2020 年第一季度
中国手机安全状况报告

2020 年 05 月 09 日

前言

网络普及加快了人与人之间的信息交流，为现代数字化生活带来了诸多便利与快捷。截至 2020 年 3 月，我国网民规模达 9.04 亿，互联网普及率达 64.5%，为数字经济发展打下坚实的用户基础，为我国互联网发展提供有效助力。宏观当代互联网发展现状，实际上离不开各项数字化核心技术。近几年，我国互联网技术取得了突飞猛进的发展，并不断的发展壮大。

互联网技术的成熟，更加多元化的资源整合，技术能力获取的入门门槛也随之降低。这本应是推动中国互联网发展的“润滑剂”，但却出现众多利用互联网技术实施不法行径的现象。从网站源码搭建到第三方平台利用，甚至衍生出支持黑灰产业的硬件设施以及“销赃”渠道。根据长期针对黑灰产业的挖掘及分析，这些不法团伙呈现出产业化、规模化的特点，上下游团伙配合默契，形成稳定且生态化黑灰产业链条，社会合力共治刻不容缓。

2020 年初受到新冠肺炎疫情影响，在线教育、网络支付等大部分网络应用的用户规模呈现较大幅度增长。在此积极发展前景下，却存在不法分子利用疫情话题传播不法内容及实施诈骗的现象。诈骗电话与短信的肆意传播，防疫物资诈骗、贷款诈骗等案件的频发，严重危害移动信息安全及大众利益。

本文结合 2020 年第一季度各维度数据，分析目前移动安全现状以及新冠肺炎疫情期间网络安全发展趋势。360 安全大脑将持续抵制互联网不法信息传播，维护用户移动信息安全。

注：部分数据引用自中国互联网络信息中心（CNNIC）于 2020 年 4 月 28 日发布的第 45 次《中国互联网络发展状况统计报告》

摘要

恶意程序：

- 2020 年第一季度，360 安全大脑共截获移动端新增恶意程序样本约 39.2 万个，平均每天截获新增手机恶意程序样本约 0.4 万个。新增恶意程序类型主要为资费消耗，占比 83.6%；其次为隐私窃取（11.5%）、流氓行为（2.2%）、恶意扣费（1.8%）、远程控制（0.7%）与系统破坏（0.1%）。
- 2020 年第一季度，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 9.8 亿次，平均每天拦截手机恶意程序攻击约 1.1 亿次。
- 从省级分布来看，2020 年第一季度遭受手机恶意程序攻击最多的地区为河南省，占全国拦截量的 8.4%；其次为山东（8.2%）、广东（7.5%）、江苏（6.6%）、河北（6.2%）等。
- 从城市分布来看，2020 年第一季度遭受手机恶意程序攻击最多的城市为重庆市，占全国拦截量的 2.2%；其次为北京（1.8%）、成都（1.5%）、上海（1.3%）、石家庄（1.1%）等。

钓鱼网站：

- 2020 年第一季度，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 206.4 亿次，PC 端拦截量约为 202.7 亿次，占总拦截量的 98.2%，平均每日拦截量约 2.2 亿次；移动端拦截量约为 3.7 亿次，占总拦截量的 1.8%，平均每日拦截量约 411.1 万次。
- 2020 年第一季度，移动端拦截钓鱼网站类型主要为境外彩票，占比高达 71.9%；其次为假药（11.5%）、虚假购物（7.9%）、虚假中奖（3.2%）、金融证券（2.5%）、网站被黑（2.0%）、假冒银行（0.4%）、模仿登陆（0.4%）、彩票预测（0.1）与虚假招聘（0.1%）。
- 2020 年第一季度，360 安全大脑共截获各类新增钓鱼网站 458.2 万个，平均每天新增 5.0 万个。观察钓鱼网站新增类型，金融证券类占据首位，占比 61.9%。
- 从省级分布来看，2020 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 28.6%；其次为山东（12.9%）、广西（12.3%）、四川（8.0%）、北京（5.8%）等。
- 从城市分布来看，2020 年第一季度移动端拦截钓鱼网站最多的城市为北京市，2.0%；其次为广州（1.9%）、石家庄（1.9%）、上海（1.8%）、成都（1.7%）等。

骚扰电话：

- 2020 年第一季度，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 400.8 万个，平均每天标记约 4.4 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 44.9 亿次，平均每天识别和拦截骚扰电话约 0.5 亿次。

- 从骚扰电话标记类型来看，响一声以 67.3%的比例位居首位；其次为广告推销（9.9%）、骚扰电话（7.2%）、疑似欺诈（5.9%）、房产中介（3.9%）、保险理财（3.6%）、招聘猎头（1.9%）与诈骗电话（0.2%）。

- 从骚扰电话拦截类型来看，骚扰电话以 48.9%的比例位居首位；其次为广告推销（25.6%）、疑似欺诈（18.3%）、房产中介（5.4%）、保险理财（1.0%）、响一声（0.4%）与招聘猎头（0.4%）。

- 2020 年第一季度，从骚扰电话拦截号码个数分布看，被拦截运营商为中国移动的个人手机号最多，占比高达 34.0%；其次为运营商为中国联通的个人手机号（23.2%）、固话（22.2%）、运营商为中国电信的个人手机号（16.7%）、虚拟运营商（3.2%）与 95/96 开头号段（0.6%）。

- 从省级分布来看，2020 年第一季度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 11.1%；其次是山东（6.8%）、江苏（6.6%）、四川（5.6%）、河南（5.1%）等。

- 从城市分布来看，2020 年第一季度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 4.6%；其次是上海（4.1%）、广州（3.1%）、深圳（1.9%）、天津（1.8%）等。

- 从省级分布来看， 2020 年第一季度广东省用户接到骚扰电话最多，广东省用户接到骚扰电话最多，占全国骚扰电话拦截量的 11.1%；其次是山东（7.6%）、河南（5.8）、四川（5.7%）、江苏（5.5%）等。

- 从城市分布来看，2020 年第一季度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 3.4%；其次是上海（3.1%）、广州（2.6%）、重庆（2.1%）、成都（2.1%）等。

垃圾短信：

- 2020 年第一季度，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 34.4 亿条，平均每日拦截垃圾短信约 3784.7 万条。

- 2020 年第一季度，垃圾短信的类型分布中广告推销短信最多，占比为 92.2%；诈骗短信占比 7.6%；违法短信占比 0.2%。

- 2020 年第一季度，短信平台 106 开头号段发送垃圾短信占比高达 79.2%；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，利用虚拟运营商发送垃圾短信的最多，占比 36.5%；其次是运营商为中国电信的个人手机号（30.6%）、运营商为中国联通的个人手机号（19.6%）、95/96 号段（7.6%）、运营商为中国移动的个人手机号（4.7%）、固话（0.5%）与 14 物联网卡（0.4%）等。
- 从省级分布来看，2020 年第一季度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 16.2%；其次是山东（8.5%）、浙江（6.1%）、江苏（6.0%）、河南（5.8%）等。
- 从城市分布来看，2020 年第一季度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 7.4%；其次是北京（5.7%）、深圳（3.8%）、重庆（3.0%）、上海（2.9%）等。

网络诈骗：

- 2020 年第一季度 360 手机先赔共接到手机诈骗举报 856 起。其中诈骗申请为 414 起，涉案总金额高达 340.2 万元，人均损失 8218 元。
- 在所有诈骗申请中，金融理财占比最高，为 30.2%；其次是虚假兼职（15.9%）、赌博博彩（14.3%）、虚假购物（8.7%）、网游交易（8.7%）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 128.5 万元，占比 37.8%；其次是赌博博彩诈骗，涉案总金额 105.8 万元，占比 31.1%；身份冒充诈骗排第三，涉案总金额为 39.2 万元，占比 11.5%。
- 2020 年第一季度，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；虚假兼职属于中危诈骗类型。赌博博彩类人均损失最高，约 1.8 万元；身份冒充类人均损失约为 1.3 万元；其次为金融理财类，人均损失约为 1.0 万元。
- 从举报用户的性别差异来看，男性受害者占 61.5%，女性占 38.5%，男性受害者占比高于女性。从人均损失来看，男性为 8207 元，女性为 8286 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 33.7%；其次是 00 后占比为 33.3%；80 后占比为 21.4%；70 后占比为 8.0%；60 后占比为 3.6%。
- 从用户举报情况来看，2020 年第一季度广东（12.8%）、山东（6.8%）、河南（6.1%）、四川（6.1%）、河北（5.6%）这 5 个地区的被骗用户最多。
- 从用户举报情况来看，2020 年第一季度天津（2.7%）、深圳（2.4%）、东莞（2.4%）、昆明（2.2%）、上海（1.9%）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 6
一、 恶意程序新增样本量与类型分布 6
二、 恶意程序拦截量 7
三、 恶意程序发展趋势分析 7
四、 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占比及拦截量 10
二、 移动端钓鱼网站类型分布 10
三、 移动端钓鱼网站新增量 11
四、 移动端钓鱼网站拦截量地域分布 12
第三章 骚扰电话 13
一、 骚扰电话标记数与拦截量 13
二、 骚扰电话标记与拦截类型分布 14
三、 骚扰电话拦截号码号源分布 15
四、 骚扰电话归属地分布 16
第四章 垃圾短信 19
一、 垃圾短信拦截量 19
二、 垃圾短信类型分析 20
三、 垃圾短信发送者运营商号源分布 20
四、 垃圾短信拦截量地域分析 21
第五章 2020 年第一季度手机诈骗现状 23
一、 报案数量与类型 23
二、 受害者性别与年龄 24
三、 受害者地域分布 26
第六章 2020 年第一季度移动安全重点趋势分析 28
一、 疫情期间反诈骗数据概况 28
二、 互联网平台及技术“沦为”黑灰产敛财的工具 35
第七章 2020 年第一季度典型诈骗“剧本” 48
一、 疫情当前，骗子们将口罩做成了资金盘 48
二、 抖音成新型传播渠道，金融理财你来不来？ 53

360企业安全 360手机卫士 360安全大脑

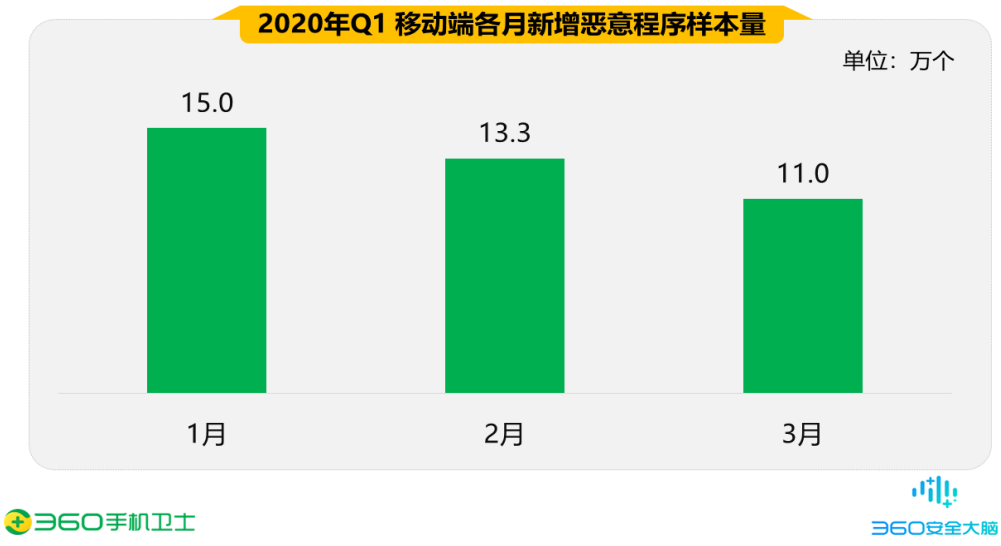
第一章　恶意程序

移动终端作为移动互联网的重要组成部分，近年来，持续遭受恶意程序的侵扰，对人们的日常生活产生日益恶劣的影响，更造成人民群众的财产损失和隐私泄露。

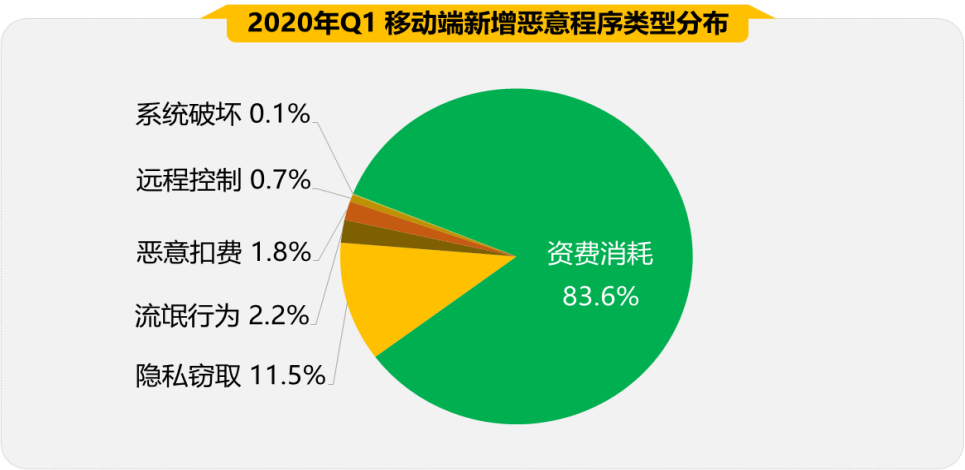
近几年，从安卓端恶意程序新增个数上看，呈现逐年减少，发展走势趋于平缓。但从安卓端恶意程序对设备的影响程度看，截获恶意程序次数出现爆发式增长态势。2020 年一季度拦截量已超过 2019 年全年拦截总量。恶意程序类型以资费消耗类为主，并呈现持续直线涨幅态势，移动端恶意程序“攻坚战”将再一次打响。为有效防护移动互联网安全，360 安全大脑持续加强对移动互联网恶意程序的识别和拦截力度，以保障移动互联网健康有序发展。

一、 恶意程序新增样本量与类型分布

2020 年第一季度，360 安全大脑共截获移动端新增恶意程序样本约 39.2 万个，同比 2019 年第一季度（56.7 万个）下降了 30.8%，平均每天截获新增手机恶意程序样本约 0.4 万个。下图为 2020 年第一季度移动端各月新增恶意程序样本量统计：



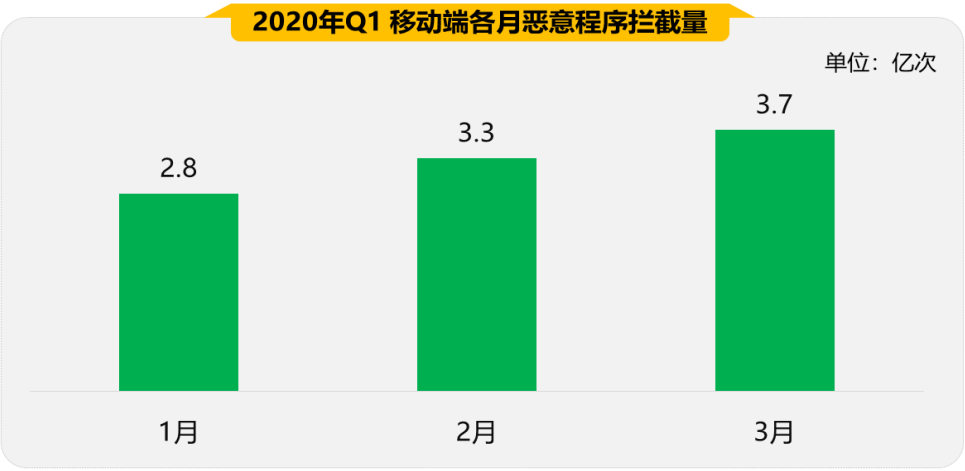
2020 年第一季度，移动端新增恶意程序类型主要为资费消耗，占比 83.6%；其次为隐私窃取（11.5%）、流氓行为（2.2%）、恶意扣费（1.8%）、远程控制（0.7%）与系统破坏（0.1%）。下图为 2020 年第一季度移动端新增恶意程序类型分布：



360手机卫士 360安全大脑

二、 恶意程序拦截量

2020 年第一季度，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 9.8 亿次，平均每天拦截手机恶意程序攻击约 1.1 亿次。下图为 2020 年第一季度移动端各月恶意程序拦截量统计：

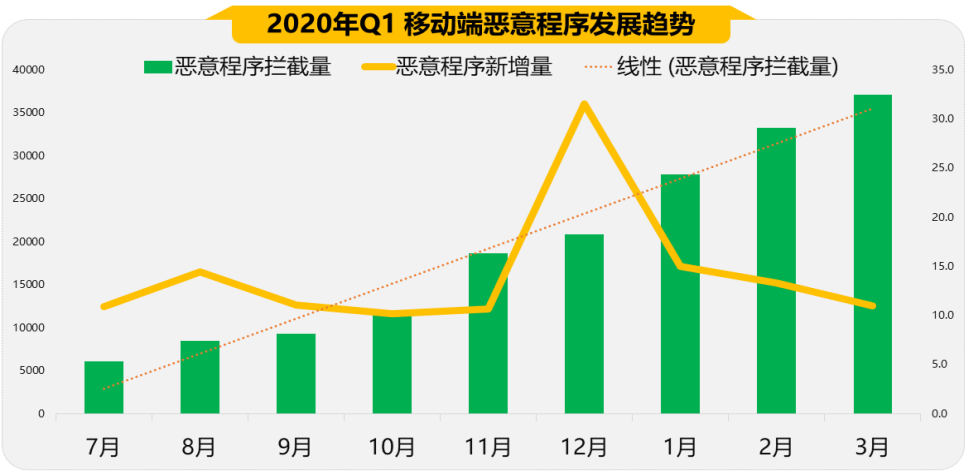


360手机卫士 360安全大脑

三、 恶意程序发展趋势分析

2019 年下半年至 2020 年第一季度期间，恶意程序新增量在 2019 年 12 月出现激增峰值，当月恶意程序新增量为 31.6 万。自 2020 年 1 月起，恶意程序持续呈现持续下降趋势，恢复以往平均新增值。观察新增样本类型，主要体现在资费消耗类型。

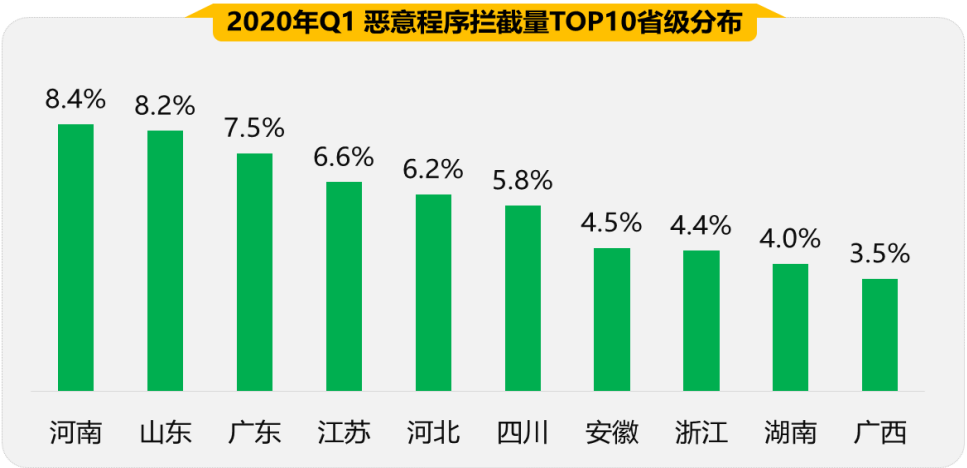
反观恶意程序拦截量趋势，直线上涨走势明显。新增恶意程序个数减少，但遭受恶意程序侵害的现象频发，并且受春节假期前后与疫情影响，大众日常使用网络时长增加，无形中提高了遭受网络不法信息侵害的几率。不法分子利用这一敏感时间段，大肆传播恶意程序，实现不良获利。通过统计 2020 年第一季度恶意程序 TOP 排行，色情视频类 APP 传播范围较广，且 APP 数量众多，均存在恶意消耗用户资费行为。



