电信网络诈骗治理研究报告

(2019上半年)

Tencent 腾讯

指导单位:国务院打击治理电信网络新型违法犯罪工作部际联席会议办公室

指导出品:最高人民检察院第一检察厅、新闻办公室 公安部新闻宣传局、刑事侦查局

出品:守护者计划 微反诈行动 腾讯110


Tencent 腾讯

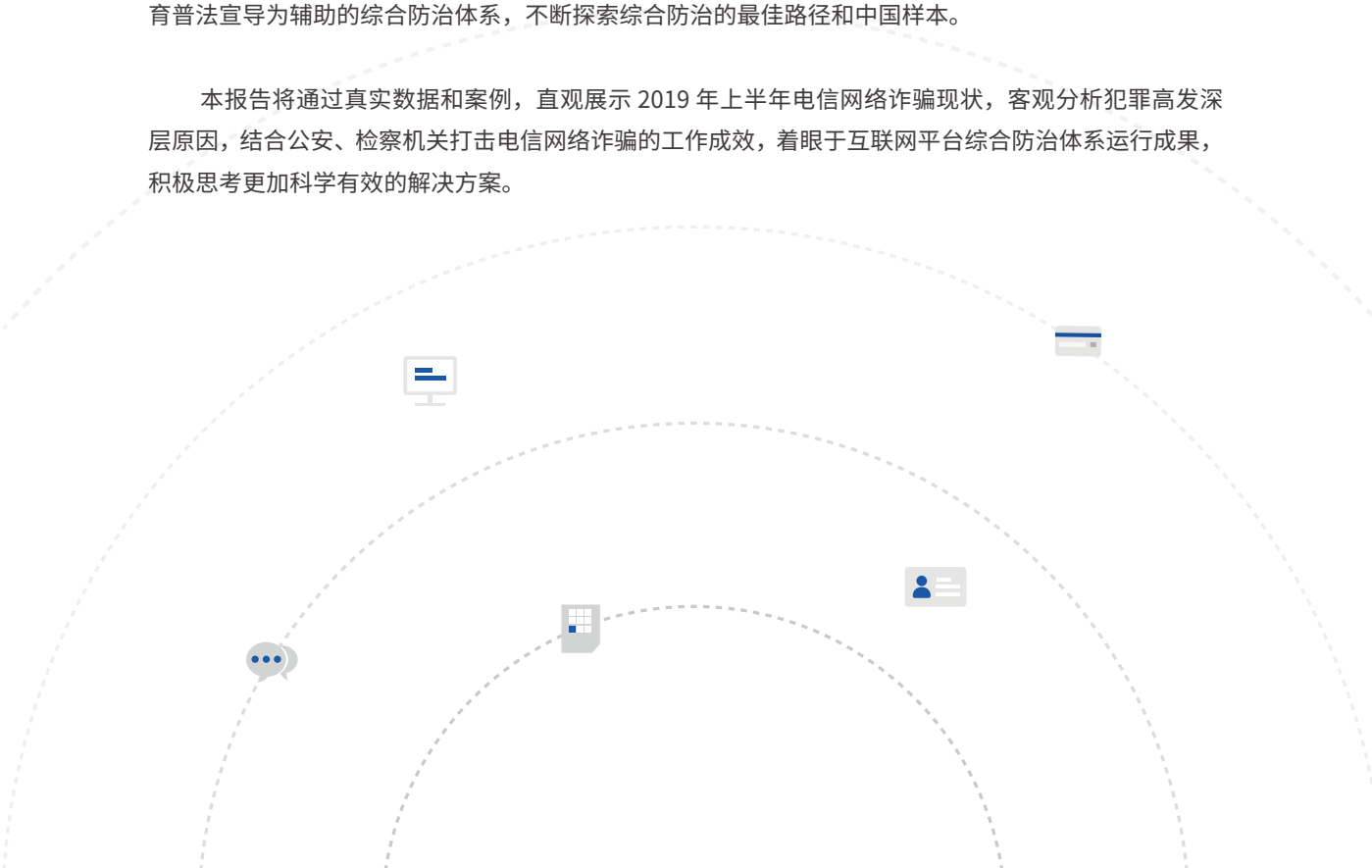
前言
PREFACE

近年来，随着移动互联网的快速发展和智能手机的高度普及，人们的工作、生活及社交方式都发生了巨大的变化。然而互联网给公众带来便捷的同时，也开始被不法分子利用。他们利用通信技术和移动支付，在低成本、高效益的巨大诱惑下，不断翻新手法、迭代技术、细化分工，更加隐蔽化和智能化地实施诈骗犯罪。近年来，电信网络诈骗犯罪屡打不尽，犯罪数量依旧处于高位，严重影响公众的财产安全和互联网生态的清朗环境，甚至破坏社会秩序的和谐与稳定，危害性极大。

面对总体高发的诈骗态势，公安、检察机关始终以维护人民群众的财产安全为己任，协同配合，不断更新理念、创新打法，严厉打击和整治电信网络诈骗犯罪活动，坚决遏制电信网络诈骗的高发蔓延势头，取得良好的效果。

同时，以腾讯公司为代表的互联网运营者，始终致力于以实际行动保护网络生态安全、维护网络环境清朗，依法履行平台义务，主动承担社会责任，多措并举参与网络空间治理，充分发挥资源优势，构建起以信息技术和用户举报数据为基础，优化产品安全策略为主导，警企合作打击犯罪为保障，安全教育普法宣导为辅助的综合防治体系，不断探索综合防治的最佳路径和中国样本。

本报告将通过真实数据和案例，直观展示 2019 年上半年电信网络诈骗现状，客观分析犯罪高发深层原因，结合公安、检察机关打击电信网络诈骗的工作成效，着眼于互联网平台综合防治体系运行成果，积极思考更加科学有效的解决方案。



目录

CONTENTS

第三章 腾讯针对电信网络诈骗的防护及治理体系

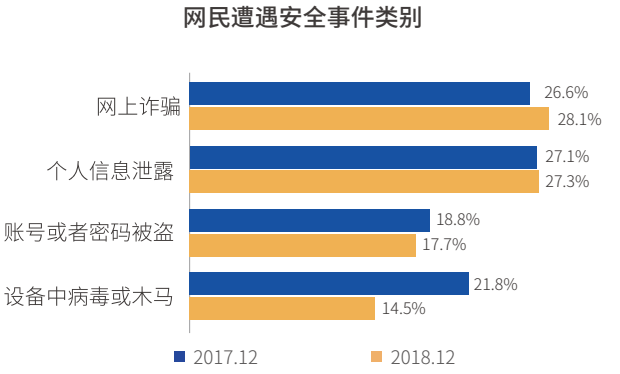
第四章 提升电信网络诈骗综合防治实效的建议

第一章

2019 年上半年电信网络诈骗现状分析

第一章 2019 年上半年电信网络诈骗现状分析

近年来，随着通讯和网络的发展、普及，电信网络诈骗日益成为威胁公众财产安全和社会稳定的一大公害。中国互联网络信息中心（CNNIC）发布的第 43 次《中国互联网络发展状况统计报告》显示，网上诈骗及其黑产链条中密切相关的个人信息泄露、账号密码被盗等，是近两年公众在上网过程中最常遭遇的安全事件。随着刑事打击和普法宣传力度的不断加大，电信网络诈骗犯罪得到了一定程度上的遏制，但总体而言，仍是威胁公众上网安全的首要问题，形势严峻。

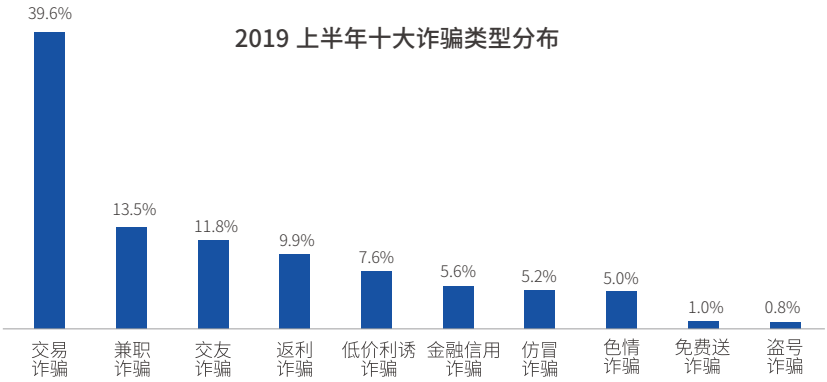


（数据来源：CNNIC 中国互联网络发展状况统计调查）

一、电信网络诈骗总体概况

通过对 2019 年上半年各种电信网络诈骗手法的举报情况进行盘点归总，聚类分析，归纳为交易诈骗、兼职诈骗、交友诈骗等十大诈骗类型。

其中，交易诈骗、兼职诈骗、交友诈骗、返利诈骗合计占比超 70%，免费送诈骗、盗号诈骗少量存在，其余诈骗类型比例相当，诈骗场景总体呈现多样化。



（数据来源：腾讯 110）

附：十大诈骗类型介绍

交易诈骗

在商品交易过程中或以提供非法业务为由，通过不发货、不付款或诱导扫描付款码、点击钓鱼链接等方式，实施诈骗。

兼职诈骗

在网络平台发布虚假兼职信息，以高佣金为噱头招聘网络兼职，通过诱骗入职费、刷单本金、代理费等实施诈骗。

交友诈骗

以交友为幌子骗取信任，随后以各种借口索取钱财、推荐虚假理财产品、诱导至赌博平台等方式实施诈骗。

返利诈骗

以回馈粉丝、商家活动等名义，谎称支付指定金额后可获高倍金额返还，或购物后可获高价值赠品，引诱支付金钱或购买商品，实施诈骗。

低价利诱诈骗

以超低价购买商品为噱头，诱骗被害人付款实施诈骗。

金融信用诈骗

以办理金融服务（贷款、信用卡、投资理财、荐股等）的名义，骗取服务费、会员费、本金等，实施诈骗。

仿冒诈骗

在社交工具上冒充被害人的亲友、同事、上级或公职人员、客服代表等身份，实施诈骗。

色情诈骗

以提供色情服务为由，收取会员费、服务费等，实施诈骗。

免费送诈骗

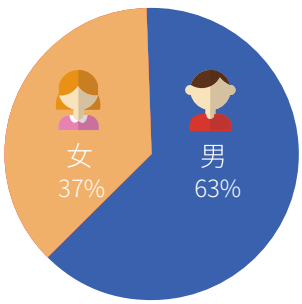
以免费赠送礼品的幌子，诱导被害人转发活动信息、填写个人信息，骗取邮费、公民信息，实施诈骗。

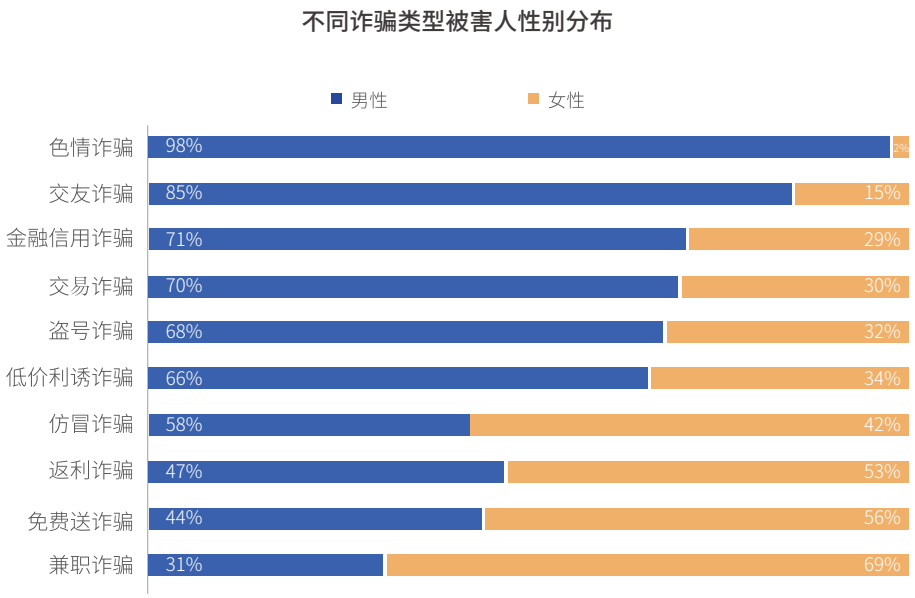
盗号诈骗

盗取他人账号，以被盗账号本人的身份，通过向账号好友借钱或请求帮充值话费等方式，实施诈骗。

电信网络诈骗被害人性别比例

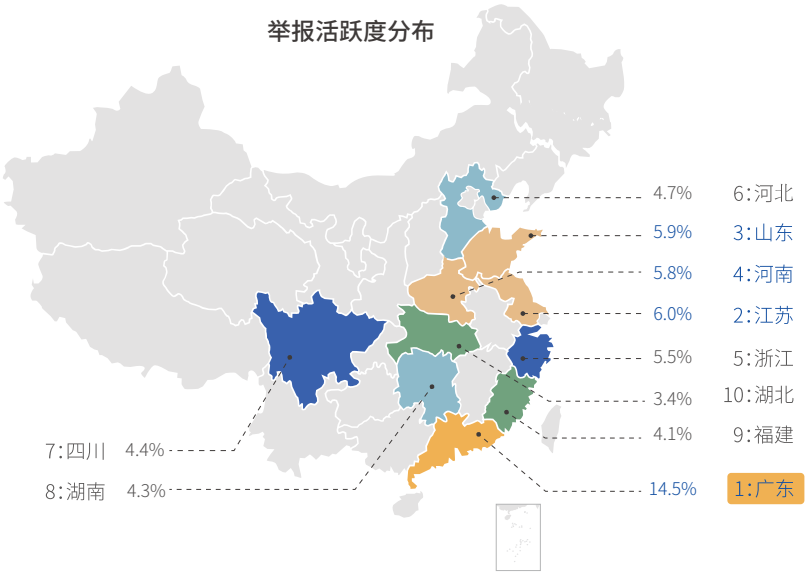
（数据来源：腾讯 110）





（数据来源：腾讯 110）

被害人性别分布上，男女比例分别为 63%、37%，男性被害人数量是女性的近两倍。在十大诈骗类型中，除返利诈骗、兼职诈骗和免费送诈骗外，其余色情诈骗、交友诈骗、金融信用诈骗、交易诈骗、盗号诈骗、低价利诱诈骗、仿冒诈骗等诈骗类型中男性被害人均占比过半。



（数据来源：腾讯 110）

随着公众防骗意识的提升，越来越多具有正义感的用户参与到举报行列中。地域分布方面，主要集中在华南、华中、华东等经济较为发达的地区，广东省位居榜首。

二、电信网络诈骗的七大特征

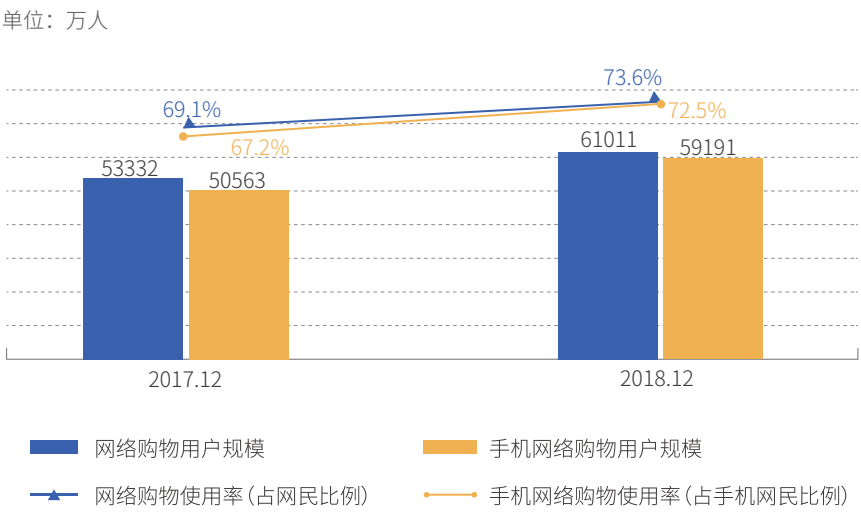
与以往“简单结伙”“单兵作战”不同，近年来电信网络诈骗运作模式日趋专业化、公司化，犯罪手段日趋智能化，活动地域呈现跨境化，并逐渐形成恶意注册、引流、诈骗、洗钱等上下游环节勾连配合的完整链条，各环节精细分工、专业运作、技术应用迭代升级，形成电信网络诈骗“新范式”。

进入 2019 年，电信网络诈骗无论是在高发类型、目标人群还是诈骗套路方面都在不断发生新变化，呈现新趋势，并衍生出多种新类型新手法。这些新型电信网络诈骗，手段更加隐蔽，利益关联更加复杂，给电信网络诈骗的防范和治理带来了新的挑战。具体可总结为以下七大特征：

（一）交易型诈骗最为高发，纯获利类诈骗日渐淡出

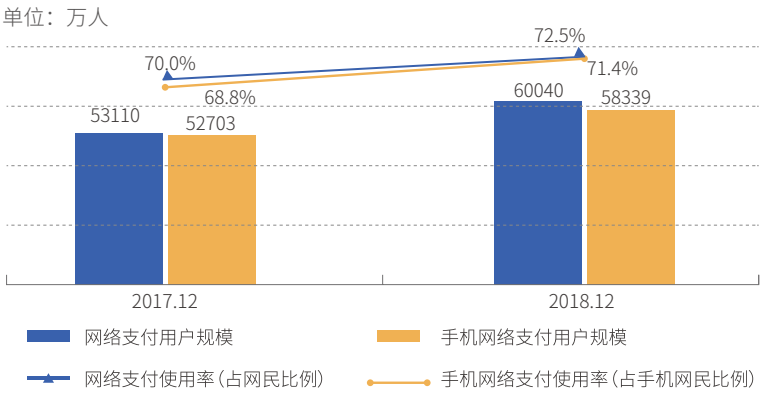
由于网络购物和网络支付的普及，交易诈骗占比遥遥领先，是最为高发的诈骗类型。

2017.12-2018.12 网络购物 / 手机网络购物用户规模及使用率



（数据来源：CNNIC 中国互联网络发展状况统计调查）

2017.12-2018.12 网络支付 / 手机网络支付用户规模及使用率



（数据来源：CNNIC 中国互联网络发展状况统计调查）

据统计，截至 2018 年底，我国网络购物用户规模达 6.1 亿，占网民总数的 73.6%。随着电商行业的兴起，网络购物和服务已成为一种生活方式，诈骗行为人针对不同类型的网络购物人群和场景，衍生出更加多变的话术和手法，以致交易诈骗所占比例居高不下、连年攀升。

同时，在网络购物、支付时，消费者日趋理性，面对 “免费送”这种“天上掉馅饼”的诈骗伎俩，警惕性明显提高，纯获利类诈骗随之大幅减少，并有淡出之势，这与长期不懈的宣传教育和针对性的专项治理密不可分。

