2019 年上半年
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 8 月 12 日

摘　要

恶意程序：

- 2019 年上半年，360 互联网安全中心共截获安卓平台新增恶意程序样本约 92.0 万个，平均每天截获新增手机恶意程序样本约 0.5 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 1.9 亿次，平均每天拦截手机恶意程序攻击约 107.5 万次。
- 2019 年上半年，安卓平台新增恶意程序类型主要为隐私窃取，占比高达 66.2%；其次为资费消耗（23.6 %）、流氓行为（4.9%）、远程控制（4.3%）、恶意扣费（0.7%）、欺诈软件（0.2%）。
- 从省级分布来看，2019 年上半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 10.2%；其次为山东（7.6%）、河南（6.8%）、江苏（6.6%）、浙江（5.7%）等。
- 从城市分布来看，2019 年上半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 2.1%；其次为广州（1.9%）、重庆（1.8%）、上海（1.6%）、成都（1.4%）等。

钓鱼网站：

- 2019 年上半年，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 404.2 亿次，其中，PC 端拦截量约为 390.4 亿次，占总拦截量的 96.6%，平均每日拦截量约 2.2 亿次；移动端拦截量约为 13.8 亿次，占总拦截量的 3.4%，平均每日拦截量约 760.1 万次。
- 2019 年上半年移动端拦截钓鱼网站类型中，境外彩票类比重最高，为 69.3%；其他占比较高的类型包括网站被黑（24.0%）、假药（2.6%）、金融证券（1.1%）、虚假中奖（1.1%）、虚假购物（0.9%）、虚假招聘（0.5%）、模仿登陆（0.3%）等。
- 从省级分布来看，2019 年上半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 21.4%；其次为广西（8.6%）、山东（5.7%）、福建（5.1%）、湖南（3.6%）等。
- 从城市分布来看，2019 年上半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 4.1%；其次为深圳（3.3%）、北京（3.1%）、东莞（2.8%）、泉州（2.3%）等。
- 2019 年上半年，360 互联网安全中心共截获各类新增钓鱼网站 1019.2 万个，平均每天新增 5.6 万个。观察钓鱼网站新增类型，境外彩票类占比为 81.2%，居于首位。
- 从新增钓鱼网站的服务器地域分布来看，71.0%的钓鱼网站服务器位于国外，26.0%位于国内。其中，国内服务器位于香港的占比为 56.3%，居于首位，其次为广东（10.0%）、北京（8.0%）、浙江（5.1%）、河南（3.1%）等。

骚扰电话：

- 2019 年上半年，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 3659.8 万个，平均每天标记约 20.2 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 114.8 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 年上半年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 57.1%的比例位居首位，其次为广告推销（14.6%）、骚扰电话（8.7%）、疑似欺诈（7.2%）、房产中介（5.4%）、保险理财（4.5%）、招聘猎头（2.3%）、诈骗电话（0.2%）。

- ✧ 从骚扰电话拦截类型来看，广告推销以 46.7%的比例位居首位，其次为骚扰电话（25.4%）、房产中介（18.3%）、疑似欺诈（5.6%）、响一声（2.0%）、保险理财（1.6%）、招聘猎头（0.3%）。

- ✧ 2019 年上半年，从用户标记的骚扰电话号码的运营商归属分布看，被标记的中国移动的手机号码最多，占比高达 43.1%；其次为固定电话（21.6%）、中国电信（19.2%）、中国联通（16.2%）。

- ✧ 从骚扰电话拦截号码的运营商归属分布看，被拦截的中国移动的手机号码最多，占比高达 31.3%；其次为固定电话（29.5%）、中国电信（20.3%）、中国联通（19.0%）。

- ✧ 从省级分布来看，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 11.6%，其次是山东（6.7%）、河南（6.4%）、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 4.9%，其次是广州（3.4%）、上海（3.1%）、深圳（2.2%）、重庆（2.1%），此外杭州、成都、石家庄、天津、武汉的骚扰电话标记号码个数也排在前列。

- ✧ 从省级分布来看，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%，其次是江苏（7.1%）、浙江（6.7%）、山东（6.7%）、河南（6.0%），此外河北、北京、四川、湖南、福建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 6.1%，其次是广州（4.5%）、上海（3.2%）杭州（2.7%）、成都（2.6%），此外郑州、深圳、南京、重庆、武汉的骚扰电话拦截量也排在前列。

- ✧ 从骚扰电话号码拦截个数看，虚拟运营商号段中 95/96 号段拦截号码最多，占比达 43.1%；其次为 170 号段与 400/800 号段，分别占比 21.6%与 19.2%。

- ✧ 从骚扰电话号码类型来看，虚拟运营商号码中广告推销以 46.9%的比例位居首位，其次为骚扰电话（25.1%）、疑似欺诈（12.1%）、响一声（8.3%）、房产中介（6.8%）、保险理财（0.7%）、教育培训（0.1%）。

- ✧ 从骚扰电话虚拟运营商号码标记类型看，虚拟运营商号码中骚扰电话以 21.1%的比例位居首位，其次为广告推销（20.7%）、疑似欺诈（20.6%）、响一声（11.3%）、保险理财（9.5%）、房产中介（9.4%）、招聘猎头（5.6%）。

- ✧ 从省级分布来看，从各地骚扰电话虚拟运营商拦截号码数上分析，广东省用户接到骚扰电话的个数最多，占全国骚扰电话虚拟运营商拦截号码总数的 9.7%，其次是山东（7.3%）、河南（6.4%）、江苏（5.9%）、四川（5.7%），此外浙江、河北、安徽、湖北、湖南的骚扰电话虚拟运营商拦截号码数也排在前列。

- ✧ 从城市分布看，从各地骚扰电话虚拟运营商拦截号码数上分析，北京市用户接到的骚扰电话个数最多，占全国骚扰电话虚拟运营商拦截号码总数的 1.3%，其次是上海（1.2%）、广州（1.1%）、深圳（1.1%）、东莞（0.9%），此外佛山、苏州、杭州、成都、郑州的骚

扰电话虚拟运营商拦截号码数也排在前列。

垃圾短信：

- ✧ 2019 年上半年，360 手机卫士共为全国用户拦截各类垃圾短信约 23.4 亿条，平均每日拦截垃圾短信约 1289.4 万条。
- ✧ 2019 年上半年垃圾短信的类型分布中，广告短信最多，占比为 95.9%，诈骗短信占比 2.9%，违法短信占比 1.1%。
- ✧ 2019 年上半年，收到广告短信最多的是广东省，占全国广告短信拦截量的 8.9%，其次是浙江省（4.0%）与山东省（4.3%）；收到诈骗短信最多的是广东省，占全国诈骗短信拦截量的 18.7%，其次是湖南省（4.2%）与广西省（4.0%）；收到违法短信最多的是广东省，占全国违法短信拦截量的 7.1%，其次是山东省（2.7%）与河南省（2.5%）。
- ✧ 2019 年上半年，从垃圾短信发送者号码的运营商号源分布看，利用 1065/1069 渠道号发送垃圾短信的最多，占比高达 90.6%，其次为 170 号段（3.8%）与 95/96 号段（2.3%）。
- ✧ 从省级分布来看，2019 年上半年收到垃圾短信最多的是广东省，占全国垃圾短信拦截量的 10.7%，其次是山东（4.9%）、浙江（4.6%）、河南（4.4%）、江苏（4.2%）。
- ✧ 从城市分布来看，2019 年上半年收到垃圾短信最多的是广州市，占全国垃圾短信拦截量的 5.6%，其次是北京（4.0%）、深圳（3.0%）、南京（2.5%）、上海（2.3%）。

网络诈骗：

- ✧ 2019 年上半年 360 手机先赔共接到手机诈骗举报 2508 起。其中诈骗申请为 1095 起，涉案总金额高达 638.0 万元，人均损失 5826 元。
- ✧ 在所有诈骗申请中，金融理财占比最高，为 22.7%；其次是赌博博彩（19.7%）、虚假兼职（13.6%）、身份冒充（11.3%）、网游交易（6.2%）等。
- ✧ 从涉案总金额来看，赌博博彩类诈骗总金额最高，达 248.0 万元，占比 38.9%；其次是金融理财诈骗，涉案总金额 160.1 万元，占比 25.1%；身份冒充诈骗排第三，涉案总金额为 109.6 万元，占比 17.2%。
- ✧ 从人均损失来看，赌博博彩诈骗人均损失最高，为 11481 元；其次是身份冒充诈骗为 8840 元，信用卡诈骗为 8092 元。
- ✧ 从举报用户的性别差异来看，男性受害者占 73.3%，女性占 26.7%，男性受害者占比高于女性。从人均损失来看，男性为 6344 元，女性为 5785 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 36.1%；其次是 80 后占比为 26.9%，00 后占比为 22.3%，70 后占比 9.9%，60 后占比为 3.9%，其他年龄段占 0.9%。如图分布，2019 年上半年中，90 后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 26.5%。
- ✧ 2019 年上半年，从用户举报情况来看，广东（13.2%）、广西（7.1%）、山东（5.2%）、浙江（5.2%）、江苏（5.1%）这 5 个省级地区的被骗用户最多。

✧ 从各城市手机诈骗的举报情况来看，东莞（2.3%）、广州（2.2%）、北京（2.1%）、成都（2.0%）、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 7

一、　恶意程序新增样本量与类型分布 7

二、　恶意程序拦截量地域分布 8

第二章　钓鱼网站 10

一、　移动端钓鱼网站拦截量及类型 10

二、　移动端钓鱼网站拦截量地域分布 11

三、　钓鱼网站新增量与服务器地域分布 12

第三章　骚扰电话 13

一、　骚扰电话标记数与拦截量 13

二、　骚扰电话类型分布 14

三、　骚扰电话运营商归属分布 15

四、　骚扰电话归属地分布 16

五、　骚扰电话虚拟运营商 17

第四章　垃圾短信 20

一、　垃圾短信拦截量 20

二、　垃圾短信类型分析 20

三、　垃圾短信运营商号源分布 21

四、　垃圾短信拦截量地域分析 22

第五章　重点趋势分析 24

一、　网络借贷现状分析 24

二、　备案域名黑灰产业分析 29

三、　代充黑灰产业分析 36

第六章　手机诈骗形势 44

一、　报案数量与类型 44

二、 受害者性别与年龄 45
三、 受害者地域分布 47

第七章 典型案例 49

一、 信用卡提额诈骗 49
二、 交友理财诈骗 50
三、 明明付款“0 元”，怎么就背上了千元贷款？ 51

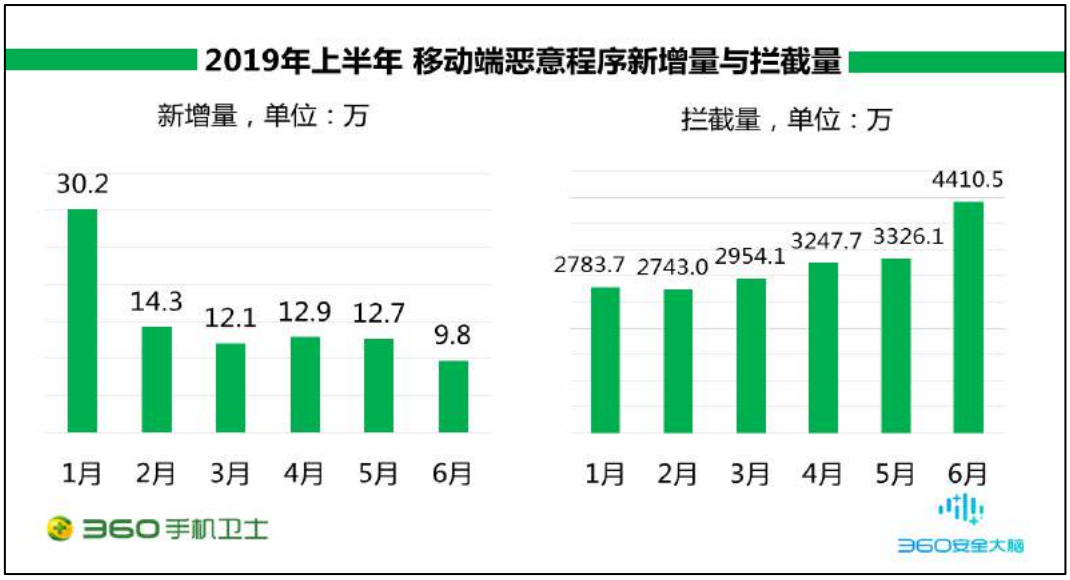
第八章 热点事件 54

一、 流量造假，明星应援 APP 54
二、 微信挂机平台 55
三、 走路就能赚钱的“趣步 APP” 56

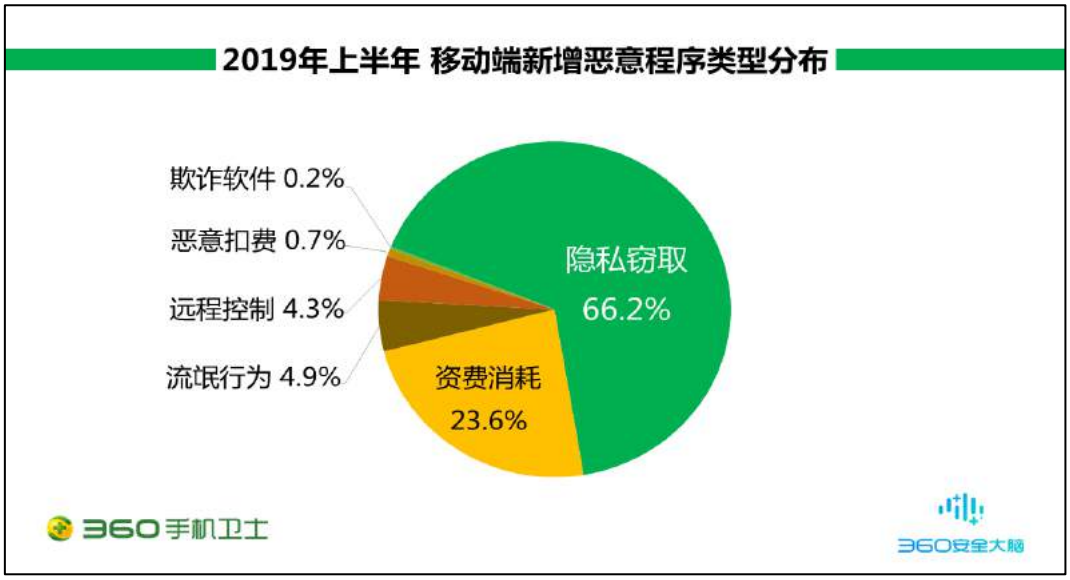
第一章　恶意程序

一、　恶意程序新增样本量与类型分布

2019 年上半年，360 互联网安全中心共截获安卓平台新增恶意程序样本约 92.0 万个，同比 2018 年上半年（283.1 万个）减少了 67.5%，平均每天截获新增手机恶意程序样本约 0.5 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 1.9 亿次，平均每天拦截手机恶意程序攻击约 107.5 万次。下图给出了 2019 年上半年移动端恶意程序新增量与拦截量统计：

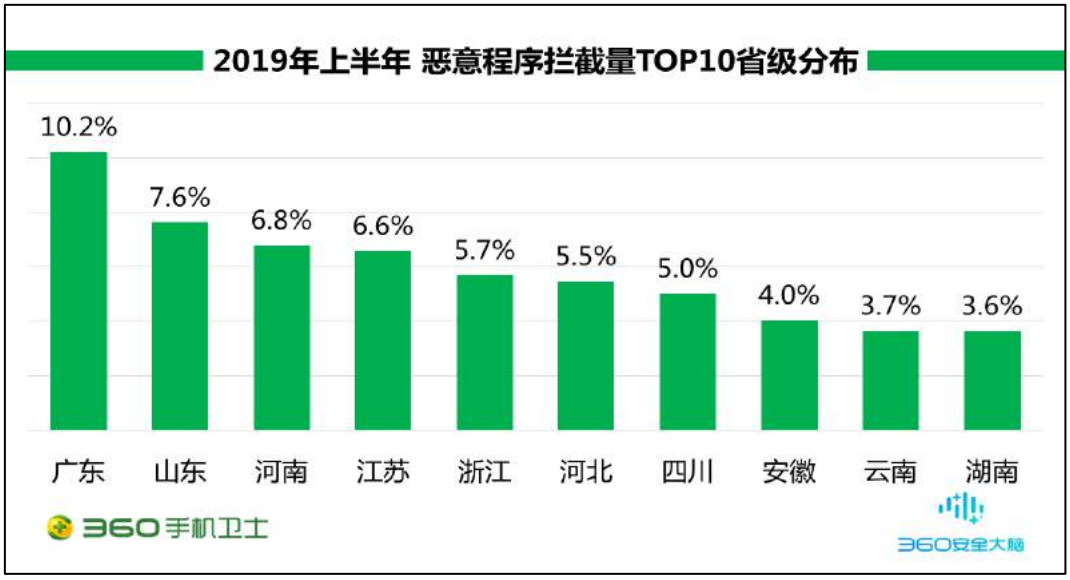


2019 年上半年，安卓平台新增恶意程序类型主要为隐私窃取，占比高达 66.2%；其次为资费消耗（23.6%）、流氓行为（4.9%）、远程控制（4.3%）、恶意扣费（0.7%）、欺诈软件（0.2%）。具体分布如下图所示：

