2018 年

大学生人群受骗情况分析

2019 年 9 月 19 日

目录

第一章 大学生受骗概况

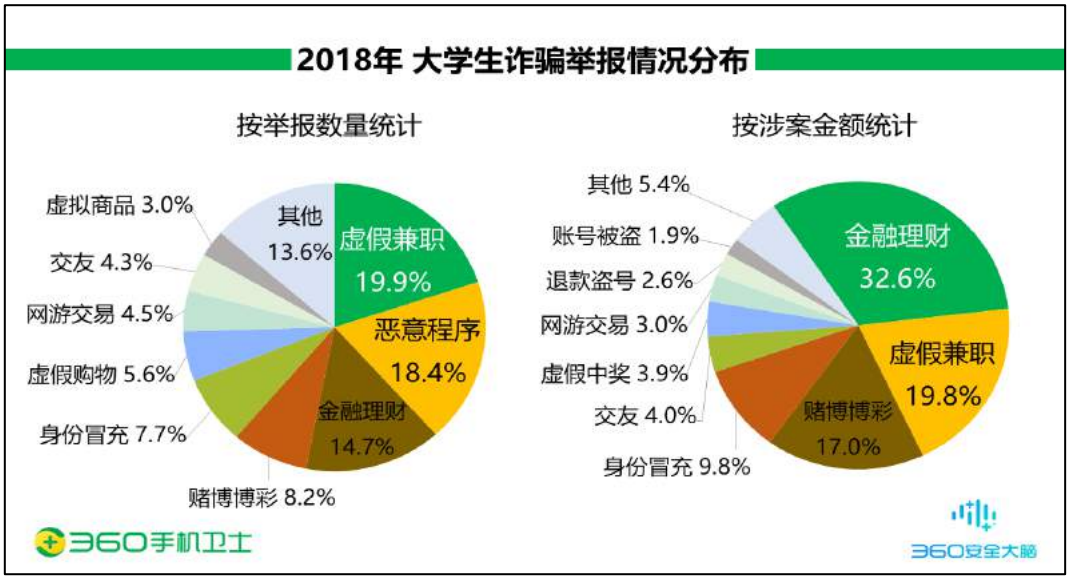
一、 大学生高发诈骗类型

2018 年全年，360 手机先赔与 360 猎网平台共接到大学生诈骗举报 1152 起。涉案总金额达 509.6 万元，人均损失 4423 元。

在所有诈骗举报中，虚假兼职占比最高，为 19.9%；其次是恶意程序（18.4%）、金融理财（14.7%）、赌博博彩（8.2%）与身份冒充（7.7%）。

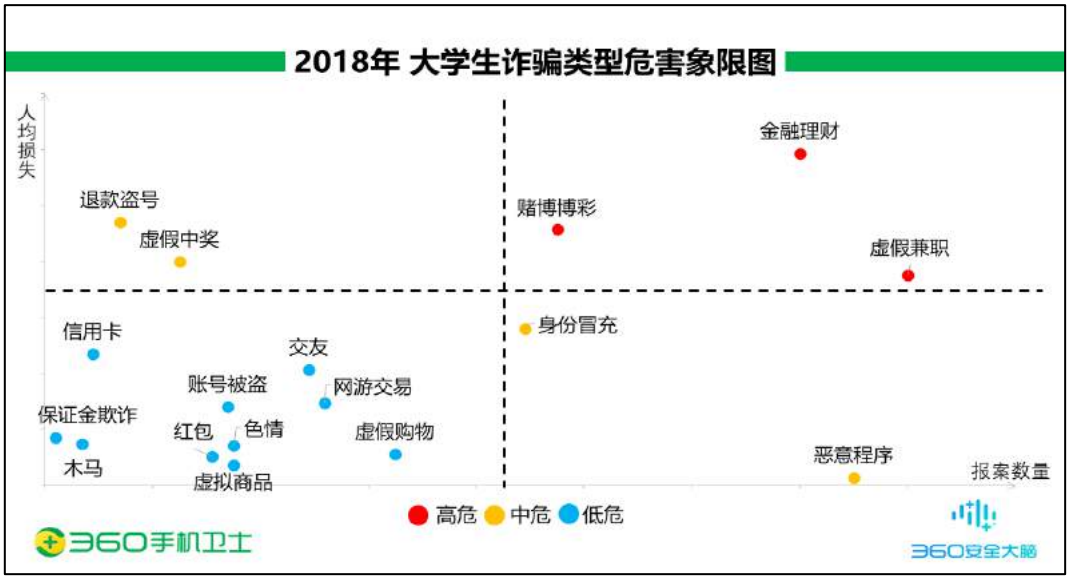
从涉案金额来看，金融理财类诈骗总金额最高，达 166.0 万元，占比 32.6%；其次是虚假兼职诈骗，涉案总金额 101.0 万元，占比 19.8%；赌博博彩诈骗排第三，涉案总金额为 86.7 万元，占比 17.0%。

下图给出了大学生诈骗类型的举报量和涉案总金额分布情况：



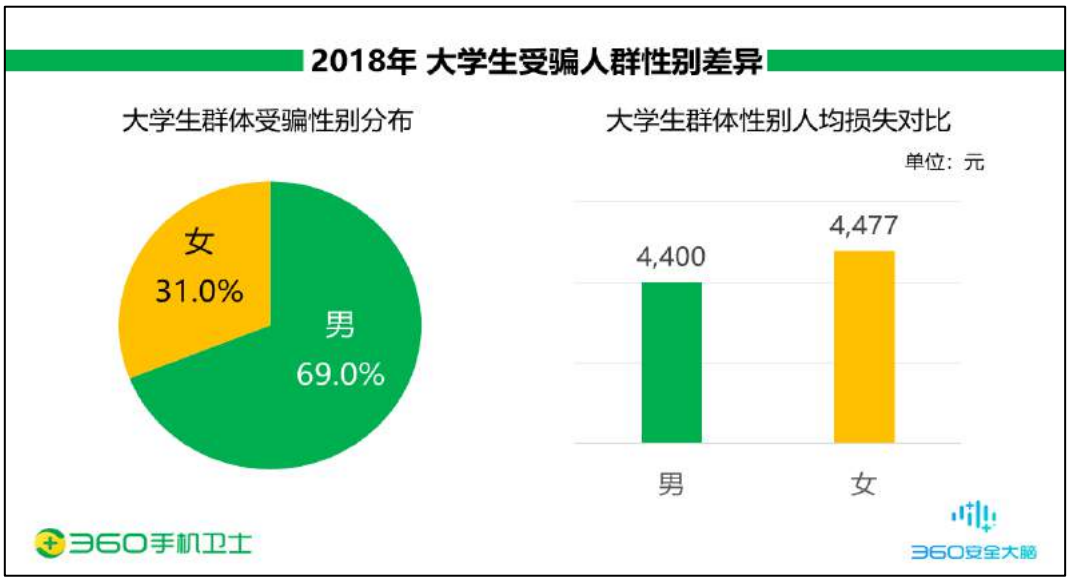
下图给出了各种诈骗类型在人均损失和举报数量的象限图。从图中可见，金融理财、赌博博彩、虚假兼职属于高危诈骗类型，受害人数较多且人均损失高。

退款盗号与虚假中奖虽受害人数少，但人均损失较高。退款盗号主要利用个人信息泄露发起定向退款诈骗，声称商品快递问题需赔付或订单问题需退款等，属于中危诈骗类型。虚假中奖多利用钓鱼网站获取用户信息，要求用户缴纳中奖保证金等，属于中危诈骗类型。



二、 大学生受害者性别与年龄

从大学生受骗人群性别差异来看，男性受害者占 69.0%，女性占 31.0%，男性受害者占比高于女性。从人均损失来看，男性为 4400 元，女性为 4477 元，女性人均损失略高于男性。



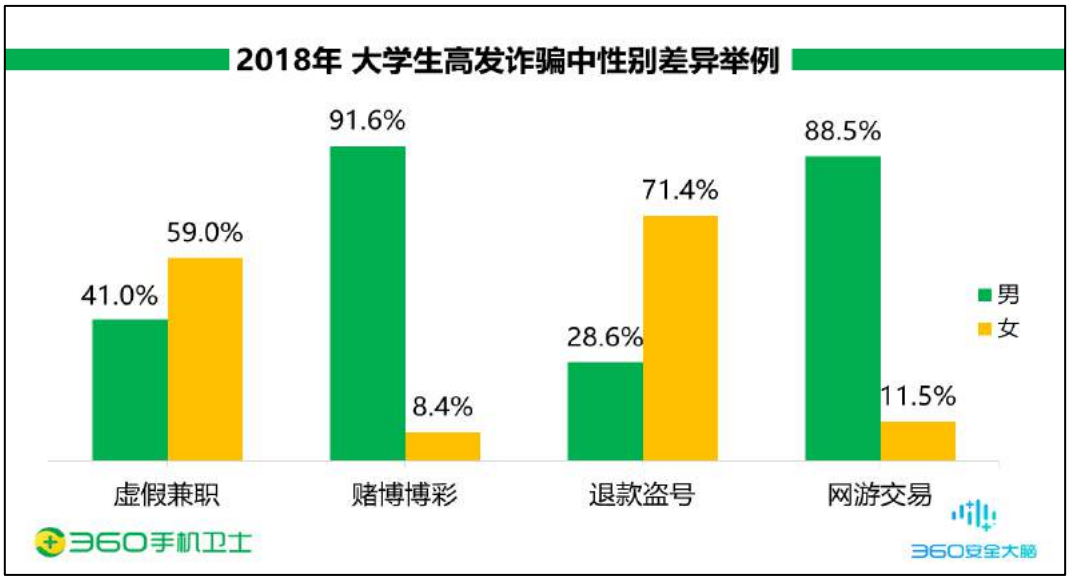
根据大学生高发诈骗中受骗人群性别对比可见，不同诈骗类型的受害人群数受性别因素影响，代表类型举例：

