2018 年

网络诈骗趋势研究报告

2019 年 1 月 15 日

360安全大脑

摘　要

在本报告中，360 安全大脑通过对猎网平台成立以来累计收集的 11.5 万余条有效诈骗举报和 360 互联网安全中心近五年（2014-2018 年）拦截的逾 4500 万个钓鱼网站进行了调研和分析，从网络诈骗受害者画像及心理解析、钓鱼网站演变趋势、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。

✧ 2018 年，猎网平台共收到有效诈骗举报 21703 例，举报者被骗总金额超过 3.9 亿元，人均损失 24476 元，创近五年新高，较 2017 年人均损失增幅 69.8%。

✧ 90 后连续五年成为“最大受骗群体”；在猎网平台收到的网络诈骗举报中，00 后受骗群体从 2014 年的 0.7%迅速增至 15.8%，，近五年的年复合增长率高达 87.0%，增长趋势迅猛。00 后正在成为网络诈骗的“新目标”。

✧ 2018 年第三季度网络诈骗举报量达到高峰，其中虚假招聘和网游交易类诈骗较其它季度增加明显，而举报者也多为 11 岁至 25 岁的青少年群体。这与三季度包含暑期，学生群体闲暇时间增多有一定关系。

✧ 金融理财诈骗高发且带来的人均损失惨重。2018 年，金融理财诈骗是举报数量最多的网络诈骗，共收到举报 2985 例；人均损失方面，损失最严重的也为金融理财诈骗，损失金额 70985 元。

✧ 2018 年网络诈骗受害者年龄段分布中，90 后占比 4 成，80 后占比约为 3 成；而在人均损失方面 60 后损失最严重，为 67985 元，其次为 70 后 42086 元。60 后群体是金融理财诈骗高发群体，而这类诈骗的人均损失额较大。

✧ 90 后最易遭受虚假招聘、保证金、网游交易诈骗，结合 2018 年网络诈骗类型与性别特征，90 后女性是“虚假招聘”的“最易感人群”；80 后最易遭受赌博博彩、信用卡、身份冒充诈骗。70 后、60 后+(1960 年及以前出生)群体最易遭受金融理财诈骗。

✧ 猎网平台对受害者的问卷调查显示，网络诈骗受害者中有近六成是看到骗子发布的信息后主动联系对方，约四成是骗子主动联系的受害者。骗子联系受害人的最主要方式是通过社交媒体，比例超四成；其次会选择打电话的方式，占比 37%；短信方式占比 10.5%。

✧ 猎网平台对受害者的问卷调查显示，在被骗前，绝大多数的受害人对网络诈骗有过了解，这一比例超过了九成，仅有不到一成的受害者从未听过网络诈骗。而在受骗的过程中，有一半人怀疑过，近三成受害人怀疑过多次。这从侧面可以反映出网络诈骗的难以识别以及骗术的高明。

✧ 猎网平台对受害者的问卷调查显示，超过五成受害者会对社交平台内容及网友怀有质疑态度；三成受害者尽量避免使用第三方支付工具。

✧ 猎网平台对受害者的问卷调查显示，受害者被骗后，约有六成会选择不报警，四成选择报警。

✧ 猎网平台对受害者的问卷调查显示，超过六成的受害者能在一个月内平复心情，可以看出大多数人即使遭遇了金钱损失也能保持较为积极乐观的生活态度；但仍然有超过二成的用户需要半年及以上的时间来平复心情。

✧ 境外彩票类钓鱼网站始终盘踞在“近五年钓鱼网站类型 Top5”中，在 2014 年、2016

年、2017 年、2018 年均为第一大钓鱼网站类型。

- ✧ 从“近五年钓鱼网站模仿对象 Top10”的情况来看，综艺类电视节目曾深受诈骗分子“青睐”，2014 年、2016 年《奔跑吧兄弟》均上榜，《中国好声音》在 2015 年上榜。这些综艺节目收视率高，有较大规模的群众基础，诈骗分子更容易“借题发挥”，利用群众的侥幸心理和对节目的信任实施诈骗。
- ✧ 明星网游类产品成为钓鱼网站争相模仿的对象。2017 年，腾讯游戏 DNF 首次出现在“近五年钓鱼网站模仿对象 Top10”榜单中。2018 年，除 DNF 外，腾讯的另一款游戏绝地求生也上榜了，此外还有具备游戏币充值功能的腾讯充值中心和主打虚拟物品交易的 5173 上榜。

关键词： 网络诈骗、虚假购物、钓鱼网站、身份冒充、虚假中奖、网游交易

目 录

第一章 网络诈骗案情综合分析 1

一、2014 年-2018 年网络诈骗举报数量与人均损失 1
二、2014 年-2018 年网络诈骗受害者年龄段分布 1
三、2018 年网络诈骗各季度举报量及人均损失 2
四、2018 年网络诈骗主要类型举报量与人均损失 3

第二章 网络诈骗受害者画像及心理解析 4

一、网络诈骗受害者地域特征 4
二、网络诈骗受害者性别特征 5
三、网络诈骗受害者年龄特征 6
四、网络诈骗受害者职业、婚姻特征 7
五、网络诈骗受害者心理解析 8

第三章 近五年钓鱼网站演变趋势 12

一、钓鱼网站类型发展趋势 12
二、钓鱼网站模仿对象发展趋势 13

第四章 网络诈骗发展现状及特点 16

一、从刷单到刷赞，网络兼职诈骗“分羹”短视频红利 16
二、经典桥段永流传，冒充领导诈骗卷土重来 16
三、网上交友套路深，为“爱”豪赌不值得 16
四、就怕骗子有文化，职称评级催生论文诈骗 17
五、跟上移动支付步伐，骗子“巧”用付款码劫财 17
六、新年将至，蹭“年味”网络诈骗将迎高发期 17

第五章 年度经典网络诈骗案例 19

一、最痴情受骗者：为求张学友演唱会门票，粉丝三次被骗近万元 19
二、最知名受骗者：沈梦辰卖二手用品遭遇“假客服” 21
三、最会蹭热点诈骗：假借 ofo 小黄车退押金行骗 22
四、最专业诈骗者：着急评职称遭遇“高知”骗子，初审复审都设套 25
五、最高科技诈骗：诈骗分子玩降维打击，短信嗅探盗刷银行卡 26
六、年轻人最易中招诈骗：网络刷单诈骗专坑兼职一族 27
七、年度最具影响网络诈骗：“卖茶女”诈骗风靡社交平台 28
八、最典型金融诈骗：轻信网友发财秘籍，误入假外汇平台被骗 29

第六章 2018 年十大网络诈骗经典话术 30

一、“明天来我办公室一趟” 30
二、“外公家的茶叶滞销了，可以帮忙买一点吗？” 30
三、“看到通讯录好友推荐，以为是熟人就加了” 30
四、“你的快递丢了，我们将进行双倍赔偿” 31
五、“免费提供长期贷款，无担保” 31
六、“您的银行账户涉嫌洗钱” 31
七、“教大家一个网上日赚 XX 元的方法,手机在家就可以做的兼职” 31
八、“您的微信需二次实名认证” 32
九、“推荐股票，稳赚不赔” 32
十、“低价出售游戏币” 32

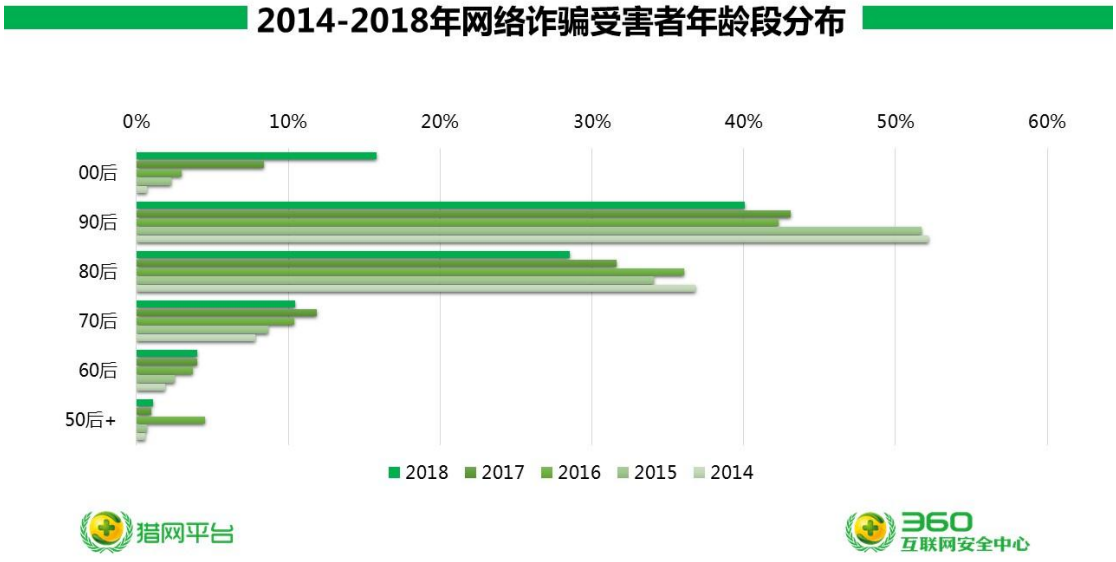
附录 猎网平台/联盟相关工作 33

第一章 网络诈骗案情综合分析

一、2014 年-2018 年网络诈骗举报数量与人均损失

2018 年，猎网平台共收到有效诈骗举报 21703 例，举报者被骗总金额超过 3.9 亿元，人均损失 24476 元，创近五年新高，较 2017 年人均损失增幅 69.8%。

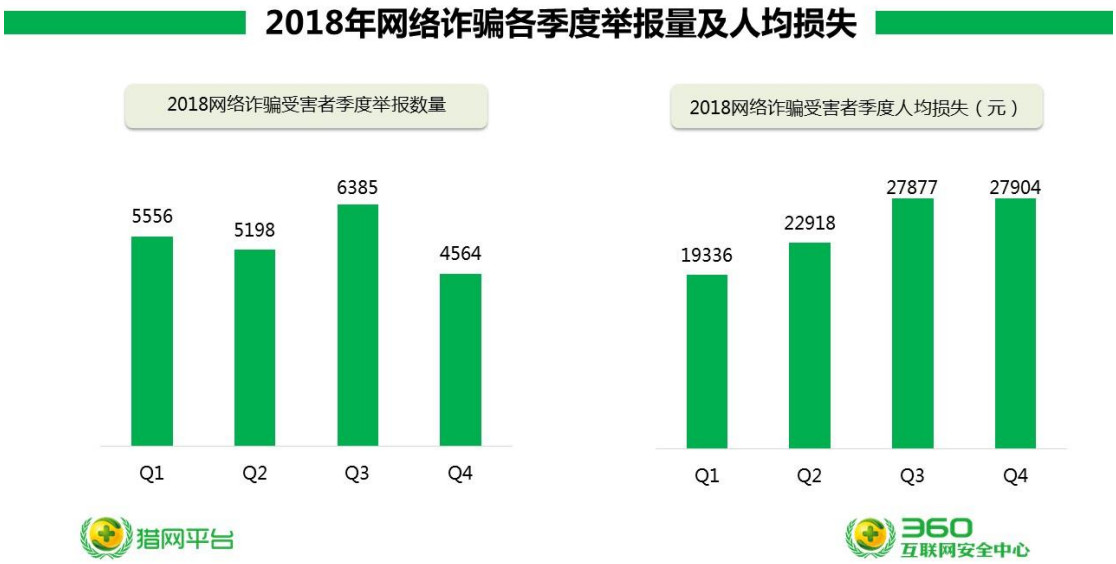
二、2014 年-2018 年网络诈骗受害者年龄段分布



2014-2018 年，90 后人群连续五年成为最大受骗群体，但整体呈下降趋势；80 后为第二大受害群体。这与 80 后、90 后群体频繁接触互联网，容易接受新兴事物，且具有良好的经济能力不无关系。

