第 2 卷◆第 4 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

新型电信网络诈骗手段解析报告

乔喆　周宇飞
中国移动通信集团有限公司信息安全管理与运行中心
DOI:10.12238/acair.v2i4.10322

[摘　要] 近年来,随着对电信网络诈骗的严厉打击和深入治理,诈骗犯罪上升势头得到有效遏制[1]。然而,技术的飞速发展也带来了新的挑战,各类新型诈骗手法不断翻新花样,伪装性越来越强,网络空间的安全治理仍面临诸多难点。基于对新型诈骗手段的长期观察与研究,本文归纳了近年来新型电信网络诈骗的发展态势,并针对五种典型手段进行了详细分析和手段拆解,旨在为电信网络诈骗治理工作提供有效的理论依据和实践指导,助力清朗网络空间建设。
[关键词] 电信网络诈骗；人工智能；诈骗手段；诈骗态势
中图分类号：TP18　文献标识码：A

Analysis Report on New Telecom Network Fraud Methods

Zhe Qiao　Yufei Zhou
Information Security Management and Operations Center of China Mobile Communications Group Co., Ltd.

[Abstract] In recent years, with the strict crackdown and in-depth governance of telecommunications network fraud, the upward trend of fraud crimes has been effectively curbed. However, the rapid development of technology has also brought new challenges, with various new fraud methods constantly innovating and becoming increasingly disguised. The security governance of cyberspace still faces many difficulties. Based on long-term observation and research on new types of fraud methods, this article summarizes the development trend of new telecommunications network fraud in recent years, and conducts detailed analysis and decomposition of five typical methods, aiming to provide effective theoretical basis and practical guidance for the governance of telecommunications network fraud and assist in the construction of a clear cyberspace.
[Key words] telecommunications network fraud; artificial intelligence; Fraudulent means; Fraudulent situation

引言

近年来,随着数字产品功能的不断迭代,大众对手机等产品的依赖性不断增强。人工智能技术的爆发式发展推动AI产品逐渐融入人们的日常生活,潜移默化的开始影响人们的生活方式。但同时,产品与技术的持续发展使电信网络诈骗犯罪活动也随之呈现出新的趋势和手段。面对最新的电信网络诈骗形势,监督部门、政策制定部门和执法部门需要持续的信息支持改进自身工作内容与流程,为广大群众提供及时的保护。因此,跟踪电信网络诈骗态势,及时更新新型诈骗手段对反诈治理具有重要意义。

1 近年新型电信网络诈骗态势

1.1利用AI技术实施诈骗成为最“热门”手段。以ChatGPT等为代表的人工智能技术给社会带来便利的同时,也被不法分子所利用[2],通过AI换脸等方式,伪造出极为逼真的视频,冒充受害者的亲朋好友或权威机构,实施精准诈骗,使得诈骗的辨识和防范难度大大增加。同时,随着AI技术的不断进步,诈骗分子在技术利用上也不断深化,意图提高AI制造出来的人物形象的实体化、具体化,以提升诈骗成功率。

1.2针对苹果手机的诈骗手段逐渐向安卓系统蔓延。iMessage和Facetime均为苹果手机系统内置的即时通信工具,不同于运营商短信/彩信业务,用户仅需要通过WiFi或者蜂窝数据网络进行数据支持,就可以完成通信。这种设计使得用户在通信时不需要使用手机号码,从而有可能绕过实名制认证,难以进行有效监管。此类诈骗手段因具有较强隐蔽性及欺骗性,如今已成为诈骗分子新的诈骗“工具”,并逐渐蔓延至安卓系统平台,华为手机内置的畅连软件也成为诈骗重灾区。

1.3受害人群呈年轻化发展趋势。基于近两年诈骗事件公开报道数据统计,新型电诈受害者的年轻化程度相较于往年有明显加深,90后、00后,甚至是10后已成为主要的受害群体。“FaceTime”诈骗和利用AI实施诈骗中11-25岁年龄层占比均接近50%。诈骗分子通常利用年轻群体对金融投资、网络交友等方面的需求和关注点,通过精心设计的话术和剧本,在社交媒体、网络平台等渠道,设计各种诱惑性的骗局,实施精准诈骗。