1） 在虚假兼职诈骗中，女性受骗人群占比高于男性，说明女大学生在网络兼职过程中的防骗意识低于男大学生。

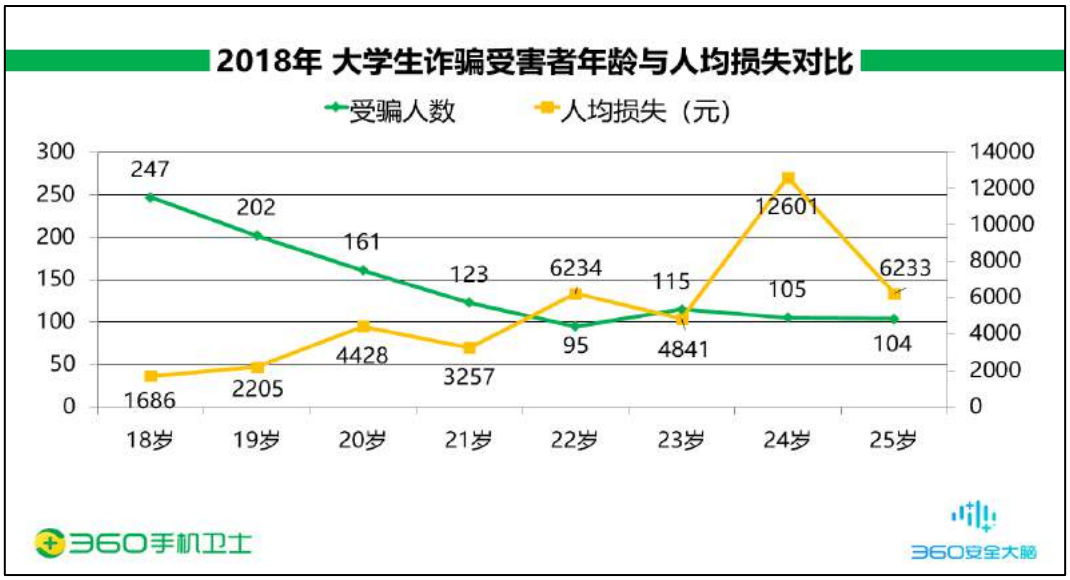
2） 在赌博博彩诈骗中，受害人几乎都为男性，说明拥有博弈娱乐心理、喜欢寻求刺激，希望通过赌博盈利的大学生以男性为主。

3） 在退款盗号诈骗中，女性受骗人群占比高于男性。由于女生比较喜爱网络购物，如果遭到信息泄露，对比男性更容易遭遇退款诈骗。

4） 在网游交易诈骗中，受害人同样是男性居多，说明大学生人群中，男游戏玩家数量远多于女游戏玩家。在看到优惠充值广告时，若不能对其真实性做出判别，极易遭遇网游交易诈骗。

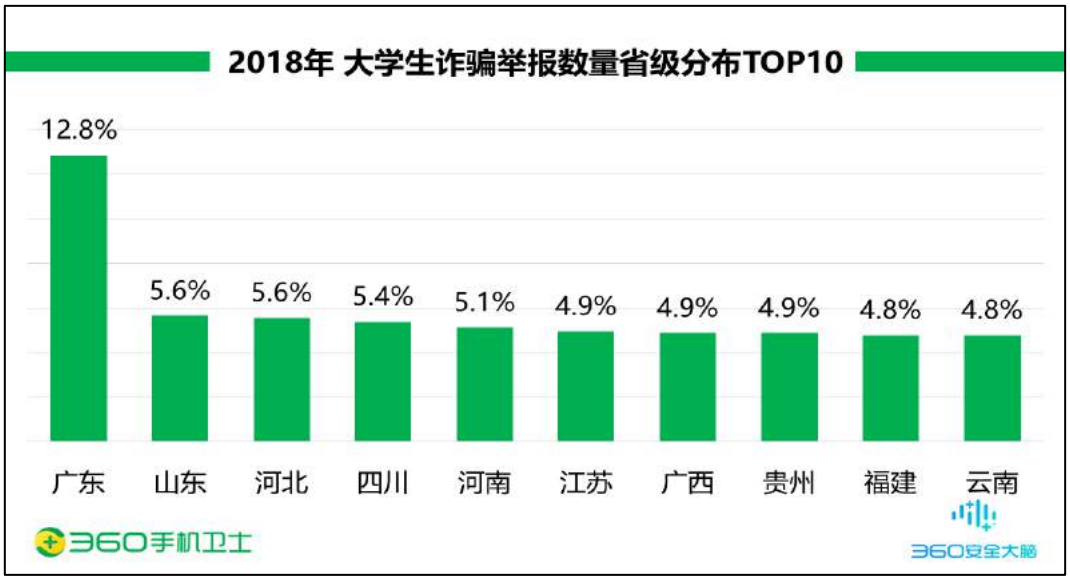


现在大学生年龄区间主要集中在 18 岁-25 岁，下图给出了大学生诈骗受害者年龄与人均损失的对比。从图中可以看出，大学生步入大学校园时大多都刚刚成年，对于外界事物真实性的判断能力不高，容易轻信他人，防范能力薄弱，诈骗举报量也较高。但在独立 2-3 年后，拥有了客观判断能力，相对不易遭到诈骗。

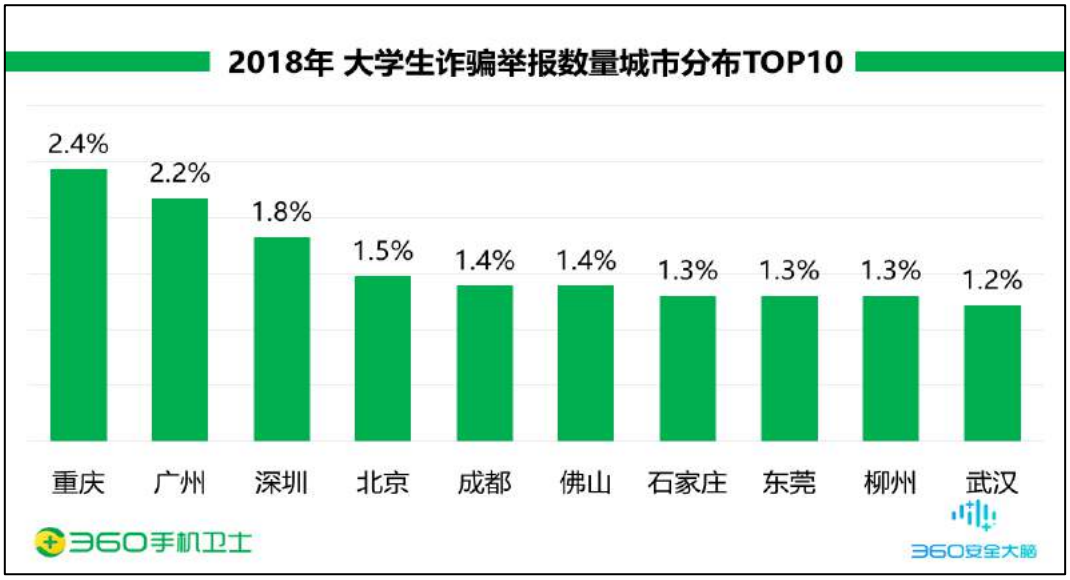


三、大学生受害者地域分布

2018 年全年，从大学生诈骗举报情况来看，广东（12.8%）、山东（5.6%）、河北（5.6%）、四川（5.4%）、河南（5.1%）这 5 个省级地区的被骗大学生最多。下图给出了 2018 年大学生诈骗举报数量最多的 10 个省份：



从各城市大学生诈骗举报情况来看，重庆（2.4%）、广州（2.2%）、深圳（1.8%）、北京（1.5%）、成都（1.4%）这 5 个城市的被骗大学生最多。下图给出了 2018 年大学生诈骗举报数量最多的 10 个城市：



第二章 大学生遭受网络诈骗的现状

互联网为人们的日常生活来了便利，对人们生活的影响也日渐深入。随着互联网的普及，青少年接触网络的机会日益增多，但互联网的开放性对青少年的影响也愈见明显。由于青少年人群尚未踏足社会，对于网络中的不良信息尚未有良好的鉴别能力，容易遭到不法分子的侵害。根据手机先赔诈骗举报，当代年轻人已成为不法分子的主要目标人群。而这其中，即将步入社会的大学生人群成为遭受网络诈骗受害重灾区。

一、大学生网赚频入“坑”

