2019 年第三季度
中国手机安全状况报告

360手机卫士

360互联网安全中心

2019 年 11 月 28 日

摘要

恶意程序：

- 2019年第三季度，360互联网安全中心共截获安卓平台新增恶意程序样本约36.5万个，平均每天截获新增手机恶意程序样本约0.4万个。360手机卫士累计为全国手机用户拦截恶意程序攻击约2.4亿次，平均每天拦截手机恶意程序攻击约260.2万次。
- 2019年第三季度，安卓平台新增恶意程序类型主要为资费消耗，占比高达66.5%；其次为隐私窃取（17.9%）、远程控制（10.6%）、流氓行为（3.9%）、恶意扣费（1.1%）。
- 从省级分布来看，2019 年第三季度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10.1%；其次为山东（8.0%）、江苏（7.1%）、河南（6.6%）、浙江（5.9%）等。
- 从城市分布来看，2019 年第三季度遭受手机恶意程序攻击最多的城市为北京市，占全国拦截量的2.3%；其次为上海（2.1%）、重庆（2.0%）、广州（2.0%）、成都（1.9%）等。

钓鱼网站：

- 2019年第三季度，360互联网安全中心在PC端与移动端共为全国用户拦截钓鱼网站攻击约217.9亿次。其中，PC端拦截量约为212.6亿次，占总拦截量的97.6%，平均每日拦截量约2.3亿次；移动端拦截量约为5.3亿次，占总拦截量的2.4%，平均每日拦截量约577.3万次。
- 2019年第三季度，移动端拦截钓鱼网站类型主要为境外彩票，占比高达83.1%；其次为网站被黑（9.2%）、假药（3.0%）、虚假购物（2.0%）、虚假中奖（1.2%）、金融证券（1.1%）等。
- 从省级分布来看，2019 年第三季度移动端拦截钓鱼网站最多的地区为广东省，占全国拦截量的36.8%；其次为广西（13.3%）、山东（8.0%）、四川（5.1%）、北京（3.1%）等。
- 从城市分布来看，2019 年第三季度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 5.2%；其次为深圳（3.9%）、东莞（3.1%）、泉州（2.7%）、杭州（2.3%）等。
- 2019年第三季度，360互联网安全中心共截获各类新增钓鱼网站1050.0万个，平均每天新增11.4万个。观察钓鱼网站新增类型，境外彩票类占比为78.6&，居于首位。
- 从新增钓鱼网站的服务器地域分布看，77.9%的钓鱼网站服务器位于国外，22.1%的钓鱼网站服务器位于国内。其中，国内服务器位于广东的占比为19%，居于首位；其次为北京（14%）、河北（11.1%）、湖北（10.0%）、浙江（9.0%）等。

骚扰电话：

- 2019年第三季度，用户通过360手机卫士标记各类骚扰号码（包括360手机卫士自动检出的响一声电话）约1487.5万个，平均每天标记约16.2万个；从拦截量上看，360手机卫士共为全国用户识别和拦截各类骚扰电话约43.2亿次，平均每天识别和拦截骚扰电话约0.4亿次。
- 从骚扰电话标记类型来看，响一声以57.8%的比例位居首位；其次为广告推销（15.2%）、骚扰电话（8.3%）、疑似欺诈（6.6%）、房产中介（5.7%）、保险理财（4.3%）、招聘猎头（1.9%）、诈骗电话（0.1%）。
- 从骚扰电话拦截类型来看，广告推销以36.4%的比例位居首位；其次为骚扰电话（32.4%）、疑似欺诈（20.3%）、房产中介（8.1%）、保险理财（1.2%）、响一声（1.1%）、招聘猎头（0.3%）与教育培训（0.1%）。
- 2019年第三季度，从骚扰电话拦截号码的号源分布看，被拦截的固定电话最多，占比高达31.5%；其次为运营商为中国移动的个人手机号（21.1%）、运营商为中国联通的个人手机号（20.0%）、95/96开头号段（14.4%）、运营商为中国电信的个人手机号（9.5%）、虚拟运营商（2.8%）与400/800开头号段（0.8%）。
- 从省级分布来看，2019年第三季度广东省用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的11.0%；其次是山东（7.0%）、河南（5.9%）、江苏（5.8%）、四川（5.3%）等。
- 从城市分布来看，2019年第三季度北京市用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的5.0%；其次是上海（3.9%）、广州（3.3%）、深圳（2.2%）、重庆（1.9%）等。
- 从省级分布来看，2019年第三季度广东省用户接到骚扰电话最多，占全国骚扰电话拦截量的12.5%；其次是山东（7.0%）、江苏（6.5%）、浙江（5.7%）、河南（5.7%）等。
- 从城市分布来看，2019年第三季度北京市用户接到的骚扰电话最多，占全国骚扰电话拦截量的3.6%；其次是上海（3.2%）、广州（3.2%）、成都（2.2%）、深圳（2.1%）等。

垃圾短信：

- 2019年第三季度，360手机卫士共为全国用户拦截各类垃圾短信约25.9亿条，平均每日拦截垃圾短信约2823.2万条。
- 2019年第三季度，垃圾短信的类型分布中广告短信最多，占比为95.6%；诈骗短信占比

3.7%；违法短信占比0.6%。

- 2019年第三季度，从垃圾短信发送者号码的运营商号源分布看，利用1065/1069渠道号段发送垃圾短信的最多，占比高达89.2%；其次为中国电信（2.7%）与中国联通（2.7%）。
- 从省级分布来看，2019年第三季度广东省用户收到的垃圾短信最多，占全国垃圾短信拦截量的4.2%；其次是山东（1.7%）、江苏（1.7%）、浙江（1.7%）、河南（1.5%）等。
- 从城市分布来看，2019年第三季度广州市用户收到的垃圾短信最多，占全国垃圾短信拦截量的4.9%；其次是北京（3.4%）、深圳（2.6%）、南京（2.2%）、上海（2.0%）等。

网络诈骗：

- 2019年第三季度，360手机先赔共接到手机诈骗举报667起；其中诈骗申请为414起，涉案总金额高达462.3万元，人均损失11167元。
- 在所有诈骗申请中，金融理财占比最高，为27.5%；其次是身份冒充（17.9%）、虚假兼职（15.0%）、赌博博彩（14.3%）、虚假购物（4.8%）等。
- 从涉案总金额来看，金融理财类诈骗总金额最高，达178.8万元，占比38.7%；其次是赌博博彩诈骗，涉案总金额120.5万元，占比26.1%；身份冒充诈骗排第三，涉案总金额为77.0万元，占比16.6%。
- 从人均损失来看，赌博博彩诈骗人均损失最高，为20423元；其次是金融理财诈骗为15683元，信用卡诈骗为12425元。
- 从举报用户的性别差异来看，男性受害者占58.0%，女性占42.0%，男性受害者占比高于女性；从人均损失来看，男性为10158元，女性为13717元。
- 从被骗网民的年龄段上看，90后的手机诈骗受害者占所有受害者总数的36.3%；其次是80后占比为28.5%；00后占比为21.0%；70后占比为8.3%；60后占比为4.7%；其他年龄段占比为1.3%。
- 从用户举报情况来看，广东（11.6%）、山东（8.5%）、河北（7.2%）、河南（5.8%）、广西（5.3%）这5个地区的被骗用户最多。
- 从用户举报情况来看，深圳（2.4%）、上海（2.4%）、武汉（2.2%）、广州（2.2%）、重庆（1.9%）这5个城市的被骗用户最多。

关键词：恶意程序、钓鱼网站、骚扰电话、垃圾短信、网络诈骗

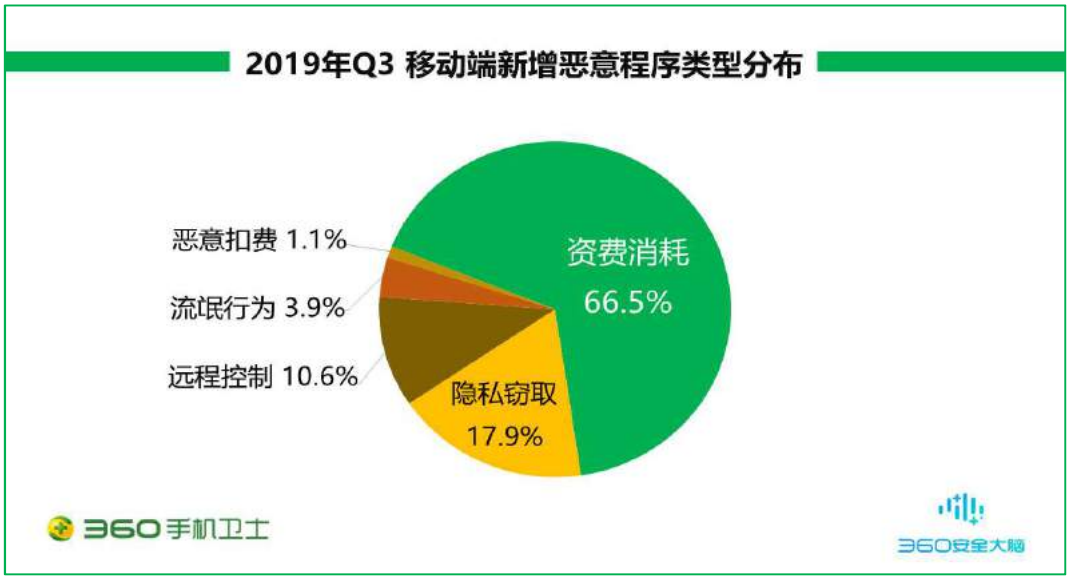
目录

第一章 恶意程序

一、 恶意程序新增样本量与类型分布

2019 年第三季度，360 互联网安全中心共截获安卓平台新增恶意程序样本约 36.5 万个，环比 2019 年第二季度（35.4 万个）增加了 1.1 万个，平均每天截获新增手机恶意程序样本约 0.4 万个。360 手机卫士累计为全国手机用户拦截恶意程序攻击约 2.4 亿次，环比 2019 年第二季度（1.1 亿次）上升了 54.1%，平均每天拦截手机恶意程序攻击约 260.2 万次。下图给出了 2019 年第三季度移动端恶意程序新增量与拦截量统计：

2019 年第三季度，安卓平台新增恶意程序类型主要为资费消耗，占比高达 66.5%；其次为隐私窃取（17.9%）、远程控制（10.6%）、流氓行为（3.9%）、恶意扣费（1.1%）。具体分布如下图所示：



二、 恶意程序拦截量地域分布

2019 年第三季度从省级分布来看，遭受手机恶意程序攻击最多的地区为广东省，占全国拦截量的 10.1%；其次为山东（8.0%）、江苏（7.1%）、河南（6.6%）、浙江（5.9%），此外河北、四川、安徽、湖南、辽宁的恶意程序拦截量也排在前列。

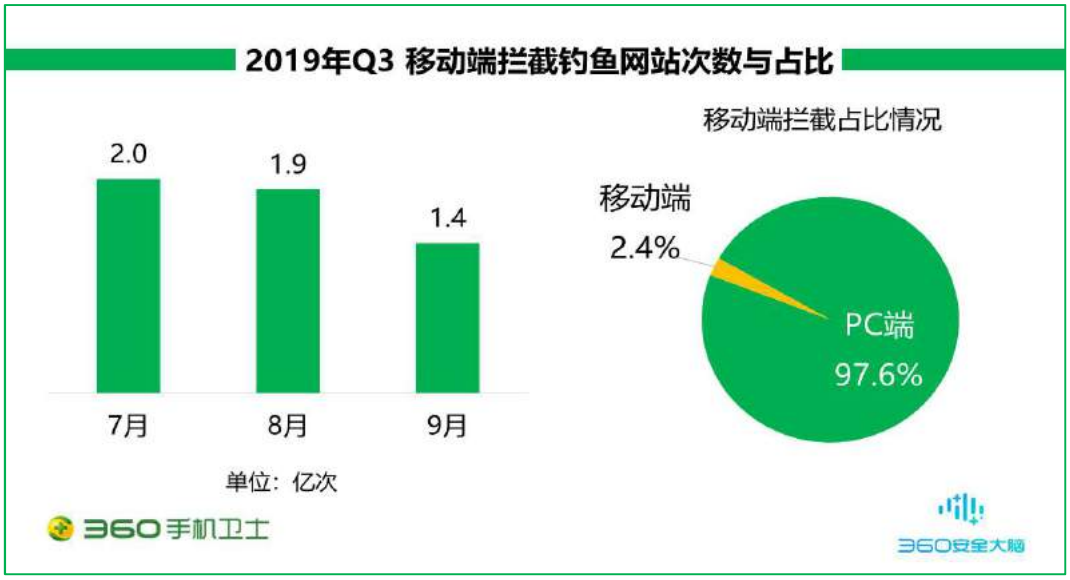
从城市分布来看，遭受手机恶意程序攻击最多的城市为北京市，占全国拦截量的 2.3%；其次为上海（2.1%）、重庆（2.0%）、广州（2.0%）、成都（1.9%），此外深圳、东莞、苏州、郑州、天津的恶意程序拦截量也排在前列。


