Research on Cultivating Cybersecurity Awareness among High School Students

He Jianni[1], Yuan Hangru[1]

[1]Xinjiang University of Political Science and Law, Tumxuk, Xinjiang, 832000, China

Abstract: This study aims to explore the cultivation of network security awareness among college students. By defining and emphasizing the importance of network security awareness, the urgency and necessity of cultivating network security awareness among college students are revealed. The research findings indicate that there are many issues in network security education for college students. In response to these issues, this study proposes corresponding strategies that can effectively enhance college students' network security awareness, enabling them to better cope with network security challenges. This research provides valuable references for improving and enhancing the cultivation of network security awareness among college students.

1. Introduction

1.1 Research Background

With the popularity of the Internet and the rapid development of information technology, college students increasingly rely on the Internet in their daily lives and studies. However, the online environment poses various potential security risks and threats, such as phishing, malware, and personal information leakage. In this context, the cultivation of network security awareness and skills among college students becomes particularly important. As the new generation of Internet users and information disseminators, college students face increasingly complex network security challenges. Without effective network security awareness and skills, they are susceptible to becoming targets of cyberattacks, compromising the security of their personal information, and even causing adverse effects on the school network and the entire societal network environment[1]. Therefore, conducting in-depth research on the cultivation of network security awareness among college students, analyzing the existing issues, and proposing corresponding strategies and improvement measures are of significant importance in enhancing college students' level of network security awareness and strengthening their ability to defend against online threats. This not only helps safeguard the security and privacy of students' personal information but also contributes to maintaining the stability and security of the entire online environment.

1.2 Research Significance

By studying the cultivation of network security awareness among college students, effective

educational strategies and training plans can be developed to help students acquire basic network security knowledge and skills and enhance their ability to prevent online threats. This contributes to safeguarding the security of students' personal information and reducing the risk of cyberattacks. As colleges and universities are open network environments, students' online behaviors and security awareness directly impact the overall security of the school network environment. Through studying the cultivation of network security awareness among college students, it is possible to promote the formation of correct online behaviors and security awareness among students, reduce the occurrence of cybersecurity incidents, and maintain the stability and security of the school network environment. The cultivation of network security awareness among college students involves not only technical aspects but also the cultivation of legal education and legal consciousness. By studying the cultivation of network security awareness among college students, it is possible to enhance students' understanding and compliance with laws and regulations, promote the construction of a legal campus, and foster students' legal awareness and legal literacy[2].

2. Definition and Importance of Network Security Awareness

2.1 Definition of Network Security Awareness

Network security awareness refers to the level of understanding and comprehension that individuals or organizations have regarding network security issues, as well as their awareness and ability to take action to protect themselves and others from online threats and attacks. It includes the following aspects:

High school students possess awareness regarding the diverse risks and threats prevalent in the digital realm, such as viruses, phishing, and the potential exposure of personal data. It is crucial for individuals to acquire a comprehensive comprehension of the potential hazards they might encounter online and maintain vigilance towards these risks.

Furthermore, high school students recognize the significance of internet security, encompassing the protection of personal accounts, passwords, and privacy. They understand the importance of implementing necessary precautionary measures and defending against cyberattacks or breaches.

In addition, high school students strive to cultivate positive online habits, including regular password changes, exercising caution when confronted with unfamiliar links, and refraining from downloading unknown software. The adoption of these habits contributes to a reduction in the occurrence of online risks.

High school students acquire proficiency in cybersecurity skills, which involve employing specific technical strategies to prevent viruses and hacking attempts, such as utilizing antivirus techniques and employing effective password creation methods. Additionally, they develop the ability to respond appropriately in the event of a network security incident[3].

Furthermore, high school students actively monitor the online environment, remaining vigilant to the presence of harmful content or activities, and promptly reporting them. They take proactive measures to report network vulnerabilities or security concerns to the appropriate departments, thereby contributing to the establishment of a safe and harmonious online environment.

2.2 Importance of Network Security Awareness for College Students

As the main users of the Internet, college students frequently utilize the internet in their daily studies and lives. They store and transmit a significant amount of personal sensitive information, including academic records, personal identification information, and bank accounts. Having a strong network security awareness helps them identify and prevent various online threats, protecting the security of personal information and avoiding privacy breaches and identity theft. College

students' online behaviors are susceptible to becoming targets of cyberattacks, including phishing, malware, and online scams. Possessing network security awareness enables students to identify suspicious links and information, learn how to correctly use network tools and applications, and reduce the risk of being deceived or attacked. By strengthening the cultivation of network security awareness, college students can develop good online behavioral habits, such as complying with laws and regulations, respecting online ethical norms, and avoiding the spread of rumors and harmful information. This contributes to maintaining a good order in the online environment and fostering a harmonious online community atmosphere. The cultivation of network security awareness is not only for the purpose of protecting personal safety but also for promoting students' comprehensive development. Through learning and mastering network security knowledge, students can enhance their ability to acquire and process information, improve their information literacy and innovative capabilities, and enhance their problem-solving skills, thereby better adapting to the development and demands of the information society. The cultivation of network security awareness among college students is an important component of establishing a campus based on the rule of law. By strengthening network security education, students can understand and comply with relevant laws and regulations, fostering a sense of the rule of law and legal compliance. This contributes to the construction of a legal campus environment, promoting the healthy development of schools and the comprehensive growth of individual students[4].

