

**防 诈 骗**

**大学生必备技能**

近年来，全国多地电信诈骗事件引发广泛关注，电信诈骗之所以容易得手，首先是通过大量个人信息被肆意买卖，另一方面是虚假的来电显示号码具有极强的欺骗性。互联网技术发展至今，个人信息特别是身份证号、住址、电话等基础信息，在流动过程中的多个环节均有不同方式的泄露发生，违法分子就是通过掌握公民详细信息进行的精准诈骗。

**一、向“退款”陷阱说NO！**

此类骗局中，诈骗分子先通过非法渠道获取受害人网购信息，然后冒充淘宝客服拨打电话，以主动退货、双倍赔偿为由，引导受害人一步步陷入骗局，向对方汇款。

 

2018年3月4日，白杨派出所接到学生小佳报警，称其在宿舍内接到一个电话，对方自称是淘宝“小H家实拍女装”的客服，说小佳去年5月份购买她们店里的裤子存在质量问题，店家要进行回收并退款赔偿。小佳翻了手机淘宝，确实在5月份的时候有在这家店购买过裤子，就相信对方了。然后对方让小佳填写买家信息，说之后系统会处理退款，小佳也通过了对方支付宝的好友邀请，随后对方通过支付宝发给了小佳名叫“客户服务中心系统”的链接，让小佳填写信息，填写信息需要先登录支付宝账号，小佳就输入了自己的支付宝账号和密码，之后链接内显示需要填写银行信息，姓名，身份证号码，最后一个页面为验证码，验证码是通过手机短信发送给小佳的，但是小佳输入了之后并未成功，对方说让小佳试试输入支付宝密码也许会成功，小佳没有照做。此时小佳的手机收到银行的打款提醒，短信显示小佳银行卡里汇出两笔钱，第一笔是900元人民币，第二笔是1000元人民币，小佳意识到不对，对方说这是因为小佳操作太慢，系统冻结了自己卡里的钱，并给了小佳一个微信收款二维码，让小佳赶紧汇款给对方，若不赶快操作，卡里的钱将全部被冻结，小佳此时心存疑虑，便拨打了之前自称是客服的电话，可电话怎么也接不通，这才意识到自己被骗。

2018年3月20日，白杨派出所接到学生小杨报警，称其在淘宝网一家服装店选购了一件衣服，已经付款成功，但是第二天，小杨接到一陌生电话，说是淘宝卖家，对方称由于支付宝异常、订单无效，要退款给小杨。对方将小杨买的衣服、及淘宝订单号和物流信息都截图给了小杨，小杨信以为真。然后，对方很快又打来电话称正在为小杨办理退款，等会儿系统会给小杨发一条退款转账验证码，需要小杨将验证码发回。小杨发过去验证码后，自己的手机接到短信提醒，显示消费4000元，小杨意识到自己已经被骗，选择报警求助。

民警温馨提示：

1. 在网上购物时，千万不能将银行卡号、身份证信息、手机收到的在线支付短信验证码提供给陌生人，也不要打开对方传来的网址链接，不要轻信陌生的来电或短信，不要轻易转账汇款；
2. 在网络购物中如果发生交易失败现象，可以登录官方购物网站客服电话咨询，不要轻信百度等搜索引擎搜索到的客服电话，发现可疑情况可拨打110报警。

**二、票务售卖暗藏“骗机”**

演唱会门票诈骗的受害者多以学生群体为主，大都是在“抢票大战”中败下阵来的歌迷。在此类骗局中，嫌疑人注册大量微博和微信小号，寻觅大牌明星在各地开演唱会的信息后，他们就在微博上发帖，称有多余的门票抛售。只要有人回复要购买，他们就引导受害人添加他们的微信小号交易。交易时，嫌疑人说会以快递方式寄票，但实际上只要钱款一拿到手，他们就“消失”了。

 

