

静海区电信网络诈骗真实案例精选

近年来，电信诈骗案件持续多发，不法分子不断翻新犯罪手法，利用通讯和网络形式，紧跟社会热点，精心设计骗术，针对不同群体量身定做、步步设套，对受害人进行欺骗、引诱、威胁、恐吓，严重危害人民群众财产安全，扰乱正常生产生活秩序。针对我区今年以来发生的电信网络诈骗案件情况，静海公安选择有代表性的案例编辑成册，以案说法，提醒人民群众防范电信网络诈骗，切实提高防范意识，护好自己的钱袋子。

一、网络兼职刷单诈骗

兼职刷单诈骗案件作案目标以学生、家庭主妇等年轻人为主。犯罪分子利用短信、网络等平台发布以通过**刷单帮助提高商家信誉**的虚假信息，骗取被害人信任，让其在网上购买指定的物品，犯罪分子承诺交易成功后将按一定的比例返还给刷单人，刷单人可以得到高额回报并且能提高网店信誉，诱骗刷单人不断刷单，但以各种理由拒绝返还本金和报酬，直到被害人意识到被骗后，犯罪分子将被害人联系方式拉黑，完成诈骗。

案例：2020年3月份，我区居民刘某（匿名）因疫情赋闲在家，想利用空闲时间增加收入。其通过微信好友介绍，添加了一名商家QQ号，对方以网络刷单可返本金及佣金为由，要求刘某通过手机网银向对方提供的银行卡转账。刘某先后向对方转账43万余元。后发现被骗，对方却已失联。

防范提示：1. 做兼职找工作时，要核对对方公司信息，“天

上不会掉馅饼”，正规的工作是**不需要**在上岗前缴纳**押金、保证金、诚信金**的。

2. 要对招工方的资质以及所做工作的性质进行全面的了解，千万不能抱着轻松挣大钱的心态，对自己的**身份信息**要有保护意识，特别是涉及转账汇款等相关业务时，要注意维护好自己的权益。

3. 遇到网络刷单就是遇到诈骗，要及时报警。

二、杀猪盘诈骗

杀猪盘，网络流行词，主要是指通过婚恋平台、社交软件等方式寻找潜在受害者，通过发展感情取得信任，然后将受害者引入博彩、理财等诈骗平台进行充值、骗取受害者钱财的骗局。杀猪盘把那些感情寂寞的人叫做“猪”，建立恋爱关系叫做“养猪”，最后的诈骗行为叫做“杀猪”。

案例：2020年5月份，我区一女青年马某（匿名）通过手机“抖音APP”添加了一名异性好友，对方以交往为由对其进行追求。交往一段时间后，该名网友向马某推荐了一款名叫“中银国际”的APP，马某在该平台进行了投资。投资后该平台称其获取了300万元证券礼金，系统将自动派发388888元证券礼金至马某的账户，但前提是马某在平台的投资须达到一定金额。为获得礼金，马某陆续向平台提供的账户中转账250余万元。但转账后，马某发现平台内余额无法提现，此时推荐投资的异性网友已失联。

防范提示：1. 网络世界是虚拟的，对方自称是“白富美”、“高富帅”还是“魑魅魍魉”很难甄别，望广大群众树立正确的

婚恋观。

2. 接到自称是投资专家、投资平台工作人员等加好友拉你进入股票、虚拟货币等平台转账投资的均是诈骗。

3. 不要太贪图美色和利益，要赚钱还是要靠脚踏实地。

三、网上贷款诈骗

犯罪分子通过短信、微信、QQ、网络发布贷款信息，等受害人主动与其联系，或盗取、购买网贷平台贷款申请信息后，冒充平台工作人员电话联系，骗取受害人信任，后以缴纳手续费、做假流水、钱款被冻结需要激活费等名义向受害人骗取钱财。

案例：2020年6月份，我区一群众李某（匿名）的手机中收到一条“海印金融”贷款软件广告，通过该广告下载了其手机软件，并在该软件内进行相应操作，上传了自己的身份证反面照片、手持身份证照片及个人信息。数据上传后，该软件内余额显示为30000元，但李某进行提现操作时，软件提示其银行卡输入有误。为解决问题，李某联系了软件的在线客服，在线客服推送给李某一个主管客服QQ号。李某添加该QQ号后，对方要求其交纳30%的认证费，李某随即向对方转款9000元，后对方又称其操作超时，需要进行第二次认证，又因李某软件内余额已变为39000元，故第二次认证需要交纳余额钱数的二倍，李某又向对方转款78000元，此后依然提现失败。对方称因李某信用值不够，需要再次交纳费用提升信用度。此时，李某才发现陷入诈骗犯罪分子的圈套。

