安徽建筑大学保卫处

校园警讯

（2021 年第 2 期）

保卫处报警电话：北区 0551-63513112；南区 0551—63828112

“诈骗”排行榜，绝对让你叹为观止！

各二级学院、相关部门：

2021 年 1 月至 10 月 20 日，学校共发生诈骗案件 41 起，较 2020 年同期发案 23 起，同比增长 78.3%%。现将诈骗详情公布如下：

“诈骗”排行榜		
诈骗类型	发案数	排名
网络兼职刷单诈骗	13	1
冒充平台客服诈骗	8	2
游戏账号交易诈骗	5	3
网络购物（二手交易、代购）诈骗	5	3
投资理财诈骗	4	4
裸聊诈骗	2	5
社交软件冒充亲戚/好友诈骗	2	5
网聊交友诈骗	1	6
抽奖中奖诈骗	1	6

1.网络兼职刷单诈骗

不法分子在微信、QQ、论坛、网页等撒网式发布帮助淘宝商家刷信誉的兼职消息，以优厚的佣金为诱饵，骗取受害人的信任，然后让受害人购买充值卡、游戏点卡等商品并发来刷单链接或二维码链接，待受害人用自己的银行账户付款后，不法分子会立即消失或以各种理由拒绝退款，从而骗取受害人刷单的本金。

案情回顾：9 月 15 日张同学在看网络小说时，页面跳出名叫“鱼欢”的 APP，学生出于好奇下载了此软件，9 月 15 日晚 7 点 46 分，学生因想赚取佣金（充值 30 元，返还 50 元）开始在名叫“鱼欢”的 APP 内充值 300 元，但被告知充值 300 元提现 400 元的活动已结束，只能参与充值 1200 元的活动，于是学生又充值 900 元，但 900 元充值后又被告知 1200 元的活动已结束，只能参与 3500 元的充值活动才能将之前已经充值的本金和佣金完成提现，之后学生为了提现自己的本金，陆续充值 5888 元、8800 元和 14999 元，截止 9 月 18 日，共计在 APP 内充值被骗金额三万三千一百八十七元，学生反馈手机已安装国家反诈中心 APP，在被骗过程中因未启用软件导致被骗。被骗后，学生打开并启用了国家反诈中心 APP 后，收到了 APP 内的防诈提示。

案例分析：目前在校的大学生中，有很多人有兼职的经历和需求。它已经成为大学生课余锻炼自己能力、积累社会经验和改善经济状况的重要途径。然而一些不良商家利用了他们涉世不深、不知如何维权等特点，给大学生设计陷阱，使得许多大学生在兼职时上当受骗。这些“兼职”披着“挣钱快”、“无门槛”的外衣，利用网络支付的方便快捷的特点，使诈骗也变得容易起来，并且，骗子“得手”后即丢掉使用

过的账号，消失得无影无踪，受骗者往往无处追讨。

2.冒充客服诈骗。

案情回顾：张同学于2021年5月27日接到自称是淘宝客服的陌生电话，以张同学今年5月12日左右在百草味淘宝店铺消费为由，称张同学被百草味工作人员私签定为该公司铂金会员，铂金会员每月需缴纳500元会员费，为期一年共6000元，让张同学缴费。张同学表示这怎么可能，骗子感受到张同学的疑惑和否认，便询问张同学是办理会员还是解除该铂金会员业务，张同学一听办理会员会自动扣除6000元便回答他取消该铂金会员业务。然后骗子以银联的名义说取消该会员业务的话要中国建设银行接入，如同意就转接银行，张同学当然同意，随即转到一名自称中国建设银行北京总行的客服人员，该建行客服说，取消会员要按照对方方法并且本人操作，如果不是本人操作就会影响个人征信，同时自己名下的所有银行卡都会被冻结，还会造成支部宝、微信等支付账号一旦有超过500元就会自动扣除，损伤征信和冻结账户让张同学果断进行账户财产认证，开始转了1元，1元没有转出，张同学发现确实如骗子所说对方不是账户只是后台在认证你的资产，而后跟着手机电话进行第二笔操作，4元也被退回，然后第三笔1700元也被退回，这就更增加了张同学的肯定—这不是骗子，所有钱都退回来了，最后转入8200元（微粒贷转账操作也是骗子告诉他的），但是发现没有退回，这时张同学发现感觉不对劲，情急之下立即拨打110报警。

