2022 年第一季度

中国手机安全状况报告

2022 年 05 月 13 日

前言

随着移动互联网技术的高速发展，犯罪结构发生了根本性变化，以电信网络诈骗为代表的新型犯罪日益猖獗、危害巨大，特别是新冠疫情背景下，人们生产生活加速向网上转移，进一步加剧了案件的高发。隐私窃取、网络洗钱等行为，以及隐藏在背后的工具、资源、平台、渠道已经形成了一系列稳定且生态化的黑灰产业链条，社会合力共治刻不容缓。

近年来，利用互联网技术衍生出的黑灰产犯罪行为越来越专业，职能分配更加精细，诈骗方式越来越“职业化”。现如今的诈骗集团呈现出多行业支撑、产业化分布、集团化运作、精细化分工、跨境式布局等跨国有组织犯罪特征。同时诈骗分子也紧跟时事热点，不断升级话术，“量身定制”剧本，实施“精准”诈骗。

2022 年第一季度发现，黑灰产业在渠道引流、洗钱手段等均进行了“迭代更新”，攻防对抗也在不断升级。从诈骗手段看，诈骗分子利用区块链、虚拟货币、AI 智能、GOIP、远程操控、共享屏幕等新技术新业态，不断“优化”犯罪工具。从通讯网络通道看，利用境外加密聊天、小众聊天进行引流，进而躲避监管打击。从资金通道看，传统的三方支付、对公账户洗钱占比逐步减少，大量利用跑分平台加虚拟货币洗钱。

《2022 年第一季度中国手机安全报告》将从电信网络诈骗手法、洗钱方式、产业链为切入点，依托 360 安全大脑能力，深度剖析电信网络诈骗，对相关反制手段、思路予以探讨。360 也将积极发挥自身技术优势，综合运用人工智能、大数据、云计算等技术手段有效打击涉诈产业链，维护用户网络安全。

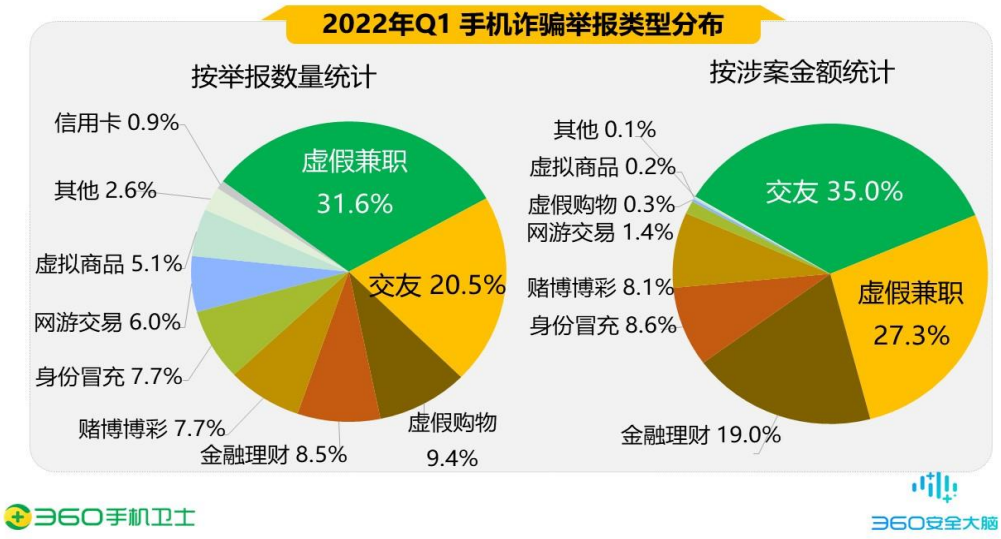
目录

第一章 2022 年第一季度手机诈骗概况

一、 用户举报

1. 报案数量与类型

2022 年第一季度 360 赔付保（原手机先赔）共接到 11 类手机诈骗举报，涉案总金额高达 273.5 万元，人均损失 23375 元。在所有诈骗类型中，虚假兼职占比最高达 31.6%；其次是交友（20.5%）、虚假购物（9.4%）、金融理财（8.5%）、赌博博彩（7.7%）等。从涉案总金额来看，交友类诈骗总金额最高，达 95.8 万元，占比 35.0%；其次是虚假兼职诈骗，涉案总金额 74.6 万元，占比 27.3%；金融理财排第三，涉案总金额为 52.1 万元，占比 19.0%。下图为 2022 年第一季度手机诈骗的举报类型与涉案金额分布情况：



2022 年第一季度，手机诈骗中交友、虚假兼职、金融理财属于高危诈骗类型，其中，金融理财人均损失最高，约 5.2 万元；其次为交友类人均损失约为 4.0 万元。

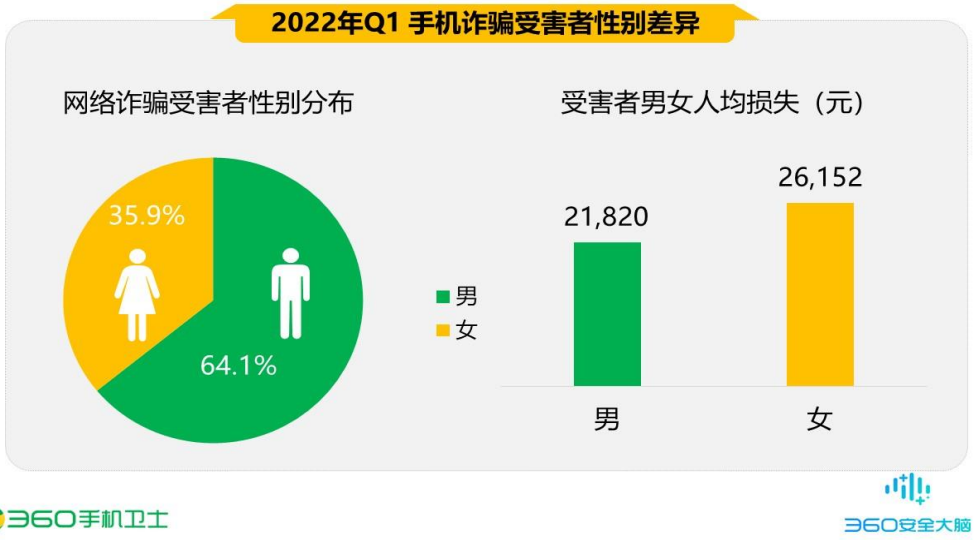
1) 2022 年第一季度中交友类诈骗仍以裸聊遭欺诈为主，但与去年对比，裸聊敲诈类诈骗在引流渠道和 APP 诈骗样本上均发生了改变。引流渠道从早期传统的社交软件，转向境外对端加密聊天软件，使得监管难度加大。同时在 APP 诈骗样本中对回传数据的代码进行混淆，并增加端口校验，提高了攻防识别难度。

2) 2022 年第一季度中虚假兼职类诈骗仍以刷单赚佣金为主，但项目名称从原先的虚假博

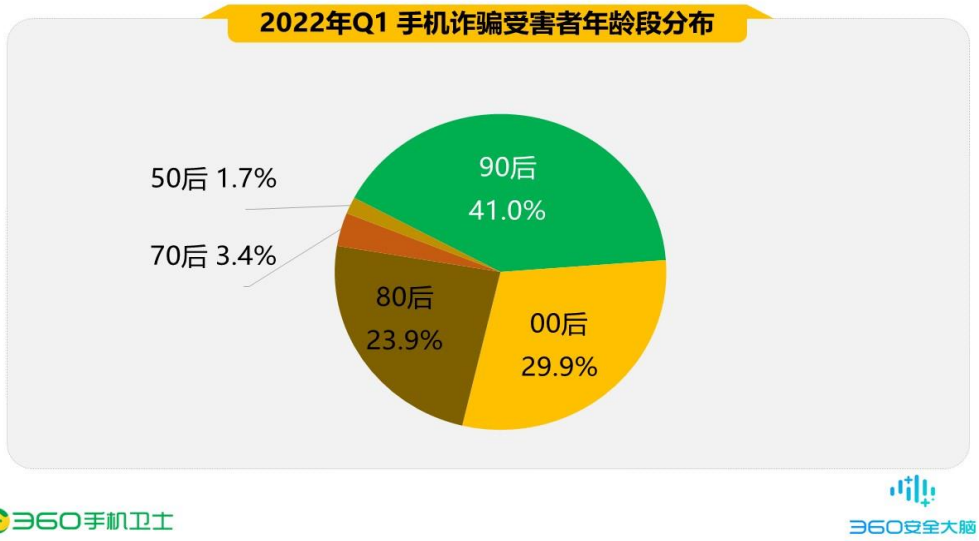
彩平台、虚假投资平台刷单，变成公益平台刷单。实际上公益平台仅是将原先博彩平台中的项目名称改成公益，但对于受害人来说迷惑性更强，识别难度更大。

2. 受害者性别与年龄

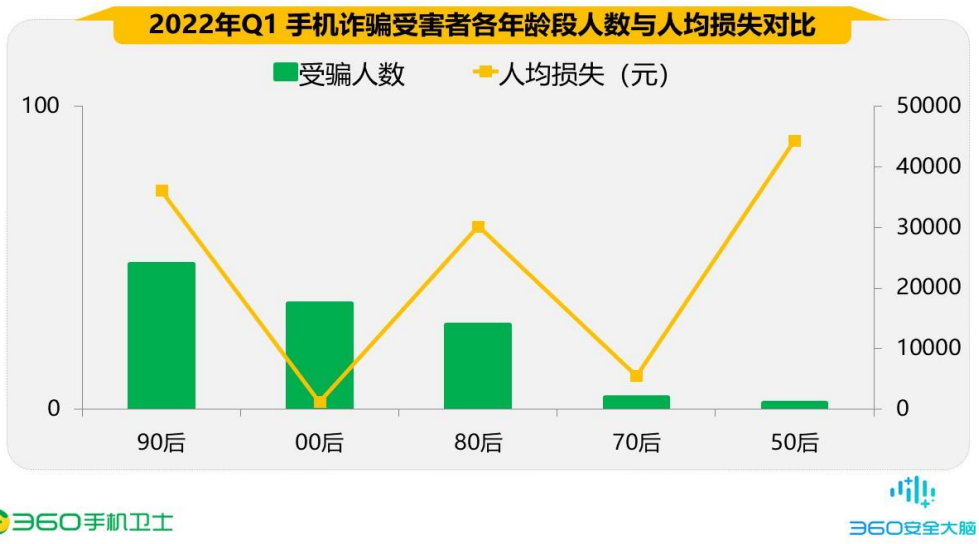
2022 年第一季度，从举报用户的性别差异来看，男性受害者占 64.1%，女性占 35.9%，男性受害者占比高于女性。从人均损失来看，男性为 21820 元，女性为 26152 元，男性人均损失低于女性。下图为 2022 年第一季度手机诈骗受害者性别差异：



从被骗网民的年龄段看，90 后的手机诈骗受害者占所有受害者总数的 41.0%，是不法分子从事网络诈骗的主要受众人群；其次是 00 后，占比为 29.9%；80 后占比为 23.9%；70 后占比为 3.4%、50 后占比为 1.7%。下图为 2022 年第一季度手机诈骗受害者年龄段分布：



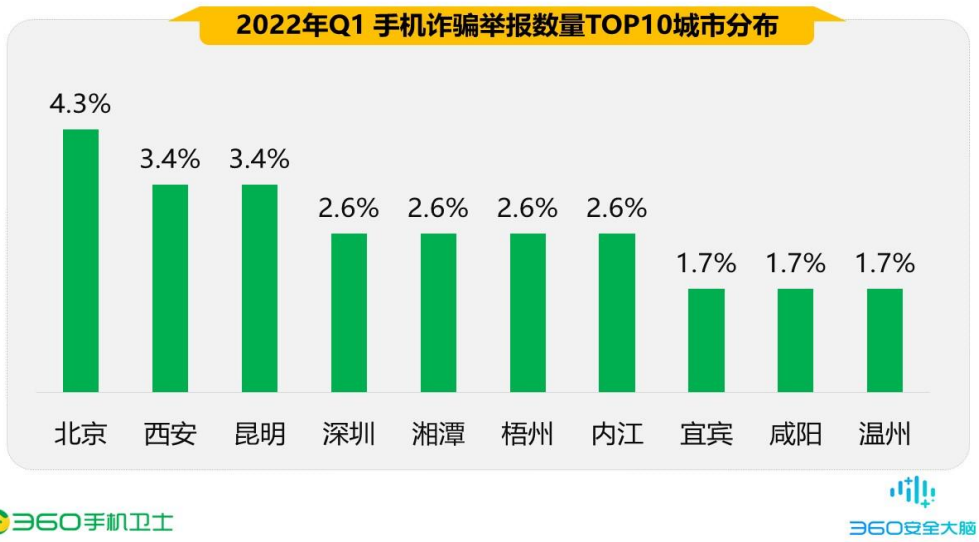
从被骗网民的年龄段及人均损失来看，2022 年第一季度， 90 后为诈骗高发人群，受骗类型主要以交友为主。疫情期间寂寞难耐，上网寻求视觉刺激，一部分成为裸聊诈骗团伙囊中“猎物”，另一部分成为虚假网络招嫖的目标。



