

2019

网络诈骗趋势 研究报告

2020.1.7



出品：360企业安全

猎网平台

技术支持：360安全大脑

摘要

在本报告中，360 安全大脑通过对猎网平台 2019 年收集的 15505 条有效诈骗举报进行了调研和分析，从网络诈骗举报数据综合分析、网络诈骗受害者画像、网络诈骗典型案例等维度，揭示了网络诈骗的发展现状及发展趋势，并对金融诈骗、交友诈骗、兼职诈骗等 2019 年典型网络诈骗做了深入分析，总结出 2019 年网络诈骗六大变种、十大话术和五大防范锦囊。

- ✧ **人均损失创近六年新高。**2019 年，猎网平台共收到有效诈骗举报 15505 例，举报者被骗总金额达 3.8 亿元，人均损失为 24549 元，较 2018 年人均损失略有增长。数据显示，2014 年至 2019 年，网络诈骗人均损失呈逐年增长趋势，至 2019 年，创下近六年新高。
- ✧ **金融诈骗位居举报量之首。**2019 年，金融诈骗是举报量最高的诈骗，高达 3314 例。其次为游戏诈骗，举报量 1927 例，兼职诈骗 1823 例。从人均损失上看，人均损失最高的诈骗为网络赌博诈骗，人均损失高达 73953 元。其次为交友诈骗，人均损失 53351 元；金融诈骗人均损失 53265 元，是人均损失第三高的诈骗类型。
- ✧ **Q4 季度人均损失最高。**2019 年 Q1 季度举报量最高，为 4066 例。从人均损失上看，Q4 季度人均损失最高，为 27376 元。通过举报数据梳理发现，Q4 季度网络赌博诈骗、金融诈骗较为高发，且这两类诈骗人均损失较高。
- ✧ **骗子最爱北上广。**2019 年，广东省举报量位居首位，占比 10.7%。山东位居第二位，占比 7.1%；河南位居第三位，占比 6.2%。从人均损失上看，北京人均损失最高，为 39443 元；上海人均损失排在第二位，为 34867 元；福建人均损失排在第三位，为 34290 元。
- ✧ **男人更易上当，女人受伤更深。**2019 年网络诈骗受害者中，男性占比 66.9%，女性占比为 33.1%。从人均损失上看，女性人均损失更高，为 30740 元。
- ✧ **男性高危诈骗类型：金融、游戏、赌博。**男性举报量最高的网络诈骗类型为金融诈骗，共 2208 例。男性举报量第二高的网络诈骗为游戏诈骗，共有 1603 例。从人均损失上看，网络赌博诈骗是男性人均损失最高的诈骗，人均损失 70895 元。
- ✧ **女性高危诈骗类型：金融、兼职、交友。**与男性一样，女性举报量最高的网络诈骗类型为金融诈骗，共有 1106 例；女性举报量第二高的诈骗为兼职诈骗，共有 1083 例。交友诈骗是女性人均损失最高的诈骗，人均损失为 94542 元。
- ✧ **年轻人受骗多，老年人伤更深。**从 2019 年网络诈骗受害年龄分布及人均损失上看，80 后、90 后举报量最高，60 后、50 后人均损失最高。
- ✧ **金融诈骗老中青通吃 兼职诈骗瞄准大学生。**23 岁至 58+ 岁人群，举报最多的诈骗都是金融诈骗。18 岁至 22 岁人群，即大学生人群举报最多的诈骗是兼职诈骗。
- ✧ **社交平台成骗子“大舞台”。**QQ 成为受害者接触诈骗者或诈骗信息的最主要途径，占总量的 10.69%。其次为微信，占总量的 10.38%。
- ✧ **“直播间”诈骗人均损失最高。**通过“直播间”接触到的诈骗，造成的人均损失最高，为 134729 元。
- ✧ **花钱借钱都有坑。**在金融诈骗各类型中，投资类金融诈骗占比最高，占比 46.6%；贷款类金融诈骗次之，占比 45.6%。两类诈骗合计占金融诈骗总量的 92.2%，是最高发的两

类金融诈骗。

- ✧ **骗子蹭上“区块链”风口。**从各类型金融诈骗造成的人均损失来看，虚拟货币诈骗导致的人均损失最高，为 134522 元。
- ✧ **女性因金融诈骗损失“扎心”。**在各类型金融诈骗受害者人均损失中，男性损失均低于女性。女性人均损失最高的诈骗是虚拟货币诈骗，人均损失 181348 元。
- ✧ **金融诈骗“啃老”。**从人均损失看，18 岁至 52 岁，金融诈骗损失与年龄增长呈正相关趋势，年纪越大，人均损失越高。
- ✧ **交友诈骗主要靠转账敛财。**从各类型交友诈骗的举报量来看，交友转账占比最高，为 63.1%。交友投资占比为 19.1%，排在第二位。交友博彩占比 17.7%，排在第三位。
- ✧ **交友投资诈骗人均损失最高。**在各类型交友诈骗中，交友投资造成的人均损失最高，为 138791 元。
- ✧ **“刷单”成兼职诈骗最热门职业。**在兼职诈骗举报中，打着刷单名义的兼职诈骗占比最多，为 72.3%。兼职诈骗是指利用虚假兼职招聘为幌子，骗取用户钱财的诈骗方式。
- ✧ **大学生成兼职诈骗主要受害者。**在兼职诈骗中，18 至 22 岁人群为最大受害群体，占比 36.1%。该年龄段人群一般多为大学生。
- ✧ **女性更易遭受兼职诈骗。**在网络诈骗 Top10 类型中，兼职诈骗是唯一一个女性受害者占比高于男性的诈骗，女性占比为 59.4%。
- ✧ **奔五人群因兼职诈骗人均损失近 5 万元。**在兼职诈骗中，从女性人均损失上看，48 岁至 52 岁女性人均损失最高，为 34200 元；从男性人均损失上看，48 岁至 52 岁男性人均损失最高，为 60940 元。

目 录

第一章 网络诈骗举报数据综合分析	1
一、2014 年至 2019 年网络诈骗举报数量及人均损失	1
二、2019 年网络诈骗主要类型举报量与人均损失	2
三、2019 年网络诈骗各季度举报量与各季度人均损失	2
第二章 网络诈骗受害者画像	4
一、2019 年网络诈骗受害者地域特征	4
二、2019 年网络诈骗受害者性别特征	6
三、网络诈骗受害者年龄特征及人均损失	8
四、受害者被骗来源分析	10
第三章 典型网络诈骗类型分析	12
一、金融诈骗	12
二、交友诈骗	17
三、 兼职诈骗	20
第四章 2019 年网络诈骗六大变种	25
一、投资诈骗追风口：“炒外汇、黄金”变“区块链骗局”	25
二、贷款诈骗出续集：“零担保贷款”变“注销网贷账号”	25
三、交友诈骗换场景：从“微信加好友”到“短视频私聊、游戏组队”	26
四、中奖诈骗玩普惠：从“天降大奖”到“粉丝福利”	27
五、裸聊诈骗变敲诈：从“充会员”到“视频敲诈”	28
六、冒充公检法诈骗加戏码：从“远程忽悠”到“远程操控”	28
第五章 2019 年典型网络诈骗案例	29
一、ETC 诈骗“刷屏”：骗子追逐政策风口 李鬼短信里藏钓鱼链接	29
二、金融诈骗现“高仿潮”：山寨 APP“一条龙”行骗 网贷行业深受黑产困扰	30
三、双 11 诈骗“应景”：互助盖楼购物成风 骗子趁乱盖起“海市蜃楼”	30
四、车辆年检现连环套：假短信配上假公号 在线年检现“诈骗闭环”	31
五、骗子变戏精：《庆余年》全集资源便宜卖 转账之后被拉黑	33
六、交友诈骗专找知识盲区：网恋美国兵要定居中国 骗子编造名目行骗	34
七、网络诈骗产业化：60 人骗了 1 个亿 炒期货诈骗现上下游产业链	35
第六章 2019 年十大网络诈骗话术	37
第七章 春节期间常见网络诈骗预警	39
第八章 网络诈骗五大防范锦囊	40

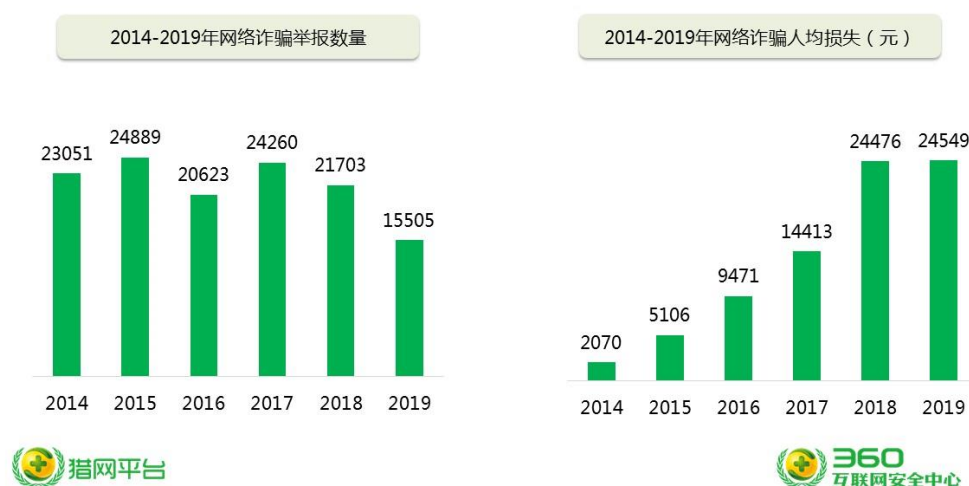
附录一：网络诈骗各类型定义	42
---------------------	----

附录二：猎网平台/联盟相关工作	44
-----------------------	----

第一章 网络诈骗举报数据综合分析

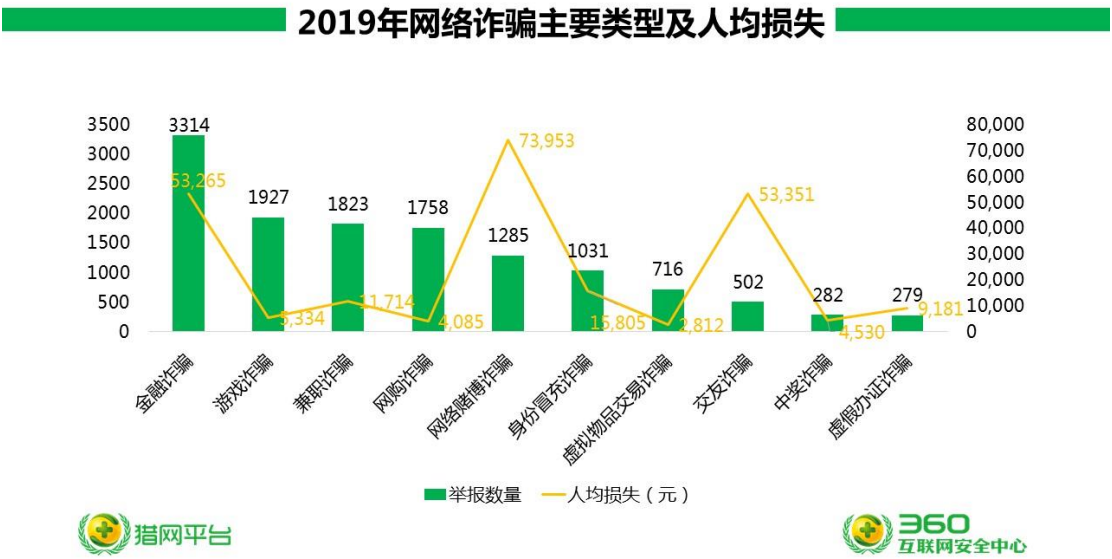
一、2014 年至 2019 年网络诈骗举报数量及人均损失

2014-2019年网络诈骗举报数量及人均损失



2019 年，猎网平台共收到有效诈骗举报 15505 例，举报者被骗总金额达 3.8 亿元，人均损失为 24549 元，较 2018 年人均损失略有增长。数据显示，2014 年至 2019 年，网络诈骗人均损失呈逐年增长趋势，至 2019 年，创下近六年新高。

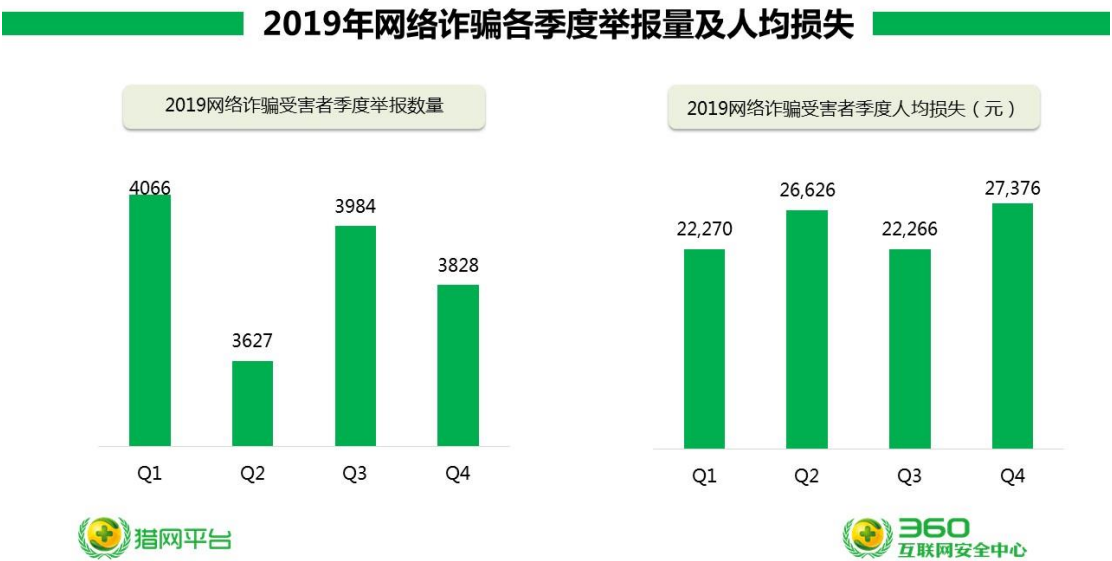
二、2019 年网络诈骗主要类型举报量与人均损失



2019 年，金融诈骗是举报量最高的诈骗，高达 3314 例。其次为游戏诈骗举报量 1927 例，兼职诈骗 1823 例。

从人均损失上看，人均损失最高的诈骗为网络赌博诈骗，人均损失高达 73953 元。其次为交友诈骗，人均损失 53351 元；金融诈骗人均损失 53265 元，是人均损失第三高的诈骗类型。交友诈骗人均损失较高，主要因为近期越来越多的交友诈骗都采取诱导受害人投资和赌博的形式，以骗取高额钱财。

