反诈拒赌　安全支付

《防范电信网络诈骗宣传手册》

为落实党中央、国务院关于打击治理跨境赌博、电信网络诈骗的决策部署，助力推动全社会形成防范电信网络诈骗、跨境赌博及相关黑灰产业的宣传浪潮，大幅提高反诈拒赌知识社会知晓率，显著增强群众反诈拒赌能力，明显增强企事业单位和个人依法开立和使用账户的法律意识，上海农商银行按照中国人民银行、公安部、银保监会、中国支付清算协会“反诈拒赌，安全支付”相关要求，在全行范围内积极开展反诈拒赌宣传活动。

防范电信网络诈骗
宣传手册

国家反诈中心

国家反诈中心提醒

1.凡是“不要求资质”，且放款前要先交费的网贷平台，都是诈骗！
2.凡是刷单，都是诈骗！
3.凡是通过网络交友，诱导你进行投资或赌博的，都是诈骗！
4.凡是网上购物遇到自称客服说要退款，索要银行卡号和验证码的，都是诈骗！
5.凡是自称“领导”、“熟人”要求汇款的，都是诈骗！
6.凡是自称“公检法”让你汇款到“安全账户”的，都是诈骗！
7.凡是通过社交平台添加微信、QQ拉你入群，让你下载APP或者点击链接进行投资、赌博的，都是诈骗！
8.凡是通知中奖、领奖，让你先交钱的，都是诈骗！
9.凡是声称“根据国家相关政策需要配合注销账号，否则影响个人征信的”，都是诈骗！
10.凡是非官方买卖游戏装备或者游戏币的，都是诈骗！

诈骗手法千变万化，但万变不离其宗。要牢记“三不一多”原则：

未知链接不点击　　陌生来电不轻信

个人信息不透漏　　转账汇款多核实

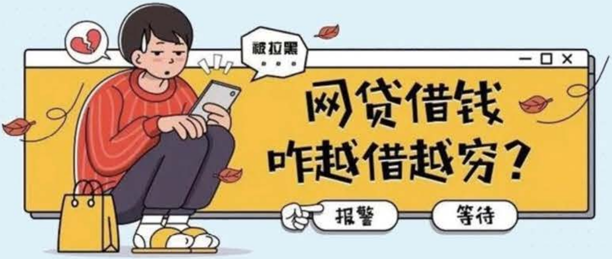
目　录

一、网络贷款诈骗
二、刷单返利诈骗
三、“杀猪盘”诈骗
四、冒充电商物流客服诈骗
五、冒充熟人或领导诈骗
六、冒充“公检法”诈骗
七、虚假投资理财诈骗
八、虚假购物诈骗
九、注销“校园贷”诈骗
十、网络游戏虚假交易诈骗

网络贷款诈骗

典型案例

2020年11月27日，马某接到一自称某贷款平台客服的陌生电话，对方以**无需征信、无需抵押、快速放款**为由，诱骗马某添加客服QQ，并下载“某某E贷”APP。马某在该APP申请5万贷款额度后却无法提现，对方谎称马某银行卡号填写有误，导致账号被冻结，需要交纳**解冻费**才可提现，同时承诺解冻后交纳的解冻费会全额退还给马某。马某因急于贷款，遂按要求向对方转账5000元解冻费，却还是无法提现，对方又以验证还款能力、刷流水等理由，陆续要求马某多次向对方账户转账**共计8万余元**，后将马某拉黑。



国家反诈中心提醒

办理贷款一定要到正规的金融机构办理，正规贷款在放款之前不收取任何费用！

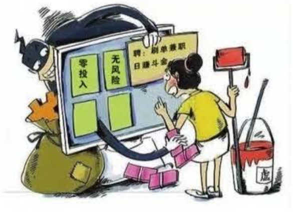
切记：任何网络贷款，凡是在放款之前，以交纳“手续费、保证金、解冻费”等名义要求转款刷流水、验证还款能力的，都是诈骗！

