责编/李娜　美编/唐旺勋
2026.4.9 星期四
财会信报 3·15消费

内蒙古自治区消费者权益保护服务中心指导

定制“骗局网”、诱导借贷、退费无门：部分“AI+”培训“围猎”年轻人

近年来，随着人工智能技术席卷各行各业，一股以“AI创作”“Python编程”“AI配音”等为名的新型“AI+”培训热潮异军突起。然而，这场技术盛宴的背后，一条精准瞄准涉世未深年轻群体的“割韭菜”产业链正在悄然成形。

一个精心设计的陷阱

“零基础学AI，轻松月入过万”“适合在校大学生，课余时间就能做”——在不少短视频平台上，类似广告非常具有诱惑力。

来自四川内江市的大学生小张正是被这样的诱惑击中，掉进了精心设计的陷阱。

2025年6月，小张在网络直播间看到一则“零基础学AI轻松变现、学不会全额退款”的广告。课程顾问热情介绍，只需支付2690元购买基础课程，学成后接单每月至少收入5000元。小张心动付款后，课程顾问却开始以“账号流量低、起步慢、变现难”为由制造焦虑，接连推销5000—10000元的高阶课程和流量套餐。当小张意识到不对劲、要求按承诺退款时，对方却搬出电子合同，称“开课后仅退10%”。小张这才发现，报名时匆忙勾选的电子合同里，一堆密密麻麻的条款中竟然藏着高额违约金的“暗雷”。

“快要毕业了，想着能学一门新技术也好，没想到就被骗了。”小张懊恼地说。

无独有偶，四川德阳小伙朱先生近期花费9580元购买了某科技公司的“AI+”视频剪辑教学服务，却发现所谓的“精品课程”不过是画质模糊、内容简陋的录播材料，与宣传的“名师一对一指导”相去甚远。该公司只同意退还1376元人工服务费，拒绝退还8204元技术服务费。纠纷直至当地消委会介入才得以解决。

令人忧心的是，短期内四川内江市消委会就收到上百起情节雷同的投诉。涉事经营者虽公司名称不同，但操作模式惊人一致：以免费或低价“AI+”培训体验课引流，用虚假成功案例制造信任感，再以“仅剩最后优惠名额”催促消费者仓促付款，甚至诱导经济能力有限的大学生办理分期贷款。不少年轻人在“随时可退”的口头承诺下签订了分期付款合同，签署后才发现合同内暗藏高额违约金条款。

近期，四川省保护消费者权益委员会发布的统计报告显示，2025年全年“AI+”培训相关投诉达3739件，同比上升2.21个百分点。“通过对投诉案例的分析，我们发现受骗的年轻群体比较多。”四川省保护消费者权益委员会投诉部主任彭欧说。

为年轻人定制“骗局网”

记者调查发现，“AI+”培训乱象频发，其危害远不止是几千元的学费损失，它更像一张精心编织的大网，将涉世未深的年轻人牢牢套住。

——虚假宣传，定制“围猎”产业链。记者采访发现，一些商家编造虚假成功案例、伪造收益截图诱导消费，重点瞄准社会经验不足、经济需求迫切的大学生群体。不少所谓的“AI+”培训老师、培训课程都是从第三方打包购买的，不少直播课程实为录播。

更恶劣的是，涉事企业往往在收取大量学费后快速“隐身”，通过列入经营异常名录、注销公司等方式逃避维权责任。四川省消委会律师顾问团成员、四川川商律师事务所主任张义文认为，这类行为已涉嫌违反广告法、消费者权益保护法乃至刑法的相关规定，构成虚假宣传与欺诈行为。

——诱导大学生办理分期贷款。记者采访了解到，部分商家以“兼职收入能覆盖分期付款”为由，诱导经济能力较弱的大学生开通分期贷款，一旦培训课程无法兑现承诺，学生不仅学无所成，还要背负债务。

——退费无门、维权困难。“类似的培训大多都在网上，培训课程运营的是一个公司，贷款的又是另一个公司，经营主体非常复杂，维权的时候双方扯皮，很难找到具体负责的经营主体。”一位被骗大学生坦言。

“我们接到的投诉受害者也遍布全国多地，这类骗局往往会设置层层掩护，有的甚至是空壳公司，即便消委会出面调解，也很难找到实际经营者。”彭欧说。

构建多方共治的防“坑”屏障

面对“AI+”培训乱象频发的趋势，业内人士呼吁，亟待从“源头管控+精准维权+行业引导”三维发力，通过深化消费者教育、强化多部门联动监管、督促平台履行主体责任，多措并举推动新兴消费领域规范健康发展。

监管部门需向前一步，建立联动处置机制。四川内江这起案件经当地政法委统筹，协调公安、网信等部门联合处置，为小张拿回了2421元退款，并批量化解百余起投诉，累计挽回损失40余万元。四川省消委会相关负责人建议，开展“AI+”培训商家专项排查整治，对违规经营、投诉集中的商家依法曝光，严厉查处虚假宣传、设置霸王条款等违法行为，对涉嫌合同诈骗、卷款跑路等行为依法移交公安部门立案侦查。同时，全面推行“AI+”培训服务合同标准化，明确双方权利义务，杜绝不合理限制条款。相关部门也应建立联动机制，动态筛查线上培训广告，重点整治“保收益”“速成”等虚假宣传。

