2017 年上半年

网络诈骗数据研究报告

2017 年 6 月 20 日

摘　要

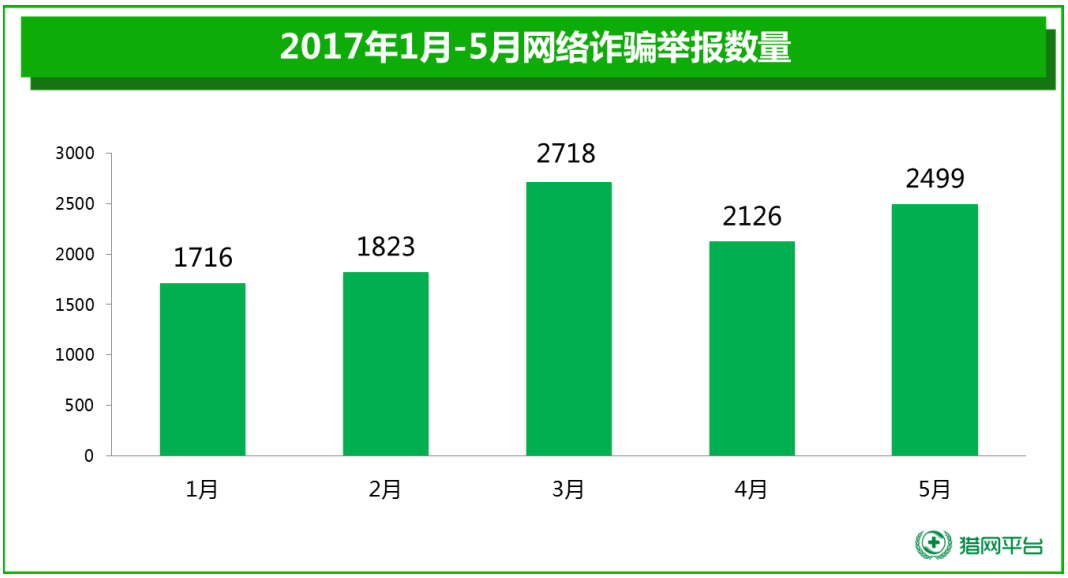
- 2017 年第上半年猎网平台共接到来自全国各地的网络诈骗举报 10882 起，高达 12668.5 万元，人均损失 11641.7 元。
- 从用户举报数量来看，虚假兼职依然是举报数量最多的诈骗类型，共举报 1617 例，占比 14.9%；其次是虚假购物 1539 例（14.1%）、金融理财 1414 例（13.0%）、网游交易 1236 例（11.4%）、和虚拟商品 1226 例（11.3%）。
- 从涉案总金额来看，金融理财类诈骗总金额最高，达 6450.9 万元，占比 50.9%；其次是赌博博彩诈骗，涉案总金额 2361.0 万元，占比 18.6%；虚假兼职诈骗排第三，涉案总金额为 852.8 万元，占比 6.7%。
- 从人均损失来看，金融理财类诈骗人均损失最高，达到了 45621.7 元；其次是赌博博彩诈骗为 33067.1 元，身份冒充为 8159.9 元。
- 从用户举报数量来看，有 7166 人是通过银行转账、第三方支付、扫二维码支付等方式主动给不法分子转账，占比 65.9%，其次有 3378 人在虚假的钓鱼网站上支付，占比 31.0%；
- 从涉案总金额来看，钓鱼网站支付，占比 62.8%，累计 7958.3 万元；其次受害者主动转账占比 35.4%，累计 4480.9 万元；
- 广东（12.8%）、山东（7.1%）、江苏（5.4%）、浙江（5.3%）、和四川（5.1%）这 5 个省级行政区的被骗用户最多。举报数量约占到了全国用户举报总量的 35.7%。
- 从各城市网络诈骗的举报量来看，北京是举报人数最多的城市，为 376 起，其次，广州 309 起，成都 272 起，深圳 264 起，上海 250 起，重庆 183 起，东莞 153 起，武汉 145 起，杭州 131 起和南京 130 起。
- 从各城市网络诈骗涉案总金额来看，北京以 753.4 万元位居榜首，其次是上海（437.1 万元）、重庆（433.8 万元、）广州（420.1 万元）、长沙（399.8 万元）、成都（244.0 万元）、深圳（241.3 万元）、西安（226.6 万元）、郑州（183.2 万元）、泉州（179.8 万元）。
- 从举报用户的性别差异来看，男性受害者占 72.3%，女性占 27.7%，男性受害者占比大大高于女性。但从人均损失来看，男性为 11306 元，女性为 13666 元。
- 从被骗网民的年龄上看，90 后的网络诈骗受害者占所有受害者总数的 44.7%，其次是 80 后占比为 30.8%，70 后占比为 11.4%，60 后占比为 3.4%，而更年轻的 00 后占比 8.7%，其他年龄段仅占 1.0%。
- 而从具体年龄上来看，16 岁至 35 岁的人群是网络诈骗受害者最为集中的年龄段，每个年龄中均有 200 名受害者进行举报，占所有网络诈骗受害者的 61.5%。

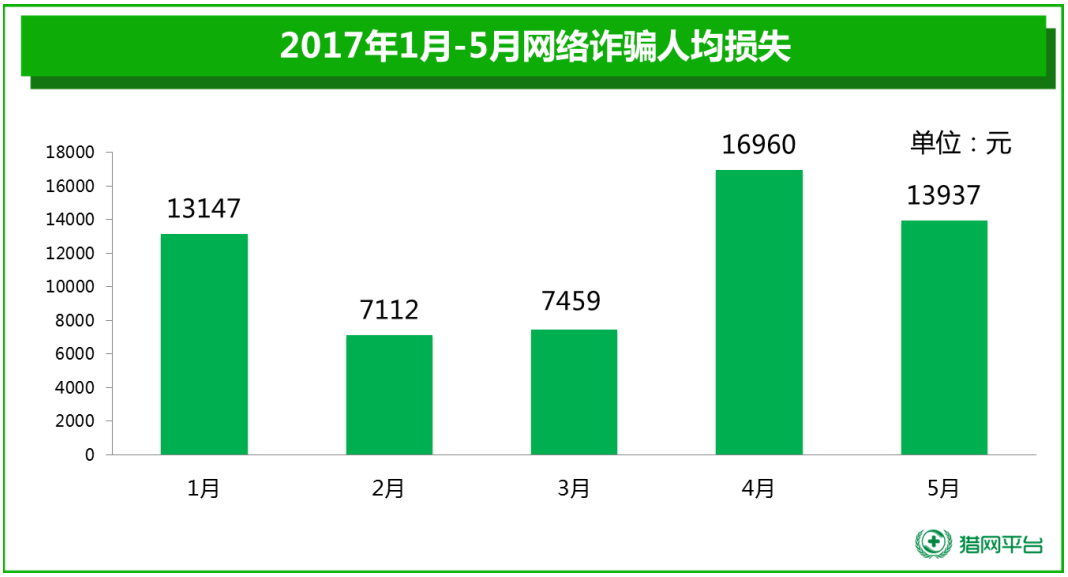
关键词： 网络诈骗、虚假兼职、虚假购物、退款欺诈、二维码、朋友圈

目　　录

第一章　网络诈骗综述

2017 年上半年，猎网平台共接到来自全国各地的网络诈骗举报 10882 起，涉案总金额高达 12668.5 万元，人均损失 11641.7 元。





猎网平台

第二章　网络诈骗案情分类对比

一、举报数量与类型

2017 年上半年，从所有举报的诈骗案情来看，猎网平台共收到全国用户有效申请的网络诈骗举报 10882 例，虚假兼职诈骗依然是举报数量最多的类型，共举报 1617 例，占比 14.9%；其次是虚假购物 1539 例（14.1%）、金融理财 1414 例（13.0%）、网游交易 1236 例（11.4%）、和虚拟商品 1226 例（11.3%）。

从涉案总金额来看，金融理财类诈骗总金额最高，达 6450.9 万元，占比 50.9%；其次是赌博博彩诈骗，涉案总金额 2361.0 万元，占比 19.18.6%；虚假兼职诈骗排第三，涉案总金额为 852.8 万元，占比 6.7%。

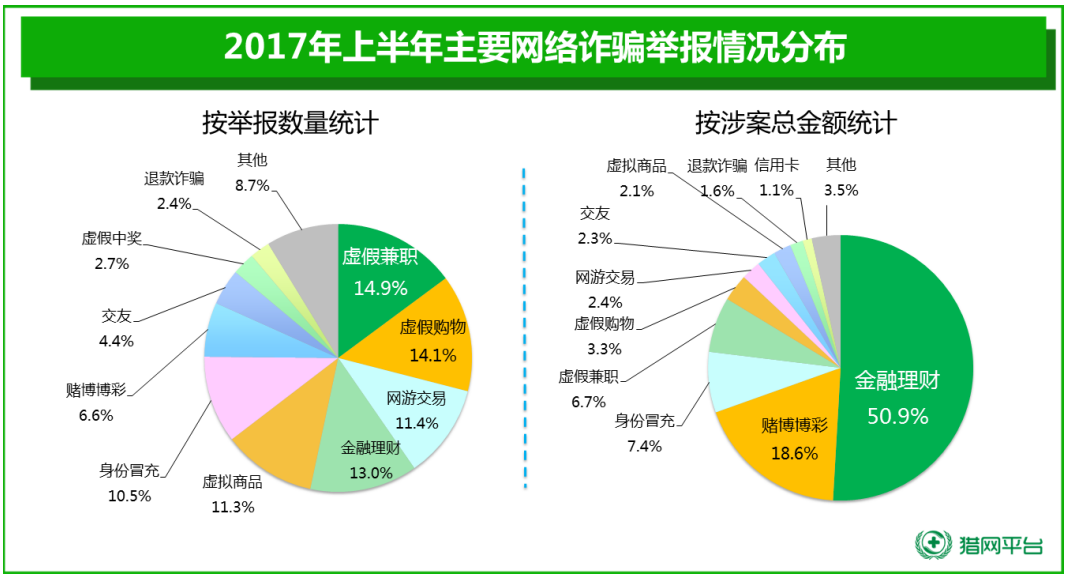
从人均损失来看，金融理财类诈骗人均损失最高，达到了 45621.7 元；其次是赌博博彩诈骗为 33067.1 元，身份冒充为 8159.9 元。

