2023 年度
中国手机安全状况报告

2024 年 03 月

前言

当前，电信网络诈骗呈集团化、产业化、链条化、跨境化态势，境外出现以“工业园”“科技园”为幌子的超大犯罪集团，从单独实施诈骗犯罪到衍生出故意伤害、非法拘禁等严重暴力犯罪，严重损害人民群众安全感。同时，为境外电信网络诈骗犯罪集团提供帮助的境内外相关黑产链条更为完整，人员、信息、技术、资金等黑产模块更为稳定，技术门槛进一步降低，资金渠道交织隐蔽，社会危害性极大[1]。

同时，不法分子不断寻求新的技术和手段，试图绕过反诈类产品的识别。2023 年出现的、迭代的新型简易组网 GOIP、无感盗刷远控、1 人 1 包等技术已凸显出现阶段黑产行业整体的变革，从早期使用引导话术“麻痹”用户，到现在全方位技术“升级”，对安全行业的反诈手段做定向绕过。在推广引流方面，新型简易组网 GOIP 利用高频电话风控“漏洞”，绕过呼叫频率、离散度风控模型；在技术开发方面，1 人 1 包样本利用其同一个下载链在不同时间下载的样本不同，突破了传统的样本库收录、识别策略；在转账洗钱方面，“无感盗刷远控”利用安卓系统的辅助功能等机制，突破账号异地登录、同网络环境、新设备风控机制进行盗刷；在黑灰产业链方面，黑产担保中介的出现，使得黑产供需双方的交易更加隐蔽，追踪和溯源变得更加困难。

2023 年，全国公安机关持续向电信网络诈骗犯罪发起凌厉攻势，共破获电信网络诈骗案件 43.7 万起，抓获一大批违法犯罪嫌疑人，自 2023 年 8 月以来电信网络诈骗发案数连续下降，打击治理工作取得显著成效。全链条打击电信网络诈骗及关联犯罪，深入开展“斩链”“清源”“利剑”三大战役，抓获了一大批违法犯罪人员，破获了一大批诈骗案件；会同最高人民法院、最高人民检察院等相关部门联合部署开展“拔钉”专项行动，成功将 263 名电信网络诈骗犯罪集团重大头目和骨干缉捕归案；组织开展“鄂湘鲁豫”区域会战，共捣毁诈骗窝点 1800 余个，实现规模打击效能最大化；针对涉诈黑灰产链条，组织发起打击涉诈固话语音专线、简易组网 GOIP、跑分洗钱等各类集群战役 277 起，取得了显著战果[2]。

为坚决彻底铲除缅北涉我电信网络诈骗犯罪“毒瘤”，公安部与缅甸警方持续开展执法安全合作，云南公安机关不断深化与缅甸相关地方执法部门的边境警务执法合作，在前期持续不断打击下，截至目前，已有 4.4 万名缅北涉我电信网络诈骗犯罪嫌疑人移交我方，其中幕后“金主”、组织头目和骨干 171 名，网上在逃人员 2908 名，有力打击了境外诈骗集团的嚣张气焰，打击工作取得历史性重大战果。公安机关将始终保持对此类犯罪的严打高压态势，不断深化国际执法合作，持续缉捕电信网络诈骗犯罪集团重要头目，纵深推进专项打击行动，坚决维护人民群众生命财产安全，切实维护边境安全稳定[3]。

《2023 年度中国手机安全状况报告》基于 360 安全大脑和 360 移动安全黑灰产研判、分析、溯源能力，持续以电信网络诈骗手法、攻防技术、产业链为切入点，深度剖析电信网络诈骗及关联的重点黑灰产业链。面对层出不穷的新型诈骗手段，公众需提高自己的反诈意识和能力，360 也将发挥在网络安全行业积累的攻防打击技术优势，赋能反诈，增加反诈行业综合打击能力。

目录

第一篇 电信网络诈骗-黑灰产攻防技术

随着反诈力度的不断加强和公众反诈意识的提高，大量涉及网络诈骗的黑灰产逐渐受到打击，其所使用的诸多技术手段也被纷纷封停。在此背景下，不法分子不断寻求新的技术和手段，网络诈骗的攻防对抗变得愈发激烈。2023 年 360 移动安全团队捕获到黑产使用新型简易组网 GOIP、“伪国显”号码、无感盗刷远控、1 人 1 包、AI 换脸等新技术。这些手段增强了诈骗的迷惑性，使得公众容易上当受骗，同时增加了“免杀”策略，尝试绕过例如 360 手机卫士等反诈 APP 识别。面对这些新型的诈骗手段，公众需提高警惕，不断学习和了解新的诈骗手法，提高自己的反诈意识和能力，360 也将发挥在网络安全行业积累的攻防打击技术优势，赋能反诈，增加反诈行业综合打击能力。

第一章、简易组网 GOIP 增加 AXB 模式，实现号码防封

360 移动安全团队曾揭露过黑产搭建简易组网 GOIP 环境，实现境外诈骗人员远控境内人员的手机拨打诈骗电话的手法。境外手机 A1 安装远控 APP，控制境内的手机 A2 拨打诈骗电话，境外手机 B1 安装具有语音聊天的 APP，与境内手机 B2 进行语音通话，境内手机 A2 与境内手机 B2 通过音频连接线连接，实现 A2 与 B2 实时共享音频，从而实现境外手机 B1 代替境内手机 A2，与境内手机 A2 电话呼叫的人员进行实时通话。此类简易组网 GOIP，2022 年黑产使用第三方公司开发的远控、聊天类应用搭建环境。随着相关的软件线路遭受风控限制，黑产开始自研例如杨*、云*插卡端、火*语音端等具有远控、语音聊天功能的应用。

图 1 简易组网 GOIP 流程

图 2 简易组网 GOIP 应用界面

2023 年黑产为提升简易组网 GOIP 诈骗的成功率，一方面加大招兵买马的力度，黑产渠道出现了大量 GOIP 上课群，手把手教授下游马仔安装简易组网 GOIP 应用，按照电话呼叫的时长支付费用。另一方面增加样本的更新速度，样本更新从 2023 年 5 月出现激增，提升追溯难度。2023 年 360 移动安全团队，累计发现国内简易组网 GOIP 设备数十万，按照 IP 地域划分，TOP10 省份分别为陕西、广东、云南、四川、湖南、广西、河南、贵州、湖北、江苏。

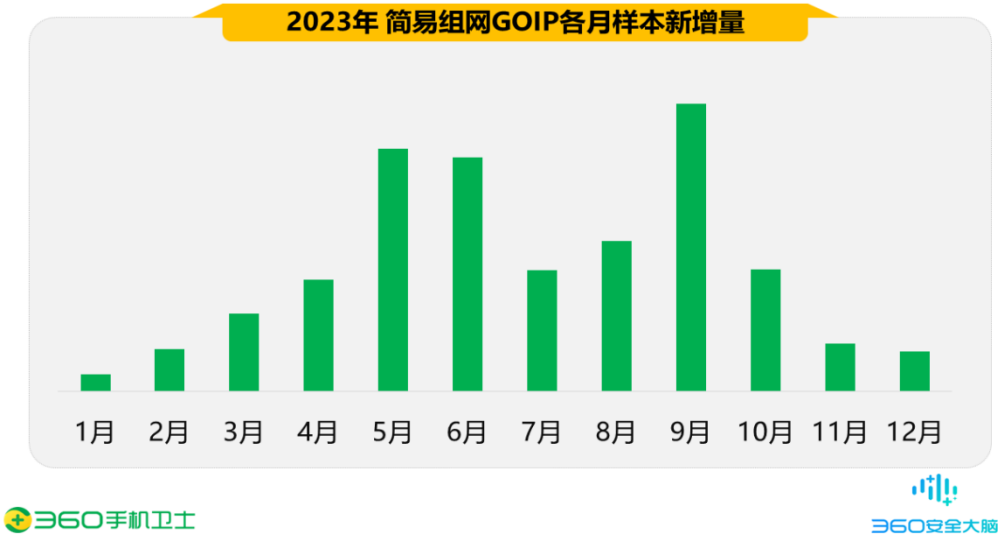

图 3 2023 年简易组网 GOIP 各月样本新增量

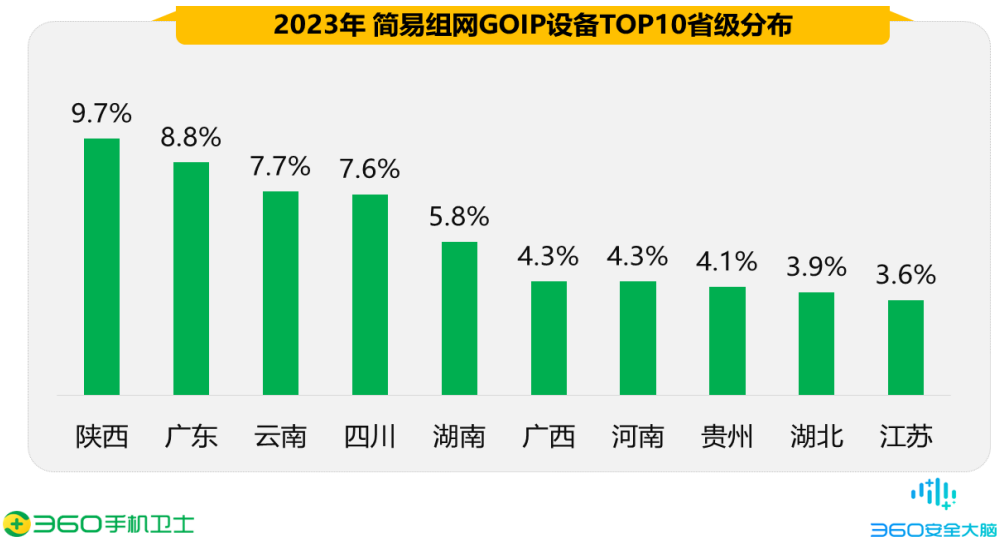

图 4 2023 年简易组网 GOIP 设备 TOP10 省份分布

随着全国执法机关持续开展打击简易组网 GOIP 专项行动，黑产进行产业升级，在远控式控制电话外呼的基础上，新增 AXB（也称中继）方式进行外呼，诈骗人员在境外使用号码 A，呼叫境内的马仔手机号 X，马仔根据诈骗人员提供的受害人号码 B，将手机号 X 设置呼叫转移至指定的受害人号码 B。当诈骗人员使用号码 A 拨打 X 号码时，实现 A 和 B 通话。为了方便马仔快速、批量化设置呼叫转移，目前黑产已将此套方案开发成 APP。

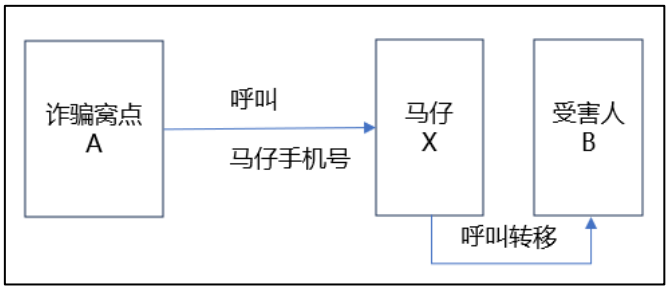

图 5 AXB 流程

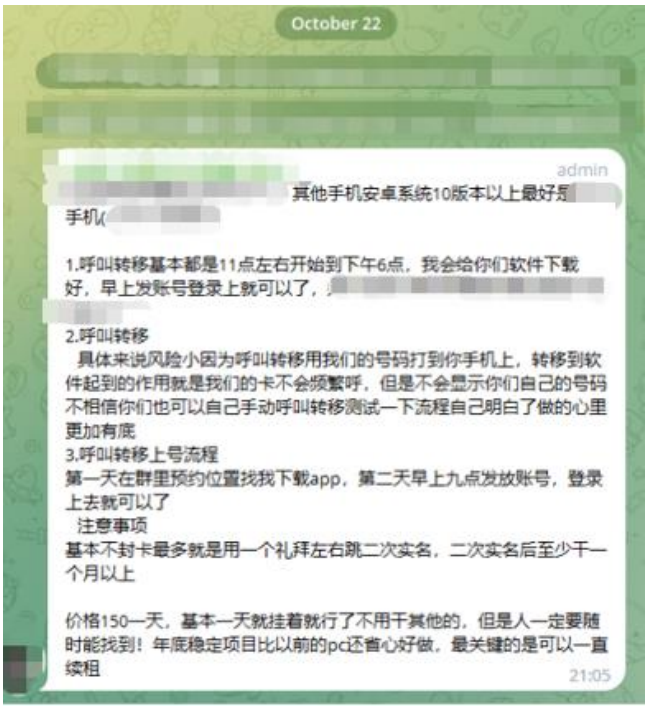

图 6 黑产群交流 AXB 流程

第二章、伪“国显”号码成为黑产电销主流线路

在 2023 年 360 移动安全团队监测到部分黑产渠道售卖的电销号码，其号码区别于常见号码，但却能正常显示号码归属地。深入分析后发现是骗子在来电号码上动“心思”加以伪装，冒充其当地归属地的号码向当地民众拨打诈骗电话。此种电话伪装技术，黑产行业称为“国显线路”。截至 2023 年底，从黑产渠道捕获的国显类号码，主要对固话归属地、手机号码归属地进行伪装。此类号码归属地伪装技术，在 2023 年已成为黑产电销（电话）供应商主流线路，360 移动安全团队每日发现识别大量此类国显号码。

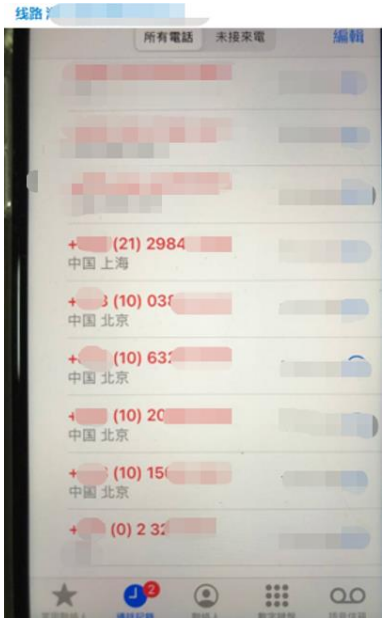

图 7 黑产展示的伪国显号码

此类号码被黑产封装成电销线路，对接到呼叫中心系统软件中，通过售卖呼叫中心平台子账号的方式售卖电话资源。或向下线提供账号、密码，诈骗窝点使用 SIP 类软件远程调用电销线路中的号码拨打诈骗电话。借助此类系统，诈骗窝点具备了批量外呼的能力。

为增加受害人的信任度，黑产提供的电销线路增加了轮拨呼叫策略，给同一个手机号拨打电话，若当前使用的号码对方未接听，系统会自动切换号码池中的号码再次进行呼叫。同时为了防止号码池被追踪，加入了混拨技术，同一个电销线路使用不同类型的号码拨打。

这种手段最终的目的是让受害者误以为来电方是本地某个机构或者熟人，从而降低受害者的警惕性，更容易相信诈骗电话的内容。对于陌生来电，尤其是涉及财务、个人隐私等敏感信息的电话，要保持高度警惕，不轻易相信对方的身份和要求。可以在手机上安装反诈软件，如 360 手机卫士等，这些软件可以识别并拦截诈骗电话和短信，提高手机的安全性。

第三章、安卓远控木马伪装成色情、赌博等应用，盗取支付密码进行无感盗刷

2023 年 3 月，360 移动安全团队在日常的威胁分析运营中捕获到多个黑产渠道出售安卓远控木马，售卖方宣称木马具备“操控手机进行转账、位置监控、账号捕捉等功能”，其建议买家可将远控木马伪装成色情、赌博、诈骗等类型应用，提升传播成功率。此类木马，可实现用户未使用手机的情况下私自解锁手机，远程控制手机进行资金盗刷，危害性巨大。

经分析后发现，此类木马早期在虚拟货币黑产圈中流转，主要为盗刷虚拟货币钱包，黑

产内部称为盗 U 技术。为扩大销售市场，目前将目标用户扩大到电诈、赌博、色情产业。从捕获到的情报看，此类木马主要通过对市面的开源远控软件修改后生成，修改后的主控名称包括天线远控、Craxs Rat（也称克拉克斯鼠）等。

图 8 黑产群发布的远控教程

部分黑产基于安卓虚拟化技术开发了特殊的工具，支持将编写的安卓远控程序，注入到正常的 App 中，运行 App 时安卓远控程序也会上线。例如下图是某款支持将远控代码注入到常见应用的远控，其宣传页的功能描述。

图 9 安卓远控注入工具介绍

此类木马由于需要对手机进行大量的执行操作，会通过话术诱导受害人安装应用，开启手机无障碍、通知栏监听、悬浮窗等权限，进而实现各类监控功能。捕获到的某款伪装成色情应用的远控应用，行为链如下表。通过对比多个此类安卓远控类样本，猜测此类样本目前以色情为幌子，利用辅助功能权限，窃取支付密码并远程控制手机，当监控到用户长时间未使用手机时，远控手机访问第三方平台的支付 API 接口，并使用已窃取到的密码购买平台对应的虚拟币、虚拟商品等。

过程	内容
步骤 1	申请权限
步骤 2	连接远控后台
步骤 3	监控顶层页面与键盘，窃取某些应用的支付密码、设备密码
步骤 4	上传密码、设备型号、用户使用设备情况
步骤 5	频繁监控用户是否在使用设备（即设备是否锁屏）并将结果实时更新上传
步骤 6	当步骤 5 监听到用户已超过半小时未使用手机，设置 20s 设备唤醒锁
步骤 7	使用手势密码解锁设备
步骤 8	静音，并开启视频聊天以确认用户未使用手机
步骤 9	浏览器打开指定 URL，猜测为支付 URL
步骤 10	支付过程中，若需人脸检测，则点击 back 键跳过
步骤 11	输入支付密码，完成转账
步骤 12	向左滑动删除列表中的软件（避免用户发现浏览器软件被运行过）
步骤 13	退出视频聊天，解除静音
步骤 14	卸载自身软件

第四章、突破病毒库识别策略的 1 人 1 包类样本

传统对恶意 APP 样本的检测和识别多依托病毒库，通过源源不断收录样本，结合动态静态分析手段，增加病毒库识别量。360 移动安全团队通过长期对恶意应用的传播特点和黑灰产业链的分析研究发现，冒充公检法、虚假兼职、裸聊敲诈等诈骗场景使用的应用，其同一个下载链在不同时间下载的样本不同，即 1 人 1 包策略，提升了诈骗样本的收录及识别难度。

