内部学习资料
仅供校内分享

# 大学生防范电信网络诈骗

# 宣传教育手册

学生工作部（处）

2021 年 5 月

# 第一部分 大学生常见电信网络诈骗典型案例

## 一、刷单返利

【防骗提醒】

1.刷单既是诈骗也是违法行为。

2.切勿相信任何网络、短信刷单广告。

3.大学生是刷单诈骗的主要受害群体，应养成正确价值观，勿相信高收入低门槛的所谓网络兼职。

**案例一：**某学院大三学生小周在某QQ悬赏群看到有人发布招募刷单员的信息，遂添加对方好友。之后，按对方发送的操作流程下载了企业微信和“资和信”APP（注：企业微信APP看起来非常正规）。对方提供给小周一个账号，并发给小周一个链接，要求登录指定账号并购买1张100元星礼卡，佣金6元。小周通过微信支付购买后，对方随即向小周转账106元。第一笔刷单完成后，小周逐渐放松了警惕。对方又让小周按照同样的方式购买了5张100元的京东电子卡和4张500元的星礼卡，并告知在完成10单后集中返现。小周随机通过微信支付购买，而对方并未如数返现，且将小周的账号强制关闭。小周意识到被骗，遂报警，被骗金额2494元。

**案例二：**某学院大二学生小杨在某QQ悬赏群看到一则网络刷单兼职信息，遂通过对方提供的微信二维码，添加了对方的微信并

咨询相关兼职信息。对方告知是淘宝刷单业务，并提供了刷单步骤的操作视频，视频显示在拍下商品后会出现企业代付界面，但小杨根据对方提供的步骤下单后，并未出现企业代付界面，而是直接从支付宝花呗转走了 799 元。小杨立即联系对方要求退款，对方让小杨添加了一个客服微信，该客服解释操作失败是因为系统冻结导致的，现需要刷单激活，才能退款。小杨信以为真，遂进行了第二次操作刷单 1000 元，以便激活“账户”。“账户”激活后，小杨再次联系对方要求退还 1799 元，对方告知需要过银行流水才可退款，并让小杨向他的银行卡转账 4000 元。此时，急于退款的小杨未经思索，再次向对方转账 4000 元，转账成功后对方便不再回复任何信息。小杨意识到被骗，遂报警，被骗金额 5799 元。

**案例三：**某学院大一学生小刘收到一条备注为“有事找”的微信好友申请，同意申请后，小刘出于好奇问他何事，对方未回答。随后，对方将小刘拉进了一个 A 微信群，群内有人发布了“任务单”，任务内容为“关注微信或者抖音制定人物，并把截图发至群里，完成任务即发放佣金”。小刘抱着试试看的目的，按流程完成了操作，即收到了佣金。随后群内又发布了下载并注册“首创创投”APP 的任务消息，小刘按照提示下载注册，并加入了另一 B 微信群。此时，因 A 微信群不再发布任何消息，小刘退群，并开始关注 B 微信群的“任务单”。B 微信群发布了类似于暗箱操作买彩票的任务，在完成 2 次任务后，对方“导师”询问了小刘的一些个人基本信息，并开始向小刘推送 1000 元以上的大额任务，在小刘完成任务需要退款时，APP 界面出现“网络问题”提示语。小刘随即联

系“导师”,“导师”告知需要进行5000元的补单任务，任务完成后方可退款。此时的小刘虽然有些警醒,但本着完成补单就能退款的想法，小刘完成了补单任务。但是 5000 元的补单任务完成后，“导师”告知要再转账 20000 元方可完成补单任务。小刘意识到被骗，遂报警，被骗金额6000元。

