

深入推进“全民反诈在行动”集中宣传月活动——多一句提醒 多一道防线

■《人民日报》记者 张天培

电诈案件仍多发高发 威胁人民群众财产安全

目前,电诈危害覆盖全年龄段、渗透日常生活各场景,多重风险交织叠加。“电诈犯罪具有很强的顽固性和反复性,案件仍然多发高发。”公安部刑侦局副局长朱磊介绍。

从案件总量与损失结构看,当前十大高发诈骗类型占全部电诈案件85%,分别为刷单返利、虚假购物服务、虚假网络投资理财、冒充电商物流客服、贷款征信、网络游戏虚假交易、网络婚恋交友、冒充公检法、冒充领导熟人、机票退改签诈骗。其中虚假网络投资理财诈骗成为财产损失“重灾区”,百万元、千万元级重大被骗案件几乎均出自此类骗局,一次受骗足以掏空普通家庭多年积蓄。

伴随互联网业态迭代升级,诈骗分子作案隐蔽性更强、迷惑性更大——

线上平台成主要引流渠道。短视频、社交软件、网游成为骗子物色受害者的主要途径,通过评论私信、扫码进群、短视频植入二维码等方式接触群众,此类线上引流占比高达66%。不少群众被“免费领礼品”“噱头诱导入群”,一步步落入连环圈套。河北一名受害者通过交友软件结识伪装证券高管的嫌疑人,对方以身份保密为由哄骗其下载小众聊天软件,最终被骗160万元。

定制诈骗APP实现远程盗刷。脱离官方应用市场下载的不明软件暗藏屏幕共享、远程控制功能,一旦安装,手机银行卡、验证码、支付密码尽数暴露。

依托黄金、现金实物规避资金拦截。面对银行、支付机构严密资金管控,骗子转而哄骗群众提取大额现金、购买黄金、高端腕表等贵重物品,交由专人上门收取或邮寄指定地点,大幅提

升资金追查、拦截难度。浙江一名受害者深陷虚假投资骗局,多次购置黄金交付诈骗团伙,累计损失数百万元。

多部门协同发力治理 反诈防线全域提效

信息通信行业是反诈源头治理的重要关口。

工业和信息化部网络安全管理局二级巡视员张正介绍,2025年以来,行业坚持“事前防范、事中拦截、事后处置”全链条治理,从卡、号、设备、APP、链路等多维度清源固防。“我们坚持以执法压实企业主体责任,常态化开展反电信网络诈骗法落实专项检查,对责任落实不力的企业进行考核问责、约谈挂牌、行政处罚。”张正说。

源头断卡断号成效显著。截至2025年底,全行业累计核查处置涉诈高风险电话卡近2亿张、互联网账号超4亿个,协助公安机关缴获用于拨打诈骗电话的“插卡集群设备”,即“猫池”设备21万个,打掉“猫池”犯罪窝点11.7万个,彻底斩断一大批诈骗通信链路。

技防拦截能力持续升级。工业和信息化部联动200余家电信、互联网企业搭建实时反诈技防体系,2025年全年

累计拦截诈骗电话、短信64.8亿次,处置涉诈域名网址超1100万个,实现风险信息秒级预警、批量封堵。

多项便民反诈服务惠及数亿群众。跨境业务按需关停服务已服务5.87亿人次;境外来电风险提醒累计推送25.23亿次;12381涉诈预警短信累计发送17.26亿条;反诈名片助力公安预警劝阻6.6亿次,预警接通率提升32.8%。

金融支付领域同步筑牢反诈屏障。中国人民银行支付结算司副司长杨青介绍,为方便群众自主管理名下账户,防范“被开卡、被冒用”风险,央行指导银联在云闪付上线“一键查卡”功能。“目前查询范围已覆盖18家全国性商业银行,450余家区域性银行,截至5月末,累计生成查询报告超3000万份。”杨青表示,群众可通过官方云闪付一键摸清名下全部银行卡,及时注销闲置、风险账户,从源头防范账户涉诈、出租出借、跑分洗钱风险。

据指成拳,综合治理。近年来,公安、工信、金融、网信、教育等行业建立常态化联动机制,执法检查、线索移送、联合惩戒同步落地,形成“打击、管控、惩戒、宣传”闭环治理体系,跨部门协同共治格局已然成形。