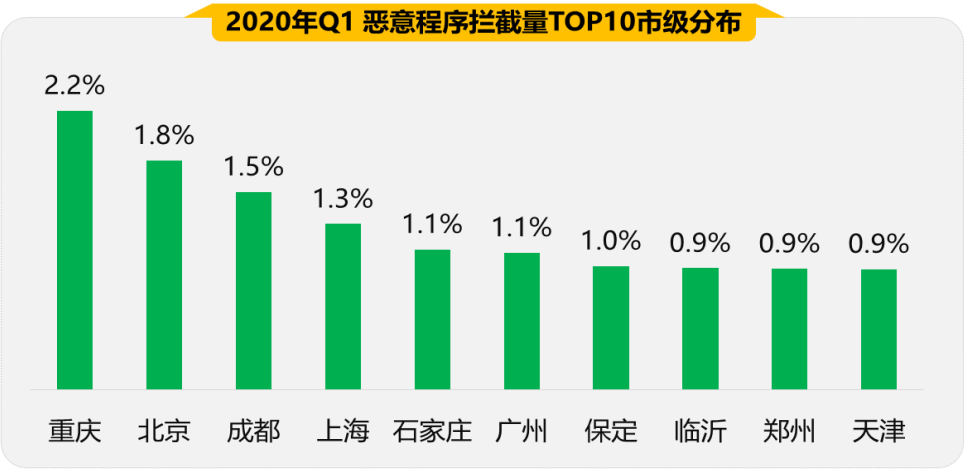
单位：万

四、 恶意程序拦截量地域分布

2020 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河南省，占全国拦截量的 8.4%；其次为山东（8.2%）、广东（7.5%）、江苏（6.6%）、河北（6.2%），此外、四川、安徽、浙江、湖南、广西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重庆市，占全国拦截量的 2.2%；其次为北京（1.8%）、成都（1.5%）、上海（1.3%）、石家庄（1.1%），此外广州、保定、临沂、郑州、天津的恶意程序拦截量也排在前列。

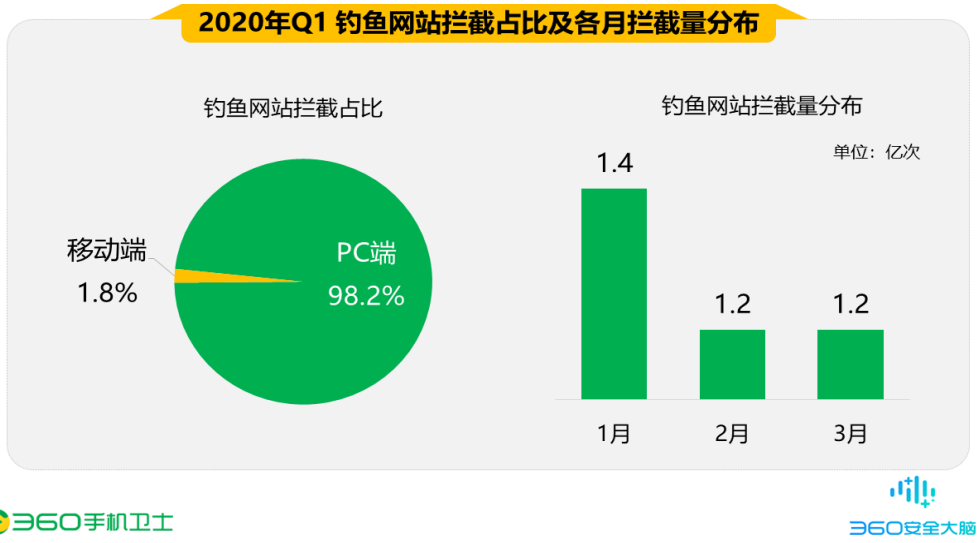


第二章　钓鱼网站

网络钓鱼作为威胁网络安全的突出问题，依然呈现严重化趋势。随着移动互联网的高速发展，移动端网络钓鱼形势趋于严峻。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。“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。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。

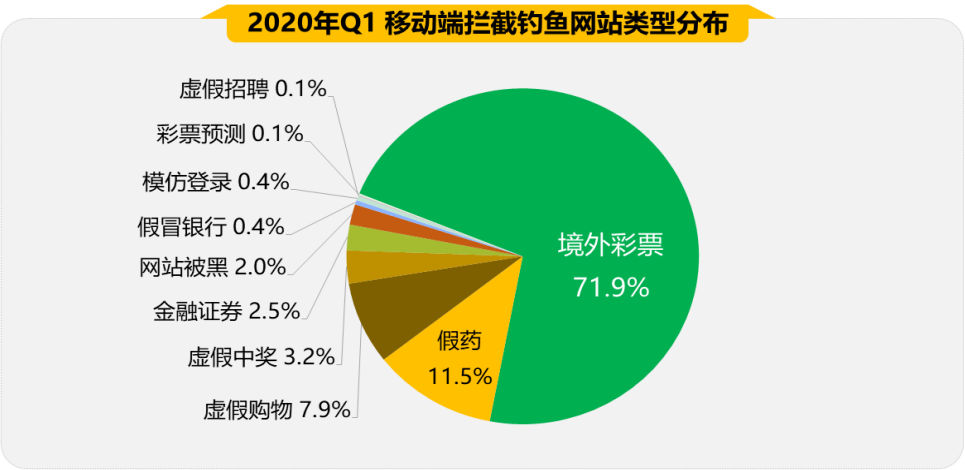
一、 移动端钓鱼网站拦截占比及拦截量

2020 年第一季度，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 206.4 亿次，同比 2019 年第一季度（220.9 亿次）下降了 6.6%。其中，PC 端拦截量约为 202.7 亿次，占总拦截量的 98.2%，平均每日拦截量约 2.2 亿次；移动端拦截量约为 3.7 亿次，占总拦截量的 1.8%，平均每日拦截量约 411.1 万次。下图为 2020 年第一季度钓鱼网站拦截占比及各月拦截量分布：



二、 移动端钓鱼网站类型分布

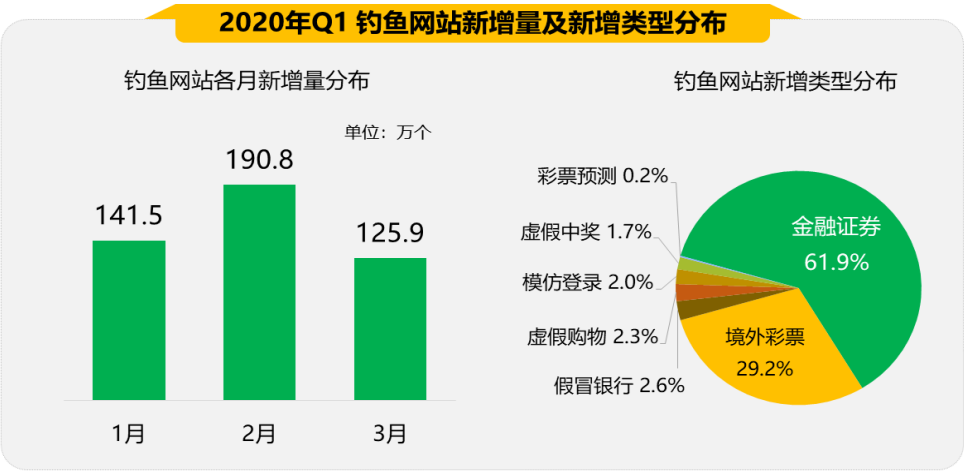
2020 年第一季度，移动端拦截钓鱼网站类型主要为境外彩票，占比高达 71.9%；其次为假药（11.5%）、虚假购物（7.9%）、虚假中奖（3.2%）、金融证券（2.5%）、网站被黑（2.0%）、假冒银行（0.4%）、模仿登陆（0.4%）、彩票预测（0.1）与虚假招聘（0.1%）。下图为 2020 年第一季度移动端拦截钓鱼网站类型分布：



三、 移动端钓鱼网站新增量

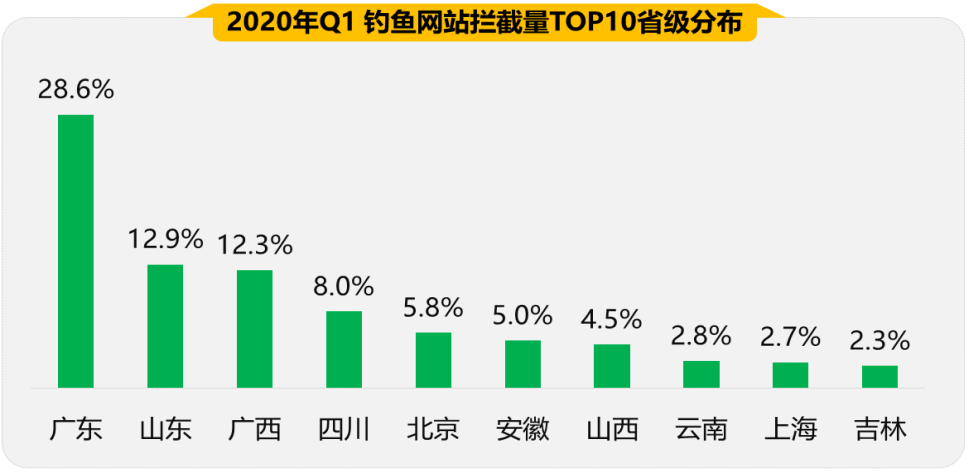
2020 年第一季度，360 安全大脑共截获各类新增钓鱼网站 458.2 万个，同比 2019 年第一季度（525.5 万个）下降了 12.8%，平均每天新增 5.0 万个。观察钓鱼网站新增类型，金融证券类占据首位，占比 61.9%。

随着近几年网络贷款的兴起，互联网中贷款平台丛生，资质参差不齐，滋生了大量虚假贷款平台。第一季度受疫情原因影响，部分大众收入来源遭受影响，由于网络贷款具备快捷、便利、下款快的特点，很多人选择利用网络贷款缓解经济压力，不法分子便利用此社会现象大肆传播虚假贷款平台，导致贷款诈骗案件频发。

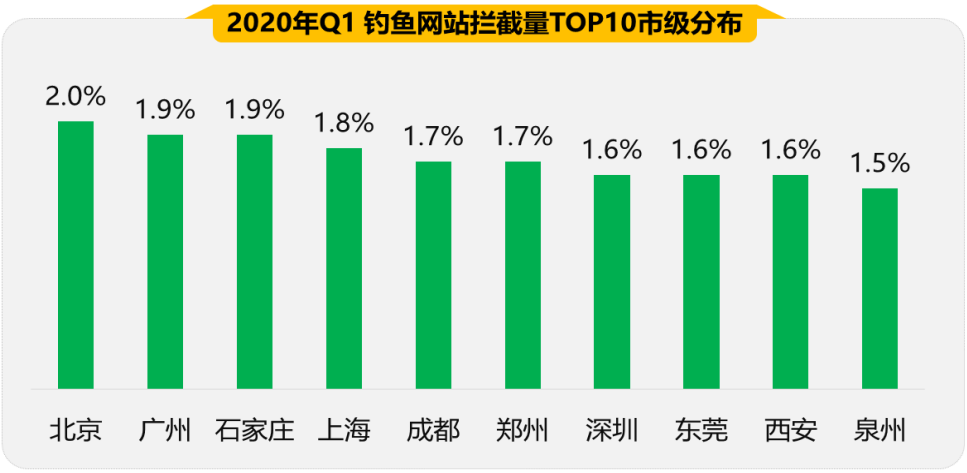


四、 移动端钓鱼网站拦截量地域分布

2020 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 28.6%；其次为山东（12.9%）、广西（12.3%）、四川（8.0%）、北京（5.8%），此外安徽、山西、云南、上海、吉林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北京市，占全国拦截量的 2.0%；其次为广州（1.9%）、石家庄（1.9%）、上海（1.8%）、成都（1.7%），此外郑州、深圳、东莞、西安、泉州的钓鱼网站拦截量也排在前列。



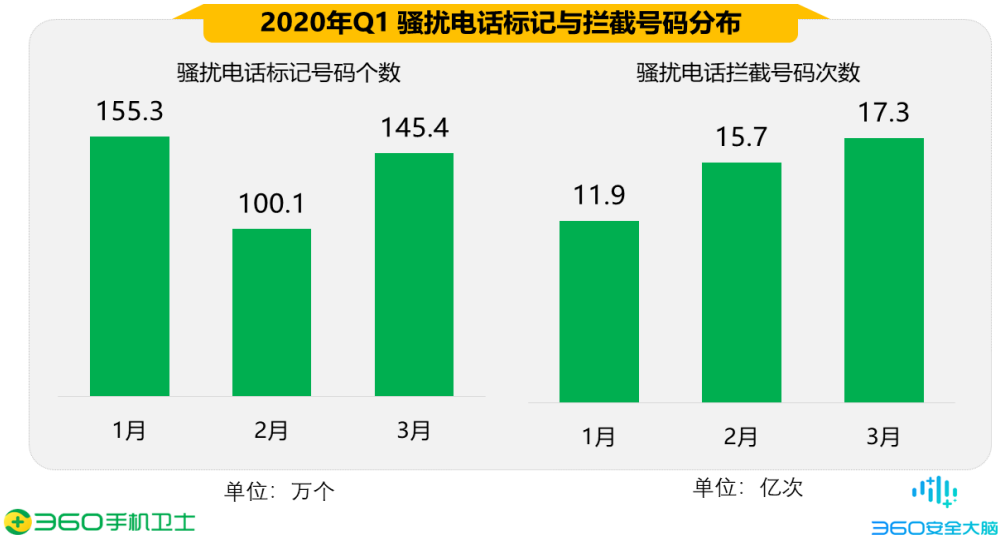
第三章　骚扰电话

骚扰电话问题如今持续肆虐，人工智能技术的日渐成熟，为拨打骚扰电话提供了更加高效的方式。骚扰电话背后的极具规模的灰色产业链在各环节紧密衔接下形成闭环，并相互推动。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。

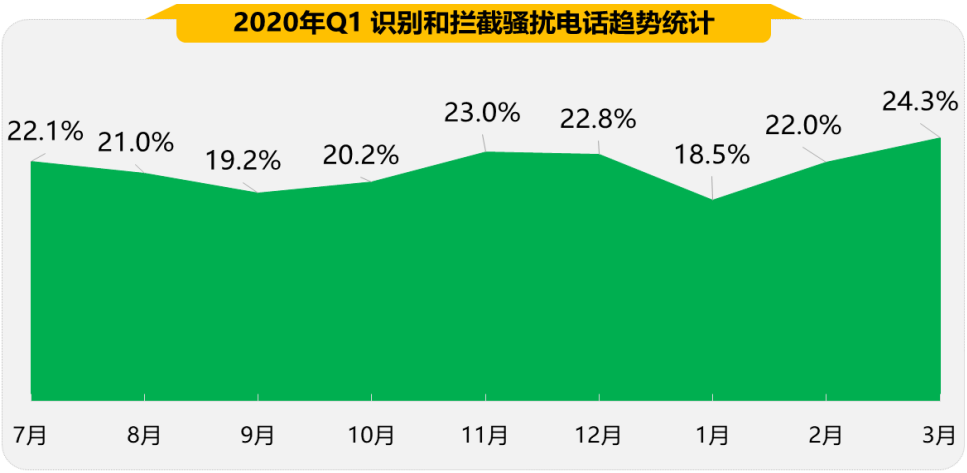
一、 骚扰电话标记数与拦截量

2020 年第一季度，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 400.8 万个，平均每天标记约 4.4 万个。从标记号码个数上看，同比 2019 年第一季度（1649.1 万个）下降了 75.7%。

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 44.9 亿次，平均每天识别和拦截骚扰电话约 0.5 亿次。环比 2019 年第一季度（58.2 亿次）下降了 22.9%。下图为 2020 年第一季度骚扰电话标记与拦截号码分布：



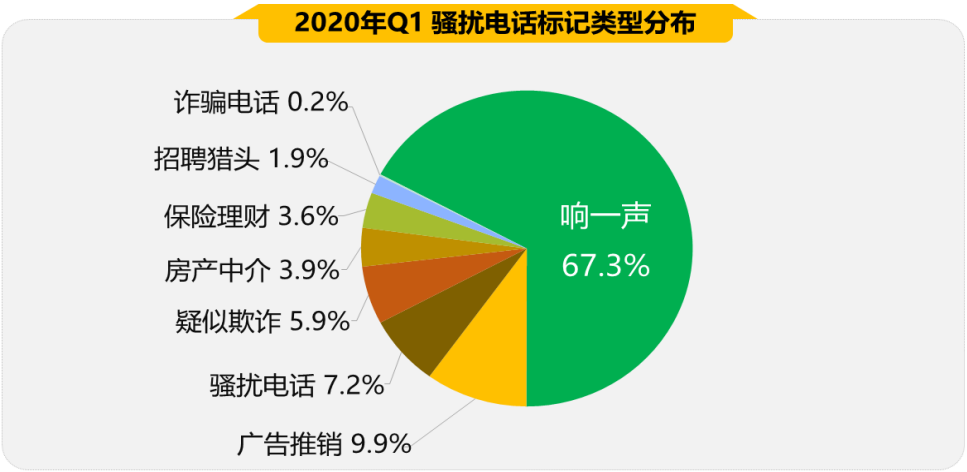
根据各月骚扰电话呼入占比分析，2020 年 1 月份临近春节假期，骚扰电话拦截量最低。在春节前后，从事拨打骚扰电话的人员减少，从而导致骚扰电话的呼入量降低。2020 年第一季度，360 手机卫士识别陌生来电并拦截骚扰电话呈现逐步上涨趋势。下图为 2020 年第一季度识别与拦截骚扰电话趋势统计：



360手机卫士　360安全大脑

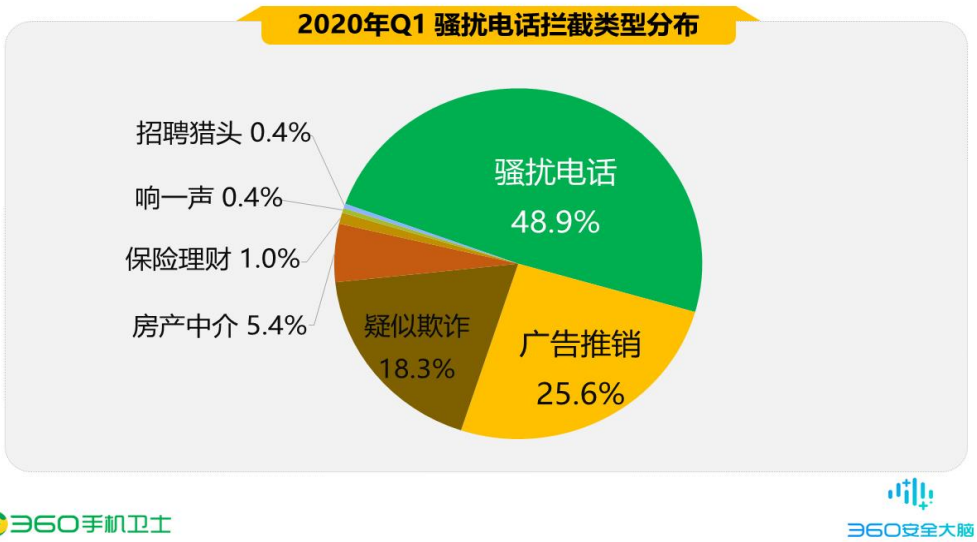
二、 骚扰电话标记与拦截类型分布

2020 年第一季度，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 67.3%的比例位居首位；其次为广告推销（9.9%）、骚扰电话（7.2%）、疑似欺诈（5.9%）、房产中介（3.9%）、保险理财（3.6%）、招聘猎头（1.9%）与诈骗电话（0.2%）。下图为 2020 年第一季度骚扰电话标记类型分布：