3. 受害者地域分布

2022 年第一季度，从各地区手机诈骗的举报情况来看，山东（8.5%）、陕西（8.5%）、江苏（8.5%）、云南（7.7%）、广西（6.8%）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 40.2%。下图给出了 2022 年第一季度手机诈骗举报数量最多的 10 个省份：

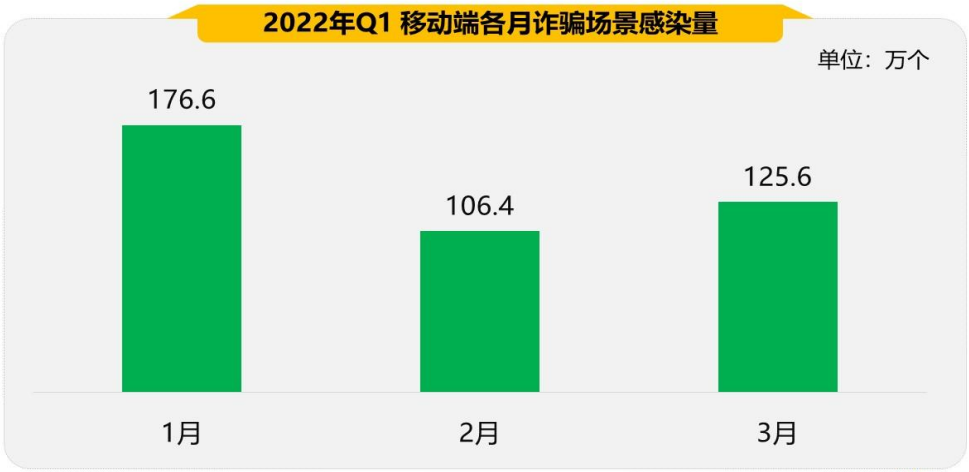
从各城市手机诈骗的举报情况来看，北京（4.3%）、西安（3.4%）、昆明（3.4%）、深圳（2.6%）、湘潭（2.6%）这 5 个城市的被骗用户最多，举报数量约占到了全国用户举报总量的 16.2%。下图给出了 2022 年第一季度手机诈骗举报数量最多的 10 个城市：



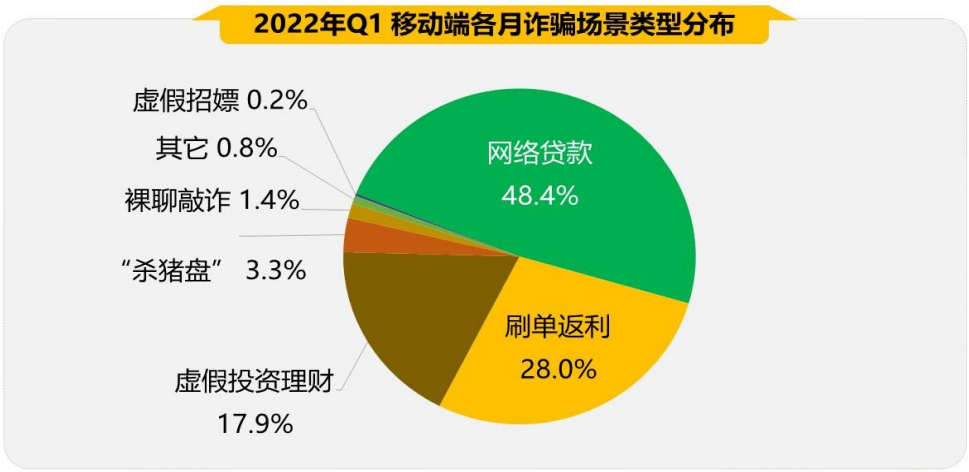
二、 场景识别

1. 移动端诈骗场景感染量与类型分布

2022 年第一季度，360 安全大脑针对移动端涉诈应用进行分析研究，通过其共识别出主流诈骗场景感染量约 408.6 万，下图为 2022 年第一季度移动端各月诈骗场景感染量统计：



2022 年第一季度，移动端诈骗场景类型主要为网络贷款，占比 48.4%；其次为刷单返利（28.0%）、“杀猪盘”（3.3%）、裸聊敲诈（1.4%）和虚假招嫖（0.2%）等。360 手机卫士安全攻防团队通过对黑灰产近年来的持续研究，发现通联类应用（使用聊天 SDK 框架生成的内嵌诈骗网页的 APP）为刷单返利场景中的主流应用，此类应用具有云控、自有生态、监管难度大等特点，360 安全大脑目前对此类应用可以实现独家识别。下图为 2022 年第一季度移动端诈骗场景类型分布：



2. 移动端诈骗场景感染量地域分布

2022 年第一季度，从省级分布来看，诈骗场景感染量最多的地区为北京，占全国感染量的 9.3%；其次为广东（8.4%）、山东（6.7%）、四川（5.9%）、河南（5.6%），此外江苏、河

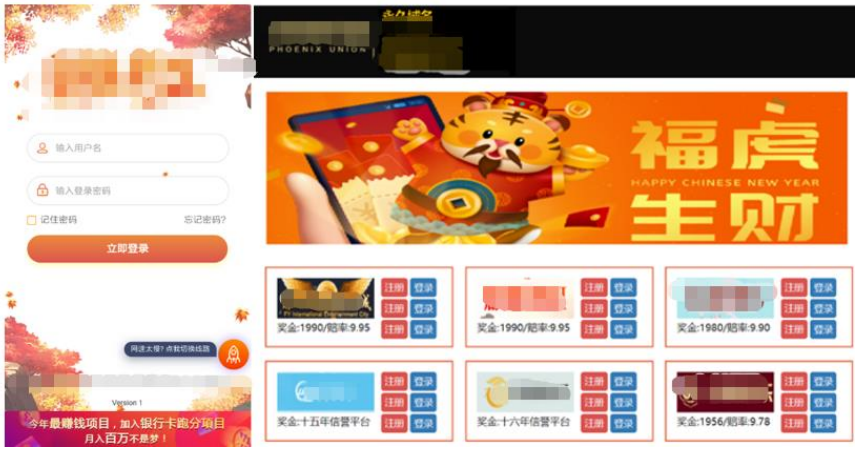
北、浙江、天津、湖南的诈骗场景感染量也排在前列。

从城市分布来看，诈骗场景感染量最多的地区为成都，占全国感染量的 2.7%；其次为深圳（2.0%）、重庆（2.0%）、广州（1.6%）、西安（1.5%），此外郑州、武汉、苏州、长沙、青岛的诈骗场景感染量也排在前列。

第二章　黑灰产趋势分析

一、　继包网平台之后，博彩联盟成博彩平台新技术、渠道商

360 手机卫士安全攻防团队在研判一款名为恒*的博彩 APP 时，发现其有别于常见的博彩应用，无注册入口，页面在线客服也不直接提供注册入口，而是引导赌客通过搜索引擎寻找注册入口，根据搜索结果页跳转的博彩导航平台入口进行注册。汇总这些博彩导航页面后发现其页面标题多包含联盟字样，例如多*联盟、凤*联盟，跳转的博彩注册链接含有特定的博彩返点参数。结合博彩平台客服描述的平台无注册入口原因“为保证代理权益，给予代理更好的发展空间，平台客服严禁参与任何开户，所以客服无法提供注册链接。请您**搜索平台关键词进行注册”。推测此类博彩平台背后可能存在一个集博彩平台开发、支付通道、游戏接口、挂机应用、跑分平台、担保中心、色情推广于一身的博彩联盟产业。



1. 博彩平台隐藏注册入口，通过搜索引擎、色情网站引流

恒*APP 打开后，首先映入眼帘的是界面中的“跑分”关键词，由于没有注册入口，很难将其与博彩平台相关联，会误以为是跑分应用。通过 360 安全大脑对 APP 分析，发现其为封装 WEB 类 APP，并使用了博彩平台常用的 CDN 平台，进一步证实其为博彩类应用。通过其隐藏的注册入口，注册成功进入页面后，观察到该平台相较于常见的博彩平台，页面除了彩票、真人、棋牌、电竞等博彩板块外，还多了奖源认证和托管跑分。点击页面中的奖源认证，会跳转至多*联盟的会员认证入口，其页面内容介绍“恒*为多*联盟认证钻石级会员，已缴交 100 万保证金”，从而让赌客相信赌博平台不会“跑路”。

点击页面中的犀*、金**富，则跳转至跑分平台，并在页面发现了其使用的三种跑分方案。在对犀*和金*财富的上游引流页分析时，发现其除通过博彩平台引流外，还在色情网站进行引流，且通过色情平台进行赔付承保。

2. 博彩平台背后的技术、支付承兑商

在多*联盟的会员功能介绍页面，我们注意到金*正是其旗下的产品。除此之外，还包含

*支付、**娱乐、k**棋牌、**挂机、**统计等多种产品，即多*联盟为博彩平台提供了支付接口，博彩平台为多*平台的跑分通道提供引流页面，增强其产业洗钱通道。

通过以上的分析，博彩联盟产业主要包含博彩平台、博彩联盟平台、色情网站、赌客/跑分客几个部分。博彩联盟为博彩平台提供技术、支付通道，是整个产业的核心，同时通过博彩网站、色情网站为其推广旗下跑分平台，增强自身的支付通道及洗钱能力。博彩联盟、博彩平台、推广平台相互间通过押金方式进行约束。赌博平台向多*联盟缴费成为其会员后，多*联盟为赌博平台与赌客之间提供纠纷处理服务；博彩联盟/跑分平台向色情网站缴纳押金，依托色情网站推广跑分平台，色情网站为跑分平台承担纠纷处理服务。博彩平台不直接展示注册入口，通过博彩联盟进行 SEO，或依托博彩代理的推广页拉新，实现双方佣金结算。

二、 黑灰产利用跑分平台加数字货币洗钱，泰达币危害最严重

洗钱黑产与上游犯罪呈链条式发展，存在明显的相互依存关系，特别是对资金流转需求巨大的电信网络诈骗产业。根据 360 手机卫士多年来对电信网络诈骗的研究，目前其主要通过虚假兼职、身份冒充、交友敲诈等诈骗场景、话术，利用区块链、虚拟货币、AI 智能、GOIP、远程操控、共享屏幕等新技术骗取受害人资金，借助免签、跑分、虚拟货币等手段进行资金流转。随着技术对抗的升级，传统的三方支付、对公账户洗钱占比已减少，大量利用跑分平台加数字货币洗钱，尤其是利用 USDT（泰达币）危害最为严重。

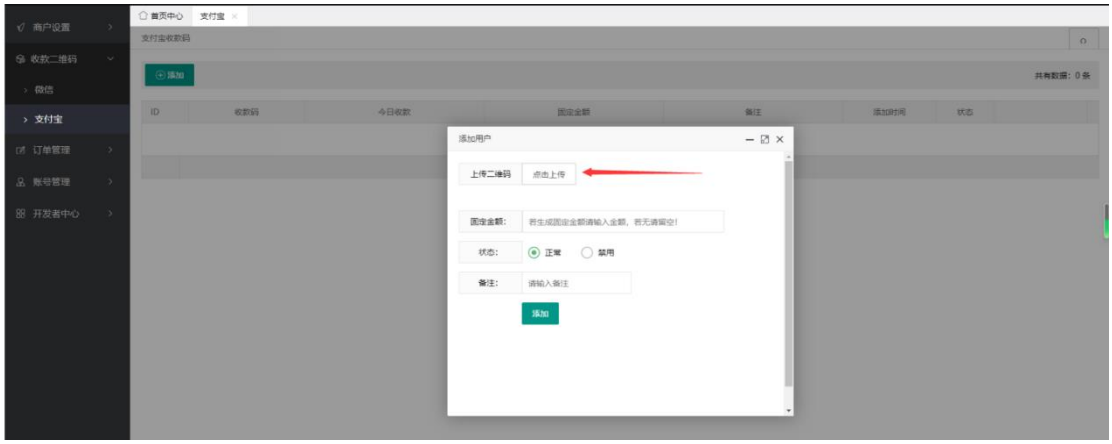
1. 绕过第三方支付平台接口限制的免签支付

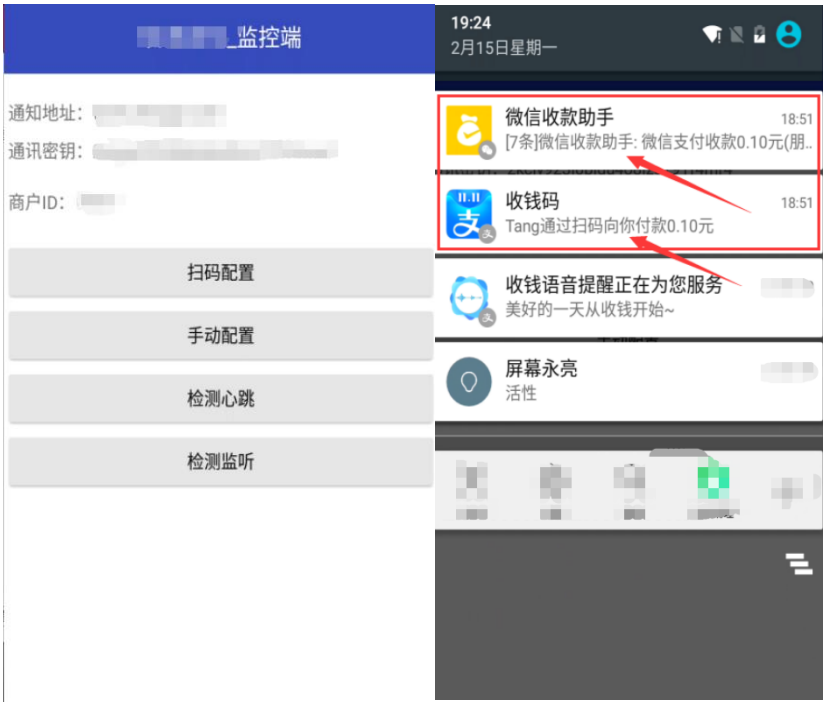
免签支付相当于绕过了支付平台的接口开通限制，自己搭建了一套支付接口，脱离了监管，且由于免签支付手段的成熟，该类工具、源码已经在黑灰产泛滥，轻易可获得并进行二

