

01 五大高发诈骗类型及防范指南

冒充电商物流

易受骗群体 ▶ 经常网上购物、对网购退费流程不熟悉的群体

作案手法

冒充身份 ▶ 诱导配合 ▶ 实施诈骗

典型案例:周女士网购了一件衣服,几天后,她接到自称是物流客服的电话,对方声称由于自己的失误,错将包裹丢失,要通过官方支付平台给她进行三倍理赔。随后,周女士添加了这位“客服”的好友,对方以“协助操作”名义要求下载会议软件并开启屏幕共享功能。对方引导周女士逐个点击银行App,并进行操作,没过多久,周女士收到银行发来的转账短信,其名下银行卡陆续转出4笔资金,共计损失13万元。

警方提示

接到自称电商、物流客服电话时,务必到官方平台核实。

切记

正规网络商家退款无需事前支付费用,切勿随意打开屏幕共享功能,切勿轻易点击来源不明的网址链接,更不要随意填写银行卡密码、短信验证码等信息。

虚假购物

易受骗群体 ▶ 喜欢在网购平台、微信群、朋友圈等渠道淘货或查找有关服务的群体

作案手法

寻找目标 ▶ 虚构交易 ▶ 实施诈骗

典型案例:李女士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,并向李女士发送了身份信息和经营资质,以此获取了李女士的信任。随后对方方向李女士提供了支付二维码,李女士扫码支付后,对方又声称还有其他商品代购名额,而且优惠力度很大,李女士便继续转账让对方帮忙代购。几日后李女士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。

警方提示

网上购物一定要选择正规的购物、服务平台。

切记

对异常低价的商品要提高警惕,避免脱离官方平台进行私下交易。

虚假投资理财

易受骗群体 ▶ 有一定收入、资产,且有投资需求的群体

作案手法

寻找目标 ▶ 怂恿投资 ▶ 实施诈骗

典型案例:李先生在微信公众号阅读投资理财类文章后,扫码加入名为“投资-特训营”的群聊,并通过群内指引添加了自称“基金经理”的客服人员。该客服发送安装包要求李先生下载了指定的投资平台软件,并以“股票推荐”的名义诱导李先生向平台转账充值。初期账户持续显示盈利,面对账户余额不断增长,李先生放松警惕持续追加资金投入。数日后,该投资平台突然无法登录,客服人员也将其拉黑,李先生才发现被骗,最终造成82万元损失。

警方提示

不要轻信非正规渠道推荐的投资理财项目。

切记

凡是宣称“掌握内幕消息”高额回报”“稳赚不赔”的网络投资理财,都是诈骗。

刷单返利

易受骗群体 ▶ 学生、宝妈、待业、兼职群体

作案手法

前期引流 ▶ 小额返利 ▶ 实施诈骗

典型案例:张女士在浏览短视频时下载了评论区推荐的所谓“赚钱软件”,注册后平台客服以“刷单返利”为由诱导其垫资购物。初期张女士投入392元获得26元返利,随后客服提供支付二维码,要求其分七次扫码转账1344元,将获得204元佣金。张女士完成转账后,客服以做错任务为由,声称需要重新转账才能获得之前的返利,于是张女士按照客服要求再次向对方转账7600元。张女士照做后,对方又谎称账户因操作异常被冻结,需要继续充值才能解冻,张女士在多重话术诱导下连续转账,最终累计损失14万。

警方提示

“刷单、刷信誉”本身就是违法行为,并非正当兼职。

切记

不要被蝇头小利诱惑,不要轻信网络上高额报酬的兼职刷单信息,找兼职一定要通过正规渠道,所有刷单都是诈骗。

虚假征信

易受骗群体 ▶ 有贷款需求、征信有问题难以正常申请贷款的群体

作案手法

引流推广 ▶ 洗脑引导 ▶ 骗取钱财

典型案例:王先生在网上添加一陌生网友,对方称可以帮助其办理贷款,王先生随即向其咨询贷款流程。对方方向王先生索要了相关个人信息和放款银行账户信息,随后便称王先生的贷款资质不足,提供的银行账户流水没有达到放款要求,声称可以帮助王先生免费“刷流水”。王先生便按对方指示分多次向指定账户转账共计5.2万元,但对方始终以各种理由拖延放款并要求继续转账。最终,王先生发现该网友失联,方知上当受骗。

警方提示

如有贷款需求,建议通过正规渠道办理,不要轻信网络贷款广告,个人征信由中国人民银行征信中心统一管理,任何单位和个人都无权删除修改。

切记

凡是在放款前要求缴纳手续费、保证金等费用,或诱导进行“刷流水”转账操作的,都是诈骗。

三不一多

不轻信 不透露 不转账 多核实

三问三查

问来源 问资质 问风险 查官方 查备案 查口碑

02 防跨境电诈利器



防范境外诈骗,若无跨境通话需求,轻松设置屏蔽!移动、联通、电信、广电四大运营商均支持通过官方App、微信公众号/小程序、拨打客服电话或前往营业厅,免费关闭境外来电。立即操作,守护财产安全!