2019年Q3 恶意程序拦截量TOP10城市分布
2.3%
2.1%
2.0%
2.0%
1.9%
1.6%
1.3%
1.3%
1.2%
1.1%
北京
上海
重庆
广州
成都
深圳
东莞
苏州
郑州
天津
360手机卫士
360安全大脑

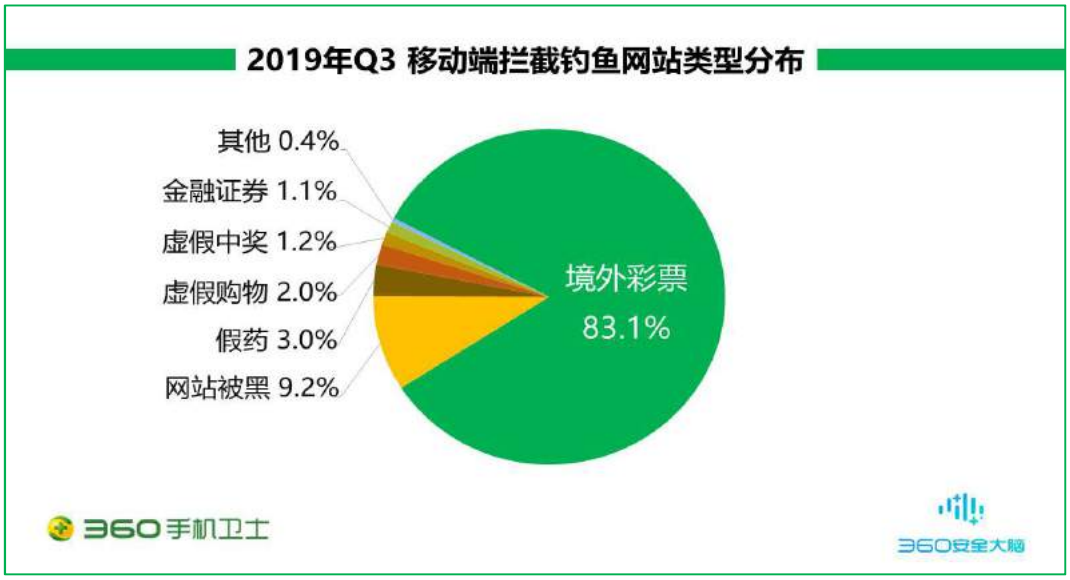
第二章　钓鱼网站

一、 移动端钓鱼网站拦截量及类型

2019 年第三季度，360 互联网安全中心在 PC 端与移动端共为全国用户拦截钓鱼网站攻击约 217.9 亿次，环比 2019 年第二季度（183.2 亿次）上升了 15.9%。其中，PC 端拦截量约为 212.6 亿次，占总拦截量的 97.6%，平均每日拦截量约 2.3 亿次；移动端拦截量约为 5.3 亿次，占总拦截量的 2.4%，平均每日拦截量约 577.3 万次。移动端钓鱼网站拦截次数及占比具体见下图：



移动端拦截钓鱼网站类型主要为境外彩票，占比高达 83.1%；其次为网站被黑（9.2%）、假药（3.0%）、虚假购物（2.0%）、虚假中奖（1.2%）、金融证券（1.1%）等。具体分布如下图所示：



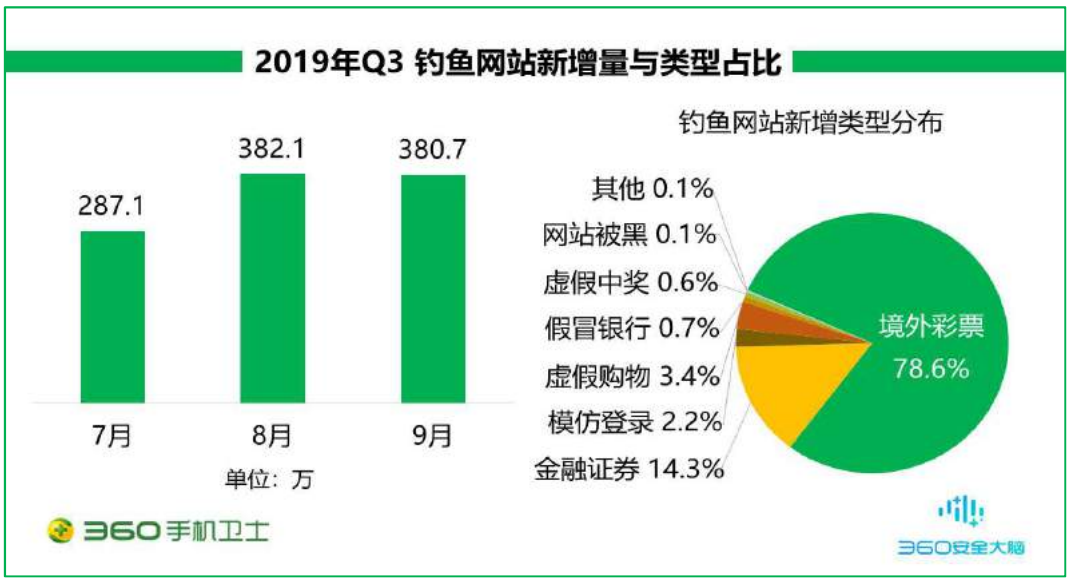
二、 移动端钓鱼网站拦截量地域分布

2019 年第三季度从省级分布来看，移动端拦截钓鱼网站最多的地区为广东省，占全国拦截量的 36.8%；其次为广西（13.3%）、山东（8.0%）、四川（5.1%）、北京（3.1%），此外安徽、山西、福建、上海、云南的钓鱼网站拦截量也排在前列。

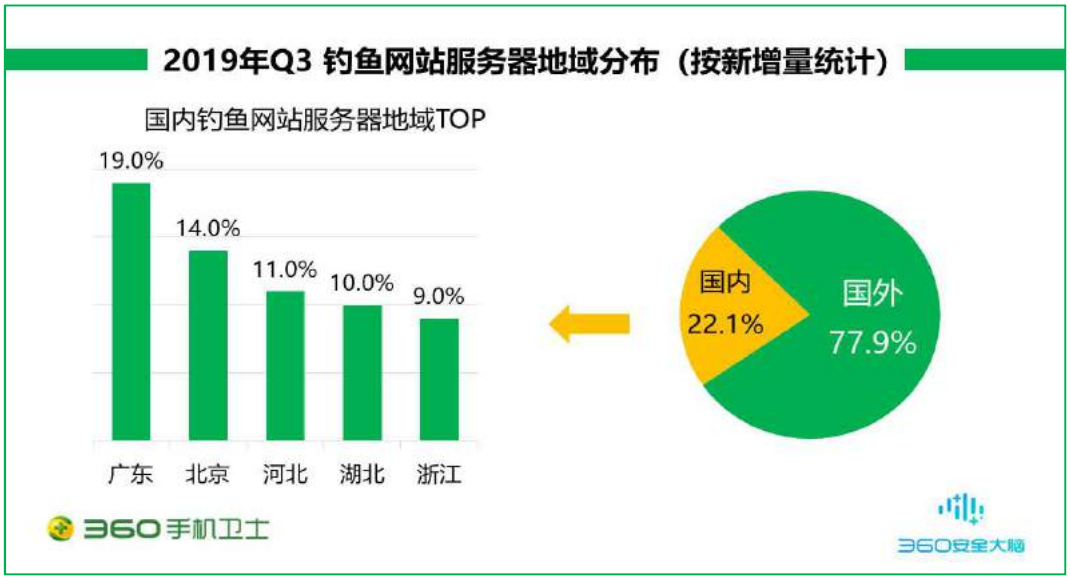
从城市分布来看，移动端拦截钓鱼网站最多的城市为广州市，占全国拦截量的 5.2%；其次为深圳（3.9%）、东莞（3.1%）、泉州（2.7%）、杭州（2.3%），此外南宁、石家庄、福州、佛山、成都的钓鱼网站拦截量也排在前列。

三、 钓鱼网站新增量与服务器地域分布

2019 年第三季度，360 互联网安全中心共截获各类新增钓鱼网站 1050.0 万个，环比 2019 年第二季度（493.7 万个）上升了 53.0%，平均每天新增 11.4 万个。观察钓鱼网站新增类型，境外彩票类占比最高，属于新增钓鱼网站中的重点打击类型。



从新增钓鱼网站的服务器地域分布看，77.9%的钓鱼网站服务器位于国外，22.1%的钓鱼网站服务器位于国内。其中，国内服务器位于广东的占比为 19%，居于首位；其次为北京（14%）、河北（11.1%）、湖北（10.0%）、浙江（9.0%）等。

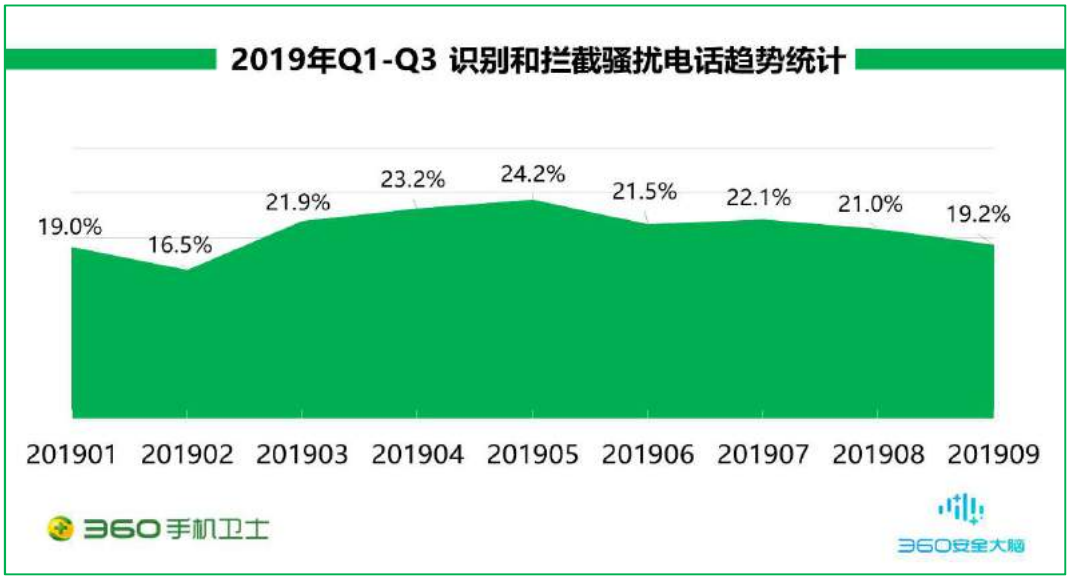

2019年Q3 钓鱼网站服务器地域分布（按新增量统计）
国内钓鱼网站服务器地域TOP
19.0%
14.0%
11.0%
10.0%
9.0%
广东
北京
河北
湖北
浙江
国内
22.1%
国外
77.9%
360手机卫士
360安全大脑

第三章　骚扰电话

一、 骚扰电话标记数与拦截量

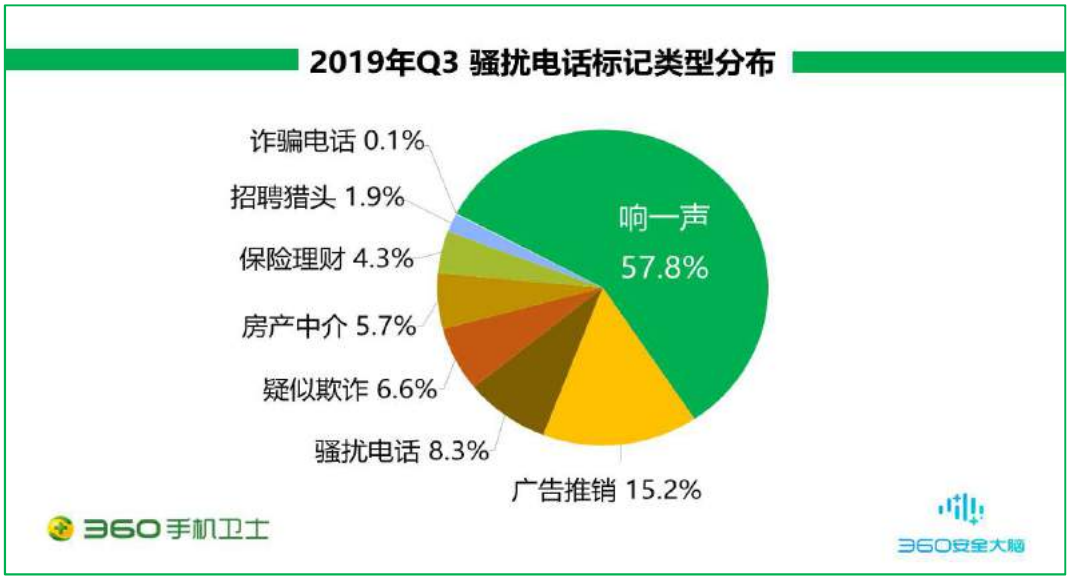
2019 年第三季度，用户通过 360 手机卫士标记各类骚扰号码（包括 360 手机卫士自动检出的响一声电话）约 1487.5 万个，平均每天标记约 16.2 万个。从标记号码总量上看，环比 2019 年第二季度（2010.7 个）下降了 26.0%。从拦截量上看，360 手机卫士共为全国用户识别和拦截各类骚扰电话约 43.2 亿次，平均每天识别和拦截骚扰电话约 0.4 亿次。