守住群众内心“第一道防线” 构建常态长效反诈格局

电信网络诈骗属于可预防性犯罪,守住群众内心“第一道防线”,才能从根本上压降发案。今年“全民反诈在行动”集中宣传月以“不听不信不贪恋,构筑反诈‘心’防线”为主题,提醒避免落入心理陷阱。

近日,北京一女子遭遇了一起冒充公检法机关的电信网络诈骗。骗子谎称女子涉嫌洗钱罪,利用其恐惧心理,试图骗取该女子35万元存款。幸好民警第一时间赶到,成功拦截了被骗资金。

北京市公安局刑侦总队政治处主任李小燕提醒:“电诈分子善于利用群众心理弱点,一定要提高警惕,凡是陌生人要求转账汇款,或提供银行卡密码、验证码等个人信息,都有可能涉嫌诈骗。”

反诈宣传需要久久为功。“宣传月是载体,常态化宣防是根本。通过宣传让反诈观念深入人心,让更多群众增强防范诈骗的能力。”朱磊说。

近期,各地立足基层阵地,全域铺开常态化反诈宣传。社区依托党群服务中心、小区广场开展集中宣讲;银行、商超等线下网点布设反诈提示,工作人员对异常转账群众第一时间介入拦截;校园联动民警开设反诈课堂,面向青少年拆解刷单、游戏充值骗局……一系列围绕实景劝阻、案例科普、互动宣讲等多元形式的反诈宣传活动在基层展开。

“多一分警惕,少一次受骗,多一句提醒,多一道防线。”警方呼吁,全社会同心共治、警民携手联防,持续挤压诈骗生存空间,坚决守住人民群众财产安全底线。

评论

诱导下载陌生App打卡,使受害者逐步“入局”最终上当转账;打着“专业荐股”等旗号,哄骗股民掉入“暴富”陷阱;使用小众通联软件对被害人进行深度洗脑……公安部近期通报显示,电信网络诈骗犯罪手段持续翻新,迷惑性不断增强。面对新形势新变化,需以更有效有力之举措筑牢防线,守好百姓“钱袋子”。

这两年来电信诈骗打击治理成果显著,但电信诈骗案件仍然多发高发,诈骗手段不断迭代升级,伪装形式愈发隐蔽。犯罪分子从以往主要通过电话、短信方式,转为现在更多通过网络聊天、短视频直播、电商购物、平台生活服务、网络游戏等寻找作案目标。未成年人及学生群体已成电诈重点侵害对象。

有力有效遏制电诈,必须保持高压严打态势不放松。相关部门提升识别精准度、打击成功率和防骗有效性,把反诈防火墙砌在高危领域中,让更多好用、实用、易用的防骗工具走进老百姓的日常生活。

构筑更坚实的反诈防线,重点要抓好薄弱环节。一些不法分子通过在直播平台里投放有害链接等方式完成诈骗,凸显部分平台和领域反诈责任落实不严不细。对于电诈犯罪多发易发领域,当务之急是借助好人工智能、大数据等技术,提升线索发现敏感性、信息查询便利性、危害预警主动性,及时堵住漏洞。

对广大老百姓而言,反诈的关键是提高警惕,不听不信不贪恋,对利益仔细甄别,对诱惑保持警惕,对威胁不要轻信,对哄骗不要上头。电诈分子之所以得逞,正是抓住了一些群体易受利益诱惑、辨别能力不强等弱点。相关部门对电诈打防并举的同时,也要加强有效宣传,帮助大家提升防骗意识和识别能力。家长还应妥善保管好自己的银行卡、支付密码等敏感信息,避免让未成年人轻易接触从而造成经济损失。

网友评论

⑥卢云: 不接境外陌生电话,不乱扫二维码,只要不贪小便宜就不会吃大亏!

⑥翠翠: 不听不信不转账,构筑反诈“心”防线。

⑥无名: 建议严厉打击虚假网络投资平台,特别是一些冒充项目,危害太大了。

⑥海鸟与鱼: 天上不会掉馅饼,正在求职的大学生等一定要警惕境外高薪陷阱。

⑥铁塔梦: 如果遇到冒充客服等可疑来电,可以拨打110或96110反诈专线咨询举报。

⑥嘟嘟嘟: 骗子可能会针对性地设计专属骗局,大家一定要提高警惕性。

(本报综合整理)

“手机口”藏猫腻 本地来电也可能是电诈号码

■新华社记者 李明辉

公安部近日公布5起电诈及其关联违法犯罪典型案例,其中架设“手机口”为诈骗分子提供通信支持案引发关注。

随着全民防范电诈意识提升,公众对于“00”“+”开头的境外来电或许已具备较强甄别能力,但若来电显示为熟悉的本地号码,您是否还能保持警惕?

