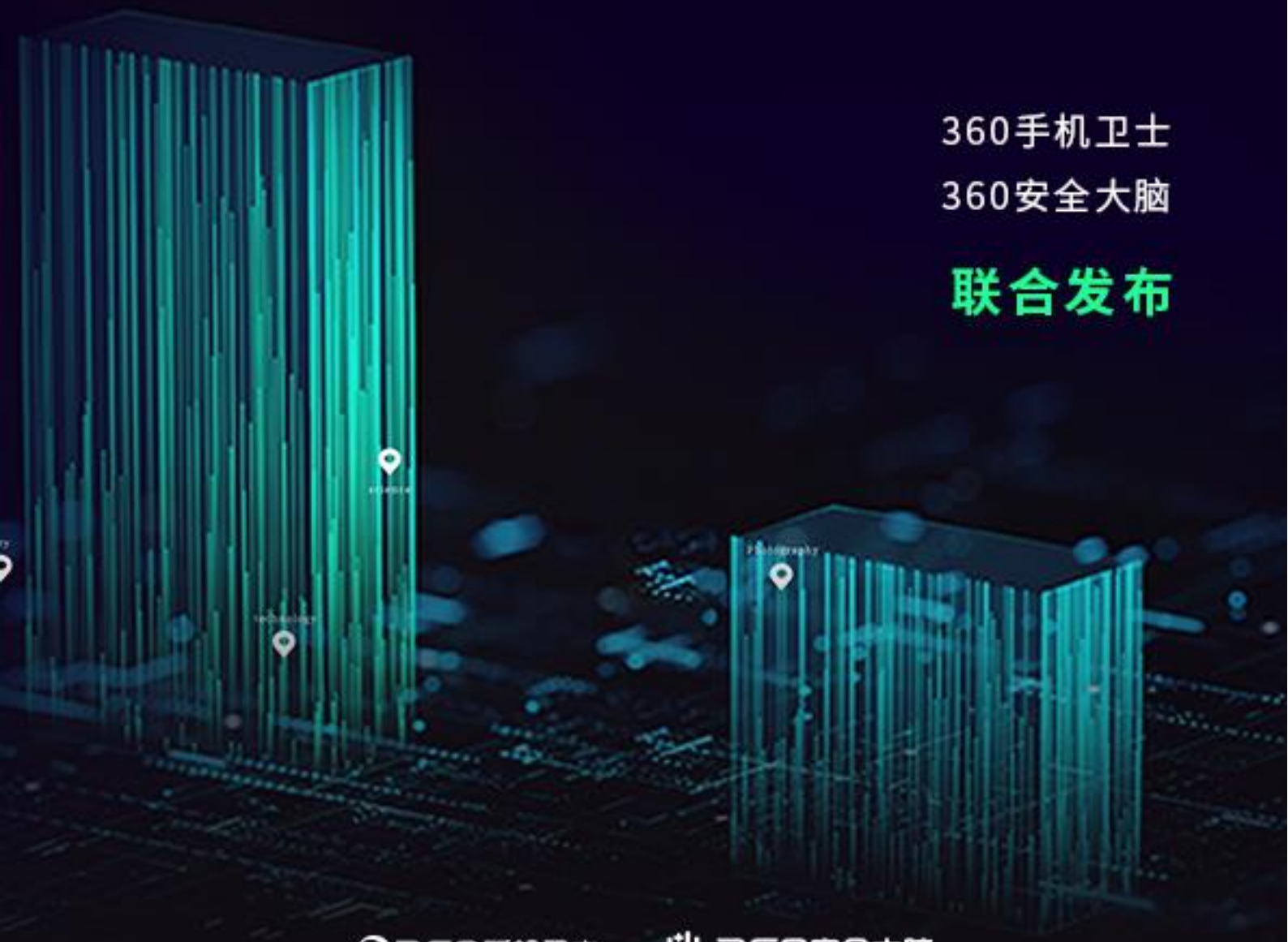
2020假期
安全防骗指南

360手机卫士
360安全大脑
联合发布



360手机卫士　360安全大脑

导语

2020 年受疫情影响，人们被迫宅在家中，这也令大部分人改变了自身的生活习惯。无论家庭办公还是打发时间，人们的生活已经潜移默化地被手机、电脑、平板、电视等电子设备所支配。因此，疫情也成为了骗子行骗的摇篮，并借此萌生了一批新型的诈骗手段。

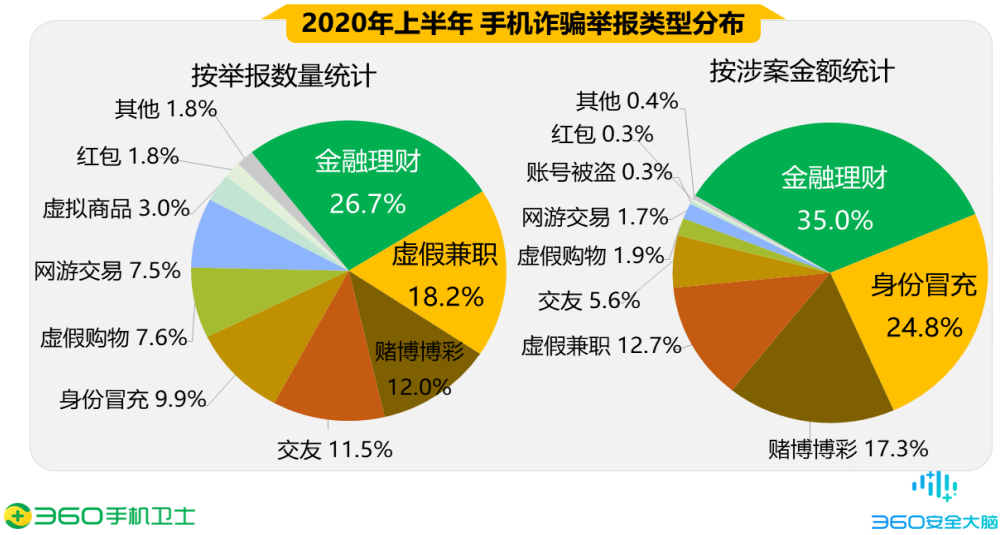
随着疫情的态势逐渐放缓，人们也开始走出家门。同时伴随“十一长假”的来临，势必将迎来一波假期出行的小高潮。骗子们当然也绝不会放过这种千载难逢的“赚钱”机会。随着信息技术的发展，诈骗、窃取隐私的手段更加专业、多样，不法分子利用电话、短信、钓鱼网站等方式作案，通过摄像头等设备窃取用户的隐私，严重影响了社会稳定，威胁到了广大人民群众的财产、个人隐私安全。借此发布十一假期安全防骗指南，为宅家或出行的您提供多一份生活保障。

目录

第一章 疫情下手机诈骗的态势，这个假期不得不防

一、 报案数量与类型

2020 年上半年度 360 手机先赔共接到手机诈骗举报 1561 起。其中诈骗申请 776 起，涉案总金额高达 778.9 万元，人均损失 10037 元。在所有诈骗申请中，金融理财占比最高，为 26.7%；其次是虚假兼职（18.2%）、赌博博彩（12.0%）、交友（11.5%）、身份冒充（9.9%）、虚假购物（7.6%）等。从涉案总金额来看，同样是金融理财类诈骗总金额最高，达 272.4 万元，占比 35.0%；其次是身份冒充诈骗，涉案总金额 193.4 万元，占比 24.8%；赌博博彩排第三，涉案总金额为 135.1 万元，占比 17.3%。下图为 2020 年上半年度手机诈骗类型的举报类型与涉案金额分布情况：



2020 年上半年度，手机诈骗中身份冒充、赌博博彩、金融理财属于高危诈骗类型；虚假兼职属于中危诈骗类型。其中，身份冒充类人均损失最高，约 2.5 万元；赌博博彩类人均损失约为 1.5 万元；其次为金融理财类，人均损失约为 1.3 万元。