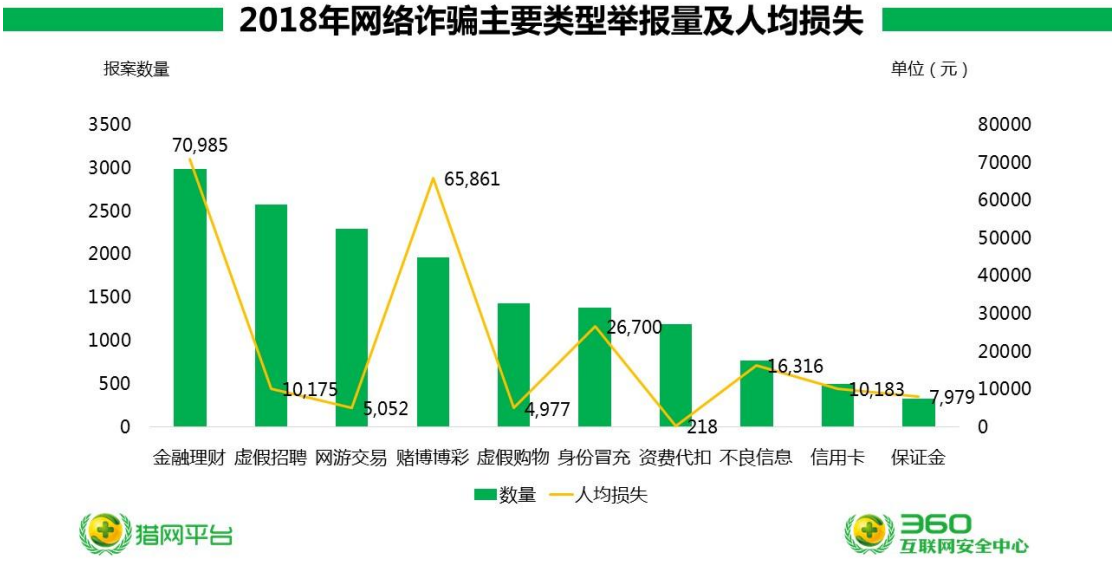
年轻人群体始终是网络诈骗的主要受害群体。随着年龄增长，经济能力逐渐增强的 00 后正在成为网络诈骗的“新目标”。在猎网平台收到的网络诈骗举报中，00 后受骗群体从 2014 年的 0.7%迅速增至 15.8%，近五年的年复合增长率高达 87.0%，增长趋势迅猛。

三、2018 年网络诈骗各季度举报量及人均损失



2018 年 Q3 季度在举报数量上达到了高峰，其中虚假招聘和网游交易诈骗较其它季度增加明显，而举报人群也多为 11 岁至 25 岁的青少年群体。这与三季度包含暑期，学生群体闲暇时间增多有一定关系。而在人均损失上则是 Q4 最为严重，人均损失约 28000 元。

四、2018 年网络诈骗主要类型举报量与人均损失



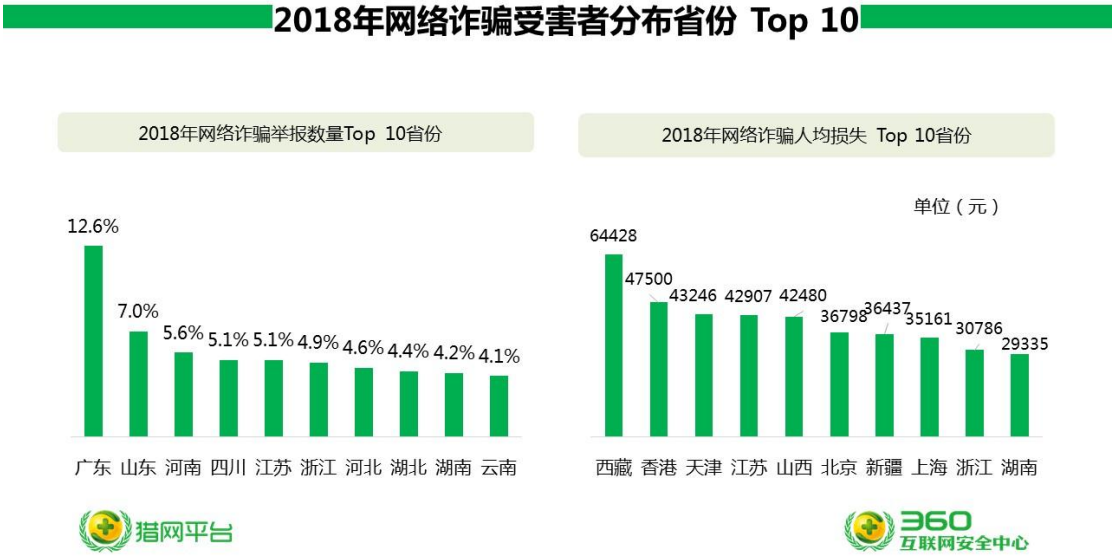
2018 年，金融理财诈骗是举报数量最多的网络诈骗，共获得举报 2985 例，其次为虚假招聘诈骗 2570 例，网游交易诈骗 2297 例。

人均损失方面，损失最严重的也为金融理财诈骗，人均损失金额 70985 元，其次为赌博博彩诈骗，人均损失金额为 65861 元。身份冒充类诈骗人均损失 26700 元，排在第三位。

第二章 网络诈骗受害者画像及心理解析

一、网络诈骗受害者地域特征

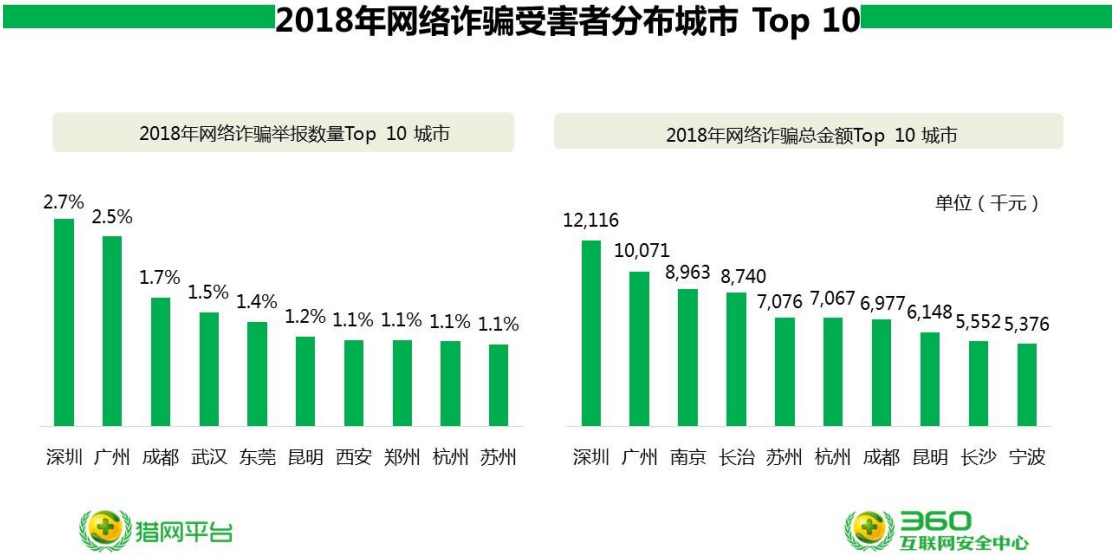
（一）广东位居网络诈骗举报量之首，西藏人均损失最大



从 2018 年网络诈骗举报量最多的省份来看，广东（12.6%）最多，其次是山东（7.0%）、河南（5.6%）。

人均损失方面，损失最严重的为西藏，人均损失金额为 64428 元，其次为香港，人均损失 47500 元；天津第三，人均损失为 43246 元。

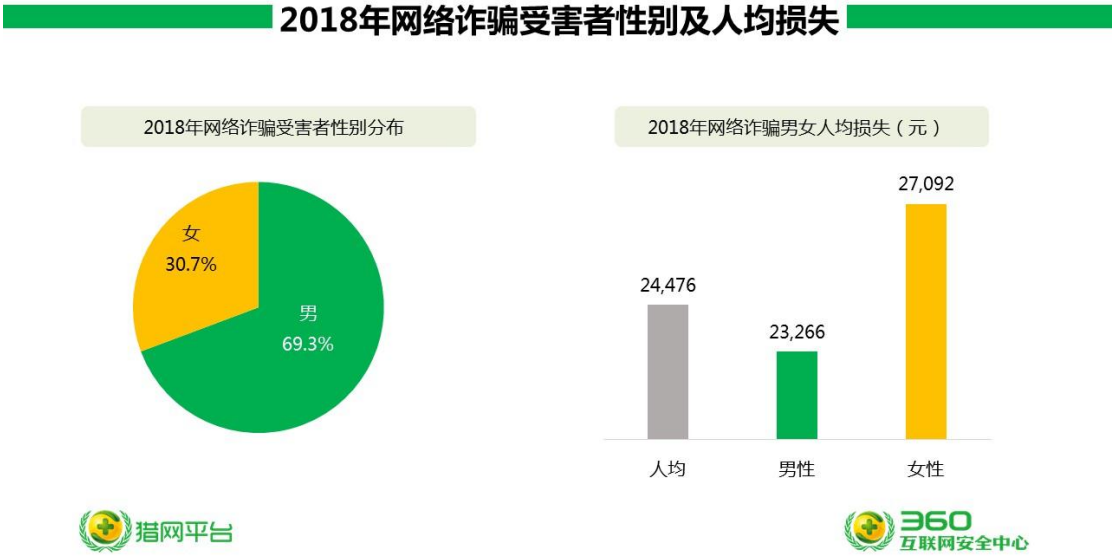
（二）深圳成网络诈骗高发城市，举报数量、被骗金额居首



从 2018 年网络诈骗举报量最多的城市来看，深圳（2.7%）、广州（2.5%）、成都（1.7%）为举报数量最多的城市，而总金额损失最严重的城市为深圳，约 1200 万；其次为广州约 1000 万；南京为第三，约 900 万。