一、 恶意应用的制作与分发流程

诈骗人员将自研或购买的诈骗平台源码部署到服务器上搭建 APK 自动生成流程，生成的应用上传至 APK 分发平台，由分发平台生成 APP 下载链供访客下载。部分诈骗人员使用自建的 APK 分发平台，部分使用外采 APK 分发平台，实时替换分发平台的 APK 或定期检测样本是否被手机厂商或安全厂商报毒来替换新的 APK，实现应用下载的 1 人 1 包，达到免杀效果。

为进一步提升恶意样本传播的成功率，分发平台会同时在 APP 下载链做免杀策略，当下载链被报毒时，通过域名轮换的方式，将 APK 下载链解析到未被查杀的链接上。

二、 1 人 1 包类恶意样本识别

由于恶意应用从传播、发现、分析、识别需要时间，这种 1 人 1 包方案突破了传统依托病毒库识别的安全运营逻辑，真实传播的样本难以捕获，捕获到的样本与传播的样本又存在差异，导致识别存在滞后性。

1 人 1 包的样本虽包名、签名等基本信息不相同，但其使用的代码结构、行为逻辑基本相同，仍属于同源、家族类样本的范畴。基于 360 在反病毒引擎、主动防御技术、AI 分析、样本同源分析、动态行为分析等方面的技术积累，可精准识别此类 1 人 1 包类样本，每周可检测发现几万至几十万此类样本，类型覆盖冒充公检法、虚假兼职、裸聊敲诈等 1 人 1 包主流应用场景。

第五章、眼见不一定为真，诈骗场景使用“换脸”技术

随着 2023 年上半年 AI 换脸技术诈骗被持续揭露，引发大众关注与担忧。从 360 移动安全的威胁情报库中，我们发现“换脸”技术目前被黑产应用于裸聊敲诈、身份冒充等诈骗场景以及部分无人直播场景中，其原理是替换手机相机的画面，主要使用事前合成视频替换、实时替换两种方式。以下以黑灰产场景为切入点，针对这两类技术进行剖析。

一、 手机相机内容“劫持”替换指定视频

在裸聊敲诈场景中，诈骗人员在互联网社交平台撒网式交友，吸引用户上钩，通过话术套出该用户的工作、爱好进而了解这个人。再以话术聊感情，引诱该用户开视频裸聊，录制对方视频画面。以信号不好挂掉视频，诱导下载安装含窃取通讯录功能的 APP，并诱导给该 APP 相关的手机权限，获得通讯录后，以掌握到对方通讯录好友信息，会将其裸聊视频发送给通讯录好友为由进行敲诈勒索。

在这个诈骗场景中，受害人之所以相信对方，源于看到了对方的“裸聊”画面，但实际上，用户看到的裸聊画面是诈骗人员通过互联网收集的“美女视频”。通过 APP 劫持手机相机加载该“美女视频”，与受害人视频通话时，对方看到的就是预先加载的“美女视频”画面。原理是通过对手机 ROOT，获得手机“管理员”级别的权限，再使用相机劫持类 APP 接管手机相机内容，将事前通过互联网收集的视频画面，例如美女视频，导入到相机劫持类 APP，

实现手机相机画面内容的替换。当视频通话时，视频软件调用手机相机，手机提供给视频软件的画面就是替换后的内容，可以理解为播放指定的视频内容给对方看。出于对手机安全性、稳定性的保障，目前手机厂商均提高了对手机 ROOT 的难度，故黑产多采用 ROOT 难度低、系统版本低的手机搭建相机劫持设备，如下图展示，虚假相机类支持的系统版本及黑产售卖虚拟相机手机演示视频画面。

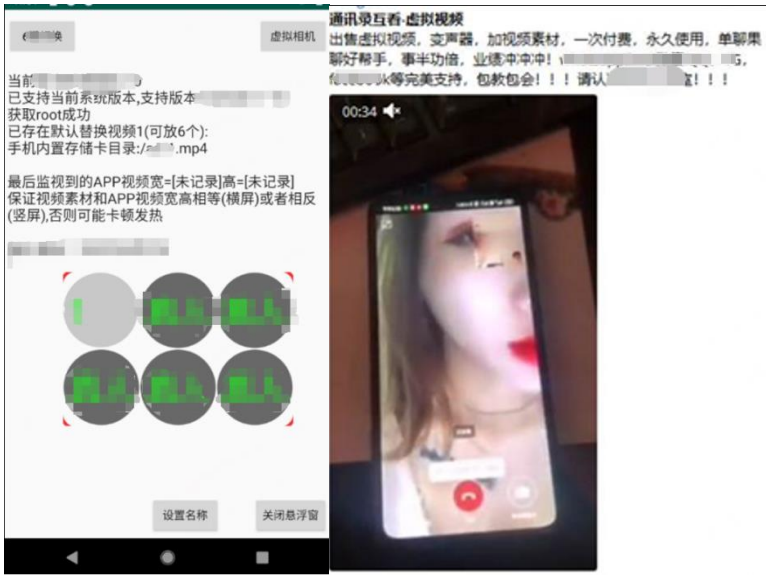

图 10 裸聊敲诈场景使用的虚假相机软件

在无人直播场景中，黑灰产一方面也像裸聊敲诈场景那样使用提前收集的视频，替换直播 APP 相机的画面内容；一方面针对虚拟相机 APP 进行版本升级，如下图展示的增加视频推流功能，将主流直播平台中他人的直播内容，转播至自己的直播间，同时导入提前编写的话术，进行边播边评论，营造直播间有大量活跃观众的假象。

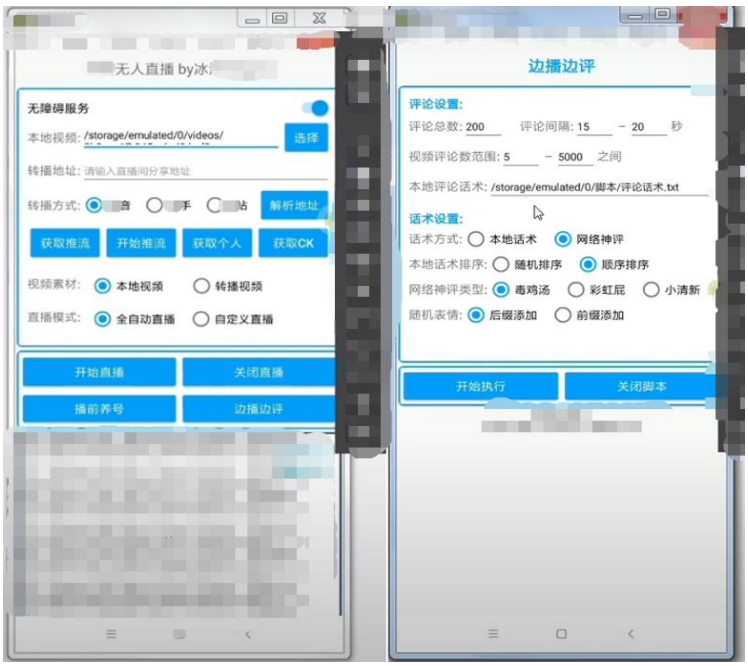

图 11 无人直播场景使用的虚假相机软件

二、 AI 合成高仿及实时换脸视频

为了增加受害人的信任以及绕过某些平台的人脸认证，诈骗人员增加了对所使用的替换视频的真实性投入，使用经过模型训练的高仿合成视频或使用静态人脸转动态人脸工具。包括使用离线合成换脸视频和实时合成换脸视频，其主要原理是针对原视频、目标视频进行视频图片抽帧，分别提取图片中的人物脸部进行模型训练，随后使用新的人脸画面覆盖原视频中的人脸画面，合成换脸视频。再结合上述使用的手机虚拟相机类 APP，替换手机相机展示的内容，达到以假乱真的目的。

部分黑产将训练后的人脸模型，配合电脑视频推流+虚拟相机软件，用于诈骗、直播等换脸场景中，其原理是利用视频推流软件捕获电脑实时生成的换脸画面，将该视频推送给虚拟相机软件，虚拟相机软件替换原电脑的画面，展示给使用电脑相机的应用，实现展示换脸内容。

第二篇 电信网络诈骗-黑灰产业链

电信网络诈骗之所以难以彻底根除，关键在于其背后存在着一个庞大的“黑灰产业链”，特别是帮助诈骗人员“拉客”的引流产业、承接黑灰产供需的担保平台，使得诈骗行为更加隐蔽和难以打击。为有效遏制电信网络诈骗，我们需要深入了解这些产业的运作模式，从源头上进行技术反制和打击，如电销引流是如何让受害人相信对方的，担保平台是如何承接黑灰的，产业是如何分工运作的。本文将深入剖析这些产业链，探讨其运作模式和特点，旨在为打击电信网络诈骗提供有益的参考。

第一章、为诈骗引流的礼品电销产业

360 移动安全团队发现黑产招聘电销人员，冒充电商平台，通过赠送礼品的话术，引导用户添加“客服”社交账号，为诈骗人员引流。由于引流话术仅涉及礼品赠送，不涉及诈骗场景，用户在与电销人员沟通时很难发现处于诈骗陷阱中。同时由于后期诈骗人员真的邮寄礼品，用户出于好意也会同意对方要求，添加“客服”社交账号参与更多礼品任务，增加了诈骗引流的成功率。此种方式下，引流人员还可在与受害人沟通过程中，过滤掉防骗意识高的人群，例如不愿意核对地址的，不愿添加社交账号的，进一步增加后续诈骗的成功率。此类引流方式，由于涉及礼品话术，需要多次电话联系受害人，被黑产称为礼品电销、电销一道（也称地址核对或地核）、电销二道（也称推账号）。

第一批电销人员，主要与用户沟通，确认用户电话、地址信息准确性。以赠送用户免费礼品为由，询问用户 XX 地址是否可以收到快递。用户确认后，告知用户后续快递收到会有客服再次来电，再次确认礼品事宜，为第二次通话做铺垫。第二批电销人员，主要与用户沟通，引导用户添加“客服”社交账号。询问用户是否收到免费礼品，若收到是否可以添加客服的微信，完成礼品领取的操作，同时与客服登记，领取新的活动礼品，为诈骗完成引流操作。

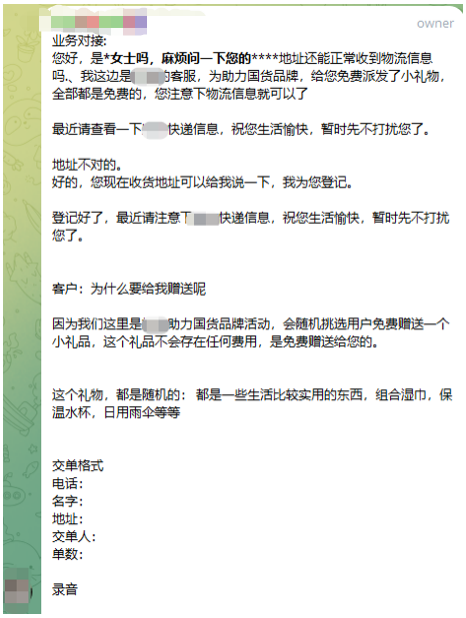

图 12 黑产使用的礼品电销话术

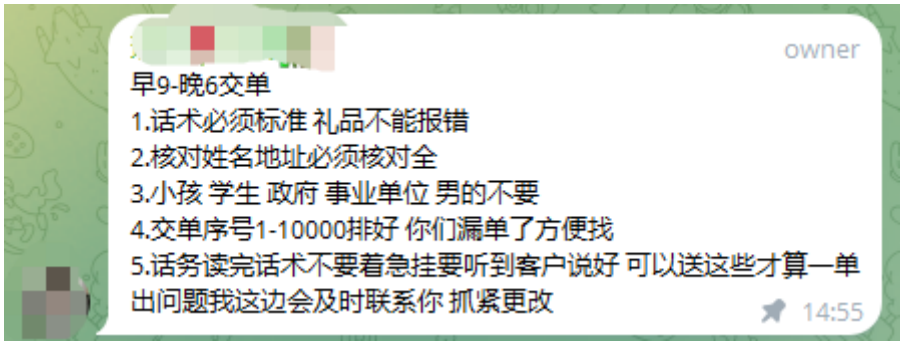

图 13 黑产礼品电销话术要求

引流人员完成核对地址、受害人添加指定的社交账号后，需向上线提交电话录音文件证明完成电销任务，这与目前电销行业的工作流程相似。同时由于引流话术的隐蔽性，这些号码被举报的概率较低，存活周期远超简易组网 GOIP 使用的号码。结合某地公安破获的同类引流窝点所揭露的诈骗人员特征，不法分子利用网络公司伪装，在某地写字楼租赁办公场所，从上线获得客户信息，雇佣人员冒充电商平台客服人员向客户拨打电话，以免费发放小礼品的方式为电信网络诈骗活动进行引流。由此推测，礼品电销产业与上文介绍的简易组网 GOIP 雇佣兼职马仔模式不同，其雇佣的人员可能多来自具有电话号码养号、号码防封经验的电销人群或机构。

第二章、承接黑产供需双方的担保中介

2023 年 6 月，捕获到某黑产平台招募人员针对某平台进行洗资，通过对该洗资手法的上游追溯，我们发现了为洗钱、诈骗行业提供的黑产担保产业，鉴于其在黑产中有着重要的

作用，下面将针对其运营模式进行分析。

目前市面为黑产提供担保服务的平台较多，如汇*、丝*、火*等，但运营方式基本相同，通过自建平台、使用第三方社交群的方式，分别搭建担保公群、供需群等用于对接黑产供需双方。

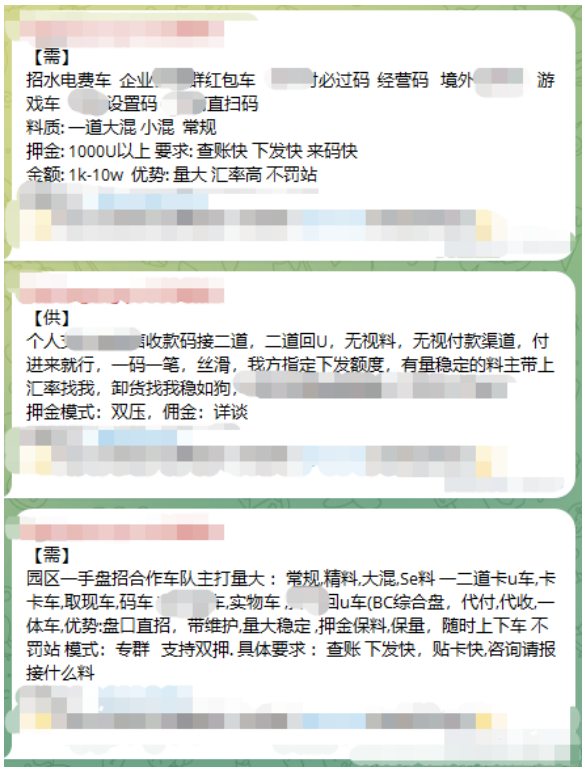

图 14 担保群黑产发布的供需内容

担保公群指的是公布担保流程、供需群链接、客服联系方式的群，一方面方便黑产人员快速了解该平台，一方面防止其他人冒充该担保平台人员实施诈骗。

供需群指的是发布供需的群，类型包括洗钱（代收、承兑、回 U）、电销（固话、手机口）、推广（贴卡片、快递代发）、服务类（设计、搭建）、买卖类（个人信息、手机卡）等，基本覆盖主流黑灰产涉及的场景。其流程为供需人员向担保平台缴纳费用后在供需群发布内容，供需双方选定交易目标后，由担保平台安排交易群进行担保交易，在群内协商并确认交易详情。买家将货款转入担保平台上押账户（虚拟货币地址）并提供凭证，担保平台交易员确认收款后通知卖家发货，卖家按照通知发货并提供凭证，买家确认收货后通知交易员放款，交易员扣除佣金向卖家解押放款并提供放款凭证，卖家确认收款，交易完成。

第三篇 电信网络诈骗案例

第一章、群里炒股的人都赚钱了，自己按照要求投资却无法提现

2023 年 5 月用户在短视频平台看到有人免费推荐股票后私信对方，双方沟通后，对方引导用户下载名称为“多*聊”的软件进行深入沟通，并将用户邀请至“多*聊”中的专属投资群。用户在群里观察几日后，发现群里大家都发赚钱截图，便动心想加入，在对方的引荐下安装了名为“华*券”的应用，通过联系该 APP 中的在线客服，获得充值账号进行充值转账，投资多笔，进行盈利提现时，无法提现，发觉受骗。

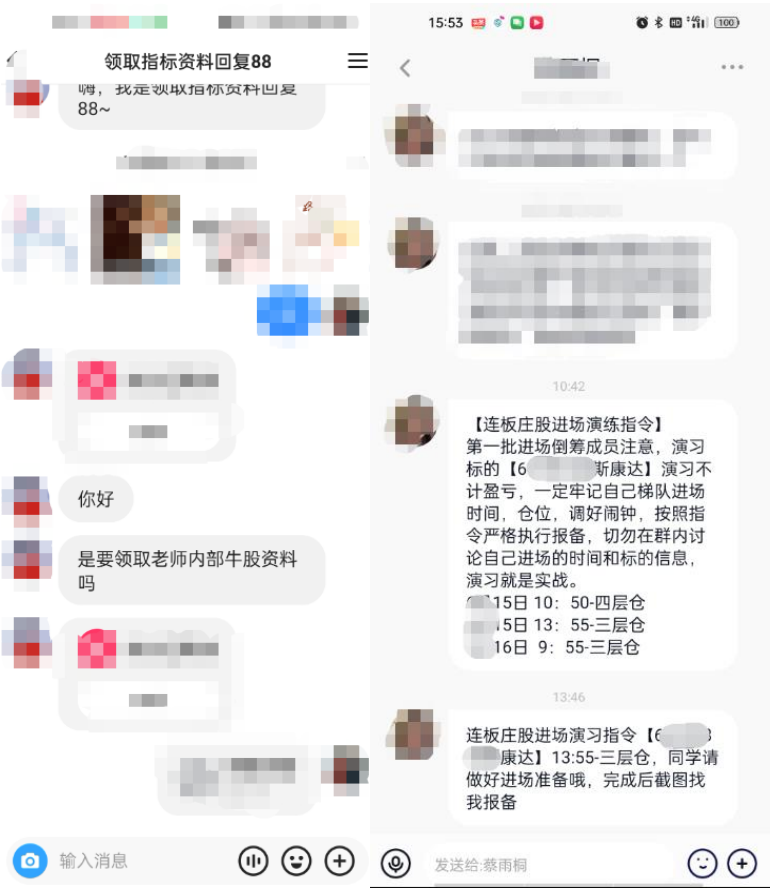

图 15 虚假投资中的荐股话术

案例解读及安全提示

在这个案例中，不法分子通过短视频传播快、受众多的特点，以赠送牛股资料为幌子，吸引受害人关注，并引导用户使用事前制作的私有化聊天软件进行深入沟通，在该聊天软件

中，不法分子通过“炒群”的方式，使用提前进群的小号大量发送赚钱信息，增大受害人的关注度和信任度，当受害人开始投注后，给予用户甜头诱导增加投入，最后拒绝用户提现操作。不要轻信来自陌生人的荐股信息，特别是在社交媒体、聊天群等非正式场合发布的信息，同时谨慎参与“内幕消息”、“高手带盘”等投资活动，因为这些往往是一些不法分子利用投资者的投机心理进行诈骗的手段。

