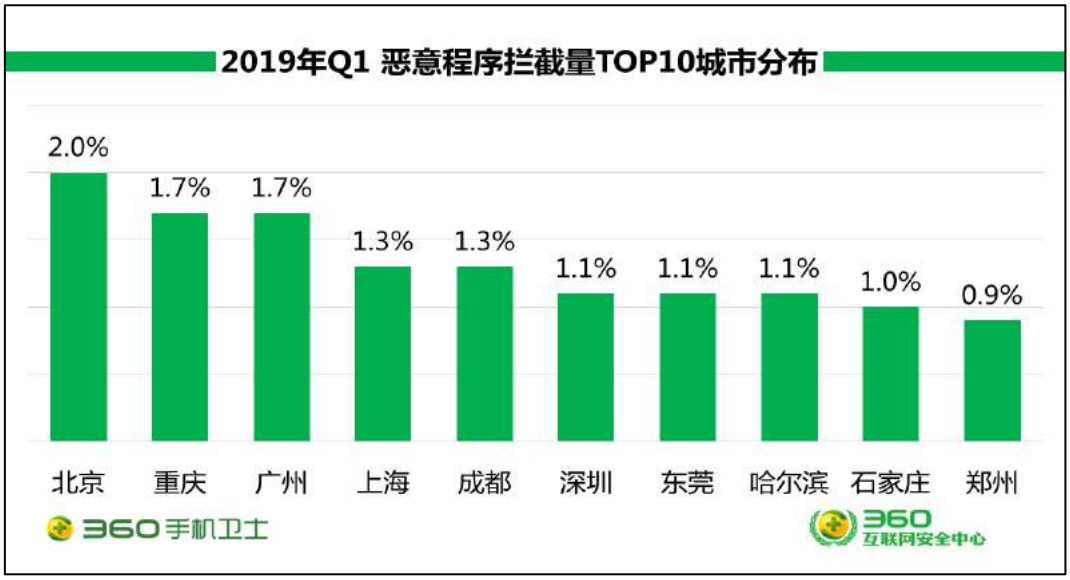


二、 恶意程序拦截量地域分布

2019 年第一季度从省级分布来看，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 9.6%；其次为山东（8.1%）、河南（7.3%）、江苏（6.2%）、河北（5.7%），此外浙江、四川、安徽、广西、云南的恶意程序拦截量也排在前列。



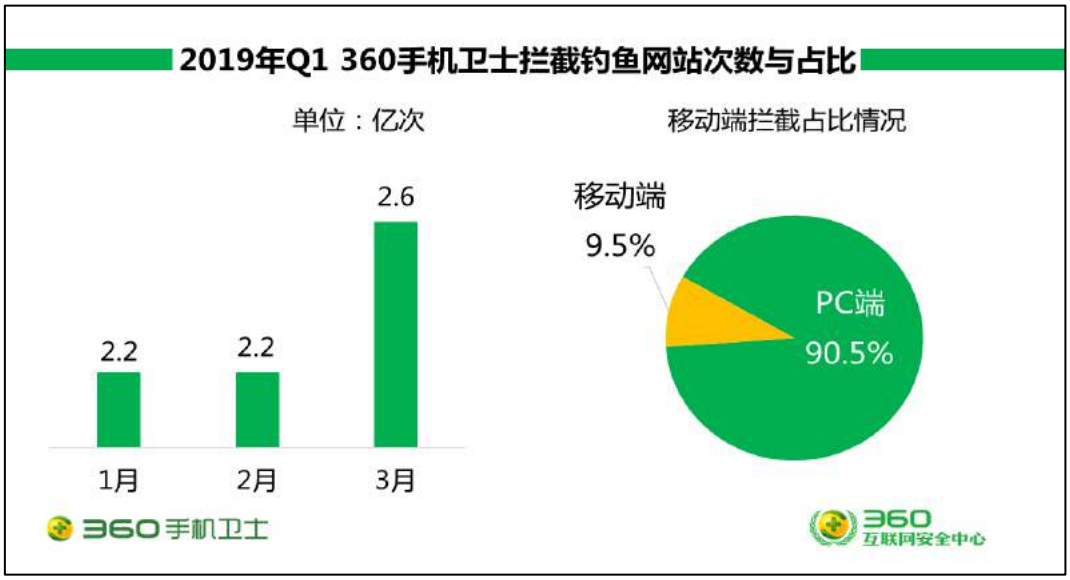
从城市分布来看，遭受手机恶意程序攻击最多的城市为北京市，占全国拦截量的 2.0%；其次为重庆（1.7%）、广州（1.7%）、上海（1.3%）、成都（1.3%），此外深圳、东莞、哈尔滨、石家庄、郑州的恶意程序拦截量也排在前列。


2019年Q1 恶意程序拦截量TOP10城市分布
2.0%
1.7%
1.7%
1.3%
1.3%
1.1%
1.1%
1.1%
1.0%
0.9%
北京
重庆
广州
上海
成都
深圳
东莞
哈尔滨
石家庄
郑州
360手机卫士
360互联网安全中心

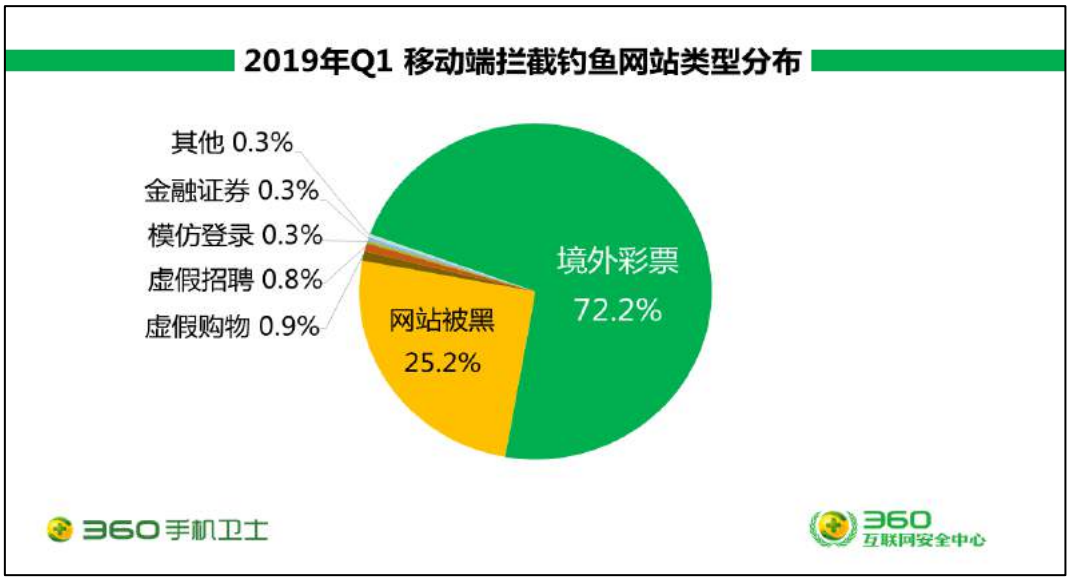
第二章 钓鱼网站

一、 移动端钓鱼网站拦截量及类型

2019 年第一季度，360 互联网安全中心在 PC 端与移动端共为全国用户拦截钓鱼网站攻击约 73.6 亿次，其中，PC 端拦截量约为 66.6 亿次，占总拦截量的 90.5%，平均每日拦截约 0.7 亿次；移动端拦截量约 7.0 亿次，占总拦截量的 9.5%。移动端钓鱼网站拦截次数及占比具体见下图：

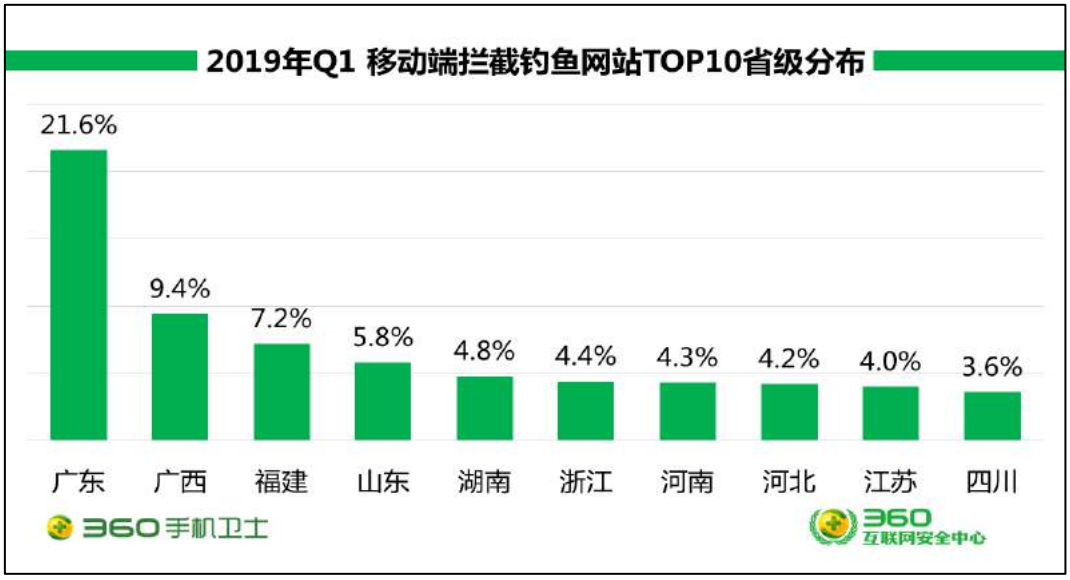


移动端拦截钓鱼网站类型中，境外彩票类比重最高，为 72.2%；其他占比较高的类型包括网址被黑（25.2%）、虚假购物（0.9%）、虚假招聘（0.3%）、模仿登陆（0.3%）、金融证券（0.3%）等。具体分布如下图所示：

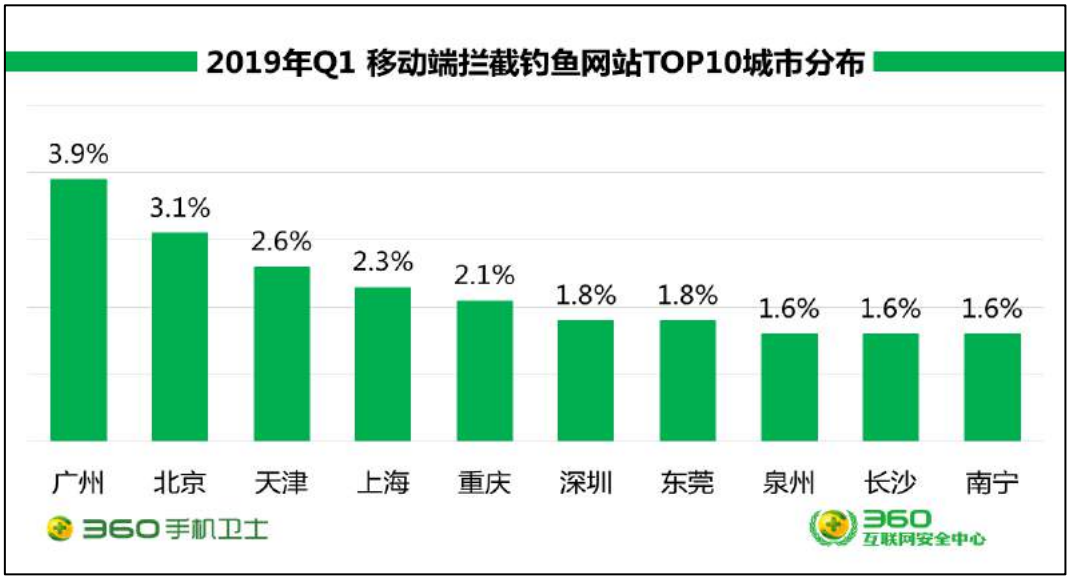


二、 移动端钓鱼网站拦截量地域分布

2019 年第一季度从省级分布来看，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 21.6%；其次为广西（9.4%）、福建（7.2%）、山东（5.8%）、湖南（4.8%），此外浙江、河南、河北、江苏、四川的钓鱼网站拦截量也排在前列。