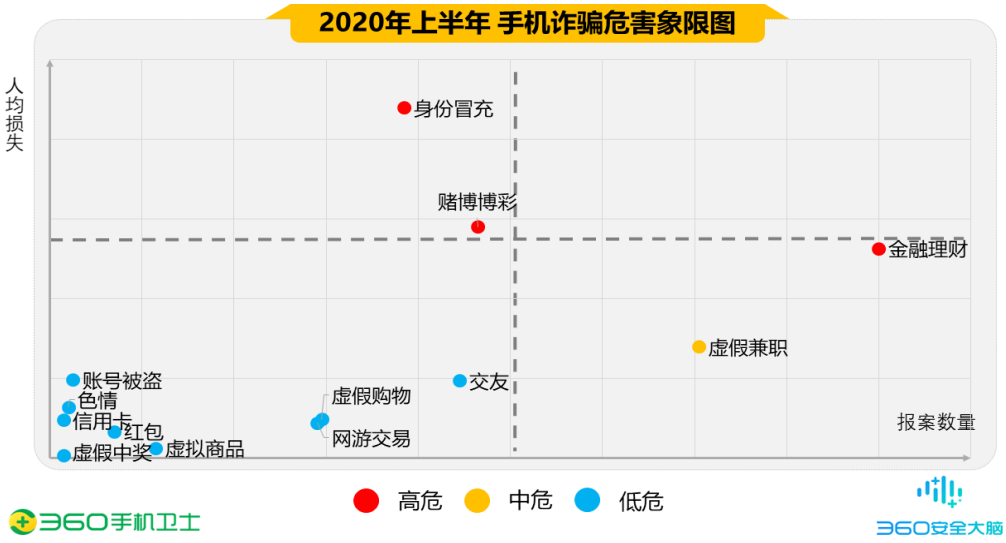
1） 2020 年上半年度身份冒充类主要以冒充亲友与冒充客服为主，其次为冒充公检法。其中，冒充亲友主要为伪装身份向通讯录好友借钱、伪装亲友出事讨要费用；冒充客服人员主要为冒充官方平台客服，以订单异常、快递丢失、商品质量存在问题需退款等借口实施诈骗，诱导用户进行转账；另外在 2020 年在疫情期间，存在不法分子冒充公检法机关人员，利用疫情期间受害人护照被扣留、存在不明出境记录、社保卡涉嫌骗保等借口实施诈骗的案例发生，且涉案金额巨大。

2） 赌博博彩类一直属于手机诈骗中的高发类型，在 2020 年第一季度疫情期间尤为突出，半年度也依然处于诈骗 TOP 前三。其手法主要以事前“赠送彩金”为吸引点，诱导用户

在赌博网站充值赌资，后期限制提现导致用户损失；或以“赚钱”为噱头引导用户至赌博平台进行兼职操作，例如兼职刷单、彩票跟投等，但后期不返还本金与佣金。随着移动端用户群体的激增，赌博博彩跟随潮流，呈现出 PC 端向移动端倾斜发展的现状。诈骗实施中，不法分子引导用户通过移动端设备访问赌博网站或下载 APP 充值赌资成为主流手段。由于第一季度疫情的出现，用户居家隔离且缺少社交娱乐活动及赚钱方式，因此利用网络寻找消遣及赚钱成为多数用户的选择，不法分子在此期间“推波助澜”，借助互联网渠道大肆宣传赌博平台，导致赌博博彩类案例频发，人均损失高达 1.5 万元。

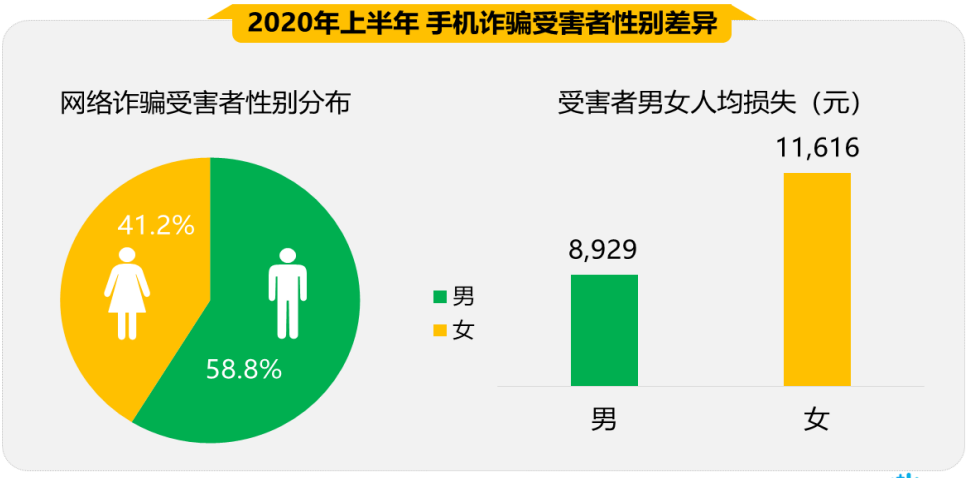
3） 2020 年上半年度中金融理财类是受骗人数最多且涉案损失最高的类型，主要体现为网络贷款被骗。收取贷款手续费、包装费或引导用户下载借贷 APP 操作属于借贷诈骗的主要手法。同样受到疫情影响，大多数人选择利用网络贷款缓解经济压力。一般来说网络中无抵押贷款、秒下款等借贷广告更易吸引眼球，在双方成功取得联系后，不法分子将会通过多种方式要求用户进行付款操作。超前消费已成为普遍社会现象，贷款诈骗正是利用这一社会痛点实现疯狂蔓延，目前依然呈现高发态势。贷款诈骗案例中，首次与用户联系时，通过电话方式与用户沟通的现象较多，但通过上半年度金融理财案例的汇总，通过社交平台实施贷款诈骗的比例上升，疑似成为宣传并实施贷款诈骗的新兴渠道。

4） 2020 年上半年度虚假兼职类型以兼职缴纳会费的手法居多。受到疫情影响，尝试通过网络赚钱缓解经济压力成为部分人的选择之一。由于不法分子通常利用社交平台发布兼职广告，吸引众多用户进行兼职任务，在此敏感时间段，更是打着疫情的旗号，招揽更多用户参与，导致遭受诈骗的用户数量居高不下。

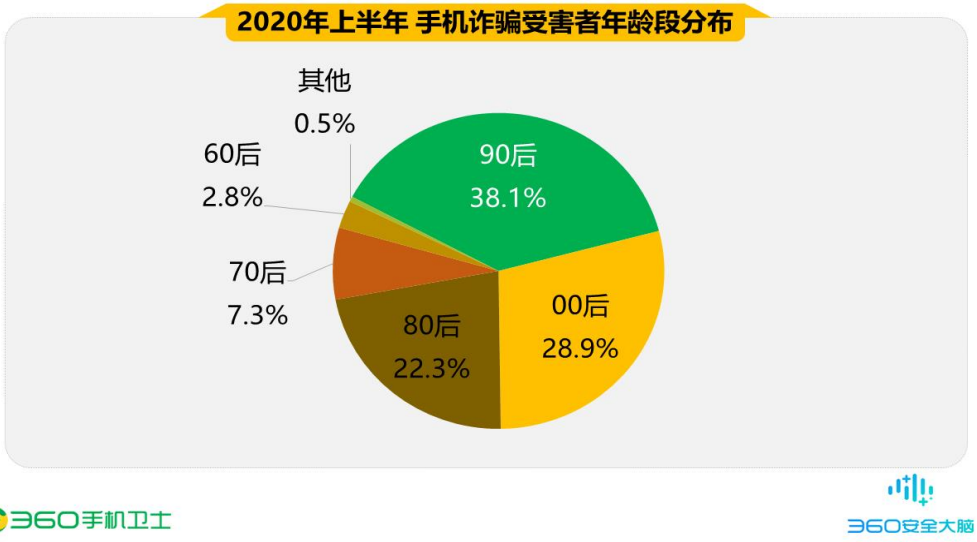


二、 受害者性别与年龄

2020 年上半年度，从举报用户的性别差异来看，男性受害者占 58.8%，女性占 41.2%，男性受害者占比高于女性。从人均损失来看，男性为 8929 元，女性为 11616 元，女性人均损失高于男性。下图为 2020 年上半年手机诈骗受害者性别差异：