案例分析： 诈骗分子冒充电商平台客服谎称受害人购买的物品出现问题，以可给予受害人退款、理赔、退税；或者

以受害人会员积分、芝麻信用积分不足不能退款为由，让受害人提高会员积分进行贷款等理由，让受害人将钱款打入指定账户，或诱导受害人泄露银行卡和手机验证码等信息，将受害人银行卡内钱款转走；或者因商品质量原因导致交易异常，将冻结受害人账户资金；或者误将受害人升级为会员、授权为代理、办理了商品分期业务等，如不取消上述业务将扣费。案例中骗子获取受害者准确的私密消费为突破口，获得沟通基础。后利用受害者对“社会机构运转规则”不了解，辅以思想胁迫，让受害者处于无助状态顺从状态从而骗取钱财。本案中，学生盲目听信所谓的银行人员编制征信、冻结银行卡谎言，形成恐慌心理是骗子得逞的关键。

3.游戏账号交易诈骗。

案情回顾：因好友找张同学借钱帮忙，张同学想到有一闲置游戏账号遂准备在交易平台上贩卖来赚钱帮助朋友。6 月 17 日晚 10:30 左右，骗子从闲鱼平台上联系张同学并加上 QQ 最终商定以 1850 元交易游戏账号，并准备在 6 月 18 日中午进行交易。6 月 18 日中午骗子与张同学联系，介绍了一个他经常使用的交易平台哄骗张同学在该平台上进行交易。张同学登录后，经过简单信息注册后，收到对方给自己的一笔转账，但无法提现，与客服联系，客服声称因为银行账号填写错误，资金被冻结，需要高额保证金重新激活才能返还全部金额，同时哄骗诱导张同学本次没有成功的原因责任在他，同时冒充公安人员进行教育威胁，不断打电话骚扰，并提供一些借贷平台让其借款。之后张同学与父母联系，父母亲友奉劝他不要轻信网络陌生人，但后面骗子盗取了张同学个人信息，并威胁要报警，张同学害怕且存在一定的侥幸心

理，前后给骗子汇款 6350 元希望息事宁人，由于骗子不满足，继续要挟，张同学于 6 月 18 日晚报警。

案例分析：目前，虚拟装备、账号交易主要有两种途径，一是通过第三方游戏交易平台，如交易猫、转转、5173 等官方交易平台，风险小，但平台会收取一定比例的手续费；另一种是私下交易，风险较大，权益无法得到保障。诈骗分子就盯上了这之间的矛盾点，架构虚假交易平台，以游戏装备交易、游戏账号交易、游戏币交易等名义,假冒买家和平台客服通过高价收购等方式引诱受害者进行交易，一旦受害者表示有“意向”，骗子就会在交易过程中以解冻金、保证金等为由，骗取钱财。

4.网络购物（二手交易/代购）诈骗

案情回顾：张同学于 7 月 2 日在闲鱼 APP 看到一款二手苹果手机，本打算在闲鱼平台购买，后该卖家以闲鱼联系不方便为由要求加微信详谈。学生本来想上门去看手机，后该卖家发了地址，并表示距离太远过来不方便，于是该学生便也没有去亲自验证，后来谈拢价格，那人说要求付全款，付款就立即发货，并发了顺丰快递上门取件的订单截图，于是学生防备心下降就立即付了钱。后来该学生去查快递，并未查询到相关快递信息，于是就去询问卖家，卖家以各种理由推脱没有时间查询，后来第二天该学生用另一个微信加好友，并咨询该卖家地址，发现地址和之前发的不一样，结合学校辅导员教育的关于反诈骗知识，意识到自己被骗了。于是就打电话给该卖家，电话并未接听，后来该卖家把微信电话都拉黑了。该学生于 7 月 4 号去派出所报案。

案例分析：一些二手交易平台是专业闲置转让的平台，

买家对平台本身有一定的信任度，犯罪分子就利用买家对这些平台的信任来提升自己的可信度，诱骗买家私下交易即时转账，而事实上由于二手交易平台的准入门槛较低，平台使用者良莠不齐，犯罪分子一般用信誉较好的闲鱼号，然后挂假装要卖的东西，诱骗买家购买，后发货给买家垃圾商品；或者通过低价诱骗买家通过即时转账打款给犯罪分子后，拉黑买家，同时也不发货。针对二手交易平台的卖家，犯罪分子一般假冒买家称商品无法购买让卖家联系客服，后假冒二手交易平台的客服以激活店铺、资金冻结等理由让受害人转账。

5.投资理财诈骗

案情回顾：张同学，2021 年 10 月 14 日至 10 月 17 日，因在网上随意添加陌生人好友，进入网络理财赚取“外快”的圈套。在前几次，张同学确实获取了一两百元的利润，遂深信不疑，逐步进入了电信诈骗的套路之中。在后续过程中因“操作问题”个人资金被“冻结”，与对方联系沟通后，对方授意只有继续充钱才能拿出自己的钱，张同学心里焦急不安，因而继续冲动充钱，直至后面联系不上对方，才发觉事情诡异，明白是自己上当受骗。随后联系辅导员，并去学校保卫处登记备案，说明情况。