这种“障眼法”背后的技术支撑,便是犯罪分子搭建的“手机口”。

反诈民警介绍,所谓搭建“手机口”,是指利用两部手机同时运作:一部手机通过网络软件接通诈骗分子,另一部手机插入国内本地电话卡拨打受害者电话。两部手机通过扬声器等方式实现语音中转,使境外诈骗电话在受害者手机屏幕上显示为本地正常号码。此外,一些犯罪团伙还会使用GOIP、VOIP等设备批量组网,同时接入多条电话或宽带网络,实现批量拨号。

近年来,公安机关持续加大电诈打击力度,严打买卖电话卡、银行卡黑灰产,加之各大运营商对境外呼入号码加大识别和拦截力度,诈骗团伙为突破防线转而采用搭建“手机口”的手法。

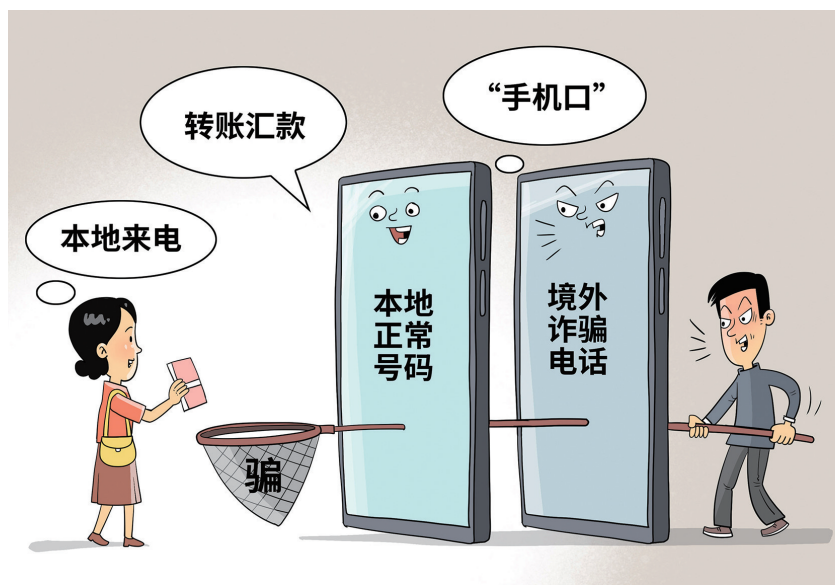
为何这一手段成为新方法?反诈部门分析有三方面原因:一是可规避境外来电拦截模型,绕过群众对陌生归属地的警觉;二是设备门槛低,两部旧手机加一张电话卡即可搭建,隐蔽性强、流动性大、不易溯源;三是诈骗分子常以“高薪兼职”“只需两部手机拨号日结佣金”等为诱饵,诱骗公众充当“工具人”,自己则躲在境外远程操控。

在此次公安部公布的案例中,康某伙同侯某在明知上线实施诈骗的情况下,仍架设“手机口”提供通信传输,关联全国3起电诈案件,非法获利近6万元,已被法院以帮助信息网络犯罪活动罪分别判处有期徒刑。

面对翻新的骗术,公众该如何防范?

警方提醒,无论来电显示是本地还是外地号码,凡陌生人提及转账汇款、索要短信验证码、要求开启屏幕共享或下载不明软件的,务必通过其他渠道核实身份,切勿轻信。

特别要注意的是,出租、出借、出售本人电话卡或参与架设“手机口”,涉嫌



漫画/朱慧卿

帮助信息网络犯罪活动罪,将被依法追究刑责。同时,公众要留意96110来电

预警,发现可疑“手机口”窝点或兼职广告等,及时向公安机关举报。

公益广告

低洼处, 勿逗留
避险意识刻心头

河岸旁, 莫近堤
水位上涨速撤离

观气象, 听预报
暴雨来临先知道

预警早一秒
安全多十分

责编/张会 版式/杨丽丹 校对/李雅