 DOI: https://doi.org/10.12345/iptm.v3i1.15713

The Causes, Characteristics, and Prevention Mechanisms of Online Fraud in Universities under the Background of Big Data Applications

Weimeng Li

Dalian University of Foreign Languages, Dalian, Liaoning, 116000, China

Abstract

With the rapid development of Internet technology, the application of big data has penetrated into various fields. Its powerful attributes as a tool provide support for preventing and combating online fraud. In recent years, the clutches of fraudsters have frequently reached out to university campuses, turning campuses into hotspots and high-incidence areas for online fraud, seriously infringing upon the financial and even personal security of students. Through reviewing relevant literature and analyzing the cases of fraud in university settings, this paper believes that the causes of internet scams among college students mainly include the following aspects: students' lax protection and chaotic management of personal information, lack of social experience and weak awareness of prevention, and a lack of proper guidance in values, leading to irrational consumption. In terms of fraud forms, online scams exhibit characteristics such as being frequent, diverse in methods, covert in criminal behavior, and highly technological in fraudulent means. In terms of fraudulent methods, the main scenarios include enticing with high-paying opportunities, deposit fraud, false training fraud, online shopping and refund fraud, impersonation fraud, fraudulent claims for student assistance or scholarships, and online loan fraud, among others. Based on the above content, this study proposes preventive measures for addressing online fraud issues in universities: schools should increase the publicity and guidance on online fraud, and establish a grid-based regulatory mechanism; students should establish correct values and consumer perspectives, and enhance personal security awareness; law enforcement agencies should innovate investigation models and improve big data anti-fraud platforms.

Keywords

big data; internet fraud; colleges and universities

大数据应用背景下高校网络诈骗的成因、特征及防范机制

李唯萌

大连外国语大学，中国·辽宁 大连 116000

摘　要

随着互联网技术的飞速发展，大数据的应用已经深入到各个领域。其强大的工具属性为预防和打击网络诈骗提供了支撑。近年来，诈骗分子的魔爪频频伸向高校校园学生，使校园成为网络诈骗的多发地和高发地，严重侵害了高校在校学生的财产安全甚至是生命安全。通过对相关文献的查阅，论文梳理和分析高校校园诈骗案件案情，认为大学生网络受骗的成因主要有以下方面：学生个人信息疏于保护、管理混乱；社会经验匮乏、防范意识薄弱；缺乏正确的价值观引导，非理性消费。从诈骗形式上看，网络诈骗呈现出密集、手法多样、犯罪行为隐蔽、诈骗手段高科技化等特有属性。从诈骗手段上看，诈骗情形主要有：高薪诱惑诈骗、收取押金诈骗、虚假培训诈骗，网络购物及退款诈骗，网络冒充诈骗、申领助学金、奖学金诈骗、网络贷款诈骗等。基于上述内容，本研究提出高校网络诈骗问题的防范对策：学校要增大网络诈骗宣传力度与引导、重点建立网格化监管机制；大学生要树立正确的价值观和消费观、增强学生个人安全意识；公安机关要创新侦查模式、完善大数据防诈平台。

关键词

大数据；网络诈骗；高校

1 引言

在互联网时代，网络已影响人们生活的方方面面。随着大数据技术与物联网技术的发展，网络上的诈骗形式更加多样，犯罪手法更加隐蔽，他们通过网络技术获取受骗人的信息，以达到精准欺诈的目的。大学生作为尚未进入社会的青年群体，缺乏足够的社会经验和理性思考且长期处于较为单纯的生活环境中，是网络诈骗的易感人群。根据《电信网络诈骗治理研究报告（2021）》所统计的被害群体年龄分布，20~29 岁占比 41%,20 岁以下占比 18%，这正是大学生群体所在年龄层。因此，有必要对大数据应用背景下校园网络诈