3. Current Status of Network Security Awareness Cultivation among College Students

3.1 Lack of Comprehensive Network Security Education Courses

The establishment and content of network security education courses are relatively weak. The course content mainly focuses on basic network security knowledge, such as password settings, antivirus measures, and phishing prevention, while education on more complex topics such as advanced network attacks, information security management, and network privacy protection is relatively lacking. Network security education courses lack practical components, which fail to deepen students' understanding and application abilities of network security through hands-on exercises and simulations. The lack of practical components may result in students only staying at the theoretical level, making it difficult for them to truly master the practical skills to deal with network security threats. The professional competence of teachers in college network security education courses needs to be improved. The field of network security is developing rapidly, involving complex technical and legal issues. Teachers need to possess a high level of professional knowledge and practical experience to effectively impart knowledge to students.

3.2 Low Importance Attached to Network Security

College students have not yet formed a clear understanding of the importance and impact of network security. They may overlook the impact of network security on personal privacy, property security, as well as their studies and daily lives. This lack of awareness leads to insufficient attention to network security issues among students, making them prone to neglecting security risks and engaging in inappropriate behaviors. A favorable cultural atmosphere for network security awareness has not been established. Schools and society do not provide sufficient promotion and education on network security, and students lack opportunities to come into contact with and pay attention to network security in their daily lives. The lack of a culture that values network security can affect students' awareness and attitude towards network security issues. Colleges lack effective educational resources in network security education. The lack of professional network security teachers, textbooks, as well as up-to-date teaching content and methods, results in poor learning

experiences and outcomes for students in network security. Universities tend to focus more on imparting disciplinary knowledge and neglect the cultivation of security awareness. Students often only pay attention to the subject matter taught in their courses and lack sufficient emphasis on acquiring network security knowledge and skills[5].

3.3 Weak Awareness of Personal Information Protection

College students have insufficient awareness of the value and sensitivity of personal information. They may not fully understand the risks and consequences that personal information disclosure can lead to, and they lack a sufficient understanding of the importance of protecting personal privacy. College students tend to engage in oversharing personal information online. They may openly disclose detailed personal information on social media platforms, online forums, or other online channels, and even trust requests from strangers, exposing their sensitive information. College students lack vigilance regarding information security risks when using the internet. They may casually click on unknown links, download unverified applications, or use weak or identical passwords across multiple platforms, increasing the risk of their personal information being stolen or misused. College students lack effective personal information protection skills. They may not be familiar with security settings and privacy options, and do not know how to properly manage and protect their personal information to minimize the possibility of being exploited by malicious actors.

3.4 Strengthening the Ability to Identify Sensitive Information Online

College students have a poor understanding of the scope and content of sensitive information online, making it easy for them to disclose personal privacy information or sensitive data on public online platforms. They may lack accurate awareness of what constitutes sensitive information and how to properly protect such information. College students have weak abilities to recognize online scams and fraudulent techniques. They may struggle to distinguish spam emails, phishing websites, false advertisements, and other fraudulent activities, making them vulnerable to online scams. College students are unfamiliar with privacy settings and data protection tools, lacking skills in protecting personal information. They may not correctly set privacy options for their social media accounts or use secure password management tools to protect their personal accounts. College students lack systematic opportunities for network security training. They may not have received professional training specifically focused on network security awareness, resulting in a lack of systematic learning and mastery of network security knowledge and skills.

4. Strategies to Improve College Students' Network Security Awareness

4.1 Empowering College Students as the Leading Force in Network Security Education

Universities can establish student organizations dedicated to network security, with voluntary student participation as organization leaders and members. These organizations can organize network security awareness campaigns, host lectures and training sessions, collaborate with the university to promote network security education, and provide platforms for student communication and learning. Schools can collaborate with professional institutions to implement network security training programs specifically designed for students. These training programs can include the imparting of network security knowledge, skills, and practical exercises to enhance students' network security awareness and coping abilities. Additionally, the training programs can encourage students to participate in network security competitions and drills to enhance their practical

capabilities. Schools can conduct surveys and assessments on students' network security awareness to understand their knowledge levels, awareness levels, and behavioral habits regarding network security. Based on the survey and assessment results, schools can develop corresponding education plans and strategies to improve students' network security awareness in a targeted manner. Schools can organize students to participate in network security promotion activities, such as themed lectures, speech contests, and social media campaigns. Through these activities, students can take an active role in disseminating network security knowledge and awareness to their peers, thus raising the overall network security awareness of the entire school. Schools can provide students with opportunities and resources to engage in practical network security exercises. For example, establishing network security laboratories, providing secure testing platforms, and introducing security technology innovation projects allow students to learn and apply network security knowledge through practical operations, thereby enhancing their practical abilities and innovation awareness.

