Cultivation and Practice of Cyber Security Awareness among Teachers and Students in Colleges and Universities under the Background of Big Data

Genyuan Wang, Xiaona Liu
Hainan Vocational University of Science and Technology, Haikou, Hainan, China
DOI: 10.32629/jher.v5i3.2461

Abstract: In the context of big data, teachers and students in colleges and universities play a pivotal role in network security, they are not only the receivers of network information, but also the maintainers of network security, and bear the important responsibility of maintaining individual and collective information security. However, the current situation of cyber security awareness of teachers and students in colleges and universities is not optimistic. This paper analyzes the current situation and influencing factors of college teachers and students' cyber security awareness, points out the difficulties in the construction of the education system, the shortcomings of skill mastery, and the blind spots and misunderstandings of consciousness cognition, and puts forward a series of strategies for cultivating the cyber security awareness of college teachers and students, which is helpful to build a more secure and stable network environment and provide a good learning and development environment for college teachers and students.
***Keywords*:** big data, teachers and students in colleges and universities, cyber security awareness

1. Introduction

The development of the era of big data and its impact on network security With the rapid development of big data technology, data acquisition, storage, and analysis are becoming more and more convenient. However, this also poses significant cybersecurity challenges. As a distribution center of knowledge and technology, universities are not only the forefront of big data applications, but also a high-risk area for cyber attacks. Teachers and students play a vital role in the cyber security of colleges and universities, they are not only users of information, but also the first line of defense for information security.

At present, the overall level of cyber security awareness among teachers and students in colleges and universities is still uneven. Many teachers and students still have a superficial understanding of cyber security, lacking in-depth understanding and systematic awareness of prevention. In the context of big data, the cultivation of network security awareness is not only a key part of the informatization construction of colleges and universities, but also an important prerequisite for ensuring the safe and orderly progress of teaching and scientific research activities. Therefore, it has become an urgent task to improve the cybersecurity awareness and skills of teachers and students in colleges and universities.

2. Analysis of the current situation of network security awareness of teachers and students in colleges and universities

2.1 Difficulties in the construction of cyber security education system

At present, the cyber security education system of colleges and universities has obvious deficiencies in many aspects. Many colleges and universities lack systematization and continuity in the design of cybersecurity courses. Specifically, the course content is often scattered across different semesters and different majors, lacking unified planning and coordination. This scattered curriculum makes it difficult for students to form a complete and systematic knowledge structure of cybersecurity, and they are unable to fully understand and master all aspects of cybersecurity.

The pace of updating of course content lags behind the pace of technological development. Cybersecurity technologies and threats are constantly evolving, and university curricula often fail to reflect these changes in a timely manner, resulting in a disconnect between what students learn and what they actually need. Behind this problem is the lack of resource investment in curriculum development and updating, as well as the lack of sensitivity and response mechanisms to emerging threats to provide students with the most up-to-date knowledge and skills.

Some colleges and universities lack teachers with deep cybersecurity background and practical experience, and

some teachers' own professional ability and teaching level need to be improved, unable to provide students with the latest knowledge and skills. This not only limits the depth of the course, but also affects students' comprehensive understanding of cyber security knowledge and the cultivation of practical application ability.

2.2 Shortcomings in the mastery of cyber security skills

At the practical level, although many teachers and students have certain theoretical knowledge, they are often unable to apply it in practice. When faced with cyber attacks, they lack in-depth knowledge of common attack vectors such as SQL injection, cross-site scripting (XSS), denial-of-service attacks (DoS/DDoS), etc. For example, SQL injection attacks perform unauthorized database operations by inserting malicious SQL statements into input fields, but many teachers and students are not clear about their implementation and defense methods, resulting in an inability to effectively identify and respond to such attacks.

Network security not only relies on technical means such as firewalls and anti-virus software, but also requires personal security awareness and behavioral habits. However, many teachers and students lack the necessary security precautions when using electronic devices and online services. Passwords are updated irregularly, and simple and easy-to-crack password combinations are often used, making accounts vulnerable to guesswork and cracking. Another common problem is clicking on unidentified links, which can be phishing sites that trick users into entering sensitive information, resulting in information leakage and property damage.