次加工使用，行业门槛极低。

杀猪盘、刷单、虚假投资等电信网络诈骗场景中，受害人之所以轻易相信对方，缘于骗局早期，能够获得骗子返回的任务佣金，但短期向不同人员过于频繁进行多笔小额资金支付，轻则引起支付平台的风控警觉，重则遭遇冻卡、断卡风险。与此同时，由于非企业用户无法开通微信、支付宝接口，在缺乏支付接口的状态下，黑产无法及时将支付订单与支付金额进行匹配，故通过免签 APP 做支付回调完成订单匹配。此种技术早期主要用于发卡平台（卡盟），随着黑产市场需求的增加，已逐渐被“杀猪盘”、虚假刷单等电信网络诈骗产业所采用，故在大量的诈骗平台可以看到其收款账户为个人账户形式的二维码。

第四方支付平台为（黑灰产）使用者提供了免签监控 APP、对接管理后台，使用者首先将洗钱手机登录的收款（支付宝/微信）二维码与第四方支付平台绑定，获得监控端绑定二维码，随后在收款手机端安装带有监听手机通知栏功能的免签 APP，填入监控端二维码完成第四方管理后台与免签 APP 的绑定。其中的检测心跳，指的免签 APP 是否可以正确监听收款，检测监听指的是第四方支付管理后台，是否可以正确收到监控的收款记录。当手机收到支付宝/微信的收款通知信息后，将信息回传至第四方平台，由第四方平台完成与诈骗平台支付订单的对接，实现支付接口的效果。在对免签产业分析的过程中，还发现其为逃避打击，将免签 APP 安装在云手机中，以实现被控制端 IP 与实际使用者网络分离。





2. 吸纳“公众”收款账户充当洗钱资金池的跑分通道

免签支付一定程度上解决了电信诈骗等黑灰产平台支付通道接口短缺，实现自动化账单对账，但自有资金池搭建存在资金、渠道等行业门槛，同时随着“断卡行动”的持续开展，黑灰产手中的收款账户消失殆尽，难以应对大量黑灰产特别是电信网络诈骗中频繁的账户切换需求。因此将目光盯上了涉世未深的学生，通过兼职任务的方式，吸纳学生参与到洗钱流程中，增加其洗钱通道，即众包式跑分。

跑分平台以网赚为名，进行兼职众包，吸引兼职客向跑分平台提供收款二维码/银行卡号，跑分平台再提供给诈骗平台，充当收款账户。诈骗团伙以话术诱导诈骗受害人向该二维码/银行卡号转账后，跑分平台给予兼职客佣金。这个过程中，兼职客的收款账户变现成为了洗钱通道。利用白账户进行涉诈资金的流转，既规避了风控监管，又大大提高转账成功率，

跑分平台无需过度担忧洗钱资金池的银行卡被冻结的问题，为后期跑分平台与黑产/诈骗团伙利益分成转账，提供了充足的时间。同时兼职客在跑分平台进行兼职任务时，需缴纳保证金，跑分平台和诈骗平台也不怕兼职客拿钱跑路。由于诈骗受害人的资金流向了兼职客的账户，兼职客的佣金通过其他形式进行变现，执法机关在进行资金流向追溯时，很难发现兼职客上游的跑分平台。

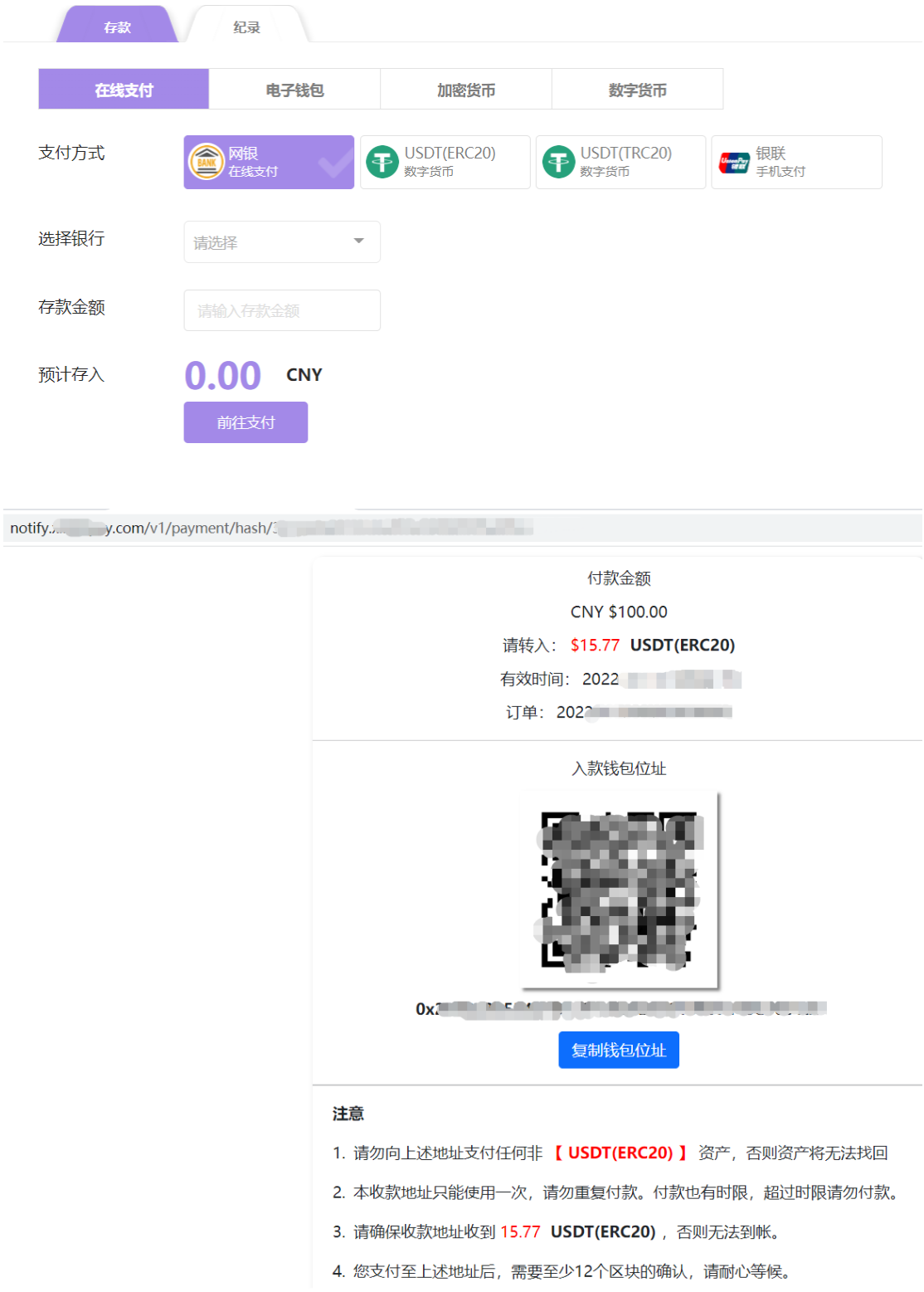
早期的跑分产业，由于上游黑产使用支付宝、微信、银行卡收款，跑分过程及押金使用网银、支付宝、微信等。随着攻防手段的升级，目前跑分及押金多使用虚拟货币进行，由于一些虚拟货币稳定币的流行，多使用 USDT 进行跑分，通过对跑分产业使用的工具挖掘，目前黑灰产市场售卖的跑分工具、源码仍以代收型为主。

随着攻防对抗的升级，现阶段跑分 APP 不像免签应用那样，使用公开的源码进行二维码修改，而是各个跑分平台各自开发具有自己特点的跑分应用，且应用名称多与订餐、食品相关，很难具有共同性，故需要对每个应用做特征专项分析。例如 360 手机卫士在 2022 年发现的跑分应用“**订餐”，其特点是当跑分客的手机收到银行短信时，并将短信上传至指定的服务器，此时境外跑分团伙/诈骗团伙，使用跑分客的银行账户进行收转款时，无需通过兼职客进行操作，即黑产宣传的跑分方案“一次性交付押金，国内存放手机，全自动化，不需要雇佣人力，更有超高技术保护，无任何技术可以发现你的手机位置”。

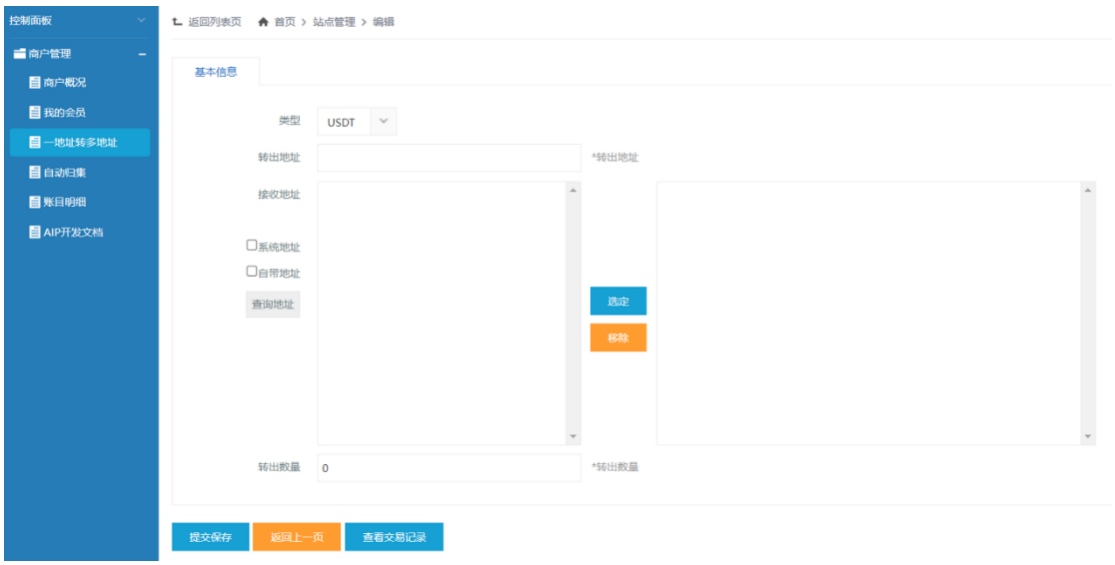

```
public static boolean requestShortMessageTest(Context context, int i, String str, String str2) {
    boolean z;
    String charSequence = context.getApplicationInfo().loadLabel(context.getPackageManager()).toString();
    String str3 = ("" + charSequence + "确认短信收发{" + Utils.getRandomString(8) + "}，请将本短信转发至" + str2 + "，5分钟内有效。["
    if (i == 0) {
        z = SmsBox.sendMessage(context, str, str3);
    } else {
        z = SmsBox.sendMessage(context, str, str3, i);
    }
    log.info("fromSlot->" + i + "; toPhoneNumber->" + str + "; backPhoneNumber->" + str2 + "; rc->" + z);
    return z;
```

3. 用于逃避“断卡”打击的虚拟货币

虚拟货币的火热，虚拟货币跑分的成熟，虚拟货币已成为电信诈骗平台支付通道的“宠儿”。原先占据主导地位的微信、支付宝收款方式，在某些杀猪盘平台甚至都销声匿迹。这里以杀猪盘平台为例，从其充值页面发现，其已经取消了支付宝、微信的充值入口，除仍保留的网银转账入口外，大部分都是虚拟货币充值的入口，包含虚拟货币钱包、虚拟货币直转两种方式。在页面点击充值后，可以看出该二维码为虚拟货币收款地址。