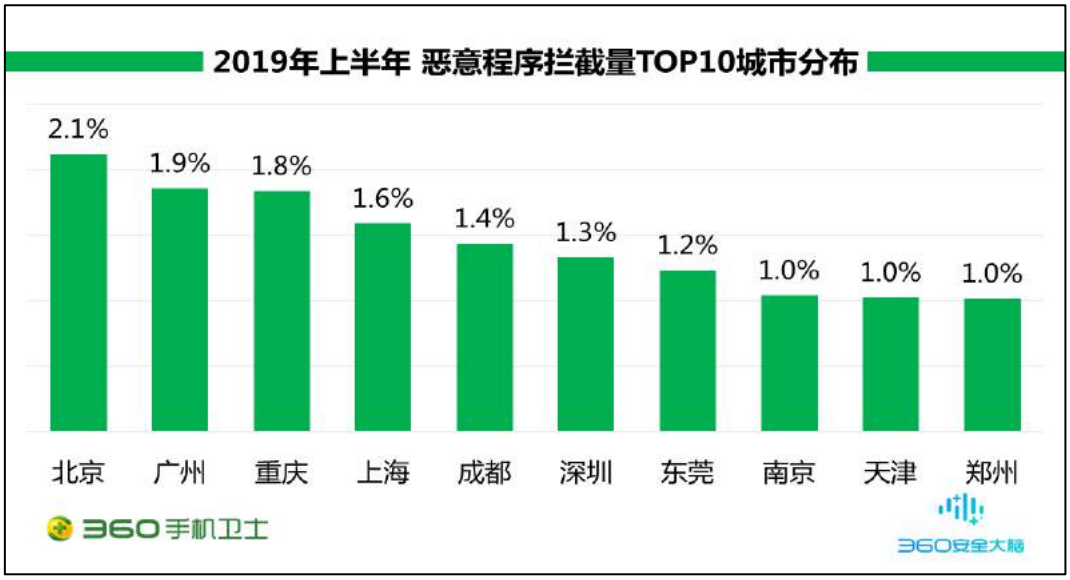


二、 恶意程序拦截量地域分布

2019 年上半年从省级分布来看，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 10.2%；其次为山东（7.6%）、河南（6.8%）、江苏（6.6%）、浙江（5.7%），此外河北、四川、安徽、云南、湖南的恶意程序拦截量也排在前列。



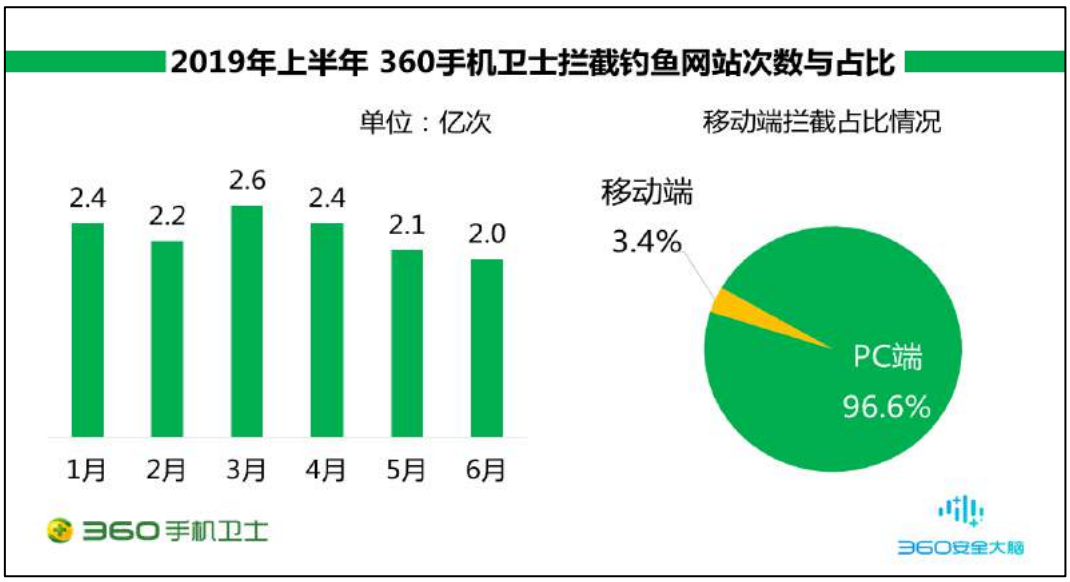
从城市分布来看，遭受手机恶意程序攻击最多的城市为北京市，占全国拦截量的 2.1%；其次为广州（1.9%）、重庆（1.8%）、上海（1.6%）、成都（1.4%），此外深圳、东莞、南京、天津、郑州的恶意程序拦截量也排在前列。


2019年上半年 恶意程序拦截量TOP10城市分布
2.1%
1.9%
1.8%
1.6%
1.4%
1.3%
1.2%
1.0%
1.0%
1.0%
北京
广州
重庆
上海
成都
深圳
东莞
南京
天津
郑州
360手机卫士
360安全大脑

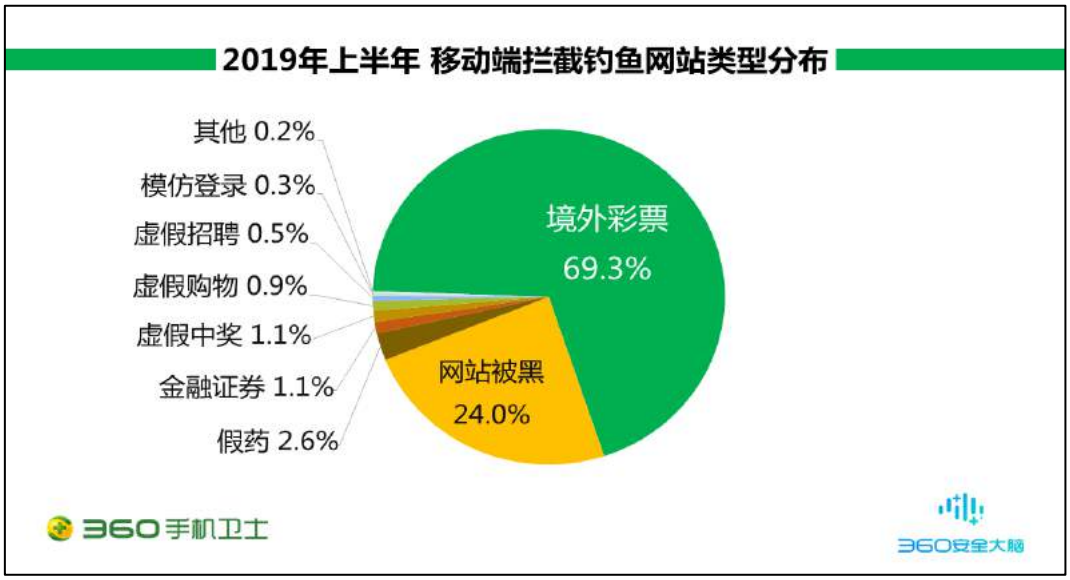
第二章 钓鱼网站

一、 移动端钓鱼网站拦截量及类型

2019 年上半年，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 404.2 亿次，同比 2018 年上半年（207.2 亿次）上升了 48.7%。其中，PC 端拦截量约为 390.4 亿次，占总拦截量的 96.6%，平均每日拦截量约 2.2 亿次；移动端拦截量约为 13.8 亿次，占总拦截量的 3.4%，平均每日拦截量约 760.1 万次。移动端钓鱼网站拦截次数及占比具体见下图：

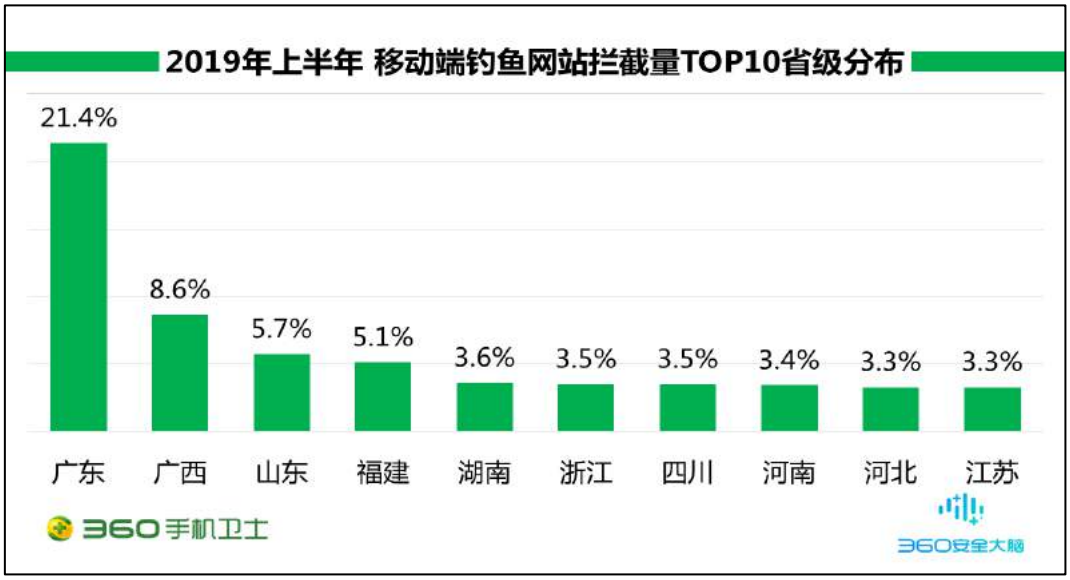


移动端拦截钓鱼网站类型主要为境外彩票，占比高达 69.3%；其次为网站被黑（24.0%）、假药（2.6%）、金融证券（1.1%）、虚假中奖（1.1%）、虚假购物（0.9%）、虚假招聘（0.5%）、模仿登陆（0.3%）等。具体分布如下图所示：

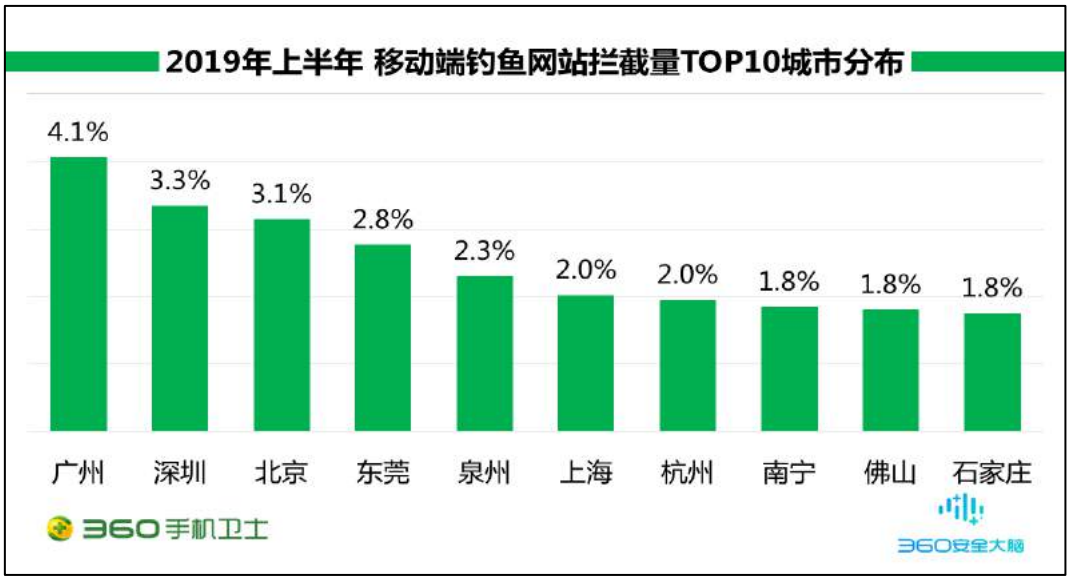


二、移动端钓鱼网站拦截量地域分布

2019 年上半年从省级分布来看，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 21.4%；其次为广西（8.6%）、山东（5.7%）、福建（5.1%）、湖南（3.6%），此外浙江、四川、河南、河北、江苏的钓鱼网站拦截量也排在前列。

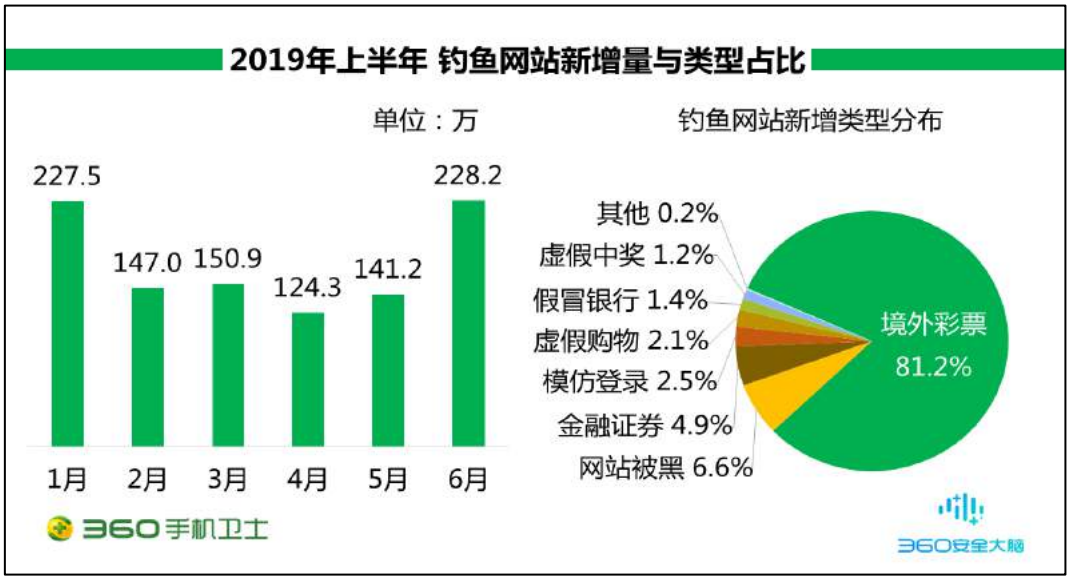


从城市分布来看，移动端拦截钓鱼网站最多的城市为广州市，占全国拦截量的 4.1%；其次为深圳（3.3%）、北京（3.1%）、东莞（2.8%）、泉州（2.3%），此外上海、杭州、南宁、佛山、石家庄的钓鱼网站拦截量也排在前列。