4.2 Enhancing College Students' Attention to Network Security

Schools should incorporate network security education content into their curricula to make students aware of the importance of network security and related knowledge. Network security courses, special lectures, or seminars can be offered to guide students in recognizing the significance of network security for individuals, society, and the country. By citing real-life network security cases and consequences, students can be shown the seriousness of network security risks and the potential negative impacts they can have. This can increase students' vigilance and attention, motivating them to proactively protect their own network security. Schools can organize network security knowledge competitions, speech contests, or awareness campaigns to enhance students' interest in and attention to network security. These activities can increase student participation and interaction, deepening their understanding of network security. Schools can provide students with security tools and resource support, such as network security software and password management tools. By providing these tools to students, they can better protect their personal information and network security, thus strengthening their attention to network security. Schools can establish dedicated platforms for network security awareness promotion, such as campus websites and social media accounts, where they regularly publish network security-related information, tips, and warnings. By continuously providing useful network security knowledge, schools can remind and guide students to maintain ongoing attention to network security.

4.3 Strengthening Awareness of Personal Information Protection

Schools should provide students with basic knowledge of personal information protection, including what constitutes personal sensitive information, how to use and manage personal information appropriately, and how to prevent personal information leakage. This can be achieved through dedicated courses on personal information protection, organizing lectures or workshops to educate students about the importance of personal information and methods of protection. Schools should emphasize and educate students about their privacy rights, helping them understand their rights to protect personal information and the risks and consequences of privacy breaches. By emphasizing privacy awareness, students can increase their level of importance placed on personal information protection. Schools can provide students with privacy protection tools and guidance, such as privacy setting guidelines, secure browsers, and encrypted communication applications. These tools and guidance can help students better protect their personal information and reduce the risk of personal information leakage. Schools can organize information security awareness training, teaching students how to be vigilant against phishing attacks, social engineering, and other attack

methods, as well as how to identify and respond to various network security threats. By cultivating students' sensitivity to information security, their awareness of protecting personal information can be enhanced. Schools should actively foster a culture of personal information protection and security. This can be achieved through organizing information security awareness campaigns, hosting discussions on privacy protection, and creating opportunities for students to exchange, share, and advocate for personal information protection experiences and ideas.

4.4 Enhancing the Ability to Identify Sensitive Information Online

Schools should provide students with definitions and specific examples of sensitive information online, helping them understand which information carries sensitivity and risks on the internet. By presenting specific cases, students can better understand and identify sensitive information online. Students should be encouraged to develop critical thinking skills and learn how to objectively analyze and evaluate online information. They should be reminded to pay attention to indicators such as information sources, authenticity, and credibility to identify potential sensitive or false information. Schools can organize training activities on identifying online rumors and false information, enabling students to distinguish and recognize common rumors, false information, and fraudulent techniques online. Through practical exercises and case analyses, students' alertness and ability to identify sensitive information online can be improved. Schools should also educate students about protecting their personal privacy information, making them aware of the sensitivity of personal privacy information and the protective measures. Students need to understand that disclosing personal privacy information can lead to risks such as identity theft and online scams, thus emphasizing the importance of identifying and protecting sensitive information online. Schools can provide students with resources and guidance for online security, such as secure browsers, anti-phishing tools, ad-blocking plugins, etc. These tools and guidance can help students reduce their exposure to sensitive information online and enhance their awareness and ability to prevent online threats.

5. Conclusion

With the rapid development and widespread use of the Internet, network security issues have become increasingly prominent, especially for college students. Developing network security awareness among college students is crucial. This research aims to explore the cultivation of network security awareness among college students, analyze the existing problems, and propose corresponding strategies. To improve college students' network security awareness, a series of strategies have been suggested. These include empowering college students as the leading force in network security education, enhancing their attention to network security, strengthening awareness of personal information protection, and enhancing their ability to identify sensitive information online. The implementation of these strategies requires joint efforts from schools, educational institutions, families, and society to work together towards a common goal.

References

[1] Mcarthur L H, Holbert D, Forsythe W A I .College Students and Awareness of Food Safety [J].Journal of Family & Consumer Sciences, 2007, 99:60-67.
[2] Duragannavar G F, Arun K H S. Wireless Network Use and Awareness of Surana College Students: A Study [J]. 2021.
[3] Garrison C P .Computer Security Awareness of College Students.[C]//International Conference on Security &Management. DBLP, 2005.
[4] Bahron H, Abdul Razak R, Hamzah P. Consumerism and environmental awareness of college students: attitude and practice/Dr. HadariahBahron, Dr. Rozana Abdul Razak, Pa'ezahHamzah [C]//IEEE International Conference on Mobile Adhoc & Sensor Systems. IEEE, 1997.
[5] He L. Status Quo of College Students' Network Security Awareness under the Background of Big Data [J]. 2021.