《反欺诈守护百姓钱袋子》

—电信网络诈骗典型案例剖析

（2025 版）

上海市银行同业公会
安全保卫专业委员会
2025 年 11 月

一、高发电信网络诈骗典型案例

（一）刷单返利类

【典型案例一】

刘先生在某平台看到刷单兼职广告后，下载“**网创”APP进行刷单。起初几单小额返利让刘先生放松警惕，当投入50000元后，发现无法提现，才意识到被骗。

【典型案例二】

张女士在短视频平台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。初期张女士小额投入几笔均获返利，随后客服提供支付二维码，要求其分七次转账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的要求再次向对方转账7600元。张女士照做后，对方又谎称账户被异常冻结，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，最终损失10余万元。

【手法解析】

刷单类诈骗，是指犯罪嫌疑人在网上发布“兼职”“招工”的信息，声称被骗事主可以在网上通过“刷信誉”“购买商品”等方式兼职赚钱，但要求事主提前缴纳费用才能将“工资”提现。常见的刷单类诈骗一般有以下三种“套路”：

一是发布网络兼职刷单信息，寻找被骗对象。骗子通过各种社交软件发布兼职刷单信息，吸引有兼职挣钱想法的人员。

二是首笔刷单返现，建立信任。事主刚刚接单的时候一般都

比较警觉，往往都是小额参与。骗子会在事主第一笔刷单之后，将本金和佣金及时进行返还，目的是与事主建立信任，为之后的大额诈骗进行铺垫。

三是大额刷单不返本金，诱使事主追加刷单资金。建立信任后，事主进行大额的资金投入。此时，有的骗子会只返佣金不返还本金，有的甚至本金、佣金都不返还，并以需要凑单等理由，诱使事主不断追加资金投入，直到事主意识到被骗为止。

【防范提示】

骗子往往以兼职刷单名义，先以小额返利为诱导，诱骗你投入大量资金后，再把事主拉黑。切记所有刷单都是诈骗，千万不能被蝇头小利迷惑，千万不要交纳任何保证金和押金!

（二）虚假投资理财类

【典型案例】

杜先生通过扫码加入一个投资理财群，并通过群内指引添加了自称“基金经理”的客服人员。该客服引导杜先生下载了指定投资平台软件，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，尝到甜头的杜先生持续追加资金投入。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。

【手法解析】

虚假投资理财类诈骗，是指诈骗分子利用互联网仿冒或搭建虚假投资平台，通过虚假宣传，引诱投资者进行投资的一种诈骗手法，常见的虚假投资理财类诈骗一般有以下四种“套路”：

一是引流。诈骗分子通过网络社交工具、短信、网页等多种渠道发布推广股票、外汇、期货、虚拟货币等投资理财的信息，或者在公众号、微博、抖音、快手、知乎等网络平台上投放广告，宣称有内部消息和投资门路从而网罗目标，寻找受害人群体并建立联系。

二是洗脑。在建立联系后，通过聊天交流投资经验、拉人进入“投资理财”群聊、听取“投资专家”“理财导师”直播授课等多种方式，以能够获取内幕消息、获得丰厚回报等谎言取得初步信任。

三是诱导。在骗取信任后，逐步诱导被骗事主登录其提供的虚假网站、扫描二维码下载其分享的手机 APP，指导进行投资理财操作，引导事主初步小额投资试水，获得低额返利，继而取得进一步信任，为诱导事主继续加大投资做好铺垫。

四是收割。继续鼓吹“稳赚不赔”“高额回报”，诱导事主加大资金投入。当在虚假投资理财账户显示有大额盈利，当事主想要提现时，对方就会以“登录异常”“服务器异常”“银行账户冻结”等理由，要求缴纳“解冻费”“保证金”才能完成提现，若不如数缴纳，投资理财账户内的资金就会全部损失。通过这样的方式持续实施诈骗，当察觉被骗后，就会发现已经被对方拉黑，投资理财网站、APP 也已无法登录。

【防范提示】

声称“有漏洞”“高回报”“有内幕”的炒虚货币、炒股、“打新股”“炒黄金”、炒期货、博彩网站的，都是诈骗！切记

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”！

（三）虚假网络贷款类

【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5.4万元，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。

【手法解析】

网络贷款类诈骗，是指诈骗分子通过开设虚假网站、电话、短信等途径，放出“无抵押贷款”“低息贷款”“免息贷款”的诱饵，待受害人与其联系后，谎称可以提供无抵押、无担保、低利息贷款。骗子在整个作案过程中与受害人都无正面接触，作案手段隐蔽，不受地域限制，常见网络贷款类诈骗一般有以下四种“套路”：

