这个钥匙扣，价值105万元

AI制图

近日，江苏阜宁市民袁女士遭遇冒充快递客服的电信网络诈骗，手机遭骗子远程操控，账户内105万元存款面临被盗刷风险。阜宁公安民警凭借随身携带的取卡针快速处置，成功保全全部资金，及时为群众挽损止损。

事发当日，袁女士接到一通陌生来电，对方冒充快递公司工作人员，谎称其网购包裹出现破损，可以申请三倍理赔。袁女士未加核实，按照对方指引下载具备远程操控功能的应用软件。安装完成后，袁女士手机迅速出现屏幕卡死、黑屏失灵的状况，电话、短信均无法正常使用，设备完全处于骗子远程控制之下。

阜宁县公安局反诈中心天鹅湖警务站接到反诈预警信息后，民警朱淑慧立即带领辅警赶赴现场。民警抵达时，袁女士仍手持黑屏手机，等待所谓“客服”继续操作，浑然不觉自己银行卡已有1.9万元被骗子转走。

“先把卡拿出来！把网断了！”千钧一发之际，朱淑慧迅速接过手机，拿出随身反诈钥匙扣上的取卡针，当即取出手机SIM卡、断开网络连接，强制手机关机，直接切断诈骗分子远程控制通道。与此同时，民辅警迅速赶赴银行，紧急办理账户止付与挂失手续，与诈骗分子争分夺秒。得益于处置及时，已经转出的1.9万元被全额拦截退回，袁女士账户合计105万元存款全部得以保全，没有造成经济损失。

事后，袁女士专程将一面锦旗送到天鹅湖警务站，向快速处置险情的民辅警表达谢意。据朱淑慧介绍，手机遭遇远程操控时，拔卡断网是最高效的应急手段。为出警时能够第一时间拿到取卡针，警务站民警统一配备定制反诈钥匙扣，将取卡针挂于钥匙扣上，全体执勤人员随身携带，以备突发劝阻现场使用。

综合新华社、江苏警方

套路分析

第一步：精准撒网，获取信任

诈骗分子通过非法渠道购买或窃取用户的网购信息，包括姓名、电话、快递单号等。他们冒充快递公司或电商平台客服，发送“快递破损”“丢失”或“滞留”的短信。因为信息准确，受害人极易放松警惕。

第二步：诱导点击，植入木马

短信中会附带一个“理赔链接”或二维码。一旦点击或扫描，手机可能会自动下载木马病毒，或者跳转到一个高仿真的钓鱼网站。

第三步：窃取信息，远程操控

在钓鱼网站上，受害人被要求填写银行卡号、密码、身份证号等敏感信息。随后，骗子会以“理赔需要验证”“操作失误需重新认证”等理由，诱导受害人下载会议软件并开启屏幕共享。

第四步：盗刷资金，卷款跑路

一旦开启屏幕共享，骗子就能实时看到你手机上的所有操作，包括弹出的短信验证码。他们利用这些信息，在你的银行账户中进行转账、贷款，瞬间盗空你的钱包。

手机被远程控制如何处置？

当发现自己的手机疑似被远程控制时，不要慌张，可以按照以下方法紧急处理：

- 拔掉手机的SIM卡
- 关掉家中的路由器
- 冻结银行卡
- 查杀是否还有其他木马病毒
- 尽快修改银行卡密码

网络安全防范小贴士

日常上网防骗要点

1. 软件只从官方应用商店下载，不点击陌生链接，不扫描来历不明二维码，拒绝安装陌生人推送的会议、客服、辅助工具类App，严防木马、恶意程序入侵手机。

2. 坚决拒绝“屏幕共享”权限。冒充电商、快递客服实施理赔退款诈骗时，骗子多以屏幕共享窃取验证码、银行卡信息，凡是要求开启屏幕共享的，一律视作诈骗风险信号。

3. 谨慎连接无密码公共WiFi，公共网络环境不要操作网银、转账、登录支付账号，关闭手机WiFi自动连接功能，避免接入钓鱼网络。

4. 重要账号开启二次身份验证，不使用简单密码；定期查看账号登录记录，出现陌生设备登录，立即修改密码并解绑可疑设备。

高发诈骗识别提醒

1. 冒充电商物流客服诈骗：骗子获取快递信息后，以包裹破损、丢失为由提出理赔退款，诱导下载陌生软件、索要验证码。理赔退款务必在购物平台官方客服渠道核实，不相信主动打来的理赔电话。

2. 刷单返利、虚假投资理财诈骗：“刷单本身即是违法行为”，凡是宣称低投入、高回报、稳赚不赔的网络理财、投资项目，均为诈骗圈套，切勿转账参与。

3. 牢记反诈口诀：未知链接不点击，陌生来电不轻信，个人信息不透露，转账汇款多核实。96110反诈预警来电务必接听，接到可疑情况及时拨打110报警。

个人信息保护提示

1. 身份证号、银行卡号、短信验证码属于核心敏感信息，绝不向陌生人提供；非必要不向App开放通讯录、位置、摄像头、麦克风权限。

2. 不租借、不出售本人电话卡、银行卡、互联网账号，避免沦为电信诈骗犯罪的工具，承担法律责任。

3. 家庭智能摄像头不要布置在卧室、浴室等私密区域，及时关闭设备不常用的远程访问功能，定期检查设备登录记录，防范隐私泄露。

综合央视网、国家反诈中心等公开科普资料