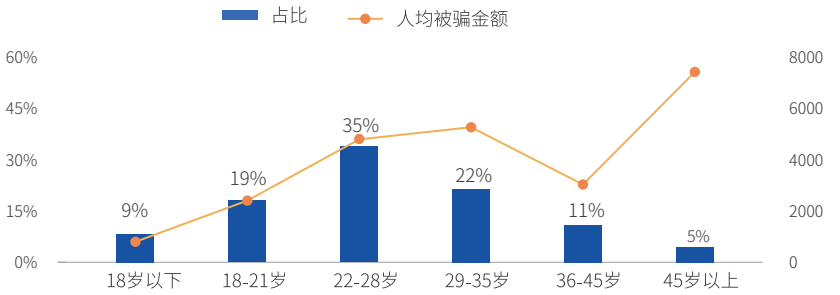
案例直击：网络购物动歪念，窥探隐私反中连环套

诈骗行为人张某等人在电商平台以提供查询公民隐私信息、手机定位等服务为由，吸引被害人的注意，并以内容敏感，不能在电商平台直接交易为借口，诱骗被害人添加指定联系方式后实施诈骗。在被害人进行联系后，诈骗行为人首先要求被害人支付 50 元定金。然后根据被害人提供的个人资料，伪造制作成带有真实证件照的查询结果图片，以骗取被害人的信任。随后要求被害人继续付款，以获取完整信息。待被害人付款后，诈骗行为人会发送一个加密文档，进一步要求被害人支付保密费。腾讯安全团队在接到举报后进行分析和整理，将线索和证据同步提交广东公安机关，协助警方破获该案，总计抓获 33 名犯罪嫌疑人。经查，该案受害者达到上千人，诈骗金额高逾百万。

（案例来源：腾讯“守护者计划”安全团队、腾讯 110）

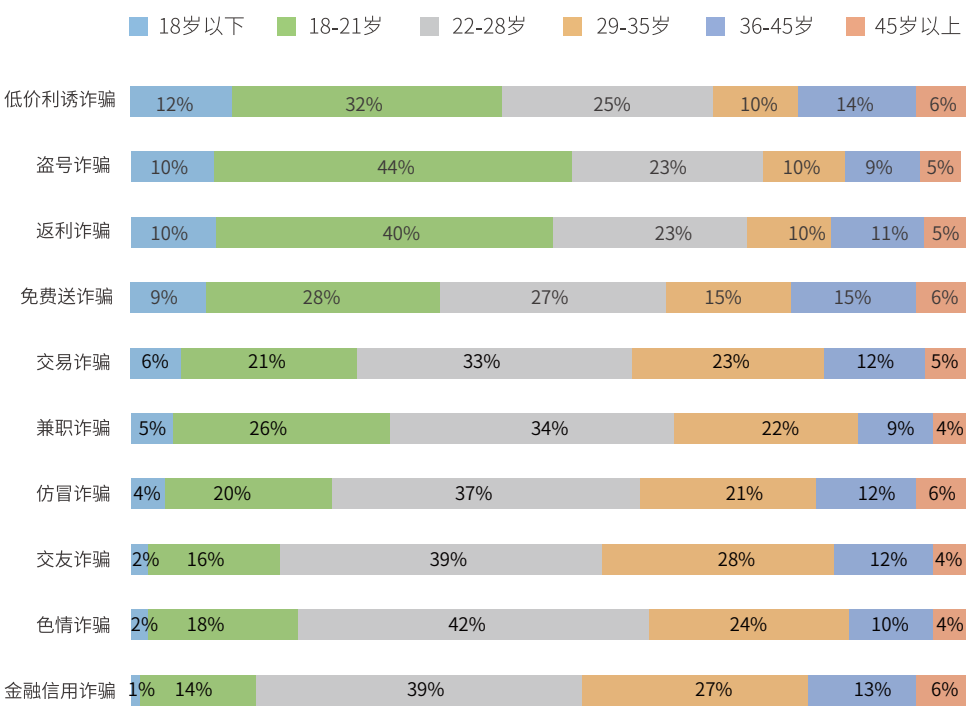
（二）90 后被骗概率高，中老年人被骗金额高

2019 年 1-6 月 被害人年龄分布及人均被骗金额分布



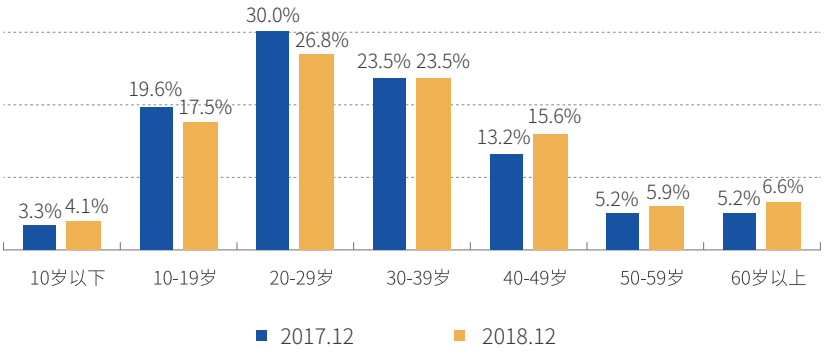
（数据来源：腾讯 110）

不同诈骗类型被害人年龄段分布



（数据来源：腾讯 110）

网民年龄结构分布

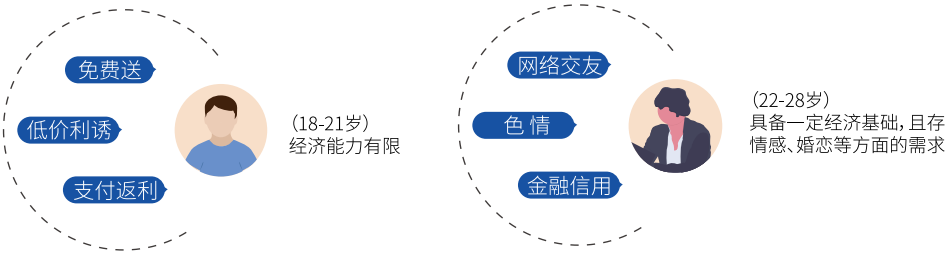


（数据来源：CNNIC 中国互联网络发展状况统计调查）

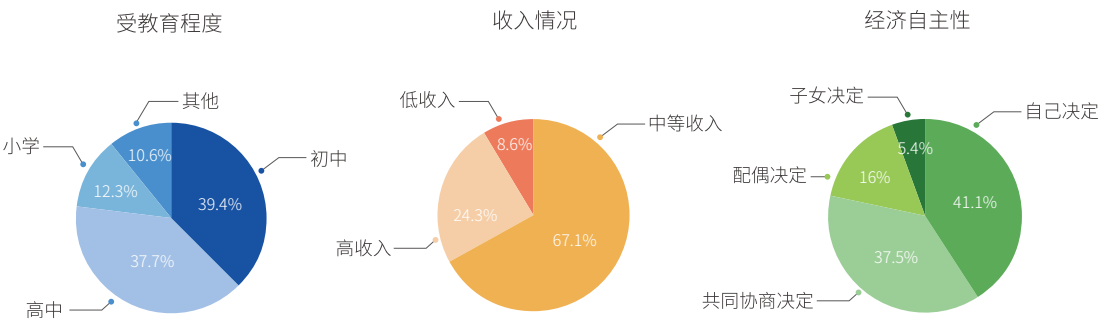
根据数据显示，18-28 岁之间的被害人所占比例高达 54%。90 后是网络用户的主力军，同时也因社会经历有限，对电信网络诈骗防范意识不足，而成为被骗概率最高的群体。

正在读书或是刚步入社会的年轻人（18-21 岁）因经济能力有限，成为支付返利、免费送、低价利诱、招聘兼职等骗术的主要实施对象；而有一定工作经验的年轻人（22-28 岁），一方面已具备一定的经济基础，另一方面存在情感、婚恋等方面的客观需求，故在色情、网络交友、金融信用方面遭遇诈骗比例较高。

90 后被害人占比例高达 54%



受骗中老年人总体情况



（数据来源：中国社会科学院 & 腾讯：《2018 中老年互联网生活研究报告》）

45 岁以上被害人的人均受骗金额约为 7000 元，远远超过其他年龄段人群。相关报告显示，中等收入、经济自主的中老年人受骗比例更高。随着年龄的不断增长，中老年人面临健康问题增加、收入来源逐渐减少等现状，养生保健和拓展收入渠道需求明显，加之触网时间相对较短、相关专业知识不足等原因，在遭遇关于金融投资、养生保健、网络技术等方面的诈骗时容易被诈骗分子利用和控制，投入大笔资金，劝导难度也较大。

心理专家 *

虽然阅历丰富，但随着年龄增大，老年人的认知活动能力不断衰退，部分老人会变得固执刻板，根据过去的经验来做出判断。一些老年人对新技术和新事物缺乏了解和理解，容易导致他们慌乱和缺乏安全感，这就给骗子创造了可乘之机。

需要注意的是，随着网民触网的日益低龄化，未成年人受骗现象也不容忽视，需要引起更多关注和保护。未成年人遭遇诈骗集中在低价利诱诈骗、盗号诈骗、返利诈骗和免费送诈骗。在某返利诈骗案件中，未成年人被教唆使用家长手机进行支付，损失高达数万元。

未成年人身心尚处于发育和发展阶段，相较于成人，缺乏经验且认知能力不足，容易受暗示，也是骗子感兴趣的群体。

* 本报告心理学专业支持：林春，中国科学院心理研究所教授；郑元洲，国家二级心理咨询师。

案例直击：洗脑套路多，我成为了你最信任的人

诈骗行为人冒充国家工作人员，以编造故事、制造焦虑、伪造资料等连环套路，对退休职工李某进行洗脑，让她坚信自己是有罪之人，而后给予机会“戴罪立功”。在诈骗行为人的诱骗下，李某分多次向对方进行转账，前后共计数百万元，在警方上门劝阻时，依然执迷不悟，甚至让自己的儿子手持铁棍对抗警方。最后，直到诈骗团伙主动切断与李某网络联系，钱款无法追回，她才相信自己被骗。

（案件来源：腾讯“守护者计划”安全团队）

（三）广撒网骗财骗信息，全面榨取被害人价值

现阶段，“随机诈骗”与“精准诈骗”相互交织，成为电信网络诈骗手法的新趋势。公民个人信息的获取，是“精准诈骗”得以实施的重要前提。诈骗行为人为拓宽公民信息获取的渠道， 在广撒网式发布诈骗信息骗取被害人金钱的同时，往往还设法获得大量公民个人的信息，为再次实施精准诈骗提供“弹药”，进一步榨取被害人的价值。

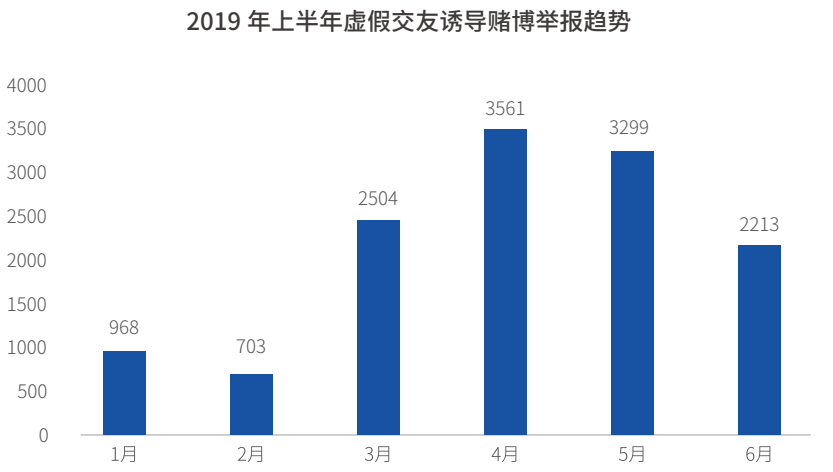
诈骗行为人常以用户注册、商品邮寄及提供服务需要等为借口，要求被害人填写姓名、身份证号、手机号码、家庭地址、账号密码、银行卡号等个人信息，被害人往往防不胜防，甚至被骗后仍对其隐私信息的泄露毫无感知。

案例直击：不止骗你 9.9 元，个人信息更值钱

近期有诈骗行为人蹭水果价格上涨的热度，发布虚假广告称参加活动付 9.9 的邮费再转发该推广消息，即可以试吃水果礼盒，待用户付款并转发信息之后便将用户拉黑，上当人数众多。此外，诈骗行为人以邮寄水果为由向用户索取电话、住址等信息，在骗取用户金钱的同时，也收集到大量公民个人信息。

（案例来源：腾讯 110）

（四）交友骗入“杀猪盘”，多种黑产相互勾连



（数据来源：腾讯 110）

近期，电信网络诈骗开始与赌博黑产相互勾连。在交友诈骗中，诈骗行为人以投资名义拉拢被害人参与赌博，或在博彩网站充值，在“情感攻势”“高利诱惑”和“赌徒心理”三重因素的影响下，被害人往往不能理性判断，越陷越深，不断投入大额资金。

以上就是所谓“杀猪盘”，一种新近兴起的东南亚博彩骗局。诈骗行为人以交友为名义博得被害人的好感和信任后，以各种方式诱骗被害人进入赌博平台或虚假的投资平台投入资金，骗取钱财。在“杀猪盘”中，诈骗行为人将那些急于寻找感情和婚姻的人叫做“猪”，把建立恋爱关系叫做“养猪”，把最后的诈骗叫做“杀猪”。据举报数据显示，近期被骗金额巨大的交友诈骗案件，多是采用该种手法。有用户遭遇“杀猪盘”，被骗金额高达 600 万元。

2019 年 1 至 4 月，虚假交友诱导赌博的月均举报数量总体急剧上升，后经平台专项治理和宣传曝光，该类诈骗增长势头有所遏制，数据开始回落。

觅猪：

在各大婚恋网站或是交友网站伪装成高富帅、白富美等成功人士，寻觅符合诈骗的目标，在找到目标后以交友软件不常用为由，引导添加社交账号。

养猪：

诈骗行为人在网络中将自己包装为完美成功人士形象，并给予被害人无微不至的关心及对未来的畅想，被害人一步一步陷入骗子的陷阱中，最终骗子获取到被害人的信任并掌握财务状况，为下一步的“杀猪”计划展开布局。

杀猪：

在建立感情和获取信任后，诈骗行为人会透露自己有投资副业或发现平台漏洞等，表明可以带领被害人一起赚钱，共同富裕。在多次小额盈利后被害人也逐渐放下戒心，此时对方会引诱被害人去借钱、贷款加大投入，当被害人竭尽所能，无法再投入资金后，诈骗行为人选择“杀猪”，关闭平台。

案例直击：这场骗局，像极了爱情

王某通过婚恋平台认识了自称丁某的男士，并添加其社交账号，对方通过包装自己的社交形象，伪装成成功男士，并经常发送甜言蜜语俘获王某芳心。在确定男女朋友关系后，丁某便引诱王某去彩票平台帮忙充值刷流水，声称充值后随时可以提现。王某先后充值 2 万元后，发现所谓可以提现的网址无法打开，也无法联系到丁某时，才意识到被骗。

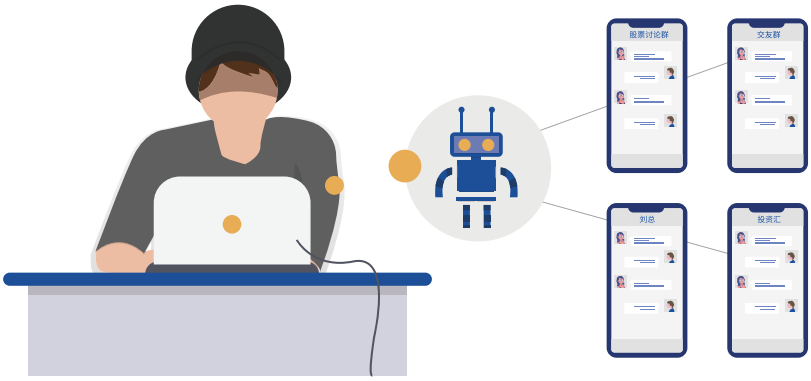
（案例来源：腾讯 110）

（五）群聊群控做迷局，新型技术成诈骗工具

科技是把双刃剑。如今人工智能（AI）开始用于智能搜索、自动驾驶、疾病诊断等领域，同时因其相比人力更加稳定、高效、成本低廉，也开始被诈骗行为人用作实施犯罪、破坏网络秩序的工具。

在电信网络诈骗上游犯罪中，黑产分子利用人工智能技术破坏网络平台安全策略，为非法获取公民个人信息和批量注册黑产账号提供了便利，成为网络黑恶源头犯罪的重要技术支撑。

在电信网络诈骗实施过程中，人工智能被用于群聊群控场景，诈骗行为人制作聊天机器人程序，配合人工操作，将被害人引入迷局。

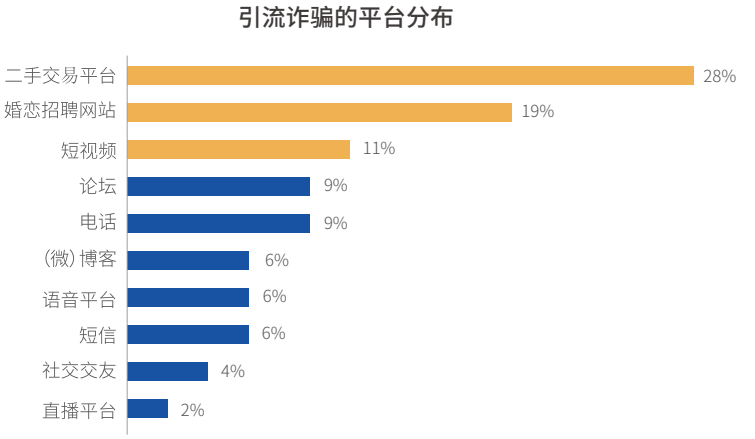


案例直击： 荐股大神套路深，机器人陪玩别当真

针对近期荐股诈骗的高发态势，腾讯安全团队配合各地警方开展专项打击。在这些案件中，诈骗行为人伪装成“荐股大师”，通过群控设备向目标人群发送推荐股票的消息。在将被害人诱骗入炒股群后，又通过群聊，诱使被害人缴纳高额会员费、购买软件，或进一步引入虚假交易平台。而这些精心设计的聊天群中，除了被害人本人，其余鼓掌、点赞，鼓吹荐股佳绩的成员实际上均为诈骗行为人以及经过“训练”的聊天机器人，以制造踊跃参与的假象，诱骗被害人投资。利用上述群控群聊设备，单个诈骗行为人可同时向多个被害人实施诈骗。

（案件来源：腾讯“守护者计划”安全团队、微信安全团队、腾讯 110）

（六）跨平台诈骗日益增加，多平台成引流入口



（数据来源：腾讯 110）

互联网的普及带动了各类平台的出现和发展。通过对社交场景下诈骗行为的分析，发现相当一部分诈骗行为源自多平台、跨平台的引流。诈骗行为人利用多平台运作场景丰富、触达面广、传播速度快的特点，精心设计场景，将被害人诱骗至其他平台进一步实施诈骗。根据统计，二手交易平台（28%）、婚恋招聘网站（19%）、短视频（11%）平台出现诈骗引流较为突出。

此外，部分电信网络诈骗虽然也通过社交平台进行沟通，但最终实施诈骗的场所却是将被害人引诱于社交平台之外，譬如钓鱼网站、赌博网站等，如前文所述东南亚“杀猪盘”，整个诈骗环节及场景更加立体化、生态化。

案例直击：二手交易平台里的虚假链接

诈骗行为人先冒充买家，在二手交易平台获取被害人的信息后，通过被害人社交账号添加好友，以拍下被害人出售的商品为名，向被害人发送虚假交易截图，声称无法支付或无法下单，并同时发送钓鱼网站链接让被害人联系客服。被害人点开链接后，会弹出一个客服聊天界面，诈骗行为人冒充二手交易平台的客服，以平台名义向被害人收取几百元至上千元不等的交易保证金，谎称保证金在交易结束后会自动退还，诱骗被害人支付。根据腾讯安全团队提供的线索，江西警方迅速开展调查和打击，已打掉多个涉案团伙，破获案件一百余起。