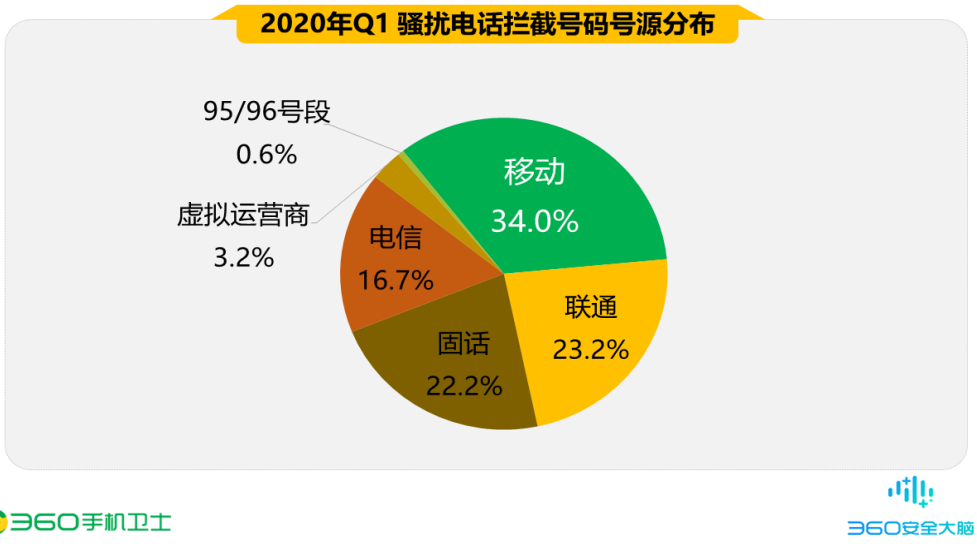
360手机卫士　360安全大脑

从骚扰电话拦截类型来看，骚扰电话以 48.9%的比例位居首位；其次为广告推销（25.6%）、疑似欺诈（18.3%）、房产中介（5.4%）、保险理财（1.0%）、响一声（0.4%）与招聘猎头（0.4%）。下图为 2020 年第一季度骚扰电话拦截类型分布：

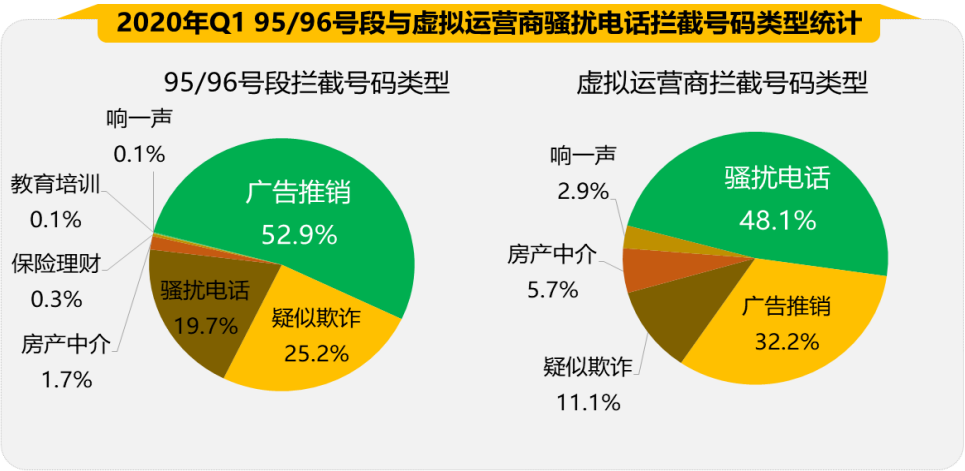


三、 骚扰电话拦截号码号源分布

2020 年第一季度，从骚扰电话拦截号码个数分布看，被拦截运营商为中国移动的个人手机号最多，占比高达 34.0%；其次为运营商为中国联通的个人手机号（23.2%）、固话（22.2%）、运营商为中国电信的个人手机号（16.7%）、虚拟运营商（3.2%）与 95/96 开头号段（0.6%）。下图为 2020 年第一季度骚扰电话拦截号码号源分布：

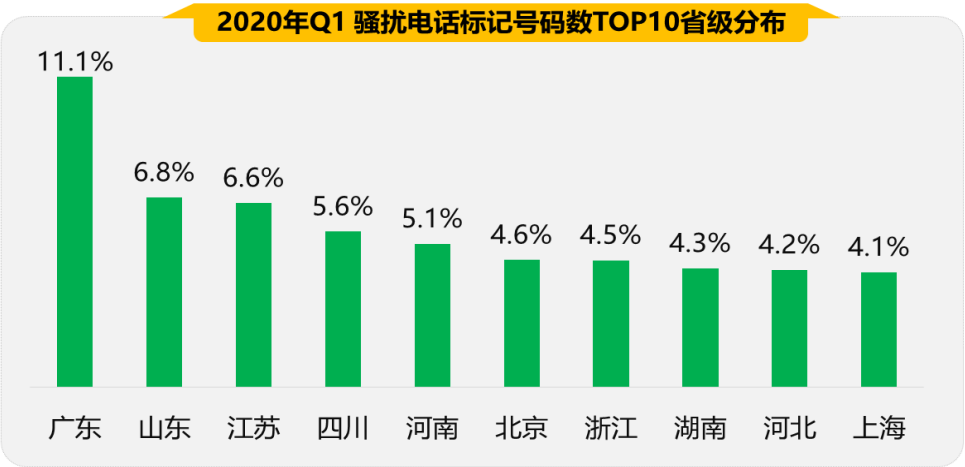


观察 95/96 号段与虚拟运营商骚扰电话拦截号码类型，95/96 号段广告推销类占据首位，占比 52.9%；虚拟运营商骚扰电话类占据首位，占比 48.1%；疑似欺诈类分别占比 25.2%与 11.1%，类型比例占据前列。95/96 号段与虚拟运营商号码遭不法分子利用，成为从事非法行径的主要号源之一。

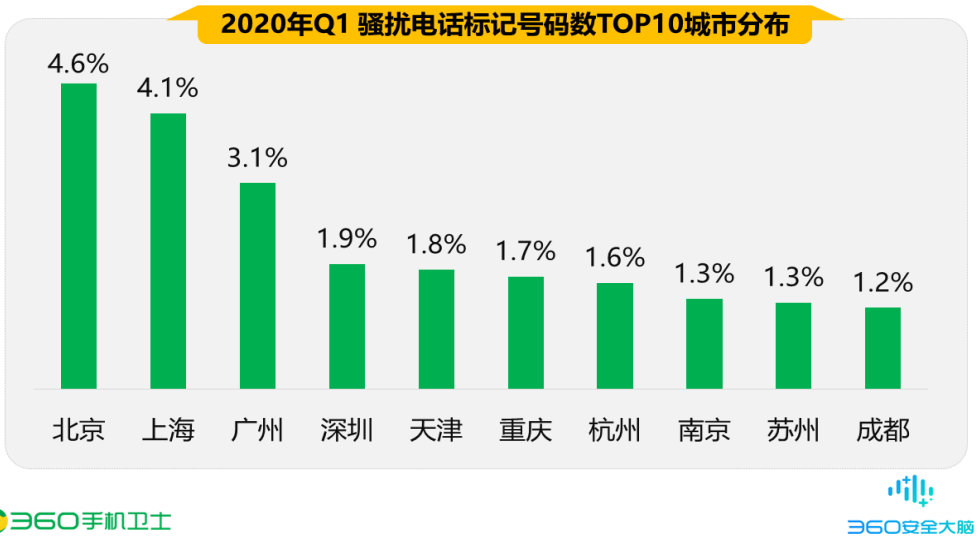


四、 骚扰电话归属地分布

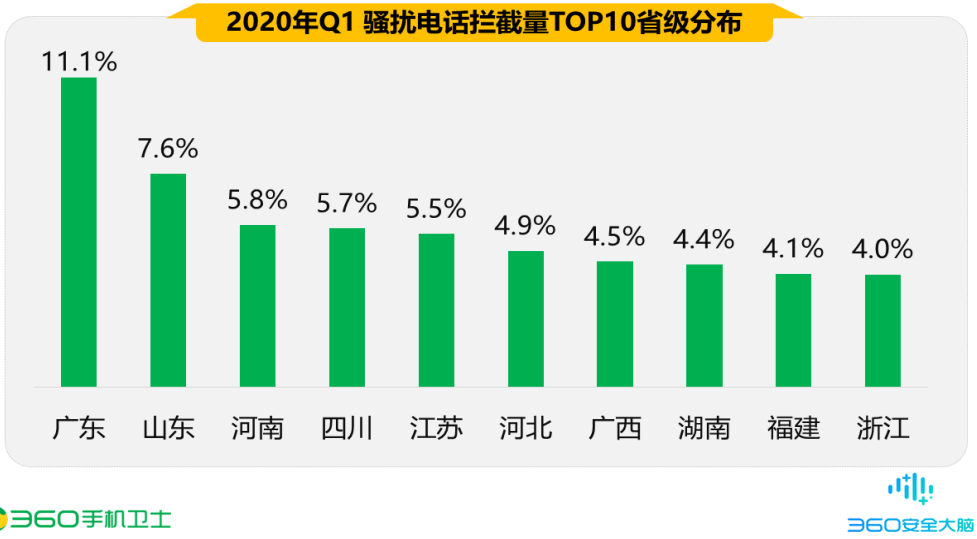
2020 年第一季度，从各地骚扰电话标记号码个数上分析，广东省用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的 11.1%；其次是山东（6.8%）、江苏（6.6%）、四川（5.6%）、河南（5.1%），此外北京、浙江、湖南、河北、上海的骚扰电话标记号码个数也排在前列。



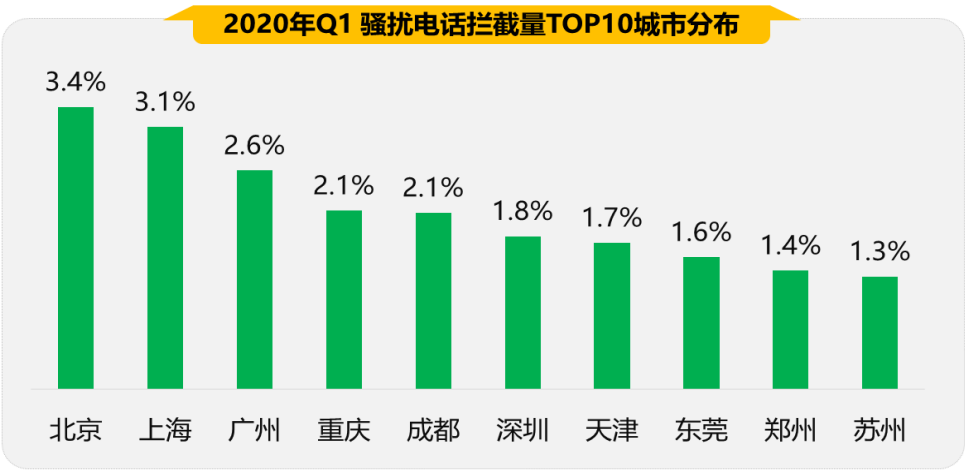
从城市分布来看，北京市用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的 4.6%；其次是上海（4.1%）、广州（3.1%）、深圳（1.9%）、天津（1.8%），此外重庆、杭州、南京、苏州、成都的骚扰电话标记号码个数也排在前列。



2020 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 11.1%；其次是山东（7.6%）、河南（5.8）、四川（5.7%）、江苏（5.5%），此外河北、广西、湖南、福建、浙江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 3.4%；其次是上海（3.1%）、广州（2.6%）、重庆（2.1%）、成都（2.1%），此外深圳、天津、东莞、郑州、苏州的骚扰电话拦截量也排在前列。



360手机卫士　360安全大脑

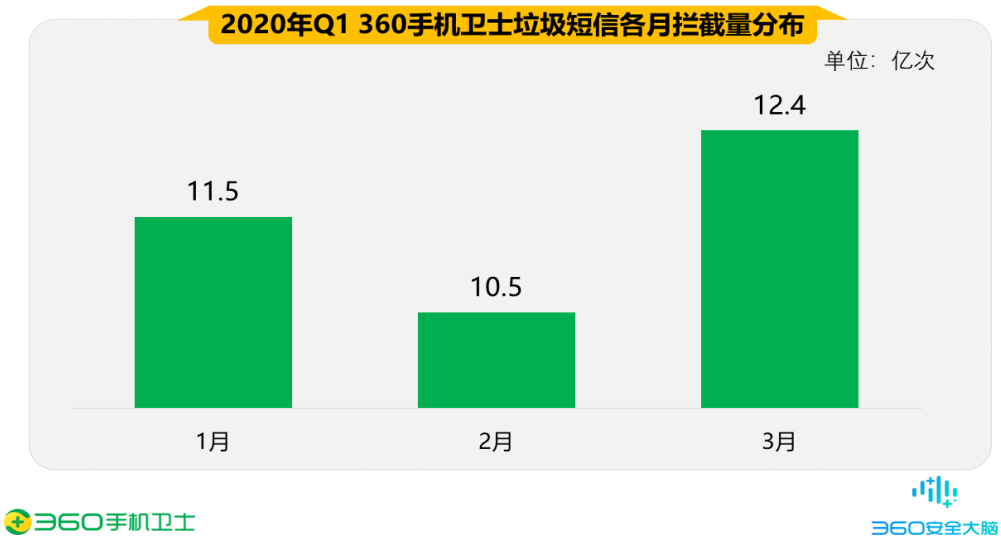
第四章　垃圾短信

在移动短信的发展过程中，从日常沟通发展至身份验证、支付校验的重要方式，出现了质的转变。与此同时，短信成为传播不法信息的载体之一，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。

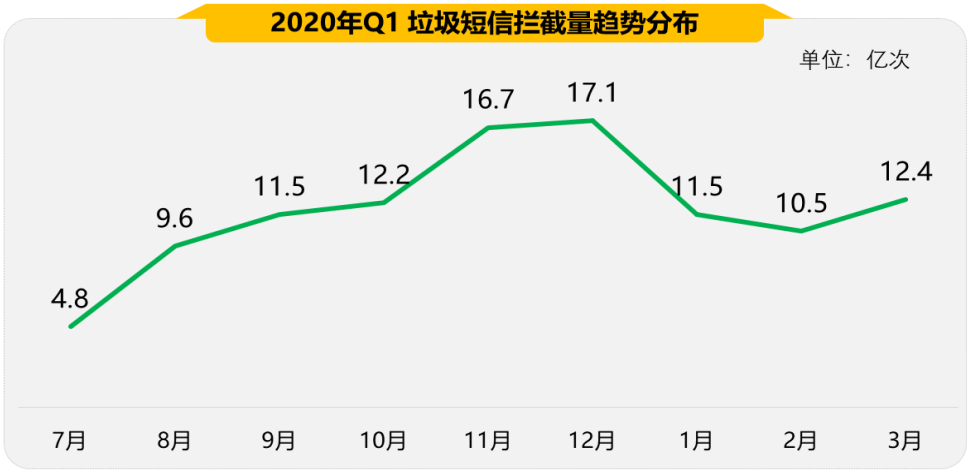
目前，短信平台已成为垃圾短信的主要传播手段，其泛滥的主要原因是部分卡商企业未严格管控短信群发主体，致使垃圾短信产业链形成完整闭环。为此，360 与运营商、手机厂商达成合作，借助 360 安全大脑的云端拦截规则与本地算法能力，为用户防御垃圾短信保驾护航。

一、 垃圾短信拦截量

2020 年第一季度，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 34.4 亿条，同比 2019 年第一季度（12.2 亿条）上升了 64.7%，平均每日拦截垃圾短信约 3784.7 万条。下图为 2020 年第一季度 360 手机卫士垃圾短信各月拦截量分布：



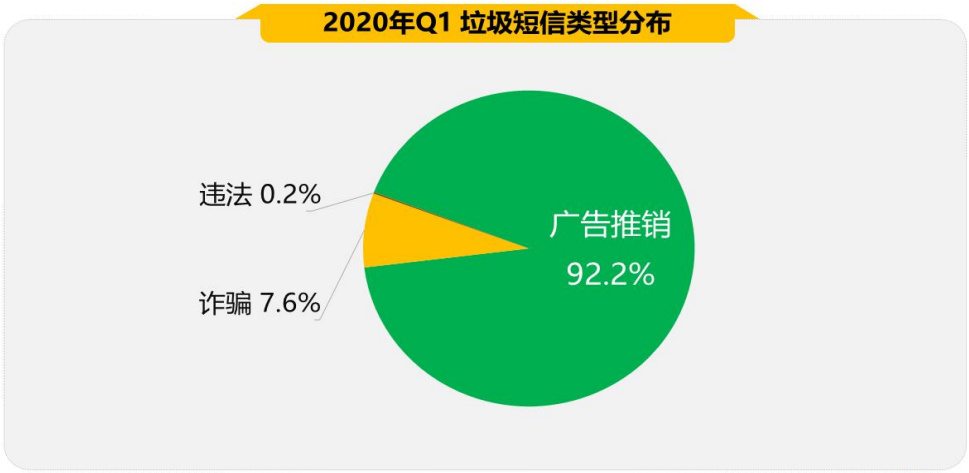
根据垃圾短信拦截量趋势分布，2019 年 Q4 季度呈现涨幅态势。根据往年趋势，年底一般为垃圾短信传播高峰期，临近春节假期期间垃圾短信拦截量逐渐回落。同时由于疫情影响，2020 年 2 月份垃圾短信拦截量持续降低，在 3 月份恢复复工后，垃圾短信拦截量逐渐回升。



360手机卫士　360安全大脑

二、 垃圾短信类型分析

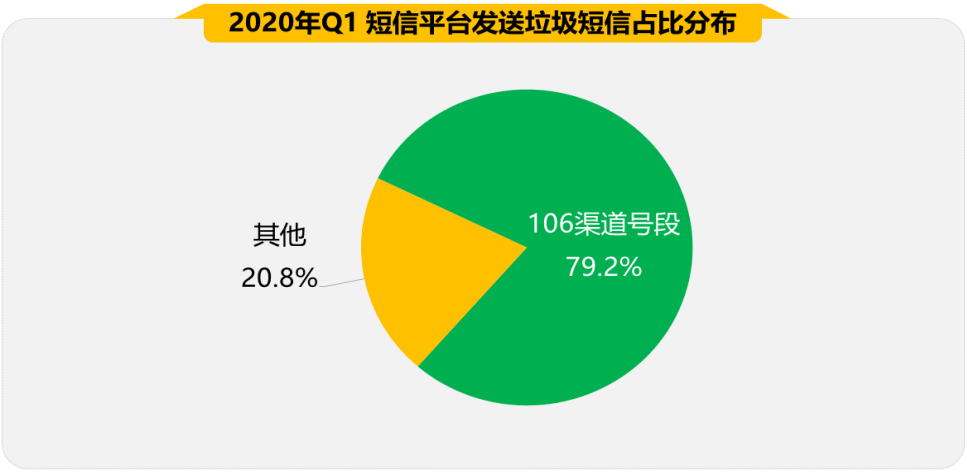
2020 年第一季度，垃圾短信的类型分布中广告推销短信最多，占比为 92.2%；诈骗短信占比 7.6%；违法短信占比 0.2%。