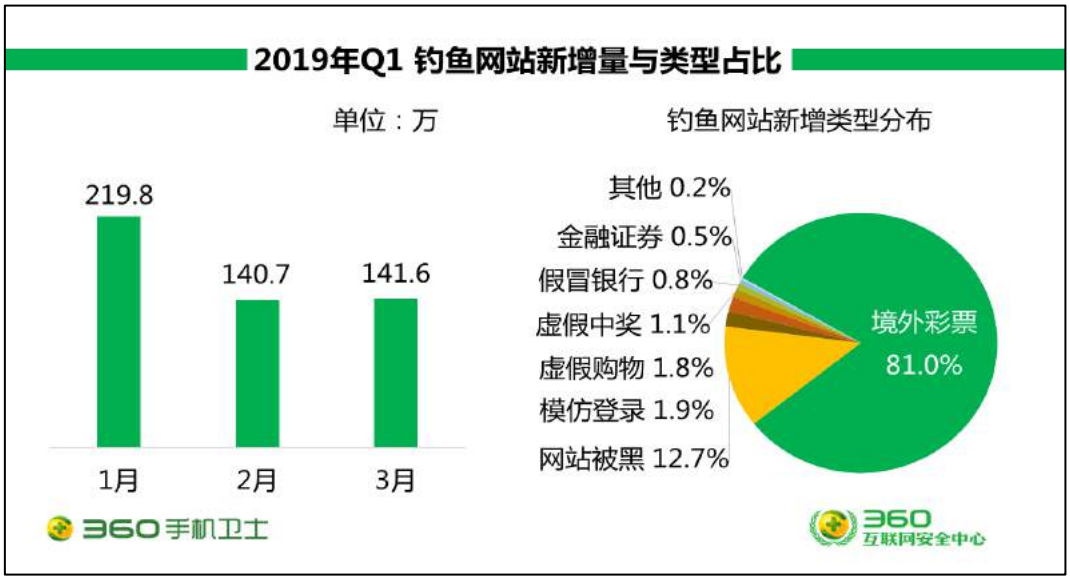


从城市分布来看，移动端拦截钓鱼网站最多的城市为广州市，占全国拦截量的 3.9%；其次为北京（3.1%）、天津（2.6%）、上海（2.3%）、重庆（2.1%），此外深圳、东莞、泉州、长沙、南宁的钓鱼网站拦截量也排在前列。

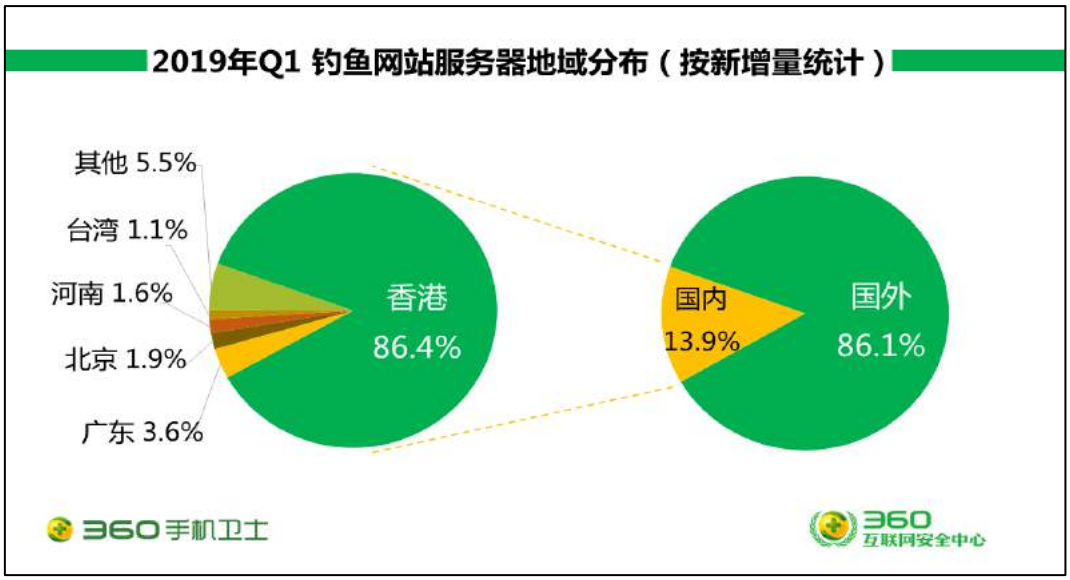


三、 钓鱼网站新增量与服务器地域分布

2019 年第一季度，360 互联网安全中心共截获各类新增钓鱼网站 502.1 万个，同比 2018 年第一季度（1331.9 万个）下降了 62.3%，平均每天新增 5.6 万个。观察钓鱼网站新增类型，境外彩票类占比最高，属于新增钓鱼网站中的重点打击类型，近几年由于打击力度的加大，这一类钓鱼网站数量大幅降低。



从新增钓鱼网站的服务器地域分布来看，86.1%的钓鱼网站服务器位于国外，13.9%位于国内。其中，国内服务器位于香港的占比为 86.4%，居于首位，其次为广东（3.6%）、北京（1.9%）、河南（1.6%）、台湾（1.1%）等。

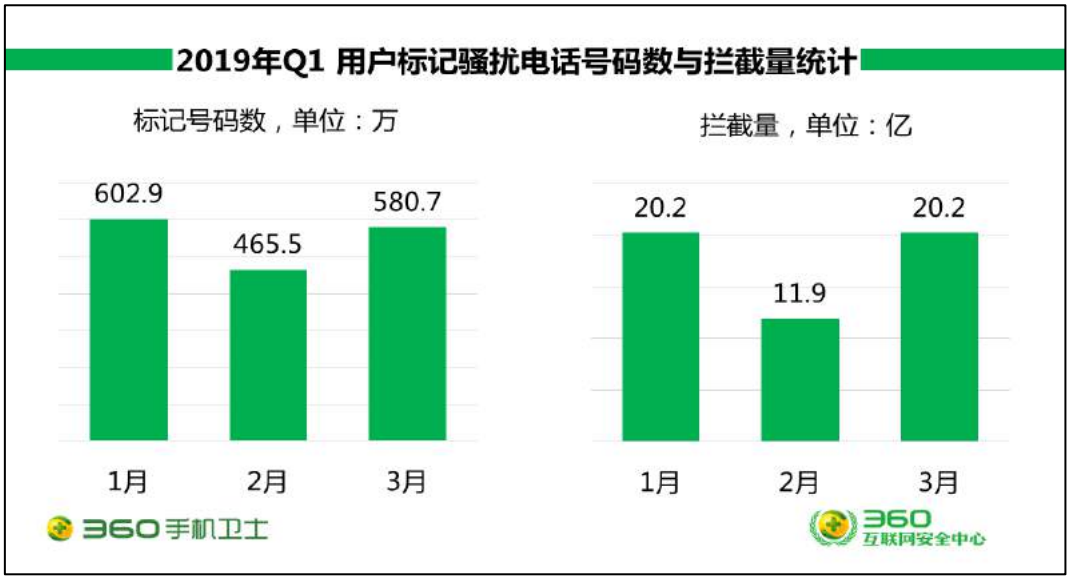


第三章 骚扰电话

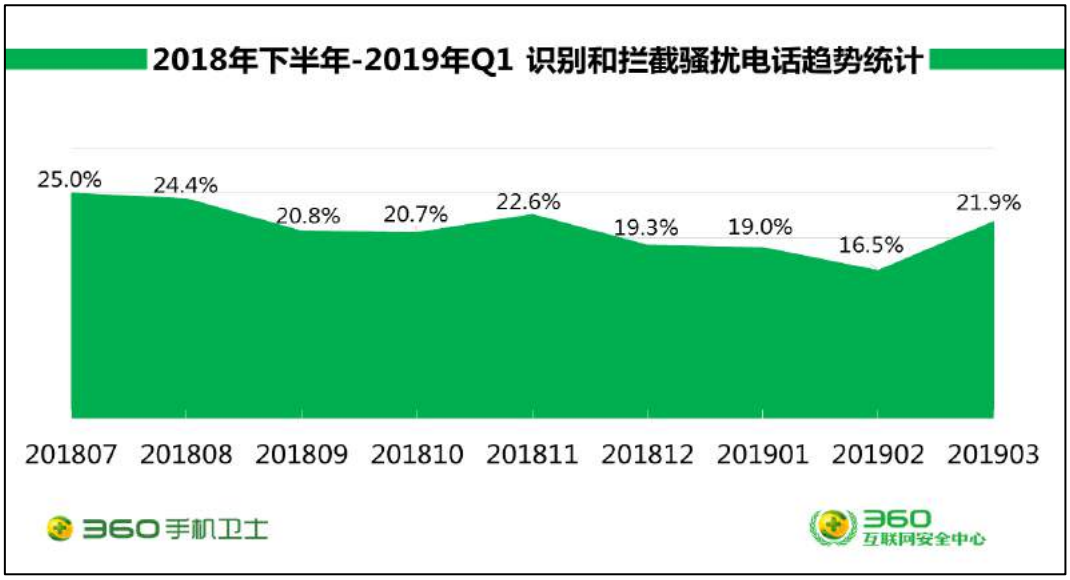
一、骚扰电话标记数与拦截量

2019 年第一季度，用户通过 360 手机卫士标记各类骚扰号码（包括 360 手机卫士自动检出的响一声电话）约 1649.1 万个，平均每天标记约 18.5 万个。从标记总量上看，相比 2018 年第一季度（1505.4 万个）上升了 8.8%。从拦截量上看，360 手机卫士共为全国用户识别和拦截各类骚扰电话约 52.3 亿次，平均每天识别和拦截骚扰电话约 0.6 亿次。

2019 年第一季度用户标记骚扰电话号码数与拦截量统计如下。与以往趋势相同，由于 2 月份春节期间从事广告推销、电话诈骗的人员回家过年，骚扰号码数量明显下降，在 3 月份迅速回升。

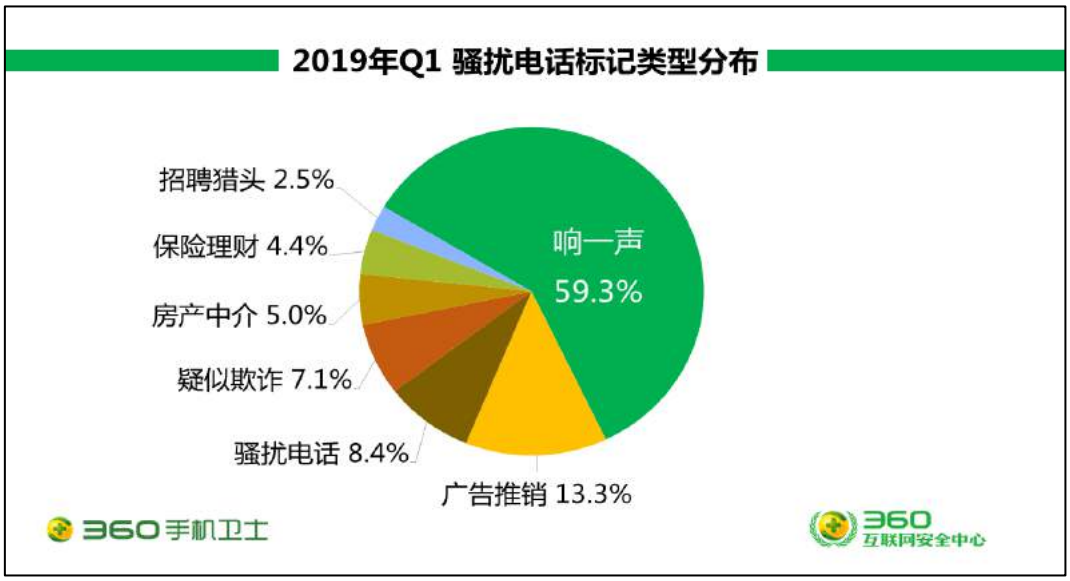


从下图 2018 年下半年至 2019 年第一季度 360 手机卫士识别和拦截骚扰电话趋势可见，临近年底骚扰电话拦截量呈逐渐降低趋势，2019 年 2 月份期间正值春节假期，骚扰电话拦截量最低。通过往年趋势可知，在春节期间，从事拨打骚扰电话的人员减少，从而导致骚扰电话的呼入量降低。2019 年 3 月份起，骚扰电话拦截量回升。

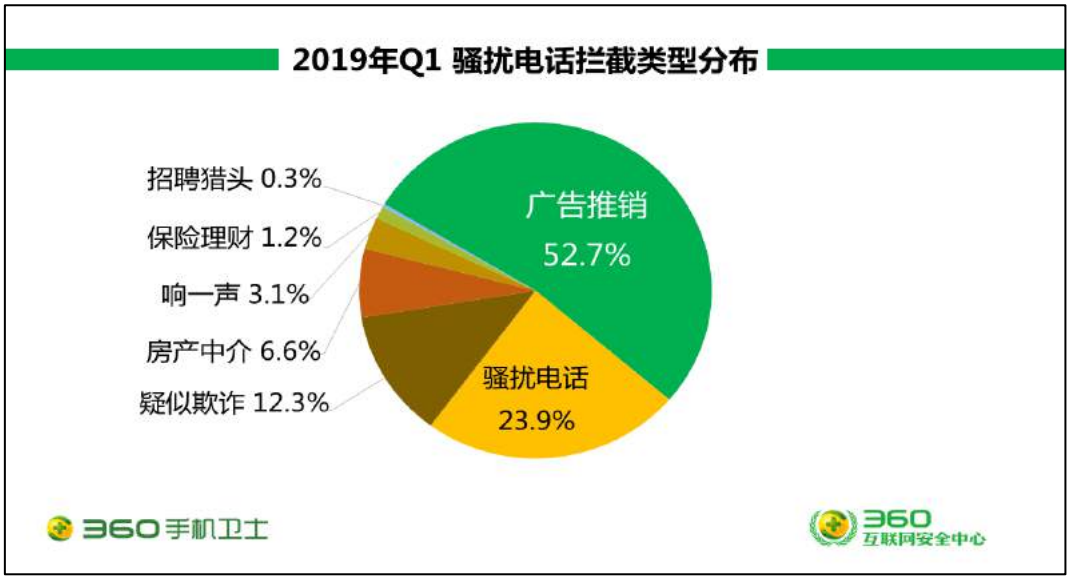


二、骚扰电话类型分布

综合 360 互联网安全中心 2019 年第一季度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 59.3%的比例位居首位，其次为广告推销（13.3%）、骚扰电话（8.4%）、疑似欺诈（7.1%）、房产中介（5.0%）、保险理财（4.4%）、招聘猎头（2.5%）。具体分布如下图所示：