从下图 2019 年前三季度 360 手机卫士识别和拦截骚扰电话趋势可见：2019 年 2 月份期间正值春节假期，骚扰电话拦截量最低。通过往年趋势可知，在春节期间，从事拨打骚扰电话的人员减少，从而导致骚扰电话的呼入量降低。2019 年 3 月份起，骚扰电话拦截量回升，并呈持续小幅增长态势。自 2019 年 6 月份起，骚扰电话拦截量回落，并持续呈下降趋势。

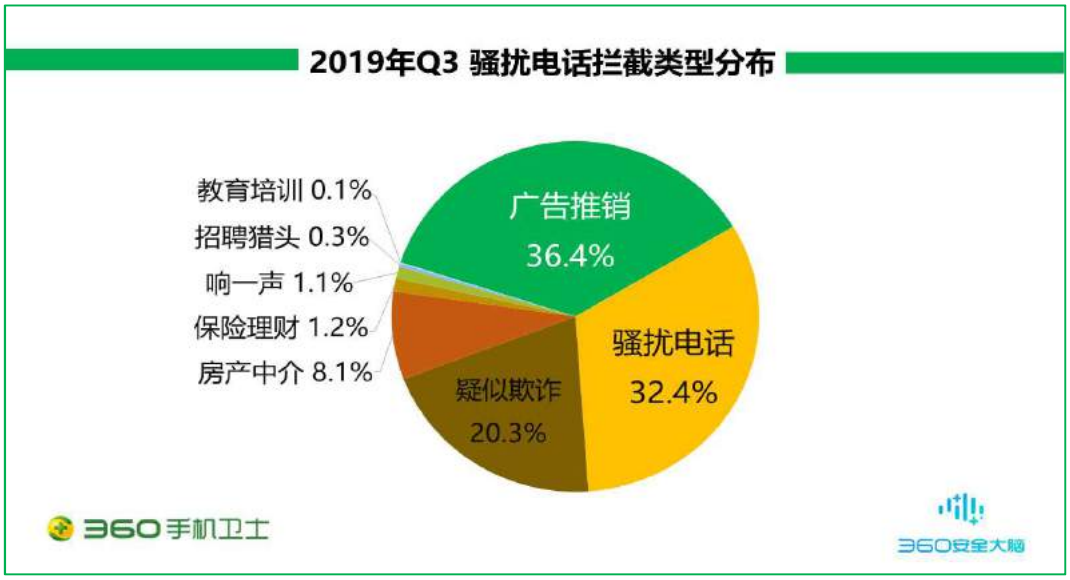


二、 骚扰电话类型分布

综合 360 互联网安全中心 2019 年第三季度的拦截监测情况及用户调研分析，从骚扰电话标记类型来看，响一声以 57.8%的比例位居首位；其次为广告推销（15.2%）、骚扰电话（8.3%）、疑似欺诈（6.6%）、房产中介（5.7%）、保险理财（4.3%）、招聘猎头（1.9%）、诈骗电话（0.1%）。具体分布如下图所示：

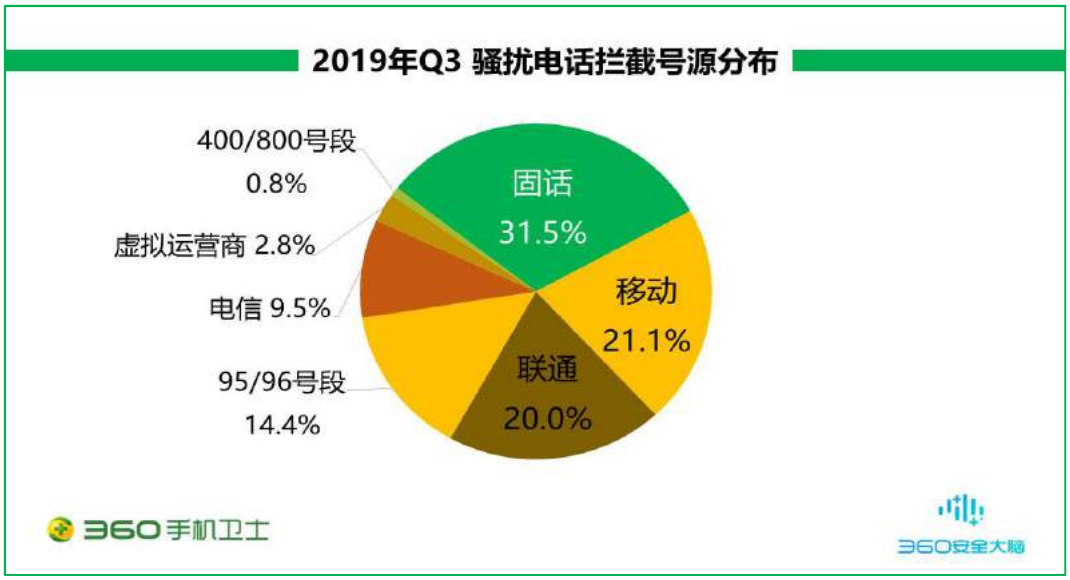


从骚扰电话拦截类型来看，广告推销以 36.4%的比例位居首位；其次为骚扰电话（32.4%）、疑似欺诈（20.3%）、房产中介（8.1%）、保险理财（1.2%）、响一声（1.1%）、招聘猎头（0.3%）与教育培训（0.1%）。具体分布如下图所示：



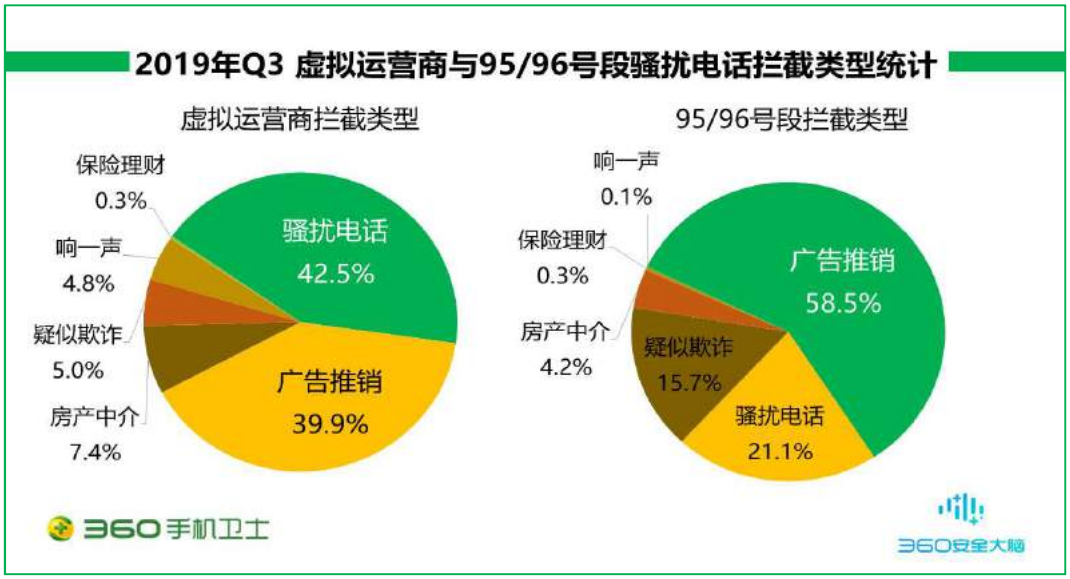
三、 骚扰电话拦截号源分布

2019 年第三季度，从骚扰电话拦截号码的号源分布看，被拦截的固定电话最多，占比高达 31.5%；其次为运营商为中国移动的个人手机号（21.1%）、运营商为中国联通的个人手机号（20.0%）、95/96 开头号段（14.4%）、运营商为中国电信的个人手机号（9.5%）、虚拟运营商（2.8%）与 400/800 开头号段（0.8%）。



近几年，“手机用户实名登记制度”的实施，从源头上遏制了骚扰、诈骗等通信犯罪的实施，增加了不法从业者实施手法的成本。通过对骚扰电话号源分布的统计，发现不法从业

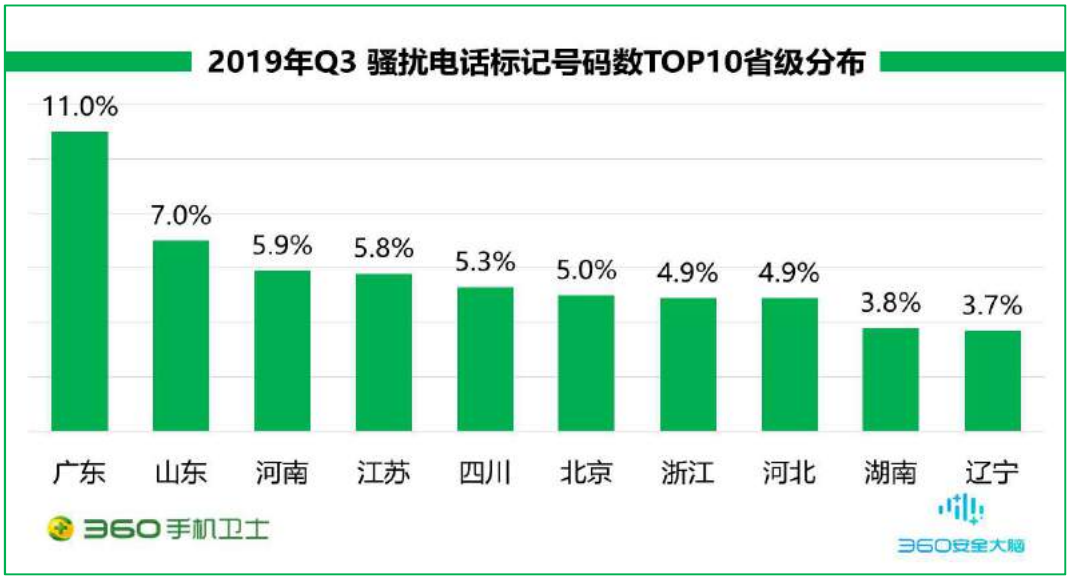
者利用虚拟运营商号码与 96/96 号段从事非法行径的数量激增，频频爆出诈骗成功案件。以下针对 2019 年第三季度虚拟运营商与 96/96 号段与骚扰电话类型进行统计：



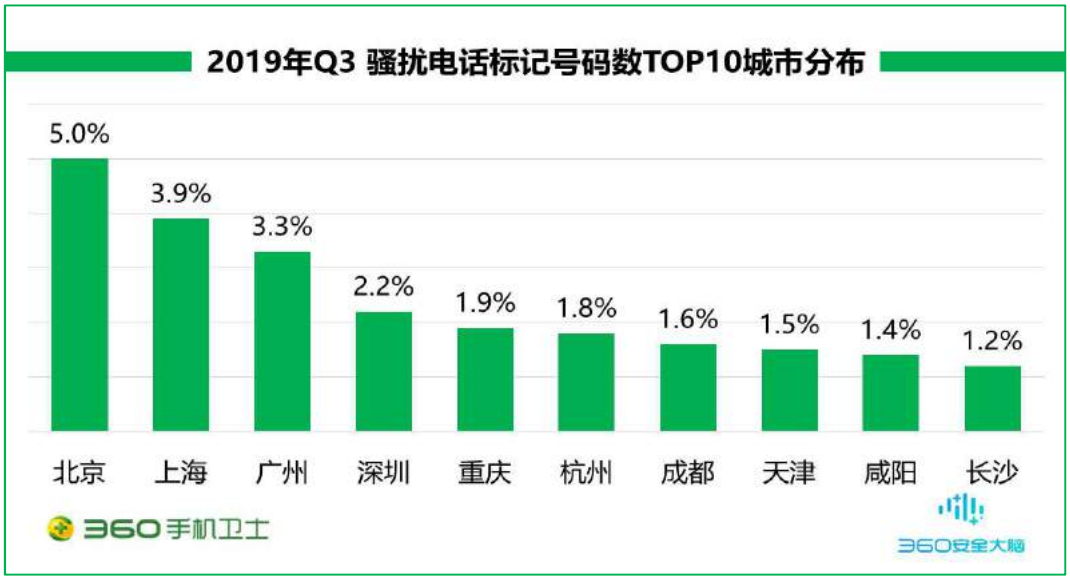
通过以上统计可见，利用虚拟运营商号码与 96/96 号段从事电信骚扰与广告推销的情况占据较高比例。同时，利用以上号段实施欺诈行为的类型比例也占据前列。

四、 骚扰电话归属地分布

2019 年第三季度，从各地骚扰电话标记号码个数上分析，广东省用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的 11.0%；其次是山东（7.0%）、河南（5.9%）、江苏（5.8%）、四川（5.3%），此外北京、浙江、河北、湖南、辽宁的骚扰电话标记号码个数也排在前列。