【作者简介】李唯萌（2004–），女，中国辽宁沈阳人，在读本科生，从事大数据分析研究。

骗的手段与机制进行梳理，为建立更为完善的校园网络诈骗防范机制提供借鉴。

2 概念界定与文献回顾

大数据起源于互联网技术（Internet Technology，IT）行业，从一般意义上讲，大数据是指无法在有限时间内用常规软件工具对其进行获取、存储、管理和处理的数据集合，但目前还没有一个统一的定义。它具有容量庞大、结构复杂、处理速度快及使用价值高等特征，呈现出数据资源化、实时处理、多样化数据融合分析、与新技术深度结合等发展趋势（陈静等，2022）[1]。大数据的发展对网络信息安全既是机遇，也是挑战。一方面，大数据技术的深入应用，使得各类网络攻击手段的不断升级，网络信息安全问题日益严重。另一方面，大数据应用也能为信息安全提供保障。相较于传统安全技术，大数据技术不仅能更好地应对网络攻击，还能更加精准、快速地识别和处理安全事件，有效保障网络信息安全。

网络诈骗是指以非法占有为目的，借助于网络信息系统采取虚构事实或者隐瞒真相的欺骗方法，骗取数额较大的公私财物的行为，其花样繁多、行骗手法日新月异，常用手段有假冒亲友、网络购物退款等。伴随着互联网的发展，传统诈骗在大数据技术加持下衍生出精准诈骗的特点，基于个人信息数据挖掘的电信网络诈骗案件日益攀升。从特征上看，曲晓艳等[2]（2033）认为大数据时代的网络诈骗具有诈骗手段高科技性、诈骗方式多样性、诈骗行为隐蔽性及诈骗犯罪团伙化、产业化、链条化的特点。但从目前来看，有研究者认为高校网络诈骗的宣传教育存在宣教主体协同效应薄弱、宣教载体窄化、宣教内容针对性不强、传播与价值导向效果甚微等问题（杨剑光、陈思，2023）[3]。因此，有必要对大数据时代高校网络诈骗的特征、机制及对策进行梳理研究，提高全社会对高校网络诈骗的防范意识。

3 网络受骗成因

3.1 个人信息疏于保护、管理混乱

在当今信息化的高强度发展和互联网在人们生活中的不断扩展，对于大学生来说，一方面他们与社交网络、线上购物、网游等网络活动更加紧密，个人会在网络上进行信息分享。例如，在网络社交上发布与自己和家人相关的信息，这些信息会被不法组织进行利用，造成损失。另一方面，在进行网络活动时，大学生对外部信息会放松警惕，掉进骗局。当下信息的传播和获取更加快速便捷，大学生往往处于信息极不对称的劣势地位，有些社交平台都是实名制登录，需要提供自身相关证明等基本信息，学生在无意间就把个人信息泄露了，网络诈骗分子会通过利用这些个人相关信息进行精准诈骗，提高诈骗的成功率。

3.2 社会经验匮乏、防范意识薄弱

大学生由于社会经验匮乏，对网络诈骗没有充足的重视，对网络诈骗的手段、方式方法不了解，遇到诈骗的时候会轻易相信，受骗后也不自知，从而导致了严重的后果。网络相关软件都有个人信息的设置和登录，具有很强的隐私性，一旦上当受骗，很难被人发现。有的大学生在被骗后会选择自认倒霉；有的则会盲目自信，认为通过自己的学识能判断事物真假，从而滑向不可挽回的深渊；有的在思想冲动下会犯一些常识性错误，让诈骗分子钻了空子而不自知。

3.3 缺乏正确的价值观引导，非理性消费

当今大学生大多自我意识较强，有的大学生进入大学后，更是冲动消费、不理性消费，在生活费无法负担其消费水平下，走上非法网贷、分期付款的道路。无法偿还贷款的同学会遭受来自家庭、校园或社会的压力，更甚者会影响其自身或他人的生命危险，其主要原因是缺乏正确的价值观与消费观引导。

