

## 典型案例

对方换脸并拟声  
骗他转账430万元

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,两人经过短暂聊天后,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“高端”骗局,对方通过智能AI换脸技术,伪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,向福州市公安局提供了剩余款项93.16万元资金流出信息,为深入查找该案剩余资金提供了突破方向。

# AI换脸 骗术揭秘

好友通过微信视频联系郭先生,称自己的朋友在外地竞标,需要430万元保证金,且需要公对公账户过账,想借用郭先生公司的账户走一下账。随后,他把银行转账底单的截图发给了郭先生。基于对好友的信任,郭先生把430万元转到了他的银行卡。然而,当郭先生拨打好友电话时,对方说没有这回事……

随着人工智能的迅猛发展,诈骗团伙的诈骗手段也越来越科技化。近日,包头警方发布了一起利用AI实施电信诈骗的典型案例。案件披露后,“AI诈骗正在全国爆发”话题一度冲上热搜第一,引发网友热议。

## 多知道点

## AI诈骗有哪些手段

## 第一种: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账2万元,并将转账信息以邮件形式发送,转账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小时内转账完成,后发现被骗。

## 第二种: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,真是防不胜防!

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,遂报案。警方判断,那段视频很有可能是被人换了脸。

## 第三种: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。

## 警方提醒

防范新型诈骗  
请记住这几点

面对利用AI人工智能等新型手段的诈骗,我们要牢记以下几点:

## 1. 多重验证,确认身份

在涉及到转账交易等行为时,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。

## 2. 保护信息,避免诱惑

加强个人信息保护意识,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”。

## 3. 相互提示,共同预防

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。

## 4. 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。

## 法律护航

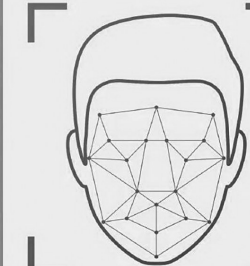
互联网信息服务  
深度合成有规定

针对技术手段日益更新的AI诈骗事件,2022年11月25日,国家互联网信息办公室、工业和信息化部、公安部联合发布《互联网信息服务深度合成管理规定》(以下简称《规定》),自2023年1月10日起施行。

近年来,深度合成技术快速发展,在服务用户需求、改进用户体验的同时,也被一些不法人员用于制作、复制、发布、传播违法和不良信息,诋毁、贬损他人名誉、荣誉,仿冒他人身份实施诈骗等,影响传播秩序和社会秩序,损害人民群众合法权益,危害国家安全和社

《规定》明确了深度合成数据和技术管理规范。要求深度合成服务提供者和技术支持者加强训练数据管理和技术管理,保障数据安全,不得非法处理个人信息,定期审核、评估、验证算法机制机理。深度合成服务提供者对使用其服务生成或编辑的信息内容,应当添加不影响使用的标识。提供智能对话、合成人声、人脸生成、沉浸式拟真场景等生成或者显著改变信息内容功能的服务的,应当进行显著标识,避免公众混淆或者误认。要求任何组织和个人不得采用技术手段删除、篡改、隐匿相关标识。

据新华每日电讯微信公众号



AI换脸  
应显著标识