（案例来源：腾讯“守护者计划”安全团队、腾讯 110）

（七）转发分享需谨慎，裂变式传播害己害人

随着互联网的广泛覆盖，网络裂变传播逐渐成为一种重要的营销策略。诱导分享的方式，能以较小的成本，在短时间内使产品迅速得到曝光，实现潜在用户数量的快速增长。

这种营销方式也开始被诈骗行为人利用，通过“免费送”、低价利诱等手段，诱骗被害人转发分享带有诈骗链接或二维码的海报、宣传稿等内容，使大量用户在短时间内上当受骗。这种裂变式传播利用熟人关系的特性和从众心理，降低了被害人的警惕意识，无形中为诈骗行为作了掩护，得手率更高。而参与其中的用户，不但是电信网络诈骗的被害人，也间接帮助诈骗行为人“扩大战果”，影响十分恶劣。

为维护用户的合法权益和产品体验，2019 年 5 月 13 日，微信安全中心发布《关于利诱分享朋友圈打卡的处理公告》，该公告申明，根据《微信外部链接内容管理规范》，微信禁止通过利益诱惑，诱导用户分享、传播外链内容或者微信公众账号文章，对违规行为采取下调每日分享限额、限制功能、封停账号等多级措施。该项措施，极大地遏制和打击了利用诱导分享方式进行网络诈骗的行为。

案例直击：盲目转发，失财又失信的赔本生意

近期，腾讯安全团队配合警方破获一个以“免费送”为套路行骗的团伙。该团伙将成本不到两元的劣质手环，宣称为价值千元的运动手环，以某知名企业旗舰店开业酬宾的名义，在线上举办“包邮免费送”活动。参与者必须要转发指定的海报至全部好友才可领取，而最后收到的竟是需支付 29 元费用的“到付快递”。此活动以裂变的形式迅速传播，短时间内有大量用户受骗。

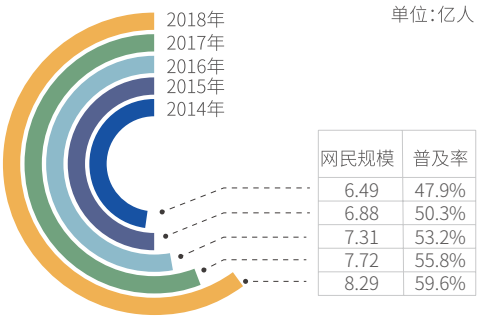
（案例来源：腾讯“守护者计划”安全团队、微信安全团队、腾讯 110）

三、电信网络诈骗高发的原因

一直以来，公安、检察机关对电信网络诈骗保持高压打击态势，各网络平台亦不断完善安全策略，取得了可喜的成果，电信网络诈骗蔓延之势有所遏制。但现阶段，作为网络空间治理的顽疾，电信网络诈骗犯罪数量和金额仍然处于高位，究其原因，既是犯罪分子的贪念作祟，亦是社会、科技、心理、法律等多方面原因共同作用的结果。

（一）社会环境因素——移动互联网时代的负面产品

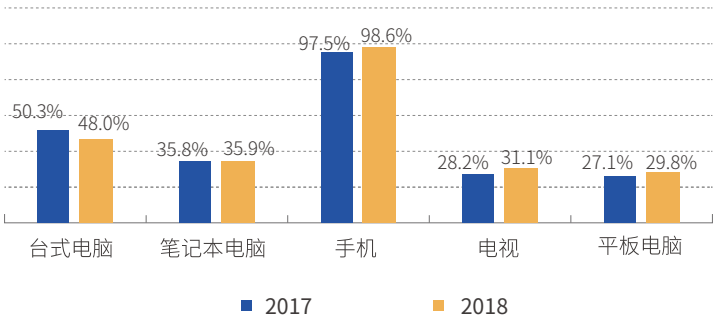
网民规模和互联网普及率



网民规模	普及率
6.49	47.9%
6.88	50.3%
7.31	53.2%
7.72	55.8%
8.29	59.6%

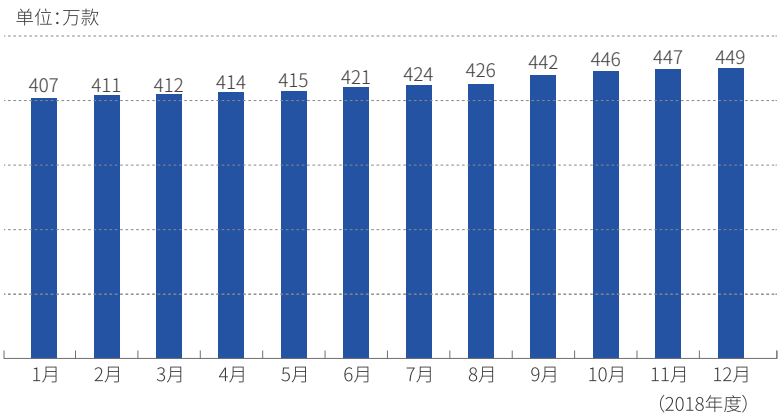
（数据来源：CNNIC 中国互联网络发展状况统计调查）

互联网络接入设备使用情况



（数据来源：CNNIC 中国互联网络发展状况统计调查）

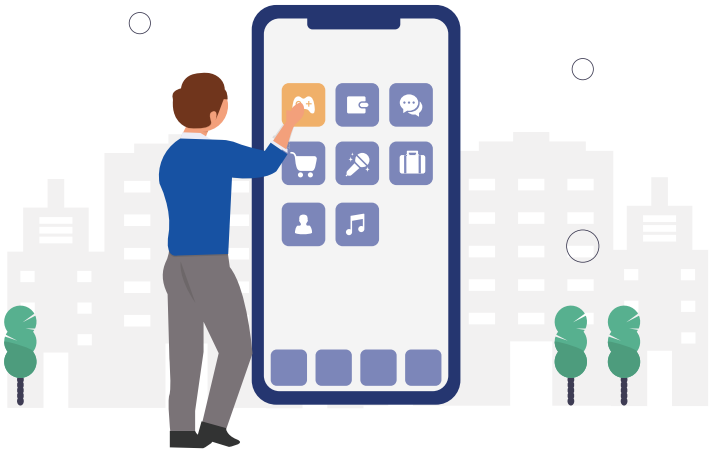
移动应用程序（APP）在架数量



（数据来源：工业和信息化部）

1. 信息网络对生活的高渗透，客观上也给电信网络诈骗提供了更多的空间场域

中国互联网络信息中心（CNNIC）发布的第 43 次《中国互联网络发展状况统计报告》的数据显示，截至 2018 年 12 月，我国网民规模为 8.29 亿，互联网普及率达 59.6%，其中使用手机上网的比例为 98.6%，使用手机网络支付的用户规模达 5.83 亿，手机上网已成为网民最常用的上网渠道之一。中国全面进入移动互联网时代，借助移动通信功能的高用户粘度，移动网络从“信息媒介”转换为“生活平台”，成为人们日常活动的第二空间*。网络空间占据了公众大量的时间与精力，也聚集了越来越多的社会财富，为诈骗行为在网络空间滋生、蔓延、壮大，提供了土壤。



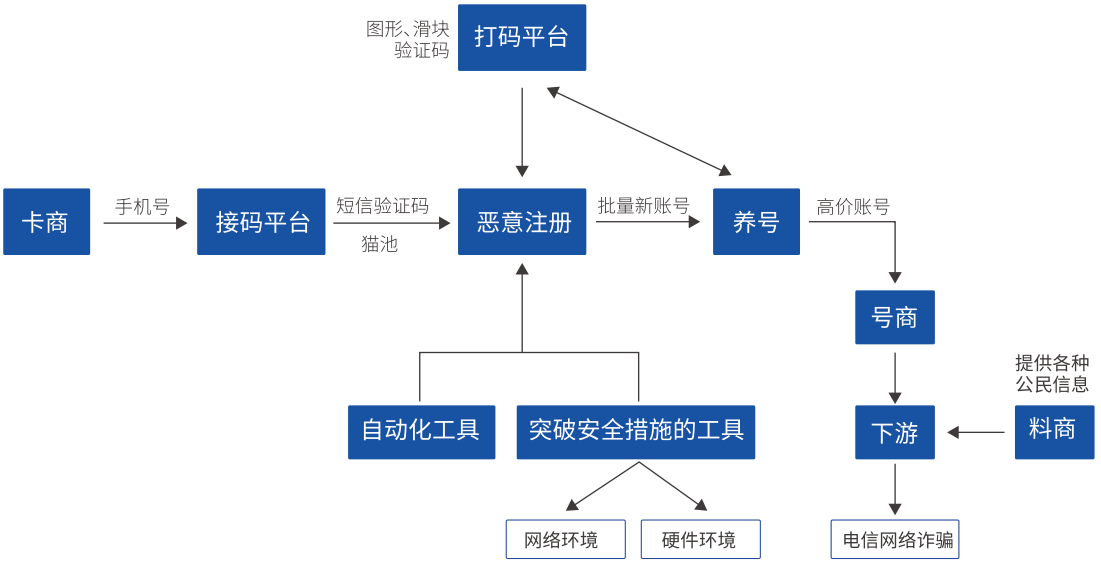
* 于志刚：《“双层社会”中传统刑法的适用空间——以“两高〈网络诽谤解释〉的发布为背景》，载《法学》2010 年第 10 期。

2. 更多的技术应用，使得电信网络诈骗可利用的场景增加

截至 2018 年 12 月，我国市场上的移动应用程序（APP）在架数量为 449 万款，如此庞大的应用集群，涵盖电子商务、社交、游戏、娱乐、支付、投资等领域，渗透进我们生活的每一个角落。这些应用程序在满足生活各种需求的同时，也为电信网络诈骗提供了丰富的场景，一些新类型、新套路随着互联网新型业态而产生。

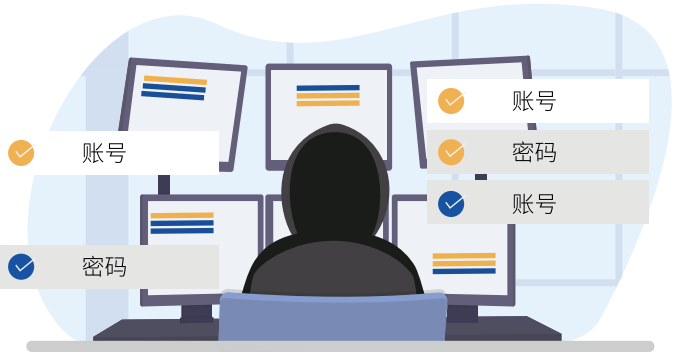
（二）上游、源头黑产因素

随着互联网技术的发展和社会分工的日益细化，网络黑产日趋产业化、链条化、生态化。电信网络诈骗的迅速蔓延和高效敛财，离不开“海量账号”和“精准信息”这两大手段，与此相关的上游源头犯罪尤为重要。但现阶段，对上游黑产的刑事规制困难重重，使得其依然能够源源不断地为电信网络诈骗输送“弹药”，严重威胁整个互联网生态安全。



1. 互联网恶意账号是电信网络诈骗的源头

首先，恶意注册养号黑产为电信网络诈骗源源不断地供应各类账号资源。为逃避打击，用于电信网络诈骗的账号基本不会重复使用，因此诈骗行为人需要囤积大量账号资源用于提供网络身份并隐藏真实身份，以增加平台溯源难度、逃避法律追究。



其次，恶意注册及养号黑产为保持账号的正常存续和使用，养号群体会模拟真实账号使用场景，将账号加入更多好友、群组，定期更新日志，绑定真实身份，开通支付等功能，甚至开设网店，以此提升账号价值。这些账号营造出一种真实、连贯的工作场景和生活场景，使诈骗场景更加立体化、生态化，让被害人更容易放松警惕。

2. 公民个人信息泄露情况依旧严峻

首先，公民个人信息是恶意注册及养号环节不可或缺的要素。精确的个人信息，例如身份证信息和银行卡信息等，使账号能够适用多种场景，包括支付等敏感场景，从而更具真实感和欺骗性。绑定了身份信息的账号，更易绕过互联网行业的安全策略，得以“存活”。

其次，公民个人信息是“精准诈骗”得以实现的关键因素。当公众对电信网络诈骗的既有观念还停留在“广撒网”的方式时，精准诈骗因其针对性强，更易突破公众的心理防线，为诈骗实施起到了推波助澜的作用。

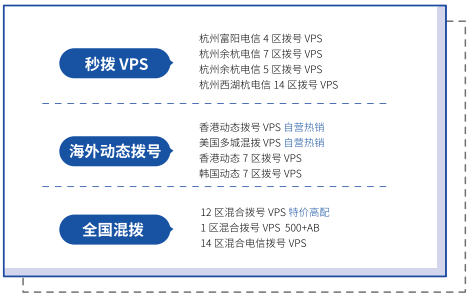
现阶段，黑产团伙通过多种方式获取公民个人信息，包括在有漏洞的目标网站服务器中建立“后门（webshell）”以拖取存储数据，通过交易、互换等方式批量获取，公开渠道抓取，甚至利用少量金钱报酬诱导个人出卖自己的身份信息。除此之外，亦存在部分公民自愿提供个人信息甚至身份资料的情况。他们基于各种诉求，明知他人可能会将自己的身份信息用于多种用途，甚至在对方明确告知会用于注册账号、收款等情况，亦自愿提供。

侵犯公民个人信息犯罪包括提供技术工具、居间倒卖、渠道疏通、资金结算等各个环节，可形成黑产闭环，尤其是在提供技术工具环节，对证明主观明知状态的证据要求较为严格，法律适用存在难点，致使侵犯公民个人信息的犯罪屡打不尽。

3. 黑灰产源头平台工具泛滥

用于电信网络诈骗的账号，在注册及养号过程中，需要对抗和突破互联网安全保护措施，也需要进行批量自动化操作，各类黑灰产平台工具因此应运而生，服务于源头犯罪的各个环节，日益泛滥。

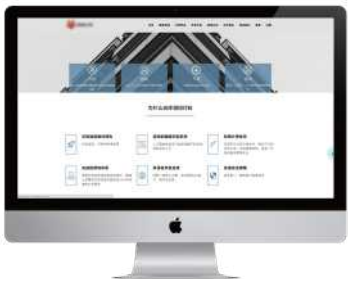
针对单一 IP 短时间注册或登录大量网络账号会触发相应的安全策略，黑产分子开设“秒拨”动态 IP 服务平台，使运行在同一网络环境下的不同虚拟账号对应不同 IP，绕过安全策略，供多人使用。



代理 IP

针对互联网平台采取“手机号 + 下行或上行短信验证码”方式进行用户鉴权的安全策略，黑产分子开设接码平台，使用“猫池”工具（指有通信模块、可收发短信、支持多张手机卡同时使用的设备），用于接收短信验证码或语音验证码，并反馈给注册群体，从而帮助完成验证过程*。

接码平台



打码平台

针对部分产品和场景（如用户异地登录或更换设备登录）下，注册或登录过程还可能触发字符、图片识别或滑块验证码识别等验证环节，黑产分子开设打码平台，通过平台接入的图文验证码识别技术，快速、批量实现账密的验证及账号的登录。

针对部分社交软件采取的好友辅助验证策略，黑产分子开设辅助验证平台，以发布任务的方式，付费招募人员扫描二维码进行验证。

* 引用自《互联网账号恶意注册黑色产业治理报告》，腾讯网络安全与犯罪研究基地

（三）技术因素——高科技手段的应用助推网络诈骗高效运转

一方面，高科技手段的应用帮助诈骗行为人大量获取数据、快速整理数据、智能分析数据。在大数据时代的背景下，诈骗行为人为达到控制系统、获取数据的目的，需要利用多种科技手段，以求“道高一尺、魔高一丈”，突破各系统设置的安全技术措施。公民个人信息可能散乱存在于各个数据库或是存储介质中。基于大数据和人工智能技术，诈骗行为人通过扫描漏洞建立后门或制作恶意 SDK 植入 APP，获取大量包含公民个人信息的数据，并利用计算机人工智能算法等技术手段，对杂乱无章的数据进行分类整理、智能挖掘与分析，最终实现对被害人的精准画像，定向设置不同的诈骗场景，提高诈骗成功率。

另一方面，高科技手段的应用使得电信网络诈骗黑产实现从“一对一”到“一对多”的跨越。电信网络诈骗黑产链条高效运转的流程日趋批量化、自动化，目前已开始运用人工智能的技术和手段，制作自动化程序、工具，进行深度学习，不断训练其模拟输入和模拟点击的操作能力，结合特定脚本，实现自动化操作。在自动化程序、工具的帮助下，黑产团伙的犯罪成本大大降低，效率极大提升，获利空间也不断增大，几十人的犯罪团伙便可在短时间内给数以万计的被害人造成财产损失。群发群控设备、改号软件日益成为诈骗黑产的标配，利用 GSM 劫持、嗅探技术进行盗刷、诈骗的案件也在各地陆续出现。

群控系统

改机工具

最后，高科技的应用也为电信网络诈骗黑产上游犯罪行为对抗和突破互联网安全保护措施提供了支持。前文所述“秒拨”IP 服务平台、接码平台、打码平台等黑灰产源头平台工具，均需要有先进的技术支撑，以应对各大互联网平台不断改进完善的安全策略。以打码平台为例，从早期人工识别和输入，到利用人工智能训练机器批量识别，再到近期除使用 AI、OCR 等技术手段之外，已开始采取 Hash 值匹配校验与人工打码相结合的稳定方式，大大提高了破解验证码策略准确率。

（四）被害人因素

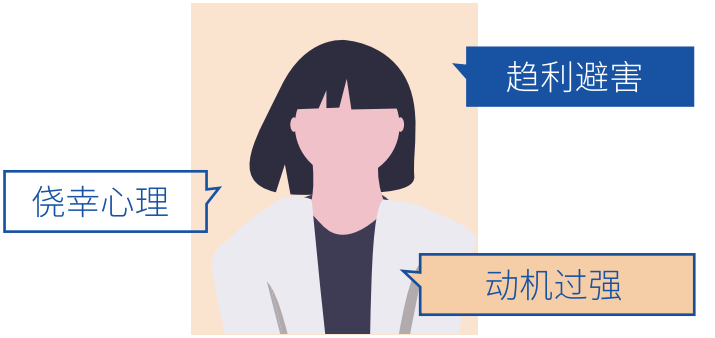
1. 知识因素

数字时代的今天，人们的生活与网络密切联系在一起，各式各样的新功能新应用极大地提高了公众的生活效率和生活质量。但是，受年龄、性别、职业、受教育程度、触网时间等因素的影响，不同网民对于互联网知识的关注度、学习能力各不相同，部分网民互联网应用知识的更新滞后，在遭遇骗局时易陷入错误认识。

在电信网络诈骗中，蹭热点、炫科技、装专业是诈骗行为人的惯用套路，将一些专业概念与互联网包装在一起，更具迷惑性，特别是涉及互联网金融投资这种需要专业知识的领域尤为突出。区块链、5G、虚拟币、MT4 平台等概念，对于普通网民来说，既常见又陌生，知其然却不知其所以然。诈骗行为人便利用网民专业知识上的缺口，包装概念、虚构平台，骗取被害人的钱财。

2. 心理因素

针对电信网络诈骗被害人的心理状态，我们结合心理学家专业解答，通过回溯、重现真实案件中被害人的所思所想，勾勒出一幅被害人的心理画像。



（1）“趋利避害是人的本能”