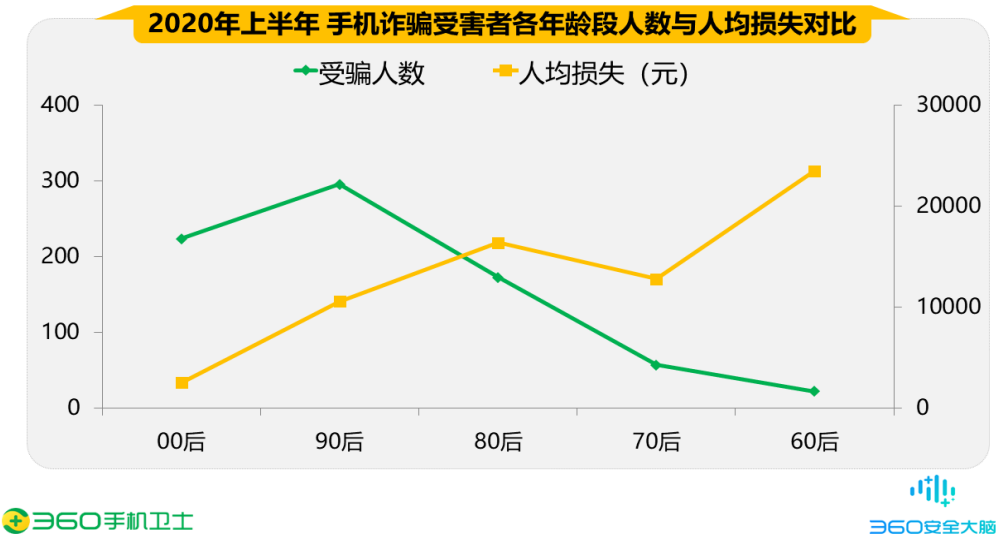


从被骗网民的年龄段上看，90 后的手机诈骗受害者占所有受害者总数的 38.1%，是不法分子从事网络诈骗的主要受众人群；其次是 00 后，占比为 28.9%；80 后占比为 22.3%；70 后占比为 7.3%；60 后占比为 2.8%等。下图为 2020 年上半年手机诈骗受害者年龄段分布：



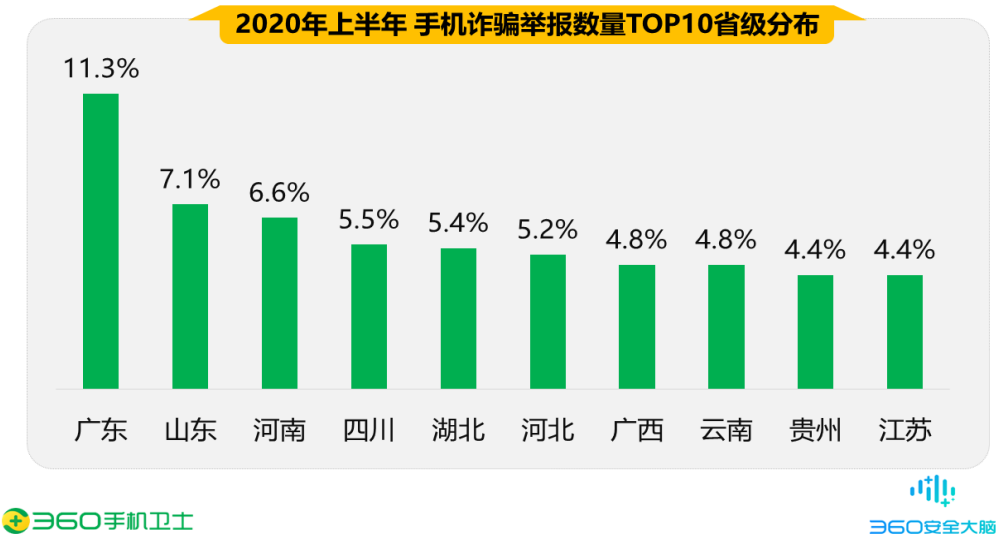
2020 年上半年度，00 后与 90 后受骗人数较为接近。但是通过对比发现，00 后被骗的人数虽多，但由于这个年龄段用户经济能力有限，被骗平均金额相对较少。90 后作为 2020 年上半年度诈骗主要针对人群，人均损失也较高。80 后及以上年龄段日常使用网络的时间

有限，遭受诈骗的人数也较少，但由于这部分用户有一定经济实力，在遭受诈骗时，损失金额也相对较高。

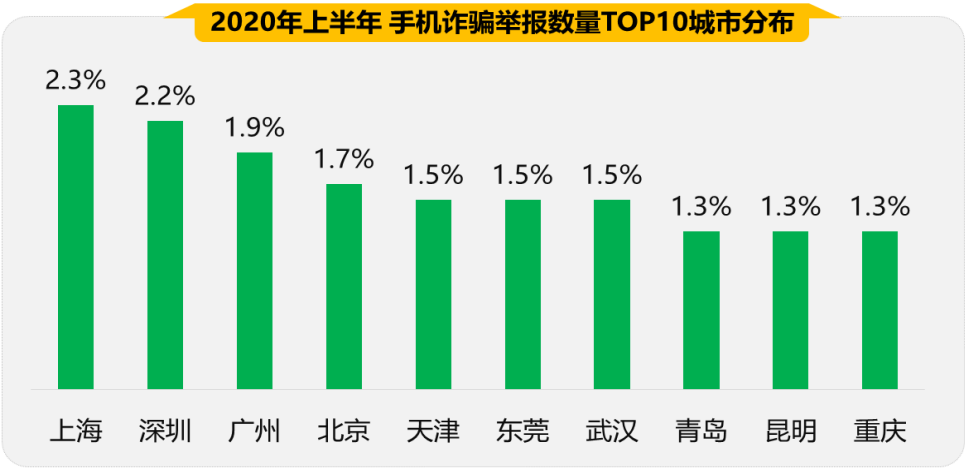


三、 受害者地域分布

2020 年上半年度，从各地区手机诈骗的举报情况来看，广东（11.3%）、山东（7.1%）、河南（6.6%）、四川（5.5%）、湖北（5.4%）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 36.0%。下图给出了 2020 年上半年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，上海（2.3%）、深圳（2.2%）、广州（1.9%）、北京（1.7%）、天津（1.5%）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 9.7%。下图给出了 2020 年第一季度手机诈骗举报数量最多的 10 个城市：



360手机卫士　　360安全大脑

第二章 钓鱼骗局瞄准手机用户，假期用机需谨慎

随着移动设备数量的不断增长，针对移动设备的钓鱼网站攻击也愈加明显。排除有明显恶意行为的典型钓鱼网站，金融借贷、网购以及出行类钓鱼网站同样具备高风险，用户易遭到信息泄露、高利贷款，甚至贷款诈骗等风险。网络借贷具备申请便利、下款快等特征，近几年受到大众的追捧。网络借贷的火热，吸引了众多“鱼龙混杂”的借贷平台上线。受疫情影响，金融借贷诈骗案件持续高发，已成为受害人数最多、涉案金额最高的诈骗类型。

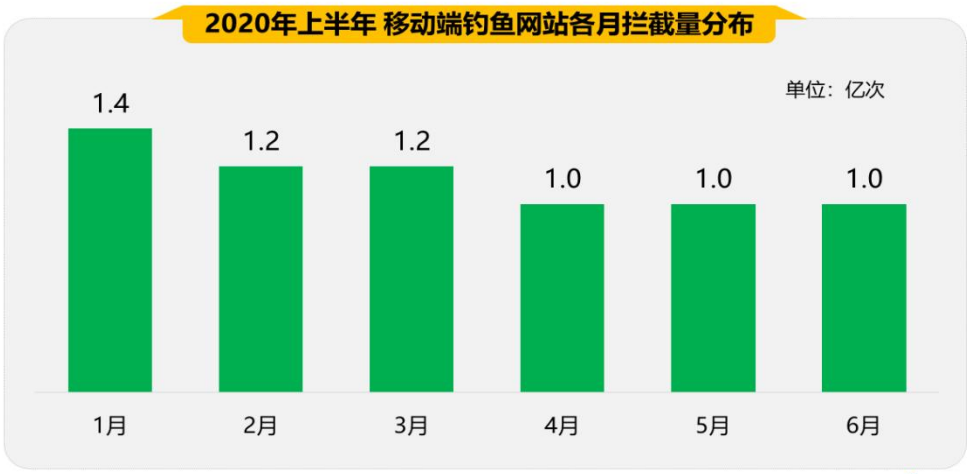
针对金融借贷发展现状，360 安全大脑及时调整相关拦截策略，针对金融借贷类钓鱼网站建立研究专项，大大提升了样本检测量与样本拦截能力，在用户遭遇欺诈前，及时识别疑似包含恶意行为的金融借贷类网站，以防护用户的信息安全与财产安全。

一、 移动端钓鱼网站拦截占比

2020 年上半年度，360 安全大脑在 PC 端与移动端共为全国用户拦截钓鱼网站攻击约 435.8 亿次，同比 2019 年上半年度（404.2 亿次）上升了 7.3%。其中，PC 端拦截量约为 429.1 亿次，占总拦截量的 98.5%，平均每日拦截量约 2.4 亿次；移动端拦截量约为 6.7 亿次，占总拦截量的 1.5%，平均每日拦截量约 369.6 万次。下图为 2020 年上半年度钓鱼网站拦截占比分布：

