

来源：南海公安

现如今

手机的功能越来越丰富

从最开始的打电话、发短信

到如今的网购、看剧、玩游戏

只要我们能想到的

手机几乎都可以做

不过，手机上的

来电呼转模式别轻易设置

屏幕共享功能也别随意打开

平洲一女子因此差点丢了100万

近日中午，平洲派出所接到佛山市反诈骗中心南海分中心的紧急预警：胡女士（化名）正遭遇“冒充公检法”诈骗。民警随即多次拨打胡女士电话，但电话却一直处于无法接通的状态。根据工作经验，民警判定是诈骗分子诱导胡女士设置了来电呼转模式，导致民警的电话一直打不进去。

经民警的不断尝试，电话终于打通了。“喂，您好！请问您是不是接到了一个以00853开头的境外电话？”接到民警电话后，正被假“警察”骗得晕头转向的胡女士一时回不过神来。民警随即在电话中耐心安抚胡女士慌乱的情绪，并拆解了假“警察”的招数。



“打开‘屏幕共享’功能，你在手机上的任何操作，对方都看得一清二楚。”在民警的指引下，胡女士快速卸载了屏幕共享App，并让其马上联系银行，将转移出去的100万元再转移到其他账户中，防止被骗子转走。因民警的及时劝阻，胡女士并无财产损失。



无论是你的登录账号密码

还是支付密码

只要点击了“屏幕共享”功能

对方都能看得一清二楚

怎么样？

“屏幕共享”功能里暗藏的猫腻

大家都了解了吗？

诈骗套路

01

骗取信任、切断与外界联系

骗子通过非法渠道取得受害人信息

，准确说出受害人的身份证号、住址，并使用技术手段将来电号码仿冒为驻外使领馆电话号码，获取受害人初步信任。同时，诱导受害人开启来电呼叫转移功能，切断其与外界的联系，使受害人身陷“孤岛”。

02

诱导设置屏幕共享或下载视频会议

不法分子通过一些App自带的屏幕共享功能或者视频会议的形式，假借引导受害人进行操作为由，实则实时监控受害人手机上的所有操作，盗取受害人的个人隐私信息和验证码等内容。

03

转账汇款

不法分子监控受害人手机后，开始引导受害人转账，如被发现，或者受害人迟疑，不法分子将通过偷偷获取的验证码进行转账操作，在受害人毫不知情的情况下被转账。

常见的呼叫转移设置方式

手机怎么设置呼叫转移？

学起来，别被套路了！

01

在手机正常待机状态下输入 “\*\*21\*号码#” 后按拨号键，即可设置全部来话呼叫转移。

02

在手机正常待机状态下输入 “\*\*67\*号码#” 后按拨号键，即可设置遇忙呼叫转移。

03

在手机正常待机状态下输入 “\*\*61\*号码#” 后按拨号键，即可设置无应答呼叫转移。

04

在手机正常待机状态下输入 “##002#” 后按拨号键，即可取消所有呼叫转移设置。

（适用移动、联通用户）

警方提醒

手机越来越先进

形形色色的智能功能

在便利了人们生活的同时

也为安全埋下了隐患

市民不要轻易设置

来电呼叫转移功能

不要与陌生人开启屏幕共享功能

涉及私人信息

特别是银行卡密码、验证码时

一定要谨慎

如若被骗

请立即拨打110报警

素材来源 | 平洲派出所