刷单返利诈骗

易受骗群体

学生群体、待业群体等。

作案手法



第一步：

骗子通过网页、招聘平台、QQ、微信等发布兼职信息，招募人员进行网络兼职刷单，承诺在交易后立即返还购物费用并额外提成，并以“零投入”“无风险”“日清日结”等方式诱骗你。

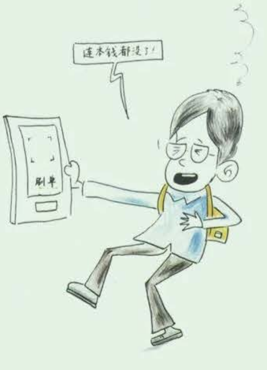
第二步：

刷第一单时，骗子会小额返款让你尝到甜头，当你刷单交易额变大后，骗子就会以各种理由拒不返款，并将你拉黑。

刷单返利诈骗

典型案例

张某是某高校大二**学生**。一日，张某在QQ群看见一条招聘网络兼职的信息，称有一份兼职刷单赚取佣金的工作，并且留下了QQ号，通过QQ与“客服人员”联系后接到了第一笔刷单任务。对方给了张某一个某知名购物网站的**购买链接**，要求加入购物车、不付款，直接截图。张同学发送购物截图后，对方发给张某一个**支付宝二维码**，让其扫码支付。张某支付完后，对方通过支付宝返还了本金和“佣金”。随后，张某按照对方的指令继续刷单，连续刷了5单之后，张某不但没有收到“佣金”，连本金的**5万元**都没有收回。



国家反诈中心提醒

骗子往往以兼职刷单名义，先以小额返利为诱饵，诱骗你

投入大量资金后，再把你拉黑。

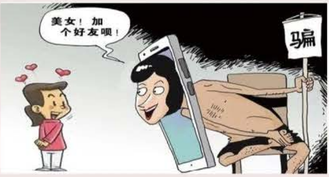
切记：所有刷单都是诈骗，千万不要被蝇头小利迷惑，千万不要交纳任何保证金和押金！

“杀猪盘”诈骗 3

易受骗群体

大龄未婚、离异单身男女，女性被骗比例较高。

作案手法

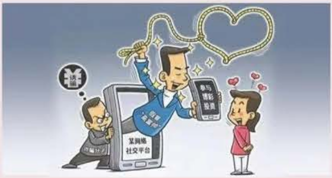


第一步：

“寻猪”。骗子伪装为成功人士，通过婚恋网站、网络社交工具寻觅、物色诈骗对象，与你聊天交友，确定男女朋友、婚恋关系，甚至远程下单赠送昂贵礼品，取得信任。

第二步：

“诱猪”。骗子推荐博彩网站、赌博APP，谎称系统存在漏洞、有内幕消息、有专业导师团队等，只要投注就能稳赚不赔，甚至先提供一个账号让你帮忙管理，进行体验，从而诱导你投注。

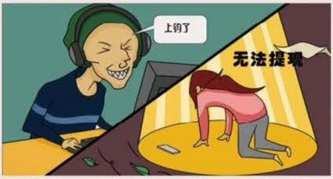

诱骗
参与博彩投资
某网络社交平台
诈骗分子

第三步：

“养猪”。当你少量投注时，回报率很高，提现很快，让你逐渐产生贪婪的欲望，继续加大投注金额。

第四步：

“杀猪”。在你投入大额资金后，发现网站、APP账户里的资金无法提现，或在投注过程中，全部输掉。此时，才发现对方已将自己拉黑。



“杀猪盘”诈骗

3

典型案例

阿芬（女，40岁，大学专科学历，财务咨询公司员工），通过某交友软件认识了**一名男子**，双方聊得很投机，便互相加了微信，对方还远程下单给阿芬送鲜花、定外卖。聊了20多天之后，对方发来一个网址，告诉阿芬这是一个**博彩网站**，能通过后台操作赚汇率的差价。一开始男子让阿芬操作自己的账号来玩，但是每次在网址内买大或者买小都提前告知阿芬。头几天，阿芬操作账户都是赢钱的，几天之后阿芬自己也开通了账户，向客服发送的银行卡号充值了3万元，不但赢利，还能提现。在相信了对方后，阿芬陆续给对方的“某某网络科技有限公司、某某小妹广告制作部”等账户**充值了276万元**，等再要提现时，才发现网站无法登陆，微信被**拉黑**，共计被骗276万元。

