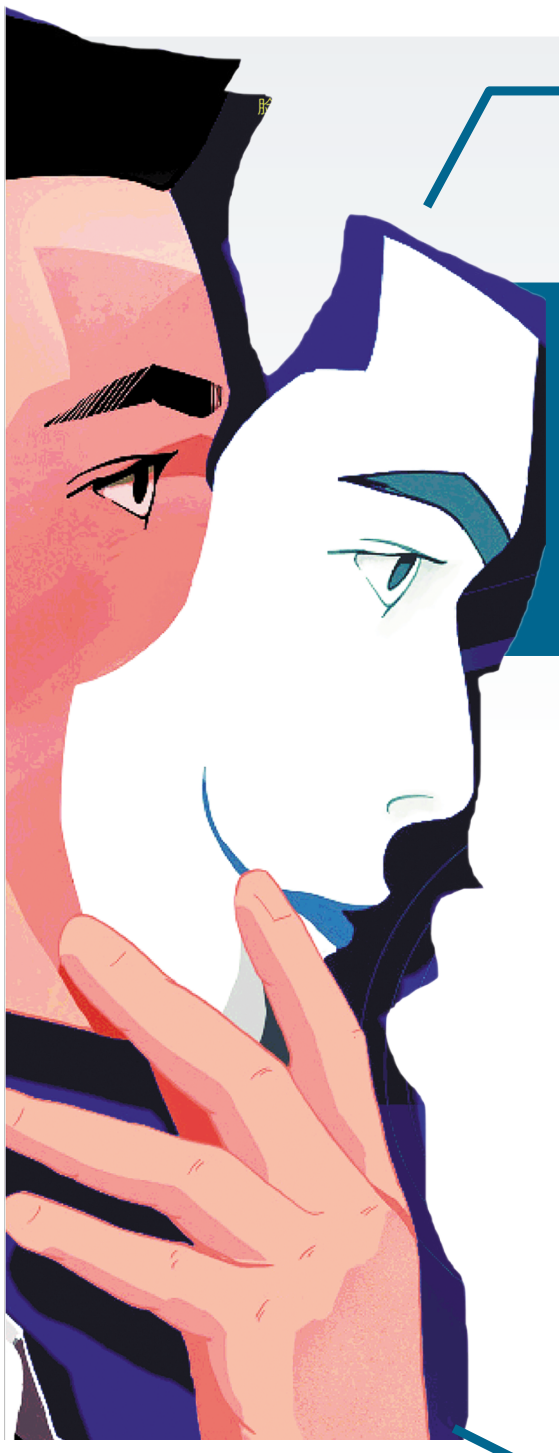

眼见耳听也不一定是真
AI换脸新骗局骗走老板430万

用AI骗你

随着人工智能(AI)的迅猛发展，诈骗团伙的诈骗手段也越来越科技化，竟然用上了AI换脸技术。近日，包头警方发布一起利用AI实施电信诈骗的典型案例，福州市某科技公司法人代表郭先生10分钟内被骗430万元。5月22日，“AI诈骗正在全国爆发”的话题冲上热搜，引发网友热议。

10分钟被骗走430万

据平安包头官方微信号5月20日消息，5月8日，包头市公安局电信网络犯罪侦查局发布一起使用AI技术进行电信诈骗的案件。

4月20日11时40分左右，福州市某科技公司法人代表郭先生的好友突然通过微信视频联系到他，经过短暂聊天后，好友告诉郭先生，自己的朋友在外地投标，需要430万元保证金，且需要公对公账户过账，所以想要借用郭先生公司的账户走一下账。好友向郭先生要了银行卡号，声称已经把钱打到郭先生的账户上，还把银行转账底单的截图通过微信发给了郭先生。基于视频聊天信任的前提下，郭先生没有核实钱是否到账，于11时49分先后分两笔把430万元给对方打了过去。钱款转账后，郭先生给好友微信发了一条消息，称事情已经办妥。但让他没想到的是，好友回过来的消息竟然是一个问号。

郭先生拨打好友电话，对方说没有这回事，他这才意识到竟然遇上了骗局，对方通过AI换脸技术，佯装成好友对他实施了诈骗。

“从头到尾都没有和我提借钱的事情，就说会先把钱给我打过来，再让我给他朋友账户转过去，而且当时是给我打了视频的，我在视频中也确认了面孔和声音，所以才放松了戒备。”郭先生说。

4月20日12时21分，包头市电信网络犯罪侦查局接到福建省福州市公安局刑侦支队的外协请求，称福建省一知名民营企业负责人被骗走430万元，而涉案的银行卡为包头市蒙商银行对公账户，希望包头警方能够帮忙进行紧急止付。

包头市公安局电信网络犯罪侦查局立即启动“包头市警银联动绿色查询机制”，当班民警以最快速度完成核查、报审程序，第一时间将涉案卡的信息通报至蒙商银行相关部门。在银行的全力协助下，仅用时10分钟，就将该诈骗账户内的336.84万元被骗资金成功拦截。