三、2019 年网络诈骗各季度举报量与各季度人均损失



2019 年 Q1 季度举报量最高，为 4066 例，其次为 Q3 季度，为 3984 例。Q2 季度举报量最低为 3627 例。

从人均损失上看，Q4 季度人均损失最高，为 27376 元。通过举报数据梳理发现，Q4 季度网络赌博诈骗、金融诈骗较为高发，且这两类诈骗人均损失较高。Q2 季度人均损失数额排在第二位，为 26626 元。Q1 季度人均损失数额排在第三位，为 22270 元。

第二章 网络诈骗受害者画像

一、2019 年网络诈骗受害者地域特征

（一）维权意识哪里强？广东位居举报量之首

2019年网络诈骗受害者分布省份 Top 10

2019年网络诈骗举报数量Top 10省份



2019年网络诈骗人均损失 Top 10省份



2019 年，广东省举报量位居首位，占比 10.7%。山东位居第二位，占比 7.1%；河南位居第三位，占比 6.2%。

从人均损失上看，北京人均损失最高，为 39443 元；上海人均损失排在第二位，为 34867 元；福建人均损失排在第三位，为 34290 元。

(二) 广州位居举报量第一 莆田付出最贵人均损失

2019年网络诈骗受害者分布城市 Top 10



从城市维度看，广州位居举报量之首，举报量占比 2.10%。其次为深圳占比 1.65%，成都占比 1.62%。

从人均损失上看，福建莆田人均损失最高，为 66567 元，主要因为一些金融诈骗受害者损失较高导致，而这些金融诈骗都不约而同打着“区块链”、“数字货币”、“挖矿”的名义行骗。

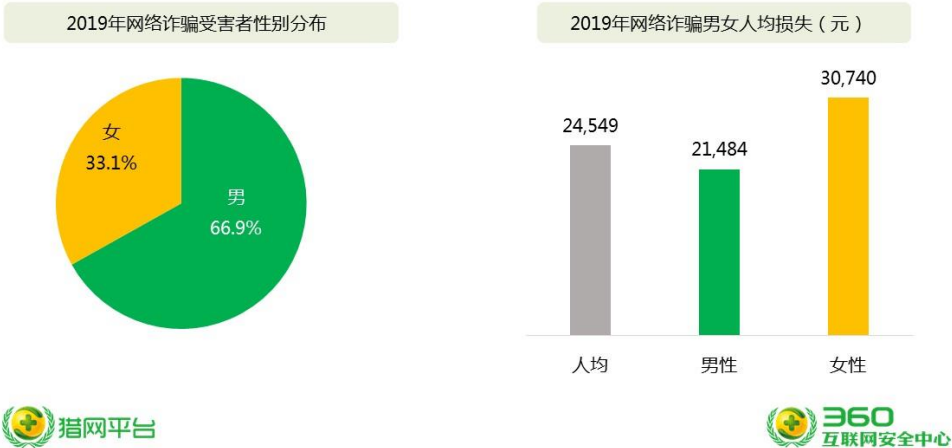
比如，有用户举报“万通启元”APP 诈骗后跑路。我们注意到这一 APP 在今年 6 月曾被媒体曝光，以虚拟货币融资为名，高收益诱惑投资者，等大量投资者上当后，便人去楼空。

此外，还有用户投诉 CantoEx 平台，称有骗子以老师之名带单炒“区块链—数字货币”。暗箱操作导致其亏损严重。也有用户举报 GCCX 交易所，该平台也曾被媒体曝光，指其虚假宣传，以区块链、挖矿等名义行骗。

二、2019 年网络诈骗受害者性别特征

（一）男人更易上当，女人受伤更深

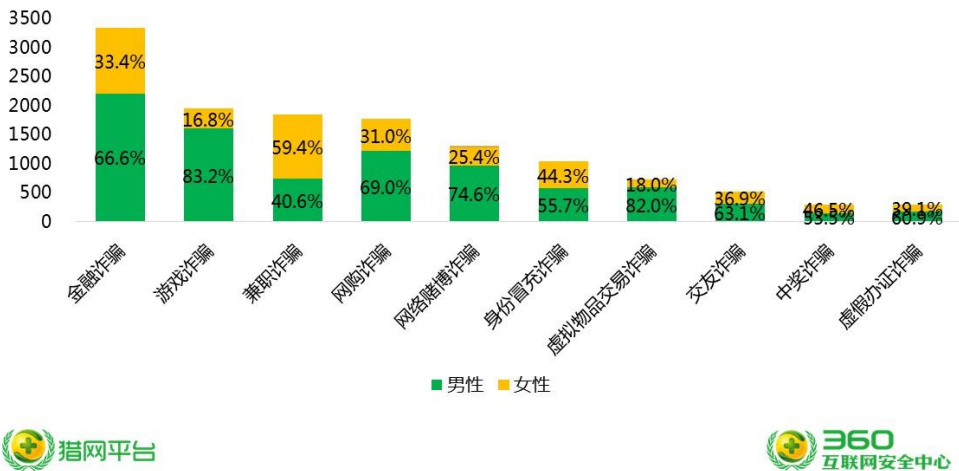
2019年网络诈骗受害者性别及人均损失



2019 年网络诈骗受害者中，男性占比 66.9%，女性占比为 33.1%。从人均损失上看，2019 年网络诈骗人均损失为 24549 元，其中女性人均损失更高，为 30740 元，男性人均损失为 21484 元。

（二）男性受害人数普遍高于女性 兼职诈骗是例外

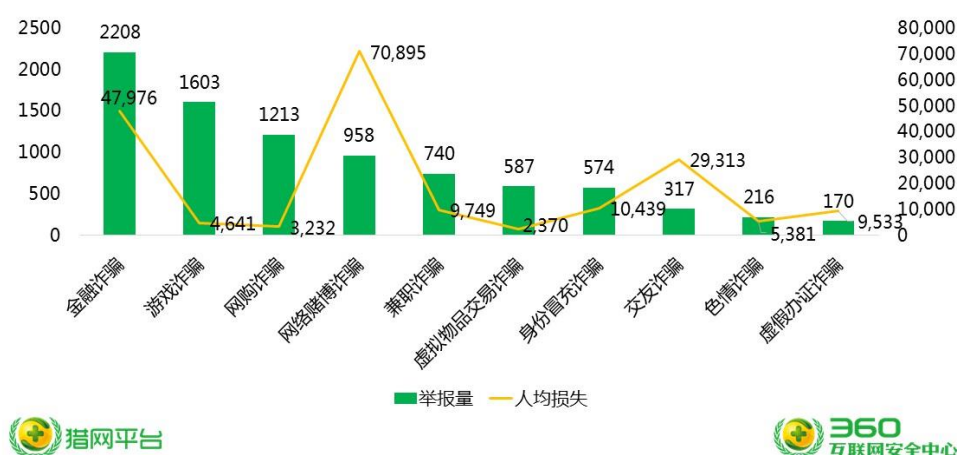
2019年网络诈骗类型及性别分布



在网络诈骗类型 TOP10 中，除兼职诈骗外，其它类型诈骗中男性比例均高于女性。尤其是在游戏诈骗中，男性占比高达 83.2%。网络赌博诈骗男性占比也远远高出女性，为 74.6%。兼职诈骗是唯一一个女性受害者占比高于男性的诈骗，女性占比为 59.4%。

（三）贪玩男性多遭游戏诈骗 因网络赌博诈骗损失最大

2019年男性网络诈骗主要类型及人均损失



男性举报量最高的网络诈骗类型为金融诈骗，共 2208 例。男性举报量第二高的网络诈骗为游戏诈骗，共有 1603 例。从人均损失上看，网络赌博诈骗是男性人均损失最高的诈骗，人均损失 70895 元。

（三）勤劳女性多中枪兼职诈骗 因交友诈骗破财最多

2019年女性网络诈骗主要类型及人均损失

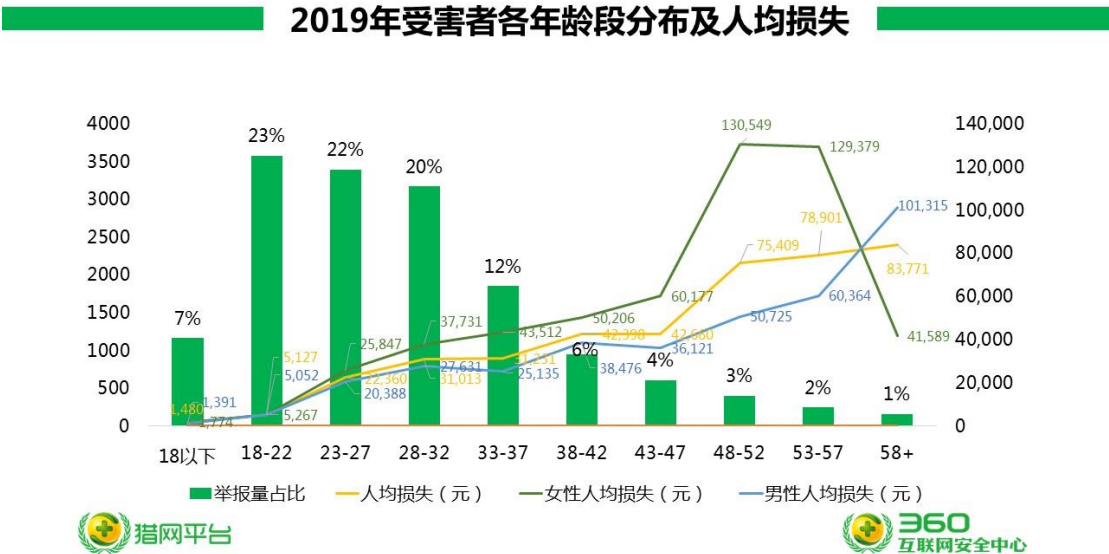


与男性一样，女性举报量最高的网络诈骗类型为金融诈骗，共有 1106 例；女性举报量第二高的诈骗为兼职诈骗，共有 1083 例。从相关举报案例分析发现，女性中赋闲在家的主妇、大学生为兼职诈骗的主要受害人群。

交友诈骗是女性人均损失最高的诈骗，人均损失为 94542 元。

三、网络诈骗受害者年龄特征及人均损失

（一）年轻人受骗多，老年人伤更深



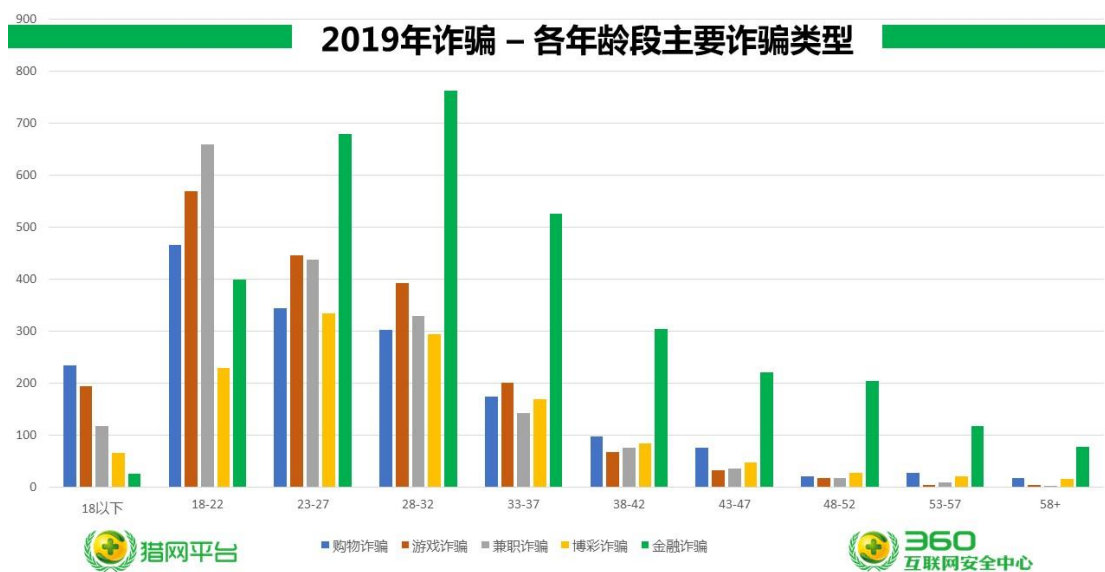
从 2019 年网络诈骗受害年龄分布及人均损失上看，18 岁-22 岁年龄段人群，举报量最高，占比 23%；23 岁至 27 岁人群举报量第二，占比 22%；28 岁至 32 岁人群举报量第三，占比 20%。该三大年龄段人群主要为 80 后、90 后。

值得注意的是，58 岁+（58 岁及以上人群）举报量最低，但人均损失也最高，为 83771 元。53 岁至 57 岁人群人均损失第二高，为 78901 元。48 岁至 52 岁人群人均损失第三高，为 75409 元。该三大年龄段人群主要为 60 后、50 后。相关举报数据显示，该年龄段人群多遭遇金融诈骗，这类诈骗往往损失较大（人均损失 53265 元）。60 后、50 后多为退休人群，有一定的经济基础，且具有较强的理财需求，应谨防误入金融诈骗陷阱。