通过支付请求的回连地址，发现其背后与免签、跑分一样，也使用了第四方平台，只不过支付接口、收款二维码换成了虚拟货币。通过场景复现，发现此类四方平台提供一键调用 API 接口、一键生成 USDT 钱包、一键自动实现 USDT 充提、一键归集全部地址、一键实名寄售 USDT 等功能。



三、 移动网络秒拨成黑灰产热门 IP 代理手段

有市场，有需求，就意味着机会丛生。说到“IP”属性的应用场景，其早已渗透到我们的生活当中。比如：一个手机号码，只能在平台注册一个账号；网上投票，一个 ID 只能投一票，这里的 ID 的“唯一性”就是平台或者活动方为了保证活动公平性及自身利益，做出的限制，因为在我们看不到的网络世界，诈骗、群控、挂机、“羊毛党”、刷量等黑灰产行为时刻发生着，这些行为从悄然滋生到发展为成熟的产业链，始终绕不开最底层的 IP 支撑。360 手机卫士在长期对黑灰产的溯源分析时，发现一些黑灰产使用的 IP 呈现出“境外设备偏爱使用境内固网或 IDC 机房 IP，境内设备偏爱使用境内移动流量 IP 的特点”。推测此种偏好方式，境外的黑灰产可能是为了防止其使用的社交账号、支付账号被冻结或满足一定的上网娱乐需求；境内的黑灰产可能是为了防止具体位置信息暴露、提高追溯难度。而这两种身份伪装的方式，代表了目前主流的两种 IP 代理手段，固网 IP 秒拨和移动网络 IP 秒拨。

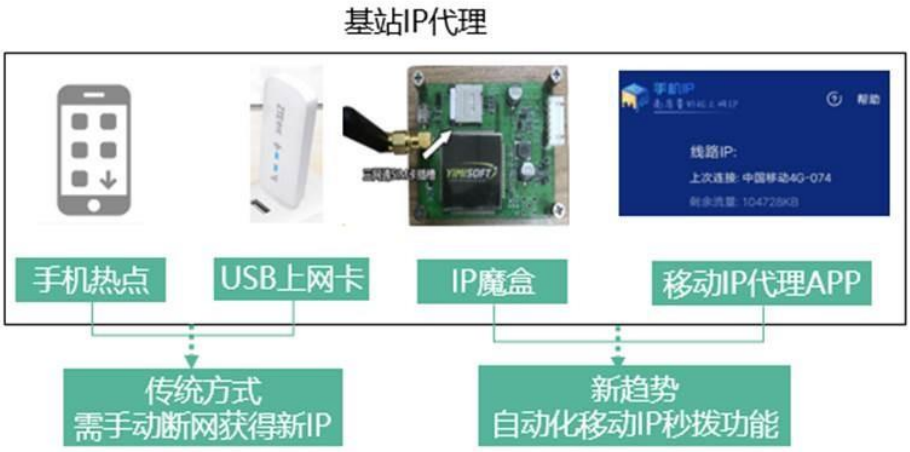
1. 固网 IP 秒拨原理及实现方式

由于 IPV4 资源的有限性，国内家用宽带主要是共享 IP，即设备联网时，运营商从 IP 池中分配 1 个 IP 给用户，用户断网时，IP 回收至 IP 池供给其他人使用，即重新拨号，运营商会重新分配 IP。秒拨利用了这种特性，短期内不断重新拨号，此时设备的 IP 就产生了变化，若把多个省市地区的秒拨资源打通，就可实现混拨。

固网秒拨指的是通过自建机房或民用宽带，向外提供代理 IP。2021 年，某地公安机关侦破一起利用“秒拨”网络设备获取电信运营商动态 IP 资源，为境外不法分子提供动态 IP 代理、动态 VPS 服务非法牟利的网络黑产案件。该案件中，不法分子利用了空壳公司，在多个地区设立多个非法机房窝点，国内多起涉赌、涉诈案件线索均指向该公司提供的 IP 资源。

2. 移动网络 IP 秒拨原理及实现方式

移动网络秒拨指的是利用移动网络提供的 IP，向外提供代理 IP。随着攻防对抗的升级，传统固网式的 IP 多已被标记识别，目前黑产将视线转移到更为隐蔽的移动网络 IP 上。从已掌握的情报来看，其实现方式有 4 种：手机热点、USB 上网卡、IP 魔盒、移动 IP 代理软件。其中手机热点、USB 上网卡需要手动断网才能获得新的 IP，存在不足，而 IP 魔盒和移动 IP 代理属于自动化类产物，弥补了手机热点和 USB 上网卡的不足，已渐渐成为主流。



USB 上网卡即便携式网络热点，插入手机卡，供电后即可共享网络。此些 USB 上网卡使用的流量业务，主要是一些第三方公司在运营，其向运营商采买流量后，分包卖给上网卡用户。

IP 魔盒为一款硬件盒子，支持多种类型的手机卡，接入电脑后可以使电脑拥有移动网络 IP，通过其自带的脚本可实现 IP 自动切换。USB 上网卡、IP 魔盒本质上是同一类产品，两者都可以通过断网再联网实现切换 IP，只是 IP 魔盒增加了自动化秒拨的功能。

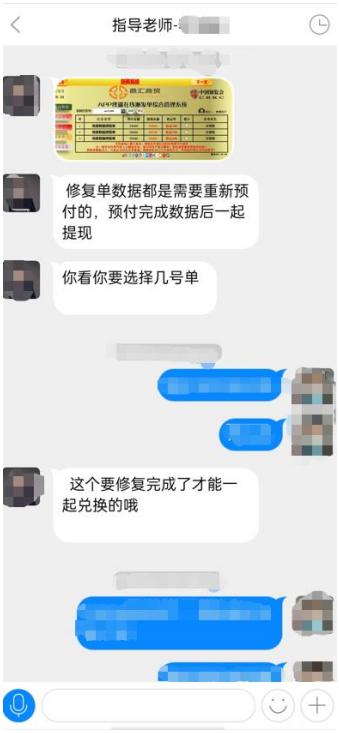
除了利用硬件产品实现移动网络秒拨外，目前一些代理软件也提供移动网络 IP，安装此类应用后，可根据其提供的移动网络线路 IP 进行 IP 伪装。利用移动网络秒拨 IP，黑产分子能实现快速变换 IP 或指定 IP 归属地，绕过时间、地域、次数的限制，同时随着 5G 网络的普及，在 5G 高带宽的背景下，黑灰产可能会以此衍生出其他的攻击手段。但从目前已知的风控手段来看，针对移动网络类秒拨 IP 并未迭代出良好的反制手段，IP 伪装攻防对抗将是一场持久战。

第三章 热门“诈骗剧本”

一、 提单需修复，请支付认购单

用户在短视频平台看到招收文具组装兼职广告，随后添加了“工作人员”的微信，在该工作人员的要求下，添加了“报名客服”的微信进行报名。报名后对方以公司准备发半成品组装笔原材料为由，索要了用户的姓名、收获地址、手机号，并以对接商家接待，领取材料、邮费为由，引导用户安装专属的聊天 APP。

在该聊天应用中，接待客服以物流发货需 5-7 天，在等待期间可以参与其他兼职活动为名，邀请用户参与刷单，即在指定的平台购买认购单。用户前期投入获得小额返利，后期用户完成认购任务后，却无法提现，对方以提单需修复为由，要求用户垫付认购单的 40%资金，用户发觉受骗。



专家解读

早期的刷单，是电商平台的商家以佣金的方式雇佣他人在其店铺购买商品，进行好评，提高其店铺在电商平台的权重，本质是商家围绕电商平台进行店铺数据造假。随着电信网络诈骗的兴起，不法分子脱离电商平台，假借刷单名义，诱导用户向其转账，骗取刷单商品费。

安全提示

网络刷单本身就是一种违法的行为，任何要求垫资的网络刷单都是诈骗，遇到“刷单”、“刷信誉”、“刷信用”的网络兼职广告时要提高警惕。

二、 小心！网络代买“冰墩墩”骗局：有人花上百元收到的竟是“耳环”

被北京冬奥会带火的吉祥物“冰墩墩”，集万千宠爱于一身，成为“一墩难求”的爆款，线下店买不到，线上也售罄，这时有人告诉你，他手里有“冰墩墩”，想要吗？

2022 年 2 月，用户在短视频平台发现有用户售卖冰墩墩，与对方沟通后便添加对方的微信。双方确认商品价格、商品数量后，用户通过微信扫码的方式向对方支付商品费。对方收款后对方向用户提供了快递单号，但用户收到货后，发现商品并不是冰墩墩，而是一对耳环，准备询问对方原因时，发现已无法联系上对方，得知受骗。

专家解读

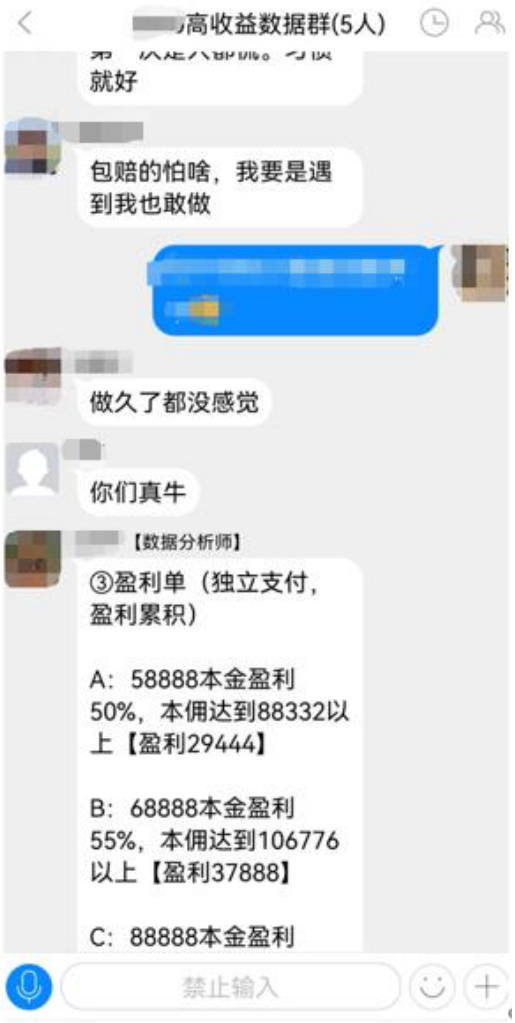
“冰墩墩”的火热，吸引了大量买家的关注，但由于购买人数多，造成货源不足。不法分子便利用此种现状，以掌握货源为由，向用户兜售“冰墩墩”，但官方都缺货的商品，他却“有货”，这本身就是自相矛盾的事情。

安全提示

切勿从陌生人处购买“冰墩墩”谨防诈骗；此外，也不要从“黄牛”手中高价购买特许商品，不要相信价格炒作跟风盲目购买，要理性消费，不让骗子有机可乘。

三、 “免费领取电饭煲”被骗上万元！

用户收到送电饭煲短信，根据短信中的领取方式，添加对方微信后，对方表示“该活动为*星举办，疫情期间为了打开市场销量做的线上推广活动，收到短信的用户不需要任何费用”，用户向其提供短信截图后，对方邀请用户进入指定的微信任务群，用户按照群内要求关注多个公众号后，收到对方佣金。随后其向用户介绍“公益竞猜”活动，即在指定平台投注，并表示该活动的收益的 10%将用于捐助公益，用户按照对方指引，在公益平台投注多次，但无法提现，对方表示需再次充值 10 万元才可提现，用户得知受骗。



专家解读

从诈骗过程看，不法分子通过短信发送赠送电饭煲进行引流，在诈骗实施过程中，以蝇头小利，将受害人诱骗至“公益项目“中进行投注，该公益项目，实际上是博彩平台，只是将博彩网站的名称及投注项目改成了 XX 公益。

安全提示

不要轻易相信免费送东西的短信，不要轻信网络上博彩等信息，更不要因为一点蝇头小利便相信所谓的高额回报。

四、 你想砍价，他想诈骗，警惕“砍价互助”骗局

电商平台 “百亿补贴”的促销，特别是助力活动的流行，吸引了大量的网民参与，为了完全助力活动，网民在网上招纳好友寻求帮助。用户在网上认识了能够协助用户完成助力的人员，对方表示用户缴纳 85 元助力费后，可帮用户完成 500 元的商品助力，用户向对方转账后，对方又以需要审核为由，要求用户向对方转账 888 元及安装**云会议应用，帮助用户进行砍单，用户发觉受骗。

专家解读

随着电商平台活动补贴力度的增加，不法分子盯上了想“薅羊毛”的用户，以能够提供快速助力技术为名，诱导受害人缴纳所谓的助力服务费，在各家电商平台日益重视风控技术的移动互联网时代，已并不纯在所谓的一键助力、一健砍单技术。于此同时，随着云会议类产品的兴起，不法分子开始通过云会议屏幕共享等方式，截取用户给个人信息进行资金盗刷。