下表详细给出了用户向猎网平台举报的不同类型网络诈骗的举报数量及占比、举报金额及占比、人均损失及占比情况。

诈骗类型	举报数量统计		举报金额统计		人均损失
	举报数量	占比	举报金额（万元）	占比	（元）
虚假兼职	1617	14.9%	852.8	6.7%	5274.2
虚假购物	1539	14.1%	419.1	3.3%	2723.2
金融理财	1414	13.0%	6450.9	50.9%	45621.7
网游交易	1236	11.4%	300.6	2.4%	2432.1
虚拟商品	1226	11.3%	270.4	2.1%	2205.5
身份冒充	1146	10.5%	935.1	7.4%	8159.9
赌博博彩	714	6.6%	2361.0	18.6%	33067.1
交友	475	4.4%	291.9	2.3%	6146.1
虚假中奖	298	2.7%	88.7	0.7%	2976.1
退款诈骗	265	2.4%	200.1	1.6%	7550.3
信用卡	212	1.9%	141.1	1.1%	6655.8
红包	114	1.0%	4.8	0.0%	421.4
保证金欺诈	45	0.4%	16.5	0.1%	3665.1
其他	581	5.3%	335.4	2.6%	5772.5
总计	10882	100.0%	12668.5	100.0%	11641.7

表 1 主要网络诈骗类型举报数量及涉案金额情况

下图给出了主要网络诈骗类型的举报量和涉案总金额分布情况:



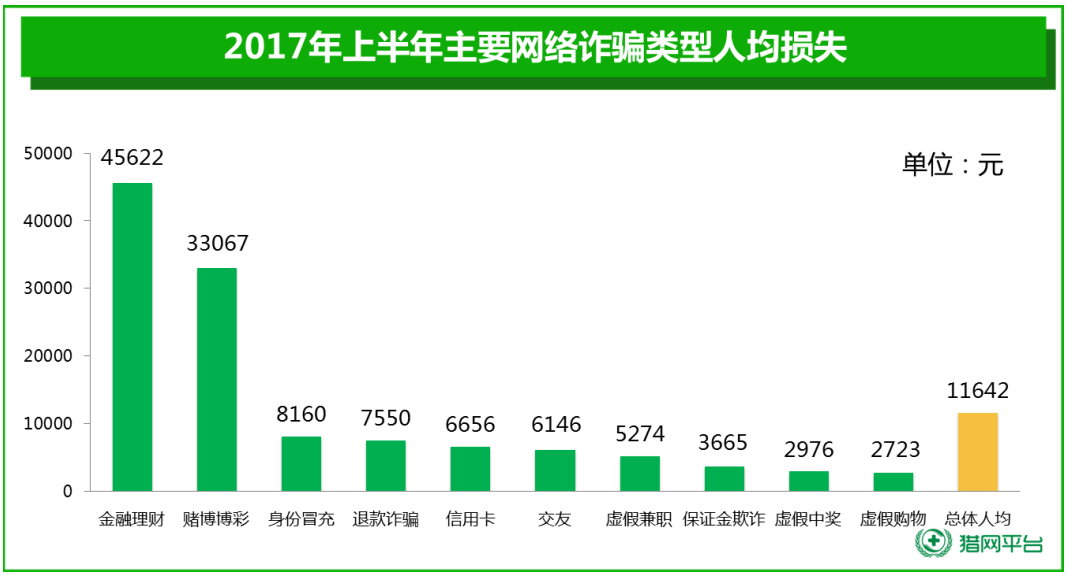
下图给出了 2017 年第上半年网络诈骗主要类型举报量 Top10：

虚假兼职诈骗主要是骗子通过 QQ、微信、知名招聘网站上发布虚假招聘信息，以时间自由，高薪来吸引较多空闲时间的大学生和在家带孩子的妈妈群体，然后以各种借口，收取押金，培训费和材料费等其他费用，交完钱后即刻被拉黑，进行诈骗。而从 2017 年上半年开始，虚假兼职刷单诈骗呈现出了新骗局，骗子让受害者先在正规电商购买商品，以防止平台发现刷单为借口，让其通过第三方支付软件扫码转账方式购买，等到受害者发现上当后，骗子迅速消失。

二、举报金额

在所有用户举报的诈骗案情中，金融理财类诈骗是用户涉案总金额最大的诈骗类型，总金额达 6450.9 万元，主要因其购买的金融理财类产品，往往单笔的涉案金额都较大。

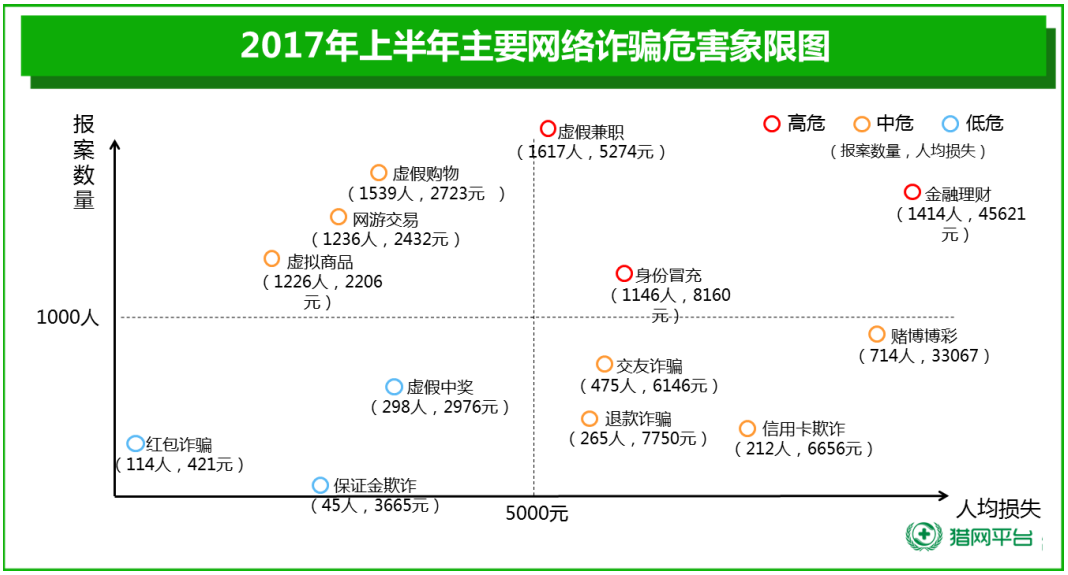
下图给出了不同类型的网络诈骗在人均损失方面的排名。从图中可见，金融理财（45622 元）、赌博博彩（33067 元）遥遥领先，是造成用户人均损失最大的诈骗类型。



自 2016 年下半年以来，信用卡欺诈中，骗子开始盯上消费金融领域，在社交工具中宣传可以套现花呗，京东白条等，然后诱骗受害者先期使用信用消费购买指定的商品，尤其是虚拟商品，一旦确认付款后，骗子就消失的无隐无踪。

下图给出了不同类型的网络诈骗在人均损失和举报数量的象限图。从图中可见，金融理

财诈骗（1414 人，45621 元）、身份冒充（1146 人，8160 元）、虚假兼职（1617 人，5274 元）属于高危诈骗类型，受害人数多，人均损失金额大。而赌博博彩（714 人，33067 元）、交友欺诈（475 人，6146 元）、网游交易（1236 人，2432 元）、虚假购物（1539 人，2723 元）、虚拟商品（1226 人，2206 元）、信用卡欺诈（212 人、6656 元）和退款盗号（265 人，7750 元）属于中危诈骗类型。

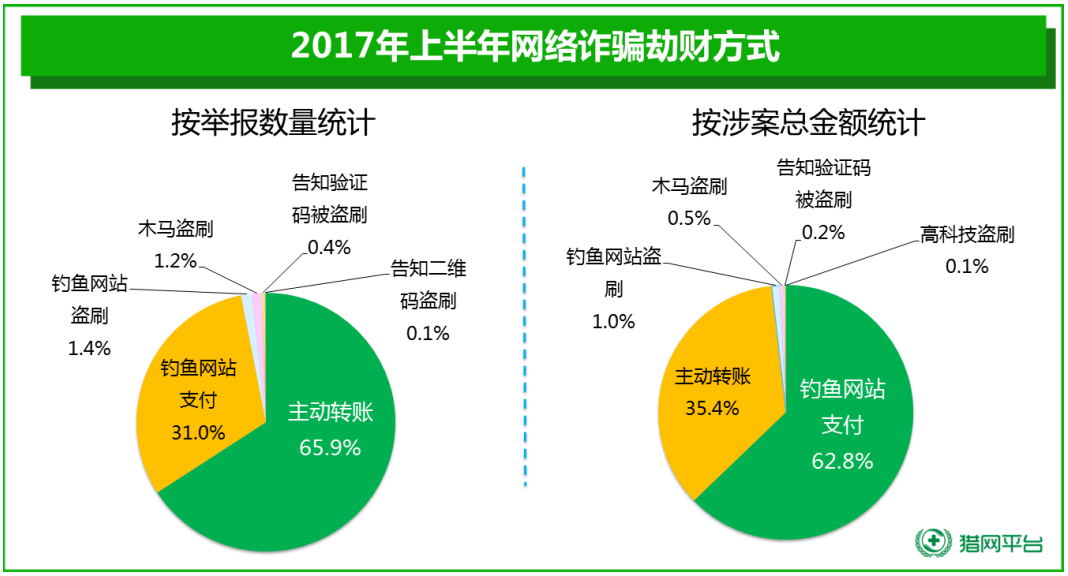


三、网络诈骗的劫财方式

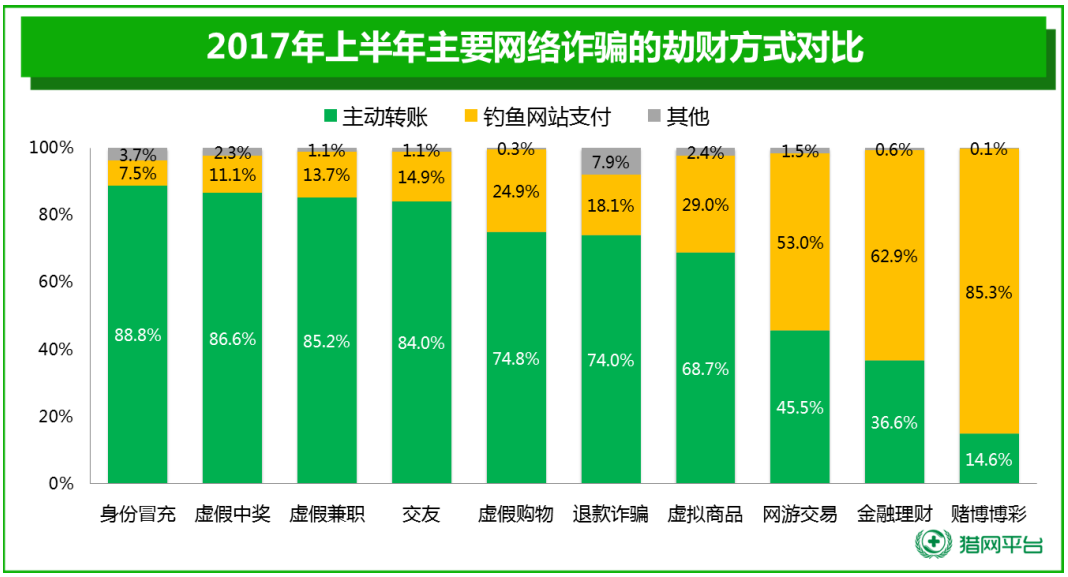
在猎网平台 2017 年上半年接到的用户举报中，有 7166 人是通过银行转账、第三方支付、扫二维码支付等方式主动给不法分子转账，占比 65.9%，其次有 3378 人在虚假的钓鱼网站上支付，占比 31.0%；在钓鱼网站上填写用户的账号、密码等隐私信息后，被盗刷的用户有 150 人，占比 1.4%；安装木马软件从而被盗刷的用户有 129 人，占比 1.2%；主动告知验证码/支付二维码从而被盗刷的有 45 人，共占比 0.4%，告知二维码被盗刷的有 11 人，占比 0.1%。