二、网络诈骗受害者性别特征

（一）男人更易上当，女人受伤更深

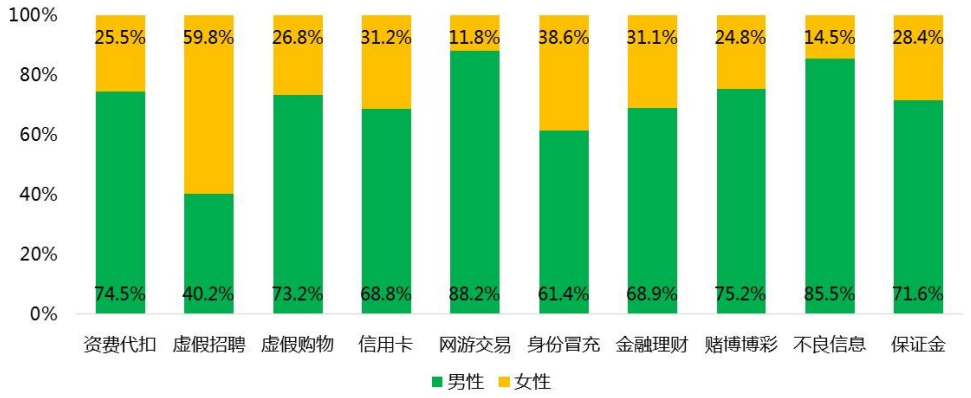


2018 年网络诈骗受害者的男女比例为 7:3，男性成为最易被骗的群体。不过，从人均损失上看，男性人均损失 23266 元，女性人均损失 27092 元，是男性的 1.16 倍。可见在网络

生活中，女性的上当几率其实要比男性低得多，可女性一旦受骗，往往会比男性付出更大的代价。

（二）女性最易中招虚假招聘诈骗，网游交易诈骗堪称男性“专杀”

2018年主要网络诈骗类型举报情况及性别分布



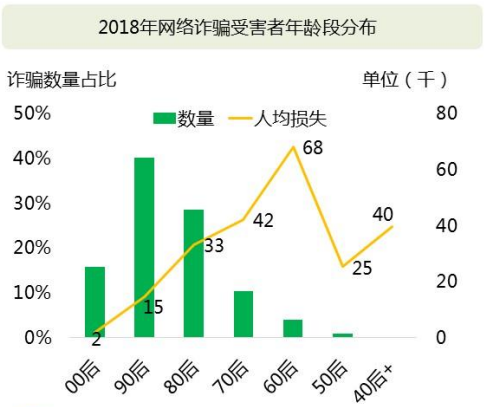
猎网平台　　360互联网安全中心

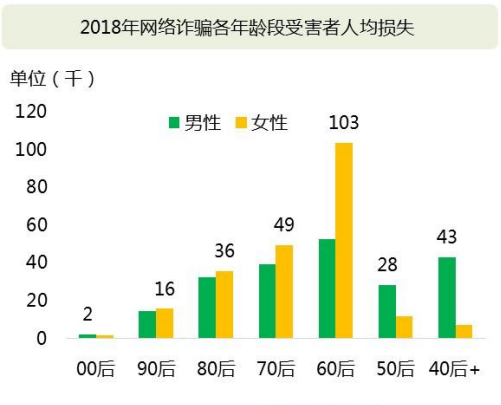
从2018年主要网络诈骗类型举报情况及性别分布上看，除了虚假招聘诈骗中女性为主要受害者（女性占比近6成）外，其余类型均以男性为主要受害者，其中以网游交易最为严重，男性占比近9成。

三、网络诈骗受害者年龄特征

（一）60后人均损失最惨重，金融理财诈骗毁掉退休生活

2018年网络诈骗受害者年龄段及人均损失分布





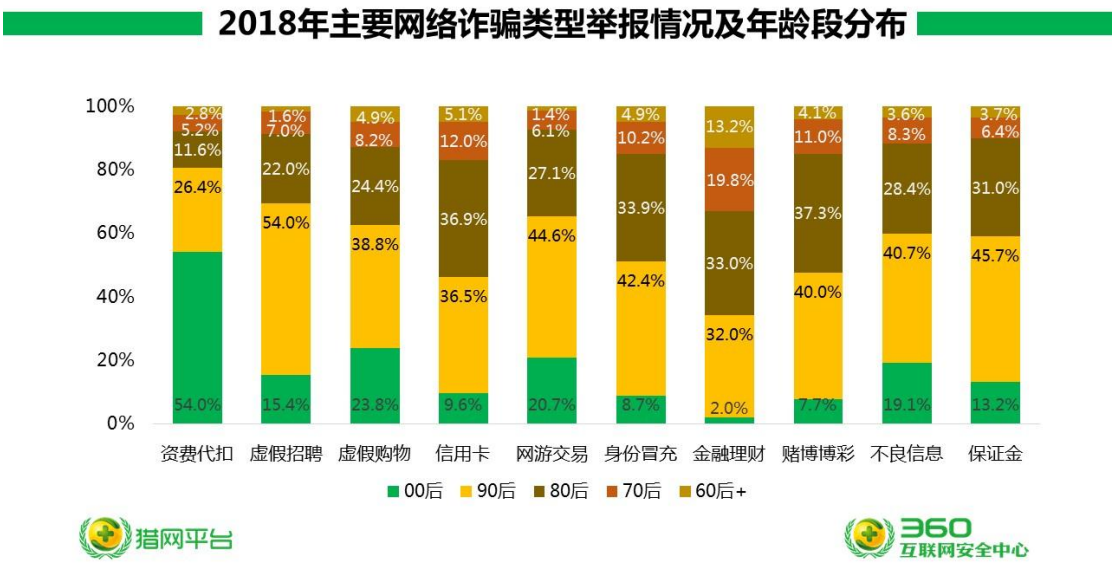
猎网平台　　360互联网安全中心

2018 年网络诈骗受害者年龄段分布中，90 后占比四成，80 后占比约为三成；而在人均损失方面 60 后损失最严重，为 67985 元；其次为 70 后，为 42086 元。60 后群体是金融理财诈骗高发群体，而这类诈骗的损失额较大。

60 后至 90 后女性人均损失均大于同年龄段男性，其中以 60 后女性人均损失最为严重，人均损失 103342 元，约为 60 后男性的 2 倍。

而 00 后、50 后、40 后+（1940 年及之前出生人群）男性人均损失大于同年龄段女性，其中 40 后+男性是同年龄段女性的 6 倍。

（二）各年龄段各有烦恼，90 后女性成虚假招聘“最易感人群”



从 2018 年主要网络诈骗类型举报情况及年龄段分布中，00 后在资费代扣诈骗中占比最高，超过半数。资费代扣诈骗主要是指用户因被诱导点击了恶意链接、下载了恶意软件等原因导致的恶意扣费情况。00 后群体网龄较短，网络安全意识相对淡薄，警惕性低，更容易受此类网络诈骗伤害。

90 后最易受到虚假招聘（54.0%）、保证金（45.7%）、网游交易（44.6%）诈骗，结合“2018 年主要网络诈骗类型举报情况及性别分布”数据可知，90 后女性是“虚假招聘”的“最易感人群”。

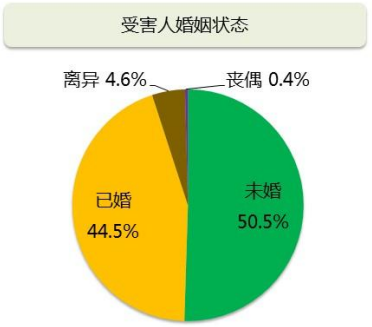
80 后最易遭受赌博博彩（37.3%）、信用卡（36.9%）、身份冒充（33.9%）诈骗。

70 后、60 后+（1960 年及之前出生人群）最易受金融理财诈骗。这一部分群体，尤其是 60 后，闲置资金较多、理财需求较高，面对诈骗分子“投其所好”的蛊惑难免中招。

四、网络诈骗受害者职业、婚姻特征

为了更充分了解网络诈骗受害群体特征，本报告从受害者职业、婚姻、被骗方式等方面，对猎网平台举报者进行了问卷调查。

网络诈骗受害者行业及其婚姻状态



猎网平台
数据来源：猎网平台2018年调研数据

360 互联网安全中心

问卷调查数据显示，受害人行业分布中，在校学生占比最高，超过四成；这与学生群体普遍涉世未深，防骗意识较为淡薄有一定关系。其次为制造业人群，占比 24%；而政府或事业单位从业者占比 13.7%。

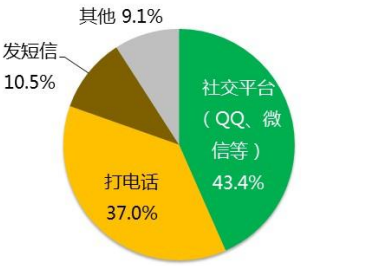
在婚姻状态方面，受害者中未婚占比超过五成、已婚为 44.5%

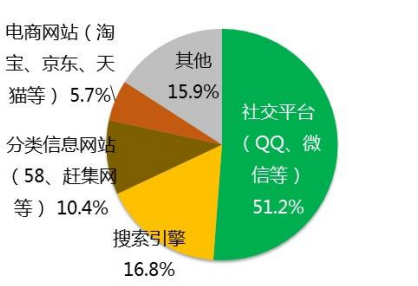
五、网络诈骗受害者心理解析

（一）社交平台成骗子最主要“作案现场”，提防陌生人加好友

参与问卷调查的受害者中，有近六成是看到骗子发布的信息后主动联系对方，约四成是骗子主动联系的受害者。

网络诈骗受害者被骗方式





猎网平台
数据来源：猎网平台2018年调研数据

360 互联网安全中心

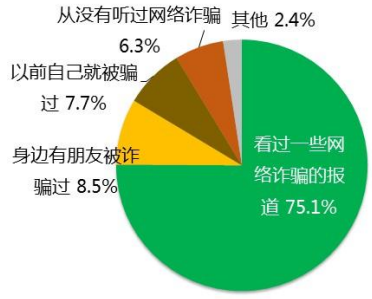
其中，骗子主动联系受害者的方式中，社交平台（QQ、微信等）最受骗子青睐，比例超过四成；其次骗子会选择打电话的方式，占比 37%；短信方式占比 10.5%。

在受害人被动接触诈骗信息的途径中，社交平台为（QQ、微信等）主要途径，占比超过五成；其次为搜索引擎，占比 16.8%；第三是分类信息网站，占比为 10.4%。

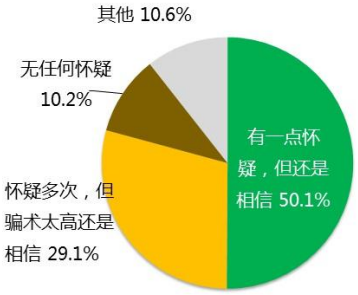
（二）骗术高明难识破，三成受害者曾怀疑多次仍被骗

受害者对网络诈骗感知度

受害人被骗前，对网络诈骗的了解



受害人在受骗过程中是否产生过怀疑



猎网平台 360互联网安全中心

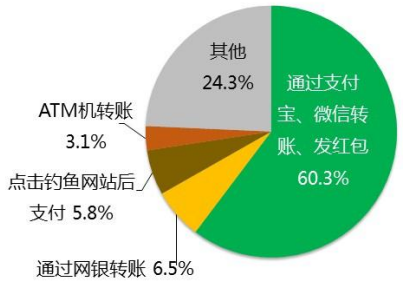
数据来源：猎网平台2018年调研数据

调研数据显示，在被骗前，绝大多数的受害人对网络诈骗有过了解，这一比例超过了九成，仅有不到一成的受害者从未听过网络诈骗。而在受骗的过程中，有一半人怀疑过，近三成受害人怀疑过多次。这从侧面可以反映出网络诈骗骗术“高明”，往往以假乱真，令受害人难以判别。