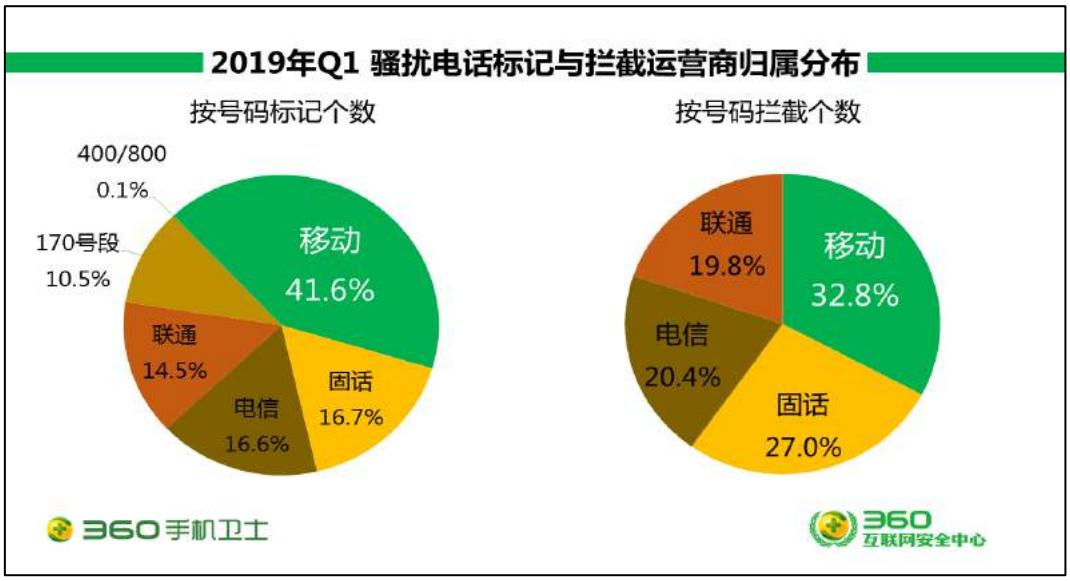


从骚扰电话拦截类型来看，广告推销以 52.7%的比例位居首位，其次为骚扰电话（23.9%）、疑似欺诈（12.3%）、房产中介（6.6%）、响一声（3.1%）、保险理财（1.2%）、招聘猎头（0.3%）。具体分布如下图所示：



三、骚扰电话运营商归属分布

下图对手机号、固定电话、虚拟运营商（170 号段）、以及 400/800 电话分别给出了不同类型号码用户标记的骚扰电话号码个数占比以及骚扰电话号码拦截个数占比：



从用户标记的骚扰电话号码个数看，被标记的中国移动的手机号码最多，占比高达 41.6%；其次为固定电话、中国电信、中国联通与虚拟运营商（170 号段）的电话号码，分别占比 16.7%、16.6%、14.5%与 10.5%，400/800 号码最少，占比 0.1%。

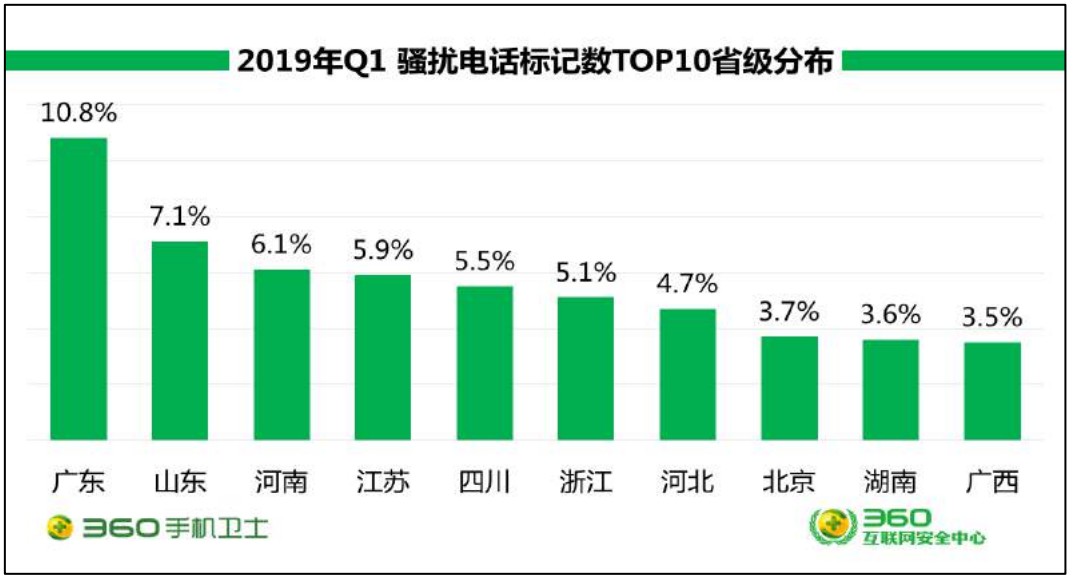
从骚扰电话号码拦截个数看，同样为中国移动的手机号最多，占比达 32.8%；其次为固定电话、中国电信与中国联通，分别占比 27.0%、20.4%与 19.8%。

总体来看，骚扰电话中，手机号码为主要使用号源，用户标记个数与拦截号码个数都是

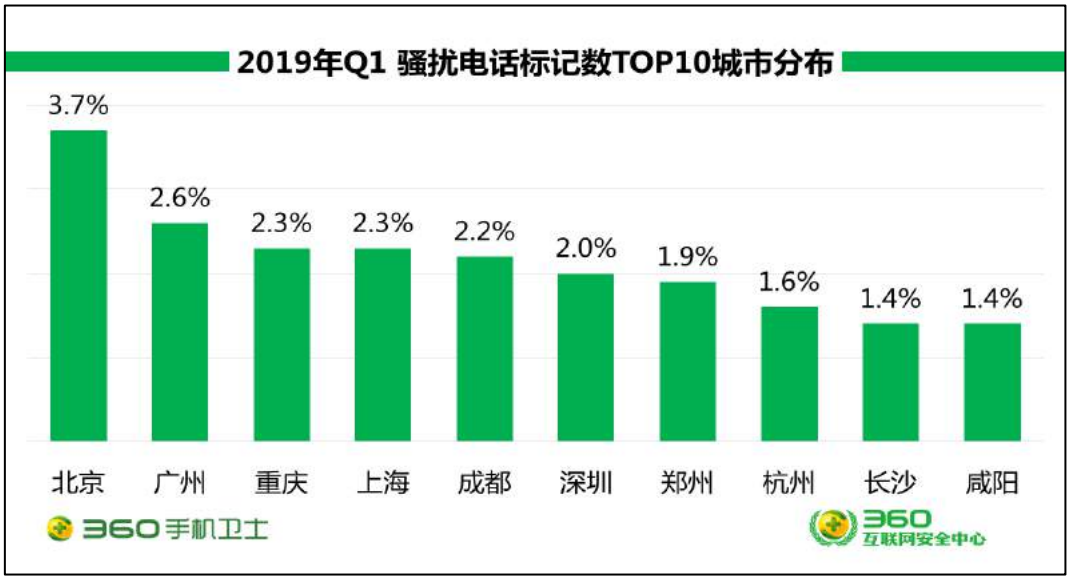
最多的，中国移动的手机号码骚扰情况较为突出。

四、 骚扰电话归属地分布

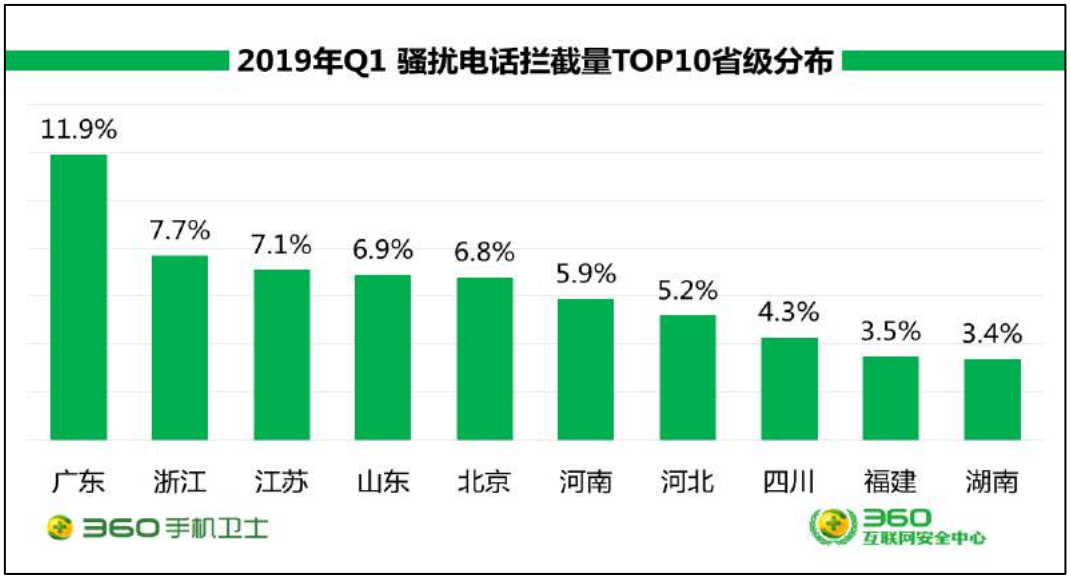
2019 年第一季度，从各地骚扰电话标记号码个数上分析，广东省用户标记骚扰电话个数最多，占全国骚扰电话标记个数的 10.8%，其次是山东（7.1%）、河南（6.1%）、江苏（5.9%）、四川（5.5%），此外浙江、河北、北京、湖南、广西的骚扰电话标记个数也排在前列。



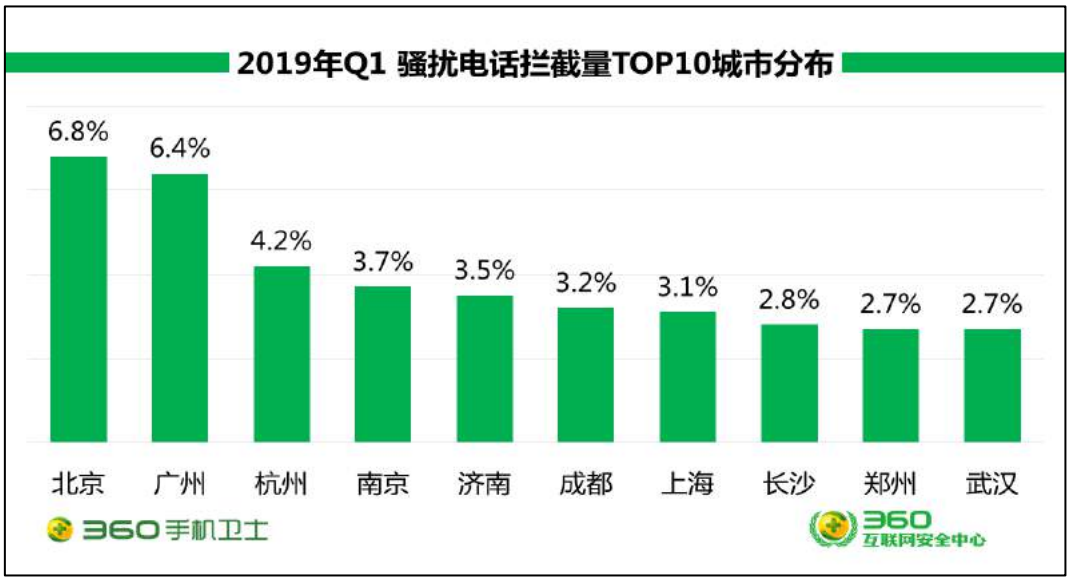
从城市分布来看，北京市用户标记骚扰电话个数最多，占全国骚扰电话标记个数的 3.7%，其次是广州（2.6%）、重庆（2.3%）、上海（2.3%）、成都（2.2%），此外深圳、郑州、杭州、长沙、咸阳的骚扰电话标记个数也排在前列。



