

“孙子”成了数字人？

视频里“孙子”哭诉惹祸急需赔钱，电话那头“好友”的声音如常，连咳嗽习惯都一模一样……你敢相信这竟是AI生成的“数字替身”吗？

随着AI技术的快速发展，一些不法分子的诈骗手段也在不断升级，从盗图、偷声到合成文书、“数字人”，让人防不胜防。黑灰产正在从“堆资源、拼人力”的传统模式，转向更隐蔽、更低成本、更接近真实用户行为的“类真人化、智能化”阶段。



从盗图、偷声到“数字人”，AI诈骗不断升级

今年3月，家住西部某市83岁的陈婆婆接到“儿子”的电话，称遭遇意外，需现金“疏通关系”，并让陈婆婆在约定地点将3万元交给前来取款的人。当陈婆婆正要钱交给两名形迹可疑的年轻人时，被路过的基层干部发现并报警，两名诈骗分子慌忙驾车逃离。后经查发现，陈婆婆接到的电话系不法分子使用AI合成声音打来的。

湖北省黄石市黄石港区人民法院去年底也审结了一起类似的AI诈骗案件。一位老人接到“孙子”打来的电话，“孙子”哭诉在学校与同学发生冲突并失手伤人，需赔偿4万元“私了”，对方家长要上门取钱。前来取款的诈骗分子吴某为让老人深信不疑，还接通了“孙子”的电话，让老

人确认……同一天，相同的骗局还在另外两位老人身上上演。吴某在“上线”的遥控指挥下，骗取3位老人共计6万元。法院审理发现，不法分子使用的AI拟声技术能高度还原人声音色，并可实时对话交互，这成为诈骗得逞的关键。

半月谈记者采访了解到，近年来AI技术持续迭代，不法分子利用AI技术进行诈骗的手段也在升级，从此前单一的盗图、换脸、偷声进行欺诈，到现在可以多模态生成以假乱真的文书证件、动态视频以及能交互的“数字人”，给群众甄别违法犯罪增加了难度。

上海一消费者利用AI软件篡改他人的医院就诊记录，伪造自己因食用某烤肉店食物而“吃坏肚子”的病历

和发票，以此向商家索赔并威胁向监管部门投诉，商家为息事宁人，最终转账赔付；福建某企业负责人郭先生在视频通话中目睹“好友”面容并亲闻其声，10分钟内被骗转账430万元，事后发现对方竟是AI合成的“数字替身”；犯罪嫌疑人利用某支付平台漏洞，利用AI技术将他人照片合成视频进行人脸识别验证，从而盗刷他人医保卡……

此类新型AI诈骗在全国各地屡见不鲜。国内一家专注于黑灰产情报和反欺诈技术的机构发布的《2025年互联网黑灰产趋势年度总结》显示，生成式AI与智能体技术的爆发，不仅为产业创新带来了机遇，也为黑灰产提供了低门槛、高效率的自动化工具。

新技术为何成了新骗术？

AI技术的快速迭代让使用AI的要求与成本大幅降低，加上监管制度尚不完善、平台责任落实不到位、公众防范意识薄弱等，让不法分子找到了可乘之机。

《2025年互联网黑灰产趋势年度总结》指出，传统网络黑灰产依赖昂贵的硬件，并对编程等技能有较高要求，而AI智能体赋能后，不法分子无需硬件以及编程等技能，通过语言指令就能一键式操作，且视觉效果从“僵硬”

走向“毛孔级真实”，让攻击成本呈指数级下降。

一些网络黑灰产团伙在暗网和一些论坛获取AI工具，价格从几元到数百元不等，并通过社交平台、公共视频等渠道获取人脸或语音数据，成本几乎为零。外交学院信息化办公室主任王大印表示，造假成本低，但通过诈骗、流量变现可获得暴利，形成了AI诈骗的经济驱动力。

在AI诈骗技术升级的同时，相应

的拦截和识别技术仍滞后。专注于人工智能安全与治理的“安远AI”安全治理主管方亮认为，造假技术的进步也推动着检测技术的发展，但目前造假技术的迭代速度往往更快。从事数字笔迹AI识别技术的重庆亲笔签数字科技有限公司联席总裁贺英辉表示，人脸、指纹、声音等单一生物特征认证方式，正面临AI深度伪造的威胁，已无法满足高安全场景需求，数字身份基础设施亟待升级加固。

介绍，与人脸、指纹等静态生物特征不同，数字笔迹包含笔画、笔序、笔压、笔速等上百项动态生物特征数据，这些笔迹数据具有极强的个人唯一性，AI也难以模仿，可有效避免AI盗图进行认证造假。

受访民警提示，如遇亲友、领导、客服等线上要求转账，务必当面二次核实，绝不轻信单一渠道信息。视频通话可让对方做眨眼、挡脸等动作辨别AI换脸，留意语音有无机械感、有无自然呼吸停顿。及时安装国家反诈中心App，一旦被骗，立即报警并留存聊天、转账等全部证据。 据新华社