（三）一成受害者“受伤”惨重，受骗损失为年收入 1-4 倍

网络诈骗受害者被劫财方式及损失情况

受害者被劫财方式



受害者被骗金额在年收入中的占比

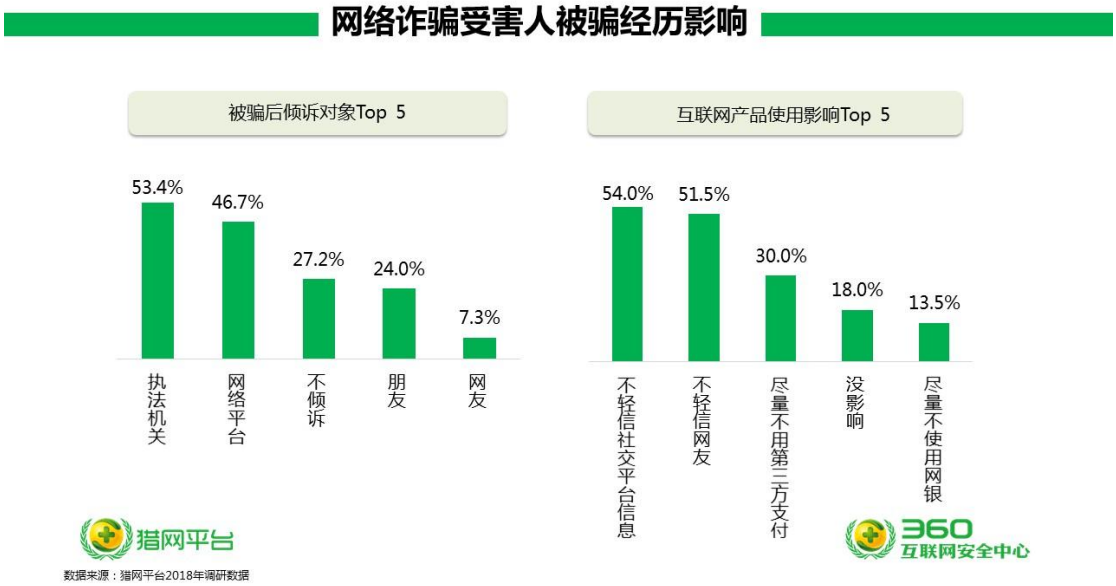
猎网平台 360互联网安全中心

数据来源：猎网平台2018年调研数据

调研数据显示，超过六成的受骗者是通过社交媒体转账给骗子，其次为网银转账 6.5%及钓鱼网站支付 5.8%。

从受害人损失上看，约一半的受害者被骗金额在年收入中的占比不足 10%，可以反映出大多数人对于涉及金钱交易的行为持有小心谨慎的态度；但有超过一成的受害者损失惨重，其损失占到全年收入的 1-4 倍。

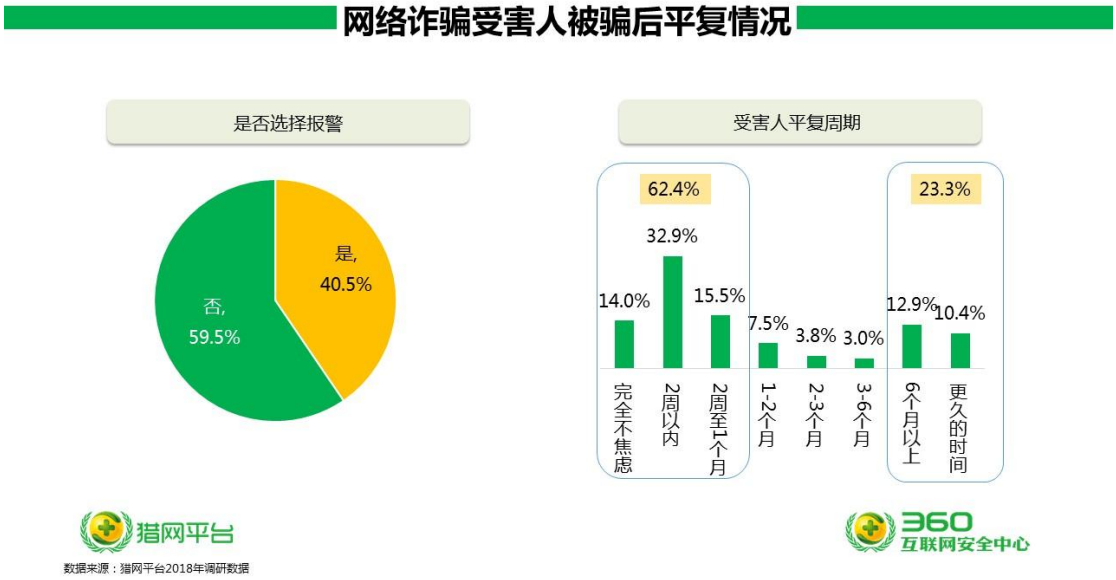
（四）超五成受害者患“社交平台被骗后遗症”，三成受害者忌用移动支付



调研数据显示，约一半的受害者被骗后会选择向执法机关、网络平台倾诉；但约有三成受害者选择默不作声。

而在产品影响方面，超过五成受害者会对社交平台内容及网友持有怀疑态度；三成受害者尽量避免使用第三方支付工具。

（五）约六成受害者成“沉默羔羊”，两成用户需半年以上时间“痊愈”



调研数据显示，被骗后，约有六成受害者会选择不报警，仅四成选择报警。

从受害人的平复周期来看，超过六成的受害者能在一个月内平复心情，可以看出大多数人即使遭遇了金钱损失也能保持较为积极乐观的生活态度；但仍然有超过二成的受害者需要半年及以上的时间来平复心情。

第三章 近五年钓鱼网站演变趋势

钓鱼网站通常指伪装成正规网站来行骗的网站，是网络诈骗的主要工具。超过半数的网络诈骗会利用钓鱼网站作案。

在网络诈骗中，钓鱼网站往往会模仿正规网站网址，以假乱真；或者干脆“黑掉”正规网站，取而代之。从网络诈骗的过程上看，钓鱼网站扮演着不可或缺的角色。比如，在退款诈骗中，钓鱼网站会伪装成电商客服中心、支付平台、理赔平台，以窃取用户的银行、电商账户密码等个人信息。在赌博博彩类诈骗、金融理财类诈骗中，钓鱼网站会伪装成相关网站，诱骗用户进行充值。

本章主要以 360 互联网安全中心近五年来（2014 年-2018 年）拦截的逾 4500 万个钓鱼网站为样本，从钓鱼网站类型和模仿对象情况分析了钓鱼网站了演变趋势，以此透视网络诈骗的发展特征。

一、钓鱼网站类型发展趋势

在近五年的钓鱼网站类型 Top5 榜单中，境外彩票、虚假购物、假冒银行在这 5 年中依然是最主要的模仿类型，而虚假中奖 2014 年、2016 年、2017 年、2018 年均上榜，仅在 2015 年被金融证券类钓鱼网站代替。2015 年至 2018 年，模仿登录类钓鱼网站连续上榜。

（一）境外彩票类钓鱼成“常青树”，诈骗套路惑人心

境外彩票类钓鱼网站始终盘踞在“钓鱼网站模仿类型 Top5”中，在 2014 年、2016 年、2017 年、2018 年均为第一名。

境外彩票钓鱼网站的服务器都开设在境外，主要原因在于境外对网站注册的审核机制较为宽松，而钓鱼网站的受害者及相关法律诉讼也大多不在国外，客观上为不法分子逃避法律监管提供了便利，也给相关部门监管工作造成了一定障碍。

2018 年，猎网平台共接到赌博博彩类网络诈骗举报 1966 起，人均损失 65861 元，仅次于金融理财类诈骗，是人均损失额第二大的网络诈骗类型。

赌博博彩类诈骗抓住部分人群依靠彩票、赌博暴富的心理，通过宣传中奖率高等暴利的钓鱼欺诈方式诱惑网民上当。而从近年来猎网接到的举报来看，赌博诈骗的“套路”也越来越深。

2018 年 5 月，猎网平台协助天津宝坻警方破获的一起赌博博彩类诈骗中，据犯罪嫌疑人崔某等人交代，他们通过微信加好友，冒充美女、帅哥联系客户（被害人），以能预知开奖结果、彩票挣钱等事由，诱导客户在其虚假的彩票网站注册账号并充值，以“吃大赔小”、修改中奖号码、冻结账户等方式操纵网站后台，对客户实施诈骗。

此外，还有利用网络游戏、相亲平台等方式交友骗取受害人信任的诸多案例。遇到世界杯等大型赛事活动，赌博博彩类诈骗也会“蹭热点”。

（二）模仿登录类钓鱼连年猖獗，盗号仍是诈骗“重点”

在近五年钓鱼网站类型 Top5 榜单中，“模仿登录”类型的钓鱼网站从 2015 年至 2018 年连续四年上榜。网络安全形势不容乐观。

“模仿登录”类钓鱼网站主要采用模仿正规网站域名的方式诈骗，例如模仿 QQ 邮箱、QQ 空间、163 邮箱等。如果只看域名前缀，很容易上当。尤其是专门为手机端设计的钓鱼网站，由于手机屏幕限制，使网民更不易注意网址信息，迷惑性更强。一旦用户中招，就会被盗走相关账户密码，继而引发财产损失。