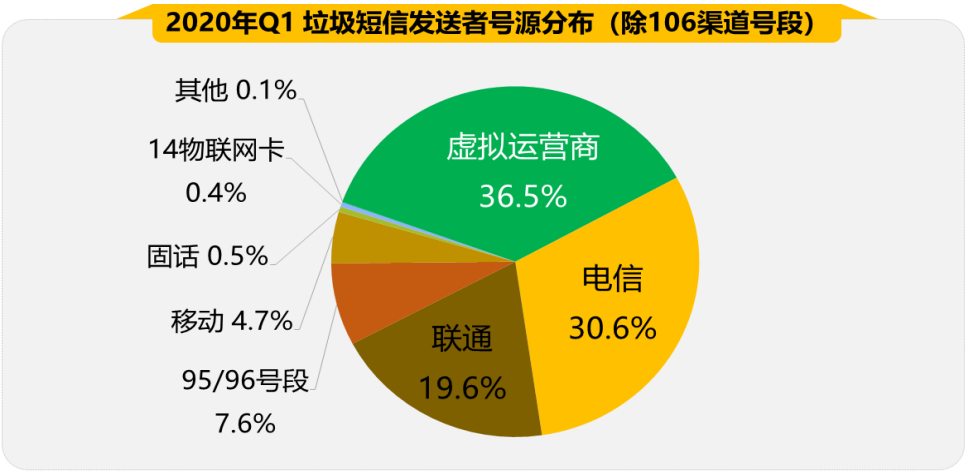
360手机卫士　360安全大脑

三、 垃圾短信发送者运营商号源分布

2020 年第一季度，短信平台 106 开头号段发送垃圾短信占比高达 79.2%；其他号段占比 20.8%。利用短信平台、虚拟运营商传播各类型短信，已成为目前主流趋势。从获取用户联系方式到群发短信，已形成完整产业链条。与此同时，其发送成本低、传播范围广的特点被黑灰产业利用，成为传播违法诈骗类短信的重要渠道。下图为 2020 年第一季度短信平台发送垃圾短信占比分布：

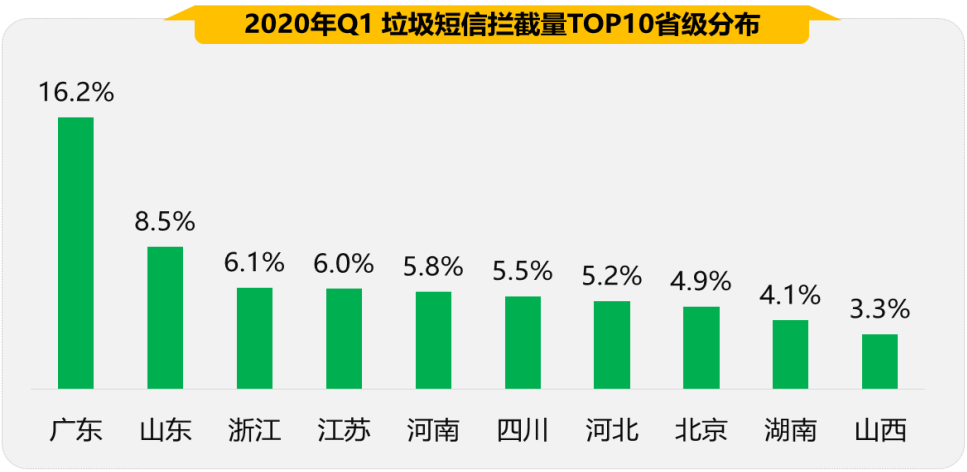


2020 年第一季度，除短信平台 106 开头号段发送垃圾短信外，从其他发送者号码个数分布看，利用虚拟运营商发送垃圾短信的最多，占比 36.5%；其次是运营商为中国电信的个人手机号（30.6%）、运营商为中国联通的个人手机号（19.6%）、95/96 号段（7.6%）、运营商为中国移动的个人手机号（4.7%）、固话（0.5%）与 14 物联网卡（0.4%）等。

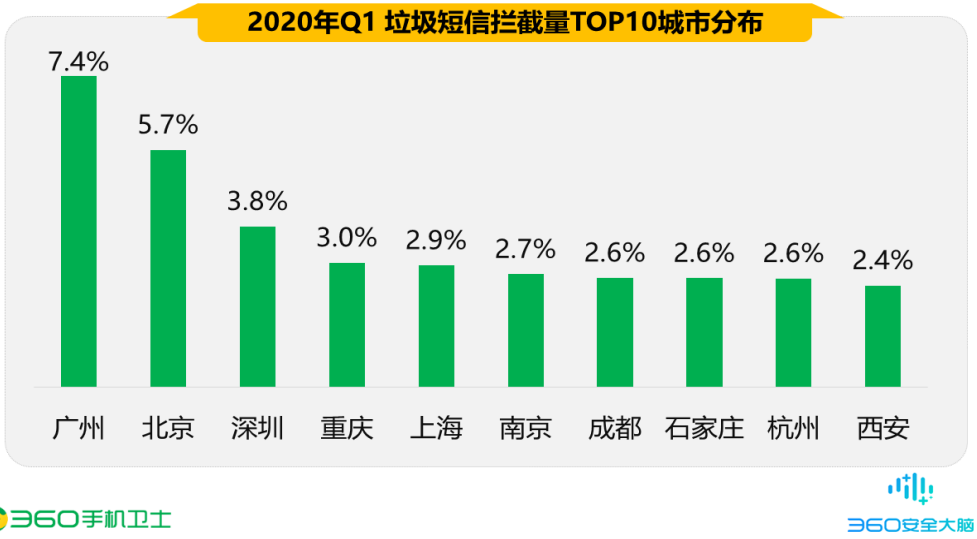


四、 垃圾短信拦截量地域分析

2020 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 16.2%；其次是山东（8.5%）、浙江（6.1%）、江苏（6.0%）、河南（5.8%），此外四川、河北、北京、湖南、山西的垃圾短信拦截量也排在前列。



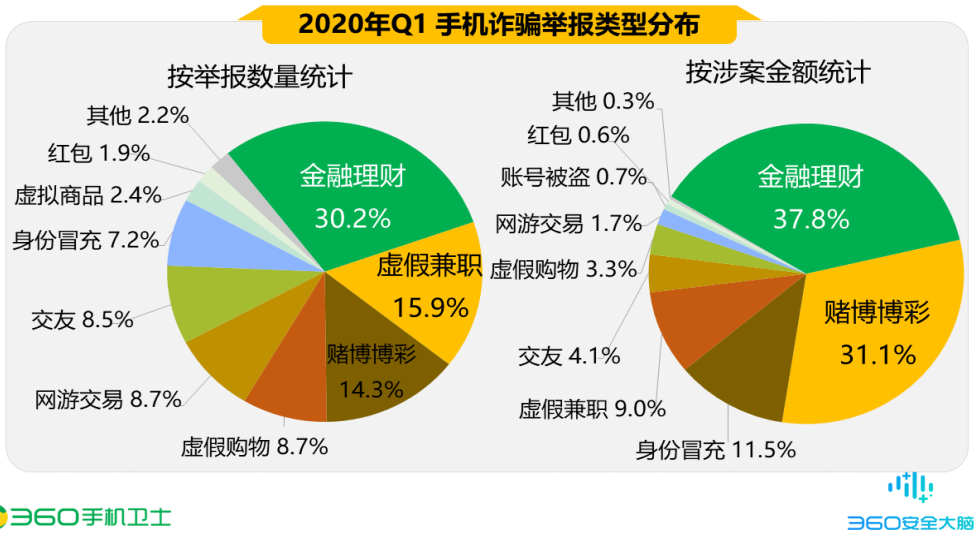
从城市分布来看，广州市用户收到的垃圾短信最多，占全国垃圾短信拦截量的 7.4%；其次是北京（5.7%）、深圳（3.8%）、重庆（3.0%）、上海（2.9%），此外南京、成都、石家庄、杭州、西安的垃圾短信拦截量也排在前列。



第五章 2020 年第一季度手机诈骗现状

一、 报案数量与类型

2020 年第一季度 360 手机先赔共接到手机诈骗举报 856 起。其中诈骗申请为 414 起，涉案总金额高达 340.2 万元，人均损失 8218 元。在所有诈骗申请中，金融理财占比最高，为 30.2%；其次是虚假兼职（15.9%）、赌博博彩（14.3%）、虚假购物（8.7%）、网游交易（8.7%）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 128.5 万元，占比 37.8%；其次是赌博博彩诈骗，涉案总金额 105.8 万元，占比 31.1%；身份冒充诈骗排第三，涉案总金额为 39.2 万元，占比 11.5%。下图为 2020 年第一季度手机诈骗类型的举报类型与涉案金额分布情况：



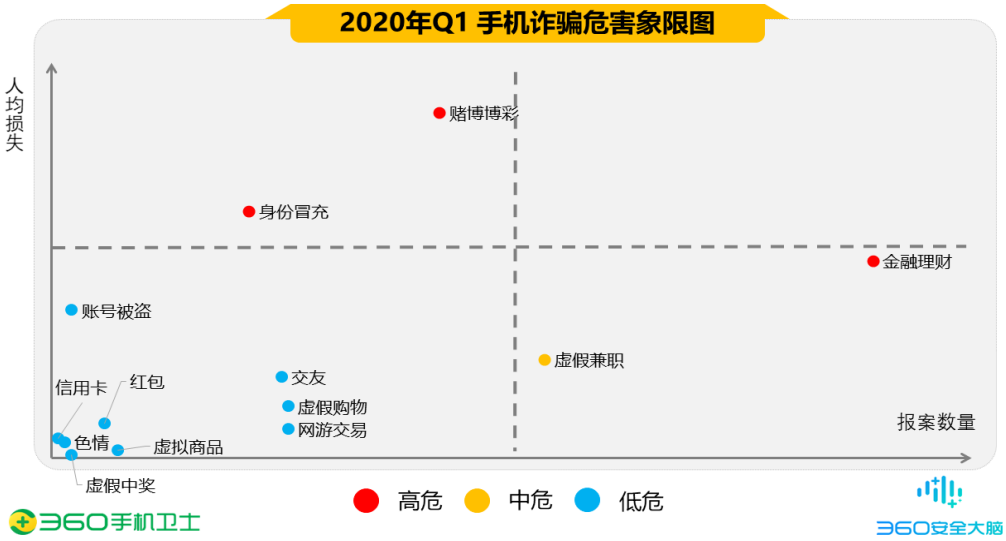
2020 年第一季度，手机诈骗中赌博博彩、身份冒充、金融理财属于高危诈骗类型；虚假兼职属于中危诈骗类型。赌博博彩类人均损失最高，约 1.8 万元；身份冒充类人均损失约为 1.3 万元；其次为金融理财类，人均损失约为 1.0 万元。

1） 赌博博彩类一直属于手机诈骗中的高发类型，其手法主要以事前“赠送彩金”为吸引点，诱导用户在赌博网站充值赌资，但后期限制提现导致用户损失；或以“赚钱”为噱头引导至赌博平台进行兼职操作的，例如兼职刷单、彩票跟投等，但后期不返本金与佣金。随着移动端用户群体的激增，赌博博彩跟随潮流，呈现出 PC 端向移动端倾斜发展的现状。诈骗实施中，不法分子引导用户通过移动端设备访问赌博网站或下载 APP 进行充值赌资成为主流手段。由于第一季度疫情的出现，用户居家隔离后，缺少社交娱乐活动及赚钱方式。利用网络寻找消遣及赚钱成为多数用户的选择，不法分子在此期间“推波助澜”，借助互联网渠道大肆宣传赌博平台，导致赌博博彩类一跃成为 2020 年第一季度手机诈骗危害类型首位。

2） 观察 2020 年第一季度中身份冒充类的诈骗实施手法，主要以冒充他人为主。具体表现为：一是冒充亲友借钱、伪装亲友出事讨要费用；二是冒充公检法机关人员实施诈骗；三是冒充平台客服人员实施诈骗等。对比其他高危类型，具备受害人数少但人均损失高的特点。诈骗实施中均是通过获取用户信任后进行非法敛财。在疫情期间，存在冒充公检法机关人员，利用疫情期间受害人护照被扣留或存在不明处境记录等借口实施诈骗的案例发生，且涉案金额巨大，属于 2020 年第一季度手机诈骗高危类型。

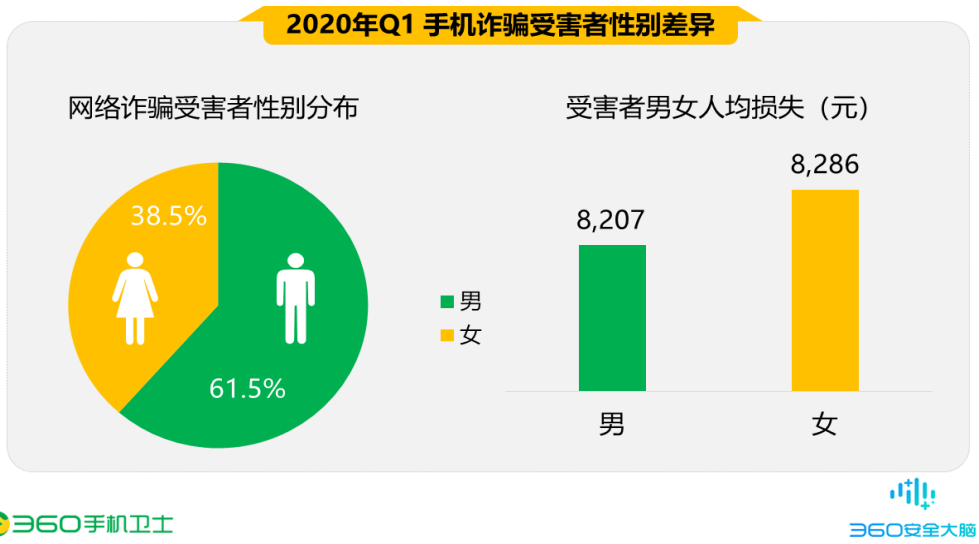
3） 2020 年第一季度中金融理财类是受骗人数最多的诈骗类型，主要体现于网络贷款被骗。收取贷款手续费、包装费或引导用户下载借贷 APP 操作属于借贷诈骗的主要手法。同样受到疫情影响，大多数人选择利用网络贷款缓解经济压力。网络中无抵押贷款、秒下款等的借贷广告更易吸引眼球，在双方成功取得联系后，将会通过多种方式要求用户进行付款操作。超前消费已成为普遍社会现象，贷款诈骗正是利用这一社会痛点实现疯狂蔓延，目前依然呈现高发态势。

4） 2020 年第一季度虚假兼职类型以兼职缴纳会费的手法居多。同样受到疫情影响，尝试通过网络赚钱缓解经济压力成为部分人的选择之一。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，在此敏感时间段，更是打着疫情的旗号，招揽更多用户参与，导致遭受诈骗的用户众多。

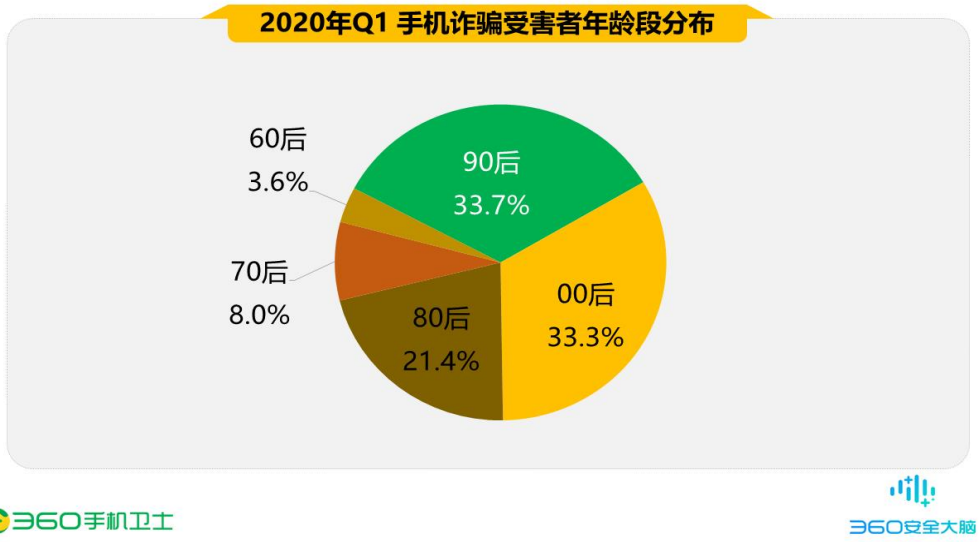


二、 受害者性别与年龄

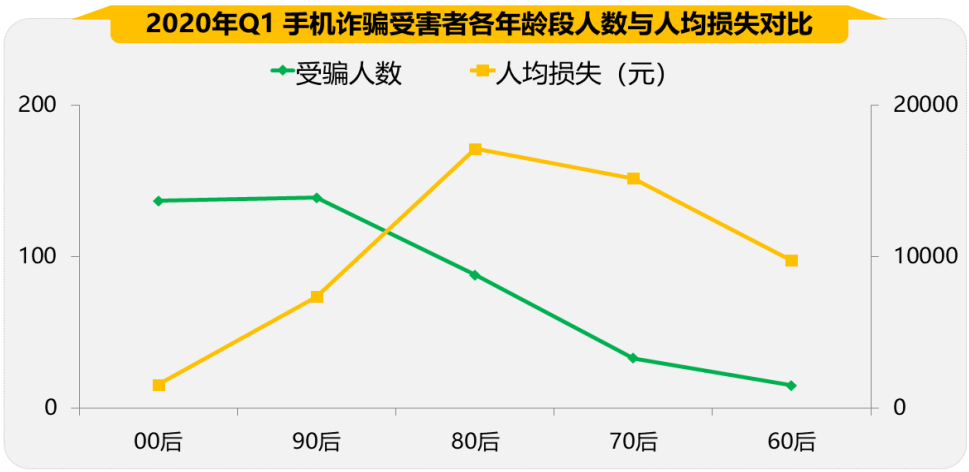
从举报用户的性别差异来看，男性受害者占 61.5%，女性占 38.5%，男性受害者占比高于女性。从人均损失来看，男性为 8207 元，女性为 8286 元，双方人均损失接近持平。



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 33.7%；其次是 00 后占比为 33.3%；80 后占比为 21.4%；70 后占比为 8.0%；60 后占比为 3.6%。如下图所示，2020 年第一季度 90 后为手机诈骗主要针对人群。



