【“3.15 消费者权益保护日”之反洗钱宣传】警惕“AI”换脸诈骗！

随着 AI 技术的广泛应用，AI 技术为社会公众提供了个性化、智能化的信息服务，同时也给不法分子带来可乘之机。一些不法分子开始利用 AI 技术通过面部替换、融合他人面孔和声音等方式，制造非常逼真的合成图像来实施新型网络诈骗，这类骗局常常会在短时间内给被害人造成较大损失，侵害消费者合法权益。**在“3.15”国际消费者权益保护日来临之际，前海联合基金提醒您：远离洗钱犯罪，保护个人信息安全和财产安全，配合金融机构履行个人反洗钱义务。**

那我们应该如何看清这类 AI“深度造假”？辨别“AI 换脸”有没有什么好方法？

首先，我们看看近期发生的 “AI 换脸”诈骗案例。

案例一：

陕西西安财务人员张女士与老板视频通话，老板要求她转账 186 万元到一个指定账号。

被害人张女士：老板让把这个款赶紧转过去，这个款非常着急，因为他声音还有视频图像都跟他人长得一样的，所以就更确信这笔款是他说的了，然后我直接就把这笔款转了。

转账之后，张女士按照规定将电子凭证发到了公司财务内部群里，然而出乎意料的是，群里的老板看到信息后，向她询问这笔资金的来由？

被害人 张女士：然后我们就打电话再跟老板去核实，老板说他没有给我发过视频，然后也没有说过这笔转账。

意识到被骗的张女士连忙报警求助，警方立刻对接反诈中心、联系相关银行进行紧急止付，最终保住了大部分被骗资金 156 万元。

案例二：

近期，香港警方也披露了，一起 AI“多人换脸”诈骗案，涉案金额高达 2 亿港元。据央视新闻报道，在这起案件中，一家跨国公司香港分部的职员受邀参加总部首席财务官发起的“多人视频会议”，并按照要求先后转账多次，将 2 亿港元转账到了 5 个本地银行账户内。其后，向总部查询才知道受骗。

警方调查得知，这起案件中所谓的视频会议中只有受害人一个人是“真人”，其他“参会人员”都是经过“AI 换脸”后的诈骗人员。

香港网络安全及科技罪案调查科网络安全组署理高级警司陈纯青表示，这名受害员工在收到据称来自该公司驻英国首席财务官（CFO）的信息后，原本怀疑是一封钓鱼诈骗邮件，因为内容涉及秘密交易。

然而，在和诈骗分子视频通话后，这名员工就打消了起初的怀疑，因为在场的其他人看起来和听起来都和他认识的同事一模一样。

结合以上两个案例，我们来看看 AI 诈骗常用手法有哪些呢？

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。

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。

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。

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。

第四种：AI 程序筛选受害人

骗子利用 AI 来分析公众发布在网上的各类信息，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。

此类诈骗手段，迷惑性、隐蔽性较强，诈骗金额较高，为保护广大金融消费者合法权益，前海联合基金提醒大家，做好以下防范措施：

一、识别假脸

多数假脸是使用睁眼照片合成，假脸极少甚至不会眨眼，缺少眨眼是判断一个视频真假的好方法。辨识“深度伪造”换脸视频的方法还包括语音和嘴唇运动不同步、情绪不符合、模糊的痕迹、画面停顿或变色。

二、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，要小心；

对突如其来的电话保持警惕，即使是来自你认识的人，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；

在涉及到转账交易等行为时，通过电话等形式询问具体信息，多重验证确认对方是否为本人。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，将转账到账时间设定为“24 小时到账”，以预留处理时间。

三、保护信息，避免诱惑

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，陌生好友不要随便加，防止手机、电脑中病毒，微信、QQ 等被盗号；

加强个人信息保护意识，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”。

四、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，让他联系你当地的派出所。

五、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。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。

六、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”。