

“为民办实事”之消费者权益保护

案 例 汇 编 (一)



消费者权益保护部

2025 年 6 月

编者按

在信息化浪潮快速发展的当下，电信网络诈骗犯罪如同一颗“毒瘤”，迅速蔓延滋长，威胁着人民群众的财产安全与社会的和谐稳定。

根据最高法工作报告，2024 年全国审结电信网络诈骗案件 4 万件 8.2 万人，同比增长 26.7%。最高检工作报告显示，2024 年检察机关依法惩治电信网络诈骗犯罪，起诉 7.8 万人，同比上升 53.9%。反电信网络诈骗形式依旧严峻。

近年来，渤海银行全面落实习近平总书记视察天津四个“善作善成”重要要求，始终坚持“金融服务守初心，消保为民显担当”的消保品牌理念，持续深化警银合作，构建“技防+人防”的全方位、多维度、立体化反诈防控体系，积极通过反诈宣传、柜面止付、预警劝阻等举措保障金融消费者金融财产安全，取得积极成果。

本期，我行收集营业网点报送的消费者权益保护案例 15 篇，提炼形成关键字，对阶段性典型案例进行全面剖析，并结合案例特点对广大金融消费者发出风险提示。





关键词：百万医疗保障



2025 年 1 月 20 日



长沙友谊路支行

你好，我是**百万保险客服，您在平台上开通了“**百万保险”服务，若不及时取消，您的账户将在 30 分钟后自动扣款 2000 元！

这样的电话，您接过没？

金融服务守初心 消保为民显担当

【案例回顾】

2025 年 1 月 20 日下午，客户肖阿姨与丈夫匆忙赶到长沙友谊路支行，称手机被控制无法解锁。经网点工作人员小汪询问，肖阿姨表示她接到一个自称“微信客服”的电话，对方告知其微信“百万保障”功能免费期已过，若不取消将每月自动扣款 2000 元。由于对金融产品功能不熟悉，肖阿姨信以为真，在对方的诱导下下载了一款屏幕共享软件，导致手机屏幕被控制无法解锁。幸运的是，肖阿姨曾参加过渤海银行组织的金融知识讲座，对电信诈骗的常见套路有了一定了解。意识到问题蹊跷后，她立即与家人赶到网点寻求帮助。小汪迅速为其核查手机状态，确认状态异常后判定肖阿姨遭遇了电信诈骗。为避免资金损失，小汪第一时间指导客户在柜台办理了银行卡紧急挂失。经查询，肖阿姨名下 3 笔共计 46 万元的“渤定存”已被提前支取至活期账户，但她本人对此毫不知情。小汪迅速协助肖阿姨办理账户密码重置、限额调整及银行卡更换等操作，成功避免了客户资金损失。

【常见套路】

不法分子通常会先冒充客服人员，声称被害人之前开通的“百万保障”保险到期，如果不关闭，系统将每月自动扣费。由于担心被扣费，被害人会在“客服人员”的要求下尝试关闭“百万保



障”。此时，“客服人员”会引导被害人下载“银联会议”APP 并开启屏幕共享和远程操作权限，并利用操作权限让被害人手机屏幕黑屏，要求被害人进行人脸识别或指纹验证等操作，将银行卡内资金进行转移。

【小渤提示】

1. 声称即将开通“保险自动扣费”业务时，凡是以远程办理业务为名要求下载各类软件并开启共享屏幕功能的都是诈骗；接到自称保险公司、银行或网站客服来电，不要盲目轻信，务必多方核实确认，避免被诈骗。

2. 在购买保险产品时，切记选择正规机构、官方渠道，遇到不明人员与自己联系保险业务时，应拨打保险公司服务热线进行核实，并且保护好个人信息，增强安全意识。

3. 遇到可疑情况，请及时拨打反诈专线 96110，如果不幸遭遇电信诈骗，要立即拨打 110 报警并采取相应的应对措施以减少损失。





关键词：代理退保



2025 年 2 月 19 日



青岛市北支行

近年来，一些不法分子自称资深专业律师、业内专业人士，在微信、抖音、快手等自媒体平台发布信息，宣称“国家出台退保政策”“退保新规”等，以“代理退保”“代理维权”等名义招揽业务，声称消费者购买的保险无论多长时间、多少金额均可帮助其“全额退保”，怂恿或诱骗消费者委托其办理退保等事项以谋取不正当利益。

金融服务守初心 消保为民显担当

【案例回顾】

2025年2月19日，客户徐先生收到一条自称是“专业金融维权机构”发来的短信，声称可以帮他办理高额保险退保，手续费低廉。徐先生此前购买了一份期交保险，近期因资金周转问题，正犹豫是否要退保。看到短信后，他心动不已，随即联系了对方。

对方信誓旦旦地表示，他们有专业的团队和渠道，与保险公司内部人员熟悉，保证能帮徐先生全额退保。对方诱导徐先生按照要求提供身份证、保单、银行卡等个人重要信息，并签订一份所谓的“代理退保协议”和支付一笔前期费用。

所幸的是徐先生马上意识到情况不对，来到青岛市北支行，找到熟悉的客户经理小刘求助。小刘看到徐先生收到的短信后，立即告知可能是诈骗短信，同时具体讲解了类似的诈骗案例。在小刘的耐心讲解下，徐先生识破了“代理退保”骗局，保住了15万元保单权益。

【小渤观察】

2021年11月16日，国家金融监督管理总局微信公众号发布《关于防范“代理退保”等风险的提示》，提醒消费者依法理性维护自身权益，远离“代理退保”“代理维权”不法行为侵害，防范警惕风险。

2024年5月11日，国家金融监督管理总局微信公众号发布



《关于警惕涉金融领域“代理维权”风险的提示》，提示广大消费者通过正规渠道表达诉求，依法理性维权。

【常见套路】

1. **虚假宣传、假冒身份。**不法代理退保组织或个人，会通过微信群、朋友圈、短视频、网络论坛、电商平台等渠道进行虚假宣传，引诱消费者点击链接、留言咨询，联系并锁定客户后，冒充法律工作者、保险公司工作人员甚至监管部门执法人员实施不法行为。

2. **谎言欺骗、怂恿退保。**不法代理退保组织或个人，会谎称“保险公司存在欺诈，多名消费者已经投诉”，或者欺骗消费者“继续持有保单将会蒙受巨大经济损失”，以“全额退保”为幌子，怂恿消费者进行退保。

3. **诱导代理、非法牟利。**不法代理退保组织或个人，会诱导消费者签署代理退保服务协议，甚至以扣留保单、银行卡、身份证件等手段，对消费者加以控制，牟取高额的咨询费、手续费。

