

网络谣言要明辨

“实锤”“爆料”不轻传

真实案例

一则“某酒店发生命案，受害者被分尸”的微信聊天截图在网络社交平台传播，警方开展调查后，证实为网络谣言，并将造谣散布谣言的两人抓获。经侦，嫌疑人为了在聊天中制造话题，谎称自己消息灵通，将造谣信息发给朋友炫耀，后在群将二人微信聊天截图转发至微信群，造成不良社会影响。二人已被警方依法予以**行政拘留**。



互联网不是法外之地，各位网民要擦亮双眼，文明上网，理性发言。

**不造谣 不信谣
不传谣**

饭圈追星要理性

“打榜”“抢票”不冲动



我是明星，我的QQ是XXXX，大家快帮我加个吧！



不法分子以明星图片伪造QQ头像，在群聊“明星粉丝QQ群”中添加未成年粉丝为好友，虚构明星身份实施诈骗。

终于加上明星QQ啦

假明星以自己网上投票、打榜为由，将投票现金链接等称为“投票链接”，向受害者发送收款二维码或称为投票二维码。需要受害者用微信扫码并输入二维码，输入“投票链接”后完成所谓的“投票”，实则骗取财产。



手法

诈骗分子先“建鱼塘”（虚构所谓的“明星粉丝福利群”）；而后“拉人头”，想方设法诱使未成年人进粉丝群；接下来“做营销”（在群内发布“充100送888”“有渠道抢到明星演唱会门票”等虚假信息，引诱未成年人付费，实施诈骗。

防范要点

理性追星，理性消费，在粉丝群、周边群等社交平台要保持清醒的头脑，不要冲动消费或泄露个人敏感信息。家长要特别注意孩子的“偶像崇拜”现象，如果追星不当，很可能产生一系列的风险。

网游消费要当心

“扫码”“免费”不可信

真实案例

10岁的小亮在刷短视频时，看到一条可以**免费领取**游戏皮肤的视频，就添加了对方的QQ。对方让**小亮先扫描二维码**，跳转到一个**游戏服务平台**，并**下载APP**进行下一步操作。小亮在对方诱导下还把母亲的**银行卡密码**都告诉了对方。很快，小亮的母亲发现银行卡莫名转出10多万元，立即报警。



手法



不法分子散布类似“**加群领免费游戏道具**”的消息，并谎称需要扫码领取。待受害者扫描后往往会提示“**领取失败，账号被冻结**”。不法分子便会告知需**扫描付款码**进行解冻，并且运用各种话术诱导受害者**反复付款**，骗取大额钱财后立刻“消失”。

防范要点



宣称“**免费领皮肤、领道具**”很有可能是骗局，特别是需要**扫码和下载APP**的，**一定不要轻信**。受害者多为未成年人，**家长应多关心孩子使用手机情况**，**避免财产损失**。

免费不受信 扫码需谨慎 信息不泄露

网恋交友要谨慎

“周转”“救急”不信任

真实案例



李某在相亲网站认识网友叶某, 对方风趣幽默, 帅气多金, 两人互生情愫, 迅速发展成男女朋友。

叶某对李某说他在香港维护彩票票后台时发现该网站漏洞, 并指导李某赌博, 几天下来赚了2万元。

这时叶某要李某在“VIP场”玩个大的, 为以后幸福婚姻生活积攒一笔资金。李某东拼西借充值60万元, 赚了近10万元却发现不能提现, 叶某也随即消失。



手法

白富美、高富帅嘘寒问暖, 与受害者建立网恋关系, 直接以各种理由骗钱, 或者诱导受害者参与网络赌博、网上投资等。

防范要点

切勿被网络贴心暖男、温柔美女甜言蜜语冲昏头脑。

不轻信网友以“周转”“救急”“投资”等为理由的转账要求。



法治常识要加强

“涉案”“核查”不慌张

真实案例

李女士接到电话，对方自称**公安机关**，通报李女士名下**一张银行卡被犯罪嫌疑人利用，涉嫌洗钱罪**，并表示要**调查李女士名下的财产**。李女士按照对方要求添加了3个“**公检法工作人员**”的QQ号，然后把账户里所有的钱都转到对方指定的**银行卡**，配合银监会调查。李女士转账后才发现被骗。



手法



诈骗分子冒充**公检法机关工作人员**等身份，以**受害者涉嫌犯罪进行恐吓**，要求集中转账户资金到所谓的“**安全账户**”实施诈骗。

防范要点

- 1 公检法机关办案会当面向涉案人员出示证件或相关法律文书。
- 2 不会通过QQ、电话、邮件等形式办案，更不会在电话中通报当事人罪名。
- 3 公安机关不存在安全账户或核查账户，更不会让公民提现转账汇款。骗子多以非法入境、贩毒、洗钱等罪名引你入扣，不要上当。