从城市分布来看，北京市用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的 5.0%；其次是上海（3.9%）、广州（3.3%）、深圳（2.2%）、重庆（1.9%），此外杭州、成都、天津、咸阳、长沙的骚扰电话标记号码个数也排在前列。



2019 年第三季度，从各地骚扰电话的拦截量上分析，广东省用户接到骚扰电话最多，占全国骚扰电话拦截量的 12.5%；其次是山东（7.0%）、江苏（6.5%）、浙江（5.7%）、河南（5.7%），此外河北、四川、湖南、广西、福建的骚扰电话拦截量也排在前列。

从城市分布来看，北京市用户接到的骚扰电话最多，占全国骚扰电话拦截量的 3.6%；其次是上海（3.2%）、广州（3.2%）、成都（2.2%）、深圳（2.1%），此外重庆、东莞、苏州、郑州、佛山的骚扰电话拦截量也排在前列。

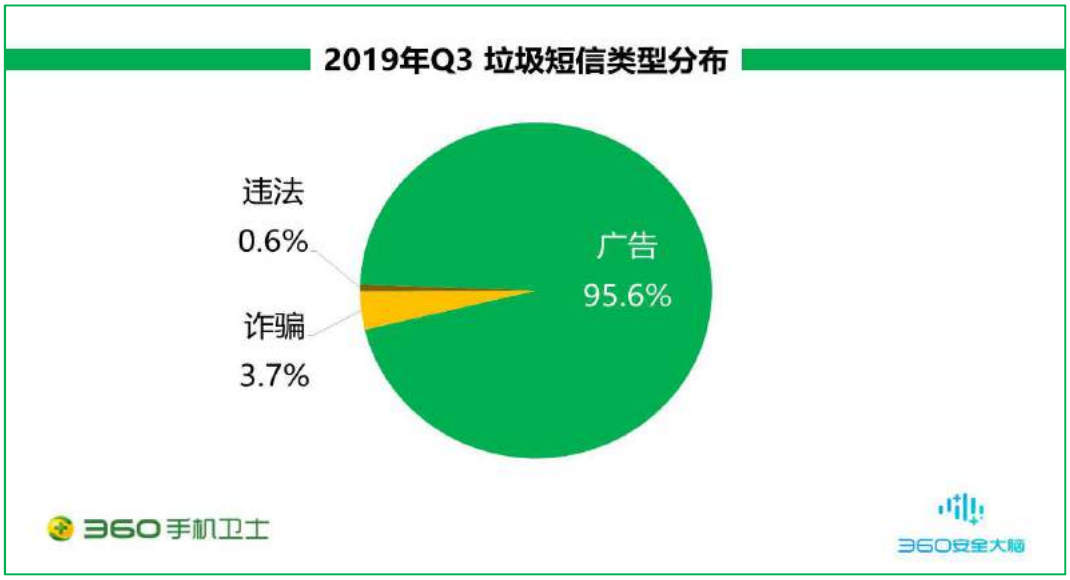
第四章　垃圾短信

一、 垃圾短信拦截量

2019 年第三季度，360 手机卫士共为全国用户拦截各类垃圾短信约 25.9 亿条，同比 2019 年第二季度（11.2 亿条）上升了 56.8%，平均每日拦截垃圾短信约 2823.2 万条。自 7 月份起，垃圾短信拦截量呈直线上升趋势。

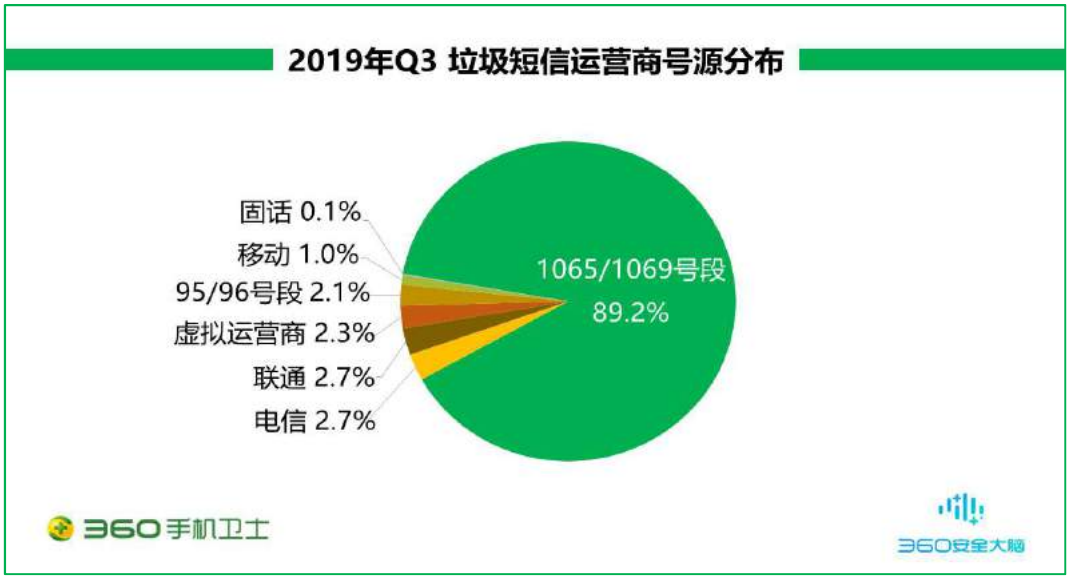
二、 垃圾短信类型分析

2019 年第三季度，垃圾短信的类型分布中广告短信最多，占比为 95.6%；诈骗短信占比 3.7%；违法短信占比 0.6%。具体分布如下图所示：



三、 垃圾短信运营商号源分布

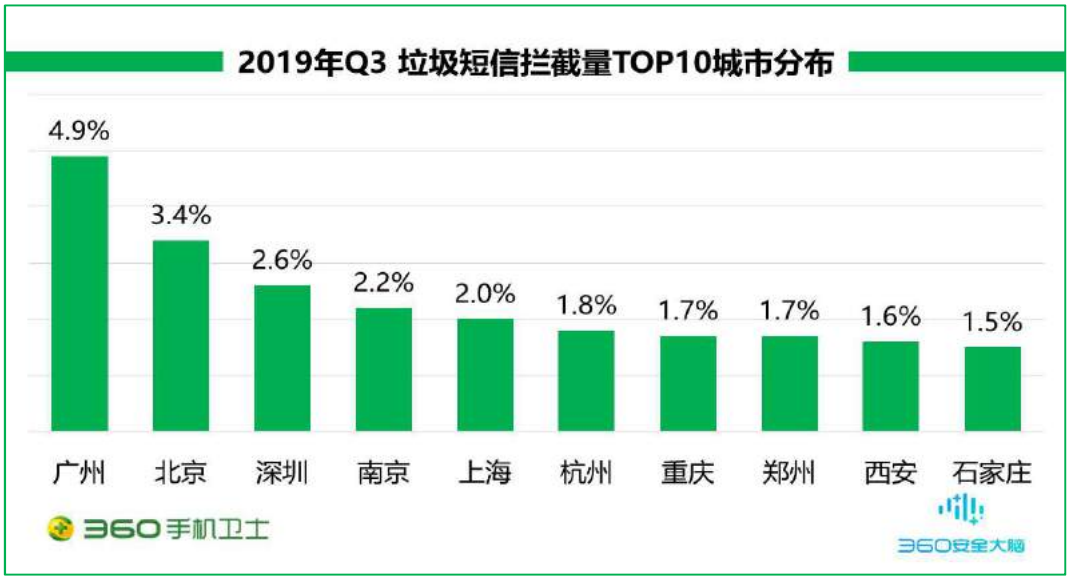
2019 年第三季度，从垃圾短信发送者号码的运营商号源分布看，利用 1065/1069 渠道号段发送垃圾短信的最多，占比高达 89.2%；其次为中国电信（2.7%）与中国联通（2.7%）。



四、 垃圾短信拦截量地域分析

2019 年第三季度，从各地垃圾短信的拦截量上分析，广东省用户收到的垃圾短信最多，占全国垃圾短信拦截量的 4.2%；其次是山东（1.7%）、江苏（1.7%）、浙江（1.7%）、河南（1.5%），此外北京、河北、四川、湖南、陕西的垃圾短信拦截量也排在前列。

从城市分布来看，广州市用户收到的垃圾短信最多，占全国垃圾短信拦截量的 4.9%；其次是北京（3.4%）、深圳（2.6%）、南京（2.2%）、上海（2.0%），此外杭州、重庆、郑州、西安、石家庄的垃圾短信拦截量也排在前列。



第五章 手机诈骗

一、 报案数量与类型

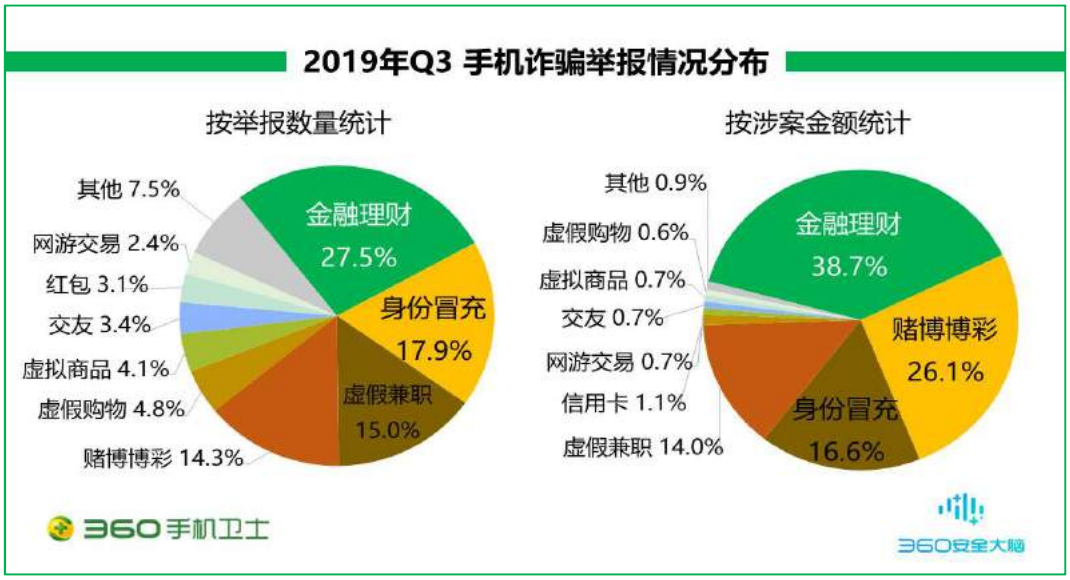
2019年第三季度，360手机先赔共接到手机诈骗举报667起。其中诈骗申请为414起，涉案总金额高达462.3万元，人均损失11167元。

在所有诈骗申请中，金融理财占比最高，为27.5%；其次是身份冒充（17.9%）、虚假兼职（15.0%）、赌博博彩（14.3%）、虚假购物（4.8%）等。

从涉案总金额来看，金融理财类诈骗总金额最高，达178.8万元，占比38.7%；其次是赌博博彩诈骗，涉案总金额120.5万元，占比26.1%；身份冒充诈骗排第三，涉案总金额为77.0万元，占比16.6%。

从人均损失来看，赌博博彩诈骗人均损失最高，为20423元；其次是金融理财诈骗为15683元，信用卡诈骗为12425元。

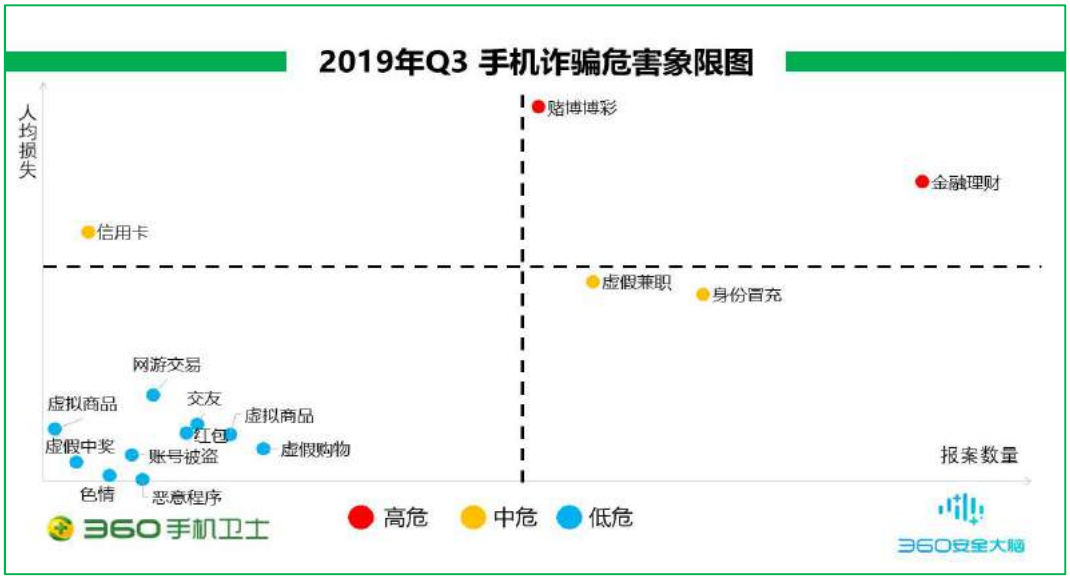
下图给出了主要手机诈骗类型的举报量和涉案总金额分布情况：



下图给出了不同类型的手机诈骗在人均损失和举报数量的象限图。从图中可见，赌博博彩、金融理财属于高危诈骗类型，受害人数较多且人均损失高。赌博博彩类型主要手法为设立非法赌博平台或组织非法赌博游戏诱导用户进行支付；金融理财类型主要为贷款诈骗。