**案例四：**某学院大一学生小孟在某QQ群内看到一则招聘补单人员的广告,好奇心促使其点进链接,并添加了“客服A”进行咨询。随后“客服A”向小孟推荐了“客服B”，“客服B”向小孟详细介绍了刷单流程并推荐了名为“淘购网”的刷单APP,并提供了存有3000元启动资金的刷单账户。小孟认为过程简单，且是用“客服B”提供的有资金的账号进行操作,对自己信息和财产不会造成损失,于是进行了第一次刷单操作。接下来的几天,小孟利用课余时间,通过“客服B”提供的账号,登陆“淘购网”进行刷单操作。“客服B”承诺将所赚佣金的12%返给小孟，小孟每刷1单大约赚取3元。佣金提现的要求是需完成60单且佣金积累到100元后方可向“客服B”申请。待小孟刷单满足上述条件向“客服B”反馈时，“客服B”告知其需再刷60单，即可直接提现100元，该生按照“客服B”要求进行操作。几天后,小孟操作完成并如愿提现100元佣金。

初次尝到甜头,让小孟彻底放松了警惕。当小孟再次获得佣金满100元提现的机会，准备继续刷满60单提现时，却发现APP出现了问题。咨询“客服B”后，被告知是出现了“联单”(系统卡顿会出现抢到多单且无法取消的情况),账户资金余额不足以支付

抢到单子，要想继续刷单提现，就必须进行充值。此时小孟意识到可能存在问题，但想到马上就能到手的 100 元佣金，抱着“诈骗应该不会落到自己身上”的心理，将自己近 2000 元的生活费进行了账户充值。充值后小孟发现仍无法提现，随后向家人要钱，家人多次提醒此为网络诈骗并拒绝给钱，但此时小孟已陷入“一定要把前边投入的钱财取出来”的执念，随后又向朋友借款 4000 元，在多次投入仍无法取出的情况下方才意识到被骗，遂报警，被骗金额 6261 元。

## 二、冒充熟人

【防骗提醒】

1. QQ、微信、微博、抖音、快手等网络聊天工具中，任何亲友、熟人、同学以任何理由向你借钱的，一律打电话与本人确认。

2. 称不方便打电话、不方便语音或视频连线的切勿轻信，核实查证前勿汇款。

**案例一：**某学院大一学生小宋收到 QQ 好友陈某消息，对方称其表妹生病在医院，着急交医疗费，且只能通过支付宝缴纳，但是陈某的支付宝未绑定银行卡，遂提出自己把钱转至小宋银行卡，由小宋通过支付宝将钱转给其表妹。小宋同意并告知了其银行卡号，随后，陈某称已经将 7600 元转入小宋银行卡，并将转账成功截图发给了小宋，但小宋查询后并未收到任何款项。陈某告知小宋，银行扣款已完成，可能是周末跨行转账有延迟、银行受理时间为 6 小

时等原因，要求小宋先通过支付宝转账给其表妹缴费治病，因小宋余额不足，遂通过支付宝转账6400元。陈某称其表妹病情十分紧急医药费还差1200元，要求小宋可先向朋友借钱救急，小宋意识到可能有问题，即与陈某电话联系，陈某告知其QQ号被盗正在申请找回。小宋意识到被骗，遂报警，被骗金额6400元。

**案例二：**某学院大三学生小胡收到了多年未联系的高中同学的QQ消息，因个人事务向其借款2500元。小胡未加思索，即在对方引导下，通过微信-搜索电话号码转账的方式分两次向其转账，第一次为1000元，第二次为1500元。当天小胡即发现，其高中同学在QQ空间里发布了QQ号被盗的声明，经与其电话确认后，意识到被骗，遂报警，被骗金额2500元。