故事一*

主人公：刘某

诈骗套路：金融理财诈骗

被骗经历：

刘某经人介绍，下载了一个理财 APP，该平台承诺高额利息。在刘某的首笔投资获得高额利息后，平台便以系统遭不法分子入侵，需存入等额资金才能提现为由，先后多次诱骗刘某投资近 20 万元。

心理状态：

“一开始也是不太相信，后来推荐人引导操作后就放下了戒心。特别是第一次投入 20000 多块钱，1 天就能赚几百块，我就被冲昏了头脑，没有想是不是骗局。”

* 案例来源：“贪念高利息，女子被骗 19 万多”，湖北电视台，2019 年 5 月 30 日。

故事二

主人公：李某

诈骗套路：仿冒公检法诈骗

被骗经历：

李某接到一个自称警察的人打来的电话，称李某的银行卡在一起犯罪案件中出现，可能会被认定为同伙，要其配合调查。“警察”要求李某通过指定网址下载名为“公安防护”的 APP，并输入银行卡号、身份证号等信息，当李某正在操作时，真正的警察赶到制止。

心理状态：

“当时被对方的话吓懵了，稀里糊涂的就按照对方的指示来做。”

专家解析：

趋利避害是人类的一种本能，不需要学习。在高息投资受骗的案例中，受害者往往贪念高额的利息回报。骗子总是虚虚实实，先予后取。在信息不充分的情况下，骗子利用一些诱导策略，很容易使认知能力不强的人上当。因此防骗教育要直击要害，讲清骗局后面的逻辑，让老百姓既有常识又有知识。

* 案例来源：“注意！这个警察都不知道的‘公安局’APP，你得当心啦！”，法制网，2018 年 4 月 29 日。

（2）“心存侥幸，总觉得还有机会翻盘”

故事三

主人公：陈某

诈骗套路：投资共享产品诈骗

被骗经历：

陈某的朋友推荐了一个投资共享洗衣机的项目，宣称是“躺赢模式”，698 元购买一台共享洗衣机，每天收益 30 元，持续 365 天，合计 1 万多元，推荐其他人还额外有奖励。陈某觉得有利可图，就参与了投资，因为前期获得收益，还介绍给了亲友，结果骗子跑路，竹篮打水一场空。

心理状态：

“当时也觉得坚持一年会有风险，但算算 23 天即可回本，只要自己跑得快，还是有回本和获利的可能，上当的只会是后面进来的人。大家都是侥幸心理，觉得自己可以在投资项目停止之前获利。”

专家解析：

受骗者很容易把自己和骗子连成一个命运共同体。由于自我价值保护的需要，受害者往往把项目失败归因为外部因素，比如运气或政策的原因等，心存侥幸，期待并觉得还有机会翻盘。侥幸心理类似于赌徒心理，觉得最倒霉的不一定是自己。有人知道受骗了，为了减少损失，继续投入，期望通过击鼓传花，把损失转嫁出去。

* 案例来源：“698 元投资一台共享洗衣机，开启‘躺骗模式’”，腾讯 110 公众号，2019 年 7 月 13 日。

（3）“动机过强，人的理性水平会降低”

故事四

主人公：孙某

诈骗套路：修改学信网信息诈骗

被骗经历：

孙某为了谋求更好的个人发展准备跳槽，无奈大专学历无法满足应聘公司的基本入职条件。后其在网上结识的一个人，自称可以在 20 天内更改学信网信息，孙某信以为真，给对方转账 6000 元，最后不仅学历信息未按约定时间修改，自己也被对方拉黑。

心理状态：

“为了不放弃这次好的工作机会，急于求成，便动起了歪脑筋。”

专家解析：

需要背后是不平衡感和缺憾。需要会推动人去行动，这种推动力量就是动机。动机过强，人的注意变窄，认知活动受影响，容易受环境的作用和他人的暗示，导致受骗。

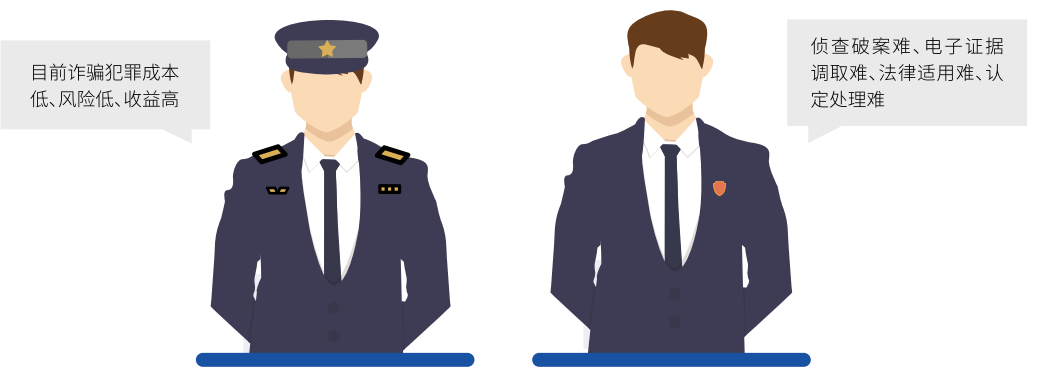
* 案例来源：“学历不高动了‘歪脑筋’ 改学历信息不成反被骗六千”，扬子晚报网，2018 年 7 月 7 日。

（五）刑事打击困难

针对电信网络诈骗持续高发的形势，公安、检察机关也积极深入研究，总结刑事打击面临的困难，针对犯罪成本低、收益高，跨境打击难、法律适用难、打击成本高等突出因素，研究破解方法，遏制电信网络诈骗的蔓延势头。

公安机关在总结诈骗案件态势时指出：“目前诈骗犯罪成本低、风险低、收益高。犯罪分子流窜程度加剧、地域性犯罪突出、职业化趋势明显，传统犯罪与互联网犯罪高度融合，团伙构成、作案手段更加复杂，隐蔽性更强，侦查打击的难度更大。”*

在成功破获某跨境作案犯罪团伙时，办案人员表示说：“因为成本低、收益高。我们估算过，每 40 人的窝点每个月诈骗的基本业绩，收入在 1000 万人民币左右。”



检察机关将打击惩治电信网络犯罪方面遇到的问题总结为“四难”，即“侦查破案难、电子证据调取难、法律适用难、认定处理难。”**

* 《继续保持高压严打态势切实维护群众财产安全和合法权益 公安部召开新闻发布会就破获特大海外医疗诈骗案情况答记者问》，载于公安部官方网站，2018 年 12 月 7 日。

** 《严厉惩治电信诈骗犯罪 切实保护百姓合法权益——访最高人民检察院第一检察厅副厅长罗庆东》，载于“信用中国”网站，2019 年 6 月 21 日

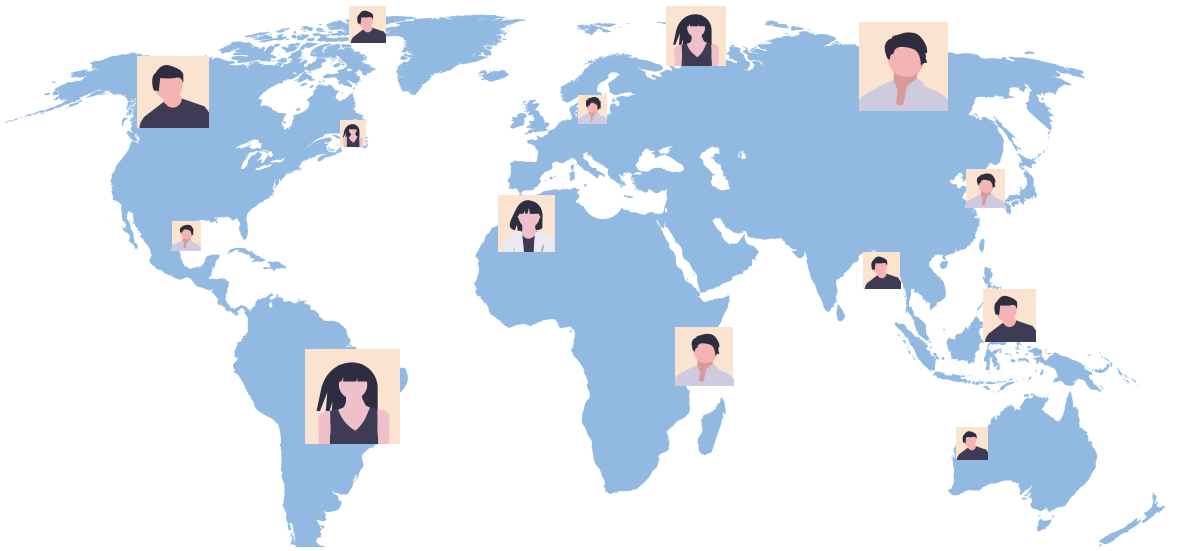
具体情况如下：

1. 犯罪成本低，回报率高

诈骗行为人通过网络实施诈骗，依靠技术手段实现全自动、批量化运作，极大地节省了资金、人力和物力投入，特别是随着黑产链条分工的日益细化，每个犯罪节点只需集中投入特定的设备、程序、人员等即可实现自上游到下游诈骗实施的整个过程，而且随着技术的不断升级，成本会日益降低，一旦得手，将会获得巨额的收益。

2. 被害人分散，打击成本高

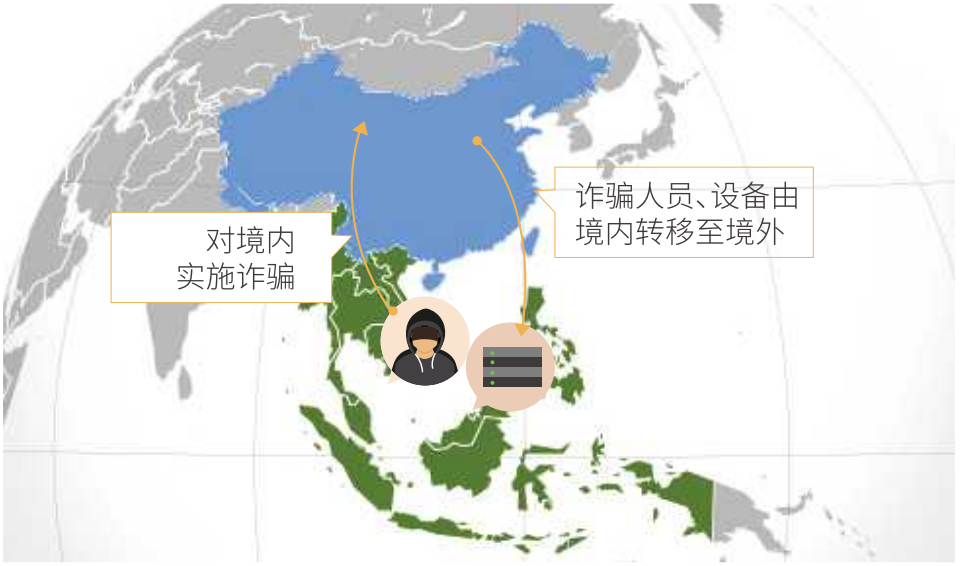
首先是被害人地域的分散。由于电信网络诈骗具有非接触性，基本不受时空限制，涉及地域范围广，被害人数众多，跨区域作案已成常态。多地报案，多地办理，极大地浪费了警力资源，也给案件侦破带来了很大的难度。



其次是被害人受骗金额呈小额分散的特点。为了降低被害人警惕心，便于犯罪得手，诈骗行为人往往采用小额诱骗的方式，特别是在免费送、低价利诱等诈骗中，由于单笔金额较小，被害人在受到诱骗处分财产时会降低戒备，同时在知晓自己被骗之后，很多人会因损失可以承受而放弃报案。诈骗行为人为了规避刑事打击，将单笔诈骗金额控制在立案标准之下，导致单个案件无法立案，需多地或多个案件联动处理，使司法机关需要付出巨大的时间成本，也易错过案件侦破的最佳时机。

3. 跨境作案，侦查取证难

近年来我国打击电信网络诈骗的力度不断加大，多地联动打击逐渐增多，使境内实施电信网络诈骗成本和风险上升，大量诈骗行为人开始转移至境外，以逃避国内监管和打击。他们将设备、人员均安置在境外，借助日益先进的科技手段和便捷的移动支付手段，对境内实施诈骗。其中，东南亚国家毗邻国境、社会治理较为薄弱，成为诈骗行为人首选，欧美国家也日渐受到“青睐”。这些犯罪团伙通过网络直接实施或者遥控犯罪，增加了执法和司法工作的难度，如管辖与司法协作困难、取证与固定证据困难、境外抓捕的成本巨大等。同时由于存储核心证据的服务器均位于境外，很难快速、准确查明运营商及服务器所在，容易被诈骗行为人利用时间差将服务器中的数据销毁。



4. 分工细化，法律适用难

针对电信网络诈骗的具体实施行为，我国刑法及相关司法解释已有比较完善的法律适用体系，之所以屡打不尽，与上游犯罪打击不力不无关系。例如上游恶意注册养号、提供各种专门工具和支付结算服务的黑产，为下游电信网络诈骗源源不断地提供账号、工具和资金来源，危害巨大。事实上，随着网络黑产分工日益细化，各个环节专业化运作，经层层交易，那些并非直接参与电信网络诈骗的行为和行为人，往往难以认定存在 “共谋” 。亦难以作为诈骗犯罪的共犯处理，因此只能对其进行单独评价和规制。

然而针对上游恶意注册养号黑产，现有的法律实践中，多以侵犯公民个人信息罪及提供侵入、非法控制计算机信息系统程序、工具罪进行处理，仅打击了侵害刑法所直接保护法益的犯罪，对于向下游电信网络诈骗恶意提供账号这个行为，因为证据原因，打击较少，从而给了黑产人员规避相关刑事责任的可能。

又例如公民自愿提供个人信息的行为，侵犯公民个人信息是刑法中侵犯人身权利、民主权利的犯罪，故而被害人的自愿将阻却犯罪成立，由此在被害人自愿提供身份信息被用于黑产的各个环节时，如何认定行为性质，尚需讨论。这些法律规制上的困难，客观上也影响了治理电信网络诈骗工作的总体效果。

第二章

公安、检察机关
打击治理电信网络诈骗的工作及成效

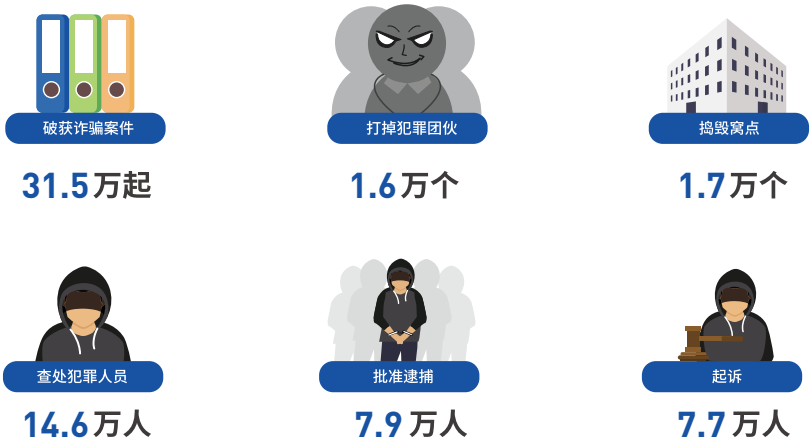
第二章 公安、检察机关打击治理电信网络诈骗的工作及成效

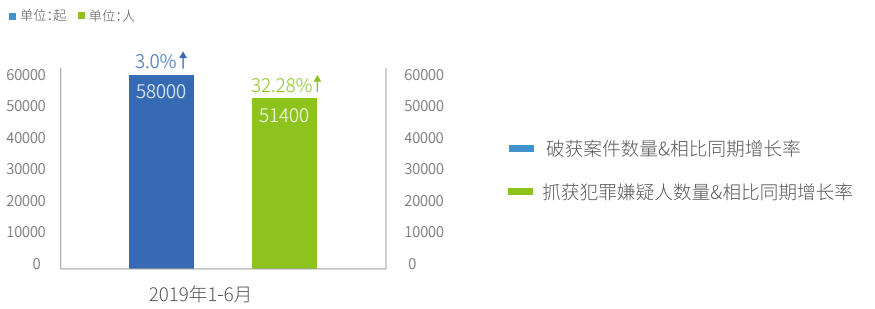
一、电信网络诈骗案件刑事打击成果

近年来，电信网络诈骗严重危害人民群众财产安全，扰乱正常生产生活秩序，破坏社会诚信和社会公德，已成为影响社会大局稳定、严重影响人民群众安全感的一大突出问题。对此，党中央、国务院高度重视。

2015 年 6 月，国务院批准建立了由公安部牵头，最高人民法院、最高人民检察院、工业和信息化部、人民银行等 23 个部门和单位组成的打击治理电信网络新型违法犯罪工作部际联席会议制度（以下简称：国务院部际联席会议），加强对全国打击治理工作的组织领导和统筹协调。

国务院部际联席会议各成员单位落实责任、齐抓共管，在防范打击和综合治理等方面不断取得新突破、新进展。近三年来，全国公安机关共破获电信网络诈骗案件 31.5 万起，打掉犯罪团伙 1.6 万个，捣毁窝点 1.7 万个；共查处电信网络诈骗违法犯罪人员 14.6 万人，检察机关批准逮捕 7.9 万人，起诉 7.7 万人。





2019 年 1 至 6 月，全国各级公安机关共破获电信网络诈骗案件 5.8 万起，同比上升 3.0%；共抓获电信网络诈骗犯罪嫌疑人 5.14 万人，同比上升 32.28%。

二、公安、检察机关专项打击及治理工作

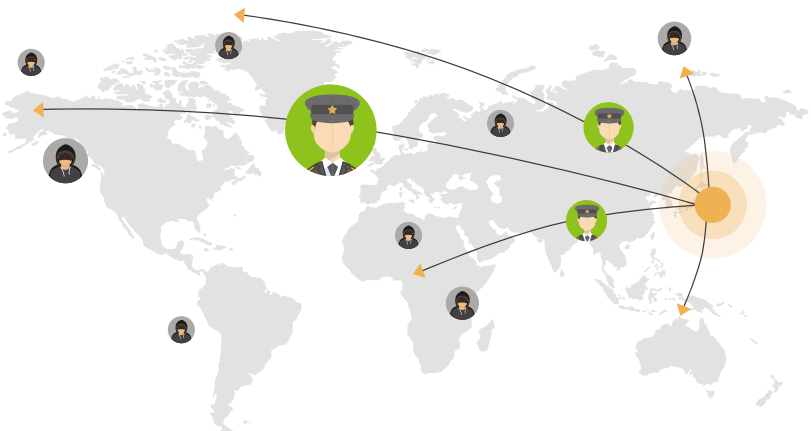
（一） 公安机关专项打击及治理工作

四年来，公安部依托国务院部际联席会议合成作战平台，与成员单位各司其职、密切协作，攻坚克难，持续不断地开展专项打击行动。

1. 重点工作开展

（1） 坚持依法严厉打击

近年来，按照党中央、国务院的部署和要求，公安部始终把电信网络诈骗犯罪作为打击重点，组织全国公安机关开展专项打击。



一是严厉打击在境外设立诈骗窝点。在我驻外使领馆领导和参与支持下，公安部先后 64 次组织各地公安机关赴东南亚、欧洲、非洲、中美洲等 34 个国家和地区开展侦查打击，先后打掉一大批犯罪团伙，捣毁一大批境外诈骗点窝点，抓获一大批犯罪嫌疑人，破获一大批电信网络诈骗案件，有力震慑了境外电信网络诈骗犯罪。