中国电信

★青语1

第一步:第一步:打开微信,搜索进入“天翼防骚扰”公众号绑定手机号,点击底部菜单栏“更多服务”-“境外电话免打扰”

第二步:点击“立即开通”

拦截开关开启拦截



★青语2:发送短信至10001

发送至	拦截境外来电	拦截境外短信	接收境外来电	接收境外短信
10001	DGDHLJ	DGDXLJ	TDDHLJ	TDDXLJ

中国移动

★青语1

第一步:打开微信,搜索进入“中国移动高频骚扰电话防护”公众号点击底部菜单栏选择“电话防护”-“骚扰拦截设置”



第二步:进入骚扰拦截设置页面找到“国际及港澳台号段拦截”开关点击打开,开启后将显示“操作成功”系统将开始自动为您拦截此类来电



★青语2:发送短信至10086

发送至	拦截境外来电	拦截境外短信	接收境外来电	接收境外短信
10086	QXGJLH	QXGJDX	KTGJLH	KTGJDX

中国联通

★青语1

第一步:微信搜索公众号“联通助理”绑定手机号,点击底部菜单栏“安全管家”选择“来电防护”



第二步:点击“国际电话拦截”打开“国际电话拦截”开关



★青语2:发送短信至10010

发送至	拦截境外来电	拦截境外短信	接收境外来电	接收境外短信
10010	GBGJLH	GBGJDX	KTGJLH	KTGJDX

中国广电

★青语1:在微信小程序中,找到“中国广电营业厅”选择“业务大厅”→“服务”→“国际来话”→“国际来话拦截”然后开启拦截功能



★青语2:发送短信至10099

发送至	拦截境外来电	拦截境外短信	接收境外来电	接收境外短信
10099	KTGLLJ	KTGDLJ	QXGLLJ	QXGDLJ



反需要全民
诈共同参与



扫码观看
防范电信网络诈骗
宣传手册(2025版)

03 反诈关键词

屏幕共享

屏幕共享是指通过网络将一台设备(如电脑、手机)的屏幕画面实时传输给其他设备或用户的技术。在电信网络诈骗中,诈骗分子会诱导受害人下载具有屏幕共享功能的App,利用屏幕共享功能获取受害人的账户信息、银行卡号、验证码等,从而骗取钱款。



警方提示

在未确认对方身份和目的前,切勿随意点击对方发来的下载链接或开启屏幕共享,在涉及资金操作时需格外谨慎。

AI换脸

AI换脸诈骗指利用人工智能技术将他人面部合成到虚假视频或图片中,冒充亲友、领导或公众人物实施诈骗。常见手法包括伪造身份索要钱财、虚假宣传或勒索,因逼真度高极易迷惑受害者。需警惕异常转账要求,通过多重验证防骗。



警方提示

提高安全防范意识,防止个人脸部信息被非法获取利用。妥善保管个人信息,把好个人信息保护的第一道关。

刷单

刷单做任务是一种虚假交易行为,通常指商家或个人通过组织“刷手”进行虚假的商品或服务交易,以达到提升店铺销量、信誉、排名等目的,在刷单诈骗中,诈骗分子通常以刷单做任务为由诱导受害人进行转账,前期给予小额返利,当受害人大额转入资金后实施诈骗。

警方提示

刷单就是诈骗!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。

快递引流

快递引流是指诈骗分子利用快递包裹作为媒介,通过在快递包裹里附加传单或小礼品吸引受害人注意,引导受害人扫码添加联系方式再将其拉入群聊中,为下一步实施诈骗进行准备。



警方提示

不要随意扫描快递里的二维码,遇到邀请进群、转发可领取礼品等情况,务必要高度警惕。

04 法律知识

刑法-帮信罪

帮助信息网络犯罪活动罪

《刑法修正案(九)》增设帮助信息网络犯罪活动罪,针对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、支付结算等帮助的行为独立入罪。

惩戒办法-电信惩戒

惩戒范围

电话卡、物联网卡、电信线路、短信端口等电信业务,以及存在涉诈风险的互联网账号功能及业务等。

惩戒措施

限制存量业务使用,不得办理新业务。



反电信网络诈骗法-违法行为

超量办理电话卡、银行卡、支付账户

严重后果

异常开办卡账户将被拒绝,已办理的账户可能被冻结

出售、提供个人信息;帮他人通过虚拟货币等方式洗钱

严重后果

视为诈骗同伙,依法追究刑事责任

制造、买卖或使用改号软件、GOIP、批量账号等非法设备软件

严重后果

为诈骗提供技术支撑,是重点打击对象

出租、出借、买卖自己的电话卡、银行卡、微信/支付宝账号

严重后果

一经发现,所有账户功能将被限制(暂停非柜面、限制入网等)

帮他人进行人脸识别或实名认证,冒充他人开立账户

严重后果

承担法律责任,并可能被记入信用记录



反诈防骗 ANTI FRAUD STRATEGY

全民反诈 你我同行

你没被骗只是因为
还没遇到适合你的骗局



云南省通信网络保障中心
云南省互联网协会