整体来看，自 18 岁至 58 岁，举报量呈现从高到低的递减趋势，而人均损失趋势恰好相反，自 18 岁至 58 岁，人均损失大致呈从低到高的增长趋势。

从性别上看，各年龄段受害者中，男性数量均高于女性数量，但女性的人均损失普遍高于男性。

（二）金融诈骗老中青通吃 兼职诈骗瞄准大学生



从各年龄段人群网络诈骗举报情况来看，18 岁以下人群举报最多的诈骗是购物诈骗，其次是游戏诈骗、兼职诈骗。

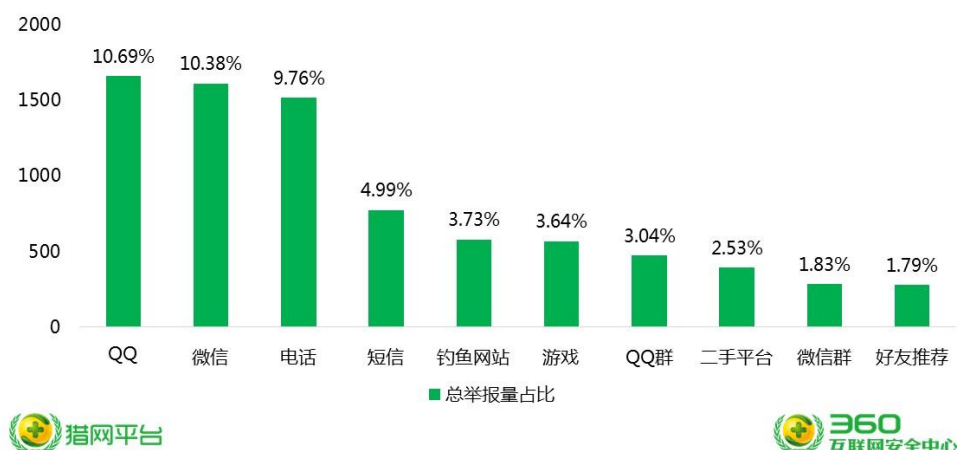
18 岁至 22 岁人群，即大学生人群举报最多的诈骗是兼职诈骗，其次是游戏诈骗、购物诈骗。

23 岁至 58+ 岁人群，举报最多的诈骗都是金融诈骗。

四、受害者被骗来源分析

（一）不要和陌生人说话：QQ、微信成骗子使用最高频工具

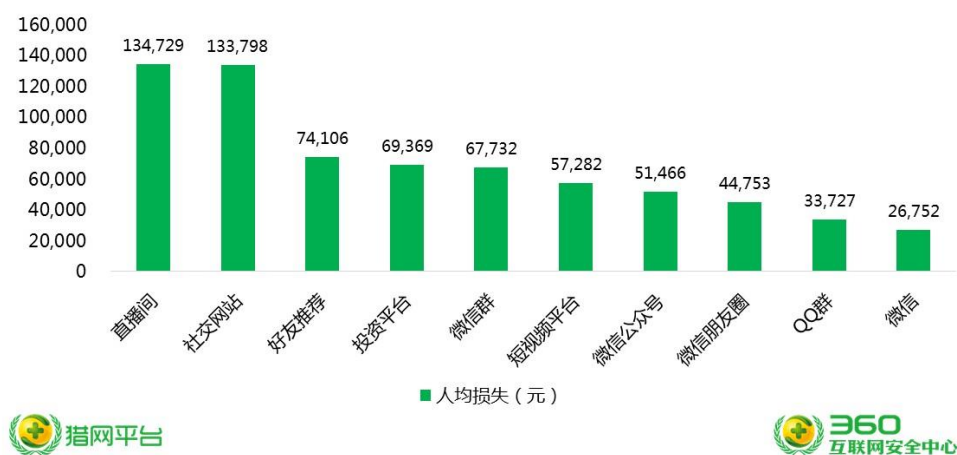
2019年网络诈骗主要诈骗来源 – 举报量



数据显示,QQ 成为受害者接触诈骗者或诈骗信息的最主要途径,占总举报量的 10.69%。其次为微信, 占总举报量的 10.38%。电话这种相对传统的工具,排在第三位, 占总举报量的 9.76%。可以看出, 社交平台 APP 正取代电话成为诈骗者实施网络诈骗利用最多的工具或路径。

（二）眼见未必为实：“直播间”诈骗人均损失最高

2019年网络诈骗主要诈骗来源 – 人均损失



从人均损失维度分析诈骗来源可见，通过“直播间”接触到的诈骗，造成的人均损失最高，为 134729 元。相关类型案例显示，这类直播间主要以“投资指导”、“股票交流”为名义设立，一般冠以涨停培训班、千万集中营、XXX 炒股大赛等名称，直播间主播多自称“导师”，会向观众推荐各类以炒“数字货币”为名的钓鱼理财平台。直播间观众往往夹杂大量“托”误导受害者。

因“社交网站”引发的诈骗，人均损失排在第二位，高达 133798 元。相关案例出现的社交网站，主要为婚恋交友网站，诈骗类型多属于交友诈骗，与陌生人交友需格外谨慎。

因“好友推荐”接触到的诈骗造成的人均损失排在第三位，为 74106 元。好友推荐为诈骗披上一层“信任”的外衣，因此也需注意。

此外，近期较火的短视频平台也榜上有名，排在第六位。

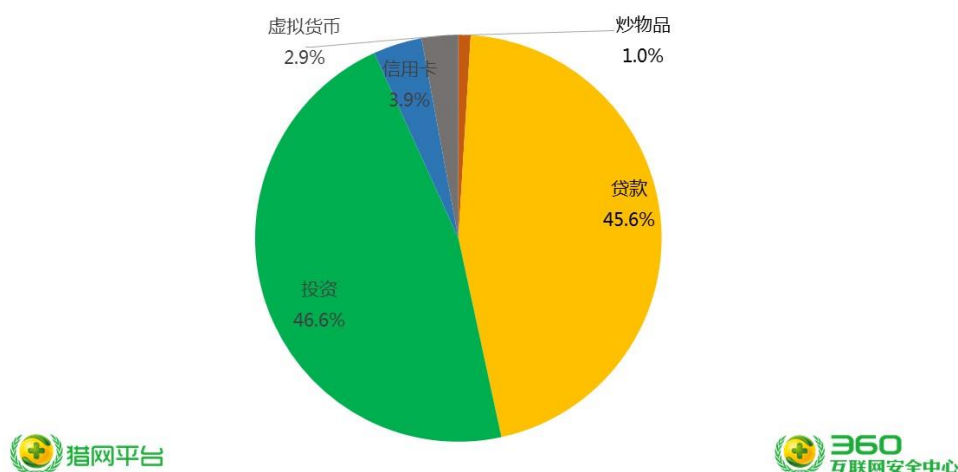
第三章 典型网络诈骗类型分析

本章根据举报量、人均损失、社会影响、舆论关注度等因素，选取金融诈骗、兼职诈骗、交友诈骗进行深入分析，以进一步透视这些网络诈骗特征。

一、金融诈骗

（一）花钱借钱都有坑 投资、贷款需求遭遇金融诈骗“双杀”

2019年金融诈骗各类型 – 举报量分布



在金融诈骗各类型中，投资类金融诈骗占比最高，占比 46.6%；贷款类金融诈骗次之，占比 45.6%。两类诈骗合计占金融诈骗总量的 92.2%，是最高发的两类金融诈骗。

投资类诈骗主要利用被害人的投资心理，以高额回报、人生赢家等案例，哄骗被害人下载理财 APP 软件或登录钓鱼网站，进行投资理财，但实际上受害人登录的网站、APP 都是由诈骗者人为操纵的，等受害人察觉时，前期投入钱财已转入骗子口袋。

虽然投资类诈骗套路大同小异，但投资“标的”却五花八门，最常见的是股票、期货、外汇及各种金融衍生品。此外，还有一些被巧妙包装的项目投资，比如电影投资、旅游券投资等。

在贷款类诈骗中，诈骗分子通过开设虚假网站、手机短信、网络广告等途径发布“无抵押贷款”、“低息贷款”、“免息贷款”等诱导性贷款信息，待受害人与其联系后，便谎称可以无抵押无担保贷款，并且以较低的利率申请到贷款取得受害人信任，再诱骗受害人通过银行转账形式预付利息、保证金、保险费、工本费等费用，从而达到诈骗目的。第一次转账后，不法分子往往以账户冻结需要解冻贷款等理由，让受害人继续转账。

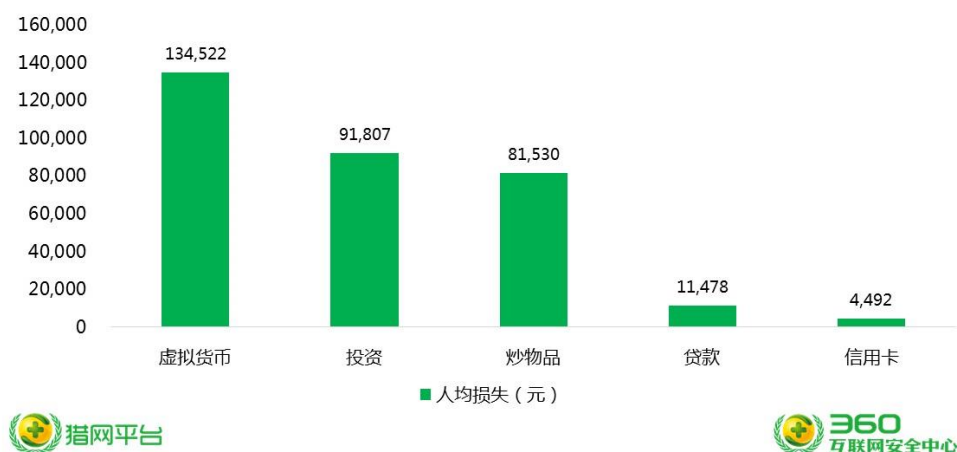


受害者提供的假冒“人人贷”的APP

值得注意的是，在贷款诈骗的大量举报案例中，一些诈骗分子通过假冒知名金融 APP 的形式实施诈骗，更容易骗取用户信任实施诈骗，大大提高了诈骗成功的可能性。

（二）虚拟货币人均损失最高 骗子蹭上“区块链”风口

2019年金融诈骗各类型 – 人均损失

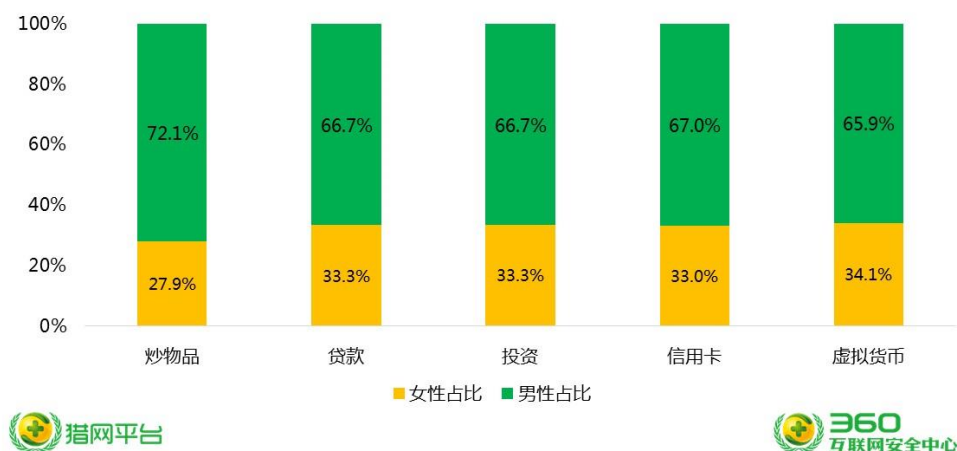


从各类型金融诈骗造成的人均损失来看，虚拟货币诈骗导致的人均损失最高，为 134522 元。投资类诈骗排在第二位，人均损失 91807 元；炒物品类诈骗排在第三位为 81530 元。

虚拟货币诈骗，主要冠以“区块链”、“数字货币”、“比特币”、“挖矿”的名义诱导受害者，本质上是诈骗分子跟风、蹭热点，以市场上的热门概念为幌子行骗。因为这些虚拟货币投资额较大，引发的人均损失也较高。

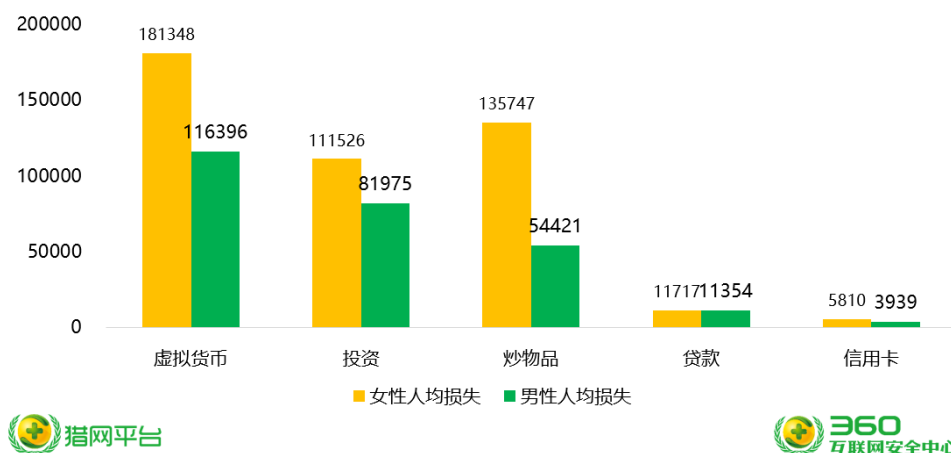
（三）男性成金融诈骗“易感人群” 女性人均损失“扎心”