4. **伪造证据、要挟退保。**不法代理退保组织或个人，会唆使消费者无视合同约定，通过电话录音、微信聊天等方式诱骗销售人员回复，进行虚假取证，或者通过伪造微信聊天记录、捏造违规销售的虚假事实，要挟保险公司全额退保。



5. **切断联系、反复施压。**不法代理退保组织或个人，会切断消费者的正常维权通道，阻止消费者和保险公司、监管部门进行有效联系，或者打着“维权”旗号，鼓动或替代消费者采取缠访、闹访等过激行为，通过反复向监管部门恶意投诉等方式给保险公司施压。

【小渤提示】

1. **防范信息泄露，保护个人隐私。**消费者要注重提高个人信息保护意识，切勿轻信“代理退保”，妥善保管重要身份信息以及银行卡、保单等敏感信息，切勿将银行卡、身份证、保险合同等重要单证轻易转交他人，以免给自身信息安全埋下隐患。消费者若发现个人信息被恶意使用、泄露或买卖，银行卡账户被冒用、被盗刷，应保存相关证据，及时向公安机关报案。若发现非法金融活动线索，可向金融监管部门进行举报。

2. **警惕非法代理，谨防资金损失。**建议消费者提高警惕，多了解非法“代理退保”的表现形式和潜在风险，切勿轻信非正规渠道宣传，不盲目听信非法“代理退保”组织或个人作出的“全额退保”“免费维权”的不实承诺，不要向其支付手续费或代理费，避免自身财产损失。

3. **正视保险功能，选择合适产品。**保险是风险管理的重要手



段，对保障个人及家庭财产安全和生活安定、保证企业持续经营和扩大再生产、维护社会稳定和经济发展，具有重要意义。消费者应根据自身的实际需求和风险承受能力选择合适的保险产品，购买前应充分了解保险产品的保障范围、责任免除、犹豫期、现金价值、退保损失等重要内容。如确有退保需求，应理性分析退保利弊、全面了解再次投保的相关政策，警惕“更高收益”“更全保障”等诱惑，购买或换购超出自身经济和风险承受能力的产品和服务，避免轻率退保、盲目换保造成损失。

4. 依法理性维权，拒绝非法代理。为维护自身权益，建议广大消费者增强理性维权意识，不要轻信不法分子虚假承诺，拒绝参与捏造事实、伪造证据、提供虚假信息等非法“代理退保”活动。如对保险产品或服务有疑问，可以通过保险公司官方客服电话、线下营业网点进行咨询了解。如发生纠纷，可与保险机构协商处理，也可通过向行业调解组织申请调解或向金融监管部门反映等方式提出合理诉求，依法维护自身合法权益。





关键词： 抖音客服



2025 年 1-2 月



全国各地

抖音，作为记录美好生活的平台，深受大众喜爱。然而，近期抖音客服诈骗事件频发，不少诈骗分子利用抖音 APP 客服的身份进行欺诈活动。对此，广大抖音用户务必保持警惕，谨防上当受骗。

金融服务守初心 消保为民显担当

【案例 1 回顾】

2025年1月6日中午，客户佐女士致电德阳支行零售客户经理小赵，称自己已将20万元未到期的定期存款转为活期，并咨询手机银行转账操作事宜。经小赵进一步询问了解到，佐女士接到一个自称“抖音工作人员”的电话，对方称佐女士已签约抖音直播服务，若不立即解约，每月将扣除800元费用，同时还要求佐女士把资金“虚拟转出”以“降低风险评级”。佐女士信以为真，按照对方指示将定期存款转为活期存款，并尝试通过手机银行进行转账操作。

小赵敏锐地察觉到情况异常，立即安抚客户情绪，对佐女士的转账操作进行及时劝阻，与此同时，联动支行营运经理小黄对佐女士的账户采取了“暂停非柜面业务”的紧急管制措施。随后，小赵向佐女士详细讲解了此类诈骗的常见套路，成功说服她前往网点办理换卡、修改密码及调降非柜面转账限额等一系列安全防范操作。最终，佐女士认清了诈骗风险，对德阳支行专业、高效的处置与服务表达了诚挚的感谢。

【案例2回顾】

2025年1月3日，大连中山支行接到一通焦急的求助电话，营运经理小曲从60岁的安阿姨颤抖的声音和慌乱的表述中意识到她可能遭遇了电信诈骗。小曲在确认安阿姨尚未进行任何转账操作



后，第一时间指导其拨打110报警电话，并详细告知需要向警方说明的要点信息。随后，小曲指导安阿姨按照账户资金余额由多到少的顺序逐个拨打银行客服电话进行紧急挂失。期间，由于过度紧张，安阿姨多次说错信息，小曲不断安抚，帮助其厘清思路，最终成功挂失安阿姨名下所有可能存在风险的账户，成功守住安阿姨6万余元积蓄，未遭受任何资金损失。

在确保资金账户安全后，小曲进一步与安阿姨沟通，得知诈骗分子冒充抖音客服，电话告知安阿姨误点击了直播会员功能，每月需要收取800元费用，如果安阿姨不在该平台做直播的话可以协助她关闭此功能。由于安阿姨刚刚下载抖音不久，便信以为真，跟着诈骗分子的诱导下载某浏览器，点击未知链接后手机彻底被对方控制，直至无法拨打电话。此时，安阿姨发现可能被骗，立即到附近商店借了电话，由于联系不上子女，刚好看到衣兜里小曲的名片，便立即拨打电话求助。

【案例3回顾】

2025年2月13日，海口金茂支行厅堂内一位72岁的曹姓阿姨一直在情绪激动地打着电话，引起了营运经理小孙的注意。小孙忙来到曹阿姨身边查看情况，只听见电话那头一位普通话不是很标准的男士声称为抖音官方客服，告知曹阿姨因涉及违法商城



活动，次日要扣取曹阿姨 9200 元。出于职业敏感性，小孙初步判断这可能是电信诈骗，遂询问曹阿姨发生了什么，是否需要帮助。曹阿姨摆手示意没事，但小孙丝毫不敢松懈，一直站在阿姨旁边关注此事。当听到“抖音客服”需要曹阿姨添加微信时，小孙马上在曹阿姨耳边提示其可能正在遭受电信诈骗，不要轻信。但曹阿姨仍未挂断电话，而是情绪激动地质问“抖音客服”为什么要扣她的钱，“抖音客服”则一直催促曹阿姨添加微信，此时小孙已经非常确定这就是电信诈骗，于是果断拿过曹阿姨手机告知“抖音客服”自己的身份，并称已经报警，随即挂断电话。