In the face of increasingly sophisticated cyber security threats, it is difficult for students to effectively cope with various security challenges in a real work environment if they only rely on classroom theory teaching without sufficient practical training. The importance of the Cyber Security Lab as a bridge between theory and practice is self-evident. In such an environment, students can experience simulated real-world attack and defense scenarios, and deepen their understanding of attack mechanisms, exploits, and defense strategies through hands-on experience. However, due to the quantity and quality of experimental equipment, the realism of the simulated environment, and the allocation of teachers, it is often difficult for students to obtain sufficient practical opportunities, resulting in the difficulty of effectively transforming theoretical knowledge into the ability to solve practical problems.

2.3 Blind spots and misunderstandings of cyber security awareness

Many teachers and students mistakenly believe that cybersecurity issues are irrelevant to them, and that only people with information technology-related majors need to pay attention to this issue. This notion ignores the pervasiveness and importance of cybersecurity issues in modern society. With the widespread application of Internet technology, cybersecurity threats are everywhere, and anyone can be a target. Therefore, this misconception leads to a lack of proactive awareness among teachers and students in the face of potential threats, and cannot effectively prevent cyber attacks.

Some teachers and students believe that technical means can solve all problems, and overrely on technical measures such as firewalls and anti-virus software, while ignoring the adjustment and improvement of daily usage habits. For example, they may share personal information at will, connect to unsecured Wi-Fi networks, use weak or duplicate passwords, etc. These actions not only increase the risk of personal information leakage, but can also provide an opportunity for attackers to exploit them. In fact, network security not only needs to rely on technical means, but also needs to cultivate good usage habits and security awareness in order to form a comprehensive protection system.

Social engineering attacks are fraud that exploits human weaknesses to obtain sensitive information by pretending to be a trusted authority or acquaintance. These attacks often do not rely on technical vulnerabilities and instead use psychological manipulation to gain the victim's trust. Many teachers and students do not have enough understanding of the dangers of this attack method and are easy targets for attackers. Attackers may obtain login credentials or other sensitive information through phishing emails, fake phone calls, or social media messages, resulting in serious information leaks or property damage.

3. Strategies for cultivating network security awareness among teachers and students in colleges and universities

3.1 Refine the curriculum and teaching content of cyber security education

3.1.1 Targeted curriculum design

Targeted curriculum design should be carefully formulated according to the student's professional background and grade level. For students majoring in computer science, due to their deeper involvement in network and information technology, they may be engaged in work directly related to network security technology in the future, and the course

content should cover the details of network security technology and protection methods in more depth to meet their needs in security development and system maintenance, including network attack and prevention, encryption technology, security programming, etc. Non-technical students may be more exposed to the cybersecurity threats faced by ordinary users, and they need to pay more attention to basic cybersecurity awareness and daily protection skills, such as password management, safe surfing, and online fraud detection. The course design can be carried out according to the actual needs of students in different majors, which can make the course closer to the learning and career development needs of students, and improve the effectiveness and attractiveness of the course.

3.1.2 Combination of theory and practice

In cybersecurity education, a combination of methods such as hands-on, lab training, and case studies is crucial. This approach not only improves students' practical and problem-solving skills, but also enables them to better address increasingly complex cybersecurity challenges. By adding hands-on courses, students can practice what they have learned by themselves, so that they can understand the course content more deeply, and transform abstract theoretical knowledge into concrete practical skills. For example, students can participate in the practical operation of simulating cyber attacks and defenses, and master the use of various defense techniques and tools in practice, so as to improve their practical skills.

Simulating various cybersecurity attack and defense scenarios in the laboratory environment can help students understand the principles and applications of cybersecurity technologies more intuitively, and enhance their practical and problem-solving skills. Through a virtual lab environment, students can simulate real-world cyberattack and defense scenarios to further improve their hands-on skills.

Through the analysis of real-life cyber security incidents and cases, students can learn about various cyber security threats and attack methods, and learn rich experiences and lessons. Case studies allow students to think deeply about the root causes and solutions of problems, improve their problem-solving and adaptability, and prepare them for complex cybersecurity challenges in the future.

