

# 以假乱真的AI诈骗，如何防范？

□ 人民日报记者 张天培 苏滨

上传一张静态照片，即可生成动态视频；只需几秒语音，就能克隆声音……这不是科幻电影，而是发生在身边的真实事件，“AI换脸”正成为侵权违法的重灾区。

近期，为规范应用人脸识别技术处理人脸信息活动、保护个人信息权益，国家互联网信息办公室、公安部联合公布《人脸识别技术应用安全管理办法》，对应用人脸识别技术处理人脸信息的基本要求和处理规则、人脸识别技术应用安全规范、监督管理职责等作出了规定。办法将于2025年6月1日起施行。

人脸识别技术应用与人脸信息安全紧密相关。人脸识别具有唯一性、不可更改性、不可匿名性，一旦泄露，极易对个人的人身和财产安全造成危害，还可能威胁公共安全。

## AI诈骗形式多样 换脸、变声、对口型

贵州省黔东南苗族侗族自治州凯里市公安局反诈中心负责人吴西福介绍，一家科技公司的负责人郭先生有一天接到好友打来的视频电话，说自己正在外地投标，需要几百万元保证金，想用郭先生的公司账户走一下账。不久后，好友说已经把钱转到郭先生的账户并截图证明。郭先生觉得通过视频能看到好友本人，便没等收到转账成功的通知就给好友转了钱。后来，郭先生迟迟没收到转账，联系好友时才发现自己已被骗。

宁夏回族自治区银川市某公司部门经理张先生接到“老板”视频电话，对方称因情况紧急，急需转账汇款。在视频中确认是“老板”后，张先生放下了戒心，十几分钟内将20万元转入指定账户。直到下午当面汇报工作时，张先生才发现上当受骗。

这些案件都是典型的AI诈骗。“你以为是和朋友亲人视频聊天，其实是骗子使用的‘AI换脸’技术，让别人的嘴能够‘对口型’。”宁夏回族自治区公安厅刑侦总队副队长、反诈中心负责人吴克刚介绍，如今，“AI换脸”技术不仅限于静态照片的活化，还能在即时视频通信中实时换脸。虽然需要采集大量不同角度的照片进行模型训练，但一旦成功，便可以假乱真。过去，公民个人身份证号、手机号以及家人信息需要重点防范，现在，人脸、声音、指纹等同样要避免泄露。

新型AI诈骗主要有以下类型：语音合成诈骗，不法分子利用AI技术，合成受害人亲友或熟人的声音，让受害人误以为是亲友或熟人需要帮助，进而实施电话诈骗；图像生成诈骗，不法分子通过AI技术，生成虚假的照片或视频，制造出受害人亲友紧急且合理的情景，从而获取个人信息、骗取钱财；智能客服诈骗，不法分子利用AI技术，制作智能客服系统，通过语音或文字同受害人交流，诱骗受害人提供个人信息或进行转账操作；AI情感诈骗，不法分子运用AI训练面向网聊的大语言模型，通过伪造场景、声音与受害人建立情感关系，进而获取个人信息。

吴西福介绍，共享屏幕等新型诈骗也要注意。不法分子以“提升信用卡额度”“航班延误退费”“赠送礼品”等为借口，向个人发送短信或拨打电话，诱导受害人下载指定软件，并开启软件的“共享屏幕”功能，就可以“实时监控”受害人手机、电脑屏幕，同步获取个人银行账户、口令、验证码等重要信息，从而窃取银行卡资金。

## AI诈骗危害广泛 造成经济损失、心理创伤

相较于电信诈骗、网络诈骗，新型AI诈骗的受害者身份更广泛、多元，成功率更高，更难以追踪。

警方梳理后发现，新型AI诈骗有以下危害：造成经济损失，新型AI诈骗具有针对性强、高度逼真等特征，普通群众短时间内难以分辨，很容易上当受骗、遭受经济损失，甚至会给家庭带来沉重的经济负担；发生信息泄露，新型AI诈骗往往能获取受害人的个人信息，包括身份证号、银行账户、人脸、指纹等，进而滥用这些信息从事非法活动，导致受害人信息泄露，身份被盗窃，引发潜在的法律风险；造成心理创伤，遭受新型AI诈骗，除了面临经济损失，受害人还可能产生焦虑、自责、抑郁等情绪，造成严重的心理创伤；危害社会治安，如果新型AI诈骗案件增多，容易让群众对社会产生不信任感，甚至造成恐慌情绪，有些受害者也因无法承担损失，走上违法犯罪道路。