第二章、退还买课的费用，却要求在理财平台投资进行返款

2023 年 6 月用户收到教育清退短信“【***胜】传达您多次了，先前这边课程交的費都还给您了，没有收到的及时联络工作人员补，**：2**3 逾时当放弃”，便联系了短信中的工作人员，对方表示办理清退需要通过指定的平台购买证券，每次购买返回 20%用于退还买课的费用。用户按照操作后，对方又以用户买错证券，需要再购买 2 次大额证券消除失误记录才能提现为由要求用户继续充值，用户按照要求又多次进行购买但仍无法提现，得知受骗。

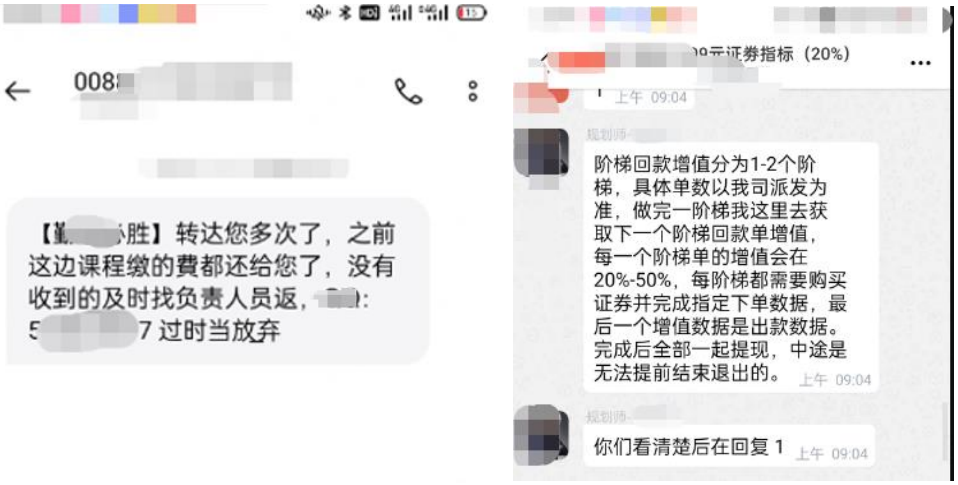

图 16 虚假教育清退短信以及引流话术

案例解读及安全提示

不法分子通过非法渠道获得教培机构的用户信息，通过短信告知用户之前买的课程可以申请退款进而获取用户信任。待用户上钩后，便以该教培机构的退款服务由第三方机构承接为由，将用户引导至虚假的投资理财平台，给用户安排退款计划，即在该投资平台充值，充值返利当作课程退款，并给用户安排规划师保障用户的投资能够盈利，前期投资过程中给予返款，待用户增大金额后，限制提现。当接收到培训机构称“退款”的短信时，切记要提高警惕，特别是提及需要在第三方平台进行投资返款的。

第三章、快递损坏进行赔偿，却误打开支付通道，关闭需要向对方转账

2023 年 6 月，用户收到快递电话，称用户的快递损坏，要给用户进行赔偿，随后双方添加了社交账号。客服以协议用户退款为由，引导用户安装名为“全**”的会议 APP，并开启屏幕共享功能。随后对方称已将赔偿款退到用户的账户中，但用户查询后未收到宣称的款项，对方联系“技术人员”后宣称用户被误打开支付通道，导致退款失败，若不关闭会影响用户的征信，用户在对方的引导下进行转账操作。

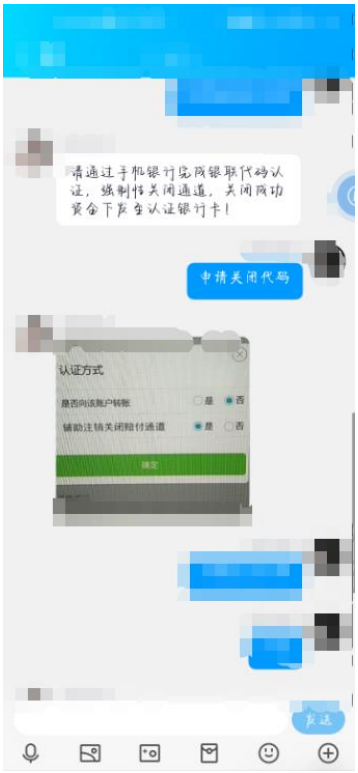

图 17 “客服”诱导话术

案例解读及安全提示

在这个场景中，不法分子冒充快递人员，以用户快递损坏给予赔款为由，吸引用户的信任，并以协助用户进行操作为由，诱导用户安装开启会议类 APP 的屏幕共享功能。“共享屏幕”相当于手机的录屏操作，它会把屏幕上显示的内容实时同步给对方，也就是说你在手机上的任何操作对方都能看到，包括输入银行卡账号、密码、收到的短信验证码等，对方掌握到此些信息后可能在自己无感知的情况下盗刷资金，切勿轻易向陌生人开启屏幕共享功能。

第四章、使用“邀请码”注册应用后，手机信息被盗

用户通过社交软件认识一个网友，对方以和用户视频为由，引导用户安装指定的聊天应用“暧*”，用户安装该应用，并根据其提供的“暧*”注册邀请码进行注册。随后双方通过社交软件进行视频聊天，视频聊天期间，对方偷录下用户的不雅视频，并通过“暧*”应用窃取用户手机通讯录信息，以将用户的不雅视频群发给用户通讯录好友为由，进行敲诈勒索。用户按照对方的要求，陆续向对方指定的账号转账共计 5 万元。

图 18 诱导用户安装恶意应用

案例解读及安全提示

用户被引导安装的“暧*”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，在双方视频聊天后，以将受害人的不雅视频群发给通讯录好友为由进行敲诈勒索。网络交友需谨慎，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。

第五章、免费赠礼品？当心是“陷阱”

2023 年 9 月，用户收到冒充短视频平台客服的电话，以用户是该平台优质用户为由给用户赠送不锈钢锅。在用户收到礼品后，对方表示为帮某电器平台提升知名度，用户参与指定的任务后将赠送用户该品牌的电饭锅或者空气炸锅。用户在对方的引导下添加了指定的社交账号及群，并按照群内的要求下载安装名为“**TOP”的安卓应用，后续通过该应用内置的聊天功能与任务“客服”进行沟通。对方表示为帮助多个电商平台提高活跃度，需要用户浏览指定的店铺，按照浏览情况支付佣金，用户按照要求操作后，获得佣金。次日用户按照对方要求向对方指定的多个账号转账，参与任务，用户多次转账后，对方又以用户任务操作错误为由，要求用户再次转账，用户发觉受骗。

案例解读及安全提示

不法分子冒充平台客服，以免费赠送礼品的方式取得受害人的信任，进而诱导受害人进入设置好的陷进。前期给予蝇头小利，给受害人造成能“赚钱”的假象，后期以“任务未完成”、“操作异常，账户被冻结” 等各种借口诱骗受害人加大投入，直至受害人发现被骗。“做任务赚佣金”不过是刷单诈骗的诱饵，你看中的是佣金，骗子看中的却是你的本金。

第四篇 反电信网络诈骗行业动态

第一章、政策法规颁布落实

一、 深入实施《反电信网络诈骗法》 信息通信行业反诈工作再上新台阶

治网之道，法治为本。2022 年 12 月 1 日，《中华人民共和国反电信网络诈骗法》（以下简称反诈法）正式施行，这是国家法治治理的重要组成，掀开了电信网络诈骗依法治理的新篇章。反诈法施行一年来，工业和信息化部认真贯彻落实习近平总书记关于打击治理电信网络诈骗犯罪工作的重要指示精神，以落实反诈法为指引，履职尽责、主动作为，举全行业之力，切实推动各项工作落实落细、取得实效。

始终坚持法治思维，高效推进宣贯落实

组织开展 7 场行业反诈法宣贯培训，覆盖各省通信管理局、基础电信企业、移动通信转售企业、互联网企业等近百家单位的 1400 余名反诈工作负责同志，设立全行业学法、懂法、用法“大讲堂”。完成首次行业反诈法落实情况执法检查，分赴北京、上海、江苏、广东、四川 5 省市，依法对 4 家基础电信企业集团公司及 7 家省公司、8 家互联网企业、3 家移动通信转售企业开展执法检查，对落实不力企业启动立案调查，督促全行业绷紧反诈“责任弦”。

始终坚持源头治理，重拳夯实行业根基

从严加强电话卡、物联网卡、短信端口等基础管理和风险防范，持续推进“断卡”“打猫”等专项行动，累计清理涉诈高风险电话卡近 2000 万张，联合公安机关打击“猫池”窝点 1 万余个。积极参与制订《电信网络诈骗及其关联违法犯罪联合惩戒办法》，明确非法买卖、出租、出借电话卡等惩戒措施，划清依法办卡（号）“警戒线”。建立“事前充分评估、事后及时治理”涉诈风险防范体系，明确评估标准规范，建立“以案促改、一点发现、行业整改”的涉诈风险管控机制，针对“一号双终端”、“共享屏幕”、iMessage、FaceTime 等涉诈高风险业务，累计下发行业风险警示和问题通报 10 余期，构建风险防范“新格局”。会同有关部门开展金融类 APP 反诈电子标识试点工作，累计监测发现仿冒金融类 APP 近 600 款，相关试点 APP 被仿冒数量下降近 70%，开辟涉诈 APP 源头治理“新思路”。

始终坚持以技管网，牢固构建技防屏障

完善全国一体化反诈技防体系，持续提升涉诈资源精准监测识别、动态封堵处置、高效共享联动、紧密协同配合的技术能力，筑牢重点地区电信网络诈骗技术防护能力，累计拦截涉诈电话和短信超 45 亿次，核查处置涉诈高风险互联网账号近 2 亿个，封堵关停涉诈域名 511 万余个，织牢反诈技术“防护网”。聚焦人民群众反映强烈的突出问题，在“12381 涉诈预警劝阻系统”、“一证通查”、“反诈名片”基础上，创新推出“跨境提醒服务”和“涉诈 APP 安装预警”，累计发送跨境提醒信息 40 亿条，APP 风险预警超万次，扩充技术反制“武器库”。加快推进行业反诈专业队伍建设，持续完善结构合理、衔接配套、覆盖全面的行业反诈标准体系，聚焦治理难题强化专项技术攻关，擘画行业反诈“路线图”。

始终坚持人民至上，大幅提升服务水平

组织全行业建立完善用户申诉渠道，进一步规范涉诈异常电话卡投诉处置工作流程。广泛开展社会反诈宣传，多渠道普及防骗识骗知识，推广反诈特色服务，组织开展进学校、进企业、进社区、进农村、进家庭等宣传活动 5000 余场，针对新型诈骗手法等发送公益提醒短信超 200 亿条，构建社会反诈“同心圆”[4]。

二、 公安部就《电信网络诈骗及其关联违法犯罪联合惩戒办法（征求意见稿）》面向社会公开征求意见

人民网北京 11 月 13 日电，据公安部消息，为深入贯彻落实《中华人民共和国反电信网络诈骗法》，近日，公安部会同有关主管部门起草了《电信网络诈骗及其关联违法犯罪联合惩戒办法（征求意见稿）》（以下简称《惩戒办法（征求意见稿）》），面向社会广泛征求意见。

《惩戒办法（征求意见稿）》共 19 条，主要包括惩戒原则、惩戒对象、惩戒措施、分级惩戒、惩戒程序、申诉核查 6 个方面内容，遵循依法认定、过惩相当、动态管理原则，明确个人和单位纳入惩戒对象的范围，规定金融、电信网络、信用惩戒的具体措施，根据惩戒对象违法行为分级适用惩戒，规范审核认定、惩戒期限和告知等程序，明确申诉、受理、核查、反馈和解除的程序和时限。

《惩戒办法（征求意见稿）》坚持依法认定、预防为主，严格按照《反电信网络诈骗法》确定惩戒对象范围和认定标准，列举了依法被实施惩戒的具体行为，区分了设区的市级以上公安机关和省级以上公安机关审核认定惩戒对象的范围，切实强化警示教育，以实现预防犯罪的效果。

《惩戒办法（征求意见稿）》坚持分级惩戒、过惩相当，对于因实施电信网络诈骗及其关联犯罪被追究刑事责任的人，惩戒期限为 3 年；经设区的市级以上公安机关认定的惩戒对

象，惩戒期限为 2 年。在综合运用金融惩戒、电信网络惩戒、信用惩戒以及纳入金融信用信息基础数据库等惩戒措施的同时，保留了惩戒对象基本的金融、通信服务，确保满足其基本生活需要，充分体现惩戒的适度性。

《惩戒办法（征求意见稿）》在强化依法惩戒的同时，对惩戒信息数据实行动态管理，明确要求将惩戒依据、期限、措施和申诉权利书面告知被惩戒对象，并明确了申诉、受理、核查、反馈和解除等工作的程序和时限，充分保障被惩戒对象的合法权益[5]。

第二章、政府重拳出击

一、 最高检发布《检察机关打击治理电信网络诈骗及其关联犯罪工作情况（2023 年）》依法严惩境外诈骗集团 协同推动网络综合治理

在《中华人民共和国反电信网络诈骗法》实施一周年之际，11 月 30 日，最高人民检察院发布《检察机关打击治理电信网络诈骗及其关联犯罪工作情况（2023 年）》（下称《工作情况》），系统分析当前电信网络诈骗及其关联犯罪主要态势，总结检察机关打击治理的举措与成效，提出下一步工作对策与展望，并就当前电信网络诈骗犯罪的严峻形势进行风险提示及建议。

《工作情况》指出，检察机关起诉电信网络诈骗犯罪案件同比呈明显上升趋势。随着打击治理特别是境外抓捕力度加大，2023 年 1 月至 10 月，全国检察机关共起诉电信网络诈骗犯罪 3.4 万余人，同比上升近 52%。起诉帮助信息网络犯罪活动罪案件仍高位运行，但上涨幅度逐步放缓。与此同时，起诉掩饰、隐瞒犯罪所得、犯罪所得收益罪激增，已成为仅次于帮信罪的第二大电信网络诈骗的关联犯罪。此外，起诉妨害国（边）境管理犯罪快速上涨，已成为电信网络诈骗犯罪链条上的多发罪名。

《工作情况》指出，犯罪人员低龄、低收入、低学历特征依然明显，但文化程度较高人员涉罪呈上升趋势。2023 年前三季度，全国检察机关起诉电信网络诈骗、帮信、掩隐三类犯罪人员中，大学专科以上（包括本科、硕士、博士）人员分别为 4400 余人、5900 余人、7600 余人[6]。

二、 公安部：2023 年共破获电信网络诈骗案件 43.7 万起

中新网 1 月 9 日电，公安部 9 日举行新闻发布会。公安部新闻发言人贾俊强介绍，2023 年，全国公安机关持续向电信网络诈骗犯罪发起凌厉攻势，共破获电信网络诈骗案件 43.7 万起，抓获一大批违法犯罪嫌疑人，自 2023 年 8 月以来电信网络诈骗发案数连续下降，打击治理工作取得显著成效。

一是始终保持高压严打态势。全链条打击电信网络诈骗及关联犯罪，深入开展“斩链”“清源”“利剑”三大战役，抓获了一大批违法犯罪人员，破获了一大批诈骗案件；会同最高人民法院、最高人民检察院等相关部门联合部署开展“拔钉”专项行动，成功将 263 名电信网络诈骗犯罪集团重大头目和骨干缉捕归案；组织开展“鄂湘鲁豫”区域会战，共捣毁诈骗窝点 1800 余个，实现规模打击效能最大化；针对涉诈黑灰产链条，组织发起打击涉诈固话语音专线、简易组网 GOIP、跑分洗钱等各类集群战役 277 起，取得了显著战果。

二是切实运用好法律规定。在依法严厉打击的同时，部署全国公安机关统筹抓好《中华人民共和国反电信网络诈骗法》的贯彻实施工作，联合最高人民法院、最高人民检察院进一步完善“两卡”犯罪法律适用标准，严格依法办案，持续加大打击力度，全面提升打击质效，形成有力震慑。

三是深入推进源头治理防范。依托国务院部际联席会议机制，积极会同相关部门加强科技支撑、强化预警防范，坚持系统观念、深入推进行业监管源头治理，努力构建更加严密的防范治理体系。公安部指导各地公安机关建立分级分类预警劝阻机制，推动“厦门经验”在全国落地生效，截至 2023 年 12 月底，国家反诈中心累计向各地下发资金预警指令 940 万条，公安机关累计见面劝阻 1389 万人次，会同相关部门拦截诈骗电话 27.5 亿次，短信 22.8 亿条，处置涉诈域名网址 836.4 万个，紧急拦截涉案资金 3288 亿元。人民银行深入推进“资金链”治理，支付行业常态化治理格局持续完善，组织商业银行、支付机构、清算机构协助公安机关阻断大量涉诈资金转移，挽回大量人民群众损失。工信部持续推进“断卡行动 2.0”，开展“不良 APP 安全治理”，严格落实实名制，全力整治虚商卡，对短信端口、语音专线、云服务等重点业务加大清理整治力度，不断提升全流程及时反制能力。中央网信办集中整治互联网接入、域名注册、服务器托管、APP 制作开发、网络直播、引流推广等涉诈重点领域，约谈曝光问题突出企业，网络生态环境不断得到净化。

