



防范电信网络诈骗案例分析集

识诈是反诈的前提，知骗是止骗的关键。为提升全校师生员工的反诈能力，筑牢校园安全防线，安全保卫部立足高校防范电信网络诈骗形势，总结出7类学生群体易发多发受骗类型和1类涉诈违法案件，用真实的警示案例，帮助师生看清骗局本质；用通俗的防骗知识，教会大家识破诈骗陷阱。校园反诈，人人有责，希望以此为契机，推动形成“师生同心、家校联动、全员反诈”的校园安全氛围，守护好每一位师生的“钱袋子”，为建设平安校园筑牢坚实的反诈屏障。

一、参与帮助信息网络犯罪活动

法律链接：《中华人民共和国刑法》第二百八十七条之二第一款规定“明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供**广告推广**、**支付结算**等帮助，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

【情景再现】某学生经校友介绍下载“京东易购”APP并注册账户，用来帮助他人购买手机。购买方将钱转入其“京东易购”账户（**非法资金转入**），学生通过该账户帮助其购买手机（**提供支付结算**），每笔可赚取到消费额度5%至10%的佣金（**非法收益**）。最终，该学生涉嫌从事帮助信息网络犯罪活动，被公安机关依法采取强制措施。

【安全提示】帮信犯罪的被告人呈现低龄化、低学历、低收入、初犯比例高的“三低一高”特点，35岁以下被告人占比超过80%，25岁以下被告人占比三分之一。学生群体容易被“零成本”“高收入”

所诱惑，出租、出售、出借自己的银行卡、电话卡或网络支付账户，陷入违法犯罪的深渊。广大学子应当提高警惕，穿好“防御甲”，不做电诈“工具人”。

二、“约炮”类刷单诈骗

【情景再现】某学生在抖音平台点击了弹出的消息框，下载**不明软件**。该软件以“充值返利+完成任务可约女生见面”为诱饵，诱导其参与活动。学生先小额充值 20 元获返现 22 元、充值 120 元获返现 144 元，随后在“约见面”的诱惑下充值 1200 元。此后，对方以操作失误**冻结**资金需交 5000 元**解冻**、账号被封需分两次交 3050 元、6000 元解封、银行卡号输错需交 9000 元解冻、需交 1700 元由程序员解封等理由多次要求转账。最后发现自己被骗，共计被骗 27000 元。

【安全提示】“约炮见面”“充值返利”等都是诈骗团伙的套路，“返利”是诱饵，“约见”是骗局。同学们应当自洁自律自爱，不浏览涉黄信息，不随意点击陌生链接、不下载陌生软件，一律拒绝任何转账汇款操作。

三、“社交软件账号被盗”诈骗

【情景再现】某学生收到初中同学王某的 QQ 消息，称朋友住院急需用钱，该生便通过**二维码**向对方转账 1000 元，凌晨 5 时通过微信向对方核实才知道王某 QQ 号被盗。

【安全提示】在用网络社交平台与好友联系时，若对方以紧急情况为由，发出帮忙**付款**、**充值**、**借钱**等请求时，要通过拨打电话等渠

道，对好友身份进行核对确认，不能仅凭文字信息就配合转账。同时还要注意保护个人信息，不要随便泄露自己的银行卡号、身份证号码等信息，以防骗子利用软件生成虚假转账单实施诈骗。此外，在第三方支付平台进行大额转账时，可以设置延迟到账，为追回损失争取时间。

四、“刷单”兼职诈骗

【情景再现】某学生在“小红书”平台上看到一则招募网络兼职的广告，内容宣称看视频点赞点关注完成小任务即可赚钱。起初该学生完成任务后确实得到了获利，随后对方称任务升级，要求其转账到指定账户，帮忙刷账户流水，学生便往对方账户转账 500 元，完成后对方表示账户流水仍不足，需要再次转账才能退款，最后发现自己被骗。

【安全提示】网络刷单本身就是违法行为，不要轻信网络上“高佣金”、“先垫付”等兼职刷单的信息，不能抱侥幸心理相信骗子的退款承诺，以免遭遇连环骗局。

五、“网购”诈骗

【情景再现】某学生通过社交软件结识了一位自称经营电脑业务的陌生网友，对方声称可以帮忙在电商平台代购电脑，并发送了身份信息和经营资质，以此获取学生信任。随后向该生提供了支付二维码，支付成功后，对方又称还有其他代购名额，而且优惠力度很大，学生便继续转账让对方帮忙代购。几日后，学生收货时发现均为空包裹且

无法与对方取得联系，遂发觉自己被骗。

【安全提示】网购务必选择大型、正规的电商平台，并全程使用平台官方的聊天工具和支付系统进行交易，坚决不点击陌生链接付款，不通过社交软件直接向个人账户转账。请牢记“天上不会掉馅饼”，面对价格明显低于市场正常水平的商品广告，务必保持清醒，多方核实，这极有可能是骗子精心布置的陷阱。交易前，要多方查看商家的信誉度、用户评价和交易历史。对于新注册、内容空白、无真实购买记录的商家发布的异常优惠信息，要高度警惕。在最终确认收货前，切勿轻易完成转账，务必核实清楚所有交易细节。

