为何AI诈骗成功率那么高?

现在的技术就像“大脑”一样，可以让多个模态完美地结合，并自如地切换和应用，从而能更容易地生成那些逼真的诈骗素材。

记者 | 陈 冰

AI诈骗爆发！ 10分钟从老板手里骗走430万元！

AI换脸诈骗200多万元！

涉嫌寻衅滋事罪！甘肃公安侦破首例利用AI炮制虚假信息案……

日前，有关AI诈骗、非法获利的新闻层出不穷，“AI诈骗正在全国爆发”的话题多次冲上微博热搜。

AI生成的声音越来越自然流畅，视频越来越逼真，普通人的耳朵和肉眼已经难辨真伪，甚至连科技从业者也可能被骗。以至于有消息称，AI技术的新骗局来袭后，诈骗成功率竟接近100%。

一直在不断自我优化、升级换代的深度伪造技术，让一些群体开始野蛮生长，利用AIGC（生成式人工智能）从事违法犯罪的勾当。

但中国有句老话，“魔高一尺道高一丈”。AI大潮已经将我们裹挟其中，要想更好地应对，预防技术滥用，需要社会各界一起通过向善的价值观进行技术防御。如此，我们才能够用“魔法打败魔法”！

AI诈骗在全国爆发

AI换脸、AI换声技术都不是新鲜事物。

早在2019年，国内就出现过一款换脸软件“ZAO”，许多明星、名人遭到恶搞、被造黄谣。很快，这款应用便因为涉及侵犯隐私而遭到下架。但由此带来的换脸诈骗技术却开始暗自滋生，直到今年出现大爆发。据报道，第一起“AI换声”诈骗也发生在2019年。

过去几年，“AI诈骗”时有发生。但从去年底开始，美国、加拿大等地发生此类案件的数量明显增多。今年开始，我国发生此类案件的数量同样明显增多，涉案金额也越来越大。

“我们认为，这和深度合成技术的成熟度、普及度是分不开的。”瑞莱智慧联合创始人、算法科学家萧子豪说。

AI换脸、AI换声主要使用的是深度合成技术。随着深度合成技术的开源开放、深度合成产品和服务的增多，深度合成内容制作的技术门槛越来越低，实现了技术的“平民化”，普通人也能用少量图像、音频等样本数据，利用简便易用的合成工具，制作深度合成内容。想想美图秀秀的漫画形象、导航里的自我语音导航、抖音里的一键生成，就能知道它们的功能到底有多强大。

萧子豪介绍，目前视频聊天或直播的AI换脸有两种方式：一种是事先做好的换脸视频直接播放，一