

践行金融为民理念 筑牢金融安全防线

——2025年“全民反诈在行动”知识普及

编者按:金融安全关乎民生福祉,诚信环境系于行业根基。为帮助公众提升金融素养、筑牢反诈防线,树立理性投资观念,连日来,长治市银行业协会在国家金融监督管理总局长治监管分局的指导下,组织我市各银行业金融机构先后开展“金融知识万里行”“全民反诈在行动”集中宣传月活动,通过线上线下相结合的方式,深入社区、校园、企业等场所,系统普及防范电信网络诈骗、识别非法集资、合理配置资产等金融知识,揭露“高息理财”“虚假贷款”等骗局套路,传授识诈反诈实用技巧,从源头增强公众风险防范意识和自我保护能力,让金融服务真正惠及民生、护航发展。

每一次宣传都是一次守护,每一份认知都是一道防线。本报特推出金融反诈知识专刊,通过典型案例向广大读者普及防范非法金融活动知识,强化风险揭示,凝聚行业与公众的合力,共筑清朗诚信的金融生态环境。



一、什么是电信诈骗？

电信诈骗是指不法分子通过电话、网络和短信方式,编造虚假信息、设置骗局,对受害人实施远程、非接触式诈骗,诱使受害人给不法分子打款或转账的犯罪行为。电信诈骗手段翻新速度很快。有时候一、两个月就能产生新的骗术,令人防不胜防。

二、什么是网络诈骗？

网络诈骗是指以非法占有为目的,利用互联网采用虚构事实或者隐瞒真相的方法,骗取数额较大的公私财物行为。凡是打着“网络兼职”旗号,以返佣金为诱饵,要求你以刷单形式做任务的。凡是打着“零门槛”“无抵押”“当天放款”等旗号,以预付手续费、预交保证金、增

加银行流水记录等为由,要求先行转账汇款或者索要银行卡密码、手机验证码的。凡是自称公检法机关或金监局、医保局工作人员,以涉嫌严重违法犯罪并需要保密等为由,索要银行卡信息及密码、验证码进行“资金清算”或者让你直接把钱打到所谓的“安全账户”的。

案例分析



快递送礼引流骗局

典型案例:2024年4月2日,受害人(46岁)在家门口发现一个自己的快递包裹,包裹内有一张淘宝购物节宣传单,宣传淘宝正在做活动抽奖。受害人刮开抽奖区后发现中奖,遂按宣传单上提示扫码添加企业微信,根据对方指引加入到微信群领取奖品。在微信群内,受害人看到有网友发布兼职信息,称可以刷单返利。受害人遂按对方要求下载“万源”APP进行操作,先后转账7笔共计115万人民币。直至民警上门,受害人才发现被骗。

关键词:个人信息泄露、不明快递、二维码、领奖、群聊做任务。

受害对象:“70后”至“90后”女性为主。

防范要点:警惕“非买自来”的快递,所谓商家活动都是幌子,请勿扫不明来路二维码。

预防诈骗常识

◆ 保护个人信息

要保护好个人身份信息和账户信息,在非必要情况下不向陌生人提供身份证号、家庭成员、家庭住址等重要信息。

◆ 不轻信他人

不轻信他人,不点击不明链接、不贪图小利,绝不出售、转让、出租、出借或购买银行卡、支付账户等,若发现以上行为,要及时向公安机关举报。

◆ 不透露密码

将银行卡、网上银行、手机银行设置复杂程度较高的密码;任何时候都不向任何人透露或转发短信验证码及其他形式动态密码。

◆ 确认信息核实无误

接到熟人请求发送的转账信息,或询问银行卡密码等重要信息时,务必要通过电话、微信视频通话进行核实确认;避免在与移动支付软件绑定的银行卡中存放过多资金,以便分散和锁定风险。

◆ 安装国家反诈中心APP

牢记96110全国反诈劝阻专号,安装国家反诈中心APP,完成实名注册,并开通来电预警及APP自检功能。

常见诈骗类型

◆ 冒充公检法、政府部门诈骗

通过电话、短信或网络通知你涉嫌违法犯罪,发送伪造的通缉令、逮捕令,要求配合“保密调查”,需将资金转入“安全账户”或索要银行卡信息、验证码。

◆ 冒充电商、快递客服诈骗

自称平台工作人员,以“订单异常(缺货、质量问题)”“快递丢失”为由,向客户提出“退款、理赔、补发”,诱导点击钓鱼链接、下载不明APP,或索要银行卡号、短信验证码,甚至要求“先转账刷流水”。