二、 移动端钓鱼网站各月拦截量分布

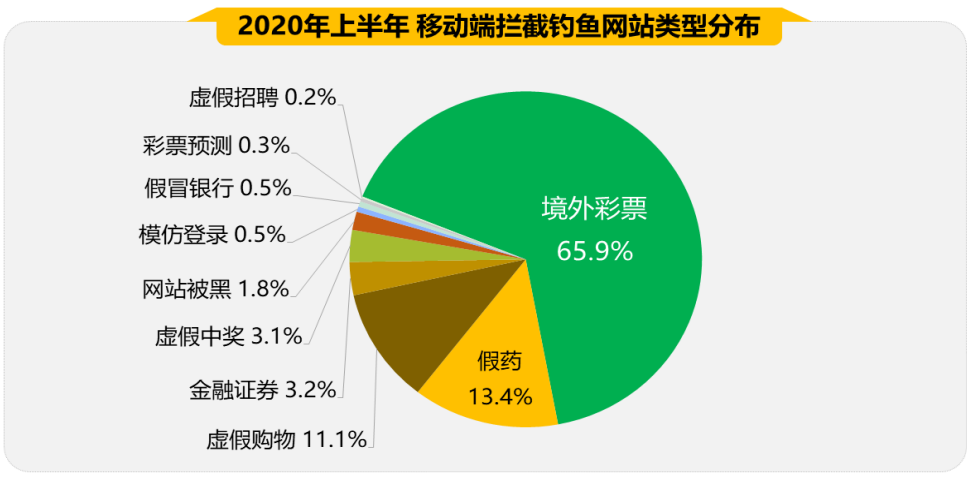
2020 年上半年度，360 安全大脑在移动端拦截钓鱼网站攻击约为 6.7 亿次，同比 2019 年上半年度（13.8 亿次）下降 51.1%。下图为 2020 年上半年度钓鱼网站各月拦截量分布：



360手机卫士　　360安全大脑

三、　移动端钓鱼网站类型分布

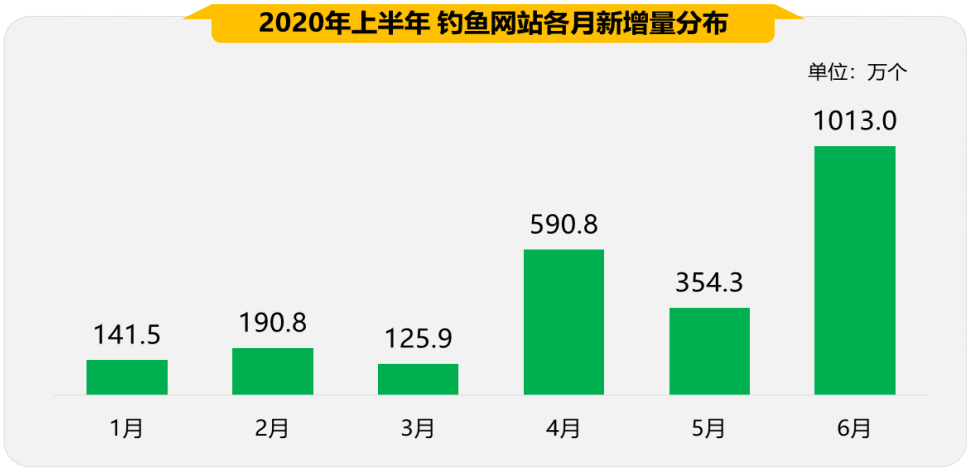
2020 年上半年度，移动端拦截钓鱼网站类型主要为境外彩票，占比高达 65.9%；其次为假药（13.4%）、虚假购物（11.1%）、金融证券（3.2%）、虚假中奖（3.1%）、网站被黑（1.8%）、模仿登陆（0.5%）、假冒银行（0.5%）、彩票预测（0.3%）与虚假招聘（0.2%）。下图为 2020 年上半年度移动端拦截钓鱼网站类型分布：



360手机卫士　　360安全大脑

四、　移动端钓鱼网站新增量

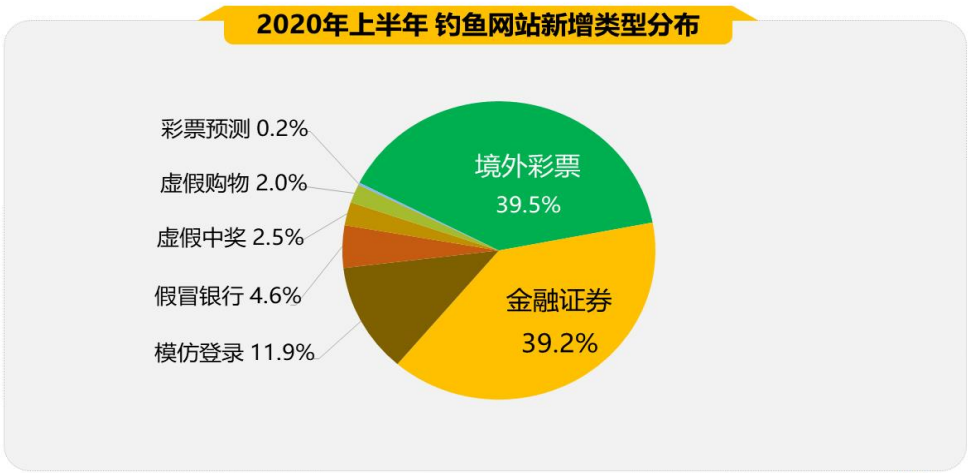
2020 年上半年度，360 安全大脑共截获各类新增钓鱼网站 2416.3 万个，同比 2019 年上半年度（1019.2 万个）上升了 57.8%，平均每天新增 13.3 万个。



360手机卫士　　360安全大脑

观察钓鱼网站新增类型，境外彩票类占据首位，占比 39.5%；其次为金融证券类，占比 39.2%。

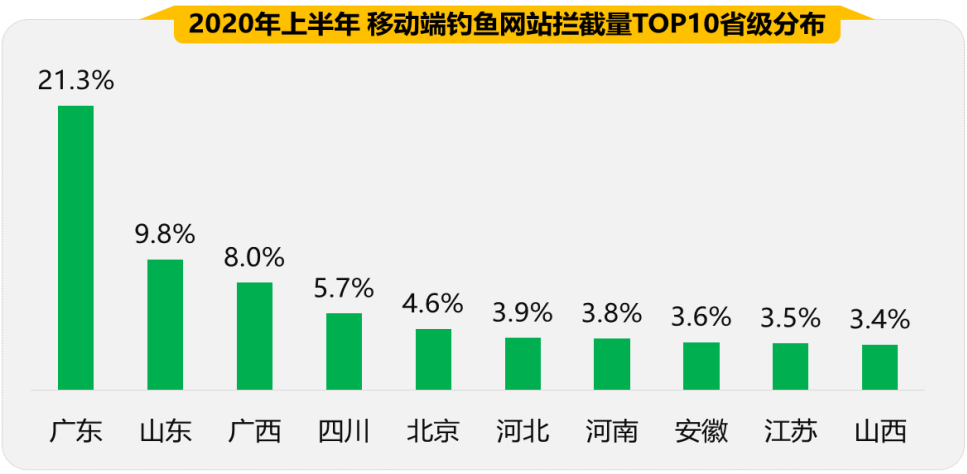
随着近几年网络贷款的兴起，互联网中贷款平台丛生，资质参差不齐，滋生了大量虚假贷款平台。第一季度受疫情原因影响，部分大众收入来源遭受影响，由于网络贷款具备快捷、便利、下款快的特点，很多人选择利用网络贷款缓解经济压力，不法分子便利用此社会现象大肆传播虚假贷款平台，导致贷款诈骗案件频发。针对这一现状，360 安全大脑及时调整相关拦截策略，针对金融借贷类钓鱼网站建立研究专项，大大提升了样本检测量与样本拦截能力，在用户遭遇欺诈前，及时识别疑似包含恶意行为的金融借贷类网站，以防护用户的信息安全与财产安全。