经小孙事后了解，曹阿姨当天本是来网点购买理财产品，途中收到几次“0096”开头的自称“抖音客服”打来的电话，显示来电地址为也门、阿曼等地，“抖音客服”称曹阿姨加入了抖音商城且涉嫌违法，次日将从其银行卡中扣取 9200 元。因不熟悉抖音操作，曹阿姨便相信了“抖音客服”地话，“抖音客服”在通话中一边询问曹阿姨个人信息，一边指导其在抖音操作并要求添加个人微信，并警告曹阿姨如果挂断电话，就不会帮其处理了。好在小孙及时发现异常并果断处理，避免了曹阿姨的经济损失。

【案例 4 回顾】



2025 年 2 月，张女士收到自称“抖音客服”的来电，对方告知张女士之前开通了抖音直播带货功能，现在试用期将过，若须继续使用，每个月将会扣除张女士 800 元会费。张女士表示自己并未进行过相关操作，要求对方立即关闭相关功能。随后“抖音客服”以帮助张女士确定绑定扣款银行卡信息为由，要求张女士下载指定的 APP，下载成功后，“抖音客服”对其手机进行了一系列远程操控。结束通话后，张女士收到一条保单质押贷款受理成功的短信，察觉异常的张女士赶紧联系了合肥分行营业部零售负责人小张，咨询如何处理。凭着专业的职业素养，小张立刻意识到张女士是遭遇到了新型电信诈骗，立即就相关情况向分行进行了汇报，分行管理层高度重视，迅速启动三级联动机制。分行在核实客户保单信息后，第一时间联系保险公司请求配合尽快完成该笔保单质押贷款止付，并最终在贷款资金发放前成功进行止付，阻止了犯罪分子的资金转移，为客户挽回了 28.82 万元的资金损失。

【案例 5 回顾】

2025 年 2 月 27 日，客户孙阿姨来到深圳福田中心支行，希望激活其长期未使用的银行卡。在柜员进行常规核查时，发现该账户主要用于定期存款，且近期并无任何交易记录。孙阿姨向工作



人员小刘透露，她曾接到了一个自称“抖音客服”的电话，对方声称她即将被扣费 688 元用于“抖音年度会员 VVIP 服务”，并提出可以协助其取消该服务，但需要她提供短信验证码。

小刘凭借敏锐的洞察力和丰富的反诈经验，立刻意识到这可能是一起电信网络诈骗。在安抚孙阿姨情绪的同时，迅速为其办理了银行卡挂失，并重置了密码，并向孙阿姨详细介绍了犯罪分子惯用手法。孙阿姨听后恍然大悟，对我行员工的专业素养和高度的责任心表示由衷的感谢。

【小渤观察】

早在 2024 年 2 月 1 日，“抖音安全中心”微信公众号便发布了《关于近期冒充“抖音客服”诈骗的提醒》一文，文中表示收到不少网友反馈，有诈骗分子仿冒“抖音客服”拨打网友电话，声称网友开通了抖音某项会员服务，以如不关闭将持续产生会费为由，一步步诱导网友下载第三方 APP 并进行转账等行为。

2024 年 12 月 23 日，“抖音安全中心”微信公众号发布《“客服来电”怀疑有诈？抖音上线“验证助手”帮助客户识别诈骗》一文，文中详细介绍了“验证助手”使用指引，客户可在“验证助手”中将自称“抖音客服”的来电号码、短信文本或网址链接录入进行一键验证，还可通过“线索举报”功能举报可疑的诈骗



信息。

2025 年 5 月 28 日，“抖音集团”微信公众号发布《抖音推出“官方动态验证口令”，校验“真假客服”防诈骗》一文，官宣抖音升级验证工具，在官方验证助手基础上推出新功能“官方动态验证口令”。该功能目前已进入试运行阶段，并将逐步扩大服务范围。

【常见“抖音客服”诈骗套路】

1. 骗子电话自称抖音客服，表示客户开通了某项会员服务。
2. 骗子谎称如不取消将持续产生费用，甚至影响征信，引导客户添加好友。
3. 骗子要求客户下载第三方 APP 并绑定银行卡，以“核实账户”为由要求转账测试。
4. 骗子以“转账失败”等理由诱骗客户持续转账。

【小渤提示】

1. 关注“抖音安全中心”微信公众号，实时接收官方一手公告信息。抖音已开通 24 小时“安全与举报专线”400-140-2108。
2. 如接到来电声称“您已开通直播付费服务，每月将自动扣费 xx 元”，并以“扣费失败将影响征信甚至面临起诉”等话术的



电话，请立刻挂断。

3. 抖音官方从未推出“抖音会议”APP，所有要求下载第三方软件、添加私人社交账号或开启屏幕共享远程操作的“客服”均为诈骗。





关键词：境外投资



2025 年 1 月 27 日



北京大望路支行

“杀猪盘”假冒淡马锡太白投资，上千人被卷走超亿元
新加坡总理黄循财遭“AI 换脸”，被用于多种诈骗活动

.....

今年上半年以来，新加坡境内已发现多起数额巨大、受骗人员众多的电信网络诈骗案件，国内不少投资者中招，犯罪分子多以“境外投资”为诱饵实施犯罪。

金融服务守初心 消保为民显担当

【案例回顾】

2025年1月27日(腊月二十八)，老年客户闻某来到北京大望路支行，要求提前支取一笔存期三年、金额为20万元的定期存款，闻某表示家中急需用钱，自己通过手机银行办理提前支取失败，故亲自前来柜台办理。

厅堂人员小李发现闻某的存单开立近两年，提前支取将损失全部利息，加之客户年龄较大，便引起了警觉。小李耐心地向闻某解释提前支取的损失，并询问其取款的具体用途。闻某起初含糊其辞，坚称取款是用于家庭开支，但在进一步沟通中，闻某透露自己计划将资金转入新加坡的一家投资公司，并表示自己之前已在该公司投资了几千元，已获得高额回报，因此决定追加投资以在春节期间获取更多收益。闻某还自信地表示，自己退休前有丰富的金融投资经验，能够识别诈骗。

小李意识到客户可能正在遭遇电信诈骗，立即联系了闻某的理财经理小耿和另一名厅堂人员小陈，三人共同为其进行了专业的投资分析，逐步引导客户认识到此次“投资”可能是一场精心策划的骗局。经过耐心劝说，闻某产生了动摇，暂时放弃了提前支取定期存款并转账的打算，离开了银行。