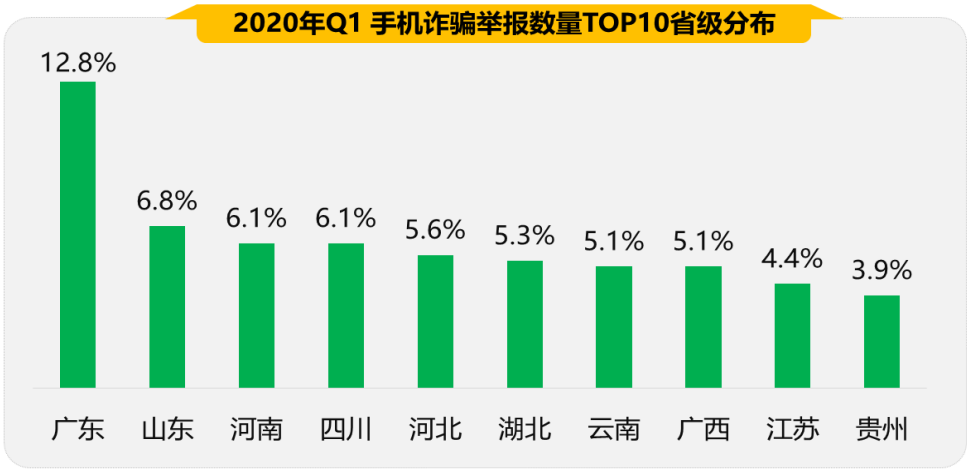
2020 年第一季度，00 后与 90 后受骗人数接近持平。对比发现，00 后被骗的人数虽多，但由于这个年龄段用户经济能力有限，被骗平均金额相对较少。90 后作为 2020 年第一季度诈骗主要针对人群，人均损失也较高。80 后及以上年龄段日常使用网络的时间有限，遭受诈骗的人数也较少。但由于这部分用户有一定经济实力，在遭受诈骗时，损失金额也较高。其中，80 后用户主要受骗类型为赌博博彩与贷款诈骗。



360手机卫士　360安全大脑

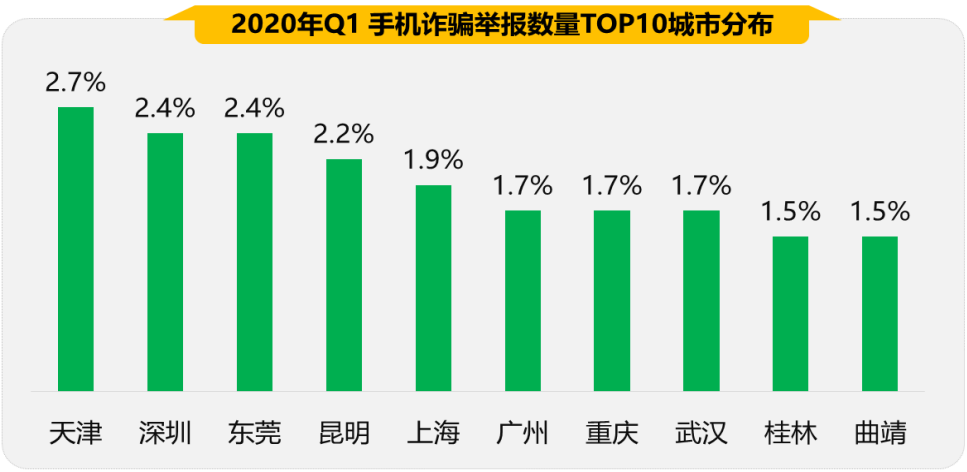
三、 受害者地域分布

2020 年第一季度，从各地区手机诈骗的举报情况来看，广东（12.8%）、山东（6.8%）、河南（6.1%）、四川（6.1%）、河北（5.6%）、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 37.3%。下图给出了 2020 年第一季度手机诈骗举报数量最多的 10 个省份：



360手机卫士　360安全大脑

从各城市手机诈骗的举报情况来看，天津（2.7%）、深圳（2.4%）、东莞（2.4%）、昆明（2.2%）、上海（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 11.6%。下图给出了 2020 年第一季度手机诈骗举报数量最多的 10 个城市：



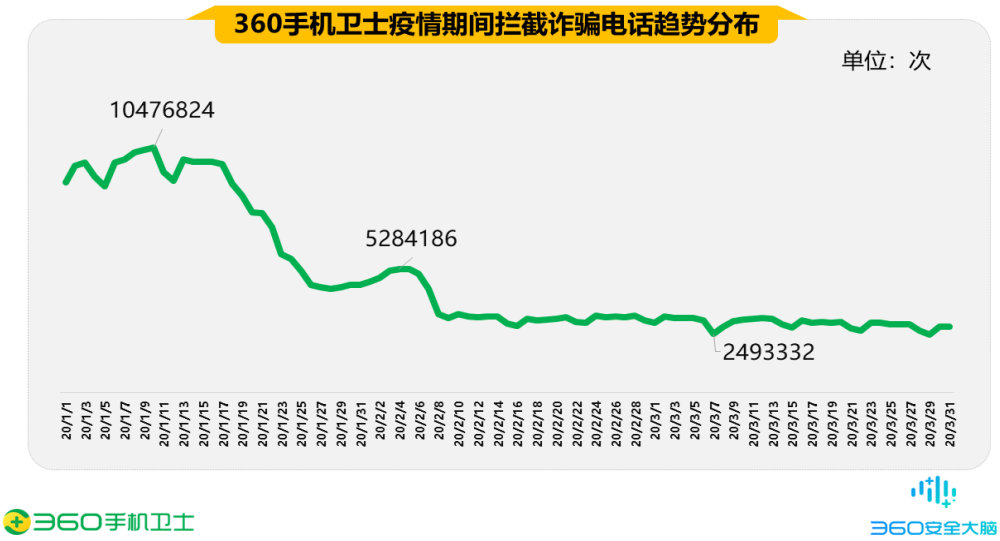
360手机卫士 360安全大脑

第六章　2020 年第一季度移动安全重点趋势分析

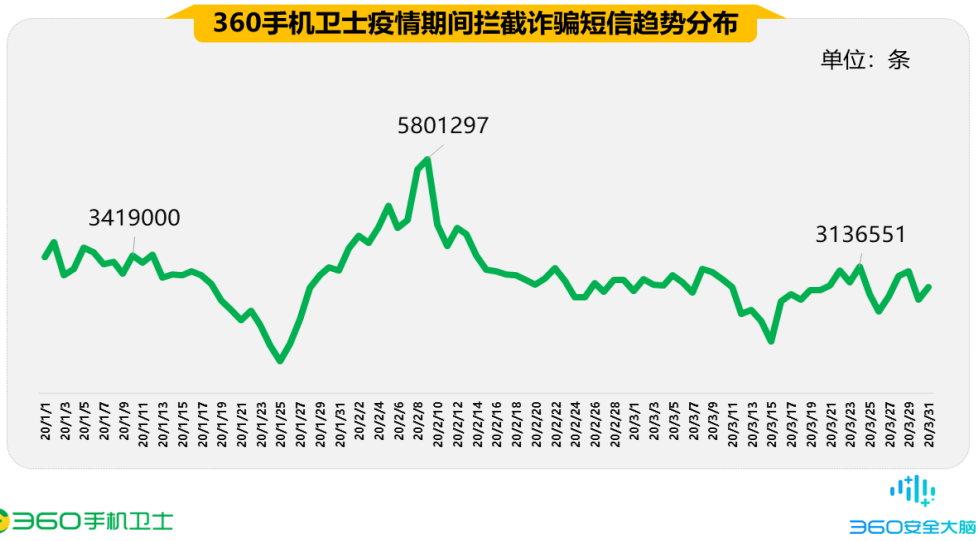
一、 疫情期间反诈骗数据概况

1. 疫情期间诈骗电话&短信拦截趋势

疫情发生前后，诈骗电话拦截呈现骤降趋势，在疫情发生期间，诈骗电话发展趋势平缓。2020 年 1 月份，诈骗电话平均每日拦截量约为 802 万次；2 月份，诈骗电话平均每日拦截量约为 360 万次，环比 1 月份每日拦截量下降 55.1%；3 月份，诈骗电话平均每日拦截量约为 294 万次，环比 2 月份每日拦截量下降 18.4%。

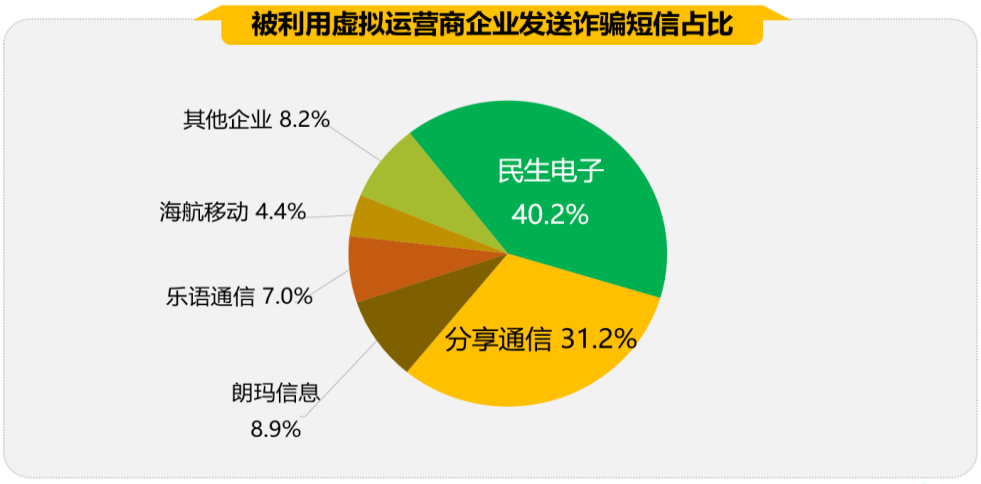


2020 年 1 月份，诈骗短信平均每日拦截量约为 270 万条，在 1 月份月底且疫情爆发初期，呈现下降趋势，但后续呈现逐日上涨趋势，并在 2 月 9 日出现诈骗短信拦截量峰值，约为 580 万条。自 2 月 10 日起，呈现下降趋势，并趋于平稳。2 月份，诈骗短信平均每日拦截量约为 348 万条，环比 1 月份每日拦截量上升 28.7%。3 月份，诈骗短信未见涨幅态势，总体拦截量下降，平均每日拦截量约为 255 万条，环比 2 月份每日拦截量下降 26.7%。



由图可见，1 月份底正值春节假期，从事诈骗活动的人员减少，导致诈骗电话与短信的拦截量骤减。在 2 月初，诈骗电话拦截量出现小幅回升态势，而诈骗短信出现激增态势。由于此时间区间，疫情防控工作陆续开展，民众对于疫情防护的关注度提高，不法分子利用疫情这一敏感时段，从事各类涉及疫情的诈骗行动。如：售卖口罩、口罩资金盘、疫情兼职、贷款等。由于后期政府、媒体等渠道公开曝光各类诈骗，并予以打击，有效提高大众的防骗意识。并结合疫情防控工作有序进行，2 月下旬至 3 月底，诈骗电话与短信的拦截量趋于平缓发展并呈现明显降低态势。

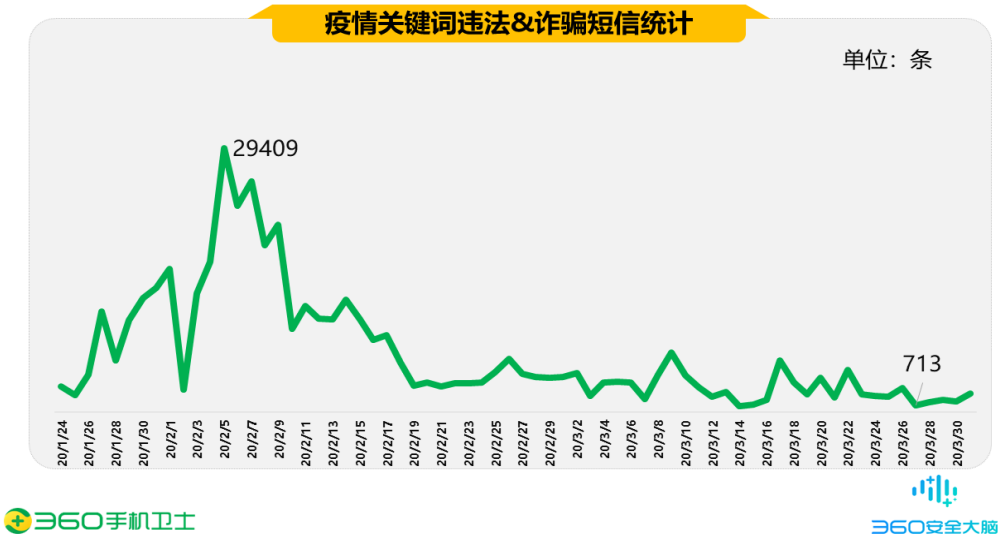
2 月份是疫情防控工作开展的重要时段，诈骗短信在此时段内呈现激增态势，其中包括借助疫情期间传播的诈骗短信。根据诈骗短信的发送者号段统计，利用虚拟运营商号段传播非法内容的占比较高。抽取 2 月份上旬虚拟运营商号段所发送的诈骗短信，统计被不法分子利用传播不法内容的虚拟运营商企业。其中，民生电子占比 40.2%；其次为分享通信（31.2%）、朗玛信息（8.9%）、乐语通信（7.0%）、海航移动（4.4%）等。



简称	公司全称
民生电子	民生电子商务有限责任公司
分享通信	北京分享在线网络技术有限公司
朗玛信息	贵阳朗玛信息技术股份有限公司
乐语通信	北京乐语通信科技有限公司
海航移动	海南海航信息技术有限公司

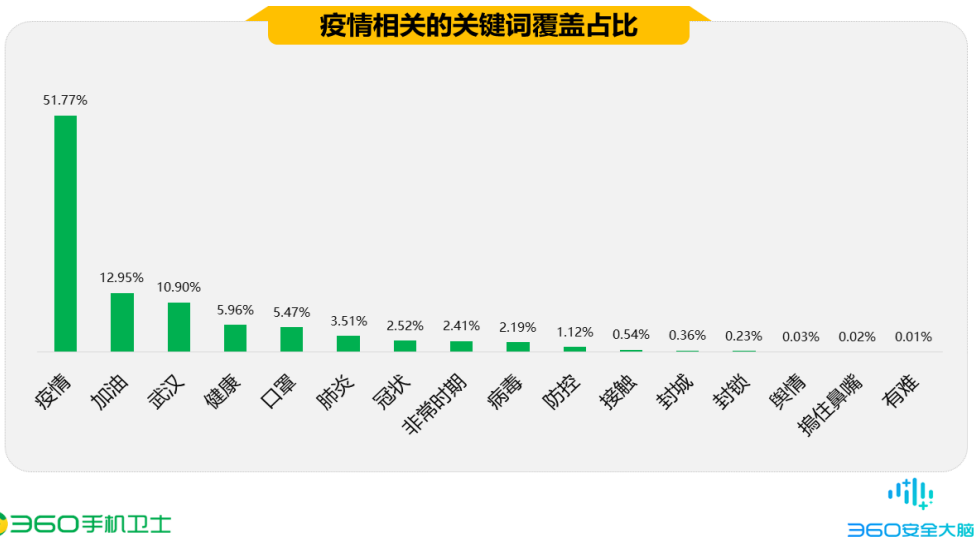
2. 疫情关键词违法&诈骗短信统计

疫情期间（0124-0331）短信内容中包含与疫情的关键词并判定属于违法&诈骗短信的，共拦截约 44 万条，平均每日拦截量约为 6416 条。其中北京市共拦截 8805 条，占疫情期间违法&诈骗短信总量的 2%，平均每日拦截约 129 条。



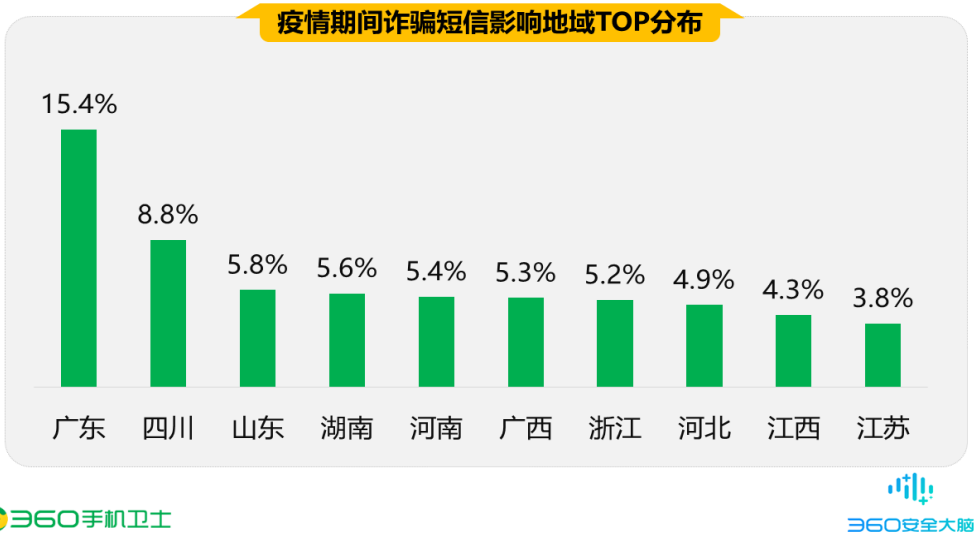
3. 疫情相关的关键词覆盖度

随机抽取（0205-0212）短信进行关键词覆盖度统计，其中与疫情相关的关键词“疫情”占比最高，占比 51.77%；其次为“加油”（12.95%）、“武汉”（10.90%）。详细关键词占比统计如下：



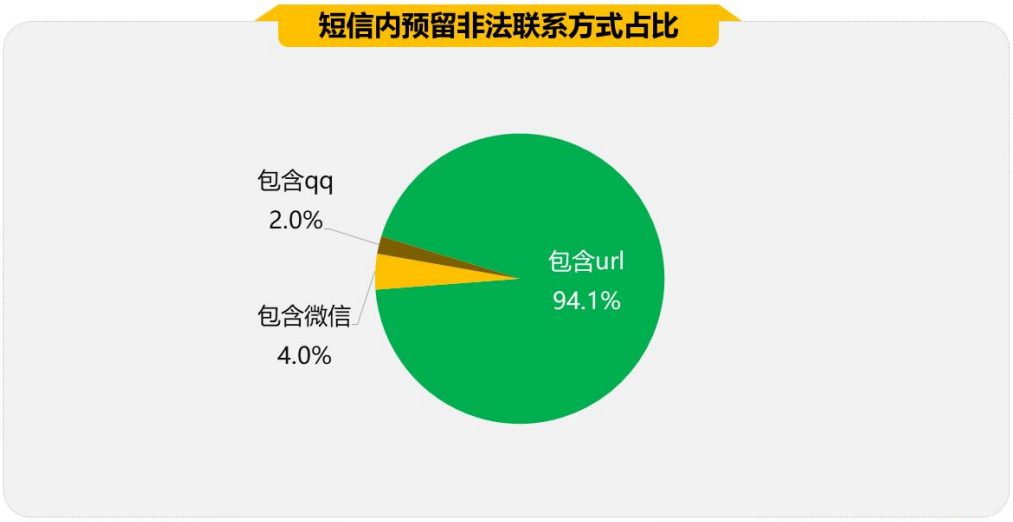
4. 疫情期间违法&诈骗短信影响地域

疫情期间（0203-0331），通过各地域与疫情相关的违法&诈骗短信拦截量统计，用户接收违法&诈骗短信最多的是广东省，占全国与疫情相关的违法&诈骗短信拦截量的 15.4%；其次为四川（8.8%）、山东（5.8%）、湖南（5.6%）、河南（5.4%），广西、浙江、河北、江西、江苏与疫情相关的违法&诈骗短信拦截量也排在前列。