新型AI诈骗案件增加，侦破难度加大，对公安机关来说也是挑战。吴西福说，只有不断提升民警的专业素质和侦查能力，加强对新型电信网络诈骗犯罪的研究，才能创新侦查手段和方法，提高打击效能。要加强与其他地区公安机关的协作配合，建立健全跨区域警务合作机制，形成打击合力。

## 有效防范AI诈骗 保护个人信息、学习识别方法

新型AI诈骗花样频出，伪装性越来越强，该如何防范？

吴克刚给出了两条防骗建议：视频通话时，让对方做出指定动作，比如眨眼3次、摸摸鼻子，或者让对方用手指或其他遮挡物在脸前晃动，如画面出现延迟或者异常扭曲等不自然的微小变化，那对方很可能正在使用“AI换脸”技术。在与对方的沟通中，也可以问一些只有对方知道的问题，比如生日、电话号码、喜好等，来验证对方身份的真实性。

我们也应该提高安全防范意识，防止人脸面部信息被非法获取利用。贵州警方提示，不轻信他人，不贪图小便宜。妥善保管个人信息，把好个人信息保护的第一道关。在非必要情况下，不向陌生人提供身份证号码、工作单位、家庭住址、职务等重要信息，不将身份证照片或号码保存在手机中，尽可能避免将人脸、照片、声音、指纹等留存到网站和小程序上。在日常生活中，加强对人脸、声音、指纹等生物特征数据的安全防护，做好个人手机、电脑等终端设备的软硬件安全管理，不登录来路不明的网站，以免感染木马病毒。另外，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，不要轻易给他人收集个人信息的机会，也能在一定程度上远离“AI换脸”诈骗。

此外，公安机关也要创新线上线下反诈宣传，打造全方位反诈宣传矩阵。一方面，利用线上平台，深入挖掘本地发生的电信网络诈骗典型案例，结合地区特色、民俗以及当下流行的网络文化，拍摄制作风格独特、通俗易懂的反诈宣传短视频。通过短视频的形式还原诈骗分子的话术、作案流程以及背后的犯罪逻辑，帮助群众提高反诈意识。

推动反诈宣传进校园、进社区、进企业，将反诈宣传与群众喜爱的文化娱乐活动紧密结合，打造出一系列具有贴近性的反诈宣传场景。坚持精准施策，针对不同群体、行业和地区特点，开展有针对性的宣传，做到有的放矢，切实增强群众防骗意识和识别能力。

警方也警告不法分子：通过“AI换脸”进行视频合成、实施诈骗的行为，是利用新技术进行的诈骗，与传统诈骗行为没有本质区别。对于构成诈骗罪的，将依照我国刑法第二百六十六条的规定追究刑事责任；对于为利用“AI换脸”实施诈骗行为提供技术支持、帮助的，将根据反电信网络诈骗法的规定进行行政处罚，构成犯罪的，还要追究刑事责任。

# 从春招市场看人工智能产业人才供需

□ 人民日报记者 黄超

浙江杭州春季首场大规模线下人才招聘会，830家企业推出2.1万个岗位，半数聚焦人工智能算法、大模型研发；华东理工大学春季重点单位专场招聘会，前十号展位成了人工智能、集成电路的“热门求职走廊”……人工智能赋能千行百业，不少用人单位“扩招”相关岗位。

“人工智能+”为就业市场提供新机遇。当前，在就业市场活跃的人工智能岗位有哪些？反映出怎样的产业发展趋势？长期来看，人工智能产业哪些职业值得关注？近日，记者走进校园和产业应用一线采访。

## 人工智能广泛落地，算法人才供需两旺

宁夏吴忠利通区扁担沟中心学校，是当地智慧课堂创新实践应用项目试点校。智慧教室里，一堂语文课正在进行，学生们分组讨论，并通过平板电脑将答案上传系统。

“27次问答，追问占比22%。”下课后，教师收到一份人工智能课堂报告，涵盖师生问答、课堂行为等，提醒其针对性地改进教学方法。这份报告源自2000公里外的广东，由广州视睿电子科技有限公司研发的课堂智能反馈系统提供。