2019 年第一季度，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 11.9%，其次是浙江（7.7%）、江苏（7.1%）、山东（6.9%）、北京（6.8%），此外河南、河北、四川、福建、湖南的骚扰电话拦截量也排在前列。



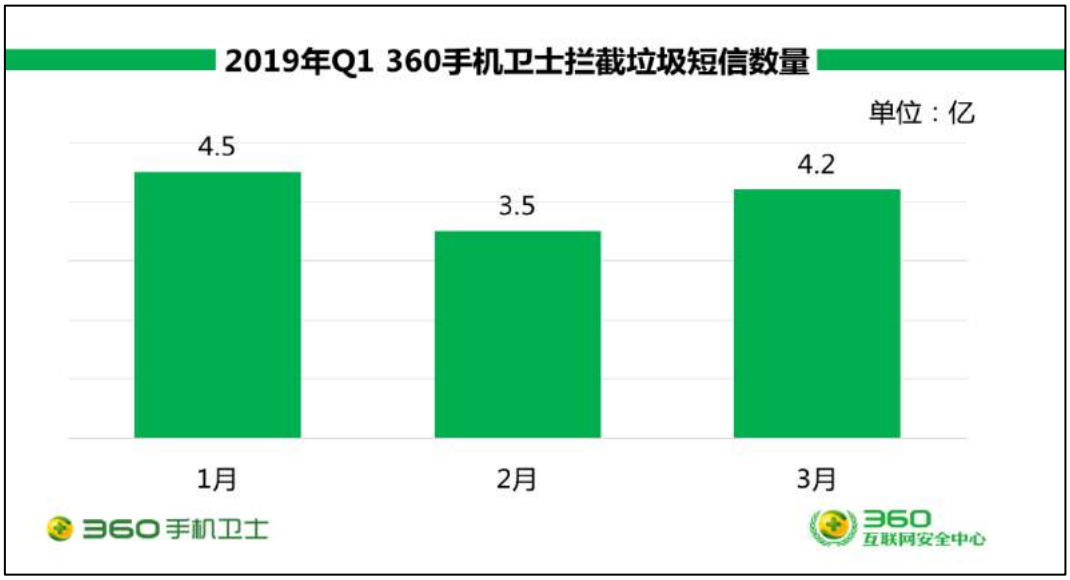
从城市分布来看，北京市用户接到的骚扰电话最多，占全国骚扰电话拦截量的 6.8%，其次是广州（6.4%）、杭州（4.2%）、南京（3.7%）、济南（3.5%），此外成都、上海、长沙、郑州、武汉的骚扰电话拦截量也排在前列。



第四章 垃圾短信

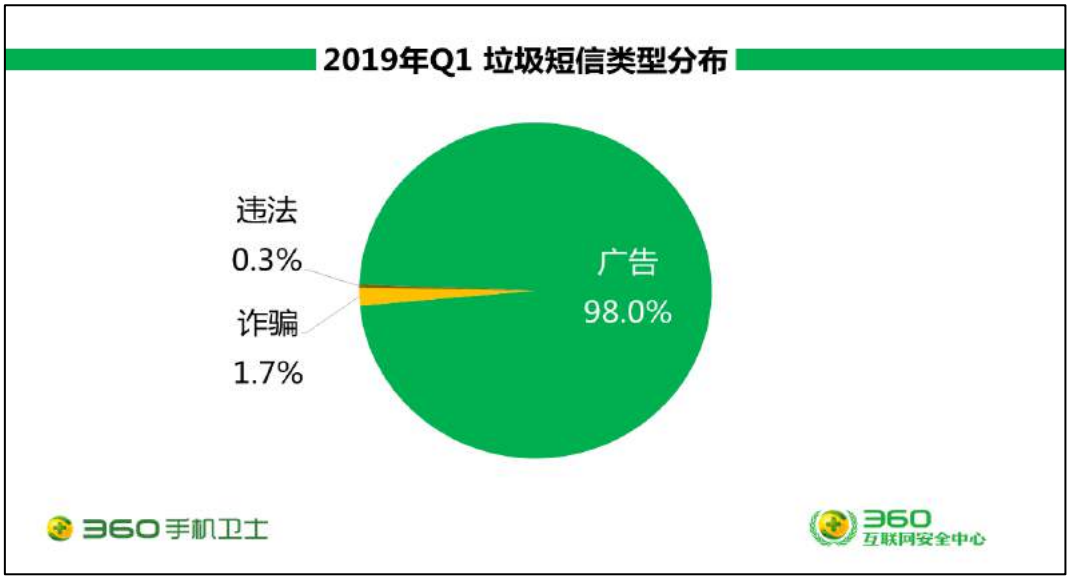
一、 垃圾短信拦截量

2019 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 12.2 亿条，较 2018 年第四季度（19.1 亿条）环比下降了 36.1%，平均每天拦截垃圾短信约 1367.4 万条。由于第一季度 2 月份春节期间，各类发送垃圾短信的从业人员减少、企业放假休息，各类广告推销类型短信减少，导致 2 月份垃圾短信数量降低，在 3 月份后有明显回升态势。



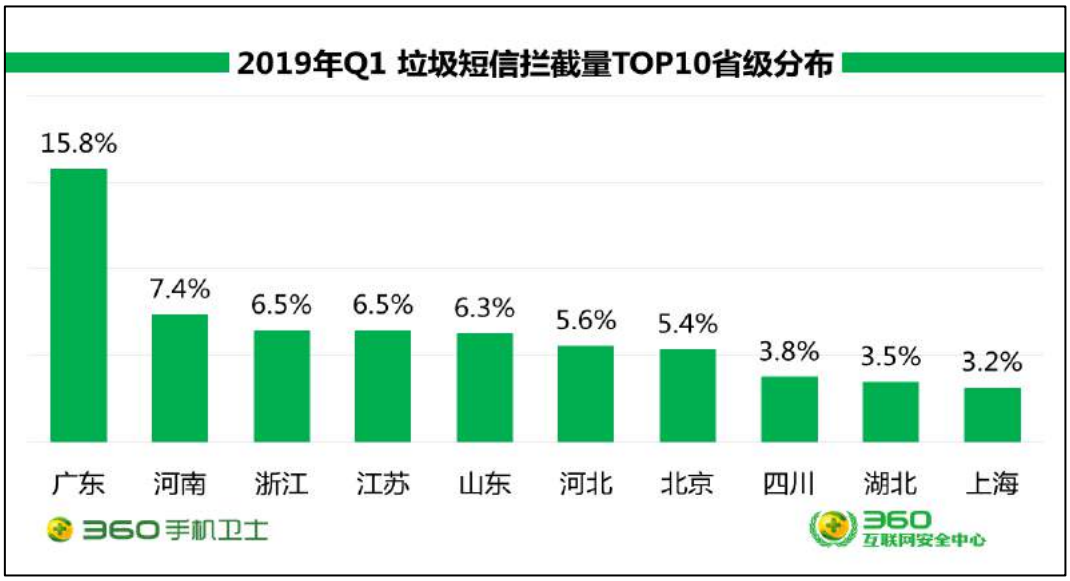
二、 垃圾短信类型分析

2019 年第一季度垃圾短信的类型分布中，广告短信最多，占比为 98.0%，诈骗短信占比 1.7%，违法短信占比 0.3%。具体分布如下图所示：

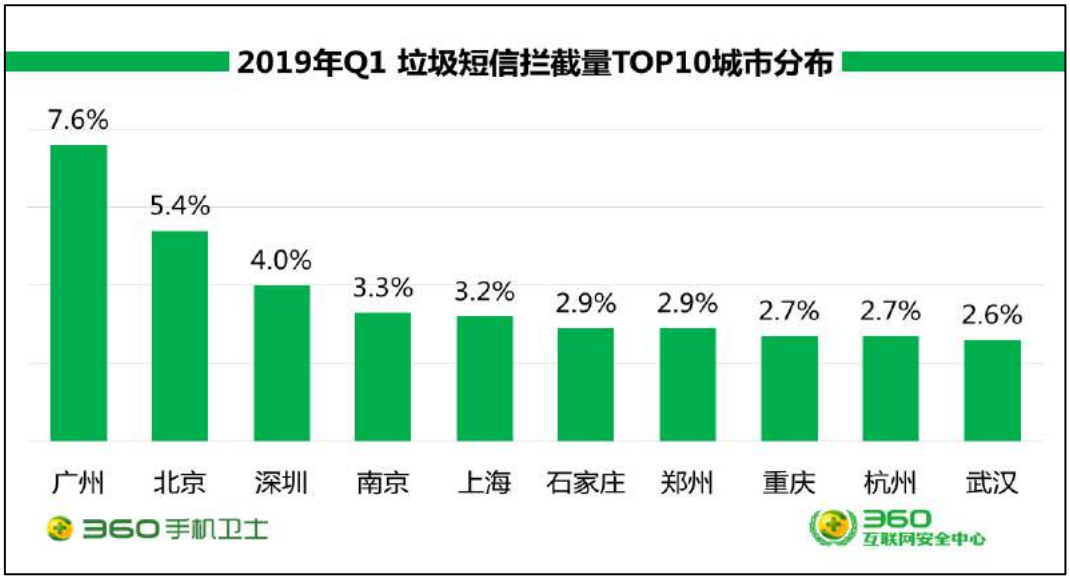


三、 垃圾短信拦截量地域分析

2019 年第一季度，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 15.8%，其次是河南（7.4%）、浙江（6.5%）、江苏（6.5%）、山东（6.3%），此外河北、北京、四川、湖北、上海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 7.6%，其次是北京（5.4%）、深圳（4.0%）、南京（3.3%）、上海（3.2%），此外石家庄、郑州、重庆、杭州、武汉的垃圾短信拦截量也排在前列。


2019年Q1 垃圾短信拦截量TOP10城市分布
7.6%
5.4%
4.0%
3.3%
3.2%
2.9%
2.9%
2.7%
2.7%
2.6%
广州
北京
深圳
南京
上海
石家庄
郑州
重庆
杭州
武汉
360手机卫士
360互联网安全中心

第五章 重点趋势分析

一、网络借贷现状分析

网络借贷模式引入中国以来，在国内迅速发展并形成规模，平台数量、每月成交金额及投资人数量不断增加。不同于传统借贷，网络借贷手续简便、形式灵活，已成为当下一种潮流趋势。国内的 P2P 网贷在原有平台中介的基础上成长创新了多种运营模式，再赶上市场的机遇，助力了网贷的加速成长，国内 P2P 网贷进入飞速发展期。

网络借贷主要运营模式、行业现状及风险

1） P2P 模式为网络借贷的主要运营模式

网贷平台作为中介，提供金融信息服务，由合作的小额借贷公司与担保机构提供担保。借贷双方中，出借人实现了资产的收益增值，而借款人则可以用这种方便快捷的方式满足自己的资金需求，网贷平台则依靠向借贷双方收取一定的手续费维持运营。

2） 网络借贷行业现状及风险

网络借贷飞速发展，其行业内更是呈现出爆炸式增长的态势，由此，也导致行业内乱象丛生。部分平台以高收益、银行风控、安全系数高等口号大肆宣传，诱导投资人注资，实为疯狂圈钱，在平台吸收资金到一定金额后，利用平台升级等借口关闭提现入口，投资人察觉后才发现，平台已卷钱跑路。

近几年，社会上频频爆出借贷平台逾期兑付、经营不善停业等新闻，其中部分被爆“暴雷”的机构已因涉嫌非法吸收公众存款被公安机关立案侦查。可见，网络借贷对比传统借贷虽存在居多优点，但其存在的风险也愈加明显。

行业内多数小额借贷平台存在资质参差不齐，风控不稳，经验、资金不足等问题。由于小额借贷平台资金流量规模小，多数银行并不给予这类借贷公司资金托管服务，这便给部分恶意创办的网贷平台提供了利用管理不严的资金托管机构进行欺诈的机会;同时由于网贷平台创立初期运营成本较高,加上行业内的激烈竞争,长期难以盈利的平台将不得不面临关闭;另由于网络借贷审核放款门槛低，但借款人信用体系尚未规范，逾期坏账率无法平衡控制，最终平台将由于坏账率过高而面临关闭。而对于投资者而言，如不能对投资平台进行甄别，极有可能遭受财产损失。

借贷 APP 成网络借贷主要运营方式

1） 借贷 APP 的应用成行业趋势

如今，网络借贷平台为满足市场使用需求，增加用户使用频率，提高曝光度，开发借贷 APP 并予以推广传播。通过对手机应用市场的观察发现，“贷款中介”平台居多，此类平台