2 新型电信网络诈骗手段详解

AI换脸诈骗、苹果imessage诈骗、新型“蟹卡”诈骗、“Facetime”诈骗、电话手表兑换卡诈骗是近年典型的新型诈骗手段。这些诈骗行为不仅依托于新兴技术，而且在专业性上不断提升，使得公众在识别和防范上面临更大的挑战。

2.1 AI换脸诈骗。AI换脸诈骗是近年热度最高的新型诈骗手段，且涉案金额通常较大。不法分子利用非法获取的个人信息，通过人工智能(AI)仿真技术合成受骗者亲人、领导同事或公职人员的肖像面容与声音，冒充上述人员身份行骗。在获得受害者信任后使用事先准备好的套路话术向受害人发送银行卡转账、虚拟投资理财、刷单返利等诈骗信息，并利用视频通话、语音轰炸等手段进一步降低受害者的防备心，受害者往往在短时间内难以察觉异样，一旦听信诈骗分子的骗术并完成转账，对方便杳无音信。

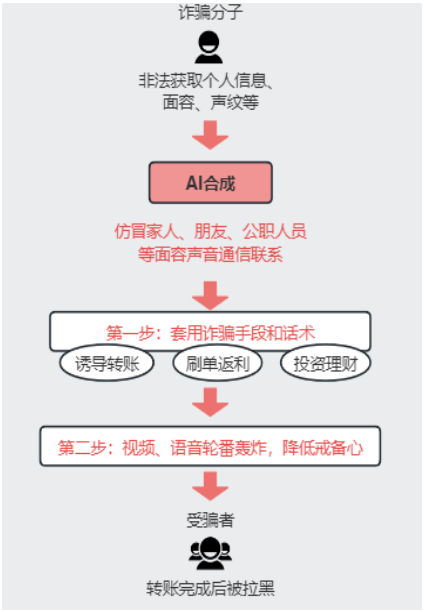

图1　AI换脸诈骗作案流程示意图

2.2苹果imessage诈骗。苹果imessage诈骗是诈骗分子利用苹果imessage的无线网络联系功能，冒充领导或熟人编造各种理由进行诈骗。

为了取得受害人信任，诈骗分子通过非法渠道获取受害人及其领导或其他关系人的个人信息后，使用imessage以“新换号码”为由发送信息，要求受害人添加其微信或继续通过imessage聊天，同时诈骗分子也会非法获取领导或其他关系人的微信昵称、微信头像，并加以伪装，从而骗取受害人的信任。诈骗分子以领导、朋友关心的口吻与受害人沟通，降低其戒备心，随后编造各种困难理由，如打点关系、垫付、代付款项、急需就医费用等，让受害人转账到指定账户。一旦得手，诈骗分子仍不罢休，继续编造转账失败等谎言，持续行骗，导致受害者损失扩大。

2.3新型蟹卡诈骗。新型蟹卡诈骗通常单起涉案金额较小但事件多发，“广撒网”特点明显。诈骗分子通过非法手段获取消费者的个人信息，并通过寄送带有螃蟹卡的礼盒来迷惑受害者，以扫码验证领取大闸蟹或奖品为由，吸引事主扫码进入预先设定好的群聊当中，再通过完成任务领取红包、领取大闸蟹、提交快递费等为由引导转账从而实施诈骗。