“报告的生成离不开背后的算法工程师。”吴捷是广东工业大学硕士生，在视睿科技自然语言处理方向的算法工程师岗位实习。这段时间，他参与了课堂智能反馈系统的数据处理，以及大模型训练、评测工作。

“系统搭载了教育大模型，我们对课堂环节进行多模态数据采集和分析，让系统准确捕捉师生问答等有效信息，反复学习这些数据。”吴捷说，与此同时，将教育教学理论转换为人工智能掌握的语言，训练其提出专业建议。

随着人工智能技术向更多场景延伸，“人工智能+”浪潮以前所未有的速度，改变着人们的工作与生活。“人工智能+教育”“人工智能+金融”“人工智能+医疗”……传统行业迎来智能化新机遇。

以视睿科技为例，其主营的液晶显示主控板卡、交互智能平板等人工智能产品，广泛应用于家电、教育、企业服务等领域。“人工智能技术涉及研发、生产、服务全流程，需要大量算法人才。”公司首席技术官杨铭表示。

在多地春招市场，算法工程师岗位供需两旺。招聘平台数据显示，今年春招，机器人算法工程师招聘同比增长超30%。从行业分布看，招聘机器人算法工程师最多的行业是人工智能。

“一方面，要对现有大模型进行性能调优及工程化落地，通过技术创新降低成本；另一方面，需突破具身智能、多模态融合等技术瓶颈。这些技术需求，带动了算法工程师等岗位的招聘需求。”杨铭说，“数理基础扎实、动手能力强、具备一定的人工智能学习背景，我们就非常欢迎。”

## 算力需求激发关键硬件发展潜力，为求职带来利好

算力是人工智能发展的核心要素之一。人工智能在各领域的快速应用发展，也增加了对高算力、高性能的人工智能加



速器的需求，相关产品产量快速增长。

“人工智能加速器是专门用来加速人工智能任务处理的硬件，能快速理解大量信息，帮助手机、电脑等设备完成以往难以高效解决的任务，比如图像识别、语音识别、自然语言处理等。”上海交通大学博士生王旭航即将毕业，入职上海华为技术公司从事研发工作。

“读博期间，我见证了人工智能从起步进入‘深思考’阶段，用户需求指数级增长。这让我们相关专业的学生在找工作时，选择面更宽了。”王旭航说，这几年明显感到人工智能加速器研发岗位的需求在增加，“我应聘的岗位今年还招了几名博士生和硕士生。”

在企业办公、工业互联网等场景中，高效部署人工智能加速器非常重要。我未来参与研发的主要涉及通信领域，通过设计专用的人工智能加速器提高运行效率。”王旭航介绍。

根据中国人工智能算力发展评估报告，2024年我国智能算力规模同比增长74.1%。“这意味着人工智能加速器作为关键硬件，将有更大的发展潜力和市场空间。”上海交通大学人工智能学院教授张娅表示，对有志于投身这场科技革命的年轻人来说，正是抓住机遇的时候。

这两年，张娅指导的一些学生也进入科技企业从事相关工作。“人工智能加速器设计和研发是跨学科的，不仅需要深厚的电子工程知识，还要对计算机体系结构、机器学习算法有较深刻理解。”张娅说，相关团队通常由软件工程师、硬件工程师和系统架构师等组成，“行业对专业人才的需求很大，为学生求职带来利好。”

采访中记者发现，有的地方积极布局算力基础设施建设，招商、引才同步推进，通过项目落地汇聚人才要素。多地在人工智能人才吸引和产业布局方面主动作为，以在人工智能产业竞争中赢得先机。

“请规划最快的回家路线。”杭州一名

车主坐进汽车，对着车内搭载的智能系统发出指令。几乎同一时间，车辆启动导航，根据实时交通信息选择最佳路径。要想语音指令快速响应，让系统迅速做出可靠判断，就需要数据传输更高效。

数据，是人工智能大模型训练的“燃料”。通过海量数据的训练，大模型才能具备强大的泛化能力。近年来，数据科学家、分析师、工程师等，成为人工智能领域较受欢迎的岗位。与此同时，一些聚焦技术底座的职业，因其处于打基础、利长远的重要环节，也受到科技企业关注。