给技术戴上“紧箍”

近年来，相关部门先后出台了《生成式人工智能服务管理暂行办法》《人工智能生成合成内容标识办法》等，推动AI技术合规发展。业内人士认为，对于用AI换脸实施诈骗或诽谤的定性、平台应承担的审查责任边界等问题，现有法律法规还需进一步明确和细化，压实互联网平台对AI造假内容的识别和监管责任，建立AI诈骗的国际执法协作机制。实施“风险分级治理”：对医疗诊断、司法证据等“高风险”场景，设定严格的技术标准、透明度与监管要求；对普通娱乐、创作等“有限风险”场景，则

以显著标识和用户知情管理为主。王大印认为，在现有法律框架内，可明确对利用AI实施诈骗、诽谤、侵犯肖像权等行为的加重处罚情节，提高违法成本。

相关执法部门可开展专项行动，完善举报投诉机制，严惩实施AI诈骗的关键主体。对组织研发AI诈骗技术、工具者，策划实施诈骗的组织者，以及累犯、惯犯，坚持依法从严惩处。

王大印认为，技术上的可追溯是实现法律上可问责的前提，需要强制推行数字水印等可追溯技术。贺英辉

法国18岁及以上居民对人工智能态度分化明显

法国一项新公布的调查结果显示，65%的法国人使用人工智能工具，但法国公众对人工智能的态度分化明显。

这项名为《法国人与人工智能》的调查由埃拉贝民意调查公司12日发布，样本为1503名法国本土18岁及以上居民。调查结果显示，法国公众对人工智能的态度分化明显，54%的受访者认为人工智能首先是威胁，45%则认为首先是机会。

此外，在各个群体使用人工智能的比例方面，存在明显的代际、阶层和地域差异。18岁至34岁人群中为87%，而50岁以上人群中只有54%；管理人员中为86%，而工人中只有56%；大城市居民中为71%，而农村居民中只有57%。

调查显示，大多数受访者认为，使用人工智能将成为未来社会的核心能力，应当被引入学校教育。 据新华社

首尔禁止中小学生对AI眼镜参加期末考试

韩国首都首尔市教育厅12日说，已于前一日向该市中小学校及辖区教育部门下发通知，禁止考生戴AI智能眼镜参加期末考试。

据韩国《中央日报》报道，首尔市教育厅担心学生利用AI眼镜在期末考试中作弊，因此将其列入考场违禁物品清单。这份通知要求学校提前告知学生及家长，如携带这类眼镜进入考场，将一律按作弊处理。

AI智能眼镜集成摄像头、麦克风与生成式人工智能，可对拍摄画面进行解析，通过镜片或内置扬声器向使用者传递答案等信息，该眼镜因此存在被用于将考题传出考场或接收答案的作弊风险。

这份最新通知给出区分AI眼镜与普通眼镜的要点：AI眼镜往往镜腿粗厚、末端厚重，内部装有电池与控制主板，镜片周边隐藏微型摄像头和传感器，镜腿内侧有LED指示灯、触控按键或实体按键、扬声器开孔、充电接口等。通知还提醒监考教师在考试期间重点留意反复触碰镜框的学生。

上月，韩国两名考生被查出在托业(TOEIC)英语能力考试中利用AI眼镜作弊，因此成绩作废，且今后4年内不得再次参加托业考试。这一新型作弊方式引起相关方面重视，韩国教育部门正考虑在高考中禁用这类用品。 据新华社

南极半岛出现超过正常水平20多摄氏度异常高温

阿根廷观测数据显示，南极半岛6月初已出现15.4摄氏度的异常气温，比正常水平高出20多摄氏度，创下历史同期新高，冰层也出现异常融化。

阿根廷埃斯佩兰萨南极科考站的6日观测数据显示，南极半岛当日气温达到15.4摄氏度，超过历史上6月的单日最高气温纪录，即1998年录得的13.3摄氏度。

阿根廷国家气象局专家何塞·路易斯·斯特拉11日在接受媒体采访时表示，虽然今年6月初距南极半岛较近的阿根廷各地气温普遍偏高，但南极半岛的气温“比正常水平高出20多摄氏度，这是不寻常的现象”。

据阿根廷媒体《第12页报》报道，历史记录中埃斯佩兰萨南极科考站6月的平均最高气温为零下6.2摄氏度。此外，6月5日至6日，阿根廷马兰比奥南极科考站和圣马丁南极科考站的最高气温分别达到11.8摄氏度和9.4摄氏度，而这两个科考站6月的平均最高气温分别为零下10.7摄氏度和零下5.6摄氏度。

科研人员说，由于过去三周每日最高气温都在零摄氏度以上，埃斯佩兰萨南极科考站所在区域至今没有积雪，这对极地生态系统产生不利影响。 据新华社