

# 开学季 请签收这份防诈骗指南

开学季, 诈骗分子开始暗中布局, 精心策划针对师生和家长的诈骗手段。开学期间有哪些常见的诈骗手段? 如何应对? 潍城公安分局的民警为您解答。

□本报记者 王晓萌

## 冒充公检法诈骗

如今, 诈骗分子将冒充公检法诈骗的黑手伸向了学生。诈骗分子会冒充公检法机关、政府部门等工作人员, 通过电话、微信等与学生们取得联系, 以涉嫌洗钱、快递藏毒等为由, 要求配合调查并严格保密。为阻断学生与外界联系, 诈骗分子通常要求其到宾馆等封闭空间配合工作, 诱骗其将所有资金转移至所谓“安全账户”, 从而实施诈骗。

**警方提醒:** 公检法等部门绝不会采取电话、短信、微信、QQ等形式办理案件, 不存在所谓的“安全账户”“验资账户”, 任何要求把资金转入指定账户要求开通网银、提供银行账号、密码、验证码的都是诈骗。

## 刷单返利诈骗

刷单返利类诈骗仍是变种最多、变化最快的诈骗类型, 以招募兼职刷单、网络色情诱导刷单等复合型诈骗居多。诈骗分子在骗取学生信任

后, 以“充值越多、返利越多”等为诱骗同学们做任务, 再以“连单”“卡单”等为借口诱骗学生不断转账。

**警方提醒:** 凡是打着“网络兼职”旗号, 以返佣金为诱饵要求以刷单形式做任务的都是诈骗, 此类诈骗发案量和造成的损失数均居首位, 在校大学生是主要受骗群体之一。

## 虚假征信诈骗

诈骗分子冒充银行、金融机构客服人员, 谎称学生之前开通过微信、支付宝、京东等平台的百万保障、金条、白条等服务, 或申请校园贷、助学贷等账号未及时注销, 或信用卡、花呗等信用支付类工具存在不良记录, 需要注销相关服务、账号或消除相关记录, 否则会严重影响个人征信。随后, 诈骗分子以消除不良征信记录、验证流水等为由, 诱导同学们在网络贷款平台或互联网金融App进行贷款, 并转到其指定的账户, 从而骗取钱财。

**警方提醒:** 凡是自称金融机构、贷款平台客服, 可提供网上注销账号或消除不良征信记录的都是诈骗。凡是自称京东金融平台客服, 提供消除不良个人征信记录的都是诈骗。个人征信由中国人民银行征信中心统一管理, 个人无权删除、修改。

## 购买演唱会门票诈骗

诈骗分子通过制作虚假购票网站, 或发送虚假链接, 或自称有“内部渠道票”“黄牛票”转售, 或在二手交易平台发布虚假售票信息, 或自称票务平台客服, 声称购票订单有问题需退款或重新支付, 引导学生点击虚假链接或提供银行账

户信息进行诱骗, 学生付款后无法收到门票, 会直接被诈骗分子拉黑或删除。最终, 受害人不但遭受财产损失, 还面临个人信息泄露的风险。

**警方提醒:** 购买演唱会门票务必选择正规票务平台, 不要轻信“内部渠道票”和“黄牛票”, 谨慎对待陌生链接和客服信息。

## 冒充电商物流客服诈骗

诈骗分子通过非法途径获取学生的购物信息后, 冒充电商平台或物流快递客服, 谎称学生的网购商品出现质量问题、快递丢失需要理赔或因商品违规被下架需重新激活店铺等, 诱导学生提供银行卡和手机验证码等信息, 并通过共享屏幕或下载App等方式逃避正规平台监管, 从而诱骗学生转账汇款。

**警方提醒:** 在接到自称电商物流客服电话时, 要保持警惕, 要通过官方平台或购买渠道进行核实, 切勿与陌生人开启屏幕共享功能。

## 虚假网络游戏交易诈骗

诈骗分子在社交、游戏平台发布买卖网络游戏账号、道具、点卡的广告以及免费、低价获取游戏道具、参加抽奖活动等相关信息。与学生取得联系后, 诈骗分子以私下交易更便宜、更方便为由, 诱导其绕过正规平台进行私下交易, 或诱骗学生参加抽奖活动, 再以操作失误、等级不够等理由, 要求其支付“注册费”“解冻费”“会员费”, 得手后便将受害人拉黑。