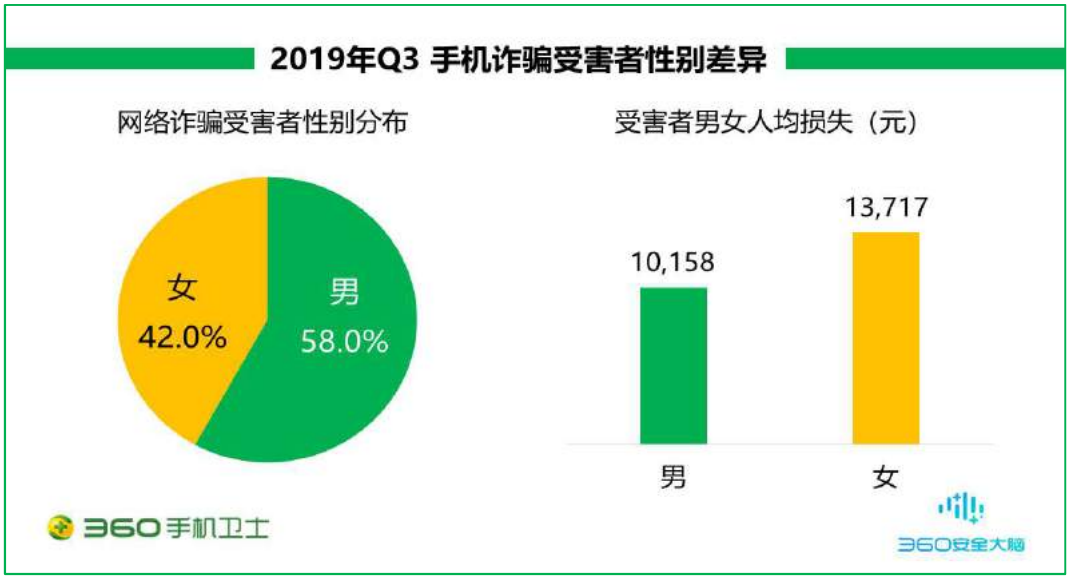
信用卡类型虽受害人数少，但人均损失较高，此类诈骗主要利用个人信息泄露发起的定向诈骗，危害性较高，属于中危诈骗类型；身份冒充类型主要反馈为遭到虚假客服诈骗，属

于中危型诈骗；虚假兼职虽人均损失偏低，但受害人数多，兼职缴纳会费的诈骗手法居多，属于中危诈骗类型。



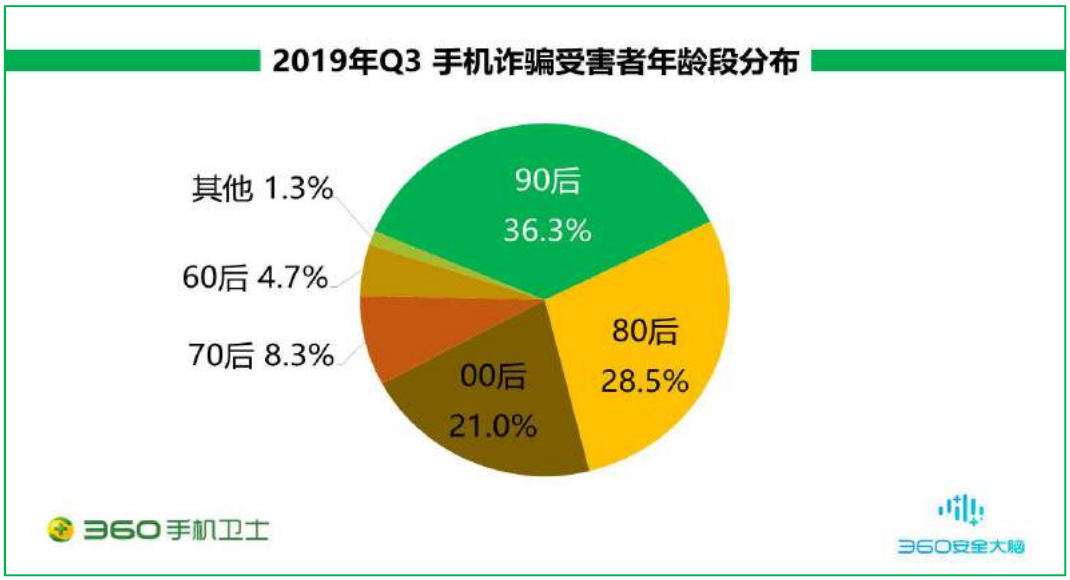
二、 受害者性别与年龄

从举报用户的性别差异来看，男性受害者占 58.0%，女性占 42.0%，男性受害者占比高于女性。从人均损失来看，男性为 10158 元，女性为 13717 元，男性受害者人数高于女性，但人均损失低于女性。

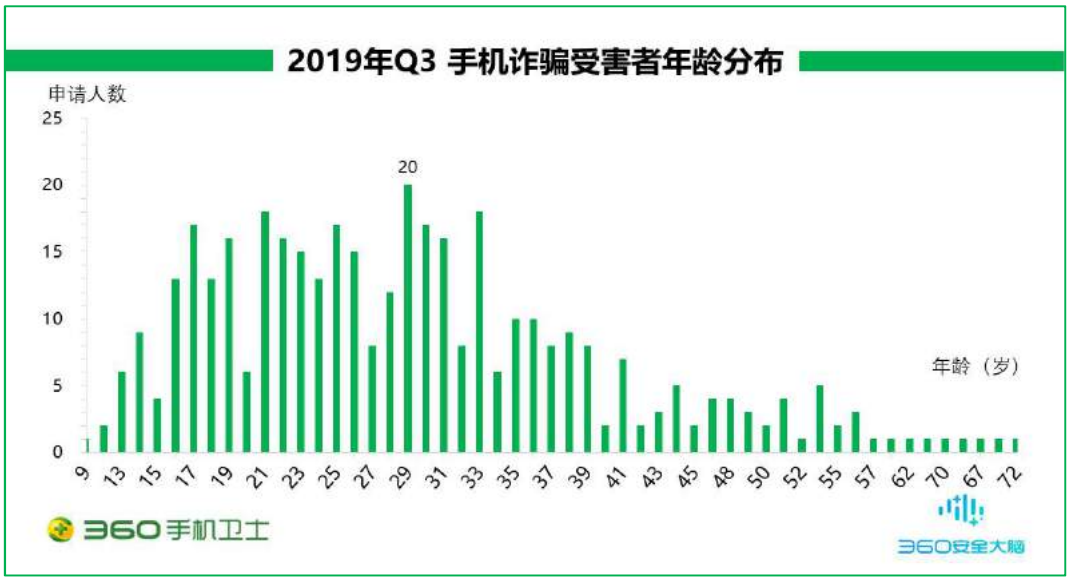


从被骗网民的年龄段上看，90 后的手机诈骗受害者占所有受害者总数的 36.3%；其次是 80 后占比为 28.5%；00 后占比为 21.0%；70 后占比为 8.3%；60 后占比为 4.7%；其他年龄段

占比为 1.3%。如图分布，2019 年第三季度中，90 后为手机诈骗主要针对人群。



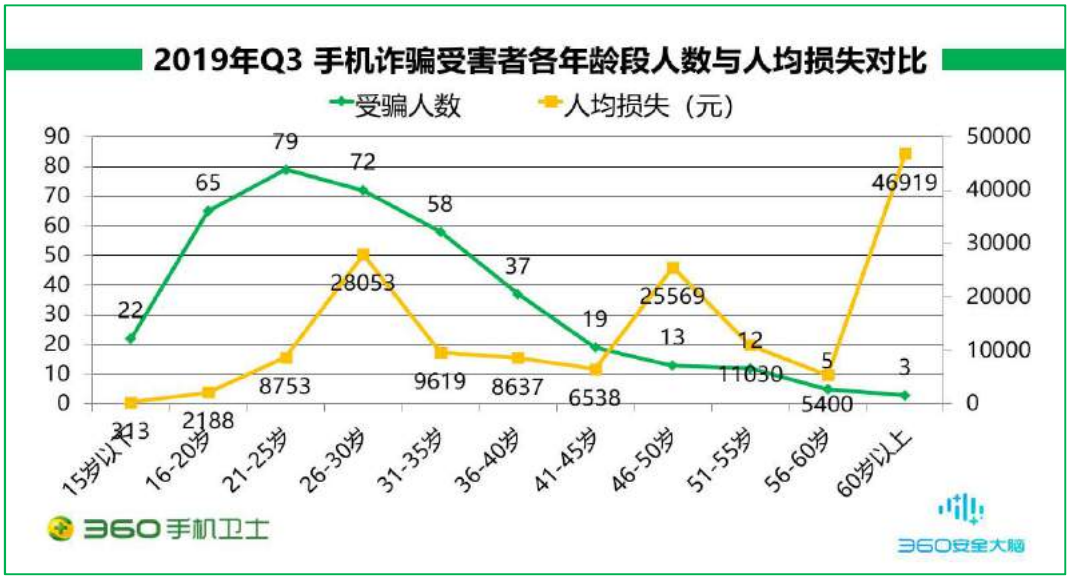
而从具体年龄上来看，21-25 岁的人群是手机诈骗受害者最为集中的年龄段，占所有手机诈骗受害者的 19.1%。其中金融理财类型受骗反馈较多，主要为申请贷款时遭遇诈骗。网络贷款已成为当下年轻人满足物质需求的渠道之一，多数人盲目在网络中寻找无抵押、快速下款的贷款平台，容易轻信缴纳保证金、激活额度等欺诈接口，极易遭遇贷款诈骗。



下图给出了手机诈骗受害者年龄段人数与人均损失的对比。从图中可以看出，20 岁以下的用户，被骗的人数虽多，但由于这个年龄段用户经济能力有限，被骗平均金额相对较少。21 岁-30 岁之间的用户是 2019 年第三季度举报受骗的主要人群，这个年龄段用户有一定经济实力，人均受骗金额也较高。

46-50 岁之间的用户，虽然已经不是上网的主力人群，但人均损失突破 2.5 万元。观察

这个年龄段的用户，被骗类型均为投资理财被骗。60 岁以上的用户，人均损失突破 4.6 万元，是由于其中一位用户遭遇投资理财诈骗，损失 14 万元，导致拉高这个年龄段人均损失金额。通过观察发现，投资理财在中老年人群中依然受到追捧，在不明确投资市场大环境的情况下，投资风险高。



三、 受害者地域分布

2019 年第三季度，从各地区手机诈骗的举报情况来看，广东（11.6%）、山东（8.5%）、河北（7.2%）、河南（5.8%）、广西（5.3%）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 38.4%。下图给出了 2019 年第三季度手机诈骗举报数量最多的 10 个省份：

从各城市手机诈骗的举报情况来看，深圳（2.4%）、上海（2.4%）、武汉（2.2%）、广州（2.2%）、重庆（1.9%）这 5 个城市的被骗用户最多，举报数量约占到了全国用户举报总量的 11.1%。下图给出了 2019 年第三季度手机诈骗举报数量最多的 10 个城市：

第六章 重点趋势分析

一、 通信技术发达时代，骚扰治理形势严峻

互联网的萌发，技术能力的演进，对于互联网用户而言，本是一件便捷生活的好事。短信、电话作为生活中必不可少的一部分，拓宽了社交渠道，增加了信息来源。但随着黑灰产业的介入，信息爬取、新型短信、电话骚扰技术成为了困扰正常生活的绊脚石。以下通过对被黑灰产介入并利用的短信及电话行业所产生的黑灰原理及手法进行分析：

1、 “闪信”成为黑灰产业从事非法行径的新“渠道”

1) “闪信”通信

短信作为功能机时代的必须品，进入智能机时代后，变得更加重要。平台注册，交易信息校验，用户无时无刻都在与短信打交道。2019年8月多个用户在互联网反馈收到“闪信”短信，寻求科普。

“闪信”，又称霸信、屏信、0级短信、弹屏消息、免提短信、来电名片，是一种在屏幕上即时显示的特殊文本信息。通俗来说，收到“闪信”的用户，信息内容直接显示在手机屏幕上。“闪信”本意是帮助政府和运营商，发送紧急信息，如极端天气、自然灾害、防诈骗的提醒。随着短信技术的发展，运营商根据时代需求，推出利用新技术达到和“闪信”相似可以在手机屏幕显示的功能，用来提示用户，如运营商帮用户拦截骚扰电话提示功能。此种技术的应用，意味着屏幕直显短信技术商业化。

