网络图片

“接了个会议电话，手机银行App里面的存款就被诈骗分子转走了。”近日，受害者常燕（化名）向记者说起了被诈骗的经历。对方利用一款名为“银联会议”的会议软件，将她多个银行卡账户中30多万元资金“盗”走。据常燕回忆，诈骗分子分别谎称抖音平台客服、中国银联工作人员，让其下载了“银联会议”App，这款软件看上去与普通会议软件无异，却在接通电话后无法挂断、出现“黑屏”。

拥有多年反诈经验的专家陈国平告诉记者，“黑屏”时就是诈骗分子控制常燕手机、转移资金之时。今年以来类似案件频发。中国银联今年初就此事专门发布严正声明，澄清“银联会议”App非中国银联产品，提醒公众提高警惕。

揭秘“银联会议”App骗局：

一通来电几次“黑屏”后，存款被转走

诱导下载“银联会议”App 使用时无法挂断、出现“黑屏”

今年4月的一天，刚刚退休的常燕接到一通自称抖音客服的电话，对方准确报出常燕的姓名和身份证号码后称，常燕在抖音平台购买了价值9600元的包年会员。该会员按月扣费，且从当月开始。

常燕告诉记者，虽然自己从未在抖音上注册，也未开通任何会员，但对方能够准确报出身份证信息，因此对其话术将信将疑。对方还引导她回忆是否有人动过她的手机，让她一度以为是小孙子贪玩误点了会员。对方告诉她，可以关闭会员，防止扣除更多的资金。

然而，这一看似“贴心”的服务，才是常燕掉入陷阱的开始：所谓关闭会员的方法，是让常燕关掉银行的免密支付功能。由于常燕不知道是哪张银行卡扣费，也不知如何关停免密支付，对方便让她下载“银联会议”App，并称会有“银联专员”指导操作。也正是在这个所谓“专员”的“帮助”下，让她痛失数十万元。

“这个软件看起来跟银联有关，让我放下不少防备。”常燕告诉记者，银联是正规机构，且会议软件从华为手机官方App商城下载，并非点击对方提供的链接地址，因此她并未质疑该App的真实性。

但这看似是“正规军”的App，却是诈骗分子精心设计的诈骗工具。常燕回忆，该软件的界面与普通的会议软件相差无几，但在接通后“猫腻”逐渐显露。

“刚开始他们引导我挨个打开手机银行App，输入用户名、密码、手机验证码等信息。”常燕告诉记者，但每次在成功登录手机银行App后，手机就会突然“黑屏”，持续几秒钟。对方告诉她，这是在帮她“关闭免密支付功能”。

而在如此操作了几个常燕经常使用的手机银行App后，对方告诉她，她手机里还有几个手机银行App没有处理。

“这都是我不常用的手机银行，而且并未视频通话，他们怎么知道我手机里还有别的银行App？”常燕开始心生疑惑。此时她又发现，她竟然无法挂断会议电话。但对方“安慰”她马上结束了，她又将信将疑地打开了另一个手机银行App。最终，常燕儿子发现了母亲这通电话时间过长、通话内容有问题后，强行将手机关机才中断了通话。

诈骗分子控制手机转移存款 资金在多家银行来回转账

在手机重启后，常燕发现，自己在交通银行、建设银行等多家银行的活期存款均被转走。部分银行账户中的定期存款也被全部赎回变成活期存款，随后转走。她购买的理财产品由于无法实时到账才“幸免于难”。在使用“银联会议”App期间，常燕无法正常接听电话，也无法收到来自银行转账的信息。

陈国平告诉记者，这些所谓的“会议软件”实际上都内含“病毒”或“后门”。尽管受害者无法看到对方，但对方却已经掌控了受害者的手机。“屏幕共享，如同钱包被抢。”陈国平指出，受害者在输入账户名、密码时，信息已经泄露给对方。而所谓“黑屏”，是诈骗分子操纵手机银行App转账的过程。主动退出该App只能强行关机。如果对方知道了受害者的账户和密码，银行也很难识别是诈骗分子的恶意转账。

广发银行工作人员告诉记者，在控制了手机、掌握了手机银行密码后，诈骗分子就可以随意进入被害者的手机银行进行操作，由于此时手机银行验证码也被诈骗分子看到，因此可以轻松转移受害者的存款。

常燕告诉记者，她在梳理各家银行损失时发现，不少资金在多个银行之间来回转账，最终分多批汇出，有两笔资金分别转入了不同的个人账户。目前，对其被诈骗的资金具体去向，常燕称警方仍在进一步调查中。

常燕的资金为何会在多家银行来回转账，又为何会出现两个实名的个人账户？

陈国平表示，通常来讲，银行与银行之间相互转账，可以从一定程度上迷惑警方、拖延调查时间。这将让诈骗分子更有时间将资金进行转移。针对两个个人实名账户，陈国平猜测，这两个实名账户背后的人有可能也是受害者。

“现在诈骗分子‘洗钱’路径更加隐蔽。”陈国平解释道，一些诈骗分子会利用不知情的商家，用骗来的资金直接购买某种商品（如茅台酒、黄金等），随后他们再将这些商品卖掉来“洗白”赃款，这让警方难觅资金踪迹。

要关注App、手机系统、银行卡账户安全

常燕的遭遇并非个例。有银行透露，仅3月初至4月底，该行北京分行发现并堵截了类似案例30起左右，涉及金额近500万元，这些“未遂骗局”的受害者均为老年客户。

在这些案例中，诈骗分子使用的身份千差万别，但套路雷同。有的冒充平台客服，称受害者订购了“百万保险保障”，需要每月扣除一定费用，但可以协助取消；有的则冒充“法院”人士，称受害者因涉案被诉，可帮助其消除误会等。在取得信任后，他们会诱导受害者下载“银联会议”“银监会议”等与权威机构有关名字的会议软件，操控和监视受害者手机，并转走所有可转走的资金。

近期记者查看苹果、华为等多个品牌手机App商城发现，目前已无法找到该App。

银联安全专家表示，金融消费者首先要关注App安全。下载App不要点击或扫描短信和社交软件中的网址或二维码。若误点击，也不用紧张，手机系统会提示即将下载文件，此时，要点击拒绝。如果在手机新安装了相关企业的App，应当立即致电该企业官方客服电话核实真实性，金融企业的官方客服电话是全国统一号码。

“是否为官方客服的最好验证方式是，先挂断打入的客服电话，然后再拨打平台官方渠道公布的客服电话询问，对相关情况进行求证。”陈国平指出，当前个人信息泄露渠道较多，因此即便对方报出了准确的身份信息，也不能轻信。

银联专家还提示，金融消费者还需要关注手机系统安全。如果用户发现手机系统中存在陌生App，应使用手机系统自带的安全软件进行安全扫描，对于提示未知来源或有风险的，应当立即卸载。此外，还可在工信部政务平台信息备案管理系统网站查询此App备案情况，若提示没有备案，应立即卸载。

“金融消费者还应关注银行卡账户安全。”银联专家指出，部分诈骗类App的恶意程序含有屏幕共享功能，有的App还含有特殊的手机黑屏程序，虽然用户看不到屏幕，但不法分子可以远程查看到支付验证码。建议用户及时关注银行账户大额资金变动情况，如有疑问及时致电发卡银行。 （据《新京报》）