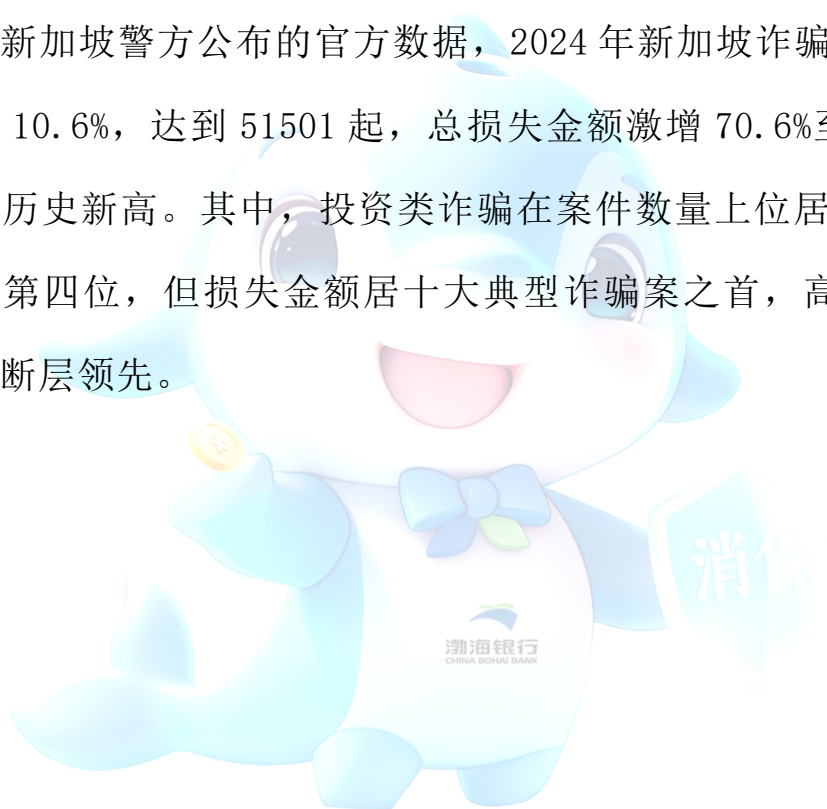
为确保客户资金安全，厅堂人员随后联系了属地派出所，报告了此情况。经派出所反诈专员进一步确认，闻某确实陷入投资骗局，警



方再次联系开展劝阻，同时联络闻某子女协作劝阻，最终闻某意识到自己陷入骗局。在银行、警方的通力协作下成功在春节前堵截了这起电信诈骗案件，避免客户损失20余万元。

【小渤观察】

根据新加坡警方公布的官方数据，2024年新加坡诈骗案数量同比上升10.6%，达到51501起，总损失金额激增70.6%至11亿新币，创历史新高。其中，投资类诈骗在案件数量上位居十大典型诈骗案第四位，但损失金额居十大典型诈骗案之首，高达3.2亿新币，断层领先。



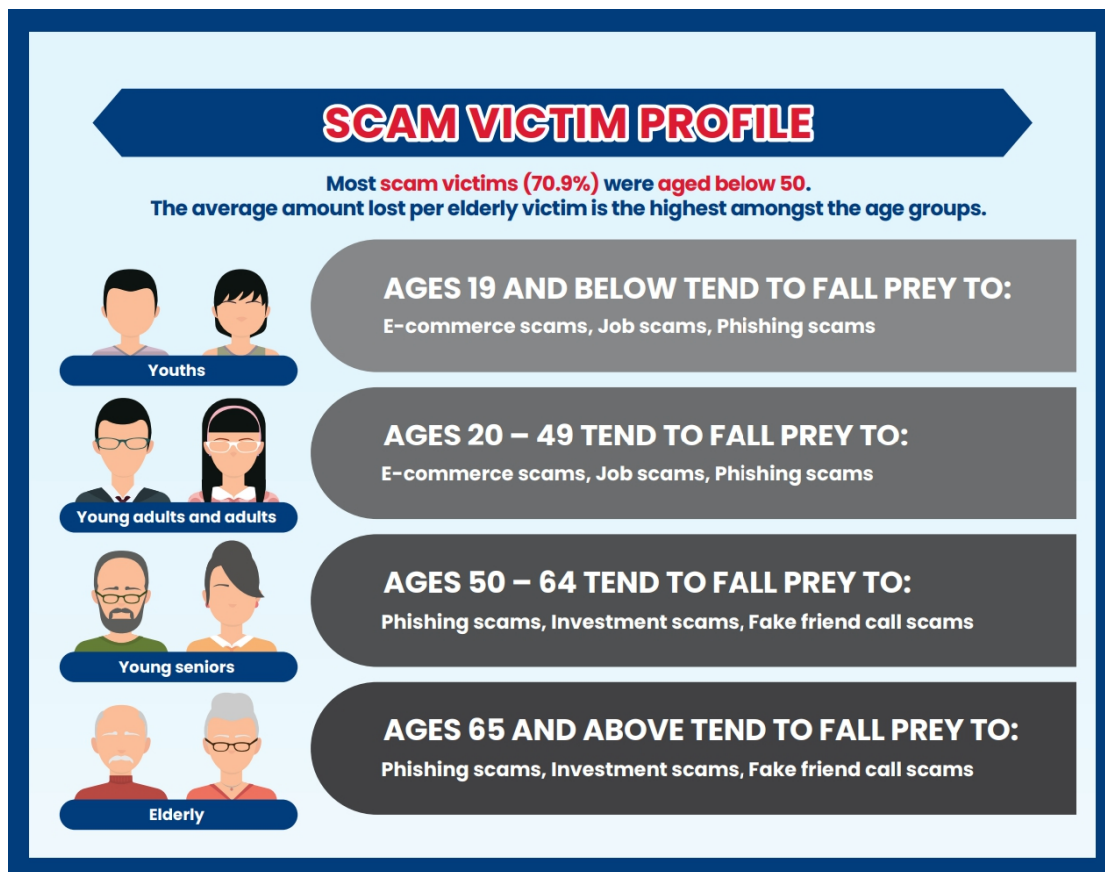


(图片来源: police.gov.sg 公布的 Annual Scams and Cybercrime Brief 2024 Infographic)

从受害者画像来看, 投资类诈骗“客群”清晰, 主要面向 50



周岁以上的中老年群体，而 65 周岁以上的老年群体被骗金额是所有被骗年龄段中最高的。



(图片来源: police.gov.sg 公布的 Annual Scams and Cybercrime Brief 2024 Infographic)