不直接面对用户进行借款，而是为用户提供一款“贷款超市”，引导用户在多家小额借贷平台提交申请，增加贷款成功率。而这些平台面对的用户群体，往往是一些信用指数不高，无法通过银行等正规渠道进行贷款的“黑户”或学生。

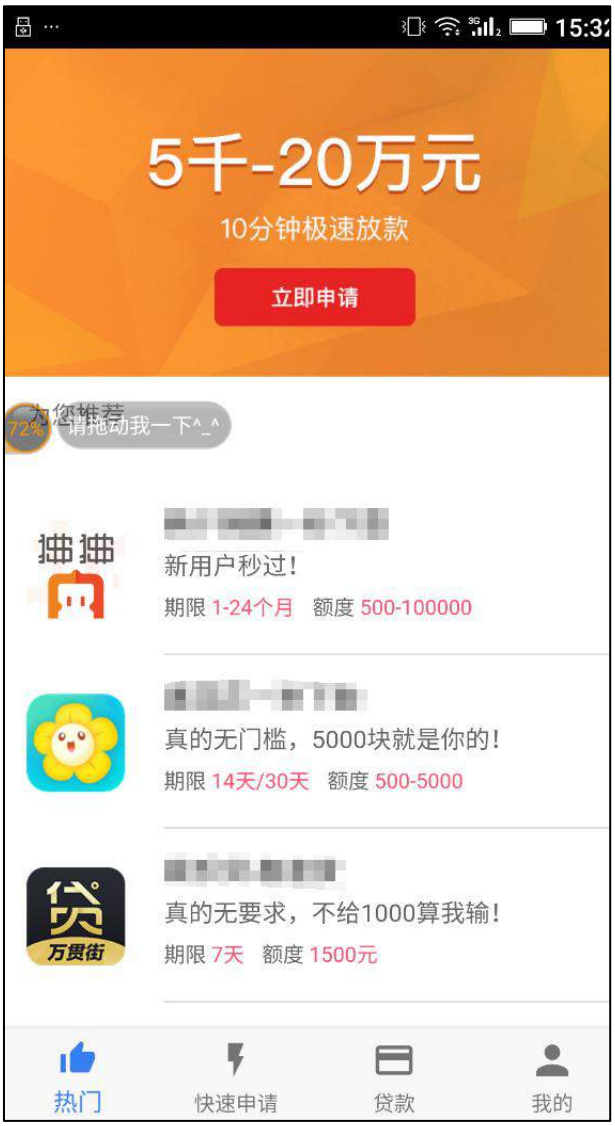


图 1:某“贷款中介”APP 首页

由于国家金融政策方面的监管，现在的应用商城已经开始控制并拒绝网贷 APP 上架，这也就让一些新上线的网贷 APP 找不到客源，也让一些有借款需求的用户找不到新的借贷平台。这时网贷推广平台无缝衔接网贷公司与借款用户，实现闭环，共赢发展，有的推广平台为了增加曝光量，在其他推广平台上同样进行上架推广。

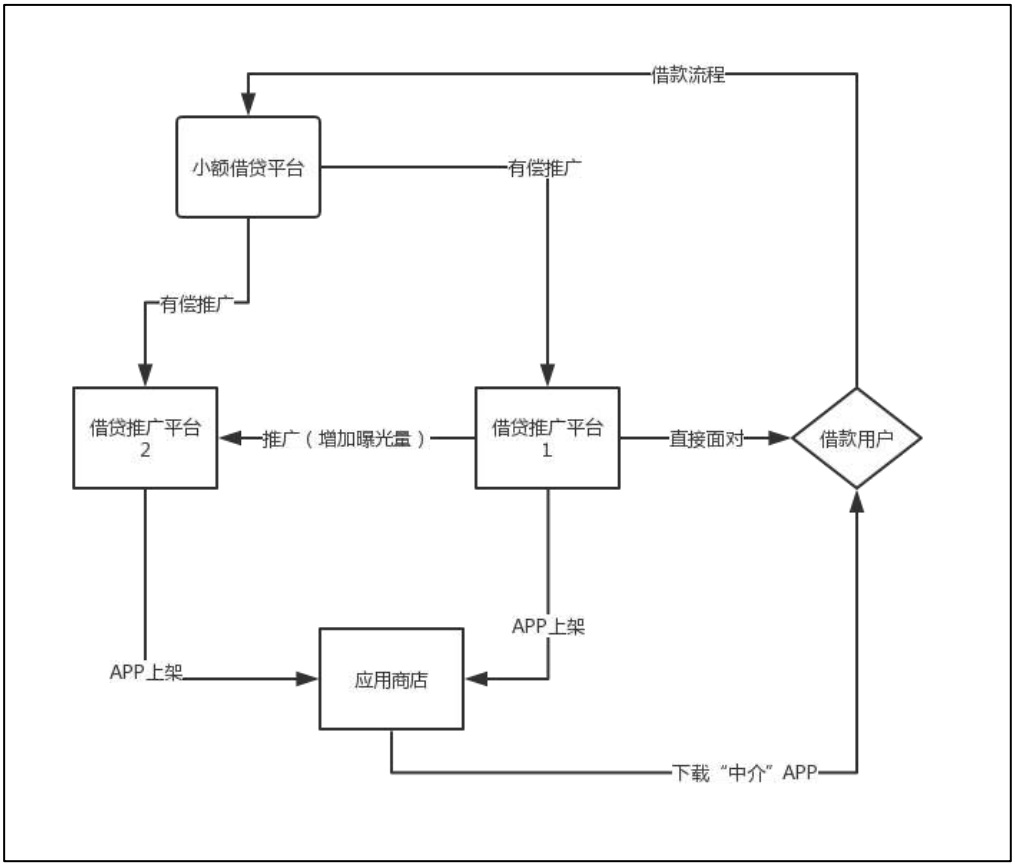


图 2:借贷 APP 推广平台利益链

通过多渠道获取的用户源，最终操作都将引导至 APP 内进行，在成功下款前，要求用户填写基础个人信息、证件信息用作资质审核。部分 APP 会获取通讯录权限，或进行运营商服务密码验证，以获取用户手机号的通话记录详单，作为第二联系方式备用。有的借贷平台会要求用户缴纳会员费、激活费或手续费，缴纳后才可成功下款。表面上看，借款利率虽正常，但变相收取的各项费用支出加上后续缴纳的利息，已超过国家法定利率，不少借贷平台均利用这种方式获利。

图 3:某借贷 APP 首页

2） 借贷 APP 运营方式所蕴含的风险

如雨后春笋一般的借贷 APP，其中蕴含的风险不容小觑。现网络上不乏一些 APP 制作渠道，针对借贷，通常会有多套 APP 模板供选择，无论是个人在开发平台中自行制作还是寻找第三方制作，都十分方便快捷，无形中也为不法分子建立了快速通道。另外，在诈骗反馈中发现，虚假贷款 APP 样本下载渠道多为第三方应用分发平台，此类平台一般是帮助应用开发者测试应用，过程中无需提交详细的信息资料，不法分子正是利用此类平台传播虚假贷款 APP。部分虚假借贷 APP 甚至借助“合法外衣”在部分应用商店进行了商家推广，用户不易辨别，很容易遭遇借贷诈骗。

图 4:某 APP 开发平台模板选择项

图 5:某贷款诈骗 APP 下载链（利用某第三方分发平台）

小额借贷突出问题与如何防范

央视 3·15 晚会曝光后，“714 高炮”这一名词出现在大众视野中。“714 高炮”指的是一些期限为 7 天或 14 天的高利息网络贷款，“高炮”是指其高额的“砍头息”及逾期费用。“714 高炮”的野蛮催收引发了一系列不良后果。这种套路贷在行业内已不是新鲜玩法，相比抵押贷款，网络上这种无抵押信用贷款风险更大，切忌轻信这些看上去简单的办理条件流程。进行借款理财前需要了解平台真实性和可靠性，可以通过查询企业是否拥有金融经营资质和网站备案信息来判断理财平台的真伪。

二、 备案域名黑灰产业分析

随着网民安全意识的提高，一些网民会通过查询网站是否备案确认网站真伪。据 360 手机先赔用户反馈，其曾在手游喊麦中了解到低价游戏装备售卖平台，确认网站是企业备案后，在平台充值购买了商品，但后续客服却要求缴纳各式各样的费用才给予所购买商品，用户多次缴费后也未得到应有商品。此类虚假网游交易平台借助低价商品吸引用户，再通过域名企业备案信息迷惑用户，同时也给安全软件鉴别增加了一定的难度。鉴于此，以下通过不同维度对域名备案产业进行分析，探究其产业背后的链条。

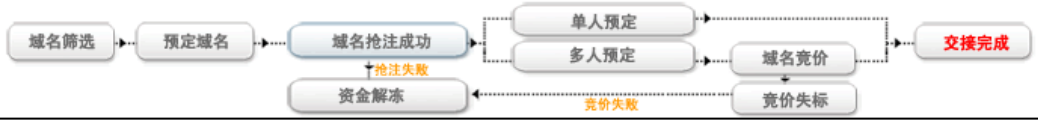
1） 已备案钓鱼网站域名渠道来源

在对多个已备案的钓鱼网站域名溯源分析时，发现此些域名曾经出现在域名售卖平台，跟踪发现，此类域名为抢注域名。原注册备案过的域名，因到期后未续费而被域名注册商进行售卖，由于未进行备案销户，备案信息仍与原域名绑定。此类域名被抢注并使用时，备案信息为原注册备案信息。同时此类备案域名售卖平台，往往设置多条服务器线路进行域名监控抢注。如下图展示的冒充银行的域名，为企业备案，在某备案域名出售平台发现其踪迹。

域名拍卖-域名购买-域名预定-注册域名-xz域名交易网
wangshanglicai.net ￥199 购买 yichenggo.net ￥199 购买 wanghongbg.net ￥199 购买 huangjiayizhan.net ￥199 购买 szdsyynk.net ￥199 购买 juweibang.net...
35599.com/ - 百度快照

¬请选择¬	成功率	选择指南	抢注价格	预定保证金	支持后缀	抢注商
1号通道	超高(99%) (成功最高)	查看	¥470 元	¥50 元	.com/.net/.org/.cc/.tv	25个
2号通道 荐	很高(97%)	查看	¥188 元	¥20 元	.com/.net/.org/.cc	21个
3号通道 荐	很高(95%) (推荐)	查看	¥119 元	¥10 元	.com/.net/.org/.cc	18个
4号cn通道	cn通道(97%)	查看	¥45 元	¥10 元	.cn/.com.cn/.org.cn/.net.cn	9个
5号通道	中高(90%)	查看	¥99 元	¥10 元	.com/.net	15个
6号通道	高(80%)	查看	¥85 元	¥10 元	.com/.net	13个
7号通道	中等(70%) (先定先得)	查看	¥75 元	¥10 元	.com/.net	11个
9号通道	超低(20%)	查看	¥52 元	¥10 元	.com	3个
10号cn通道	cn低价通道(20%)	查看	¥20 元	¥5 元	.cn/.com.cn/.org.cn/.net.cn	2个
11号cn通道	cn通道,不含66cn(85%)	查看	¥44 元	¥10 元	.cn/.com.cn/.org.cn/.net.cn	8个
12号通道 新	新后缀专用通道(99%)	查看	¥39 元	¥10 元	.top/.vip	10个

域名预定流程图



同时发现备案域名售卖市场还存在“快速备案”即代备案的情况，如共享备案与独立备案。共享备案指的是同一个机构或个人旗下允许多个域名存在。备案域名产业利用此特点，将需备案的域名的 whios 改为已备案域名的机构或个人名下，实现域名挂靠备案。独立备案指的是企业对应独立域名。由于企业域名备案需提供营业执照，不法分子将需备案的域名的 whios 信息更改，再使用指定的营业执照进行备案。如下图某备案网站展示的快速备案要求。