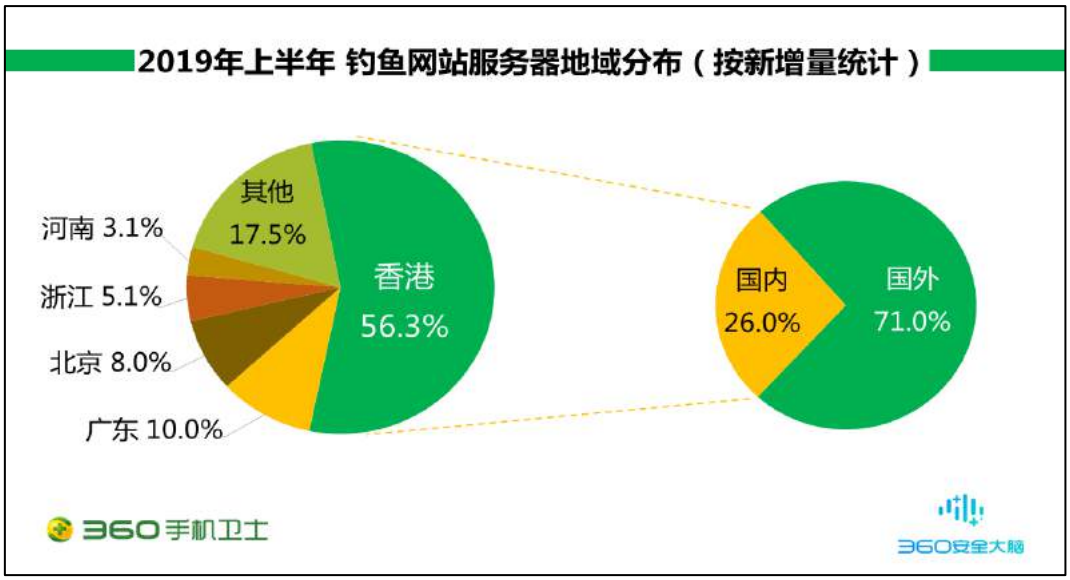


三、 钓鱼网站新增量与服务器地域分布

2019 年上半年，360 互联网安全中心共截获各类新增钓鱼网站 1019.2 万个，同比 2018 年上半年（1622.6 万个）下降了 37.2%，平均每天新增 5.6 万个。由于近几年打击钓鱼网站的力度加大，新增钓鱼网站数量大幅降低。其中，钓鱼网站新增类型主要为境外彩票类，占比高达 81.2%，属于新增钓鱼网站中的重点打击类型。



从新增钓鱼网站的服务器地域分布看，71.0%的钓鱼网站服务器位于国外，26.0%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 56.3%，居于首位，其次为广东（10.0%）、北京（8.0%）、浙江（5.1%）、河南（3.1%）等。

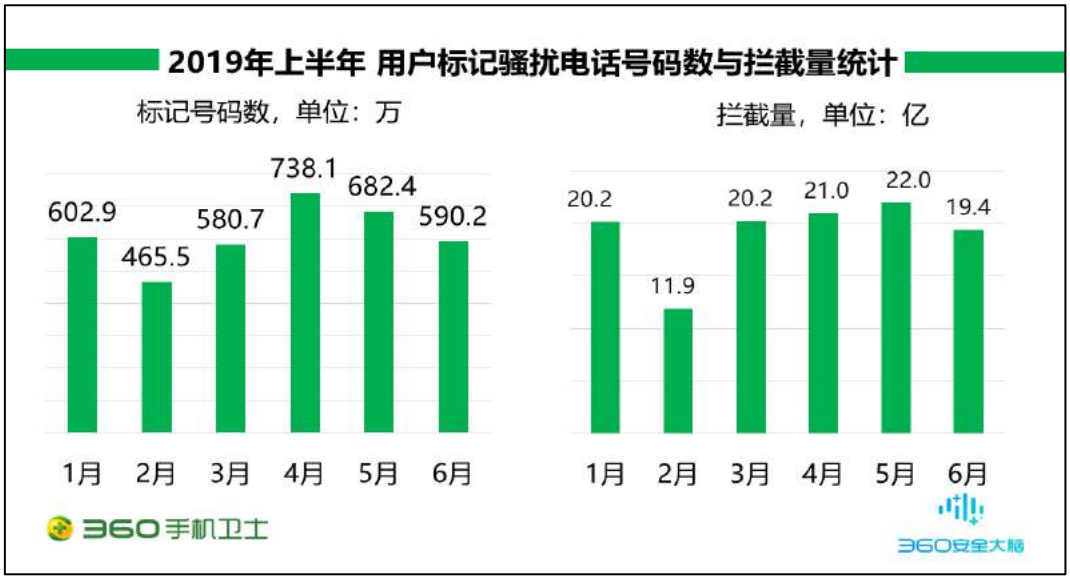


第三章 骚扰电话

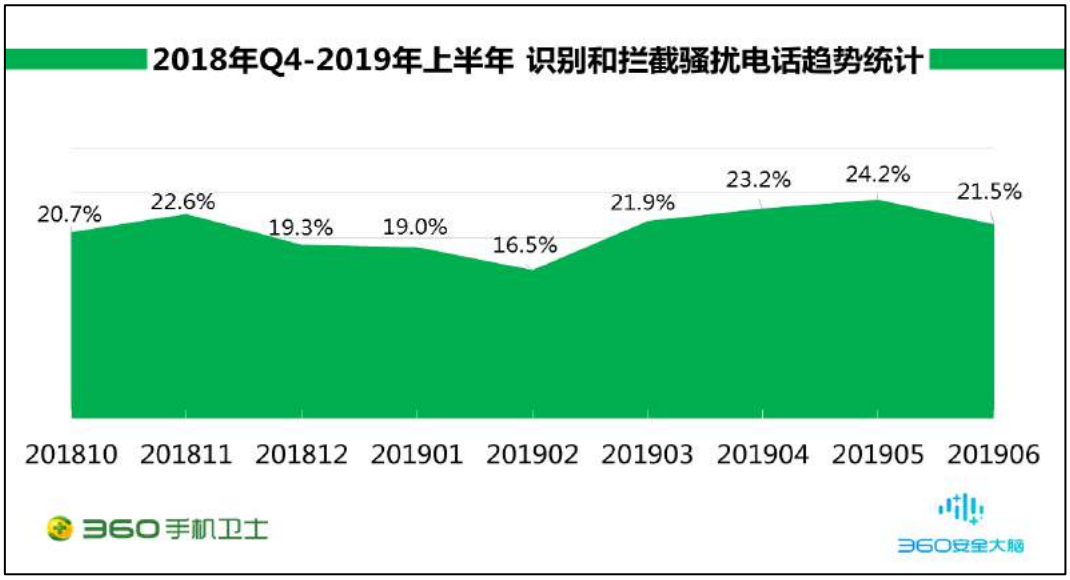
一、骚扰电话标记数与拦截量

2019 年上半年，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 3659.8 万个，平均每天标记约 20.2 万个。从标记号码总量上看，同比 2018 年上半年（2943.7 个）上升了 19.6%。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 114.8 亿次，平均每天识别和拦截骚扰电话约 0.6 亿次。

2019 年上半年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，在 4 月份达到峰值，后续骚扰号码数量呈逐渐回落趋势。

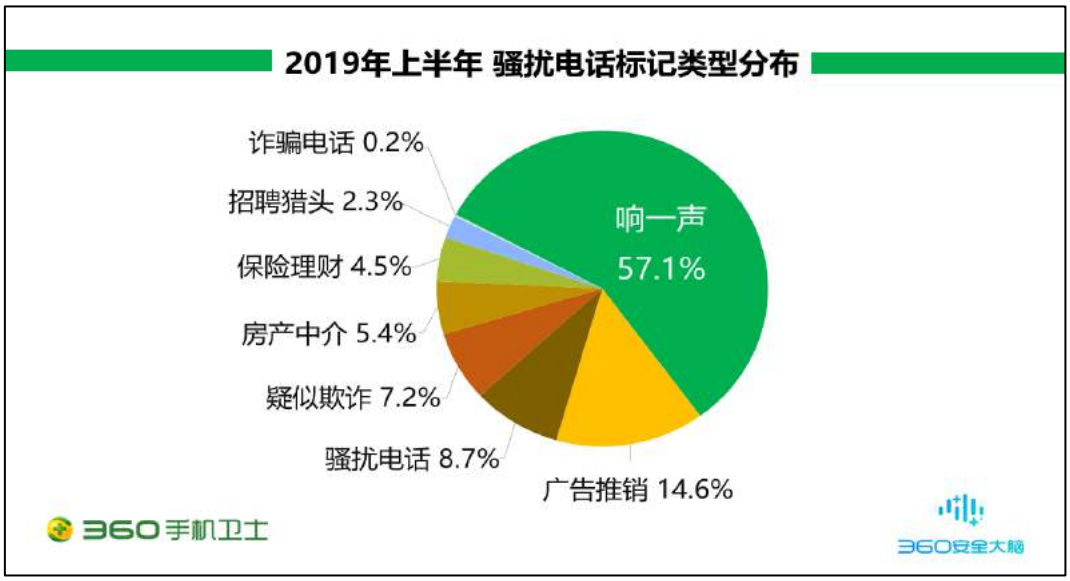


从下图 2018 年第四季度至 2019 年上半年 360 手机卫士识别和拦截骚扰电话趋势可见，临近年底骚扰电话拦截量呈逐渐降低趋势。2019 年 2 月份期间正值春节假期，骚扰电话拦截量最低。通过往年趋势可知，在春节期间，从事拨打骚扰电话的人员减少，从而导致骚扰电话的呼入量降低。2019 年 3 月份起，骚扰电话拦截量回升，并呈持续小幅增长态势。在 2019 年 6 月份时，骚扰电话拦截量回落。

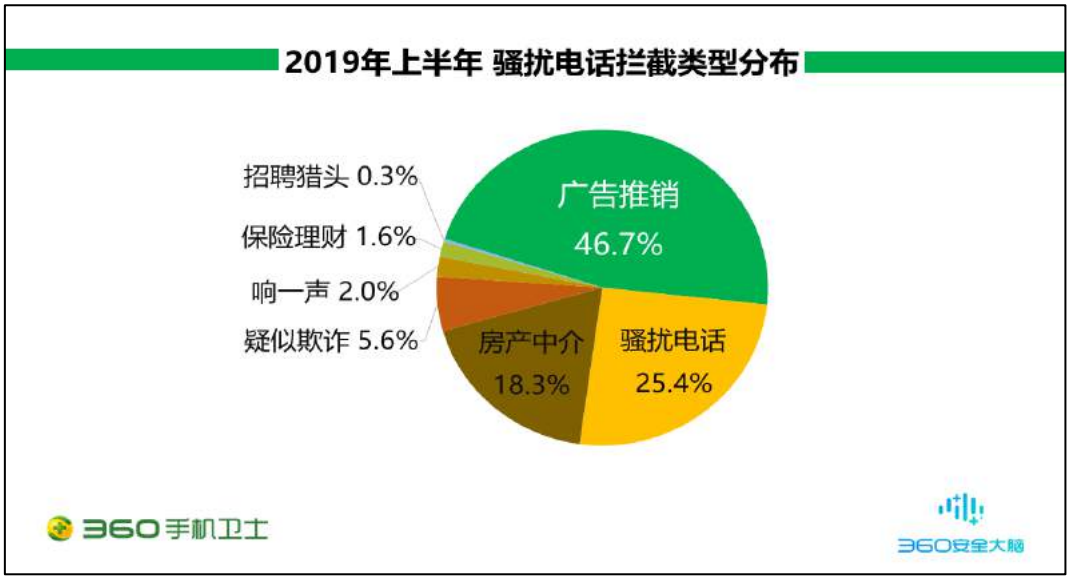


二、骚扰电话类型分布

综合 360 互联网安全中心 2019 年上半年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 57.1%的比例位居首位，其次为广告推销（14.6%）、骚扰电话（8.7%）、疑似欺诈（7.2%）、房产中介（5.4%）、保险理财（4.5%）、招聘猎头（2.3%）、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 46.7%的比例位居首位，其次为骚扰电话（25.4%）、房产中介（18.3%）、疑似欺诈（5.6%）、响一声（2.0%）、保险理财（1.6%）、招聘猎头（0.3%）。具体分布如下图所示：

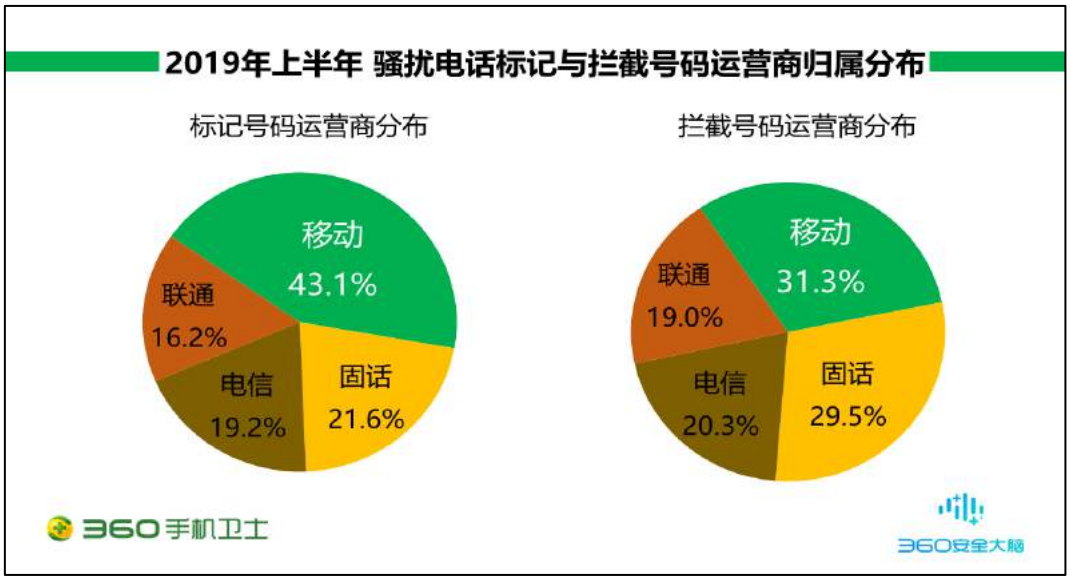


三、骚扰电话运营商归属分布

2019 年上半年，从用户标记的骚扰电话号码的运营商归属分布看，被标记的中国移动的手机号码最多，占比高达 43.1%；其次为固定电话（21.6%）、中国电信（19.2%）、中国联通（16.2%）。

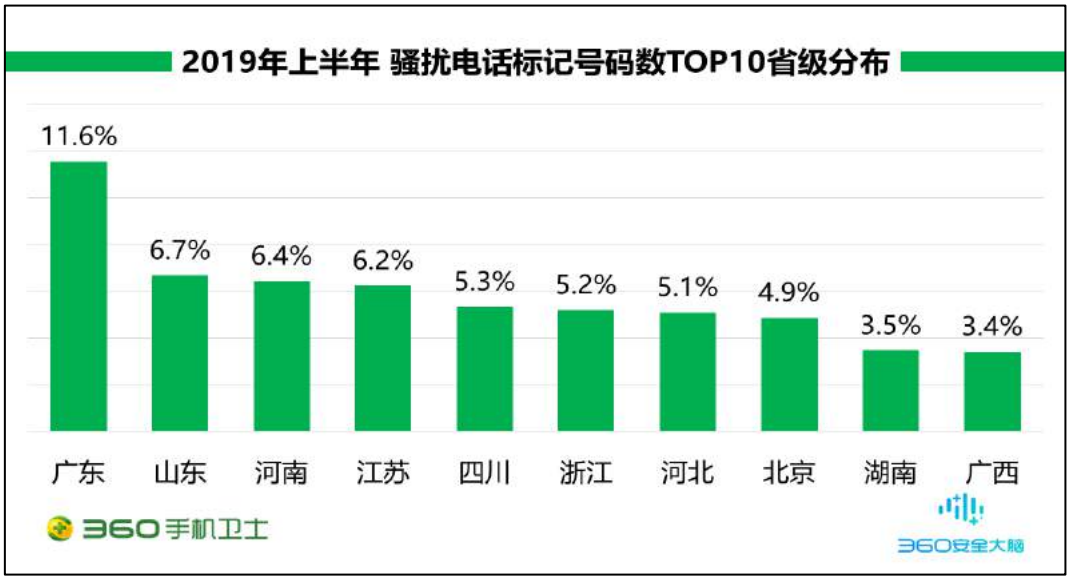
从骚扰电话拦截号码的运营商归属分布看，被拦截的中国移动的手机号码最多，占比高达 31.3%；其次为固定电话（29.5%）、中国电信（20.3%）、中国联通（19.0%）。

