

高校学生网络安全能力现状调查与对策研究

阙凤仪

武汉工程大学, 湖北 武汉
Email: 1078079327@qq.com

收稿日期: 2021年7月30日; 录用日期: 2021年8月25日; 发布日期: 2021年8月31日

摘要

随着信息技术的迅猛发展和广泛应用, 互联网逐渐渗透到各行各业的应用创新之中, 而中国高校学生已成为使用网络的重要群体, 其网络安全能力不仅影响着素养及价值观的形成, 也影响国家信息化发展目标的顺利进行。本研究基于武汉某高校的493份抽样调查数据, 选择网络安全法律法规、网络攻击与防御、个人信息保护、网络诈骗、网络道德五个关键指标调查高校学生网络安全能力情况, 采用KNN分类算法将高校学生网络安全能力进行分类, 并提出相关对策建议。

关键词

高校学生, 网络安全能力, KNN分类算法, 现状, 培养对策

Investigation and Countermeasure Research on College Students' Network Security Capability in Current Situation

Fengyi Que

Wuhan Institute of Technology, Wuhan Hubei
Email: 1078079327@qq.com

Received: Jul. 30th, 2021; accepted: Aug. 25th, 2021; published: Aug. 31st, 2021

Abstract

With the rapid development and wide application of information technology, the Internet has gradually penetrated into the application and innovation of all walks of life, and Chinese college students have become an important group of network users. Their network security ability not only affects the formation of literacy and values, but also affects the smooth progress of national

information development goals. Based on 493 sampling survey data of a university in Wuhan, this research selects five key indicators of network security laws and regulations, network attack and defense, personal information protection, network fraud, and network ethics to investigate the cyber security capabilities of college students. KNN classification algorithm is used to classify college students' network security capability, and we put forward some relevant countermeasures and suggestions.

Keywords

College Students, Network Security Capability, KNN Classification Algorithm, Present Situation, Training Countermeasures

Copyright © 2021 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

习近平总书记在 2019 年 9 月 16 日的国家网络安全宣传周上明确强调,“国家网络安全工作要坚持网络安全为人民、网络安全靠人民,保障个人信息安全,维护公民在网络空间的合法权益”,这是党中央在精准把握网络发展趋势后,对网络安全工作提出的根本宗旨和更高要求,也充分体现了党中央高度重视网络宣传工作。互联网信息科技的不断发展与更新,在给人们的日常生产工作、生活以及学习方式带来极大便利的同时,也制造了无数的社会风险,例如人类社会的经济、隐私以及信息安全都受到了不同程度上的威胁,安全漏洞与病毒数量仍然偏高,各式各样的虚假信息、钓鱼链接接踵而来,语音识别技术和自然语言处理技术的发展也对人们的意识形态产生了一定的影响。

2021 年第 47 次中国互联网发展状况统计显示,截至 2020 年 12 月,中国网民数量从 2008 年的 2.98 亿人增长到 9.89 亿人,互联网普及率达到 70.4%,受过大学专科、大学本科及以上教育的网民群体占比为 19.8% [1]。可见,高校学生是使用网络的重要群体,并且高校学生作为推动国家经济发展、改善社会治理的生力军,其网络安全能力的强弱将直接影响国家信息化发展目标的顺利进行。目前,高校学生社会经验不足,还处于人生观、价值观的成长期,在复杂的网络环境中,信息传播方式多种多样,其交互性极高,高校学生易受网上虚假信息和过激言论的煽动,难以明辨是非、理性分析,对高校学生的思想造成冲击,甚至使他们遭受不良文化的渗透,从而发生一系列如重大信息泄露、网络诈骗抢劫、校园网贷、网络恋爱等网络安全事件,这严重威胁着高校学生的成长与安全,影响到国家信息化发展战略的有效实施。高校学生频繁接触网络,网络安全问题日渐突出,党和国家也表示了对网络安全的高度重视和关注,各国对网络安全教育的重视程度也逐渐提高。因此,调查高校学生网络安全能力,重视高校学生网络安全问题研究,提出合理有效的解决办法,既是帮助高校学生树立科学网络安全观的迫切需要,也是促进国家信息化发展目标顺利实现的必然要求。