如果从涉案总金额来看，钓鱼网站支付，占比 62.8%，累计 7958.3 万元；其次受害者主动转账占比 35.4%，累计 4480.9 万元；钓鱼网站导致盗刷占比 1.0%，累计 132.5 万元；木马软件导致盗刷占比 0.5%，累计 60.8 万元；主动告知验证码/二维码从而被盗刷占比 0.2%，累计 29.0 万元。

下图给出了网络诈骗受害者钱财被骗方式的情况：

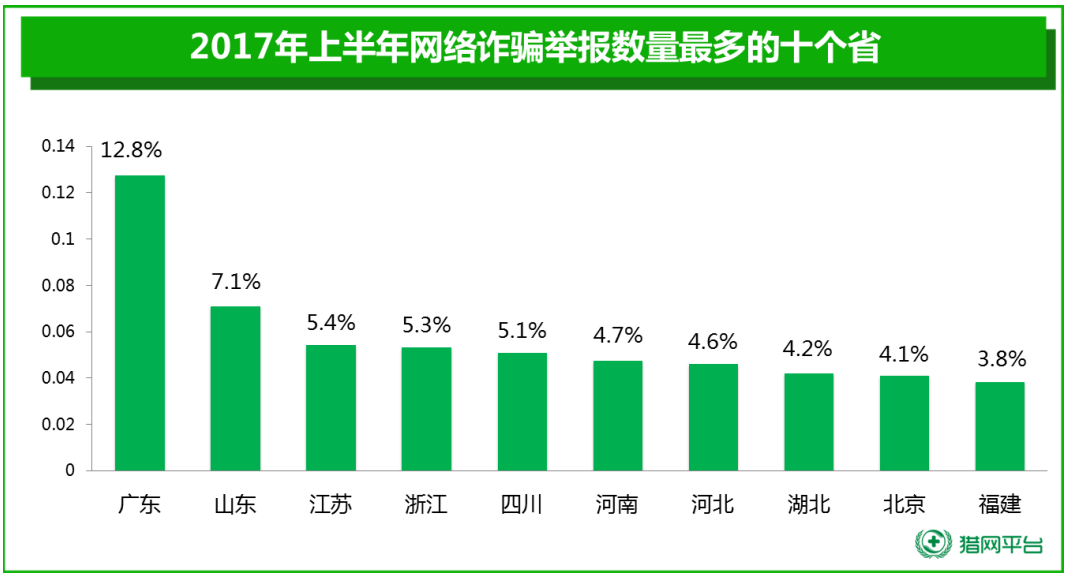


不同类型网络诈骗的劫财方式也有很大的不同，下图给出了部分主要网络诈骗类型的劫财方式对比，从中可以看出，身份冒充、虚假中奖、虚假兼职、交友欺诈类网络诈骗形式，八成以上的受害者都是深受骗子的蒙骗和蛊惑主动将钱转至骗子的指定账户中；而如赌博博彩、金融理财、网游交易类诈骗，绝大多数受害者都是因为登录了钓鱼网站并进行支付而被骗的。

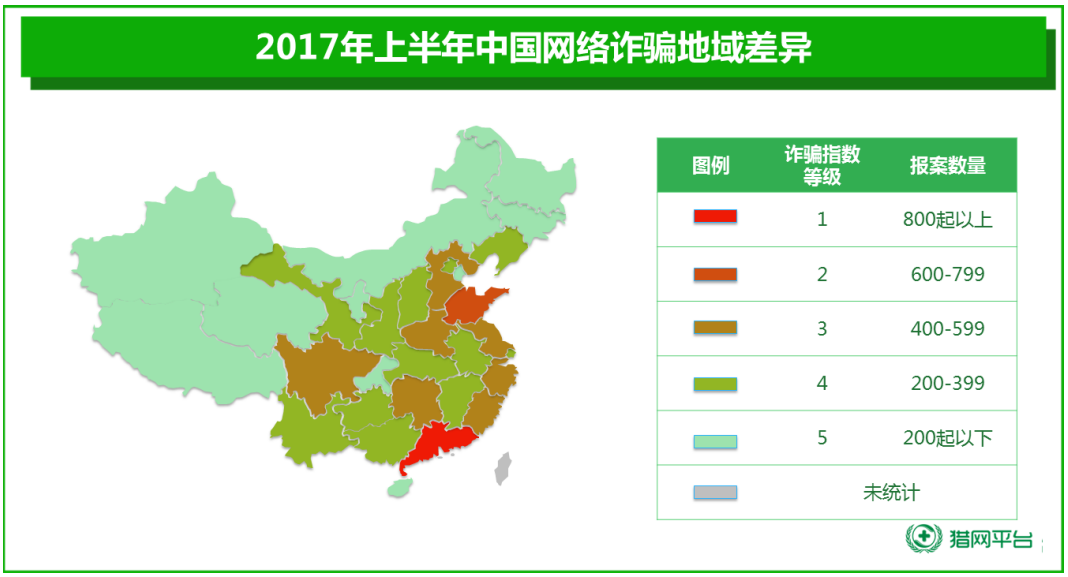


第三章　网络诈骗受害者地域分析

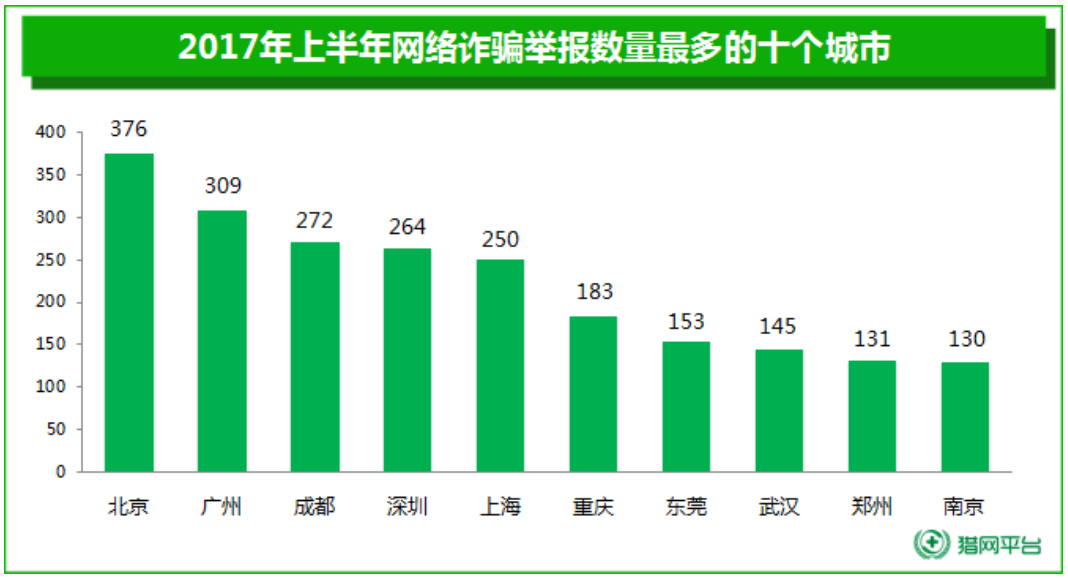
从用户举报情况来看，广东（12.8%）、山东（7.1%）、江苏（5.4%）、浙江（5.3%）、和四川（5.1%）这 5 个省级行政区的被骗用户最多。举报数量约占到了全国用户举报总量的35.7%。



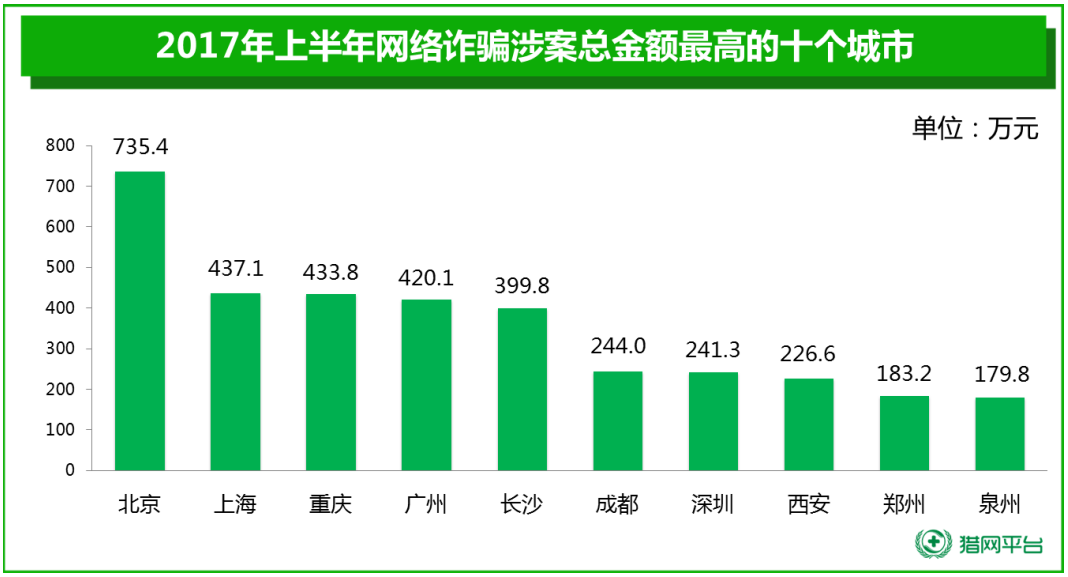
从下图可以看出，经济发达及人口大省是网络诈骗高发区域。



从各城市网络诈骗的举报量来看，北京是举报人数最多的城市，为 376 起，其次，广州 309 起，成都 272 起，深圳 264 起，上海 250 起，重庆 183 起，东莞 153 起，武汉 145 起，杭州 131 起和南京 130 起。