总体来看，骚扰电话中，个人手机号码为主要使用号源，用户标记与骚扰电话拦截号码都是最多的。其中，中国移动的手机号码骚扰情况较为突出，其次为固定电话。



四、 骚扰电话归属地分布

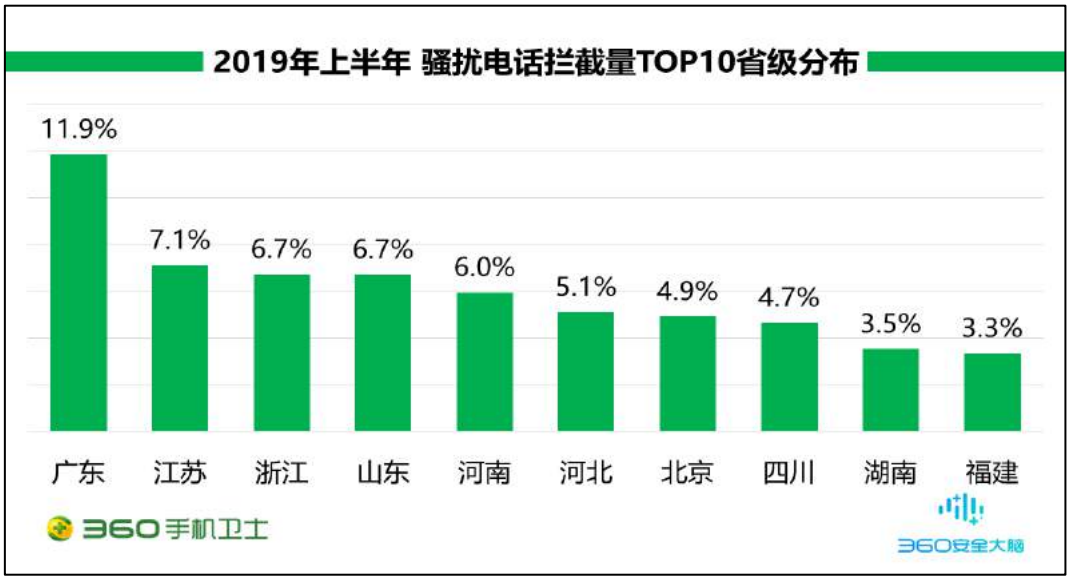
2019 年上半年，从各地骚扰电话标记号码个数上分析，广东省用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的 11.6%，其次是山东（6.7%）、河南（6.4%）、江苏（6.2%）、四川（5.3%），此外浙江、河北、北京、湖南、广西的骚扰电话标记号码个数也排在前列。



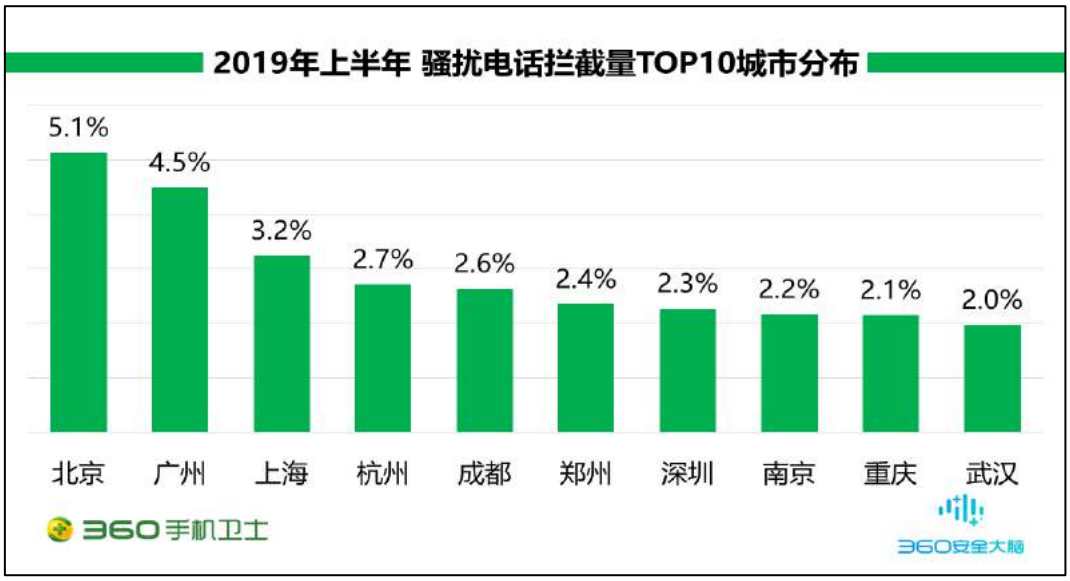
从城市分布来看，北京市用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的 4.9%，其次是广州（3.4%）、上海（3.1%）、深圳（2.2%）、重庆（2.1%），此外杭州、成都、石家庄、天津、武汉的骚扰电话标记号码个数也排在前列。

2019 年上半年，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 11.9%，其次是江苏（7.1%）、浙江（6.7%）、山东（6.7%）、河南（6.0%），

此外河北、北京、四川、湖南、福建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 6.1%，其次是广州（4.5%）、上海（3.2%）杭州（2.7%）、成都（2.6%），此外郑州、深圳、南京、重庆、武汉的骚扰电话拦截量也排在前列。

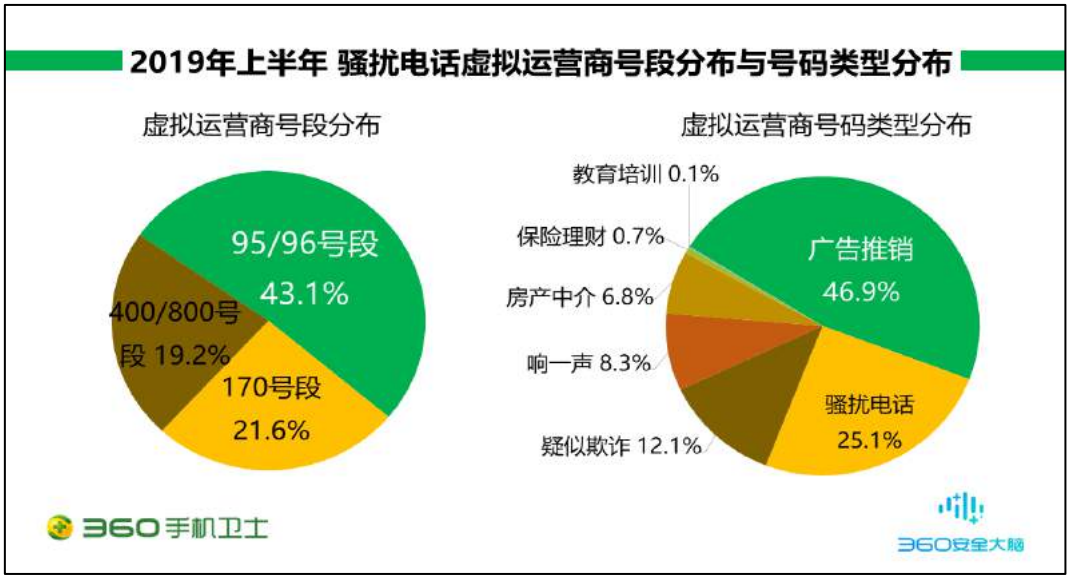


五、 骚扰电话虚拟运营商

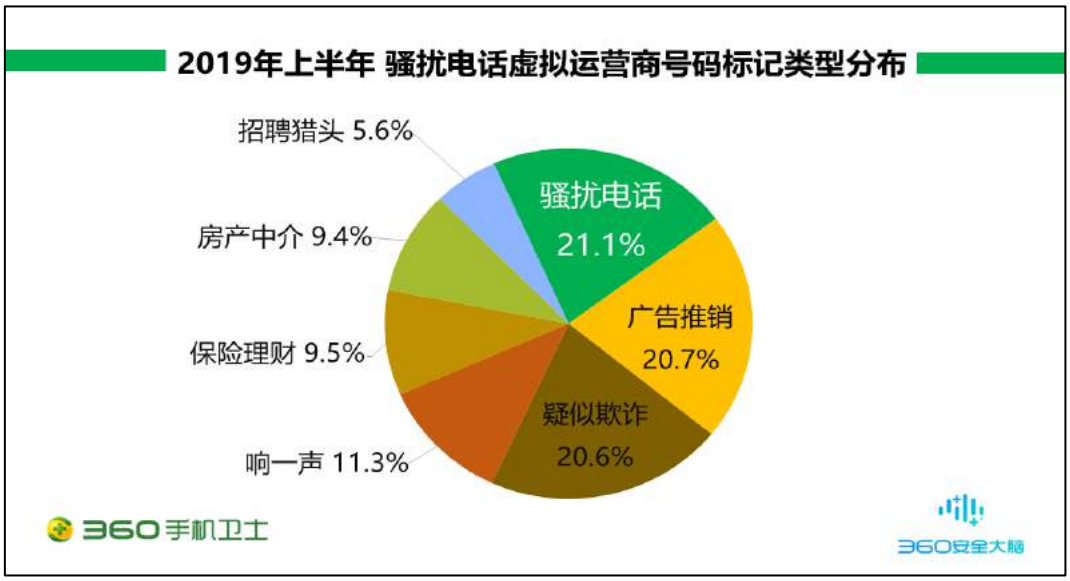
下图对虚拟运营商号段分布及号码类型分布分别进行了占比统计：

从骚扰电话号码拦截个数看，虚拟运营商号段中 95/96 号段拦截号码最多，占比达 43.1%；其次为 170 号段与 400/800 号段，分别占比 21.6%与 19.2%。

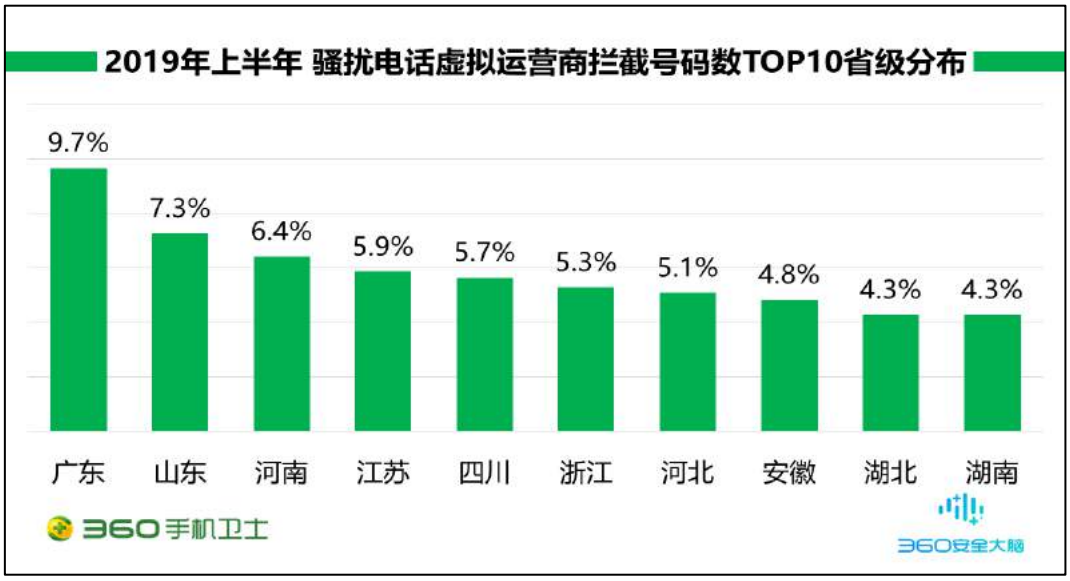
从骚扰电话号码类型来看，虚拟运营商号码中广告推销以 46.9%的比例位居首位，其次为骚扰电话（25.1%）、疑似欺诈（12.1%）、响一声（8.3%）、房产中介（6.8%）、保险理财（0.7%）、教育培训（0.1%）。



从骚扰电话虚拟运营商号码标记类型看，虚拟运营商号码中骚扰电话以 21.1%的比例位居首位，其次为广告推销（20.7%）、疑似欺诈（20.6%）、响一声（11.3%）、保险理财（9.5%）、房产中介（9.4%）、招聘猎头（5.6%）。



2019 年上半年，从各地骚扰电话虚拟运营商拦截号码数上分析，广东省用户接到骚扰电话的个数最多，占全国骚扰电话虚拟运营商拦截号码总数的 9.7%，其次是山东（7.3%）、河南（6.4%）、江苏（5.9%）、四川（5.7%），此外浙江、河北、安徽、湖北、湖南的骚扰电话虚拟运营商拦截号码数也排在前列。

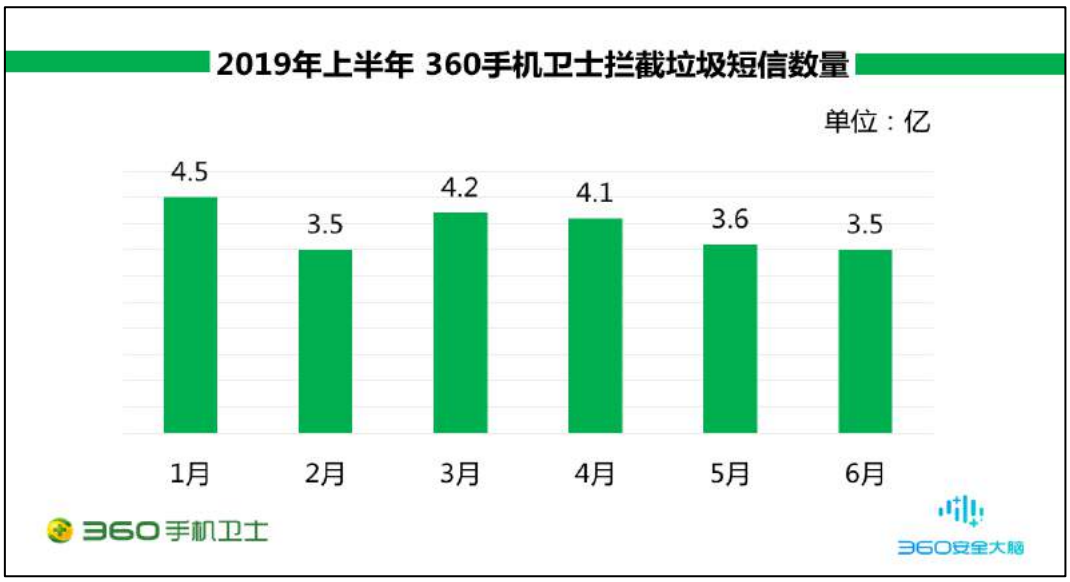


从城市分布来看，北京市用户接到的骚扰电话个数最多，占全国骚扰电话虚拟运营商拦截号码总数的 1.3%，其次是上海（1.2%）、广州（1.1%）、深圳（1.1%）、东莞（0.9%），此外佛山、苏州、杭州、成都、郑州的骚扰电话虚拟运营商拦截号码数也排在前列。

第四章 垃圾短信

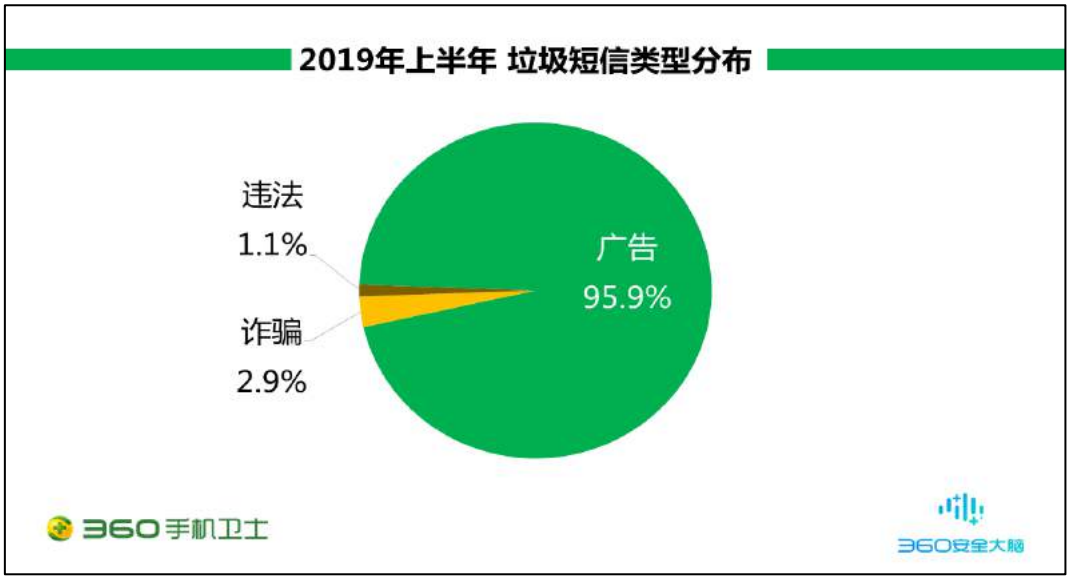
一、 垃圾短信拦截量

2019 年上半年，360 手机卫士共为全国用户拦截各类垃圾短信约 23.4 亿条，同比 2018 年上半年（48.7 亿条）下降了 52.0%，平均每日拦截垃圾短信约 1289.4 万条。由于上半年 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，自 4 月份起呈小幅下降趋势。