2018年3月5日，白杨派出所接到学生小沈报警，称其昨日中午在微博搜索“Bruno Mars”的演唱会门票，找到了一个名叫“永乐票务服务”的微博，小沈私信对方表示想购买两张演唱会门票，对方让小沈关注一个叫“永乐票务在线服务”的微信公众号，说上面有显示一张票600元，并给了小沈一个微信二维码，让小沈扫码付款1200元。小沈扫描之后显示的收款方是名为“虚无缥缈”的用户收款码，没发现异常，就用微信绑定的银行卡支付了1200元，并给对方提供了自己的收货地址和联系方式。随后对方又给小沈一个二维码让自己选座，小沈扫描二维码后显示的依然是“虚无缥缈”的用户收款码，上面显示收取金额1200元，小沈便问对方，对方说这是一个虚拟二维码，不会收取任何费用。小沈此时想退款，对方说办理退款要找永乐票务的财务部，之后便给了自己一个名为“永乐票务”的QQ，小沈添加了该账户后，对方打QQ电话问小沈银行卡里还有多少余额，并要求小沈告诉对方的微信余额，说是银行卡余额一定要在1200元以上才能办理退款，小沈没有告诉对方并挂断了电话，随后对方在QQ上问之前买票付款时是微信余额还是银行卡付款，小沈说是绑定的银行卡付的，这时对方就给了自己一个二维码，让小沈扫描二维码输入1200元金额才能退款，小沈没有扫描，让对方直接退款，对方坚称一定要按照他们的流程来，小沈拒绝，于是对方说让小沈等待24小时后自动退款，之后便无音信。小沈到第二天中午查看手机，依然没有退款，于是意识到被骗。

民警温馨提示：

1. 不要轻信黄牛，买票一定要选择正规渠道，以免被骗；
2. 存好购票证据，以防万一。

**三、冒充“熟人”来骗钱**

诈骗犯罪分子通过非法渠道获取公民个人信息或随机选择，通过电话、网络和短信方式，编造虚假信息，称自己是对方好友、同学甚至亲戚等熟人设置骗局，谎称有十分要紧的事情需要用钱来应急，诱使被害人汇款、转账。

 

2018年3月3日，白杨派出所接到学生小宋报警，称其在寝室收到同班同学QQ的消息，说帮她的手机充300元话费，小宋知道那位同学周末人不在学校，她手机可能停机就帮她充了，后来她和小宋发消息称手机还是停机，叫小宋再充500元话费，小宋没有丝毫怀疑就充了，紧接着她又让小宋往另一个手机里充值200元话费，却听到室友说也收到了那位同班同学让大家帮忙充话费的事情，小宋这才意识到自己被骗。

2018年3月16日，白杨派出所接到学生小周报警，称其初中同学用QQ联系小周，说有个朋友因为意外受伤而住院，急需用钱，让小周把自己的银行卡号发给对方，对方会往自己的卡里转1000元，然后小周再给受伤住院的朋友微信转1000元，小周想也没想就同意了，把自己的银行卡号发了过去，这时对方就发了一张汇款1000元的截图，但此时小周手机并未收到汇款提示，对方说银行的短信提示会需要一点时间，不会马上就有的，小周也相信了，就在微信上向受伤住院的朋友转账1000元。就在此时小周收到之前的初中同学的群发消息，称自己QQ号码被盗，让大家都不要相信所发的消息，小周这才意识到被骗。

民警温馨提示：

1. 无论是QQ、微信、微博等聊天工具还是手机短信收到好友或是亲友等“熟人”发来要求转账等消息时，一定要通过拨打对方电话进行核实，如对方称电话已换号或停机，应联系其亲朋进行核实；
2. 在聊天中如涉及汇款，一定要谨慎，以防钱财两空。

**四、兼职刷单有风险**

刷单是网店卖家付钱请人假扮顾客，用以假乱真的购物行为，提高网店销量、信用度及好评，从而吸引更多顾客的行为。兼职刷单诈骗中，诈骗分子冒充客服人员向被诈骗的对象发送链接，声称点击了其中的链接，购买商品成功后，货款会退还，还有返利提成，甚至会让被诈骗对象填写一份入职资料，让其以为自己是被正当公司聘用赚钱。完成第一单购买任务后，被诈骗对象会收到客服之前约定的刷单返利，并以此为诱饵，吸引被诈骗人购买更加大额的商品。当交易达到一定数量后，“客服人员”就会切断与被诈骗人的联系，就此消失。因工作轻松、有收益，刷单行为吸引了不少大学生参与，此类诈骗案件高发。



2018年1月25日，白杨派出所接到学生小婷报警，称其在QQ群里看到有人发淘宝刷单的广告，小婷加了广告上的QQ，首先对方让小婷刷单买一件衣服，在付款的操作时，对方提供小婷一个二维码用来扫码付款，第一单数额100元，对方随后返还了小婷100元本金和附加5元的佣金。之后对方继续要求小婷刷5单，买5件同样的衣服，用同样的二维码扫码支付了500元后，对方不再返回本金和佣金，并要求小婷继续刷25单，只有这样才能退还所有费用，小婷自知被骗，就赶忙报警。