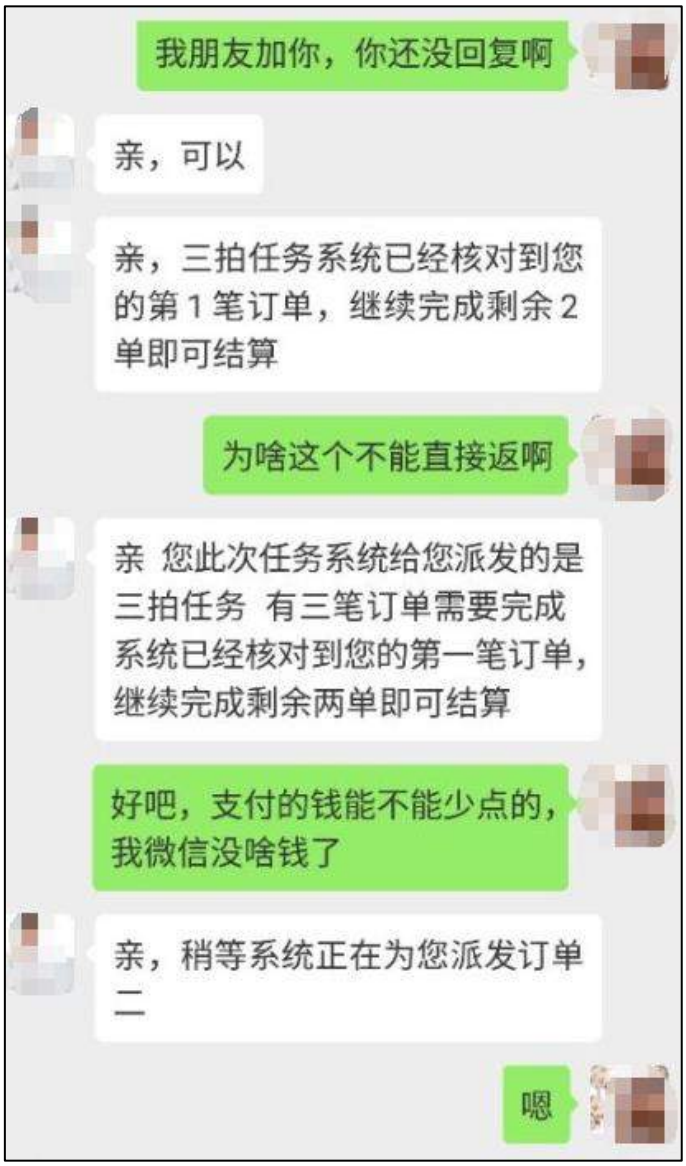
大学生人群作为即将注入社会的“新能量”，为了丰富课余生活，加强社会实践能力与沟通能力，参与兼职成为多数大学生的首选。互联网的高速发展，也为大学生提供了高效寻找兼职工作的渠道。但面对网络上各种各样的网络赚钱的宣传，很多大学生不能对其真实性进行正确判别，致使很多大学生的“网络赚钱之路”变成了“网络丢钱之路”。结合当下网络赚钱诈骗的流行趋势，大学生受骗情况分为以下典型：

1） “生命力顽强”的兼职诈骗

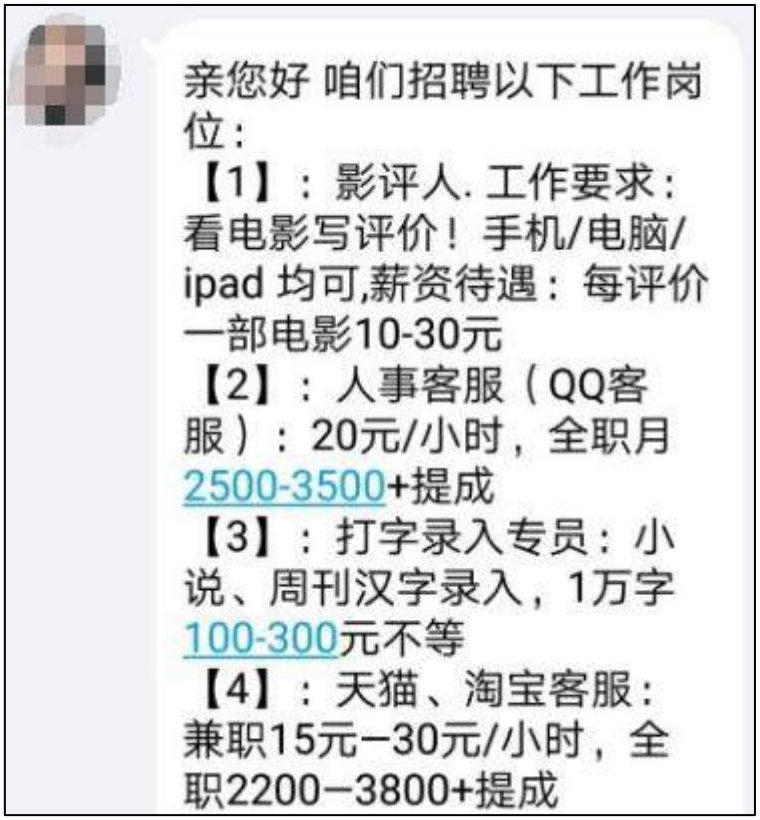
兼职诈骗是指利用虚假兼职招聘为幌子，骗取用户钱财的诈骗方式。根据历年手机先赔接到的诈骗举报量看，兼职诈骗持续处于网络诈骗举报类型首位。当下大学生遭遇兼职诈骗主要类型分为：

一是刷单诈骗。网络刷单主要模式是商家请人假扮买家，用“以假乱真”的购物方式提高店铺的排名和销量，并以“虚假好评”吸引更多的真实顾客的一种作弊形式。一般情况下，由买家提供购买费用，交易完成后，由商家返还买家本金与佣金，实现双赢。如今，网络刷单已涉嫌违法，在各相关部门的严厉打击下，得到了遏制。但诈骗分子早已盯上这一灰色产业，假借网络刷单名号，实施诈骗。

在典型的刷单诈骗中，不法分子伪装成中介平台或商家，打着刷信誉、刷销量的旗号通过社交软件等渠道发布刷单广告招聘“刷客”。同时承诺，按照任务要求拍下指定商品，待交易完成后，将返还本金与佣金。但这只是不法分子的幌子，骗钱才是最终目的。首先，不法分子会下发一到两个小额任务，结束后为兼职者返还本金和佣金，借此获取兼职者的信任。后续，不法分子逐渐提高任务数量和任务金额，利用“任务超时”、“系统卡单”等理由，引导兼职者继续投入本金，利用这种手法，反复套取兼职者的资金。



二是会员费诈骗。“招聘：文字录入员 1000 字 30-50¥ 多劳多得”这类兼职广告，在网络中随处可见，简单的兼职流程就可赚取佣金，吸引了不少兼职者参与。但在真正参与兼职前，需要向平台缴纳会员费或入职费，一般金额不超过 100 元。在不法分子的诱导下，不少兼职者轻信广告内容进行了费用缴纳，但后续遭遇的却是培训费、手机 PC 双平台兼职通道费、高级会员费、马甲费等一系列待缴纳费用。还没有赚到钱，反而有一笔甚至多笔支出。在兼职者生疑后，客服往往不予理睬，不予退款。

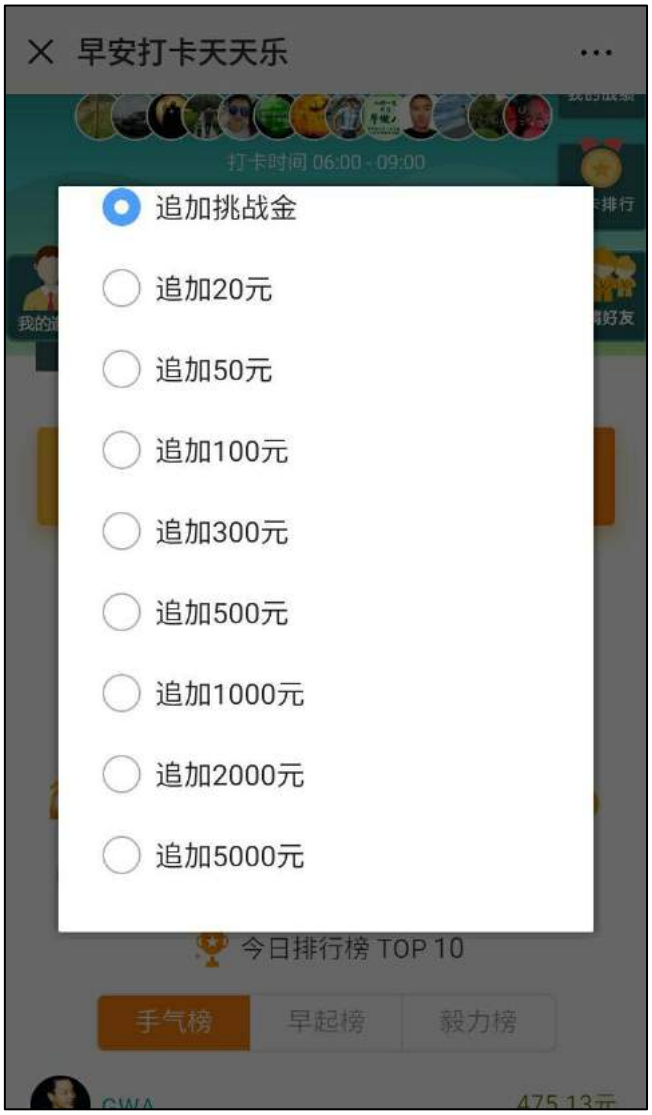


以上两种手法属于兼职诈骗中典型手法。在实施诈骗过程中，不法分子为获取兼职者的信任，通常会为兼职者展示营业执照、企业注册文件、后台系统页面等，营造自己为正规平台的假象。实际上，不法分子所展示的各种证件都是虚假的，有可能通过非法途径获取。并通过简单 PS，就可实现。

2） “起床新动力”刷爆朋友圈——打卡赚钱

每日打卡签到初期运用于各大知名公司旗下 APP，其目的在于推广产品以及提高用户活跃度，利用这一方式维系用户粘度，并取得了优异效果。但不知何时起，不少公众号创业者利用此形式实现非法敛财。