二、 垃圾短信类型分析

2019 年上半年垃圾短信的类型分布中，广告短信最多，占比为 95.9%，诈骗短信占比 2.9%，违法短信占比 1.1%。具体分布如下图所示：

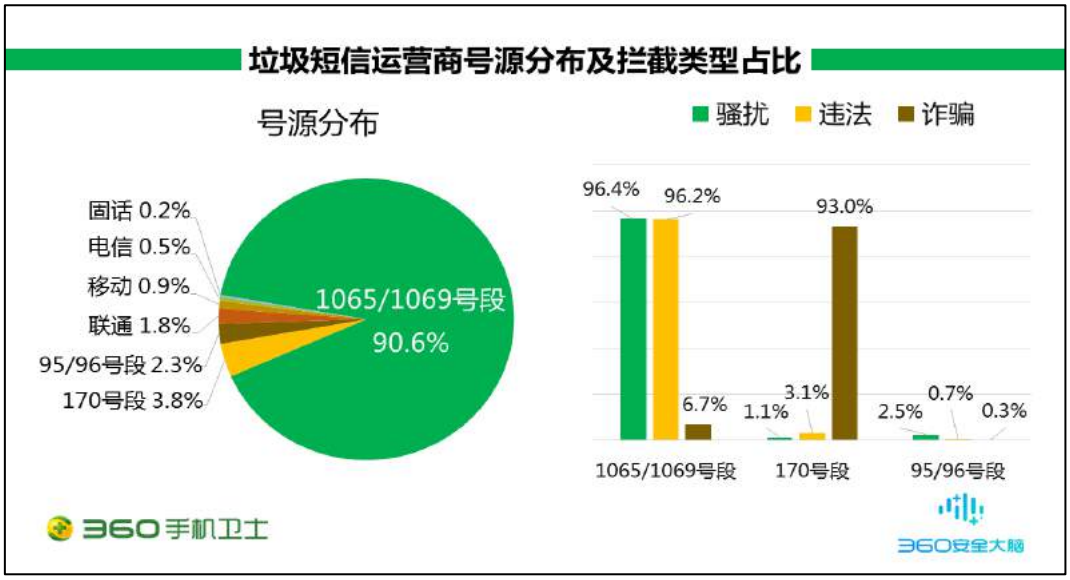


2019 年上半年，收到广告短信最多的是广东省，占全国广告短信拦截量的 8.9%，其次是浙江省（4.0%）与山东省（4.3%）；收到诈骗短信最多的是广东省，占全国诈骗短信拦截量的 18.7%，其次是湖南省（4.2%）与广西省（4.0%）；收到违法短信最多的是广东省，占全国违法短信拦截量的 7.1%，其次是山东省（2.7%）与河南省（2.5%）。

三、 垃圾短信运营商号源分布

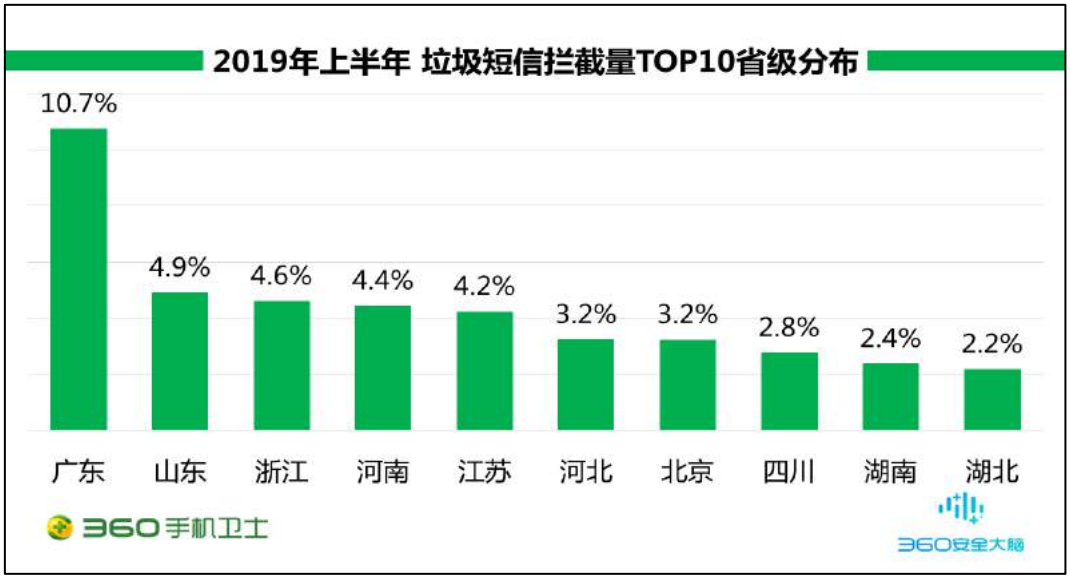
2019 年上半年，从垃圾短信发送者号码的运营商号源分布看，利用 1065/1069 渠道号发送垃圾短信的最多，占比高达 90.6%，其次为 170 号段（3.8%）与 95/96 号段（2.3%）。

从垃圾短信的拦截类型看，使用 1065/1069 渠道号发送骚扰短信和违法短信的最多，1065 号段主要是运营商自营业务号段，1069 是三网合一的企业实名制通道，此号段的号码具备号码整齐、格式统一、发送成本低的特点，利用此号段发送商家推广短信及广告已成为趋势；使用 170 号段发送诈骗短信的最多，由于 170 号段属于虚拟运营商，办理门槛低，监管制度不严，很多不法分子利用虚拟号批量发送诈骗短信，达到欺诈目的。

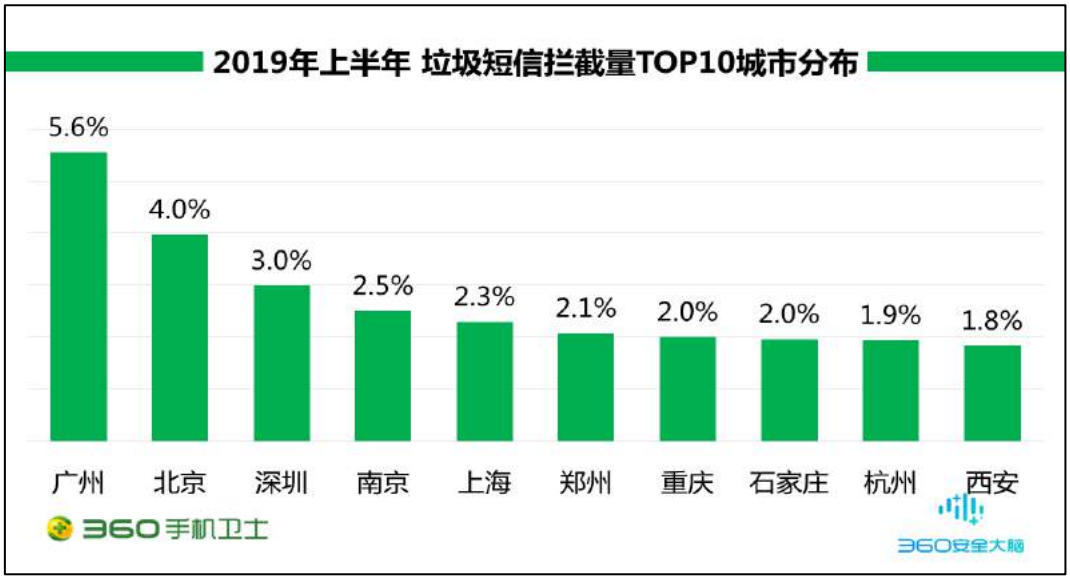


四、 垃圾短信拦截量地域分析

2019 年上半年，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 10.7%，其次是山东（4.9%）、浙江（4.6%）、河南（4.4%）、江苏（4.2%），此外河北、北京、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 5.6%，其次是北京（4.0%）、深圳（3.0%）、南京（2.5%）、上海（2.3%），此外郑州、重庆、石家庄、杭州、西安的垃圾短信拦截量也排在前列。


2019年上半年 垃圾短信拦截量TOP10城市分布
5.6%
4.0%
3.0%
2.5%
2.3%
2.1%
2.0%
2.0%
1.9%
1.8%
广州
北京
深圳
南京
上海
郑州
重庆
石家庄
杭州
西安
360手机卫士
360安全大脑

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。

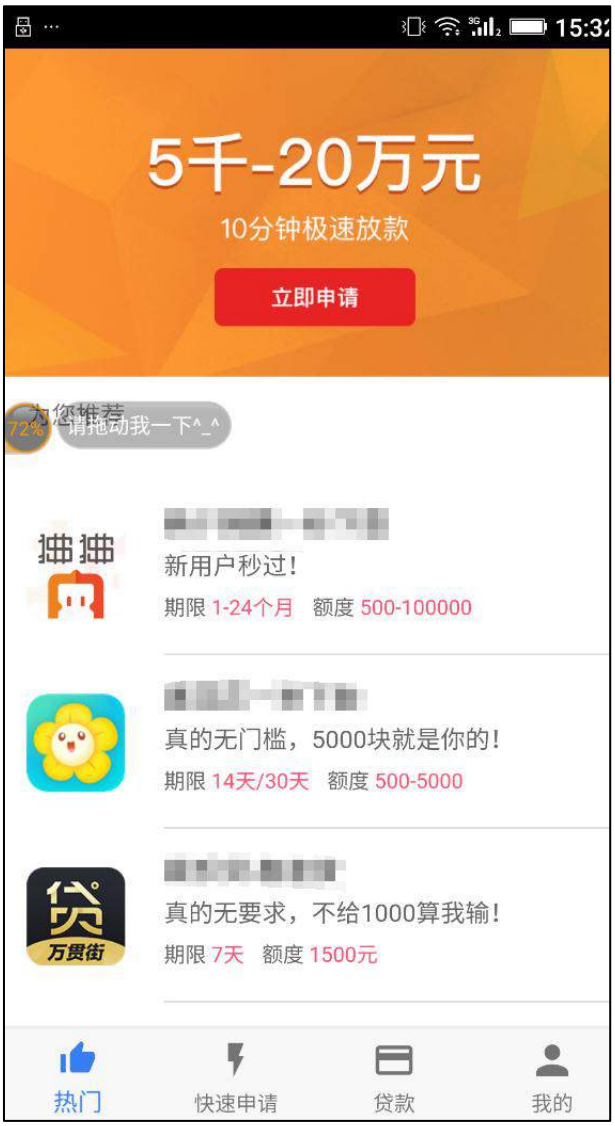


图 1:某“贷款中介”APP 首页

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。

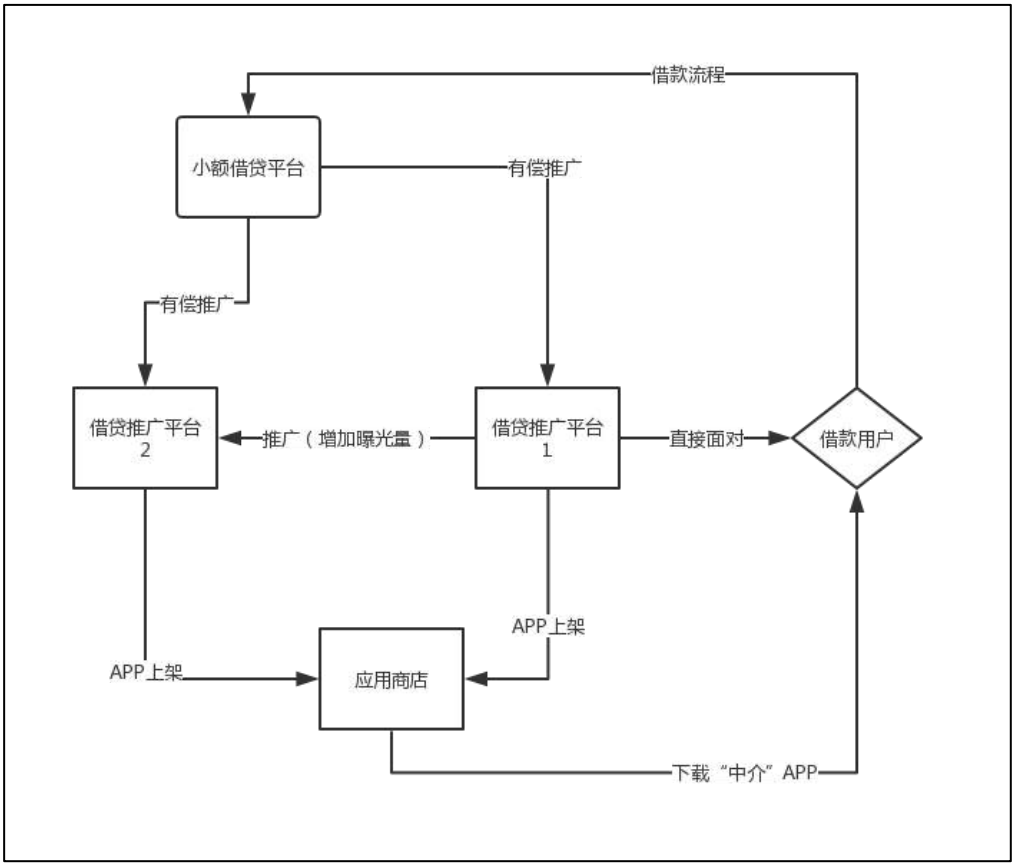


图 2:借贷 APP 推广平台利益链

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。

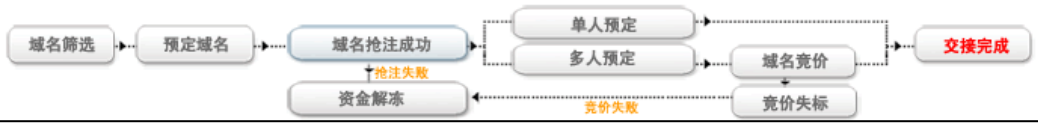
域名拍卖-域名购买-域名预定-注册域名-xz域名交易网

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
4G
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...
金币抵2%
包邮
¥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...
包邮
¥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
包邮
¥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 】
包邮
¥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	ic sky.cn	CP备1 1号-7	企业	其他	小渔	微信 QQ 360 备案查询	7	2016-10-31	2019-10-31
2	ac .cn	CP备19 6号-1	企业	腾讯云	广州 有限公司	微信 QQ 360 备案查询	5	2019-01-07	2020-01-07
3	jn ngxuan.cn	CP备180 2号-1	企业	阿里云	济南中 技术有限公司	微信 QQ 360 备案查询	11	2018-01-03	2020-01-03
4	u q.cn	ICP备190 4号-2	企业	腾讯云	广州 贸易有限公司	微信 QQ 360 备案查询	5	2019-01-07	2020-01-07
5	uiwengqi.cn	ICP备170 5号-1	企业	阿里云	智慧	微信 QQ 360 备案查询	12	2017-01-01	2020-01-01
6	i.cn	CP备190 号-2	企业	腾讯云	深圳 科技有限公司	微信 QQ 360 备案查询	5	2019-01-04	2020-01-04
7	z .cn	CP备190 号-2	企业	腾讯云	深圳 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	t nsi.cn	鄂 41号-1	社会团体	阿里云	白山寺	微信 QQ 360 备案查询	9	2017-01-03	2020-01-03
2	jn .cn	闽 47号-2	社会团体	其他	厦 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
m.com	1988元	-	阿里云	2015-12-23	2019-12-22	360 QQ	购买
ot.cn	2288元	企业-京	北京 公司 其他	2011-01-19	2020-01-19	360 QQ	购买
com.cn	2688元	企业-黄	双 限公司 其他	2005-01-19	2020-01-19	360 QQ	购买
nk.com	3688元	企业-苏	江 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。