2. 研究背景

网络安全是网络系统中的各种应用软件、网络硬件以及数据不会被各种外在意外或是恶意的原因所干扰,使其遭受破坏、篡改和泄露,关键是能使它们受到有效保护,保障网络系统能安全、稳定、可靠地运行并提供连续服务[2]。高校学生网络安全的主体是高校学生,网络安全是高校学生在利用网络这一

工具的过程中,用户的一切权益都受到保护不被威胁和侵害,其中不仅仅局限于网络的物理安全和技术安全两方面,还包含高校学生信息安全和意识形态安全问题[3]。

对于网络安全风险,部分学者从计算机网络安全系统自身和系统外部所面临的风险来谈,认为网络安全主要存在系统漏洞、移动存储介质携带病毒、黑客攻击、计算机病毒的攻击以及间谍软件的攻击方面的问题[4]。也有学者从管理者以及用户的角度提出网络安全的主要风险,认为由于数据时代网络空间中的信息传播速度快、受众广、内容丰富多彩,增大了国家对网络舆情工作的稳控难度,削弱了政府及有关部门对社会信息的把控力度[5]。而高校学生作为网络的主要使用群体,在它使得高校学生学习、沟通交流以及娱乐等方面都变得更便捷的同时,也使其面临着个人信息被泄露和滥用的风险,网络诈骗案件层出不穷,让高校学生防不胜防。当代高校学生的网络安全问题包括网络犯罪行为、网络失德行为、网络受害现象以及网络成瘾[6]。还有学者认为价值判断能力不强、在网上恶心转发虚假信息、发布不正当言论、沉溺于虚拟的社交网络、轻易进行网络交易、网络受害现象严重都是目前高校学生网络安全的现状[7]。国外学者 Royan W.提出防范网络安全风险的关键因素不是科技而是用户行为,如果用户倾向于使用较差的安全参数配置、不关注警告信息,甚至是做出有意违反信息安全政策的网络行为,那么设计的再极致的安全界面也变得形同虚设,用户的行为取决于用户的相关认知和判断[8]。

从现有研究来看,很多学者着重于对高校学生网络使用行为的研究。徐东华(2019)通过调查发现高校学生尚不了解安全证书有问题或已过期网站存在的风险,并且不能准确及时地辨识与抵御外界对用户信息的窃取,网络支付防护的必要技能也存在一定缺乏[9]。周建芳(2017)对高校学生网络信息安全行为与网络系统安全维护行为进行了调查,其中只有少数高校学生会在使用电脑过程中时常升级防护软件、安装安全补丁,很多高校学生不关注手机短信链接的可靠性,另外高校学生会给个人电脑和手机设置开机密码,但经常备份个人重要文件做到安全保管的比例较低[10]。

关于高校学生网络安全能力调查维度的研究,方兵(2017)从网络安全基本认知、自我网络安全意识、网络安全防护技能和网络安全教育情况四方面来展开高校学生网络安全能力现状调查,分析得出高校学生在理解相关网络安全知识方面还存在欠缺[11]。胡余波(2018)从网络认知与评价、网络批判意识、网络行为管理、网络自我发展、网络安全与道德五个方面来评价新时期高校学生网络素养,发现了高校学生在自主学习意识、独立批判意识、时间管理意识、自我发展意识和道德责任意识上的薄弱之处[12]。黄斌(2020)从网络基本技能、网络信息获取、网络信息交流、网络信息鉴别、网络信息安全、网络道德法律和网络行为管理等7个维度来调查高校学生网络安全现状[13]。徐春玲(2016)从四个维度:知——对网络安全知识的认识,行——大学生网络行为,能——大学生网络基本操作技能,意——大学生在网络空间的价值观来调查大学生的网络素养,发现大学生网络素养目前尚处于自发阶段,大学生整体的网络素养水平不高,依然存在许多问题,还需要通过教育来提升[14]。针对高校学生网络安全教育,大多数学者都聚焦于网络安全意识、网络安全知识和网络安全技能这三大内容。

校园内外网络媒介生态环境、教育和用户行为变化很快,高校学生网络安全问题不断升级,因此需要持续的最新研究来了解,并开发适当的策略来解决安全行为中的弱点。我们在前人研究的基础上,从网络安全法律法规、网络攻击与防御、个人信息保护、网络诈骗、网络道德五方面收集数据来分析高校学生网络安全能力情况,为更好地促进高校网络安全教育提供数据支持和政策建议。