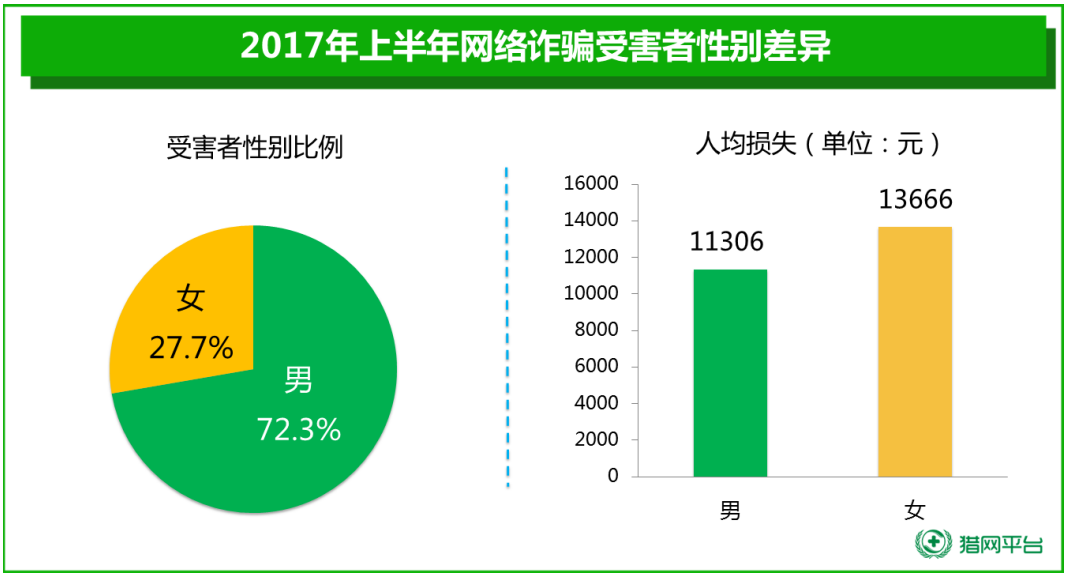
从各城市网络诈骗涉案总金额来看，北京以 753.4 万元位居榜首，其次是上海（437.1 万元）、重庆（433.8 万元、）广州（420.1 万元）、长沙（399.8 万元）、成都（244.0 万元）、深圳（241.3 万元）、西安（226.6 万元）、郑州（183.2 万元）、泉州（179.8 万元）。



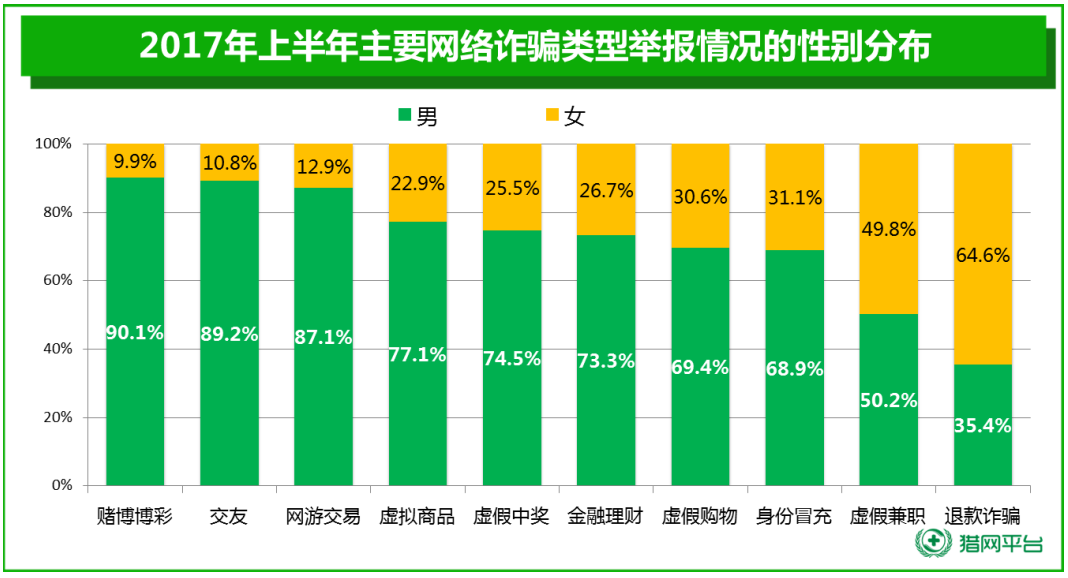
第四章 网络诈骗受害者特征

一、 受害者性别特征

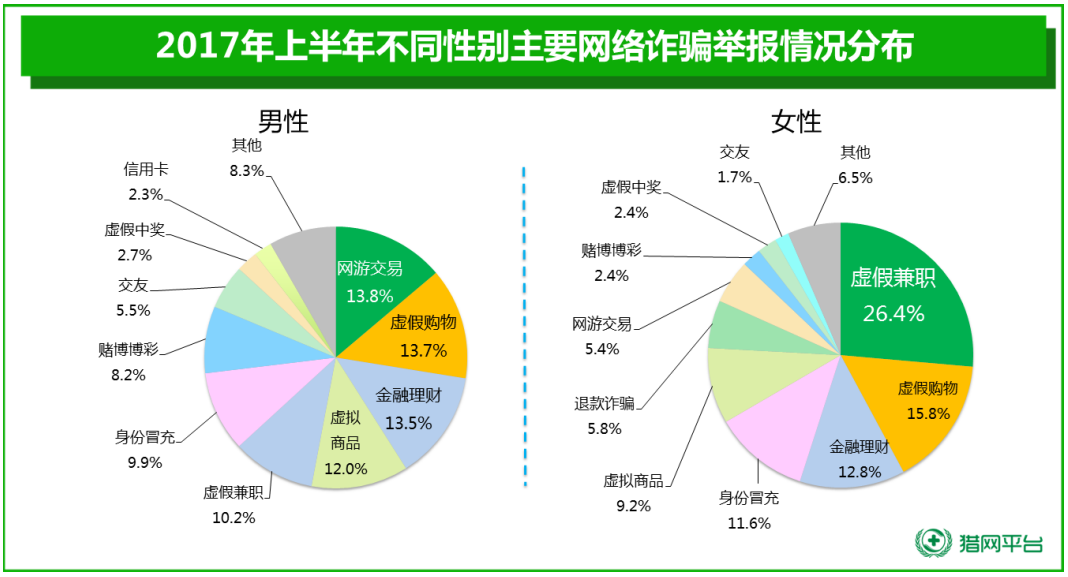
从举报用户的性别差异来看，男性受害者占 72.3%，女性占 27.7%，男性受害者占比大大高于女性。但从人均损失来看，男性为 11306 元，女性为 13666 元。可见在网络生活中，女性的上当几率其实要比男性低得多，可见女性一旦相信了骗子，往往会比男性付出更大的代价。



男性和女性在不同类型的网络诈骗中被骗几率也有明显不同。下图给出了十类常见网络诈骗受害者中男女比例对比情况。其中，在赌博博彩、交友诈骗、网游交易诈骗中，被骗的几乎 90%都是男性，特别是在赌博博彩诈骗中，男性受害者占比更是达到 90.1%。而退款诈骗、虚假兼职类诈骗是女性被骗比例最高的诈骗类型。

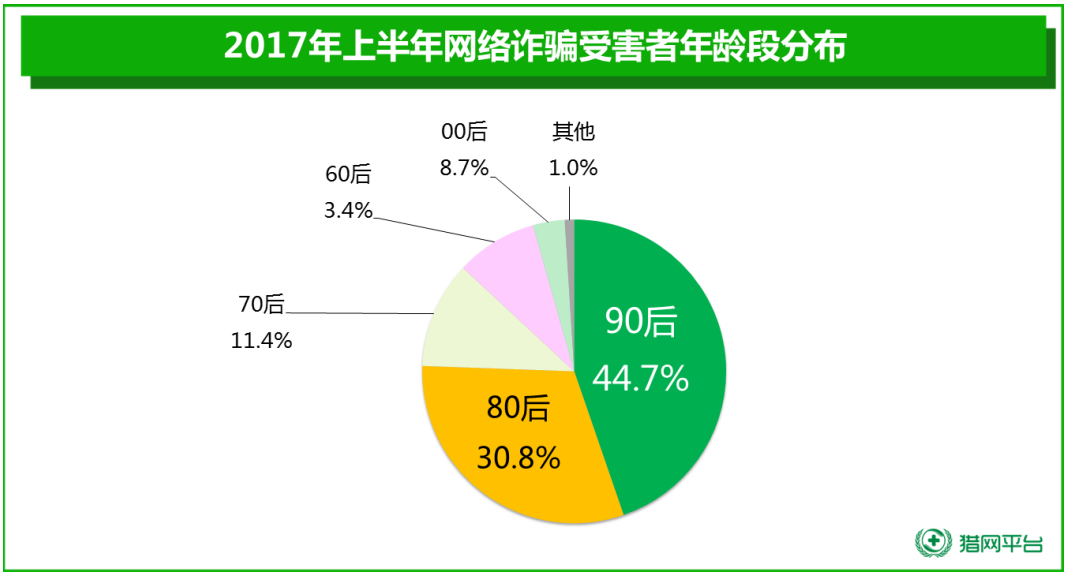


特别值得注意的是，男性和女性在被骗类型方面也有很大的区别。虚假兼职是女性被骗最多的类型，占比 31.0%，男性被骗举报数量排名第一的是网游交易诈骗，占比为 14.8%。

