友邦保险 健康长久好生活

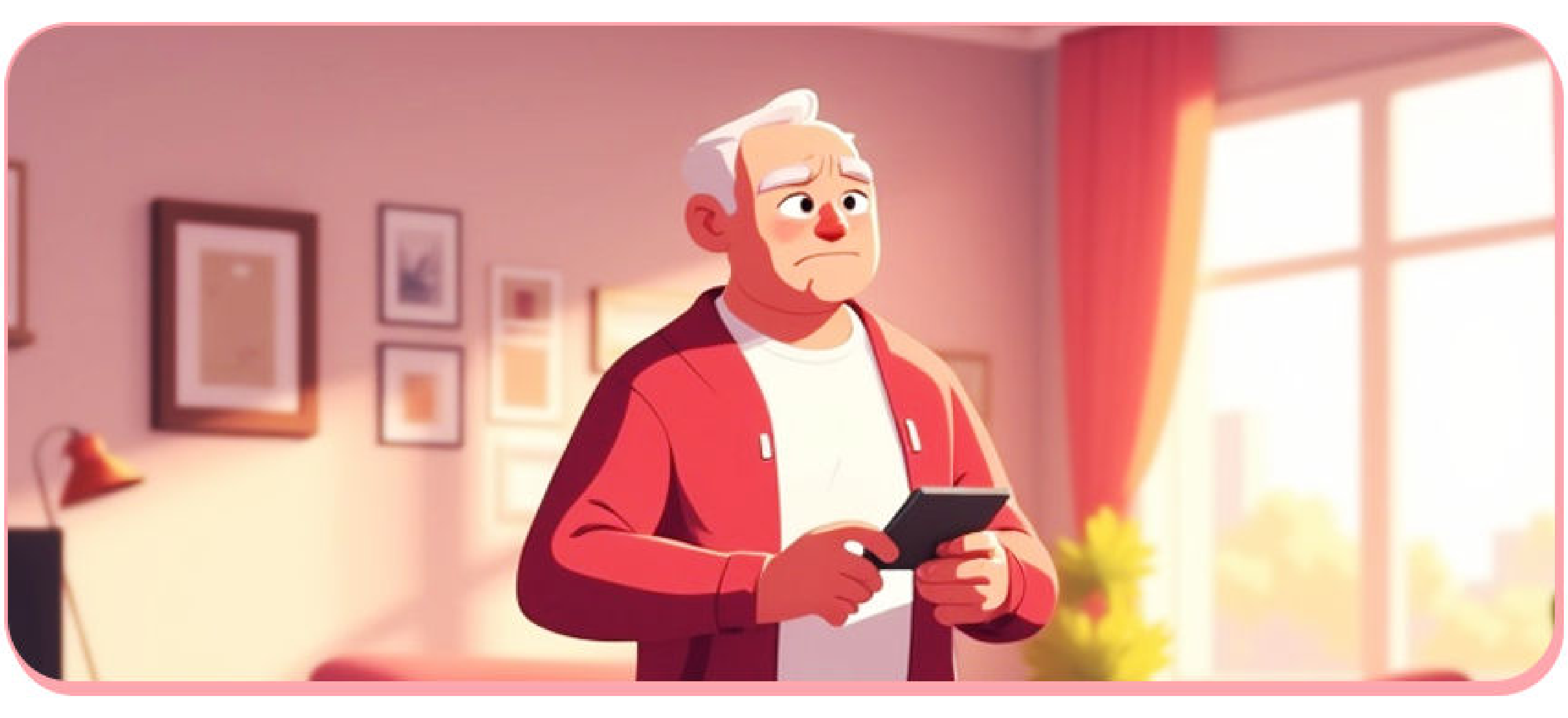
以案说险

“银龄守护·保险防线”
老年电信网络诈骗识别与防控实务指南

近年来，我国老龄化进程持续深化，老年群体已成为保险服务的重要客群，也日益成为电信网络诈骗犯罪的重点侵害对象。**尤为值得警惕的是——诈骗行为正加速“场景化渗透”，深度嫁接保险业务链条**：冒充保险公司客服、虚构保单异常、伪造理赔流程、诱导远程人脸识别等行为频发，且话术日趋“生活化”“日常化”，专挑老年人最关切的“养老金能否按时领取”“保单会不会失效”“身份证过期是否有影响”等问题切入，隐蔽性强、迷惑性高、危害性大。

案件背景

2024年6月，某省会城市65岁的退休工人张大爷接到一通显示为“955XX”开头的电话，对方自称“XX保险公司总部客户服务部专员”，声称张大爷于2015年投保的一份养老年金保险，因全国客户信息统一升级需要，在72小时内完成身份信息补录，否则将停止养老年金发放。为增强可信度，对方准确报出保单号、被保人姓名、已缴年限及当前应领取得年金金额，随即向张大爷手机发送了一条含短链接的短信，内容为：“请立即点击进入【官方保全平台】完成人脸识别验证”。张大爷未通过保险公司官方渠道核实，也未和子女沟通商量，便按语音提示操作：打开链接后，上传了本人身份证照片，并完成人脸识别授权。次日，张大爷名下另一张未绑定该保单的储蓄卡接连被转出合共4.98万元。事后经保险公司核查确认：该保单状态正常，无任何待办事项或信息补录要求；所涉链接为高仿钓鱼网站页面；对方所称“工号”在保险公司官方查询系统中查无此号。本案已由公安机关立案侦查，系典型的“冒充保险客服+钓鱼链接+远程操控”复合型电信诈骗案件。



案件剖析

本案暴露出三类典型风险断点：**一是官方渠道信任被系统性冒用**，骗子通过技术手段伪造官方号码，辅以基础信息增强可信度；**二是保险业务逻辑被蓄意扭曲与恐吓式重构**，将保单个人信息更新包装为“不办即停发”的刚性要求，叠加72小时时间压迫话术，制造紧迫感，诱导受害人仓促行动、放弃审慎核实；**三是数字身份核验机制被恶意劫持与滥用**，在受害人配合完成“眨眼、点头”等活体检测动作的同时，其生物识别特征已被非法截取；再配合短信验证码，即可绕过银行多重验证机制，实现资金“秒级转移”。

客户风险提示

为切实提升金融消费者风险防范能力，针对保险业务场景中高发、多发的诈骗行为，请广大消费者务必牢记并严格执行：

1.凡非官方渠道发出的不明短链接短信，一律不点、不传、不做——所有业务请通过保险公司官方渠道或服务网点办理；

2.凡进行远程“眨眼”“点头”式人脸识别，需提高警惕——非官方渠道要求您配合此类操作的，请立即终止操作；

3.凡声称“不操作就停发养老年金”“不更新就自动退保”，一律不信——保单效力与养老年金发放严格依据合同约定，需通过正规官方渠道做进一步核实确认。

- 友邦广东提醒您：金融产品查询平台为消费者查询合法金融产品信息提供权威渠道，您可登录https://www.Jrcpcx.cn，微信小程序以及手机APP搜索“金融产品查询平台”进行查询。

*AI协助制作

友邦广东揭阳营销服务部供稿