三、代充黑灰产业分析

1. 代充黑灰产业现状

2019 年上半年，各大知名电商、视频、社交等平台发生多起网络黑灰产事件，平台方被黑灰产通过漏洞 “盗取”大量平台资源，损失大量资金。某音乐平台打击违法违规获取音乐币的事件，将代充产业重新暴露在人们的眼前。每次的打击事件都是对黑灰产行业的一次整顿，但也意味着黑灰产行业将再次升级。

代充黑灰产业，指的是没有取得官方授权却通过电商、社交等渠道售卖远低于官方价格的网络资源。这些代充资源来源不明，稳定性较差，在获取资源及售卖资源的过程存在着欺诈、盗用等各式各样的问题。代充资源不仅损害了平台厂商的合法权益，也损害了花钱购买资源的用户的合理使用权益。代充黑灰产业经过多年的发展，已经从“单兵”作战，发展成云平台、“集团”式作战。盗取的资源及产生的影响力也越来越大。

2. 代充黑灰产业演进

1） 网络安全行业不健全时代

在互联网行业发展早期，互联网普及率不高，居民宽带多采用电话线拨号的方式，网速较慢，因此网民多通过网吧集中式上网。随着计算机的普及，黑灰产行业以爆发态势持续发展，出现了众多的黑客培训网校、批量传播盗号、远控、扫肉鸡教程，同时批量产出木马、免杀、洗号等工具。黑灰产学习难度低，教程和工具获取容易，于是大量的计算机被植入木马盗号程序，大量的 QQ 账号、Q 币、游戏账号、宽带账号被盗取。

黑灰产资源获取方式：

盗号，洗号，实现代充：黑灰产利用灰鸽子，阿里大盗等木马盗取宽带账号、QQ 账号（Q 币）、游戏装备。将盗取的资源，通过扫码工具查询账户 Q 币情况、游戏装备情况，将可利用的资源统一放在一个文本文件（行业称为信封）中，将信封根据预估价值出售给资源出售平台。一旦有人购买资源，出售平台通过 QQ 号 Q 币代充业务或宽带虚拟商品充值业务，为需求方代充各式各样的会员服务。

下图为盗号软件、QQ 信封截图。这些截图资料来自互联网：

未实名的手机卡实现代充：在互联网发展早期，手机号实名制不完善。黑灰产行业购入了大量的手机号码。通过这些号码购买 Q 币，各类会员包月服务。由于运营商与平台交易周期存在时间差，黑灰产利用这些手机号开通的服务，被发现并封杀的周期晚于出售商品的时间。

资源售卖方式：

黑灰产盗号人员将批量清洗后的资源存放在文本中生成信封，售卖给资源售卖方。售卖方通过 QQ 群，电商平台，黑灰产社区、游戏频道等方式售卖给用户。

资源购买方法：

用户通过好友推荐，电商平台，游戏频道了解到资源售卖方，联系对方后，将需充值的账户或账户及密码提供给售卖方，通过向对方提供手机话费充值卡密，银行转账等方式向对方付款，再由对方完成账户充值流程。

存在的风险：

黑灰产业获取资源的方式不合法，因此产品的稳定性非常差。用户购买代充服务后，由于用于给用户充值的手机号随时会被查封，用于给用户充值业务的 Q 币所在账号也存在被举报的情况，用户购买的服务常常失效。例如，用户购买了某平台“永久”会员账号，可能只使用了几天，会员服务就被关停。

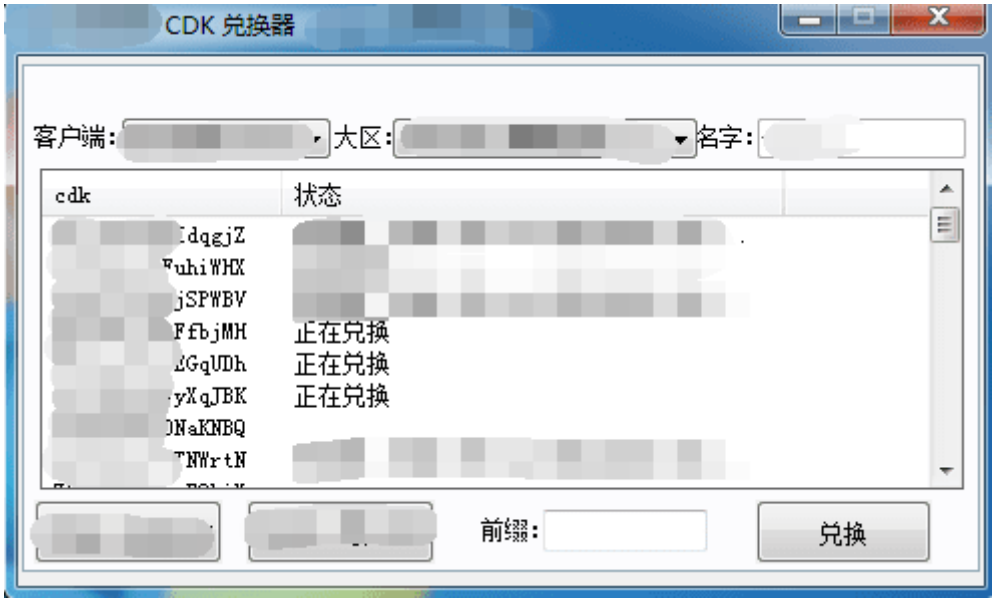
2） 安全行业进入云查杀时代

随着安全行业进入云查杀时代，病毒样本的免杀能力减弱，制作免杀木马的难度增大。各大社交平台，也增加对病毒样本传播的识别，木马病毒传播能力减弱。同时，随着互联网行业的发展，互联网行业的运营活动增多，互联网进入流量时代。代充黑灰行业也开始转型，利用平台活动，平台漏洞，批量薅取平台“羊毛”，将获取的平台资源，通过代充渠道变现。

黑灰产资源获取方式：

电脑工具批量获取活动资源。当互联网企业开展促销推送等活动时，黑灰产利用各种“羊毛”工具批量刷取推广活动的羊毛。如登录社交账号即可获得活动赠送的礼品，黑灰产使用工具批量登录社交账号，批量获取兑换码（CDKEY），部分兑换码由于不限制使用账户，获得的批量兑换码，可以使用批量兑换工具兑换给同一个账户。

下图展示的使用批量兑换工具兑换 CDK：



云控机刷时代：随着移动互联网的发展，越来越多的促销推广等活动在移动端传播，传统的 PC 设备及开设虚拟机的方式，已无法满足黑灰产的需求。黑灰产开始使用大量的手机设备，制作云控平台，设置指定的脚本，批量登录，领取厂商活动的资源。

如下图，展示在使用手机号注册并登录指定的平台，可获得相应的互联网企业的会员周卡：

平台漏洞，薅取平台羊毛：随着移动互联网的普及，推广、促销等活动成了互联网厂商增加用户量，提高转化率的重要手段，但在设置活动的过程中，存在活动风控机制、安全代码检测不完善的情况。黑灰产业利用平台存在的漏洞，发起批量获取平台资源的行为。

诈骗代充：随着移动支付的发展，用户越来越习惯使用移动支付产品进行支付。诈骗产业苦于骗取的资金无法套现，借助移动支付产品的便捷性，结合代充互联网产业实现了成功套现。如虚假电商刷单产业，诈骗产业在实施诈骗的过程中，诱导用户购买虚拟充值卡，套取用户购买的充值卡账号及密码。诈骗产业将获取的充值卡密，出售给黑灰产代充平台，通过代充平台售卖的资金实现套现。

资源售卖方式

代充黑灰产业早期通过传统电商平台售卖代充资源，如平台会员，平台币，游戏点券。后期随着传统电商平台的风控提升，电商平台根据关键词清理了一批商家。这些平台售卖人员转而通过自建站及内部朋友圈的方式，传播并售卖资源。

资源购买方法：

用户在获取资源售卖平台后，在网站选择商品，如爱奇艺月卡，饿了么会员，迅雷白金会员，滴滴代金券。填写需充值的账号，有些账户（百度超级会员，爱奇艺）需要提供验证码，关闭密码登录保护。使用支付宝/微信扫码支付后，联系平台 QQ/微信客服确认订单。获得 CDKEY 后，使用 CDKEY 在平台自己充值激活。

如下图展示的某资源售卖平台，购买商品需填写的选项：

3. 应对代充黑灰产业方式

互联网行业在不断的发展，从 PC 互联网时代到移动互联网时代。代充黑灰产业也在不断的发展，从 PC 互联网时代盗取个人资源售卖转型到移动互联网时代盗取平台资源售卖。随着黑灰产行业成长的“集团”化，人员分工的“链接”化，攻防对抗将是互联网企业与黑灰产“企业”不断厮杀成长的一场持久战。作为互联网企业，面对黑灰产的厮杀该如何应对？

1） 借助安全厂商能力，借力打力

目前安全厂商，已建立完善的黑灰产威胁情报风控体系。包含黑灰产情报、黑灰产数据、黑灰产行为、黑灰产溯源追踪。反欺诈情报包含：“黑灰产动向情报、黑灰产手法情报、黑灰产工具情报等” ，黑灰产数据包含：“黑灰手机号、黑灰 IP 等”，黑灰产行为包含：“攻击模型、接口利用、流量风控等”，溯源追踪包含：“大数据关联、行为轨迹等”。黑灰产业的发展离不开手机号、IP 等基础资源，对这些基础资源有较强的依懒性。互联网厂商借助安全厂商已具备的安全能力，可以了解关联产业的黑灰产动向、黑灰产手法，做好提前预警，在黑灰产行动前预警，行动时拦截。

2） 完善自身安全风控能力

建立企业蜜罐体系

黑灰产在进行攻击或者批量薅取活动羊毛时，会使用大量的手机号、IP 等基础资源，企业通过建立蜜罐体系，当黑灰产行动时，企业及时发现风险行为，同时还原出攻击的场景，对涉及的黑灰手机号、IP 等基础资源进行关联性围堵。

建立风控体系

建立风控体系，从感知风险到控制风险。在建立风控体系时，了解企业高风险的业务，预判可能产生的风险，判断出企业现有储备力量能处理的抗风险能力。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，及时调整自身的风控模型与机制。实现从感知风险到控制风险。

第六章 手机诈骗形势

一、报案数量与类型

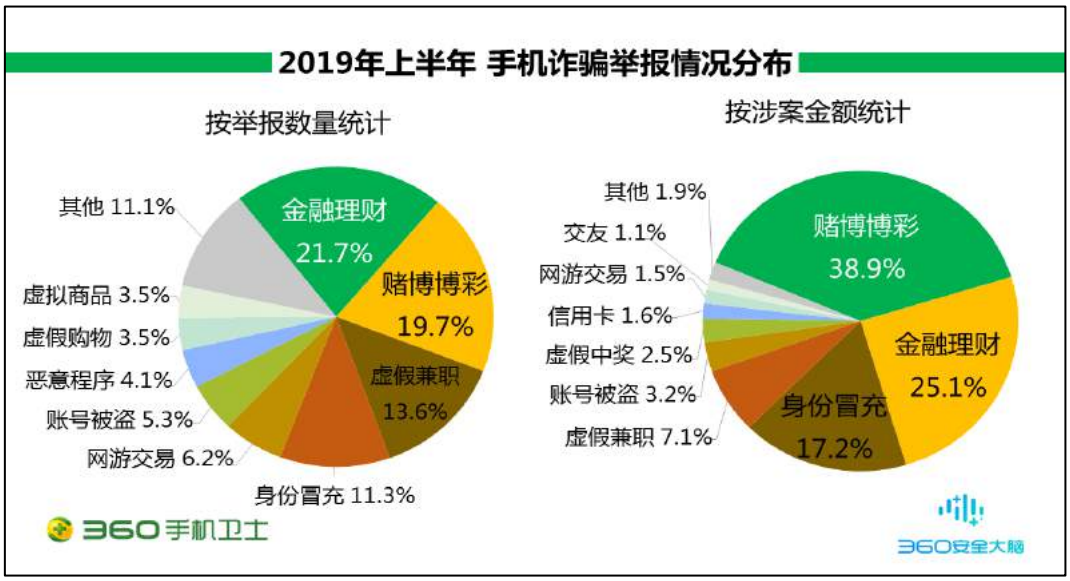
2019 年上半年 360 手机先赔共接到手机诈骗举报 2508 起。其中诈骗申请为 1095 起，涉案总金额高达 638.0 万元，人均损失 5826 元。

在所有诈骗申请中，金融理财占比最高，为 22.7%；其次是赌博博彩（19.7%）、虚假兼职（13.6%）、身份冒充（11.3%）、网游交易（6.2%）等。

从涉案总金额来看，赌博博彩类诈骗总金额最高，达 248.0 万元，占比 38.9%；其次是金融理财诈骗，涉案总金额 160.1 万元，占比 25.1%；身份冒充诈骗排第三，涉案总金额为 109.6 万元，占比 17.2%。

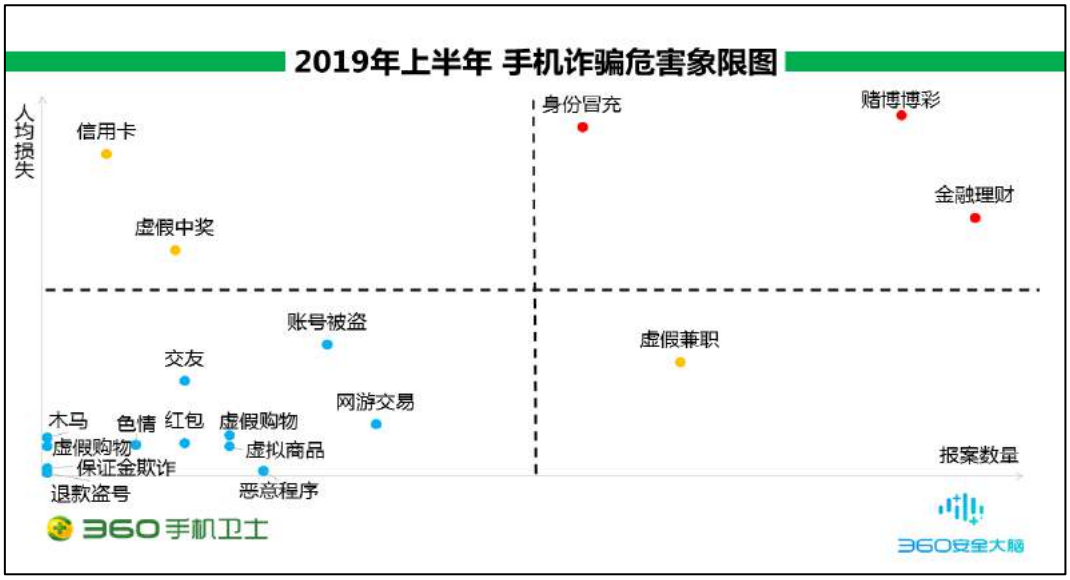
从人均损失来看，赌博博彩诈骗人均损失最高，为 11481 元；其次是身份冒充诈骗为 8840 元，信用卡诈骗为 8092 元。

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：



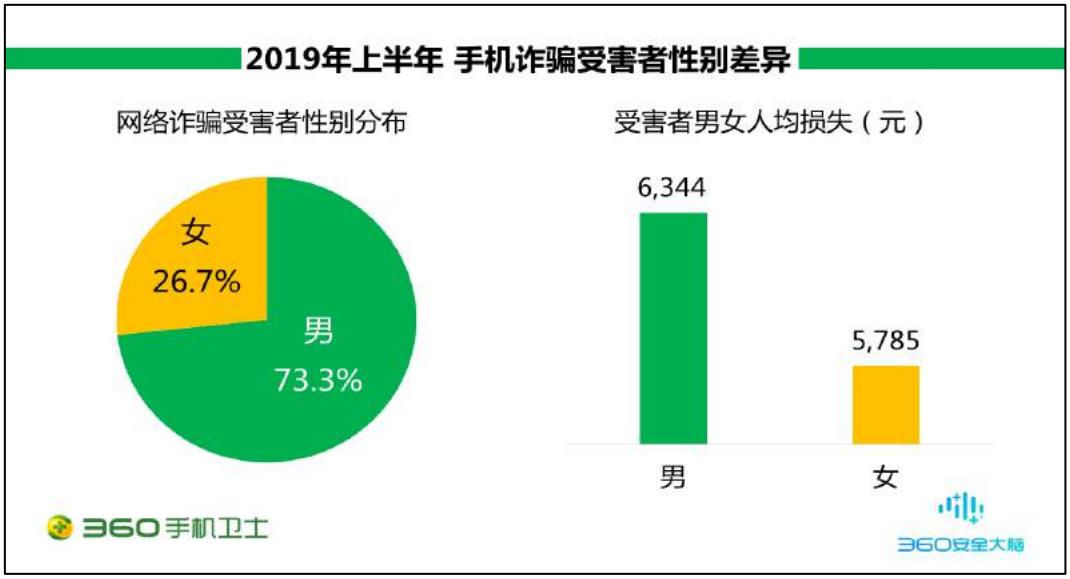
下图给出了不同类型的手机诈骗在人均损失和举报数量的象限图。从图中可见，赌博博彩、身份冒充、金融理财属于高危诈骗类型，受害人数较多且人均损失高。