## 三、冒充电商客服

【防骗提醒】

1.订单信息可能会被盗取，订单情况以正规电商官方APP显示为准，有问题咨询APP内电商客服。

2.电商“客服”以订单问题、商品质量问题需赔付、商品丢失需退款等指引你打开支付宝、登陆网银、提供验证码、下载陌生APP、点击陌生链接等极有可能是诈骗。

3.商品价格明显低于市场价的各类广告信息极有可能是诈骗。

4.陌生“客服”来电，尤其是境外电话多为诈骗电话。

**案例一：**某学院大二学生小范接到自称是淘宝客服的电话，告知其之前购买的面膜有问题质量，要向小范赔付 300 元。然后让小范在支付宝“备用金”上提 500 元，并谎称这些钱是淘宝的，需要小范将多提的 200 元通过网银返还。所以小范就从里面提出了五百元，多余的二百元让小范从网上银行返还给他们。小范操作完成后，对方告知其备用金功能目前无法关闭，会影响征信，需要资金流动方可关闭。对方让小范通过微信搜索公众号“乐花卡”，上传身份证照片，识别人脸并绑定个人信息，告知小范需通过“乐花卡”提取 3000 元到本人银行卡（据对方描述，这个钱是从淘宝提出的），再转回淘宝，即完成资金流动。小范按照要求操作后，对方告知备用金已关闭。几天后，小范收到了“分期乐”的还款提醒短信，此时小范意识到对方已经通过其身份信息在“分期乐”借贷 3000 元，遂报警。因分期乐属于正规借贷平台，如不如期还款会影响征信，小范遂进行了还款操作。被骗金额 3363.67 元。

**案例二：**某学院大一学生小张通过 QQ 空间获悉了某微商客服贩卖手机的广告消息，声称 ihpone12pro 仅需 2100 元就能买到，于是小张通过 QQ 与对方取得联系，对方向其展示了“晒单”“好评截图”等信息后取得了小张的信任，小张遂添加其微信，并支付了 2100 元手机款。随后，对方告知小张需再次支付 1000 元的“保证金”（对方承诺交易完毕后“保证金”予以退回），才能提供三年质保和免费退货服务，否则不予发货（期间拍下印有小张地址信息的快递单照片博取信任），小张支付了 1000 元的“保证金”后意识到可能被骗，遂前往派出所报案。之后，小张在配合公安部门

做材料信息收集期间，对方再次联系小张，告知其需转账1000元即可退款，小张支付1000元后，对方退还1500元，并告知小张通过这种“退款方式”将剩余货款全部退回，并承诺小张支付2000元后即退还2500元,小张信以为真,便向对方转账2000元，之后，对方不再回复任何信息。至此，小张被骗金额4600元。

**案例三：**某学院大一学生小安接到一自称为京东客服的境外电话，对方告知小安，因平台系统问题，误将其京东账户设置为了店铺代理商，每个月需扣除代理费用500元，费用直接通过支付宝账号扣除。为避免扣除小安费用，需要冻结其支付宝绑定的银行卡。对方告诉小安因办理银行卡冻结业务需要1400元，其卡内余额只有900元，需通过支付宝“备用金”提现500元至银行卡方可办理，小安遂按照对方要求，进行了转账操作，期间，对方一直以时间为由催促，一直保持电话连线。转账完成后，对方通过电话转接，直接将电话转至农行客服（对方同伙），农行客服告诉小安，办理银行卡冻结业务通过将银行卡余额全部转出至指定账户，转账失败三次后账户自动完成冻结。小安按照农行客服要求，进行转账操作，前两次均转账失败，提示“对方账户不存在”，第三次转账时，提示转账成功。小安意识到被骗，遂报警，被骗金额1400元。

## 四、网游诈骗

【防骗提醒】

1. 适度游戏愉悦身心，沉溺游戏贻误人生。

2. 不要轻易相信网络游戏中的中奖信息，购买装备和虚拟货币时尽量通过认证的方式进行交易。

3. 申请游戏账号用实名制和真实身份证填写资料，牢记密码提示问题和答案。一旦发现丢失可以立即用密码提示取回。

**案例一：**某学院大二学生小卢在玩网络游戏时，有人申请加其好友私聊，并称想购买他的游戏账号，小卢信以为真，便将自己的QQ号告知对方。对方加其QQ后，通过协商确定价格为766元。对方以通过QQ直接交易不可靠为由，提出可通过“盛万拍”网站进行交易，小卢按照对方指引登录了“盛万拍”平台，将自己的游戏账号上架，并通知对方购买，对方拍下后，小卢的“盛万拍”平台账户余额显示到账766元。小卢申请提现，平台显示“银行账户错误，提现失败”。小卢联系平台客服，客服答复：因小卢操作失误，导致账号锁定，需先在“盛万拍”平台指定账户中充值766元，才能重新提现。之后，客服发给小卢一个银行账户，小卢向该账户转账766元后，再一次尝试提现，但仍显示“提现失败”。小卢再次联系平台客服，客服答复：因小卢提现时没有零头，不符合提现规则，需小卢往平台充值6208.1元，才可提现。小卢同意并完成了充值操作，当小卢再次申请提现时，平台再次显示“提现失败”。小卢意识到被骗，遂报警，被骗金额6974.1元。