2018年3月7日，白杨派出所接到学生小颖报警，称其在宿舍上网时，看到新浪微博上有刷单兼职任务，然后小颖就添加了对方在新浪微博上留的QQ，之后对方让小颖刷单，第一次是120元，佣金5元，小颖照做了，用QQ上绑定的银行卡扫码转账给对方，过了8分钟后收到转账125元。对方提供了第二个，要下20单，小颖说自己没有这么多的钱，对方说那就先5单一结，因为数额较大，对方让我用微信转账，转完之后小颖将自己的转账记录截图发给了对方，对方提出时间超时无法返款，让小颖做完剩下的15单。小颖说自己实在没有这么多的钱并要求退款，对方坚持称要刷完剩下的单，让小颖通过蚂蚁花呗等借贷软件去借钱来完成任务，任务超时没有完成的话会被系统清零，小颖这才意识到自己被骗。

2018年3月24日，白杨派出所接到学生小吴报警，称其想利用平时做兼职打工，便通过QQ搜索添加了一位兼职行业的客服，之后对方发了一个Word文件，里面说明了兼职刷单的教学，小吴看完后就同意做这份兼职了。然后对方发了一个申请表给他，小吴就填写了自己的姓名、手机、和支付宝账号。接着，对方给小吴发了第一个任务，是一个淘宝上价值120元的发饰，小吴按照要求把这个商品添进购物车，然后截图给对方，对方就发给小吴一个收款二维码，小吴通过QQ扫描二维码用自己绑定的银行卡支付了120元，之后支付宝账号就收到了125元。紧接着，对方给小吴发了第二个任务，是淘宝上价值600元的高跟鞋，小吴按照之前操作做了，也是通过QQ扫描付款二维码用自己绑定的银行卡支付了600元，但对方称这次的任务是20单，要小吴再做19单。小吴说自己没有这么多钱，并让对方将这600元返还给自己，对方说没有任务不能返钱，小吴这才意识到自己被骗。

民警温馨提示：

1. 不要轻信网上刷单广告内容，骗子把刷单当借口，用简单的要求和丰厚的利益来吸引眼球，天下没有不劳而获的钱财；
2. 不要轻易点击或扫取陌生人发的网页链接和二维码；
3. 保管好网络账号的密码以及身份证、手机号等个人信息，常用杀毒软件对电脑进行杀毒；
4. 小心假客服用专业术语和“贴心”服务来获得你的信任；
5. 发现被骗后，应及时拨打110报警，同时要注意保留证据，如银行转账记录、通信记录、聊天记录等。

**五、游戏中的“诈骗术”**

截至2017年底，据《中国互联网络发展状况统计报告》，中国已经成为全球最大的游戏市场。网络游戏用户规模达到4.42亿，在网民总数中占比过半，大学生为主力军。

游戏账号交易是诈骗的重灾区。一种是收了钱没账号，空手套白狼；一种是交易结束后，骗子以账号被盗为名向游戏平台提交身份信息，将账号找回。第二种情况下，用户在所买账号被骗子找回后，苦于没有原始注册资料，常常无处申诉。

游戏装备也是诈骗高发区，主要有低价充值、送道具送装备、装备中奖诈骗等陷阱。具体手段包括以低价充游戏币为诱饵，收了钱就跑路；通知玩家中点券，但要求先行缴税。此外，暗含勒索病毒的游戏外挂、辅助工具也有诈骗风险，用户下载后电脑中毒，需付费才能恢复正常。

 

2018年3月1日，白杨派出所接到学生小王报警，称其在剑侠情缘三游戏上联系玩家欲购买游戏币，对方说要通过游戏平台支付，并给了小王一个QQ号，小王加上对方的QQ号，并打开了对方提供的游戏平台链接，注册了用户名。然后小王找到了平台付款的二维码，用微信零钱扫码支付了100元，并联系客服，客服说小王的个人信息填写的不全，需要充值1080元审核身份，小王就用微信继续扫平台二维码支付了1080元，随后联系客服，客服称刚才小王填写的个人信息有误，需要再充值1080元，小王信以为真又用微信扫码支付1080元。随后小王和客服说要退款，但客服称小王的个人信息里的银行卡号有错误，需要继续充值4800解冻，小王就又一次用微信扫平台的付款二维码，支付了4800元，这时客服说还要再充值4800元，用来继续审核身份信息，小王的微信此时已经没有钱了，便联系自己的姐姐，让姐姐登上自己的平台用户名和密码。随后，小王的姐姐用她微信绑定的银行卡支付了4800元。此时小王已经总共往游戏平台汇款了11860人民币，发现事情不对，就报了警。