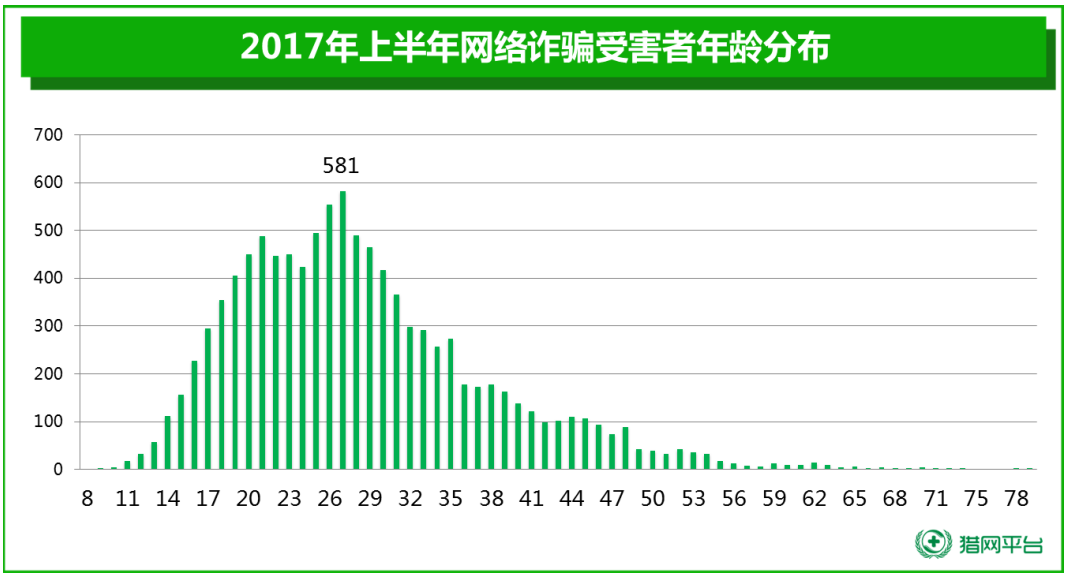


二、 受害者年龄特征

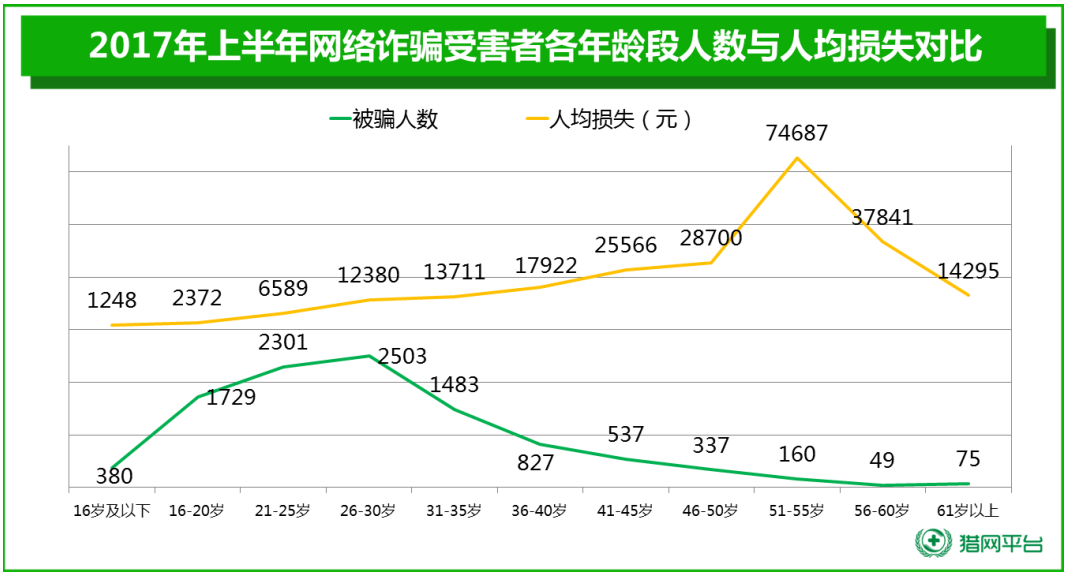
从被骗网民的年龄上看，90 后的网络诈骗受害者占所有受害者总数的 44.7%，其次是 80 后占比为 30.8%，70 后占比为 11.4%，60 后占比为 3.4%，而更年轻的 00 后占比 8.7%，其他年龄段仅占 1.0%。总体而言，即具有一定的上网能力，上网时间较长，同时又缺乏足够社会经验的年轻人是网络诈骗的主要对象和主要受害人群。



而从具体年龄上来看，16 岁至 35 岁的人群是网络诈骗受害者最为集中的年龄段，每个年龄中均有 200 名受害者进行举报，占所有网络诈骗受害者的 61.5%。



下图给出了网络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，随着年龄的增长，受害者人均损失也在增长。16-35 岁之间的用户，是上网的主力人群，被骗的人数虽多，但由于年轻人经济能力有限，被骗平均金额相对较少。45 岁以后的受害者，年龄越大，经济能力也越强，虽然上网的人群、时间在减少，但被骗平均金额迅速增长，超过了 25000 元。



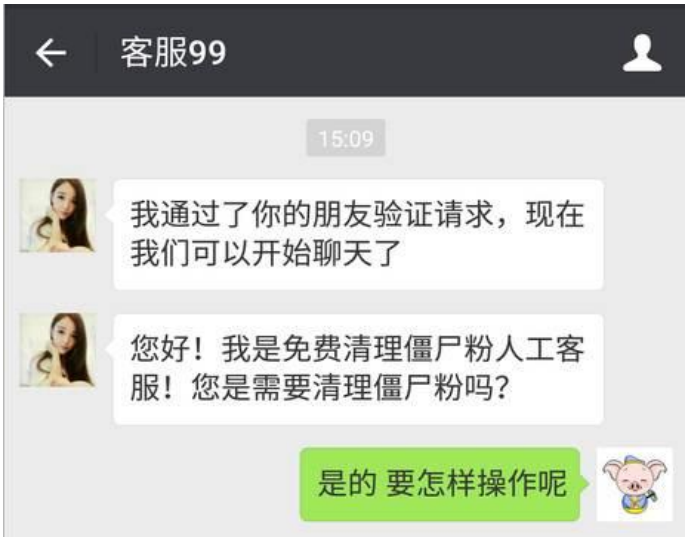
第五章 网络诈骗典型案例

一、清理微信僵尸粉诈骗

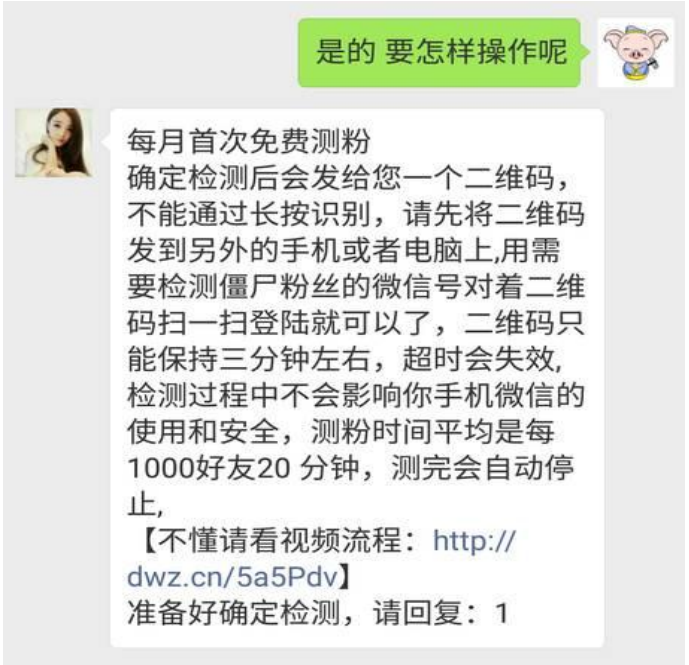
案例回放

近期，微信上经常会收到“免费帮你清理微信僵尸粉”的信息，或是“我在清理微信好友，一清吓一跳”的朋友圈吐槽。很多人点开了信息中的附带链接，按照对方说的步骤清理僵尸粉，结果可能会出现微信号被盗、好友信息被窃取，甚至手机会中木马病毒等严重后果。

首先，点击链接，关注公众号以后，你会收到自动推送消息，引导你联系客服进行清理。



添加人工客服后，对方会对清理步骤做简单介绍或发送教程视频，查看步骤后，需要回复确认是否清理。



待确认清理后，客服会发送一个临时二维码。此二维码不能直接识别，需要将它发送至其他手机或用其他手机拍照，再进行识别。

识别二维码，你的手机就会收到以下界面，经常使用电脑登陆微信的人们都知道，这是电脑登陆手机微信的确认界面也就是，确认登陆后，对方的电脑可以直接登陆你的微信！对方用你的微信开始群发消息，筛选僵尸好友。

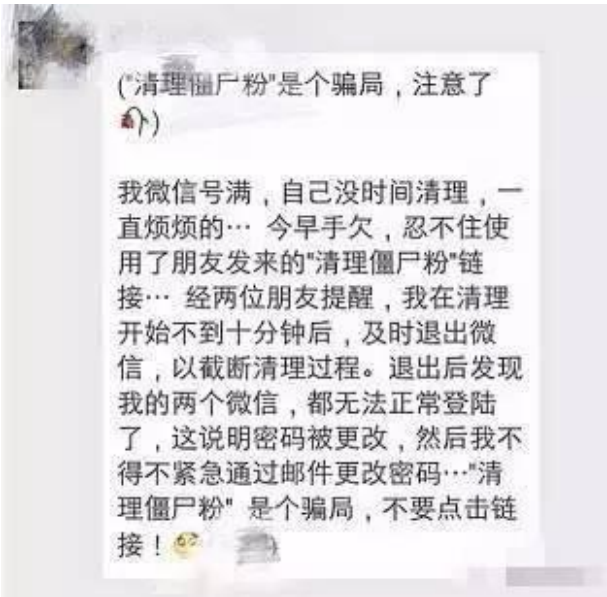
专家解读

用这种方式清理好友，存在很多弊端！

1） 用这种方法清理好友，会陷入尴尬扰人的循环之中。今天你用这种方式给朋友发送信息，就形成了对朋友的无端骚扰。而如果朋友也点击链接，也用这样的方式进行，那么不久你又会收到信息被骚扰.....就这样，会时不时看到这样的消息。

2） 你的手机可能会中木马病毒。微信好友发送的“清理僵尸粉”信息中的链接，很有可能是手机病毒。

3） 微信号可能会被盗。如果你点击了消息中的链接，微信可能会出现闪退、无法正常登陆的问题。



4） 如果你的微信有银行卡绑定，在点击链接时，经专业黑客破解了支付密码后，钱财也将遭受损失。

5） 如果骗子借清理僵尸粉为由，在电脑上登陆你的微信，就可以直接用你的微信号，以生病、出车祸、急用钱等各种理由向你的朋友群发信息进行诈骗

6） 对方可以通过你的微信群发色情信息，这样不但对自己造成不良影响，还会使你涉嫌传播色情信息，一经举报核实，微信号还会被封。

7） 如果骗子群发了带有病毒的链接，会将你的好友置于上述风险之中，形成“循环骗局”。

防骗提示

1） 保护好个人的社交账号，尤其保护好账号密码及不要让他人登录你的账号。

2） 遇到社交软件发来的链接，不要轻易点击。如果是下载安装软件，可通过大型的应用商店下载安装，不要直接点击安装链接里面的应用。防止安装上山寨程序、恶意程序。

3） 不要相信所谓的网络黑客找到应用漏洞、或者开发的外挂软件。

4） 在社交软件中收到朋友发了的转账、代付等涉及到财产信息时，最好通过其他渠道联系朋友进行确认核实，谨防盗号诈骗。

二、 虚假考研资料诈骗

案例回放

花了 1656 元，只买到一本考研资料，最后还被卖家拉黑。近日，多名考研学生向诈骗平台猎网平台举报，称遭遇钓鱼网站兜售虚假考研资料，不是付款后卖家消失，就是收到货不对版的烂书。

3 月 21 日，山东籍考生黄某向猎网平台举报称，他在网上看到卖考研资料的店铺后，便添加了卖家 QQ 进行询问。最终，他以 1656 元的价格拍下了 13 本书，并用微信扫码支付。一周后，等到资料却从 13 本“浓缩”到了 1 本，黄某立即上 QQ 联系卖家，对方却怎么也不回复，并将其删除拉黑。