◆ 虚假购物、服务诈骗

在非正规平台(如微信群、朋友圈、小电商)以“低价促销”“限量抢购”“海外代购”为诱饵,收款后不发货或发假货;冒充“导师”“专家”,以“培训、投资指导、情感咨询”等名义收费后失联。

◆ 游戏、账号交易诈骗

在游戏内或社交平台发布“低价卖装备、账号”“高价收号”信息,诱导消费者通过非官方渠道交易,以“账号冻结需解冻费、保证金”等名义要求转账,或发送钓鱼链接骗取账号密码。

◆ AI 技术诈骗(新兴高发)

利用AI换脸、AI拟声等技术,冒充亲友、领导发送视频或语音信息,以“紧急借钱”“项目垫付”等名义要求转账(如“我在外地出差,手机快没电了,先转笔钱到这个账户”)。

虚假网络诈骗途径

以“保本高息”虚假宣传吸引消费者

不法分子假借债券投资、股票投资、贵金属投资、期货投资、P2P投资、外币投资等概念,推出所谓“投资理财神器”,在网络平台发布消息宣称“稳赚不赔”,以高返利、按月返利、保持现金流等噱头吸引消费者关注。

以“专家内幕”虚假消息诱导投资

不法分子通过社交软件添加消费者好友,将其拉入“投资”群聊,然后冒充投资导师、理财专家,以“投资暴富案例”“直播课”骗取消费者信任,或通过婚恋交友平台与消费者确定婚恋关系,再以有“内部消息”“会员渠道”“特殊资源”等诱骗消费者参与投资。

以“投资返利”虚假平台转移资金

不法分子通过伪造或假冒投资平台,向消费者发送虚假链接,引导消费者下载APP进行投资,并以小额投资返利作为诱饵,不断引导消费者加大资金投入。不法分子随后迅速转移资金,甚至利用消费者急于提现的心理,以“登录异常”“服务器维护”“银行账户冻结”等名义,收取所谓“保证金”“解冻金”等,进一步扩大消费者资金损失。

防止诈骗措施

核心预防原则

1. 验证码是底线,谁要都不给

验证码是资金安全的最后一道防线,无论对方自称客服工作人员、公检法执法人员,还是政府机关领导,索要验证码时一律拒绝。

2. 转账前必核实,不见面不转账

凡是要求转账、汇款的,务必通过电话、视频等与本人确认(注意:警惕AI拟声/换脸,可要求对方说只有你们知道的“暗语”)。

3. 官方渠道最可靠,陌生链接不轻点

购物、缴费、办理业务等,只通过官方APP或官网操作;短信、网页中的陌生链接、二维码,一律不点、不扫。

4. 天上不会掉馅饼,贪心处处被套牢

凡是“低投入高回报”“免费领福利”“兼职轻松赚钱”的信息,基本都是诈骗,切勿因贪心上当。

5. 个人信息不外泄,隐私保护要做好

身份证号、银行卡号、住址、手机号等信息不随意透露;快递单、车票等含个人信息的单据需撕碎后丢弃。

分场景预防措施

1. 接到陌生电话、收到陌生短信时

自称“公检法执法人员的工作电话”:直接挂断,拨打110核实(公检法执法人员绝不会通过电话要求其转账到“安全账户”);自称“客服工作人员”:通过官方平台查询联系方式(如电商APP内的客服入口),主动回拨核实,不要相信对方提供的“新号码”;接到“中奖、退款、返利”的电话或短信时:直接拒绝,真中奖或退款都不会要求你先交钱。

2. 使用网络、APP时

只通过手机官方应用商店(苹果App Store、华为应用市场等)下载APP,拒绝“扫码下载”“链接下载”;不轻易添加陌生好友;对“荐股、投资、情感咨询”等私聊内容,一律无视;通过官方认可的交易平台,不私下转账。