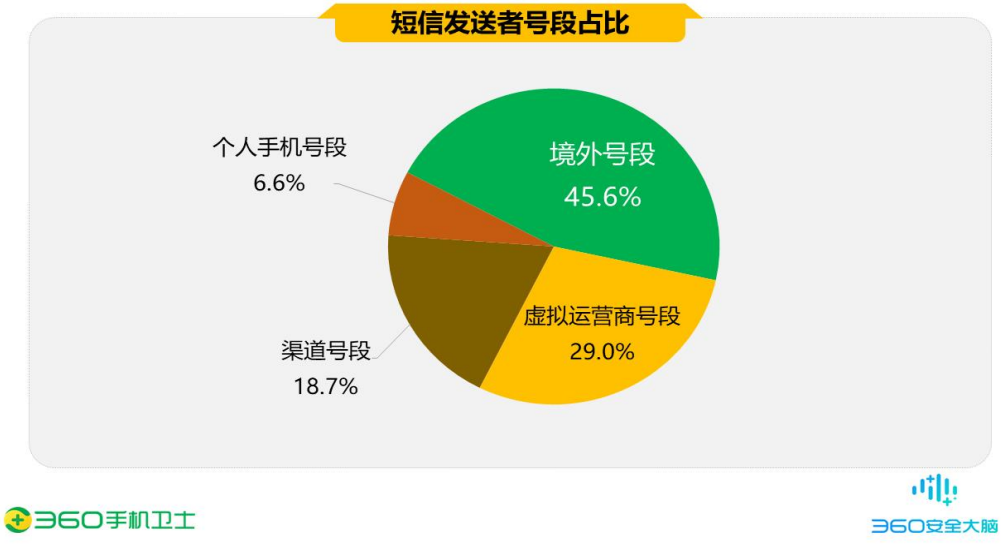
5. 疫情期间诈骗短信内预留非法联系方式统计

疫情期间，抽取 2 月份诈骗短信进行短信内预留非法联系方式统计，其中拦截 QQ 共计 4820 次，占比 2.0%；微信 9768 次，占比 4.0%；URL 231517 条，占比 94.1%；抽取短信中，赌博类诈骗短信占近 9 成，其他类型包括兼职诈骗、涉政类违法短信。预留非法联系方式去重后 QQ 725 个，微信账号 729 个，URL 5264 条。



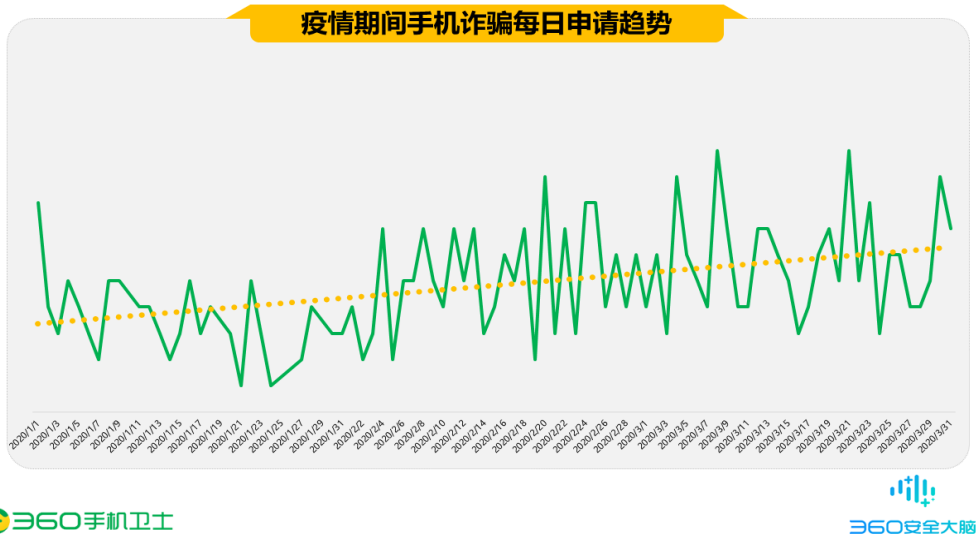
6. 疫情期间违法&诈骗短信发送者号段分布

疫情期间（0218-0331）违法&诈骗短信发送者通过运营商号段区分，境外号段占比 45.6%；其次为虚拟运营商号段（29.0%）、渠道号码（18.7%）、个人手机号（6.6%）。



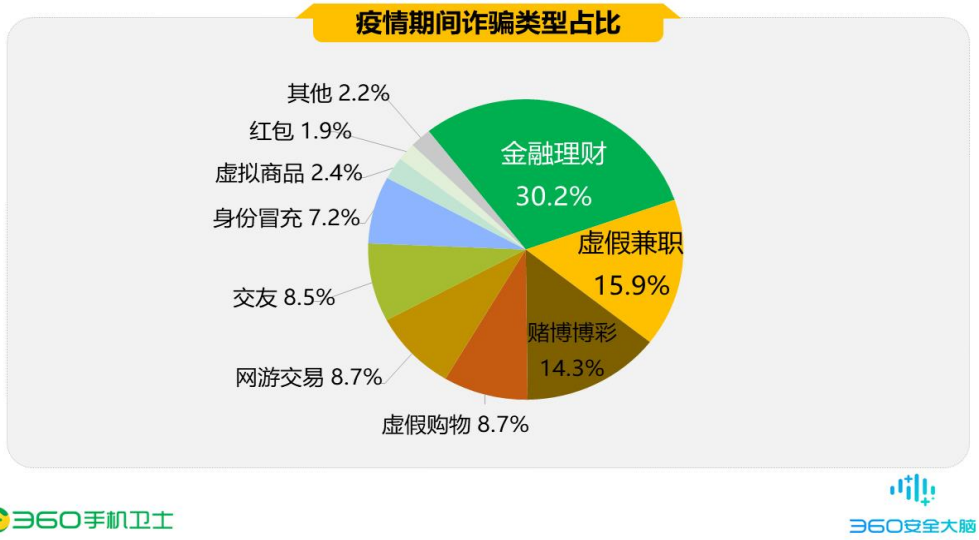
7. 疫情期间诈骗类型统计（Q1 季度）

疫情期间，手机先赔诈骗举报申请呈上升趋势。由于春节假期影响，1 月底诈骗申请量较低，目前诈骗举报申请量逐日增加，呈现回升趋势。



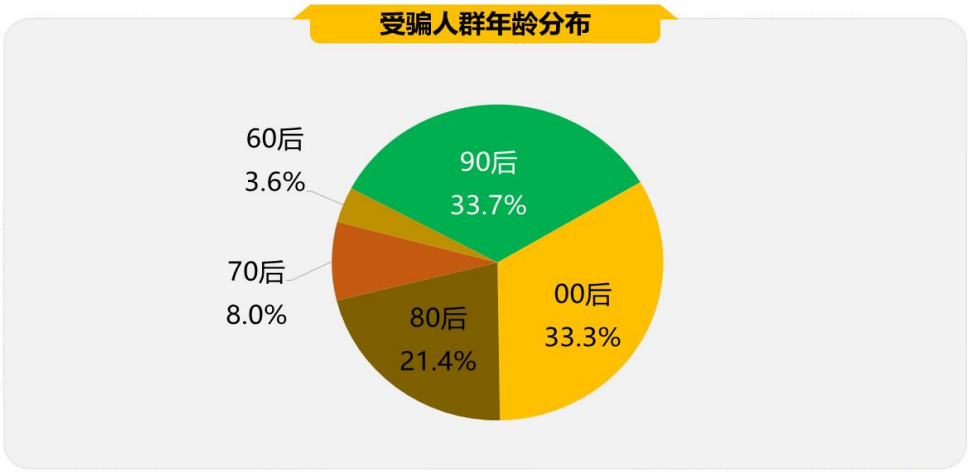
疫情期间，金融理财诈骗占据首位，占比 30.2%，反馈较多为贷款遭遇诈骗；其次为虚假兼职诈骗，占比 15.9%；赌博博彩占比 14.3%。

由于疫情居家隔离，部分民众工作收入受到影响，网络贷款成为部分人需求之一，不法分子利用此敏感时期，利用无抵押贷款、快速下款等借口诱导用户支付手续费、包装费等，从事贷款诈骗。于此同时，疫情期间在家挣钱成为欺诈宣传口号之一，导致虚假兼职诈骗受骗人数增多，主要诱导用户缴纳兼职会员费等；其次，赌博博彩一直属于诈骗类型 TOP 之一，并处于高发态势。



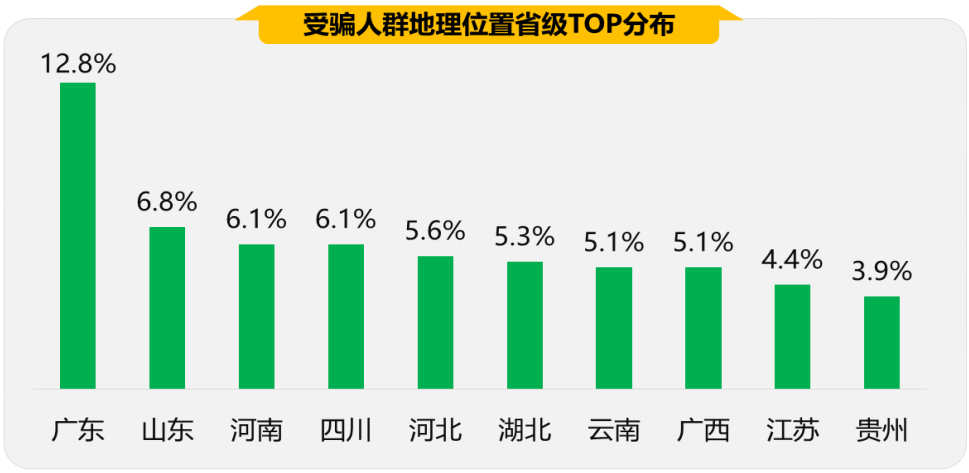
8. 疫情期间受骗人群年龄分布（Q1 季度）

疫情期间，受骗人群中 90 后占据首位，占比 33.7%；其次为 00 后，占比 33.3%；80 后占比 21.4%。

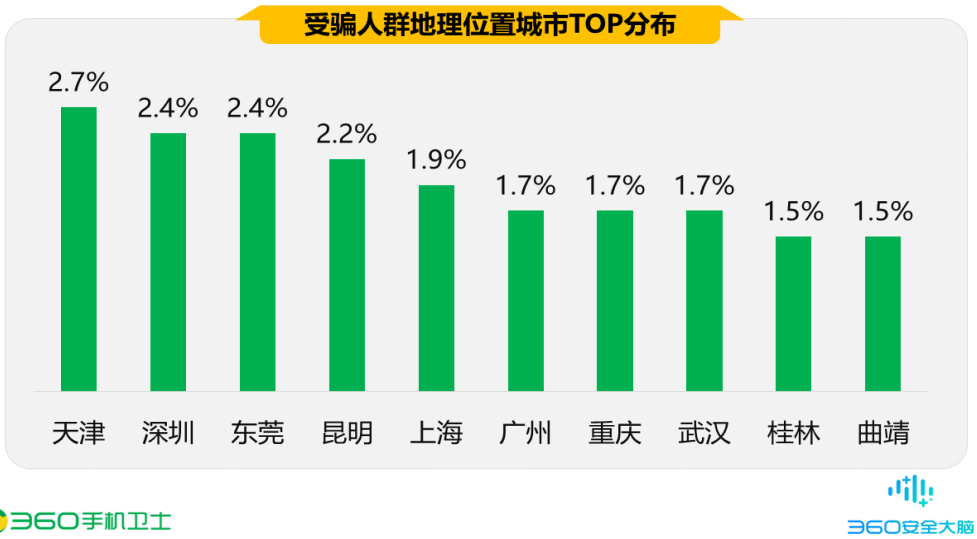


9. 疫情期间受骗人群地理位置分布（Q1 季度）

疫情期间，受骗人群地理省级分布中，广东占据首位，占比 12.8%；其次为山东，占比 6.8%；河南占比 6.1%等。



疫情期间，受骗人群地理省级分布中，天津占据首位，占比 2.7%；其次为深圳，占比 2.4%；东莞占比 2.4%等。



二、 互联网平台及技术“沦为”黑灰产敛财的工具

1. 互联网平台及技术被黑灰产利用现状

中国互联网的快速发展，造就了大量的互联网“人才”，推动并产生了大数据、云计算、物联网等技术，但这些技术行业的入门门槛相对较高。随着计算机性能的突飞猛进，“云端”模型算法能力的提升，原先“高高在上”的互联网技术，已变得“触手可及”。普通人借助“云端”模型算法的辅助，也可轻松参与互联网的开发与运营。如早期想要搭建一个门户平台，需要配备专业的网站开发人员，而现如今借助一些模块化的 H5 平台普通人也可完成门户页面搭建。

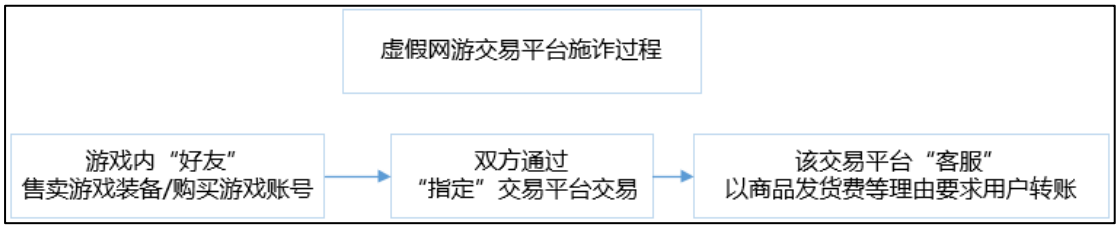
互联网技术的成熟，入门门槛的降低，本应是推动中国互联网发展的“润滑剂”，但却出现众多利用互联网技术实施不法行径的现象。究其原因是部分互联网产业及技术“被迫”成为了黑灰产用于敛财的工具。本文从黑灰产欺诈手法、原理角度“揭露”那些被黑灰产利用的互联网行业及技术。

2. 黑灰产欺诈手法原理及利用到的互联网技术

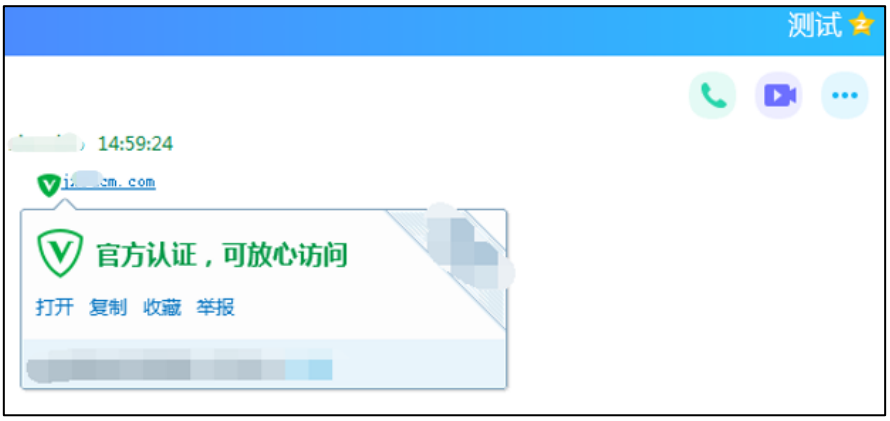
1) 使用“备案”域名搭建虚假网游平台

不法分子潜伏在各大游戏平台及交易平台，以售卖低价游戏装备或高价收购游戏账号为幌子，吸引用户添加其社交账号。待双方协商达成一致后，引导用户在指定的网游平台交易。具备较强网络安全意识的用户一般会通过网站的备案信息，来确认平台真伪。当发现平台是企业备案时便会放松警惕。于是当用户在该平台填写一系列个人信息完成注册，并在平台充

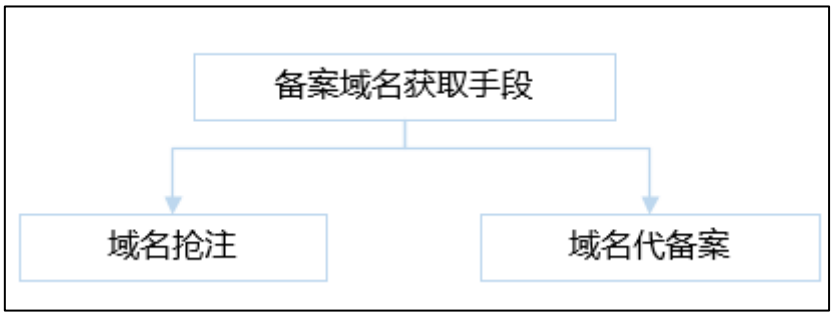
值购买游戏装备或上架游戏账号“成功”出售给买家后，便会被平台客服会以商品发货费、用户账户资料错误被冻结等理由要求用户在平台进行进一步充值或转账操作。用户按照客服要求完成一系列操作后，却发现客服仍有另套说辞要求用户继续充值或转账，用户恍然大悟，得知受骗。下图为虚假网游交易平台实施诈骗过程。



早期虚假钓鱼网站出于成本及躲避溯源的考虑，域名往往不含有备案信息，但此特征容易被网络安全产品检测识别。近几年随着游戏消费观念的升级及网游产业的兴起，不法分子也加大了对虚假网游交易平台的成本投入和技术升级，逐渐采用含备案信息的域名搭建钓鱼网站，来抵抗网络安全公司的域名检测识别。如下图展示，域名通过社交软件传播时，并没有识别出其风险行为。



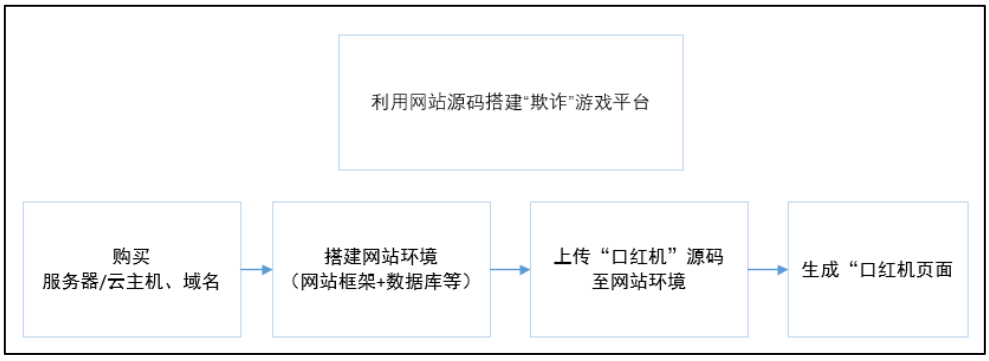
黑灰产使用的含备案信息的域名来源于已备案域名的批发商城。这些批发商城可以简单理解为一个域名“贩子”，专门售卖一些含备案信息的域名，并延展出含有攻防性质的域名，如“绿标”域名（域名通过社交软件发送时，提示绿色的官方认证，可放心访问标识）。如下图展示，这些域名商城通过域名抢注（域名过期后，原备案信息还存在）、使用个人/企业信息进行域名代备案等方式掌握到获取大量备案域名，并将此类域名根据域名性质（企业、个人）、域名接入商、社交软件/网络安全厂商是否拦截进行分类并售卖。