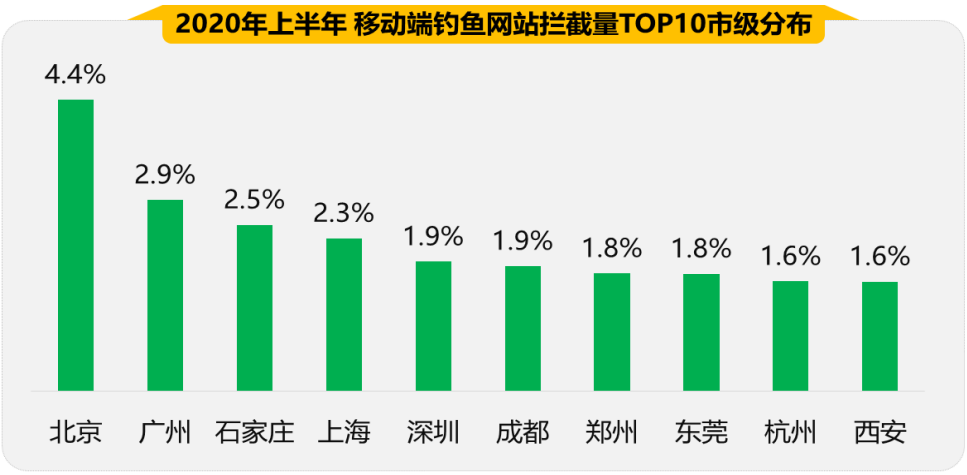
360手机卫士　　360安全大脑

五、 移动端钓鱼网站拦截量地域分布

2020 年上半年度，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 21.3%；其次为山东（9.8%）、广西（8.0%）、四川（5.7%）、北京（4.6%），此外河北、河南、安徽、江苏、山西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北京市，占全国拦截量的 4.4%；其次为广州（2.9%）、石家庄（2.5%）、上海（2.3%）、深圳（1.9%），此外成都、郑州、东莞、杭州、西安的钓鱼网站拦截量也排在前列。



第三章 假期出行，时刻警惕个人隐私保护

科技进步除了让人们的生活更加舒适之外，也带来不少关于隐私的问题，网络摄像头偷拍就是其中一种。

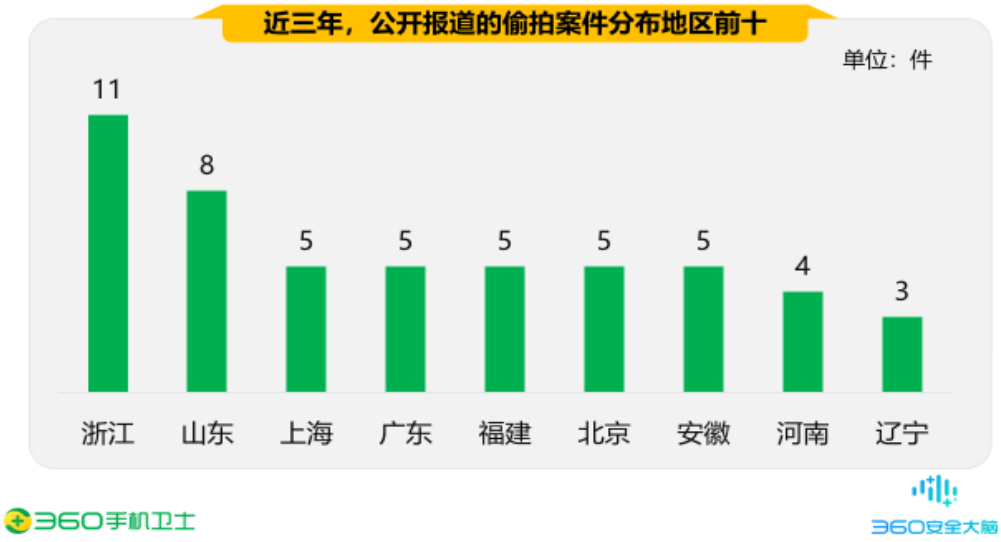
近年来，此类事件频发。2019 年的公安部专项“净网行动”中，各地警方曾协作破获了一起涉案针孔摄像头、配件及半成品高达上百万个的非法生产、销售针孔摄像头案件。查获的绝大多数摄像头都伪装成日常生活用品，隐藏的非常巧妙，常人轻易无法察觉，更难以防备。

面对即将来临的假期出行小高峰，我们也不能放松警惕，谨防我们个人的隐私在无意之间泄露出去。360 手机卫士推出了“摄像头检测”功能，可以一键检测同一网络环境下可疑的摄像设备，有效检出隐蔽摄像头，提醒用户关注，保护用户隐私安全。截止目前，360 手机卫士已累计为用户提供摄像头检测服务超 2500 余万次。

自中国裁判文书网及官方媒体报道中，共统计到最近 3 年中，83 起涉及“偷拍”的案件。案件被报道数量呈逐年上升趋势。案件类型较为集中，多为采用无线针孔摄像头对受害人隐私进行侵犯。以下是近三年，摄像头偷拍案件数据分析及典型案件解析：

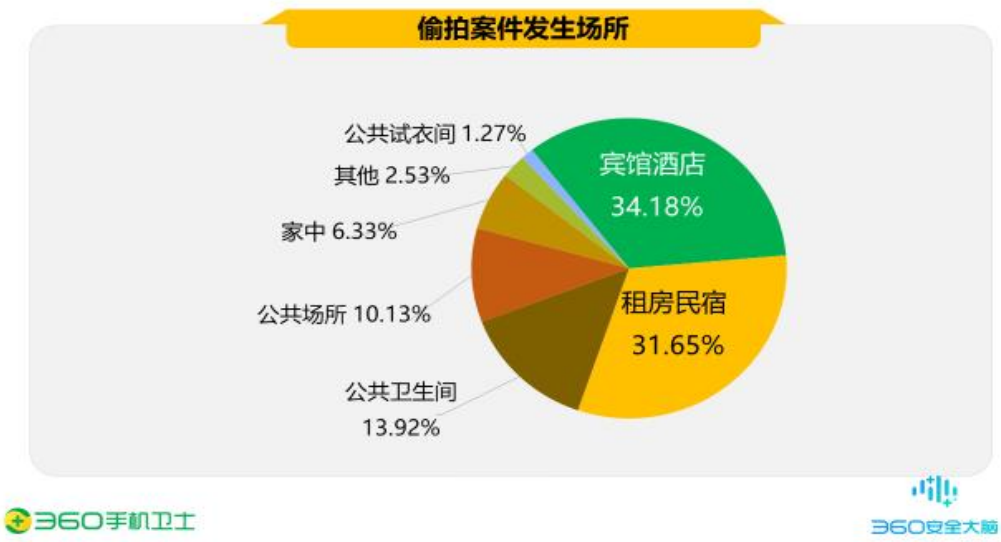
一、 地域分布

从地域来看，偷拍案件广泛发生于全国各地，不仅在一二线城市需要小心偷拍，在三四线城市也要对其多加小心。



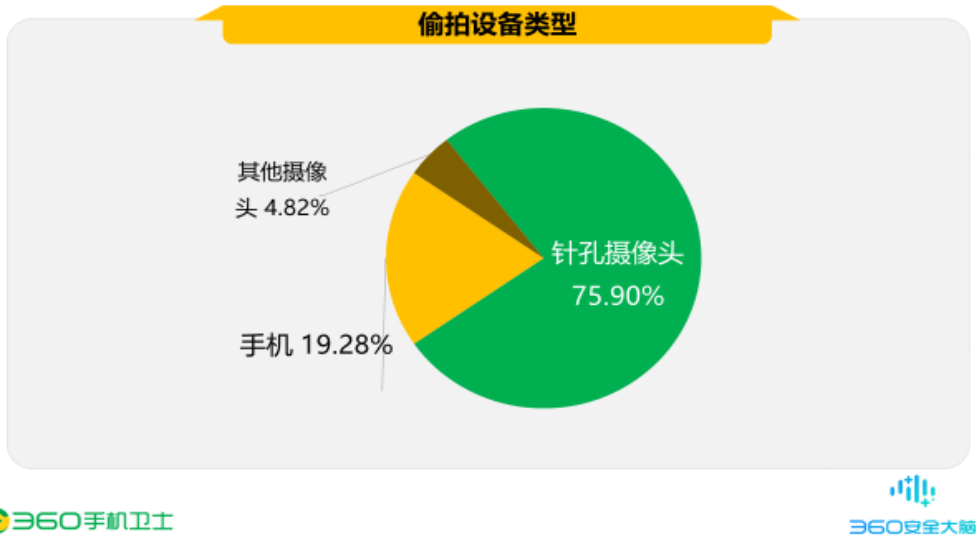
二、 偷拍场所

从偷拍案件发生场所来看，以宾馆酒店（34.18%）、租房民宿（31.65%）、公共卫生间（13.92%）这三类场所发生偷拍案件较多，其中尤以宾馆酒店和租房民宿最多。值得注意的是，不仅住在小宾馆会有被偷拍的可能，就算是在知名酒店、出租房屋、品牌公寓、短租日租房，甚至自家房屋都有被偷拍的可能，据下图显示的数据就可以看到，有 6.33%的偷拍案件发生于家中。



