

以案说险

陌生来电要退款？屏幕共享别开启！
“两司两员”防骗指南请收好

案情回顾

外卖骑手小张接到一个自称“平台客服”的电话，称其前一日订单出现异常，需要理赔退款。对方准确报出了小张的姓名、订单号和送餐地址，取得了小张的信任。随后，“客服”引导小张点击一个链接填写银行卡信息，并要求开启“屏幕共享”功能以“验证身份”。在屏幕共享过程中，小张收到的短信验证码被对方窥探，随即银行卡内的2万元存款被转走。



案件分析

本案是典型的“冒充客服+屏幕共享”组合诈骗。

首先，信息泄露是突破口。不法分子通过非法渠道获取了受害人的精准个人信息（姓名、订单、地址），使受害人产生信任错觉。

其次，“屏幕共享”是核心作案工具。许多受害人误以为屏幕共享只是视频通话，实则它会将手机屏幕上显示的所有内容（包括短信验证码、银行APP界面、密码输入过程）实时同步给不法分子。

最后，心理操控是关键。不法分子利用受害人急于解决问题或担心账号异常的心理，通过话术诱导其脱离官方正规渠道，进入私下设置的诈骗流程，从而实施盗刷。

风险提示

为了帮助广大货车司机、网约车司机、快递员和外卖骑手等新就业形态朋友识破骗局、守护好来之不易的血汗钱，请务必牢记以下防范要点：

1.核实官方渠道：遇到订单异常、退款理赔、账号冻结等问题，务必通过官方接单APP内的客服渠道或官方电话进行核实，切勿轻信陌生来电。

2.严守“三不原则”：不点击陌生链接，不透露银行卡号、密码及短信验证码，坚决不与陌生人开启“屏幕共享”功能。

3.警惕“安全账户”：公安机关及正规平台不存在所谓的“安全账户”，凡是要你转账至指定账户进行“资金核查”的，都是诈骗。

4.安装反诈软件：建议下载并注册“国家反诈中心”APP，开启预警功能，及时识别拦截诈骗电话和短信。