2023.8.10 星期四
责编:谢卫东 美编:陈恩武 组版:丁亚平
现代快报+

通过恶意剪辑、换脸变声、搭建虚假“镜头环境”等手段，伪造视频内容，混淆视听……

网络诈骗花样翻新，如何守好“钱袋子”

一公司法人代表被骗子利用人工智能“换脸”技术诈骗430万元，某单位一工作人员被“假领导”诈骗近98万元……近期，多起通讯网络诈骗案件引发关注。

“新华视点”记者调查发现，近年来各地各部门不断加大打击治理通讯网络诈骗违法犯罪力度，有效遏制了案件快速上升势头。然而，仍有犯罪分子铤而走险，不断翻新手段实施诈骗，让受害人蒙受损失，广大群众一定要提高警惕。

据新华社

8月8日，反诈电影《孤注一掷》全国上映，南京市建邺警方联合辖区星轶影城推出观影互动赢奖活动。市民只需在星轶影城反诈主题取票机上取票，就可以获得一张定制的反诈票根，根据提示扫码并回复关键字，就有可能获得电影海报、警察小熊等精美礼品。同时，民警还会不定期出现在影厅内，向群众宣传反诈知识，提高群众对通讯网络诈骗的鉴别能力，营造全民参与、全民反诈的浓厚氛围。

通讯员 国武 现代快报+记者 顾元森/文 通讯员供图

诈骗花样翻新

利用最新技术诈骗高发，需要引起高度警惕

前段时间，南方某地一市民接到自称是某公安局“王警官”的电话，称其涉嫌一起洗钱案件。为博取信任，对方还以视频通话方式向其展示“自己”身着警服以及“公安局”内部环境的画面。就在这位市民准备转账至所谓“安全账户”时，警方接到预警信息及时进行阻止。

“通讯网络诈骗呈现出一些新特点、新情况。需要引起高度警惕的是，当前一些犯罪分子利用最新技术，通过恶意剪辑、换脸变声、搭建虚假‘镜头环境’等手段，伪造视频内容，混淆视听，诱骗受害人上当。”奇安信集团行业安全研究中心主任裴智勇说。

根据公安部发布的消息，当前，冒充电商物流客服、冒充公检法、冒充领导熟人以及刷单返利、虚假网络投资理财、虚假网络贷款等10种类型通讯网络诈骗高发，占发案的近80%。

——冒充身份类诈骗突出。

犯罪分子常常使用受害人领导、熟人的照片和姓名等信息包装社交账号，以假冒身份添加受害人为好友，随后模仿领导、熟人的语气骗取受害人信任。之后以有事不方便出面、时间紧迫等理由要求受害人尽快向指定账户转账。此外，客服、公检法工作人员等也是诈骗分子常常假冒的身份。

——虚假网络投资理财类诈骗造成损失金额最大，占造成损失金额的三分之一左右。

例如，受害人于某反映，被诈骗分子拉入“投资”群，看到其他人在某款App投资获利，便下载了该App。看到小额投资都成功盈利并顺利提现，于某继续投资了数百万元，不久后发现余额无法提现并被对方拉黑，才知被骗。

——刷单返利类诈骗发案率最高，占发案的三分之一左右。

此类诈骗通常以网络兼职刷单为名，诱导受害人预先垫资，并以事后结算款项为由，最终骗取更多笔垫资款。中国人民公安大学侦查学院教授刘为军说，刷单返利类诈骗已演化成变种最多、变化最快的一种主要诈骗类型，成为虚假投资理财、贷款等其他复合型诈骗以及网络赌博等违法犯罪的主要引流方式。

为何屡屡得逞

个人信息泄露是根源，“黑灰产”推波助澜

针对通讯网络诈骗犯罪高发态势，有关部门深入摸排、重拳出击。记者从公安部了解到，2022年，全国公安机关破获通讯网络诈骗犯罪案件46.4万起，缉捕通讯网络诈骗犯罪集团头目和骨干351名。2022年以来，公安部组织开展多次打击通讯网络诈骗犯罪区域会战，共打掉犯罪窝点5100余个。