（三）虚假购物钓鱼呈下滑趋势，网购安全面临新挑战

从近五年钓鱼网站类型 Top5 榜单来看，2015 年，虚假购物类钓鱼网站成为第一大类钓鱼网站，随后便呈现出逐年下滑的趋势。

“虚假购物”类钓鱼网站随着电商大潮而兴起，是虚假购物诈骗的“帮凶”，诈骗分子通过虚假购物网站诱骗消费者下单而不发货。

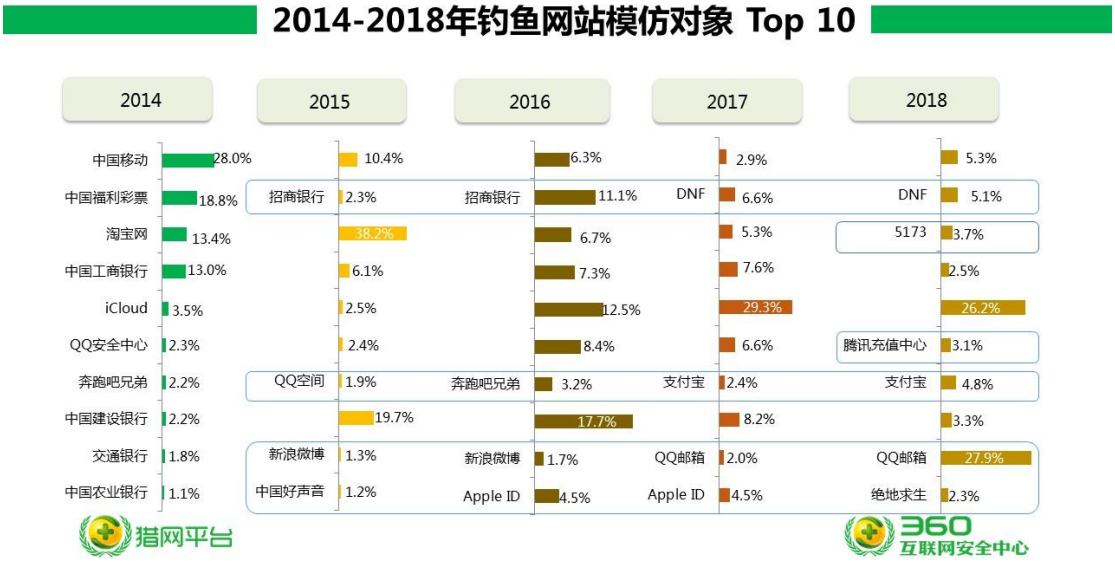
之后，随着电商市场的日益成熟，消费者安全意识和品牌意识提高，主要选择在知名度较高的几大类电商网站购物。这促使各类虚假购物钓鱼网站“降温”。此外，相关部门监管力度、防诈骗宣传力度的日益加大，也进一步打击了此类钓鱼网站的气焰。

不过，从猎网今年接到的虚假购物类诈骗举报看，诈骗分子开始“寄生”在正规的二手交易平台，诱导用户互加社交平台好友后行骗。这类新骗术的出现，也给网购安全带来新的挑战。

二、钓鱼网站模仿对象发展趋势

为了更容易欺骗受害者，钓鱼网站通常会伪装成知名网站行骗。根据猎网平台 2014-2018 年数据显示，钓鱼网站模仿产品中，近五年模仿中国移动、中国工商银行、iCloud、中国建设银行的趋势未曾改变；2014 年的中国福利彩票在 2015、2016 年由招商银行取代，2017、2018 年由 DNF（地下城与勇士）取代；2014-2017 年的淘宝网由 2018 年的 5173（游戏交易平台）取代；2014-2017 年的 QQ 安全中心由 2018 年的腾讯充值中心代替；2014 年奔跑吧兄弟由 2015-2016 年的 QQ 空间取代，之后又被 2017-2018 年的支付宝替代；2014 年的交通

银行由 2015-2016 年新浪微博取代，之后又被 2017-2018 年 QQ 邮箱替代；2014 年的农业银行被 2015 年中国好声音替代，之后的 2016-2017 年，又变为 Apple ID，2018 年绝地求生上榜。



（一）从《奔跑吧兄弟》到《中国好声音》，综艺节目曾是骗子真爱

从历年钓鱼网站模仿对象 Top10 的情况来看，综艺类电视节目曾经深受诈骗分子“青睐”，2014 年、2016 年《奔跑吧兄弟》均上榜，《中国好声音》在 2015 年上榜。这些综艺节目收视率高，有较大规模的群众基础，诈骗分子更容易“借题发挥”，利用群众的侥幸心理和对节目的信任实施诈骗。

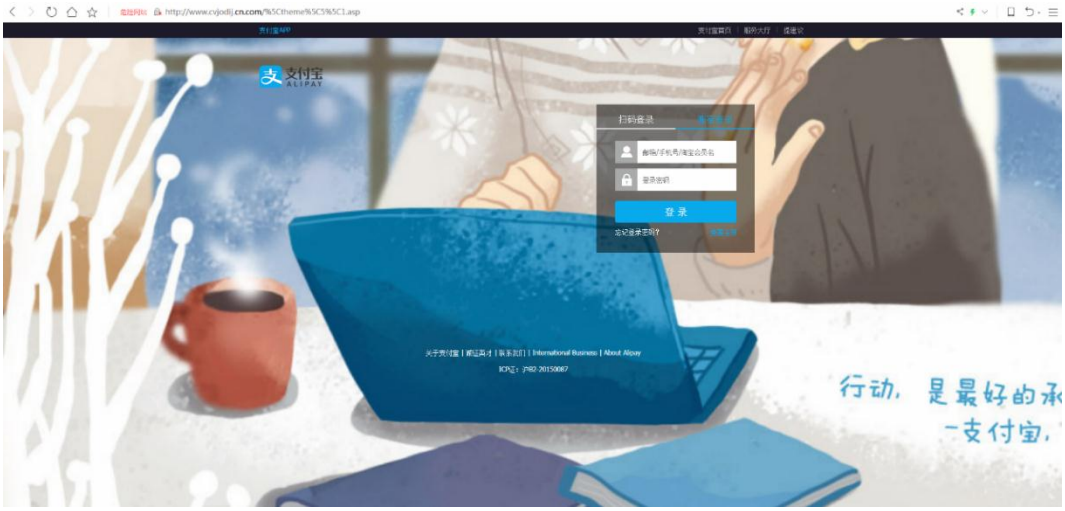
在这类诈骗中，通常骗子会以网络短消息或“伪基站”群发短信方式告知对方抽中“场外幸运观众奖”、“幸运用户”，为掩人耳目，骗子会主动提供网址及验证码、客服热线等迷惑被害人。当被害人打电话咨询时，嫌疑人以要收取风险保证金、个税等名义要求被害人向指定账号汇款。根据媒体报道，除了上述综艺节目外，骗子也曾利用《快乐大本营》、《我是歌手》、《爸爸去哪儿》等当时较为火爆综艺节目诈骗。

（二）吃鸡不成小心蚀把米，明星网游成钓鱼网站“新宠”

2017 年，腾讯游戏 DNF 首次出现在钓鱼网站模仿对象的 Top10 榜单中。2018 年，除了 DNF 外，腾讯游戏绝地求生也上榜。此外，具备游戏币充值功能的腾讯充值中心和主打虚拟物品交易的 5173 也上榜了。热门网游产品遭到钓鱼网站争相模仿。

从 2018 年猎网接到的举报数据看，网游交易类诈骗共有 2297 起，为第三大类网络诈骗。在网游交易类诈骗中，骗子的骗术五花八门，会诱骗玩家在钓鱼网站充值以盗取游戏账号、银行账户、钱款；虚假销售虚拟物品或找回已售账号、虚拟物品；伪装成游戏好友或游戏客服施行诈骗；提供虚假代练服务等。随着近年来网络游戏的火爆，广大游戏玩家需谨防此类诈骗。

（三）模仿“移动支付”成钓鱼网站新潮流，“李鬼银行”越来越少



模仿支付宝的钓鱼网站

支付宝在 2017 年、2018 年连续出现在“钓鱼网站模仿对象的 Top10”中。而模仿银行的钓鱼网站呈现整体数量下滑趋势，模仿中国工商银行的钓鱼网站虽然连续五年上榜，但已从 2014 年的 13.0%下降到 2018 年的 2.5%。模仿交通银行、中国农业银行的钓鱼网站更是仅在 2014 年上榜，此后四年均未能上榜。这与电商火热、移动支付普及的大趋势有较大关系，在猎网平台接到的举报中，有大量“退款诈骗”会利用“假支付宝”行骗，骗子会谎称用户网购商品丢失，以可为用户提供“双倍赔偿”为诱饵，诱导用户登录“假支付宝网站”行骗。

第四章 网络诈骗发展现状及特点

移动支付、共享单车、区块链、人工智能、5G 通信……

2018 年，不断涌现的各种新技术、新趋势正在逐步改变着我们的生活方式。这一年，诈骗分子也没闲着，而是不断学习新技能，蹭热点，升级诈骗话术。这让网络诈骗越来越难防范。综合猎网平台接到的网络诈骗举报线索以及 2018 年媒体曝光的部分新型诈骗案例来分析，2018 年网络诈骗主要呈现以下几个明显的特点。

一、从刷单到刷赞，网络兼职诈骗“分羹”短视频红利

网络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。从猎网平台历年接到的网络诈骗举报来看，网络兼职诈骗 “生命力顽强”，2018 年猎网共接到该类诈骗超 2000 起。

在电商兴起之时，诈骗分子就已盯上“兼职刷单”这个灰色产业，假借其名号，行诈骗之实。而以抖音、快手为代表的短视频 APP 的兴起，也让诈骗分子找到了新的门路。根据 360 安全大脑监测，诈骗分子正在利用热门短视频平台，通过“刷赞”、网络兼职、虚假抽奖、冒充公司或机构账号及发布网络借贷广告等方式实施网络诈骗。

从刷单到刷赞，诈骗分子蹭热点的能力不容小觑。骗子之所以喜欢蹭热点，主要因为大众关注热点，蹭热点既能吸引更多人关注，也能为诈骗分子提供“掩护”，令受害者放松警惕。

二、经典桥段永流传，冒充领导诈骗卷土重来

一直以来，身份冒充类诈骗案件在电信网络诈骗中占据较大比例。据猎网平台统计，2018 年共接到身份冒充类诈骗 1382 起。骗子不惜花费大量的时间和精力将伪装的每个角色刻画的“入木三分”，演什么像什么，等迷惑受害者后，再伺机诈骗。骗子常扮演的角色包括公检法等国家机关工作人员，银行、快递、电商平台等客服，领导、熟人、朋友等。

值得注意的是，2018 年一些曾火爆一时的经典诈骗桥段卷土重来。比如，“明天到我办公室来下”的冒充领导诈骗。这类诈骗的套路并未有较大“创新”，但仍有受害人上当受骗。猎网平台提醒广大用户，应警惕类似“经典”诈骗在被大众淡忘后卷土重来。

三、网上交友套路深，为“爱”豪赌不值得

骗子善于利用人性的弱点行骗，通过交友实施的诈骗便属此类。过去，诈骗分子一般通过网上交友，与受害者建立感情，再以见面为由，骗取“车票钱”、“手术费”、“红包”。不过，360 安全大脑根据猎网平台数据发现，近期的此类诈骗套路更深：诈骗分子先以交友为名，通过网络结识，建立友谊或者爱情关系后，再以分享发财秘籍，诱导受害人到钓鱼网站赌博或理财，制造获利假象。在爱情、金钱的双重催眠下，受害人入戏渐深，就会付出更大的代价，被骗取大量的钱款。

