Universe
Scientific Publishing

Analysis of Computer Network Information Security and Protection Strategies

Dachuan Tian

Chengdu City, Sichuan Province 610000, China.

Abstract: With the rapid development of modern science and technology, computer technology has been widely applied in various fields of construction in China, playing an important role. However, in practical development, it is precisely because network platforms have the characteristics of virtuality and openness that it is easy to encounter various security issues in the use of computers. This not only brings a lot of inconvenience to users' work and life, but also may pose serious security threats to their privacy and property. Therefore, we must attach great importance to the issue of computer network information security, continuously strengthen security protection, so that the property and privacy of users can be respected and effectively protected.

Keywords: Computer; Network; Information Security; Protection Strategy

Entering a new era of development, China's computer network information technology has greatly improved, playing an indispensable role in people's production and life. It brings great convenience to people, but also poses great challenges to their property and privacy security. Therefore, in the development of modern society, people are paying more and more attention to computer network security issues. It is necessary to strengthen the attention and exploration of computer network information security issues, further do a good job in computer network information security protection, effectively protect the information security of users, and maintain the order of the online world.

1. Briefly describe the important value of computer network information security and protection measures

From the current social development, many fields attach great importance to the application of computer network information technology and are committed to creating intelligent development systems in various fields. It is precisely because the information dissemination of the Internet has enormous development advantages, such as wide dissemination range and fast dissemination speed, which have strong sharing, that it has been widely used in real life, bringing great convenience to people. However, computer network technology is not perfect in its development, and its inherent technical vulnerabilities often lead to many security issues. Objectively speaking, these security issues mainly arise at the technical and operational management levels, such as malicious hacker attacks, virus spread, information theft, etc. The security issues in operation and maintenance mainly come from the application and management of computer network information technology systems, such as poor hardware equipment management and control. In the new stage of development, computer network information technology needs to continue to optimize and upgrade in terms of security prevention and control, actively create a secure network environment, and meet the actual needs of computer users.

2. Exploring Computer Network Information Security Issues in the New Era

2.1 Security issues arising from cyber hacking attacks

In the current application process of network technology, hacker attacks are often encountered, posing a serious threat to network information security. Hacker attacks are not uncommon in the online world and can often cause significant harm to users. In practical development, hackers carrying out attacks on computer systems can easily lead to the leakage of personal privacy in user computers, or the theft of important business secrets and research results in enterprises. The economic losses and adverse effects caused by these attacks are often enormous. The economic losses caused by hacker attacks reach billions of dollars annually internationally. It can be seen that continuously strengthening the prevention and crackdown on hacker attacks is not only a practical need to maintain network security, but also a practical need to protect the vital interests of the vast number of Internet users. In the world of the Internet, besides hacker attacks, computer viruses are also a common security issue. The prominent feature of computer viruses is their fast propagation speed and strong destructive power. They can also cause serious attacks and damage to computer network systems. Once a computer system is infected with viruses, it is difficult to completely eliminate them, especially for some new viruses with strong infectivity. They can invade every link of the computer in a short period of time, not only causing the entire computer system to be paralyzed, Unable to continue working normally will also cause incalculable economic losses to users. In addition, some computer viruses are relatively secretive and often rely on email, instant messaging software, and other means to achieve remote control, which can lead to information leakage. In addition, in real life, spam messages, malicious plugins, and harassing phone calls are all hidden dangers in computer information security. These junk messages not only have no useful value, but also occupy a large amount of communication resources, and even induce users to click on phishing websites or install Trojan programs, affecting the normal operation and use of computer systems.

2.2 Security issues related to data loss

After entering the era of big data, the development of almost every industry cannot do without the support and assistance of computer network technology. In the process of practical application of computer network technology, a large amount of user personal information is stored on the cloud server. These personal information not only include basic personal information such as name, phone number, ID card number, education background, but also include important information such as bank cards bound to individuals. Once embezzlement or disclosure occurs, it is likely to bring great adverse effects to users. In addition, we all know that cloud computing has the characteristics of strong elasticity and scalability, convenient resource sharing, etc., which gives hackers the opportunity to obtain more user data through illegal means and illegally exploit it, thereby posing a serious threat to the public security of the entire society. In real life, some other unexpected situations may also cause data loss, such as hardware failures, software vulnerabilities, improper human operations, etc. Data loss caused by virus intrusion or malicious program tampering is also quite common. Objectively speaking, the risk of data information stored in the cloud has greatly increased, and it is always at risk of being stolen or tampered with. Once these data successfully fall into the hands of criminals, they are likely to use the data information to engage in some illegal activities, such as fraud, extortion, etc., which may seriously threaten the stability and security of society.