安全提示

不要轻易相信互联网上售卖的一键助力、一键砍单服务；在通过会议类应用与陌生人进

行交流时，切勿轻易通过屏幕共享的方式向对方展示银行账户、支付校验短信等敏感信息。

五、 那一晚我们赤诚相见，你却用我的照片敲诈我

2022 年 3 月，用户在境外某聊天软件中认识了好友，以为其是性情中人，在与其聊天的过程中，被对方诱导进行裸聊，裸聊之前对方要求用户安装名为“爱*”的 APP 进行远程操作。用户根据对方提供的网址下载安装了“爱*”，输入指定的邀请码完成了应用注册。双方裸聊后，对方以掌握用户的裸聊画面、手机通讯录为由，对用户进行敲诈勒索，用户按照对方的要求向对方转账 1.2 万元后，对方仍要求用户转账 11 万元，用户发觉即使转账也无法解决事情后，便不再向对方转账。

专家解读

用户被引导安装的“爱*”应用，其本质是一个窃取用户通讯录信息的恶意程序，不法分子通过色情诱惑的方式引导受害人安装，在双方裸聊后，以将受害人的裸照群发给通讯录好友为由进行敲诈勒索。

安全提示

网络交易需谨慎，主动提供色情视频聊天的，多半为诈骗分子的套路，不要随意点开陌生人发来的链接，更不要下载来源不明的 APP。

第四章　2022 年第一季度安全数据

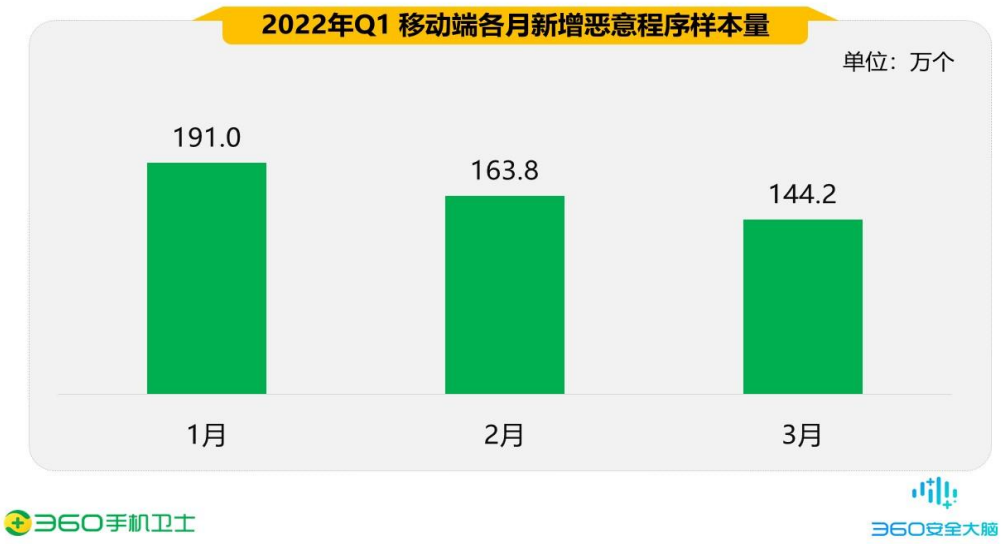
移动终端作为移动互联网的重要组成部分，安全风险形势牵动用户个人信息、财产安全。不法分子通过恶意程序、钓鱼网址、诈骗电话、短信等方式实施诈骗，对人们的日常生活产生恶劣影响的同时，更造成了个人财产的损失和隐私泄露。

本季度 360 安全大脑不断提升针对移动互联网恶意程序的识别收录能力，截获的移动端新增恶意程序同比有显著提升。基于自身已有的海量数据进行实时研判，实现事前预警、事中阻断、事后溯源，不断提升黑灰产的诈骗成本，为移动互联网的健康有序发展提供强有力的技术支持。

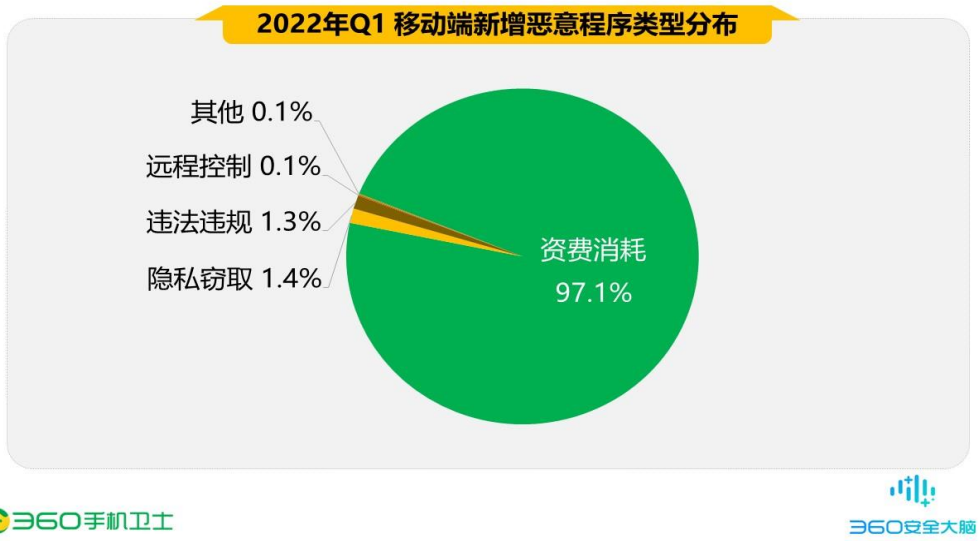
一、 恶意程序

1. 恶意程序新增样本量与类型分布

2022 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 499.0 万个，同比 2021 年第一季度（206.5 万个）上升了 141.7%，平均每天截获新增手机恶意程序样本约 5.5 万个。下图为 2022 年第一季度移动端各月新增恶意程序样本量统计：

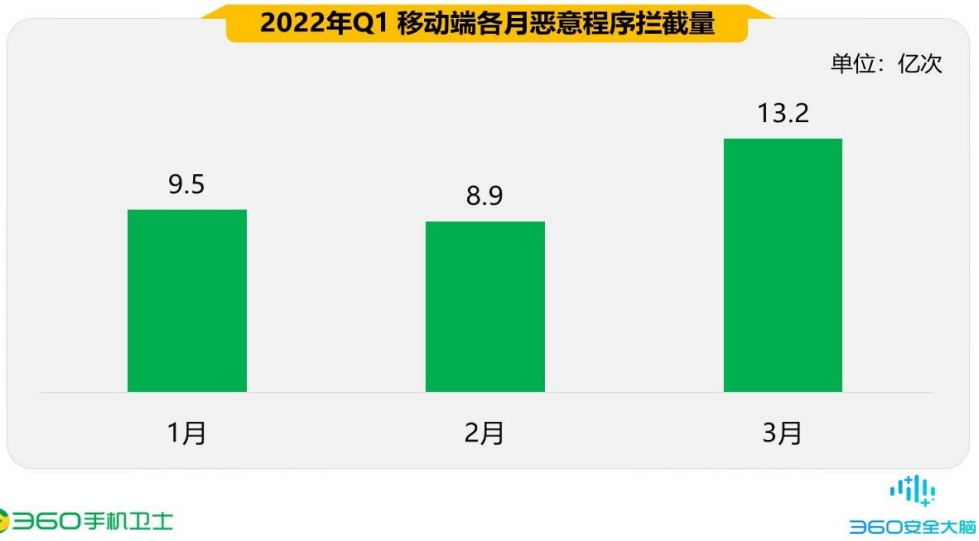


2022 年第一季度，移动端新增恶意程序类型主要为资费消耗，占比 97.1%；其次为隐私窃取（1.4%）、违法违规（1.3%）、远程控制（0.1%）等。下图为 2022 年第一季度移动端新增恶意程序类型分布：



2. 恶意程序拦截量

2022 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 31.6 亿次，平均每天拦截手机恶意程序攻击约 3512.2 万次。下图为 2022 年第一季度移动端各月恶意程序拦截量统计：



3. 恶意程序发展趋势分析

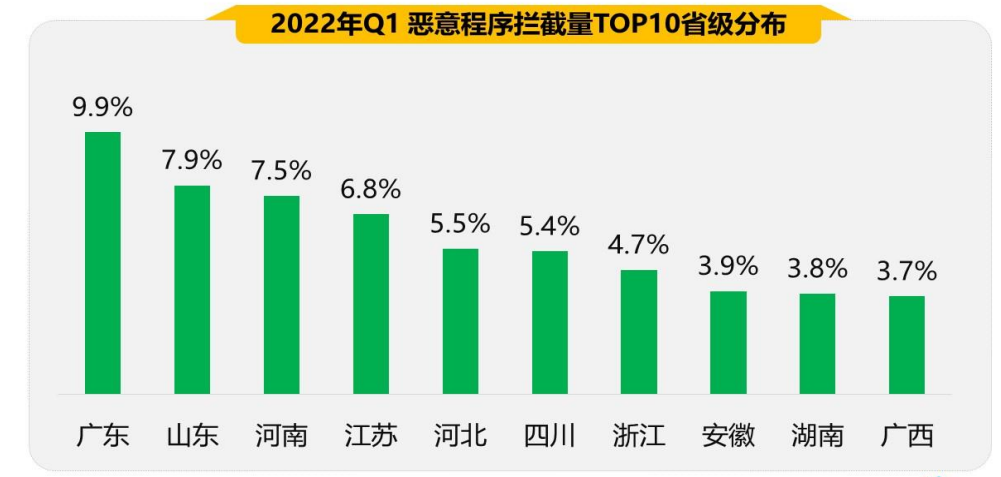
2021 年下半年至 2022 年第一季度期间，恶意程序新增量在 2022 年 1 月出现激增峰值，当月恶意程序新增量为 191.0 万，观察新增样本类型，主要体现在资费消耗类型。同时，由于 360 安全大脑不断提升针对移动互联网恶意程序的识别收录能力，恶意程序拦截量趋势，较去年也有明显增长。由于 3 月疫情的反复，广泛应用的线上场景使用愈加频繁，360 对此

一直在持续保证拦截，以便尽可能多地减小用户隐私泄露或者财产损失的风险。

360手机卫士　　单位：万　　360安全大脑

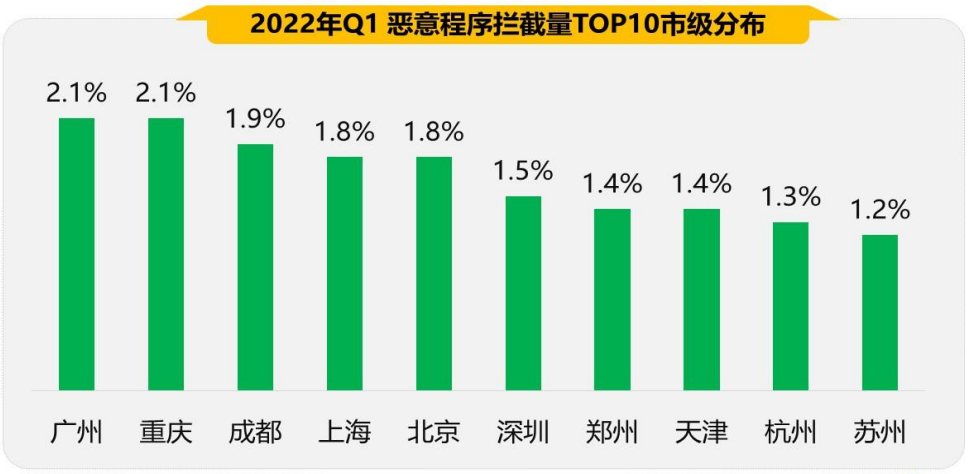
4. 恶意程序拦截量地域分布

2022 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 9.9%；其次为山东（7.9%）、河南（7.5%）、江苏（6.8%）、河北（5.5%），此外四川、浙江、安徽、湖南、广西的恶意程序拦截量也排在前列。



360手机卫士　　360安全大脑

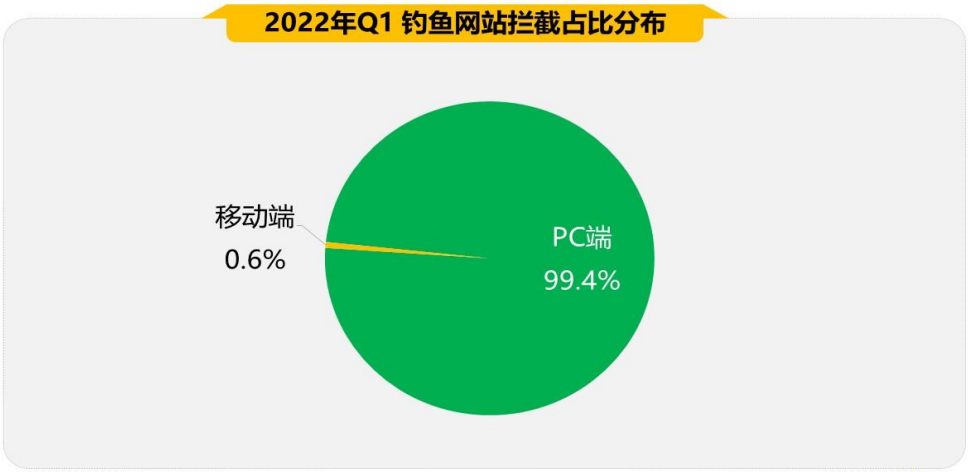
从城市分布来看，遭受手机恶意程序攻击最多的城市为广州市，占全国拦截量的 2.1%；其次为重庆（2.1%）、成都（1.9%）、上海（1.8%）、北京（1.8%），此外深圳、郑州、天津、杭州、苏州的恶意程序拦截量也排在前列。