三、 偷拍设备属性

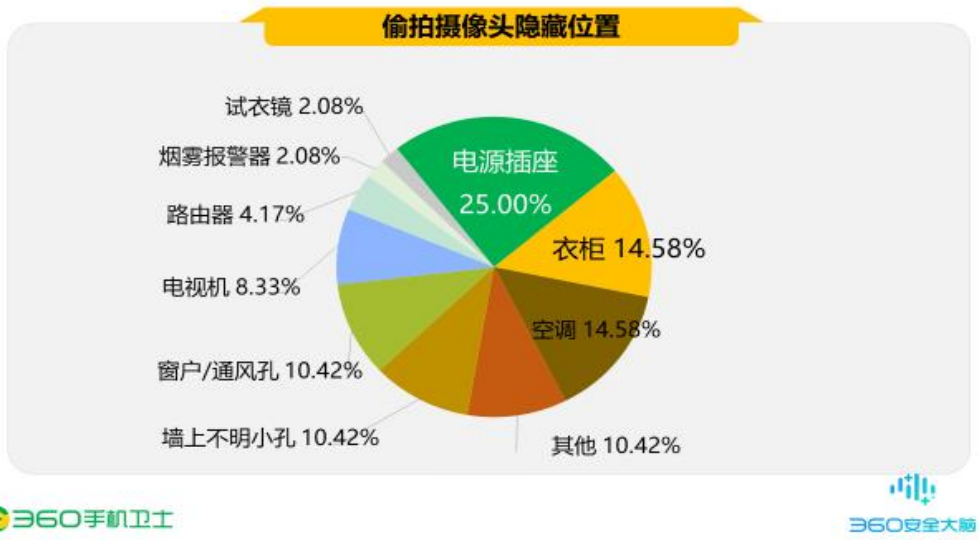
科技进步带来的不仅是生活便利，也使得某些犯罪手段变得更加难以发现。根据已统计到的偷拍案件数据显示，有 75.90%偷拍设备使用的是隐蔽性良好的针孔摄像头，排名第二位的是在公共场所偷拍中常见的手机，其他类偷拍设备（如监控摄像头）仅占 4.82%。



偷拍者使用的针孔摄像头中，绝大多数（96.23%）都采用了无线 Wi-Fi 网络进行连接，使用网线连接的仅有 3.77%。也就是说，目前主流的非法针孔摄像头都采用了无线 Wi-Fi 连接网络。

四、 摄像头隐藏在房间何处

以下为我们统计到的案件中，偷拍摄像头在房间内所隐藏的具体位置，其中电源插座（25.00%）、衣柜（14.58%）、空调（14.58%）、电视机（8.33%）为偷拍摄像头隐藏的重灾区。

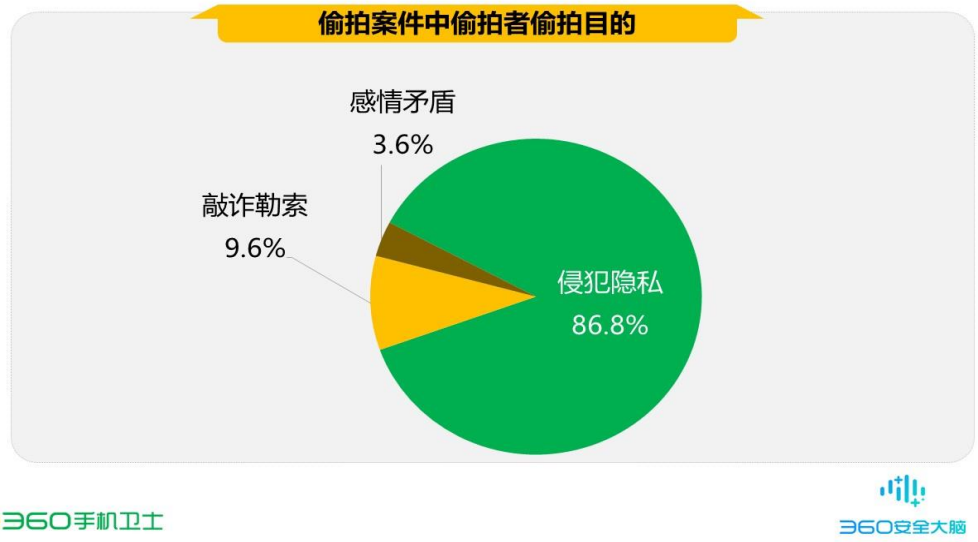



图中标记的位置,都有可能隐藏着针孔摄像头。
以下物品更需仔细检查!
1 插板插座
2 充电器
3 路由器
4 烟雾报警器
5 纸巾盒
6 钟表

五、 偷拍者身份及目的

由于偷拍具有很强的隐秘性，往往即使找出摄像头也很难发现偷拍者。在我们统计到的案例中，仅有一半左右可以发现明确的偷拍者。一般来说，公共场所偷拍者往往与该场所具有直接关系；宾馆酒店偷拍案件中，往往无法找到偷拍者；民宿租房案件中，偷拍者往往为房东或者其他合租房客；部分偷拍者系累犯惯犯。

有 86.75%的偷拍者表明其目的为偷窥他人隐私，此类案件的受害人绝大部分为女性；9.64%的偷拍者则为了利用偷拍下来的视频对受害人敲诈勒索；还有 3.61%的偷拍者是因为家庭内部矛盾对家庭其他成员进行偷拍监视。



第四章 典型骗局揭露，遇见此“坑”请绕行

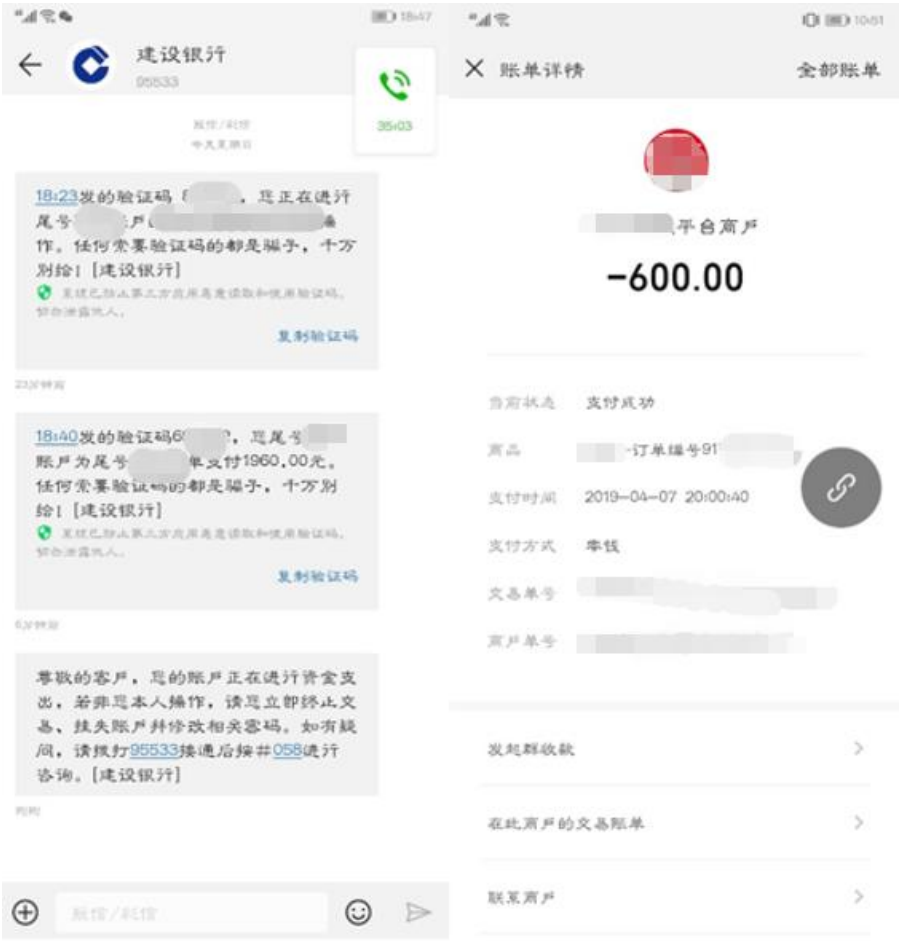
一、 宅家篇

1、冒充客服实施快递退款、购物退款诈骗

案例回顾

用户 2019 年 4 月 2 日在某电商平台购买食品。4 月 6 日收到快递后，发现商品损坏。电商平台卖家确认为快递运输原因导致商品损坏，要求用户等待快递协商电话。4 月 7 日下午 6 时左右收到了“快递电话”，对方表示为**快递，询问用户购买的蛋黄酥是否需要理赔，并以用户年龄不足，无法在支付宝退款为由，引导用户添加客服微信。退款客服索要了用户的支付宝余额截图、微信余额等截图。

