大数据时代高职学生网络安全素养提升的策略研究

王芳
（沙洲职业工学院　江苏张家港　215600）

摘要：通过调研发现，高职学生存在安全防护技能薄弱、网络伦理规则感不强、不同生源学生网络安全教育差异明显等问题。要提升高职学生网络安全素养，我们需要构建三位一体支撑体系，优化社会环境；打造三维融合育人体系，强化校园教育；加强素养的内生性发展，实现自我教育。

关键词：高职学生；网络安全素养

大数据时代的全面纵深发展重塑了网络空间的安全生态。随着 5G、物联网、人工智能等技术的广泛应用，网络安全威胁呈现智能化、隐蔽化、精准化的新特征，AI 换脸诈骗、自动化钓鱼攻击、数据挖掘隐私泄露等新型风险持续涌现。高职学生作为我国数字经济发展的技能型主力军，其网络安全素养直接关系到产业数字化转型的安全根基。面对国家《网络安全法》《数据安全法》的战略要求与“网络强国”建设目标，传统碎片化的素养培育模式已难以应对大数据时代的多维挑战。因此，构建契合高职教育特色、融合技术赋能与社会协同的系统化策略体系，成为当前职业教育数字化转型的紧迫命题。

1 高职学生网络安全素养现状分析

1.1 有一定的防范意识，但应对能力欠缺

通过调查，我们发现高职学生普遍存在着“知易行难””的困境。有 96.5%的学生认为，“设置安全的网络密码很有必要”，但只有 38.9%的学生会真正使用复杂密码设置。在人才培养方案中，有 78%的院校没有设置独立的网络安全必修课程；实训平台的教学覆盖率不足 40%；关于“网络安全”教育，大部分高校以说教为主，缺少攻防演练、应急响应等情境化的训练。

1.2 有一定的技术能力，但伦理规则感不强

与艺术、文科类学生相比，理工科学生“技术能力与伦理责任的失衡性”现象较为突出。在计算机相关专业学生中，具备独立编写与开发爬虫程序能力的学生占比达 46.2%，仅 31.8%的学生会主动考量隐私保护以及遵守相关法律法规的重要性。代码抄袭现象也较为普遍，主动参与和被动参与的比例高达 58.6%。

1.3 不同生源学生面临的的网络安全教育困境存在差异

在农村地区，存在“数字资源与防护需求之间的不平衡”。个人信息泄露的比例高达 63.7%，显著高于城镇生源学生的 39.2%；在获取网络安全教育资源方面农村生源学生显得相当不足，特别是参与网络安全竞赛的学生比例非常低。城镇学生面临“信息过载与辨识能力不足”的问题。因接触网络信息的渠道多样，在面对海量信息时，易受网络谣言或虚假广告影响，辨识真伪的能力相对较弱。

2 高职学生网络安全素养失衡的深层成因剖析

2.1 教学内容滞后于技术演进

当前的教育内容和理念在很多方面都显示出滞后于技术演进的迹象。教材更新周期平均为 3.2 年，这个时间跨度远远落后于网络威胁的迭代速度。教学内容主要集中在传统的网络安全知识，对于新兴的网络安全问题，覆盖程度明显不足。师资队伍中，具备实际企业实战经验的“双师型”教师所占比例仅为 28%，这导致了教学内容与行业实际需求之间存在脱节。

2.2 数据环境加剧风险复杂性

我们在享受人工智能带来的各项便利之余，随之而来的是一系列新型的网络安全威胁。①精准诈骗。利用大数据分析技术，犯罪分子能够构建详细的用户画像，从而实施更为精准的刷单骗局。②隐私挖掘。在日常手机 APP、小程序存在过度采集学生的生物信息。③信息茧房。算法推送机制使得用户更容易接触到与其兴趣相符的信息。

2.3 个体认知的局限和法律意识淡薄

从小学到高中，法律条纹与法律意识的教育相对较少。在理工科领域，学生对于技术的突破和创新的热情

极易忽略伦理和法律的边界。在文学艺术领域，由于数字艺术作品易于被复制，经常面临盗用和被非法盗用的风险。此外，低年级学生由于认知受限，极易陷入那些以“创业精英”、“成功校友”形象出现的诈骗行为。