虽新加坡警方未就投资类诈骗的诈骗渠道进行单独解析，但从警方公布的诈骗渠道 Top5 可见，即时通讯工具和社交媒体牢牢占据前两位，且均较 2023 年有不同幅度的增长。





(图片来源: police.gov.sg 公布的 Annual Scams and Cybercrime Brief 2024 Infographic)

近年来,新加坡警方不断发布警方提示,提醒公众加强防范,避免陷入各类投资骗局。特别是 2025 年以来,在互联网上开始出现不法分子以政治人物和名人的名义宣传投资机会。根据互联网数据,仅 1 月份,至少 470 人报案,损失金额超过 3260 万新元。今年 2 月中旬至 3 月初,新加坡警方和当地银行联手开展“全岛大扫荡”,专项打击那些冒充政府官员搞投资诈骗和虚假招聘的骗子团伙。

【常见的投资诈骗类型】

1. 虚假投资平台。骗子仿冒合法金融机构或创建虚假网站/APP,承诺“高回报、低风险”,诱导投资者注资。
2. 社交工具诈骗。骗子通过即时通讯工具于投资者建立关系,



逐步诱导受害者参与虚假投资。

3. **加密货币与 NFT 骗局。**骗子利用投资者对区块链技术的陌生，通过虚假 ICO、伪造交易所、假钱包等实行诈骗。

4. **冒充政府或金融机构。**骗子伪装成 MAS、警方或银行，谎称账户涉及洗钱，要求受害者将资金转入“安全账户”。

【诈骗套路】

根据新加坡警方发布的诈骗月刊，不法分子主要通过两种方式诱导受害者上钩。

一是利用素未谋面的陌生人引导受害者加入虚假投资聊天群组，在群内营造高收益投资氛围，蛊惑受害者参与投资。

二是借助网络平台投放虚假投资广告，以极具诱惑性的宣传话术吸引民众点击，进而实施诈骗。这些虚假广告往往承诺超高回报率，却不提及潜在风险，误导民众做出错误投资决策。

在投资诈骗案中，骗子深谙心理战术，通常会先让受害者尝到小额收益的“甜头”，随后以“加大投资获取更高收益”“限时优惠”等理由，诱使受害者投入大量资金或加密货币。而当受害者投入巨额资金后，往往会发现难以获得承诺的回报，甚至无法取回本金，最终血本无归。



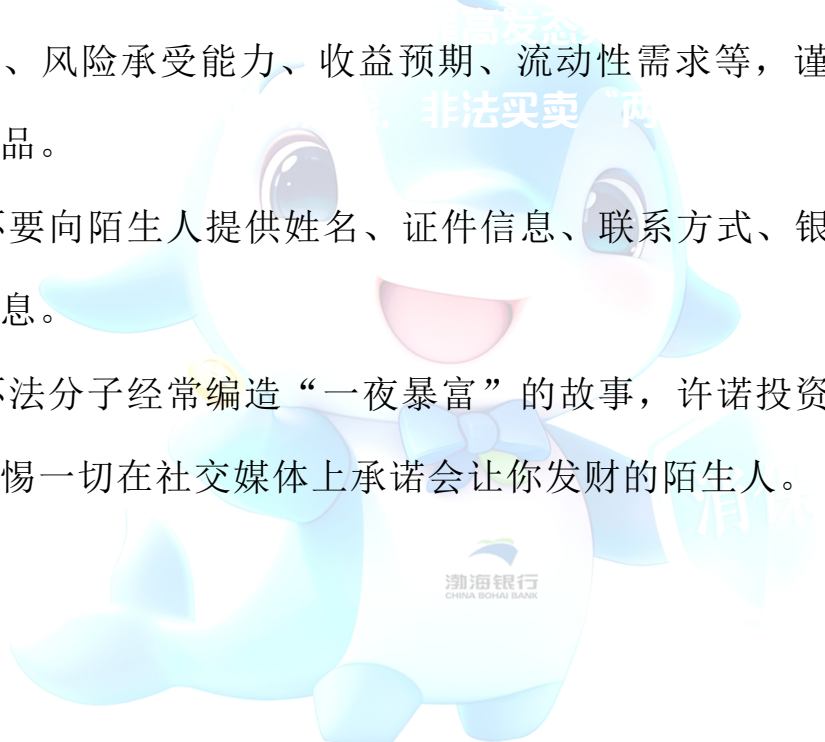
【小渤提示】

1. 在进行任何投资交易前，务必确认交易对象资质，避免与未经监管的平台和个人进行投资交易；不法分子编造各种虚假项目，有的甚至组织免费旅游、考察等，骗取社会公众信任。

2. 保持冷静与理性，不要贪心高回报，充分确认、了解风险后再进行投资交易。购买投资理财类产品要综合考虑个人及家庭财务状况、风险承受能力、收益预期、流动性需求等，谨慎选择合适的产品。

3. 不要向陌生人提供姓名、证件信息、联系方式、银行账户等个人信息。

4. 不法分子经常编造“一夜暴富”的故事，许诺投资者高额回报；警惕一切在社交媒体上承诺会让你发财的陌生人。



渤海银行
CHINA BOHAI BANK





关键词：实物黄金



2025 年 1-2 月



深圳前海支行

上海自贸试验区分行营业部

近期，黄金交易市场异常活跃。一些不法分子也嗅到了“商机”，利用实物黄金进行诈骗。此类骗局通常要求受害者以网约车、跑腿“闪送”、快递邮寄等方式，将黄金送至指定地点，以不见面、不现身的方式进行交易。黄金到手后，诈骗分子便会去金店销赃变现。与电信诈骗相比，此类骗局减少了网络转账，躲避了警方等部门的监管，追踪取证更为困难。

金融服务守初心 消保为民显担当

【案例 1 回顾】

2025 年 2 月 27 日下午，深圳前海支行迎来神情紧张的老年客户陈阿姨，她急切地要求提前支取 10 万元的定期存款。当柜员小张询问提前支取的原因时，陈阿姨表示她打算去兑换实物黄金，并提到有朋友可以帮她兑换投资金条，还能享受优惠。

小张凭借丰富的经验，判断陈阿姨可能遭遇了电信网络诈骗，于是立即将情况上报给了营运经理小王。小王将陈阿姨引导至会客室，进一步询问为何不通过手机银行 APP 购买黄金，而是急于购买实物黄金。陈阿姨解释说，一位所谓的“投资大师”通过社交软件添加她为好友，并邀请她加入一个“投资”群聊。该“大师”声称投资黄金可以赚取高额利润，并以大额转账不安全为由，诱导她通过购买黄金并通过邮寄的方式进行投资。只需将购买黄金的发票和快递单号发送给他，就可以在该软件上看到自动产生的收益。