2019年金融诈骗各类型 – 性别比例



在各类型的金融诈骗中，男性占比均高于女性，占比均超过六成。

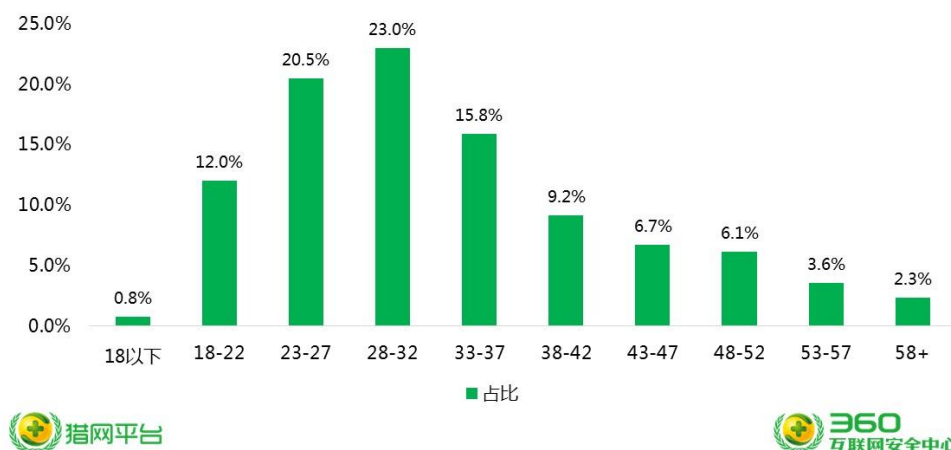
2019年金融诈骗各类型 – 男女人均损失对比



在各类型金融诈骗受害者人均损失中，男性损失均低于女性。女性人均损失最高的诈骗是虚拟货币诈骗，人均损失 181348 元。男性人均损失最高的也是虚拟货币诈骗，人均损失 116396 元。

（四）80 后、90 后成金融诈骗受害大户 年轻化趋势明显

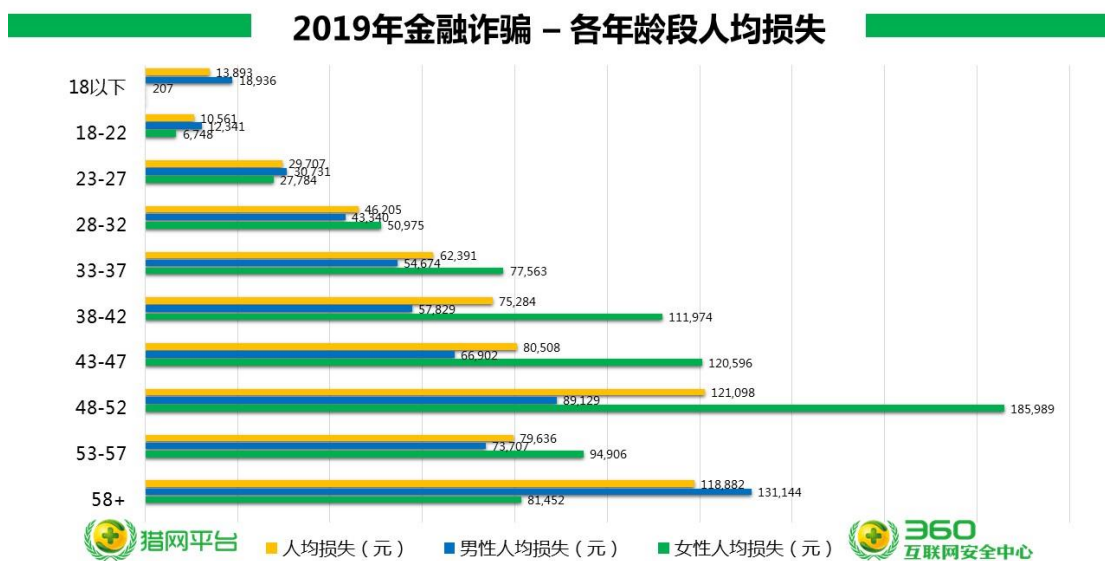
2019年金融诈骗 – 受害者年龄分布



在网络诈骗受害者人群中，28 岁到 32 岁人群最多，23 岁至 27 岁人群次之，33 岁至 37 岁人群排在第三位。这三个年龄段人群，主要为 80 后、90 后。

值得注意的是，18 岁至 22 岁人群受害者数量排名第四，占比 12%，该年龄段人群多为大学生。

（五）金融诈骗“啃老” 年纪越大人均损失越高



从金融诈骗举报者各年龄段人均损失来看，48 岁至 52 岁人群人均损失最高，为 121098 元。其中尤其以女性人均损失最高，为 185989 元。

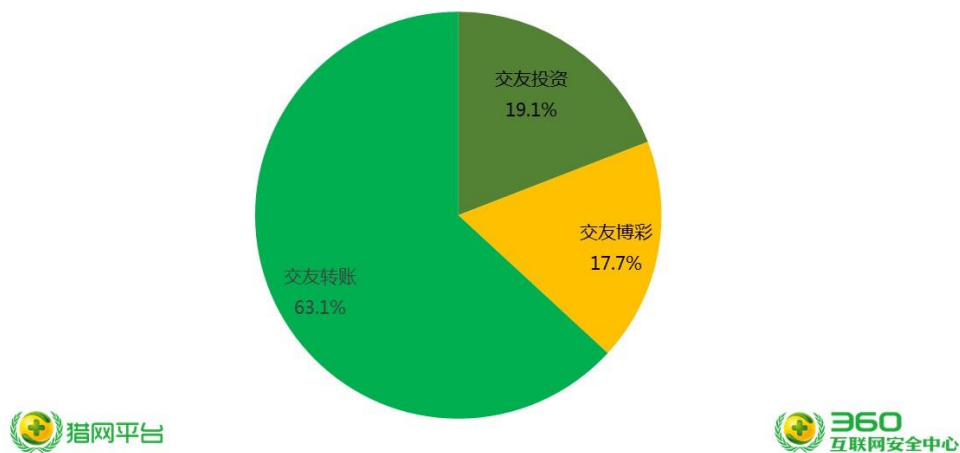
58 岁以上受害者，人均损失排在第二位，为 118882 元。43 岁至 47 岁受害者，人均损失排在第三位，为 80508 元。

从人均损失看，18 岁至 52 岁，金融诈骗损失与年龄增长呈正相关趋势，年纪越大，人均损失越高。这也基本与各年龄段的财富储备量较为相关。

二、交友诈骗

（一）交友诈骗套路多 转账剧本不断更

2019年交友诈骗各类型 – 举报量分布



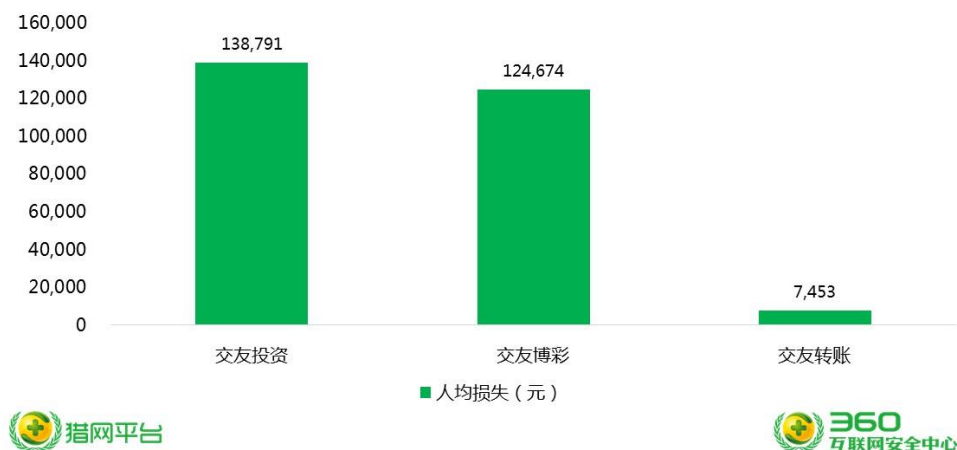
从各类型交友诈骗的举报量来看,交友转账占比最高,为63.1%。交友投资占比为19.1%,排在第二位。交友博彩占比17.7%,排在第三位。

在交友转账中,诈骗分子一般通过网上交友,与受害者建立感情后,再以各种理由骗取“车票钱”、“手术费”、“红包”。该类交友诈骗“剧本”很多,更新频繁。此前,也曾出现“卖茶女”、“支教女”、“维和部队军人”等热门交友诈骗套路。

交友投资、交友博彩骗术,也是基于交友建立感情行骗,但诈骗分子往往都会以“分享发财秘籍”一起赚钱等借口为由,诱导受害人与自己一起投资或参与赌博。

（二）“爱情+金钱”诱惑难挡 交友投资诈骗人均损失最高

2019年交友诈骗各类型 – 人均损失

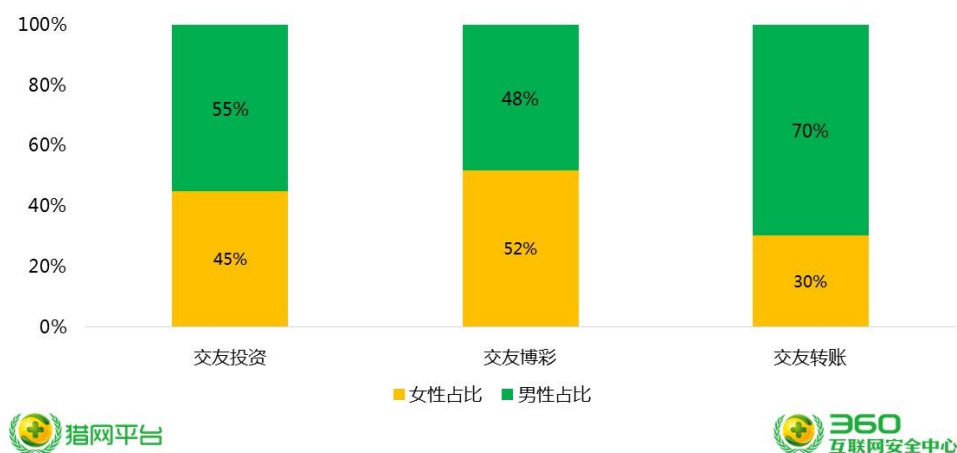


在各类型交友诈骗中，交友投资造成的人均损失最高，为 138791 元；交友博彩次之，人均损失为 124674 元。举报量较高的交友转账则人均损失最低，为 7453 元。

在交友投资、交友博彩类诈骗中，诈骗分子获得受害人信任后，会通过投资、博彩骗取更大额的金钱。在爱情、金钱的双重催眠下，受害人入戏更深，会付出更大的代价。

（三）交友转账诈骗受害者男多女少 交友博彩诈骗女多男少

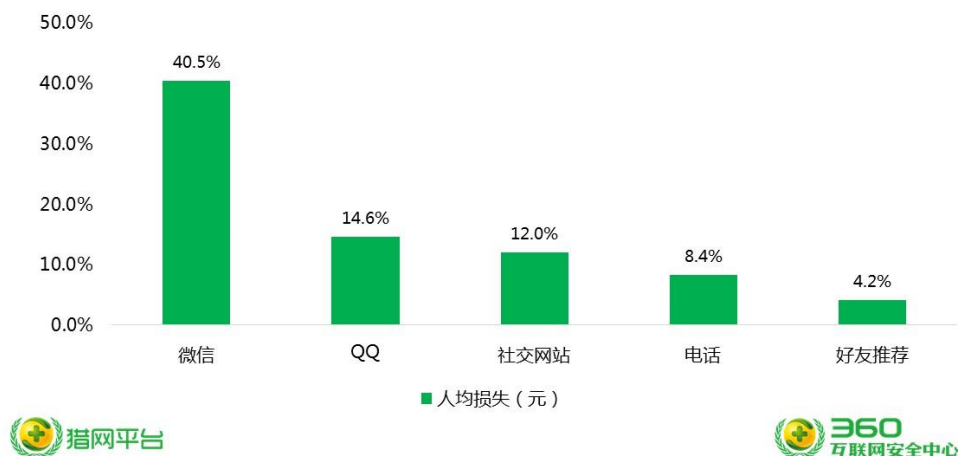
2019年交友诈骗各类型 – 性别比例



从交友诈骗受害者性别上看，交友转账诈骗中，男性受害者比例远高于女性，占比 70%。在交友博彩诈骗中，女性占比 52%，略高于男性占比 48%。

（四）加好友需谨慎 社交平台成交友诈骗“大舞台”

