警惕高科技骗术

1. 声音合成。2020年12月，某公司财务小王接到“领导”电话，要求其立刻给供应商转款2万元，并将转账信息以邮件形式发送。由于该声音与单位领导的口音十分相似，小王信以为真，在1小时内完成转款，后发现被骗。骗子是通过骚扰电话录音等来提取某个人的声音，获取素材进行声音合成后实施诈骗。

2. AI技术换脸。最近，小李的大学同学通过QQ跟她借钱，对方打过来一段四五秒的视频电话，小李看到确实是她的同学，便放心转账3000元。然而，转账后她感觉异常，便再次拨通对方电话，这才得知同学的账号被盗，遂报案。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，令人防不胜防。

3. 转发微信语音。今年3月，市民小刘收到一条来自好友的微信语音，声称自己遇到困难，需要向小刘借钱。小刘通过语音听出确实是好友的声音，随即向其转账2500元，后发现被骗。骗子在盗取微信号后，便向其好友“借钱”，为取得对方信任，骗子会通过提取语音文件或安装非官方版本插件，“转发”之前的语音，进而骗取钱款。

4. 通过AI技术筛选受骗人群。不久前，市民小胡在某社交平台发布了几条自己近期有投资意向的信息。没过几天，小胡的手机上就收到一条投资广告，小胡开始在某虚拟币交易平台进行投资，在累计投入10万元都亏损后，小胡产生了怀疑，随即报警。骗子根据所要实施的骗术对人群进行筛选，锁定特定对象。比如，当进行金融诈骗时，他们会将经常搜索投资信息的人群锁定为潜在目标。

做好防范：

1. 多重验证，确认身份。在涉及转账交易时，尽量通过电话询问具体信息，确认对方是否为本人，即便对方应用AI技术手段行骗，也可以通过提问的方式进一步确认身份。在无法确认对方身份时，可以将到账时间设定为“2小时到账”或“24小时到账”，以预留处理时间。建议采取银行账户转账，既利于核实对方身份，又有助于跟进转账信息。

2. 保护信息，避免泄露。加强个人信息保护意识，不管是在互联网还是社交软件上，要尽量避免过多地暴露个人信息。对于不明平台发来的广告、中奖、交友等信息链接，要提高警惕，不要轻易点击和填写个人信息。

3. 拒绝诱惑，提高警惕。应提高应对高科技诈骗的能力，学会拒绝诱惑，避免占便宜心理，警惕陌生人无端“献殷勤”。

摘编自《重庆科技报》