3. 研究设计

3.1. 数据来源

本次调查以武汉某高校学生为研究对象,采用无记名问卷形式收集资料。共选择10个学院,每个学院各发放50份调查问卷,共发放500份,实际回收有效调查问卷493份,有效回收率为98.6%。

3.2. 问卷设计

本次采用的调查问卷包括网络安全法律法规、网络攻击与防御、个人信息保护、网络诈骗、网络道德五个关键指标，每个指标包含 10 道题目，共设计 50 道题，均为客观题。根据信度和效度的检验结果可知，本问卷达到了教育与心理测量学的要求。

3.3. 数据分析

首先确定问卷题目中各个选项的得分(0, 1, 2, 3)，每个指标满分为 30 分，问卷总计 150 分，再将五个指标的题目根据难易程度进行排序，本文主要选取五个部分中的部分题目进行分析。问卷回收之后，筛选出未认真作答(所有问题均选择同一选项)、未作答完所有题目(超过 5 题)等情况的问卷并将其剔除，然后对每份问卷的结果进行整理打分，其中 375 份问卷运用在分类模型设计之中，确定好分类模型之后，再将另外 118 份问卷的分数分别放入模型之中，则可直接得到每位高校学生网络安全能力的类别(高校学生网络安全能力共被划分为差、较差、一般、较好、好五个类别，用 1~5 的数字来表示)，最后根据模型测试的结果进行数据分析。

4. KNN 分类算法的高校学生网络安全能力总体情况

针对回收的调查问卷，用 a 代表网络安全法律法规得分， b 代表网络攻击与防御得分， c 代表个人信息保护得分， d 代表网络诈骗得分， e 代表网络道德得分，将它们作为函数的输入变量，建立预测模型。公式(1)给出了输入变量和输出之间的相关性，函数的输出结果 C 为高校学生网络安全能力的类别。

$$F(a,b,c,d,e) = C \tag{1}$$

收集整理的数据样例如表 1 所示。在数据集中随机抽取 375 个数据作为训练集，剩下 118 个数据作为测试集，采取 K 最近邻(k-Nearest Neighbor, KNN)分类算法，该方法是最经典的机器学习算法之一。其思路是：如果一个样本在特征空间中的 k 个最相似(即特征空间中最邻近)的样本中的大多数属于某一个类别，则该样本也属于这个类别。其分类过程分为：① 收集数据集：获取高校学生网络安全风险意识的样本数据，并将所有样本的得分情况规范化到同一个尺寸；② 分离数据集：将样本分为训练集和测试集两个部分；③ 训练分类器：使用训练样本集训练 KNN 分类器，其实就是将训练集存下来；④ 评估分类器：使用测试集来评估训练好的 KNN 分类器性能。KNN 算法的三要素包括：距离度量、 k 值的选择、分类决策规则。通过循环比较实验，本文确定了高校学生网络安全能力数据分类的最佳 k 值为 1，确定最佳距离参数为 2，使用欧氏距离，原理如公式(2)所示。

$$D(x,y) = \sqrt[2]{(|x_1 - y_1|)^2 + (|x_2 - y_2|)^2 + \dots + (|x_n - y_n|)^2} = \sqrt{\sum_{i=1}^n (|x_i - y_i|)^2} \tag{2}$$

Table 1. Sample data of college students' network security capability

表 1. 高校学生网络安全能力数据样例

网络安全法律法规得分	网络攻击与防御得分	个人信息保护得分	网络诈骗得分	网络道德得分	网络安全能力分类
17	10	15	16	20	1 (差)
22	18	19	17	18	2 (较差)
25	25	23	21	20	3 (一般)
25	23	22	26	24	4 (较好)
27	28	25	26	28	5 (好)

分类模型的性能评估指标包括精确度 precision, 召回率 recall, F1 值。精确度和召回率有时也被称为查准率和查全率。P 和 R 指标有时会相互矛盾, F-Measure 用与综合这二者指标的评估指标, 从而反映整体的指标。F-Measure 是 Precision 和 Recall 加权调和平均。精确度和召回率都高时, F1 值也会高。F1 值在 1 时达到最佳值(完美的精确度和召回率), 最差为 0。实验结果如图 1 所示, 分类的精确度达到了 87.88%, 召回率达到了 86.3%, 综合评估指标 F1 达到了 86%, 可见此分类模型性能良好, 之后可直接将调查问卷的数据输入模型, 即可得到其高校学生网络安全能力属于哪一类别。