四是加强宣传提升防骗意识。加强对易受骗群体、案件高发行业和重点地区的精准宣传，联合中央宣传部组织开展“全民反诈在行动”集中宣传月活动，组织各类反诈宣传“进社区、进农村、进家庭、进学校、进企业”活动 2 万余场次，发送反诈宣传短信 30.7 亿条，国家反诈中心官方政务号发布短视频 9800 余条、播放量超 52 亿次，形成全社会反诈的浓厚氛围

[2]。

三、 中缅联合打击跨国电信网络诈骗犯罪取得标志性重大战果

针对当前缅北涉我电信网络诈骗犯罪严峻形势，公安部持续加强与缅甸执法部门的国际警务合作，1 月 30 日，缅甸警方依法向我公安机关移交了白所成、白应苍、魏怀仁、刘正祥、刘正茂、徐老发 6 名缅北果敢电诈犯罪集团重要头目和另外 4 名重大犯罪嫌疑人。当晚，随着一架中国民航包机降落在云南昆明长水机场，缅方移交的 10 名重大犯罪嫌疑人被我公安机关成功押解回国。此次行动是中缅两国开展国际警务执法合作取得的又一标志性重大战果，充分彰显了两国联合打击跨国电信网络诈骗犯罪、共同携手维护安全稳定秩序的坚定决心和坚强意志。

长期以来，缅北果敢自治区以白所成、魏怀仁、刘正祥、徐老发等为首的多个犯罪集团大肆组织开设诈骗窝点，公开武装护诈，针对中国公民疯狂实施电信网络诈骗犯罪活动，诈骗数额巨大，同时涉嫌故意杀人、故意伤害、非法拘禁等多种严重暴力犯罪，犯罪情节极其恶劣，社会危害极其严重，人民群众深恶痛绝。在掌握相关犯罪事实和证据的基础上，2023 年 12 月 10 日，我公安机关对白所成等 10 名缅北果敢自治区电信网络诈骗犯罪集团重要头目进行公开悬赏通缉。在外交部和我驻缅大使馆大力支持下，公安部派出工作组赴缅甸开展国际警务执法合作，工作组与缅方进行多轮会谈磋商，就联合打击电信网络诈骗犯罪、全力缉捕并移交电信网络诈骗集团重要头目等达成一致意见。随后，缅甸警方陆续抓获了我公安机关公开通缉的白所成、白应苍、魏怀仁、刘正祥、刘正茂、徐老发 6 名犯罪嫌疑人，白应兰、魏榕、魏青松、刘积光 4 名犯罪嫌疑人在逃。1 月 30 日，缅警方决定将到案的上述 6 名犯罪嫌疑人以及我公安机关前期向其通报的另外 4 名重大犯罪嫌疑人移交我方。当天，公安部组织云南公安机关民警赴缅甸执行包机押解任务，成功将相关犯罪嫌疑人押解回国。

公安机关有关负责人表示，为坚决彻底铲除缅北涉我电信网络诈骗犯罪“毒瘤”，公安部与缅甸警方持续开展执法安全合作，云南公安机关不断深化与缅甸相关地方执法部门的边境警务执法合作，在前期持续不断打击下，截至目前，已有 4.4 万名缅北涉我电信网络诈骗犯罪嫌疑人移交我方，其中幕后“金主”、组织头目和骨干 171 名，网上在逃人员 2908 名，有力打击了境外诈骗集团的嚣张气焰，打击工作取得历史性重大战果。公安机关将始终保持对此类犯罪的严打高压态势，不断深化国际执法合作，持续缉捕电信网络诈骗犯罪集团重要头目，纵深推进专项打击行动，坚决维护人民群众生命财产安全，切实维护边境安全稳定[3]。

第五篇 电信网络诈骗趋势预测与反制建议

第一章、新型网络犯罪趋势预测

当前，电信网络诈骗呈集团化、产业化、链条化、跨境化态势，境外出现以“工业园”“科技园”为幌子的超大犯罪集团，从单独实施诈骗犯罪到衍生出故意伤害、非法拘禁等严重暴力犯罪，严重损害人民群众安全感[7]。同时，不法分子不断寻求新的技术和手段，试图绕过如 360 手机卫士等反诈安全类产品的识别。2023 年出现的、迭代的新型简易组网 GOIP、无感盗刷远控、1 人 1 包等技术已凸显出现阶段黑产行业整体的变革，从早期使用引导话术“麻痹”用户，到现在全方位技术“升级”，对安全行业的反诈手段做定向绕过。

在推广引流方面，新型简易组网 GOIP 利用高频电话风控“漏洞”，传统治理涉诈、骚扰等类型电话，主要依托电话的呼叫频率、离散度等进行风险号码识别，但新型简易组网 GOIP 利用的 AXB（呼叫转移）模式，从通话行为看是用户给自己进行频繁呼叫，没有实际发生高频呼叫行为，从而绕过识别策略。

在技术开发方面，传统对恶意 APP 样本的检测和识别多依托病毒库，通过源源不断收录样本，结合动态静态分析手段，增加病毒库识别量。1 人 1 包样本，其同一个下载链在不同时间下载的样本不同，即“无限量”应用。此种情况下，样本量无法完全收录，突破了传统的样本库收录、识别策略。

在转账洗钱方面，“无感盗刷远控”利用安卓系统的辅助等功能机制，将原本便于用户操作手机的功能“恶意化”使用，诱导用户将该权限授予恶意应用，从而实现手机远控。由于盗刷转账在本机、常用网络环境实施，绕过传统的账号异地登录、同网络环境、新设备风控机制。

在生成式 AI 方面，传统黑产通过人脸图片合成技术，让图片动起来，实施身份仿冒诈骗、恶意绕过各类人脸认证系统。随着 AI 技术的快速发展，AI 生成的人脸越发逼真，降低了身份伪造、绕过人脸认证的门槛。从掌握的黑产情报来看，出现了为诈骗、洗钱行业提供 AI 人脸技术的供应商，特别是贩卖 AI 人脸过“三色人脸认证”方案。目前，虽然 AI 诈骗案尚未成气候，但我们应该提前警惕，防止 AI 技术被滥用。

第二章、黑产攻防对抗应对手段

反诈行业与传统行业的区别在于，它不是一成不变的，它要面临持续的攻击，仍保守使

用传统技术和固有思维，就会面临“落后就要挨打”的困境。而对抗的关键是掌握对黑产的持续捕获、研究、实战反制能力，我们尝试通过分享反诈经验的方式，为反诈行业提出建议，以期促进反诈行业健康发展。

一、 情报共享，提升黑产捕获能力

攻防对抗的升级，黑产交易也藏匿的越深，特别是黑产担保平台的出现，让供应双方更加的隐蔽，使得黑产的情报挖掘、溯源成为反诈行业的痛点。目前针对电信诈骗行业的威胁情报平台仍是以自建自用为主，知识库标准不统一，还未形成类似网络安全行业使用的威胁情报平台共享机制，例如恶意样本分类、家族分类、攻防手段共享。借助共享机制，各行业可以针对性的对新兴黑产技术、趋势进行预警反制，避免出现黑产已淘汰的技术被当成新技术进行反制。基于多年情报运营经验，通过深入分析黑产攻击行为链，关联样本，360 移动安全积累了大量的高价值黑灰产情报数据、指纹特征，包括黑产使用的 IP、号码、工具、产业链运营模式等，搭建了多套自动化+人工辅助运营的黑产情报捕获系统，并通过合作、培训等方式向反诈行业输出最新的黑产情报。

二、 技术革新，提升黑产识别能力

利用大数据、大模型技术，挖掘潜在黑产模式，形成反制特征。基于多年对于大量诈骗电话、短信、恶意应用、钓鱼网址等黑产样本的研究，结合动态沙箱检测能力，360 移动安全设计出多个自动化分析引擎，积累了各类样本特征，黑产攻击链行为，从而分析出攻击链全貌，对新型、未知恶意样本实时识别，特别是考验引擎上下文本理解能力的“纯内容”类黑灰样本。通过 360 手机卫士，安全 SDK 等产品赋能给用户，提升用户及行业反诈能力。

参考文献

[1] 中华人民共和国最高人民检察院. 最高检向 28 个省份交办督办涉缅北电诈案件，涉案人员达 4.5 万名[EB/OL]. https://www.spp.gov.cn/spp/zdgz/202402/t20240204_642611.shtml，2024/02/04

[2] 中国新闻网. 公安部：2023 年共破获电信网络诈骗案件 43.7 万起[EB/OL]. https://www.chinanews.com.cn/gn/2024/01-09/10142690.shtml, 2024/01/09

[3] 中华人民共和国公安部. 中缅联合打击跨国电信网络诈骗犯罪取得标志性重大战果[EB/OL]. https://www.mps.gov.cn/n2253534/n2253535/c9421395/content.html, 2024/01/30

[4] 中华人民共和国工业和信息化部.深入实施《反电信网络诈骗法》 信息通信行业反诈工作再上新台阶[EB/OL]. https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2023/art_f52146c1deaa43e6913f43f5e0935b5f.html，2023/12/01

[5] 人民网. 公安部就《电信网络诈骗及其关联违法犯罪联合惩戒办法（征求意见稿）》面向社会公开征求意见[EB/OL]. http://society.people.com.cn/n1/2023/1113/c1008-40116913.html，2023/11/13

[6] 中华人民共和国最高人民检察院. 最高检发布《检察机关打击治理电信网络诈骗及其关联犯罪工作情况（2023 年）》依法严惩境外诈骗集团 协同推动网络综合治理[EB/OL]. https://www.spp.gov.cn/xwfbh/wsfbt/202311/t20231130_635181.shtml#1, 2023/11/30

[7] 中华人民共和国最高人民检察院. 最高检厅长访谈|专访最高人民检察院第四检察厅厅长张晓津：坚持治罪与治理相结合，优化金融生态[EB/OL]. https://www.spp.gov.cn/spp/zdgz/202402/t20240205_642908.shtml，2024/02/05

附录-2023 中国手机安全数据报告

一、2023 年手机诈骗概况

1. 报案数量与类型

2023 年全年，360 反诈赔付保（原手机先赔）共接到 8 类手机诈骗举报，人均损失 36869 元。在所有诈骗类型中，交友占比最高达 41.4%；其次是虚假兼职（24.3%）和身份冒充（12.0%）。从涉案总金额来看，依然交友类诈骗总金额最高占比 50.6%；其次是身份冒充诈骗占比 19.1%；虚假兼职排第三占比 16.7%。下图为 2023 年度手机诈骗的举报类型与涉案金额分布情况：

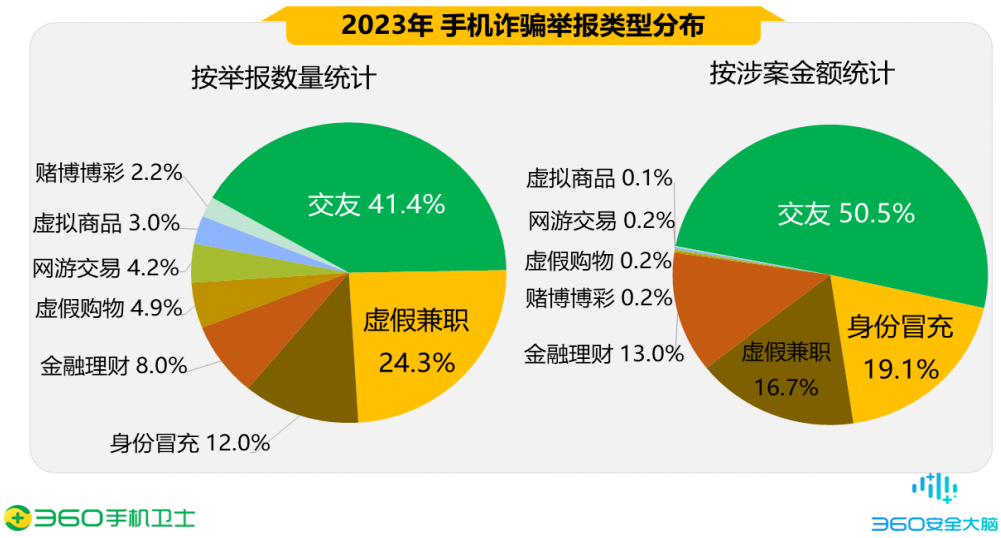

图 19 2023 年手机诈骗举报类型分布

2023 年度，手机诈骗中交友、虚假兼职、身份冒充、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 6.0 万元；其次为身份冒充类，人均损失约为 5.9 万元。交友类诈骗主要为裸聊敲诈，前期对方以和用户视频为由，诱导用户安装含窃取手机通讯录功能的 APP，随后双方进行视频聊天，在此期间对方偷录下用户的不雅视频，以将用户的不雅视频群发给用户通讯录好友为由，进行敲诈勒索。同时，2023 年也出现多个“空降任务”诈骗案例，不法分子利用色情平台传播，诱导安装虚假招嫖 APP，以“免费上门服务”为噱头进行引流，诱导用户参与其平台的虚假刷单活动，骗取资金。

2. 受害者性别与年龄

2023 年度，从举报用户的性别差异来看，男性受害者占 71.5%，女性占 28.5%，男性受害者占比高于女性。从人均损失来看，男性为 40653 元，女性为 27369 元，男性人均损失高于女性。下图为 2023 年度手机诈骗受害者性别差异：

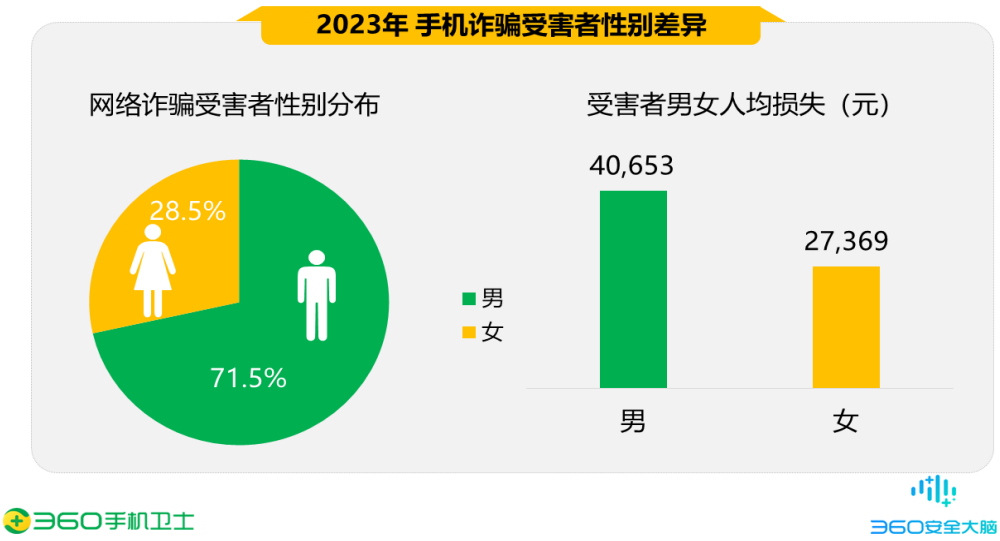

图 20 2023 年手机诈骗受害者性别差异

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 38.2%，是不法分子从事网络诈骗的主要受众人群；其次是 80 后，占比为 33.3%；00 后占比为 19.8%；70 后占比为 5.7%、60 后占比 2.3%、50 后占比 0.6%。下图为 2023 年度手机诈骗受害者年龄段分布：

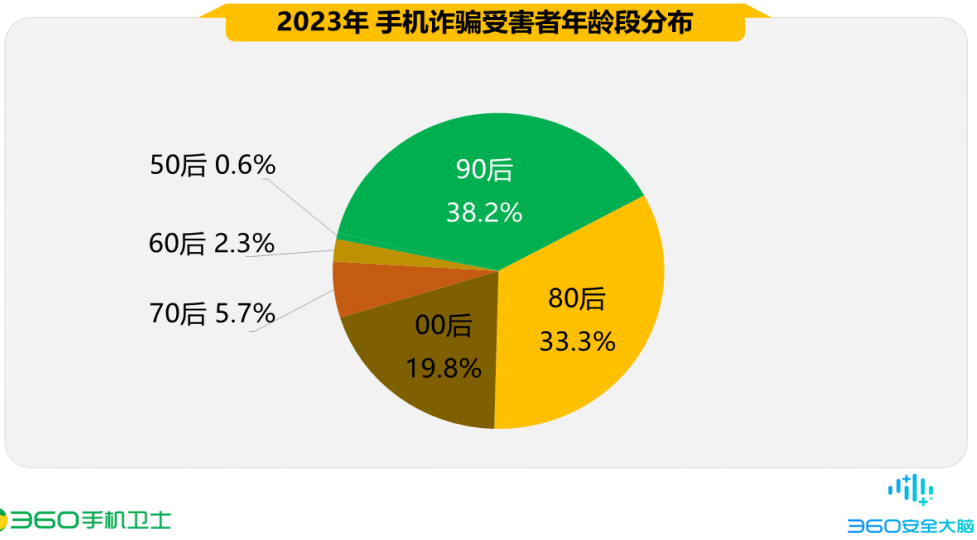

图 21 2023 年手机诈骗受害者年龄段分布

从被骗网民的年龄段人数来看，2023 年度 90 后、80 后、00 后均为诈骗高发人群，受骗类型以交友、虚假兼职类为主。

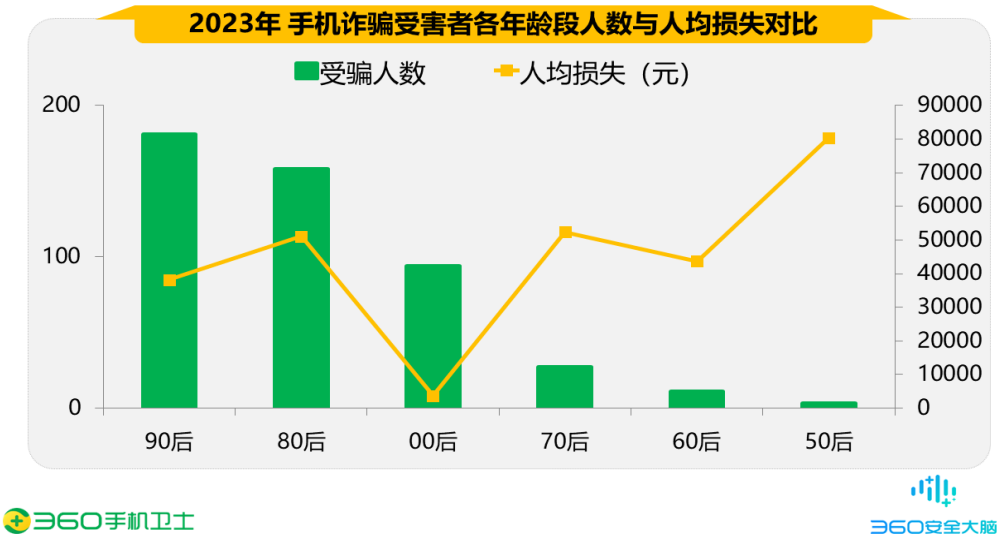

图 22 2023 年手机诈骗受害者各年龄段人数与人均损失对比

3. 受害者地域分布

2023 年度，从各地区手机诈骗的举报情况来看，广东（9.5%）、山东（8.4%）、河北（6.8%）、河南（6.1%）、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 35.9%。下图给出了 2023 年度手机诈骗举报数量最多的 10 个省份：