案情分析：大学生是刚从高中步入大学校园的青少年，较为青涩懵懂，因此对社会的各种诱惑的防范较少，易相信他人。而对方也正是利用这种思想来对涉世未深的大学生进行网络电信诈骗。对方通过互联网仿冒或搭建虚假投资平台，并推荐受害人添加微信群、QQ 群，邀请加入他的战队一起赚钱。当受害人添加这些群，深信跟着“导师”有钱赚时，

他们早已盘算好通过操纵虚假平台数据，以“高收益”“有漏洞”等幌子吸引受害人转账实施诈骗。

案例中的张同学，正是因为个人性格较为内向，且对电信诈骗的各种形式不太了解，缺少了有关的防备知识才导致中招。

6.裸聊诈骗

案情回顾：2021 年 5 月 9 日，张同学打开了 QQ 空间刷空间，然后看到了一则情色广告，学生就点了进去，根据引导，加了一个人的 QQ 号，最开始让学生下载一个软件，下载之后学生点进去发现软件并没有什么响应，就卸载了。后来知道这个软件是用来窃取学生的微信联系人和手机通讯录信息，于是该人与学生就继续在 QQ 上聊天，并开始了视频裸聊，并且学生露了脸。然后犯罪人就把学生与他裸聊的照片和手机通讯录里的联系人电话发给学生，并威胁学生如果不给他钱他就把这些东西发给学生的家人和朋友，并让学生加 qq 群处理此事，学生由于害怕家人知道、害怕学校处理，就想着不如大事化小就同意了。最开始犯罪人找学生勒索要三千，学生说没有，犯罪人就各种引导学生在各个借款软件上借钱，大部分借款软件因为该学生是在校大学生，借不到，最后下载了一个叫做分期乐的软件，学生在上面的乐花卡界面贷到了七千，于是就把三千给了他，随即犯罪人说就开视频把照片删除了，但是犯罪人随后又告诉学生还有备份，让学生再给他 8888 元，这时学生意识到这就是个无底洞，学生拒绝并且说明天再给，但对方不同意让学生现在就给，就这样，双方争论了十几分钟，最终学生把剩余的四千也转给了对方。 5 月 10 号下午 3 点半左右报警。

案情分析：骗子的基本套路都是以网络聊天交友工具为平台，先以女性身份散布诱惑性内容吸引受害人关注，在添加好友后邀请对方点击伪装成聊天工具的木马程序（该代码程序可以把本属于用户隐私的手机通讯录、地理位置、手机短信的信息通过服务器进行收集并植入到对方提供的社交软件中）进行裸聊，随后通过后台录制受害人不雅视频，并套取其手机通讯录、银行卡等，以此获取相关信息。然后对受害人进行敲诈、勒索、诈骗。

7.网聊交友诈骗

案情回顾：2021 年 4 月 18 日，张同学通过 QQ 交友，结识了一位年轻女子，经过网络聊天，双方决定网友见面，于是约定好见面的时间地点。张同学与该女子在见面之后，女子便找张同学要钱。张同学分两次给对方转了总共 650 元钱。聊完天后女子以要回自己的车子里拿东西为理由，便离开了宾馆，之后就联系不上。过了一段时间，学生感觉自己被骗了，情急之下，就选择了报警。

案情分析：不法分子利用 QQ、微信等社交软件，通过频繁的聊天接触，取得受害人的信任，同时骗子利用大学生涉世不深、猎奇等不成熟的想法以及防骗意识不强的心理，成功骗取钱财。

8.抽奖中奖诈骗

案情回顾：2021 年 9 月 25 日下午四点多，骗子通过微博加该同学为好友，通过聊天获取该生的信任后发送二维码让该生付款买东西抽奖，付款后骗子发送抽奖二维码截图。开始抽中香水，折现要求再次购买。第二次购买抽奖是一部手机，做完之后骗子以折现交税金为由要求付款 300，之后骗

子不回信息，该生发现上当受骗。

案例分析：诈骗分子先是通过不法渠道在一些网购平台设置非法链接，消费者一时辨别不清误认为是正规网站。骗子利用消费者信息不对称或者未详细核实的情况获取对方信任，接下来就以各种理由开始行骗了，诱导受害人扫描骗子发过来的二维码、或是填写银行卡号、支付宝账号、密码等等，从而将受害人账号内的钱财转移，套现获利。

主题词：治安、诈骗、安全教育

抄送：学生处、各学院、辅导员

印发：各班级