4 大数据应用背景下校园网络诈骗的特点

4.1 网络诈骗行为密集覆盖

大学生的生活离不开网络活动，大学生由于防范意识薄弱，会轻易在网络上留下个人信息，犯罪分子会通过相关信息，假冒身份、设置骗局来进行诈骗。同时大学校园人群的密集性间接降低了诈骗成本，使得网络诈骗愈发蔓延不绝。

4.2 网络诈骗手法多样性

当今大数据技术充斥在人们生活中的方方面面，诈骗分子在诈骗方式上运用新技术、新手段。利用网络钓鱼转移钱财、盗号转账、扫描二维码和输入验证码、虚假购物诈骗、网络游戏虚假交易诈骗层出不穷，新型诈骗手段迷惑性强，更容易造成财产损失，让大学生防不胜防。

4.3 诈骗行为隐蔽性

在互联网上进行的网络诈骗，一般没有地域边界的限制，没有实质性的接触，诈骗嫌疑人与大学生之间也由于互联网造成的“屏障”而看不到彼此，诈骗分子通过隐藏网络IP、修改电话号码、改变语音特征及上传虚假视频或照片等技术手段掩盖犯罪事实，增加了犯罪行为的隐蔽性，这就使得大学生在被网络诈骗后，无法通过其他途径掌握犯罪嫌疑人的身份信息和其居住地，公安机关对于诈骗犯罪的侦查和取证难度大大增加。

4.4 诈骗手段高科技化

网络诈骗分子通过新的网络技术手段，比如网络信息技术、短信群发技术、电话改号技术、木马技术等进行电信网络诈骗，抑或散布和传播木马病毒程序进行电信网络诈骗，这种技术对大学生来说有很强的诱导性和欺骗性。

4.5 诈骗组织团伙化、产业化、链条化

目前电信网络诈骗犯罪团伙化、产业化、链条化的特点突出。诈骗团伙分工日益精细，从设计场景、建设圈套、收集信息到通过虚拟式操作，分工合作，犯罪分子形成了完整利益链条的团伙化、产业化、链条化模式。因此，大学生

几乎无法分辨，一旦落入诈骗分子设计的圈套很难逃离。

5 大数据应用背景下校园网络诈骗的常见类型

5.1 高薪诱惑、收取押金、虚假培训诈骗

诈骗分子利用大学生善良以及涉世不深的特点发布虚假招聘信息，以高薪为诱饵吸引受害者，骗取学生钱财，或者要求大学生交纳一定数额的押金，承诺完成任务后返还来行骗；又或以提供培训资料、兼职刷单为借口，骗取大学生的相关信息甚至财务。这样的诈骗手段不仅使大学生们遭到了经济的损失也给他们带来了精神的打击。

5.2 网络购物及退款诈骗

随着网上购物的急速发展，大学生大多选择网络购物。诈骗分子以多种方式对大学生诈骗。例如，以消费退货诱导大学生输入个人信息或进行交易，从而盗取资金或个人信息；抑或以货到付款为骗局，以各种理由要求先付款后验货，一旦付款后便消失不见。这些都给受害的大学生带来了极大的负面负担。

5.3 网络冒充亲友、公检法等相关人员诈骗

高校网络诈骗的常见类型还有网络冒充诈骗，诈骗分子进行假冒大学生的亲人、朋友或者公检法等机关工作人员，编造一些如交通肇事、生病住院等紧急情况，大学生由于慌张便匆匆汇款。这种骗局虽然俗套但成功率很高。