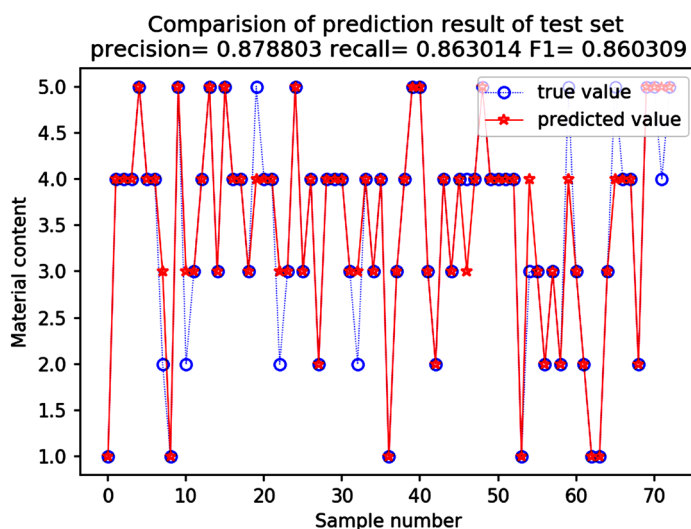


Figure 1. Test results of KNN classification algorithm
图 1. KNN 分类算法的测试结果

根据 KNN 分类模型呈现的结果显示, 网络安全能力一般、较差和差的高校学生分别有 35 人、24 人和 11 人, 占比分别为 29.7%、20.3%、9.3%, 接近 60% 的高校学生网络安全能力处于一般甚至是更差的水平, 网络安全能力好和较好的人数占比分别为 12.7% 和 28.0% (见表 2)。总体来说, 高校学生网络安全能力较为薄弱, 很多学生只看到互联网发展带来的便利, 而没有意识到网络给我们生产生活以及学习方式带来的巨大风险, 尤其是网络安全知识的匮乏、网络安全意识的缺失使得高校学生难以应对出现的各类安全问题, 所以增强高校学生的网络安全能力刻不容缓。另外根据调查结果分析, 我们还可得出如下结论: 一是大部分高校学生对《国家信息化发展战略纲要》、《网络安全法》了解甚少, 对网络攻击知识与网络防御知识和技能的学习也有待增强, 目前多数大学已逐渐开始提供专门为非计算机专业学生设计的网络安全课程, 一些学校强制要求所有学生接受网络安全培训, 但对网络安全教育重要性的认识不够, 知识体系结构有待完善, 学生操作技能有待加强。二是高校学生个人信息保护意识薄弱, 如有的高校学生在使用公共设备上的网络工具后, 没有检查账号是否退出的习惯, 可能导致用户账号、邮箱、身份证等敏感信息泄密; 有的高校学生在使用软件时, 不会阅读用户条款以及隐私条例, 直接完成下载安装; 有的高校学生在网上发送比较重要的文件如个人简历、论文时, 不能有意地对文件提前加密或不清楚如何加密, 导致内容被篡改或窃取等, 但数据结果显示进行过网络安全教育的高校学生网络安全意识强于未进行或较少进行网络安全教育的高校学生。三是高校学生上网时间长、社会经验不足, 缺乏网络诈骗识别能力, 深陷网络诈骗骗局, 如高校学生会参与网络刷单兼职, 与网友分享联系方式、家庭住址、经济状况, 点开网上发布的“点赞有奖”、“在线抽奖”等信息等, 但网络安全教育会降低高校学生遭受网络诈骗的比例。四是部分高校学生的网络道德行为违反社会规范与准则, 网络具有隐匿性、间