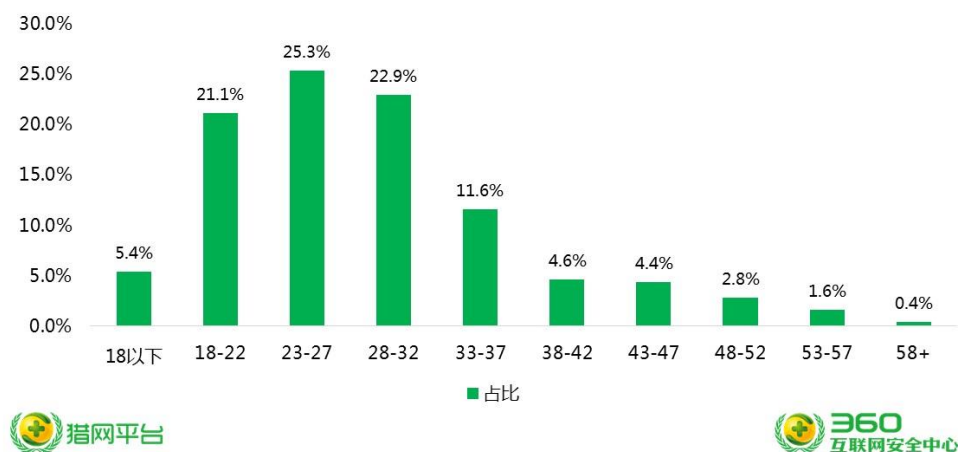
2019年交友诈骗 – Top5诈骗途径及占比



从交友诈骗的诈骗途径来看，微信、QQ 成为交友诈骗的最主要途径，合计占比 55.1%。交友诈骗依托交友聊天培养“感情”，社交工具成为诈骗分子利用最多的工具。

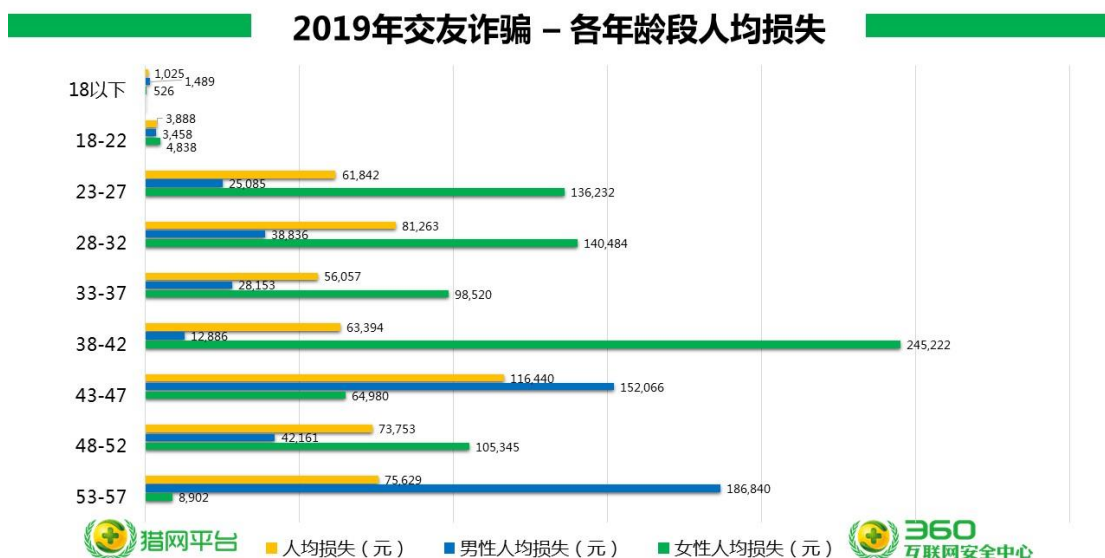
（五）80 后、90 后成交友诈骗主要受害人群

2019年交友诈骗 – 受害者年龄分布



在交友诈骗中，23 岁至 27 岁人群受害者最多，占比 25.3%。28 岁至 32 岁人群受害者数量排在第二位，占比 22.9%。18 岁至 22 岁人群举报量排在第三位，占比 21.1%。三大年龄段受害人群主要为 80 后、90 后。

（六）阅历丰富也被骗 43 岁至 47 岁受害者人均损失最高



在交友诈骗中，43 岁至 47 岁受害者人均损失最高，为 116440 元；28 岁至 32 岁受害者人均损失排在第二位，为 81263 元；53 岁-57 岁人均损失排在第三位，为 75629 元。

结合受害人性别与人均损失看，在 23 岁-27 岁、28 岁-32 岁、33 岁-37 岁、38 岁-42 岁、48 岁至 52 岁中，女性人均损失均高于男性。

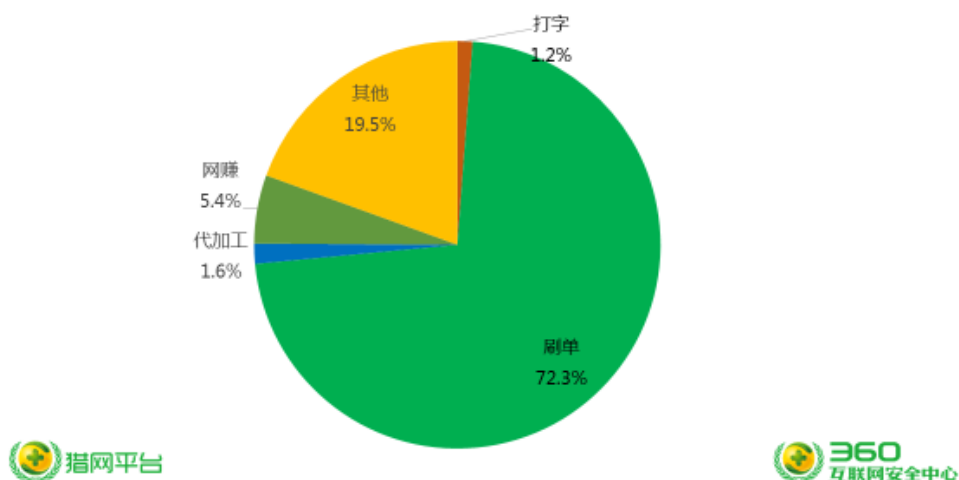
从女性人均损失上看，38 岁至 42 岁女性人均损失最高，为 245222 元。从男性人均损失上看，53 岁-57 岁男性人均损失最高，为 186840 元。

注：58 岁及以上年纪受害人群较少，不计入统计范畴。

三、兼职诈骗

（一）电商火帮忙坏骗子 “刷单” 成兼职诈骗最热门职业

2019年兼职诈骗各类型 – 举报量分布

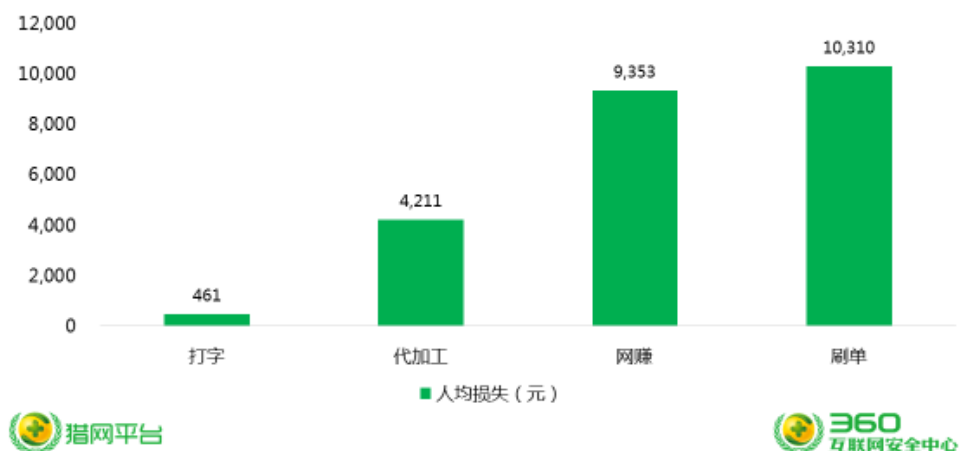


在兼职诈骗举报中，打着刷单名义的兼职诈骗占比最多，为 72.3%。兼职诈骗是指利用虚假兼职招聘为幌子，骗取用户钱财的诈骗方式。

刷单伴随着电商的兴起而来，店家付款请人假扮顾客，用以假乱真的购物方式提高网店的排名和销量获取销量及好评吸引顾客。这一行为被电商平台明令禁止，但生命力顽强，也由此衍生了刷单产业链。网络诈骗分子也盯上了这一灰色地带，通过发布虚假兼职广告吸引受害者上钩，再以小额订单成功返现取得受害人信任，然后用“任务未完成”、“卡单”等理由要求受害人多次付款，从中骗取钱财。

（二）刷单诈骗人均损失最高 兼职打字诈骗式微

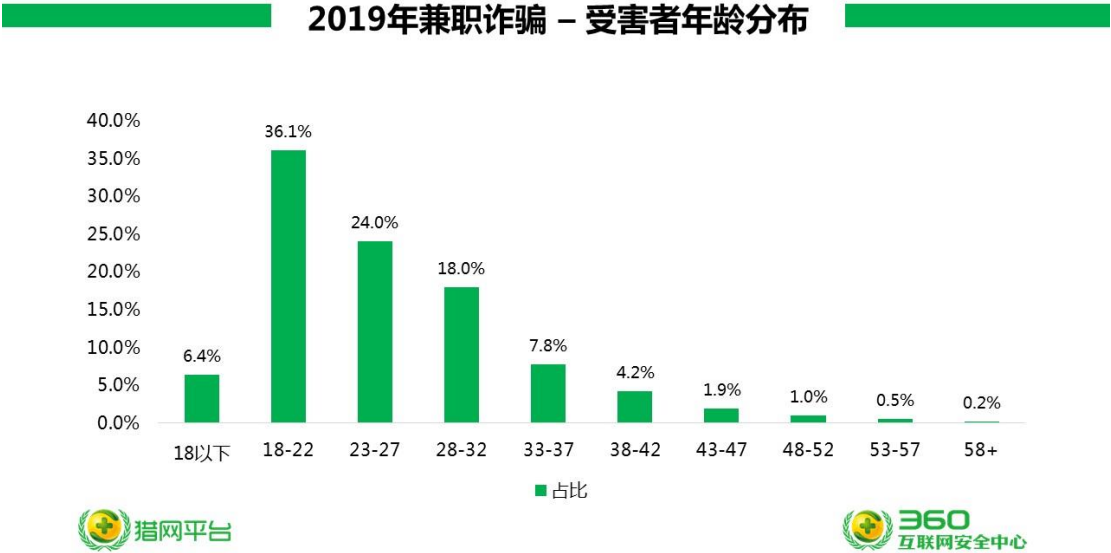
2019年兼职诈骗各类型 – 人均损失



在各类兼职诈骗中，刷单类兼职诈骗造成的人均损失最高，为 10310 元。网赚类兼职诈

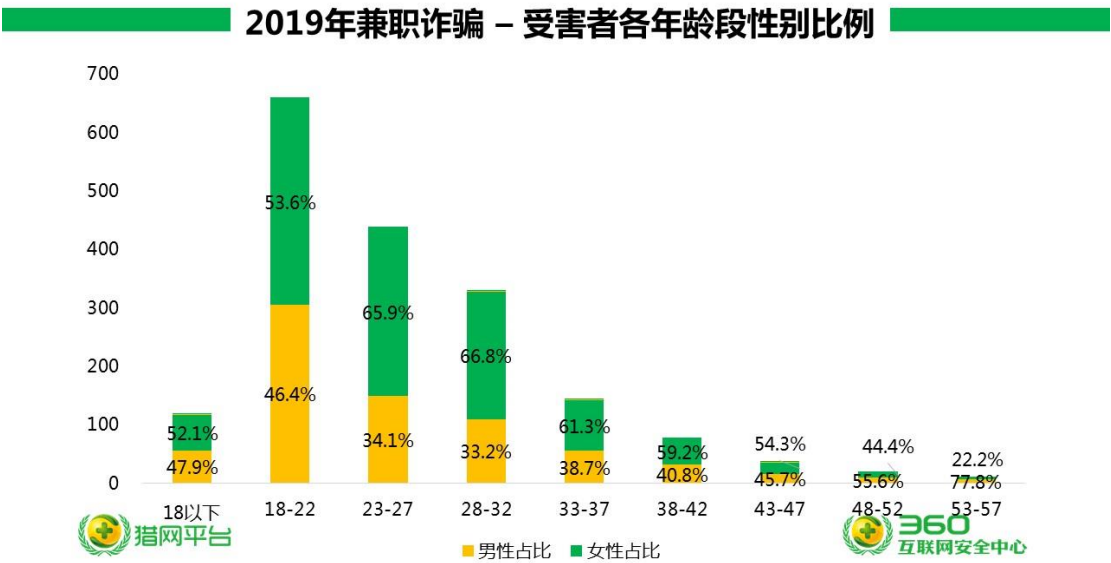
骗人均损失排在第二位，为 9353 元。打字类兼职诈骗人均损失最低，仅有 461 元。随着社会的发展，打字类兼职热度明显降低，此类诈骗也逐渐式微。

（三）有闲没钱 大学生成兼职诈骗主要受害者



在兼职诈骗中，18 至 22 岁人群为最大受害群体，占比 36.1%。该年龄段人群一般多为大学生；23 岁至 27 岁人群为第二大受害群体，占比 24%。28 岁至 32 岁人群为第三大受害群体，占比 18%。前三大受害人群合计占比 78.1%。可见 80 后、90 后是兼职诈骗的主要受害人群。