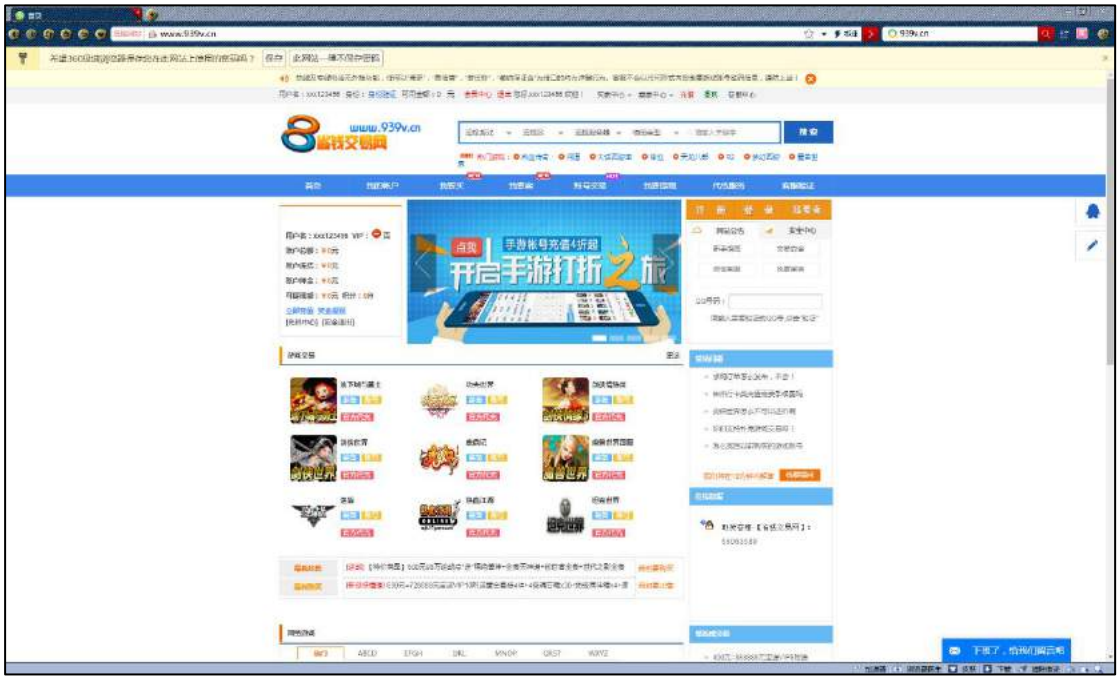
备案类型	备案时间	是否关站	价格(元)
个人共享（无需资料 需要改whois）	8-9个工作日	需关站（不支持阿里）	现价：300
个人共享（无需资料 需要改whois）	8-9个工作日	可开站（不支持阿里）	现价：400
企业共享（无需资料 需要改whois）	8-9个工作日	需关站（不支持阿里）	现价：450
企业共享（无需资料 需要改whois）	8-9个工作日	可开站（不支持阿里）	现价：500
个人独立备案（需身份证幕布照）	5-7个工作日	需关站	现价：400
个人独立备案（需身份证幕布照）	5-7个工作日	可开站	现价：650
企业独立备案（需执照身份证幕布照）	8-9个工作日	需关站	现价：450

2） 购买人群及购买人群用途

备案域名是网络营销、网络黑产的必备消耗品。在特殊的网络一角，备案域名乃当之无愧的快消品。

在网络营销方面，如在黑帽 SEO 领域，一些组织通过一些作弊的手段优化网站在搜索引擎的排名，通过大量不同域名的网站制作站群达到霸占搜索引擎搜索结果的目的，而备案域名则是站群模式的必须品。在流量裂变领域，微信公众号成为时代新宠儿，备案域名则是制作微信公众号的“优良”条件。在淘宝客领域，由于电商平台的火热，越来越来的人投入到推广各类电商平台优惠券的淘宝客领域，利用备案域名加网站一键式搭建程序生成淘宝客网站则是淘宝客产业的主要方式。在网赚领域，随着互联网的发展，出现越来越多的“羊毛党”，此类人群需要最新的羊毛活动，而网赚平台建站也需要使用大量的备案的域名。

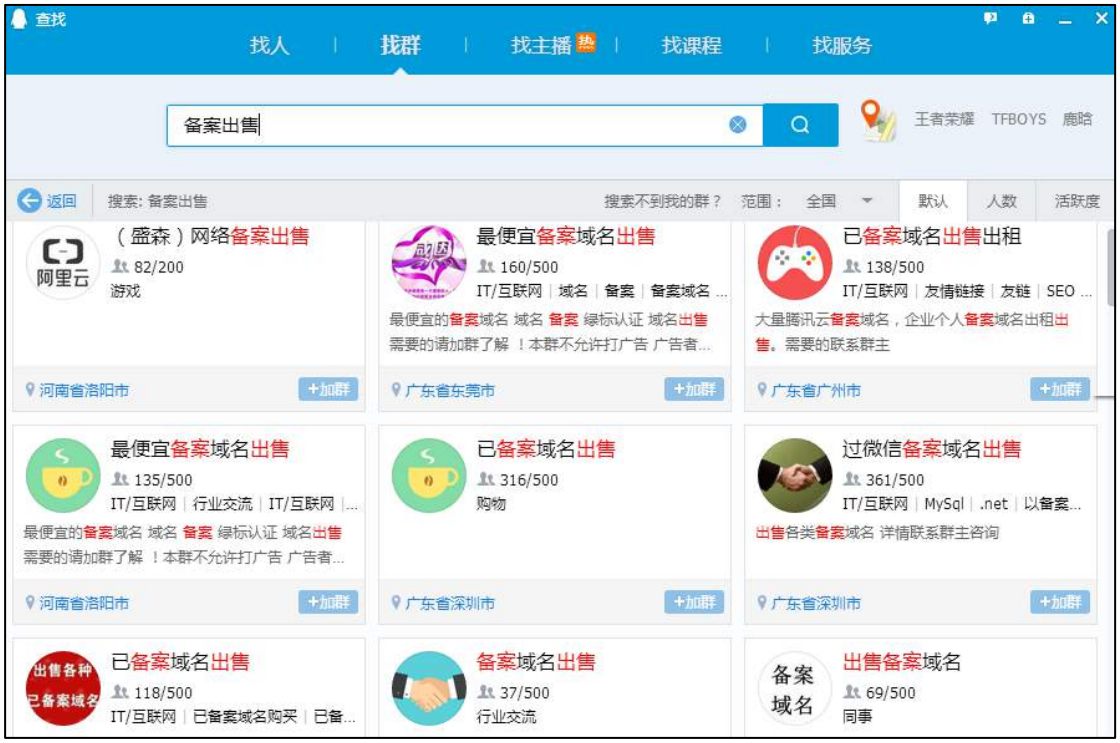
在网络黑产行业，备案网站对受骗者具有一定的迷惑性，同时也可通过安全软件的初步审核。如博彩类网站通过企业备案信息假冒棋牌类游戏，通过金融类备案域名冒充银行及金融平台，通过某科技有限公司备案域名冒充网游交易平台，通过企业备案域名开展各类虚假红包、游戏活动。如下图展示的虚假网游交易平台，诈骗事发时域名曾用备案主体为山西口吕品商贸有限公司。



3） 备案域名售卖渠道广泛、分类多样

备案域名售卖渠道多样化。互联网具有延伸性，商品的购买渠道也多种多样，在多个渠道均发现了售卖备案域名的踪影，如电商平台、搜索引擎、社交平台等。


下午4:38
网址
综合
销量
视频
筛选
国外
域名注册
香港域名注册.hk 国外域名
网址购买 .us .jp .com.uk 澳洲...
¥100 2人付款 上海
进店 >
海盗域名
备案域名
网址，域名交易，cn、com、top
等，可用于站群、蜘蛛池、SEO...
¥5 99人付款 南京
进店 >
海盗域名
老域名、老备案、独立备案
60元-150元
相对批量备案风险小，更
耐封
老域名、老备安，网址网站域名
交易，站群棋牌打赏
¥10 5人付款 南京
进店 >
转让 域名
20元 65元 120元
图片价格是真实价！
com转让 老玉米转让 域米网址
批发【 图片真实价 】
¥10 23人付款 广州
进店 >
域名转发服务，网址跳转，隐藏
转发，URL转发



待出售的备案域名品类多样化，包含个人备案、企业备案、社会团体备案、政府机关备案、事业单位备案。其中各备案属性中又包含大量不同类别的内容，如某市雕塑有限公司、医院门诊部、培训学校、律师事务所、某市卫生局、某市教育局、某省司法厅、某县法院、某县人民政府、某市公安局治安警察支队、某区人民武装部、某市出入境检验检疫局等。

ID	域名	备案号	类型	接入商	网站关键字	安全检测	长度	注册时间	到期时间
1	ichesky.cn	沪ICP备11049261号-7	企业	其他	小渔便利	微信 QQ 360 备案查询	7	2016-10-31	2019-10-31
2	aokvj.cn	粤ICP备19012976号-1	企业	腾讯云	广州付帝贸易有限公司	微信 QQ 360 备案查询	5	2019-01-07	2020-01-07
3	jnzhongxuan.cn	鲁ICP备18008272号-1	企业	阿里云	济南中轩信息技术有限公司	微信 QQ 360 备案查询	11	2018-01-03	2020-01-03
4	uwayq.cn	粤ICP备19012344号-2	企业	腾讯云	广州市韬漾辉贸易有限公司	微信 QQ 360 备案查询	5	2019-01-07	2020-01-07
5	zhihuiwengqi.cn	蒙ICP备17002275号-1	企业	阿里云	智慧翁旗	微信 QQ 360 备案查询	12	2017-01-01	2020-01-01
6	txzvi.cn	粤ICP备19014310号-2	企业	腾讯云	深圳市泰兴科技有限公司	微信 QQ 360 备案查询	5	2019-01-04	2020-01-04
7	zploq.cn	粤ICP备19014311号-2	企业	腾讯云	深圳市征艳贸易有限公司	微信 QQ 360 备案查询	5	2019-01-07	2020-01-07

ID	域名	备案号	类型	接入商	网站关键字	安全检测	长度	注册时间	到期时间
1	taishansi.cn	赣ICP备17001141号-1	社会团体	阿里云	江西省安义县台山寺	微信 QQ 360 备案查询	9	2017-01-03	2020-01-03
2	jnlhzy.cn	闽ICP备11013747号-2	社会团体	其他	厦门思明立和中医门诊部	微信 QQ 360 备案查询	6	2018-10-17	2020-10-17

4） 虚假备案域名鉴别

随着安全攻防技术的升级，黑灰产业产出了绿标域名、防红域名、二级防封域名用于对抗安全软件拦截，如将已被安全软件拦截的域名生成企业备案的短链网址、只使用二级域名或抢注某些事前已被安全软件收录并标记为安全的域名。如下图展示，此域名原先被社交平台标记为官方认证，实际上域名已被域名平台抢注并出售，已脱离原备案信息。

域名	价格	建站记录-地区	简介	注册时间	到期时间	安全检测	购买
jxbdcm.com	1988元	-	阿里云	2015-12-23	2019-12-22	360 QQ	购买
gxeiot.cn	2288元	企业-京	北京工信双华科技有限责任公司 其他	2011-01-19	2020-01-19	360 QQ	购买
jnny.com.cn	2688元	企业-晋	双鲁鑫|晋中能源股份有限公司 其他	2005-01-19	2020-01-19	360 QQ	购买
huaqingbank.com	3688元	企业-苏	江苏华擎商务咨询有限公司 阿里云	2017-12-23	2019-12-22	360 QQ	购买

安全厂商可以根据 whios 信息的续注时间与首次注册时间判断域名属于是否属于抢注域名，如正常过期删除域名，此类域名注册时间在抢注成功后重新计算。再对网站内容、备案信息、备案企业经营范围进行关联性判断，判断此些信息是否匹配，一旦域名不匹配，通过大数据挖掘威胁域名的关联域名进行威胁域名预警。

消费者可以通过结合网站内容、备案信息、备案企业经营范围进行判断。如下图展示的冒充中国工商银行的网站，此网站界面虽与中国工商银行页面类似，但备案信息为某市门诊部，属于网站内容与备案信息不匹配，可判断出此网站属于虚假网站。

第六章 手机诈骗形势

一、报案数量与类型

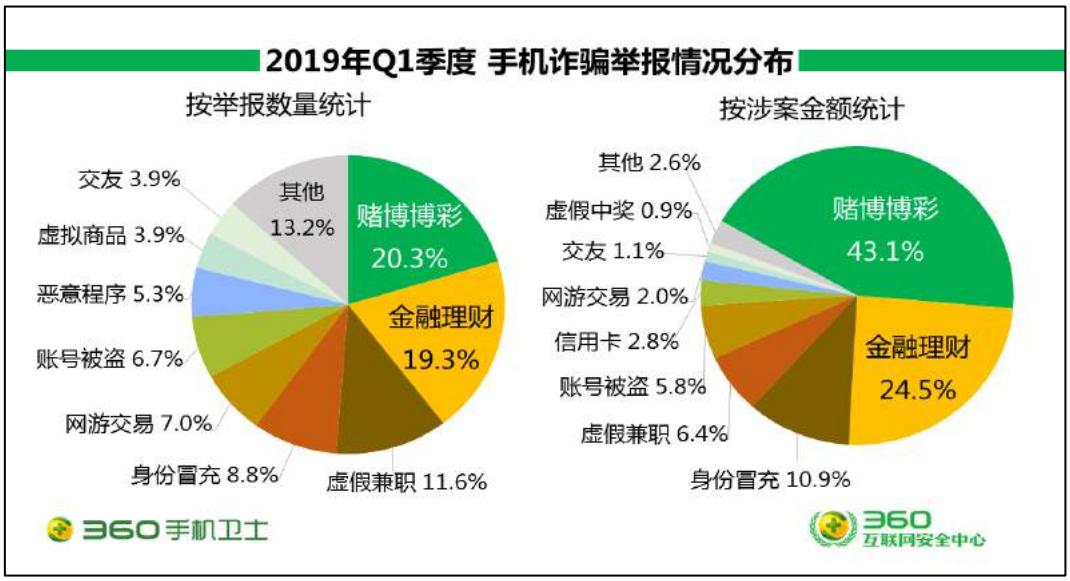
2019 年第一季度 360 手机先赔共接到手机诈骗举报 1391 起。其中诈骗申请为 571 起，涉案总金额高达 306.1 万元，人均损失 5360 元。

