

以案说险 | 网购“客服”谨慎核实，谨防电信网络诈骗

一、案例简介

市民小北在某电商平台购买了一款价值 500 元的护肤品，下单后第二天接到一个自称“平台客服”的电话。对方准确报出了小北的订单信息，包括商品名称、收货地址和联系电话，称由于仓库发货时操作失误，将她的订单标记为“批发商代发”，需要她配合取消，否则每月会自动扣除 500 元会员费。

小北信以为真，按照对方指示下载了一款“退款客服 app”，并在“客服”的引导下，先后在多个页面填写了个人信息后提交申请，并多次填写了手机验证码。直到后续收到多个借贷平台的提醒还款短信，小北才意识到被骗，此时已损失近 8 万元。

二、案例分析

本案例中，诈骗分子通过不法手段获悉了小北的交易信息，并据此获得了小北的信任。引导小北下载了诈骗 app 实施诈骗行为。整个事件中，小北有两次可以规避诈骗的时机：

一是莫名其妙的 app 不能下载，任何平台产生的交易或沟通信息均应通过平台完成，否则可能掉入诈骗陷阱。

二是在操作过程中，将个人信息和手机验证码填写至诈骗 app 内，收到手机验证码后，应谨慎核实验证信息内容，了解验证码来源，切勿盲目使用“快速填写”功能，避免被虚假引导办理业务。

三、风险提示

1. 警惕虚假客服联系：电商平台客服不会通过私人电话、短信或第三方社交软件联系用户，更不会要求下载非官方 APP。若接到类似电话，可通过平台官方渠道核实，切勿直接相信对方提供的联系方式。

2. 拒绝屏幕共享和远程操作：屏幕共享会导致个人信息、银行卡密码等被对方获取，远程操作更是可能被直接转移账户资金。任何情况下，都不要向陌生人开启屏幕共享或允许远程控制手机、电脑。

3. 切勿转账至“安全账户”：所谓的“安全账户”都是诈骗分子的陷阱，公检法机关、银行、电商平台等正规机构绝不会要求个人将资金转入陌生账户。遇到要求转账的情况，务必高度警惕，及时停止操作。

4. 保护个人订单信息：网购时不要随意泄露订单号、收货地址、联系方式等信息，收到包裹后及时销毁快递单上的个人信息，避免被不法分子利用。

5. 谨慎对待“退款、取消会员”等说辞：若对方以

“商品质量问题退款”“误开会员需取消”等为由要求操作，要通过平台官方客服确认。对于需要输入银行卡信息、验证码的操作，务必再三核实，防止信息泄露。

6. 及时报警并留存证据：一旦发现被骗，立即拨打 110 报警，并保存好聊天记录、通话记录、转账凭证等证据，为警方破案提供线索。