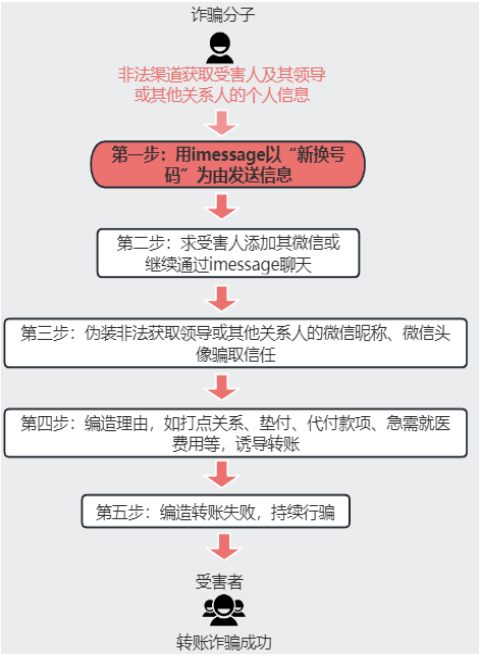

图2　涉苹果imessage诈骗作案流程示意图

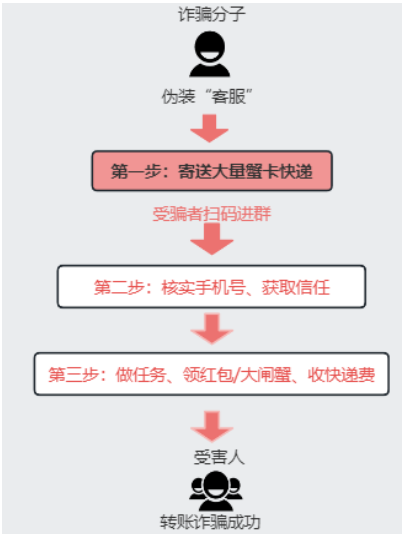

图3 新型蟹卡诈骗作案流程示意图

2.4 “FaceTime”诈骗。FaceTime诈骗是诈骗分子利用国内用户对FaceTime功能不了解的弱点，进行的针对性诈骗。诈骗分子多自称金融平台客服，通过FaceTime拨打语音电话，以“金融账户异常”“影响征信”等话术威胁受害人，制造心理恐慌，而后引导受害人下载腾讯会议、Zoom等各类具有实时屏幕共享功能的App，打开不明网址联系在线客服，诱骗其将钱款转至指定账户，或向银行与其他网贷平台申请贷款，承诺资金审核后将钱款返还，待转账完毕，便将受害人拉黑[3]。

此外，FaceTime诈骗还衍生出变种手法，如在视频会议、实

时屏幕共享时，诱骗其安装境外翻墙软件及云闪付，并指导被害人使用云闪付“一键查卡”功能，或通过“屏幕共享+翻墙软件”结合，获悉其名下银行卡、密码、验证码等关键个人信息，诈骗过程时间更长，隐蔽性更高。

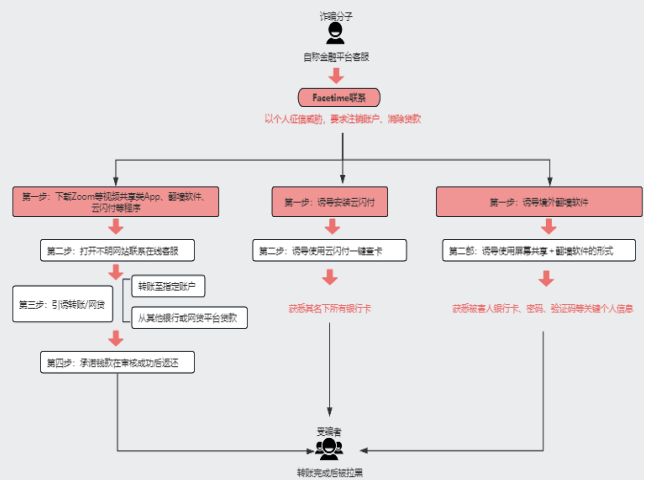

图4 “FaceTime”诈骗作案流程示意图

2.5“电话手表兑换卡”诈骗。“电话手表兑换卡”诈骗，其手法具有一定的迷惑性。诈骗分子印刷包装精美的“电话手表兑换卡”，卡片有电话手表图片，并标注“安全守护”“¥300”“中国移动儿童手表专属电话卡”等字样。一旦扫描电话手表兑换卡上面的“微信扫码兑换二维码”，并填写个人信息，将落入骗子的圈套。诈骗者会以领取手表为由，诱骗受害者进群、刷单、做任务等，进而套走钱财。

