

不贪便宜不吃亏，不捡馅饼不上当。

大学生必备
反诈知识



不要轻信涉钱信息，严防骗子乘虚得逞。

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、各种“冒充客服”诈骗

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，然后冒充淘宝客服或快递小哥拨打电话，以货物丢失主动退货、双倍赔偿为由，引导受害人一步步陷入骗局，向对方汇款。



2020年1月2日，江苏苏州市民李女士在单位接到一个陌生电话，电话里的男子自称是支付宝客服，给李女士来电是因为李女士近期在网上购买的一瓶精华液检测出有毒化学成分，平台将对客户进行全额退款。李女士一看，对方主动表示要给退款，还能准确说出自己的交易信息，便放松了警惕。对方让李女士在支付宝备用金里申请178元（商品金额）的退款金额，李女士便依言操作，在支付宝备用金里申请了500元（备用金默认申请金额）。但对方却说申请不合规定，需将多申请到的备用金转至指定账户。为方便指导李女士操作，对方让李女士下载一款会议视频软件，将她拉进一个叫“蚂蚁金服理赔中心”的二人视频会议室，视频中只能听到对方声音，看不到对方。二人挂断电话，继而用会议软件保持通讯。李女士将多申请的322元备用金转入对方提供的指定账户，对方却称归还超时，导致系统卡单，需要刷一下系统流水，不然就会上银行的征信黑名单。就这样，李女士在对方指导下，先后在平安消费金融、微信小鹅花钱、招商银行APP内贷款18万余元，并转至对方提供的指定银行账户内。直到接到银行的提醒电话，李女士才发现会议视频被对方主动切断了，惊觉自己被骗。警方初步调查发现，这起案件是一起典型的冒充客服购物退款的案件。诈骗团伙通过非法手段购买受害人购物信息，并使用这些信息联系到受害人，以“产品有瑕疵须作退款”为由，诱导受害人到各种陌生的金融平台贷款。目前，此案正在进一步侦查中。

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。(3)接到自称“卖家”或“客服”的电话说需要退款或重新支付时，当事人一定要登录官方购物网站查询相关信息，不要点击对方提供的网址链接，更不能在这些网址上填写任何个人信息。一旦发现被骗，及时向当地公安机关报案。

二、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。



2020年1月20日，江苏宿迁市民王某收到一个微信名叫邱某的人主动发信息添加好友，王某看其微信头像正是朋友邱某在某地讲话时截取的照片。因平时和邱某比较熟悉，王某没有多想，立即接受了添加微信好友的请求。过了几天，该微信号主动与王某打招呼，简短地聊了几句后，便发送文字称最近准备给上级领导送礼，想找个关系好的人帮忙转一下，希望王某代为支付18万元礼品钱，并发来一个银行卡账户。王某没有进一步核实，通过手机银行向该账户转了18万元。之后，该微信号又请王某再转一部分，并提供另一个银行账户，如此反复4次，直至王某已无现金。过了几天，王某到邱某办公室询问借钱之事时，方知被骗。警方调查发现，这起案件是一起典型的冒充熟人诈骗。诈骗分子利用受害人熟人之间缺乏戒备心的心理，假借某种事由要求汇款转账。案件正在进一步侦查中。

民警温馨提示：(1)无论是谁，通过微信、QQ、短信让你转账汇款时，一定要用电话、视频等方式核实，切勿盲目转账。一旦发现被骗，请及时报警。(2)在聊天中如涉及汇款，一定要谨慎，以防钱财两空。

三、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，并以此作为诱饵，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。