一是打着专业公司的旗号开设网站。这类网站往往打着“贷款公司”“投资咨询公司”的名义，有时网站上还会出现“全国各地均有代办处”的字样。其目的就是为了包装自身，进一步骗取事主的信任。但这类网站一般不留座机和地址，只有手机或者QQ，即使留有地址也经不起细查。

二是大力宣传“无抵押、无担保”“当天放贷”。在许多的“网络贷款骗局”中，往往会出现“无抵押、无担保”“当天放贷”等极具诱惑性的标语，这些标语极其精准地切中了广大急需资金的企业主及个人的要害。一般来说，项目方在寻求正规贷款途径而遭拒的原因往往是没有良好的抵押资产或担保。在这类骗局中，被骗事主一旦上钩，便被要求“因为无须担保、无须抵押”所以贷款前要先缴纳一定手续费、担保金等，有些甚至要求事先缴纳一定期限的利息。

三是假扮正规机构。有一些骗子公司高度仿照知名贷款机构网站，具有极大的欺骗性，这些冒牌网站的页面往往和正规贷款机构网站相似，其域名和正规贷款机构网站只差一两个字母。

四是逐步开始网络转账骗局。在骗局中，以受害人征信出现问题需要修复征信、贷款审核为由要求受害人缴纳“保证金”“手续费”，再以受害人操作失误、征信有问题、流水不足等为由要求受害人缴纳各种费用。行骗者也会以款项需要中间账户中转为由，让被骗事主在一个伪造的银行网站或者在有木马病毒的网站上输入银行账号及密码，以盗取被骗事主的银行账号信息，并进一步将银行卡内的资金盗走。

【防范提示】

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

（四）冒充公检法类

【典型案例】

刘阿姨接到一个自称某市公安局警察的电话，刘阿姨名下一张银行卡涉嫌洗钱，要求配合调查。对方添加刘阿姨 QQ 好友，并发来“财产冻结书”，以案件涉密为由进行威胁恐吓，要求其到无人房间配合调查并禁止对外联络。随后让刘阿姨将银行卡里的所有钱款转到“安全账户”，声称案件查清后将全部返还。在完成转账后对方失联，刘阿姨方才意识到被骗。

【手法解析】

冒充公检法类诈骗，是指犯罪嫌疑人以公安局、法院等为名，称客户本人或亲属涉案，再将电话转至所谓的“有权机关”，诱使被害人将钱转入“安全账户”，常见的冒充公检法类诈骗一般有以下四种“套路”：

一是建立信任，吸引被骗事主。在此环节中，骗子会冒充通信管理局、卫健委、疾控中心等国家单位与事主进行沟通联系，告知一些涉及事主个人利益的受损情况，而事主能明确所谓的情况他本人并没有参与。当事主进行辩解，对方就会告知事主，是由于身份信息被泄露才造成这样的结果，之后会帮事主转到公安机关进行解决。

二是树立权威，震慑事主。当冒充的“公安机关”与事主联系后，冒充的“民警”会先了解事主一些基本情况，然后会明确告知事主就是涉及案件的犯罪嫌疑人，用突如其来的言语震慑住事主。

三是深度洗脑，控制住事主。骗子会不断变换身份，利用不同的道具、话术告知事主存在犯罪行为，让事主相信自己确实涉嫌案件，并且如果想洗清罪名就必须配合假冒的“公检法”机关的调查。

四是转账汇款，榨干事主的资金。在事主被控制住后，对方就会要求事主进行转账汇款，将资金转入假冒“公安机关”的“安全账户”，或者盗刷事主资金，有的甚至还会要求事主到贷款公司进行贷款或者抵押，之后再将这些资金转给骗子。

【防范提示】

公检法机关办理案件时，会当面向涉案人员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！

（五）虚假征信类

【典型案例】

汪某接到陌生来电，对方自称“某电商平台客服”，先是准确报出了汪某的个人信息，接着告知汪某需要注销平台的某分期支付业务，否则将产生高额利息，还将影响个人征信。虽是满头雾水，慌乱中汪某还是信以为真，听从“客服”的指示，按照对方要求通过社交软件与对方开启了“分享屏幕”功能。接着对方称需要对汪某的账户进行资金核验，向汪某提供了一个假冒的“公民个人征信”网站，称需要在该网站上进行“信息核实”，

将其银行卡内的资金打到“安全账户”就能关闭分期业务，还承诺成功关闭后资金将被全额返还。待汪某发现被骗时，钱已经落入了骗子的口袋。

【手法解析】

一是伪装成“电商客服”，主动说出受骗者身份信息。不法分子会假冒“电商平台客服”的身份电话联系受骗者，同时为了获取信任，不法分子会利用非法获取的个人信息，在沟通中准确提供受骗者的姓名、身份证号等，以消除受骗者的疑虑。