缘起自朋友圈早起打卡的潮流，大学生圈子内的流行程度更为突出，玩法简单，只要动动手指，就可以赚到零花钱。只要关注微信公众号，每日完成早起打卡任务，即可获得金额从几毛到几十块不等的红包。“早起的鸟儿有虫吃，早起的人儿有钱赚”，在这里进行了验证。参与打卡活动的平台用户，需要预付挑战金，可以自行选择挑战等级进行充值，所有挑战金全部在奖池里。每天在规定的时间内打卡，即可瓜分奖池里的奖金，金额取决于当天忘记打卡的人有多少。另一种形式则是，前期无需支付任何费用，只要每天参与打卡，即可获得红包。连续打卡，领取的红包金额可能越大。但众多参与活动的大学生却表示，刚开始确实可以拿到一些低额奖金，但在追加挑战金后，平台跑路，投入资金无法追回。



这种利用公众号、小程序搭建的平台并不可信。运营系统与规则完全由公众号运营者控制，利用用户的投资心理，在获取到一定资金后，容易产生卷款跑路行为。对于用户来说，投入资金难溯源，追回几率极低。

3） “低级智商税”——返利

返利在人们的日常购物中较为常见，促使商家提升整体销量是返利的最主要目的。方式类似于价格补贴，能够刺激人们的购买欲望，是商家提升销售业绩的常用方式。正是由于返利二字能够吸引众人眼球，导致遭到不法分子非法利用，网络上也频频爆出返利受骗的案件。

红包返利是大学生返利诈骗中的典型手法。不法分子一般在社交平台中散布红包返利游戏规则，如：你发给我 10 元红包，我返你 100 元；你发给我发 100 元红包，我返你 1000 元。这种看似低级、简单粗暴的诈骗手法，依然能够吸引众多玩家前来参与。在游戏前期，不法分子确实会根据游戏规则为玩家进行返利，但在后期要求加大玩家的投入金额。由于前期尝到了甜头，在玩家听信不法分子的说辞投入更高金额后，不法分子则卷钱跑路，不予退还玩

家的本金。

另一种返利诈骗中的典型手法为购物返利。不法分子建立购物平台，在平台内上架多种低于市场价的商品，宣称前期为了做推广、扩大品牌知名度，特别推出返利活动。诱导平台会员进行购物，商品走虚拟物流，承诺在周期结束后进行返款，同时给予付款金额 3%-5%的佣金，如果发展下线，平台承诺三倍佣金返利。这样的返利玩法通过朋友圈等社交平台广为散播，平台会员发展下线，赚取佣金。但最终发现平台先前承诺的种种福利，根本无法兑现。平台吸金到一定程度后，卷钱跑路。这种经营模式如果是真实的，其平台自身根本无法盈利，更没有资金源为平台会员发放佣金。

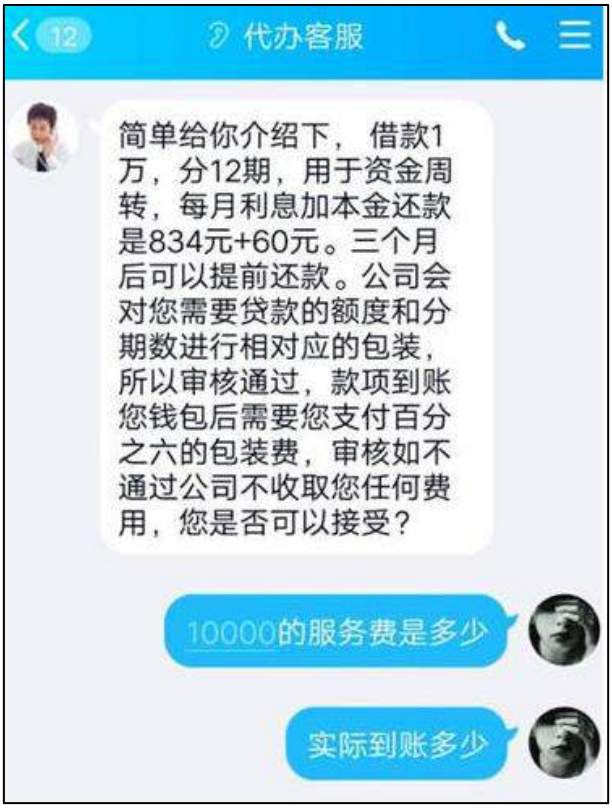
二、大学生网络贷款“套路深”

网络借贷模式引入中国以来，在国内迅速发展并形成规模，平台数量、每月成交金额及投资人数量不断增加。不同于传统借贷，网络借贷手续简便、形式灵活，已成为当下一种潮流趋势。于此同时，网络借贷中所蕴含的风险也日渐显露，近年中金融借贷诈骗已成为高发诈骗类型之一。

随着社会经济的发展，人们的消费水平相对提高，大学生人群的消费结构与习惯也产生了巨大变化。大学生人群作为一个特殊的消费群体，同时也成为网络贷款的主要需求方之一。各大网贷平台相继推出大学生专属业务，并提供了众多优惠政策。越来越多的大学生开始接触网络贷款。随之而来的，不少不法分子将大学生作为主要目标人群，实施贷款诈骗。结合当下贷款诈骗的流行趋势，大学生受骗情况分为以下典型：

1） 缴纳贷款保证金、合同费

主要通过引导借款人签订虚假贷款合同，以缴纳贷款保证金、银行流水不足为由，要求借款人向指定银行账号转账。在沟通过程中，不法分子承诺放贷额度大、审核制度较为宽松、保证可以下款等，打消借款人疑虑，从而得手。



2） 利用虚假贷款 APP

不法分子使用贷款 APP 的主要目的是为了在 APP 内生成虚假贷款额度向借款人展示，并提示借款人下款需要支付激活费用或手续费用。在借款人支付后，实际上并不能得到贷款主要诈骗点为不法分子可针对 APP 内展示内容随意修改，下款金额为“暗箱操作”，其目的为了借助虚假 APP 获取用户信任。

3） **利用虚假贷款平台**

前期借款人在平台网站内填写贷款申请并提交，在获取到借款人信息后，不法分子与借款人进行联系并告知申请通过。下款前同样要求借款人支付激活费用或手续费用，在借款人支付后并不能得到贷款。

三、 网游交易中的“钓鱼关卡”

在网络游戏的虚拟世界中，游戏玩家们可以暂时忘记自己的烦恼，借助游戏，缓解日常学习生活中的压力。大学生作为网络游戏的主要受众人群，上网玩网络游戏已占据了一大部分大学生的业余时间。网络游戏中的游戏币、游戏道具、装备等五花八门，除了付诸于时间获得外，有的游戏物品可以利用真实货币进行购买换取。随着网络游戏的发展，专门为玩家提供网游交易的平台应运而生。更多的大学生会选择在这类交易平台中买卖游戏账号、游戏物品等。

在网游世界中，时刻可看到各类游戏物品售卖广告，对比官方售卖价格，优惠力度大。很多游戏玩家轻信低价广告联系对方进行充值购买。接着，不法分子诱导玩家访问充值平台网站，并称在平台内注册后，可立即获得游戏商品。但在玩家注册充值后，不法分子将利用账号冻结、账号第一次在平台内充值需要交纳保证金等缘由，要求玩家继续向账号内充值解

冻，并承诺后续可提现，但在玩家完成充值想要提现时，不法分子则又以提现账户填写错误等理由要求继续充值，在用户察觉被诈骗时，充值的资金已无法追回并发现游戏平台实际属于钓鱼网站。

另外有不少游戏玩家售卖自己的游戏账号，通过卖账号获得一笔“外快”，属于通过游戏赚钱的一种好方法。一般情况下，玩家会借助第三方网游交易平台寻找买家。很多初次售卖游戏账号的玩家，由于不太了解交易平台规则，容易遭遇不法分子的“双簧”诈骗。不法分子分别冒充买家与平台客服，诱导玩家脱离交易平台，以买家支付订单完成、但玩家账户提现出现问题为理由，要求用户支付解冻金，通常在用户转账支付解冻金后，买家与客服双双消失。在玩家与交易平台核实后，订单并没有被支付，遇上的买家与客服都是骗子。

四、“买买买”的雷区

电商平台的崛起改变了当代人的购物方式，方便快捷成为网络购物的标签，更多的人选择在网上购买自己所需的商品。在这其中，大学生人群作为一个特殊群体，几乎所有人都有网络购物的经验，并且对于网络购物的需求更大。足不出户，也可购买想要的商品。“物美价廉”的商品更能吸引大学生的眼球，从而激发购买欲望。利用大学生这一特点，不法分子利用低价诱惑大学生进行消费。