**案例二：**某学院大一学生小吕在宿舍玩游戏时，想卖掉游戏装备，因通过平台售卖卖装备需支付较高手续费，遂把信息发布到一

个游戏主播的QQ群中，标价1710元。之后，有人加小吕QQ好友，告知要购买该装备，但希望让游戏主播作为中间商，即对方先把钱转给主播，待小吕将装备移交后，由主播将钱转给小吕。为打消小吕疑虑，对方发来了向游戏主播转账成功的截图，小吕信以为真，遂将装备移交给对方，对方收到装备后将其拉黑。小吕向游戏主播询问情况，发现对方是通过与游戏主播相似的QQ号骗走了游戏装备，遂报警。

## 五、其他诈骗案例

【防骗提醒】

1.对于陌生来电的身份要进行核实，不轻信、不回答，切勿转账汇款给陌生人。

2.要通过正规网站查看招聘信息、发布求职信息，不要轻信未上岗就交中介费或保证金的不合理条款。

3.不要随意连接陌生WiFi、不要随意下载安装手机软件、不要随意泄漏个人身份信息、不要轻信收到的福利信息等。

4.任何不需签订合同的贷款是不可能的。如需贷款，请选择正规融资渠道。

5.办理信用卡需要提供本人身份证件等资料到银行网点办理。即使通过银行官方网站申请，也要本人到银行网点提交身份证件等资料或银行工作人员上门核对身份无误后才能开通。

**案例一：**某学院大四学生小魏想利用业余时间挣点零花钱，遂

通过搜索本地的家教QQ群找到一份家教的工作，薪资是80/小时，每天2小时。因小魏之前做过家教，且都是通过电话或视频确认，本次没有确认步骤，小魏没有起疑，而是直接缴纳了中介费270元。随后，对方让等待一段时间看家长回复，一天后，没有回应。小魏意识到被骗，遂报警，被骗金额270元。

**案例二：**某学院研究生小陈接到一陌生电话，对方告知小陈个人征信存在问题，可以帮助其恢复征信。为打消小陈的疑虑，对方与小陈确认了其姓名、电话、家庭信息、学校信息等。之后，小陈按照对方提示进行了个人支付宝的积分验证，并根据对方提示，登陆了对方提供的中国人民银行征信中心（虚假网址），并查阅了本人征信信息的相关文件，网站上显示小陈的“征信状态”存在问题。因小陈之前曾办理过信用卡，加之对方提供的信息真实无误，小陈逐渐放松了警惕，并按照要求加入了对方开设的腾讯会议。通过对话，对方以恢复征信、清空教育额度为由，要求小陈申请开启绿色通道资金流水认证，并通过向制定账户转账，提高征信分，征信分提高后，转账资金原卡退还。为恢复个人征信“正常状态”，小陈按照对方要求，先后三次向对方提供的账号转账累计40640.7元，待小陈要求退款时，对方将小陈踢出了腾讯会议。小陈意识到被骗，遂报警。

**案例三：**某学院大三学生小陆接到一陌生电话，对方声称是支付宝注销部工作人员，以大学生今后不能再使用借呗、花呗为由，要求注销其学生账号并更新为成人信息。随后对方诱导小陆进入

某腾讯会议开启录屏，查看其银行卡余额，并告知要进行金额安全保障，要求小陆分两笔把卡里的所有余额转入指定账户，第一笔为5378.50元，第二笔为5666.11元。之后，对方又以额度清零为由，让陆某通过饿了么平台开通“饿用金”并借贷6900元转到指定账户，并承诺之后会把已转账的款项全部原路返还。在小陆转账完成要求退款时，对方告知因转账数额不足，仍然无法进行身份更新，必须下载“云闪付”APP进行借贷方可更新。小陆意识到被骗，遂报警，被骗金额17944.61元。