二是编造欺诈事由，让受骗者陷入恐慌。获取受骗者的信任后，不法分子谎称需要其配合注销该电商平台的某分期支付产品，否则会影响个人征信及产生额外费用，同时不断以“国家政策”“资金安全”等字眼强调不操作带来的严重后果，让受骗者落入圈套。

三是以协助操作为由，要求开启分享屏幕功能。当受骗者产生恐慌情绪时，骗子进而以“协助指导关闭操作”为名义，诱导受骗者打开网络社交或会议软件中的分享屏幕功能，殊不知打开该功能后，受骗者手机屏幕上显示的内容都能被诈骗分子尽收眼底。

四是发送欺诈链接，诱导受骗者操作转账。不法分子给受骗者发送欺诈链接，引导受骗者进入虚假的“国家金融监督管理总局/公民个人征信”等高仿网站，输入个人信息、账户信息等进行“身份核实”。或是诱导受骗者把银行卡资金转进指定账户，进行所谓的“转账认证”。殊不知这些钱款有去无回，统统落入

了骗子的腰包。

【防范提示】

1.接到自称“电商客服”打来的声称需要“注销分期支付业务”的电话，或是有关“注销贷款账号”“清空贷款额度”“影响个人征信”等内容的电话，不要轻易相信，很可能是骗局。

2.涉及钱财交易需谨慎，在确认对方身份前，切勿轻易向不明人士进行转账支付。

3.对于陌生人通过短信、网络等方式发送的不明网站链接或二维码，请勿轻易点击或扫码，更不要进行信息填写。

4.加强个人信息保护意识，警惕陌生人的“分享屏幕”邀约，避免重要信息被他人窥取。

（六）虚假购物服务类

【典型案例】

陆先生在购物平台上认识了一个“**代购”声称专做品牌运动鞋生意能拿到优惠价，两人加了社交平台好友进行后续交易，按对方提议陆先生完成了付款，然而他查询快递单号时却发现查无此单。陆先生十分生气，准备与代购理论时才知道自己早就被拉黑了。

【手法解析】

虚假购物类诈骗看似单笔金额不多，但骗子广泛撒网，靠的就是“走量”。一般惯用的套路有以下三种:

一是诈骗分子在网络平台、朋友圈、直播平台发布优惠打折、海外代购、低价转让等极具诱惑性的商品信息，或是声称可以提

供论文代写、私家侦探、提供定位等服务吸引有购买意向的潜在受害人。

二是诈骗分子会诱骗受害人不走官方渠道而转为私下交易，“平台管得严加V私聊”“帮很多人都带过不信任就别买了”还会发去商品实物图、成功交易记录等骗取受害人的信任，进而要求他们以私下转账的方式先付费，有的骗子会向受害人发送虚假付款链接，点开后看似正规付款页面，实际上钱款直接进入了骗子账户，而他们也不会真的发货。

三是一旦付款，受害人将面临漫长的等待，等到忍无可忍前去质问才发现自己早就被拉黑了，更有甚者骗子会以加缴关税缴纳定金、交易税、手续费等理由要求受害人继续转账榨干他钱包里的每一分钱。

【防范提示】

通过网络平台交易，一定要详细了解商家的真实信息，交易时最好有第三方做担保，选择正规的购物、服务平台，对于异常低价的商品要提高警惕，更不要相信所谓的论文代写、私家侦探等违法服务。

（七）冒充熟人类

【典型案例】

公司财务王先生被拉入一个工作群中，因群成员昵称均为公司员工便未加核实。几天后，王先生收到群内消息，“老板”称需支付货款，要求核对公司账户余额。在王先生核对完账户资金后，群内“老板”要求其将全部资金转至指定账户，并以紧急事

由不断催促王先生尽快操作。因怕耽误工作，王先生未经核实便将公司账上80万元全部转出，后因公司老板收到银行短信询问才发觉被骗。

【手法解析】

冒充熟人类诈骗，是指诈骗分子通过冒充被害人朋友、同学、老师、领导等，利用熟人之间缺乏戒备心的心理，借某种事由，以要求帮助垫钱转账等话术实施诈骗。常见的冒充熟人类诈骗一般有以下三种“套路”：

一是冒充领导骗下属。骗子一般通过伪装微信头像、昵称等方式冒充受害人较为熟悉的领导，并添加受害人微信。与受害人联系期间，表现出对受害人信息了如指掌，让受害人深信不疑，然后骗子就会以给“领导送礼”或者“领导急需用钱”等各种理由，要求受害人向指定的账户进行转账汇款，并利用受害人惧怕领导、不好意思和领导当面或电话核实等心理实施诈骗。