这类诈骗瞧准了人性的弱点，利用网络交友这一手段，为赌博博彩、金融理财诈骗披上了一层“糖衣”。

四、就怕骗子有文化，职称评级催生论文诈骗

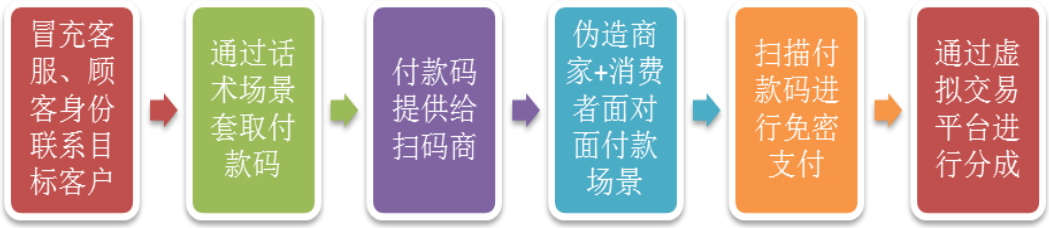
据媒体称，按照规定，职称评定须在国家级和地方级期刊杂志上刊登论文。在这一需求下，“论文产业”也出现了，评职称者只要交纳上千元的稿费，就可以堂而皇之变成一些杂志的撰文作者。而依附这一灰色产业，评职称诈骗也见缝插针。

猎网平台数据显示，评职称诈骗的受害群体主要为需参与职称评级的学校老师、学术机构研究人员等，要对其实施诈骗，需要诈骗分子掌握过硬的“专业知识”。

在猎网收到的一些举报中，诈骗分子能对“客户”的论文发表需求有问必答，甚至还能与“客户”讨论选题方向，发送英文录用通知，几可乱真。由此可见，只要一个领域有利可图，骗子就能不断深入这一领域，快速形成与之适配的“专业能力”。

五、跟上移动支付步伐，骗子“巧”用付款码劫财

随着移动支付的普及，手机已经成为了很多用户的“钱包”。扫码付款既简单又方便，交易中只需要扫描付款的二维码即可完成交易。正因为交易场景简单，很多不法分子也盯上了二维码交易，2016 年出现了很多骗取用户二维码截图后盗刷的骗局，但近两年由于支付公司付款二维码截图过程中进行了防骗提示或很难截图，使得这一骗术变得困难，骗子转换思路，骗取付款码数字进行盗刷，也形成了一条持续火热的产业链。从近期猎网平台收到的举报来看，很多退款诈骗都会对受害者使用这一方式“劫财”。



六、新年将至，蹭“年味”网络诈骗将迎高发期

每逢岁末年终，诈骗分子也会伺机而动。根据猎网平台历年春节期间接到的举报来看，订机票诈骗、红包骗局、信用卡提额诈骗是这一时期最高发的网络诈骗。其中，订机票诈骗主要利用“特价机票”、“便宜机票”为诱饵，诱导消费者在钓鱼网站购买“假机票”。也有诈骗分子以“退改签”为由，诱骗消费者一步步落入圈套。红包诈骗则以“诱导分享”居多，其中还会让用户填写个人信息，并进一步借此实施诈骗。

除了订机票诈骗、红包诈骗外，以“信用卡提额”为幌子的诈骗也需提高警惕。因为每逢年末都是信用卡调整授信额度的时候，骗子见缝插针，以“提额”为幌子行骗。诈骗分子往往会以十分官方的语气，通过短信形式提示“信用卡提额”，并附上钓鱼网址链接。一旦用户中招就会泄露银行卡号、身份证号、验证码等重要信息，导致财产损失。

售卖抢红包软件的钓鱼网站

此外，就在近期，猎网平台还接到以“售卖抢红包软件”为名的网络诈骗。据用户举报称：其轻信骗子宣传，花费 600 余元购买了抢红包软件，但下载后又被索要上千元的激活费，但其付款后依然无法使用该软件，才意识到是骗局。

第五章 年度经典网络诈骗案例

一、最“痴情”受骗者：为求张学友演唱门票，粉丝三次被骗近万元

即便是有着“破案歌神”威名的张学友，也成了诈骗分子利用的对象。

近期，猎网平台接到一起举报，诈骗分子利用了粉丝对于明星的喜爱和追捧，来来回回骗取受害者三次转账近万元。

据悉，家住北京的方女士听闻自己的偶像张学友要来北京开演唱会，心情十分激动。但她在上网购票时，却发现演唱会一票难求。因为不想放弃这次与偶像见面的机会，于是方女士便开始在网络上寻找购票途径。通过微博，她认识了一个叫“快乐小票”的人，对方声称自己正好有两张张学友北京演唱会的门票，价格为 3760 元，方女士觉得可以接受这个价格，加上对方微博是“加 V 认证”的，也就没有对此产生怀疑，随后便按要求添加了对方微信。

通过了微信好友验证后，对方发给方女士一个收款码，称直接扫码付款即可。在转账成功后，对方却以演唱会门票需要激活为由，让方女士再转账支付 3110 元，并承诺激活后钱会立刻返还，于是方女士按对方要求再次进行了转账。但随后对方又以未备注，暂不能激活为由，要求方女士重新转款 3110 元。在方女士完成了第三次转账后，对方却依然找借口要让方女士继续转账 2000 元，这时的方女士才反应过来自己遭遇了诈骗。随后方女士立即停止转账，向公安机关报案，同时向猎网平台进行了举报。

专家提示：

1）购票一定去官网或正规渠道购买，切勿进行私人交易，避免受骗；

2）切勿相信陌生人的说法，随意向他人转账汇款；

3）激活、卡单等是骗子常用话术，遇到时可直接断定对方为骗子，并停止转账；

4）发现自己被骗，一定要及时到公安机关报警，并到猎网平台（110.360.cn）进行举报。

二、最知名受骗者：沈梦辰卖二手用品遭遇“假客服”

2018 年 11 月 19 日，明星沈梦辰在微博分享了一段“被骗经历”。她在二手交易平台闲鱼卖一件衣服，买家付款时说付不过去，原因是沈梦辰没有开通二手交易服务。她一心想着赶紧解决，就扫了买家给的二维码，来到一个闲鱼的客服页面，并按要求先交了 3000 元定金。在客服要求更新闲鱼 ID 并支付 6000 元时，她才恍然大悟上当受骗了。

实际上，沈梦辰的遭遇并不少见。猎网平台也接到了大量发生在二手交易平台的诈骗举报。

在唐女士的举报中，她在某二手平台上出售自己一只玉镯，没过多久，就有人通过平台询问唐女士玉镯情况，表示想要购买。唐女士向对方介绍了情况。对方了解后，告诉唐女士

支付宝绑定的银行卡余额不够，想用手机转账给唐女士。唐女士同意了，并通过平台将自己的银行卡账户发送了过去。没多久，唐女士手机就收到了一条银行入账信息，显示自己银行卡收到转账 5600 元。唐女士登录自己的网银查询，发现并未收到 5600 元入账，仔细查看入账信息时，才发现对方用的是 170 开头手机号码发送的入账信息，并非银行电话。唐女士这才醒悟自己遇到了骗子，幸好及时登录网银查询，未造成损失。

除了卖家被骗外，买家也难幸免。根据猎网平台接到的举报显示，有诈骗者以可以使用分期支付为由，诱骗用户扫码支付。还有诈骗者诱导用户加“微信”，并以其它平台更便宜为由，发来钓鱼网站网址，诱导用户上当受骗。

专家提示：

1) 在互联网平台上交易物品时，一定要谨慎小心，交易要走官方平台，切勿私下交易，同时请认真阅读官方平台的风险提示；

2) 收到入账短信息时，一定要查看入账短信的发送号码，并登录自己网银查看是否有该笔金额入账；不要轻易相信短信提醒；

3) 网上交易商品时，一定要保护好自己的个人信息，谨防个人信息泄露；

4) 发现自己被骗，一定要及时的到公安机关报警，并到猎网平台（110.360.cn）进行举报。

三、最会蹭热点诈骗：骗子假借 ofo 小黄车退押金诈骗

近期，ofo 押金退款难成为社会热点。猎网平台发现，有骗子利用用户急于退押金的心理，通过假网站、假人工客服等方式行骗。

猎网平台近期接到的举报显示，受害人李女士搜索小黄车客服电话，点开一个网址后，发现了共享单车人工客服电话，并标明提供“账户异常、资金申请不到账、投诉等问题”的服务。

李女士拨打号码后，对方声称是小黄车客服。李女士询问为何近期提交的退押金申请一直无果。对方声称要验证李女士的押金渠道，要求李女士打开微信的付款码，并关闭手机网络。对退款流程并不熟悉的李女士便按照对方说的操作。后来对方以验证失败为由让李女士

打开手机网络，再次向李女士索要付款码，由于前几次操作均没有成功付款，李女士放松了警惕直接把付款码数字给了对方，当手机弹出需要指纹确认付款时，李女士直接确认了。

没过多久，李女士手机收到了扣款短信，急忙问对方为什么退押金还要收钱。对方表示，“是虚拟信息不必在意，要退押金需继续提供付款码的数字”，李女士又照做了，结果又收到扣款短信。此时李女士才意识到自己被骗了，累计损失 7500 元。

另一外受骗者王女士的经历与上述类似，她通过搜索小黄车人工客服，也登录到一家钓鱼网站，拨打此网址上电话，对方声称是 ofo 小黄车平台的客服人员，可以办理押金退款，但是必须按照他的要求操作。

对方要求王女士关掉手机网络，打开手机支付宝付款码，将付款条形码告知，并声称这样后台就会进行还款操作。而当王女士重新打开手机网络后，却发现支付宝提示，自己的账

户被以商品消费的形式扣除了 999 元。

除了退押金被骗外，还有用户在使用小黄车时遭遇退款诈骗。赵先生称，自己扫码使用“小黄车”时，出现车锁未打开，但钱已经扣除的情况。于是，赵先生拨打了小黄车上显示的客服电话，未打通。

之后，赵先生从网上搜索 ofo 客服电话，并根据搜索结果，拨打了客服电话。对方称，钱可以退还，并让赵先生打开支付宝进行退款操作。赵先生按照对方要求操作后，对方告知手机上稍后会收到验证码，请收到后把验证码提供给对方。

收到验证码后，赵先生也没细看内容，就将验证码提供给了对方，一共提供了两次验证码。最后，赵先生手机连续接收到了两条扣款 999 元的短信，共损失 1998 元。

专家提示：

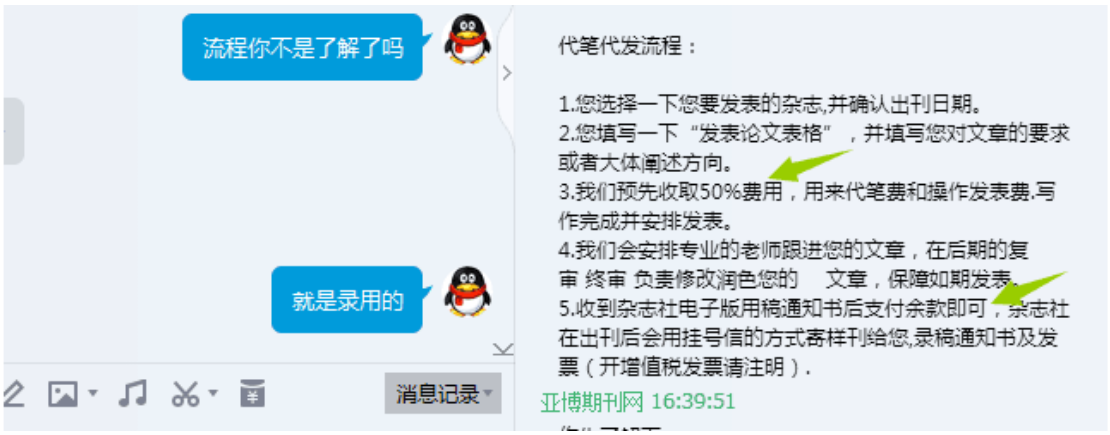
1) 办理共享单车业务，要在共享单车官方 APP 中进行操作，切勿盲目上网搜索，以免上当受骗；

