“AI换脸”诈骗如何防 看完这篇不上当

近年来，随着人工智能技术的进步，一些不法分子开始利用AI技术融合他人面孔和声音，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。那么，如何识别“AI换脸”诈骗？有哪些防骗妙招？相关专家作出详细解答。

“AI换脸”背后的技术原理

在技术层面，“AI换脸”是如何实现人脸的精确识别与替换，创造出逼真效果的？中国网络空间安全协会人工智能安全治理专委会专家薛智慧表示，“AI换脸”过程主要包括人脸识别追踪、面部特征提取、人脸变换融合、背景环境渲染、图像与音频合成等几个关键步骤。其背后最核心的可概括为三个部分，首先，利用深度学习算法精准地识别视频中的人脸图像，并提取出如眼睛、鼻子、嘴巴等关键面部特征。其次，将这些特征与目标人脸图像进行匹配、替换、融合。最后，通过背景环境渲染并添加合成后的声音，生成逼真度较高的虚假换脸视频。

专家介绍，以诈骗为目的，实施点对点视频通话，需要AI人工智能生成仿真度极高的视频。想要达到以假乱真效果用于诈骗，难度不小。薛智慧介绍，AI人工智能生成背后需要有大量的资金投入，包括图片的采集、专业算法的人员等。且各方面的投入需要长时间不断地迭代，才能达到一个相当逼真的效果，才有可能达到诈骗的实际效果。

识别“AI换脸换声”有办法

“AI换脸”这一技术的出现，导致耳听为虚、眼见也不一定为实了。那我们该如何防范呢？专家表示，其实AI人工换脸无论做得多么逼真，想要识别视频真假还是有一些方法的。

“实际上从目前的深度伪造实时视频上来看，是可以通过一些方式进行验证的”。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认为，我们可以要求对方在视频对话的时候，在面部前挥手。由于实时伪造的视频要对视频进行实时生成和处理“AI换脸”，因此在挥手的过程中，就会造成对面部数据的干扰，而伪造的人脸此时会产生一定的抖动或者闪烁等异常情况。再就是可以通过点对点的沟通，比如问一些只有对方知道的问题来验证。

避免泄露个人生物信息

专家表示，除了一些辨别“AI换脸”诈骗的小诀窍，我们应该提高防范意识，在日常生活中也要做好相关防范措施，养成良好的上网习惯：做好日常的信息安全的保护，加强对人脸、声音、指纹等生物特征数据的安全防护，做好个人的手机、电脑等终端设备的软硬件的安全管理；不要登录来路不明的网站，以免被病毒侵入。对可能进行声音、图像甚至视频和定位采集的应用，做好授权管理；不给他人收集自己信息的机会，也能在一定程度上远离“AI换脸”诈骗。 **据央视新闻客户端**

谜语直播间 可能暗藏陷阱

一段时间以来，一些直播平台上出现了大量“谜语人”直播间——主播或戴着面具，或在纸上写着让人看不懂的话，或在直播页面呈现各种符号，他们的目的很简单，就是尽可能吸引观众点进直播间，再引导观众落入陷阱。

网络直播是当下最火的领域之一。数据显示，截至2023年6月，我国网络直播用户规模达7.65亿人。通常情况下，网络主播都以真面目示人，也以通俗易懂的表达与粉丝、网友互动。如今却出现大量“谜语人”直播间，充满神秘气息，让人难以捉摸。

无论是主播隐藏真面目，还是发布一般人看不懂的信息，目的之一是通过故弄玄虚来显示与其他主播的不同，吸引观众进入直播间，进而达到某种目的。由于看惯了透明式直播，一些网友难免对这种神秘直播感到新鲜，就特别容易关注。目的之二是为了逃避监管。从报道来看，这类“谜语人”直播间吸引观众进入后，大多引导观众加入粉丝群、企业号等，来推广其不法活动。还有的甚至提供色情服务、诱导他人去赌博平台、刷单诈骗等。