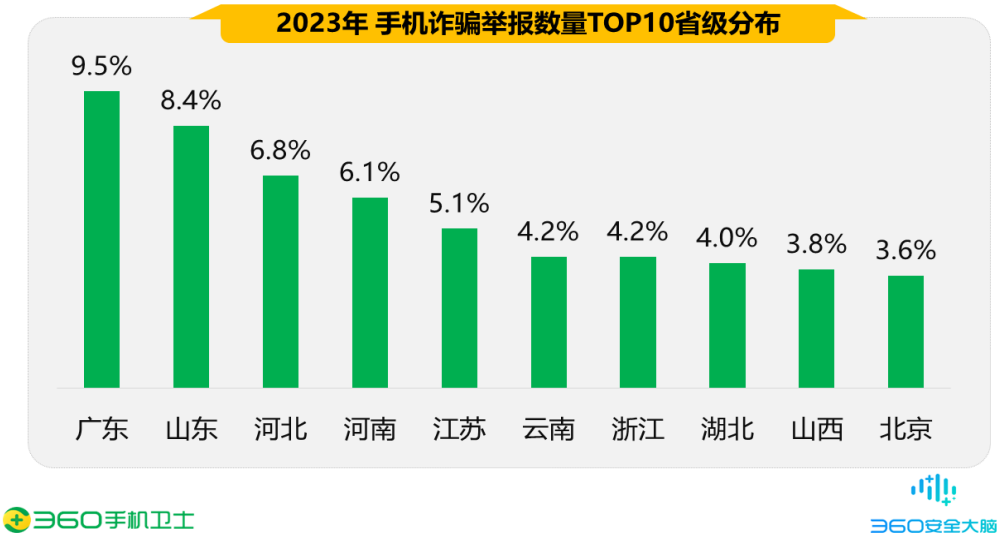

图 23 2023 年 手机诈骗举报数量 TOP10 省级分布

从各城市手机诈骗的举报情况来看，北京（3.6%）、上海（1.9%）、西安（1.9%）、广州（1.7%）、济南（1.7%）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 10.8%。下图给出了 2023 年度手机诈骗举报数量最多的 10 个城市：

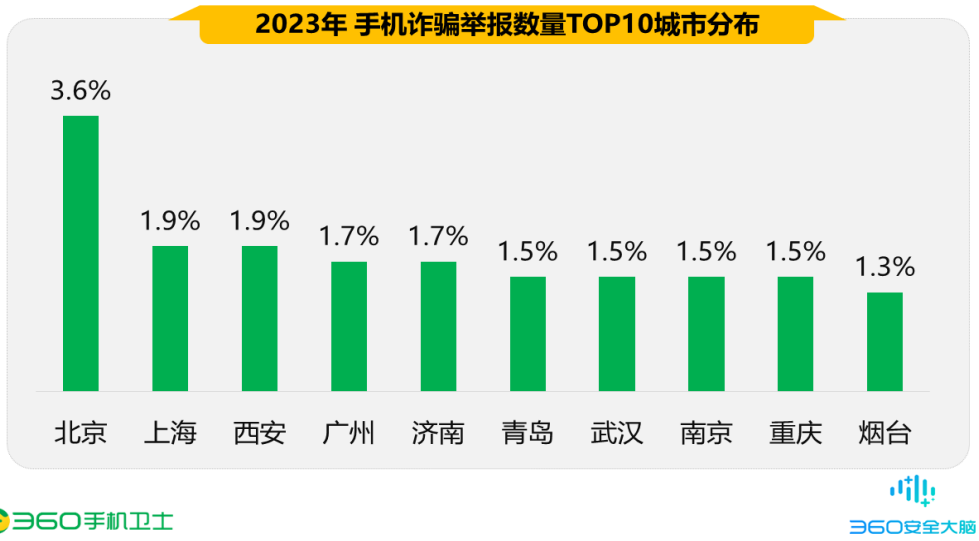

图 24 2023 年 手机诈骗举报数量 TOP10 城市分布

二、移动端诈骗场景识别

1. 移动端诈骗场景感染量与类型分布

2023 年全年，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 3590.8 万，下图为 2023 年度移动端各月诈骗场景感染量统计：

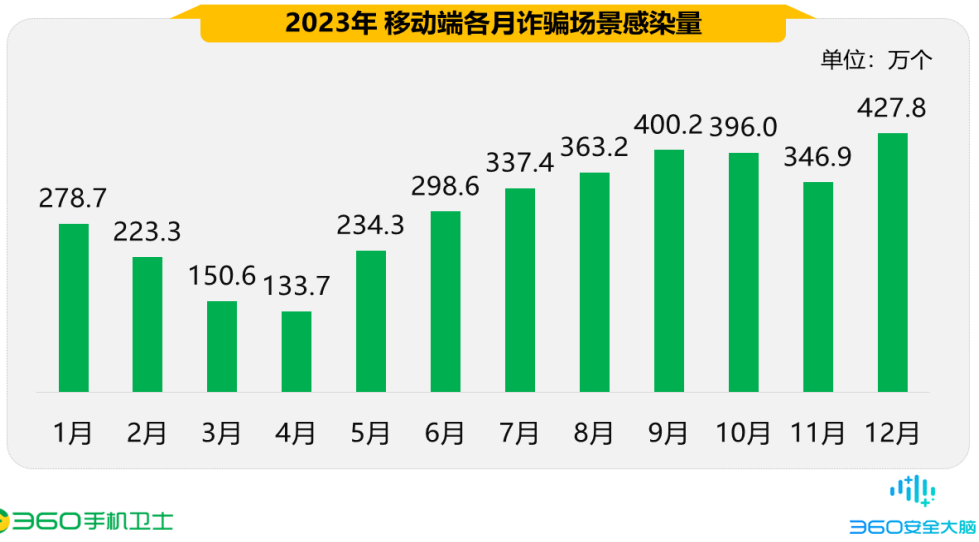

图 25 2023 年 移动端各月诈骗场景感染量

2023 年全年，移动端诈骗场景类型主要为刷单返利，占比 87.6%；其次为网络贷款（7.2%）、虚假投资理财（3.9%）、裸聊敲诈（0.8%）、“杀猪盘”（0.3%）等。针对持续高发的诈骗态势和日益激烈的攻防对抗，360 移动安全团队加大技术反制研发投入，通过各种模型策略增加黑灰产样本的识别能力和数量，下半年有明显增加。下图为 2023 年度移动端诈骗场景类型分布：

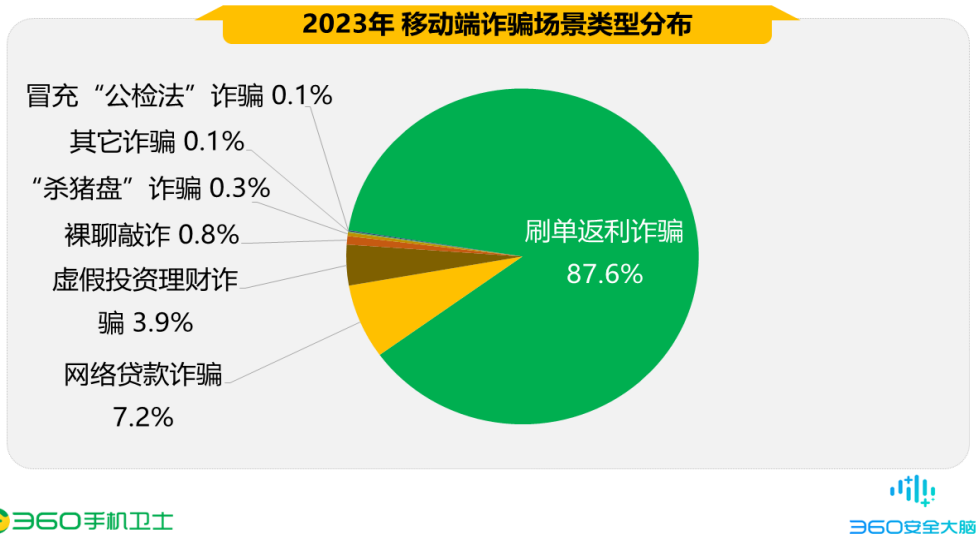

图 26 2023 年 移动端诈骗场景类型分布

2. 移动端诈骗场景感染量地域分布

2023 年全年，从省级分布来看，诈骗场景感染量最多的地区为广东，占全国感染量的 8.8%；其次为山东（7.0%）、河南（6.9%）、江苏（6.4%）、四川（6.3%），此外河北、浙江、陕西、云南、贵州的诈骗场景感染量也排在前列。

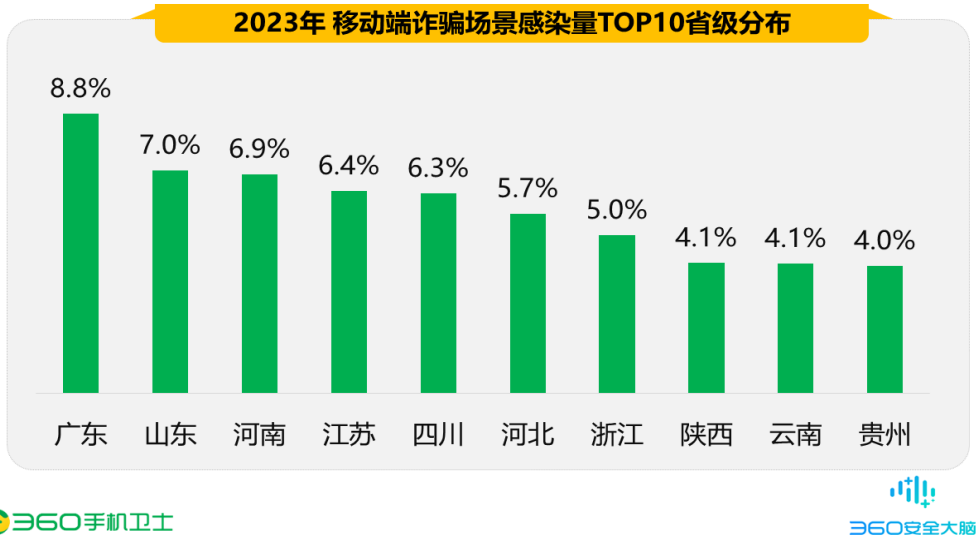

图 27 2023 年 移动端诈骗场景感染量 TOP10 省级分布

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 2.2%；其次为新疆（1.8%）、重庆（1.8%）、西安（1.7%）、深圳（1.6%），此外广州、苏州、郑州、武汉、昆明的诈骗场景感染量也排在前列。

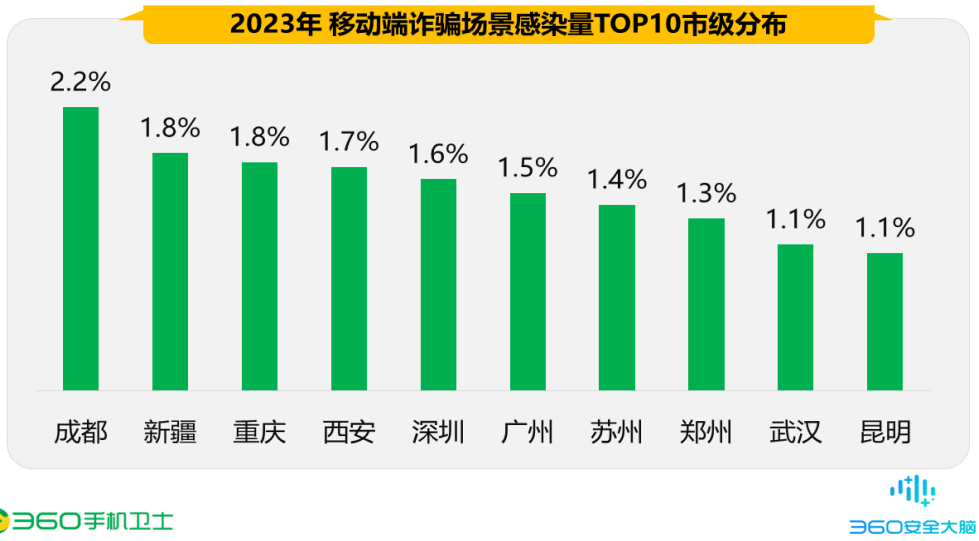

图 28 2023 年 移动端诈骗场景感染量 TOP10 市级分布

三、恶意程序

1. 恶意程序新增样本量

2023 年度，360 安全大脑共截获移动端新增恶意程序样本约 5964.0 万个，同比 2022 年度（2407.9 个）上升了 147.7%，平均每天截获新增手机恶意程序样本约 16.3 万个。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。下图给出了 2013 年-2023 年移动端新增恶意程序样本量统计：

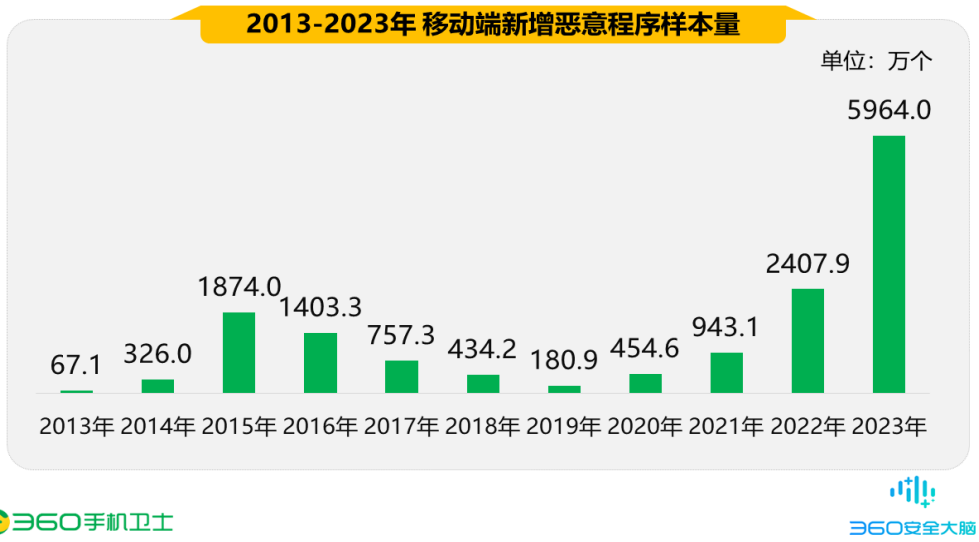

图 29 2013-2023 年 移动端新增恶意程序样本量

2023 年全年，从第三季度开始，新增样本量开始逐步增加，8 月达到峰值，具体分布如下图所示：

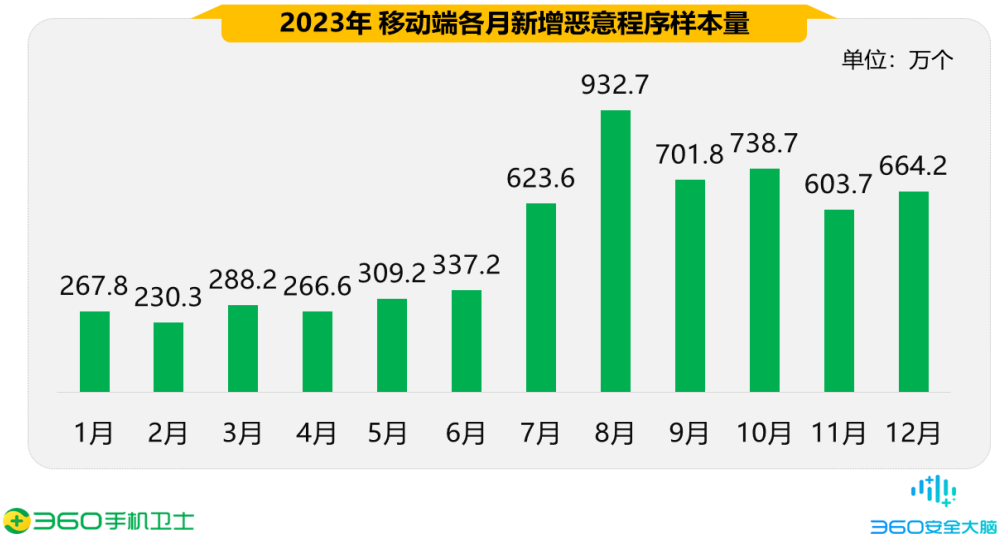

图 30 2023 年 移动端各月新增恶意程序样本量

2. 恶意程序拦截量

2023 年度，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 115.5 亿次，平均每天拦截手机恶意程序攻击约 3163.4 万次。下图为 2023 年度移动端各月恶意程序拦截量统计：

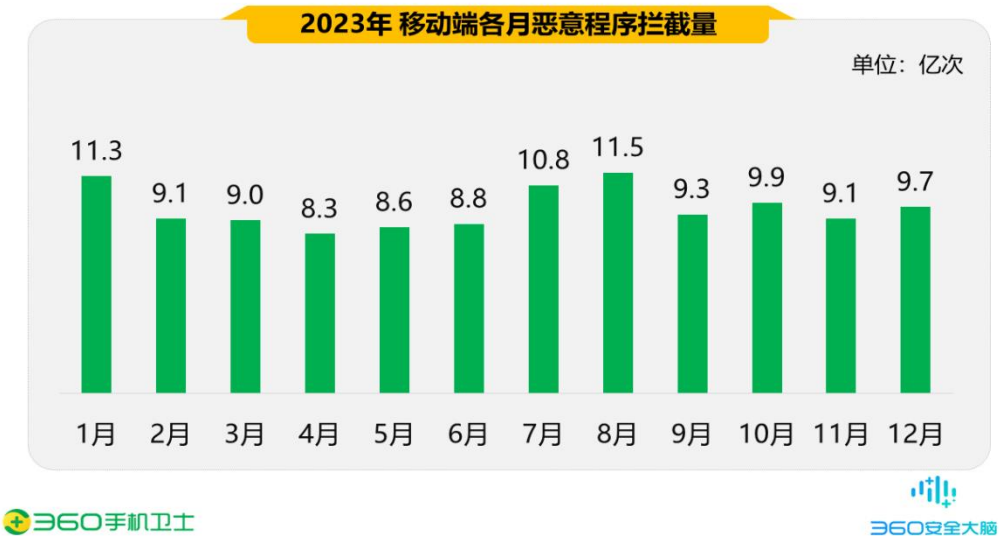

图 31 2023 年 移动端各月恶意程序拦截量

3. 恶意程序拦截量地域分布

2023 年度，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 10.9%；其次为江苏（7.5%）、山东（7.4%）、河南（7.3%）、河北（5.4%），此外浙江、四川、安徽、湖南、广西的恶意程序拦截量也排在前列。