在所有诈骗申请中，赌博博彩占比最高，为 20.3%；其次是金融理财（19.3%）、虚假兼职（11.6%）、身份冒充（8.8%）和网游交易（7.0%）。

从涉案总金额来看，赌博博彩类诈骗总金额最高，达 131.8 万元，占比 43.1%；其次是金融理财诈骗，涉案总金额 74.8 万元，占比 24.5%；身份冒充诈骗排第三，涉案总金额为 33.2 万元，占比 10.9%。

从人均损失来看，赌博博彩诈骗人均损失最高，为 11359 元；其次是信用卡诈骗为 9355 元，金融理财诈骗为 6804 元。

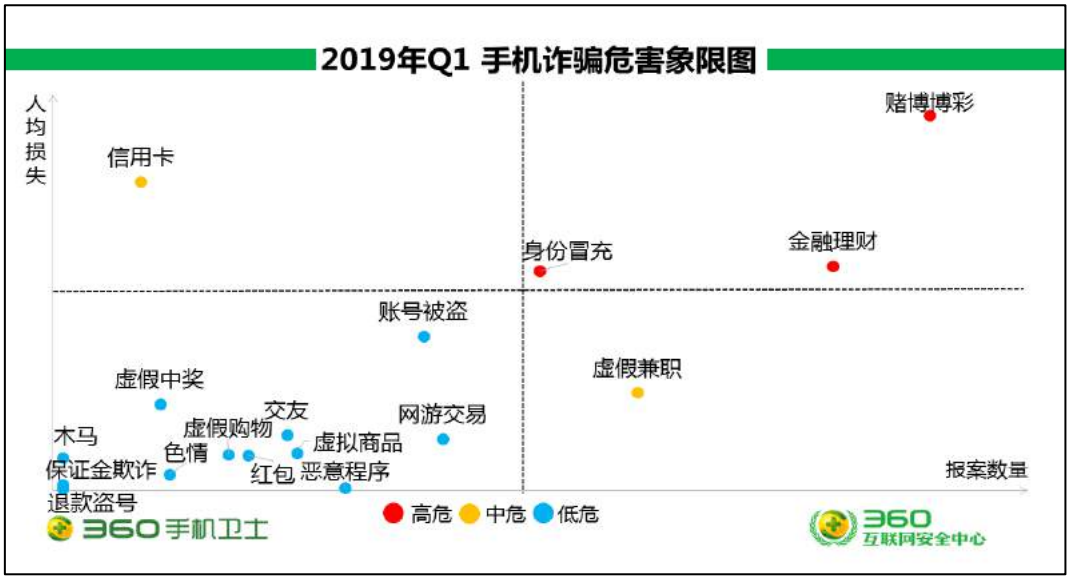
下图给出了主要手机诈骗类型的举报量和涉案总金额分布情况：



下图给出了不同类型的手机诈骗在人均损失和举报数量的象限图。从图中可见，赌博博彩、金融理财、身份冒充属于高危诈骗类型，受害人数较多且人均损失高。

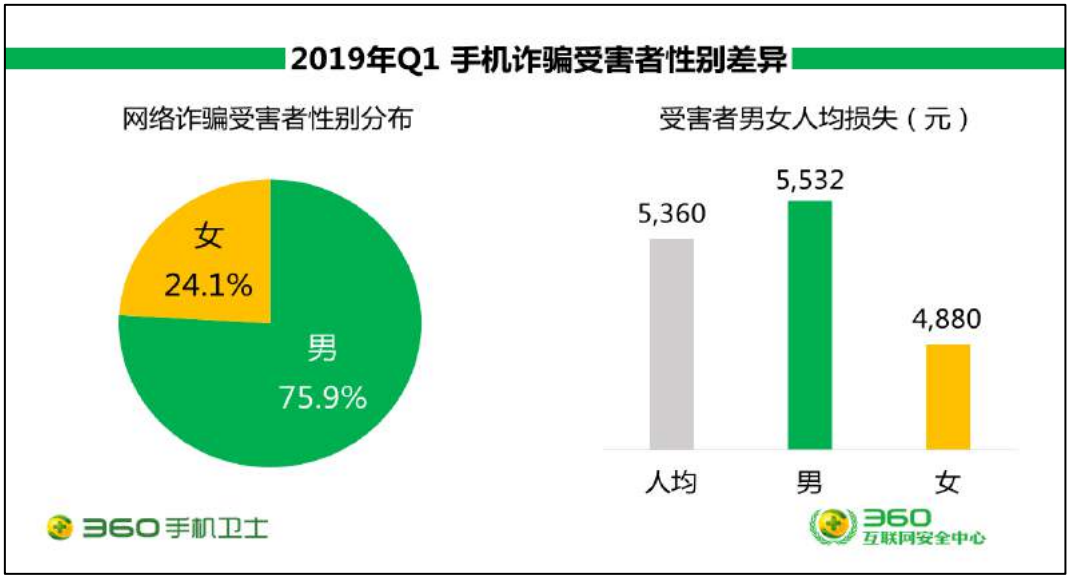
信用卡类型虽受害人数少，但人均损失较高，此类诈骗主要利用个人信息泄露发起的定向诈骗，危害性较高，属于中危诈骗类型。而虚假兼职虽人均损失偏低，但受害人数多，兼职缴纳会费的诈骗手法居多，属于中危诈骗类型。

结合以往统计分析，恶意程序类型一直属于高发诈骗类型，有着人均损失低，但受骗人数多，且低龄化的特点。但在 2019 年第一季度诈骗分析中，恶意程序类诈骗整体诈骗举报量骤减，可见，由于各大安全厂商与手机厂商不断完善恶意程序查杀机制，用户感染率降低。举报量的减少同时说明，用户安全意识提升，对于手机安全性也愈加重视。

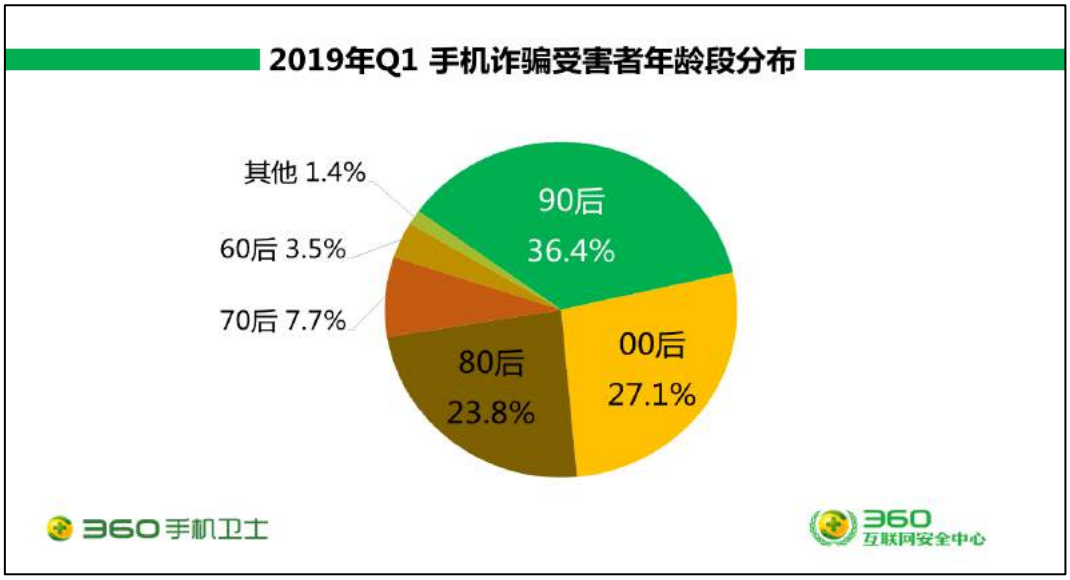


二、受害者性别与年龄

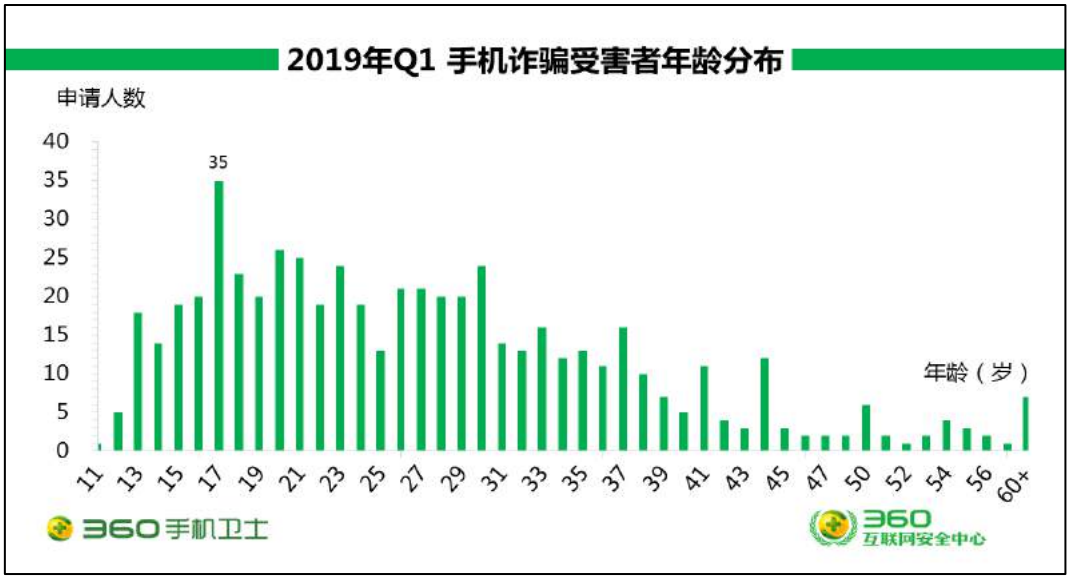
从举报用户的性别差异来看，男性受害者占 75.9%，女性占 24.1%，男性受害者占比高于女性。从人均损失来看，男性为 5532 元，女性为 4880 元，男性受害者人均损失同样高于女性。



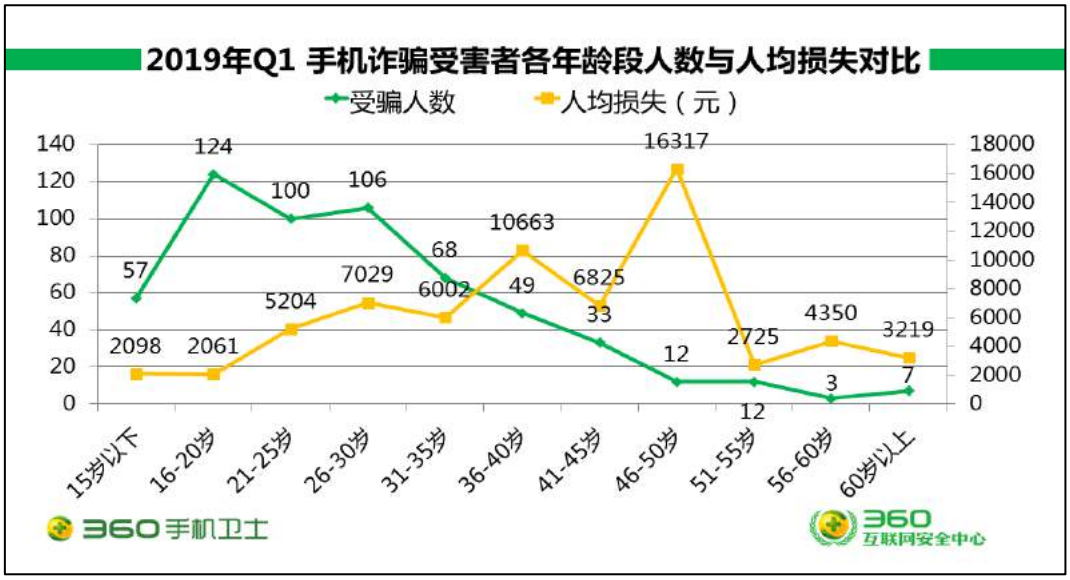
从被骗网民的年龄段上看，90 后的手机诈骗受害者占所有受害者总数的 36.4%；其次是 00 后占比为 27.1%，80 后占比为 23.8%，70 后占比 7.7%，60 后占比为 3.5%，其他年龄段占 1.4%。如图分布，2019 年第一季度中，00 后诈骗举报量减少，90 后再次成为手机诈骗主要针对人群。