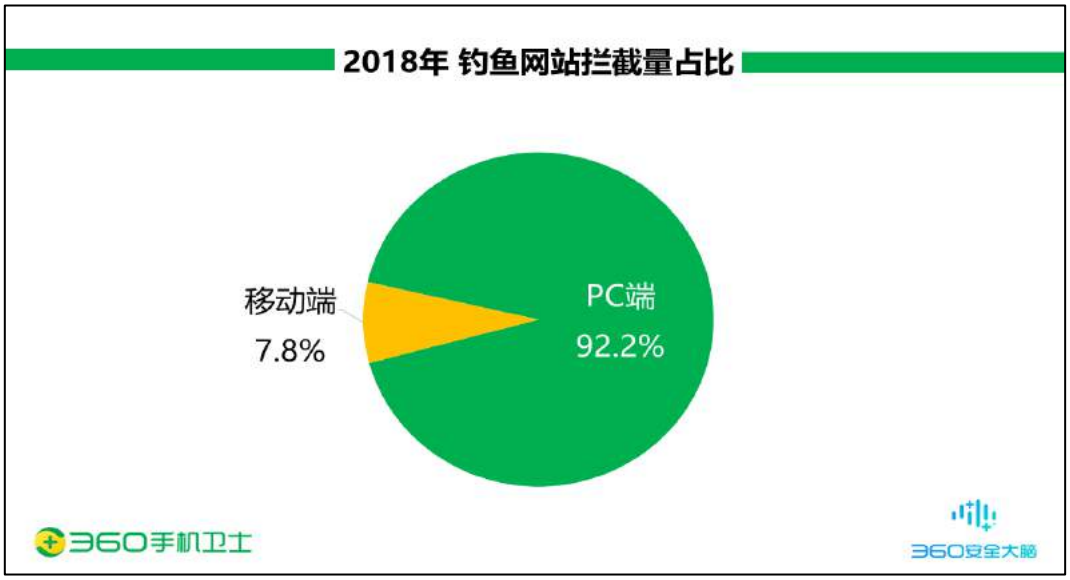
付款不发货是网购诈骗的主要类型之一。不法分子一般通过社交平台进行宣传，低价售卖商品，如：数码产品、球鞋、化妆品等。在进行诈骗前期，不法分子首先进行“包装”，在朋友圈内发布各种商品图、收款图或低价活动，伪造商品物美价廉、广受好评、销量突出的假象，诱导买家付款购买。在买家付款后则遭到删除好友的情况居多。

利用钓鱼网址属于网购诈骗的常见手法。不法分子建立虚假购物商城，通过发送虚假购物短信、社交平台发布虚假广告的形式吸引买家，商城页面模仿热门电商平台，购买过程流程化，买家通过页面无法辨别商城真实性。在买家付款后找不到任何订单查询入口，也未能收到商品时才会察觉被骗。

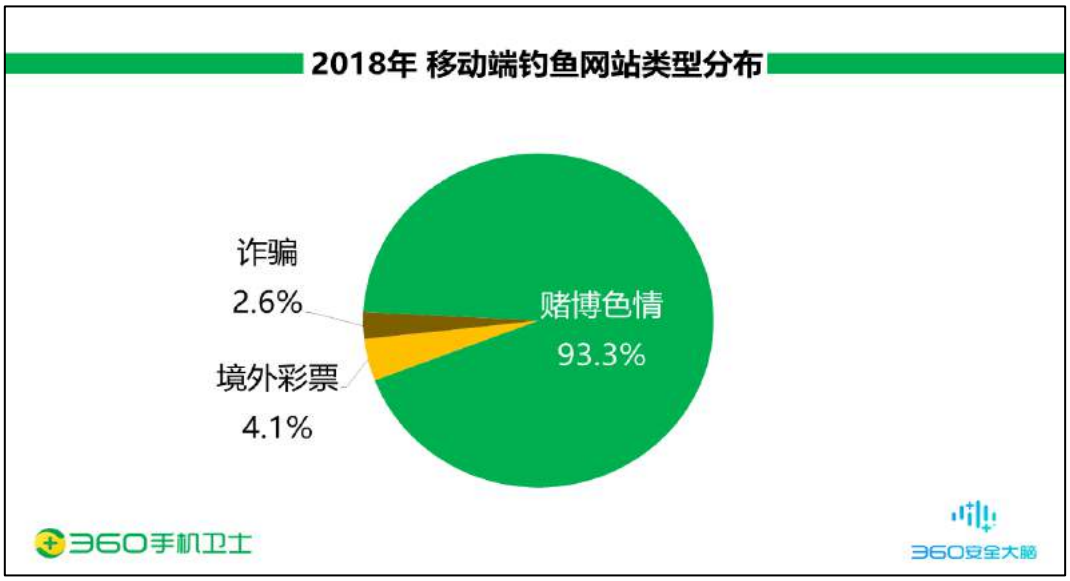
第三章 大学生高发诈骗的传播形式

一、利用钓鱼网站

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。2018 全年，360 安全软件的 PC 端与移动端共为全国用户拦截钓鱼网站攻击约 369.3 亿次。其中，移动端拦截量约为 28.8 亿次，占总拦截量的 7.8%，平均每日约拦截 787.4 万次。



移动端钓鱼网站拦截类型中，赌博色情网站比重最高，为 93.3%。其他包括境外彩票（4.1%）与诈骗（2.6%）。具体分布如下图所示：



在网络诈骗中，钓鱼网站往往会模仿正规网站网站，以假乱真；或者干脆“黑掉”正规网站，取而代之。从大学生遭受网络诈骗的过程上看，钓鱼网站扮演着不可或缺的角色：

1） 拍卡商城、任务平台真假难辨

在兼职诈骗实施中，钓鱼网站的应用一直属于行业内的典型手法。网站内布局及展示内容模仿当下正规电商平台或交易平台，结合流程式的兼职引导，打消用户疑虑，起到迷惑用户的效果，让用户误以为访问的是正规兼职平台。网站备案信息通常为皮包公司认证，多数情况下的网站备案与平台运营内容无直接联系，或使用非法手段篡改正规网站的页面内容，实现非法内容的展现。通常不法分子所运用的拍卡商城，一般为引导用户购买点卡、话费充值卡等商品，并生成支付连接要求用户支付，而收款方、资金流向等信息用户无从查询，导致无法追回。

而任务平台的运用，有效提升了用户兼职的参与力度。用户可根据佣金金额自选任务，平台注册、APP 推广、游戏代玩等，但任务平台自身的真实性用户无法进行核实，平台内宣传的各种兼职任务的安全性也有待考究，很容易遭到信息泄露及诈骗。

2） 购物钓鱼、网游钓鱼层出不穷

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”。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”。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。但其具有的危害性，仍不可小觑。不法分子开始“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，发送给用户钓鱼链接并要求支付。用户访问后发现页面与真实平台极为相似，无法在第一时间发现问题所在。一般在支付成功后，发现收款方不是二手交易平台后才会察觉被骗。

大学生除了购物需求，游戏充值也属于日常消费需求之一。热门网游产品遭到钓鱼网站争相模仿。除了页面信息相像外，在首页底部增加了表达绿色安全的标志，并有其他正规平台的 logo 标志，传达给用户此平台安全系数高、并与多家平台合作的假象。观察平台网站的备案信息，大多钓鱼网站无相关备案、或备案企业信息与页面显示内容不一致。并且不法分子实施诈骗基本通过社交平台，平台网站中的客服一般无法取得联系。

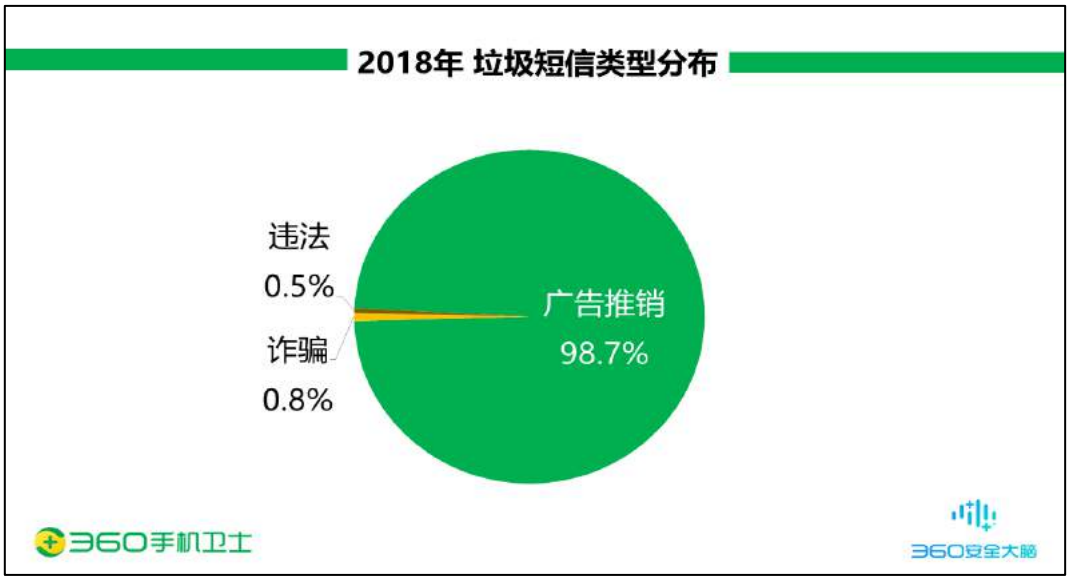
3） “盗号”钓鱼连年猖獗，日常购物不例外

“盗号”类型的钓鱼网站主要通过“模仿登陆”的形式，主要采用模仿正规网站域名的方式诈骗。日常生活中，用户使用手机访问网站时，一般不能看到完整的网站内容，只能看到域名前缀，用户不易查看网站信息，不去主动查看也属于当下手机端用户的使用习惯。这种情况下，一旦用户中招，就会被盗走相关账户密码，引发财产损失。

以上盗号形式被不法分子利用运用于购物退款诈骗。根据手机先赔用户举报，有大量退款诈骗会利用“假支付宝”等电商平台行骗，不法分子首先会联系用户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”。在用户录入自己的账户密码后，不法分子同步获取账户密码后，进行支付宝账户登陆或订单的支付，在用户收到验证码后进行录入，不法分子将利用此验证码进行盗刷。

二、 利用短信平台

随着社交方式的转变，短信内容也由日常交流、沟通信息转变为各类广告、金融理财等信息。2018 年全年，360 手机卫士共为全国用户拦截各类垃圾短信约 84.0 亿条，较 2017 年（98.5 亿条）同比下降了 14.7%，平均每天拦截垃圾短信约 2301.4 万条。其中广告推销最多，占比为 98.7%，诈骗短信占比 0.8%，违法短信占比 0.5%。