3. 面对“领导、亲友借钱”时

务必通过本人常用电话确认(不要用对方提供的新号码);或故意说错信息试探(如“你上周不是说去北京了吗?怎么现在在上海要钱?”)。

被骗后如何减少损失

1. 保留证据

截图聊天记录、转账凭证、对方账号、手机号、诈骗链接等。

2. 紧急止损

立即拨打银行客服冻结涉案银行卡,或登录手机银行挂失;若通过支付宝、微信转账,立即联系平台客服冻结账户并申请止付。

3. 立即报警

拨打110或到就近派出所报案,提供证据并说明情况(报警越及时,追回资金的可能性越大)。

实用工具推荐

1. 安装国家反诈中心APP

可开启“来电预警”功能,自动识别诈骗电话、短信;还能学习反诈知识、举报诈骗线索。

2. 开启手机自带拦截功能

开启“陌生号码拦截”“垃圾短信过滤”,减少诈骗信息干扰。

温馨提示

一、不盲目轻信,不贪小利防骗局。树立科学理性的投资理财观念,提高风险防范意识和信息甄别能力,对退还费用、礼品赠送、保本高息、高价收购等“天上掉馅饼”的说辞保持警惕,避免贪图小便宜、遭受大损失。避免盲目跟风或投机心理,不轻信来路不明“小道消息”,不轻信“稳赚不赔”或“保本高收益”等说辞。在选择理财产品时,应选择正规金融机构并仔细阅读合同条款,充分评估自己的风险承受能力,选择符合自己需求的产品,提升识骗防骗能力,谨防财产遭受损失。

二、拒绝“共享屏幕”,保护信息防泄

露。增强个人信息保护意识,妥善保管身份证号、银行卡号、账户密码、验证码、个人生物识别等信息。不随意点击不明链接,不随意下载陌生软件、注册陌生平台或添加陌生好友,对个人社交账户的安全状况保持警惕,拒绝陌生人“共享屏幕”要求,避免无关人员操纵本人手机、电脑等电子设备,避免因个人信息泄露造成经济损失。同时,应加强对个人信息的保护措施,定期检查账户安全设置,及时发现并处理异常情况。

三、转账汇款严把关,谨慎操作护财产

涉及转账、汇款操作时要提高警惕,

防范资金被骗风险。在接到涉及要求转账汇款的电话、短信或网络信息时,及时通过官方机构核实信息的真实性,不轻信陌生人的转账要求或诱导信息,不贸然向陌生人提供的账号转账汇款,不随意向无关账户转账汇款。在转账汇款前,务必认真核对对方身份和信息,确保资金是转给真正可信的人员或机构。

四、正规渠道保权益,遭遇诈骗速报警。群众如遇经济纠纷,应依法通过正规渠道进行维权,可通过第三方调解组织进行调解、向司法机关提起诉讼。如发现自己陷入诈骗陷阱导致资金受损,或发现涉

嫌违法犯罪线索,应保存好聊天记录、通话录音、交易截屏等有关证据,及时向公安机关反映。同时,不可轻信网络上自称“网警”“黑客”等组织或人员,避免受骗。



网络交友骗局

典型案例:2024年3月22日,受害人(32岁)使用手机浏览到一款交友APP,注册后平台客服联系其称可以做兼职赚钱,其遂按照对方微信号指引注册账号并办理会员做任务,陆续向对方指定账户转账(期间有返现)共计70余万元。3月23日,受害人发现平台无法提现,意识到被骗,遂报警求助。

关键词:网络引流、约会APP、涉嫌色情、充值刷单

受害对象:以有不正当想法的青年男性为主。

防范要点:色字头上一把刀。抵制诱惑,洁身自好,遇到问题要及时报警。

演唱会门票骗局

典型案例:2024年3月10日,受害人在“闲鱼”平台上购买演唱会门票时,有人冒充平台客服联系其称购票款被冻结,需要其添加QQ号并进行转账验证,后按照对方指引向相关账户转账8.2万元,对方要求其继续转账,意识到被骗,遂报警求助。

关键词:网络引流、闲鱼平台、演唱会门票、虚假交易。

受害对象:年轻人群,学生群体等。

防范要点:注意在闲鱼、小红书等平台上,购物不要离开平台,更不要忽略平台风险提示,拒绝私下交易或提前确认收货,否则容易上当受骗。

虚假贷款骗局

典型案例:受害人想在网上申请50万元贷款,一名自称其是平安普惠银行的工作人员加受害人为微信好友,对方说可以帮受害人做低息贷款。于是,对方发给受害人一个二维码,要求其添加客服后,按照客服要求操作。受害人自己需垫付资金做流水提升自己的贷款额度。受害人做流水后,对方称受害人垫付资金做过的流水被冻结了,需要继续转账解冻资金,后发现被骗,损失125万元。

关键词:虚假广告、主动添加好友、二维码引流、刷流水。

受害对象:急需用钱“慌不择路”的人群。

防范要点:如有贷款需求,请通过正规渠道办理。正规机构在放款之前不会收取任何费用。