当心“钱包”被“共享”

防范“共享屏幕”骗局还需双管齐下

“你涉嫌洗黑钱，请你配合调查……”当“公检法人员”打来电话，要求你“共享屏幕”，并“指导”你转账至安全账户时，千万不要相信。因为这是诈骗新套路。

据媒体报道，日前，一种借助“共享屏幕”围猎受害者的新型诈骗手段正在兴起，因其具有较强的隐蔽性，受害者往往会放松警惕，导致上当受骗。原本是互联网应用场景的“共享屏幕”，却被诈骗分子用于诈骗，并为诈骗行为披上了隐形外衣。

近年来，随着移动互联网的快速发展，形形色色的网络诈骗借助互联网科技的最新成果，不断变换出新形式。在对网络诈骗加大打击力度的同时，如何避免技术被恶意利用，是互联网时代一个不容回避的命题。

资料图片

“共享屏幕”诈骗暴露监管漏洞

冒充公检法人员要求配合处理、冒充银行工作人员指导贷款提额、冒充客服人员操作退款申请……在警方的披露中，诈骗分子的借口五花八门。由于提前通过非法渠道获取了当事人的基本信息，诈骗分子在初步取得当事人的信任后，诱导当事人进入手机“共享屏幕”模式，并且“手把手指导操作”。

由于“共享屏幕”相当于开启了手机的录屏功能，它会把屏幕上显示的内容全都记录下来，并同步让对方看到。这就意味着，你输入的银行卡号、密码和验证码等重要信息，都能被诈骗分子轻松捕获。然后，对方可以神不知鬼不觉地转走你银行卡里的资金。

大部分人会以为，现在手机卡和银行卡（以下简称“两卡”）都实名制了，警方可以顺藤摸瓜迅速破案，把被诈骗的钱财追回来。然而事实上，诈骗分子使用的手机卡号和银行账户几乎都是从非法渠道购买来的。而且，大部分诈骗分子也是通过境外远程操控诈骗，通过“实名不实人”的“两卡”和警方“躲猫猫”，这为警方的追查打击带来了巨大干扰。

实名制的手机卡和银行卡是如何落到诈骗分子手中的？中南财经政法大学数字经济研究院执行院长盘和林教授分析，有一些手机卡在实名制之前就已经存在，电信企业早先也办理了一些非实名制的虚拟卡，这些手机卡可能通过种种非法途径落到了诈骗分子手上，成为他们的作恶工具。银行卡的出处也有多种可能，有经实名注册后被盗窃或因其他原因流入市场的，但也不排除个别银行职员为牟利而违规办理的情况。

“像‘共享屏幕’诈骗这类披着科技外衣的行为之所以屡屡得逞，首先就在于不法团伙利用了人工智能、大数据等现代信息技术。”国研新经济研究院创始院长、新经济智库首席研究员朱克力直言，一方面，不法团伙日益走向公司化、专业化，产业链式的新型诈骗模式层出不穷；另一方面，“两卡”监管上的漏洞和“共享屏幕”在安全设置和隐私保护等方面的隐患，也让诈骗分子钻了空子。

网络诈骗仅靠升级法规还不够

如何才能让诈骗分子无处遁形？

盘和林说，“共享屏幕”虽然是一种新型的犯罪模式，实际上受害者并非因为科技受骗，而是诈骗分子利用了受害者不熟悉“共享屏幕”功能的特点，对其进行诱导和诈骗。本质上，这和以往的电话诈骗和短信诈骗并没有两样。因此，对一些不熟悉互联网的农民工、老年人、未成年人等特殊群体，应加强宣传和教育力度，让他们与时俱进了解数字技术，提升反网络诈骗的意识。

在中铁八局三公司的工地上，各种反诈骗的宣传深受农民工的欢迎；在贵州省贵阳综保区，党员干部走上街头宣传反诈骗；警方的反诈骗提示，更是一场防范诈骗的及时雨……

近年来，针对网络诈骗，公检法的打击力度空前。据统计，2020 年，全国检察机关起诉涉嫌网络犯罪 14.2 万人，全国公安机关共破获电信网络诈骗案件 25.6 万起，抓获犯罪嫌疑人 26.3 万名，拦截诈骗电话 1.4 亿个、诈骗短信 8.7 亿条，为群众直接避免经济损失 1200 亿元，可谓战果累累。

为了斩断手机卡、银行卡的买卖链条，公安部会同工信部、人民银行等部门在全国开展“断卡”行动，剑指非法出租、出售“两卡”的违法犯罪行为。自去年 10 月以来，全国公安机关累计打掉涉“两卡”违法犯罪团伙 2.7 万个，查处违法犯罪嫌疑人 45 万名，查处金融机构和通信企业内部人员 1000 余名。

“‘断卡’行动逐渐扫清了‘实名制’的死角，大大挤压了电信诈骗的空间，同时产生了极大的震慑效果，从根本上遏制住了电信诈骗案件的高发势态。”盘和林说，“严打”的同时，社会需要织密一张综合防控网。

不过，在接受媒体采访时，全国人大代表、贵州省贵阳市公安局刑事侦查支队政委石蓉表示，仅仅依靠打击并不能彻底解决新型电信网络诈骗犯罪问题，有关行业监管、治理和全社会的防范宣传力度还需加大，才能齐抓共管形成“全国一盘棋”。