2018年3月13日，白杨派出所接到学生小黄报警，称其在寝室里看虎牙直播上的QQ飞车手游直播，里面的说抽奖可以包中奖的，对方说最少给他700元就可以帮小黄抽奖。小黄之前在虎牙直播上也，但不是这个主播，上一次小黄给对方转钱，对方帮小黄抽到了奖，所以这次小黄就轻信了，直接给对方微信转账700元，之后被对方删除了好友。

2018年3月26日，白杨派出所接到学生小王报警，称其在手机上添加了一个微信好友，向他购买狼人杀游戏的道具。小王跟他商谈好相关的游戏道具和价钱后，就微信转账给了对方，分两次转，每次248元，共496元。转完账后小张登陆了游戏账号发现确实充值了相应的道具，然后小张就再次向对方购买其他的游戏道具，与对方商量以555元购买，并微信转账给对方，但转完账后发现游戏账号里并无充值的道具，想询问对方时发现自己已经被删。

民警温馨提示：

1. 为电脑安装安全防护软件，从正规网站上下载网游插件，并注意核实网游地址；
2. 上网玩游戏千万不要轻易打开商家发来的不明链接、文件、压缩包及二维码，并安装病毒查杀软件定期查杀电脑，保护账户隐私；
3. 如发现账号异常，应立即与游戏运营商联系。

**六、利滚利之“校园贷”**

“校园贷”作为一种新兴的网络金融平台，在给学生提供资金便利的同时，也引发了不少社会问题，滋生诸如“电信诈骗”“敲诈勒索”“寻衅滋事”“暴力催债”等违法犯罪行为。由于在校学生社会经验不足、防范意识较差、心理承受能力弱、法律维权意识不强，“校园贷”违法犯罪给学生的心理、精神造成严重伤害，个别甚至因无力偿还所受胁迫而自杀，社会影响极其恶劣。

目前“校园贷”诈骗的形式主要有以下几种：

1. 通过互联网平台向在校大学生推送贷款广告，以免抵押、低利息为诱饵诱导学生贷款，并要求缴纳贷款“手续费”“管理费”“保证金”等费用，收到学生支付款项后即将其“拉黑”不再联系。
2. 串通“职业培训机构”举办职业指导讲座，夸大培训效果，与学生签订声称能提高综合技能的培训合同，并与贷款公司勾结，诱导学生贷款支付学费，从中诈骗学生。
3. 更为极端的，要求学生提供隐私照片、视频、身份证和家属电话号码等作为贷款抵押和担保，一旦学生无法如期还款，便以此威胁，勒索钱财。

 

2017年12月17日，市民林先生来派出所向民警求助，称其儿子第一次校园贷的借款是800元，利滚利后他儿子所背负的债务，已是高达20万了。林先生说，当借款金额累计到合同签订的上线两万元时，上一家放贷人就会将借款人债务转移到下一家放贷人，儿子为了还钱，也丧失了理智，同时向多个放贷人借款，债务额急剧上升。林先生说儿子一笔借款的年利率高达1300%，再加上每一次借款还要给一笔不小数额的上门放款费和上一家放贷人的介绍费，800元的借款一下子就滚到了20多万元。他也曾经想过报警，但是在借款时，儿子向放贷人登记了家庭、学校、老师、同学的联系方式，有的同学还录制借款视频。他担心放贷人采取不法或极端方式讨债，影响儿子学习，甚至威胁儿子的人身安全，所以才选择妥协。最终百般无奈之下，林先生选择报警求助。

民警温馨提示：

1. 大学生要树立正确的消费观，要充分认识网络不良借贷存在的隐患和风险，增强金融风险防范意识；
2. 要树立理性科学的消费观，养成艰苦朴素、勤俭节约的优秀品质，尽量不要在网络借款平台和分期购物平台贷款和购物，利息和违约金非常之高；
3. 要积极学习金融和网络安全知识，远离不良网贷行为。