浙江大学应届毕业生席少珂前不久通过校园招聘，收到阿里云智能集团的录用通知，岗位是网络技术高级开发工程师。“我报考的基础设施事业部负责为用户提供计算、存储、网络等基础云服务。”在她看来，这个岗位就是为人工智能世界建造和维护“数字高速公路”“超级计算工厂”。

“大模型训练过程中，海量数据进出

## 热度高，更需多些冷思考

□ 韩文榕

今年就业季，“人工智能”是热门。打开求职软件评论区，“人工智能方向的就业机会主要集中在哪些岗位”“我是文科生，‘上船’人工智能，有机会吗”……类似问题吸引很多关注。

伴随人工智能产业发展，企业人才需求更加旺盛：算法架构师、硬件工程师、数据分析师……岗位细分，体现着行业对人才的多元期待。多个高校在新兴前沿领域扩大招生，是对产业快速发展的积极回应。

热度高，更需要多些冷思考。从人才培养的角度看，高校应紧盯经济社会发展趋势，跟上节奏、抢占先机；但也应因地制宜设专业、定规模，将行业场景融入教学环节，切不可盲目跟风头、抢

服务器。我们会研究设计更宽敞快速的数据通道，让训练速度更快、成本更低。”席少珂说，数据既要“跑得快”，还要“不迷路”。比如，当服务器宕机，数据传输需要自动切换路线，绕过“危险路段”。“我们的工作可以让人工智能基础设施更高效、更稳定。”

这类岗位需求为何增加？席少珂认为：首先，人工智能网络基础设施涉及硬件传输、协议设计、故障容错等多个细分领域，需要大量网络“匠人”各展所长。其次，技术底座一旦出问题，会影响用户安全、企业利益，这就要求每个技术细节极致打磨。最后，随着人工智能快速发展，网络技术必须同步升级，既要追赶现有技术，又要预研未来需求，需要更多人手参与快速迭代。

据介绍，阿里巴巴集团已启动春季2026届实习生招聘。更加注重人工智能方向，相关岗位占比近五成；部分人工智能业务部门占比更高，在阿里云超80%。阿里云资深招聘总监曹彬介绍，公司涉及数据的岗位增多。比如多模态工程师，开发和优化支持文本、图像、音频、视频等多模态数据的人工智能模型；再如合规专家，制定人工智能系统的数据隐私保护策略，确保技术应用符合法律法规。

校园招聘中，人岗相适度如何？曹彬告诉记者，随着新岗位需求扩大，存在一定的人才结构性短缺。“从企业用人角度看，打好理论基础的同时，希望增加与应用场景相关的实践经历，人才培养与技术迭代同频共振。”

面对产业发展“热度高”，专家表示，人才培养要“冷思考”。“行业对高层次、具备综合能力的人工智能人才有着较大需求。”中国科学院自动化研究所研究员王亮表示，近年来高校人工智能专业的报考升温，但关键在于优化人才培养结构，注意质量的提升和人才的合理分布。未来，随着人工智能技术深入应用，不同层次和领域的人才需求会更加细分，高校在专业设置和课程设计上应更加注重人才的差异化培养，以适应不同产业方向的需求。

“大模型训练过程中，海量数据进出

于求职学生而言，全方位提升能力才能“拿票上船”。打牢基本功的同时提升实践能力，结合行业需求挖掘自身优势，就更容易在竞争中获得机会、脱颖而出。

对用人单位来说，把觉得人才作为起点，将人才与研发生产流程精准匹配，完善人才培养机制，创新发展方能更上台阶。

面对人工智能热潮，多一些冷静的思考，才能多一分成长的从容。总之，进一步形成人才辈出、人尽其才、才尽其用的生动局面，人工智能产业发展前景可期。

## ■ 子夜走笔



## 最是一年春好处

▲近日，游客在湖北省宣恩县珠山镇和平社区赏花游玩（无人机照片）。  
▲近日，游客在河北省石家庄市植物园赏花游玩。  
最是一年春好处，繁花似锦，春风和暖，人们踏春赏花尽享春光。

宋文 摄  
陈其保 摄  
新华社发