Security Instruction to Stop Hacking the Campus

Shihe Wang

School of Business Hangzhou City University，Hangzhou City Zhejiang Province，310015；

Abstract： With the evolution of online society toward mobility, socialization, and intelligence, campus network security faces increasingly severe challenges. Traditional cybersecurity education, which focuses on interaction protocols and human vulnerabilities, can no longer meet current security demands. Cybersecurity education must become more strategic, persistent, and dynamic to safeguard security baselines and maintain the purity, effectiveness, and safety of campus networks.

Keywords： Cybersecurity；Security Education；Security Strategy

DOI:10.69979/3041-0843.25.03.030

1 Introduction

The advent of the internet era has provided the public with a convenient interactive environment and free, vast, and rapid access to information. However, it has also introduced vulnerabilities, backdoors, viruses, trojans, rootkits, and other flaws, while fostering breeding grounds for botnets, the dark web, and gray-hat activities. Coupled with the lure of illicit profits, the security and authenticity of information have become difficult to guarantee, giving rise to cybersecurity risks.Looking back at the history of the internet, we find that many of these negative effects did not originate from malicious intent. For example, the first computer virus was created to combat piracy, rootkits were developed to provide customized services, and technologies like the dark web and blockchain even carry strong ideological imprints with highly ambiguous ethical boundaries. In this sense, political correctness and moral righteousness in technological development alone cannot fully address cybersecurity issues. What truly matters is who uses the technology and for what purpose—ethical and regulatory constraints must be enforced throughout the entire lifecycle, from development to application. In the relatively pure environment of campuses, users primarily consist of intellectually curious students and well-intentioned teachers. This group actively seeks information online but, due to their strong thirst for knowledge and limited discernment, is highly susceptible to unpredictable problems and risks. Therefore, adopting effective strategies to strengthen cybersecurity education in higher education institutions and enhance the cybersecurity awareness of teachers and students must be a top priority in current campus initiatives.

2 Current Status and Issues of Cybersecurity Education

The main problems in campus network security include: frequent cybersecurity education incidents, incomplete coverage of cybersecurity education, and insufficient cybersecurity awareness among teachers and students. The current situation is highly vulnerable in all aspects.

2.1 Weak Infrastructure with High Demand

Campus networks often suffer from relatively weak hardware and software while serving a large user base. Limited infrastructure struggles to provide both a smooth network experience and necessary security resources. Due to inadequate security measures, campus networks face high risks of intrusion. For example, cyberattacks targeting Google were traced back to computers at Shanghai Jiao Tong University and Lanxiang Vocational School. According to Shanghai Morning Post, the perpetrators were likely Eastern European criminal organizations that used technical means to hijack school computers as "botnets," enabling large-scale attacks on high-security targets. Even when investigators traced attacks to a specific school, students and staff were often unaware of the breach.

2.2 Incomplete Coverage of Cybersecurity Education

As reported by Sohu News, Shanghai Jiao Tong University recently issued a security alert: seven faculty members and

students fell victim to scams. Other prestigious universities also regularly publish fraud cases on their websites. Despite preventive measures and global crackdowns on telecom fraud hubs, cyber scams persist. The reason lies in insufficient education—simply warning against trusting strangers or transferring money is inadequate.

Cyber fraud extends beyond deception; it exploits social engineering to amplify human weaknesses, such as impersonating authorities or relatives. Fraudsters even trade stolen data on the dark web for targeted scams, making individual vigilance ineffective. Only organized efforts can counter such sophisticated attacks.

2.3 Insufficient Awareness and Response Mechanisms

Many users lack basic cybersecurity knowledge, such as identifying phishing emails or securing passwords. Schools must integrate practical training (e.g., simulated phishing tests) and establish rapid response protocols.