国家反诈中心提醒

素未谋面的网友、网恋对象推荐你网上投资理财、炒数字货币（虚拟币）、网购彩票、博彩赚钱的都是骗子！你当他（她）是神，他（她）当你是猪！

切记：始于网恋，终于诈骗！网友教你投资理财的都是诈骗！

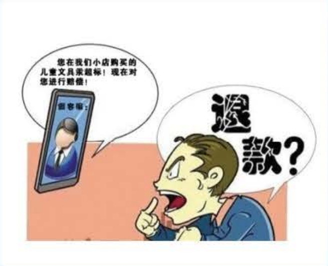
冒充电商物流客服诈骗

4

易受骗群体

经常进行网上购物的群体。

作案手法

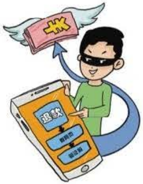


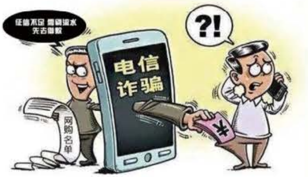
第一步：

骗子冒充购物网站客服工作人员给你打电话，说出通过非法渠道获取的你的购物信息和个人信息，谎称你购买的产品质量有问题，需要给你进行退款赔偿。

第二步：

诱导你在虚假的退款理赔网页填入自己的银行卡号、手机号、验证码等信息，从而将你银行卡内的钱款转走，或者是利用你对支付宝、微信等支付工具中借款功能的不熟悉，诱导你从中借款，然后转给骗子。



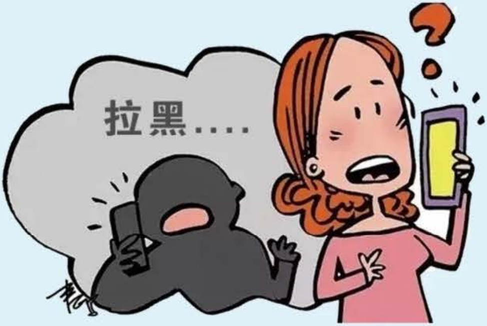


4

冒充电商物流客服诈骗

典型案例

2020年11月，市民王小姐接到电话，称其在网上购买的奶瓶**有质量问题要给其退款**，王小姐加了对方QQ后，对方发来一条**链接**，点开后页面显示为退款中心，并要求填写**身份证号、银行卡号、预留手机号、余额等信息**，在填完相关信息后，骗子跟王小姐索要手机收到的验证码，王小姐在提供验证码后发现**银行卡内钱款被划走**。



国家反诈中心提醒

当有网络卖家或者客服主动联系为你办理退货退款时，一定要小心！

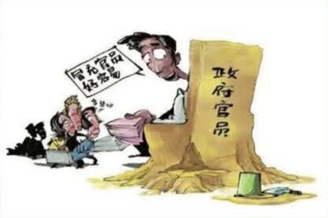
切记：正规网络商家退货退款无需事前支付费用，请登录官方购物网站办理退货退款，切勿轻信他人提供的网址、链接！