3.1.3 Strengthen practical links

For different network security technologies and scenarios, it is essential to design a variety of practical projects and tasks. Cyber security technology requires hands-on operation and immersive practice to feel its application effect more intuitively. By participating in practical projects such as cyber attack and defense, security vulnerability mining and repair, and encryption technology application, students can master the use of various network security technologies and tools in practice, and significantly improve their hands-on ability and practical experience.

If the knowledge of cyber security is only at the theoretical level, it is difficult for students to truly understand its application. Therefore, it is essential to apply theoretical knowledge to practical projects and tasks. For example, students are organized to participate in cyber security competitions, simulation drills and project practice, so that they can solve practical problems in teamwork and cultivate innovative thinking and teamwork skills. In these activities, students can simulate cyber attack and defense scenarios and conduct practical operations, thereby deepening their understanding and mastery of cyber security technologies.

Students are encouraged to actively participate in cybersecurity communities and open source projects, and by being exposed to the latest cybersecurity technologies and research results, students can broaden their horizons and enhance their practical skills. These hands-on activities not only enhance students' competitiveness in the field of cybersecurity, but also lay a solid foundation for their future career development. Through a wealth of hands-on sessions, students will not only master the basic skills of cybersecurity, but also flexibly apply these skills in complex real-world environments.

3.2 Enhance teachers' professional competence in cyber security and teaching innovation

Improving teachers' professional competence and teaching innovation in cyber security is an important task to ensure the effectiveness of cyber security education and adapt to the rapidly developing cyber threat environment. Here are some strategies and pathways colleges and universities can take:

Actively introduce teachers with rich practical experience and high-level professional background to enrich the teaching team. By establishing close cooperation with industry enterprises, we bring in professionals in the field of cybersecurity as part-time teachers or provide professional guidance. It can not only provide students with richer learning resources and practice opportunities, but also promote in-depth exchanges and cooperation between teachers and the industry. Industry and enterprise professionals can also provide professional guidance for college teachers, and invite teachers to visit the enterprise site, so as to deepen the school-enterprise cooperative relationship, effectively promote the combination of theoretical knowledge and practical application, and improve the teaching level and students' employment competitiveness.

Encourage faculty members to participate in research projects and academic forums to enhance their academic standards and research capabilities. Through the participation of scientific research projects, teachers can conduct in-depth research

on cutting-edge issues in the field of network security, keep abreast of the latest network security technologies and research results, update their knowledge structure, and accumulate more practical experience and research results, so as to provide more rich and cutting-edge content for teaching work.

Vigorously promote teachers to adopt innovative means in teaching to improve teaching effectiveness. Introduce case teaching, simulation exercises, project-driven teaching methods and other teaching methods to allow students to learn and master cyber security skills in practice. By simulating real-life cyber attack and defense scenarios, students can gain an in-depth understanding of cyber security principles and techniques through interaction, and improve their practical skills and problem-solving skills. These innovative teaching methods can stimulate students' interest in learning and improve their learning effectiveness, so as to better promote the implementation and promotion of cybersecurity education.

3.3 Strengthen the network security management mechanism of colleges and universities to ensure efficient implementation

The academic affairs department needs to conduct a detailed needs analysis to understand the level of knowledge and needs of students in various majors and grades in cybersecurity. Based on the results of the analysis, develop cybersecurity courses suitable for different majors and grades. For computer science majors, advanced cybersecurity technology courses can be set up, including intrusion detection, cryptography techniques, and secure programming; For non-technical students, a basic cybersecurity course can be designed that covers practical skills such as password management, staying safe online, and preventing online fraud. and coordinate teacher resources and teaching facilities to ensure that the course can run smoothly.

The Information Technology Department shall be responsible for school-wide technical support and security. The information technology department assigns professional and technical personnel to each college, and the information technology personnel should maintain the security of the campus network infrastructure, update and patch system vulnerabilities in a timely manner, configure firewalls and intrusion detection systems, and the technical personnel of the college are responsible for the security of the network infrastructure of each college. The Information Technology Department manages the IT talent across the school, providing the necessary technical training to help teachers and students master basic cybersecurity skills and protective measures.