防范提示：1. 不要轻易相信网络的贷款信息。

2. 需要贷款，要到正规的银行、金融部门履行正常手续进行

贷款。

3. 不要轻易下载短信、微信、QQ 信息中的 APP，也不要点击不明来源的贷款链接。

4. 加强防范意识，不要随意透露自己的私密信息，尤其是银行卡号、密码、验证码等信息。

四、虚假购物诈骗

犯罪分子通过 QQ、微信、短信、第三方交易平台、二手物品交易平台等途径发布低价商品消息，诱骗买家与其联系和购买，一旦买家上钩，便以缴纳定金、交易税、手续费等借口实施诈骗；或者给买家发送链接，要求买家填入银行卡等个人信息，利用这些信息直接操作银行卡实施诈骗；或者虚构商品，虚假出售，故意不发货、不退货款。

案例：我区一从事钢材中间买卖的经营人王老板（匿名），其经常在微信群中发布买卖钢材的广告，广告中有自己的联系方式。今年 4 月份，王老板到陌生电话来电，对方自称其朋友手中有酸洗板（钢材的一种），两人便互加了微信，商谈酸洗板价格，为增加可信性，对方还在微信中发来了酸洗板视频及货物所在地定位。商谈好价格后，王老板便将对方发给自己的酸洗板视频在自己朋友圈发布以便售卖。当日下午，王老板的一微信好友与其联系欲购买此批酸洗板，并通过微信支付给该人 500 元定金。几天后，王老板收到卖家微信发来的磅单，买方将 78000 元尾款转入该人银行账户，王老板扣除中介费后，将钱款打入卖方账户，后该卖方失联，王老板至今未收到货物，共计损失 7 万余元。

防范提示：1. 不要贪图便宜，被超低价货品迷惑。

2. 尽量去大型的、知名的、有信用制度和安全保障的购物网站购买所需的物品，且用第三方支付平台付款。

3. 不要轻易点击对方发送的链接、二维码。

4. 加强防范意识，不要随意透露自己的私密信息，尤其是银行卡号、密码、验证码等信息。

五、冒充公检法诈骗

犯罪分子冒充公检法工作人员拨打受害人电话，以事主身份信息被盗用涉嫌洗钱等犯罪为由，要求将其资金转入所谓“国家账户”“公证账户”、“安全帐户”配合调查或者走“资金清查”程序进行诈骗活动。

案例：2020年4月份，刚刚大学毕业的小张（匿名）在静海区子牙镇家中接到一个电话，对方自称是北京通信管理局的工作人员，说有群众举报其贩卖非法口罩，后转接“北京昌平公安局”的电话，对方自称是民警，称其涉嫌一起网络诈骗案件，要核实其身份信息，让其到一个宾馆内给其取笔录。后对方给其一个QQ号让其添加，小张在对方的指使下，打车到了静海区某宾馆，在宾馆内将所有银行卡的后三位卡号及银行卡余额提供给了对方。第二天，小张又来到宾馆内，对方称现在有一个优先审核的机会，可以提前审核她的情况，排除他的嫌疑，要想获得此机会首先需要办理一张中国银行或者邮政储蓄的银行卡，并办理网银和动态口令。后小张办理了一张中国银行银行卡，办完卡后对方给其另一个QQ，称是领导，该领导称小张现在无法申请这个提前审核机会，上面已经下了拘捕令，让其登录一个网址并注册登录，登录信息输入了其新办理的中国银行卡的账号密码等相关

信息后，网站弹出了小张的拘捕令，后对方称其身份信息可能已经泄漏，必须将自己所有的钱转入这张中国银行卡内，转入后会冻结。小张将自己 9.9 万元余额全部转入此卡中，后对方又骗其从多个贷款 APP 上贷款共计 13.07 万元并转入此卡中。几天后，对方又骗其需要交 23.7 万元的保释金，否则就要将其拘留 45 天，小张先后从朋友处借款 18.2 万元转入对方卡中。后对方又引导其从支付宝花呗套现 3.1 万元也转入此卡中，转款后的几天，小张查询银行卡内余额为零，这才意识到被骗，共计损失 44.27 万元。

防范提示：1. 公检法机关没有“安全账户”！要求你“电话/QQ 视频/微信视频”做笔录的，都是骗子！要求你通话内容“绝对保密”，通过 QQ、微信发送“通缉令、逮捕令”的都是骗子。