平台方则必须扛起主体责任，不能当“甩手掌柜”。当前，培训机构正是利用平台广告引流，再转入私域社群运营，客观上形成了监管缝隙。张义文建议：“短视频、直播等平台需严格核查入驻机构的营业执照、办学资质，对‘月入过万’‘轻松赚钱’等涉嫌虚假宣传的内容建立前置审核机制，及时清理违规话术。”此外，还要抓实源头管控，推动完善行业监管标准，明确准入、服务及收费规范。

消费者自身也需提升“免疫力”，理性看待“暴富神话”。多位专家呼吁，年轻消费者在购买“AI+”培训课程时，要理性看待宣传案例与收益承诺，切勿轻信“学员高收益案例”，谨慎对待抽奖等促销手段。更重要的是，要保存好聊天记录、页面截图、交易凭证等相关证据。

（据《新华每日电讯》记者/董小红）

“词元”这么火，该注意点啥？

近期，国家数据局正式定名的AI领域核心术语——词元（Token）成为网络热词。据统计，截至今年3月，我国日均词元调用量已超过140万亿，较2024年初增长1000多倍。“词元”这个新词实际上早已融入我们生活的方方面面。面对新技术新应用，我们既要主动拥抱、善加运用，又要防范风险、确保安全。

什么是词元（Token）？

简单来说，词元是AI大模型处理信息的最小单元，兼具可计量、可定价、可交易三大特征。它不仅是智能时代的价值锚点，更是连接技术供给与商业需求的“结算单位”。词元应用场景远超AI领域，与日常生活紧密相关。

——身份凭证类，相当于数字世界的“临时身份证”，用于便捷登录各类平台、完成转账授权等，如微信登录第三方小程序、手机银行动态口令等，有明确有效期，兼顾便捷性与安全性。

——AI场景类，即官方定名的“词元”核心应用，是使用如AI写作、修图、剪辑等AI服务的消耗性资源。

——权益凭证类，可以理解成区块链场景下的“通证”，相当于数字化权益证明，如电子票、游戏皮肤、会员积分等，具有不易伪造、便于流转的特点。

词元（Token）热潮下的信息安全隐患

随着词元的爆火，一些不法分子开始打起了词元的主意，伺机布设各种陷阱。同时，词元本身在使用过程中也存在一定的安全风险，需要我们加以防范。

——泄露劫持风险。不法分子可通过跨站脚本攻击（XSS）、公共Wi-Fi嗅探等方式，窃取、截获未加密的词元。一旦词元泄露，攻击者可直接盗用用户身份，获取隐私信息、登录账号、篡改数据，甚至实施诈骗、转账等操作，直接威胁个人财产安全。如果海量词元被汇总分析，则可能引发系统性风险，危害数据安全与国家安全。

——伪造篡改风险。若词元缺乏加密或签名防护，不法分子可直接修改词元的权限字段，伪造管理员身份绕过系统验证，非法获取用户敏感隐私数据、实施越权操作。同时，不法分子还有可能制造“虚假词元”，诱导用户泄露身份证号、手机号等隐私信息。

——诈骗陷阱风险。当前，各类“词元骗局”层出不穷：用低价AI词元套餐、词元投资等噱头，诱骗用户资金；冒充官方平台，以官方升级、验证为由，骗取个人隐私信息。尤其是宣称“囤词元能暴富”“场外交易赚差价”等行为，不仅涉嫌非法金融活动，还可能被境外间谍情报机关用以开展数据窃取、资金渗透，危害国家经济安全与数据安全。

词元（Token）这么火，应该注意点啥？

面对词元热潮，我们既要理性看待其价值，又要注意信息安全、隐私安全，提高安全防范意识，做到了解词元、善用词元。

——认清词元属性。词元可作为数字身份凭证，并非投资品，防范以“词元投资”“高收益回报”“词元理财”“词元挖矿”等为噱头的各类骗局，切勿盲目购买未经官方认证的小众、虚拟词元，不随意注册来路不明的词元服务，从源头上避免因贪利、跟风导致的个人隐私信息泄露和财产损失。

——强化使用规范。使用词元相关服务时，优先选择正规平台与加密传输通道，不在公共网络、不安全环境下进行登录、转账、填写隐私信息等敏感操作；不点击陌生链接，不下载非官方App，不扫描可疑二维码，及时更新设备系统与安全软件；严格保管词元口令、授权码及绑定的手机号、身份证号等信息，开启双因素认证，不共用账号，不设置通用密码，发现账号异常立即采取改密、解绑、报备等止损措施。

——遵守法律法规。面对词元等AI领域的新兴应用与概念，应保持理性认知，既不盲目追捧，也不跟风炒作，自觉遵守法律法规与监管要求，主动学习官方发布的词元安全知识与风险提示，提高辨别能力；科学区分身份凭证类、AI场景词元与区块链通证、加密货币，不参与非法加密货币交易，如遭遇诈骗、信息泄露或发现非法活动，应及时向有关部门反映。

（据国家安全部微信公众号）