3 高职学生网络安全素养提升策略

3.1 构建三位一体支撑体系，优化社会环境

政府部门出台精确的网络安全相关政策法规，实行全面的网络监管机制，加强网络安全环境治理。在政策法规层面，政府等相关部门应加速《数据安全法》和《网络安全法》在职业教育领域实施细则的制定，明确数据采集的“最小必要”原则和“知情同意”的底线要求。可考虑由网信部门牵头，建立针对高职学生的专项保护机制，强制网络平台对高职生账号实施“高风险操作熔断”以及推广“隐私风险可视化”功能；网信办应与教育部联合建立应用商店安全评级制度，对校园常用 APP 进行安全审计，并强制下架未通过等保 2.0 认证的教育类应用，从源头减少数据泄露的风险。在监管层面，需要建立跨部门跨行业的协同机制。公安机关应定期向高校通报新型诈骗案例的特征，金融监管部门应严格控制校园贷数据的滥用，文化部门应建立游戏厂商与渠道方的联合问责制，对诱导高职生超额充值的行为实施“双罚制”。

政校企协同构建一个由平台自律与技术创新共同驱动的防护体系以应对日益复杂的网络威胁。一是要加强智能化防护工具的普及。政府要鼓励网络安全企业开发针对高职院校的定制化产品。例如，360 公司推出的“校园安全卫士”集成了 Wi-Fi 安全检测、诈骗链接实时拦截以及隐私权限一键优化功能。二是将数据安全技术的嵌入实际应用。可在校园系统中强制实施区块链存证技术（以防止成绩和证书的篡改）、动态数据脱敏技术（如在学籍查询中仅展示身份证号的后四位数字）、以及联邦学习技术（在训练人工智能模型时无需导出原始数据）等关键数据安全技术减少学生关键信息和的泄露和恶意使用。三是优化网络信息内容过滤机制。通过人工智能技术识别并屏蔽诸如“躺平攻略”、“刷单秘籍”等不良信息，同时提升“数字工匠榜样”、“安全技能微课”等积极健康内容的推荐权重。在条件允许的情况下在短视频平台为高职学生构建专属的内容池。

校政社家携手共创优质网络内容，净化网络生态与文化环境。一是加快网络平台优质内容供给侧改革，鼓励创作符合高职生认知特点的安全教育产品，如共青团北京市委《反诈 RAP》短视频。二是强化平台责任，要求网络平台对内容创作者进行资质审核，确保安全教育内容的准确性和专业性。三是建立网络内容分级制度，针对不同年龄段和认知水平的高职学生提供适宜的安全教育资源。四是加大对违法和不良信息的打击力度，建立快速响应机制，对发布和传播有害信息的账号进行封禁处理，维护清朗的网络空间。社会各界也应积极参与到网络生态的净化中来，通过举办网络安全知识竞赛、讲座、展览等活动，提高高职学生的网络安全意识和防范能力。同时，家庭、学校要加强对学生的网络行为监督，引导学生树立正确的网络安全观念，共同营造一个健康、安全的网络环境。

3.2 打造三维融合育人体系，强化校园教育

课程体系与教学模式创新。针对高职生技能实操需求强、理论耐受力较低的特点，构建“普及—融合—实战”课程框架。在课程体系构建上，根据不同上课群体选择不同课程内容。面向全体学生的，可考虑通识课程，以知识普及为要，开设诸如《大数据安全通识》、《网络安全法》等，将“安全+法治”相融合，嵌入真实案例。对于不同专业类学生，可考虑不同的网络安全加强课程。如工科专业开设“工业互联网安全”，文科增设“信息辨伪与舆情分析”，艺术类强化“数字版权管理”。对于计算机学习能力突出者，可开设《CTF 攻防演练》、《企业红蓝对抗》等实战课程，将 OWASP Top 10 漏洞清单转化为实训任务。另外，在教学模式上，也可进行“三维场景迁移”。在虚拟战场，部署仿真平台，模拟钓鱼攻击、勒索病毒等多个场景，学生通过 VR 设备完成“数据泄露溯源”任务；在真实对抗中，参与企业渗透测试项目，提升应对实效；在社会服务中，通过校政社联动协助“净网行动”，共建社区“网络安全防护墙”。

加强和丰富师资队伍与资源建设。为解决师资困境，可采取企业互聘、联合开发教学资源、借助智能教辅工具等措施来应对。学校可通过线上聘请行业协会专家担任技术支持，线下聘用周边城市或区域企业引进技术骨干担任产业导师，同时要求专业教师每学年赴企业实践 2 个月，实地参与“数据安全防护实战”等项目，多措并举拓展师资团队；建设“国产为体、开源为用”的资源