2. 凡是电话中自称“通信管理局、电信运营商、银行、保险、邮政”等客服人员，以你“个人信息泄露、涉嫌洗钱、涉案”等为由，主动帮你转接“公安机关”的，都是骗子！

3. 任何要求把资金归集到指定账户（无论是自己名下的账户，还是对方提供的账户），要求开通网银，提供银行账号、密码、验证码的，都是骗子！

4. 如遇拨打亲友电话时发现有“停机、空号”等异常情况，需要提高警惕，设法通过其它途径联系该亲友，核实并提醒谨防上当受骗。

六、冒充客服诈骗

犯罪分子假借“淘宝客服”、“快递公司”等客服的名义，以网购商品“甲醛超标”“降价返利”“退款”、快递丢失赔偿等名

义，通过微信（QQ）发送虚假激活网址，套取支付宝、银行卡、验证码等信息骗取事主扫码、转账汇款。直到被害人意识到被骗后，犯罪分子将被害人联系方式拉黑。

案例一：2020 年 4 月，我区一群众孙某（匿名）在家中玩手机时，接到冒充淘宝客服的电话，“客服”在电话中准确的说出了孙某购买物品的信息，成功获取了孙某群众信任。孙某添加群众 QQ 后，该“客服”在 QQ 上声称孙某购买的物品存在质量问题，可以进行退货退款，但需要保证金，让孙某对其转账 19999 元。在该“客服”诱导下，孙某通过支付宝借呗软件将钱借出至银行卡中，后又将钱转至对方提供的银行卡中，随后发现被骗，共计损失 19999 元。

案例二：2020 年 7 月，我区一群众郝某（匿名）在淘宝网上花费十几元购买了垃圾桶。次日中午，郝某接到自称淘宝客服人员的电话，称其购买的垃圾桶在运输过程中损坏了，将对郝某进行赔偿。客服人员先将郝某加为 QQ 好友，并通过 QQ 给郝某发来链接，让其填写个人信息。郝某填写信息后无法回传，客服人员又称需提升郝某的支付宝芝麻信用额度，以此为由骗取了郝某支付宝付款验证码并将支付宝内 1100 元钱转走。后客服人员以支付宝的信用度不足为由再次诱骗郝某在美团、微博软件借款 9000 元和 4000 元，并将钱转至客服人员指定的账户中。在客服人员编织新的理由要求郝某继续借款时，郝某意识到上当，客服挂断电话。

防范提示：1. 消费者网购时如果要退货，一定要在电商或网银的官方网址上进行操作，不要随意扫陌生人提供的二维码；对

于打进来的电话，只要与“退钱”“赔付”有关，记住，十有八九是骗子。

2. 真正的网店官方客服，并不会通过 QQ 为您服务；您在交易过程中，使用正规的联系和交易渠道，不要轻信他人；如发现可疑之处，应及时与网店官方客服联系，或及时拨打 110 报警，以免造成损失。

3. 商品质量有问题，一定要通过正规的网购平台和商家进行处理，正规的客服和商家是不会通过第三方渠道来联系消费者的。要求在第三方平台上进行退款、登录陌生链接填写个人信息、索取验证码的行为都是诈骗行为。

七、冒充熟人诈骗

诈骗分子利用木马程序盗取对方微信、QQ 密码，截取对方聊天视频资料，熟悉对方情况后，冒充该微信、QQ 账号主人对其账号好友以“患病、出车祸、急需用钱”等紧急情况为由实施诈骗。受害人一般不假思索就会转账给对方，等原账号主人上线后挨个通知后才发现被诈骗。

案例：2020 年 7 月 20 日，我区一企业会计主管尚某（匿名）被拉进一个 QQ 群，群内有其公司所谓“领导”。在群内，该“领导”询问尚某公司账户内还有多少可用资金，随后给尚某发送了一个收款账户并要求其支付一笔款项，手续后补。见到公司领导发出指令，尚某未经核实的情况下，立即给“领导”提供的账户转账 95 万元，后“领导”再次要求尚某进行一笔 395 万元的转账操作时，尚某觉得可疑遂给公司领导打电话询问核实，才发现被骗。

防范提示：1. 核实对方身份，在不是面对面的情况下，不管对方有多着急，关系有多密切，转账前打个电话、语音或视频进行确认无误后再进行下一步操作。

2. 注意管理好自己的网络通讯账号，设置密码时尽量编写为大小写加数字或标点符号的形式达到高安全防护级别，定期更换密码，在其他设备上登录自己的账号后离开或不需要时及时退出并删除聊天记录；以 QQ、微信为例，绑定自己常用手机号码或者邮箱，方便接收提醒短信或邮件，QQ 设置设备锁，微信设置好常用登录设备管理。

3. 安全使用网络账号，不要浏览危险网站或点击来路不明邮件，防止被恶意木马破解。