（以下附图来自互联网）

2) “闪信”功能介绍

根据“闪信”类营销人员介绍，目前此种短信售卖渠道，存在多种发送通道，显示效果不同。有的渠道屏幕直显短信显示发送者号码和有的渠道则不显示。部分渠道发送的屏幕直显短信，在某些手机上可实现保存。显示发送者号码的短信平台，对发送的内容范围无限制，可以发送棋牌、博彩、贷款、兼职、理财等类型短信。此类短信价格每条约 6-8 分，量大甚至还可以获得批发价。不显示发送者号码的短信推送平台，发送的短信内容会有相应的限制，限制为地产、金融（贷款）等合法的营销内容。事前发送短信的语料需要审核，且审核周期较长。此类短信通道中，由于显示发送者号码的闪信，发送的内容基本无限制。此种类型的“闪信”被黑灰产利用的可能性较大。

下图为两种不同效果的界面，及保存到手机中的效果：

3) “闪信”产业链

屏幕直显文本技术的成熟，商业化的推进，带动了相关黑灰产业链的完善。上游短信渠道商通过搜索引擎、社交软件等渠道毫不隐晦的推广屏幕直显短信，部分渠道商在售卖此类通道时并不关心发送的内容是否违规违法，只关心发送的量级。下游短信渠道需求方，如违法小额贷、博彩、虚假广告，依托强大的短信直显技术推广自己的产品，以求达到近乎 100%的短信达到率。下图为闪信渠道交流群发送的广告，其中 BC、6h、QP、JZ、WD 分别为博彩、

六合 、棋牌、兼职、网贷的简称。

屏幕直显短信技术成为了一种黑灰的商业交易，用这种无法屏蔽的信息，打造出了效果近乎 100%广告投递效果。对于手机用户而言，这远比传统意义上的营销短信伤害大。目前主流安全厂商对于利用此类屏幕直显文本技术推广的黑灰短信，已可进行内容识别，并进行安全提示，降低了黑灰产业对此行业的恶意影响。

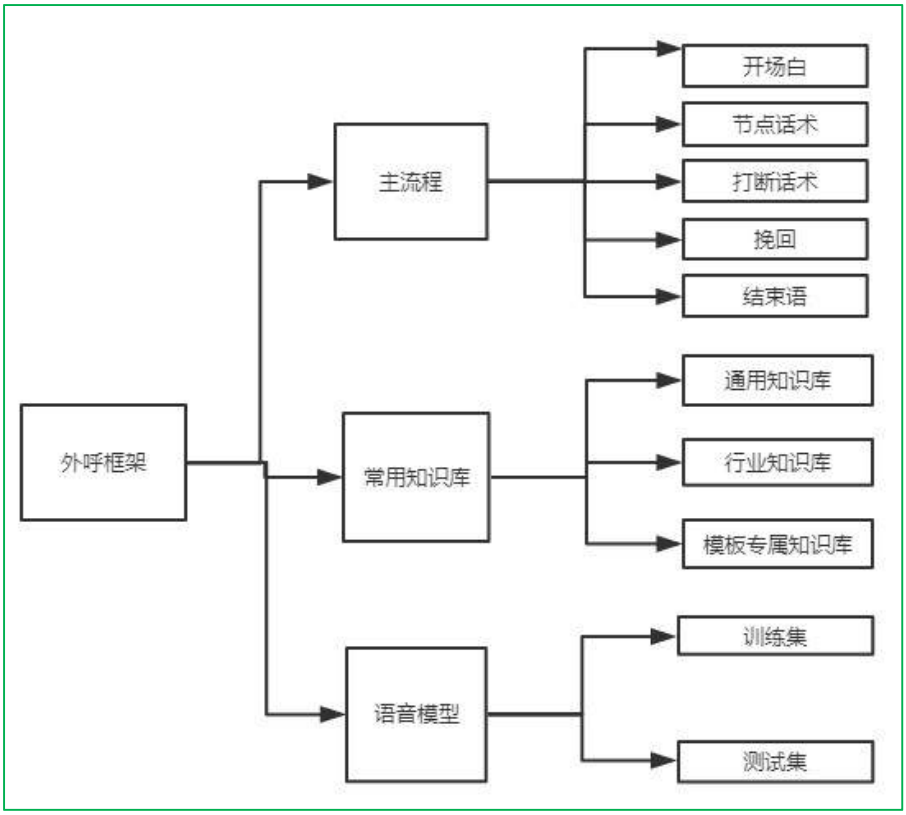
2、 骚扰程序化，外呼机器人被广泛应用

伴随着短信技术的发展，电话技术也进行了快速演进，进入了智能语音时代，模拟人工客服的外呼机器人应运而生。传统的销售行业，往往是通过人工拨打电话并筛选海量用户号码。此种人工客服群拨电话的方式，往往挂断率居高不下，筛选意向客户花费时间多，无法实施跟踪记录，调整获客方案。随着语音识别技术与人工智能技术的发展与成熟，集合拨打、回答、采集、推销于一身的外呼机器人出现，并在 2019 年呈现爆发增长趋势，各种电话机器人集成商打包提供服务。智能外呼机器人似乎成为了企业电话营销的利器，但作为接电话的一方，它的负面影响也很巨大。以下通过原理、产业链、应对方式等多个维度对外呼机器人行业进行解读分析：

1) 外呼机器人原理

外呼机器人的框架包含 3 个部分，主流程、常用知识库、语音模型。主流程为拨打电话的流程，包含开场白（电话开始的语音）、节点话术（在进行下一步时的场景转换语音）、打断话术、挽回话术（对已无意向的用户进行深度挖掘）。常用知识库为电话行业及所在行业

的术语，包含通用知识库（电话技巧）、行业知识库。语音模型为外呼机器人的语料库，帮助外呼机器人了解语音类型，识别语音、识别语义，包含训练集和测试集。



外呼机器人的工作流程，拨出电话→接听→通话→挂断→标签分类→云端存储。外呼机器人通过呼叫中心拨打电话，利用语音识别、语义理解等技术方式识别接入方的语音。通过电话场景模板，了解接电话方的语义意图，进行正确的电话回复操作。对接听情况进行分析，判断没有接听到是由于网络原因、关机、挂断还是正在通话中，将此些信息进行标签分类。如意向用户，无意向用户，可进行转化用户。随着拨打电话次数的增加，借助增加的语料，增强对外呼机器人的学习能力，交互能力。筛选完之后会再根据标签来进行二次沟通。达到客户的筛选、沟通和分析的目的。

如下图展示的某外呼机器人平台的外呼话术流程。对外呼机器人的外呼话术、外呼节点进行了规定，帮助外呼机器人更好的疏通外呼流程：

2) 外呼机器人带来的不良影响

“你需要买房吗？”、“你最近在做股票吗？”、“你需要投资吗”，不想被陌生电话打扰成为一种奢望。很多人接到骚扰电话后，出于礼貌总是会让对方先表明来意，如不需要再委婉拒绝。随着时间的推移，忽然发现，以前那套委婉拒绝，无法产生效果。无论怎么回答，对方总是像“老师”一样耐心开导“你”。原因在于电话背后的，并不是真人，而是外呼机器人。

3) 外呼机器人黑灰产业链

外呼机器人行业借助计算机算法技术的成熟、语音识别能力 SDK 集成化在 2019 年迅猛发展。智能外呼系统搭建包含四个部分，运营商线路、呼叫中心、AI 能力、服务平台。运营商线路提供通讯能力，呼叫中心提供集中化呼叫服务，AI 能力提供外呼机器人的语音、语义等识别技术能力，服务平台提供外呼机器人运营操作平台。组成外呼系统的四个部分，随着技术的发展，已经可以集成打包。在部分云服务器厂商平台就可能接入这种能力，搭建成本和难度进一步降低。

目前大多数的外呼机器人平台已将平台运营接口话，根据需求方输出在线或本地版的入口。需要外呼业务的人员，只需登录外呼网站后台，导入话术及需拨打号码，即可开始引导外呼机器人执行号码任务，一台机器每日可拨打上千个号码。但同时也意味着电话骚扰的严重。目前外呼机器人市场鱼龙混杂，各种渠道都可以发现他们的踪影，如搜索引擎，社交软件。

此些外呼机器人售卖渠道一般不会审核接入方资质及拨打的内容，企业是否有营业执照都不会过于审核。由于渠道商的放任，各类营销、欺诈电话蜂拥而至，带来了严重的骚扰。

在外呼机器人的语音、语义日益增强的情况下，接听电话的一方，在接听到外呼机器人电话时，无法察觉对方是真实还是虚拟的电话，轻则随着机器人的话术进行下一步，重则被对方套取多个角度的语音进行画像分析，后续源源不断的进行电话骚扰。虽然外呼机器人行业较火，但对于接听电话的一方则较为陌生，未接听过此类电话，或者接听电话后也无法识别此类电话，呈现出一种无奈的状态。

4） 外呼机器人识别

外呼机器人虽然宣称强大，但仍存在不少缺陷，对于接听电话的一方可以通过以下的方式进行识别。接听陌生电话时不主动说话，尝试让对方先发生，根据对方第一句话的语义话术和停顿时间判断，人在接打电话时，说话的语速和话术会随着场景产生不顺畅性，不会像外呼机器人那样一次性完整毫无停歇的表达出语义。根据对方语速的流畅性，初步怀疑对方是外呼机器人后，可尝试表示不明白，打断对方的说话。查看对方的停顿周期，或在对方说完话后，不说话，停顿几秒。后续可能会发现外呼机器人已经无法准确对话。通过此种方式打破外呼机器人的常见认知、常见场景，让自身无法准确回复下一步话术。

5） AI对抗AI的时代

企业希望通过技术实现业务流程效率。对于企业而言，外呼机器人降低了运营成本，增加了获客率。企业希望外呼机器人能够不断提高自然语言处理的准确性，更加的智能化。对于用户而言，高频的营销电话影响了人们的正常生活。面对频繁的骚扰电话，用户想拒接陌生来电又有可能错过重要信息。用户希望通过技术避免自身遭受的电话骚扰问题。鉴于此种情况，网络安全行业借助AI的力量与骚扰电话行业进行了一场AI与AI对抗的比赛。

网络安全行业通过预防与识别两种手段增加对骚扰、欺诈电话的识别率，事前借助大数据实现对各种骚扰、欺诈电话号码的标记，在用户来电时对用户提示此为骚扰、欺诈电话。事中充当用户电话助理，帮助用户接听电话，通过语音、语义等技术识别来电方的意图行为，帮助标记并记录来电者的语音内容和意图，通过移动设备的通知栏、短信、社交软件推送电话信息。通过事前预防与事后识别两种方式，帮助用户阻挡电话骚扰。

3、 总结

在大数据和云计算的帮助下，各种新型的计算机技术运用到了现实生活，企业获取了互联网发展的红利，用户改善了生活方式，但技术一旦被滥用，甚至用于非法用途，将来带来社会问题，如短信、电话技术的骚扰、欺诈场景。对于技术提供方而言，可以通过几个维度降低这种“不良效应”产生的影响。对于技术提供方而言，进行行业限制，审核使用方的资质，避免骚扰类、欺诈类接入方使用该产品。进行场景限制，避免此类短信、电话技术被盗用于骚扰、欺诈。对于安全类产品而言，借力打力，顺应时代推出反制产品，如结合号码标记+语音语义识别的安全大脑，帮助用户识别，解决用户痛点与烦恼。

二、 虚假兼职刷单产业链剖析

1、 兼职刷单产业概述

电商行业的兴起，越来越多的人通过电商平台购买商品，而电商店铺的销量、评价成为影响该店铺在电商平台排名的重要因素（权重）。于是电商刷单行业应运而生，电商店铺找寻虚假“买家”，在店铺购买商品。店铺给“买家”邮寄空包裹或低金额的替代商品，完成交易后，“买家”在平台给店铺进行“好评”。店铺给“买家”刷单佣金。刷单行业通过模拟正常的电商消费过程，来躲避电商平台的监测。如不直接访问店铺购买商品，先在电商平台搜索指定的“商品关键词”，浏览多个商品页后，并在商品页停留几分钟，才选择需刷单商

品。操作后期，店铺商家给“买家”发货时，为防止快递商品重量检测，从邮寄空包裹转移到邮寄相同重量的商品。

店铺对刷单“买家”的要求比较严格，一般需满足指定需求或特征的消费者用户。曾经购买过同类产品，或者是该产品的潜在用户。如：男性一般购买科技或运动类产品，女性一般购买服饰或化妆类产品；学生的消费水平一般较低，购买的商品性价比较高。由于电商刷单属于黑灰产业，出于躲避监管的目的，刷单行业往往较为隐蔽，多为内部交流，想要进入内部圈层需要缴纳多重身份信息进行验证。且刷单人员在交流群沟通刷单的过程中，多使用行业话术，如恰饭，初入人员一般难以理解，同时刷单的过程中，会将话语通过图片的形式展示。由此可见，电商刷单产业对于从事刷单人员、刷单的流程都有较为严格的要求，常人无法轻易参与其中。较为容易进入的刷单渠道，并且宣传刷单过程简单，佣金较高的刷单即有可能是虚假诈骗。