域 名	价格	接入商	备案号	性质	介绍	到期时间
z c.top	120元	景安	豫icp备1 542号-8	企业	景安备案,微信无拦截!	2020-11-20
nor net.com	170元	其他	吉icp备15 314号-1	企业	其他备案,微信无拦截!	2020-12-10
gor wang.net	200元	西部	皖icp备17 42号-1	个人	西部备案,微信无拦截!	2021-01-15
lar ji.net	200元	西部	苏icp备17 42号-6	个人	西部备案,微信无拦截!	2021-01-23
kn ts.com	150元	其他	滇icp备16 3号-1	个人	其他备案,微信无拦截!	2020-07-11

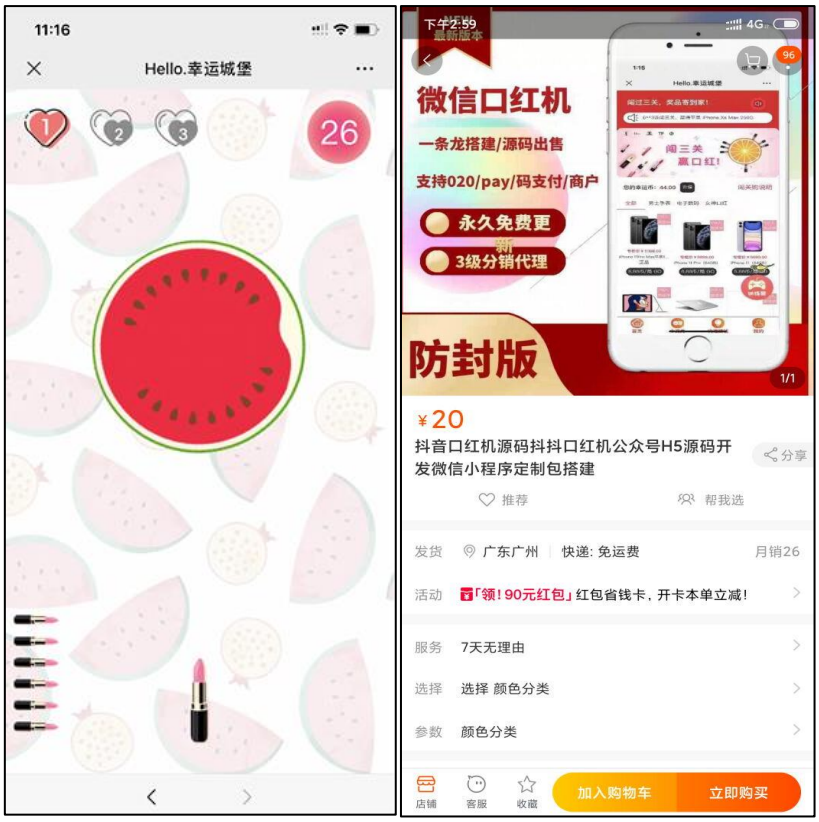
2) 利用网站源码搭建“欺诈”游戏平台

早期中国计算机资源缺乏，开发难度大成本高，为降低开发成本难度，出现了一些帮助企业快速建网站的程序 CMS。近些年随着中国互联网的快速发展，互联网共享精神得到推广，各类开源程序在互联网涌现。 如下图展示，利用服务器、域名，网站框架、网站源码即可完成平台的搭建。甚至部分云服务厂商在售卖云服务器时，已经将网站环境搭建好，用户只需上传网站源码，绑定域名即可完成平台搭建。



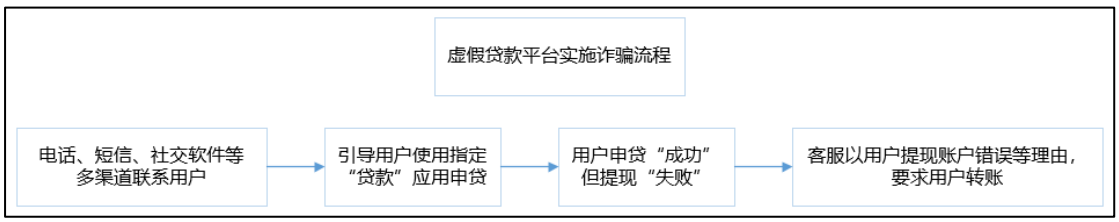
而作为搭建“欺诈”类游戏平台最重要的网站源码，在搜索引擎、电商平台也随处可见。在售卖源码的过程中，一方面提供演示站供买家了解平台使用方式，一方面提供安装教程，甚至提供躲避网络安全厂家识别出其风险的手段。

如下图展示，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的线上版口红机。就是借助源码快速搭建出来的。由于其玩法简单，短期内在互联网风靡。试玩环节，操作简单，给用户一种易中奖的假象，但由于此类平台商家可以设置游戏难度，修改中奖概率，即使玩家投入大量资金，最终也无法获得奖品。

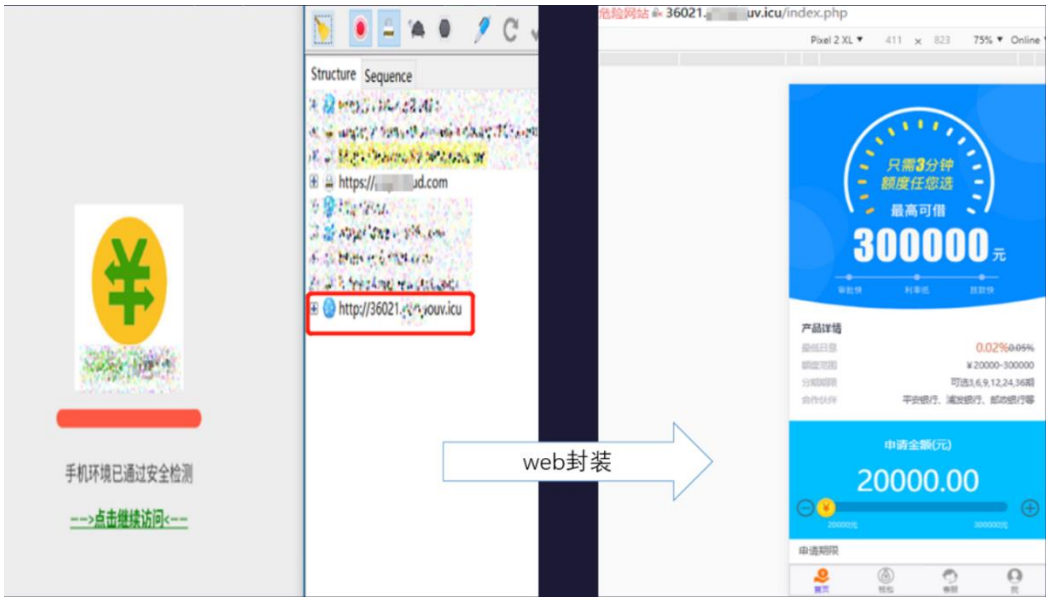


3） 利用封装分发平台搭建虚假贷款平台

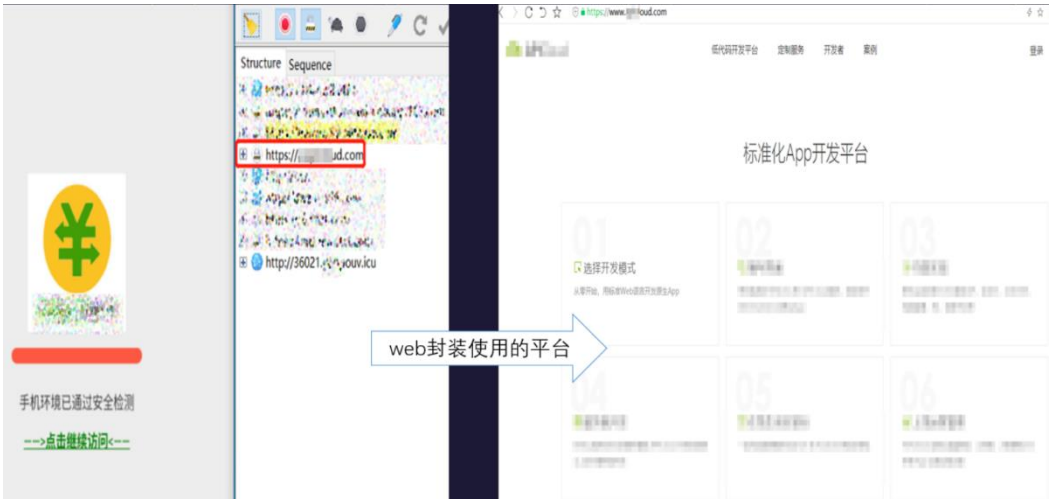
如下图展示的虚假贷款平台实施诈骗流程，不法分子首先通过短信、电话、社交软件等方式联系用户并取得用户信任后，引导用户使用指定的虚假贷款 APP 申请贷款。待用户在平台上传完个人信息后，便给用户推送资质审核短信，引导用户在平台提现。当用户在平台提现时，平台则显示用户征信不足、提现银行错误，账户被解冻，要求用户缴费解冻；甚至设置平台提现密码，索要提现密码费。即使用户按照要求向对方转账，对方也不会给予用户放款。



在对应用逆向分析后发现虚假贷款 APP 使用了封装平台的 WEB 转 APP 技术，并通过分发平台将 APP 制作成应用下载链。



360企业安全 360手机卫士 360安全大脑

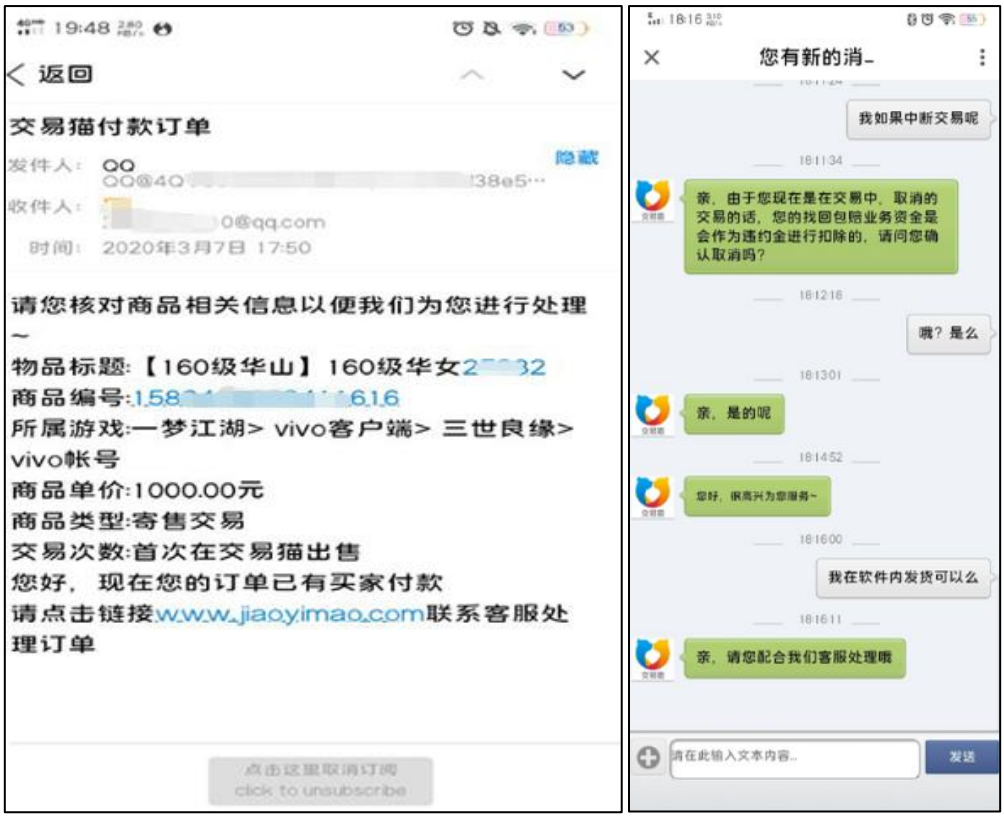


伴随着互联网的发展，除了数不胜数的网站外还有众多建设网站的教程。相较于手机 APP 产业，网站开发产业成熟度和规模都大的多，将 WEB 直接转成 APP 成为了开发 APP，降低开发难度及成本的首选。同时对于黑灰产人员而言，WEB 转 APP 还可以批量生成多个虚假平台。如下图展示，在封装平台，提交网站信息、需生成的 APP 图标、APP 名称后，即可将 WEB 页面封装成 APP。

APP 分发平台是一种应用托管服务，开发者可以将应用上传至分发平台，由平台提供应用下载链方便应用开发者将应用进行传播。此种平台原意是解决 APP 短暂无法上架 APP 应用商店的问题，但由于其无需像传统的手机应用商店需要严格的应用风险审核和身份验证，近年来 APP 分发平台逐渐沦为黑灰产实施诈骗的工具。如下图展示的应用分发平台，在平台注册（无需实名）后，上传应用安装包后，即可生成应用下载链。

4) 利用第三方在线客服平台冒充网游交易平台“官方”客服

用户在游戏交易平台上架出售自己的游戏账号后收到买家的信息，对方以确认下单需求填写用户信息为由，索要了用户的 QQ 账号。 随后给用户发送了“已下单，已用 QQ 邮箱邮件方式告知卖家发货”的截图。用户 QQ 邮箱收到了“付款订单”邮件后，便访问了邮件内容内的“游戏平台交易”网站，与该网站内的在线客服沟通后，网站内客服以防止用户不发货为由，要求用户缴纳保证金。用户按照客服指引转账后，客服却以用户的积分未达到安全转账为由，要求用户继续转账，用户发现受骗。



通过对用户收到的“付款订单”邮件内提及的网站分析，发现该诈骗团伙首先利用了邮箱的超链接功能。虽表面看起来是访问 www.jiaoyimao.com，但点击该网址后却会跳转至第三方在线客服的网址。之后再利用第三方在线客服平台网站冒充网游交易平台，诱骗用户缴纳所谓的网游交易保证金。

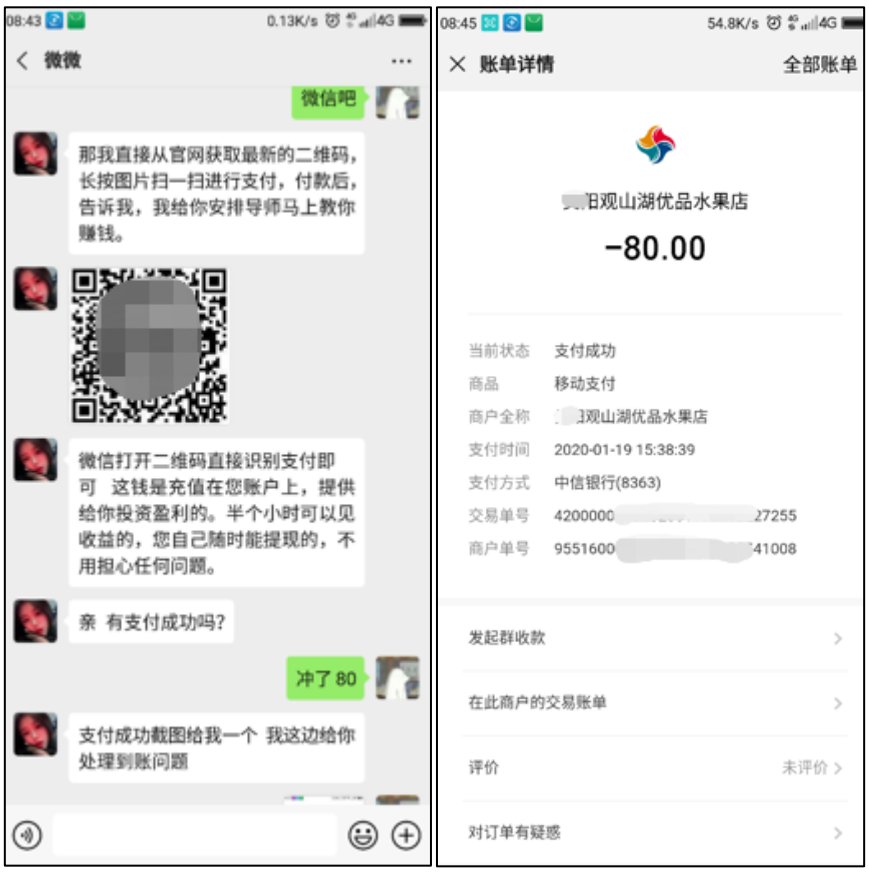
第三方客服系统类似于 CMS（网站内容管理系统），本身是帮助企业解决平台客服接入管理问题。通过平台接口的方式接入企业平台，降低企业研发和运营成本。但随着网络安全

360企业安全 360手机卫士 360安全大脑

监管的升级，黑灰产人员使用的 QQ、微信等社交账号存在易被查封关停的风险。为解决查封问题，黑灰人员盯上了第三方客服系统，利用“虚假”的认证信息，将第三方客服系统接入到黑灰平台，为虚假平台提供在线客服服务。

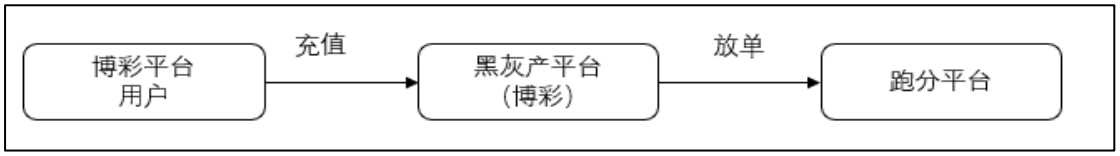
5） 利用第四方支付平台实现黑灰产平台充值、提现、资金“洗白”

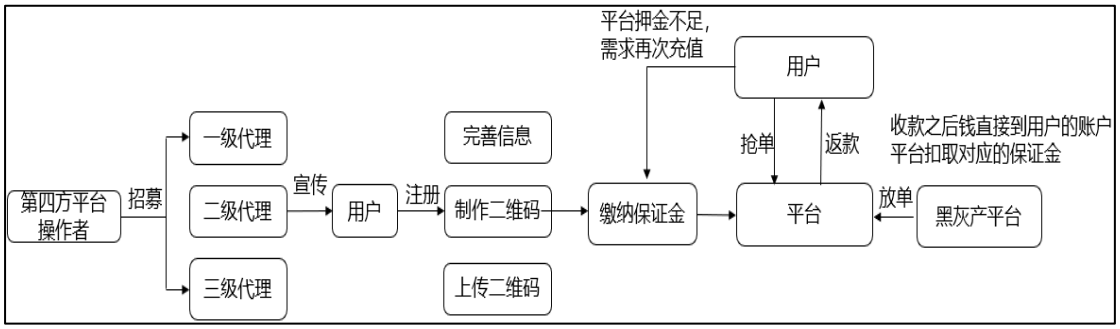
网络博彩是违法的行为。他们自己的收款账户很容易被查被封，为了降低风险和逃避打击，他们借助第四方支付平台提供的收款账户进行资金流转。第四方支付平台指的是未获得国家支付结算许可，通过大量注册/收集商户或个人账户，非法搭建的支付通道，非法对外提供支付结算服务。黑灰产平台由于无法使用正规的支付接口，多采用第四方支付平台提供的接口。如下图展示某博彩平台提供的收款二维码及支付截图，使用的就是商户类收款账号“水果店”。