网络兼职要注意

“刷单”“抽佣”不实际



真实案例

王女士被拉到一个微信群里，群里人给她的家刷单可赚取佣金。王女士按照对方要求操作赚取了佣金300元。后群内有人发了一个链接，让王女士下载APP赚取更多任务。王女士按照要求添加了导师好友，导师称可做大额任务，对方提供卡号让其通过转账方式进行刷单。王女士向对方指定的银行卡转账5000元后，未返本金和佣金，发现被骗。

手法

违法分子在社交平台发布刷单信息，先给受害者一至两单的小额返利，然后会派发需垫付大额资金但佣金高的刷单任务，一旦受害者垫付，对方就会以“任务未完成、资金冻结”等理由要求受害者继续垫资完成更多任务，直至受害者发现被骗。



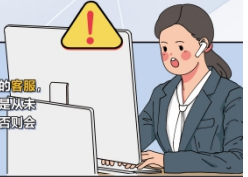
防范要点

所有刷单都是诈骗，做任务赚佣金不过是刷单诈骗的诱饵，切勿相信“免费送、轻松赚”等兼职广告，不要贪图小便宜，不要轻易点击陌生链接或扫描陌生二维码下载APP。


客服沟通要官网

“注销”“福利”不上当

真实案例




李先生您好，我是京东的**客服**，您开通**金融服务**，但是**初次使用**，需要进行**注销**，否则会影响**征信**。



李先生在指定网站确认客服工牌后放松了警惕。按照对方要求向其提供的银行账户转账，并下载了数个贷款软件，贷款3000元，对方称都是虚拟的，只是为了注销走流程。后续该客服又让李先生用APP贷款十万元转到指定账户，李先生才发现被骗。

手法



通过冒充金融平台客服来电，以注销金融账户或调整利率为借口，通过屏幕共享等手段，掌握受害者操作过程，同时窥探输入的密码和验证码等重要信息。

防范要点

凡是接到要求注销金融账户或调整利率的陌生电话要警惕，应独立登录官方网站核实。如果您有过贷款经历，只要按时还清贷款，就不会影响征信。

网络投资要思量

“稳赚”“暴利”不正常

李先生被拉入一个投资群，有人称投资“平安金融”能返还全部投资金额并获取高额利息。李先生点击群内链接下载APP，并按投资顾问要求向指定账户转账共计十余万元。当李先生想进行提现时，发现提现失败，APP客服称李先生操作失误，需要再次进行转账。李先生才意识到被骗。



高回报

低风险

稳赚不赔

手法



通过社交平台发送二维码、链接寻找目标，以内幕消息、高额回报等字眼诱导受害者下载虚假APP平台，以群内成员为托，发布赚钱盈利的消息引诱受害者在平台投资充值，当受害者想提现时客服则以系统维护、提现额度小等理由要求继续投注。

如何防范

有理财需求一定要通过正规渠道进行投资，凡是承诺不合乎常理的高回报率的，一定是有问题的。陌生链接不要点，陌生二维码不要扫，不要相信稳赚不赔的博彩、理财宣传，远离“非法荐股”。

网络安全口诀

要牢记



- 密码口令要多样 “生日”“连号”不妥当
- 陌生邮件要确认 “收集”“统计”不轻信
- 软件下载要正规 “破解”“盗版”不理睬
- 公共Wi-Fi要鉴别 “免验”“无密”不连接
- 人脸识别要规范 “偷拍”“倒卖”不能办
- 智能家居要警惕 “远程”“监控”不保密
- 隐私数据要仔细 “过度”“敏感”不同意
- 扫码点餐要慎利 “关注”“强制”不合理
- 网络谣言要明辨 “实锤”“爆料”不轻传
- 饭圈追星要理性 “打榜”“抢票”不冲动
- 网游消费要当心 “扫码”“免费”不可信
- 法治常识要加强 “涉案”“核查”不慌张
- 网络诈骗要留意 “刷单”“抽佣”不实际
- 网恋交友要谨慎 “周转”“救急”不信任
- 客服购赠要自问 “注销”“福利”不上当
- 网络投资要思量 “稳赚”“暴利”不正常

北京市民 网络安全意识体检



您的网络安全
意识达标了吗？

扫码体检试试吧！



感谢您的支持与参与！
让我们一起创造更安全的网络空间