六、“游戏代练”诈骗类

【情景再现】某学生在一款游戏内收到一条需要“游戏代练”的兼职信息，佣金 300 元。该学生便联系到对方，对方要求走正规平台完成交易，让学生在“闲鱼”发布代练订单，学生随即在“闲鱼”上架了相关订单。不久后，对方发来一个假的付款成功图片，同时要求学生向指定银行卡转 1000 元**保证金**才能登录其游戏账号。学生转账后，对方以“信誉不好”，无法付其佣金，学生便要求退还之前的 1000 元，但对方要求交 50000 元**违约金**，学生称自己没钱，对方又让该生在“闲鱼”上给一个账号充值 2200 元 Q 币，充值后对方又以其他理由称无法转账。学生发现自己被骗，共计被骗 3200 元。

【安全提示】陌生代练邀约别轻信，“保证金”“解冻费”都是坑。第三方平台要辨真伪，对方发的二维码、链接别乱扫，即便是闲鱼等正规平台，也务必通过官方 APP 内部自行联系客服，任何在交易

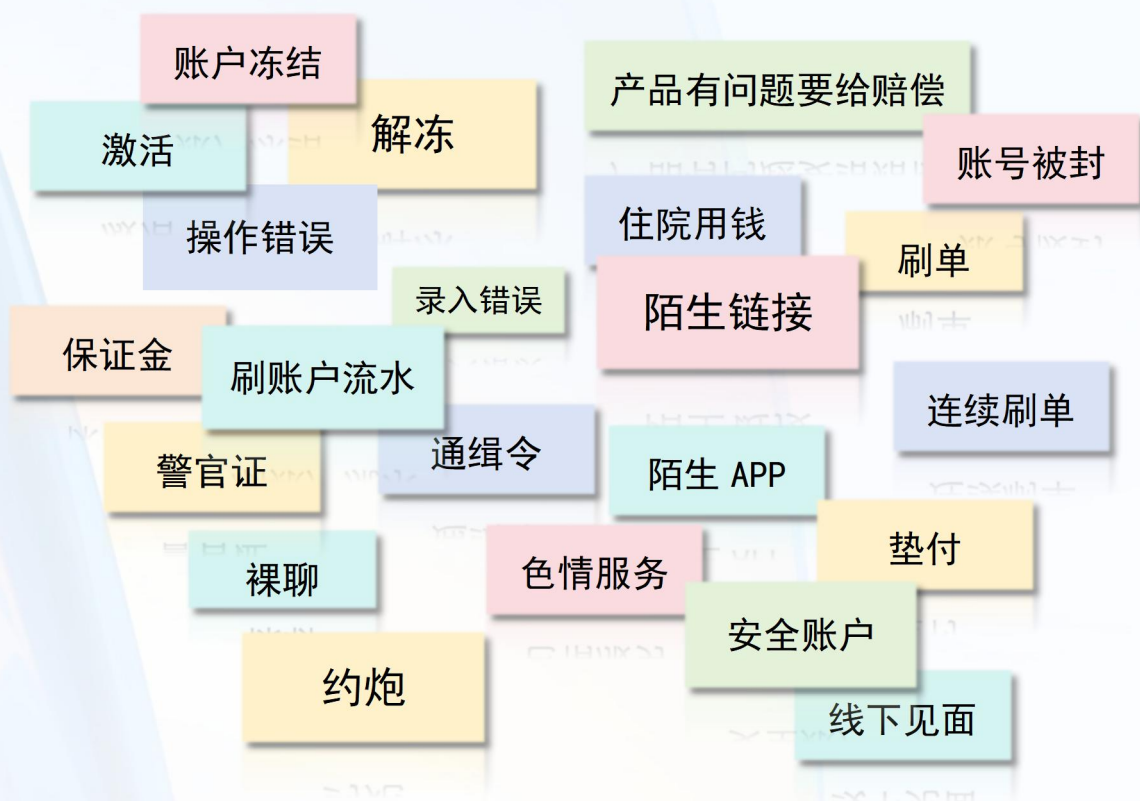
过程中突然弹出或引导你跳转至其他网站的“客服”都是骗子，万不可相信。

七、参与“抽奖、奖品折现”诈骗

【情景再现】某学生在抖音平台浏览视频时刷到一段测姻缘的视频，便添加了对方微信。经过测试后对方给出了所谓的姻缘测算结果，同时称朋友圈点赞可获得一次抽奖机会。学生便花费 600 元在指定小程序参与抽奖，抽到了一瓶香水，对方告知学生奖品可以折现 18000 元。该生希望折现，便添加了名为“深圳市和佳曼贸易公司”的企业微信，对方称领取奖品折现费需先缴纳 13% 的海关增值税，学生按要求向对方转账 2405 元，可随后被告知备注不对，学生再次向对方转账 2405 元。转账后，对方又称微信限额，让学生加其 QQ 好友，承诺会在 QQ 上给其奖品折现费。学生便添加了对方 QQ 好友，对方再次以学生账户流水预存不足为由，多次诱导其转账，学生又累计转账 15382 元。学生意识到被骗，共计被骗 20792 元。

【安全提示】切勿盲目轻信网上的中奖信息，凡是以中奖折现为由要求向陌生账户转账汇款的都是诈骗，必须牢记“所有正规的抽奖活动都不会要求你先转账”，所有需要中奖者转账、支付的都是诈骗行为。

反诈 关键信息



防范电信网络诈骗，从识别关键信息做起。发现上述关键字眼，请及时停止操作，如已转账马上报案求助。

公安报警电话：110 或 96110

校园报警电话：主校区 6997110 南校区 6938458