接性和虚拟性的特点，因此容易诱使一些高校学生规避现实社会的约束而成为网络的破坏者，产生网络暴力行为、网络侵权行为、制造传播网络谣言行为等。

Table 2. The overall situation of college students' network security capability

表 2. 高校学生网络安全能力的总体情况

类别	人数	百分比
网络安全能力	差	9.3%
	较差	20.3%
	一般	29.7%
	较好	28.0%
	好	12.7%
合计	118	100.0%

高校学生网络安全法律法规基本知识欠缺、防范意识淡薄、网络安全风险识别与应对技能较弱、网络道德与责任感缺失都将直接影响到国家意识形态安全及政权安全。我们的调查结果表明，教育很重要，但也还需要社会各方的共同努力与合作，切实增强大局意识、发展意识、风险意识、责任意识，并将其落实到实际工作中。

5. 提高高校学生网络安全能力的对策

5.1. 深化教育理念，制定并实施高校学生网络安全能力提升规划

教育理念对教育的发展方向、发展进程以及发展效果起着异常重要的作用。坚持高校是促进大学生网络安全发展的关键平台，教育是提升高校学生网络安全能力的重要途径，依照《国家信息化发展战略纲要》、《国家安全法》等相关战略与法律法规，高校从本学校的实际情况出发，制定高校学生网络安全能力提升规划，其中包括深化高校学生网络安全意识的指导思想、主要原则、培养方式和手段以及培养目标，坚持部门联动多措并举，确保高校网络安全教育有序、保质保量地开展。

5.2. 构建高校学生网络安全教育道德法规体系

目前，网络风险的发展速度远远超过网络立法速度，网络的匿名性、虚拟性导致网络谣言风起云涌、乱象丛生，网络诈骗层出不穷，网络社会道德日趋弱化，因此当务之急便是构建网络道德法规体系。一方面，国家应健全网络安全教育与管理相关法律法规，如《信息网络保护权传播条例》、《中华人民共和国网络安全法》等，保障网络环境健康发展。其次，地方政府部门制定适应该地该行业的法律法规，将高校学生网络安全教育目标以法律的形式确定下来，使之具体化、规范化，进而成为高校学生普遍认同和自觉遵守的准则，同时加大监管和督查力度。另外，各高校要积极响应上级号召，建立适合各高校的网络安全管理机制，各级各部门明确具体职责，严格高效落实，建立安全长效监管机制。

5.3. 优化高校学生网络安全教育的课程设置，提高科教水平

目前多数高校已逐渐将网络安全教育纳入课程规划，但在培养过程中，还需努力提高课程趣味性及其吸引力，同时保证课程内容的教育性，形成系统的培养体系。一是在《大学计算机基础》课程的基础上，通过课堂讲授、小组讨论、知识竞赛等方式引导学生关注网络安全趋势，学习网络安全法律法规与网络攻击防御知识，不仅有助于高校学生合理利用法律维护自己的合法权益，也在一定程度上规范高校学生

的网络行为；通过上机操作加强高校学生计算机系统安装、设置等实践操作能力；通过真实案例分析增强高校学生网络安全风险识别能力，同时重视各项学习内容之间的有机联系，使之相辅相成、相互促进。并且将高校学生网络安全意识与防范技能水平纳入学生综合素质测评，着力提升大学生信息素养及数字能力。二是高校应加强高校学生网络心理健康教育，包括疏导情绪和情感问题、解惑人际关系问题、挫折与压力教育等，建立心理健康服务中心，同时可以创建如“心情香蕉”、“馨兰心理”等公众号，对有困难的学生提供心理辅导，降低网络安全风险和意外发生的概率。三是优化升级教育基础设施，强化软硬件建设，建立网络安全主题实验室、开展情景模拟等，提高科教水平。四是开辟网络安全宣传专栏，分析计算机网络常见的安全威胁及应对策略，提供正版杀毒软件等工具，定期更新网络安全典型案例并开展主题讲座，高校学生可以在平台上分享自己的网络安全学习心得或提供网络安全防范的技巧，促进学生之间的沟通交流，拓宽网络安全教育途径，同时各高校也应设计合理的网上学习打卡方式，督促学生完成课外学习。