高压之下，通讯网络诈骗犯罪为何屡禁不绝？

首先是犯罪分子作案手法智能化程度不断提高，对受害群体分析更加精准。记者进入一个所谓“机器人群”，在相关界面中输入自己的电话号码后，弹出QQ号、微博账号地址等个人信息。获取完整信息，仅需支付价格相当于1元至10元不等的虚拟币。

办案人员表示，个人信息泄露是诈骗的根源。网络黑客会把非法获取的金融、旅游、求职平台的个人信息进行整合，形成专门的数据库并不断更新。诈骗人员得到这些信息后，通过数据对诈骗对象进行人物画像，实施精准诈骗。

同时，通讯网络诈骗分工日益精细化，“黑灰产”推波助澜。记者调查发现，在通讯网络诈骗链条上，每一环节都寄生着一批提供“专业服务”的“商家”，通过辅助犯罪获利。

“一些组织和个人专门为诈骗集团提供买卖电话卡和物联网卡、推广引流、技术开发、转账洗钱等服务，增加了骗局的迷惑性和防范打击难度。”厦门市打击治理电信网络新型违法犯罪中心民警洪恒亮说。

此外，诈骗人员跨境作案，手法日趋高科技化。“随着国内打击力度不断加大，一些诈骗人员把窝点转移至境外，使用成本更低、隐蔽性更强、操作更简单的新型‘简易组网GOIP’设备，操控境内手机拨打诈骗电话，具有很强的伪装性，老百姓很难分辨。同时，也给执法取证等带来巨大挑战。”一名办案人员表示。

如何防范打击

强化预防和协同治理，提升技术防范手段

受访人士表示，遏制通讯网络诈骗不能仅依靠事后打击，必须强化预警防范和源头管控，提升优化技术防范手段，加强国际合作，不断铲除“黑灰产”土壤，斩断犯罪链条。

“您好，我是上海市反诈中心民警，您刚刚可能接到一个疑似通讯网络诈骗的电话，现在对您进行预警提示……”在上海市反电信网络诈骗中心，民警正在进行预警劝阻。“我们通过搭建预警数据模型，有效监测疑似通讯网络诈骗电话和短信，并针对低危、中危、高危潜在被害人采取分级、分类联动劝阻。”上海市公安局刑事侦查总队九支队情报综合大队副大队长朱光耀说。

反诈工作不仅在前端劝阻上下功夫，还要在后端资金止付止损机制上有所建树。“接到报警后，我们会立即启动资金紧急查询止付工作机制，对涉案资金封堵拦截，快速冻结资金。”洪恒亮说。

专家表示，通讯网络诈骗往往是环环相扣的犯罪链条，立足源头治理、系统治理，才能不断挤压犯罪空间，铲除犯罪土壤。

人力资源社会保障部要求人力资源服务机构建立个人信息保护、个人信息安全监测预警等机制；工业和信息化部加强App全链条治理，持续推进针对涉诈电话卡、物联网卡等的“断卡行动”；中国人民银行深入开展涉诈“资金链”治理；公安部集中捣毁一大批为境外诈骗集团提供支撑服务的犯罪团伙，依法严惩一大批境外诈骗窝点回流人员和从事各类“黑灰产”的犯罪嫌疑人……

“通讯网络诈骗犯罪和治理是‘攻防对抗’关系。”刘为军说，在犯罪手段和方式不断升级的情况下，要大力推动反制技术的研发应用，通过抢占技术高地来挤压犯罪空间。

“当前通讯网络诈骗花样繁多，公众要提高风险防范意识，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。”平安银行消费者权益保护中心主任颜恒说，遇到疑似通讯网络诈骗时，要多方求证核实，并及时向公安机关反映。