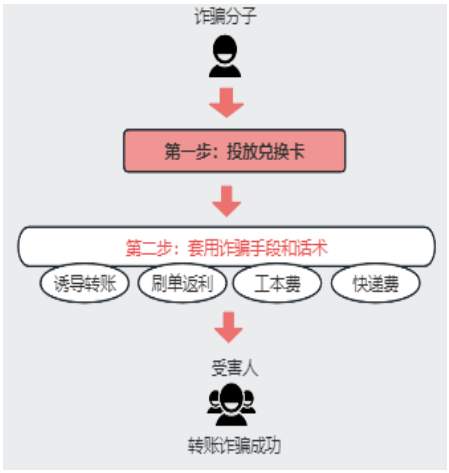

图5 “电话手表兑换卡”诈骗作案流程示意图

3 对策建议

3.1加大技术创新研发投入，提高反诈工作效率。为应对电信诈骗治理面临的严峻挑战，需加大研发创新投入，以借助现代科技手段推动电信网络诈骗防治模式的变革，加速电信诈骗犯罪治理由传统模式向智能化、数字化的转型升级；强化人工智能技术在电信网络诈骗防治领域的应用，通过分析识别电信诈骗电话、屏蔽高风险网站、标记易受骗人群等技术手段，助力犯罪治理由被动打击向主动预防转变[4]；提升反诈溯源能力，对典型案例特征进行提炼分析，开展事后溯源及复盘工作，全面提升全链条治理能力，从而更有效地提升电信诈骗犯罪的防范和打击效能。

3.2推动部门反诈协同合作，形成常态工作机制。强化政府、社会组织与企业等部门间的协同合作，打造反诈信息共享平台，建立反诈信息共享机制，实现社会各方优势资源的共享与交换；明确部门间反诈职责和任务，完善反诈工作评价、考核指标以及奖惩机制，引导各部门在反诈工作的持续投入，推动开展常态化反诈工作，确保工作过程的系统性和连贯性；完善部门间反诈资源整合和综合管理办法，推动信息的快速流通与反馈，提高反诈资源利用效率。

3.3构筑立体反诈宣传格局，动员社会力量参与。面向不同群体开展针对性反诈宣传，尤其针对易受骗人群，如老年人、青少年、学生等，帮助易受骗人群树立防诈意识；优化宣传内容输出，结合真实诈骗案例，以故事演绎等易于传播的方式，提高信息的吸引力和传播力，强化宣传内容的教育警示效果；创新宣传方式，构建“媒体+”反诈宣传格局，整合央媒和地方媒体资源，形成多层级、立体化的宣传网络，全面提升反诈宣传覆盖面和影响力；建立反诈志愿者队伍，鼓励和引导社会组织、志愿者、社区居民等社会力量参与反诈工作，通过开展社区反诈讲座、组织反诈知识竞赛等形式，形成群防群治的良好局面。

4 结束语

电信网络诈骗的趋势变化与手段更新是一个长期持续的过程，技术、消费观念和生活方式的变化都会引发新型网络骗局。面对日益变化的网络环境，持续跟踪、快速识别、及时应对因新型网络诈骗引起的社会影响需要公共管理部门、监督执法机关和网信安全企业形成合力，明确技术研发路径、利用自身优势资源、建立跨部门合作流程，形成常态化联防联控机制，以打击网络诈骗行为，保护广大群众的财产安全，维护社会的稳定。

[参考文献]

[1]王菲.打防并举综合施策坚决遏制电信网络诈骗犯罪——专访公安部刑事侦查局反诈负责人[J].中国安全防范技术与应用,2022(1):19-22.

[2]刘宪权.生成式人工智能对数据法益刑法保护体系的影响[J].中国刑事法杂志,2023(4):20-34.

[3]黄琦清,黄传盛.高校电信网络诈骗的特点、成因及治理策略——基于F市视角[J].产业与科技论坛,2024(7):29-31.

[4]黄俊杰.电信网络诈骗犯罪治理难题及应对[J].中国检察官,2021(17):12-15.

作者简介：

乔喆(1981--),男,汉族,北京人,硕士研究生,经济师,主要从事网络信息安全管理工作。

周宇飞(1980--),女,汉族,河南人,硕士研究生,高级工程师,主要从事不良信息治理方面的研究工作。