二是挂牌整治一批重点地区。将诈骗犯罪突出、诈骗窝点和人员较多的重点地区列为挂牌整治地区，强力推进侦查打击和重点整治，取得明显效果，涉及重点地区的案件已明显减少。

三是广泛开展宣传，引导社会公众提高自我保护。各地把加强宣传教育、提高防范意识作为重要工作内容，深入开展宣传教育，不断创新宣传手段，增强广大群众识骗、防骗的意识和能力。如，广东深圳开动“反诈专列地铁”等等。

反诈地铁专列

（2） 预警防范实现突破

公安部作为国务院部际联席会议牵头单位，整合运营商、银行等联席会议成员单位资源，同时大力开展警企合作，利用互联网公司大数据优势，根据重点地区本地犯罪的新变化和新形势，建立并不断更新预警模型，预防案件发生。同时对重点地区当地的寄递业、数码商城、手机卡、游戏点卡销售商等重点领域开展整治，切断支撑电信诈骗犯罪的黑灰产业链。

（3） 完善法律法规，保护个人信息，依法严惩打击犯罪

为严厉惩处此类犯罪，全国人大常委会通过的刑法修正案（九）在刑法中增设了第二百八十七条之一“非法利用信息网络罪”，第二百八十七条之二“帮助信息网络犯罪活动罪”，有利于及时处理，“打早打小”。公安部会同最高法、最高检联合发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》，明确规定了十种从重处罚的情形，进一步依法从严惩处此类犯罪。为保护公民个人信息，公

安部多次组织开展打击侵害公民个人信息犯罪专项行动，并商中央网信办、工业和信息化部推动完善相关立法和管理规范。

2. 下一阶段工作思路

尽管打击治理电信网络诈骗等新型违法犯罪和灰黑产业工作取得了一定的成绩，但受巨额利益驱使，电信网络诈骗及侵犯公民个人信息犯罪涉及巨大黑色产业链条，犯罪成本较低，犯罪手法隐蔽且花样翻新，案件仍高发多发，形势依然严峻。下一步，公安部将继续依托国务院部际联席会议，进一步加大打击力度，进一步强化源头监管，持续开展防骗宣传，坚决严厉打击此类违法犯罪，切实维护社会和谐稳定，切实维护人民群众财产安全。

（1） 进一步加大侦查破案工作力度

积极适应犯罪形势新变化，研究、深化各项打击、防范、治理、管控措施，探索创新打法、新战法，进一步强化多警种合成作战，集中攻坚境内重点类案，严厉打击地域性职业犯罪群体和跨境跨国电信诈骗犯罪团伙，坚决打击电信诈骗犯罪分子的嚣张气焰。同时，会同中央网信办、工业和信息化部等有关部门加强对网络黑产各环节的监测和溯源，建立网络黑产线索库，开展全链条打击，加大对互联网上生产销售“黑广播”、“伪基站”，买卖公民个人信息，贩卖非实名手机卡、银行卡等灰黑产业的打击力度，切实维护人民群众合法权益。

（2） 进一步提升防范打击工作效能

将充分运用互联网思维和信息化、大数据手段，积极适应犯罪形势新变化，研究、深化各项打防控措施，探索创新打法战法。进一步完善各级反诈骗中心建设，加强银行和第三方支付平台账户线上查询、止付、冻结功能，大幅提升接警受案、电话快速拦截、涉案资金快速止付、信息流资金流查询、案件串并研判、侦查组织指挥等工作效能。进一步攻坚重点类案、重点地区及重点环节，探索资金流、电信流和人员流技战法，有效斩断电信网络诈骗犯罪的源头。

（3） 及时研究解决相关法律问题

加强对打击电信诈骗犯罪、侵害公民个人信息犯罪法律层面的研究和总结，将刑法中关于打击电信网络诈骗犯罪相关条款在实践中的执行情况，适时通报全国人大法工委、最高法、最高检、司法部等相关部门，及时沟通协商，积极完善相关法律法规，为有效打击此类犯罪提供坚强的法律保障。

（4） 进一步强化源头监管综合治理

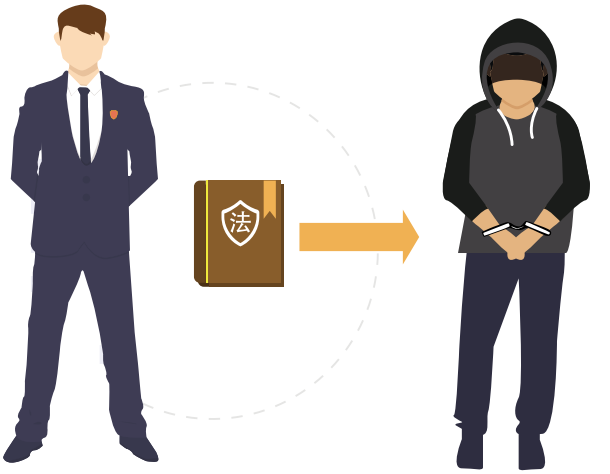
继续坚持开展一案双查，及时发现行业管理上的漏洞和不足，并落实相关部门责任；加强各成员单位沟通协调，巩固前期防范治理成效，优化防范打击经验做法，完善落实防范治理工作机制，聚焦问题、综合施策，积极推动相关部门堵塞监管漏洞，加强综合治理。

（5） 进一步强化宣传防范工作

会同人民银行、银监会指导各商业银行、支付机构和互联网金融企业深入开展反诈骗宣传。会同工业和信息化部指导主要基础运营商，定期向手机、固定电话用户推送最新防诈骗短信、语音提醒，及时发现归纳不法分子实施诈骗的新手法、新伎俩，及时通过电视、报纸、微信、微博等多种渠道向公众发布预警防范提示，提高群众防范意识和能力，同时再选取一批典型案例适时向社会公布，教育警示广大人民群众，震慑犯罪分子，最大限度挤压诈骗犯罪空间。

（二） 检察机关专项打击及治理工作

2015 年打击治理电信网络新型违法犯罪专项行动开展以来，全国各级检察机关紧紧围绕“查处违法犯罪嫌疑人数明显上升、破案数明显上升，发案数明显下降、人民群众财产损失明显下降”的“两升两降”目标，依法履行检察职能，严惩电信网络诈骗犯罪。



1. 高度重视，充分发挥检察职能，严厉打击电信网络诈骗犯罪

电信网络诈骗犯罪严重侵害人民群众财产安全和合法权益，严重影响人民群众安全感。最高检连续三年将严厉打击治理电信网络诈骗犯罪列为重点工作，部署、要求全国各级检察机关要从全面推进依法治国、巩固党的执政地位、维护国家长治久安的高度，深刻认识做好此类案件办理工作的重要意义，充分发挥检察一体化优势，形成打击合力，依法稳妥办理电信网络诈骗犯罪案件，坚决遏制电信网络诈骗的高发蔓延势头。最高检院领导多次作出重要批示和指示，并在每年提交给全国人大审议的工作报告中将严厉打击电信网络诈骗犯罪工作作为重点内容进行报告。

2. 制定规范性文件，加强顶层设计

最高检制定下发《关于切实做好打击整治电信网络诈骗犯罪有关工作的通知》，对检察环节电信网络诈骗案件办理工作提出了明确要求，各级检察机关侦查监督部门对于重大疑难电信网络诈骗案件要适时介入侦查，引导公安机关依法全面客观收集固定证据，符合逮捕条件的要及时批准逮捕，确保打击质量和效果。与国务院部际联席会议成员单位先后联合制定出台了《关于进一步防范和打击电信网络新型违法犯罪的若干意见》和《关于防范和打击电信网络诈骗犯罪的通告》，制定下发《关于切实做好打击整治网络侵犯公民个人信息犯罪有关工作的通知》，进一步做好打击治理电信网络新型违法犯罪的顶层设计，实现对此类犯罪的源头治理和综合治理。

3. 制定司法解释和指导意见，明确法律适用标准

最高检密切关注新型网络诈骗犯罪在案件定性、证据采信适用等方面存在的新情况新问题，不断总结经验，加强对下指导，解决新型网络诈骗犯罪法律适用难题。2016 年 12 月，联合最高法、公安部颁布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》，对电信网络诈骗犯罪的定罪量刑、关联犯罪的定罪量刑、电信网络诈骗共同犯罪和主观故意的认定、电信网络诈骗案件的管辖、涉案财物的处理、调查取证和证据认定等作了详细规定，进一步明确了法律标准，统一了司法尺度。联合最高法颁布《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》，组织编写《检察机关办理电信网络诈骗案件指引》《检察机关办理侵犯公民个人信息案件指引》，针对通过信息网络发布公民个人信息的行为，对设立用于实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组的行为，网络服务提供者拒不履行信息网络安全管理义务的行为进一步明确了认定标准。

4. 开展调研督导，加强对下指导力度

一是召开联合督导会。2016 年，最高检与公安部联合召开电信网络新型违法犯罪典型案件剖析调研会和电信网络新型违法犯罪重点整治、突出地区督导会，剖析典型案例，总结当前全国重点整治、突出地区打击治理电信网络诈骗犯罪基本情况、存在问题和取得的成效，并对打击治理工作进行现场督导和部署。

二是组织培训交流。与公安部、最高法联合组织《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》电视电话培训会，邀请专家深入解读《意见》精神和主要内容。派员参加在湖南湘潭举办的《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》座谈会，与公安、法院同志一起研讨《意见》的理解与适用，进一步统一了认识，形成打击合力。

三是加强专题调研。在浙江省杭州市临安区组织召开办理电信网络诈骗和侵犯公民个人信息犯罪案件专题调研会，江苏等五省（市）检察院分管此项工作的负责同志、业务骨干以及两类案件多发地区办案一线检察官参加了会议。会后形成《关于办理电信网络诈骗及侵犯公民个人信息犯罪案件专题调研会相关情况的报告》，围绕典型案例深入分析了此类犯罪的特点、存在的问题，并就下一步工作提出建议。

5. 挂牌督办案件，确保专项行动落到实处

最高检先后挂牌督办了三批电信网络诈骗重特大案件，包括山东临沂徐玉玉被电信诈骗致死案等涉校学生被诈骗重点案件，“8.20”亚美尼亚专案等跨国境引渡回国诈骗团伙案件，以及公安部重点督办系列诈骗专案共计 65 起。其中，仅第二批督办案件涉案金额近 4 亿元，被害人数达 25 万余人，犯罪嫌疑人约 1100 余人，串并案共 5600 余起。

6. 建立健全专业化办案部门和办案组织，提高惩防电信网络诈骗犯罪专业化水平

为加强对电信网络诈骗犯罪案件办理工作的组织领导，2017 年 9 月，最高检专门成立计算机网络犯罪案件检察官办案组，承办和指导办理涉及网络安全犯罪案件以及利用网络实施的相关犯罪等案件。地方各级检察机关优化办案资源配置，有的设立专门的计算机网络犯罪办案机构，有的单独设置计算机网络犯罪案件检察官办案组，提升办案人员专业化水平，不断提高计算机网络犯罪案件的办理质量。如北京市检察机关成立 5 个计算机网络犯罪办案部门，其中北京市东城区人民检察院设立了网络和电信犯罪检察部，海淀区人民检察院设立了科技犯罪检察部，负责计算机网络犯罪案件的办理。

7. 加强国际司法协作，共同应对跨境犯罪

2016 年以来，我国相继从肯尼亚、马来西亚、柬埔寨、老挝以及亚美尼亚等国成功抓捕归案电信网络诈骗犯罪嫌疑人数百人。为此，最高检向江苏、浙江、广东三省检察机关下发通知，要求苏州、杭州、东莞和惠州四地检察机关配合当地公安机关依法、从快、妥善依法办理境外电信网络诈骗犯罪批捕工作。检察机关成功从西班牙遣返 84 名台湾籍犯罪嫌疑人，及时追回赃款赃物并做好返还工作，实现了良好的法律效果和社会效果。除依法办理案件，最高检还积极努力与多国检察机关一起协商解决电信网络诈骗犯罪刑事管辖权冲突等问题，特别是在跨境协助调查取证、缉捕遣返犯罪嫌疑人、涉案赃款赃物移交、证据转换、司法文书送达、通信与网络证据的转换及互相采信问题等方面都有深入合作，为联合跨境打击犯罪打下了良好的基础。最高检还派员与公安部有关同志，先后赴西班牙、捷克、克罗地亚、匈牙利、斯洛文尼亚、波兰及越南、老挝等国家，与当地检察机关和警方对接，就共同开展打击电信网络犯罪执法合作进行交流。还与东欧国家建立检检和警警双线联动合作机制和落实有关国际协作办案经费，即我国警方在对“检察官主导侦查”司法体制的国家组织开展境外执法行动时，由检察机关根据需要适时派员加入公安机关专案组，负责与外方检察机关的沟通协调。

国际司法协作

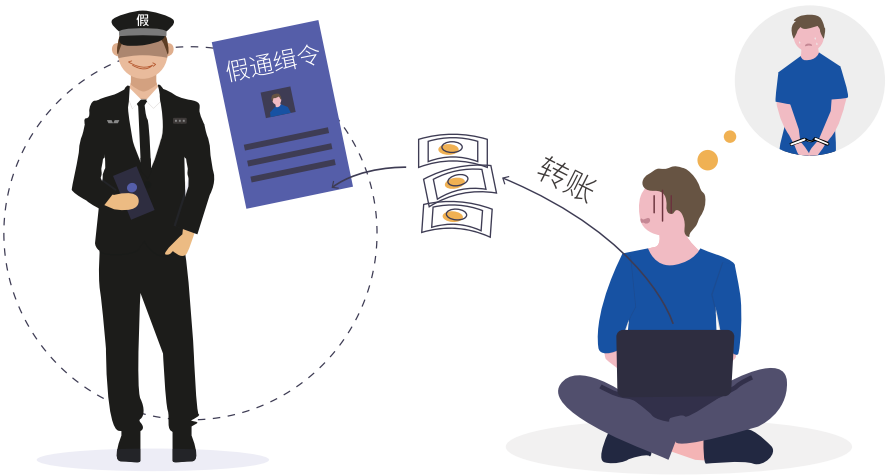
- 调查取证
- 缉捕遣返犯罪嫌疑人
- 赃款赃物移交
- 证据转换
- 通信与网络证据的转换
- 司法文书送达
- 互相采信问题

三、典型案例展示

案例一、跨境冒充公检法诈骗案

1. 作案手法：

不法分子假冒公安、检察官或者法官等以涉嫌各种违法犯罪为理由，要求被害人提供账户核查资金或将资金转入安全账户。骗子为了体现真实性，甚至还会制作假的通缉令，以达到操控被害人的目的。



2. 案情重现：

北京市公安机关接群众黄某某报案称有诈骗行为人假冒“北京市朝阳区公安分局国际刑警”实施诈骗，期间为骗取事主信任，还主动让事主拨打 +8610114 核实电话真伪。北京市局刑侦总队立即会同有关单位成立专案组开展侦查调查工作，技术研判发现犯罪窝点位于菲律宾。随后，公安部派出专案组赴菲律宾开展打击工作，克服地域、生活习惯以及中菲双方法律制度上的重重困难，取得突破进展。经 100 余天奋战，专案组会同菲律宾国家警察局在菲律宾老沃市郊区成功打掉一个以冒充公检法手段对中国大陆居民实施电信诈骗犯罪的团伙，抓获犯罪嫌疑人 22 名（其中台湾籍 13 人，大陆籍 2 人，菲籍 7 人），现场缴获用于实施诈骗犯罪的笔记本电脑、语音网关、作案用手机、话术若干。初步核实该团伙共实施诈骗案件 33 起，涉案金额 3300 余万元。

防骗提醒：

一是留意来电号码。此类案件中，大多数来电都是通过改号软件从境外拨打，来电显示上会有“+”或“00”等前缀，如出现此类异常，可以基本判定为骗子无疑；

二是假冒检察官、法官人员多为南方口音，当对方来电不符合常用语习惯时，就要存疑；

三是公检法人员绝对不会通过电话、社交账号通知你已涉案或要求核查资金、将钱款转移安全账户，更不会让你上网浏览自己的通缉令或者逮捕令，或者将此类材料邮寄到个人手中。凡通过电话、短信等要求进行转账、汇款、资金核查操作的都是诈骗，切记不相信、不转账；

四是如实在不能辨别真伪，要拨打 110 核实并了结情况，对方电话不清楚时，一定要拨打来电号码当地的 110 进行核实（当地区号 +110）。

案例二、交友投资类诈骗案

1. 作案手法：

在相亲网站或者普通社交软件结识，一旦两人发展成为恋人关系，便诱惑被害人参与网络赌博、网上购买彩票、网上投资等，骗取钱款。

2. 案情重现：

江苏省苏州市王某报案称之前在网上加了一个好友，对方自称是老师，后以买蛋糕过生日、闺蜜生病等名义让其转账，共计被骗 8700 元。苏州市公安机关接报案后，立即成立专案组开展侦查调查工作。经缜密侦查，苏州市公安机关在湖北武汉、天门抓获陈某等 12 名犯罪嫌疑人，在福建省福州市成功抓获赖某等 14 名犯罪嫌疑人。经查，陈某犯罪团伙在网上冒充幼师，结交男性网友，以去云南支教、过生日等为由向男性网友索要财物，骗取财物后立即更换手机和社交账号进行下一周期诈骗，并将骗得财物通过多次转账方式洗钱取现。犯罪嫌疑人赖某成立公司组织多人冒充女性在交友网站以交友恋爱的方式骗取被害人信任进而注册平台进行投资，后以控制平台后台涨跌的方式，诈骗被害人钱财。被害人遍及全国各地百余人，涉案金额 60 万余元。

防骗提醒：

一是网络交友要谨慎，应比现实社会交友更加谨慎，遇到异常热情，短时间内主动要求确立情侣关系的人需要提高警惕；

二是深度交友务必深入了解，特别是婚恋网站、社交网站、交友 APP 上的好友，深度交往时务必核实信息，防止对方以虚拟身份实施诈骗，此类案件，作案全程对方不见面。不要轻信网上发过来的图片和视频；

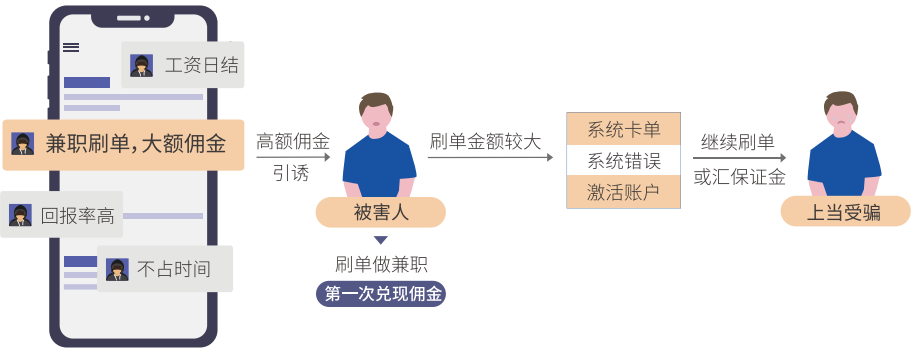
三是在与网友接触时，切莫起贪念；

四是不要随意转账或者汇款，当素未谋面的网友忽然提及财物时，要提高警惕，不要被甜言蜜语冲昏头脑。

案例三、兼职刷单类诈骗案

1. 作案手法：

在各种群组或者短信息中发布兼职信息，工作内容大多是招募网络兼职刷单，声称“回报率高”“工资日结”“不占时间”，以高额佣金为诱饵吸引当事人上钩，要求事主刷单做兼职。第一次往往会兑现佣金，待当事人刷单金额较大时，就会以系统卡单、系统错误、激活账户为由，要求事主继续刷单或汇保证金，骗取金额。