1） 1065/1069 号段成为诈骗传播主流渠道

1065 号段主要是运营商自营业务号段，1069 是三网合一的企业实名制通道。相较于个人号码的短信，这两个号段的号码整齐、格式统一，发送成本低。因此各大型购物、社交平台也会经常申请通过该号段发送各种平台促销或者招聘、金融广告等内容。于是，越来越多的诈骗类内容也会趁机通过该短信通道进行传播。

由于公众对 1065 和 1069 号段的官方代言的认可行性变强，但如果用户不熟悉各号段的具体运营情况，就很容易误以为这些垃圾短信都是正规渠道发送的内容。这类号段各级代理业务比较多，一些中间代理商为求暴利，对申请者资质和短信内容的审核流程不规范，审核内容不严格。这都为不法分子传播违法、诈骗信息提供了可乘之机。

此外，运营商对个人号码、虚拟号段（170/171）和 400/800 等其他号段管控比较严格，同时警方在这两年对电信诈骗的打击力度非常大，因而通过传统号段源发送违法、诈骗信息的成本日益加大，常见诈骗手段也易被识破，所以灰、黑色产业也相继转换了信息发送方式。

2） 兼职、借贷、博彩成为短信传播主要类型

网络兼职主要通过短信发布兼职广告与兼职联系方式。短信内容中包含诱导性文字，并利用高薪吸引用户上钩，并附有联系方式，通常为社交平台账号。在用户添加好友进行兼职时，不法分子则利用网络刷单、缴纳兼职保证金等缘由诱导用户支付，最终导致用户损失。

金融借贷主要通过短信寻找借款人。收到短信的人确实有借款目标时，则会轻信短信内容进行下一步借贷操作。一般借贷短信内容中包含借贷网站或借贷方的联系方式，用户可通过访问借贷网站填写自己的个人信息与借款需求，不法分子将通过用户提供的联系方式致电用户或通过社交平台添加用户好友，实施下一步诈骗。而短信中包含借贷方联系方式的，则是不法分子利用社交平台与用户沟通，直接实施诈骗。以上两种方式，联系用户后以缴纳保证金等方式引导用户转账或支付，用户若予以信任，则会遭到损失。

赌博博彩主要通过短信寻找有赌博需求的用户。短信主要宣传六合彩、赌博游戏、赌博网站等，吸引用户进行赌博。短信内容中包含赌博网站或客服联系方式。用户在访问赌博网站后充值可进行赌博游戏，但不法分子通常会设置赌博规则、赔率等逻辑，前期让用户赢得游戏，让其尝到一点甜头，在用户加大赌资后，则会“幕后操作”致使用户全盘皆输。而短信中包含客服联系方式的，利用社交平台与用户进行沟通，同样会引导用户至赌博网站内进行游戏，但会在社交平台内指导用户，主动为用户账号内充值小金额，供用户“试水”。另外告知用户每期押金或者购买点数，在用户获得利润后，不法分子将诱导用户自行充值进行游戏，但在用户充值后，会很快输掉赌资。这时，不法分子将利用各种借口诱导用户向网站内充值更多的金额。

三、社交平台成为诈骗的重要平台

当下各类违法、诈骗类信息的发布均在不同程度上借助了社交平台，主要手法的实施同样在社交平台中进行：

1） 短信渠道传播，引导至社交平台进行诈骗

通过各种渠道收集用户的联系方式，借助短信通道散布消息，采用群发的方式寻找诈骗目标。面对“主动上门”的用户，不法分子告知用户自己可提供的主要服务内容或项目。在社交平台内的进一步沟通，探知用户的需求，发送诈骗话术、传送涉及诈骗的工具也较为方便，如：钓鱼网站、虚假合同、虚假文档、恶意程序等。如果用户对服务内容存在潜在意愿，那么离不法分子的圈套也就更近了。

2） 诱导用户在社交平台内转发，实现广泛传播

社交平台中建立账号作为“客服”，是不法分子行业中的通用手法，除了实现诈骗目的，挖掘下一个诈骗目标同样为不法分子的目的之一。观察社交平台中的各个交流群，时不时会出现发送各类广告的群友，如：招聘兼职打字员，日入 100-200；办理无抵押贷款，5 分钟下款等。实际上，这些群友并不是发送广告的需求方，但在无形中帮助不法分子散播了非法广告内容。在实施诈骗的过程中，一部分不法分子将转发广告作为硬性指标，而用户为了达成自己的目的，则会听信不法分子的说辞，将非法广告散布至自己的朋友圈、社交群或者是好友，如果在此期间，有人轻信广告内容主动联系“客服”，则将成为不法分子的下一个诈骗目标。

第四章 大学生高发诈骗深度剖析

一、虚假兼职

在大学生网络诈骗举报中，虚假兼职类型位于举报量首位。近年来，通过网络媒体的曝光，其常见手法已被人们熟知。但随着网络的飞速发展，不法分子也在不断学习“新技能”，带来了更多风险隐患。针对这一发展现状，进行以下专项分析：

1） 兼职诈骗行业敛财“新趋势”

早期较为典型的兼职诈骗手法是设立虚假点卡商城、购物商城等性质的钓鱼网站，诱导用户在网站内拍下商品并直接付款购买，反复操作实现“刷单兼职”。这类钓鱼网站陈列商品虽为虚假信息，但在支付时链接中嵌套真实支付链，用户可跳转网上银行或其他支付工具进行订单支付。但随着针对这类钓鱼网站的打击力度加大，虚假兼职诈骗行业内钓鱼网站利用率下降，诈骗成功率随之降低。于是，不法分子跟紧时代潮流，“二维码支付”成为兼职诈骗行业中新晋敛财手法。

由于二维码人眼识别难度大、制作门槛低的特点，极易被不法分子利用。不同于钓鱼网站内进行支付，二维码支付拥有低成本、更加快捷获取赃款的特点。大部分大学生在遭遇诈骗期间，对于不法分子提供的支付类二维码并没有持怀疑态度，并给予不法分子极大信任，在毫不质疑的情况下进行支付，最终导致损失惨重。

2） 二维码支付结合第三方正规平台，实现“高效率”诈骗

根据手机先赔诈骗举报，在正规第三方平台内生成订单，将支付二维码发送给用户进行代付款属于当下行业内的惯用手法。通过该支付方式，用户在支付时虽然可看到购买物品及价格，但在支付完成后，用户方只有订单付款信息，无法获知第三方平台内订单获益人信息，追回钱款困难。

3） 兼职诈骗中转账支付依然高发

除了利用第三方平台支付二维码，不法分子同时会引导用户直接转账。常见形式包括：银行卡转账、社交平台红包或转账、社交群收款等。这种形式更为简单直接，在不法分子的要求下，依然有大学生轻信陌生人指示，将钱款转入陌生账户。

4） 虚假兼职行业典型运营模式

宏观虚假兼职诈骗行业的发展，实质接近“传销式”的运作模式。其组织内部分工明确，运用各项技术手段等，已形成完整的诈骗产业链。网络上铺天盖地的兼职广告，均由组织内部专人发布，其主要目的为了招揽更多的人参与兼职。整个传播组织构架成“金字塔”状，以招揽人头数、缴纳会员费金额为标准计算报酬。招揽的人越多、缴纳的会员费越高，则报酬越高。并且，上一级人员的报酬与下一级人员的传播业绩挂钩。而我们常见的朋友圈兼职广告、群发兼职广告，则由已被吸引参加兼职的人员发布。这部分人员处于金字塔底层，目的主要为了通过发广告完成上级发布的兼职任务，从而获得佣金。

5） 虚假兼职诈骗打击难点

网络中第三方平台内存在的流程漏洞容易被不法分子利用实施诈骗行为，再加上个别平台只注重自身利益，对网络系统或漏洞未能及时改进处理，更是给不法分子进行诈骗提供了有利条件。根据手机先赔诈骗举报，用户被骗时在第三方平台支付的订单，话费充值卡、游戏点卡等充值类订单较多，这类商品一般需要通过订单卡密实现充值动作，不法分子正是利用订单卡密实现非法敛财。在不法分子的黑色产业链中，有一些非法平台专门进行“销赃勾当”，其面对的客户就是这些通过诈骗得手的不法分子。不法分子可以通过非法“寄售平台”售卖卡密实现资金回流，而非法平台在其中抽成，形成完整的利益产业链。

不法分子在实现诈骗的过程中，必定有需要个人身份验证的环节。包括第三方平台账号的身份验证、社交平台中流转资金必要的身份验证、敛财银行账户开户等。如果使用自己的真实信息，则会增加暴露身份的风险。一般情况下，不法分子在诈骗期间所使用的所有账户信息，都可以通过网络进行非法获取。

通过以上分析可见，虚假兼职诈骗并不属于低端诈骗，而是存在一条流程完整并且专业运作的黑色产业链条，具有一定的社会危害性。由于诈骗资金流向无法快速找到，并且无法精准定位到不法分子真实身份，在警方处理案件过程中，无疑增加了侦破难度。

6） 大学生为何容易遭遇兼职诈骗

在大学生群体的课余生活中，兼职属于重要组成部分。对于兼职，大学生对行业的大环境认识不够深刻。寻找兼职的过程中，由于大学生自身没有社会人脉积累，只能通过互联网投递简历，并且急于求成，渴望高薪，容易遭到网络不良信息的蒙蔽。