The Student Management Department is responsible for cybersecurity awareness and student engagement activities. Through organizing cyber security lectures, competitions, theme activities, etc., students can enhance their cyber security awareness and self-protection ability. The student management department should also establish a feedback mechanism to collect students' problems and suggestions in the study and practice of cybersecurity, and improve relevant work in a timely manner.

Colleges and universities should formulate detailed implementation rules for cybersecurity education, clarifying the educational objectives, content, and evaluation standards, and establish regular inspection and evaluation mechanisms to supervise and evaluate the effectiveness of each department's work. Through regular cyber security knowledge tests, simulation drills and educational effect evaluations, we ensure that all measures are truly implemented. At the same time, an efficient emergency response mechanism should be established to ensure that all departments and personnel can quickly and efficiently cooperate in response to emergencies in the event of a network security incident, so as to ensure the security and stability of the campus network.

3.4 Increase publicity on cyber security and deepen students' awareness of protection

The information technology department of colleges and universities should act as an event planner and organize various colleges to hold various activities, such as lectures, competitions, and theme activities, to popularize network security knowledge. At the same time, cyber security experts can be invited to give special lectures to students from different colleges and grades, sharing the latest cyber security threats and protection tips, covering how to prevent phishing, identify malware, protect personal privacy and other practical content, to help students build a comprehensive security awareness.

As the organizer of the cyber security competition, the information technology department encourages students from various colleges to form their own teams to participate in the competition. During the competition, students will work as a team to solve real-world cybersecurity problems, such as cracking simulated cyber attacks and defending against security vulnerabilities in virtual environments. This format not only exercises students' technical skills, but also develops their teamwork and problem-solving skills, while stimulating their interest and passion for cybersecurity.

Each college can carry out cyber security theme activities on a class basis, such as cyber security month, cyber security day, etc., and attract students' attention and participation through various forms such as posters, promotional videos, and interactive games. During Safety Month or Safety Day, you can launch a cyber security tip every day and promote it through

social media such as campus bulletin boards, campus websites, and college official accounts. At the same time, creative promotional videos are produced to show common cyber security threats and their countermeasures, so that students can learn security knowledge in a relaxed and happy atmosphere.

Encourage students to actively participate in cyber security practices, and set up a cyber security volunteer team to allow them to participate in the maintenance and promotion of campus cyber security. At the same time, students are organized to participate in off-campus cyber security internships and training to gain more practical experience. Through these hands-on activities, students not only gain an in-depth understanding of cyber security issues, but also learn how to effectively protect themselves in real life.

4. Conclusions

In today's era of big data, network security issues have increasingly become the focus of social attention. In this context, as the core group of network use, the cultivation and practice of network security awareness of teachers and students in colleges and universities is particularly crucial. This not only involves the security of personal information, but also directly affects the stability of the entire campus network ecology. Based on the development background of the era of big data, this paper deeply analyzes the current situation and influencing factors of network security awareness of teachers and students in colleges and universities, and proposes corresponding training strategies. By deepening the reform of the education system, improving the professional ability of teachers, strengthening the management mechanism and increasing publicity, we can effectively improve the cyber security awareness of teachers and students in colleges and universities. However, with the development and application of technology, cybersecurity education in colleges and universities will also face more new challenges and opportunities. Only continuous innovation and improvement can ensure the continuous promotion and effectiveness of cybersecurity education in colleges and universities.

References

[1] Jiang Yuanhong. Journal of Security and Environment,2023,23(09):3381-3382.
[2] Li Yunfu. Heilongjiang Higher Education Research,2023,(09):141-146.DOI:10.19903/j.cnki.cn23-1074/g.2023.09.012.
[3] Jin Yi. Mass Standardization,2024,(06):172-174.
[4] Zhu Binyong. Network Security Technology and Application,2024,(03):76-78.
[5] Wan Fang. Journal of Hubei Open Vocational College,2024,37(03):150-151+163.