小王迅速识别出该 APP 是一个虚拟交易平台，已被反诈中心判定为诈骗软件，遂耐心且专业地向陈阿姨解释了情况，揭露了这位“投资大师”实际上是一个诈骗分子，同时向陈阿姨展示了近期类似的诈骗案例，现场拆解了诈骗分子的话术漏洞，及时阻止了她的取现行为，成功保住了陈阿姨的 10 万元的养老钱。

【案例 2 回顾】



2025年1月23日,客户王女士致电上海自贸试验区分行营业部,预约24日取现50万元。营业部客户经理小范在与王女士的电话沟通中,王女士未对取现用途进行确认,仅表示自己使用,且在对话期间提及黄金、美元、装修、旅游、还债、医疗保健等词汇。因支行前期接到属地派出所提示目前被骗客户多涉及取现、黄金等,结合该客户属于老年客户、又涉及大额取现,担心王女士遭遇不法分子诈骗。小范计划于王女士次日临柜取现时和客户当面沟通确认。1月24日,王女士如约临柜,小范与其进行了充分沟通,结合近期电信诈骗典型案例、作案手法、危害等进行风险提示,并向其展示了公安局反诈中心的告知书,在沟通中确认王女士疑似遭遇黄金诈骗,经过小范的耐心劝阻,王女士最终放弃取现,同时小范及时向属地派出所进行了案情汇报。

【小渤观察】

2024年8月27日,天津市反电信诈骗中心微信公众号发布《夏季行动 | 警惕! 诈骗手段再更新? 凡是要邮寄黄金都是诈骗!》一文,公布三个典型案例并给出警方提示。

2024年11月27日,中国人民银行广西壮族自治区分行发布《警惕实物黄金诈骗 保护自身财产安全》一文,揭示骗局手法,提醒社会公众加强风险防范。



【骗局手法】

1. **诈骗手法多样。**兼职刷单、投资理财、冒充公检法等，这些都可以成为骗子骗取黄金的手段。骗子对受害人进行深度“洗脑”后，引诱受害人购买黄金、手机等容易变现的贵重物品，通过快递等方式寄送到骗子的指定地点。

2. **追查难度增加。**黄金保值性好，容易变现，方便运输，成为诈骗分子眼中的“理想工具”，通过诱导受害人购买黄金，诈骗分子能够更隐蔽、更快速地转移资金，增加追查难度。

3. **容易让人放松警惕。**购买黄金的行为再受害人心中往往具有更强的实体感和信任感，相较于无形的电子转账，黄金更能让人产生“真实投资”的错觉，从而放松警惕。

【小渤提示】

1. 不要轻信网上陌生人的投资建议，不要轻信不劳而获的高额返利，投资黄金务必通过正规平台渠道。

2. 网上陌生人不论以何种理由，要求使用自有资金购买黄金或为他人代购黄金或其他贵价物品，并要求邮寄至指定地点或派人上门来取的，都是诈骗。

3. 公检法及其他机关单位调查案件不会要求“验资”“打款”，所有通过私下联系，并要求转账、汇款、邮寄财物的，都是诈骗。



4. 广大黄金经营商户要谨慎接受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。不要因随意提供银行账户或收款二维码过账，而成为诈骗分子“洗钱”的工具。





关键词： 养老诈骗



2025 年 1 月



济南青年东路支行

近年来，针对银发族们的诈骗屡见不鲜，养老诈骗“套路”层出不穷、防不胜防。一些不法分子利用老年人信息闭塞、同情心重等特点，瞄准他们的“钱袋子”，花样百出地实施诈骗。

金融服务守初心 消保为民显担当

【案例回顾】

2025 年春节前夕，老年客户张阿姨到济南青年东路支行办理转账业务，工作人员小部发现其手机微信群频繁弹出“健康养生”产品接龙信息，群内宣称某多功能枕头可治疗失眠和脊椎问题，并承诺赠送价值 3888 元的智能心率仪。经询问，张阿姨已在该群购买过 3 万元理疗床，自称“使用后睡眠改善”，听说“枕头+床”组合治疗效果更佳，且春节期间有特惠活动，故前来网点办理转账。

小部一方面通过医疗器械查询系统帮助张阿姨查询，发现未能查到该款枕头的备案信息；另一方面向张阿姨展示了近期公安机关公布的同类诈骗案例，揭露犯罪团伙“先体验后消费”“专家讲座洗脑”“群托营造抢购假象”等新型作案手法，并结合各种案例向张阿姨解析了诈骗分子如何利用“亲情牌+伪科学+饥饿营销”的三重攻势突破老年人心理防线。经过近一个小时专业、耐心的劝导，张阿姨最终认清骗局本质，打消了转账的念头，并退出 3 个健康养生群。

【小渤观察】

近年来，会销、直销、传销的目标一直紧盯老年群体，利用老年群体对健康的迫切需求、情感孤独以及对新事物辨别能力较弱的特点，设计多种套路诱导其高价购买虚假产品或无效产品。

2025 年 4 月 14 日，市场监管总局印发《关于维护广告市场



秩序 营造良好消费环境的通知》，聚焦重点民生领域和互联网新兴媒介，从“医疗、药品、保健食品、特殊医学用途配方食品、医疗器械广告”“普通食品广告”“金融广告”“教育培训广告”“互联网广告”5个方面明确2025年广告监管有关重点任务，组织依法严查“神医”“神药”广告、食品广告疗效化宣传、保本无风险的金融理财广告、职业技能培训类违法广告、互联网违法广告等，切实守护消费者合法权益。

【常见“养老诈骗”套路】

2024年10月11日，公安部网安局发布针对老年群体常见的诈骗手段，“养生保健”赫然其中。不法分子以免费体验、领取奖品为诱饵，吸引老年人参加“健康讲座”“专家义诊”等活动，以“祖传秘方”为噱头，虚构或夸大产品功效，诱骗老年人购买“保健品”。

【小渤提示】

1. 老年群体要端正保健理念，从正规渠道获取科学的保健常识，到正规医疗机构就医，不轻信所谓的“特效药”。
2. 老年群体要主动增强防骗意识，警惕各种“讲座”“上门推销”，不盲目相信所谓的“公司实力”和“品牌效应”。



3. 子女要加强对家中老人关爱，多与老人沟通，向老人宣传反诈知识，可协助老人通过官方渠道核实医疗器械备案信息、公司备案信息等。如发现老人被骗，应耐心劝导，及时止损并报警。





