海峡都市报 报料：智慧海都 968880
2024年3月3日 星期日 责编/关菁 美编/唐昊 校对/德峰

久未露面的57岁著名音乐人、曾担任《快乐女声》评委的包小柏，最近用AI技术“复活”了去世的女儿，“她”不仅可以即时回复对话，而且还在妈妈生日时唱了生日快乐歌。

同样是最近，另一群中老年网友却被AI的深度伪造伤了心。他们发现自己真心实意追了一阵的几位俄罗斯美女博主通通不存在，都是有人“偷”了一位乌克兰女孩的脸，批量生产的AI换脸数字人。

而上了“AI换脸”当的，还有香港的一位职员，参加“多人视频会议”时被骗了2亿港元。

生成式AI时代下，耳听未必为真、眼见未必为实，你接收到的文字、图片、音视频信息都可能是AI的产物。而逐渐模糊的现实边界，正在诞生新的数字鸿沟。

唐昊/漫画

海都故事绘

AI正引发新的数字鸿沟

乌克兰姑娘的脸被“偷”来卖特产

俄罗斯大妞叶琳娜，在中国生活8年、能说一口流利中文的April安娜，卖俄罗斯进口食品的31岁娜塔莎，喜欢分享中国日常的艾莉儿……

过去的一两个月，只要爱逛短视频和社交平台，大概率就会刷到一些长相精致的俄罗斯美女博主。她们热爱中国文化，表示想嫁中国男人，还会谈论一些争议性的热门话题，像是婚嫁的彩礼问题，聊着聊着还会推荐起俄罗斯特产。

但她们的脸都是从一位乌克兰网红身上“偷”的。

不久前，在美国一家视频网站上拥有1万多粉丝的奥尔嘉在一段近15分钟的视频中，控诉了这件事。

“她们有我的脸、我的声音，且能说一口流利中文。”奥尔嘉愤怒而无奈。这些账号用AI生成的短视频内容赚取流量，为俄罗斯巧克力、糖果等特产带货。其中，卖进口零食的娜塔莎，在账号被平台下架前已拥有超20万粉丝，远多于她本人的账号。

“这让人不寒而栗。”奥尔嘉说以前见过名人被模仿，从未想过自己也会深陷其中。“在这些AI生成的博主背后，作为原型的普通女性可能还不知道自己的脸被盗了，然后被用于何处。”

对此，相关平台很快采取了行动，并且强调“禁止任何以他人照片或视频进行换脸的行为”。然而，换脸的“潘多拉魔盒”已经被打开，仅靠自觉和举报，似乎无法阻挡。

参加“多人视频会议” 男子被骗2亿港元

参加多人视频会议结果只有自己是真人，这事听上去似乎匪夷所思却真实地发生了。

近期，香港警方披露了一起多人“AI换脸”诈骗案，涉案金额高达2亿港元。

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2亿港元分别转账15次，转到5个本地银行账户内。

之后，其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。

近期，在陕西西安也发生了一起“AI换脸”诈骗案例。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。老板称，这笔款要得非常急。因为声音和视频图像都跟老板一样，所以张女士没有怀疑就转账了。

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。打电话跟老板核实后，才发现上当受骗，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。

“文件传输助手”是真人？女子称被骗9年隐私

近日，一则“女子被好友改名文件传输助手骗9年”的消息引发热议。

安徽合肥一女子发文称，自己的一位微信好友把昵称改为“文件传输助手”，还使用了同样的头像，自己用了9年，近日才发现这不是官方账号。而她在不知情的情况下，曾给对方发过手持身份证照片、学信网证书、房产证等隐私信息，对方从未提醒。

该女子称，这个好友是2015年左右出于工作原因加上的，没有改备注。那时才刚刚开始用微信，不太熟悉相关功能，用文件传输助手时，直接搜索出来两个相似的账号，误以为微信本身就有两个“文件传输助手”，于是选择一个一用就是9年。

而这个账号最近发了两条朋友圈，且昵称改为“文件传瑜助手”，女子这才注意到有问题，随后报警，并向微信客服反映。

据澎湃新闻报道，2月28日，安徽舒城县城中派出所民警表示，事件正在处理，主要看事件对当事人有没有造成影响。如果银行卡内钱财被人转移，或者身份证被他人用来贷款，警方就能追踪到具体的人。只把对方当成文件传输助手发送信息，对方没有造成什么实际损害的情况下，就没有办法处理。

支招

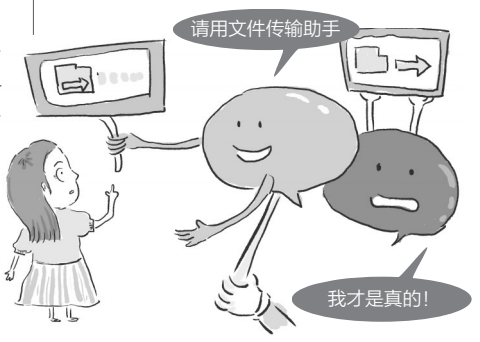
学会几招 识别AI“换脸换声”

