全民反诈14

共享屏幕 手机被远程操控 警方出手 止损430万元

下载共享屏幕软件后，锦州王先生的手机很快被骗子远程操控。手机银行登录密码也被修改，账户里450万存款已经被转出了20万。幸亏民警迅速操作，多方联系冻结账户，成功拦截了剩余430万元。

报警人来到派出所 银行卡已被转出20万

2022年12月5日晚9时许，辽宁锦州北镇市公安局中安派出所接到“110”指令，辖区群众王先生正在遭遇电信诈骗。接到指令后，派出所民警立即联系报警人，了解基本情况，但电话却突然被挂断。当工作人员再次将电话回拨，对方却称其没有被诈骗，匆匆挂断了电话。

细心的工作人员发现，前后两次虽然拨通的电话号码一致，但通话人的声音却有差别。民警再次拨打电话，又始终无法接通。此时，疑似受害人的王先生却匆忙自己来到派出所。办案民警第一时间查看了王先生的手机，发现其手机多次出现无法接到来电的情况。民警判断，一定是诈骗分子操控了手机，为转移钱款延长时间。

王先生被诈骗了，要抓紧时间处置，争取最大限度减少损失，民警立即接过王先生的手机登录手机银行，却发现登录密码已被操控更改，经多次申请重置，终于成功登录。办案人员发现银行卡已被转出20万元，另有430万元，部分购买了澳元、加元、新元外汇，虽转变形式，但未被转出。

民警迅速处置 成功拦截止付430万

民警马不停蹄采取多方措施开展工作，迅速与指挥中心、市局反诈中心进行沟通，及时提供王先生相关详细信息，并冻结王先生个人账户。同时，拨打银行人工客服电话，对账户“口头挂失”，连番紧急操作后，确保了卡内剩余资金安全。

因“共享屏幕”手机被远程操控

原来，当晚6时许，王先生接到一家快递公司电话，告知其购买的快递包裹感染了新冠病毒，要将快递销毁并对自己进行赔偿。

在按照对方指挥操作过程中，王先生陷入了层层陷阱。对方以减少损失为由，让王先生下载了屏幕共享软件，对王先生的手机远程操控，进而得知了其银行卡账号密码等重要信息。

如果不是民警迅速联系冻结了王先生账户，很可能其账户内的430万元存款也落入骗子手中。12月12日，王先生专程来到派出所为办案民警送来一面写有“人民警察为人民，失而复得暖人心”的锦旗。

插图 丁锐

警方提醒：

涉及疫情的快递退款诈骗，是近年来兴起的新型诈骗手段，广大市民一定高度重视，个人身份、银行密码等重要信息坚决不能泄漏。诈骗手段不断更新，但万变不离其宗，提高自身防范意识才能够真正筑起安全“防火墙”。

辽沈晚报记者 吕洋

购置百万黄金如“买菜” 原来是跑分洗钱

“年纪轻轻就要买这么多黄金？”“不现场刷卡，非要往我们的账户打钱。”

“也不挑款式和设计，只问重量和价格。”

“什么品类都买，感觉不像是投资的。”

沈阳中街步行街附近的多家金店常常有几名年轻男子“光顾”，购买价值百万的黄金饰品，出手阔绰引起金店营业员注意。究竟是“硬实力”还是有“猫腻”？

近日，沈阳市公安局沈河分局打掉一个帮助电信诈骗犯罪集团“洗钱”的犯罪团伙，抓获5名犯罪嫌疑人，当场查获准备为实施“洗钱”犯罪而购买的黄金饰品，价值107万余元。

11月中旬，沈河公安分局民警在工作中发现：有一伙人在沈阳中街步行街附近各大金店频繁出入，多次购买高额黄金饰品，形迹可疑。随后，民警开展工作，通过调查发现2名男子有购买黄金“洗钱”的嫌疑。

11月28日，民警在中街步行街某金店内将正欲购买黄金的犯罪嫌疑人38岁男子贺某、25岁男子林某抓获。

随后，民警又根据掌握的线索将另外3名犯罪嫌疑人33岁男子张某、37岁男子吕某某及60岁男子庄某某抓获。

犯罪嫌疑人贺某交代，他们的“上家”是境外电诈组织。电诈组织在实施诈骗活动时，会将大量涉案资金打进贺某持有的银行卡内，然后由贺某再通过购买黄金的方式将涉案资金第一时间消费，躲避公安机关的冻结止付。因为黄金流通性强、损耗小，他们在购买后会立即变卖，再通过购买虚拟货币的方式将钱转给境外电诈组织，这样一来就达到了将不法资金“洗白”的目的。

目前，犯罪嫌疑人贺某、林某等5人因涉嫌帮助信息网络犯罪活动罪已被警方依法采取刑事强制措施，案件正在进一步办理中。

辽沈晚报记者 吕洋

“共享屏幕”不安全 小心屏幕后的“第二双眼”

只要有人跟你提到视频会议、共享屏幕等，一定要当心了！因为“共享屏幕”就是骗子在你手机屏幕上的“第二双眼睛”。不久前，殷女士（化名）也因此被骗走了18332元。

被“共享屏幕”引导落入刷单骗局

这天下午，殷女士在刷短视频时看到一条刷单广告。出于好奇，她根据内容下载了APP。在客服的指导下，殷女士很快熟悉了刷单流程，并拍下了500元的指定商品。完成任务后，殷女士联系客服要求返还本金和佣金，却得到了这样的回复：“需要继续完成指定任务才能返现哦。”同时，“客服”要求她进行共享屏幕，来完成接下来的操作。

殷女士在客服“话术”的刺激下，再次输入银行卡密码，拍下了两笔千元订单。可殷女士刚完成订单，卡内1万元就被悄无声息地转走了。

“共享屏幕”就是第二双眼睛

警方介绍，目前“共享屏幕”已经成为不法分子进行电信网络诈骗的关键一环。

有不法分子让受害人下载远程会议软件，再利用其中的视频会议、共享屏幕等功能实施诈骗，共享屏幕就是把屏幕上显示的内容同步让对方看到，包括弹框显示短信、微信、其他APP推送的内容。也就是说，你在手机上的任何操作，对方都能看到，一旦受害人使用此功能，即使诈骗分子不主动询问，也能看到受害人手机上的所有信息，包括输入密码时跳动的字符、收到的验证码等，从而转走受害人卡内资金。

警方提醒：建议不要开启“屏幕共享”功能

建议大家不要开启“屏幕共享”功能，这会让你毫无秘密可言，特别是涉及银行卡密码、验证码的，一定要谨慎、谨慎、再谨慎！

比如收到验证码，诈骗端就能看到信息；受害人输入的支付密码等信息也会被犯罪分子一览无余。殷女士就是这样被“偷”走了银行卡密码和手机验证码，一个不留神钱就没了。

辽沈晚报记者 吕洋

总值班：杨 军
一版编辑：吴 昊
一版美编：王晨同
零售专供报
6 935970 566666

总第9849期 | 订报热线：22895302 广告部：22699260 | 社址：沈阳市青年大街356号 电报挂号：1032 邮编：110003 | 广告经营许可证：辽工商广字01—257号 发行单位：沈阳红马甲报刊发行物流配送有限公司 | 印刷：辽宁金印文化传媒股份有限公司 地址：沈阳市浑南新区世纪路4号 | 零售价：1.00元/份 订阅价：300元/年