用户在对方引导下使用微信扫码访问了钓鱼网站，填写了姓名，手机号，银行账号，网银登录密码等信息，并向对方提供了银行支付短信验证码。但该过程未发生资金损失。不法分子继而登录用户的京东账号，拍下 7 笔总计 6182 元的电子商品充值卡代付款订单。引导用户在网络贷款平台申贷，并将所贷资金转至微信余额，使用微信支付京东账户待付款订单。直至 4 月 7 日下午 8 时左右用户收到真实快递赔偿电话，才得知此前已经受骗。



专家解读

通过冒充快递电话，以赔偿用户快递损失为由，要求用户登录退款网页，套取用户银行信息及支付验证码，此环节用户虽提供验证码，但未实施成功。由于用户京东账号为银行账户预留手机号，京东登陆密码与网银登录密码相同，不法分子登录用户的京东账号购买虚拟商品，引导用户在贷款平台申请贷款后，支付京东平台代付订单，套取虚拟商品卡密。

防骗提示

遇到以上情况，要拨打官方客服电话进行咨询，切勿相信陌生人打来的电话或发来的短信，更不要轻易点开陌生网址。

2、冒充二手交易平台工作人员，诱导用户向指定账号转账

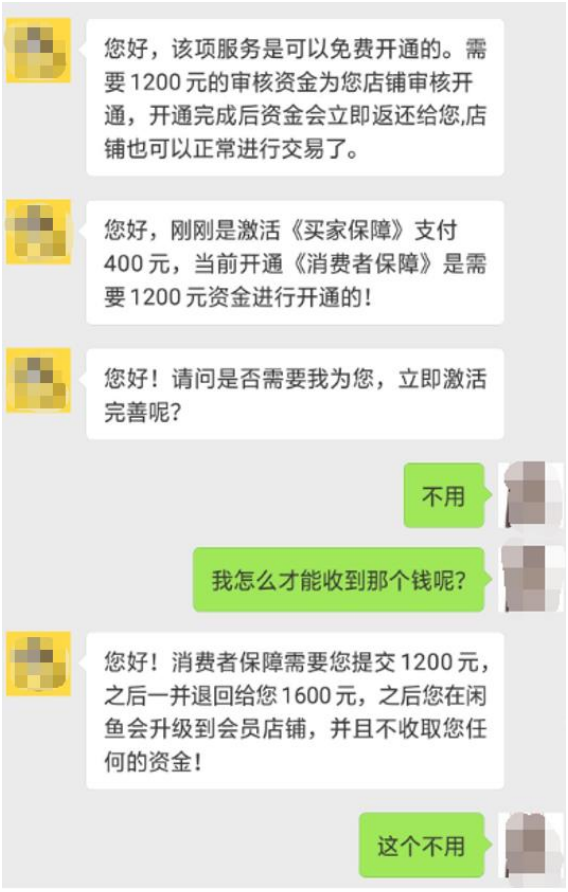
案例回顾

2018 年 10 月，叶女士将自己的化妆品放置在某二手交易平台进行出售，几日后，叶女

士收到平台信息，有“买家”咨询商品价格。对方以正在上班，不方便使用平台 APP 为由，引导叶女士添加对方的 QQ。双方通过 QQ 进行了一番商品“讨价还价”，不久后，叶女士收到了“买家”发送的购买叶女士出售商品失败的截图。

叶女士由于不了解平台的规则，添加了“买家”截图中所提及的平台官方微信公众号。该公众号的人工客服索要叶女士的平台账号后，表示叶女士的情况是由于未开通《买家保障服务》。叶女士按照“客服”提供的支付二维码扫码支付了 400 元《买家保障服务》费用。

叶女士将此情况告诉“买家”后，买家表示此时可以下单，但无法查询到订单信息。叶女士再次联系“客服”反此情况，客服表示此次是由于叶女士未购买《消费者保障》服务。



叶女士按照对方提供的二维码扫码转账时注意到支付的商品是 Q 币，询问客服该情况时，客服未回复，且发现被“买家”删除 QQ，叶女士得知受骗。

专家解读

随着生活观念的改变，越来越多人在二手平台进行商品买卖。但由于二手平台较多，平台规则不相同，用户存在对平台规则不了解的情况。不法分子为了防止平台的监管，一般会将买家或卖家引导至其他的社交工具进行沟通，如 QQ、微信等，再利用用户对平台的不了解，以商品不能支付，无法完成订单为由，引导用户联系假冒的“官方客服”。该“官方客服”以未开通消费者服务，店铺未开通授权为由，要求用户向指定的账号转账。用户转账后，发现仍不能交易，反问对方原因时会遭遇被对方删除的情况。

防骗提示

常见的二手交易平台一般都有自己的平台社交工具，平台的聊天记录可以作为纠纷审核时的材料。如遇到要求在平台外进行沟通，买卖商品的行为，该交易可能存在一定的风险。

常见的二手交易平台为了保障买卖双方的利益，买家支付的资金会暂存在交易平台，待买家确认收货后，卖家即可收到货款。不会通过直接向个人转账的方式缴纳商品费用。如遇

到买家或卖家要求通过个人账号转账，该交易可能存在一定的风险。

3、虚假网游交易平台，诱导用户向指定账号转账

案例回顾

2018 年 10 月张先生在手游中遇到想要购买自己游戏账号的玩家，双方协商账号价格后，张先生添加了对方的 QQ。对方表示为了防止交易风险，交易账号需要在正规的交易平台进行交易，张先生按照对方的引导，通过搜索引擎搜索了“网*218 城”关键词，访问了搜索引擎排名靠前的“网*218 城”网站。在“网*218 城”进行了账号注册，之后在上架游戏账号的过程中填写了游戏账号、游戏密码、游戏区号、手机号等信息。

张先生上架商品后，买家表示已支付 850 元，购买了该商品。张先生在该平台提现时，网站后台显示由于张先生提现银行账号填写错误，需要张先生联系在线客服申请解冻。张先生联系了网站内的在线客服，客服表示申请解冻需缴纳一笔解冻资金，该资金解冻后退回。张先生按照客服的要求向指定的支付宝二维码转账，解冻成功后，张先生申请提现时，系统显示张先生由于转账时资金未带零头，需张先生再次缴纳 6800.1 元解冻。张先生表示需要投诉，索要客服电话号码时被拒绝，再联系 “买家”时发现被对方删除 QQ。张先生意识到被骗。

专家解读

在诈骗前期，不法分子通过域名抢注的方式收集大量的备案域名并借此搭建钓鱼网站，再通过“SEO”的方式增加搜索引擎对此些网站关键词的收录，达到关键词在搜索引擎高排名的目的。

在诈骗实施时，不法分子利用贪便宜的心理，将商品以非常低廉的价格为幌子进行宣传。通过游戏喊麦，论坛等渠道与用户取得联系，引导用户通过搜索引擎搜索指定的关键词，访问预先解析好的钓鱼网站，购买虚假的网游账号及装备。用户购买商品后，以商品发货费，充值未带零头，提现账号填写错误需解冻为由，继续要求用户支付费用。即使用户后续支付了该些费用，对方仍不会提供用户所需商品，若用户后续未按照要求支付费用，则会被对方直接“拉黑”。

防骗提示

为了防止网站从事非法的活动，正规的网站需要进行网站信息备案。钓鱼网站普遍存在网站未备案或备案信息与内容不符的情况，可以通过查看网站备案信息确认网站真伪。

虚假网游交易平台常使用二维码和银行账号作为收款账号，且收款方名称以个人、线下餐饮、服饰、生活超市为主。正规的网游交易平台，支付方式比较严谨，一般使用第三方支付工具或银行账号代扣，收款方也与备案网站企业相同。

虚假网站以提供商品价格远低于市场价的行为来吸引用户上当，因此如果一个商品的价格非常离谱的低于市场价，一定要小心切不可因贪小便宜而吃大亏。

4、兜售色情视频的“卖片党”，原来就在你身边

5G 冲浪时代，用户沉浸网络的时间越来越长，然而，我们在通过网络获取资讯的同时，却发现一个现象，具有社交性质 APP 应用的评论区被“卖片哥”盯上了，他们以评论、关注、发私信等方式为违规网站引流，其发送的不雅内容已经成为了网络世界的“牛皮癣”。违规引流产业链，在评论区“小黄文”泛滥的背后，是一条隐秘的违规引流产业链。