**案例四：**某学院大四学生小郭有创业的想法，遂通过某网站填写了个人信息申请办理贷款，当天就接到了自称平台工作人员的电话，对方称将马上帮助他办理贷款。效果根据对方要求办理了一张银行卡等待贷款到账，并将银行卡信息如实在平台上进行了登记。之后，平台工作人员便称能帮助他以最低的利息申请更大金额的贷款，但是需要他先向刚办理的银行卡转账5万元证明还款能力。为了争取更多的贷款，小郭便按照对方指示向卡内转账5万元，并将手机收到的验证码告知了对方，随后小郭收到了5万元转出的提示短信。小郭意识到被骗，遂报警。

# 第二部分 大学生容易遭遇的网络电信诈骗类型

## 一、网络兼职刷单被骗

进入大学，网上兼职，操作简单、赚钱较快的刷单成了理想的选择。起初，刷单金额较低，诈骗分子会及时返还报酬赢得学生信任，随着刷单的进行、金额的增大，他们不会再返还本金，更不可能返利。

## 二、网上购物被骗

诈骗分子通过各种手段获取网购客户的订单信息；冒充天猫、京东、淘宝等客服人员和银行客服人员电话联系受害人，准确说出受害人购买的商品信息，使得诈骗更具有迷惑性；以网购平台系统升级造成网购订单丢失、网购商品缺货无法安排交易、网购商品存在质量问题需召回等原因，要退钱给受害人，要求受害人提供银行卡号、密码等，或以手机短信、微信、QQ 等形式给受害人发送退款链接或二维码，通过钓鱼链接或二维码，获得受害人银行卡号、身份证号、网银登录密码、手机验证码，盗取受害人银行卡资金；或者声称客服操作失误，误将受害人加为会员，能享受购物折扣，但每月需扣一定费用，诱导受害人提出解除会员的要求，到 ATM 机进行操作，诱骗受害人转账汇款。

## 三、手机或者 QQ 号码被盗，冒充熟人诈骗

微信、QQ 因其方便快捷，已成为学生与父母之间、朋友之间最主要的联络方式之一。而犯罪分子也利用这一平台，采取盗号或

仿冒身份注册账号等方法，模拟亲朋好友，谎称生病、车祸、手机需要充话费、缴纳学费、生活费不足等以急需用钱理由借款实施诈骗。

## 四、购买游戏装备被骗

很多大学生喜欢通过玩网络游戏缓解压力放松心情，犯罪分子也看准了网络游戏这个平台，他们冒充游戏玩家、异性玩家、游戏运营商等，以代练游戏角色、低价销售游戏币、装备以及出售游戏账号等种种理由，让玩家线下银行汇款，收钱后消失或盗回账号；或以高价收购游戏账号为名，诱使玩家登陆钓鱼网站交易，获取银行卡信息后盗取钱财；或者谎称可升级代练游戏角色，玩家汇款后即将装备、游戏币洗劫一空，并立即消失。

## 五、网上交友被骗

此种类型被骗者男性居多，进入大学心理空虚，对虚拟网络产生依赖，不法分子大多在网络上以美女照片、裸聊等方式进行诱惑，在聊天中以生活遇到各种困难为借口向对方索要金钱，达到一定金额后，就无法再取得联系。

初级版：冒充“高富帅”“白富美”。嫌疑人往往通过网络交友、相亲网站，编造出“高富帅”或“白富美”等虚假身份，在与受害者进行网络交流，骗取受害者信任、确立交往关系后，选择时机提出借钱周转、家庭遭遇变故等各种理由，骗取钱财后便销声匿迹。

中级版：冒充“特种兵”“卖茶女”。

高级版：冒充“证券、投资公司内部人员”拉你“投资”。

## 六、网上借贷被骗

部分大学生因为攀比、或者想证明自己在财力不济的情况下干自己想干的事。诈骗分子利用这种心理，通过建立假贷款网站平台、办理信用卡网页，并以月息低，无需担保、手续简单等条件诱使大学生步入陷阱。