2) 不能随意向别人提供自己的手机短信验证码及付款码；

3) 发现自己被骗，一定要及时到公安机关报警，并到猎网平台（110.360.cn）进行举报。

四、最专业诈骗者：着急评职称遭遇“高知”骗子，初审复审都设套

根据猎网平台接到的举报信息，今年 8 月，因为着急评职称需要，李先生在网上查找 SCI 论文相关内容，点开一个网址后，有客服联系他表示可以代写代发相关论文，总计需要 16000 元。在聊天过程中对方表现很“专业”，对李先生的询问都能有问必答，并表示“保证如期发表，否则承诺全额退款并赔偿您费用的 30%”。着急评职称的李先生选择相信对方，并支付了 8000 元的定金。



诈骗嫌疑人发来的“代写代发”流程

十多天后，李先生收到了对方发来的论文录用通知书，但他发现这封英文通知书不够严谨，未写明是否录用。充满疑虑的李先生便向对方索要稿件，可对方则借机要求他尽快支付余款，还强调“为了避免文章被一稿多投，发生版权纠纷”无法发表文章。

在之后的交谈中，对方不断强调自己“讲信誉，做得不是一单生意”，“做代理靠得是关

系，走得是渠道，跟普通的论文投稿流程不一样”，还给李先生发去了之前“客户”转账记录。禁不住对方的巧言善辩，李先生又一次支付了 8000 元。

没过多久，对方又以论文进入“排版阶段”为由，要求李先生尽快支付 3200 元的版面费用，否则影响杂志社印刷出刊时间。李先生这才觉得自己可能被骗了。当对方发觉李先生已对其失去信任后，就与李先生断了联系。

李先生的遭遇并不鲜见，从猎网平台目前接到的论文诈骗类举报案例来看，本类诈骗普遍存在上述案例中出现的特征。受害者都有着迫切的评职称需求，而论文发表数量则是职称考核的一项重要指标。行骗者通过钓鱼网站发布代发论文的广告，诱骗受害者上当。

与其它网络诈骗不同，论文诈骗的行骗者堪称“专家”，对国内外各领域期刊如数家珍，能针对客户提出的多样化论文发表需求有问必答，提供针对性的“贴心建议”。这些“专业”能力，帮助行骗者一步步诱导受害者缴纳论文初审费、复审费、版面费等五花八门的费用。如果不注意甄别，很容易上当。

除了论文诈骗外，虚假职称诈骗也利用了用户职称评级的需求。今年 7 月，猎网平台联合宝坻警方，成功摧毁了一个专门以办理中高级职称证书为诱饵、涉案金额高达 200 余万元的电信网络诈骗犯罪团伙，共有 11 名犯罪嫌疑人被捕。

专家提示：

1) 切勿相信网上“100%审稿通过”、“快速代发论文”、“短期见刊”等言论，这些信息大多为虚假信息。

2) 发表论文期刊应当选择正规渠道。

3) 用户在日常生活中应当注意保护个人资料，防止外泄招致网络电信诈骗，尤其不可轻信社交平台上的陌生人，假如对方提及钱款往来时，更要提高警惕，切勿贸然转账或汇款。

4) 发现自己被骗，一定要及时的到公安机关报警，并到猎网平台（110.360.cn）进行举报。

五、最高科技诈骗：诈骗分子玩降维打击，短信嗅探盗刷银行卡

据媒体报道，今年全国多地破获了一类蹊跷案件。受害人手机放在家里，银行卡和身份证也在身上，没扫二维码，也没点链接，一夜间却收到十几条甚至上百条验证码短信，以及银行扣款短信。据警方介绍，这是今年出现的一种新型诈骗，利用了“GSM 劫持+短信嗅探技术”。

犯罪嫌疑人主要通过四步实现盗刷。一，利用 GSM 技术的单向鉴权体系漏洞，通过伪基站自动搜索附近（一般是周边几百米内）的潜在手机号码；二，通过查询地下出售的个人隐私数据，或登录第三方支付平台、网上银行等，碰撞查询到目标手机号码对应的身份证号码、银行卡号等；三，通过短信嗅探设备，嗅探目标手机号码收到的验证码及运营商、银行所发短信；四，在网上银行或者移动支付平台，通过验证码登录、修改账户信息，进行账户支付、借贷等资金流转操作，如绑定银行卡、申请网络贷款、打白条等，实施盗刷和信用卡犯罪等犯罪行为。

这种犯罪手法主要针对 2G 手机的 GSM 信号，因此犯罪分子常常会干扰附近的基站通

信，使手机信号从 4G 降级到 2G，然后通过嗅探设备窃取手机短信等信息。由于嗅探设备只能嗅探但不能拦截短信，因此犯罪分子通常会选择在深夜作案，这时受害人大多在酣然入睡，不会注意到短信异常。

专家提示：

1) 保护好个人手机号、身份证号、银行卡号、支付平台账号等私人敏感信息。

2) 存有大额资金的个人银行账户，建议不要开通网银功能。网上支付账户应设置支付限额，支付密码与取款密码要有区别。

3) 对不明来历的短信、微信、验证码链接，不点、不收、不回复。对自行发起的转账和支付短信，一定要分辨清楚。

4) 睡觉前，可将手机关机或设置为飞行模式，防止被短信嗅探设备探测。

5) 如账户遭遇攻击，应立即查看自己的银行卡和支付应用，一旦确认资金被盗刷，要立即冻结相关账户并报警。

六、年轻人最易中招诈骗：网络刷单诈骗专坑兼职一族

2018 年 11 月 7 日，公安部发布通报称，2018 年 11 月 7 日 12 时许，36 名利用网络刷单实施电信网络诈骗的犯罪嫌疑人从菲律宾被押解回国，涉及国内多个省、自治区、直辖市的 700 余起电信网络诈骗案成功告破，涉案金额 1800 余万元。

据介绍，2018 年 7 月，公安部发现，部分利用网络刷单实施电信网络诈骗的犯罪窝点位于菲律宾境内，针对国内实施诈骗。2018 年 9 月 14 日、26 日，工作组联合菲警方对位于马尼拉的电信网络诈骗窝点开展行动，先后捣毁 7 个诈骗窝点，抓获 47 名犯罪嫌疑人，现场缴获大量用于实施诈骗的电脑、语音网关、话术剧本等作案工具。

办案民警介绍，诈骗分子先是通过社交软件等渠道发布兼职刷单广告，称给网店刷单提高商家信誉可“足不出户、日赚千元”。受害人轻信虚假宣传后，诈骗分子便要求其在网络平台“购物刷单”，其中购物所需费用即本金由受害人支付，诈骗分子承诺在交易成功后返还本金并支付报酬。

最初的几单任务中，诈骗分子会向受害人返还本金并支付小额报酬，使其放松警惕。随着受害人刷单量不断增多，诈骗分子会以未完成任务量、网络故障等诸多理由不按照事先的约定返还本金和报酬，还要求受害人继续刷单并投入更多的本金。此类案件受害人多为大学生等年轻群体，有的甚至被骗十几万。

实际上，虚假招聘一直是近年来较为活跃的网络诈骗形式。2018 年，猎网平台就接到 2570 例虚假招聘类举报。根据 360 安全大脑分析，年轻的 90 后女性是目前最易受到虚假招聘诈骗的群体。

专家提示：

1） 刷钻或刷信誉等行为助长了商家不诚信的风气，涉嫌违法，不论真假都应坚决拒绝参与。

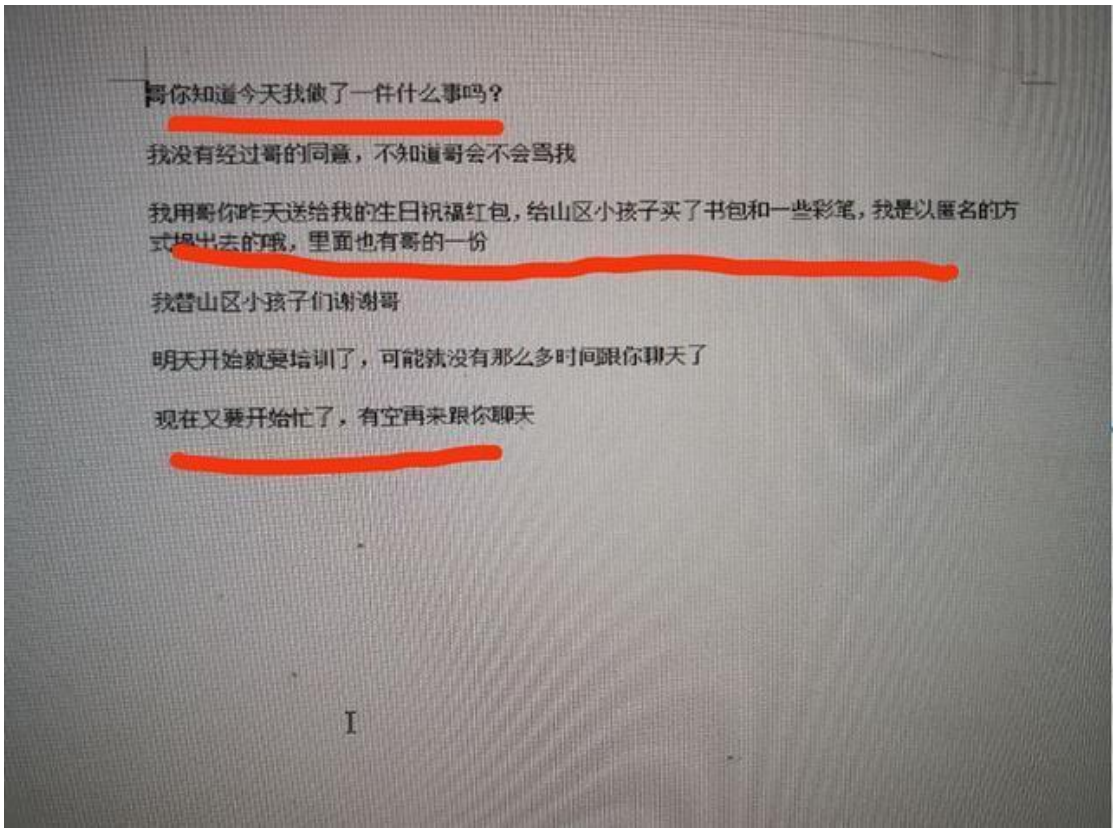
2） 所有宣称技术门槛低，工作轻松但又赚钱很快的工作，多是诈骗。

3） 不要相信所谓的资金冻结、激活订单等说法，更不要相信所谓的操作慢、操作不合要求等说法，这些都不过是骗子们拒绝返款，并诱骗受害者进一步投入资金的借口而已。

七、年度最具影响网络诈骗：“卖茶女”诈骗风靡社交平台

2018 年，“卖茶女”刷爆了社交平台，也忙坏了各地警方。据不完全统计，甘肃、深圳、广东、广西等地警方都破获了“卖茶女”相关的网络诈骗。

别小看这类诈骗的危害。2018 年 8 月，有媒体报道了广西北海破获的一起 “失恋卖茶女”网络诈骗案，刑事拘留犯罪嫌疑人 7 人。这个网络团伙大多是“90 后”男性，他们用同一个美女头像作头像，在微信上编造“失恋卖茶女”及“过生日讨要红包”等剧本进行诈骗。从 2018 年 3 月份至今，该团伙共成功诈骗 1900 余人，目前查清涉案金额已超过 500 余万。