库，开发“安全+”系列数字化教材，建设虚拟仿真实训室，开发网络安全实训项目，覆盖工业控制系统安全等前沿场景；嵌入 GPT 安全助手解答学生疑问，如开发“风险行为诊断器”自动分析学生网络操作视频并生成防护建议。

构建可量化可追踪的素养评价体系和激励创新机制。可在高职学生群体中进行“网络安全素养”雷达图动态评估。通过信息保护、法规遵守、风险识别、工具应用、隐私管理、责任担当六个维度构建个人素养画像，数据来源包括课堂测试（占 30%）、行为日志（占 20%）、竞赛成果（占 30%）、企业认证（占 20%）；结合大学生第二成绩单，可考虑设立“安全素养银行”，一方面，将防护行为转化为“安全币”，例如正确处置钓鱼邮件积 3 分，参加反诈宣传积 5 分，参加实习或竞赛积 20 分；另一方面，设立负面清单约束：对参与网络赌博、传播谣言等行为实施“评优一票否决”，并在素养雷达图中标红预警。

3.3 加强素养内生性发展，实现自我教育

创设活动，重构认知。针对普遍存在的“知易行难”现象，我们可以从提升风险感知能力—纠正认知偏差—培养法律敬畏感入手。通过实施“隐私泄露沙盘推演”活动，让学生亲身体验数据泄露的连锁反应，深刻理解从“单点泄露”到“群体危机”再到“国家安全”的传导机制。针对理工科学生普遍存在的“技术至上主义”倾向，组织“黑客伦理辩论赛”，深入剖析“技术中立性”的误解。邀请网警对“帮信罪”校园案例进行解析，并组织学生走进真实法庭旁听“网络安全类”案件审判，有效提升学生的法律认知水平，筑牢法治屏障。

行为管理，习惯养成。从学校管理层面，可基于用户画像技术实现个性化行为干预一是可通过记录高危操作及防护行为（如 VPN 使用、权限关闭）等，进行标签生成，分别标注“低意识—高诈骗风险”“高技能—低伦理”等群体特征。二是向不同专业类型学生进行精准干预。可向艺术类学生推送版权法动画，为农村生源定制“防刷单情景剧”，为文科类学生推送防诈小技巧等。从个人层面，可推行“网络安全自律契约”。一方面学生可自行安装“数字戒尺”APP 管理上网时长，自动屏蔽涉赌网站；另一方面，可通过签订《无诈寝室公约》，实行“1 安全员监督 6 人”机制，加强网络安全防范与共管。在班级层面，也可开展“21 天安全打卡”，对关闭 APP 权限、核实可疑信息等行为积分排行等活动，最大限度提升学生安全防护意识。

能力转化，实践参与。促进知识技能向防护能力与社会责任的转化。学校可构建“学生安全卫士”团队，从网络安全原创作品、校园安全防护、家庭安全防护等多方着手，发挥学生网络安全技术能力服务、辐射身边人、周边社区。学校可组建社会服务实践团队，走进老年群体，参与“银发数字安全助老计划”，为社区老年人安装反诈 APP 并讲解安全知识；走进中小学，开展网络安全知识和技能普及，这样既增强了技能又培养了责任感；另外，学校可鼓励学生将安全方案转化为创业项目，例如深圳职业技术学院学生开发的“校园 Wi-Fi 安全哨兵”系统已在 30 所院校部署。

大数据时代高职学生网络安全素养提升是关乎国家网络安全战略的系统工程，需通过社会环境筑底线、高校教育强主干、自我教育生枝叶的三维联动，共同助力兼具技术硬实力与伦理软素质的数字工匠培养，为网络强国建设注入可持续的青年力量。

参考文献：

[1]吴迪.高职院校学生网络素养教育提升路径研究[J].辽宁师专学报.2023(2);95-96.

[2]王芳.信息化条件下高职辅导员校园危机应对方式现状调查[J].统计与管理.2017(11);36-37.

作者简介:作者简介:王芳,(1979—),女,江苏张家港,汉,硕士,副教授,研究方向为学生教育管理;

基金项目:2023 年江苏省高等教育学会辅导员工作研究会专项课题:大数据时代高职学生网络安全素养提升路径探析 项目编号: 23FYHLX056

2025 年江苏省高校哲学社会科学研究一般项目(思政专项):人工智能赋能高职学生网络安全教育的“三全育人”体系构建研究 项目编号:2025SJSZ0716