二是冒充老师骗家长。骗子会冒充老师的身份潜伏在班级群聊中，对学生和家长以收取资料费、课外班辅导费或其他学杂费等理由，通过群内收款的方式诈骗学生家长的钱财。犯罪分子实施诈骗的时间一般是在上午或者下午，在群内老师上课的时间冒充老师，将自己群内头像、昵称更改为和老师一样或者极为相似的字样，以骗取信任。

三是冒充好友或同学骗亲属。诈骗分子盗取受害人微信、QQ账号，或者通过更换同样昵称、头像等方式，伪装成受害人的同学或好友，向账号内联系人群发虚假求助消息，收到联系人回复

后，再步步引诱骗取钱财。

【防范提示】

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转账操作！

（八）网络游戏产品虚假交易类

【典型案例】

游戏“发烧友”小李的朋友圈被某款游戏刷屏了，小李非常心动，想要立马化身为“游戏天命人”去打怪升级。无意间，小李在某游戏聊天群中看到陌生人发的消息，得知通过某二手交易平台店铺购买礼品卡充值，可以低价入手游戏。为了省钱，小李便进行了付款。没多久，小李确实收到了以礼品卡形式入库的游戏，这时他没有多想，便在二手平台确认了收货。正当小李兴致勃勃准备开始玩游戏时，却发现游戏竟然被回收了，再去联系卖家时，发现自己已经被对方拉黑。

【手法解析】

网络游戏产品虚假交易类诈骗就是诈骗分子在网络发布低价售卖游戏的虚假信息，诱导游戏玩家绕过正规渠道进行交易，待玩家确认收货之后利用平台规划回收游戏“礼品卡”，从而实施诈骗。一般有三种套路:

一是虚假游戏充值。诈骗分子打着“超低价游戏币充值”的旗号，对虚假诈骗链接进行包装，然后通过游戏聊天系统等途径发布，诱导玩家点击。

二是诈骗分子在游戏中发布虚假广告，称可以代打别人的账号，帮别人提高分段或等级，然后收取一定费用，然而一旦预先收到钱款后就会销声匿迹。

三是虚假幸运抽奖。一些诈骗分子向玩家发布虚假宣传链接，称点击链接即可领取游戏装备、礼包等，实则是利用钓鱼网站试图盗取资金。

【防范提示】

网络游戏要适度，不能沉溺其中。通过正规网站平台买卖游戏账号、道具。高度警惕网络游戏类诈骗的各种套路，不论骗术怎么变，防范之心不能减！

（九）交友投资类（杀猪盘）

【典型案例】

张先生通过网络交友平台认识了“周女士”，对方自称因长期遭受家暴导致婚姻破裂，目前正在闹离婚。对方通过频繁倾诉婚姻不幸博取到张先生同情，期间还将离婚证发来，两人很快发展成为恋人关系。在随后的交往中，“周女士”先后以经营周转、信用卡还款、生病住院等理由骗取张先生10万余元。张先生再联系时发现对方已拉黑自己，此时意识到自己被骗。

【手法解析】

交友投资类诈骗（杀猪盘），是指犯罪分子通过社交网站与事主结识。在与事主建立信任之后，声称自己在投资平台或者赌博网站上工作，能获得内部消息，进行投资稳赚不赔，诱使事主在虚假的平台上进行投资或赌博。常见的交友投资类诈骗（杀猪

盘）一般有以下四种“套路”：

一是“寻猪”。诈骗分子会伪装为成功人士，通过婚恋网站、网络社交工具寻觅、物色诈骗对象，与受害者聊天交友，确定男女关系、婚恋关系，甚至远程下单赠送昂贵礼品，取得信任。

二是“诱猪”。诈骗分子会推荐投资网站、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其帮忙管理，进行体验，从而诱导受害者投注。

三是“养猪”。当受害者少量投注时，回报率很高，提现很快，让受害者逐渐产生贪婪的欲望，继续加大投注金额。

四是“杀猪”。在受害者投入大额资金后，会发现网站、APP账户里的资金无法提现，或在投注过程中全部输掉，发现被骗后，网恋对象会将受害人拉黑。

【防范提示】

素未谋面的网友、网恋对象推荐网上投资理财、炒数字货币（虚拟币）、网购彩票、博彩赚钱的都是骗子！切记始于网恋，终于诈骗！网友教你投资理财的都是诈骗！

（十）非法“校园贷”类

【典型案例】

某日，大学生小姜在宿舍无意间点开了一个申请贷款的广告链接，被“只需要身份证，即可进行小额贷款”的字样吸引。“当时想换一个新手机、买一台新电脑，就看到有这样一个网站，步骤流程比较简单，只需提供身份证就可以申请贷款。”小姜立即

