COMPUTER APPLICATION ANALYSIS UNDER THE MANAGEMENT OF NETWORK INFORMATION SECURITY TECHNOLOGY

Xiaoqin Yang[1*], Leelavathi Rajamanickam[2], Hui Wang[3], Wang Shi[4]

Abstract:
Due to the Internet age, network information has achieved all-round penetration into people's social life. However, while the emergence and development of the Internet has brought convenience and other positive effects to people's life and work today, it has also caused a series of network information security issues. Therefore, how to use network information security technology to effectively eliminate these network security problems and create a safe network environment for network users has become a top priority. On the basis of elaborating the forms and causes of information security problems existing in the current network environment, this paper further analyzes the computer application strategy under the management of network information security technology.

Keywords: computer application, network security, information management

[1*]PhD Research Scholar, Faculty of Engineering, Built Environment & Information Technology College of Computer and Communication Engineering, SEGi University, Nanjing Tech University Pujiang Institute, Kota Damansara, Malaysia Nanjing, China, Email: yangyxqcsy@163.com
[2]Centre for Software Engineering, Faculty of Engineering, Built Environment & Information Technology SEGi University, Kota Damansara, Malaysia, Email: leelavathiraj@segi.edu.my
[3]College of Computer and Communication Engineering, Nanjing Tech University Pujiang Institute Nanjing, China Email: chnhwang@163.com
[4]Public Education Department line, Hainan Vocational University of Science and Technology, Haikou, China Email: ws10121@126.com

***Corresponding Author:** Xiaoqin Yang
[*]PhD Research Scholar, Faculty of Engineering, Built Environment & Information Technology College of Computer and Communication Engineering, SEGi University, Nanjing Tech University Pujiang Institute, Kota Damansara, Malaysia Nanjing, China, Email: yangyxqcsy@163.com

DOI: - 10.48047/ecb/2023.12.si5a.0271

INTRODUCTION

The use and popularization of Internet technology canbe said to be one of the greatest applications in the 21st century, and its emergence is a strong guarantee for the current social progress and development. The wide range of applications and powerful effects of Internet technology are unmatched by other science and technology. However, during the operation of the computer, there are always some criminals who destroy the network information, which not only affects the normal network experience of the user, but also may steal the user's personal information to do some illegal activities, which brings great harm to the user's information security big threat. Therefore, it is very necessary to ensure the network information security of each user, strengthen the management of network information, and conduct in-depth research on network information security. From the gradual popularization of computer equipment to the wide application of Internet technology to the arrival of the era of big data, people's work and lifestyle have undergone tremendous changes compared with the past.

1. SYMPTOMS OF COMPUTER NETWORK IN FORMATION SECURITYP ROBLEMS

However, it is worthy of people's vigilance that the development of modernity does not always bring positive benefits to human society, such as increased work efficiency and more colorful life. Along with this, there is also the security of network data information hidden dangers. The current network information security problems not only damage the rights and interests of the majority of network users, but also restrict the further development of computer network technology[1].Therefore, the management of network information security technology in computer applications should be strengthened. While creating a safe network environment for network users, it also provides a more suitable network environment for the continued development of computer network technology.

Computer network information security problems include these problems. First, the problem of computer virus infringement. For a long time, the problem of computer virus damage to computer systems has been a network information security problem that cannot be ignored. It not only spreads widely, but also has the characteristics of strong repetition. Experience of virus infestation. The manifestations of computer viruses are extremely active, and they have a variety of virus types, and at the same time, different types of viruses can cause different damages to computer equipment. Given that computer viruses have a series of characteristics such as various virus types and forms of infringement, long incubation period, strong transmission and destructive power, people have not been able to effectively prevent and completely eliminate computer viruses, which is a network information security problem.

