警惕AI技术新型诈骗

最近，不法分子使用AI技术进行电信诈骗的案件频发。那么，AI技术诈骗常用手法有哪些？如何防范？

AI技术诈骗常用手法：

1. 声音合成。骗子通过骚扰电话录音等来提取某人声音，获取素材后进行声音合成，从而用伪造的声音骗过对方。

2. AI换脸。人脸效果更易取得对方信任，骗子用AI技术换脸，可以伪装成任何人，再通过视频方式进行信息确认。骗子首先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。在视频通话中利用AI换脸，骗取对方信任。

3. 转发微信语音。骗子在盗取微信号后，便向其好友“借钱”，为取得对方信任，他们会转发之前的语音，进而骗取钱款。尽管微信没有语音转发功能，但他们通过提取语音文件或安装非官方版本（插件），实现语音转发。

4. AI程序筛选受害人。骗子利用AI技术分析公众在网上发布的各类信息，根据所要实施的骗术对人群进行筛选，在短时间内便可生产出定制化的诈骗脚本，从而实施精准诈骗。例如，实施情感诈骗时，可以筛选出经常发布感情类信息的人群；实施金融诈骗时，可以筛选出经常搜索投资理财信息的人群。

如何防范？

1. 多重验证，确认身份。如果有人要求你分享个人身份信息，如你的地址、出生日期或名字，要当心。对突如其来的电话要保持警惕，哪怕是来自你认识的人，因为来电显示的号码可能是伪造的。网络转账前要通过电话等多种沟通渠道核验对方身份，一旦发现风险，及时报警求助。如果有人自称“熟人”“领导”通过社交软件、短信以各种理由诱导你汇款，务必通过电话、见面等途径核实确认，不能未经核实就随意转账汇款，不要轻易透露自己的身份证、银行卡、验证码等信息。

2. 保护信息，避免泄露。不轻易提供人脸、指纹等个人生物信息给他人，不过度公开或分享动图、视频等。陌生链接不要点、陌生软件不要下载、陌生好友不要随便添加，防止手机、电脑中病毒以及微信、QQ等被盗号。

3. 提高安全防范意识。公检法没有安全账户，警察不会网上办案。如果有网络警察说你犯事了，让他联系你所在地派出所，你也可以主动打110咨询。如不慎被骗或遇可疑情形，请注意保存证据并立即拨打96110报警。

周　煜/绘

来源：“科普中国”微信公众号