后来黄某发现这家店铺整个网页都是用图拼凑的，并没有超链接，所谓的官网电话，打过去不是关机就是空号，黄某这才意识到自己被骗。

无独有偶，今年 3 月，猎网平台已先后接到多起类似诈骗案例举报。骗子借出售考研资料的名义，传播虚假钓鱼网址，等到受害者支付高额书本费后，要么随便发一些虚假资料应付，要么干脆“销声匿迹”玩失踪。

专家解读

考研无异于另一场高考，属于人生的转折点，重要程度可想而知。犯罪分子正是利用考生急于寻找合适考研资料的心理，冒充大学学长学姐和受骗学生沟通，并主动推荐学生购买多本虚假资料。受害者由于临近考研，心情比较着急，通常没有经过核实就轻易相信了对方所描述的内容，最后钱书两空。

防骗提示

1） 购买考研等材料时一定要到正规的交易平台购买，切勿轻易相信未知网站客服人员的描述内容；

2） 上网时开启 360 安全卫士等安全产品，如遇虚假钓鱼网站可及时提示风险并拦截；

3） 如仍不慎遭遇诈骗，第一时间报警并登录猎网平台举报。

三、 购物退款诈骗（2017 版）

案例回放 1：

2017 年 2 月初，山东省济宁市的张女士接到骗子冒充淘宝卖家的电话，说受害人购买的物品丢失，需要给受害人办理退款，退款金额是用户购买物品价格的数倍，由第三方理赔公司支付。

骗子以降低店铺损失为由，让受害人将理赔公司退款多余的钱退还给他，因受害人是这家店铺的老顾客，出于对“店家”的信任，受害人答应“店家”的请求，帮忙操作，以降低其损失。

因当时退款金额并未到受害人账上，受害人个人账户上的钱不够，骗子要求受害人向招联好期贷和蚂蚁借呗借款 1200 和 44000 元。在此期间骗子一直给受害人打电话、发短信，催促受害人转账。当招联好期贷到账后，骗子发送二维码要求受害人转账给他 1176 元。

因蚂蚁借呗数额较大，到账较慢，受害人发现受骗后，没有再次损失。

案例回放 2：

而另一位受害人赵先生，也是接到一个声称是淘宝客服的电话，该“客服”告诉受害人购买的衣服（核对店铺名称、衣服信息正确），因为指标严重超出，淘宝介入调查，需要退款给用户。

询问受害人是否收到此退款，赵先生表示没有后，“客服”说可能是因为赵先生的芝麻信用不够，不能自动退款，该店铺会转给赵先生 17000 元保证金，以提高芝麻信用额度，等额度提升后，需要赵先生将保证金退还给店铺。

赵先生按照“客服”要求，在支付宝首页输入“招”字，搜索的第一个结果点进去操作后，赵先生的账户上多了 17000 元，之后，赵先生扫描了“客服”发送的二维码，将 17000 元转账给了“客服”。

之后，赵先生发现，自己并没有将 17000 元转账给“客服”，而是转到了点券充值平台，其账户上的 17000 元，也不是店铺给转的保证金，而是赵先生在“支付宝”平台的贷款（赵先生在按对方操作时，对方完全没有提到贷款二字）。

专家解读

之前冒充电商客服的退款诈骗，是骗子在得到用户的个人信息和购买记录后，以购买物品丢失，损害为由，打电话诱骗用户在自己所发送的链接中输入账户、密码、付款密码，以此来骗取受害人的金钱。

而新出现的骗局，则是骗子货品有质量问题等各种理由，承诺给受害人退款、赔偿，再以转账不通过等理由，要求受害人按照其要求操作，在受害人不知情的情况下，在支付宝等金融机构贷款，再将贷款金额转账给他的方式进行诈骗。

自从 2016 年下半年开始，退款诈骗利用互联网贷款业务进行行骗已经变为诈骗的新方式，这类骗局最大的特点就是利用受害者不了解最新的互联网贷款业务（只要经过平台设置的身份验证，即可在几分钟内将小额款项打入借款人指定的账号）而透支未来的钱财诈骗。该类诈骗手法，最大的危害就是实现了没钱也能骗，并且给受害者造成沉重的经济负担和精

神打击。因为后续可能还要面临每月偿还金融结构贷款，有的受害者甚至被贷款十万、二十万元，如果不能够按时偿还，还将会影响个人征信，而金融机构也会面临坏账等风险。因此这类诈骗手法骗取钱财更多，影响范围更大，危害时间更长。

防骗提示

1） 所有来电：“您好，您是 x 女士/先生么？您在我们的网店购买了 xx”，这种多是骗子话术，如有疑问，可以挂断电话后，联系购物网站上的官方电话核实；

2） 正规的电商网站都没有所谓的异常处理流程或退款流程，还有类似卡单、掉单等词语也都是诈骗专用术语。退款仅需在订单界面点击退款来办理；

3） 切记“我没钱，不怕骗”的心理，谨防骗子利用个人信用进行贷款、预支等行为；

4） 填写验证码，要看清验证码办理的业务内容，遇到办理不明业务的验证码，千万不要着急填写，可先了解该业务后再填写。

5） 遇到账号资金变化时，请详细看清资金往来情况，不要盲目相信多打款，提高信誉额度充值等话术。

四、 骗取付款码刷单兼职诈骗

案例回顾

3 月 10 日，在校大学生小曾在 QQ 群中看到有人发布兼职消息，只要支付宝有剩余的流动资金就可以进行兼职，刷单立返。

小曾心动后主动添加了对方 QQ，与客服沟通过工作内容后，客服要求用户将支付宝付款条形码下面的数字发送给他，完成任务后将提供佣金；于是小曾按照要求将支付宝中付款码的数字 28094261411505371 发送给了对方，对方要求在发送一遍，因为之前的是失效的，用户再一次生成后的付款码 282779473246788892 发送了给了对方，后续发现支付宝产生了 2 笔 99.99 元的扣款，账单收款方是一家经营炒面的普通商户。

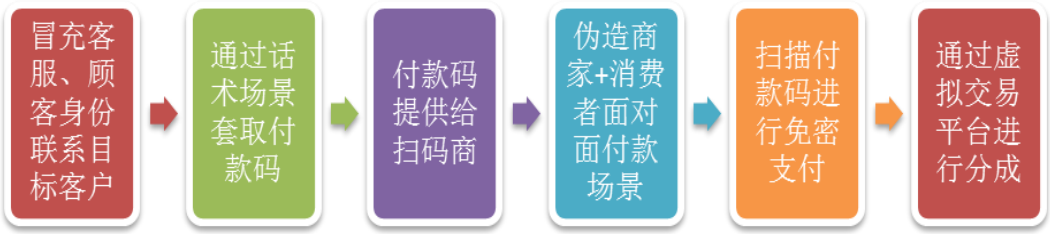

能支付宝接收佣金么
怎么了
你手机打开支付宝吧这个数字发给我
28094261411505371
再重新发一遍新的
任务亲、
282779473246788892
2
你这是失效的啊
怎么了
时间鼓励
你手机打开支付宝吧这个
发送
发送


精领团队-最强辅助:不错
每天特价购物-16-68特价商品发布员:[图片] 领券下单：h
你截图支付宝账单
你在重新发一次那个数字 我给你退 刚才看错了
不能啊 我看看怎么扣你的钱了呢
你就别骗人了那明明是付款码
刚才搞错了
我要是骗你 我何不吧你钱都弄走
请你直接支付宝转账
你自己看看
扣了198
不能直接转账 因为钱在平台里
发送
发送

小曾询问对方为什么交易了两笔，客服回答称卡单了，继续向小曾索取付款码。此时，小曾觉得不对劲，可能遭到了诈骗，并质问对方，要求退还本金，但客服称钱卡在平台中，不能进行支付宝转账给用户返款，并承诺第二天处理好之后给用户，并且还继续要求再次提供数字码，但后续小曾没有提供，客服没有给提供答复。

专家解读

随着手机支付扫码越来越普及，手机已经成为了很多用户的“钱包”；扫码付款既简单又方便，我们在与商家的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，甚至形成了一整条产业链：



1） 冒充兼职客服、淘宝消费者等方式来联系目标用户，伺机套取付款码；

2） 通过话术场景来套取付款码，如兼职人员告知用户需要购买商品，只需提供付款码的数字码即可完成；

3） 付款码收集者处于整个诈骗环节的第一环，将获得的付款码提供给可兑现的扫码商；

4） 付款码支付时针对商家扫描用户二维码（或条形码）来交易时使用，扫码商通过建立商家与用户的面对面支付场景，来完成面对面付款的交易过程；

5） 第三方支付对付款码交易有免密交易上限，一般在 1000 元或 100 元以下，因此很多交易都是 999 元或者 99 元，用户只有在发生交易后才能知道账户已经扣费；

6） 在完成扫码交易后，扫码商与付款码提供者往往通过虚拟商品交易平台（游戏点券）进行分成。

防骗提示

1） 付款码不管是数字还是付款的二维码，都是用于支付场景，提供给对方就会在自己账户中付款，切记一定要确认收款商家后才可以提供；

2） 付款码是用于在面对面商家付款时使用的，一旦有人在聊天或者电话中索要，大多数是有问题，请立刻停止联系；

3） 面临好友的转账打款需求，可通过语音辨别、电话确认，避免遭遇冒牌好友损失财产。

五、 兼职诈骗-微信朋友圈广告

近日，朋友圈开始流行入会发广告轻松兼职的项目。

只要预缴 200 元会费，每天在自己的微信朋友圈里转发推荐信息，每天就能够拿到 20 元的返还工资，按照这样一个说法，这种投资，只要 10 天，就能轻松回本。

除了入会金额和公众号可能不同，但手段都是一样的！看完是不是心里“咯噔”一下，如果家里的老人或孩子遇到了这样的骗子，真说不定就会上当受骗！

专家解读

虚假兼职类诈骗是猎网平台举报类型最多的诈骗，其主要利用高薪、低门槛、简单轻松赚钱为借口，吸引受害者参加。

最近流行在朋友圈分享广告的案例，就是一种很典型的诈骗方式，看上去不用浪费太多时间，只要把相关的广告转发到朋友圈，就可以轻松赚上几十元，其实幕后就是拉你进入所谓的兼职群，缴纳会员费。通常这类诈骗不仅先要收取小额会费，后期还会索要押金、保证金、vip 会员费等，如果相信了骗子所说的话，被骗金额可达上千元。受害者一旦发现了上当受骗，骗子就马上拉黑，消失的无影无踪。