2.3 Security issues related to network viruses

In the new era of development, people’s dependence on computer network technology in daily life is gradually increasing. However, the emergence of network viruses has brought serious challenges to network security. These viruses can enter users’ computer systems through various means, steal personal privacy information, or steal commercial secrets. The biggest characteristic of network viruses is their strong concealment, destructiveness, and contagiousness, which can seriously hinder the normal operation of computers and cause varying degrees of losses to users. The current network viruses are mainly divided into two types. Firstly, active viruses refer to viruses that can self replicate and spread quickly. Secondly, passive viruses mainly refer to viruses with weak self replication ability that require the use of some media for transmission. Both of these viruses are partially strong and can cause serious damage to computer systems.

2.4 Network monitoring security issues have occurred

In the face of complex network environments, it is necessary to strengthen the construction of network monitoring systems in order to effectively improve the security of network information. So far, China has continuously made new progress in the construction of network monitoring systems, but there are still certain loopholes in the construction. For example, some monitoring devices have limited intelligence and need to be strengthened in terms of recognition ability in order to timely detect malicious software or Trojan programs; The current monitoring technology has a certain degree of lag and cannot fully and effectively respond to various network attacks. Therefore, we need to make active efforts in network monitoring, continuously upgrade monitoring technology, and enhance the actual effectiveness of responding to network attacks.

3. Effective Strategies for Computer Network Information Security Protection in the New Era

3.1 Further strengthen awareness of network security

In today's social development, people's dependence on internet technology is gradually increasing. In order to effectively protect the vital interests of users, it is necessary to actively explore effective measures to deal with various network security threats on the Internet. One of the most crucial points is to enhance the awareness of network security among netizens. Firstly, utilizing various means to strengthen the promotion and education of cybersecurity knowledge, so as to raise awareness of the close relationship between enhancing cybersecurity and personal interests. Secondly, relevant government departments must attach importance to the supervision of network security, continuously increase law enforcement efforts, and severely crack down on and punish illegal behaviors that seriously threaten network security. Thirdly, the general public should also strengthen students, consciously learn and master certain knowledge of network security, and continuously enhance their awareness of prevention. For example, they should not click on links and QR codes of unknown origin at will, in order to protect their own network security to the greatest extent possible.

3.2 Pay attention to setting certain access permissions

In the process of using a computer, setting certain access permissions is one of the effective measures to enhance its network security, which can effectively avoid network intrusion. In the era of informatization, a large amount of data information is flooding the network, and many users need to process relevant data information according to their actual needs. Based on the different responsibilities of users, different access permissions are set to avoid unauthorized personnel from accessing and retrieving relevant information, which greatly improves the security of network information. In addition, in the early stage of setting access permissions, it is necessary to accelerate the construction of a control access system and enforce audit services. If there is an error in the access password, an alarm signal will be issued in a timely manner, and it is strictly prohibited to apply for network access again.

3.3 Emphasize the development of computer network monitoring work

In the process of exploring and improving computer network information security, doing a good job in computer network monitoring is also one of the effective measures to enhance network information security. In the current social development, effective network monitoring of computers mainly relies on monitoring network intrusion technology, which requires the use of data information to identify user information. However, this technology can only play its functional role during computer operation. In other words, monitoring network intrusion technology requires the use of network monitoring to maintain computer network security and prevent data information from being stolen from computers.

3.4 Emphasize the application of network security technology

To effectively enhance the security of computer network information, the key is to continuously enhance one's own defense capabilities. Firstly, by utilizing encryption technology to enhance the security of user information, important information such as personal privacy and trade secrets can be effectively protected. To leverage the advantages of encryption technology, relevant technical personnel need to master and apply various advanced encryption algorithms and key management systems proficiently through professional skills and work experience, in order to ensure the security of various information during transmission. Secondly, establish a sound firewall system. The establishment of a firewall mainly involves real-time monitoring of external network connections, timely detection of non security factors, and taking corresponding preventive measures to ensure network security.

4. Conclusion

In the era of informatization, computer network information security is not only related to the normal development of many industries, but also to the sustainable development of the entire society. Strengthening computer network information security is of great significance.

When maintaining the security of computer network information in practice, it is necessary to base ourselves on objective reality and constantly explore various effective protective measures, so that the security of computer network information can be truly implemented.

References

[1] Yang Yue Research on Computer Network Information Security and Protection Strategies [J] Office Automation, 2023, 28 (22): 19-21.

[2] Zhao Shenglong, Song Wenbin Analysis of Computer Network Information Security and Protection Strategies [J] Electronic Technology, 2023, 52 (10): 178-179.

[3] Yu Keshi Research on Computer Network Information Security and Protection Strategies in the Era of Big Data [J] Information Systems Engineering, 2023, (09): 130-133.

[4] Wei Xiaowei Computer Network Information Security and Protection Strategies Based on Big Data [J] Electronic Technology, 2023, 52 (08): 49-51.

[5] Li Wei Analyzing Information Security and Protection in Computer Networks [J] Network Security Technology and Applications, 2023, (08): 167-168.

[6] Jin Lufeng Analysis of Computer Network Management and Information Security Strategies [J] Integrated Circuit Applications, 2023, 40 (08): 406-407.