校园贷特点：第一，放贷门槛极低、审核如同虚设。一些“校园贷”平台为了增加业务量，明知大学生没有独立经济来源和还款能力，仍向其发放高息贷款。第二，高费率、高利率、高罚金。一些不良“校园贷”平台，利率高达30%左右，并且按周计取；或者表面上收取合法、合规利息，但实际上在放贷过程中还会收取高额的手续费、工本费、催还费等等，从而实现变相高息；而其设置的罚息，高到令人瞠目结舌。实质上成了赤裸裸的高利贷，短短几个月，要收取的费、利、逾期罚金超过本金的几倍甚至几十倍。第三，诱导借新贷还旧贷。诱导大学生从其他高利贷平台借款，以归还在本平台的欠款。第四，违规、违法、暴力催还。向借款的大学生及其同学、亲友、老师发布该生的欠款信息，逼迫其归还，更有甚者，以借款人的裸照为抵押物，逾期未还款则威胁将其裸照和个人信息公之于众。第五，引发“被贷款”问题。一些大学生本无借贷之意，却被同学利用身份信息行了借贷之实，甚至出现连环“被贷款”问题。

## 七、求职被骗

学生课余时间、周末或者假期，想兼职打工挣钱，对网上发布的求职信息，不辨真假，对方要求缴纳中介费和求职押金，但是提供的岗位是虚假的，提供几次虚假信息后，便以各种理由推脱责任，不再提供岗位，上当被骗。

## 八、奖助学金被骗

国家每年都会发放一定数额的奖学金帮助贫因大学生更好地完成学业，犯罪分子在这段时间，冒充国家工作人员,以申领补助金、救助金、奖学金等理由要求大学生提供银行卡号，然后再以资金到帐查询为由，指令学生在自动取款机上进入英文界面操作，将钱转走。

## 九、自身信息保管不好泄露被骗

学生自己有关的证件和信息处理不当，如手机号随意变更，号码不用后，不销户，贪图小便宜，随意卖给别人，不法分子利用这个手机号作案，电话联系受害人，实施犯罪。

## 十、提供考题类被骗

诈骗团伙通过黑客攻击或者网上购买得到考生信息，然后给考生群发短信或者邮件，或者在校园内张贴小广告，声称“能提供某某考试的试题、答案，也可以帮助改分，甚至是办假证”，并留下联系方式，一旦有受害人急于求成，试图作弊，按照犯罪分子的要求将钱款转入指定账户，就会被骗。

# 第三部分 大学生如何防范电信网络诈骗

## 一、牢记“四不原则”

不汇款、不轻信、不泄密、不链接。

## 二、做到“四不一多”

1.不随意连接陌生 WiFi。

2.不随意下载安装手机软件。

3.不随意透露个人身份信息。

4.不轻信收到的陌生福利信息。

5.转账前要通过电话等方式多核实确认。

## 三、牢记十个“凡是”都是诈骗

1.凡是自称公检法要求汇款的;

2.凡是让你开通网银接受检查的;

3.凡是叫你汇款到“安全账户”的;

4.凡是自称领导要求汇款的;

5.凡是通知中奖、领奖要你先交钱的;

6.凡是陌生网站要登记银行卡信息的;

7.凡是通知“家属”出事要先汇款的;

8.凡是承诺能帮你代办各种银行信用卡的;

9.凡是在电话中索要银行卡信息及验证码的;

10.凡是用各种借口引导你用英文界面操作 ATM 机的。

## 四、养成防止被诈骗的七个好习惯

1.保护好个人身份证和银行卡信息，保管好不用的复印件、睡眠卡、交易流水信息；

2.网上银行操作时，最好手动输入银行官方网址，防止登录钓鱼网站；

3.输入密码时，用手遮挡；

4.密码要设置的相对复杂、独立、避免过于简单，避免与其他密码相同，并定期更换；

5.开通账户动账短信提醒，一旦发现账户资金有异常变动，立刻冻结或挂失；

6.不随意连接不明公共 wifi 进行网上银行、支付账户操作；

7.单独设立小额独立银行账户，用于日常网上购物、消费。