二、 金融借贷

如今，金融借贷行业内，小额借贷平台如雨后春笋。其主要面对的借款人群集中在 20-40 岁，大学生贷款已成为校园中最常见的现象。不少大学生经常因冲动产生的消费欲望而贷款，但这类人群本身还款能力弱，资金来源主要依靠父母。在借贷过程中，对行业内规则认识不清，容易遭遇“校园贷”、“套路贷”，其危害性不低于贷款诈骗。

1） “套路贷”主要运营模式

网络贷款的大肆兴起，使得网贷平台数量直线增长，行业间网贷机构间的竞争也异常激烈。在网络贷款的流行趋势下，大量资质参差不齐的平台都想前来分一杯羹，纷纷降低网贷门槛，最终发展至通过个人身份证信息即可进行信用贷款。这样的运营趋势下，催生了“套路贷”这一贷款模式。

套路贷一般以小额借贷公司、借贷平台等名义对外宣传，并承诺无抵押快速贷款，诱导借款人进行贷款申请。多以贷款手续费、包装费、砍头息等形式，先扣除贷款本金的一部分，并限制还款时间。若超过还款期限，则需要在归还本金的基础上，增加高额滞纳金，按天计息。借款人无能力还款时，将进行通讯录轰炸、威胁恐吓等非法行径。

2） 高校内“校园贷”泛滥

“校园贷”实际属于套路贷中的一种。在众多网贷平台中，不少平台将主要目标锁定至大学校园。网贷平台的低门槛恰好为有资金需求的大学生创造了良好借贷条件，众多大学生

只需要依靠身份证、学生证就可以获得贷款。大学生虽然接受高等教育，但未涉足社会的他们，思想还不够成熟，对于社会上的方方面面缺乏理性判断，这是部分大学生深陷“校园贷”的原因之一。

分析大学生贷款的目的，总结起来大多是为了满足自己的虚荣心与攀比心。由于大多数大学生的经济来源主要依靠父母，生活费用有限，在面对一些昂贵的数码产品、奢侈品等，大学生并没有足够能力承担，但又无法控制自己的购买欲望。于是在虚荣心作祟下，多数大学生想到利用网贷平台分期购买自己想要的物品，想利用今后的生活费进行分期还款。但是，大部分大学生在借款前并没有熟悉平台的借款规则，对于借贷行业发展概况也并不了解，很容易掉入当下一些金融贷款陷阱中。

3） 大学生贷款的“黑暗面”

大学生一面享受网络贷款带来的消费快感，一面需要面对“校园贷”的高额利息。大学生一旦陷入贷款陷阱，很难“安全上岸”。面对“利滚利”的还款账单，众多大学生无力偿还，只能“借贷养贷”，依靠寻找新平台借款后进行还款。如此恶性循环发展，不少大学生在短时间内背上了巨额债务。甚至有一些非法网贷平台怂恿大学生通过裸照进行“裸贷”，在金钱的诱惑下，不少大学生通过裸贷获得了贷款，但在最终无法偿还贷款时才意识到问题的严重性。如果大学生贷款产生逾期，非法网贷平台进行非法威胁恐吓，并向学生家长追讨，实现非法获取暴利，危害家庭的和谐发展。

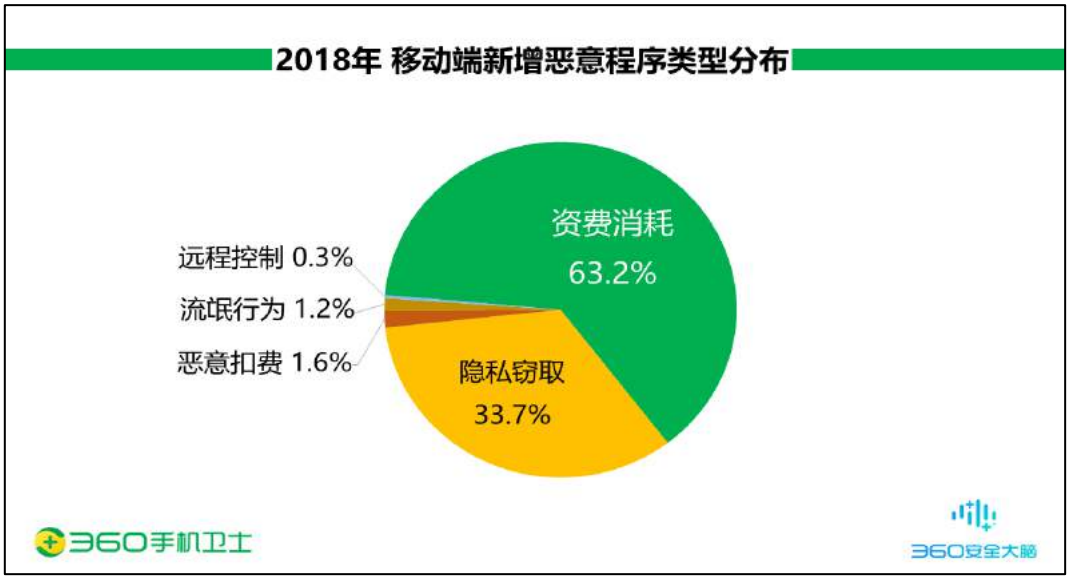
三、 恶意程序

移动设备的普及，影响着人们日常生活中的方方面面。人们利用手机刷公交、交水电费，利用手机上的第三方支付平台进行网络购物、线下付款、转账交易。手机已成为人们生活中不可或缺的一部分，大量个人敏感信息都保存在手机内。对于人们来说，手机更像是身份证和钱包。在人们享受移动便利的同时，移动安全也一直受人们所关注。一个小小的二维码、一个链接就可以实现账户盗刷、信息窃取，而恶意软件作为不法分子的主要犯罪工具，时时刻刻威胁着我们的信息安全以及财产安全。

1） 恶意程序发展现状

根据手机先赔诈骗举报，恶意程序诈骗在大学生诈骗类型中属于中危诈骗类型，虽人均损失金额少，但受骗人数众多。据统计，大学生人群一般通过社交平台内下载程序或在不明网站内下载程序的情况居多，对于手机隐私安全的保护意识并不强，对恶意程序的鉴别能力也较为薄弱。

自 2015 年起至今，恶意程序新增量与拦截量呈逐年递减趋势。新增样本类型主要为资费消耗，在恶意程序样本数量中，同时占据最大比例。说明移动端恶意程序依然是以推销广告、消耗流量等手段，增加手机用户的流量资费等谋取不法商家的经济利益。近年来，随着打击力度的加大，安全软件能力的提高，再加上人们的安全防范意识提升，恶意程序发展逐渐放缓。



2） 恶意程序高发具备特点

一是传播渠道广：在用户使用网络过程中，往往需要安装各种各样的应用程序满足日常办公、娱乐所需，但随着智能手机的普及，手机上的各种应用令人眼花缭乱。各大应用市场、网页浏览、社交平台，是用户日常安装应用程序的主要渠道。由于 APP 开发相对简单，其安全质量有待考究。并且普通用户对于应用程序无专业知识基础，下载程序时只是通过程序名判断是否是自己所需，但程序的安全性初期无法进行判断，容易下载到非法恶意程序。

二是应用程序权限获取：应用程序安装成功后都会向用户发送各项权限申请，很多用户的使用习惯是直接全部同意。这一习惯有可能导致敏感信息泄露。如果安装了一款恶意程序，被授予读取短信、读取通讯录等权限后，可实现在用户手机后台进行非法运行。窃取用户个人身份信息后，再通过拦截用户手机短信验证码，可实现盗刷用户账户资金等，并具有隐蔽性，不易被用户所察觉。

例如近几年移动端数量激增的赚钱平台。足不出户，通过手机就可以在网络获利，这一赚钱模式的新兴，汇集了大量用户。各大平台建立推广渠道，通过现金奖励吸引用户，引导用户观看视频、玩游戏、收看广告、阅读资讯等，为各大广告商带来可观流量，而用户可获得一定的佣金。再加上“收徒奖励”的机制，为平台不断进行拉新。用户覆盖范围十分广泛，甚至涉及各个一二线城市。正是由于赚钱平台数量庞大，其中不乏一些不合规平台鱼目混珠。平台内广告商来源无法确认，完成下载任务时，将在赚钱 APP 界面直接进行下载，并向用户获取下载 APP 的相关权限，并不是引导通过应用商店下载，APP 安全性无法确认。

3） 大学生人群成为受恶意程序侵害的主要人群

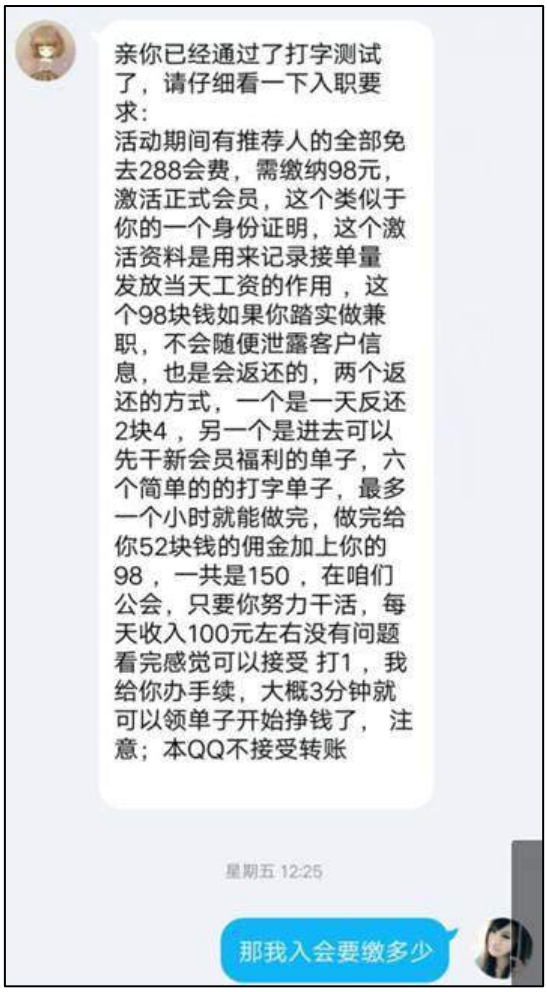
大学生作为时代新力量，同时是使用网络的主力人群，但对于网络上的不良信息，不能进行精准判别。根据手机先赔诈骗举报，大学生所下载的恶意程序类型中，游戏类、外挂辅助类、应用工具类居多，下载渠道多通过社交平台下载或访问陌生下载。