The cybersecurity awareness of teachers and students is not strong enough. Cybersecurity not only involves preventing external cyber attacks but also requires "looking inward" for self-protection. For instance, a university in Shanghai stipulated that students must complete N morning runs each semester; otherwise, their physical education grades and the annual "National Student Physical Health Standard" scores would be failing. A student, in order to sleep in, invaded the school's morning run management system and the physical education grade system's backend to modify the data. Later, he even posted on the forum that he could charge for "running on behalf of others", organizing a profit-making hacking activity, and eventually ended up in prison. This incident exposed the campus network's negligence in checking logs, managing forum public opinions, and over-reliance on the check-in system without on-site sampling verification. However, the fundamental reason for many students paying for "running on behalf of others" is still the lack of in-depth cybersecurity awareness.

3 Re-definition and Re-education of Cybersecurity

As can be seen from the above, cybersecurity incidents often result not from a single bug in a single link, but from the accumulation of multiple mistakes in software and hardware, management systems, and personnel quality. A cybersecurity system is not an isolated system but should be redefined as a suite of technologies, ranging from SD-WAN and cloud access security brokers to secure web gateways, zero-trust network access, firewall as a service, and remote browser isolation. The core of the system is identity, meaning that identity is at the center of network access. A cybersecurity system should be able to identify devices and users and apply policy-based security based on users, roles, devices, behaviors, locations, and other characteristics to ensure secure and reliable access to applications or data. This way, when users implement secure access, they can be traced back to a unique identity without exposing personal or organizational privacy information. At the same time, cybersecurity education should not only focus on raising awareness but also provide a general understanding of the network environment, a clear understanding of the entire permission system, and compliance with relevant guidelines, without overstepping or exceeding boundaries. It is necessary to make teachers and students believe that relevant departments and key figures should also abide by this permission system and that the interaction protocol should be a rigorous mutual authentication process, never a one-way instruction. Only in this way can they not be intimidated or deceived by impostors. This means that the meaning of cybersecurity has gradually shifted from being technology-focused to identity-focused. Over the past two decades, we’ ve seen fewer traditional hackers emerge, but a significant increase in telecom fraud. Hackers have also transitioned from coding enthusiasts to social engineering experts. Cybersecurity technology has made remarkable progress in the last twenty years. Various security measures. including firewalls, intrusion detection systems, antivirus software, multi-factor authentication, and secure protocols. have greatly enhanced the protection of computer systems and networks. This has made hacking attacks more difficult and increased the risk of being detected and held accountable. Many countries and regions have strengthened legal regulation and crackdowns on cybercrime. For example, the United States, the European Union, and China have all enacted strict cybersecurity laws imposing harsher penalties for hacking activities. This makes potential “hackers” think twice before engaging in malicious intrusions. Some former hackers may transition into "white hat hackers" or cybersecurity experts, providing security testing, vulnerability discovery, and other services to businesses and organizations legally. These “white hat hackers” typically earn legitimate income through “penetration testing” or “bug bounty programs,” representing a positive transformation of the “hacker” identity. However, this only signifies a reduction in individual hackers; hacking is shifting towards organized groups,

making it harder to detect and eliminate. For instance, many telecom fraud gangs operate abroad, particularly in Southeast Asia. Cross-border pursuit, evidence gathering, and crackdown on these gangs face numerous legal and operational challenges. Consequently, these groups often operate with impunity. With technological advancements, fraud methods are constantly "innovating," including identity theft, impersonation of law enforcement officials, fake prize notifications, online shopping scams, loan scams, and customer service impersonations. a constant stream of new tactics making it difficult to defend against. Data breaches are a serious problem, with large amounts of user data illegally obtained and traded on the internet. Fraudsters can leverage this data to conduct targeted scams, increasing their success rate. Many users still lack sufficient cybersecurity knowledge and fraud awareness. Fraudsters often exploit people's fears, greed, and sympathy. psychological vulnerabilities. using carefully designed scam scripts to lure victims. Beyond financial fraud, hacker organizations are increasingly interested in political issues. Global political and religious organizations are also utilizing hacker groups for infiltration. For example, Anonymous and LulzSec, organizations involved in transnational political movements, typically launch attacks against governments, large corporations, and religious organizations through methods like DDoS attacks, data leaks, and website defacement. Their motivations include supporting internet freedom, opposing copyright laws, fighting censorship, combating corruption, countering terrorism, supporting the "Occupy Wall Street" movement, and backing the "Arab Spring" revolution. The actions of politically motivated hacker groups are typically driven by political, social, and ideological factors and pose a threat to cybersecurity and social stability. As network technology continues to evolve, these organizations' tactics and strategies may also continue to change. for example, in China, offering free circumvention services to attract students to forward ideologically-charged advertisements or share certain botnet services.

