

以案说险

警惕AI新型诈骗
守护个人资金安全

案例分享

王女士系保险公司的客户，持有年金保险、增额终身寿险等多份长期人身保险合同。上述保单在犹豫期后累积现金价值，且合同条款约定具备保单质押贷款功能。近期，王女士接到一通陌生电话，对方准确报出了她的姓名、保单号及缴费年限。对方自称是保险公司“售后专员”，告知王女士其名下的旧保单可申领“**专项升级补贴**”，还能**免费提升保障额度，但名额限时有效**。

为获取信任，对方主动发起微信视频通话。借助AI深度伪造技术，“售后专员”的衣着装扮与正规保险专员别无二致，连声音都模仿得惟妙惟肖、几无破绽。这种看似“**眼见为实**”的逼真演绎，让王女士深信不疑，彻底放下了心中的警惕。

随后，“售后专员”以“线上核验业务”“系统升级验资”为由，诱导王女士开启手机屏幕共享，并在其指导下翻拍身份证、银行卡正反面信息，并录制人脸核验视频。同时，“售后专员”还指导王女士登录保险公司官方APP操作保单借款业务，谎称借出的资金仅用于“系统核对”，核验完成后即刻原路返还，且“补贴资金”将同步到账。

王女士依指引完成保单贷款后，“售后专员”随即发送一私人账户，以“**名额锁定、超时作废**”为由，施压其立即转账进行所谓“验资”。在即将转账的关键节点，王女士凭借此前积累的反诈意识，果断中止操作并联系专属代理人核实。经保险公司官方查证，该公司从未开展此类“保单补贴升级”业务，确认系不法分子利用AI技术伪造身份实施的诈骗。得益于代理人的快速响应与专业介入，成功协助王女士阻断资金流出，全额避免了财产损失。



案件剖析

以上案是典型的“AI技术”新型非法金融诈骗，骗局套路极具代表性，主要存在以下三大风险特征：

一、技术手段高科技化，迷惑性极强

传统诈骗易通过声音、样貌识破，而不法分子利用AI深度伪造技术，精准复刻保险从业者形象，使用非法获取的精准保单信息，直击消费者“眼见为实”的认知盲区。中老年客户及信息甄别能力较弱的人群极易中招。

二、诈骗场景精准化，针对性强

诈骗分子专门瞄准持有高现金价值、具备保单借款或退保权限的寿险客户群体。他们熟知保单借款、保障升级等常规保险服务流程，利用信息不对称，结合客户潜在的金融需求定制个性化诱饵。相比广撒网式的普通电信诈骗，此类骗局针对性更强、成功率更高。

三、心理战术紧迫化，闭环速度快

骗子全程利用“限时名额、过期失效”的话术制造紧张氛围，刻意阻止客户与家人、官方代理人核实沟通。通过屏幕共享窃取验证码、通过人脸采集突破生物识别防线，步步诱导客户完成资金操作，力求在最短时间内完成诈骗闭环。

消费者风险提示

骗术在升级，我们的防范意识也要随之“升级”。为了避免您的保单资产受到侵害，友邦人寿珠海中支为您梳理了针对此类AI新型诈骗的三大“避坑”指南：

1. 坚守官方渠道，拒绝私下交易

所有保单借款、退保、保障升级、权益申领等业务，仅可通过保险公司官方客服热线、线下营业网点、官方APP或官方微信公众号办理。任何通过私人电话、个人微信视频、陌生链接要求办理保单业务的行为均为骗局，切勿轻信。

2. 警惕AI合成，多重身份核验

遇到自称保险工作人员、监管人员要求视频核验或进行资金操作的情况，无论对方样貌、声音多么逼真，一律不要轻信。务必挂断通讯，通过官方联系方式或前往线下网点进行二次核验，杜绝AI诈骗陷阱。

3. 严守隐私底线，严禁屏幕共享

身份证、银行卡号、短信验证码、人脸影像以及手机屏幕共享权限，是资金安全的核心屏障。正规金融机构工作人员绝不会索要短信验证码，也不会要求用户开启屏幕共享。遇到此类要求，请直接拒绝并报警。

科技赋能生活的同时，也滋生了新型诈骗风险。在此提醒广大消费者**提高风险防范意识，擦亮双眼、谨慎操作，坚决远离各类新型电信诈骗**，全力守护个人保单资产与家庭财产安全。