2020年10月初，上海市民唐女士被拉入一兼职刷单微信群，群内自称客服的人员主动加了唐女士微信，忽悠唐女士向其提供的一网络博彩平台充值刷流水，并承诺只要根据客服提示操作肯定能赚钱。抱着试一试的心态，唐女士下载了客服推送的APP，并充值98元试水。在客服提示下，唐女士果然赚了钱，98元变成了224元，并顺利提现。接着，唐女士加大投入，又一次获利提现10488元。看着账户里的数字越来越大，唐女士投入的本金也越来越多，直到累计充值108万元，准备将盈利的120万元全部提现时，她才发现自己的账户不能提现了。唐女士连忙联系所谓的客服，却被拉黑，继而踢出群。2021年1月14日警方对该犯罪团伙实施收网抓捕，11名团伙骨干成员在多地悉数落网。目前，王某等11名犯罪嫌疑人已被依法刑事拘留，案件正在进一步侦查中。办案民警表示，诈骗分子通常会冒充快递员，以电话打不通为由添加好友，一旦发现有人通过微信申请，便将对方拉入兼职刷单群。接着，引诱这些潜在被害人参与所谓的网络博彩刷单。而博彩输赢和资金进出皆由该团伙控制，这也是唐女士下注每次都能赢钱的原因。诈骗分子还会根据被害人的“人设”来控制“诱饵”的金额。

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)不要轻易点击或扫描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。

四、游戏中的“诈骗术”

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。



2020年12月29日，浙江绍兴的小陈玩手机游戏时，看到游戏社区里有人投放“有充值渠道可以低价充值游戏币”的广告，便联系对方，并在对方指导下添加支付宝账号、打开对方给的网址链接，进入名为“付品阁”的网站。对方让小陈转账给该网站提供的银行账户充值，小陈觉得这个网站看上去挺靠谱，里面的钱均可以提现，便充值了200元。对方称200元的商品已卖完，只有700元的商品了，于是小陈又充值了500元。此时，客服又说因小陈之前未完善身份信息，账户里的钱均被冻结，需要再充值3倍金额才能解冻，于是小陈又充值2100元。如此反复多次，对方以多种理由让小陈交钱解冻账号，直到小陈醒悟过来。

民警温馨提示：(1)为电脑安装安全防护软件，从正规网站下载网游插件，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。(4)买卖“游戏币”、游戏账号时，不要轻信“低价充值”和“高价收购”，不要轻易点击对方提供的网址链接，一定要在官网上进行操作。一旦发现被骗，请及时报警。

五、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。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。2、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。3、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约定的上线两万元时，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。(4)注销“校园贷”，2020年1月9日，浙江某大学的小杨接到一个电话，对方自称是支付宝客服，要帮小杨注销“校园贷”记录，做结清证明。正在做实验的小杨直接挂断了电话。

过了不久，对方又打了过来，并说出小杨的许多个人信息。小杨将信将疑，称自己从未办理过贷款，但对方说可能是小杨朋友或者学校的人帮忙办理的。由于对方所说的信息非常准确，并说只要按其说的操作，系统就会进行统一升级，小杨的贷款记录就会注销，个人征信也不会受影响。于是，小杨在对方的指导下，开启腾讯会议并共享屏幕，向多个网贷平台申请贷款，并将贷款分别转到了4个陌生账户里。事后小杨才醒悟过来，经向支付宝官方客服联系才知道自己并没有“校园贷”记录，发现自己贷款损失近4万元。

民警温馨提示：(1)大学生要树立正确的消费观，要充分认识到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，利息和违约金非常高；(3)要积极学习金融和网络安全知识，远离不良网贷行为。(4)凡是声称你有“校园贷”记录需要注销、否则会影响征信的，都是诈骗，切勿转账汇款。一旦发现被骗，请及时报警。

如遇诈骗事件请第一时间拨打全国反诈中心电话：96110，并告知学校保卫处：86928110。

(我们承诺已经通读知晓以上内容，并在接下来的日常生活中引以为戒谨防各类通讯网络诈骗，保障自身的财产安全)

() 幢 () 寝室全体寝室成员签字：

保卫处、学生处宣

更多反诈内容请微信关注以下公众号



杭州防诈骗



浙经院安全驿站