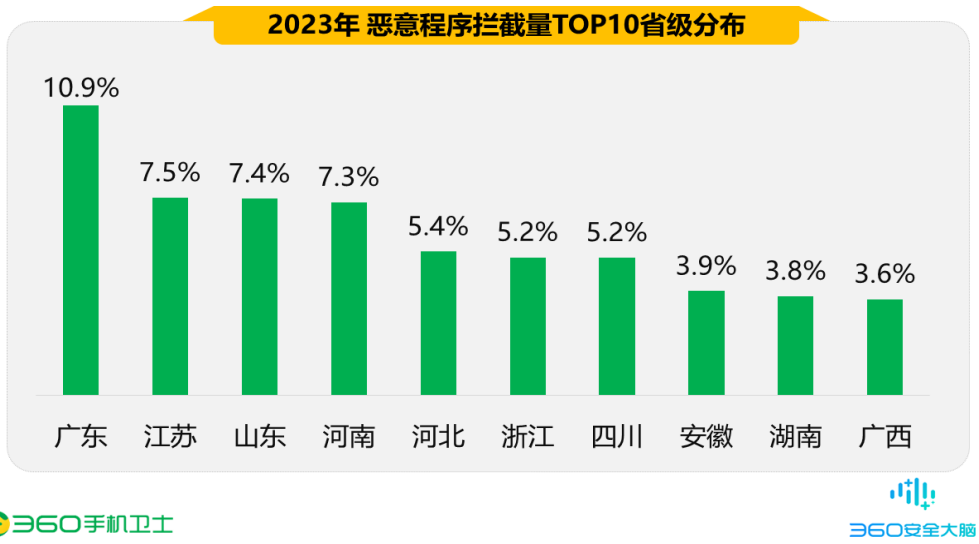

图 32 2023 年 恶意程序拦截量 TOP10 省级分布

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 2.2%；其次为重庆（2.1%）、北京（2.0%）、成都（1.9%）、上海（1.9%），此外深圳、苏州、杭州、郑州、南京的恶意程序拦截量也排在前列。

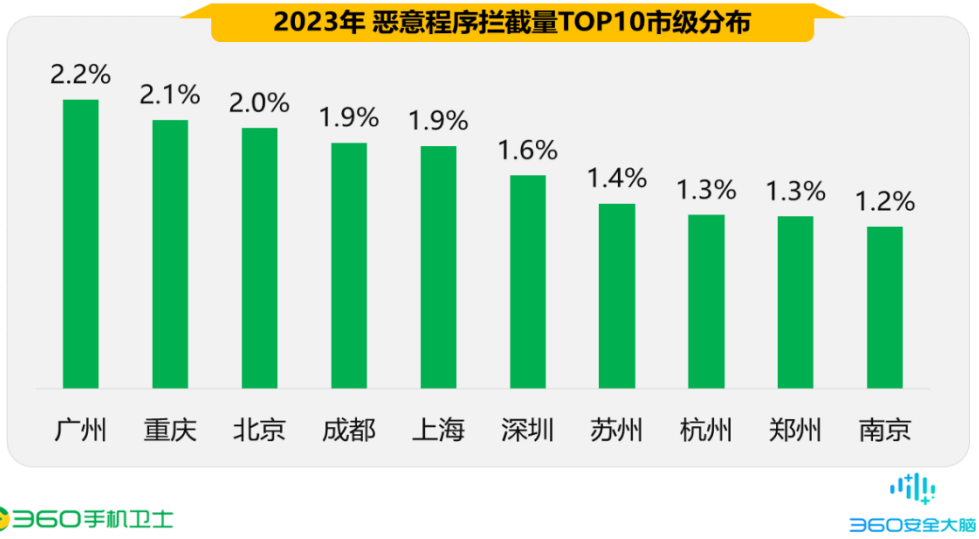

图 33 2023 年 恶意程序拦截量 TOP10 市级分布

4. 涉诈应用类型分布

2023 年度，根据 360 安全大脑捕获的涉诈应用样本分析，涉诈应用类型主要为色情类，占比 42.9%，其次为通联类（28.1%）、黄赌合流类（17.7%）、赌博类（6.4%）、贷款类（3.0%）等，其中通联类应用指使用聊天 SDK 框架生成的内嵌诈骗网页的 APP。下图为 2023 年移动端涉诈应用类型分布：

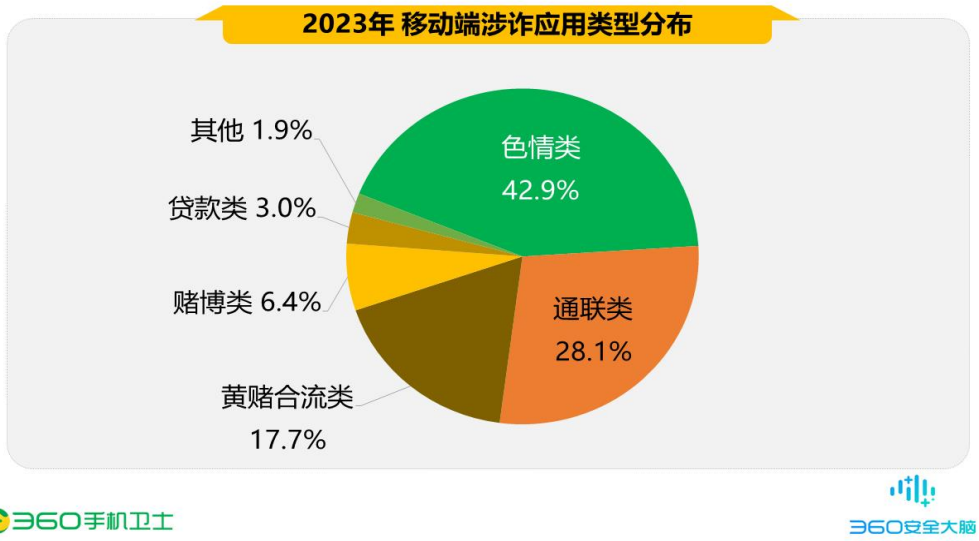

图 34 移动端涉诈应用类型分布

四、钓鱼网站

1. 移动端钓鱼网站各月拦截量分布

2023 年度，360 安全大脑在移动端拦截钓鱼网站攻击约为 4.2 亿次，同比 2022 年度（4.3 亿次）下降 1.3%。下图为 2023 年度钓鱼网站各月拦截量分布：

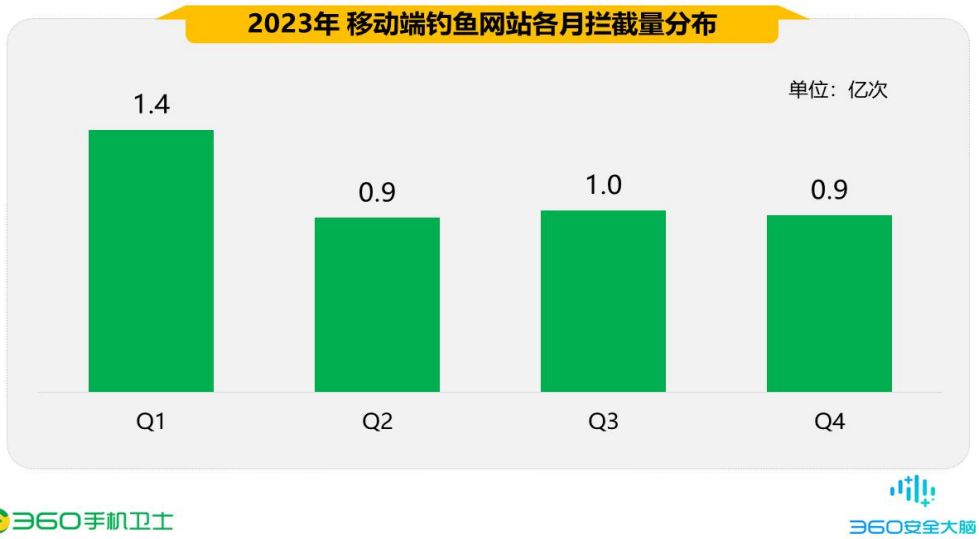

图 35 2023 年 移动端钓鱼网站各月拦截量分布

2. 移动端钓鱼网站类型分布

2023 年度，移动端拦截钓鱼网站类型主要为境外彩票，占比高达 78.9%；其次为色情（14.4%）、金融证券（3.3%）、虚假购物（1.5%）、赌博（1.2%）等。下图为 2023 年度移动端拦截钓鱼网站类型分布：

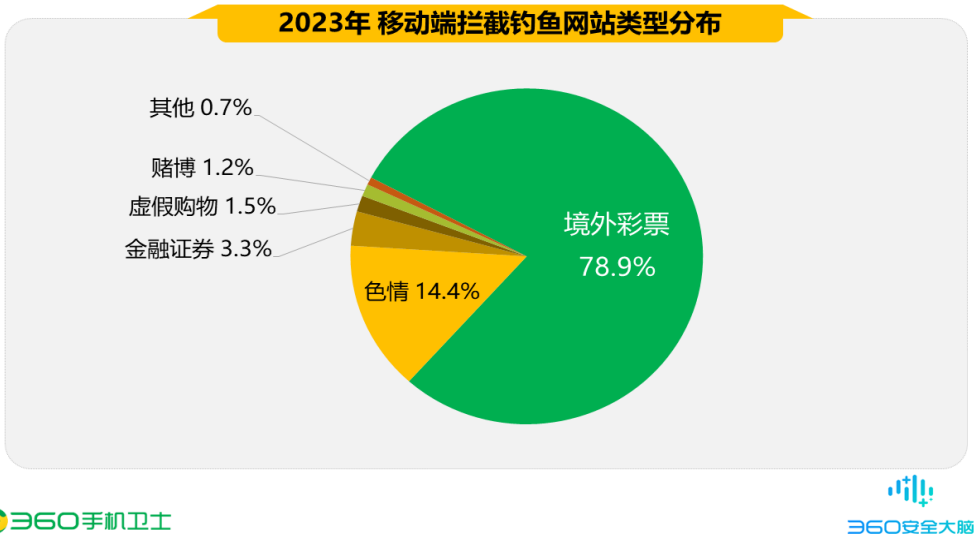

图 36 2023 年 移动端拦截钓鱼网站类型分布

3. 移动端钓鱼网站新增量

2023 年全年，360 安全大脑共截获各类新增钓鱼网站 2.0 亿个，同比 2022 年（1.9 亿个）上升了 3.3%，平均每天新增 54.4 万个。下图为 2023 年度钓鱼网站新增量分布：

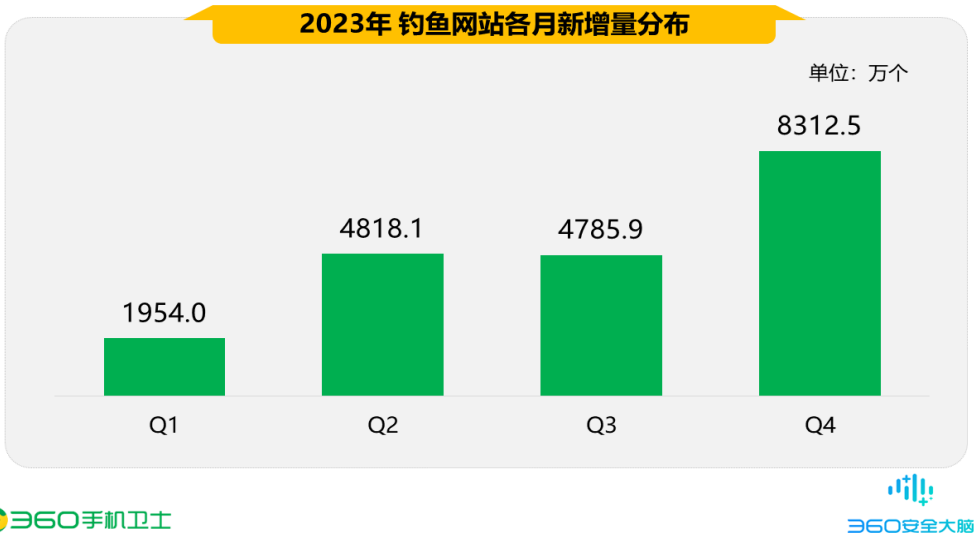

图 37 2023 年 钓鱼网站各月新增量分布

在钓鱼网站新增类型中，色情类占据首位，占比 85.4%；其次为赌博类，占比 11.5%。下图为 2023 年度移动端新增钓鱼网站类型分布：

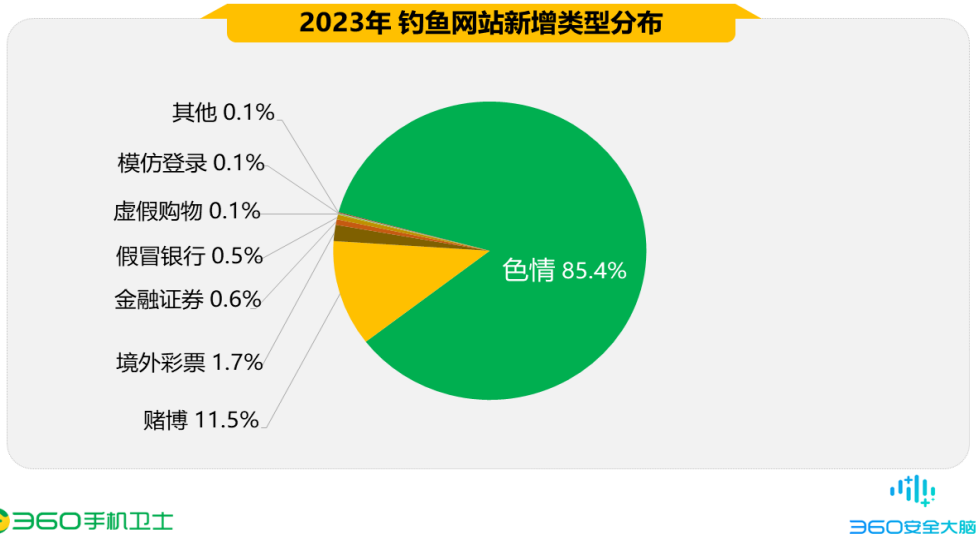

图 38 2023 年 钓鱼网站新增类型分布

4. 移动端钓鱼网站拦截量地域分布

2023 年全年，从省级分布来看，移动端拦截钓鱼网站最多的地区为广东省，占全国拦截量的 16.4%；其次为广西（10.5%）、福建（9.7%）、湖南（5.3%）、山东（4.7%），此外浙江、江苏、河南、四川、河北的钓鱼网站拦截量也排在前列。

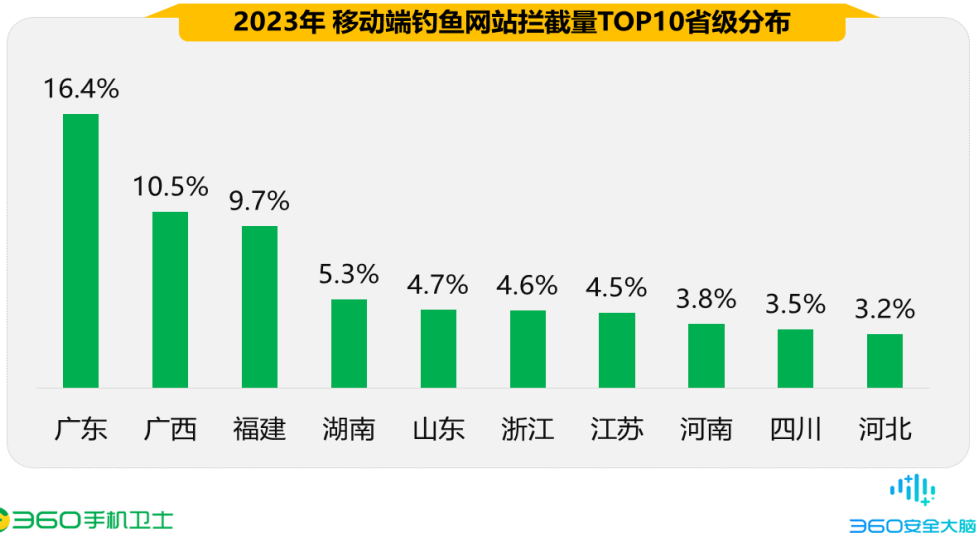

图 39 2023 年 移动端钓鱼网站拦截量 TOP10 省级分布

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 6.1%；其次为南宁（3.9%）、深圳（3.4%）、北京（2.8%）、东莞（2.6%），此外泉州、上海、漳州、成都、重庆的钓鱼网站拦截量也排在前列。

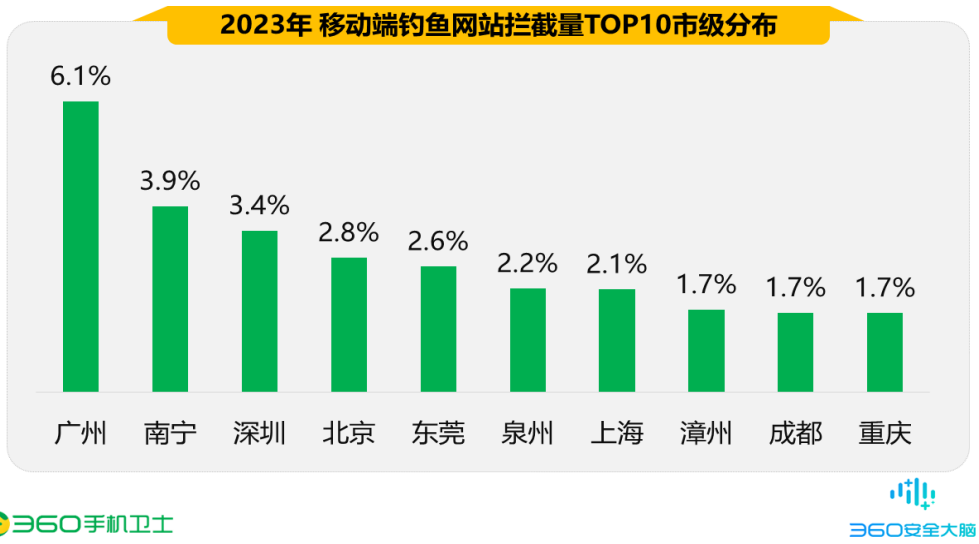

图 40 2023 年 移动端钓鱼网站拦截量 TOP10 市级分布

五、骚扰电话

1. 骚扰电话拦截量

2023 年全年，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 240.3 亿次，平均每天识别和拦截骚扰电话约 0.7 亿次。环比 2022 年（233.9 亿次）上涨了 2.7%。下图给出了 2014 年-2023 年用户标记骚扰电话拦截号码次数统计：