关键词：银联会议



2025 年 1-3 月



北京魏公村支行

深圳宝安支行

近期，一种新型诈骗软件“银联会议”APP 在全国多地出现，目前已有多人上当受骗，受骗群体多为中老年人。

金融服务守初心 消保为民显担当

【案例 1 回顾】

2025 年 3 月 12 日上午，老年客户吴某接到一“保险公司”工作人员电话，对方自称某保险公司工作人员，称吴某此前购买过该公司一款保险产品，询问是否取消投保，如不取消将自动续费。见吴某质疑，对方称吴某可下载“银联会议”APP，对其身份进行验真。在该“工作人员”的指引下，吴某下载了“银联会议”APP，视频中对方身着“保险公司”工作服，在带有“保险公司”标识的办公室背景前向吴某报出自己姓名和工号，向吴某核实个人基本信息并展示其“保单”。吴某对此深信不疑，并在对方诱导下进一步泄露了个人账户信息、短信验证码等，并在建设银行手机银行输入银行卡密码。

诈骗分子利用获取的信息将吴某名下建设银行账户 13 万元资金转入渤海银行账户，并试图进一步转移。吴某在转账后心生疑虑，周边又暂无亲人询问，便立即报警，同时前往附近的北京魏公村支行进行咨询。大堂经理小贺及小郭进行简要沟通后，察觉到吴某言行异常，神色慌张，结合其所述情况，立即联系营运经理小杨核实账户情况，并启动应急预案，优先对涉案账户采取紧急冻结措施，成功阻断 13 万元资金划转。

随后，小李全程陪同吴某前往派出所完成笔录，并在其回行后补办相关冻结手续。客户吴某深受感动，多次对渤海银行的专业能力和



服务态度表示高度认可。

【案例 2 回顾】

2025 年 1 月 3 日 12 时左右，客户彭女士来到深圳宝安支行咨询电子银行转账限额上调业务，工作人员询问上调原因时，彭女士表示要购买国库券进行投资。

支行工作人员小张立刻提高警觉，经进一步了解发现，彭女士新加入一个名为“消协清退交流群”的微信群，群主在群里发布多笔国库券交易当轮获利情况。彭女士在“客服人员”的诱导下扫描二维码进行该“国库券”的购买，支付了人民币 5000 元。之后彭女士多次尝试提现，均未能成功，“客服人员”解释称系统原因，要求彭女士继续购买 3 万元“国库券”进行账户修复，并保证购买后 10 分钟左右即可提现到银行账户。彭女士因此来到网点办理提高转账限额业务。

根据彭女士描述，小张判断其遭遇了电信网络诈骗，随即展开劝阻，但彭女士表示该平台是正规的投资平台，很多客户通过投资都获利了，并翻出群里分享的各种投资获利图片。

小张随即将彭女士带至休息室，详细分析了该类诈骗模式：诈骗分子首先会吸引受害者加入所谓的“投资群”，通过群内的“托”发布投资受益信息，制造可信度。之后诱导受害者进行小额投资，并以



“账户冻结”、“系统问题”等理由，要求受害者继续转账支付“激活、修复费”或购买更多的国库券，从而实施诈骗。

小张同时在国家反诈中心搜索相关诈骗案例，并引导客户观看相关视频。终于，在小张的耐心劝阻下，彭女士幡然醒悟，放弃调额转账并在小张的协助下进行报警处理。

【小渤观察】

2025年2月7日，“公安部刑侦局”微信公众号发布《警惕！“银联会议”APP是诈骗软件》一文，“目标客群”精准锁定老年群体，全国多地已有多人上当。

2025年2月25日，中国银联发布声明，提示公众不法分子利用电信诈骗手段诱导用户在手机上安装“银联会议”APP，存在窃取敏感信息、资金被盗等安全风险。

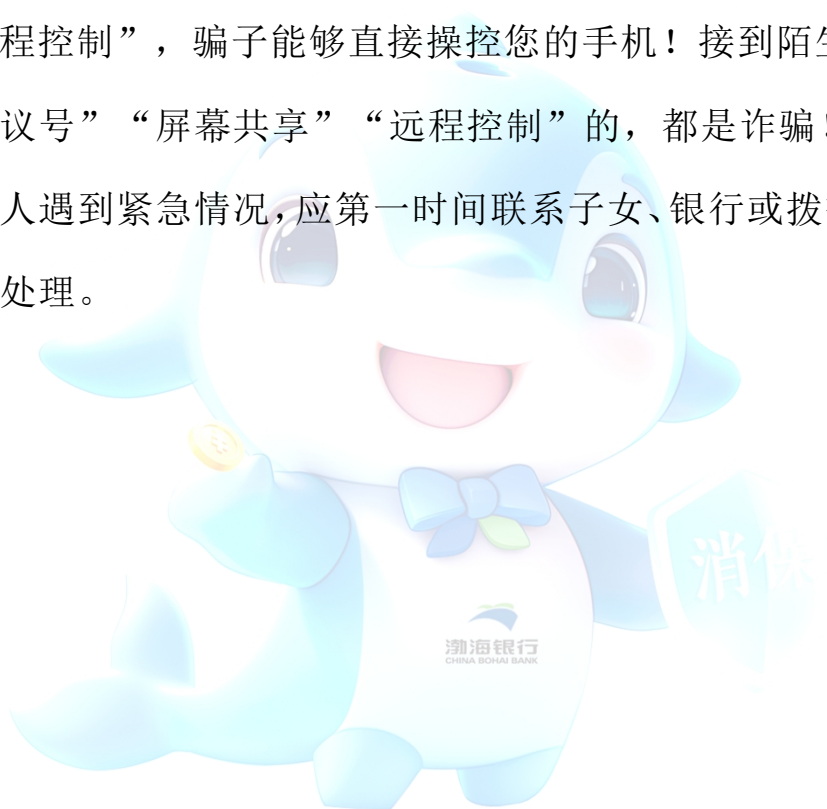
【常见套路】

骗子常常仿冒客服人员添加事主微信、QQ等聊天软件，诱导下载“银联会议”APP。下载后，骗子会要求事主打开屏幕共享或远程控制功能，要求事主登录手机银行，输入密码、验证码等信息，诱导事主对外转账或直接操控手机将事主卡内资金转走，从而实施诈骗。