填写了个人信息，申请了 8 万元的贷款。不久后，一位自称公司放款部的客服打来电话，要求小姜添加其微信，并发送身份证和人脸照片进行身份核实。小姜照做后，客服发来电子合同让他填写，并声称将提交给银行。

然而，此时小姜的贷款却出现了问题。“他说我银行卡的流水少，贷不下来款，让我往自己的银行卡里打 15000 元钱，打完之后他说申请成功了，让我把短信验证码发给他。”小姜刚发过去验证码，就发现手机上收到了银行发来的扣款通知。当小姜询问对方时，对方却以走程序为由进行敷衍。第二天，小姜发现自己的微信已被对方删除，客服电话也再也无法打通。

【手法解析】

部分看似正规的贷款平台背后，往往隐藏着骗局。平台在获取大学生的贷款需求后，迅速确认，声称贷款已获批。利用大学生急需拿到钱款的心理，以收取“保证金”“手续费”“咨询费”等理由，要求申请贷款人先向指定账户转账，才能拿到贷款。而一旦申请人按要求转账，骗子就会将其拉黑，实现诈骗目的。

【防范提示】

防范此类诈骗，首先要注重保护个人信息，对于关乎自身信息、财产安全的事情要多方求证；其次，在申请借款或分期购物时，要明确自身是否确有需求，并衡量自己是否具备还款能力；最重要的是，凡贷款前需要交费的都是诈骗陷阱。如有被骗，务必在最短时间内拨打 110 报警电话，提供骗子的收款账号，这将有助于公安机关及时挽回受害人的财产损失。

二、新型电信网络诈骗典型案例

（一）“现金花束”诈骗

【典型案例】

某花店经营者梁某，近期其在某生活服务平台收到某顾客私信，要求订购鲜花，且主动添加梁某微信好友。该顾客要求在花束中放入19999 元现金包装后制作成“现金花束”送人。因梁某在日常经营中常有此类业务，未能及时发觉存在潜在风险，便提供个人账户卡号及姓名，顾客随即转账至梁某账户，梁某收到转账后到就近的ATM 机取现，后根据要求包装在花束内并交由跑腿人员送到指定地点，至此完成该笔订单。第二天梁某的账户被公安机关冻结，经公安机关告知才知道自己成为不法分子转移不明资金的帮凶。

【手法解析】

一是诈骗分子通过网络平台或拉拢本地人员联系商户，提出个性需求。由于商户之前可能做过类似定制礼品盒或大额订单，因此容易放松警惕。

二是诈骗分子通常会优先购买方便变现的商品，如烟酒、鲜花礼盒、黄金等，并提出将钱打入商户经营者的银行卡账户内，让其提供银行卡号。

三是商户收到“预付款”后，实际是其他案件的“赃款”。商户在不知情的情况下，成为了诈骗分子的“洗钱帮凶”，导致银行卡账户被冻结，甚至出现涉案资金被划扣的重大损失。

【防范提示】

1.谨慎接收网络订单和大额线下订单，规范收款流程，拒绝来历不明的货款。

2.不要随意提供银行账户或收款二维码，避免成为诈骗分子洗钱的工具。

3.发现银行账户出现异常状况时，应第一时间到银行卡开卡行查明原因，如被警方依法处置，应积极配合调查。

（二）“购买黄金+网约车投送”诈骗

【典型案例】

随着电诈手法不断迭代升级，“线上诈骗+线下取现”的模式增多，诈骗分子以各种理由诱骗受害人邮寄大额现金或者大量黄金，通过网约车、邮寄、跑腿等方式送达，以不见面、不现身的方式将现金或黄金取走，最终成功转移赃款。

某市警方预警发现，一位六旬老人购买了540克金条（约38万），发现该市民有极高被骗风险，故警方立即开展电话核实，并将此信息下发给居住地派出所上门劝阻。经民警劝阻，被害人在网上认识一网友进行投资理财，黄金已通过某网约车运出。对此，警方迅速联动网约车运营公司，将网约车司机叫回，成功挽回540克金条。

【手法解析】

一是刷单诈骗+邮寄黄金“提现”。

诈骗分子在网上发布兼职广告，待受害者询问后，发送兼职需要做的任务，内容一般是下载 App，完成收藏视频或评论等任务，先小额返利，后称因受害人平台积分不够，需要购买黄金邮