专家表示，其实AI人工换脸无论做得多逼真，想要识别真假，还是有一些方法的。

中国计算机学会安全专业委员会数字经济与安全工作组成员方宇表示，可以要求对方在视频对话的时候，在脸部的前面通过挥手的方式，识别实时伪造的视频。挥手过程中，伪造的人脸，会产生一定的抖动、闪现，或是一些异常的情况。

此外，在点对点的沟通中，可以问一些只有对方知道的问题，验证对方的真实性。

中国科技大学网络空间安全学院执行院长俞能海提醒，可以让对方摁鼻子、摁脸，观察其面部变化。如果是真人的鼻子、脸部，摁下去是会变形的，但AI生成的鼻子和脸部并不会。



测试

“文件传输助手”的秘密只有自己知道？

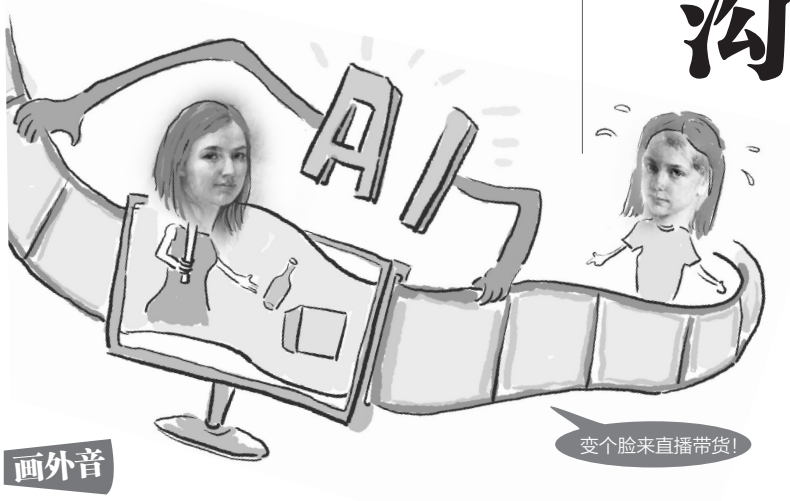
腾讯官方客服人员在接受媒体采访时表示，若工作人员核实到该账号确实存在违规的情况，会对涉事账号进行处置。客服人员提到，微信的头像和名字是可以自行设置的，有可能被有心之人钻了漏洞，将会对相关情况进行记录反馈。

27日晚，这名女子称，其投诉的高仿号已被封。

2月28日下午，“微信不能改名文件传输助手”的话题登上热搜第一。

而早在2023年6月27日，@腾讯微信团队就回应过类似传闻：“抱歉，查无此人。你发给‘文件传输助手’的小秘密，只有你自己知道。”

当天下午3时许，极目新闻记者尝试用“文件传输助手”“文件传偷助手”“文件传瑜助手”名称修改微信名，但显示“操作不成功，请修改或稍后再试”。不过，记者使用“文件专瑜助手”这一名称修改微信名却成功了。



画外音

“复制”一个人更容易了 平台和监管准备好了吗？

用AI工具生成一张美女照片，贴上“80后单亲妈妈”“每日分享自用好物”等标签，加入商品图片和介绍，这种简单而粗糙的AI美女种草/情感博主，眼下正在短视频平台上批量出现，瞄准中老年群体。

没抠好的头发丝，几乎一样的脸，循环的表情和动作，哪怕破绽多到“一眼假”，哪怕平台已经给部分作品标注了“内容疑似AI生成，请仔细甄别”，仍有大量中老年网友热情互动，并掏出真金白银。

对于许多中老年人来说，智能手机和互联网还没有完全弄明白，AI就又来捣乱。他们中的大多数，可能并不具备鉴别真人和AI数字人的能力，也理不清楚新型网络诈骗是怎么回事。

现在，只要有充足的数据，从声音、口型到整张人脸都能通过深度学习算法，活灵活现地还原出来。

随着技术持续进步，“复制”一个人更容易了，如何防止诈骗的发生，相关平台和监管政策准备好了吗？

提醒

提高防范意识 避免个人信息泄露

专家表示，除了知晓一些辨别AI换脸诈骗的小诀窍，每一个人都应该提高防范意识，在日常生活中也要做好相关防范，养成良好的上网习惯。

第一，应该做好日常信息安全保护，加强对人脸、声纹、指纹等生物特征数据的安全防护。另外做好个人的手机、电脑等终端设备的软硬件的安全管理。

第二，不要登录来路不明的网站，以免被病毒侵入。

第三，对可能进行声音、图像甚至视频和定位等信息采集的应用，做好授权管理。不给他人收集自己信息的机会，也能在一定程度上让AI换脸诈骗远离自己。

（综合央视、广州日报、都市快报、澎湃新闻、极目新闻）