第五章 大学生高发诈骗案例举例

一、 兼职会员费诈骗

小李是某高校的大一学生，偶然间在 QQ 群内看到一则兼职招聘广告，称可以日赚 80-100 元，无门槛入职。小李觉得，如果可以在空闲时间丰富自己的课余生活并且还能赚取零用钱，的确是一个好方法。于是，主动添加了广告中客服 QQ，了解兼职详情。

添加好友后，客服要求小李先通过链接查看兼职视频学习基本工作流程，然后将视频中指定录入内容（兼职宣传文案）转发至 25 个群，流程结束后才算初审通过。于是，小李在客服的要求下完成了转发。接着，客服向小李介绍快递单录入和网络小说图片录入的工作流程，并要求小李先进行打字录入的准确度测试，结束后提供截图。在小李通过测试后，客服声称兼职需要交纳 98 元成为正式会员，后期正式入职时可返还。小李心想，已经通过这么繁琐的入职环节，交纳会员费也还合理。于是，在客服的引导下，加入了指定的微信群，小李通过向群里发红包的形式，交纳了 98 元会员费。



后续小李收到了任务选择链接（实际是一篇博客文章），自行选择兼职任务。成功选择

任务后，客服要求小李缴纳 128 元升级高级会员，承诺五分钟内可返款 288 元，返现完成后电脑手机均可实现接单，做任务更加便捷。小李虽觉得再次缴纳会员费不合理，但还是选择相信。于是，继续在微信群中发送红包 128 元，用于缴纳高级会员费。

最后，小李正式进入任务环节，在客服引导下，小李在多个 APP 内进行注册、绑定银行账户信息、绑定个人身份证信息等操作。可是在最终返还佣金环节，客服称小李没有按时完成全部任务，拒绝支付小李的佣金。这时小李察觉异样，要求客服退还之前缴纳的两笔会员费，但同样遭到拒绝。随后，又发现自己被客服拉黑好友。小李这才得知，自己被骗了。

案例解读

1） 案例使用手法为虚假兼职诈骗中典型的“骗会费”手法。相比于网络刷单，这种诈

骗方式更加简单直接且成本极低，易获得用户信任。利用 QQ 群散布兼职广告属于虚假兼职诈骗的常用手段。在寻找到诈骗目标后，会要求用户将虚假兼职广告散布至用户自己已加入的 QQ 群中，并作为“硬性指标”。利用这种方式，从而衍生出更多的目标人群，实现低成本裂变。

2) 繁琐的入职流程主要目的在于迷惑用户，工作视频、文档、录入准确度测试等方法均是为后续诈骗流程做铺垫。从小李的被骗过程看，不法分子组织内部有详细的流程细则、有明确的人员组织架构，整个流程涉嫌多人参与。

3) 利用前期多项铺垫发展至最终缴纳会员费的目的，多引导通过转账方式支付，受骗用户遭受一笔或连续多笔损失。此诈骗手法实施中，虽然每个受骗用户的受骗金额少，但遭受此手法诈骗的人数众多。

二、贷款服务费诈骗

某新款 XX 品牌手机发布后，磊磊作为品牌忠实粉丝想立即入手一台，但生活费余额已不足。于是，磊磊决定通过网络贷款先买到新品手机，利用以后的生活费还贷款。磊磊通过搜索关键词网贷，找到多个小额借贷平台，均在平台内提交了贷款申请，但都未申请到额度。在磊磊正在发愁时，微信收到了新好友添加请求，磊磊同意后与之交谈。

在沟通过程中，对方已明确磊磊的身份信息，并自称贷款客服，通过平台得知了磊磊的贷款需求，通过磊磊手机号添加微信好友做进一步确认，包括理想贷款额度、有无逾期记录、芝麻信用分情况等。磊磊立即表示，想贷款 10000 元，自己没有过逾期记录，因为现在还是学生，芝麻信用分较低。但客服声称，可以为磊磊办理贷款，手续费为贷款资金的 20%，下款后需一次性交清。磊磊虽然觉得手续费过高，但由于着急买手机，同意了客服的手续费要求。

后续，客服发送了贷款平台链接，要求磊磊按照内容填写。于是，磊磊在平台内填写了客服推荐工号、姓名、手机号、身份证号码、银行卡号、最高学历、父母联系方式等信息。提交后，页面显示贷款额度 3000 元，申请下款缴纳 199 元服务费。客服称，由于磊磊征信指数低，每次只能申请 3000 元，但可以多次提交，磊磊只需要再重复申请两次，即可获得 9000 元额度，服务费也需要交纳三笔，共计 597 元，交纳后 12 小时内下款 9000 元。

最后，磊磊在平台内连续支付三笔 199 元用于交纳服务费，但迟迟未收到放款金 9000 元，与之交谈的客服也无法取得联系，磊磊这才发觉，自己遭遇了贷款诈骗。

案例解读

1） 贷款论坛推荐的平台安全指数低。用户提交贷款申请后，身份信息遭到泄露，不法分子获取到用户联系方式后，主动添加用户好友实施诈骗。使用手法中主要运用了非法网站，网站内申请流程与正规贷款平台流程相似，用户无法根据此环节判断平台真实性。

2） 不法分子声称办理贷款收取手续费，并承诺下款后缴纳，这是利用用户资金需求的急切心理，先表明并非免费操作，再承诺可满足用户贷款预期，降低用户的防备心理。但不法分子实际目的并不在此，主要目的是引导用户缴纳下款服务费。

3） 最终审核结果“暗箱操作”，让用户看到下款额度，并利用重复申请增加额度上限为借口诱导用户重复缴纳服务费，最终导致财产损失。

三、 下载恶意程序被扣费

小明作为王者荣耀手游的玩家，十分热衷收集手游内英雄的皮肤。但游戏皮肤都需要人民币充值购买，小明还是一名学生，并没有多余的钱购买皮肤。某天，在王者荣耀玩家交流 QQ 群中，某群友发送了一则广告：免费刷王者荣耀皮肤，有意加群 356******。小明看到后，立即添加 QQ 群，了解这项“黑科技”。

成功加入 QQ 群后，群公告表明，刷皮肤工具在群文件中，有需要的玩家可自行下载，按照程序内指示操作即可。小明在群文件中找到了一款命名为“王者荣耀助手”的 APK 程序，并显示可以免费领取 2888 点券和皮肤，小明下载后，发现程序有两项敏感权限需要确认，位置信息与读取短信，小明并不懂是什么意思，于是像平常安装程序一样，直接全部同意。在进入程序后，并没有操作提示。小明试了几次后，决定放弃，因为游戏中并没有获取点券，也没有收到英雄皮肤，小明只是觉得是个假程序而已，并没有多在意。

在小明将此程序卸载后，频繁收到手机短信，查看后才发现，小明的手机号频繁购买了多项游戏道具，但这并不是小明本人操作，小明这才反应过来，自己安装的是一个吸费恶意程序。

案例解读

恶意程序可以实现扣款行为，主要原因由于用户给予敏感权限。在程序安装后，均会进行权限获取，但大多用户不仔细看权限内容就给予同意，导致恶意程序可在后台进行一系列操作。在用户无意识期间，获取用户手机内的各项敏感信息，导致用户个人资料外泄，造成财产损失。

第六章 聚焦大学生防骗

大学生人群作为国家宝贵的人才资源，是民族的希望、祖国的未来，其安全问题值得社会各界重点关注。近年来，网络诈骗案件高发，大学生人群成为网络诈骗受害主体之一。此现象不但影响高校内的和谐发展，同时影响了大学生个人与家庭的幸福安危。因此，提高大学生自身防范网络诈骗的意识、建立网络安全教育体系刻不容缓。

1） 完善法律法规，加大监管力度

国家相关部门应推进网络诈骗犯罪的立法工作，严厉打击各类网络诈骗犯罪行为。同时，加强网络各类平台的监管力度，提升安全指数。加大网络诈骗案件的查处力度，降低网络诈骗危害性。

2） 网络诈骗安全教育

各高校应广泛开展网络安全教育，通过书本、教育网站、课程、讲座等形式为校内大学生普及网络安全知识。社会媒体积极曝光网络诈骗趋势、新手法、案件侦破进度等，让大学生人群更好的了解网络诈骗。

3） 大学生自身树立防骗意识

建立网络安全基本防范意识，日常购物选择正规购物网站，不被低价广告吸引，抵制诱惑。不在网页中随意泄露个人敏感信息，安装安全软件防范恶意程序的侵害，不要访问不明网址，不要下载不明程序。如果不幸遭遇诈骗，保留好所有证据，立即报警处理。

4） 建立正确的世界观、人生观、价值观

大学生应树立正确积极的三观，抛弃物质主义、享受主义等错误人生观。不贪图便宜，不抱有侥幸心理，保护个人敏感信息，维护自身财产安全。