Second, the problem of malicious attacks by computer hackers. With the progress and development of science and technology, computer hackers are also a large number of existences in today's society. It exists in the form of an individual, that is, exists alone in the form of an individual, and the individual acts alone when maliciously attacking the target of attack; The malicious attacks constitute organized collective criminal activities[2].However, corresponding to the existence of rampant hacker groups,it is an open network environment. As a result, the network environment is more vulnerable to malicious intrusions by hackers, and ineffective preventive measures lead tothe fact that the police can only protect against malicious attacks by hackers. Tracking its location after the implementation is completed is obviously not good for the arrest of criminal suspects, and it takes a lot of energy and time, which makes the current network information security situation even more worrying.

Third, the vulnerability of computer software. In view of the immediacy and other limitations of computer software in design, computer software will gradually expose some of its loopholes as time goes by during use, and this brings criminals such as computer hackers. Opportunity to practice one's own illegal intentions—to use loopholes in computer software to illegally intrude into computers or network systems to steal information. At the same time, the rapid development of computer and network technology and the substantial increase of network users will inevitably lead to a substantial increase in the number and frequency of use of computer software. In this way, if the loopholes of computer software are exploited by criminals, it will cause great damage to the security of the network environment, such as serious network security problems such as personal or corporate user privacy leaks.

Fourth, political and illegal forces are rampant on the Internet[3].As the so-called network connects

the world, the information security problem in the network does not only originate and exist in the domestic field. In recent years, with the high popularity of computers and network applications, some foreign illegal forces have colluded with domestic reactionary forces to take advantage of the openness of the network. In the domestic society, the fallacies and heresies that are not conducive to the current social stability and the unity of the people are widely spread in the domestic society, which has an extremely adverse impact on the maintenance of the current good social order. Faced with such abominable nature and extremely high frequency of illegal activities, there are still no effective measures to completely curb them.

Although the current Internet is relatively open, the information saved by users on the Internet is generally strictly confidential. For that private information, strangers cannot obtain and know through normal means. For the confidential documents of some relevant departments, there are layers of defenses, and generally they will not be stolen. However, lawbreakers such as lawless hackers, affected by interests and other factors, use some illegal technical means to use virusesand security holes to invade other people's computer programs without the user's consent, so as to obtain theuser's private information, and then use user information for profit exchange or other illegal activities. In essence, the network is the exchange and storage of different users and various types of information, which brings great convenience to humanwork and life.

In the Internet, all kinds of information are the basicmanagement content and objects. Therefore, the primary requirement of the Internet is to ensure the security of network information, and now with the continuous development of science and technology, some criminals will use some unconventional means to tamper with the normal information of users, and because the methods of modification by criminals are very rich, Moreover, some users do not understand the rules and formats of some network information, so some tampered network information is difficult to be discovered in time. If some wrong network information is used, it may cause great losses to users[4].Of course, because the tampered information is different, the consequences that can be caused are also different in severity. However, any illegal tampering of user network information should be severely punished.

2. THE REASONS FOR THE FORMATION OF NETWORK INFORMATION SECURITY PROBLEMS

Then, we must really want to know what the reasons for the formation of network information security problems are. First, from the perspective of computer viruses, they have the characteristics of various types of viruses, long incubation periods, and strong transmission capabilities. As a derivative of the Internet age, computer viruses have also driven the change and development of computer viruses with the advancement of network technology—the types and transmission routes of computer viruses are becoming more and more diverse, spread and also developed the function of sneaking in first and then starting it by itself,that is, sneaking into the computer system first without being noticed by others, and then waiting for an opportunity to attack and destroy the kernel system of the computer. When the situation is serious, It can even cause the computer system to be paralyzed, making it unable to operate normally.

Second, from the perspective of the network environment, it has the characteristics of openness. Thereason why the network environment is open is that network information has the characteristics of high- speed dissemination and sharing. Although the emergence and development of computer and network technology has promoted the overall progress of society to a certain extent and provided great convenience for people's life, the negative impact it brings, that is, the issue of information security cannot be ignored. To a certain extent, we can say that an open network information environment is a hotbed for lawbreakers to carry out illegal and criminal activities. For example, in terms of information transmission, the lack of application of network information security technology and the lack of information security awareness of network users Under the circumstances, if criminals steal the confidential information of computer users and use it illegally after stealing, it is conceivable that this behavior will cause great damage to the vital interests of computer users[3].