**警方提醒:** 买卖游戏账号、道具、点卡等物品请通过正规网络平台操作, 私下交易均存在被骗风险。

## 安全大讲堂

# 开工了 这些骗局千万要警惕



近期市民陆续返岗, 进入到工作模式, 而诈骗分子也“开工”了。寒亭公安分局民警发出提醒, 以下几种骗局请大家牢记于心, 避免被骗。

□本报记者 王晓萌

## 冒充客服诈骗

不法分子通过非法途径获取旅客购票信息, 伪装成航空公司工作人员凭借准确信息降低旅客防备。随后以航班故障、天气原因等虚假理由, 告知旅客需要改签或退票, 并给予赔偿, 诱使旅客进入诈骗圈套。最后则是诱导旅客登录陌生网站、点击恶意链接、下载虚假App, 或进行一系列涉及银行卡信息、验证码等敏感操作, 从而盗刷资金。

**警方提醒:** 客服来电别轻信, 先核身份再回应。收到航班延误等信息, 应第一时间通过官方渠道核实航班信息, 切记做到不点击陌生链接、不下载陌生软件、不泄露重要信息。

## 投资理财诈骗

诈骗分子冒充投资导师、金融理财顾问, 以发送投资成功假消息或“直播课”骗取受害人信

任, 再以有特殊资源、平台有漏洞等可获得高额理财回报的理由, 引诱受害人开设账户进行投资。

诈骗分子对受害人前期小额投资试水予以返利, 一旦受害人加大资金投入, 就会出现无法提现的情况。平台“投资充值”方式既包括线上的扫码、转账, 也包括将黄金、现金等贵重财物交给指定人员或运送至指定地点。

**警方提醒:** 高息理财是陷阱, 本金利息全清零。凡是标榜“内幕消息”“稳定高回报”的网络投资理财, 都是诈骗。同时, 投资方式为转账到个人账户, 与平台名称不符的对公账户, 要求将现金、黄金交给指定人员或送至指定地点的, 也都是诈骗。

## 网络交友诈骗

工作稳定后, 想来一场甜蜜的恋爱? 小心遭遇诈骗。诈骗分子会在各类婚恋、交友网站发布虚假个人信息, 待与受害人取得联系后, 便会用优秀的虚假身份和照片骗取受害人信任, 同时迎合受害人爱好以及习惯经常“嘘寒问暖”, 促使感情迅速升温。之后, 诈骗分子会以遭遇变故急需用钱、维持恋爱关系、帮忙管理投资账户等为由向受害人索要钱财, 达到一定数额后便会消失。

**警方提醒:** 恋爱甜如糖, 涉及钱财多提防。网络交友需谨慎, 虚拟世界难辨真。网恋不见面还让你转账或谈及投资赚钱的都是诈骗。

## 招工兼职诈骗

近期迎来求职潮。这时, 各类“招工兼职”诈骗也会趁机出动, 广大群众求职心切的同时, 要小心落入“招工兼职”网络诈骗陷阱。“招工兼职”网络诈骗途径主要有两种: 一种是假借网络兼职、加盟代理的名义, 伺机实施诈骗; 另一种是求职者在网络求职过程中泄露的个人信息, 给了不法分子以可乘之机。

**警方提醒:** 务工人员一定要到正式的、合法的劳务市场找工作, 千万不要随意相信黑中介、游击招工者, 更不要随意将贵重物品或财物、证件交由他人, 发觉上当受骗立即拨打110报警。

## 交通违法诈骗短信

不少人会自驾返岗, 然而假期结束回到家突然手机一震, “交通违法短信”紧跟而来, 同时还附有一个陌生链接。民警表示, 若收到违法信息提醒, 一定要注意辨别, 谨防诈骗短信。收到此类违法信息, 一旦点击链接进入虚假网站, 诈骗分子就会进一步诱导车主填写身份证号、银行卡号等个人信息, 从而实现盗刷。

**警方提醒:** 缴纳违法罚款, 是不会通过直接转账的方式进行的。不要随便点击短信中的链接。短信的内容如果不巧与你的情况相似, 应该通过官方门户网站查询, 或者致电交管部门询问。