冒充熟人或领导诈骗 5

易受骗群体

行政单位、企事业人员等群体。

作案手法

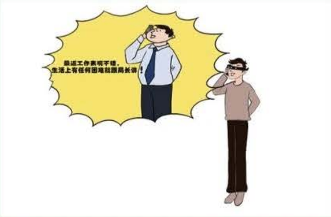

冒充官员
好容易
政府官员

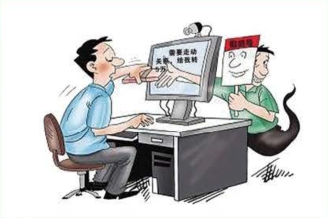
第一步：

“领导”主动添加好友。骗子通过非法渠道获取你的手机通讯录和相关信息，冒充相关“领导”通过微信或QQ添加你为好友。

第二步：

“暖心关怀”骗取信任。骗子用关心下属的口吻，降低你的戒备之心，甚至还会主动提出帮助你解决困难，让你对个人事业发展浮想联翩。.


最近工作表现不错，
生活上有任何困难就跟局长讲！



第三步：

花式理由要求转账。当你感觉与“领导”更亲近时，骗子趁势而为，向你提出转账汇款的要求，转账理由多种多样，比如借钱、送礼、请客等。

冒充熟人或领导诈骗

5

典型案例

某日，赵先生的微信上收到了一条好友验证，**备注是公司李经理**的名字，通过验证后，“李经理”称该微信是他的私人

微信，可多沟通联系。一个小时后，“李经理”发微信给赵先生说**一位领导找自己借钱**，要立即将10万元钱转给领导，为避免“麻烦”，自己要将**10万元先转给赵先生**，让赵先生帮忙转给领导。在“李经理”不断催促下，赵先生没多考虑就在未收到“李经理”转账的情况下按照其提供的银行卡账号向那位“领导”**转账10万元**。晚上11时许，赵先生发现“李经理”转给自己的10万元依然没有到账，于是电话联系李经理，李经理告知**根本就没有这回事**，赵先生才意识到被骗。

国家反诈中心提醒

如遇到自称领导通过微信、QQ等添加好友，并要求转账汇款时一定要提高警惕。

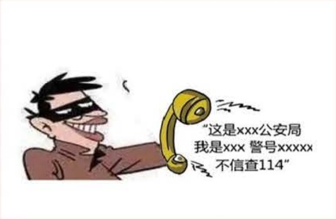
切记：凡接到领导要求转账汇款或借钱的要求时，务必通过电话或当面核实确认后再进行操作！

冒充“公检法”诈骗 6

易受骗群体

防范意识较差的各个群体，女性和老人被骗的机率更高。

作案手法

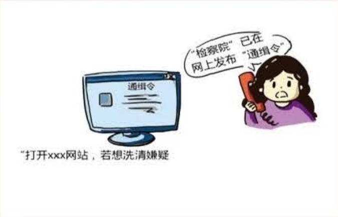

"这是xxx公安局
我是xxx 警号xxxxx
不信查114"

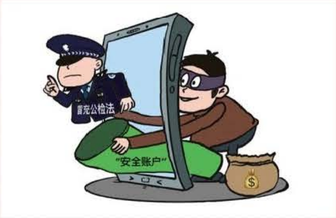
第一步：

骗子通过非法渠道获取你的个人身份等信息，冒充公检法工作人员给你打电话。

第二步：

编造你涉嫌银行卡洗钱、拐卖儿童犯罪等理由，同步发送伪造的公检法官网、通缉令、财产冻结书等，对你进行威逼、恐吓，以使你相信和就范。


"检察院"已在网上发布"通缉令"
通缉令
"打开xxx网站，若想洗清嫌疑



第三步：

诱导你去宾馆等独立空间进行深度洗脑，以帮助你洗脱罪名为由，要求你将名下账户所有钱款转账至所谓的"安全账户"，从而达到诈骗目的。

冒充"公检法"诈骗

6

典型案例

某日，市民李女士接到**自称市公安局**的林警官打来的电话，称其涉嫌诈骗并准确说出其身份信息，要求添加李

女士QQ进行调查。骗子将所谓的**“通缉令”**发给了李女士，期间不断恐吓李女士**“态度要好、要保密！”**，不能告诉任何人。接下来骗子要求李女士把手机调成飞行模式，找到一家宾馆，连上WIFI，按照对方指示将银行卡内**30多万元**全部转到指定的“安全账户”。三天后，当李女士再联系对方时，发现已经被对方**拉黑**，而拨打电话过去，对方的电话已无法接通，李女士这才意识到自己被骗。