二、 钓鱼网站

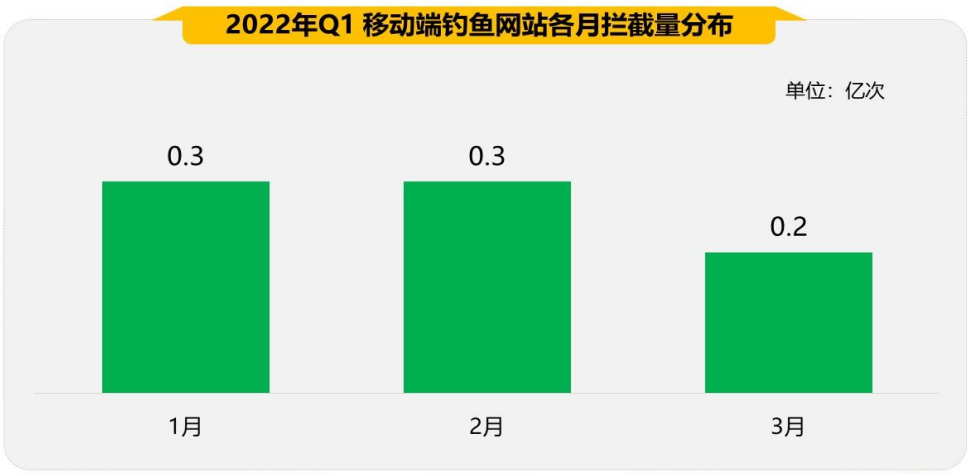
1. 移动端钓鱼网站拦截占比

2022 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 150.8 亿次，同比 2021 年第一季度（252.7 亿次）下降了 40.3%。其中，PC 端拦截量约为 149.9 亿次，占总拦截量的 99.4%，平均每日拦截量约 1.7 亿次；移动端拦截量约为 0.8 亿次，占总拦截量的 0.6%，平均每日拦截量约 93.2 万次。下图为 2022 年第一季度钓鱼网站拦截占比分布：



2. 移动端钓鱼网站各月拦截量分布

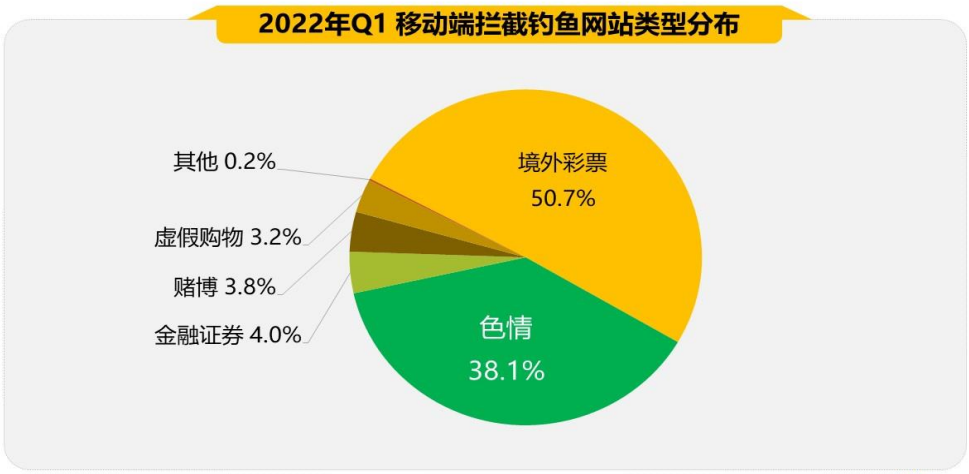
2022 年第一季度，360 安全大脑在移动端拦截钓鱼网站攻击约为 0.8 亿次，同比 2021 年第一季度（2.0 亿次）下降 57.8%。下图为 2022 年第一季度钓鱼网站各月拦截量分布：



360手机卫士　360安全大脑

3. 移动端钓鱼网站类型分布

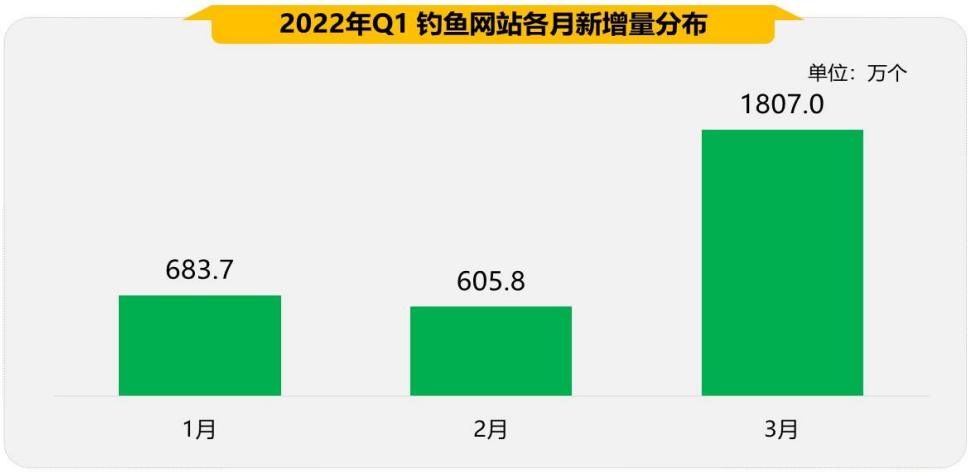
2022 年第一季度，移动端拦截钓鱼网站类型主要为境外彩票，占比高达 50.7%；其次为色情（38.1%）、金融证券（4.0%）、赌博（3.8%）、虚假购物（3.2%）等。下图为 2022 年第一季度移动端拦截钓鱼网站类型分布：



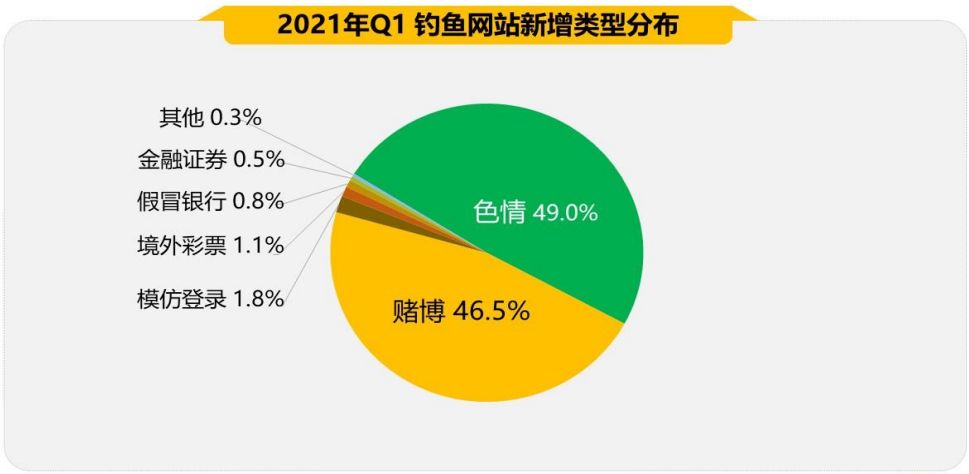
360手机卫士　360安全大脑

4. 移动端钓鱼网站新增量

2022 年第一季度，360 安全大脑共截获各类新增钓鱼网站 3096.5 万个，同比 2021 年第一季度（4239.5 万个）下降了 27.0%，平均每天新增 34.4 万个。下图为 2022 年第一季度移动端钓鱼网站新增量分布：

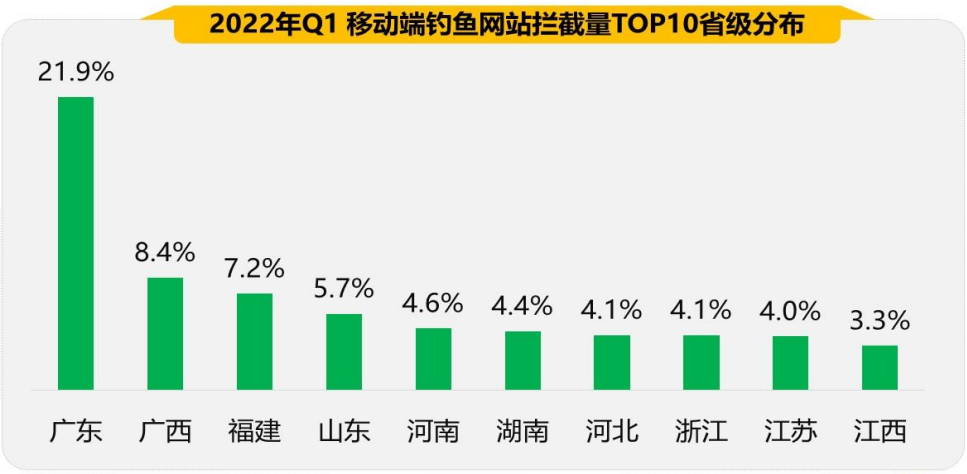


在钓鱼网站新增类型中，色情类占据首位，占比 49.0%；其次为赌博类，占比 46.5%。在本季度，360 安全大脑在机器学习上不断深入研究，进行规则优化更新，3 月截获新增钓鱼网站量有显著增加。针对钓鱼网站，360 安全大脑持续在构建更为完善的模型体系，提升样本检测量与样本拦截能力，及时识别各类黑灰产网站，尽可能全面地保证用户的信息安全与财产安全。下图为 2022 年第一季度移动端新增钓鱼网站类型分布：

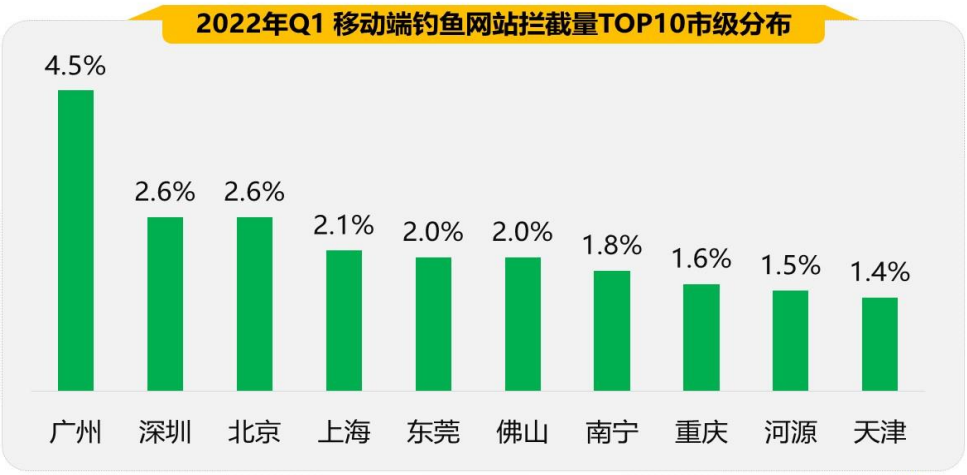


5. 移动端钓鱼网站拦截量地域分布

2022 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 21.9%；其次为广西（8.4%）、福建（7.2%）、山东（5.7%）、河南（4.6%），此外湖南、河北、浙江、江苏、江西的钓鱼网站拦截量也排在前列。