2. 案情重现：

潘某报警称，在家收到一条陌生号码发送的兼职刷单短信，以高利益诱使自己购买虚拟产品进行刷单，被不法分子诈骗 12 万余元。接报后，公安机关成立专案组，技术研判出取款人身份信息，随即赶往其住址进行蹲守，并将犯罪嫌疑人冯某某抓获。经突审，在宁波市鄞州区成功抓获另外 3 名犯罪嫌疑人。

防骗提醒：

一是通过网络平台找工作或者兼职时，不要被高额报酬盲目吸引，不要有“贪小便宜”和“轻松赚钱”的心态，不要随意点击陌生链接；

二是找兼职应当前往正规的公司或中介，签订合法劳务合同，保护自己的合法权益，特别是当对方要求预先交纳保证金以及其他费用的时候，一定要牢记风险意识；

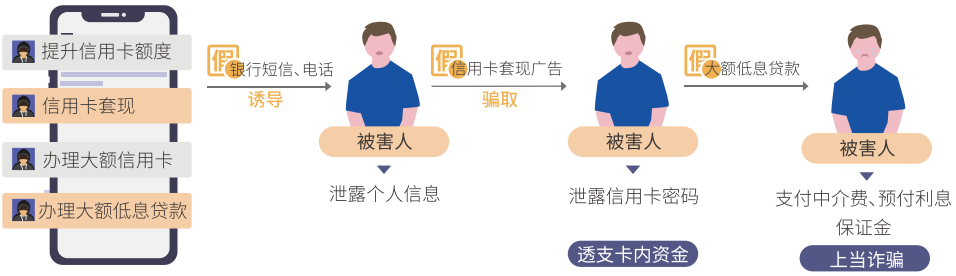
三是刷单诈骗往往要求被害人购买的物品为电话充值卡、游戏点卡等，支付时多请被害人扫描二维码付款；

四是网络刷单本就属于违法行为、严重失信行为，应珍惜个人信用，力避参与此类工作，遭遇诈骗立即报警，并将对方的聊天记录、电话号码等留存提供给警方，以便警方破案。

案例四、代办信用卡、贷款诈骗案

1. 作案手法：

骗子通过社交软件或其他广告群发可以提升信用卡额度、信用卡套现、办理大额信用卡或办理大额低息贷款等信息，假冒“银行短信” “银行电话”邀请持卡人提额，诱导持卡人按照他的要求操作，骗取用户信息；发布信用卡套现广告，骗取信用卡密码后，透支卡内资金；以办理大额低息贷款为饵，通过收取中介费、预付利息、保证金等方式实施诈骗。



2. 案情重现：

深圳坂田派出所接居民徐某报案，称其接到一个陌生电话询问是否需要办理贷款。通过电话交流后，嫌疑人添加了事主社交账号，让事主下载某贷款 APP，并要求其提交 8088 元人民币手续费以提升在该 APP 的货款额度。事主通过扫描对方发来的收款二维码转账 8088 元人民币后，便一直不予回复，徐某发现被骗。深圳市公安机关经缜密侦查，在湖南长沙市一写字楼开展收网行动，成功抓获犯罪嫌疑人 230 名，缴获大量作案设备、诈骗话术和公民个人信息。

防骗提醒：

一是任何不需要签订合同的贷款都是不可能的，请选择正规融资渠道；

二是通过正规渠道办理信用卡，不要轻信所谓的“信用卡代办机构或人员”；

三是任何正规贷款不可能请贷款人先缴纳手续费等费用，也不会让贷款人存钱以验资；

四是不要告诉他人动态验证码、银行卡卡号、有效期、卡背面上签名栏末三位校验码等关键银行卡信息。

案例五、荐股投资类诈骗案

1. 作案手法：

犯罪分子通过购买股民信息，抓住部分股民投资失败、股票亏损、急于解套的心理，以提供专业老师一对一指导、内幕消息为由，利用事先购买的盘后股信息（盘后股指在每日股票收盘后某些私募机构发布的股票代码，特点是第二天会高开，但由于股票市场 T+1 的交易模式，无法当天购买当天卖出，故并无实际投资意义），获取被害股民的信任，骗取股民交纳高额会员费。

2. 案情重现：

江苏省无锡市的赵某至公安机关报案，称其不久在股票专业公司“国泰机构”的业务员推荐下，添加了股票专家“康老师”为好友。之后二人以“专业指导” “内幕消息”，先后多次让赵某缴纳了共计22800 元的会员费，但事后推荐的股票不仅没有如期上涨，反而节节下跌，待其再次寻找“康老师”以及业务员理论时，发现对方早已将其拉黑。无锡市公安机关接报后立即开展侦查调查工作。经缜密侦查，公安机关在河北省石家庄市抓获以石某某为首的犯罪嫌疑人 12 名，并现场扣押用于实施诈骗犯罪的电脑、手机等 100 余部。

本案被害人遍及全国各地，涉案金额人民币 100 余万元。后该案被检察机关依法提起公诉。法院经审理，以诈骗罪判处相关被告人相应的刑罚。

防骗提醒：

一是留意陌生号码，尤其是陌生来电者对本人的炒股情况、资金状况等信息有所了解时，更要提高警惕，你的个人信息极有可能已经被犯罪分子非法购买；

二是冷静对待“稳赢承诺”，发现自己被拉入各类炒股群后，切勿听信“荐股者”一面之词，投资均有风险，无论是所谓“专家指导”“短线消息”“黑马行情”，还是其口中所称的“高级会员”“必赢软件”，背后都可能存在陷阱；

三是网络交友要慎重，切勿被头像、空间等信息所欺骗，真实使用者的情况可能和你通过网络所见的内容大相径庭，尤其是认识之初就极为热情的人，更加要有防范之心；

四是识别转账账户，不要轻易、随便向陌生人转账，对于他人给出的转账账户多加核实，犯罪团伙一般不会使用自己本人或者公司的账户进行收款，如果出现收款人与对方所称的人员、公司不一致时，要多加核实，即可发现破绽；

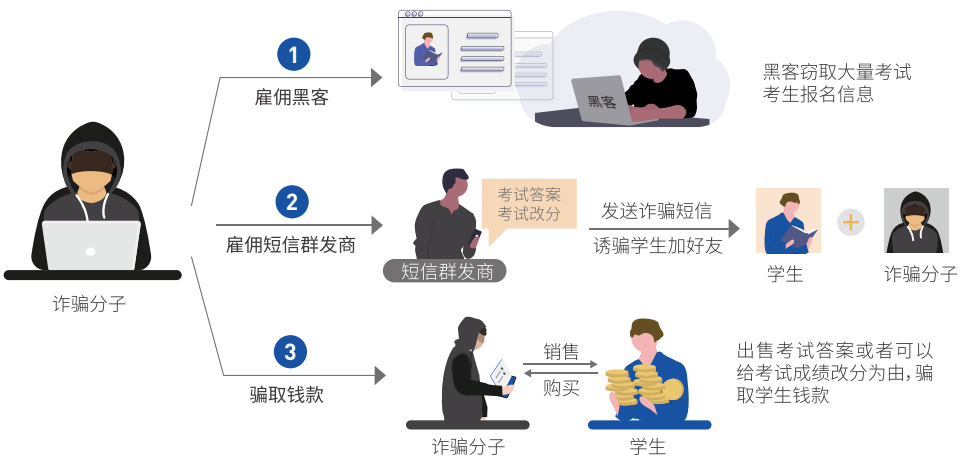
五是选择合法证券期货经营机构，获取相关投资咨询服务，合法证券期货经营机构名单可在中国证监会、中国证券业协会、中国期货业协会网站查询；

六是如果遭遇此类诈骗，要及时报警，将聊天信息、转账记录等保存好并提供给公安机关，配合公安机关做好案件侦破工作。

案例六、 “助考”诈骗案

1. 作案手法：

以在校学生为作案目标，瞄准部分学生意图通过违规渠道购买考试答案、进行考试改分的投机取巧心理，首先雇佣黑客窃取大量考试考生报名信息，然后雇佣短信群发商发送诈骗短信，诱骗学生主动添加诈骗份子社交账号后，以出售考试答案或者可以给考试成绩改分为由，骗取学生钱款。



2. 案情重现：

以曾某为首的诈骗团伙，通过向考生发送诈骗信息，以谎称可以提供考试试题、考试答案、考试改分为由，实施多起电信网络诈骗犯罪，发送诈骗信息 400 余万条，先后骗取被害人人民币 6 万余元。为帮助实施诈骗，曾某先后非法获取公民个人信息共计 1000 余万条。后该案被检察机关依法提起公诉，法院经审理，以诈骗罪判处相关被告人相应的刑罚。

防骗提醒：

广大学生不要存在通过违规渠道购买考试答案或者考试改分的错误想法，要认真对待学业。考试作弊本身属于违规行为，犯罪分子就是抓住学生的投机心理实施诈骗犯罪。很多学生被骗之后由于本身行为不端导致不愿报案，也给司法机关打击此类犯罪造成一定阻碍。

案例七、打卡 APP 网络诈骗案

1. 作案手法：

以身心健康、寓教于乐等名目，通过自我激励、团队鼓励、金钱奖励等噱头包装，诱使被害人投入金钱参与打卡挑战；利用软件设置和网络技术，人为修改 APP 挑战规则和奖励数额，骗取被害人财物；针对挑战者客户的投诉质疑，编织话术应对。

2. 案情重现：

王某某、李某某经共谋向被告人金某某购得“早起挑战团”、“准时早起”软件源代码，后王某某、李某某以某甲公司为据点，先后开设“早起挑战团” “准时早起”早起打卡 APP。打卡平台要求每位挑战者通过网络支付向某甲公司账户支付 10 元至 20000 元不等的挑战金，在挑战期的每天早晨固定时段登录打卡平台打卡。打卡平台规则明确：当天打卡成功者瓜分未打卡成功者的挑战金，挑战者成功打卡指定周期后，可以向平台申请退还挑战金。

王某某、李某某在营运过程中，多次联系金某某对“早起挑战团” “准时早起”软件进行再开发，在软件后台修改实际的未打卡金额数据入口，增加已打卡金额、减少未打卡金额。王某某、李某某等人将经修改减少后的未打卡金额作为当天的挑战金进行发还，将截留的金额据为己有。

在不到半年时间里，全国各地的打卡挑战者共参与打卡 98 万余人次，打卡成功者本应获得的挑战金真实金额为 400 余万元，而王某某、李某某等人实际发放的金额为 160 余万元。被告人王某某等人通过上述方式骗取各被害人共计 240 余万元。后该案被检察机关依法提起公诉，法院经审理，以诈骗罪判处相关被告人相应的刑罚。

防骗提醒：

一是通过网络平台参与活动时，不要盲目被或多或少的金钱奖励吸引，不要有“贪小便宜”或“轻松赚钱、一举两得”的心态；

二是尽量通过正规渠道下载、使用手机 APP，不要通过网络随意交付财物，特别要警惕不明的支付链接；

三是牢记风险意识，注意保护个人信息。

案例八、色情诈骗案

1. 作案手法：

利用男性独自在外居住酒店时易出现的“招嫖”心理，通过技术手段设置“桃色陷阱”，欺骗被害人先交钱再提供“服务”，诈骗金额较小，从 200 元到 2000 元不等。被害人即使识破骗局，也会因为金额较小，且紧张、羞愧又不愿意声张而不敢报警。此类诈骗作案门槛低，作案工具成本低廉，仅需一台手机，就可随时随地作案，可以一人单独作案或多人共同作案。

2. 案情重现：

犯罪嫌疑人黎某某、陈某某、彭某某、林某某等人在海南省儋州市等地通过在网上购买非实名登记的社交账号，包装成卖淫小姐的身份，随后联系“上号”人员即犯罪嫌疑人来某某、秦某某等人通过技术手段将该账号修改定位到指定地点（全国各地酒店附近），等候被害人搜索添加好友。随后，黎某某等人以卖淫小姐上门需要路费、先支付嫖资、转账忘记备注、缴纳卖淫小姐人身安全保证金等借口向被害人索要钱财，实施诈骗。为规避侦查，犯罪嫌疑人黎某某等诈骗份子向“洗钱”人员即犯罪嫌疑人邓某某等人购买收款二维码发送给被害人用于专门收取诈骗所得钱款，钱款经一层或多层流转后最终流入犯罪嫌疑人陈某某等人处。犯罪嫌疑人邓某某等“洗钱”人员明知黎某某等人实施电信网络诈骗行为，仍从他人处大量收购收款二维码，再提供给黎某某等诈骗行为人使用，并从中收取百分之十作为“手续费”。经查，本案涉案金额 500 万元以上。

该案线索由温州市公安局接报案获取，并抓获多名犯罪嫌疑人。检察机关挑选 4 名办案经验丰富并熟练掌握计算机、互联网专业知识的检察官成立专门办案小组，以 10 名左右的犯罪嫌疑人为一小组，同步审查，确保办案步调统一、证据标准一致，以提升办案质量与打击效果。该案被检察机关依法提起公诉后，法院经审理，以诈骗罪判处相关被告人相应的刑罚。

防骗提醒：

一是谨防“桃色陷阱”，网络招嫖行为不管是真是假，都是违法行为；

二是无论何种情况下都不要相信“先发红包后上门服务”等套路，网络支付要谨慎，发现支付异常要立即停止；

三是发现被骗之后要及时留存证据，尽快报案，最大程度挽回损失。

案例九、 “免费送”诈骗案

1. 作案手法

不法分子利用熟人间的信任，通过让被害人在网上发布虚假信息，更容易让被害人的亲朋好友上当受骗。同时，因为犯罪金额低，被害人报警意愿不强，造成大量被害人没有收到警示，继而不断有新的被害人被骗。

2. 案情重现

被告人顾某某等人成立、运营紫诺商贸有限公司，指使业务员通过社交平台添加好友，在网络社区中传播“免费赠送某名牌运动鞋” “免费赠送某名牌手环”等虚假信息，骗取被害人的信任，引诱被害人转发信息并识别信息中的二维码，按照紫诺公司事先设计的表格内容填写收货信息，获取免费赠送的物品。后采取收到货物后支付邮费的方式，将假冒名牌商标的劣质鞋快递给被害人，骗取每名被害人人民币 36 元；将劣质电子表快递给被害人，骗取每名被害人人民币 29 元。本案涉案人员多达 200 余人。经鉴定，各被告人实施诈骗涉案金额 1 万余元至 1.4 亿余元不等。后该案被检察机关依法提起公诉。法院经审理，以诈骗罪判处相关被告人相应的刑罚。

防骗提醒：

一是要注重培养网络安全意识，不要轻易相信不正规的商业信息和广告；

二是在网络活动中不要有“贪小便宜”的心理，越是贪图便宜越容易落入网络陷阱；

三是在网络活动中，一旦发现自己被骗时，一定要及时报警，给其他没有上当受骗的人警示，这样可以协助公安机关及早抓捕犯罪分子，减少其他被害人被骗的几率；

四是在发现被骗后一定要及时保存证据，收集相关链接的截图、图片以及实物证据，便于公安机关固定证据和被害人挽回损失。

第三章

腾讯针对电信网络诈骗的防护及治理体系

第三章 腾讯针对电信网络诈骗的防护及治理体系

针对持续高发的电信网络诈骗犯罪，腾讯公司始终保持对黑色产业链严厉打击的态度，构建底层安全保护、用户举报受理、大数据防控、刑事案件打击、安全知识普及五位一体的防治体系，为公众筑起一道坚固的安全防火墙。由于公司产品众多，安全保护措施也根据产品功能各有不同，故本报告将以微信在账号体系安全保护方面的措施为例。

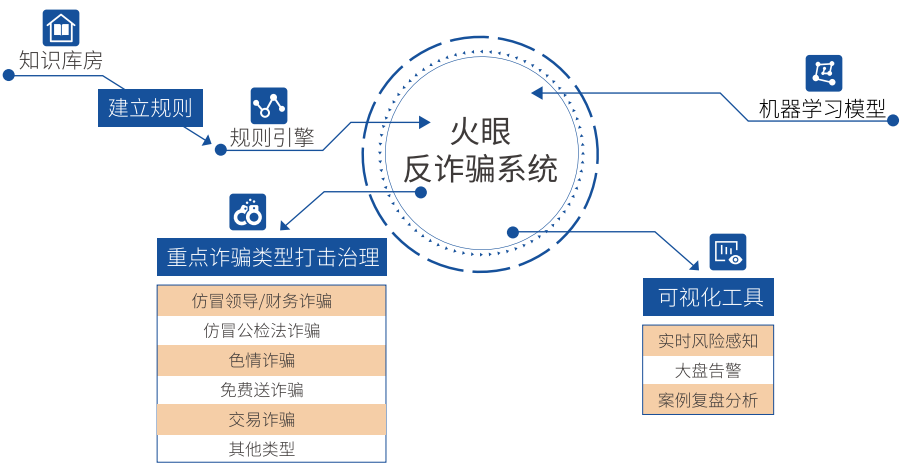
一、建立火眼反诈骗系统，筑牢底层安全保护

对电信网络诈骗的打击与治理，账号安全是基础。一直以来，微信安全团队对在微信体系内的欺诈恶意帐号保持严厉打击的态度，针对用户损失大、高发类型的欺诈模式成立了专项打击，通过反欺诈模型等技术手段，从各个维度和场景对微信上的欺诈行为进行覆盖式打击。

（一）微信反欺诈解决方案—火眼反诈骗系统

火眼反诈骗系统，是微信安全团队针对电信网络诈骗，建立的一套通用、可靠的欺诈风险防控解决方案。该系统从事前 - 事中 - 事后三个阶段分别进行风险控制，并构建了完整的反诈骗体系架构和一体化运营系统，期望为 11 亿微信用户提供反诈骗安全保护能力。

该系统采用规则引擎与机器学习模型组合而成的混合模型，及时对微信场景内所有诈骗类型的账号进行综合打击治理，即利用建立好的知识库建立不同的规则，再组建成新的规则引擎，寻找最优的解决方案，同时依赖大量特定的历史样本训练，二者最终结合成一个混合模型。



该系统重点打击治理仿冒领导（财务）诈骗、仿冒公检法诈骗、色情诈骗、免费送诈骗、交易诈骗等类型。同时，也提供实时风险感知、大盘告警、案例复盘分析等一系列可视化工具。

1. 事前——欺诈账号的发现与识别

基于腾讯在网络安全方面 20 年的技术和经验，已经积累了大量的数据，各类数据的接入最终搭建成为完整的数据仓库。同时系统采用了流式计算的技术，对大规模流动数据进行实时分析，建立行为系统，最终对账号异常特征的实时观察。通过上述技术措施，可实现对用户投诉的梳理和深度挖掘，对恶意账号的网络环境特征、行为特征等进行多维度分析，从而构建一套智能用户画像的体系。

为此微信自主研发了无监督异常聚类检测算法、外挂监测和客户端保护体系等多种技术，结合微信账号的安全审计结果，从账号的举报记录、属性等多个纬度主动发现和识别和覆盖欺诈、恶意账号。目前对恶意账号的覆盖率达 96%。