同时，向福州市公安局警方提供了剩余款项93.16万元资金流出信息，为深入突破该案剩余资金查找提供了突破方向。目前，福建警方与包头警方对此资金正在全力追缴当中。

诈骗成功率接近100%

福州郭先生的遭遇并非个例。近日，一名拥有百万粉丝的女网红也爆出了一起“AI换脸”事件。这名女网红表示，她的视频评论区突然涌来了很多人说看过她的“视频”，但她从未发布过这样的视频。

她疑惑地点开了这个视频，结果发现里面的女生和她长得一模一样，但做着一些不雅的动作，让她感到非常愤怒和无助。她突然意识到，可能是她的脸被人用AI技术盗用了。

据湖北网警巡查执法5月6日消息，AI新骗局来袭后，诈骗成功率竟接近100%。

警方提示：针对花样翻新的AI诈骗，公众要提高防范意识，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；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，不要未经核实随意转账汇款，不要轻易透露自己的身份证、银行卡、验证码等信息。如不慎被骗或遇可疑情形，请注意保护证据立即拨打96110报警。

遏制人工智能违法应用还须多方发力多管齐下

要遏制“AI换脸”等人工智能领域的深度合成技术应用乱象，还得多方主体共同发力多管齐下。

为了规范人工智能发展，尤其是规避AI换脸带来的系列问题，去年12月，《互联网信息服务深度合成管理规定》正式发布，对数据和技术管理规范进行了明确。比如，关于授权同意的原则提到，深度合成服务提供者和技术支持者提供人脸、人声等生物识别信息编辑功能的，“应当提示深度合成服务使用者依法告知被编辑的个人，并取得其单独同意”。简单来说，这些技术服务公司，不能随便使用普通人的人脸来换脸，必须经过本人同意，换脸不是想换就能随便换，也不是骗子给钱就能随便换。

今年4月11日，国家网信办发布《生成式人工智能服务管理办法(征求意见稿)》，对生成式人工智能产业给出较为详尽的规定，对用户安全保护已经迈出第一步。此外，监管部门要看到这一问题的严峻性，担负起监管责任，挖出相关产业链，给犯罪分子以震慑。平台和个人也应避免信息泄露，不给骗子留下把柄。

技术是一把双刃剑，拥抱新技术带来的发展与变革，也必须规避可能存在的风险和危险。既然有人在用它图谋不轨，就必须为这把剑装上剑鞘，这是为了保护剑，也是为了保护人。

■ 支招

防范AI诈骗可以这样做

多重验证，确认身份

在涉及转账交易等时，要格外留意，可以通过电话、视频等方式确认对方是否是本人。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”或者“24小时到账”，以预留处理时间。尽量通过电话询问具体信息，确认对方是否为本人。即便对方运用AI技术行骗，也可以通过提问的方式进一步确认身份。建议大家最好向对方的银行账户转账，避免通过微信等社交软件转账。一方面有利于核实对方身份，另一方面也有助于跟进转账信息。

保护信息，避免诱惑

加强个人信息保护意识，平时要谨防各种信息泄露，不管是在互联网上还是社交软件上，尽量避免过多地暴露自己的信息。对于不明平台发来的广告、中奖、交友等链接提高警惕，不随意填写个人信息，以免被骗子“精准围猎”。

相互提示，共同预防

高科技手段的诈骗方式，迷惑了很多人。警方提示各位，要多多提醒、告诫身边的亲人、朋友提高安全意识和应对高科技诈骗的能力，共同预防受骗。做好家中老人的宣传防范工作。提醒老年人在接到电话、短信时，要放下电话，再次拨打家人电话确认，不要贸然转账。

拒绝诱惑，提高警惕

要学会拒绝诱惑，提高警惕。避免占便宜心理，警惕陌生人无端“献殷勤”。如果事先不知道骗子的这些伎俩，被骗的可能性非常大。还是那句话：你目前还没被骗，并不是因为你多聪明，也不是因为你没钱，而是适合你的“剧本”还在路上。

■ 提醒

AI诈骗常用这些手法

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，从而可以用伪造的声音骗过对方。

案例：某公司财务小王接到领导电话，要求立刻给供应商转款2万元，并将转账信息以邮件形式发送，转款理由是避免缴纳滞纳金。由于老板的口音十分逼真，小王信以为真，在1小时内转款完成，后发现被骗。

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。在视频通话中再利用AI换脸，骗取信任。

案例：近日，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，小李看到确实是本人，便放心转账3000元。然而，她在第二次转账时感觉异常，便再次拨通对方电话，这才得知同学的账号被盗，于是报案。警方判断，那段视频很有可能是被人换了脸。

转发微信语音

骗子在盗取微信号后，便向其好友借钱，为取得对方的信任，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。

筛选受骗人群

骗子不是漫无目的地全面撒网，而是别有用心地锁定特定对象。例如，当进行金融诈骗时，经常搜集投资信息的小伙伴就会成为他们潜在的目标。运用AI技术，再加上套路和剧本的演绎，这样的诈骗手段，你能hold得住吗？

据《重庆晨报》、《广州日报》、澎湃新闻

今日16版　地址：山东省淄博市柳泉路280号　邮编：255000　广告许可证：鲁工商广字3700004000144　零售每份1.00元
新闻热线及投诉电话：0533-3585000　发行征订电话：0533-3595671　广告订版电话：0533-2270969　鲁中晨报印务有限公司电话：0533－8409106