健康长久好生活

以案说险

警惕社交平台信息泄露 筑牢个人信息安全防线

案件背景

在数字时代，您的身份证号、银行卡号、健康告知记录、保单号、联系方式、家庭住址等，不仅是个人隐私，更是受《中华人民共和国个人信息保护法》《银行保险机构消费者权益保护管理办法》严格保护的敏感个人信息。一旦泄露，将可能迎来不可估量的风险，轻则遭遇骚扰推销，重则被用于冒名贷款、伪造理赔、盗刷账户，甚至成为电信诈骗、人身威胁的源头，直接危及财产安全与人身安宁。

案例还原：一张未脱敏的保单截图，引发8000元财产损失

投保人王女士在社交平台分享投保喜悦时，上传了未作任何脱敏处理的电子保单截图及身份证正反面照片（仅马赛克遮挡银行卡后四位），导致姓名、保单号、投保日期、年缴金额、常住地址等敏感个人信息被公开暴露。半个月后，其接到自称“XX人寿客服”的电话，对方精准报出其上述信息，，以“系统检测需条款升级激活，否则48小时内保障失效”为由，诱导其提供短信验证码完成“身份核验”。因信息高度吻合，王女士未通过官方渠道核实即配合操作。3分钟内，其绑定保单的银行卡被异地转账8000元。经保险公司核查，该公司从未开展所谓“保单升级”业务，确认系不法分子通过网络爬虫非法获取、拼凑其泄露信息实施的精准诈骗。

案件分析

1. 消费者自身防护意识薄弱：王女士在社交平台公开分享含敏感信息的内容，敏感信息随意公开，极易成为诈骗“燃料”，务必坚持“最小必要+全程脱敏”原则；

2. 信息拼凑诈骗手法升级：不法分子通过爬取社交平台、电商评论、公开文书等渠道获取碎片化个人信息，再借助黑产工具非法汇聚、关联、补全，形成高度完整的“数字画像”。此类诈骗利用信息高度准确的特点，大幅削弱消费者警惕性，显著提升诈骗迷惑性与得逞率，严重侵害个人信息权益与财产安全。

3. 对官方核验流程认知不足：王女士未通过保险公司官方渠道核实来电真伪，轻信陌生来电说辞，最终导致财产损失。

消费者风险提示

1. 强化敏感信息保管，杜绝主动泄露：妥善保管身份证号、保单号、银行卡号、短信验证码等核心信息，切勿轻易将此类信息存储在未经加密的手机相册、云端硬盘中；不随意向陌生人透露个人敏感信息。

2. 规范网络分享行为，做好全面脱敏：在社交平台分享与投保、理财相关的内容时，对保单号、身份证号、银行卡号、住址、联系方式等敏感信息，一律采取全字段打码、遮挡或删除处理，杜绝“部分遮挡”；坚持“能遮尽遮、能隐尽隐”，防范信息拼凑风险。

3. 提升诈骗甄别能力，坚守核验底线：接到声称“保单升级”“账户冻结”“退款理赔”“积分兑换”等陌生来电、短信或链接时，无论对方掌握多少个人信息，都切勿轻信。务必通过官方客服电话、官方APP、线下营业网点等正规渠道反向核实，坚决拒绝向陌生方提供验证码、密码等关键信息。

4. 及时采取止损措施，依法维护权益：若发现个人信息泄露或遭遇诈骗，应第一时间冻结银行卡、关闭快捷支付权限；向公安机关报案并保留回执；同步联系联系保险公司申请保单保护、更新预留信息及账户密码。全程留存通话记录、转账凭证等证据，通过合法途径最大化止损维权。

个人信息安全无小事，保险合同相关信息更是关乎长远保障与财产安全的核心隐私。希望广大消费者引以为戒，筑牢信息安全防线，与保险公司携手共建安全、放心的金融消费环境。

· 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

友邦珠海中心支公司供稿