2. 事中——用户安全体验

针对用户的潜在风险，微信开发了基于客户端的产品体验，让用户对潜在风险再三评估，降低欺诈风险。目前针对若干重要互动场景设置安全提醒，包括异常详情、客服求助、以及结果反馈。

（1）账号侧前端安全体验

为了让用户感知到可能存在的安全风险，尽早阻断欺诈行为，微信在聊天场景设计了一套集提醒、求助、投诉于一体的防欺诈安全保护机制。根据用户举报的大数据模型，针对不同诈骗类型和账号特点，开发出了近十种不同描述的异常提醒，当对方账号满足其中一种异常时，将会显示其对应的提醒文字。

个人聊天场景下的欺诈提醒体验：

群聊场景下的欺诈提醒体验：

（2）社交支付侧安全体验

为了阻止诈骗行为对被害人造成财产损失，微信构建了一套对恶意账号支付能力进行限制，对被骗资金冻结、止损，以减少用户损失的策略模型。当系统识别出收款方账户的异常特征，付款时会弹出转账提醒的消息，比如提示“对方账号存在风险，请勿向对方转帐”等。

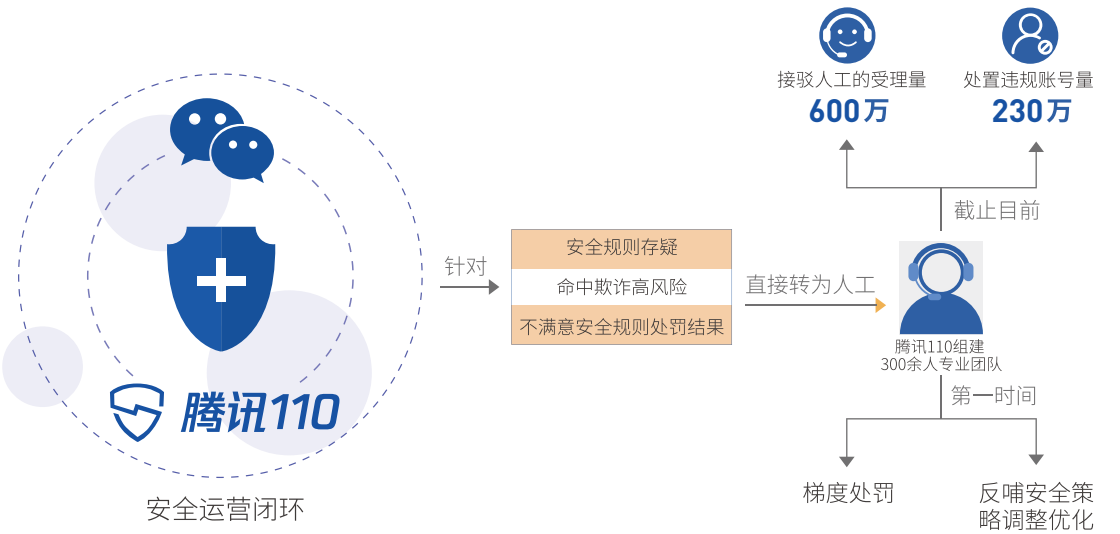
A、提醒 / 拦截（付款方）

B、拦截知会（收款方）

C、拦截解脱（收款方）

3. 事后——人工运营发现和梯度处罚

除了建立自动化、智能化的安全技术策略体系，为了能更高效地感知和提取有效的数据，微信安全团队也充分结合腾讯 110 的运营能力，搭建了完善的安全运营闭环。



人工受理审核

针对安全规则存疑、命中欺诈高风险以及不满意安全规则处罚结果的三类投诉，直接转为人工受理渠道。人工根据举报用户举证，被举报人行为特征等综合信息，甄别有害类型、恶意程度，并对其进行包括不限于封号、限制功能、警告等多种梯度处罚措施；同时人工根据受理的举报数据进行聚类分析，反哺安全策略调整优化。

人工受理团队为腾讯 110 组建的 300 余人专业团队，根据严谨规范的标准流程，支持微信客户端投诉产品流程体验。截至目前，接驳人工的受理量高达 600W，处置违规账号量 230W。

举报数据分析

除基础的人工审核外，运营团队还专设黑产情报分析与挖掘小组，一方面对举报数据进行聚类分析，深挖黑灰产上下游产业链、具体模式、行为特征等，持续提供专业报告，实时升级打击策略，保证策略的持续有效性；另一方面，通过对人工审核标记的诈骗账号进行特征提取和多维属性分析，反哺规则引擎、文本模型、黑样本库、机器学习等线上模型。

违规账号延伸挖掘

为了进一步前置恶意账号发现能力，消耗黑产团伙账号存量资源，提高作恶成本，最终降低欺诈、违规发生的概率，微信安全团队会通过人工选取确认违规的账号做为分析样本，进行延伸挖掘，对更多可疑账号和网络环境、设备等进行关注和处理。

（二）专项治理典型及高发欺诈类型

针对典型及高发的诈骗类型，微信主动进行专项治理，通过制定专项打击计划，发布专项治理公告，开放短期举报入口，分析专项运营数据，优化线上策略，并联动腾讯“守护者计划”安全团队，协助公安机关对线下团伙进行刑事打击。

（三）微信欺诈治理打击成果

微信反诈骗体系化平台自正式上线以来，通过火眼系统，结合人工审核，提升对欺诈团伙的挖掘能力，目前已对仿冒、兼职、贷款、返利等多种欺诈类型进行全面覆盖。累计发现、处罚恶意账号数百万，有效提醒用户数十万，用户投诉反馈量一直保持在历史低位水平，社交支付订单报障量自 2018 年中旬至今，同比下降 30%。

二、深耕用户举报受理，拓宽全民共治的网络途径

（一）布局欺诈举报多平台入口

为了便于用户深度参与监督治理，除产品本身举报端口外，腾讯 110 还搭建小程序、网站、公众号、微博等平台矩阵，进一步适配移动互联网用户使用习惯，为用户提供多渠道举报形式。

（二）建立严谨的欺诈举报闭环体系

腾讯 110 组建数百人的专业审核团队，建立完善的 24 小时闭环运营流程，搭建统一的举报柔性操作平台，形成了业内领先的欺诈类举报闭环服务体系。同时，建立了严谨的处置打击标准，含单账号、多账号关联处置，定期组织专家进行各个具体策略的打击与覆盖的验证，及时调整和优化安全模型。

三、协助支持刑事案件打击，强化法律规范治理作用

如果说安全技术策略和用户举报受理处置是积极防御，那么线下的刑事打击则是对电信网络诈骗黑产的主动进攻。当前网络犯罪的黑色产业与互联网行业的安全防护始终处在一种“你追我赶”的持续对抗之中，并且随着双方技术水平的更新而交替压制，呈现一种螺旋式上升的趋势，因此法律的规制特别是刑事打击必不可少。

（一）统筹内部资源，专业支持打击实践

面对不断转化升级的新型电信网络诈骗犯罪，我们需要打造一支实践经验丰富、理论知识精通的专业化团队。因此，2016 年 4 月，腾讯公司推出“守护者计划”平台，组建 “守护者计划”安全团队，与各界密切协作，共建网络生态安全体系。

腾讯“守护者计划”安全团队对内联动微信安全团队、腾讯 110，依托腾讯在安全大数据、底层技术方面的优势，在线索输出、技术分析等方面积极配合支持公安机关打击电信网络诈骗，震慑犯罪，并在案件侦破后复盘分析犯罪手法，反哺线上对抗策略，为公众加固网络安全防护。

自 2016 年推出至 2019 年 6 月底，腾讯 “守护者计划”安全团队配合公安机关开展各类网络黑灰产打击行动，共计破获案件 646 件，抓获人员超过 11000 名，涉案金额超过 220 亿元，极大地震慑和遏制了网络黑产分子的嚣张气焰。

（图为腾讯公司首席执行官马化腾在 2018 年“守护者计划”大会上致辞）

（二）构建研究平台，解决法律适用难题

推动刑事案件落地、优化安全保护策略，需要有准确的法律适用和科学的法律解读做支撑。2016 年，腾讯公司成立“腾讯网络安全与犯罪研究基地”，聚焦新型电信网络诈骗犯罪问题，开展典型案例研究、法律政策跟踪解读研讨，并推动研究成果落地，发布多份专业研究报告，助力线上安全防护策略和线下刑事案件打击工作。

针对在打击电信网络诈骗及上游黑产过程中遇到的法律适用难点，腾讯网络安全与犯罪研究基地通过其打造的“互联网刑事法制高峰论坛”“问道安全讲堂”“问道安全沙龙”等高端交流平台，发挥桥梁纽带作用，推动打击实践和前沿理论研究的结合。

1 图 1 为腾讯公司副总裁谢呼在 2018 年“互联网刑事法制高峰论坛”上致辞

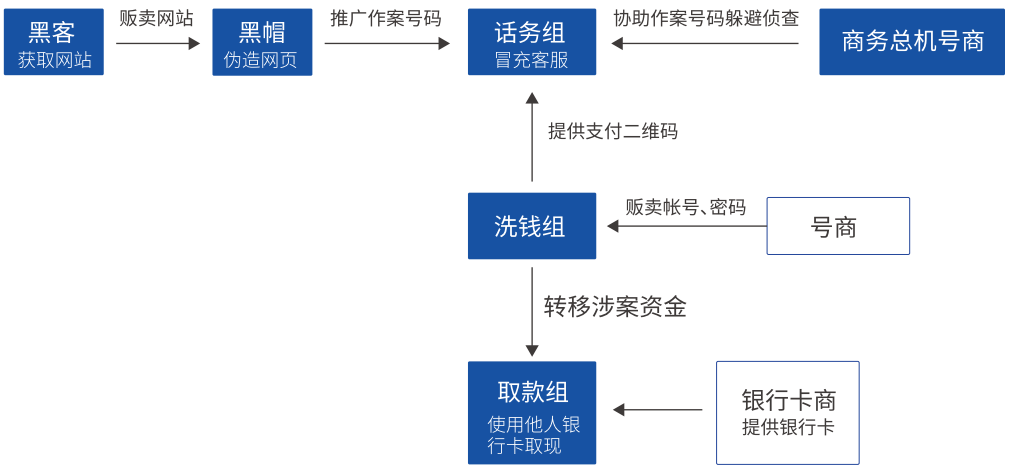
2 图 2 为 2018 年“互联网刑事法制高峰论坛”现场展示“恶意注册产业链”

3 图 3 为问道安全沙龙第四期——聚焦网络虚拟账号的“黑与恶”中，腾讯网络安全与犯罪研究基地首席研究员门美子进行发言

腾讯公司协助打击电信网络诈骗案例

案例一：仿冒诈骗全链条打击

2018 年下半年，某市贷款类诈骗高发，腾讯“守护者计划”安全团队协助警方梳理相关警情时发现：其中一部分被害人通过某类货款 APP 借款，后因急于还钱，上网搜索该 APP 的客服电话咨询还款事宜时，犯罪分子冒充该 APP 客服，要求被害人通过扫描付款二维码交纳保证金，以此骗取被害人钱财。专案组通过进一步深入摸排，发现了团伙内完整的黑灰产业链，并一举将其捣毁。



黑客：主要通过服务器弱口令、数据库注入、获取 weshell 等方式取得大量服务器权限，搜获大批量的低端网站并贩卖；

黑帽 SEO：从黑客端买到大量低端网站，伪造网页，通过增加关键字等方法提高网站的权重，将诈骗团伙需要挂网的号码植入该些已经提高了权重的网页中，使其在搜索网页中排名靠前，提高被害人点击网页、拨打挂网号码的几率；

话务组：通过将作案号码交给黑帽 SEO 进行推广后，便冒充相关 APP 客服进行诈骗；

商务总机号商：为了协助话务组躲避侦查，作了 2 层话务跳转；

洗钱组：主要负责提供收款二维码给话务组，在其得手后第一时间将涉案资金进行转移。同时，还负责美化包装涉案二维码，让其感官上更加接近官方客服；

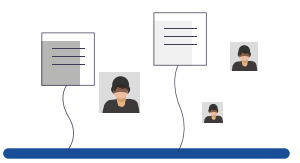
取款组：通过接受上家指示，使用他人银行卡将涉案赃款取现，扣除相应点数后返还给上家；

号商：采取公司化运作，批量获取到大量账号、密码及其他公民个人信息，并在网上进行贩卖；

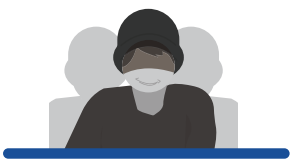
银行卡商：从黑市上买到相关的身份证，然后物色样貌较为相似的人员冒用他人身份到相关营业网点进行开户，随后将银行卡以较高的价格进行贩卖。

案例二：荐股诈骗专项行动

针对荐股类诈骗的高发态势，腾讯“守护者计划”安全团队对荐股类诈骗犯罪手法深入研究，应用大数据分析方法对荐股诈骗团伙线索进行深入挖掘，配合各地警方开展荐股诈骗专项打击，期间向各地公安机关批量输出犯罪团伙线索 200 余条，协助公安机关打掉荐股诈骗团伙 27 个，抓获犯罪嫌疑人 800 余人，有力震慑了实施荐股诈骗的不法分子。



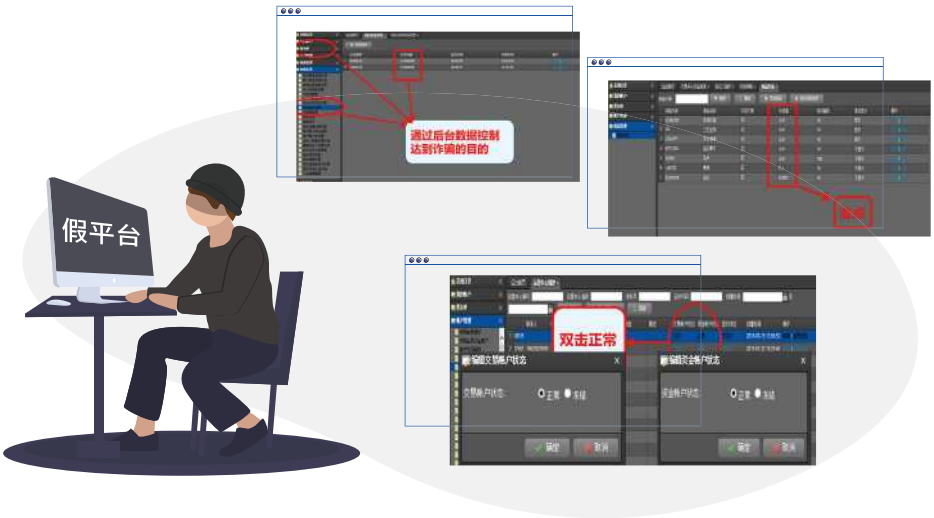
输出犯罪团伙线索**200**余条



打掉荐股诈骗团伙**27**个

抓获犯罪嫌疑人**800**余人

对案件的复盘研究发现，荐股诈骗手法在不断升级。从早期“赌概率”、“炒软件”以骗取高额会员费、软件使用费，逐步向设立“假平台”发展。诈骗团伙通过网络购买 MT4 金融交易平台软件后，对功能数据进行修改或添加，设置各种风控参数，例如延时交易、滑点、卡盘、最大单量限制等，甚至修改 K 线及设置资金冻结等，便于后台控制。搭好假平台后，诈骗团伙雇请推广团伙多渠道推广，利用荐股类话术，以高盈利为诱饵，诱骗客户入金，并在后台实时操纵行情，伪造交易记录，甚至控制被害人的资金流向，诈骗被害人大量资金。

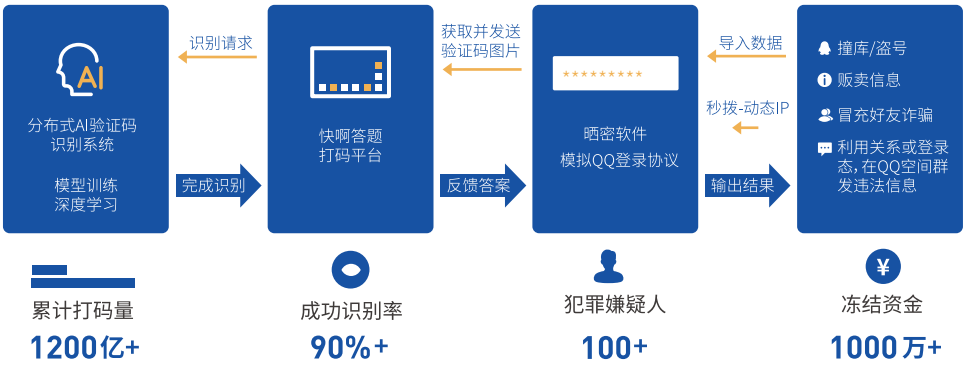


案件三：打码平台系列案

近两年，腾讯“守护者计划”安全团队协助警方，破获全国首例利用 AI 技术从事黑产活动的案件，连续打掉全国最大的两个利用 AI 人工智能神经网络，破解识别字符型验证码的打码平台：“快啊答题”和“光速打码”，并由此挖掘出一条从撞库盗号、破解验证码到贩卖公民信息、实施网络诈骗的全链条黑产。

打码平台系列案首次查获黑产从业人员把 AI 技术运用到了电信网络诈骗的黑产链中，通过撞库、盗号、钓鱼，而后利用打码平台的 AI 技术快速海量的清洗校验黑灰数据，贩卖给下游电信网络诈骗团伙，实施精准诈骗。

黑产分子使用基于神经网络模型的深度学习技术，训练多个验证码图片识别模型，搭建分布式 AI 验证码识别系统，用以毫秒级快速高效海量的识别验证码，识别率很高，基本上洞穿了大多数图片式验证码策略。



四、创建警企联合实验室，发挥大数据防控治理效能

随着电信网络诈骗犯罪手法和技术能力的不断升级，为适应形势变化，腾讯公司积极探索电信网络诈骗“警企协同，联合治理”的创新模式，建立“警企联合实验室”，借助公司大数据分析研究和科技创新优势，在事前感知、事中防控、事后研判等环节协助公安机关提升打击治理效能。

“警企联合实验室”接入了由腾讯安全团队开发的“安全态势感知系统”“鹰眼反电话诈骗系统”“麒麟伪基站定位系统”“神荼网址反诈骗系统”“神羊情报分析平台”“宾果反诈骗防控系统”六大安全应用系统。其中，“安全态势感知”属于事前预警感知；警方在事中需要进行阻断诈骗进程时，则可运用“鹰眼”“神荼”和“麒麟”系统；在事后进行溯源分析时，则使用“神羊”情报分析平台；而“宾果”兼具事前感知预警和事中拦截封堵功能，其主要功能是依托线上警企联动，线下警方预警阻断，降低发案率、抑制诈骗类犯罪的蔓延。六大系统贯穿始终，形成以大数据和人工智能为依托的全链条反电信网络诈骗体系，为警方预警和侦查各种电信网络诈骗案件提供协助。

安全态势感知系统

基于人工智能技术，俯瞰全网安全态势的可视化平台。实现对全局态势、流量攻击、恶意网址、病毒态势、重点网站、仿冒公检法等线索和态势的感知预警。

鹰眼智能反电话诈骗系统

通过对海量脱敏通话话单的大数据分析，在智能引擎的快速模型识别匹配下，实时检测出正在受骗的用户，并且通过和警方或者运营商合作，对受骗用户进行实时劝阻，在第一时间保护用户的财产，甚至人身安全。目前，鹰眼系统已经在全国 20 多个城市落地，累计挽回用户损失超过 10 亿元。