诈骗话术

据悉，这类诈骗步骤可分为“养号、刷粉、卖茶、过生日”四阶段，即前期添加客户后聊天打招呼；“刷粉”就是按照“伤心、失恋、工作忙”等内容和配图在已编排好的不同时间段发朋友圈；“卖茶”则是假装“失恋后去福建外公家看外公、外婆，然后带外公去体检发现身体有问题”等之类内容发朋友圈骗取男客户的同情，随后找点赞和点评的客户进行推销“茶叶”。当以上步骤都成功之后，就是“过生日”的剧本，和客户讲自己过生日，并称身边的人生日都可以得到红包，以撒娇等方式向客户讨要 520 元红包，直到客户发红包为止。

专家提示：

1) 提升防范意识，谨慎添加陌生人为社交平台好友。

2) 在社交平台上遇到钱财交易时一定引起警惕。

3) 发现自己被骗，一定要及时的到公安机关报警，并到猎网平台进行举报。

八、最典型金融诈骗：轻信网友发财秘籍，误入假外汇平台被骗

2018 年 11 月，猎网平台配合石家庄警方赴天津、湖南，打掉一特大投资诈骗平台，抓获涉案人员近 30 人。国内进行外汇交易是不受法律保护的，该平台通过网上炒外汇的方式骗取不特定人员钱财，共计 3100 万余元。该案也是目前最为典型的金融理财类诈骗之一，即通过“交友”取得受害者信任后，诱骗其陷入金融骗局。

据受害人称，2017 年 12 月，犯罪嫌疑人通过社交平台加其为好友，并逐渐取得受害人信任，诱导其在某外汇平台投资。

当时，受害人并不知道所谓的外汇投资只是一个幌子。据办案民警称，当客户在其平台注册充值后，客户的资金会直接进入犯罪嫌疑人的第三方金融平台账户。用户在平台进行所谓的“交易”，却不知道犯罪嫌疑人随意设置盈利率，让客户输多赢少以非法占有客户钱财。

该平台还组织“经纪人”团队，打着网络授课的名义发展更多客户。诈骗平台会为“经纪人”团队在后台输入任意金额，进行带单操作，并收取佣金。

专家提示：

1） 国内还没有完全开放外汇交易，真假难辨，风险性高，所以专家建议最好不要选择这类平台进行投资。

2） 不要轻信来历不明的电话、手机短信、微信、QQ 上传播的信息，特别是不要迷信高收益投资渠道，不要被通过网络通讯工具认识的所谓“专业投资人”、“职业操盘手”欺骗。

第六章 2018 年十大网络诈骗经典话术

一、“明天来我办公室一趟”

你是否接到过这样的电话，“XXX，明天来我办公室一趟”。对方甚至可以叫得出你的名字或姓氏，但我们又不知道他是谁。如果询问他是谁，他会严肃地责备你，“领导的声音都听不出来？”遇到这种电话要小心了，这多半是骗子冒充成领导进行诈骗。

二、“外公家的茶叶滞销了，可以帮忙买一点吗？”

跟你聊了很久的美女突然可怜兮兮地对你这么说，你还忍心拒绝吗？这一招正是骗子的“美人计”。这一经典话术出自风靡各大社交平台的“卖茶女”类诈骗。诈骗分子往往伪装成美女在社交平台加好友，与受害人套近乎、聊天和谈心，再以帮忙打理外公在福建武夷山茶庄为由，撒娇或者以外公病重博取同情，要求对方购买茶叶。

三、“看到通讯录好友推荐，以为是熟人就加了”

你在使用微信或者其他社交类软件时，是否遇到有人添加你为好友，请求显示：“来自通讯录好友”的情况呢？当心这可能是今年特别流行的“交友诈骗”。由于很多人的社交平台账号是与手机号码绑定的。利用这一点，诈骗分子会事先“搜集”手机号，先存在自己的手机通讯录里，然后通过微信的“添加朋友”选择“手机联系人”。这样就可以造成“对方通过手机通讯录添加”的假象。

诈骗分子往往伪装成“美女”，在添加完好友后，又会以“看到通讯录好友推荐，以

为是熟人就加了，看来是我存错朋友号码存成你的了”为说辞，打消对方疑虑。之后还会以“缘分”为由继续交往，获取你的信任，再进行诈骗。

四、“你的快递丢了，我们将进行双倍赔偿”

终于等到电商促销清空了购物车，却被告知“快递丢失”，但好在可以“双倍赔偿”。别高兴太早，遇到这种情况一定要去电商官网求证，当心诈骗分子冒充客服、快递公司骗你登录钓鱼网站，盗走你的账号信息。

五、“免费提供长期贷款，无担保”

谁都有手头紧的时候，但天上可不会掉馅饼。遇到有人向你推荐无担保贷款要小心了，诈骗分子会声称贷款必须先付保证金或者部分利息，并要求你自己办理一张银行卡，先打一笔“企业验资款”到账户上，证明你的还款能力，然后开通电话查询功能供他查询。而实际上诈骗分子利用新办银行卡的初始密码就会把你的钱转走了。

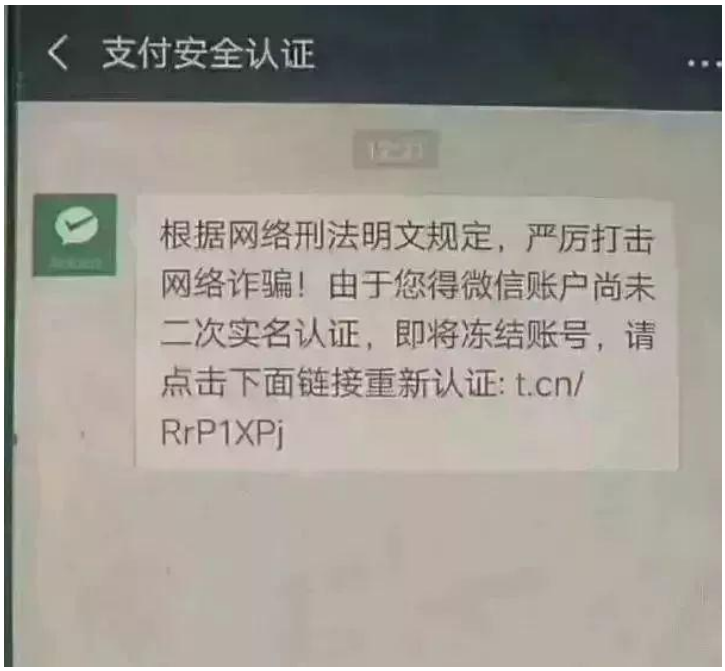
六、“您的银行账户涉嫌洗钱”

电话那头，伪装成公检法、运营商人员的诈骗分子先拿你涉嫌“洗钱”、“发送诈骗信息”等话术唬住你。如果你不信，诈骗分子甚至能给你发来身份证明、公函等。一旦吓住你，他们就会套路你把账户里的钱转到“监管账户”进行“审查”。

七、“教大家一个网上日赚 xx 元的方法，手机在家就可以做的兼职”

找网络兼职需谨慎，小心没赚到反而被骗到。“网络兼职”五花八门，但赚钱可没那么容易。找兼职要上正规的招聘网站，不要轻易在网上透露个人信息。不要从事不合法的兼职工作，否则不仅容易上当，而且可能还会犯罪。

八、“您的微信需二次实名认证”



自己的微信号明明已经通过了实名认证，却再次收到所谓“微信支付”的官方信息：根据网络刑法明文规定，严厉打击网络诈骗，由于您的微信账户尚未二次实名认证，即将冻结账号，请点击链接重新认证。一旦你点了链接，就可能感染病毒，泄露个人信息，危及财产安全。

九、“推荐股票，稳赚不赔”

股市行情跌宕起伏，一些并不成熟的股民散户习惯指望所谓“内幕”消息一夜暴富，在股市上赚大钱。如果有人告诉你，听他（她）荐股，今天买了，明天赚，您会不会心动？那就交会费，加 QQ 群、微信群。给你推荐的股票不涨？诈骗分子会告诉你继续交会费，要升级到高级会员才能给你推荐收益高的。

十、“低价出售游戏币”

看到这种好事要小心了！众多大型网络游戏的风靡，吸引了大量玩家，大多数游戏需要玩家购买装备或者虚拟货币。游戏币诈骗也应运而生。诈骗团伙先以低价诱惑游戏玩家购买游戏币，玩家上钩后，再以需要开通 VIP、资金被冻结需解冻、注册账号时银行卡号填错了等多种理由，一步步套路游戏玩家，诈骗钱财，制定“请君入瓮”的作案流程。

附录 猎网平台/联盟相关工作

截至目前，360 猎网平台已与全国 800 个地区的公安机关建立联系，共协助侦破、带破逾 600 余起重大网络诈骗犯罪案件，涉案金额达 3 亿元，抓获犯罪嫌疑人超过 700 人，打掉 60 余个组织严密、分工明确的大型诈骗团伙，多次获得公安机关认可和表彰致谢。

其中，仅 2018 年，360 猎网平台就协助公安机关侦破、带破 400 余起重大网络诈骗犯罪案件，涉案金额 1.2 亿元，抓获犯罪嫌疑人超过 240 余人。

截至目前，共 5 家网安和 144 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 4289 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 240 万次，有 20 个地区公安部门接入猎网追踪、猎网举报入口。2018 年，猎网追踪”查询次数达 42 万次。2018 年 6 月，猎网追踪还加入虚假大学的查询辨别功能。

为进一步把互联网公司的力量和公安机关的需求有机结合，探讨预防和打击网络犯罪的对策，形成打击网络犯罪的强大合力。2018 年 9 月 4 日，360 猎网平台承办的 ISC2018 网络犯罪的打击与治理论坛在北京国家会议中心召开，论坛由原公安部网络安全保卫局巡视员顾坚主持并致辞，邀请来自最高人民法院、最高人民检察院、公安部、广东省公安厅、北京市公安局、徐州市公安局、360 公司等单位的嘉宾，从立法、执法、技术、实战等角度就打击治理网络犯罪进行了深入探讨。