由于这种引流背后暗藏陷阱，见不得光，于是就以“谜语直播”方式出现，来躲避平台和有关部门的监督。而且这类直播时间较短（10至30分钟），主播都是小号，有些甚至播一次换一个号，目的是在成功引流后逃避法律制裁。

从某种意义上说，这是网络直播陷阱的一种新形式。当观众被这种故弄玄虚的直播所吸引，就有可能掉进陷阱，遭遇经济损失等不利后果。这种“谜语直播”，已涉嫌违反《互联网直播服务管理规定》《广告法》《治安管理处罚法》《刑法》等法律法规的有关规定。

然而，对这种“谜语直播”的监管却存在一些现实困难。这类“谜语直播”一般时间较短，随机性较强，行动比较隐秘，平台仅靠算法很难发现，而人工审核又存在滞后性。由此亦可见，“谜语直播”幕后的不法分子十分狡猾，既善于“钓鱼”，也善于隐藏自己。此外，某些“谜语直播”的背后很可能是团伙作案，甚至可能隐藏着大案要案，因此，观众要擦亮眼睛，避免被这种故弄玄虚的神秘直播钓上钩。如果某些直播间缺乏透明度，就应倍加小心，不要在好奇心驱使下点击进入。 **据《北京青年报》**

安全大讲堂

交警送上安全提示 护航上学路

□潍坊日报社全媒体记者 王晓萌

寒假结束，各中、小学校迎来开学季，接送学生的车辆随之增多。开学季，如何护送孩子平安上下学？昌乐县公安局交警大队作出安全出行提示，助力广大家长和学生规避出行风险，保护自身和他人的交通安全。

交警提醒，驾车出行时，家长要提前规划出行路线，预留足够的时间，注意行车安全；驾驶人和乘客都要系好安全带；行车过程中，要锁上车辆儿童安全锁，防止孩子自行打开车门发生危险；接送孩子时，要服从护学岗人员指挥，做到“即停即走”；停车时，要将车辆停放至附近停车场或者指定的临时停车位，共同维护校门口交通秩序，做到从车辆右侧上下，最安全；不超速、不超员、不超载、不疲劳驾驶、不酒后驾驶、不闯红灯、不逆向行驶，不违反交通标志标线规定，不争道抢行，不向车外乱扔杂物，开车不接听手机等。

驾驶电动自行车接送学生的家长，须在非机动车道内行驶，一定要使用注册登记的电动自行车，且只能搭载一名12周岁以下的儿童，大人和孩子都要佩戴好安全头盔。年龄稍大的孩子可以自行上下学，但未满12周岁的儿童不能驾驶自行车上马路，未满16周岁的少年不能驾驶电动自行车，家长要叮嘱孩子行走或骑车时不要看手机、听音乐，不要占用机动车道。

此外，不要搭乘“三无”车辆，不乘坐超员超载、车况不好、酒驾的车辆；不乘坐未注册登记的电动三轮车、电动四轮车、报废车辆等；家长不得租用或集体租用非运营车辆接送学生，自觉抵制非运营车辆载客行为；提醒孩子不要乘坐陌生人的车辆。

对于走路上学的孩子，家长要加强对孩子的交通安全教育，提醒孩子走路要集中注意力，走人行道或者人行横道线，做到不闯红灯、不翻越隔离栏，不在马路上、车辆周围玩耍。如果是第一次上学的孩子，监护人应与孩子一起实地体验上下学路线，教育孩子遵守交通规则，从小培养文明出行意识和习惯。

交警提示，出行途中安全第一，如果遇到突发情况不要慌张，要冷静地采取正确的自我保护措施。如发生交通事故，在可能的情况下要记住车辆的颜色、型号、车牌号以及周围认识的人，便于后期的处理，并及时打110报警电话求助。学校开学后，城区道路交通将出现早晚高峰提前、交通高峰时段延长等趋势，交通运行预计出现部分路口和路段缓行。群众出行如遇交通流量较大时，请服从交警现场指挥，自觉排队，耐心等候，有序通行。