而从具体年龄上来看，16 岁至 20 岁的人群依然是手机诈骗受害者最为集中的年龄段，占所有手机诈骗受害者的 21.7%，其中赌博博彩类型受骗反馈较多。由于这个年龄段用户对于外界事物真实性判断能力较弱，无法对网络游戏平台合法性进行判断，在日常中使用手机交友的情况居多，对陌生人防范意识不强，若被引导至不合规平台进行充值游戏，极易遭受财产损失。

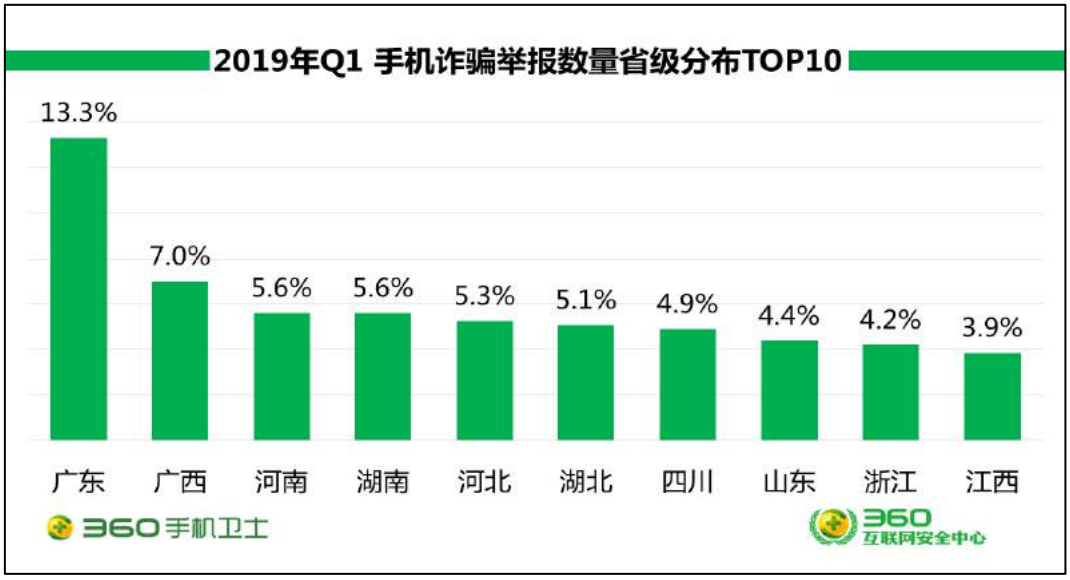


下图给出了手机诈骗受害者年龄段人数与人均损失的对比，从图中可以看出，随着年龄的增长，受害者人均损失总体上也在增长。15-20 岁之间的用户，是上网的主力人群，被骗的人数虽多，但由于年轻人经济能力有限，被骗平均金额相对较少。30 岁以后的受害者，年龄越大，经济能力也越强，虽然上网的人群、时间在减少，但被骗平均金额迅速增长，超过了 16317 元。

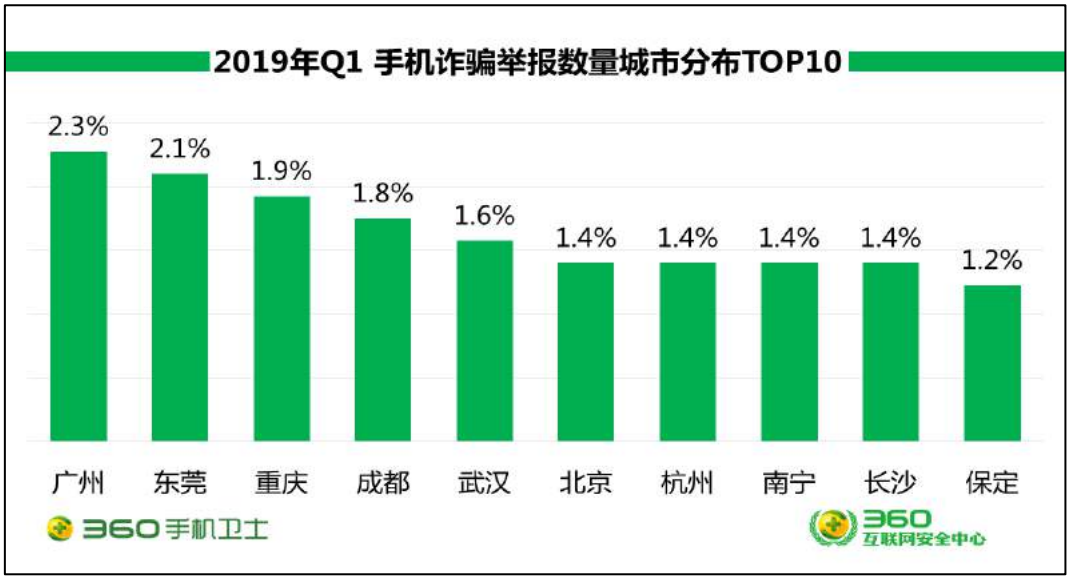


三、受害者地域分布

2019 年第一季度，从用户举报情况来看，广东（13.3%）、广西（7.0%）、河南（5.6%）、湖南（5.6%）、河北（5.3%）这 5 个省级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 36.8%。下图给出了 2019 年第一季度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（2.3%）、东莞（2.1%）、重庆（1.9%）、成都（1.8%）、武汉（1.6%）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 9.6%。下图给出了 2019 年 Q1 季度手机诈骗举报数量最多的 10 个城市：

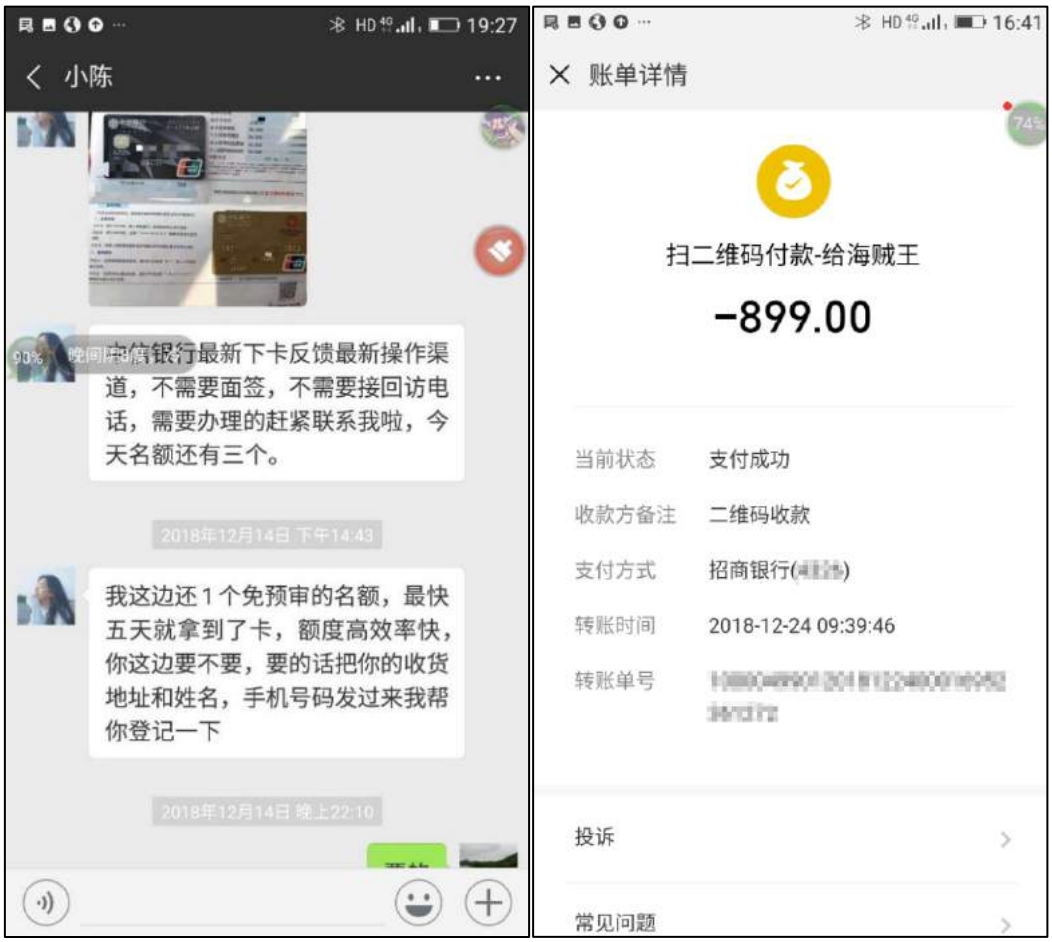

2019年Q1 手机诈骗举报数量城市分布TOP10
2.3%
2.1%
1.9%
1.8%
1.6%
1.4%
1.4%
1.4%
1.4%
1.2%
广州
东莞
重庆
成都
武汉
北京
杭州
南宁
长沙
保定
360手机卫士
360互联网安全中心

第七章　典型案例

一、办理高额信用卡诈骗

案例回顾

2018 年 12 月李先生的微信好友给用户推送无需面签、无需接回访电话、只需通过指定 POS 机激活即可获得高额信用卡的信息，李先生按照对方要求通过微信转账 899 元购买了信用卡实体合约机。



收到对方邮寄的“闪电宝 POS 机”后，在 POS 机激活客服的指引下通过李先生自己的信用卡缴费激活了 POS 机，在信用卡办卡客服提供的信用卡申请网站申请信用卡失败，得知受骗。

专家解读

此案例中，不法分子人员分工明确，如负责前期推销办理高额信用卡、中期负责 POS 机激活、后期负责信用卡申请。首先以办理高额信用卡名额有限，给予用户紧张感，待用户支付费用购买 POS 机，并收到 POS 机后，再引导用户使用自己的信用卡在 POS 内缴费激活，此步骤完成后，给用户提供各大银行信用卡自助申请链接，不管成功与否，事后都拉黑用户。

防骗提示

信用卡的额度是根据申办人的职业、收入、经济实力、偿还债务能力、之前的信用记录等维度评估的，如遇到可以无视银行限制办理高额信用卡的情况一定是诈骗。

二、 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。

三、 虚假兼职新套路“广告机”

案例回顾

2018 年 10 月童先生经朋友介绍，了解到“钱多多”广告机，投资 3980 元，每天可收益 80 元，邀请下线还可获得额外分红，一年可获利 28800 元。童先生花费 3980 元在 SCMA 微信群下单购买了 SCMA 设备机。收到邮寄的设备，按照教程指引使用设备内的 SCMA APP 自动刷广告，前期获得了 400 多元收益。

后期平台先以提现人数多，通道拥挤，系统在处理为由限制提现，之后再以上市为由，关闭提现系统，清零了用户 SCMA 收益数据。童先生此时得知受骗。

专家解读

此案例中的“钱多多”广告机以高额回报的名义，假借设备可以免费刷广告的名义，诱导用户花费 3980 元购买设备，采用多级下线的模式进行推广，相关设备价格也远远低于用户所支付的费用，属于典型的旁氏骗局。

防骗提示

高回报的，必然是高风险，切勿为蝇头小利所迷惑。凡是以广告机、虚拟货币、区块链、原始股、物联网名义宣传投资入股，保证赚钱，静态几倍、动态更多的，要求发展下线层层得利的，一定要小心，避免陷入传销骗局！

四、 全网 VIP 影视会员里的骗局

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。

第八章　热点事件

一、“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。

二、爆款网红“口红机”的秘密

在规定的时间内，点击屏幕将一定数量的口红成功射到转动的转盘上，连闯三关即可获得价值不菲的大牌口红一只，线下“口红机”游戏一夜之间火了！随之朋友圈线上版“口红机”也风靡起来，扫码关注并支付少量费用即可参与游戏。用户扫描游戏二维码登录后，会有两次游戏体验资格，可以了解“口红机”的玩法，体验模式只有两关且游戏难度较低，让用户有一种很容易中奖的错觉，坚持不懈的用户，很可能几十元钱眨眼打了水漂。

专家解读

闯关失败还真不是手速慢或运气不好，都是因为“幕后黑手”。该游戏的开发难度低，某电商平台几十元便可购买到源码与运营教程，商家可以设置游戏难度，修改中奖概率。且由于是线上交易，商品质量不可控，商家不能提供口红的正品证明，商场专柜也并不提供验货，所以商品真假无法保证。

防骗提示

对于此类平台，莫贪小便宜，凡事保持警惕，看似简单的事情，背后往往藏着猫腻。