防骗提示

1） 所有那些宣称技术门槛低，工作轻松但又赚钱很快的工作，都是诈骗。

2） 不要相信所谓的会员费、审核费等费用，兼职工作中如果需要缴纳此类费用，绝大多数是诈骗。

3） 如果发现自己已经上当，请及时停止后续的交易，以免损失更多的钱财。

六、 手游卖游戏账号被骗

案例回顾

3 月 14 日，用户曹先生是手游大唐仙妖劫的玩家，在游戏世界中看到有人买号，用户主动私聊并谈好了价钱，对方说通过第三方交易平台比较放心方便，让曹先生将售卖信息挂到乐游阁交易平台。用户通过搜索关键词乐游阁查找到了平台网址。

曹先生在平台上注册后，成功进行交易后准备提现时，平台提示卡号错误，卖号的钱被冻结了。曹先生添加了网站上提示的客服 QQ 号进行咨询，客服称由于用户提现卡号错误，导致资金冻结，需要充值同样的钱进去后，可以解冻。

曹先生通过扫描平台上的支付宝二维码，显示的是为一家公司转账，因为用户之前用过其他的游戏平台，支付也有通过扫描二维码的，以为这个平台是正规的，就没有太在意，支付了 200 元。

之后“客服”主动联系用户称，解冻后要申请特殊订单才可以提现，需充值 1600.1 元，因为用户账户冻结过，所以必须申请才可以，后续这笔钱也可以提现，用户又一次通过支付宝扫描平台上的二维码为对方进行了转账。

曹先生操作完毕后账户又被冻结，客服解释称由于用户是新申请的账号，需要升级到 vip，充值满 4000 即可，这笔钱依然可以进行提现，曹先生因为已经投入了较多资金，想一并取出，就信任了对方，继续充值了 2000.10 元。

再一次操作后客服联系用户称，被网警查到用户有洗钱的嫌疑，需要开通证书，需要继续充值，如果不充值网警会认为先前的充值操作都是洗钱，资金都会归国家进行处理。这时用户已经意识到可能有问题，但还是想将之前投入的钱都取出，在客服的反复催促与欺骗下，用户再次充值 5 笔，一笔 6000.1 元，4 笔 5000.1 元。但后续用户再没得到对方回复，也没得到回款。

专家解读

这是一起典型的通过虚假网游平台钓鱼的诈骗案例，网游交易钓鱼一直以来是诈骗的高发地，通过在游戏中喊话的方式，以“低廉、优惠”的价格为诱饵，让游戏玩家访问钓鱼网址在里面充钱的方式来进行诈骗。

随着智能手机的普及，更多的此类案件集中到了手机游戏中，通过在游戏中喊话、好友发送邮件的方式，来吸引用户联系对方。主要有以下几步：

1） 诈骗客服引导用户通过搜索关键词来找到钓鱼平台，一方面游戏中会屏蔽一些网址，所以通过关键词来规避游戏中的审核；

2） 依靠搜索排名，将钓鱼平台通过搜索优化排名靠前（通常第一位）来让用户对平台更加信任；

3） 在用户充钱后，依靠各种话术，如账户冻结、VIP 功能开启、保证金等来进一步骗取用户更多的财产

防骗提示

1） 游戏中出现的所谓低价、优惠充值，一定不要轻信，通过与实际金额完全不相符的“低廉”交易一定是虚假的，不符合实际；

2） 如果发现平台有问题，切记不要为了得到已经支付的钱，而听从对方的诱导继续充值，这样只会越陷越深；

3） 虚拟物品交易请在游戏或正规平台进行交易，切记不要胆小便宜导致上当。

七、“分享”钓鱼网站诈骗

案例回顾

2017 年 6 月 7 日，大学生小刘在电脑端浏览闲鱼网站官网，并看中了一款二手 iPhone 手机，但商品特别注明了买家要通过 QQ 与卖家进行联系。由于价格合适，看着也是比较新的 iPhone 手机，小刘添加对方 QQ，经历了一番讨价还价，最终决定以 999 元的价格购买该手机。

商谈好价格后，骗子用手机浏览器的分享功能分享了付款网址，由于手机分享的链接无法直接查看域名，好不容易讲好价的小刘还以为自己捡了个大便宜，根本没察觉到异常，毫无警惕地点开了对方发来的链接并付了款。之后，当发现卖家将自己拉黑，且刚刚的付款页面再也打不开时，小刘才意识到受了骗。

专家解读

一般来说，骗子会直接复制钓鱼网址发给用户，而用户根据域名有可能会看出来网站是假的，而这起案例中，骗子没有直接发来钓鱼网址，而是先在自己的手机端浏览器打开钓鱼网址，再利用浏览器的分享功能，把网页分享给用户，这样，用户没法直接看到钓鱼网址而是看到骗子的分享消息，然后点击分享链接，直接付款，导致被骗。

防骗提示

1） 在电商网站购物时，使用电商平台官方通信工具沟通，其既可以记录整个交易过程，方便发生纠结、欺诈时进行投诉，也能拦截非官方虚假钓鱼链接。

2） 支付时，仔细看清支付平台网址、付款对象，谨防支付时在钓鱼网站支付。

3） 购买二手商品时，明显低于市场价格的商品，要谨慎购买，防止上当。

八、退共享单车押金误入假客服陷阱

5 月 26 日，卢先生想要退掉共享单车的押金，就在网上搜索该共享单车的客服电话，在排名靠前的网站标题中找到“075561996422”的客服电话，拨打过去。电话接通后，对方自称是共享单车的客服，退还押金需要在微信平台操作，于是卢先生添加了对方微信，对方要求卢先生提供微信付款数字截图，谎称共享单车的退款系统在此页面进行退款。

想到搜索结果比较靠前，卢先生深信这就是真正的客服，不假思索的就将微信付款码数字截图发给对方，不一会儿，手机连续收到好几条扣款提醒，卢先生才反应过来被骗，立马冻结信用卡，最终损失 5000 元。

专家解读

这起案例中，骗子购买搜索关键词，并通过竞价排名使网站靠前，受害人主动拨打电话后，假客服便向受害人索要微信付款码数字截图，然后盗刷微信绑定的银行卡钱财。

防骗提示

1） 微信、支付宝等付款码数字、条形码、二维码均不能随意泄露。

2） 网上搜索客服电话时，一定要核实是否为官方号码，可通过 360 手机卫士等安全管理软件验证号码真伪。

3） 拨打客服电话，拨打 app 或者官方网站上的客服，不要相信第三方客服电话。

九、网络贷款陷阱多，高额度、低门槛要小心

2017 年 5 月，黄先生想通过互联网办理贷款业务，于是在手机上搜索，看到了一个可以贷款的网站 http://youbb13.top/ ，告知高额度，门槛低，紧凭身份证就可以申请贷款，并且 30 秒快速申请，于是在该网站进行办理。填写完自己的个人信息及贷款需求之后，黄先生接到网站发送的消息，告知其已通过审核，需要加网站客服 QQ 了解贷款具体流程。

开始时，对方要求黄先生付 1000 元作为保证金，在黄先生付款后，对方表示黄先生的银行卡流水不符合借贷要求，接连又让黄先生打了 4000 元给他们。之后，对方说用支票将贷款转账给黄先生，又以黄先生的账户从未用支票转账过为由，要求黄先生先存 4800 元激活此账户，否则支票无法到账。黄先生察觉有异，不想继续申请贷款，对方却要求黄先生再交 500 元才能退还之前的保证金。黄先生此时意识到被骗，立刻报警。

专家解读

近年来，互联网贷款业务快速发展，骗子也盯上了这块业务，制作大量贷款钓鱼网站等待受害者上当受骗。而此类钓鱼网站通常会使用方便快捷、低门槛就能申请高额度贷款的信息来吸引受害者。

这起案例中，黄先生就因为被此类信息所吸引进入网站申请贷款，且在看到这个“贷款网站”后，并没有查询此网站是否备案，是否具备相关金融资质，而是直接填写了自己的个人信息申请贷款。在一般情况下，以“top、pw、tk、xyz”为后缀的网站域名，多为非正规网站，即：没有企业备案的网站。如果遇到这种网站，不论是购物还是贷款、投资，请谨慎考虑，以免上当受骗。尤其是进行投资理财，贷款业务，不仅要看网站是否备案，还要尽量了解其背后企业是否具有资质、规模进行该类业务。尽量选择知名、规模大的企业，谨防小型企业跑路、关闭网站等事情发生。

防骗提示

1） 选择金融理财、贷款等互联网金融服务，要查询网站备案及其背后企业的相关资质，尽量选择知名、规模大的企业。

2） 正规贷款业务，需要进行征信验证，不要相信所谓的轻松放款、内部人员放款等虚假信息，此类信息多为诈骗。

3） 骗子通常会使用保证金、账号激活等借口进行行骗，如果遇到此类话术，千万不要转账或支付。

十、利用亲密付的退改签机票诈骗

机票退改签诈骗，在去年被多次报道，均是受害者收到短信后，按照要求到 ATM 机办理，从而上当受骗。但随时 ATM 转账的新规定，24 小时候到账，骗子采用了第三方支付的方式让受害者转账。

2017 年 5 月，狄先生收到了一条短信“尊敬的 XXX 旅客：您好！您所乘坐的东方航空 2017-05-18 深圳飞往南昌的 U5262 次航班因机械故障已被取消，请速电东航客服 008617319448682 办理退改签业务，您将获得 300 元的延误补偿。给您带来的不便，敬请谅解！东方航空”由于看到短信上显示的姓名、航班号完全一致，狄先生信以为真，拨通了短信中的客服电话。

虚假的客服告知让程先生使用支付宝办理退款业务，先是给了一个企业账号，但狄先生使用收款功能领取补偿金后，不能进行收款。于是虚假客服让狄先生开通亲密付功能。于是按照虚假客服的要求，添加了骗子的支付宝账号，开通亲密付功能，但没有想到，刚开通后，狄先生就发现支付宝产生了 100.10 元和 500.50 元两扣款。此时，狄先生发现被骗，立刻进行报警。

专家解读

机票退改签诈骗是典型的利用个人信息，进行精准诈骗的案例，以前都是通过 ATM 机进行转账操作，由于 ATM 机到账有 24 小时的限制，骗子把转账过程换到了第三方支付平台。并且使用了用户不常使用的亲密付功能。

实际上支付宝的亲密付功能是类似于银行的附属卡功能，有人为亲人、密友开通此功能后，对方在网购消费时，直接从开通者账户中支付，而且不需要开通者确认。目前，“亲密付”的设置额度为 100 元—20000 元。

由于狄先生不太了解这个业务，与骗子开通了亲密付后，骗子盗刷狄先生的金额也就十分容易了。

防骗提示

1） 收到类似“航班取消、航班变动、机票退签改签”等内容的短信时，应通过航空公司客服电话、机场客服电话等多方渠道核实，不要盲目轻信来路不明的信息，更不要拨打短信中提供的陌生号码按照对方的要求转账。