麒麟伪基站定位系统

利用大数据和 LBS 对伪基站进行定位，并从空间、时间维度利用地图直观呈现伪基站的聚类传播区域和实时运动轨迹，帮助警方提高打击伪基站团伙的效率。

神荼网址反诈骗系统

利用大数据分析和机器学习识别并拦截欺诈、钓鱼网址。除此之外，神荼还会对典型的网址诈骗进行线索挖掘，团伙聚集分析，为有关部门的线下打击和抓捕提供协助。

神羊情报分析平台

是基于腾讯安全大数据推出的移动互联网一站式威胁信息分析平台。输入与安全相关的病毒样本、IP、域名、电话号码或邮箱，即能通过智能化的算法直观地量化案情的影响区域、人数和传播态势，高效地追踪案情元素的分发、传播和影响趋势，提高对线索进行追踪溯源、打击犯罪的效率。

宾果反诈骗防控系统

腾讯联合公安部刑侦局研发的智能识别网络诈骗产品。其运用 AI 人工智能技术和机器学习原理，针对诈骗高危区域的窝点及仿冒公检法、贷款诈骗、刷单诈骗、冒熟诈骗、退款诈骗等多种诈骗手法进行建模分析，通过事前感知预警、事中策略拦截封堵、线下重点打击等手段，有效保护用户上网安全，降低群众遭遇诈骗的风险。自宾果反诈骗防控系统投入使用以来，全国重点诈骗区域诈骗号码大幅下降降幅接近 70%；每月向各地公安机关预警超过 1 万起诈骗，及时挽回人民群众损失。

目前，上海、深圳、浙江、北京的“警企联合实验室”已相继建成，形成跨越南北的防控打击矩阵。未来，该实验室矩阵将会相互呼应，进一步发挥腾讯安全能力优势，带动华南、华东、华北地区乃至全国，助力公安机关开创针对电信网络诈骗乃至全链条黑灰产的打击治理新局面。

图为 2017 年 11 月 21 日，腾讯联手上海市反电信网络诈骗中心正式成立“腾讯上海反电信网络诈骗联合实验室”

图为 2018 年 5 月 14 日，腾讯与浙江省公安厅签订《战略合作框架协议》，共建“腾讯浙江安全联合实验室”

五、普及网络安全知识，提高全民防骗意识

（一）运营公众号线上宣传矩阵

以“守护者计划”“微信安全中心”“腾讯 110”“腾讯网络安全与犯罪研究基地”“微信 110”等多个公众号、小程序、网站为运营宣传教育载体，分别设立常规化品牌运营栏目，提供骗局揭露、辟谣、热点安全资讯、微信安全使用技巧、安全打击事件、法律适用研究等教育内容，同时还提供各种账号基础安全功能，如找回账号密码、解封、冻结、解冻、投诉账号等。

腾讯 110（含腾讯 110 官网、小程序、公众号）：更新教育文章内容 148 篇，阅读总量累计达 1236 万。

“微信安全中心”“微信 110”公众号：发布及转载反欺诈类打击公告、教育漫画、视频、文章共 46 篇，阅读总量超过 218 万，以丰富多样的形式传达安全理念，帮助用户进行安全知识储备，以便更好地规避安全风险。

“守护者计划”公众号：发布文章 152 篇，阅读量超过 87 万，第一时间分享新型网络骗局，带用户及时了解反欺诈攻略。

“腾讯网络安全与犯罪研究基地”公众号：发布文章 109 篇，阅读量超过 31 万。塑造亲切的、有趣、专业的公众号人物化形象“鹅师傅”，连接警方、法律专业人士以及关心网络安全的公众用户。

（二）开展“守护者计划”公益行动

为进一步普及防骗知识，切实提高公众的反诈骗安全意识，鼓励更多用户参与到防治新型网络违法犯罪的行动中。自 2016 年以来，每年暑期，腾讯公司都在政府部门指导下，联合互联网企业和社会知名人士，共同开展“守护者计划”公益行动。

2016-2018 年连续三年 7-8 月，分别围绕“反电信网络诈骗”“保护公民个人信息”“防范网络传销”等不同主题开展公益教育活动，内容包括拍摄用户教育视频、走进社区和高校开展网络安全课程、展示公益宣传海报等，均取得了很好的效果。每年的“守护者计划”公益行动，线上、线下的参与人数均超过 2 亿人次。

2016 年“守护者计划”公益行动

2017 年“守护者计划”公益行动

2018 年“守护者计划”公益行动海报

（三）针对垂直人群精耕细作

针对不同的受众群体的上网安全，腾讯“守护者计划”安全团队将教育的内容进行定制化开发。

针对未成年人群体的“企鹅伴成长”项目，向未成年人普及“远离不良信息”“提防网络诈骗”“保护个人信息”等方面的知识；

“企鹅伴成长”网络安全课

针对中老年群体的“安知课堂”项目，向中老年人传递“识别网络诈骗”“识别网络传销”“识别网络谣言”等安全知识。

安知课堂

针对大学生群体的“思享计划”项目，为大学生群体提供拒绝网络传销、保护个人信息、保护国家安全等方面的知识。

“思享计划”——腾讯安全课进校园

（四）发布“微反诈”小程序

为增强用户反诈意识、揭秘各类诈骗手法、及时获取风险预警，2019 年，腾讯公司正式发布 " 微反诈 " 小程序。“微反诈”小程序是腾讯公司为广大用户提供的一整套反诈自助小工具，用户可以通过小程序的搜索功能，便捷查询诈骗手法、网址和手机号等，快速识别欺诈信息等，不断修炼自己的反诈 " 功力 "。同时，它还嵌入到“腾讯 110”“守护者计划”等小程序，使用户可以一键举报欺诈信息，更加方便用户使用。其主要功能如下：

1. 欺诈信息搜索

该功能提供诈骗类型、可疑金融 / 传销平台、网址以及手机号等的安全信息查询。腾讯 110 团队会根据用户举报及时更新诈骗类型，目前已提供 11 个大类、134 个小类的诈骗形式供广大用户搜索了解。

2. 诈骗雷达分布图

包含全国各省 top6 举报诈骗类型，让大家实时了解用户举报的欺诈态势。点击诈骗类型（如：兼职诈骗），即可查看了解相关诈骗类型的手法解析及防骗案例。

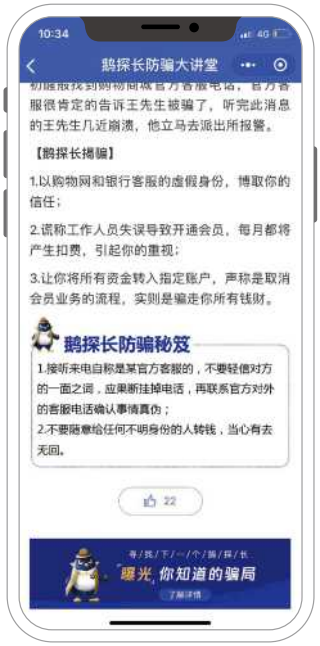
3. 反诈警示

与各地检察、公安机关建立合作预警、通告机制，第一时间预警区域性高发、新型的诈骗类型，破获案件后的被害人权利义务告知书提醒广大用户避免上当受骗，被骗后及时挽回损失。同时基于系统识别和平台举报大数据能力，对当前热门欺诈态势及最新诈骗手法进行预警通告。

4. 防骗案例

该模块以“鹅探长防骗大讲堂”专栏模式，结合用户真实举报案例，持续更新全网最新、最热门的诈骗手法解析，内容覆盖交易诈骗、兼职诈骗、交友诈骗等，帮助用户了解防骗套路，提高防范意识。


10:31
微反诈行动
全国
交易诈骗
仿冒诈骗
兼职诈骗
金融信用
交友诈骗
盗号诈骗
交易诈骗
兼职诈骗
交友诈骗
反诈警示
湖南长沙公安关于投资诈骗的紧...
花5万余元只为取消“铂金会员”，代价太大
网络兼职—永远都刷不完的单
算卦赠特殊服务，真是活久见
我要举报


10:34
鹅探长防骗大讲堂
的王先生几近崩溃，他立马去派出所报警。
【鹅探长揭骗】
1.以购物网和银行客服的虚假身份，博取你的信任；
2.谎称工作人员失误导致开通会员，每月都将产生扣费，引起你的重视；
3.让你将所有资金转入指定账户，声称是取消会员业务的流程，实则是骗走你所有钱财。
鹅探长防骗秘笈
1.接听来电自称是某官方客服的，不要轻信对方的一面之词，应果断挂掉电话，再联系官方对外的客服电话确认事情真伪；
2.不要随意给任何不明身份的人转钱，当心有去无回。
22
曝光，你知道的骗局

第四章

提升电信网络诈骗综合防治实效的建议

第四章 提升电信网络诈骗综合防治实效的建议

一、不断完善技术策略，加固安全防护屏障

面对快速变更和不断迭代的互联网诈骗现状，和不法分子作案呈跨境化、产业化、链条化及多种黑产相互勾连聚集的特点，互联网服务提供者惟有不断更新安全治理工具和完善技术策略，做好长期持续对抗的准备。

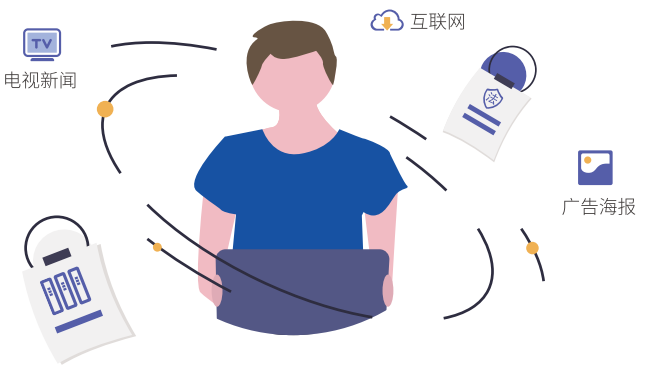
一是互联网服务提供者要不断研究升级搜索、电商、社交、内容等平台的反欺诈治理工具，强化涉欺诈内容在链接跳转、关联搜索、广告植入、用户信息共享等方面的审查功能，推动建立互联网信息审查处置机制，依法拦截、屏蔽不法内容并及时清理，积极消除安全隐患。加大安全建设投入，提高安全技术水平与风险防控能力，如加密技术的研发、防御机制的完善、大数据运算能力的升级等，从而有效阻断电信网络诈骗的链路。

二是结合反欺诈对抗实践经验，建立针对不同手法的反欺诈治理体系，及时验证、更新、发布最新特征模型与对抗策略。提高“事前”止骗命中率，同时也为“事中”和“事后”用户权益的维护、不法分子的打击处置，提供高效可靠的解决方案。

二、创新普法宣传形式，加强网络安全教育

如今的电信网络诈骗手法时常翻新，有些甚至利用高科技智能化手段，部分公众受个体知识和经验的局限，往往防不胜防。因此，从根本上加强电信诈骗犯罪的预防及治理，迫切需要提高全社会的识骗、防骗与依法维权的意识和技能。

一是广泛宣传，强化预警效果。譬如，公安、通讯、金融、互联网企业等机构在发现新型诈骗手法后，可通过互联网、电视新闻、广告海报等渠道，向公众及时宣传警示；司法机关、行政管理部门、消费者权益保护协会等，也可通过不定期地宣传典型案例，开展普法教育。



为提高宣传普及性和覆盖率，可在宣传形式上贴近用户，不断创新。如腾讯“微反诈”小程序，集案件动态统计、反诈警示、案例宣传和举报入口于一体，为用户提供一站式综合安全服务，有助于充分发挥大数据优势，强化宣传引导效果，提高全民参与度，帮助群众提升防骗意识与防骗能力。

二是引导社会公众提升个人信息保护意识和依法维权意识，注重个人信息安全的保护。无论工作还是生活，对个人信息尤其敏感信息，应时刻保持警惕，全方位守护个人信息安全。同时还要懂得善于运用法律武器维护自身合法权益，最大限度地避免或减少个人财产损失，遭受诈骗后应及时寻求法律救济。

三、完善法律规制方案，加大源头黑产治理

当前，应对电信网络诈骗，部分法律规制的障碍与不力也成为掣肘打击效果的重要因素之一。众所周知，电信网络诈骗等犯罪具有链条长、分工细化的特点，加之近年来跨境趋势明显，电信网络诈骗的治理受到管辖因素、刑事国际司法协助因素、取证固证因素、当地执法配合程度及执法水平、出境抓捕成本大等因素交叉影响，全链条打击困难突出、成本巨大、收效较慢。另一方面，电信网络诈骗的上游行为，如为诈骗提供互联网账号、提供透传工具、提供支付结算账号等行为，成为下游犯罪的源头之恶，危害性巨大，但在下游诈骗正犯未能到案实现全链条打击的情况下，对这部分行为实施打击又十分困难，客观造成了上游黑产泛滥发展，为下游“源源不断”提供助力的现状。

在此情况下，为了解决全链条打击的困境，实现对网络犯罪“打早打小”的初衷，刑法修正案（九）增加了非法利用信息网络罪和帮助信息网络犯罪活动罪，希望借此优化司法实践中对于电信网络诈骗等行为的上游和帮助行为的打击治理。然而，上述罪名自 2015 年开始适用至今，总体适用数量不多，且司法实践中争议较大，主要体现在：

一是没有明确追诉标准，各地把握不一致；

二是与共同犯罪的区分不清晰，判断标准不统一，导致适用混乱；

三是在网络犯罪非接触性特点普遍的情况下，关于行为人“明知”的主观要素证明困难。

基于以上，我们建议公安司法机关通过完善相关立法、出台司法解释、发布指导案例等方式，明确法律适用方法，进一步明确对网络诈骗上游行为及帮助行为的法律规制方案，加大对源头黑产问题（包括侵犯公民个人信息、提供黑产专门工具、提供恶意注册账号等）的打击治理，彻底斩断网络诈骗产业链条的各个环节。

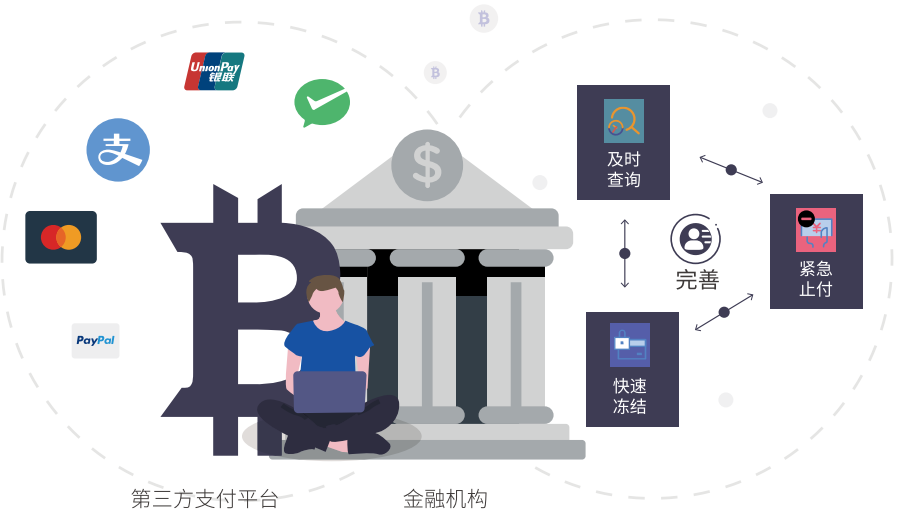
四、多行业多领域协同，加深合作优化实效

网络安全问题不能只靠政府部门，更需要社会各界和各个行业共同努力，联手共治。通讯、网络和资金是电信网络诈骗三个重要的环节，因此，通讯运营商、互联网企业和金融机构在有关部门指导下加强合作，是健全完善打击治理长效工作机制的重中之重。

譬如，通信管理部门和运营企业，可从切实加强手机号码管理入手，进一步强化用户实名管理制度，

杜绝非实名“黑号”成为诈骗工具。同时，在信息流快速查询反馈、诈骗电话拦截阻断和快速通报关停等方面，为侦查办案提供便利，及时、有效切断电信网络诈骗信息流。

再如，互联网企业可发挥技术优势，主动在线索发掘、案件协查、跨境合作等方面助力侦查机关强化打击实效。在针对部分犯罪行为利用第三方支付平台进行支付结算的情形，主动完善风控及协作机制，协助办案部门发现、识别和阻断用于诈骗的可疑资金流转。



又如金融机构在理顺涉案资金环节，对即时查询、紧急止付、快速冻结工作机制等方面进一步健全完善，提供高效服务，实现以快制快，对流转于银行间的诈骗赃款及早发现、及早冻结，进一步提高涉案资金的查控效率。

由此我们也建议，社会各方，加深互信、互通，主动破除合作壁垒，调动各方优势资源及技术能力，共同打击和防范电信网络诈骗。面对跨平台诈骗犯罪，各方共同更新治理策略和强化治理方案，有效打击更为复杂的电信网络诈骗，携手为清朗互联网环境贡献力量。

五、呼吁用户积极参与，加入“反诈行动派”

新的预防与发现技术，新的抵御与打击模式，对电信网络诈骗形成了一定的遏制作用，但同时诈骗行为人的作案意识与手法也在不断升级。新形势下，需要推动反诈工作从初步联合进一步升级到全民行动。

据中国互联网络信息中心第 43 次《中国互联网络发展状况统计报告》显示，至 2018 年底，我国网民总数达 8.29 亿，其中手机网民 8.17 亿，全年新增手机网民 6433 万。随着互联网覆盖范围的进一步扩大，全民参与已成为当前打击治理电信网络诈骗的关键。

我们知道，无论是通过诈骗电话、短信，还是钓鱼网址、外挂软件等，只要犯罪分子实施诈骗行为，必然会留下作案痕迹，而这些“痕迹”都将成为大数据的一部分。数据越多，数据分析技术越强，对于电信网络诈骗的预防、发现和打击越精准有效。在“人人都可能是亲历者”的情况下，具有针对性的安全大数据的快速累积、更新，可以持续优化反诈产品后台技术的学习能力，使新生的诈骗类型在早期就得到遏制。

这不仅要求公安机关、金融机构、通讯运营商和互联网企业要形成合力，更需要每一位用户都积极参与其中。对诈骗电话、短信、网址等信息的随手标记，对诈骗行为的及时举报，对诈骗现象的主动咨询，都有助于完善反诈骗安全数据库，壮大全社会反诈骗的行动力量。一己之力也许微小，但若每个人都能参与其中，每一次标记的数据就是亿级的，这些数据将发挥更多价值，反诈骗行动将会更加有效。

联合打击模式协助破获了诸多大案要案，能够治标；全民参与、切实行动，才能治本。面对席卷全民的电信网络诈骗，所有人都应有意识地提高警惕，主动学习法律知识，积极举报诈骗线索、配合执法打击，不懈地向亲友宣传引导。无论是出于对社会的责任之义，还是出于对家人的守护之心，每个人都需要做一个“行动派”，共同加入反电信网络诈骗的队伍中来。

结 语

腾讯公司始终以守护用户利益、维护网络空间清朗环境为己任，切实履行企业义务，积极承担社会责任，发挥自身优势，打造专业队伍，构建科学防治体系，并在司法机关与政府有关部门的指导下，不断完善、提高治理水平。

未来，腾讯将继续与政府、司法机关、行业、公众共同努力，共筑反电信网络诈骗坚固防线，坚决守护用户安全和互联网清朗环境！


Tencent 腾讯