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。虚假中奖类型同样受害人数少，但人均损失较高，此类诈骗主要利用虚假中奖借口，要求用户缴纳中奖保证金，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。

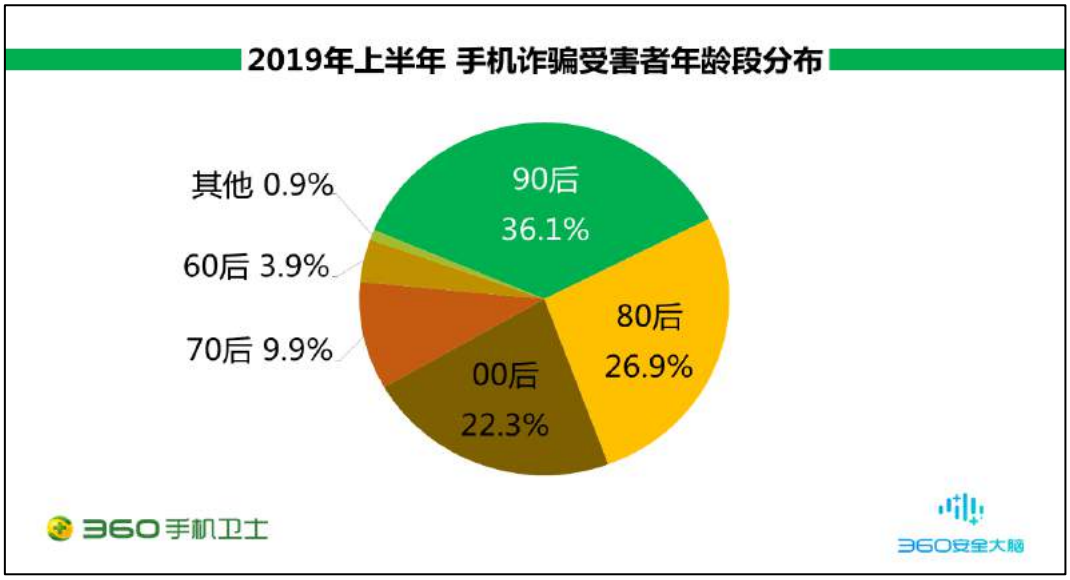


二、受害者性别与年龄

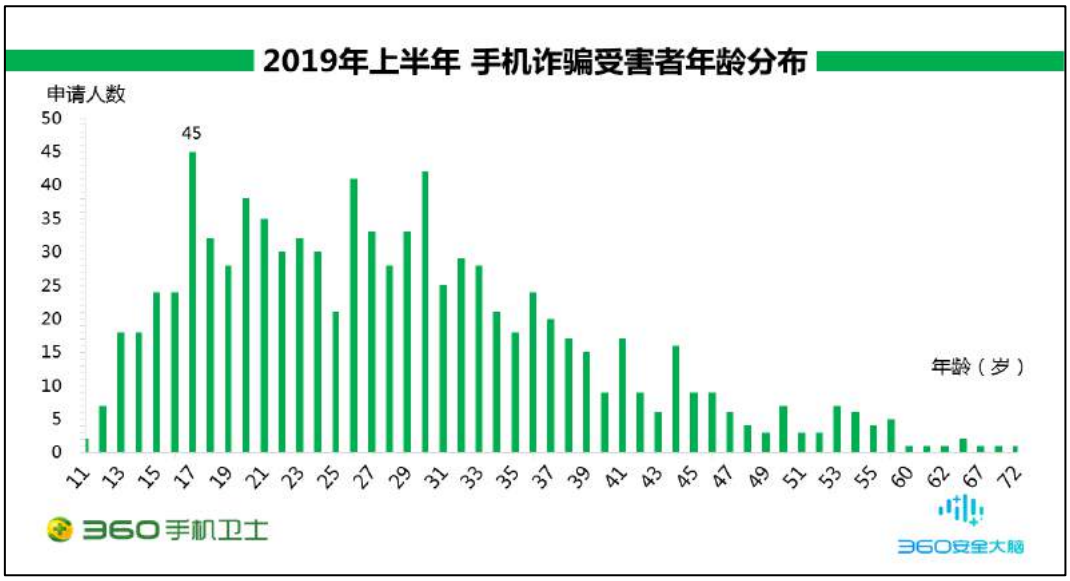
从举报用户的性别差异来看，男性受害者占 73.3%，女性占 26.7%，男性受害者占比高于女性。从人均损失来看，男性为 6344 元，女性为 5785 元，男性受害者人均损失同样高于女性。



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 36.1%；其次是 80 后占比为 26.9%，00 后占比为 22.3%，70 后占比 9.9%，60 后占比为 3.9%，其他年龄段占 0.9%。如图分布，2019 年上半年中，90 后为手机诈骗主要针对人群。

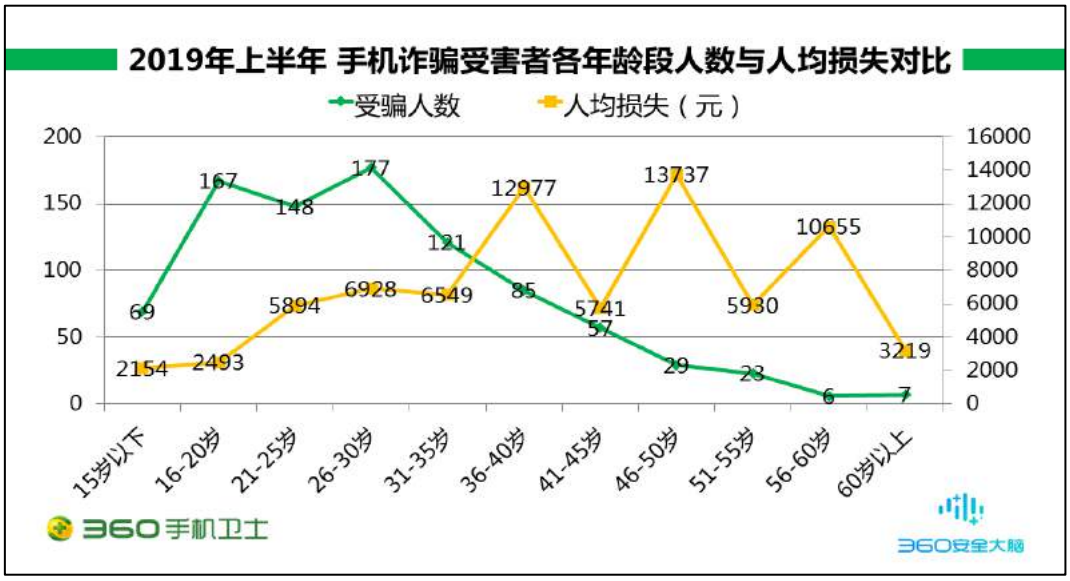


而从具体年龄上来看，16 岁至 20 岁的人群依然是手机诈骗受害者最为集中的年龄段，占所有手机诈骗受害者的 26.5%，其中赌博博彩类型受骗反馈较多。由于这个年龄段用户对于外界事物真实性判断能力较弱，无法对网络游戏平台合法性进行判断，在日常中使用手机交友的情况居多，对陌生人防范意识不强，若被引导至不合规平台进行充值游戏，极易遭受财产损失。其次为虚假兼职诈骗，由于这个年龄段用户暂未步入社会，无固定收入来源，网络兼职成为了课余时间赚取零花钱的主要方式，面对网络中所充斥的各种兼职广告，这类用户无法针对其真实性作出准确判断，极易遭到兼职诈骗。



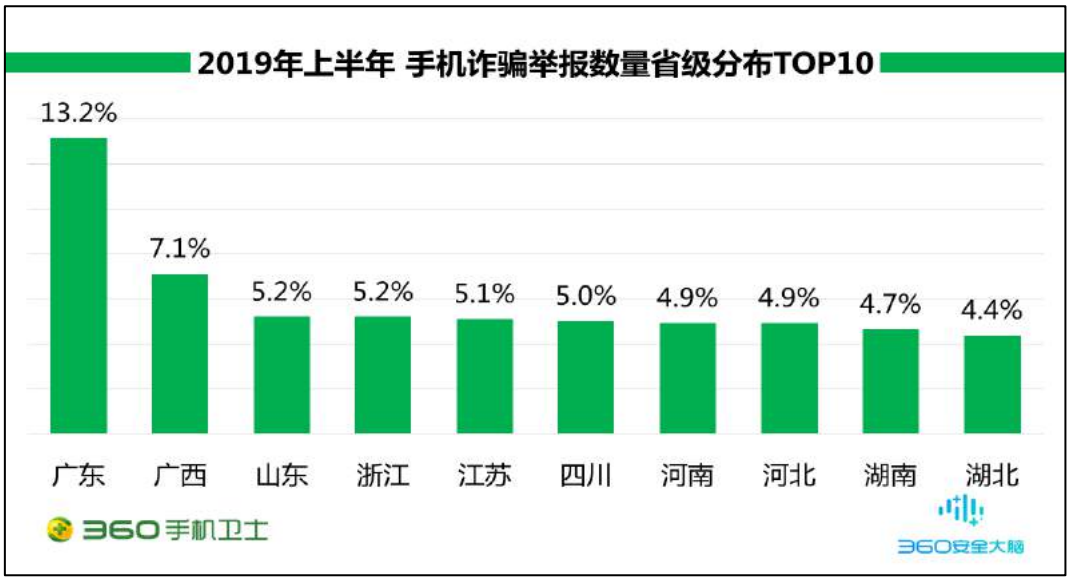
下图给出了手机诈骗受害者年龄段人数与人均损失的对比，从图中可以看出，随着年龄的增长，受害者人均损失总体上也在增长。15-20 岁之间的用户，是上网的主力人群，被骗的人数虽多，但由于年轻人经济能力有限，被骗平均金额相对较少。30 岁以后的受害者，年龄越大，经济能力也越强，虽然上网的人群、时间在减少，但被骗平均金额迅速增长，超过

了 13737 元。

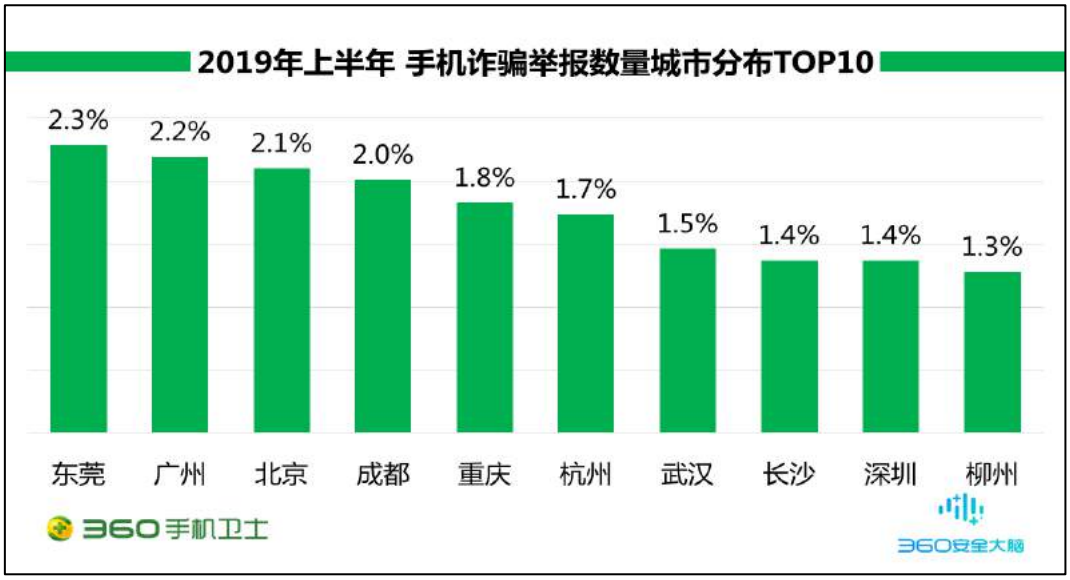


三、 受害者地域分布

2019 年上半年，从各地区手机诈骗的举报情况来看，广东（13.2%）、广西（7.1%）、山东（5.2%）、浙江（5.2%）、江苏（5.1%）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 35.8%。下图给出了 2019 年上半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，东莞（2.3%）、广州（2.2%）、北京（2.1%）、成都（2.0%）、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 10.4%。下图给出了 2019 年上半年手机诈骗举报数量最多的 10 个城市：

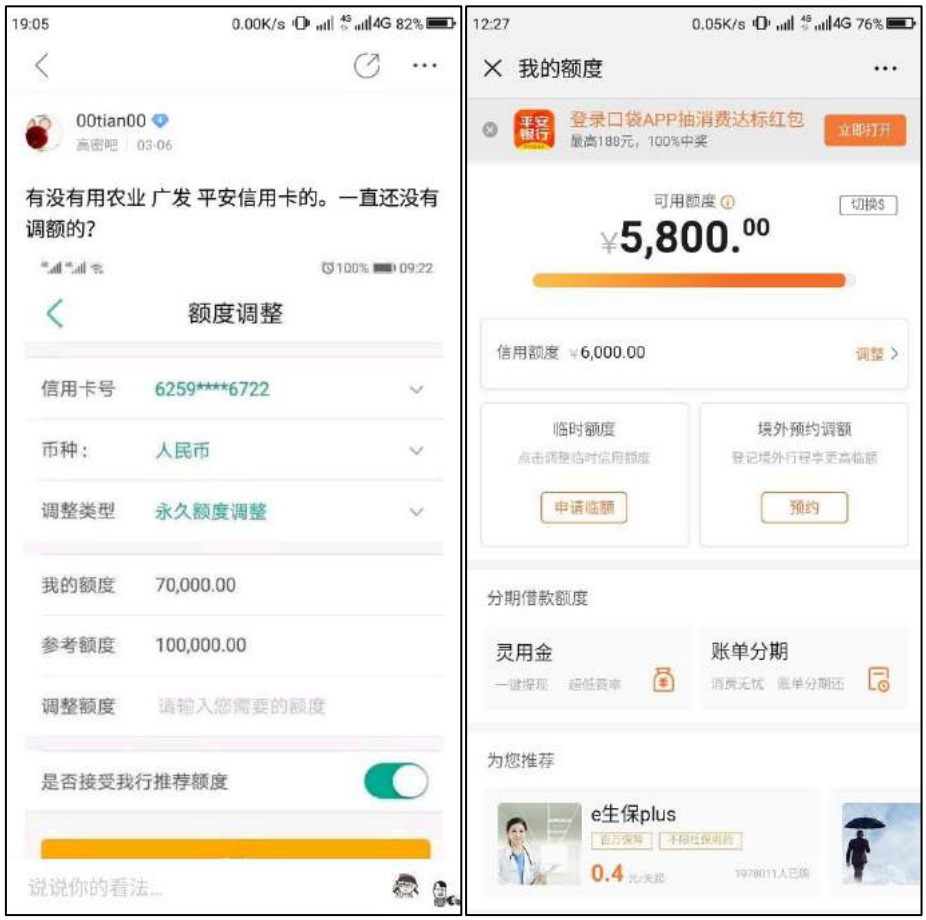

2019年上半年 手机诈骗举报数量城市分布TOP10
2.3%
2.2%
2.1%
2.0%
1.8%
1.7%
1.5%
1.4%
1.4%
1.3%
东莞
广州
北京
成都
重庆
杭州
武汉
长沙
深圳
柳州
360手机卫士
360安全大脑