寄到指定地点才能完成提现。

二是投资理财诈骗+邮寄黄金“充值”。

诈骗分子冒充投资专家，鼓吹“稳赚不赔”“高额回报”，诱导受害人转账充值投资或怂恿到黄金店购买黄金直接邮寄到指定地址，声称收到黄金后会翻倍充值到投资账户中，且马上到账。

三是冒充公检法诈骗+邮寄黄金“洗白”。

诈骗分子冒充公检法，告知受害人的账户涉嫌违法犯罪，想要办理“撤案”手续，需要购买黄金，邮寄到指定地点进行资金审查，审查后会返还购买资金。

四是杀猪盘式诈骗+邮寄黄金“赚钱”。

诈骗分子冒充“军人”或“成功人士”，以特定职业身份获取受害人的信任。待感情升温后，教受害人利用地域黄金差价赚钱，先线下购买黄金，再寄到指定地方或上门取货，并称等赚了钱会返还钱。

五是接收资金+购买黄金+邮寄黄金。

有的受害人将黄金邮寄出去后，诈骗分子还会将其他诈骗资金转入受害人账户内，让受害人继续购买黄金邮寄，这时受害人反而变成了诈骗分子洗钱的帮凶，沦为电诈工具人!

【防范提示】

1.不轻信陌生人的投资建议。

2.不轻信“点赞、分享、助力、做任务”等高额返利。

3.网上充值资金、线下托运现金的，都是诈骗。网上陌生人

不论以何种理由，要求使用自有资金购买或为他人代购黄金、香烟或其他贵价物品，并要求网约车快送、邮寄至指定地点或派人上门来取的，都是诈骗。

（三）假冒知名直播平台短信诈骗

【典型案例】

刘女士收到了假冒的“某某甄选”发送的诈骗短信。短信称刘女士会员期满，若不及时处理，将在当日自动扣款 XXX 元，并附有客服电话。刘女士未产生怀疑，随即拨通客服电话。对方自称是某某平台客服，告知刘女士因某某平台电商会员免费体验期到期，不取消的话，每月将扣除 XXX 元会员费。刘女士选择取消服务，并在客服的指导下在某某平台操作取消，但并未显示关闭成功。客服表示可能因为到了扣款日期系统暂不支持关闭，随后诱导刘女士下载安装“XX 会议”APP，在该 APP 中与刘女士进行共享屏幕，让刘女士查看其名下各个银行卡的信息。在诈骗分子的指导下，刘女士登录了自己各个银行的 APP，并在此过程中陆续收到多条扣款短信提醒，最终意识到自己被骗，共计损失17000元。

近日，不少用户反映收到了这样的短信：“【某某甄选】XX 会员您好，会员期满，即将在今日自动扣款 XXXX 元，请及时处理，如有疑问，请联系客服电话 1XXXXXXXXXX”。

这突如其来的短信让不少用户感到困惑和惊慌。截至目前，某某甄选已收到超 6000 余名用户反馈此诈骗短信问题，从用户提供的诈骗短信截图来看，诈骗短信不仅附带了虚假的客服电

话，有的还设置了一个虚假链接，不少用户因对某某甄选品牌的信任，未加甄别便点击了链接或拨打了电话从而落入了诈骗分子的圈套。诈骗分子的手法其实并不新鲜，他们利用了用户趋利避险的心理，通过假冒电商平台客服的方式实施诈骗。

【手法解析】

第一步：获取信息，假冒身份

诈骗分子通过非法渠道获取事主信息，冒充电商平台客服，通过短信、电话联系事主，谎称事主开通的会员已到期，即将扣除下一期会费，费用通常较高金额几百至几千元不等。

第二步：引起恐慌，引导操作

事主因担心扣费主动提出让诈骗分子协助其关闭服务。诈骗分子通常以两种方式引导事主完成转账前期操作：一是语音指导事主下载特定 APP 或点击其发送的网站链接，联系“专业客服”线上关闭或取消服务；二是诱导事主下载手机屏幕共享软件，手把手指导事主操作。

第三步：诱导转账，实施诈骗

诈骗分子指导事主在下载的 APP 中绑定银行卡，以“保护事主钱款”为由向事主索要验证码，诱导事主进行转账，最终完成诈骗。

【防范提示】

1.凡是声称“某某甄选”或其他电商、物流等平台的会员到期将产生大额收费扣款的信息都是诈骗！对于短信中的电话或者链接，不要拨打！不要点击！

2.如确实需要取消某项服务，最好通过官方网站、官方 APP 或拨打官方客服电话等进行操作。

3.凡是要求打开“屏幕共享”指导关闭“免密支付”的，都是诈骗!