4 Enhancing Network Security Strategies

With the widespread application of big data, artificial intelligence, and internet technologies across all aspects of society, campus network security faces new challenges. Deploying network security equipment such as firewalls, intrusion detection systems, and antivirus software is crucial to protect school networks. Employing encryption for storage and transmission of critical data prevents data leaks. Regularly scanning the network system for security vulnerabilities and promptly patching those vulnerabilities are also essential. Given the special environment of the campus and the fundamental mission of schools to cultivate virtue and talent, the campus cybersecurity system should be different from those of enterprises and governments. The campus cybersecurity system should integrate ideological and political elements, with moral persuasion as the core and technology and skills as the means, and develop persistent and dynamic cybersecurity education strategies. At present, it is necessary to establish a cybersecurity team to coordinate with various departments. A stable working group can ensure the persistence and dynamism of cybersecurity education strategies. At the same time, a cybersecurity framework should be deployed, coordinated and handled by the working group and various departments, at least including the following areas: a stable and reliable identity recognition system and a strict permission system with log backups. A software and hardware security detection system and immediate repair of vulnerabilities and removal of malicious codes. An anti-fraud monitoring and regular training program to popularize cybersecurity knowledge. A campus public opinion monitoring system to promptly detect inappropriate remarks and disciplinary violations, and take mild corrective measures with the aim of care and persuasion. Finally, it is necessary to ensure the appropriate isolation of the above systems. Campus security is not about comprehensive monitoring measures. The privacy and appropriate self-discipline space of individuals and organizations should be respected. Sensitive information should be isolated and encrypted in a black box, and the above tasks should be completed as unobtrusively as possible. Continuously improving a unified identity authentication platform to perform centralized authentication for school information systems, ensuring user authenticity. Implement strict access control based on user roles and permissions to prevent unauthorized access to sensitive data. Enhance network security management systems by establishing permission levels within administrative and academic operations, and continuously upgrade the identity recognition system. Clearly define network security responsibilities for each department and establish a network security incident response mechanism. Regularly inspect and assess network security efforts to promptly identify and resolve potential risks, ensuring the safe continuation of teaching and research

activities. Teaching and research increasingly depend on IT resources such as online learning platforms, digital libraries, and laboratory data sharing. Network security issues could disrupt these activities or lead to data loss, impacting teaching quality and research progress. Ensure faculty and students understand and master basic network security knowledge and enhance their awareness of prevention through various methods like hosting cybersecurity lectures or elective courses, distributing security manuals, and conducting knowledge competitions. Record anomalous access attempts, such as immediately alerting administrators to unusual activity, preventing unauthorized modification of student grades. Establish policies for protecting the personal information and privacy of faculty and students. The school’ s information systems store a large amount of personal data, including names, ID numbers, contact details, grades, and employment information. Relevant teaching and counseling staff have an obligation to protect this sensitive information and bear appropriate responsibility for any privacy violations or financial losses that may occur.

References

[1] Christopher C. Elisan. Malware Rootkits & Botnets: A Beginner’ s Guide [M].McGraw-Hill Education, 2013:31-36.
[2] Mensch,Scott,Wilkie,Le Ann,Information Security Activities of College Students:AnExploratory Study[J].Academy of Information and Mangaement Sciences Journal,2011, 14 (2) : 61-63.
[3] Liu Junyu. Research on the Integration of Network Behavior Analysis and Zero Trust Network [J]. Cybersecurity and Information Technology, 2024, (12): 128-130.
[4] Yu Fengyuan. Research on Countermeasures for Improving College Students' Cybersecurity Education in the New Media Era: A Case Study of Dalian [D]. Dalian: Dalian University of Technology, 2022.