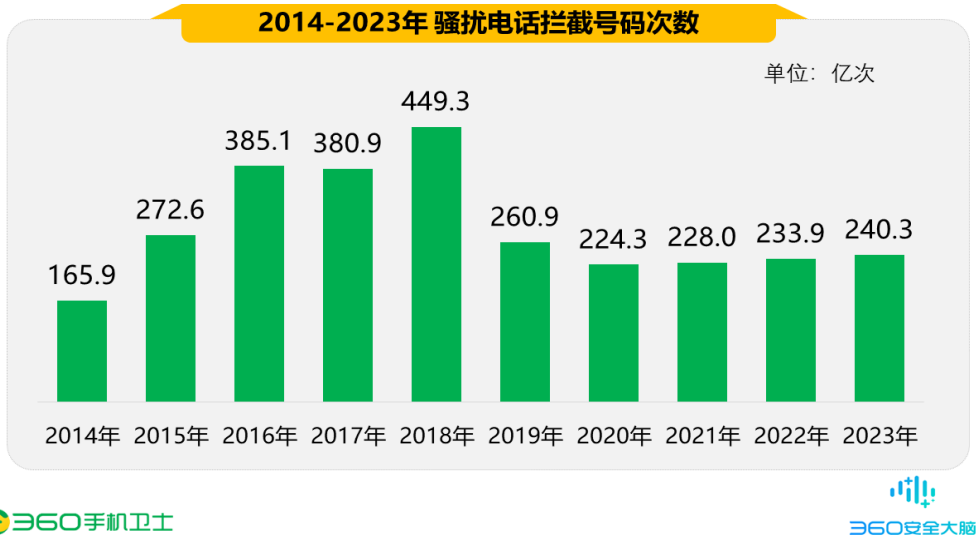

图 41 2014-2023 年 骚扰电话拦截号码次数

下图为 2023 年骚扰电话各月拦截号码次数分布：

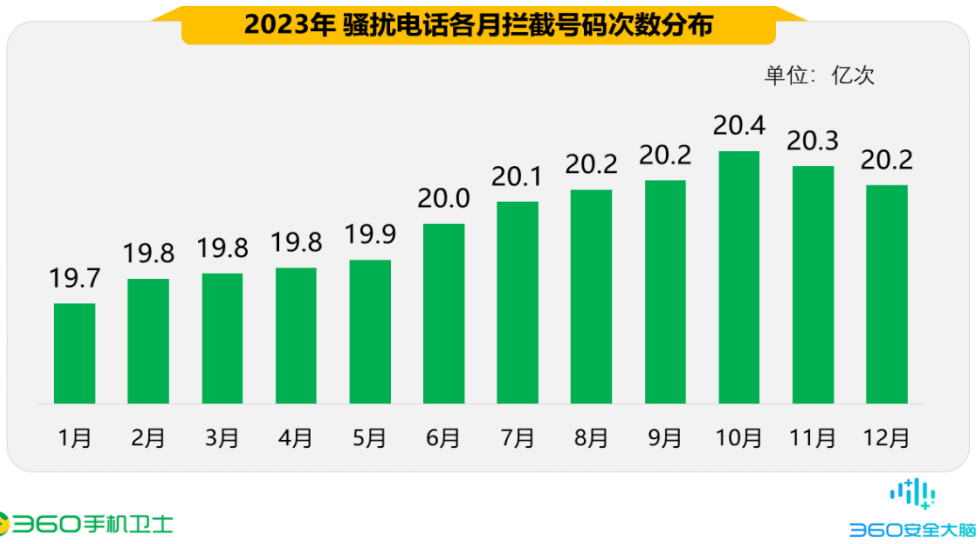

图 42 2023 年 骚扰电话各月拦截号码次数分布

根据各月骚扰电话呼入占比分析，临近过年骚扰电话拦截量呈降低趋势，2023 年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。春节结束后，从 3 月份起，骚扰电话拦截量逐步回升，持续增加到 10 月后，有所回落。下图为 2023 年识别与拦截骚扰电话趋势统计：

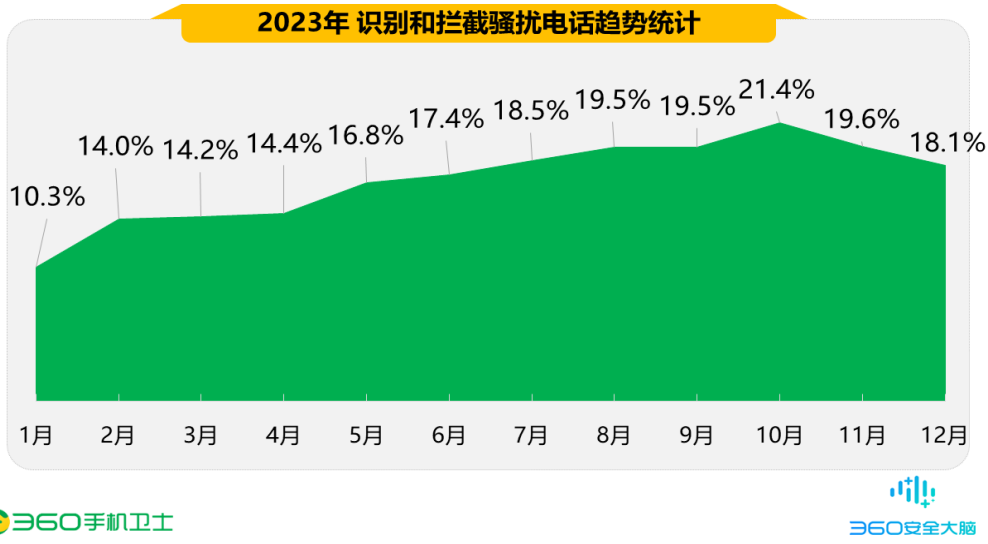

图 43 2023 年 识别和拦截骚扰电话趋势统计

2. 骚扰电话拦截类型分布

2023 年全年，综合 360 安全大脑的拦截监测情况及用户调研分析，从骚扰电话拦截类型来看，骚扰电话以 95.8%的比例高居首位；其次为广告推销（2.3%）、房产中介（1.1%）、保险理财（0.2%）、疑似欺诈（0.4%）、响一声（0.1%）与招聘猎头（0.1%）。下图为 2023 年

骚扰电话拦截类型分布：

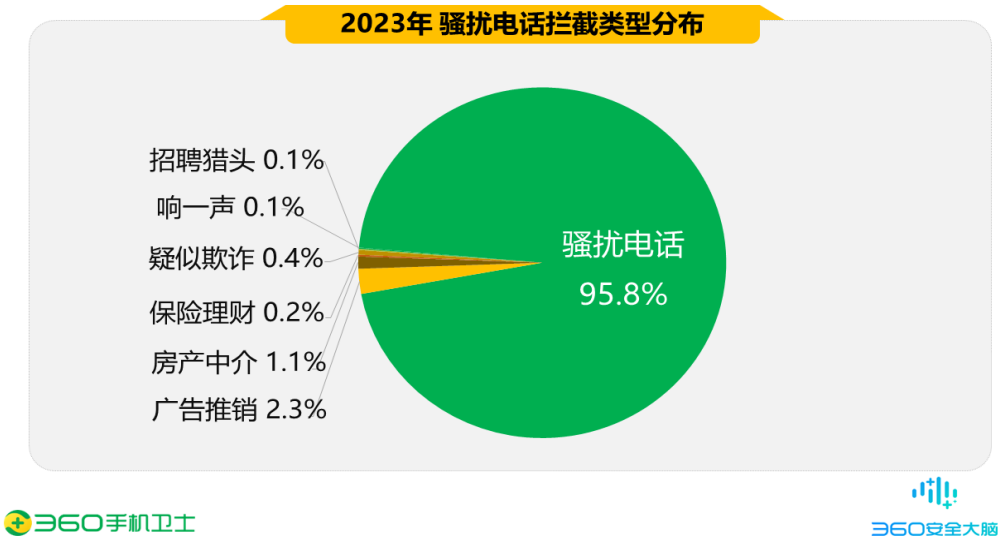

图 44 2023 年 骚扰电话拦截类型分布

3. 骚扰电话拦截号码号源分布

2023 年全年，从骚扰电话拦截号码个数分布来看，被拦截号码为固话最多，占比高达 33.8%；其次为虚拟运营商（25.3%）、运营商为中国联通的个人手机号（17.9%）、运营商为中国移动的个人手机号（13.7%）、运营商为中国电信的个人手机号（6.6%）、运营商为中国广电的个人手机号（2.1%）与 95/96 开头号段（0.5%）等。观察过往骚扰电话以及诈骗电话数据，结合 2023 年的新闻报道，“192”号段也被恶意利用，成为部分骚扰电话乃至诈骗电话的新选择。对于新运营商，我们应该给予运营商更多时间去打击号码滥用行为。为了应对不法分子使用 192 号段实施诈骗，广电已成立全国范围内的反诈工作专班，合力协同推进反诈工作。同时 360 作为安全厂商，也一直在履行其职责，持续利用自身的人工智能、多维模型等方式，建立更为准确的号码识别拦截规则，为移动互联网的健康有序发展提供强有力的技术支持。下图为 2023 年骚扰电话拦截号码号源分布：

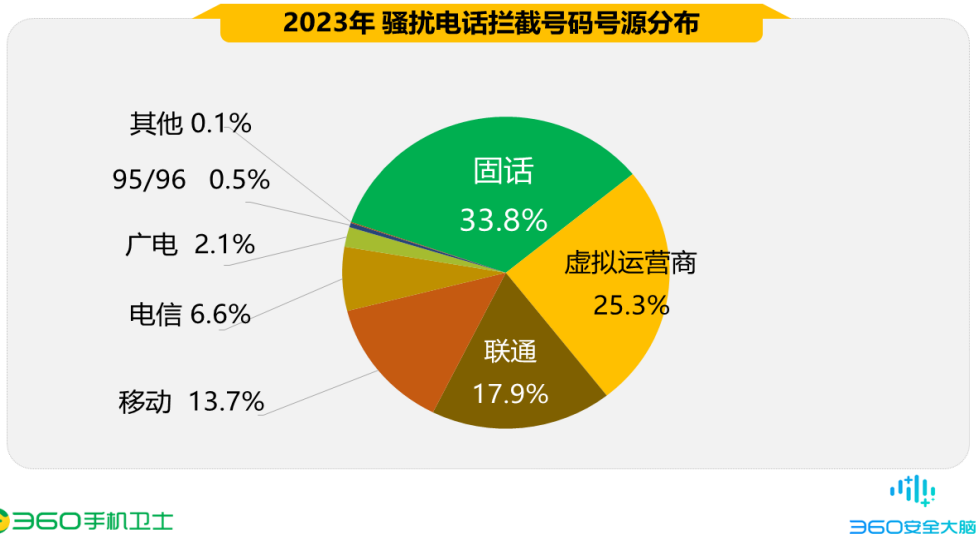

图 45 2023 年 骚扰电话拦截号码号源分布

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 96.5%；虚拟运营商也是骚扰电话类占据首位，占比 95.3%。95/96 号段与虚拟运营商号码遭不法分子利用，仍是不法分子从事非法行径的主要“工具”之一。

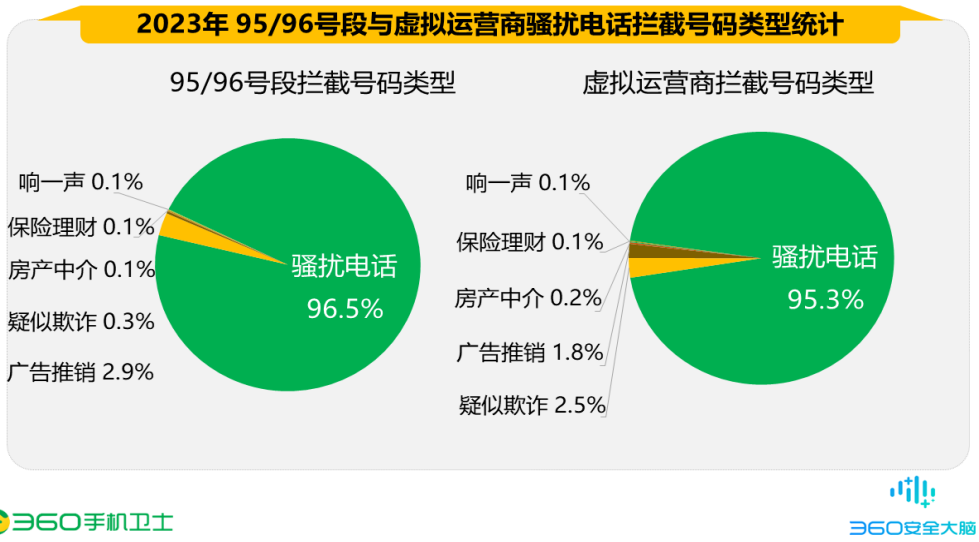

图 46 2023 年 95/96 号段与虚拟运营商骚扰电话拦截号码类型统计

4. 骚扰电话归属地分布

2023 年全年，从各地骚扰电话拦截量上分析，广东省用户标记骚扰电话拦截量最多，占全国骚扰电话拦截量的 13.2%；其次是江苏（7.9%）、山东（7.6%）、浙江（5.7%）、四川（5.1%），此外河南、北京、河北、上海、湖北的骚扰电话拦截量也排在前列。

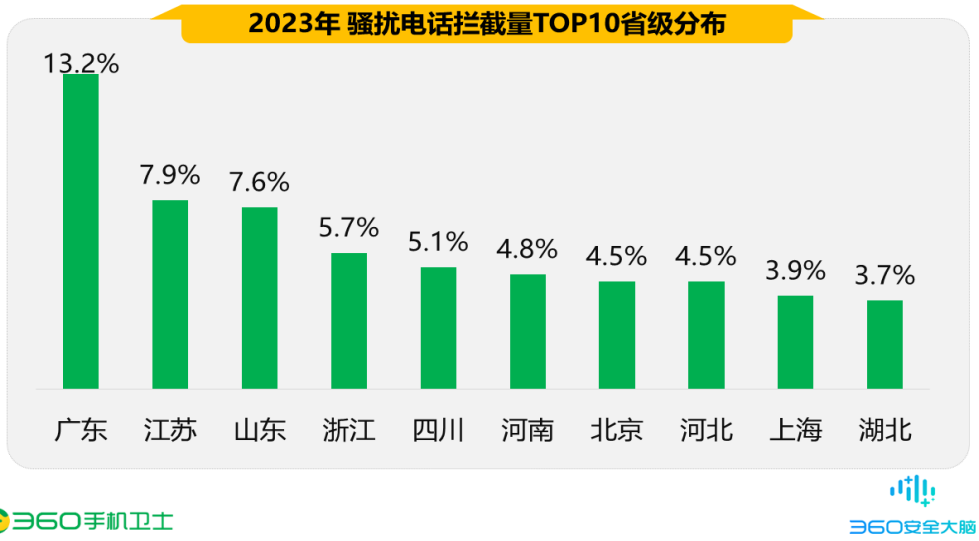

图 47 2023 年 骚扰电话拦截量 TOP10 省级分布

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 4.9%；其次是上海（4.3%）、广州（3.3%）、成都（2.7%）、深圳（2.5%），此外重庆、西安、苏州、杭州、东莞的骚扰电话拦截量也排在前列。

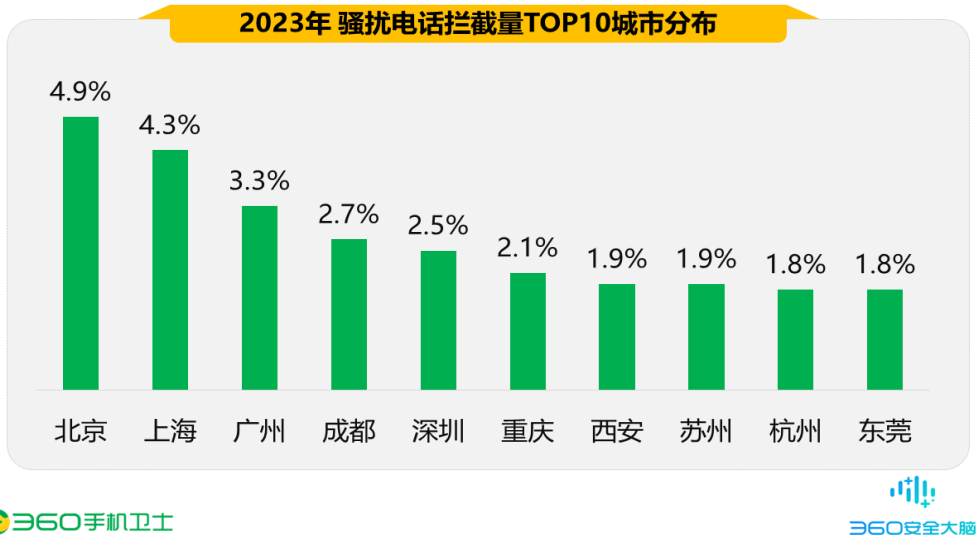

图 48 2023 年 骚扰电话拦截量 TOP10 城市分布

六、垃圾短信

1. 垃圾短信拦截量

2023 年全年，在 360 安全大脑的支撑下，360 手机卫士共为全国用户拦截各类垃圾短信约 104.1 亿条，同比 2022 年（91.6 亿条）上升了 13.6%，平均每日拦截垃圾短信约 2852.9 万条。下图为垃圾短信拦截量趋势分布：