国家反诈中心提醒

公检法机关会当面向涉案人出示证件或法律文书，绝对不会通过网络点对点地给违法犯罪当事人发送通缉令、拘留证、逮捕证等法律文书！

切记：公检法机关绝对不会通过电话、QQ、传真等形式办案，也没有所谓的“安全账户”，更不会让你远程转账汇款！

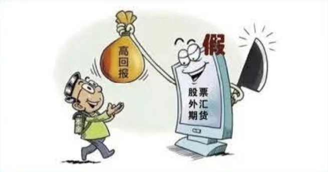
虚假投资理财诈骗

7

易受骗群体

热衷于投资、炒股的群体。

作案手法

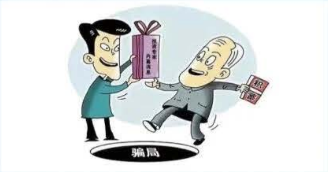


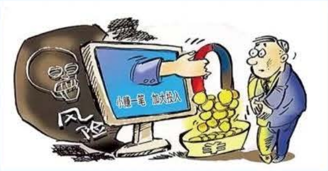
第一步：

骗子通过网络社交工具、短信、网页发布推广股票、外汇、期货、虚拟货币等投资理财的信息。

第二步：

在与你取得联系后，通过聊天交流投资经验、拉入“投资”群聊、听取“投资专家”、“导师”直播课等多种方式，以有内幕消息、掌握漏洞、回报丰厚等谎言取得你的信任。


投资专家
内幕消息
积蓄
骗局

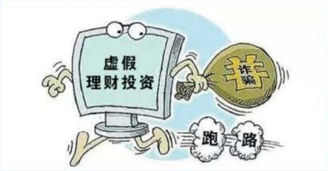


第三步：

诱导你在其提供的虚假网站、APP投资，初步小额投资试水，回报利润很高，取得进一步信任，诱导你加大投入。

第四步：

当你在投入大量资金后，发现无法提现或全部亏损，与对方交涉时，发现被拉黑，或者投资理财网站、APP无法登录。



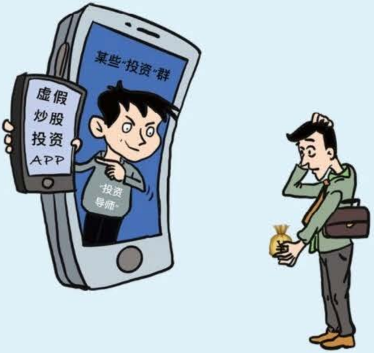
虚假投资理财诈骗

7

典型案例

陈某在网上看到一篇关于炒股的文章，感觉写得很好，就添加

了文章里发布的微信，对方将陈某拉入一个**炒股的群**。一个“股票导师”在群里进行**荐股和行情分析**，陈某看了几天后，发现群里的人按照“导师”的分析都赚到钱了，就开始根据“导师”推荐的股去**购买**，跟了几次后确实赚到钱了，陈某便加大投入。在两周时间内，陈某陆续投入**620万元**，但在提现时发现无法成功，方知被骗。


某些“投资”群
虚假炒股投资APP
“投资导师”

国家反诈中心提醒

投资理财，请认准银行、有资质的证券公司等正规途径！切勿盲目相信所谓的“炒股专家”和“投资导师”！

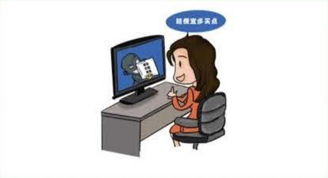
切记：“有漏洞”、“高回报”、“有内幕”的炒虚拟币、炒股、打新股、炒黄金、炒期货、博彩网站等，都是诈骗！