通过对整个产业链的挖掘，我们发现了一条由评论推广→引流用户至涉黄网站→用户付费观看淫秽视频→网站开办者与评论推广者分成的互联网黑色产业链。

专家解读

诈骗团伙购买域名、服务器，搭建了含有虚假投诉页面的色情网站、“防洪”域名网站。通过“防洪”域名为色情网站提供域名缩短服务，躲避平台的拦截。借助评论引流，吸引用户访问色情网站。在色情网站内设置支付限制，诱导用户进行支付操作。

防骗建议

猖獗的色情网站引流团伙，通过大量养号、绕过平台规则、网站多级跳转等手段躲避平台封号和拦截，大肆传播色情等低俗内容，以出售色情资源诱导用户支付，更有甚者进行诈骗变现。为了营造清新的网络环境，我们呼吁企业用户要加强监管，不断完平台善管控机制；个人用户对于这种不法信息要及时举报，不要轻信、更不要转账。

二、 出行篇

1、入住酒店需谨慎，小心偷拍摄像头

2019 年 4 月起，中年男子陈某在福州多家酒店以居住的名义进入酒店房间，在空调管道等隐蔽处，安装多部针孔摄像头，共偷拍酒店房间入住人员达到 600 余人次，并保存隐私视频 42 段、隐私照片 109 张供自己观看。案件侦破后，鼓楼法院以非法使用窃听、窃照专用器材罪判处陈某有期徒刑七个月。

专家解读

偷拍案件的一大发生场景是宾馆与酒店，由于针孔摄像头隐蔽性太高，因此不仅小旅馆会中招，一些连锁品牌与星级酒店也成了偷拍者的温床。另外由于酒店人员流动性高，所以即使发现摄像头，也很难锁定犯罪嫌疑人、判断被偷拍影像是否已流出。所以为了防患于未然，强烈建议入住酒店宾馆时，对房间环境予以检查。

防骗提示

入住酒店之后，使用 360 手机卫士“摄像头检测”功能，，检查有无可疑摄像头。如发现可疑目标，可使用遮挡物遮住可疑的小孔，尤其应该注意正对着床位的高处。同时我们建议在保护自身安全的前提下，尽快联系酒店或报警处理。

2、公寓合租也有风险？这些地方需要仔细检查

2019 年 10 月，上海一对情侣在某品牌公寓租住的房间内，发现在正对着床的衣柜上方，藏有针孔摄像头设备一套。两人迅速将相关情况反映给警方及公寓管理方。警方介入调查后，将犯罪嫌疑人目标锁定在与两人合租的男子身上。该男子交代，自己为了满足私欲，趁着两人不在家偷偷潜入其屋内安装针孔摄像头。案件侦破后，犯罪嫌疑人已被警方依法刑事拘留。

专家解读

一二线城市年轻人定居不易，往往会以合租的形式落脚。跟陌生人合租除了会带来新鲜的社交感之外，也要小心不怀好意者。类似案例中，往往都是房东或合租室友基于偷窥隐私的目的，对女性或情侣租住的房间安放针孔摄像头。部分粗心的房客入住后，没有彻底清理或者检查房间，或者针孔摄像头隐藏太过隐蔽，容易发生被偷拍的案件。

防骗提示

入住合租房之后，要对自己房间及公共卫生间等场合进行仔细检查和清理，并使用 360 手机卫士“摄像头检测”功能，检测有无可疑摄像头。如发现异常，在保证自己安全的前提下，注意及时保存证据，报警并联系房屋管理人员进行处理。

三、 金融借贷篇

1、借助虚假网贷 APP，骗取申贷保证金

案例回顾

2018 年 6 月，尹先生接到一个自称某平台客服的电话，对方询问尹先生是否有贷款需

求，随后双方通过社交软件进行详细沟通。在 QQ 聊天中，客服向尹先生发送了贷款应用的下载链接，尹先生下载安装该 App 后，在应用内提交资料申请了贷款。审核通过后，尹先生按照客服要求支付了 600 元包装费。看到放款通知，提款时却收到了账户异常的短信，客服回复是尹先生的银行卡号错误，无法不能放贷，要求用户付款 2000 元。尹先生考虑到大平台的知名度和担保降低了防备心理，后续多次支付费用后，仍无法收到贷款，得知受骗。

专家解读

移动互联网的发展，人们与手机 APP 的互动越来越频繁，但相较于传统的钓鱼网站，手机 APP 很难像网址那样可以通过某一个特征（网址备案信息），快速鉴别真伪。因此，越来越多的虚假类应用出现在诈骗场景中。

防骗建议

网络贷款在带给我们方便的同时，也存在一些风险。在申请时，尽量选择正规平台；放款要先交费的，多数情况下是骗子；不管申请哪种贷款，都会有一定的手续和流程，什么都不要就能贷款的，就要当心了；贷款的利率多是跟市场相关，如果利率高过市场或是低过市场都是不太正常的，千万要当心了。

2、博彩刷单骗局

案例回顾

用户在 2019 年 5 月通过网络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（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

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。

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

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。

四、 网络交友篇

1、一夜之间深陷投资“陷阱”，“杀猪盘”解密

案例回顾

2019 年 6 月王先生收到微信好友的添加请求，通过该申请后，与该微信好友交谈工作情况、恋爱情况以及对爱情伴侣的要求。对方在与王先生聊天的过程中，时而会告诉王先生某天又赚了几千元钱，吸引王先生的追问。王先生追问后，顺势给王先生介绍期货平台（**港投)软件，教导王先生在期货平台购买“缅甸玉石指数” 、“东南亚红木”等项目。王先生前期在对方的指导下，获得了收益，后期购买的项目出现价格波动，加上王先生自身资金紧张，不想再投入资金。对方就以王先生“大惊小怪”为由，催促投资，王先生出于“面子”问题，增加了投入，投入的资金后期基本亏损完，得知受骗。

专家解读

不法分子，从获客，用户管理，人设制造，情感经营，套路流程，转战取财再到资金转移，“杀猪盘”团伙打造了一套非常完整的“诈骗工作体系”。先以交友为幌子，通过“撩友”的话术，让用户沉迷其中。再诱骗用户在虚假理财平台投钱。通过多变的“语言”透露自己对用户不投钱的不满。最终用户处于不投钱怕“心上人”不理自己，投钱又怕上当受骗的矛盾心理，最终即使自己没钱也要借钱投进去。

防骗提示

这些“养猪”的屠夫，其实离我们并不遥远，每一个突然找上门的“陌生人”，都有可能是骗子。网络交友千万条，绝不掏钱第一条！

2、女网友裸聊背后的“桃色陷阱”

移动互联网的发展，手机应用的普及，加上交友市场的需求旺盛，手机应用市场随处可见各类交友应用。随着“新型冠状病毒肺炎”疫情的出现，人们“被迫”留守屋内，上网交友成了众多的“宅男”消遣时光的选择，出现了众多的裸聊被勒索事件。

不法分子通过社交应用结交用户，以交友为名引导用户添加对方的 QQ。在与用户聊天的过程中，使用话术，套取用户的个人信息，如姓名、职业、年龄。以请求用户帮助其增加直播间关注度为由，引导用户下载指定的虚假“直播”软件。随后以视频裸聊为由，引导用户进行视频裸聊，裸聊过程中会特意要求用户露出脸部和下体的画面。视频结束后，给用户发送刚刚的裸聊画面截图（包含用户脸部信息）及用户手机通讯录信息截图，并以会将此视频群发给用户手机通讯录好友为由，勒索用户向对方转账。用户转账后，对方仍未满足，仍反复要求用户转账。

专家解读

不法分子引导用户安装的虚假“直播”应用，存在上传用户手机通讯录的行为。表面看起来是直播应用，但安装后是无法使用直播功能的，只是不法分子用来盗取用户手机通讯录的工具。不法分子借助一些虚拟摄像机软件及色情视频，模拟与用户的裸聊画面，在于用户视频裸聊的过程中，引导用户露出脸部及下体画面，偷录用户的裸聊画面。待获得用户手机通讯录及裸聊画面后，实施敲诈勒索。

防骗提示

自古深情留不住、唯有套路得人心。试想那些有美丽头像、动听名字的女子，为何在千万人中主动找上你，假装被你撩？还会主动提出“赤诚相见”？是因为你幽默、贴心、帅气、有钱？都不是，只是因为你好骗。