第七章　典型案例

一、信用卡提额诈骗

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。

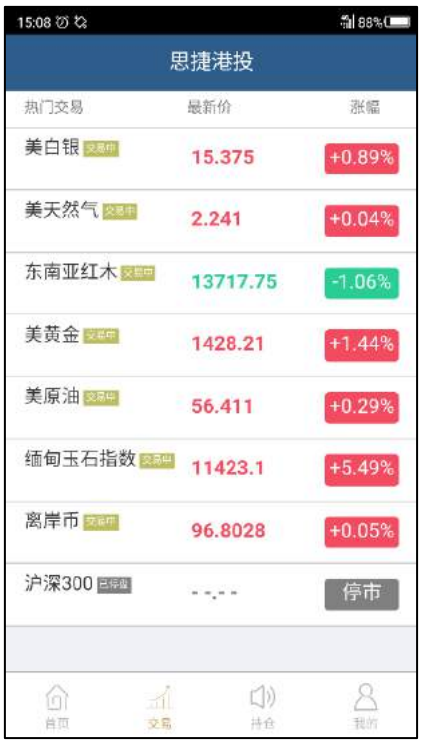
防骗提示

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。

二、 交友理财诈骗

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

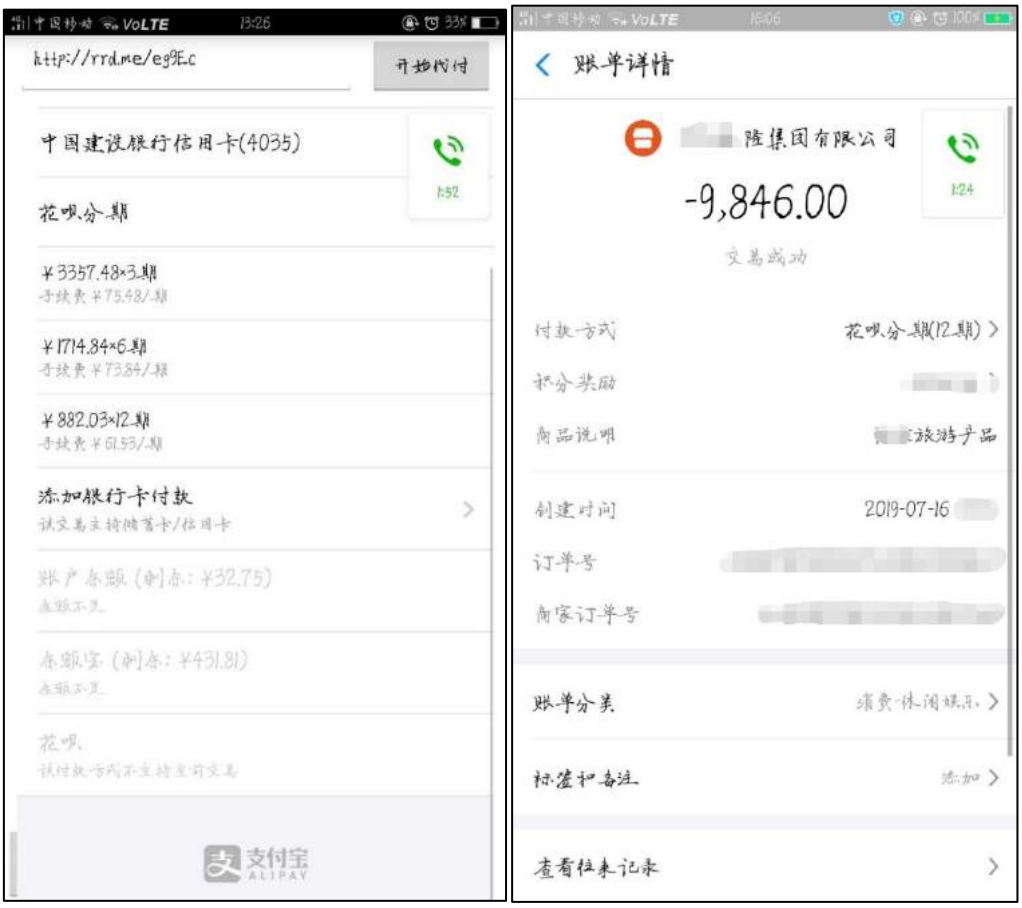
这些“养猪”的屠夫，其实离我们并不遥远，每一个突然找上门的“陌生人”，都有可能是骗子。网络交友千万条，绝不掏钱第一条！

三、明明付款“0 元”，怎么就背上了千元贷款？

案例回顾

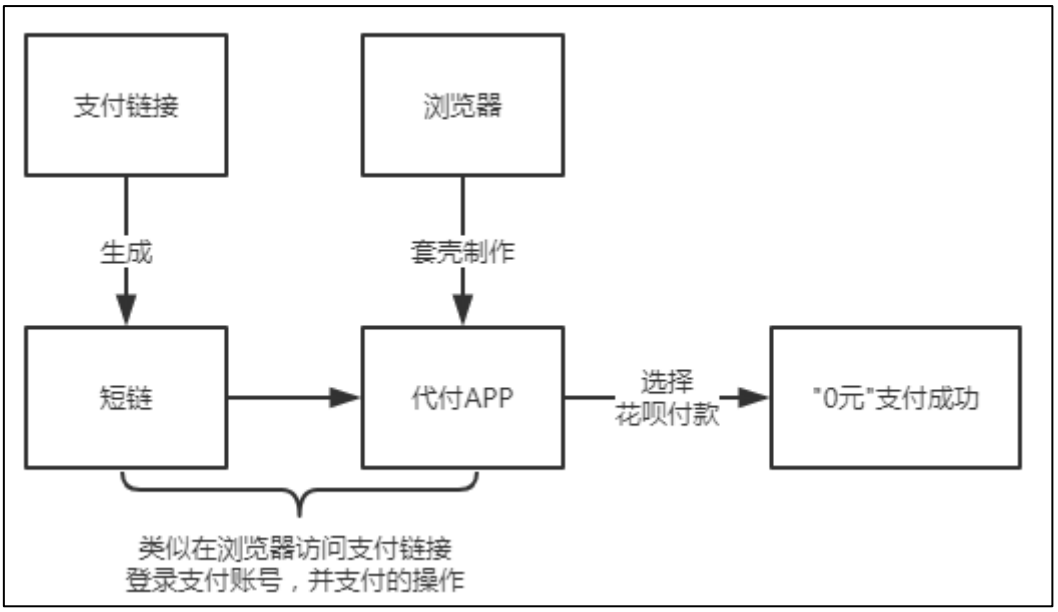
2019 年 7 月李女士在微信群了解到兼职活动，联系对方后，对方表示该兼职活动为电商刷单，费用由商家代付，无需用户付款，用户帮忙刷单后，根据金额不同，会获得不同金额的佣金，在得到李女士确认刷单的回复后，以刷单需验证刷手资质为由，索要了李女士的淘宝淘气值及花呗首页截图。

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。

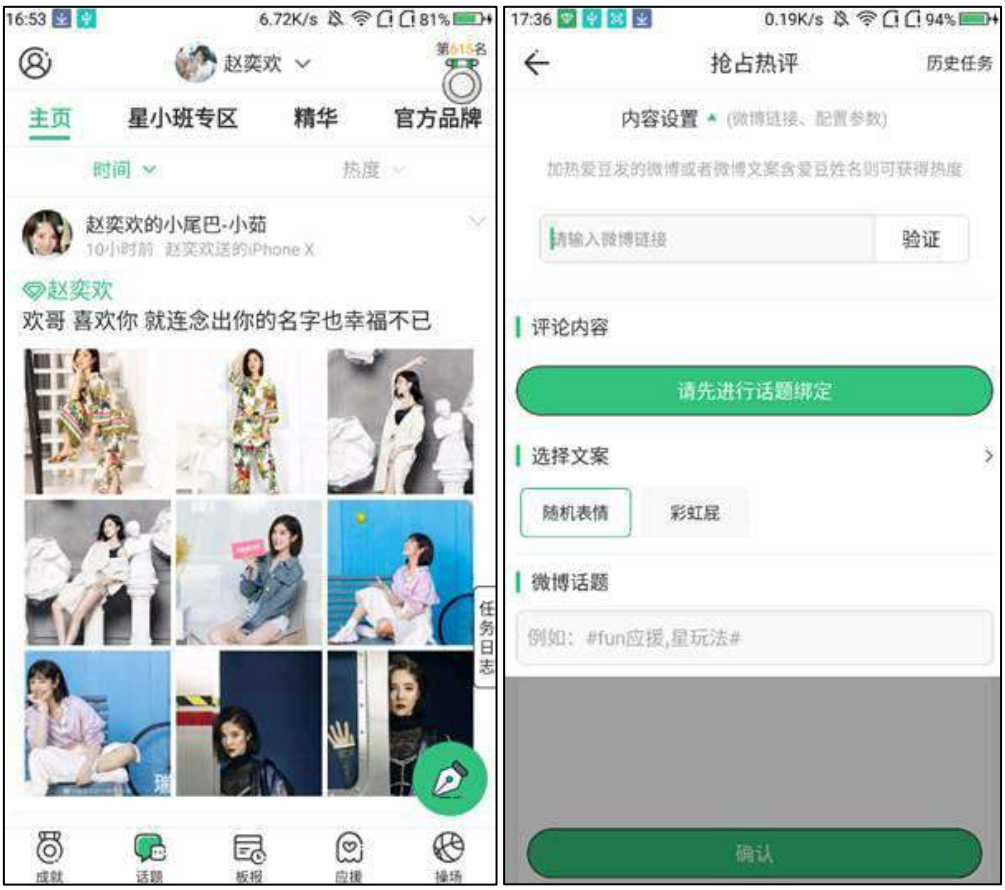
第八章 热点事件

一、流量造假，明星应援 APP

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。

二、微信挂机平台

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。

三、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。

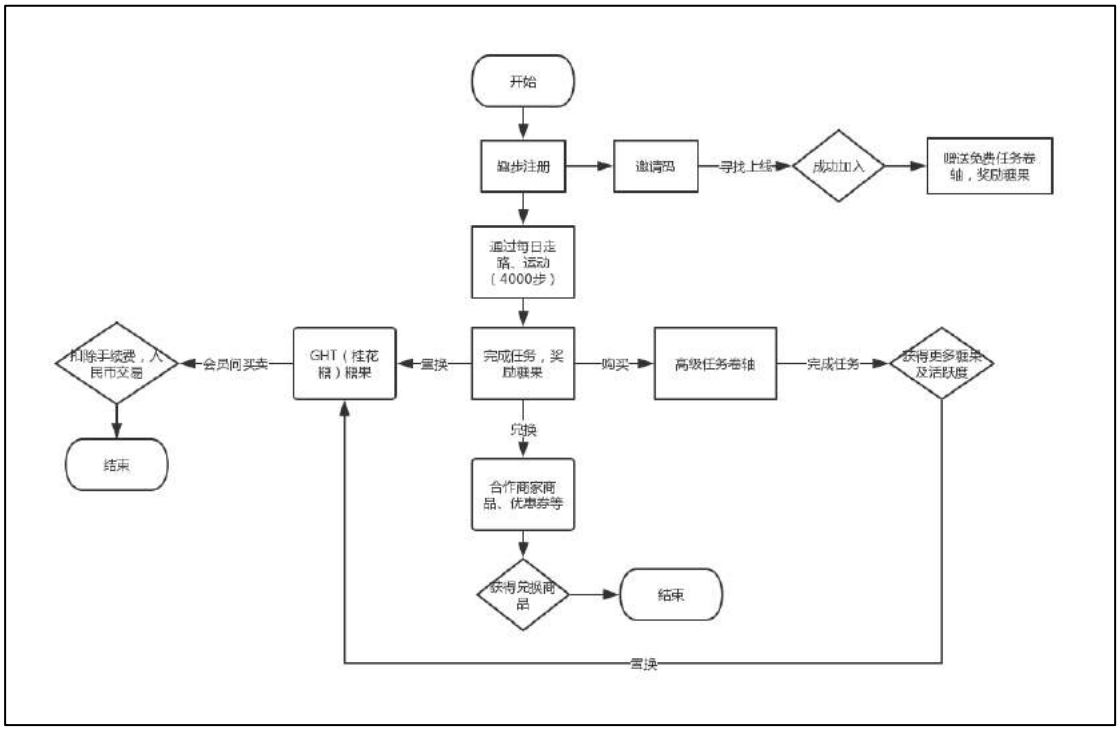
2） 趣步“传销式”的运营模式

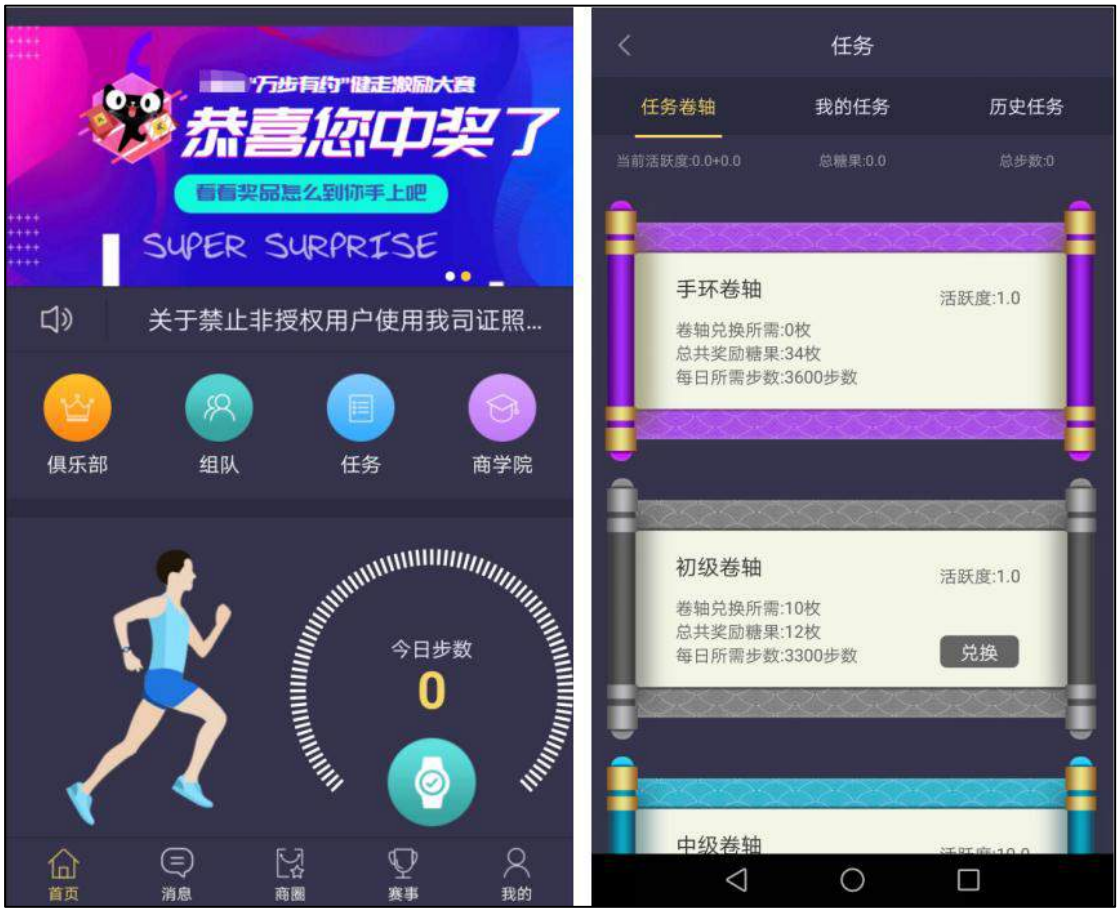
在趣步平台流通的是一种叫做“糖果”的虚拟货币，平台声称利用“区块链”技术以人体运动计步来计算“糖果”的产量，参与者的每一步都能够产出“糖果”。号称不出售糖果，只能通过运动的方式获取，并且有数量上限，总量为 10 亿枚、永不增发，糖果不具备货币功能，只是为了奖励爱运动的人们，可以利用糖果在商城中兑换商品。但同时，趣步 APP 中又支持糖果兑换成 GHT（桂花糖），这种糖果支持用户间交易，而价格每日间有浮动。交易就需要扣除手续费，由平台收取。这种否认糖果价值又支持糖果交易的“双标”举动，可见其中蕴含猫腻。

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。