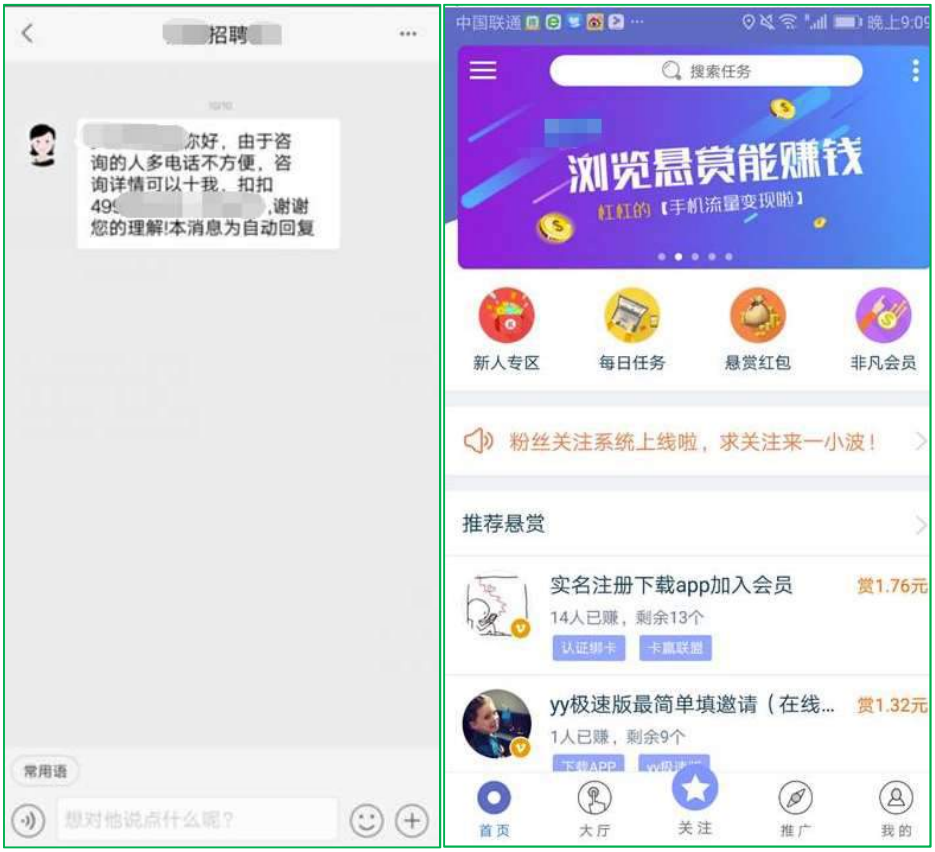
2、 虚假刷单骗局手法

随着各大安全厂商对虚假兼职产业的剖析，用户对于虚假兼职手法有了一定的了解，安全意识也不断的提升。于是，虚假兼职刷单产业也对手法不断的进行升级。以下针对不同的虚假兼职刷单场景，进行渠道及手法分析：

渠道分析

虚假刷单兼职产业通过多维渠道，以高额返佣或日赚百金为幌子吸引用户参与其中。如下图展示的，不法分子通过兼职刷单短信、社交群、招聘平台广告、网赚 APP 等方式传播虚假兼职信息。


0.41K/s
18:56
36%
详细信息
吉林长春
2018/06/04 周一 00:54
鉴于您的购买记录良好，我网商特邀您帮助（刷-单）。有手机电脑随时可做，一百二到三百元/天，易操作时间自由，详情+Q;
短信
发送
淘宝刷单群有朋...外快可以拉(279)
京东垫付立返单
垫付 190 佣金 6，立返本金和佣金 墨迹的不要来（做单）
不要在群里@我，做得直接加我好友


招聘
您好，由于咨询的人多电话不方便，咨询详情可以十我，扣扣49,谢谢您的理解!本消息为自动回复
常用语
想对他说点什么呢?
搜索任务
浏览悬赏能赚钱
虹虹的【手机流量变现啦】
新人专区
每日任务
悬赏红包
非凡会员
粉丝关注系统上线啦，求关注来一小波！
推荐悬赏
实名注册下载app加入会员
赏1.76元
14人已赚，剩余13个
认证绑卡
卡赢联盟
yy极速版最简单填邀请（在线...
赏1.32元
1人已赚，剩余9个
首页
大厅
关注
推广
我的

手法类型

1） 真网站，假收款方类

不法分子首先给予用户真实的电商平台链接，或者要求用户自行在电商平台搜索指定的关键词进入商品页，将商品加到购物车。随后以防止电商平台监控到刷单行为为由，要求用户通过指定的商品付款码付款。用户扫码转账或直接转账后，再以任务为多个，要求用户反复转账。

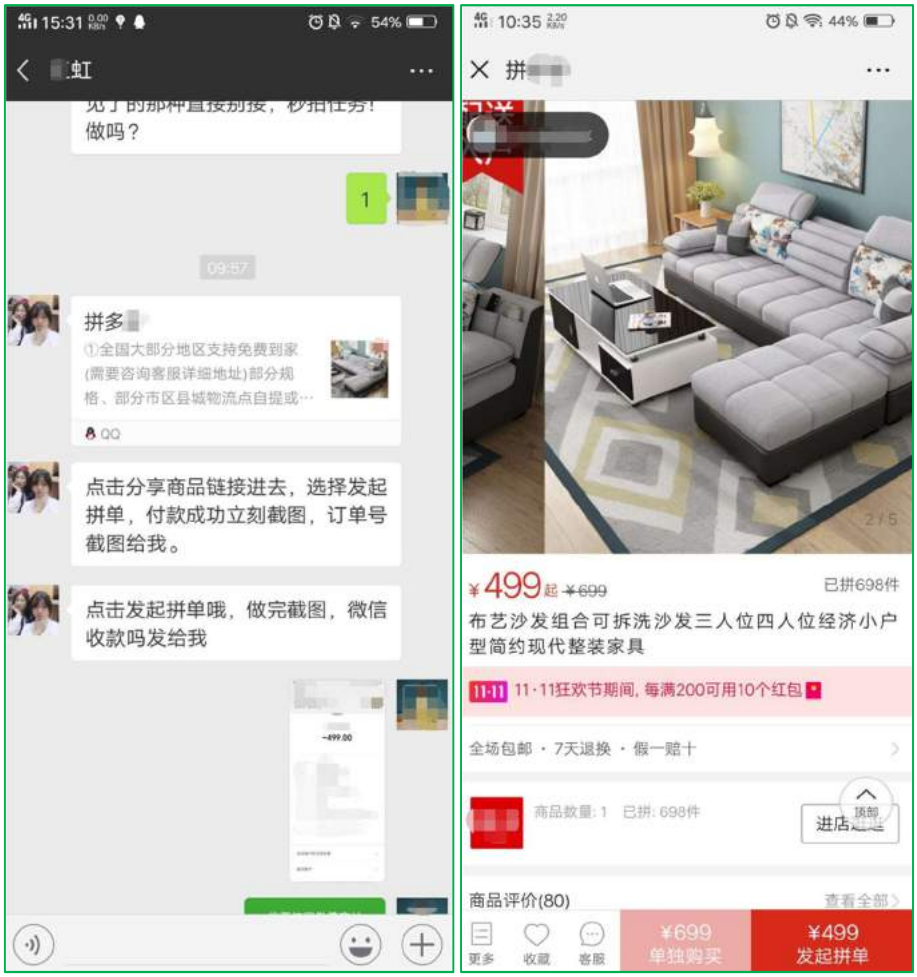
手法分析：

不法分子发送的商品链接或要求用户搜索的商品页只是一个幌子，真正的诈骗环节在于不法分子提供的收款信息，此收款信息为不法分子的收款信息与电商平台或所描述的刷店店铺没有直接关联，用户实际是转账给不法分子。

2） 假网站，假收款方类

给予用户发送“知名”电商平台的链接，要求用户访问该商品链接。浏览商品后，点击页面的购买链接，跳转至支付页面。根据页面的提示，使用支付工具支付。支付商品后，发

现同名商城内竟然无该商品订单。



手法分析：

不法分子发送的商品链接为仿冒电商平台商品的链接。用户使用社交软件直接访问时，一般不显示网址，对于用户而言，无法通过常规判断域名的方式轻易判断出访问平台的真假。

同时不法分子在制作高仿网站时，嵌套了很多真实的电商店铺的元素，达到以假乱真的目的。如商品图片，商品价格，商品平台，甚至嵌套了真实店铺的客服链接。

3) 真支付链接，假企业代付

不法分子宣传 0 元刷单、企业代付。首先给予用户真实的电商平台链接，或者要求用户自行在电商平台搜索指定的关键词进入商品页，将商品加到购物车。随后以防止电商平台监控到刷单行为由，要求用户使用企业代付的方式支付。用户按照对方提供的企业代付流程图操作，使用支付工具扫码商品二维码，选择花呗支付，输入密码后，未显示截图中的企业代

付标识，就已支付完成。

下图为虚假支付流程图：

手法分析：

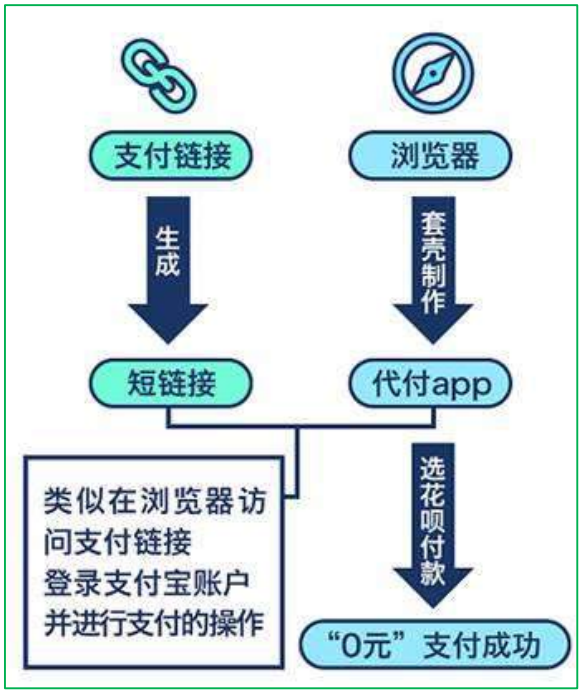
不法分子使用虚假的支付流程图蒙骗用户。不法分子提供的流程图，在用户选择商品，使用花呗支付，输入支付密码后，会出现“使用企业代付付款”使用企业代付付款的字样，但在实际操作的过程中并不会出现“使用企业代付付款”，输入支付密码后，就已完成支付流程。

4) 0 元代付

以刷单无需付款，0 元代刷为幌子，引导用户关注。询问用户之前兼职情况，以判断是否符合兼职条件为由，索要用户的花呗及芝麻信用截图。给用户发送代付 APP,表示使用此 APP 进行代付操作，刷单操作时会被用户进行代付商品费。引导用户在代付 APP 内，输入指定的短链/支付链接，完成 0 元代刷操作。用户按照指引，在 APP 内填写对方提供的链接，APP 的界面跳转至支付宝登录界面，完成支付宝登录后，显示需付款费用为 0 元，点击确认付款，输入支付密码后完成 0 元刷单操作。但事后发现多了一笔花呗账单。

手法分析：

该 APP 的功能类似浏览器，在 APP 内输入的短链为代付链接。该操作可理解为使用浏览器访问代付链接的过程。页面显示 0 元商品，是由于使用了花呗支付，当前需支付的费用为 0 元。



5） 0 元代付 APP 变种

原先的代付 APP 是需要输入代付 URL。而新发现的代付 APP，无需输入网址，输入任务数字，点击开始任务，即可跳转至支付界面。后续的流程与原先一样，登录支付宝账号，输入支付密码，完成支付操作。

手法分析：

代付 APP 通过不同的数字，调用不同的支付链接，从而达到输入不同的数字，跳转至不同代付链接的效果。

3、 虚假兼职刷单产业

目前虚假兼职产业已经形成一条技术开发、支付通道输出、诈骗话术培训、渠道推广的完整产业链。支付通道商提供支付宝、微信、银联、云闪付等支付通道及电商平台的代付链接。目前支付通道商渠道较多，在搜索引擎及社交渠道都可轻易找到提供商。

找到约 75,800 条结果 （用时 0.34 秒）

API接口自动批量代付，秒出款秒回盘-米拓信息 - 汇潮支付

www.ecpss.com.cn › news › shownews ▾

2017年9月13日 - 商家给用户出款分别有传统的单笔转账模式、批量转账出款、API接口自动代付三种类型。随互联网发展需求，针对平台用户提现笔数多、提现次数多 ...