【小渤提示】

1. “银联会议”APP 是诈骗软件！“共享屏幕”是诈骗手段！
凡是自称“客服人员”要求取消、关闭“直播会员、百万保障、百万保险”等业务，否则自动扣费、影响征信的，都是诈骗！
2. 不要“屏幕共享”，骗子能够看到您手机上的所有操作！
不要“远程控制”，骗子能够直接操控您的手机！接到陌生电话，提及“会议号”“屏幕共享”“远程控制”的，都是诈骗！
3. 老人遇到紧急情况，应第一时间联系子女、银行或拨打 110，
避免独自处理。





关键词：闲鱼



2025 年 1-2 月



深圳福田中心支行

深圳南山支行

在网络二手交易蓬勃发展的当下，闲鱼作为二手交易平台最活跃的APP，以一种新颖的方式出现在人们的面前，方便快捷的一键转卖闲置，只需要你有自己的淘宝或者支付宝账号就可以登录，买家卖家的个人信息都比较透明，备受年轻人青睐，但近年来闲鱼却也暗藏危机，各类诈骗案件层出不穷。

金融服务守初心 消保为民显担当

【案例 1 回顾】

2025 年 2 月 10 日 14 点左右，客户何女士来到深圳福田中心支行，申请办理银行卡限额提高及转账业务。在网点工作人员小刘询问业务用途时，何女士表示，第 34 届国际乒联-亚乒联盟亚洲杯乒乓球比赛将于 19 日至 23 日在深圳龙岗举行，届时孙颖莎、王楚钦等众多知名运动员将参赛。何女士计划通过闲鱼 APP 线上购买五天的门票，其中前三天票价 500 元/张，后两天决赛场次票价共 1500 元，总计 3000 元。

然而，在付款时卖家声称线上收款账户有问题，要求何女士通过微信线下付款。何女士同意后，先支付了第一天的 500 元，但因银行卡每日非柜面转账限额原因，无法完成后续门票款项的支付。何女士与“票务代购人员”协商，对方同意待何女士次日前往银行柜台调整限额后再继续付款。

小刘凭借敏锐的反诈意识，察觉到何女士可能正在遭遇电信诈骗，迅速采取行动，劝阻何女士停止操作，并协助她在微信平台进行举报申诉。同时，小刘向何女士详细介绍了电信诈骗的常见套路，明确告知客户这是典型的票务诈骗。最终，在工作人员的耐心劝说和专业指导下，何女士放弃了继续转账的念头，成功挽回了 2500 元的资金损失。



【小渤观察】

2019年8月30日和2023年8月14日，“闲鱼”官方微信公众号分别发布《闲鱼安全交易指南 | 牢记三不要，安心买买买》《闲鱼干货 | 4条你必须知道的闲鱼防骗小知识》，就平台交易进行相关风险提示。

2023年8月23日，“闲鱼”官方微信公众号发布《闲鱼干货 | 演唱会诈骗花样多，理智追星准没错！》，就闲鱼内购买演出类票务防骗小技巧进行提示。

【常见套路】

付款时，“票务代购人员”常以“账户冻结”等原因要求购买人脱离平台监控进行交易，但在并未真正在官方购票平台录入购买人信息的情况下要求购买人确认收货。

【小渤提示】

1. 所谓“内部票”“内部渠道”“联系购票客服”“福利票”都是骗子的套路。
2. 在闲鱼购买演出类门票，切不可脱离平台进行交易！脱离平台后，资金无法得到安全保障。
3. 以任何借口/理由要求转账的，务必提高警惕。



4. 在未收到门票或无法确认门票是否可用时，切勿提前点击确认收货。



【案例 2 回顾】

2025 年 1 月 10 日，年轻客户刘女士来到深圳南山支行办理非柜面限额提额业务，称仅需 935 元便可在“闲鱼”上购买 1000 元“盒马”储值卡，很划算。目前刘女士已经购买了 6 张，卖家仍有大量储值囤货，恰逢年货采购期间，刘女士本打算再买几张，但转账时发现转账限额不够，故来到网点准备办理限额调整业务。

支行工作人员小胥通过进一步询问核实，发现刘女士是通过微信与卖家联系的，对方要求刘女士提前确认收货方可提供卡密，工作人员立刻意识到这是一起典型的电信网络诈骗，立即对刘女士进行劝阻，并请其立刻通过“盒马”APP 确认礼品卡明细是否有变动。

刘女士查看“盒马”APP 发现，已经有了 2 张 1000 面额储值卡被司法冻结，赶忙通过“闲鱼”平台退款，挽回了部分损失。

【小渤观察】

2019 年 8 月 30 日和 2023 年 8 月 14 日，“闲鱼”官方微信公众号分别发布《闲鱼安全交易指南 | 牢记三不要，安心买买买》《闲鱼干货 | 4 条你必须知道的闲鱼防骗小知识》，就平台交易进行相关风险提示。

2023 年 11 月 20 日和 2024 年 7 月 6 日，无锡网上公安、张家港市公安局分别发布《警惕“双十一”前借“买卖礼品卡”实



施诈骗的预警》《网上买卖预付卡要留心，警惕诈骗圈套》公布了七起“闲鱼”平台相关案例，提示社会公众留意网上买卖预付卡骗局。

【常见套路】

不法分子在各二手交易平台发布或求购储值卡信息，利用低价售出或高价购买来吸引客源。当有人前来咨询时，不法分子会利用对方粗心大意的心理以各种理由要求在付款前获取对方卡密或诱导对方提前收货，在受害人完成交易后，将受害人拉黑。

【小渤提示】

1. 不要脱离平台沟通付款。闲鱼担保机制不能保护到平台外的交易，因站外付款产生的资金损失不能获得赔付。
2. 不要提前“确认收货”。买家点击“确认收货”后担保账户会将钱款转给卖家，由于是个人交易，平台无退款入口。
3. 不要听信保证金说辞。闲鱼售货无需缴纳任何费用，请勿轻信“保证金”“认证费”“买家保障”“店铺授权”等话术。如遇无法下单的情况，需要联系官方客服。



鸣 谢

向在一线默默付出的“反诈精英”致敬!

德阳支行

赵 莉 黄蓝仪

大连中山支行

曲笑梅

海口金茂支行

孙丽莉

青岛市北支行

刘 濛

深圳前海支行

张佩敏 王倩雯

深圳宝安支行

张慧琴

深圳南山支行

胥玉洁

北京魏公村支行

贺振刚 杨 铮 郭 瑾

北京大望路支行

李国庆 陈 翔

长沙友谊路支行

汪凯杰

合肥分行营业部

张 颖

济南青年东路支行

部琪琪

深圳福田中心支行

刘秋莹

上海自贸试验区分行营业部

范丽芳



金融服务守初心

消保为民显担当