从 18 岁开始，受害者举报量与年龄呈负相关，年纪越大，举报量越小。

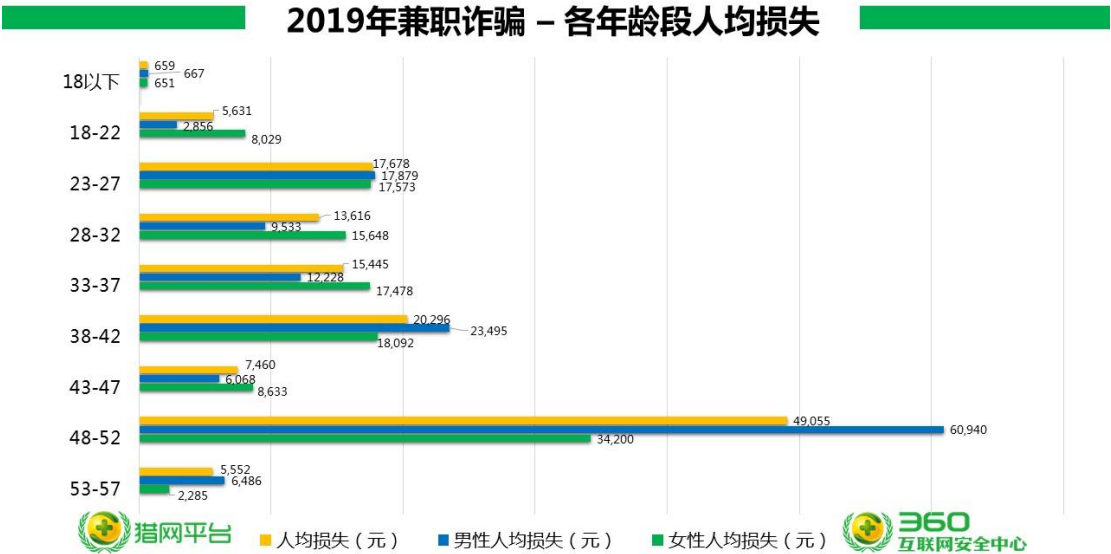


在上述网络诈骗类型 Top10 中，兼职诈骗是唯一一个女性受害者占比高于男性的诈骗，

女性占比为 59.3%。具体到各年龄段性别上看，从 18 岁至 47 岁，女性占比均高于男性。18 岁至 22 岁女性是举报量最高的人群。

注：58 岁及以上年纪受害人群较少，不计入统计范畴。

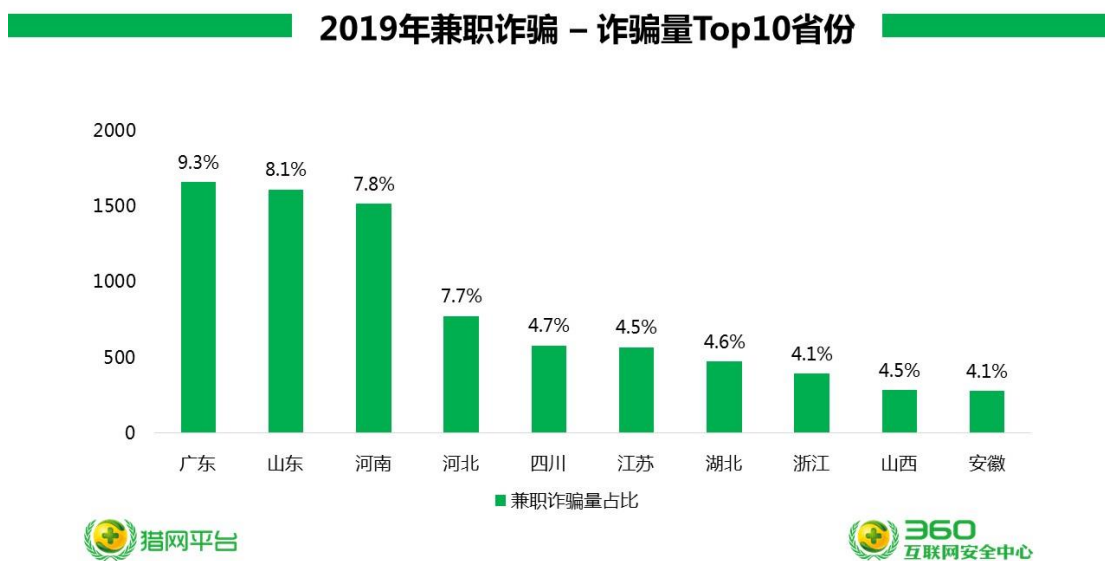
（四）知天命之年难淡定 奔五人群因兼职诈骗人均损失近 5 万元



在兼职诈骗各年龄段人均损失中，48 岁至 52 岁人均损失最高，为 49055 元；38 岁-42 岁人均损失排在第二位，为 20296 元；23 岁至 27 岁人均损失排在第三位，为 17678 元。

从女性人均损失上看，48 岁至 52 岁女性人均损失最高，为 34200 元；从男性人均损失上看，48 岁至 52 岁男性人均损失最高，为 60940 元。

(五) 广东兼职诈骗举报量最高 举报量占比 9.3%



在兼职诈骗受害者地域分布上，广东区域受害者最多，占比 9.3%。山东排在第二位，为 8.1%。河南排在第三位，为 7.8%。

第四章 2019 年网络诈骗六大变种

长期以来，网络诈骗形式不断更新迭代，新一代“变种”往往更具欺骗性与危害性。在本章中，报告根据网民举报与大量网络诈骗案例，总结提炼出一些常见网络诈骗类型的“变种”，以期引起广大网民注意。

一、投资诈骗追风口：“炒外汇、黄金”变“区块链骗局”

传统的诈骗方式：

过去，金融诈骗都打着炒外汇、黄金等名义诱导受害人，骗子会伪装成理财师、老师，在 QQ 群、微信群及各类平台接近有理财需求的潜在人群，博取信任，并逐步吸引受害人下载虚假的金融 APP 或登陆理财平台网站，实际上平台上受骗子控制。前期，骗子会以小投大回报让受害人初尝甜头，等受害人入戏渐深后就会套取其更多钱财。

最新的诈骗方式：

2019 年，尤其是随着国家层面对区块链行业的持续加码，爱蹭热点的网络诈骗分子也追逐这一“风口”，打着“区块链”、“数字货币”、“挖矿”的名义行骗。

一些不法分子打着区块链旗号推广宣传虚拟货币、资金盘，将区块链技术等同于虚拟货币，甚至出现“防范代币发行融资风险政策已过时”等言论，有的用“链”“挖矿”“IMO”“STO”等花样翻新的名目，披着区块链的“马甲”开展非法金融活动。

近期猎网也接到很多举报，有用户称“万通启元”APP 诈骗后跑路。我们注意到这一 APP 在今年 6 月曾被媒体曝光，以虚拟货币融资为名，高收益诱惑投资者，等大量投资者上当后，便人去楼空。

此外，还有用户投诉 CantoEx 平台，称有骗子以老师之名带单炒“区块链—数字货币”。暗箱操作导致其亏损严重。也有用户举报 GCCX 交易所，该平台也曾被媒体曝光，指其虚假宣传，以区块链、挖矿等名义行骗。

分析：

这一套路与传统的炒黄金、炒外汇类似，只不过嫁接上了数字货币、区块链的名头，新瓶装旧酒，更易蛊惑人心。在这些金融诈骗中，诈骗分子都用高收益、高回报诱导受害人，广大网民不可盲目被高收益误导，应谨慎选择金融平台。

二、贷款诈骗出续集：“零担保贷款”变“注销网贷账号”

传统的诈骗方式：

骗子直接以低零抵押、零担保、低利息、低门槛、30 分钟快速到账等口号，忽悠一些不具备到正规金融企业贷款却想借钱的人，随后再以各种理由索要包装费、保证金等，而受害人拿到自己的借款也是扣除了包括手续费、首周利息后的钱。

最新的诈骗方式：

骗子冒充网贷平台客服以网贷账号不注销会影响征信记录为由联系受害人，要求受害人注销账号，并以注销账号需先贷款，有了流水才能注销为由，要求受害人贷款，并将贷得款项直接转入骗子账户。

专家分析：

当大众都熟悉了一种诈骗模式后，骗子会“机智”地修改老剧本，以延长一种诈骗的生命周期。从“零担保贷款”到“注销网贷账号”，骗子紧跟金融行业的发展动向，并在网贷普及的现状下，见缝插针，以“影响征信”误导网民，确实有很强的蛊惑性。

三、交友诈骗换场景：从“微信加好友”到“短视频私聊、游戏组队”

传统的诈骗方式：

骗子通过相亲网站或社交软件结识受害人，在加为好友后，前期对受害人嘘寒问暖以获取好感，一旦两人发展成为恋人关系，骗子便会以各种理由骗取钱财，比如此前特别流行的“卖茶女”、“美国大兵”、“维和部队”诈骗套路；还有一些骗子称知晓某赌博网站漏洞，可以稳赚不赔，诱感受害人参与网络赌博、购买彩票、进行网上投资等，骗取钱款。

最新的诈骗方式：

新型交友诈骗转战抖音、快手、王者荣耀等热门平台，通过短视频营造虚假形象，吸引关注，并与受害者私信加微信，或者通过王者荣耀组队，再请求加微信语音“开黑”。当受害者加了骗子微信后，骗子会在朋友圈或者一对一聊天中，邀请对方玩另一款伪装成棋牌游戏的赌博类游戏，并以高收益、日赚 XXX 元吸引受害者。



分析：

骗子越来越“急功近利”，过去交友诈骗的“杀猪盘”会有漫长的培养感情阶段，但在游戏、短视频交友诈骗中，骗子会更简单直接，“不聊感情只谈钱”，加微信后诱导赌博行骗。

四、中奖诈骗玩普惠：从“天降大奖”到“粉丝福利”

传统的诈骗方式：

传统的中奖诈骗都是骗子群发虚假中奖短信，短信内容与热门综艺、活动中奖为噱头，称受害人成为某综艺节目的幸运粉丝。要求受害人点击链接填写个人信息，并以支付获奖的定金、税金等名目，诈骗钱财。

最新的诈骗方式：

骗子会利用一些具有一定粉丝量的社交平台账号，发布回馈粉丝活动，实际是简单直接的红包返利活动，比如受害人发 500 元，对方返还 600 元，受害人净赚 100 元。一步步诱导受害人参与大额返现，等受害人入戏渐深，对方就会以参与档位没有名额，需加钱提高档位，或者以转错、手续费、激活费等名义要求受害人再转账，如果受害人不信或者要求返钱，骗子则直接拉黑受害人消失，受害人付出的钱财也打了水漂。



分析：

天上不会掉馅饼，随着反诈宣传力度的加大，很多人已对中奖诈骗的传统套路有了免疫力，但却对粉丝返利没一点点防备。粉丝返利的套路比中奖诈骗更简单直接，但却很有效。其原因在于，骗子利用了粉丝对博主的信任。不明真相的受害人觉得博主有一定的粉丝量和影响力，再加上自己想贪小便宜的心理就参加了此类活动，最终被骗。广发网民切勿盲目相信各类博主，一些社交账号可能就是懂营销的骗子收购或长期经营的账号。

五、裸聊诈骗变敲诈：从“充会员”到“视频敲诈”

传统的诈骗方式：

通过广告、社交媒体群吸引受害人充值裸聊，包括充值入群，或者诱导受害人登录钓鱼网站，以充够多少金额才能具备“裸聊”权益为由，骗取受害人钱财。

最新的诈骗方式：

通过社交平台加好友后，骗子会伪装成“单身”、“感情经历坎坷”、“寂寞”女性，诱骗受害人下载直播软件，称可以裸聊，一旦受害人真的与骗子裸聊，骗子就会录制受害人裸聊视频，并通过挂马的直播软件敲诈，如不付钱就把裸聊视频发给通讯好友。

分析：

色字头上一把刀，裸聊诈骗生命力顽强，很多受害人难以抗拒裸聊的诱惑，愿意花钱“消费”。传统的裸聊诈骗一般都是披着“假裸聊”的幌子行骗，而在最近高发的裸聊诈骗中，骗子则“放长线钓大鱼”，以“真裸聊”套路受害人，并大肆敲诈。

六、冒充公检法诈骗加戏码：从“远程忽悠”到“远程操控”

传统的诈骗方式：

骗子伪装成公检法，通过电话、短信和社交软件联系受害人，称受害人涉嫌违法犯罪并发送伪造的通缉令，要求受害人协助调查，一步步忽悠受害人将个人财产转移至“安全账户”实施诈骗。

最新的诈骗方式：

骗子依然靠伪装成公检法人员，以涉嫌违法犯罪为由蒙蔽受害人，但当骗子获得受害人信任后，就会以检查受害人的银行卡、支付宝钱款流水记录为由要求其下载一款“调查软件”。实际上软件是远程监控软件，可远程操控、访问手机设备的软件。受害人一旦下载软件，骗子就可以轻松转走受害人银行卡里的钱款。

分析：

冒充公检法诈骗“经久不衰”，其蛊惑性不容忽视。这一冒充公检法诈骗新变种在整体诈骗步骤上与传统套路类似，只是加了下载监控软件的戏码，可别小看这一举动，很多受害人会在骗子让其转账到“安全账户”时幡然醒悟。一旦有了监控软件，骗子诈骗成功几率大大提升，过去单纯的远程忽悠，也变成了更有效的远程控制。

第五章 2019 年典型网络诈骗案例

一、ETC 诈骗“刷屏”：骗子追逐政策风口 李鬼短信里藏钓鱼链接

最近各个银行都在推广 ETC 业务，有用户办理 ETC 后，却收到了一条短信：“尊敬的车主您好，您的 ETC 审核流程还未完成，请点击以下链接尽快完成，办理即送 200 元。”看到最后一句“办理即送 200 元”，用户起了疑心，询问银行后才知是诈骗短信。

除了上述案例外，也有用户向猎网举报，称收到以“ETC 系统更新，需及时认证二次信息”要求用户登录某网站办理的短信。实际上该网址为钓鱼网站。



还有新闻曝光，今年 8 月，李小姐通过微信办理了 ETC 业务，后来想取消，但客服电话因排队人数太多无法接通。着急的李小姐在网上搜索到了一个自称是 ETC 客服的电话号码，电话那头亲切熟练的客服语气，使李小姐对对方的话语深信不疑，便按对方要求提供了自己的姓名、身份证号码，随后通过微信收付款转账功能，向对方提供的银行卡账号转账 2823 元。

紧接着，对方声称需添加其 QQ 进一步操作，并要求李小姐拿出一张余额 6000 元以上的银行卡，再按照之前操作转账。此时李小姐才明白自己被骗，报了警。

案例分析：

今年 3 月全国两会期间，《政府工作报告》中提出“两年内基本取消高速公路省界收费站，实现不停车快捷收费”，拉开了 ETC 推广的大幕，各地银行纷纷加大落实力度。骗子瞄准了这一潮流，借机编织了“ETC 诈骗”。通过伪装的电话号码发送“二次认证”、“审核未完成”等信息，以诱导受害人上钩。据猎网监测，今年下半年冒充 ETC 的钓鱼网站的日均拦截量高达 7-8 万次。猎网提醒，一定要到正规渠道办理业务，有疑问可拨打银行官方电话进行咨询。