Third, from the perspective of personnel training, there is still a lack of a reasonable personnel training mechanism. However, if the computer network information security work wants to make substantial progress, it is absolutely inseparable from the cultivation of cutting-edge talents in computer network technology. Since the emergence of computer technology is still relatively short, the current training mechanism

for professionals in the computer field still needs to be improved, and the talent team in the computer field needs to be strengthened urgently. In such a situation where cutting-edge talents in related fields are extremely scarce, it is really difficult to make progress in the research and development of network information security technology. Therefore, we should increase investment in the training of computer talents. At the same time, in order to avoid the phenomenon of computer brain drain, we should further improve the treatment of cutting-edge talents in the computer field and improve the systems related to computer talents. such as the salary system.

Fourth, in terms of unit management, there is still a lack of a complete security mechanism. The incompleteness of the security prevention mechanism is mainly manifested in two aspects: firstly, the relevant laws and regulations to ensure network information security and some units' security work management systems are not perfect; secondly, the existing laws andregulations lack sufficient feasibility. Due to the imperfection of these management systems and relatedlaws and regulations, it not only leads to the ineffectiveness of the internal security management work of the unit, but even illegal behaviors originated from the inside, and it is also extremely detrimental to the information security work of the entire network environment. The earth threatens the security of network users, including the transmission and storage of private information of individual users and enterprise users.

Nowadays, network information security has become a common problem all over the world. With thecontinuous development of society, more and more people have begun to pay attention to the issue of network information security[4].Some countries have passed legislation to address a series of issues related to network security. Make clear instructions and specifications.

3. THE COMPUTER APPLICATION ANALYSIS UNDER THE MANAGEMENT OF NETWORK INFORMATION SECURITY TECHNOLOGY

Regarding the computer application analysis under the management of network information security technology, we can analyze it from the following aspects First, the application of anti-virus technology in computers. As a computer hardware technology, antivirus technology includes three parts: virus prevention technology, detection technology and removal technology. Its working principle in the computer is: cooperate with the operating system of thecomputer, the two work together to fight against the attack of computer viruses, and protect the computer loopholes. AS far as virus prevention technology is concerned, its working principle is to use technical means to prevent computers from being infected with viruses and prevent viruses from invading and destroying computer equipment. This technology has the characteristics of strong practicability. The working principle of the so-called virus detection technology is to use information technology as a means to identify and detect computer viruses. If the existence of computer viruses is detected in the computer system, the corresponding virus processing function will be activated for the virus type. There are two identification and detection objects of this technology, one is the entire computer virus program, the detection content includes the characteristics of the virus, the mode of transmission, the second is the file or data segment, which will not only be regularly or irregularly. After the detection is completed, the detection results will be saved and compared continuously, so as to check the abnormal situation of the data in time, and take effective solutions to the abnormal situation to prevent the virus from causing further damage to the file.

Second, the application of intrusion detection technology in computer. Among all the current network information security technologies, intrusion detection technology also has a better effect on computer network protection[5].The normal operation of this detection technology in the computer is based on the intrusion detection system. The so-called intrusion detection system refers to a system composed of software and hardware, which aims to check all behaviors that violate computer security policies in the computer network play an extremely important role. The protection principle of the intrusion detection technology based on this detection system is to analyze various indicators in the computer operating system. There are two main detection modes of intrusion detection technology: one is anomaly detection mode, and the other is misuse detection mode. As a technology aimed at protecting network information security, the object of its detection and investigation must be various abnormal behaviors that intrude into the computer network, abnormal intrusion behaviors that exist in computers, or things that exist in computer operating systems such as security logs. Once the abnormal items in the indicators are detected by the detection technology, there will be

a prompt alarm signal, so that the computer operator can deal with the abnormal behavior in time, so as to ensure the security of network information[6].