5.4. 打造高素质的网络安全师资队伍，重视辅导员队伍建设

无论是教材，还是教学方式和手段等方面的改革，都需要教师来进行推进，师资队伍直接决定了网络安全的教育水平，所以高校应优化专业人才培养模式，注重培养高素质、专业化的网络安全教育工作者。各高校应加强教学团队建设，组织教师开展在职培训，聘请网络安全专家和特殊人才担任兼职教师[15]，同时鼓励教师走进企业进行带职学习，将他们的学习折合成一定的课时，给予资金上的支持，丰富网络安全教育工作者的职业经验和技能。建立国际间的校际联系，共同制定长远稳定的国际化师资培养方案，定期派遣优秀教师出国培训，聘请国外高层次的学者来高校访问、分享交流，是我国推进高校学生网络安全的坚实保障。高校辅导员作为高校学生学习生活的密切接触者，不断夯实高校辅导员组织建设也尤为重要。建立全面合理的辅导员评价考核激励机制和岗位优胜劣汰的竞争机制，增强教育工作的有效性。提升辅导员校园网络舆情导控能力，鼓励辅导员积极与学生谈心，了解学生网络安全现状，解答学生疑难问题，并形成纸质记录，做到防患于未然。

6. 结语

随着互联网技术的成熟和新媒体的普及，网络广泛地深入到高校学生生活和学习的方方面面之中，对其产生着越来越重要的影响，同时也滋生了各式各样网络安全问题的出现。本文从网络安全法律法规、网络攻击与防御、个人信息保护、网络诈骗、网络道德五个方面开展高校学生网络安全能力调查，而高校学生网络安全能力的内涵会随着信息环境变化而不断发展，所以认真审视高校学生的需求和变化，根据学生个性特点，更新并制定更具针对性的网络安全教育策略，着重强化高校学生自我修炼的能力显得尤为重要。未来我们需要继续结合时代背景开展与时俱进的研究，进一步深入有关高校学生网络安全能力的理论探索和实践研究，探索人工智能背景下高校学生网络安全能力评价新模式，挖掘其影响因素并创新策略途径，这会对高校学生网络安全能力的培养和相关政策制定具有一定的参考意义。

基金项目

武汉工程大学第十二届研究生教育创新基金项目(CX2020231)。

参考文献

- [1] 中国互联网络信息中心. 第47次《中国互联网络发展状况统计报告》[EB/OL]. http://www.gov.cn/xinwen/2021-02/03/content_5584518.htm, 2021-02.
- [2] 李涛. 网络安全中的数据挖掘技术[M]. 北京: 清华大学出版社, 2017.

- [3] 张俊. 强化新形势下的大学生网络安全教育[J]. 思想理论教育导刊, 2013(11): 116-118.
- [4] 王乔平. 浅谈对网络安全的认识[J]. 信息系统工程, 2019(7): 78.
- [5] 韩璞庚, 朱思颖. 网络空间意识形态安全问题与对策研究[J]. 贵州社会科学, 2019(12): 32-38.
- [6] 刘新华, 巢传宣. 对大学生网络安全意识及教育现状的调查[J]. 职教论坛, 2011(14): 94-96.
- [7] 张力. 大学生网络安全现状及风险防范对策[J]. 教育现代化, 2019, 6(15): 194-196.
- [8] West, R. (2008) The Psychology of Security. *Communications of the ACM*, **51**, 34-40.
- [9] 徐东华, 曾林, 王儒君, 张臻. 研究生网络安全意识和防护技能调查[J]. 中国高校科技, 2019(Z1): 125-128.
- [10] 周建芳, 张艺璇, 张春柳. 大学生网络安全行为调查研究——以南京高校为例[J]. 教育现代化, 2017, 4(19): 165-166+180.
- [11] 方兵. 新媒体时代大学生网络安全素养现状调查分析[J]. 中国医学教育技术, 2017, 31(6): 633-637.
- [12] 胡余波, 潘中祥, 范俊强. 新时期大学生网络素养存在的问题与对策——基于浙江省部分高校的调查研究[J]. 高等教育研究, 2018, 39(5): 96-100.
- [13] 黄斌, 杨馨宇, 王睿. 大学生网络素养问卷的编制及检验[J]. 扬州大学学报(高教研究版), 2020, 24(6): 48-56.
- [14] 徐春玲. “互联网+”时代大学生网络素养现状调查分析与教育建议——以河南省六所高校的抽样调查为例[J]. 新闻知识, 2016(5): 63-66.
- [15] 中央网信办. 有条件的高等院校可创建世界一流网络安全学院[EB/OL]. <http://politics.people.com.cn/n1/2016/0708/c1001-28538920.html>, 2016-07-08.