2） 对于自己陌生的业务，不要轻易开通，尤其是涉及到支付相关业务，一定要了解后再开通

附录 1 猎网平台/联盟相关工作

猎网平台与公安机关紧密合作

2017 年 Q1 季度猎网平台与贵阳、包头、黔东南、葫芦岛等多地网安开展深度合作，包含猎网校园行、猎网直播厅等活动。

2017 年 Q1 季度猎网平台与新增“猎网追踪”功能融入到猎网平台举报页面内，全面开放 360 安全大数据，向各地公安机关和网民全面开放检索功能，对可疑的手机号、网址、QQ 号码进行查询，检索欺诈信息，同时当地市民还可以通过当地官方平台进行猎网平台一键举报。新增包头市、葫芦岛市、云南省、盘锦市、贵阳市、重庆市、秦皇岛市官方平台加入猎网平台举报页面。

2017 年 Q1 季度猎网平台，已与全国 323 个地区的公安机关建立联系，正在协助侦查 76 起重大网络诈骗犯罪案件，破获 5 个案件， 打掉多个组织严密、分工明确的大型诈骗团伙。

猎网联盟成员协同处理网络诈骗信息

2016 年 5 月 12 日，在北京市公安局网络安全保卫总队指导下，360、百度、京东、58 同城等 25 家主流网站作为首批联盟成员正式接入猎网平台，并成立了猎网联盟。联盟成员将在公安部门的监督指导下，以猎网平台大数据为基础，共享网络欺诈信息并及时协同处理网上诈骗信息，通过压缩诈骗信源的传播时间和空间，有效遏制网络诈骗。

截止到 2017 年 5 月 8 日，共 4 家网安（北京、厦门、扬州、焦作）和 99 家互联网企业成员正式加入。

2017 年 Q1，猎网平台接到的与联盟成员相关的不良信息举报数量总计为 495 件，涉及联盟成员网站数量为 13 个（已经去重），通报联盟成员不良信息数量 495 件，联盟成员已处理不良信息数量 193 件，联盟成员暂未处理不良信息数量为 302 件。

月份	接到举报数量	涉及联盟成员数量	通报举报信息数量	已处理举报信息数量	暂未处理举报信息数量
1 月	130	6	130	87	43
2 月	122	9	122	28	94
3 月	243	9	243	78	165
总计	495	13（去重）	495	193	302

表 2　猎网平台接到针对联盟成员的举报信息数量及联盟成员处置举报信息表

附录 2 典型网络诈骗形式及简介

（一） 虚假兼职

骗子利用 QQ、QQ 群、邮箱和搜索引擎等渠道发布虚假兼职广告，诱骗受害者上当。网络兼职诈骗的形式很多，最常见的是保证金欺诈和刷信誉欺诈。

防骗提示：所谓的高薪、轻松的招聘信息多为诈骗，找工作在正规机构或网站寻找，并且要看清用人机构的真实性。

（二） 虚假购物

骗子通过搜索引擎、QQ 等方式诱骗用户进入虚假的购物网站进行购物消费。用户在这些虚假的购物网站上消费后，不会收到任何商品。绝大多数虚假购物网站都是模仿知名购物网站而进行精心设计和改造的。

防骗提示：不购买价格明显低于市场正常价格的商品，网购要在正规电商平台内完成。

（三） 退款欺诈

消费者在网店购物后不久，便会接到自称是网店店主或交易平台客服打来的电话。电话中，对方往往能够准确的说出消费者刚刚购买的商品名称和价格，并以交易失败，要给消费者办理退款手续为由，诱骗消费者在钓鱼网站上输入自己的银行账户、密码、购物网站登陆账户、登陆密码等信息，进而盗刷用户的支付账户。其中，消费者消费信息的泄漏，是骗子能够完成此类诈骗的重要原因。

防骗提示：退款通过电商渠道正规流程办理，需要提供银行卡号和密码的都是骗子。

（四） 网游交易

骗子通过游戏大厅喊话，QQ 群喊话等方式，兜售明显低于市价的游戏装备或游戏道具，诱骗受害者到虚假的游戏登录界面或游戏交易网站进行登录或交易，进而骗取受害者的游戏帐号、游戏装备和虚拟财富。此类欺诈还往往会结合交易卡单、解冻资金等其他骗术实施连环欺诈。

防骗提示：游戏交易要看清交易网站合法性，明显低于市价的交易大部分为诈骗。

（五） 赌博博彩

骗子诱骗受害者在虚假的博彩网站上进行赌博活动。而受害者不论在这些博彩平台上是赔是赚，都无法将赌资从自己的账户中提走。还有一些虚假的博彩网站会操纵赌博过程，诱使受害者的赌资快速输光。

防骗提示：在我们国家，赌博属于违法行为，不要参与。网上的赌博网站也属于违法网站。

（六） 视频交友

骗子通过虚假的视频交友网站或裸聊网站，诱骗受害人不断交费以获取更高级别的服务特权。但实际上，不论受害人向自己的账户充值多少钱，都看不到网站承诺的任何服务。

防骗提示：提供色情视频服务的网站属于违法网站，不要参与。同时在网络交友时，不

要轻易给对方转钱。

（七） 金融理财

骗子开设虚假的金融网站、投资理财网站，通过超高收益诱骗投资者进行投资。而投资者一旦投资，往往根本无法取回本金。常见的投资理财欺诈形式包括天天分红、网上传销和P2P 贷款欺诈等。

防骗提示：金融理财商品要在大型机构购买，不信所谓的无风险，高回报，内幕消息等宣传。

（八） 虚假团购

骗子开设虚假的团购网站诱骗用户进行消费。虚假团购网站大多通过搜索引擎的推广服务进行传播。虚假团购网站销售的商品以游乐园门票、电影票、餐饮票等居多。误入虚假的团购网站会导致财产损失。

防骗提示: 对于不知名的团购网站，需要看清网站备案等是否合法，谨慎团购商品。

（九） 虚假票务

骗子开设虚假的票务网站（包括飞机机票、火车票、轮船票等）实施欺诈。

防骗提示：办理机票退、改签业务要找航空、铁路公司或购票商办理，不可轻信陌生短信、电话告知的方式办理。

（十） 虚假批发

骗子开设虚假的批发销售网站，诱骗受害人进行购买。

防骗提示：对于低价、批发的产品，需要看清其营业资质等是否合法，谨慎批发商品。

（十一）网购木马

网购木马是专门用于劫持用户交易资金的木马。此类木马大多通过 QQ 传播。

防骗提示：不要轻易点击安装未知来源的软件，软件要在官方渠道下载。

（十二）虚假中奖

骗子通过中奖短信等方式，以巨额奖金为诱饵，诱骗受害者进入虚假的中奖网站，再以“先交费/税，后提货”为由，诱骗消费者向骗子账户付款。

防骗提示：如果参与抽奖活动，要通过官方渠道进行中奖合适，不轻信短信、邮件等告知的中奖信息。

（十三） 话费充值

骗子开设虚假的话费充值网站，通过搜索引擎等渠道，诱骗消费者进行充值交费。

防骗提示：话费充值要在官方或大型第三方购票网站购买，不可轻信所谓低价、特价信息。第三方话费充值需看清网站合法性。

（十四） 虚假药品

骗子开设虚假的药品网站，卖假药或者是只收钱不卖药。

防骗提示：购买药品品要认准生产商，在正规渠道购买，杜绝来路不明的商品

（十五） 账号被盗

骗子盗取受害者银行、社交工具等账号和密码，从而造成金钱损失的诈骗。

防骗提示: 网银、网上支付、常用邮箱、聊天帐号单独设置密码，切忌一套密码到处用，重要帐号定期更换密码。

（十六） 冒充熟人

骗子冒充被害者的父母、兄弟、姐妹、朋友、同事、领导等比较熟的人，通过短信、QQ、电话等方式来骗取受害者钱财。

防骗提示：陌生电话打来询问，不要透露过多个人信息，如遇到转账等要求，需要核实是否真实为认识的熟人，不可轻易转账。

（十七） 冒充公检法

骗子冒充公安机关、法院、检察院、国家安全局、交通局等国家机构的办公人员，谎称受害者涉嫌某类案件需要配合调查，并以恐吓、威胁等方式骗受害者取信，并要求受害者通过 ATM 机、网银等方式将资金转入所谓的保障账户、公正账户等类型的诈骗犯罪。

防骗提示：公检法机关不会要求将资金转入国家账号配合调查，遇到这样的话术全是骗子。

（十八） 代办信用卡

骗子谎称银行机构或银行代办机构，可以帮助受害者办理大额信贷信用卡，骗取受害者佣金的诈骗行为。

防骗提示：信用卡要在银行或其指定的正规渠道办理，个人所谓的办理高额透支信用卡基本为诈骗。

（十九） 信用卡提升额度

骗子谎称银行机构或银行代办机构，可以帮助受害者提升信用卡额度的诈骗行为。

防骗提示：不要信任此类信息，提升信用卡额度请在正规渠道办理。

（二十） 虚假客服

冒充银行、运营商、淘宝、腾讯等一些正规机构的客服人员，给受害者打电话谎称帮助办理某项业务，从而盗取受害者银行账号、密码等，使得受害者损失财产。

防骗提示：可通过运营商官网、客服电话等渠道查询真伪，不轻信主动打来的电话和短信。

（二十一） 代付欺诈

代付是第三方支付平台提供的一项付款服务，买家购买商品付款的时候，可以找其他人帮忙代付该笔款项。骗子伪装成卖家，在与受害者谈好交易后，将一个伪装好的代付款链接发给受害者，使得受害者付的款项并不是先前谈好的商品，造成被骗的诈骗活动。

防骗提示：网络购物，需按照电商平台正规流程付款，其他付款方式风险高，如需代付

款，请看清付款链接的商品后再付款。

（二十二） 微信红包

主要是通过微信或微信群以返还红包、借钱、充话费、进群必须发红包等为借口，骗取受害者进行钱财的诈骗。

防骗提示:不要随意给陌生人发红包，需要交钱才能进入的群大部分是从事着诈骗、赌博、色情等违法活动，此种群请不要进。

（二十三）补贴诈骗

骗子冒充民政单位工作人员，向家长打电话、发短信，谎称可以领取生育补贴，要其提供银行卡号，然后以资金到账查询为由，指令其在自动取款机上进入英文界面操作，将钱转走

防骗提示：不轻信此类电话，补助款项接收需要正规流程，到 ATM 机办理均为诈骗。

（二十四）保证金诈骗

骗子冒充商家发布“点赞有奖”、“注册送礼”等活动,要求参与者填写姓名、电话等个人资料，一旦商家套取足够的个人信息后，即以缴纳保证金等形式实施诈骗。

防骗提示：参加活动前要看准主办方资质，不轻易在泄露自己的个人信息的同时谨防对方的骗钱行为。