Third, the application of identity verification technology in computers. The so-called identity verification technology refers to the confirmation of the identity of the computer network operator through certain data identification technology means, so as to eliminate the possibility that the operator is an illegal intruder, and ensure that the current computer operator is capable of obtaining and accessing the network information. permission to use. This technology adopts a one-to-one mode for identity authentication of computer network operators, which is highly targeted, so it can effectively prevent the illegal intrusion of criminals and the leakage of network user information.No matter for individual users or enterprise users, this technology can play a good role in protecting their private information. Among the three identity verification methods of identity authentication technology, the most widely used is the information secret verification method, and the most secure performance is the biometric identity verification method. However, because this method still has certain application disadvantages, such as high application cost and complicated operation process, it has not yet been widely used among network users.

Fourth, the application of information encryption technology in computers. IN the application process of computers, information encryption technology also plays an extremely significant role. The so-called information encryption technology refers to the use of mathematical or physical techniques to encrypt software in different forms during the transmission andstorage of network information, such as the use of computer keys, so as to protect network information[6].In the actual application of this technology, it is best to use it in combination with the network user's own user password. In this way, the private information of network individuals or enterprise users can be double-protected, and the network information can be effectively protected. The protection effect is better.

Fifth, the application of firewall technology in computers. Firewall technology is the most widely used network information security protection technology under current conditions. The main task and function ofthis technology is to eliminate insecure factors in the network and protect the internal network. Specifically, there are two main forms of protection of network information by firewall technology: one is to protect thesecurity of internal network information by preventing unauthorized external network users from illegally invading the internal network and stealing userinformation. The second is to improve the security level of network information by adopting a combination of full blockade and partial opening of internal network information, so as to realize the protection of network information.

CONCLUSION

It can be seen that the emergence of the Internet hasbrought convenience to people's work and life, and a series of network information security problems such as computer virus infringement, computer hacking, and computer software loopholes have come with it. In order to create a more secure network environment, it is imperative to find out the causes of these network information security problems and analyze them, and then propose solutions in a targeted manner, and apply various information security protection technologies to overcome these problems and provide network security. Information security escort. With the advent of the Internet era, network information has achieved all- round penetration into people's social life. However, while the emergence and development of the Internet has brought convenience and other positive effects to people's life and work today, it has also caused a series of network information security issues. Therefore, how to use network information security technology to effectively eliminate these network security problems and create a safe network environment for network users has become a top priority. On the basis of elaborating the forms and causes of information security problems existing in the current network environment, this paper further analyzes the computer application strategy under the management of network information security technology.

The level of development of the Internet industry isgetting higher and higher, and the application of computers in human society will continue to deepen inthe future. It is particularly important to strive to strengthen the security and standardization of computer use, and to continuously optimize the security management of network information. Therefore, network security issues should be resolved to the greatest extent, and computer applications should be continuously explored in order to ensure that the

Internet can continue to operate normally and safely.

REFERENCES

1. Wang Jieming. Discussion on Computer Application of Network Information Security Technology Management /Jieming. Wang // J. of the computer science.– 2018.–Vol.20, iss.4.–P.147
2. Yuan Weiwei. Be based on Computer Application of Network Information Security Technology Management / Weiwei. Yuan // J. of the wireless internet technology.– 2015.–Vol.12, iss.15.–P.123-124
3. Wang Xioaning. Thinking of Computer Application Based on Network Information Security Technology Management/Xiaoning. Wang//J. of science and technology economy market.–2017.–Vol.107, iss.4.–P.40-41
4. Feng Hai. Computer application analysis/Hai. Feng//J. of the technology.–2012.–Vol.23, iss.3.–P.123-124
5. Jin Hao. Computer application analysis under the management of network information security technology/Hao. Jin//J. of the computer science.–2016.– Vol.23, iss.4.–P.54-57
6. Liang Bing. The management of network information security technology/Bing. Liang//J. technology.–2019.– Vol.5, iss.3.–P.12-16