虚假购物诈骗 8

易受骗群体

网购群体，特别是在网购平台、微信群、朋友圈等网络购物渠道淘货的人群。

作案手法

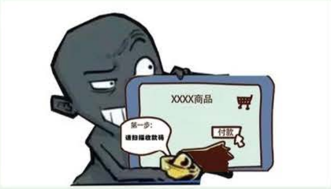


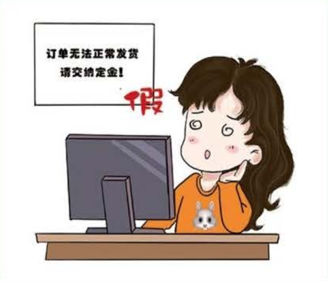
第一步：

骗子在微信群、朋友圈、网络购物交易平台上发布低价出售物品的信息。

第二步：

你发现低价销售的物品，与其聊天沟通时，对方要求你添加QQ、微信私下转款、扫码交易。




订单无法正常发货
请交纳定金！
假

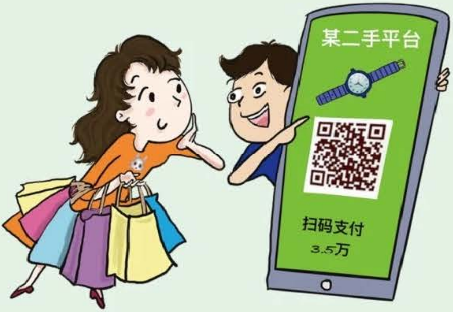
第三步：

骗子会让你先转款但不发货，还会编造收取运费、货物被扣要交罚款、收取定金优先发货等理由，一步步诱骗你转账汇款，随后把你拉黑。

虚假购物诈骗 8

典型案例

于某在某二手购物平台浏览时，发现有一款自己**“心仪已久”的九成新手表**，价格远低于同类商品，遂添加对方QQ取得联系。在一番讨价还价后达成共识，但对方要求**不能在平台付款**，要通过对方在QQ上发来的**二维码**扫码付款。于某急于得到心仪的手表，遂通过对方在QQ上发来的二维码扫码支付货款3.5万元，后被对方**拉黑**，遂报警。