二、金融诈骗现“高仿潮”：山寨 APP “一条龙” 行骗 网贷行业深受黑产困扰

目前,一种以山寨知名金融 APP 方式的金融诈骗开始抬头。诈骗分子通过制作山寨网贷网站、app 进行钓鱼,并在系统后台植入木马、病毒。当被害人遇到这些山寨网贷平台,不仅没法借到钱,甚至还会被窃取个人信息。

根据国家互联网金融风险分析技术平台发布的监测数据显示,截至 2019 年 6 月 30 日,共发现互联网金融仿冒网页 4.8 万个,受害用户 12 万人次,互联网金融仿冒 APP 2801 个,累计下载量 3343.7 万次。

由于这类山寨 APP 的名称、图标甚至用户体验都与正版 APP 的相似度极高,让大多数用户都难以分辨。根据调查,目前应用市场当中主流的各大网贷 APP,基本上都存在着仿冒的现象,有的平台甚至还存在多个。

在这类诈骗中,不法分子借用部分网贷机构的名义,采取各种手段诱骗侵吞借款人保证金,然后逃逸跑路,致使一些借款人遭受不同程度的财务损失。较为常见的现象有:开发不同名目的仿冒 App,伪造“证据链条”,制造借贷成功假象;在微信小程序中添加外部链接,伪装成快速借款入口;伪造工牌、盗用正规金融公司办公场所视频,冒充平台客户经理、业务人员、客服,编造返现、折扣优惠的噱头。直到借款人发现借款迟迟未能到账,向实名平台投诉时,才发现误入不法分子的“仿冒骗局”。

案例分析:

区别于传统的电信诈骗,这类骗局直接利用山寨网贷 App 实施犯罪活动,更加令受害者防不胜防。不法分子的伪装周密,不仅使用高仿 APP,甚至还伪造知名金融公司工牌,盗用办公场所视频,发送虚假定位。

在下载金融 APP 的过程中,一定要慎重,在正规渠道下载 APP 的同时,也要仔细查看确认图标是否清晰,软件内部图文是否清晰,能否正常启动、使用,功能是否正常,如果不能正常启动使用,那么多半是仿冒 APP。

虽然高仿 APP 层出不穷防不胜防,但是用户只要把握住一个原则,就能跳出这些新型诈骗陷阱。这个原则就是:任何正规合法的网贷机构,不会通过各种名目来收取所谓的保证金、管理费等费用,更不会通过私人账户来收取这些费用。

三、双 11 诈骗“应景”：互助盖楼购物成风 骗子趁乱盖起“海市蜃楼”

双十一已经成为全民消费节日,每逢双十一,各大平台为冲业绩纷纷都会做起各类预热活动。今年双 11 期间,猎网接到骗子以双十一活动展开诈骗的举报信息。据山东省长治市的赵同学称,其被某网购平台推出的“盖楼”活动所吸引,该活动是通过两只队伍 PK,根据所盖楼层的高矮和等级来衡量胜负,楼层越高的队伍,瓜分的红包数额也就越大。为了获得更多人的助力,不少“志同道合”的陌生人组成了盖楼互助群。



就在赵同学为了超越对手尽快达到“盖楼目标”所烦恼之际，看到了某个互助群里发布的一则“可以帮盖楼、偷塔，有意向可以加微信或QQ沟通”的消息。于是便按照所发信息加上了对方的微信。在得到对方“付款成功就可进行助力盖楼，而且还能拿得冠军”的保证后。赵同学把盖楼链接发给对方并通过微信转账8元。但是，付款后对方不再回复赵同学的任何消息。此时，赵同学意识到自己被骗了。

案例分析：

骗子善于跟风凑热闹，浑水摸鱼。历年双十一，骗子都会根据大平台官方活动编造新剧本行骗。在这一诈骗中，骗子利用大家想要尽快达成“盖楼目标”夺得冠军，从而获得更高红包的心理，骗取受害人进行转账。消费者要理性对待网购平台中双十一的各项活动，以免因小失大。

四、车辆年检现连环套：假短信配上假公号 在线年检现“诈骗闭环”

在各级政府不断推行行政程序便民化的背景下，不少官方部门都相继开通了线上服务功能，极大地方便了广大群众的日常生活。不过近日，全国首个警民联动的网络诈骗信息举报平台——猎网平台接到举报，有不法分子假造车管部门公众号，以线上缴纳车辆年检费的名义，非法窃取受害车主的银行卡账号及密码，实施电信诈骗。对此，猎网平台提醒广大用户：注意保护个人隐私信息，不要轻易将其对外透露。

前不久，霍先生收到一条陕西车管所发来的短信通知，称他的车辆六年免检已到期，可在微信中搜索并关注“陕西在线年检”公众号进行线上年审。霍先生想到自己的车确实需要

年检，便未对此产生怀疑，于是通过手机微信关注并进入到了该公众号。



霍先生按照公众号提示输入了自己姓名后，该公众号便发来一条网址，要求他点击网址缴纳 200 元年检费用。随后，霍先生点击网址，发现网站是银联网站页面，便又按照要求在该网站输入了自己的银行账户、银行密码、手机号码等个人信息。



输入完毕后，手机收到验证码，霍先生也未详细查看，便将验证码输入到了网站的输入框内。不曾想，霍先生没多久又在手机上收到了验证码短信，他仔细一瞧才发现，这是支付 4999 元的短信，这才反应过来刚才支付了 4999 元，收款方则显示是一个广州商贸公司。直到此时，霍先生才意识到自己被钓鱼短信、钓鱼网站给骗了。

案例分析：

本案中，诈骗分子利用短信平台向广大用户发送虚假在线年检的短信，引诱受害人访问公众号。接着，诈骗分子又利用公众号给受害人发送钓鱼网址，骗取受害人的个人信息、银

行账户等信息进行盗刷。在这一案例中，各类假平台形成了诈骗闭环，让受害人身在骗局不知骗。

五、骗子变戏精：《庆余年》全集资源便宜卖 转账之后被拉黑

最近人气网文 IP《庆余年》同名电视剧正在热播。剧情跌宕起伏，引人入胜，不少人开始不满足于视频平台的更新集数，纷纷在网上搜索各种资源，这无疑给了不法分子可乘之机。

近日，猎网平台接到举报，家住广东省茂名市的梁同学，最近看人气网剧《庆余年》入了迷，为了能获取到更多的集数，梁同学开始在网上搜索各种资源。最终“皇天不负有心人”，梁同学在某贴吧中发现了一个帖子，上面称：开启付款会员即可观看《庆余年》全部集数，有意者扫码加微信联系。



看剧心情急迫的梁同学想都没想就加了对方的微信。添加微信好友成功后，对方发来了一条资源链接，并称想要全部资源需先付款 30.28 元。在核实对方发来的链接可以看后，梁同学毫不犹豫的向对方扫码支付了 30.28 元钱。可就在梁同学等待对方发来全集资源的时候，对方却把梁同学拉黑，这时梁同学才反应过来自己上当受骗了，很快来到猎网平台进行举报。

案例分析：

如今骗子大多借势诈骗，值得注意的是，在这类借势诈骗中，骗子屡屡得手。当骗术与各类热点结合，人们就容易被抢眼的热点所蒙蔽。无论如何，涉及钱财交易时一定要三思而后行。

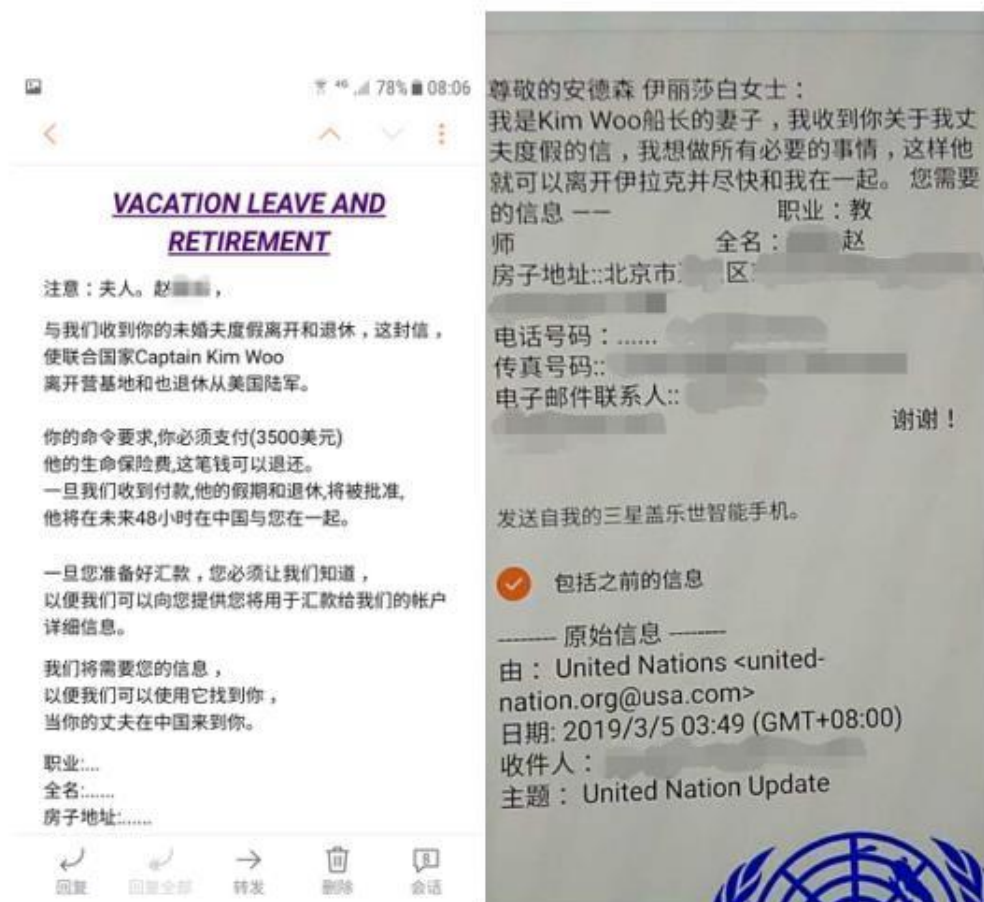
六、交友诈骗专找知识盲区：网恋美国兵要定居中国 骗子编造名目行骗

2019年3月,河北的赵女士通过社交软件,结识了一位自称在伊拉克执行任务的美国指挥官 Kim Woo,两人相谈甚欢,“美国指挥官”提出了休假来见赵女士的想法,并计划申请退休准备定居中国,但由于目前仍在伊拉克执行任务,不方便向上级直接发休假邮件,便希望赵女士以妻子的身份代其向上级请假。随后,赵女士按照“美国指挥官”的要求,向其上级联合国军事部的安德森伊丽莎白发送了申请休假以及退休的邮件。



邮件发送成功后不久,赵女士收到了“美国指挥官”上级安德森伊丽莎白的回复邮件。邮件中称,同意 Kim Woo 的休假和退休申请,但需要赵女士为 Kim Woo 支付 3500 美元的生命保险费。赵女士便按照对方要求,将 3500 美元转到了指定账户。

结果,完成转账后,对方又提出需赵女士缴纳 6.3 万元的人民币的新要求。这时,赵女士才反应过来,自己可能是被骗了。然而,不管是发邮件要求退还 3500 美元的生命保险费,还是联系“美国指挥官”的 Kim Woo,都已没了音讯。



案例分析：

本案中，骗子就是利用网民对外国人的好奇心，冒充“维和士兵”、“指挥官”等身份，并以各种借口索要费用。值得注意的是，这类美国大兵定居中国的剧本利用了大众的众多知识盲区，更易得手。

七、网络诈骗产业化：60 人骗了 1 个亿 炒期货诈骗现上下游产业链

2019 年 11 月 8 日，在公安部组织的“云剑”专项打击行动推进中，潮州市、温州市两地反诈骗中心主导侦查，360 猎网平台进行大数据支撑，最终行动专案组在温州市鹿城区、湖州市长兴县的等 20 余处窝点同步开展收网行动，抓获嫌疑人 60 余名。历时半年，这起涉案金额过亿，被害人超 3000 人的特大“炒期货”电信网络诈骗案告破！

据悉，犯罪嫌疑人唐某和刘某皆来自浙江省长兴县，因长期从事自由网络工作对国际期货的盈利模式、国际期货在国内的蔓延规律和作案方式有了较深了解。两人一拍即合，开始筹划犯罪。

刘某负责在网络寻找客户资源和代理渠道，唐某通过人脉关系寻找非法平台。2019 年 5 月份，唐某在温州鹿城朱某和韩某的帮助下，在香港某期货公司开户，为了应对国外炒期货的高额保证金，唐某和韩某形成上下级代理关系，由韩某在国外用美金充值保证金，解决外汇垫资的问题，并向韩某上交一定数额的手续费。

在国内，该团伙假冒香港合法期货公司的名义搭建交易网址，实现网站出入金和在线开户。借助温州团伙朱某、韩某，接入国际期货交易行情，搭建出给客户使用操作柜台（PC端和手机端软件）。

2019年6月至2019年11月，在平台非法运营期间，唐某和刘某及其团伙，招聘60余名业务员、财务等工作人员，以渠道商的身份，通过QQ或者微信、百度贴吧等对外招商，发展各级代理商。

最终由终端代理以冒充“老师”、“分析师”、“托”等开直播，拉建跟单群等等，欺骗广大不明真相的客户“投资”，最终被高额的手续费、汇率费、出金费等消耗一净。并通过频繁变更窝点、补偿投诉客损等手段逃避侦查。

案例分析：

据最高法称，绝大部分电信网络诈骗犯罪都是团伙作案，个人作案的比较少，近年来打掉的犯罪团伙几十人、上百人的屡有出现。司法大数据也反映出三人及三人以上的网络诈骗案件占比呈上升趋势。必须警惕的是，网络诈骗日渐产业化、组织化大大加大了诈骗的“效率”，让诈骗更易得手。