软件开发商将各类支付 API 及商品的代付链接集成在 APP 中。当访问代付链接时，直接跳转至收款二维码或商品的代付链接。

推广商通过各种渠道，以“高额返佣”或“日赚百金”为幌子，吸引用户参与其中。如下图展示的，不法分子通过兼职刷单短信、社交群、招聘平台广告、网赚 APP 等方式传播虚

假兼职信息。

非技术型诈骗则使用虚假支付流程图片，利用支付过程的逻辑顺序，需要用户在支付过程中输入支付密码，完成转账或代付的过程。技术型诈骗，使用高仿电商店铺、集成代付链接的代付 APP 诱导用户进行代付操作。

4、 安全厂商及警方应对及结果

随着互联网行业与黑灰产行业的攻防升级，互联网公司及安全厂商通过各种主防查杀及风控手法对虚假兼职类诈骗进行围栏打击。在宣传渠道、支付渠道、样本拦截、反诈知识普及等多个维度实现拦截。

在渠道上，搜索引擎网站通过各种技术手段打击黑帽 SEO 关键词，对此类网站进行降权，降低黑帽 SEO 关键词的排名；招聘类网站，通过站内文案，站内提醒等方式劝阻；安全厂商对虚假兼职类短信进行标识，使用高亮标识提示用户此为高风险性短信。

在支付渠道上，第三方支付工具通过风控机制，限制高金额，高交易次数的支付范围，增加用户向不法分子转账的难度，降低用户的受骗程度。

在样本拦截力度上，安全厂商通过行为模型算法，自动学习虚假兼职样本的行为，从而

实现对无恶意行为，但存在高风险的虚假兼职类 APP 的识别。

小海代付
谨慎应用

安装时间 2019-[redacted]

病毒描述 包含插件：com.dai[redacted]ijs 该软件存在风险代码，请在使用时注意。

恶意行为 使用有风险的权限

危险等级 ★★

更多帮助 病毒清除不了怎么办？

在防骗知识普及上，安全厂商与公安反诈部门联合，实施解读最新的虚假兼职诈骗手法，通过线上安全播报，线下地推等形式普及防骗知识。

在对此类黑灰产业打击上，警方成功打掉多个通过研发、制作、售卖网购平台代付刷单软件，骗取刷单被害人钱财的新型犯罪团伙

第七章 典型案例

一、 利用虚假电商平台，骗取“刷单”商品费

案例回顾

用户在 2019 年 7 月通过网络论坛了解到网络兼职活动，并添加了该兼职活动中预留的“工作人员”QQ。对方表示该兼职工作是帮助第三方电商平台刷销量，获得佣金。但购买商品的资金需要用户先行垫付，后期再给用户返回本佣金。

对方以判断用户是否符合兼职条件为由，索要了用户电商平台账户界面截图。确认用户符合兼职条件后，对方给用户发送所需刷单商家店铺二维码，并要求用户使用支付工具扫码访问该店铺。用户按照要求扫码后，界面出现了商品信息，在选择服饰属性后，使用第三方支付工具支付了该商品费用。支付商品后，却发现商品明细是话费充值，联系对方后，对方表示该情况是由于用户卡单，引导用户联系退款客服。退款客服表示若用户需退款，需要用户再完成一笔激活订单，此时用户得知受骗。

专家解读

1) 随着网络攻防的不断升级，黑灰产行业实施诈骗的产品仿真度越来越高，加大了用户鉴别的难度。

2) 第三方支付工具出于产品便利性，使用此类应用访问网站时，网址信息不会进行展示，不法分子正是利用此特点，结合高仿虚假店铺平台实施欺诈。

防骗建议

1) 刷单是一种作弊行为，国家法律法规、电商平台均明令禁止这种虚假交易。切莫相信低投入、高回报的幌子，通过正规渠道寻找兼职，确保付出得到回报。

2) 对于用户而言，不要轻易点击或扫描陌生人发来的网页链接和二维码。访问二维码网站前，可使用360手机卫士的安全扫码功能，查看二维码内含的网址，再通过域名预判网站的真伪性。

二、 博彩刷单骗局

案例回顾

用户在2019年5月通过社交群了解到兼职赚钱信息，添加了兼职信息内所含工作人员的微信。该工作人员表示该兼职活动是做“套利”的。使用指定的*彩国际APP，在平台购买指定的投注项目（*庆时时彩），可获取收益。在兼职活动期间，会给用户提供平台体验金和提现账号。在按照规定操作在平台盈利后，将收益资金提现至指定的银行账户，将给予用户兼职佣金。

用户在平台注册后，平台账号收到了对方充值的体验金。按照对方提供的购买项目教程投注，均获取了盈利。用户将盈利资金提现至对方指定的银行账户后，获得了兼职佣金。后续体验金周期结束后，用户在平台绑定了自己的银行账户，充值2000元，按照对方提供的操作教程，盈利后但无法提现，得知受骗。

专家解读

1) 博彩平台欺诈手法多变，早先使用博彩必赢计划，吸引用户在平台投注，使用前期盈利，后期亏损的方式骗取用户资金。现阶段使用平台提现陷阱的方式，骗取资金。使用对方的银行账户“代刷”时可提现，使用用户自己银行账户时则无法提现。

2) 此种骗局是利用刷单赚佣金降低用户的心理防线，获取用户的信任。一旦“上钩”，就会通过各种平台规则限制提现，想要解除限制，就需要投入更多的资金，被骗资金越来越多，无法及时抽身。

防骗建议

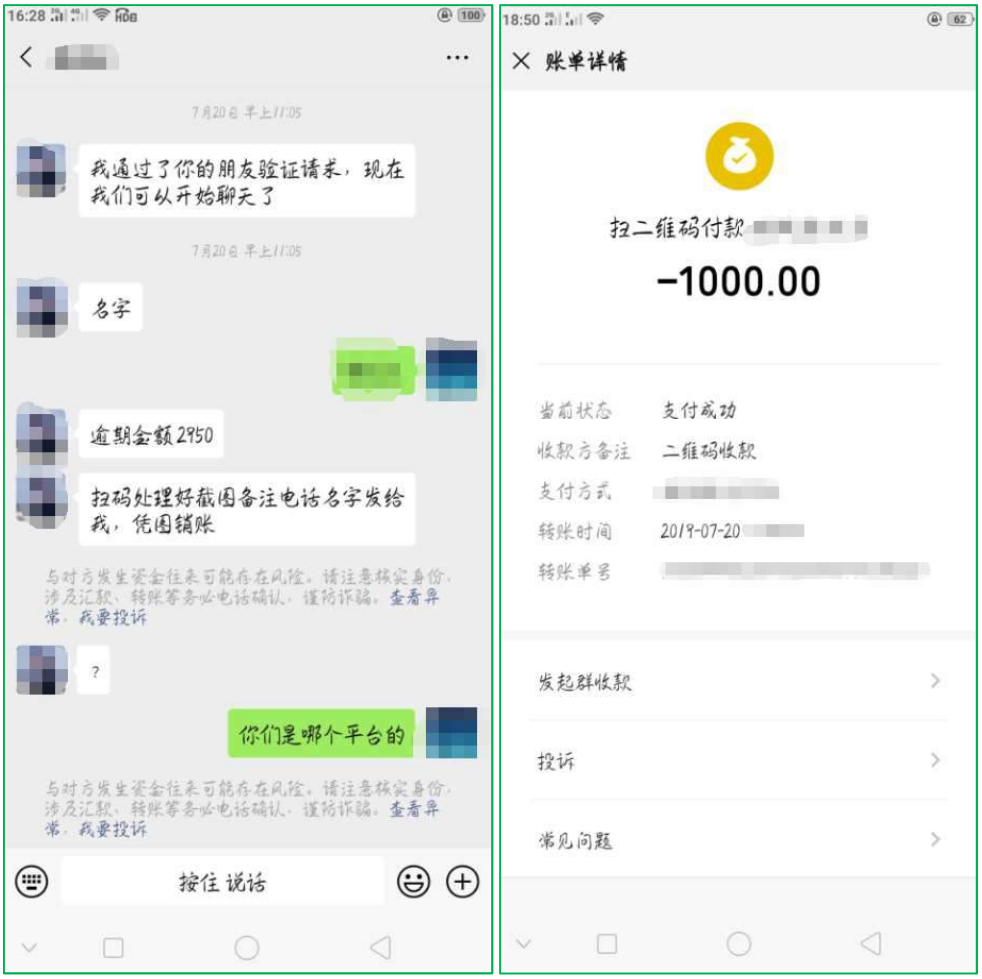
1) 在线博彩平台大多使用控制概率程序，对方通过控制输赢，造成博彩平台易赚钱的假象。教你轻松赚钱的人他其实在轻松赚你的钱，切勿因小失大。

2) 网络博彩属于违法行为，切勿向陌生人转账交易，保护好自身财产安全。

三、 冒充贷款平台催债，骗取贷款还款资金

案例回顾

用户于 2019 年在多个小额贷款平台申请过贷款。在 2019 年 7 月，用户收到贷款催收平台电话，确认用户姓名后，表示用户贷款存在逾期情况。如果不能按时还款，则会联系用户父母强制催收，在用户及时还款后会给予销账回执单。随后，平台客服通过手机彩信的方式给用户发送收款二维码，并引导用户添加还款客服微信。在用户成功添加客服微信后，分多次向对方账号转账用于还款，共计 3350 元。但事后用户没有收到还款凭证，也无法联系上对方，得知受骗。



专家解读

1) 小额贷款平台的兴起，满足了人们超前消费的心理。但由于各种原因，存在着贷款逾期的现象，不法分子正是利用此种现象，冒充贷款平台进行催债。

2） 不法分子利用催促、恐吓的语气阐述逾期还款的严重后果，攻克用户的心里防线，获取到用户的信任。当用户轻信不法分子描述的种种后果后，不法分子则顺势引导用户通过转账的方式缴纳逾期贷款。

防骗建议

1） 不管从什么平台借款，一定要通过官方渠道及时还款，切勿轻信任何对私还款。还款之前，一定要明确自己是从哪个平台借款。

2） 如果接到此类电话请提高警惕，第一时间联系平台客服确认，是否欠款有逾期、逾期金额是多少，切勿被对方的言语迷惑。

第八章 热门事件

一、 红包扫 “雷”欺诈

红包扫 “雷”原先指的是在微信群发红包，红包需标注金额和自定的数字“雷”。如果有人抢到红包的金额与所标记的“雷”的数字相同，就是踩到“雷”。需要按照扫“雷”群【规定】返还发红包者 1.5 倍的红包。

比如发红包者发了 100 块钱，定义“雷”的数字为 1，若抢到的红包金额中含有 1 或者尾数为 1，抢到此红包的人就要返还发包者 150 块钱。为防止踩“雷”者逃逸，进群者往往需缴纳一定的入会费。同时，群主和管理员踩 “雷”后有权免罚钱。由于玩法简单，输赢见效快，微信红包扫“雷”逐渐演变成一个产业。有专门分享微信扫“雷”群的平台、有专门开发微信排“雷”的外挂、也有红包扫“雷”玩法的 APP。

专家解读

1） 此类红包扫“雷”微信群，虽然每次金额不多，但往往多数人被贪念驱使，输了想赢，

赢了还想赢更多，后期投入越来越多。而且群内除自己外，可能都是提前串通好的。相当于“庄家”吃“小鱼”的过程。

2) 由于微信红包金额的随机性，红包排“雷”类外挂往往不像软件宣传的那样，可以避”雷”。且此类外挂往往售价较高，购买后往往达不到效果，还有可能下载到恶意类应用。

3) 红包扫“雷”类 APP，由于所有的功能及数据都由平台控制，用户的掌控几率更低。最终输的几率也更大。

二、 “垃圾分类”炒“币”

2019 年上海实行“最严垃圾分类”，“你是什么垃圾？”成了上海人民每天都要面临的灵魂拷问。借助垃圾分类的推行，各家知名互联网公司纷纷推出垃圾分类识别产品，但随之而来的是各大黑灰产打着“垃圾分类”噱头的项目。2019 年 9 月多个黑灰产网站开始推广一款名为“EP 环境保护”，垃圾分类赚钱 APP，但此应用实际是虚拟货币炒币项目。

平台宣传发布有限的 EP(平台货币)，每天把平台界面内的“垃圾”拖到对应垃圾桶即可完成任务， 获得 0.37EP(平台货币)，达到 10 个 EP 后，可购买资源转换器，增加 EP 收益。如花费 10EP 购买微型资源转换器，每日可释放 0.37EP，锁仓周期 30 天，可获取 11 个 EP。同时成立自己的战队，邀请他人注册，可获取不同数量的 EP。获得的 EP 可在平台的交易商城进行交易。但投入资金和时间成本，换回来的可能仅仅是服务器中的一串数字。

专家解读

此类平台都是借助热点事件推广虚拟货币。宣传数字货币的数量有限，增加平台货币的价值。但实际上此类平台货币毫无价值可言，用户花了时间，投入了资金，换回来的可能仅仅是服务器中的一串数字。同时，用户在此类平台注册时需实名认证，甚至需上传个人手持身份证照片，存在信息泄露的情况。