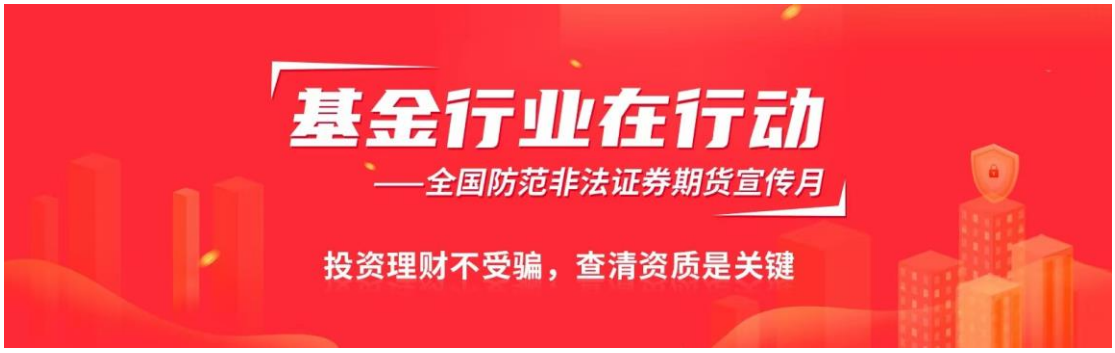
防非宣传月|警惕新型 AI 诈骗



今年以来全球生成式人工智能（AIGC）产业高速发展，各个大厂都推出了自己的预训练大模型。目前 AIGC 技术已经能够较好地实现文字、图像、音频、视频等的生成，文本学习、交互能力也颇为出色，随着模型参数和数据训练量的提升，AIGC 在这些方面甚至能够做得更好，几乎达到以假乱真的地步。AIGC 技术无疑能对很多行业的效率和质量带来大幅提升，但也渐渐被诈骗团伙发现并利用。近期使用 AI 技术的新型电信诈骗在全国范围内出现，诈骗成功率极高。

常见 AI 诈骗手段

1. 精准投放

诈骗团伙会紧跟社会热点，随时变化诈骗手法和“话术”，迷惑性强，还会针对不同群体，根据非法获取的精准个人信息，量身定制诈骗剧本，实施精准诈骗。公安机关发现的诈骗类型现在已经超过 50 种，其中网络刷单返利、虚假投资理财、虚假网络贷款、冒充客服、冒充公检法是 5 种主要的诈骗类型。

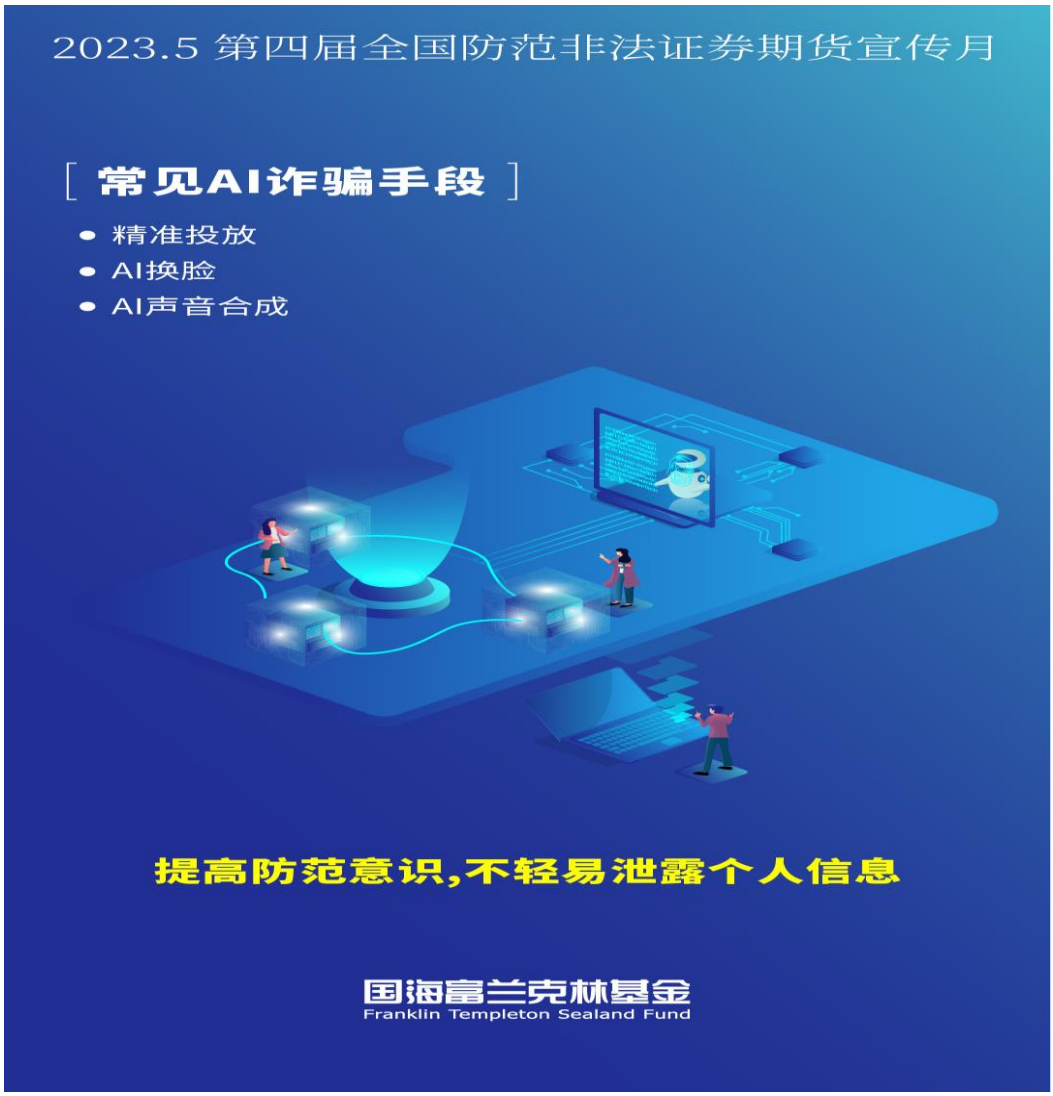
2. AI 换脸

正所谓“百闻不如一见”，亲眼看到对方的脸更容易让人放下警惕，但骗子也正利用了这一点，通过分析公众发布在网上的各类信息，根据所要实施的骗术，通过 AI 技术筛选目标人群，在视频通话中再利用 AI 换脸，骗取信任，这样的骗局成功率通常都非常

高。

3. AI 声音合成

不法分子会利用 AI 技术生成高清晰度的语音合成模型，伪造出与被骗者亲朋好友的声音，通过电话进行诈骗。此外，骗子还可以通过收集发布在网上的信息来模仿日常用语和话术，进一步提高骗局的逼真程度。近期，有许多公司高管就不幸中招，其中一名科技公司老板在 10 分钟内被骗走了 430 万元人民币。



如何避开 AI 诈骗

防止诈骗最重要的就是要提高防范意识，不轻易提供人脸、指纹等个人生物信息给陌生人；网络转账前要多留个心眼，可以通过电话、见面等多种沟通渠道核验对方身份，不要

未经核实随意转账汇款，更不要轻易透露自己的身份证、银行卡、验证码等信息。

那么遇到 AI 诈骗就没有办法识破吗？其实多数 AI 假脸由于是通过睁眼照片生成的，极少甚至不会眨眼。如果跟你视频的“人”一直不眨眼，就该提高警惕性了；此外，电话联系时如有疑问，不妨问几个双方共同知道的小秘密，这也能降低骗子的成功率。