某二手平台
扫码支付
3.5万

国家反诈中心提醒

通过微商、微信群交易时，一定要详细了解商家真实信息，确定商品真实性，多方面综合评估。交易时最好有第三方做担保！

切记：网购时一定要选择正规的购物平台！对异常低价的商品提高警惕！

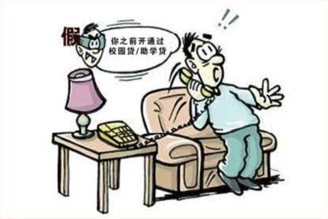
注销“校园贷”诈骗

9

易受骗群体

院校学生等群体。

作案手法

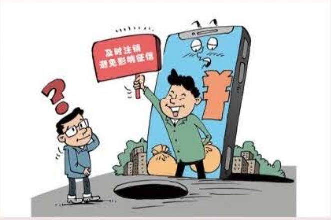


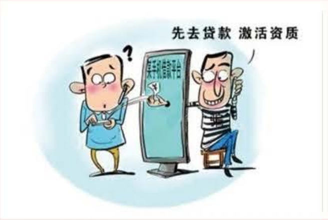
第一步：

骗子冒充网贷、互联网金融平台工作人员，称你之前开通过校园贷、助学贷等。

第二步：

骗子以不符合当前政策，需要消除校园贷记录，或者校园贷账号异常需要注销，如不注销会影响个人征信等为由，骗取你信任。


及时注销
避免影响征信


先去贷款 激活资质
某手机借款平台

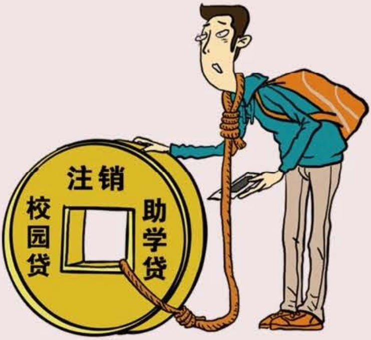
第三步：

诱骗你在正规网贷网站或互联网金融APP上贷款后，转至其提供的账户上，从而骗取钱财。

注销“校园贷”诈骗 9

典型案例

某日，小安突然接到一个自称是“**某贷款公司客服**”的电话，对方称小安在大学期间借的一笔**8000元“校园贷”**未还，现在国家正在大力整治校园贷款，如果小安再不还，将影响到个人征信。在对方的诱导下，小安向多个APP申请了贷款，最终申请到**总计2万元**的贷款并将贷款转到对方账户里。随后**无法联系对方**，发现自己被骗。



国家反诈中心提醒

不要轻信陌生人声称你之前有“校园贷”行为，更不要对“征信会受影响”信以为真。

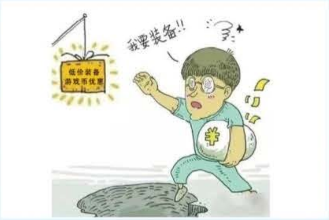
切记：如遇以“校园贷”为借口要求转账，都是诈骗！

网络游戏虚假交易诈骗 10

易受骗群体

喜爱网络游戏的群体。

作案手法

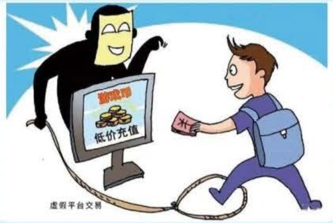

低价装备
游戏币优惠
我要装备!!

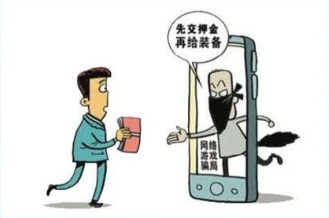
第一步：

骗子在社交平台发布买卖游戏装备、游戏账号的广告信息。

第二步：

诱导你在虚假游戏交易平台进行交易，让你以“注册费、押金、解冻费”等名义支付各种费用。


游戏币
低价充值
虚假平台交易

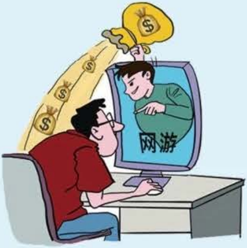

先交押金
再给装备
网络游戏骗局

第三步：

当你支付大额费用后，再联系对方时，才发现已被对方拉黑。

典型案例

毛某在玩手机游戏时，突然从窗口弹出“**低价出售游戏装备**”的消息，添加对方QQ号后，对方让毛某充值200元注册账号，毛某向对方提供的账号转账成功后，对方又让毛某再次**充值1200元**作为开通账号的押金，随后，对方对毛某说：“你现在可以用你自己注册的**账户登录**了。”在登录时突然弹出一个窗口“您的个人信息出现问题，账号被冻结”，毛某看了便立刻联系了对方，对方说：“先生，您的账户确实已被**冻结**了，现在您需要**充值6600元**才能将账号解冻。”毛某听了后，立马按照对方的提示把钱打了过去，转账成功后，毛某立马联系了对方，但这时对方已将毛某**拉黑**了。毛某这才发现自己被骗，立马报警。



国家反诈中心提醒

当在网络游戏充值、账号买卖时，一定要小心！诈骗分子会以低价充值、高价回收为由，引诱你在对方提供的虚假链接内进行交易。

切记：买卖游戏币、游戏点卡，请通过正规网站操作，一切私下交易均存在被骗风险！