4.老人若遇到所谓的客服，一定不要慌，不要随意听信陌生人，特别是涉及自己“钱袋子”的问题，可以等家人回来询问清楚，或拨打110向民警求助。

5.96110是反电信网络诈骗专用号码，一旦接到96110来电，说明您有极大可能正在遭遇电信网络诈骗，因此不论何种原因，一定要及时接听电话，以免遭受进一步损失。

（四）“百万保障+冒充反诈中心”诈骗

【典型案例】

近期，冒充“百万保障”保险客服的诈骗手段再次更新，客户接到冒充“百万保障”保险名义诈骗电话后，会再次接到冒充反诈中心提示的诈骗电话，肯定“百万保障”扣费的真实性，要求被害人根据客服指示操作。

近日，某市接受过反诈宣传的王先生接到自称是“百万保障”保险客服的电话，在对电话存疑之际，又接到来自“反诈中心”的 FaceTime 视频电话，称不是诈骗，确有保险到期，需要解绑一事，要求其配合客服进行完成。王先生遂打消疑虑，根据“客服”指令转账后，损失40万元。

【手法解析】

一是冒充“百万保障”保险客服来电。犯罪嫌疑人自称“百

万保障”保险客服来电，借故声称被害人资金保险到期，需要配合解除绑定。目前，群众对此类诈骗知晓率较高，大部分人员对此均不予理睬。

二是冒充反诈中心再次 FaceTime 视频来电。最新手段中，犯罪嫌疑人冒充反诈中心在被害人挂断电话后不久，使用 FaceTime 视频来电，声称刚刚的“百万保障”并非诈骗，以反诈中心的名义，需要被害人配合完成。此类作案手法往往利用了地区群众对反诈中心提示的信任度。

【防范提示】

1.警惕 FaceTime 电话。对非必要使用 FaceTime 功能的 iPhone 用户，建议直接关闭该功能。对部分业务、生活需要经常使用 FaceTime 功能的客户，要引导其提高警惕。政府部门均不会采用 FaceTime 功能进行信息告知。

2.不要相信“百万保障”收费或影响征信的说辞。微信、支付宝“百万保障”均为自动开启的安全设置，完全免费而且并不会影响个人征信。

3.存疑可寻求派出所、居委会工作人员确定。对陌生电话要求配合认证、取消会员、缴纳保证金等情形，存在疑问的，建议引导地区群众向属地派出所民警、居委会工作人员进行确认。

（五）“荐股”诈骗

【典型案例】

孙某在某直播平台上观看炒股知识的直播时，收到了自称是主播的好友申请，私聊后被拉入某炒股群。群内一昵称为“高级

投资总监”的用户在群内时常分析行情、推荐股票，并会有自称“助理”的用户频繁贴出“总监”帮助股民赚钱的截图，还有不少群友声称自己就是受益者。这让长期“潜水”的孙某动了心，并加了“总监”为好友。“总监”称现在为回馈用户免费带大家炒股，只要将资金转入指定APP，按指令操作即可，保证绝对不会亏损。孙某听闻兴奋不已，便下载了“总监”推荐的APP，并按照其指导在该款APP内进行投资操作。刚开始时，孙某几次小额的投资尝试收益都不错，且都成功提现，这让孙某感觉这是一个赚大钱的机会，便在该款APP加大投资。直到月底，孙某发现APP内的余额无法提现的时候，才反应过来自己被骗了。

【手法解析】

一是诈骗分子鼓吹自己能准确预测股票涨跌，并营造专业可靠的投资理财氛围，让不懂投资的人信以为真，以高盈利为诱饵诱导用户下载软件进行投资交易。

二是在前期让用户尝到高收益的甜头诱惑受害者加大投资力度，而实际这些交易系统和记录均为伪造，待受害人想要提现时就会出现“系统崩溃”“无法提现”等情况，此时受害人才发现自己上当受骗但已血本无归！