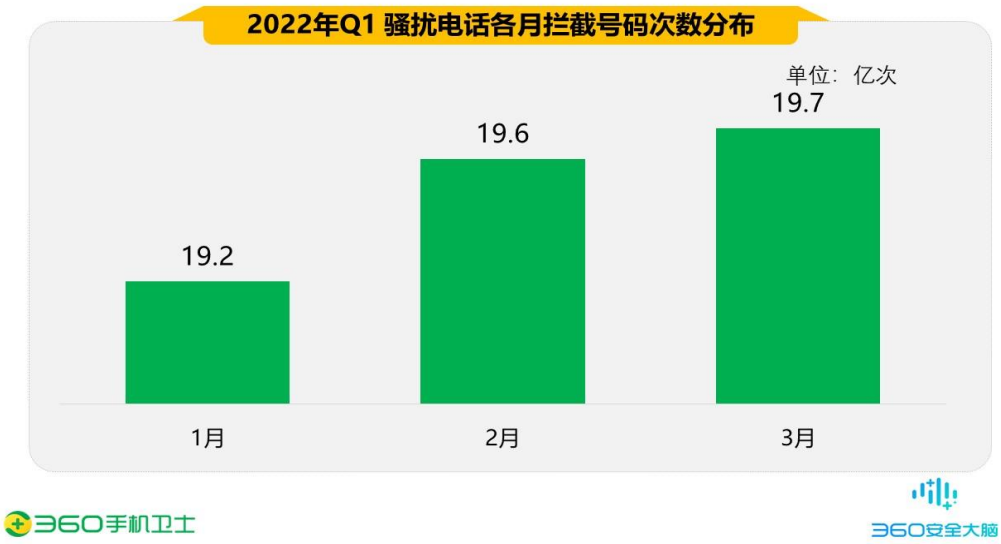
从城市分布来看，移动端拦截钓鱼网站最多的城市为广州市，占全国拦截量的 4.5%；其次为深圳（2.6%）、北京（2.6%）、上海（2.1%）、东莞（2.0%），此外佛山、南宁、重庆、河源、天津的钓鱼网站拦截量也排在前列。



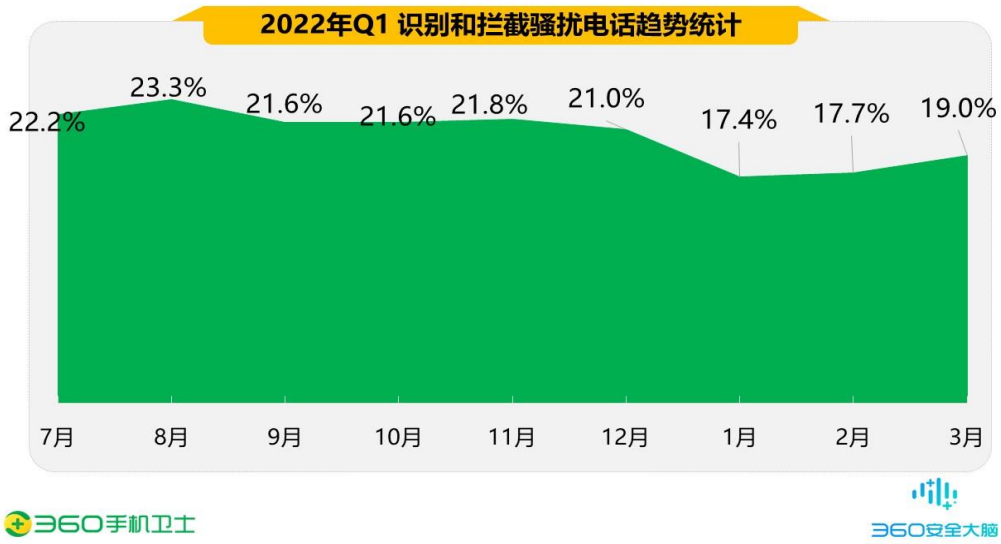
三、 骚扰电话

1. 骚扰电话标记拦截量

2022 年第一季度，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 58.4 亿次，平均每天识别和拦截骚扰电话约 0.6 亿次。同比 2021 年第一季度（54.8 亿次）上升了 6.6%。下图为 2022 年第一季度骚扰电话各月拦截号码次数分布：

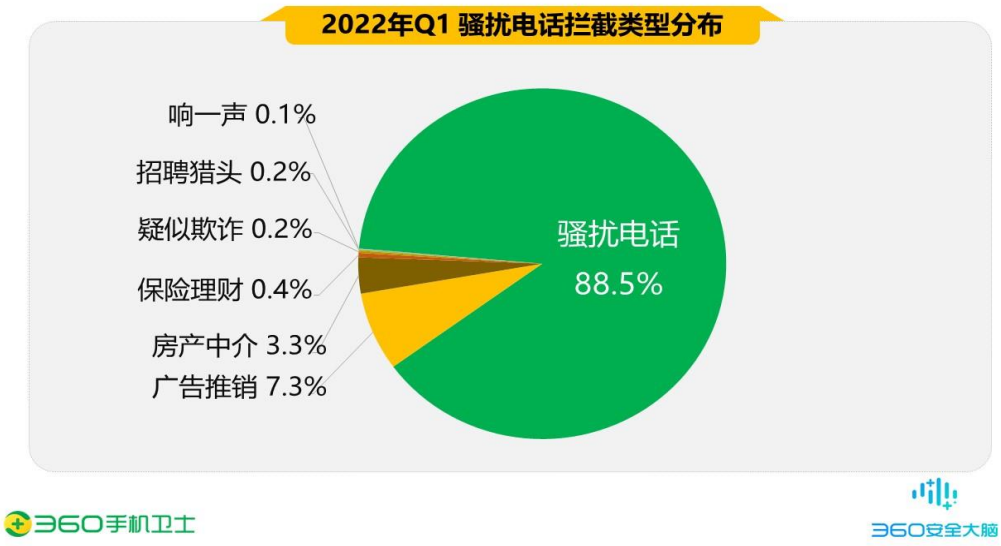


根据各月骚扰电话呼入占比分析，临近年底骚扰电话拦截量呈逐渐降低趋势，2022 年 1 月底 2 月初正值春节假期，春节期间从事拨打骚扰电话的人员减少，从而导致骚扰电话的呼入量降低。2022 年 3 月份起，骚扰电话拦截量回升。下图为 2022 年第一季度识别与拦截骚扰电话趋势统计：



2. 骚扰电话拦截类型分布

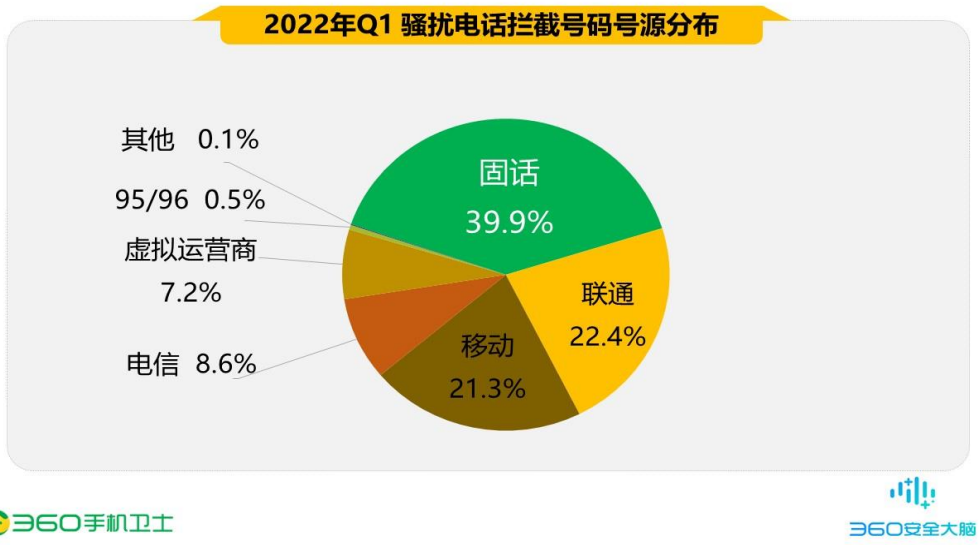
2022 年第一季度，综合 360 安全大脑的拦截监测情况及用户调研分析，从骚扰电话拦截类型来看，骚扰电话以 88.5%的比例位高居首位；其次为广告推销（7.3%）、房产中介（3.3%）、保险理财（0.4%）、疑似欺诈（0.2%）、招聘猎头（0.2%）与响一声（0.1%）。下图为 2022 年第一季度骚扰电话拦截类型分布：



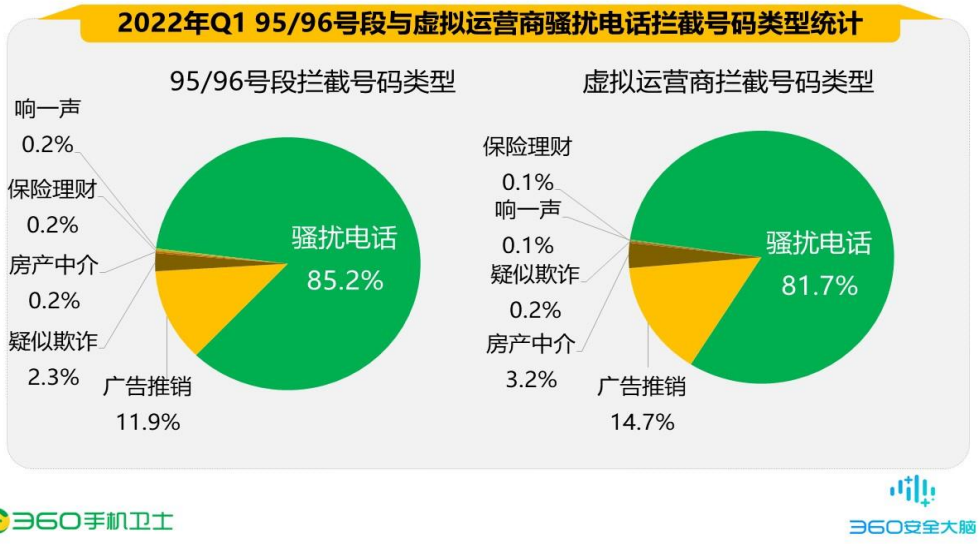
3. 骚扰电话拦截号码号源分布

2022 年第一季度，从骚扰电话拦截号码号源分布来看，被拦截号码为固话的占比最多，高达 39.9%，其次为运营商为中国联通的个人手机号（22.4%）、运营商为中国移动的个人手机号（21.3%）、运营商为中国电信的个人手机号（8.6%）、虚拟运营商（7.2%）、95/96 开头

号段（0.5%）等。下图为 2022 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 号段骚扰电话类占据首位，占比 85.2%；虚拟运营商骚扰电话类占据首位，占比 81.7%；广告推销类分别占比 11.9%与 14.7%，类型比例占据前列。95/96 号段与虚拟运营商号码依然是不法分子从事非法行径的主要“工具”之一。



4. 骚扰电话归属地分布

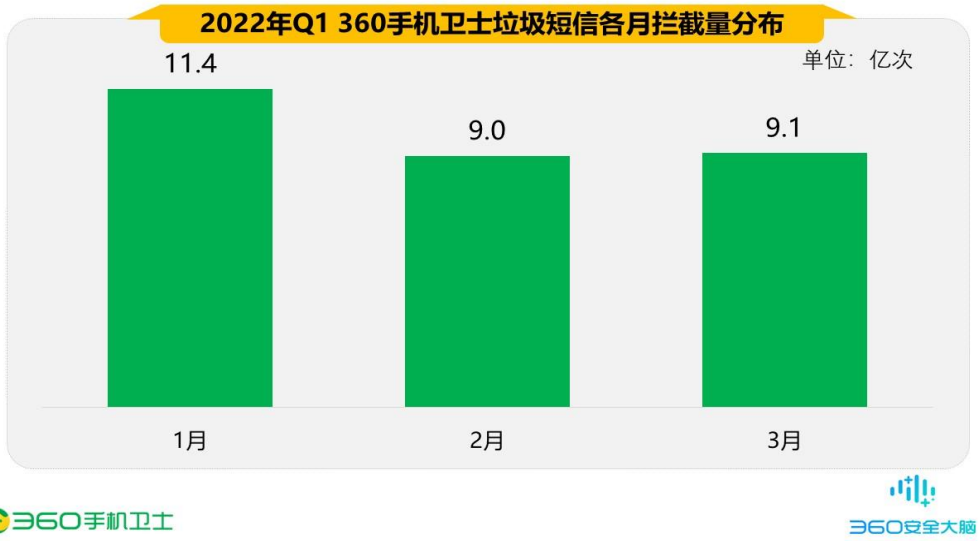
2022 年第一季度，从各地骚扰电话的拦截量上分析，广东省用户接到骚扰电话最多，占全国骚扰电话拦截量的 12.8%；其次是山东（7.8%）、江苏（6.8%）、河南（5.8%）、河北（4.7%），此外四川、浙江、湖南、北京、广西的骚扰电话拦截量也排在前列。

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 4.2%；其次是上海（3.6%）、广州（3.5%）、深圳（2.7%）、成都（2.6%），此外重庆、郑州、苏州、武汉、西安的骚扰电话拦截量也排在前列。