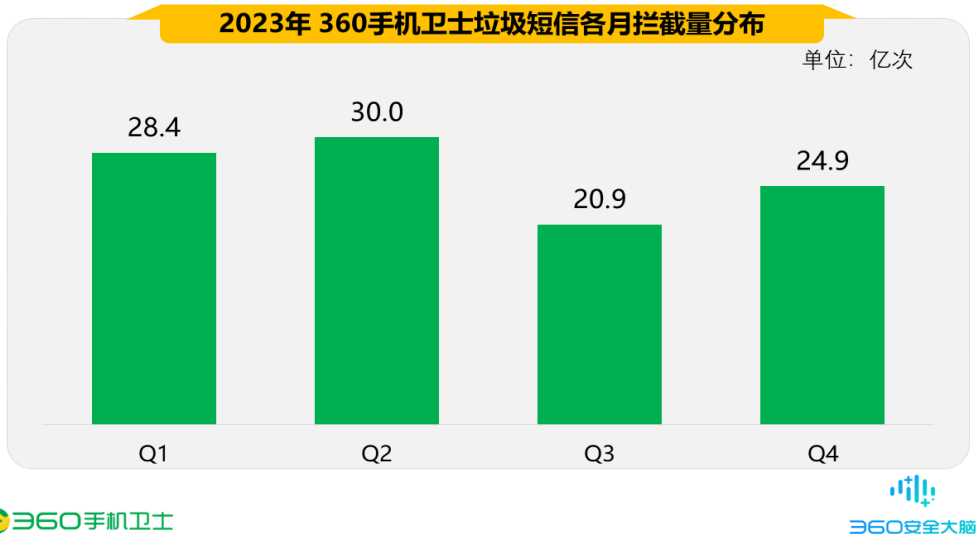

图 49 2023 年 360 手机卫士垃圾短信各月拦截量分布

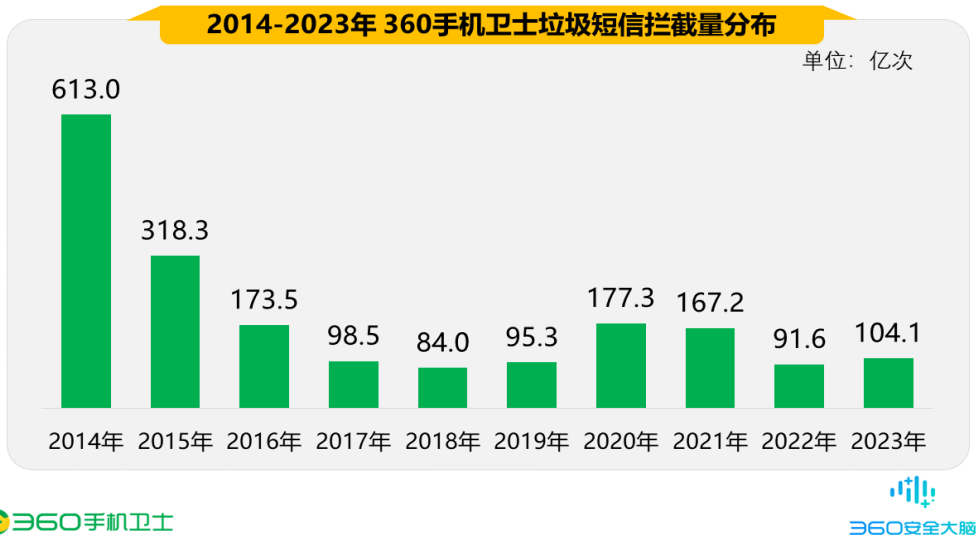

图 50 2014-2023 年 360 手机卫士垃圾短信拦截量分布

2. 垃圾短信类型分析

2023 年全年，垃圾短信的类型分布中广告推销短信最多，占比为 97.2%；诈骗短信占比 2.6%；违法短信占比 0.2%。

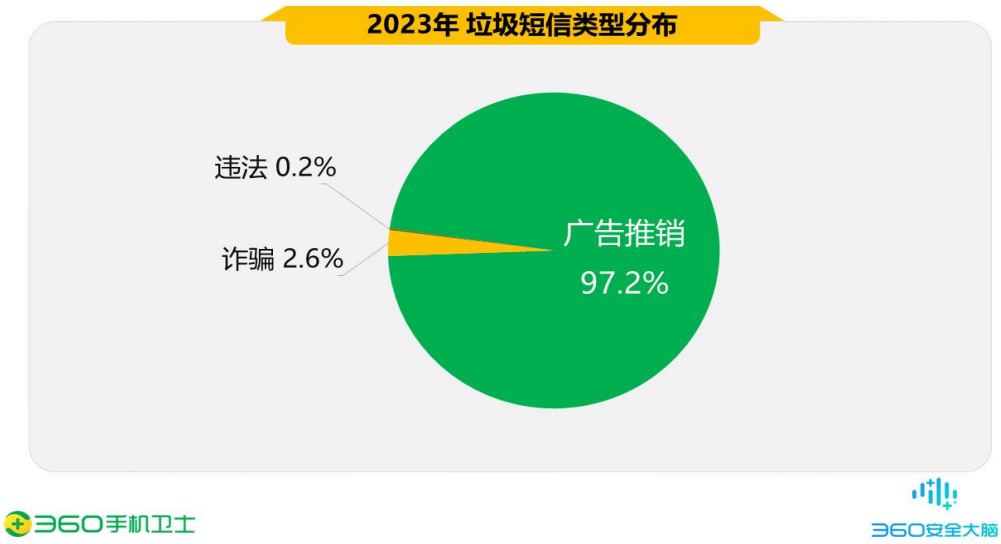

图 51 2023 年 垃圾短信类型分布

从诈骗短信拦截类型来看，诈骗短信以 55.3%的比例位居首位；其次为疑似伪装诈骗（29.6%）、赌博诈骗（10.5%）、兼职诈骗（3.1%）、股票诈骗（1.1%）等。如今越来越多的诈骗短信中仅有单一网址，此类短信内容晦涩难懂，同时域名使用防拦截策略，识别难度大，360 安全大脑一直致力于完善拦截规则，增加黑样本库，优化本地算法模型，提升实时研判垃圾短信新增与变种的能力，提升短信识别拦截能力。下图为 2023 年诈骗短信子类型分布：

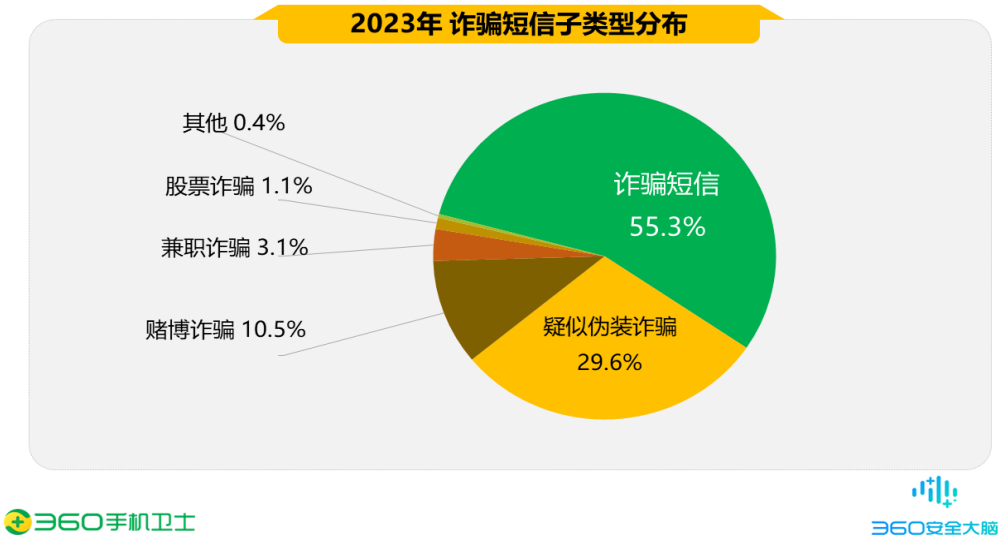

图 52 2023 年 诈骗短信子类型分布

从违法短信拦截类型来看，违法金融信贷短信以 92.6%的比例位居首位；其次为其他违法短信（3.2%）、售卖信息（3.0%）、色情短信（0.9%）与疑似伪基站发送（0.3%）。下图为 2023 年违法短信子类型分布：

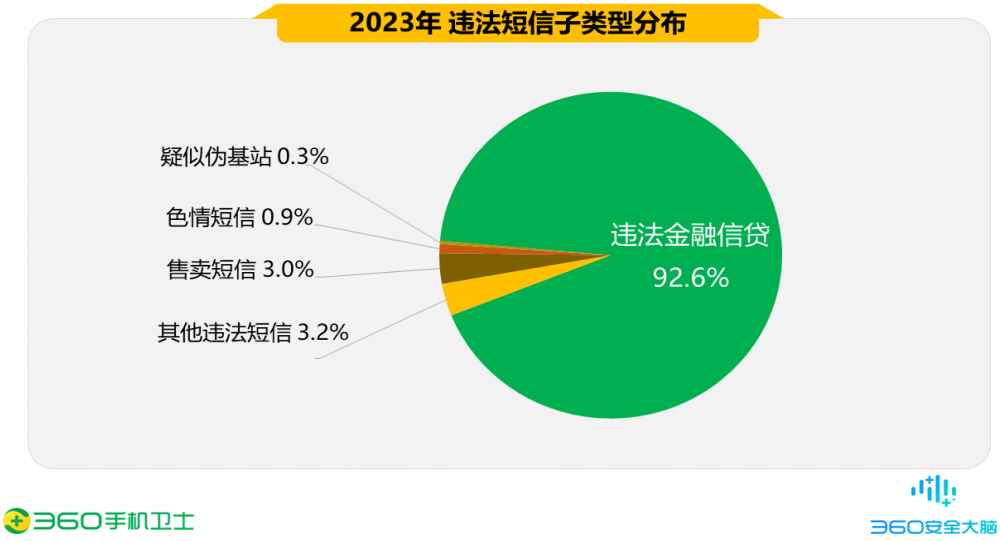

图 53 2023 年 违法短信子类型分布

3. 垃圾短信发送者运营商号源分布

2023 年全年，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 95.2%；利用其他号段传播垃圾短信占比约 4.8%。下图为 2023 年短信平台发送垃圾短信占比分布：

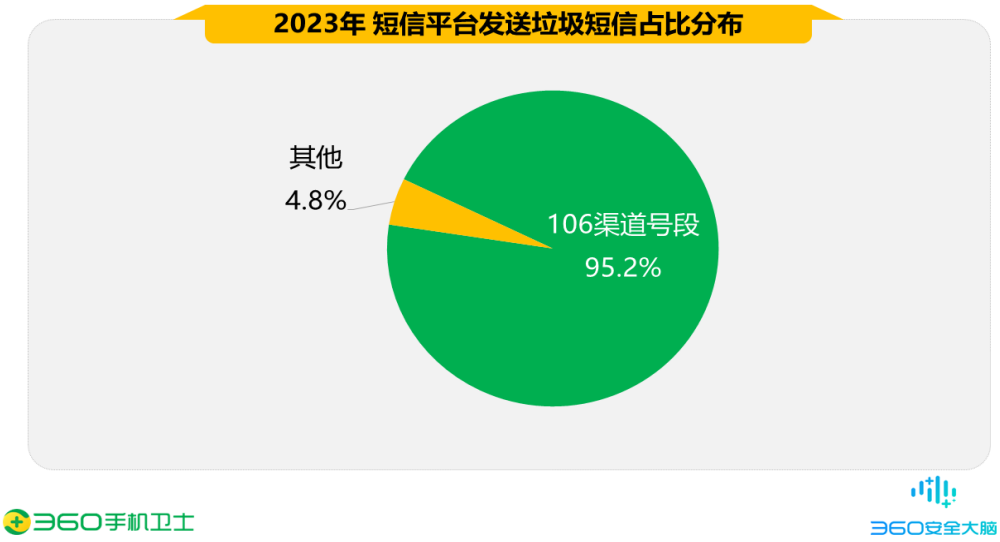

图 54 2023 年 短信平台发送垃圾短信占比分布

2023 年全年，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 41.4%；其次是 95/96 号段（15.7%）、固话（14.7%）、运营商为中国移动的个人手机号（9.4%）、运营商为中国联通的个人手机号（5.7%）、运营商为中国电信的个人手机号（4.5%）与 14 物联网卡（1.5%）等。

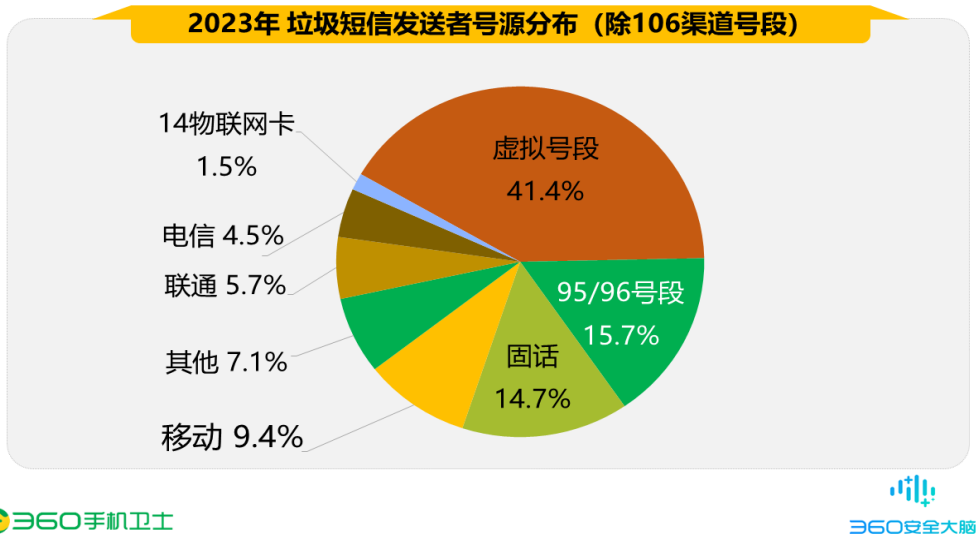

图 55 2023 年 垃圾短信发送者号源分布（除 106 渠道号段）

4. 垃圾短信拦截量地域分析

2023 年全年，从各地垃圾短信的拦截量上分析，广东省用户收到的垃圾短信最多，占全国垃圾短信拦截量的 15.8%；其次是北京（11.2%）、上海（11.2%）、山西（10.8%）、江苏（6.1%），此外河南、浙江、山东、四川、河北的垃圾短信拦截量也排在前列。

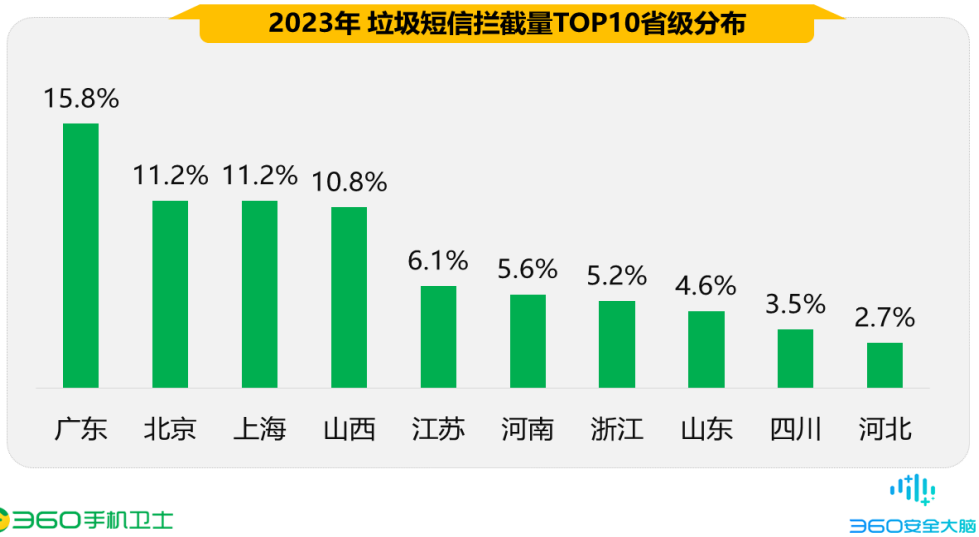

图 56 2023 年 垃圾短信拦截量 TOP10 省级分布

从城市分布来看，北京和上海用户收到的垃圾短信最多，分别占全国垃圾短信拦截量的 13.7%；其次是广州（8.4%）、郑州（4.0%）、深圳（3.9%），此外南京、成都、重庆、杭州、西安的垃圾短信拦截量也排在前列。

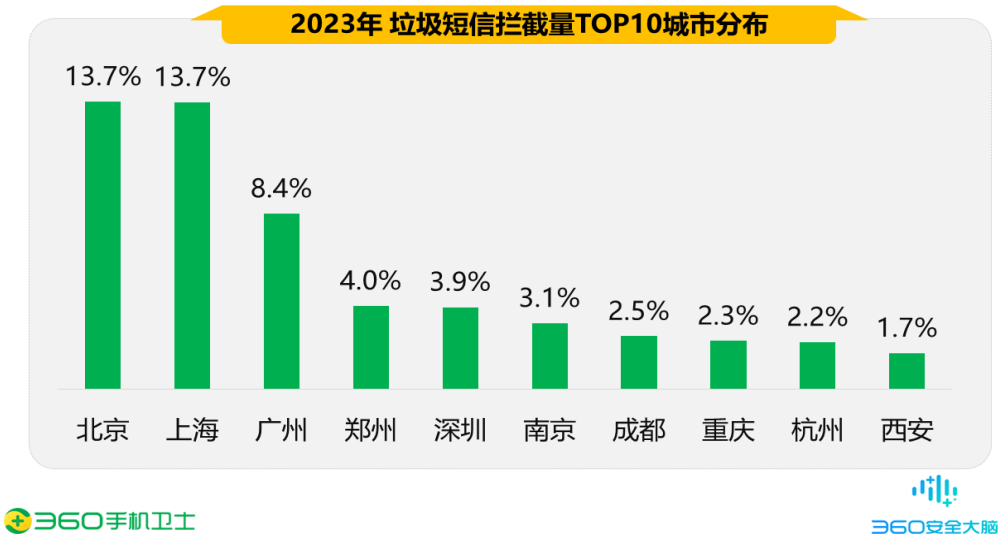

图 57 2023 年 垃圾短信拦截量 TOP10 城市分布