【防范提示】

1.投资伴随风险，不可能存在稳赚不赔，更不要盲目相信所谓的“总监”“专家”提供的“内幕消息”，务必做到“不轻信、不转账”。

2.投资一定要找正规平台进行投资。投资回报明显高于正规

平台的，或者听他人推荐的投资平台一定要谨慎投资，谨防被骗。

3.不要向陌生人提供身份证、银行卡号、密码、验证码等个人信息，不扫来历不明的二维码，不点陌生人发来的链接。

（六）实体店大额消费套现诈骗

【典型案例】

苏女士是一家小吃店的老板，有一天，一名陌生女子加上了苏女士的微信，点了排骨面套餐，让苏女士送货到指定地点，随后通过支付宝付了钱。第二天，该女子再次联系苏女士表示自己要买排骨面套餐，要求还是将餐送到指定地点。这一次付款时，该女子却称支付宝和微信无法进行转账，想要通过银行付款，要求苏女士提供银行卡账号。苏女士便将银行卡账号和名字发给对方。不一会儿，苏女士便收到一笔9980元的转账，对方称自己在开车所以不小心按错了，让苏女士将多余的钱通过支付宝返还给她，苏女士便转账给了对方。随后，对方又称自己舅舅要做手术，也让苏女士再次协助进行转账12200元，但这时，苏女士银行卡已被冻结，无法进行转出。事后她从公安机关和银行得知，这笔转入款项来自一起电信网络诈骗案受害人的转账，苏女士的银行账户因此被依法冻结。

【手法解析】

诈骗分子利用网络找到小吃店、餐饮店经营者联系方式，以订餐加微信。餐送到指定地点后，他们借口支付宝、微信限额且家人住院急需用钱，先转钱到店主账户，再让店主转至指定账户完成洗钱。就这样，商户经营者无意中成为诈骗分子的“洗钱帮

凶”，导致自己名下的账户被冻结，甚至可能承担涉案资金被划扣的经济损失。

【防范提示】

1.尽可能在店内安装高质量的视频监控设备，当遇到可疑客户，如佩戴帽子、口罩、围巾等遮挡面部时，要想办法让其取下遮挡物，并引导其到监控最佳位置，确保监控留存其清晰的面部信息；要多方面留存可疑客户的联系方式，比如微信号、支付宝账号、手机号码等。

2.警惕主动联系且声称要购买大量手机、黄金、珠宝、储值卡、烟酒等易变现商品的情况，判断对方购买需求的合理性。特别是坚持只通过数字人民币购买，并要求分多天多笔支付的情况，以及不考虑价格并加价购买，要求尽快拿到现货的情况。

3.警惕通过视频连线或拍照的方式将收款码或付款码进行传输由他人支付的情况，以及他人通过网银转账付款的情况。即现场购买人与实际付款人不一致，实际付款人未在现场，并且不能做出合理解释。

4.警惕异常行为，如有取现要求的陌生订单，以及将大额交易拆分为多笔支付。当遇到消费者年龄与其购买力不符，或主动要求拆分交易、频繁更换支付账户，等待他人转款后才进行支付等情况时，务必详细询问、多方核实，或拨打96110、110进行咨询、报警。

（七）“共享屏幕”诈骗

【典型案例一】

近日，王先生接到陌生电话称其在某购物平台点过一个保单，从明天开始扣款，王先生咨询对方如何取消该服务，对方要求先下载一个“某会议”APP，并打开全部权限，然后再打开银行APP，在APP的客服搜索栏中搜索“支付”选项，点击“支付管理”，关闭自动扣款服务，这时王先生手机突然黑屏，王先生意识不对，就强行将手机关机，再开机后发现手机银行内30万元资金不知去向，随即报案。

【典型案例二】

个体经营者施先生，接到冒充某电商服务平台客服的电话，对方以“关闭月付功能避免每月扣费900元”为由，并诱导其下载“**会议”软件加入指定会议号，随后登录银行APP时手机黑屏，其间诈骗分子远程操控其账户并进行人脸识别，分三笔向嫌疑人转账，手机恢复后施某察觉异常并报警，被骗共计12万元。

【手法解析】

一是伪装身份，制造恐慌：诈骗分子通常冒充“公检法”或各类平台的客服，利用获取到的受害人信息，编造受害人“涉嫌洗钱”“账户异常”“快递丢失需理赔”等理由，要求配合“安全调查”或“退款操作”，逐步诱导下载软件。

二是远程监控，实施诈骗：利用受害人下载的屏幕共享软件，以指导操作为由，诱骗受害人点击打开共享屏幕。一旦屏幕共享开启，手机上的任何信息都会同步显示到对方的电脑或手机上，包括银行账号、密码、验证码等重要信息。诈骗分子便利用这些信息，将受害人钱财进行转移。

【防范提示】

1.保持警惕：当陌生人要求你下载某个软件或打开某个链接进行“共享屏幕”时，请务必保持警惕，不要轻易相信。

2.核实身份：在接到自称是客服的电话时，要通过官方渠道核实对方身份，不要轻信陌生人的话。

3.拒绝共享：无论对方以何种理由要求你开启“共享屏幕”，都要坚决拒绝。记住，一旦开启屏幕共享，你的手机上的所有信息都可能暴露给对方。

4.及时报警：如遇到可疑情况或发现自己被骗，请立即拨打96110全国反诈劝阻专线进行咨询举报。