第六章 2019 年十大网络诈骗话术

在本章中，报告从 2019 年高发且影响力较大的网络诈骗案例中，选取诈骗者常用话术或关键话术，梳理、总结为“2019 年十大网络诈骗话术”，当网民看到、听到以下类似话语时，要格外注意，谨防被骗子“套路”。

一、区块链应用场景落地，XX 币躺着也能赚大钱

早在 2017 年，国内虚拟货币交易和相关交易所就被监管叫停，但随着近期国家明确提出对区块链技术的支持，一些不法分子蹭热点行骗，推出各种所谓“币”、“链”类高收益科技投资项目，实际是蹭政策热点的诈骗、传销、非法集资活动。

二、您的信用额度不够，需要刷流水，请缴纳 XX 现金证明还款能力

骗子通过贷款广告吸引受害者，等受害人入套后，会以银行记录不好、流水账不足、没有还款能力证明等，提出要预存占贷款额度一定比例的现金到个人银行卡。只要你肯转钱，他总有各种理由，直到你发现自己被骗。

三、某金融服务已经被国家下架,需要您配合注销信贷账户,否则将影响个人征信

骗子冒充网贷平台客服以网贷账号不注销会影响征信记录为由联系受害人,要求受害人注销账号,并以注销账号需先贷款,有了流水才能注销为由,要求受害人贷款,并将贷得款项直接转入骗子账户。

四、亲爱的，我有个发大财的机会

交友诈骗(杀猪盘)的惯用伎俩，骗子通过与受害人网恋后，会与受害人分享发财机会，比如自己是做 IT 的，发现了某金融平台漏洞可以套利。骗子还会为这一违法行为披上伪装，劝受害人为了双方未来生活、家庭幸福考虑，以打消受害人疑虑。等受害人入套，就会人财两空。

五、您的 ETC 审核流程还未完成，请点击以下链接尽快完成

随着各地 ETC 政策的出台，各地银行纷纷加大落实力度。骗子瞄准了这一潮流，借机编织了“ETC 诈骗”。通过伪装的电话号码发送“二次认证”、“审核未完成”等信息，以诱导受害人上钩。

六、加微信，躺着都能赚钱

好奇害死猫。如果有人在网上留微信号，还打着“网赚”的幌子现身说法鼓吹发财商机，你可要小心了。骗子们只说能赚大钱，却对所谓的“网赚”方式大卖关子，目的就是吸引你加微信。等你加了，可能就会被骗子拉进群，被花言巧语的托，骗入投资或者网络赌博陷阱。

七、回馈粉丝，给我发红包，我三倍返还

这是最新的中奖返利类诈骗，骗子会利用一些具有一定粉丝量的社交平台账号，发布回馈粉丝活动，实际是简单直接的红包返利活动，在返利过程中，受害人会以加钱提高档位，或者以转错、手续费、激活费等名义要求受害人再转账，直至骗局败露，受害人被拉黑。

八、办理各类职称证书，不用考试直接拿证

虚假办证类诈骗惯用话术，骗子声称不用培训、考试，只要交钱，就能“买到”各类职称、学历等证件。为了打消你的疑虑，骗子还会保证“免考办真证，可以官方网站查询”，实际上，骗子会将办证网民身份信息录入虚假网站，以备办证网民验证查询。

九、免费送 XX，活动真实有效

“免费送”骗局常见话术，在一些二手交易平台、公众号、朋友圈中，骗子以各种五花八门的理由免费送手机、耳机、公交卡、书籍、手环等。看宣传说明，这些产品都高大上，甚至有苹果手机、Beats 耳机、索尼相机，当下单后会支付运费，但收到产品后你会发现实物与宣传相差悬殊，价值远低于运费。通过这一骗术，骗子可以轻松赚取运费差价，另外也有骗子以包装费和手续费为由让你先交钱。

十、招聘快手抖音点赞员

传统电商平台“兼职刷单”诈骗的变体，骗子把阵地从“淘宝”转移到了“抖音”等软件中。在这一类诈骗中，骗子会让受骗者“试做”一单赚取收益，等受骗者放松警惕后，就会要受骗者“开通工作后台”，“暂时垫钱”买某软件的 VIP 激活码，并以“后续没有任何费用”诱感受骗者。

第七章 春节期间常见网络诈骗预警

一、春运大潮来临 警惕抢票类诈骗阻归途

年底春运高峰，大家都着急购买火车票、飞机票返家，骗子会跟风诈骗，宣称帮忙抢购火车票，诱导受害人登陆钓鱼网站，或者售卖专业代刷票软件，受害者支付后要么被骗子拉黑，要么下载了木马软件。猎网平台提醒广大网民购买火车票、飞机票一定要登陆正规官方网站，通过正规渠道购买。

二、大学生归巢 小心游戏诈骗凑热闹

游戏类诈骗在寒暑假期间较为高发，临近春节，很多大学生回家过年，闲暇时间增多，而各大游戏平台也推出五花八门的春节活动。此时应警惕骗子趁虚而入，利用“低价”买卖游戏装备的方式，吸引受害人登录虚假游戏交易平台或者下载虚假交易 APP，以保证金、交易费等形式诈骗。此外，一些交友诈骗也可能在游戏平台发生。

三、年底喜事多 谨防年终回馈式诈骗

年底各大商会推出年货节、瓜分红包等活动，小心骗子趁机下套，比如去年双 11 期间的互助盖楼活动中，就有骗子假借帮忙盖楼行骗。一些积分兑换、积赞、免费送活动中也往往暗藏骗局，除非能确定是正规平台推出的活动，否则遇到陌生链接千万别乱点，一旦中招可能被盗取个人信息，也可能被装上木马。

四、年终手头紧 当心贷款诈骗献殷勤

年关临近，走亲访友、置办年货、发红包处处都需要钱，骗子没好心，但却会“急人所急”。如果看到无担保贷款、零抵押等宣传一定要警惕，也不要觉得自己没钱就不会被骗，骗子往往利用受害的个人信息贷款，再将贷款转移至自己的口袋。此外，如果有人打着年底提高信用卡额度的名义宣传，也应谨防是骗子套路。

五、买买买模式开启 注意购物类诈骗抬头

除了 618、双 11，年货季也是各大电商平台的促销季，一些购物诈骗可能会在此时卷土重来，比如利用高仿的电商网站、APP 钓鱼行骗。此外，一些骗子还会趁网购发货的时机，谎称“您所购货物无货或运输途中丢失，可数倍返还货款”，一旦受害人信以为真就故伎重演，用钓鱼网站、假冒 APP 行骗。

第八章 网络诈骗五大防范锦囊

一：不可“码”虎：莫要泄漏短信验证码

骗子一般使用连环诈骗手段，先设局诱使你发起支付或登陆申请，再编造种种风险迫使你透露验证码，短信验证码是非常重要的信息，验证码代表了你本人的授权，泄漏验证码很有可能会造成财产损失。

有人要你提供短信验证码的时候一定要保持高度警惕，不论对方是任何身份，也不论对方以任何理由利诱和威胁你，都不要提供。

二：拒绝“扫”扰：切勿随意扫描二维码

在移动的迅速发展下，看见二维码扫一扫已经成为了许多人的习惯，二维码在线上线下的应用场景、使用频率也不断增加。

在这一背景下，提供二维码让受害人扫，成了骗子在实施各类诈骗过程中经常用到的手段，如：扫码入群，扫码下载，扫码支付，扫码验证等等

有陌生人让你手机扫码的时候一定要保持高度警惕，即使是熟人也要考虑账号被盗的情况，注意核实身份，保持警惕。

三、无“私”无畏：千万避免私下转账

在电商平台的迅速发展下，大家都有了品牌意识，在购买东西的时候都会主动选择知名电商平台，但是在生活社交中会有突如其来的人或者事，如一些冒充身份的诈骗在设置骗局后会以各种理由诱骗和催促你尽快转账；或者要求先私下转账后交货的，都极具风险，要知道骗子拉黑走人只需要几秒钟。

无论作为买家还是卖家，最好在正规的交易平台上进行交易，在遇到陌生人让你私下转账的时候，一定要再三思考，切记不相信不转账。

四、“费”同小可：只要先交费都须多警惕

人与人之间最重要的就是信任，但骗子在实施诈骗中利用的就是受害者的盲目轻信，在网络兼职、网络贷款、信用卡提额、虚假办证、招聘骗局等多种高发诈骗中，骗子都会以各种理由让你先交钱，如介绍费、手续费、保证金、制作费、材料费、任务押金等，最后骗取受害者钱财。

在生活中遇到让你先交钱的情况一定要小心，其实仔细想一想，在你想借钱的时候却让你交钱，这不难发现是个骗局。

五、一往无“钱”：网络交友谈钱伤感情

2019年，俗称“杀猪盘”的网络交友赌博(投资)类电信网络诈骗“横空出世”，“杀猪盘”一跃成为反诈行业内最热的词。从最古老的“酒托”到“送花篮”再到“卖茶女”最后到“杀猪盘”，此类型诈骗不断改进，上演的“爱情故事”堪比小说；不难发现，无论聊的

多投机、前戏多丰富、故事多感人，在时机成熟的时候，骗子总归会让你花钱。

在网络交友中，我们没必要谈友色变，但如果交往中对方总是拐弯抹角提到钱，或者诱导你一起发大财，那就要仔细想想是否是交友诈骗了。

附录一：网络诈骗各类型定义

金融诈骗

指在互联网上因购买办理金融相关产品或者服务而发生的诈骗，常见的有网络贷款诈骗、虚假金融理财诈骗、信用卡提额诈骗等，如：骗子通过低门槛吸引受害人办理贷款，以需缴纳手续费、设置合同漏洞、贷款陷阱等方式，骗取受害人钱财或偿还高额利息。

游戏诈骗

指在互联网上因购买网络游戏道具或者账号而发生的诈骗，骗子通过各种渠道发布远低于市场价的广告，玩家上钩后，通过第三方聊天软件向玩家发送钓鱼链接，充值后，再以需要开通VIP、资金被冻结需解冻、注册信息填写错误等理由，一步步套路游戏玩家，诈骗钱财。

兼职诈骗

指在互联网上因参与兼职工作而发生的诈骗，常见的有兼职刷单、刷赞、刷信誉等，如：骗子发布“足不出户”、“轻松赚钱”等广告语诱惑受害人，先以小额订单成功返现取得受害人信任，然后用“任务未完成”、“卡单”等理由要求受害人多次付款，从中骗取钱财。

网购诈骗

指在互联网上因买卖实物商品而发生的诈骗，常见的有商品以次充好、诱骗事主使用先汇款后交货、要求预先交纳保证金、二手交易平台诈骗等，如：骗子在网络上发布低价商品信息吸引受害人，以改价为由，通过第三方聊天工具发送钓鱼欺诈链接，骗取受害人付款实施诈骗。

网络赌博诈骗

指在互联网上因参与网络赌博而发生的诈骗，网络赌博只需要一台手机或者电脑就能参与，几乎不受环境和时间约束，一般为虚拟的游戏，骗子通过控制后台让受害人输多赢少，甚至部分赌博平台无法提现，当受害者输得一无所有的时候，就开始引诱受害人接触部分门槛低的网络贷款平台进行贷款，使得受害者负债累累，加上高额利息，最后无法翻身。手机游戏、电脑游戏、社交软件、搜索引擎、弹窗广告、社区论坛等都是骗子接触受害人的途径，通过加好友然后实施诈骗。

身份冒充诈骗

指骗子伪装成公检法、官方客服、亲友等身份，通过电话、短信和社交软件联系受害人实施的诈骗，如：骗子冒充公检法人员，称受害人涉嫌违法犯罪并发送伪造的通缉令，要求受害人协助调查，将个人财产转移至“安全账户”实施诈骗。

虚拟物品交易诈骗

指在互联网上因购买虚拟物品而发生的诈骗，常见的有会员服务、话费充值、加油卡、游戏充值、挂机软件、影视剧下载资源等，一般骗子会制作虚假网站或者伪造仿冒品牌网站，在论坛、搜索引擎和社交软件等发布商品信息，诱骗受害人付款，然后拉黑消失。

交友诈骗

指在互联网上因网络交友后被诱骗而发生的诈骗，如：骗子通过网络广告、婚恋网站、各类社交平台和游戏平台与受害人联系，在加为好友后，前期对受害人嘘寒问暖以获取好感确定恋爱关系，随后诱导其投资股票和参与网络赌博，先以小利诱惑，再怂恿加大投入，最后受害人无法提现导致财产损失。

中奖诈骗

指骗子通过电话、短信和网络等方式向受害人发送虚假中奖信息从而实施的诈骗，一般骗子以领取奖品需填写个人信息为由，诱导受害人提供个人隐私信息，盗取后实施诈骗，或者以需要保证金和支付邮寄费用等各种借口，要求受害人先汇钱。

虚假办证诈骗

指在互联网上因办理各类职称或者证书而发生的诈骗，一般骗子会制作虚假办理证书钓鱼网站，通过搜索引擎做推广，受害人通过搜索访问钓鱼网站后，骗子以各种理由骗取受害人定金、手续费和办理费用后消失。

附录二：猎网平台/联盟相关工作



截至目前，360 猎网平台已与全国一千个地区的公安机关建立联系，共协助侦破、带破逾 5000 余起重大网络诈骗犯罪案件，多次获得公安机关认可和表彰致谢。

其中，2019 年，360 猎网平台协助公安机关侦破、带破 4000 余起网络诈骗犯罪案件，涉案金额超过 2.2 亿元。

截至目前，共 5 家网安和 152 余家互联网企业成员正式加入猎网联盟，360 公司一共向联盟企业推送 5291 条诈骗欺诈信息。

360 猎网平台于 2017 年 5 月开放欺诈信息检索功能“猎网追踪”。截至目前，“猎网追踪”总查询次数达到 270 万次，有 20 个地区公安部门接入猎网追踪、猎网举报入口。2019 年，猎网追踪”查询次数达 28 万次。