四、 垃圾短信

1. 垃圾短信拦截量

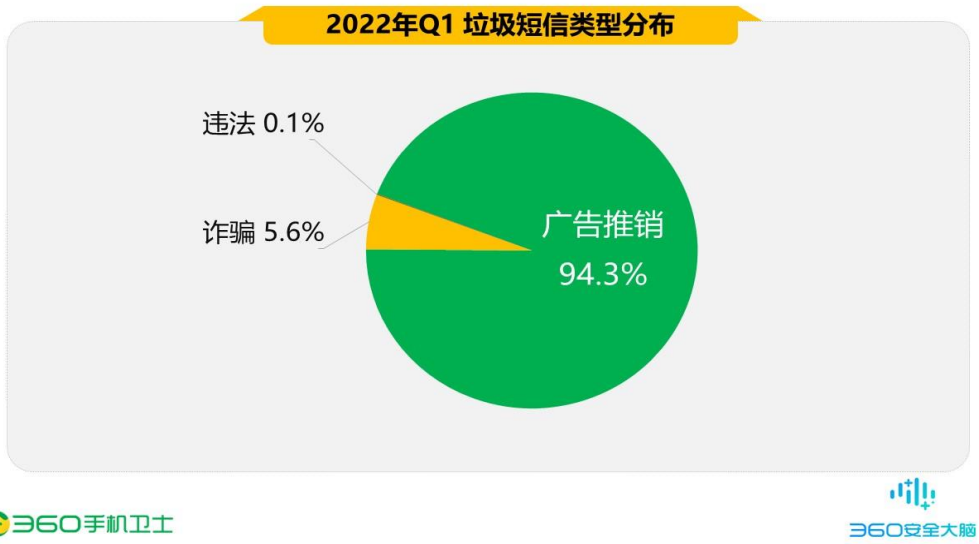
2022 年第一季度，在 360 安全大脑的支撑下，360 手机卫士共为全国用户拦截各类垃圾短信约 29.5 亿条，同比 2021 年第一季度（47.9 亿条）下降了 38.6%，平均每日拦截垃圾短信约 3272.4 万条。下图为 2022 年第一季度 360 手机卫士垃圾短信各月拦截量分布：



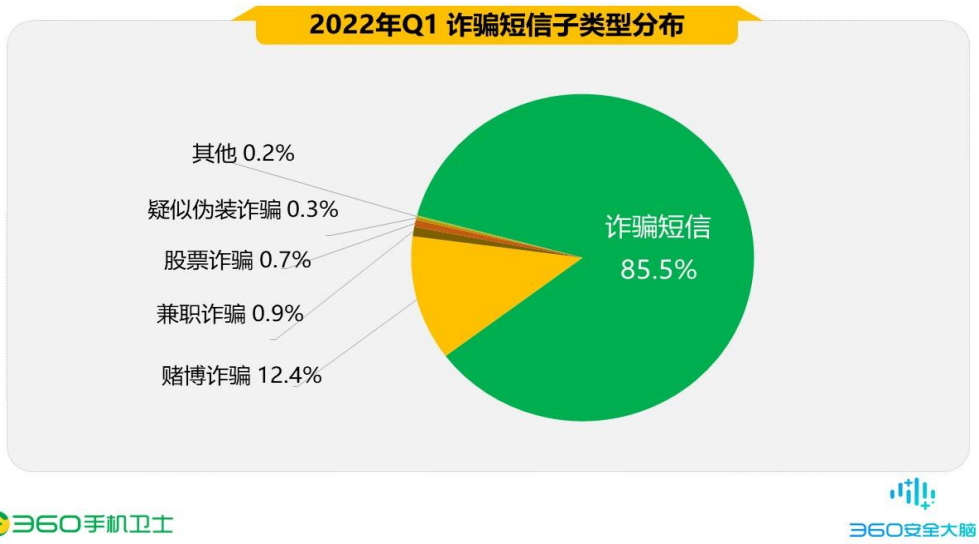
根据垃圾短信拦截量趋势分布，由于第一季度 2 月份春节期间各类发送垃圾短信的从业人员减少、企业放假休息，各类广告推销类型短信减少，导致 2 月份垃圾短信数量降低，3 月份开始逐步回升。下图为垃圾短信拦截量趋势分布：

2. 垃圾短信类型分析

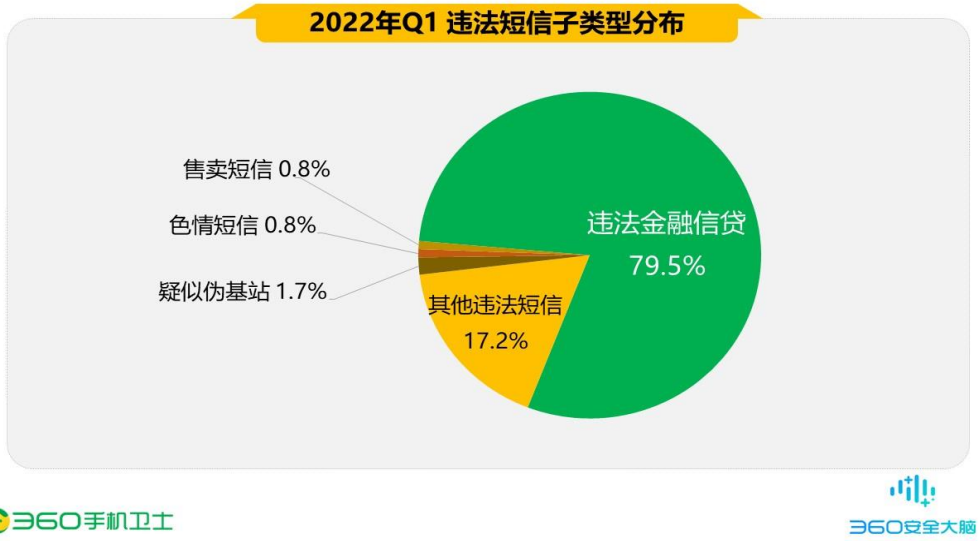
2022 年第一季度，垃圾短信的类型分布中广告推销短信最多，占比为 94.3%；诈骗短信占比 5.6%；违法短信占比 0.1%。



从诈骗短信拦截类型来看，诈骗短信以 85.5%的比例位居首位；其次为赌博诈骗（12.4%）、兼职诈骗（0.9%）、股票诈骗（0.7%）、疑似伪装诈骗（0.3%）等。现如今，越来越多的诈骗短信中包含文本字符少且仅有网址，如“可吃 www.******.rip”，此类短信内容晦涩难懂，仅通过内容难以判断其诈骗类型，360 安全大脑也在不断优化算法模型，提升实时研判诈骗短信新增与变种的能力，帮助用户抵制诈骗短信所带来的侵害。下图为 2022 年第一季度诈骗短信子类型分布：

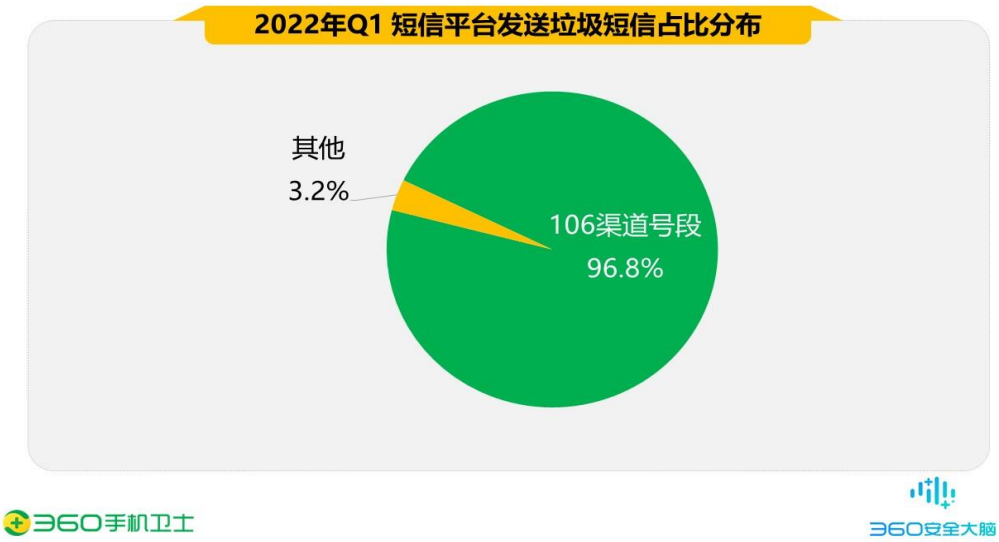


从违法短信拦截类型来看，违法金融信贷短信以 79.5%的比例位居首位；其次为疑似伪基站发送（1.7%）、色情短信（0.8%）、售卖信息（0.8%）等。下图为 2022 年第一季度违法短信子类型分布：



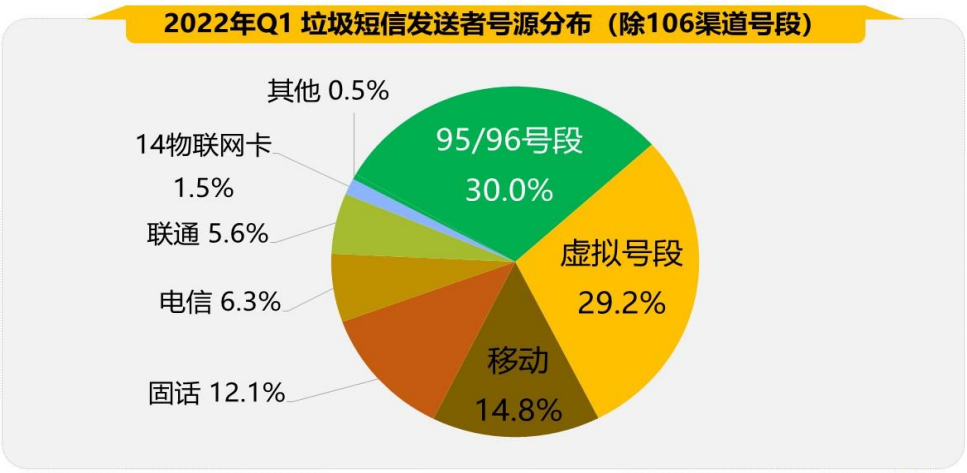
3. 垃圾短信发送者运营商号源分布

2022 年第一季度，短信平台 106 开头号段依然是传播垃圾短信的主要号源，占比高达 96.8%；利用其他号段传播垃圾短信占比约 3.2%。利用短信平台、虚拟运营商传播各类型短信依然是目前的主要途径，从获取用户联系方式到群发短信已形成完整产业链条。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。与此同时，在短信内容中利用关键词、变体字等实现“攻防”，而且越来越多的短信文本内容“短小精悍”，令人难以理解，无法仅从内容上辨别其本质，垃圾短信发展现状依然严峻，需要强而有效的法规监管。下图为 2022 年第一季度短信平台发送垃圾短信占比分布：



2022 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 95/96 号段发送垃圾短信的最多，占比 30.0%；其次是虚拟运营商号段（29.2%）、

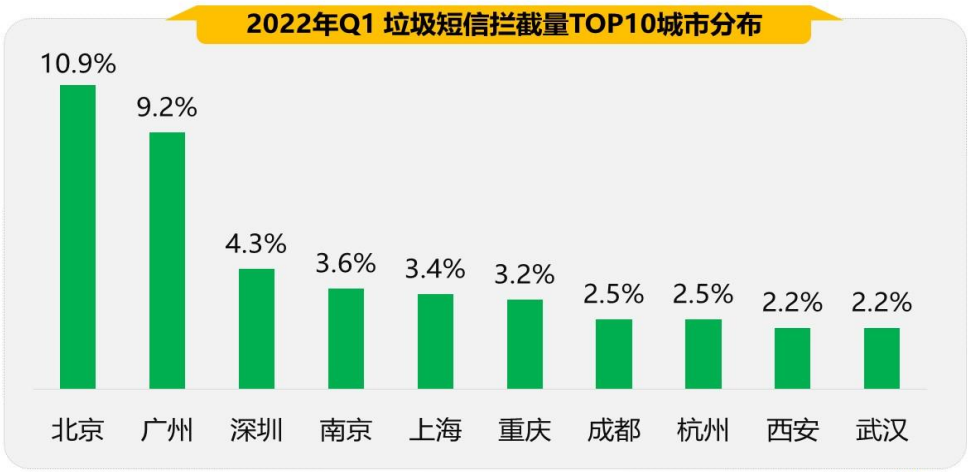
运营商为中国移动的个人手机号（14.8%）、固话（12.1%）、运营商为中国电信的个人手机号（6.3%）、运营商为中国联通的个人手机号（5.6%）、与 14 物联网卡（1.5%）等。



4. 垃圾短信拦截量地域分析

2022 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 19.3%；其次是北京（9.5%）、江苏（7.2%）、山东（6.6%）、浙江（6.1%），此外河南、四川、河北、湖南、湖北的垃圾短信拦截量也排在前列。

从城市分布来看，北京市用户收到的垃圾短信最多，占全国垃圾短信拦截量的 10.9%；其次是广州（9.2%）、深圳（4.3%）、南京（3.6%）、上海（3.4%），此外重庆、成都、杭州、西安、武汉的垃圾短信拦截量也排在前列。


2022年Q1 垃圾短信拦截量TOP10城市分布
10.9%
9.2%
4.3%
3.6%
3.4%
3.2%
2.5%
2.5%
2.2%
2.2%
北京
广州
深圳
南京
上海
重庆
成都
杭州
西安
武汉