号卡或涉非法得逞立即消失

那么，“共享屏幕”骗局究竟是怎么一回事，为何被骗风险极高呢？

江苏宿迁网警做过一个实验，当两部手机开启“共享屏幕”功能时，1 号手机上的每一步操作，都可以清晰地在 2 号手机同步反映出来。也就是说，只要在某平台、某软件中与对方开启了“共享屏幕”功能，你在自己手机上的任何操作，对方都能看到。包括输入各类密码、手机解锁、打开每个软件等过程。

采访中，记者获得 3 个“共享屏幕”诈骗者的电话，而后一一拨打测试，发现所有号码均无法正常接通。其中，有的诈骗者电话语音提示已停机，有的则提示暂时无法接通。即使在连续多天里屡次拨打诈骗者电话号码，情况也如此。

“只要得逞，电话很快就会被‘拉黑’。我们去报案的时候，警方就说这些电话号码很可能就是通过非法渠道购买或获得的，根本不是真实的本人电话。”有受害者告诉记者，在立案时，警方已经基本确认，诈骗者的电话号码所属并不是本人。“那些收款账户，是用了好几个手机号实现的。据说使用这些号码的骗子，一般都在境外活动。”

“他们通常就是打一枪换一炮，电话号码更换得很勤。请记住，如果陌生人需要你下载某个软件，或者打开某个链接，一律不要操作就好了。”不久前刚被共享屏幕骗局“找上门”但成功躲避的市民张先生表示。遇到类似骗局，不用当真就可以说是成功了一半。他呼吁大家，即使被诱骗下载了某个软件，也千万不要点击屏幕共享功能，更不要反馈任何验证码给对方。“我当天是没什么事，跟骗子周旋了一个多小时。耽误骗子一小时，可能就拯救了一个受害者。”

记者采访了解到，目前“共享屏幕”功能通常被诈骗者使用的场景是诸如冒充公检法、贷款诈骗、客服退款诈骗、注销校园贷骗局、杀猪盘等诈骗中。而今年，认证官方账号“北京反诈”曾在网络表示，“共享屏幕”骗局中，诈骗分子使用的账号几乎都是购买而来的账号，虽然开户人和账号都清楚，却无法与其本人建立关联，因此警方很难从这些账号找到幕后是谁。“这就是当前为何要在全国推行‘断卡’行动，严厉打击整治惩戒非法开办贩卖电话卡、银行卡违法犯罪活动的原因。”

对于各类不同类型和“面孔”的诈骗活动，此前国家反诈中心民警曾总结防范小贴士，并提醒大家在日常生活中牢记“三不一多”原则——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。

需要堵住技术和管理两个漏洞

科技从来都是一把“双刃剑”。数字科技在为人们带来多场景生活便利的同时，一些问题也随之浮出水面。从某种意义上说，“共享屏幕”为人们敲响了“科技向善”的警钟。

《科技向善白皮书 2020》认为，“科技向善”有两重含义，一是实现技术为善，二是避免技术作恶。技术不是万能的，本身或许无所谓善恶。从根本上说，一切对技术作恶和被滥用的担忧，都应该用法治手段来解决。

朱克力认为，由于电信诈骗具有非接触式、远程作案的特点，既能一对一地施展骗术，又能利用伪基站、任意改号软件展开“模糊轰炸”，其专业化、组织化、团伙化的程度非常高，决定了反电信网络诈骗势必是一场攻坚战、持久战。从动态监测到全链条打击，从有效反制到联防联控，都需要久久为功，尤其需要筑牢法治保障。

近年来，国家全面落实打防管控各项措施、强化跨地域跨部门协作、加强“实名制”等关键治理环节……让人欣喜的是，目前，《反电信网络诈骗法（草案）》已经通过全国人大常委会审议并公开征求意见。

有了法治护航，还需科技给力。

朱克力表示，在信息全球化、科技全球化、犯罪全球化的今天，“共享屏幕”之类的电信诈骗，无疑给监管和执法部门带来新挑战，也让社会公众面临新威胁。“但我们应当相信‘魔高一尺道高一丈’，既然不法分子可以利用新技术实施诈骗，我们同样可以充分利用通信、互联网、大数据等信息科技手段堵住诈骗漏洞，以雷霆之势高效打击电信网络诈骗和各类演化的新型犯罪。”

“金融机构在‘实名制’上要加强监管，避免非法‘两卡’流入市场，同时，我们在支付环节也需要更多地运用刷脸、指纹等生物认证手段。”数字经济智库高级研究员、中钢经济研究院首席研究员胡麒牧说，就“共享屏幕”诈骗而言，需要堵住技术和管理两个漏洞。

在朱克力看来，数字经济时代，要答好“科技向善”这道命题，除了企业的自律和监管的加强之外，我们还需要坚持以技术为矛、数据为盾，充分运用数据融合、数据驱动、数据共享的理念和方法，加快推进建设大数据反诈的长效机制，深入巩固常态化治理成效，不断提升公众的安全感、获得感、幸福感。

（来源：科技日报、北京日报）