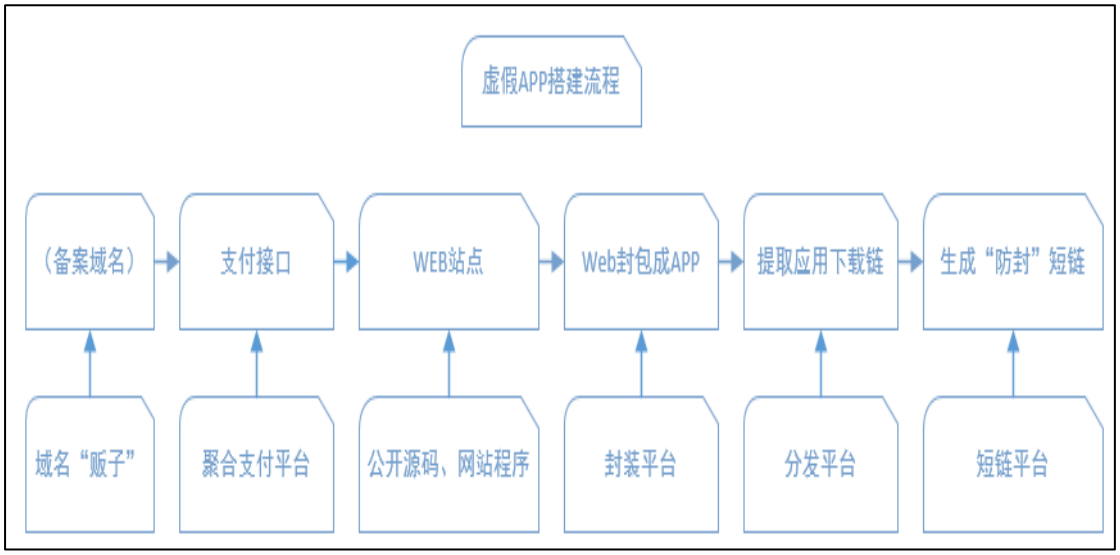
第四方支付平台为快速收集大量的商户或个人收款账户，搭建了跑分平台。跑分平台类似兼职平台中介。兼职用户在跑分平台缴纳押金，将自己的收款二维码“租借”给跑分平台，博彩平台将跑分平台提供的收款二维码用于博彩平台充值收款二维码。博彩用户向此收款二维码转账，完成赌资充值后，博彩平台给跑分平台支付佣金，跑分平台给兼职用户返回佣金。如下图展示的跑分平台的作用及操作流程。

360企业安全 360手机卫士 360安全大脑





借助以上成熟的互联网资源，我们可以发现开发、运营、推广一个黑灰产平台，已变得十分容易。于此同时黑灰产也从早些年的小团伙单打独斗转型到具有专业知识的“集团化”作战。在集团化作战过程中，黑灰产不断整合互联网上可以利用的平台与技术，并不断完成更新迭代。如在虚假贷款产业，黑灰产人员就利用了互联网众多的平台与技术。APP 搭建人员，从域名“贩子”手中 买到大量（备案）域名或境外域名，使用公开的源码或网站框架，接入第四方支付接口搭建网站。通过一些 web 封装平台将网站封装成 APP 并将 APP 上传至应用分发平台获得应用下载链，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。



3. 黑灰产欺诈手法的攻防策略及演变

从以上章节内容可以看出黑灰产的攻防策略不是一层不变的，会随着网络技术及网络安

360企业安全 360手机卫士 360安全大脑

全的技术不断发展而演变。一方面提升欺诈环境的仿真度，防止被用户识别。一方面借助攻防策略的升级来躲避网络安全、社交软件等产品对欺诈样本的识别。

在黑灰产样本方面，为了防止网站在互联网从事非法的经营活动，打击不良互联网信息的传播，在中国境内提供非经营性互联网信息服务时，需办理域名备案。众多黑灰产团伙为躲避信息溯源，实施诈骗的域名往往不含有备案信息。网络安全、社交软件等厂商掌握这一黑灰产特征后，利用域名有无备案信息，快速识别出大量存在高风险的网站。随着时间的推移，黑灰产开始给自身装备含备案信息的域名，来抵抗网络安全公司的域名检测识别。网络安全厂商掌握到这个情况后，针对这一特征，利用域名的备案信息、网页内容、经营范围、whois 历史节点等多个特征综合识别出钓鱼网站。

黑灰产自己制作的钓鱼网站躲避安全厂商识别的难度越来越高，于是开始借助第三方技术服务提供商（第三方封装、分发平台等）对自身进行包装。借助第三方封装平台封装出来的应用，由前文可知其本质是调用网站页面，一般不会像传统的恶意应用那样，恶意获取用户的设备权限，触发安全软件的“报警”机制，在一定层度上躲避了安全厂商的应用（恶意权限）识别。由前文可知第三方分发平台，由本质是一个应用商店，且第三方分发平台多为企业运作，其域名也含有此些企业的备案信息，网络安全厂商针对钓鱼网站识别的方式在此类平台无法使用。于是黑灰产借助第三方封装、分发平台包装出的产品，一方面躲避了安全厂商在应用层面的识别，一方面躲避了安全厂商在传播渠道的下载链识别。随着网络安全厂商的技术升级，一方面借助应用沙箱识别出应用调用的钓鱼网页，判断出应用存在的风险，从应用层面切断此类应用造成的恶意影响。一方面借助应用特征码，识别第三方分发平台传播的应用下载链内的应用是否存在高风险行为，对网址进行识别。

在黑灰产资金方面，移动支付的普及，极大便利了用户的生活，但第三方支付平台的严格监管，非法网站无法直接接入，于是一些非法第四方支付平台，特别是跑分平台应运而生。由前文可知，黑灰产平台使用的传统收款账户(银行账号)、第三方收款二维码，由于其数量有限，在短期内收到大量的个人账户汇款，易被管控限制其收款功能。借助第四方支付，获得了大量的个人、企业收款账户，由于其转账行为是单对单（博彩用户转账给跑分平台用户或其他私人账户），从表面上看未直接与黑灰产平台的资金池(账户)产生联系，短期内不会被限制其转账收款行为，在一定层度上躲避了金融行业的风控。

4. 防范互联网平台及技术被黑灰产利用的应对措施

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。黑灰产业也在不断的发展，从 PC 互联网时代“单兵”作战，到移动互联网时代“集团化”作战。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行业与黑灰产“企业”不断厮杀成长的一场持久战。面对黑灰产的厮杀该如何应对？

1） 平台审核机制规范化，加大二次校验力度

诈骗事件多发，究其原因，一方面是由于黑灰产资源售卖渠道多、开源程序多、制作教程多，搭建成本低、搭建难度低。通过搜索引擎、电商平台等渠道可以找到众多的源码。此些源码中，甚至存在一些法律禁止或打“擦边球”的项目，如博彩平台源码。作为渠道入口的平台，需要对此些违规的产品进行过滤，降低其在搜索结果中的权重，降低其造成的影响。

一方面是由于第三方技术平台对于其服务的使用者，没有进行完善的资格审核和二次校验。如使用第三方客服平台的注册人为某科技有限公司，但实际使用此第三方在线客服服务者是博彩平台。平台在前期校验购买服务的资格后，仍需要对使用者进行监督，防止平台被利用。

2） 关注黑灰产动向，针对黑灰产手法，通过多种方式实时调整识别拦截手段

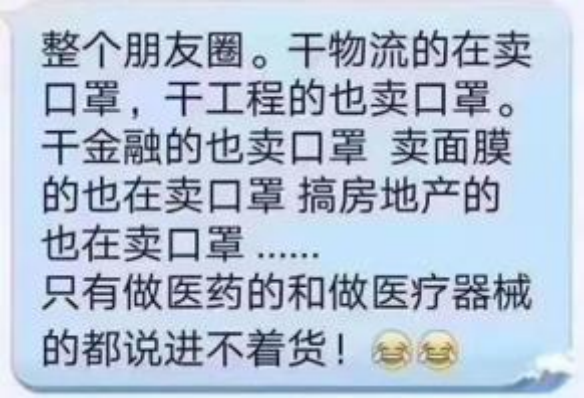
黑灰产在技术、话术等多方面，不断完善其自身的诈骗手法，防止在实施诈骗的过程中被识别。如诈骗团伙在使用未含备案信息的域名被安全厂商识别出诈骗特征后，转而开始利用含有备案信息的域名来躲避安全厂商对于欺诈类域名的识别。双方呈现出动态博弈的特征。

面对此种现象，安全厂商不能仅仅“盯着”实施诈骗的样本本身，进行事后拦截。需要从黑灰产业链的角度，看待诈骗事件。如针对诈骗团伙使用的备案域名，需了解备案域名的来源、原理、买卖方式。一方面拦截售卖渠道、一方面通过域名 WHOIS 历史节点、同源（IP）网站内容特征、历史节点内容快照等多种方式，实现对网站的识别，而非仅仅通过域名的备案信息判断网站真伪。

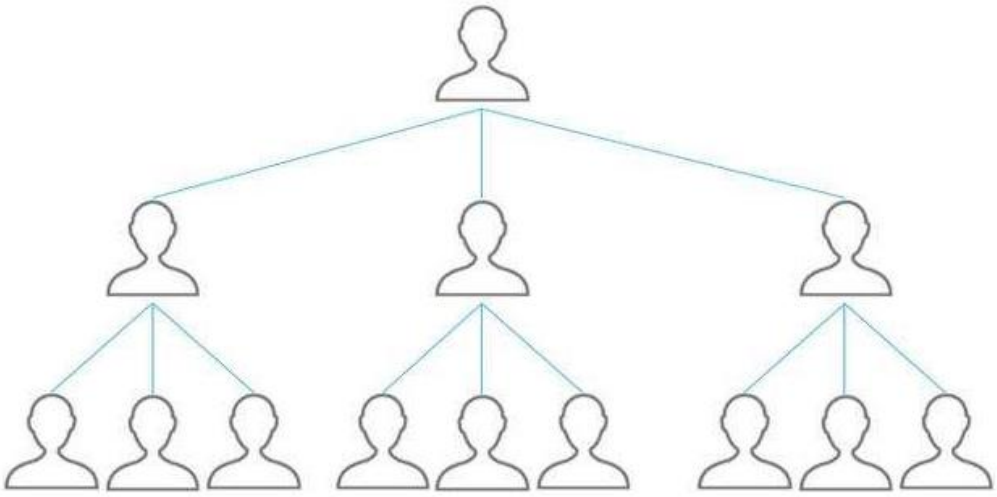
第七章 2020 年第一季度典型诈骗“剧本”

一、 疫情当前，骗子们将口罩做成了资金盘

随着新型冠状病毒肺炎疫情的出现，口罩这一生活中常见的物品，从国内电商到海淘代购，货源被“洗劫”一空。口罩瞬间成了稀缺物品，一罩难求。面对强盛的口罩需求，各类潜伏在朋友圈、QQ 群的“微商”、“代购”，纷纷“闪现”，不管以前卖的是啥，现在统一口径，卖口罩。更有甚者，玩起了“口罩”资金盘。



资金盘是将不动的资金变为流动的资金，将个人手中闲散的资金利用起来，用于保值、增值。但随着融资形式的发展，经过一部分人的加工和修饰，就异化为这样一种现象：它向社会不特定的对象吸收资金，根据行业内游戏规则，承诺高额返利。表面看上去是资本运作，实质却是庞氏骗局。



旁氏骗局即“拆东墙补西墙”“空手套白狼”，利用新投资者的钱向老投资者支付利息和短期回报，以制造赚钱的假象进而骗取更多的投资。“口罩”资金盘和 2019 年分析过的众筹还款、互助盘等资金盘诈骗手法类似，具有相同的施诈套路。

步骤 1:借助热点需求，吸引用户关注

众筹还款看重了负债者无钱还款的窘境，提出了“众筹”还款理念，帮助负债者快速解决负债，点燃了负债者的希望。口罩资金盘看重了口罩市场需求旺盛，但无法买到口罩的窘状，提出了口罩拼团的概念，点燃了缺乏口罩人群的希望。

步骤 2：设置入门门槛

众筹还款需提供负债证明、缴纳平台激活费 400 元。口罩资金盘有口罩数量起卖限制，最低 1 千至 1 万个起售。

（上图取自互联网）

步骤 3：邀人拉下线，打造资金盘金字塔

1. 众筹还款

根据个人负债金额制定一个众筹计划，把个人负债金额分成几个众筹阶段来完成。每上升一个阶段，下线需推荐三名负债者参与众筹。首次激活时需缴纳 400 元，其中 200 元给推荐人，200 元给第九阶段众筹者。每次上升阶段需给上级 200 元。以此类推至第九阶段时可以众筹 3936600 元。

360企业安全 360手机卫士 360安全大脑

2. “口罩”资金盘

5000 至 1 万个口罩的起订量，对于普通消费者而言是无法满足这个条件的。卖家会建议用户邀请他人一起拼团，力求早日达到起订目标。同时表示口罩需求量大，价格涨幅快，后期买更贵，早买还可以转手赚一笔。

步骤 4：资金盘终点始终到达不了

1. 众筹还款设置了九个众筹阶段，想要实现依靠众筹还款完成自身的还款愿望，达到第九阶段需要邀请一共 19683 人（含自己下线所邀请），难度之大可想而知。
2. 口罩“资金盘”设置了发货标准，用户需拉着众多好友一起在“商家”处付款预订口罩，但卖家始终未发货。通常卖家会使用以下几种话术拖延用户。

话术 1:

你这边没到 1 万个起订量，剩下的是跟外边的人一起拼的，目前正在跟工厂对接，定金已经下了，很快就能生产出来。

话术 2：

已经跟工厂对接上了，工厂排期长，需要生产周期的，而且口罩还需要消毒等一系列操作，耐心等待就是。

话术 3:

工厂那边有变动，原材料不够，又是春节期间，我们的单子需要往后延迟，但下一批就

360企业安全 360手机卫士 360安全大脑

是我们的了。

话术 4：

口罩已经生产出来了，现在物流还没完全恢复，全国运力紧张，工厂那边和物流还没对接好，别着急，再等等就可以发货了。

步骤 5 资金盘跑路，投入的资金被骗

1. 众筹还款计划

用户参加时，前期缴纳了费用，为了早日达到众筹目标，甚至还邀请众多好友参加，陷入了一种泥泞的境界，无法抽身，最后面临平台跑路被割“韭菜”的结局。

2. 口罩资金盘

1) 用户过长时间没有收到口罩，产生了退款的想法，但再次联系对方时，可能已联系不上对方。

2) 遇到“良心”商家，可能会给用户发送假的口罩。

3) 或者待口罩价格回顾正常后，才给用户发送口罩。但对于用户而言，无论哪种情况，在最需要的时刻还是没有买到口罩。

案例分析

对于资金盘类骗局，由于其本质是“空手套白狼”。利用新投资者的钱向老投资者支付利息和短期回报。短期看起来有盈利的假象，但最终的结局就是步入死循环继而崩盘跑路。在如今浮躁的网络社会里，网络金融到处充斥着一夜暴富的梦和陷阱，很多不明真相的人投资只盯着高利息，而忘了资金安全才是最重要的。就像口罩一样，在全中国都缺口罩的情况下，这些无资质的，无平台的“微商”一出口就是上万个口罩货源，这本身就是假的命题。

防骗提醒

1. 购买防护用户，建议通过官方或正规渠道购买，交易过程受到保障，商品质量也有保证。

2. 网络中与陌生人产生金钱交易时，需提高谨慎。遭遇需要预付定金时，需要“三思而后行”，以免被骗。

3. 网络中所获取到的陌生链接不要随意点击访问，保护好自己的账户信息，不要轻易在网

页内填写个人敏感信息，以防泄露。

二、 抖音成新型传播渠道，金融理财你来不来？

随着短视频的火爆，抖音、快手等平台成为了广告主的新宠儿。各类视频广告变着花样的模仿各类网红视频吸引用户关注。如兼职赚钱类广告，场景放置在约会、相亲。双方分享赚钱绝技（使用某赚钱 APP），引导用户点击下载该应用。此些应用良莠不齐，近期就有 360 手机先赔用户在抖音平台下载兼职赚钱理财应用，在应用投资后受骗。

案例经过

1. 用户在 2020 年 3 月 10 日，在抖音看到网赚广告（用户描述，该抖音视频下方含广告字样），下载了“单理希”应用。
2. 用户在该平台使用手机号注册后，在平台内看到了“个税申报专用项目”,“共享汽车投放”等项目。此些项目在周期结束（1 天至 10 天不等）后可获得高额的利息收益，收益达 100 元才可提现。
3. 用户通过向指定银行转账的方式，在平台充值 1 万元，购买了共享汽车项目（周期 7 天）。该项目到期后，用户成功提现 11204.64 元本息。3 月 21 日用户又在平台充值 3000 元，购买共享汽车项目（周期 8 天）。
4. 项目到期后，无法提现，客服以提现需交税为由，引导用户缴纳 1000 元税费。用户缴纳后，又以提现保证金为由，要求用户继续转账，用户发现受骗。

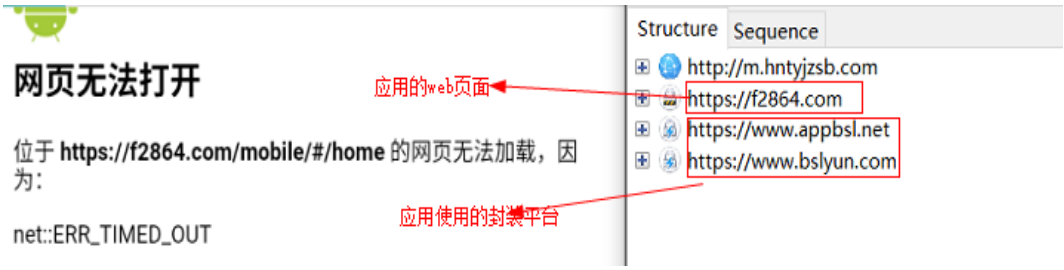
案例分析

1. 从渠道上来看，短视频平台像搜索平台一样，逐渐被黑灰产攻陷。从去年出现的视频博主卖假龙虾事件，到现在利用“官方”广告推广虚假平台。对于用户而言，鉴别难度越来越大，特别是经平台认证后加“广告”标识的。

   新闻链接：https://www.sohu.com/a/317978574_120136920

2. 从诈骗手法上看，此类平台，与去年发现的电影投资、共享投资等项目相同，采用旁氏骗局的方式。即“拆东墙补西墙”“空手套白狼”。利用新投资者的钱向老投资者支付利息和短期回报，以制造赚钱的假象进而骗取更多的投资。用户前期可以提现成功，后期一旦参与的人数增多，旁氏资金盘就会断裂，后期进入的资金无法填补提现资金的缺口，平台资金流崩塌，平台开始转移资金跑路。这个平台唯一不同的是，平台在跑路前，为压榨投资人的剩余价值，还以提现交税、保证金等理由，索要用户资金。

3. 从样本的类型看，此平台属于 web 封装的应用，应用使用的封装平台为变色龙平台。APP 对应的 web 页面一旦关闭，APP 则无法打开，用户想事后保留证据，都无法保存。f2864.com 在 2019 年 11 月 15 日手机卫士已进行拦截并予以提醒。



防骗提醒

1. 正规公司的运营信息透明化，参与投资理财项目的投资者可以随时了解平台资金运营情况。请擦亮眼球，不轻易相信虚假平台或不正规的投资理财 APP。
2. 参与投资理财项目前，建议事前了解行业内发展现状及趋势，慎重选择投资理财产品。
3. 所有承诺投资项目保证盈利、投资者不需要承担风险的投资理财平台，极有可能存在问题，不要轻信。