5.4 申领助学金、奖学金等诈骗

诈骗分子通过非法渠道获得受害大学生的个人信息，宣称为其发放奖学金、助学金，使之放松警惕，骗取其信任，诱导他们网上转账，进而要求其通过先垫付一笔费用来实施诈骗。

5.5 网络贷款诈骗

诈骗分子通过虚假网站或社交媒体平台，向大学生提供虚假贷款服务，要求大学生提供个人信息或抵押物品，然后以各种理由拒绝提供贷款或骗取大学生的钱财。

5.6 钓鱼网站诈骗

诈骗分子通过建立与正规网站相似的虚假网站，骗取大学生的个人信息或钱财。他们一般通过要求大学生输入个人信息或银行账号等敏感信息进行欺诈或盗窃。

6 大数据应用背景下校园网络诈骗的防范机制

6.1 学校：加大电信网络诈骗防范宣传力度，建立网格化监管机制

学校要通过宣传教育，增强师生的网络安全意识，增强师生的防范能力。例如，相关部门进行宣讲，分析诈骗网站；也可以印发宣传手册，描述真实案例；必要情况下可以请受骗人员进行现身说法。除此以外，学校可以组织相关活动，如班会、演讲会等活动，让同学们通过多种方式了解网络诈骗的手段，增强学生风险防范意识。

与此同时，学校或班集体要掌握大学生的学习及生活动态，可以通过师生谈话、同学汇报的形式及时发现苗头性、倾向性的问题，尤其是对于与学生自身经济不符的消费迹象，比如更换名牌手机、名牌电脑等异常消费，要建立网络诈骗的监测和处理机制。学校可以通过对学生的家庭和生活情况的了解，发放奖学金和助学金，来帮助贫困生，给予他们更多的关注，以防他们因为生活困难而被网络骗局所骗。

6.2 学生：树立正确的价值观和消费观，增强个人安全意识

当今的大学生年轻活力、精力充沛，对事物有着强烈的好奇心和尝试欲。大学生如不树立正确的价值观和消费观，很容易为了攀比或虚荣心而追求物质享受，从而产生超前消费、攀比消费、盲目消费，给网络诈骗带来了可乘之机。因此，大学生自身也应主动树立科学的价值观和消费观，根据个人经济能力合理消费，抵制急功近利心理，通过合理合法渠道实现个人诉求。

与此同时，学生还要增强自我安全防范意识。在互联网上，当需要填写个人信息时，一定要保证网站的安全性。若涉及个人银行账户、密码、身份证等信息，需要与相关人员进行核实后再填写，避免使用不正规网站的链接。很多诈骗分子会冒充行政机关人员给大学生打电话进行恐吓、威胁，这时需要保持冷静，沉着思考与他们进行对话，找到其中的漏洞准确做出抉择。

6.3 公安机关：创新侦查模式，完善反诈大数据平台

大数据时代，公安机关要借助大数据、云计算等技术，为了形成真正的维护校园网络安全的合力，应设立预防大学生网络诈骗的联动系统。学生在向学校相关部门报案后，学生应配合学校将受骗信息反馈于公安部门，针对处于预备阶段、进行阶段、发生后的网络诈骗行为，建构以数据为主导的事前预警、事中阻断、事后溯源的全新侦查模式。

与此同时，相关部门还可以完善反诈数据统一资源库并建立反诈大数据平台，通过平台功能加强线索发现、IP 锁定、追踪溯源的能力，为用户提供更加安全的交易环境。

7 结语

综上所述，大数据技术在预防和打击校园网络诈骗中具有巨大的应用价值。通过大数据分析，可以为学生提供更加安全的网络环境，为学校提供有力的数据支持，更加精准地识别诈骗行为，辅助学校制定更加科学的防诈策略。在未来的网络活动中，我们应进一步深入研究大数据技术在校园网络安全领域中的应用，推动校园防诈工作朝着更科学规范的趋势发展。

参考文献

[1] 陈静.大数据综合应用实践[D].北京:清华大学出版社,2022.

[2] 曲晓艳,杜森,孙玉昊.大数据环境下打击电信网络诈骗犯罪研究[J].辽宁警察学院学报,2023,25(1):39-43.

[3] 杨剑光,陈思.大数据时代高校防范电信网络诈骗宣传教育的问题与对策研究[J].昆明理工大学学报(社会科学版),2023,23(3):136-142.