ISSN 2616-7433 Vol. 5, Issue 13: 27-31, DOI: 10.25236/FSST.2023.051305

Challenges and Construction of Social Trust in the Internet Era — A Case Study of Information Security

Yuanyuan Fu

Zhengzhou University of Industrial Technology, Zhengzhou, Henan, China
2676004157@qq.com

Abstract: *In this era of deep internet penetration into daily life, information security issues have profound effects on the construction of social trust. Problems such as cybercrime, information leakage, and privacy infringement seriously undermine public trust in the internet. Therefore, establishing and improving an information security system to protect the public's information security and enhance trust in the internet becomes an essential task. This paper analyzes the impact and challenges of information security on social trust in the internet era, explores how to establish and improve the information security system, and proposes the responsibilities and coping strategies for governments, enterprises, and individuals in information security to promote the construction of social trust.*

Keywords: *Internet era; Cyber fraud; Social trust; Information security*

1. Introduction

With the advent of the information age, the internet has deeply integrated into various aspects of our daily lives, including work, study, and personal activities. In this era of information explosion, social trust becomes a crucial link that connects individuals and institutions. Social trust can be defined as the positive expectations that individuals hold towards other individuals or institutions in society, despite a lack of sufficient information. It is a vital component of social relationships and plays a critical role in the stability and harmony of society.

In the internet era, the importance of social trust becomes even more evident. The internet has broken the barriers of time and space, enabling information to spread at an unprecedented speed and scope. However, this has also brought about new challenges, such as information security issues and cyber fraud, posing threats to social trust. Social trust in the internet era not only involves the protection of personal privacy and information security but also concerns the fairness and stability of social justice and order. Therefore, researching social trust in the internet era and addressing the challenges it faces are of significant importance in constructing a more harmonious and secure cyberspace society.

2. Challenges of Social Trust in the Internet Era

The development of internet technology undoubtedly brings convenience to our lives, revolutionizing how people communicate and access information. However, accompanying these advancements are increasingly prominent social issues, especially concerning information leakage and cyber fraud, which seriously affect the societal trust mechanism. Below, we will explore these two problems in detail.

2.1. Information Leakage

2.1.1. Risks of Personal Privacy Leakage

In the internet era, the leakage of personal information has become a severe social problem. From individual names, phone numbers, and addresses to banking card information and even biometric data, once these sensitive details are leaked, they may pose serious threats to individuals' lives, work, and safety. For instance, personal information leakage can be exploited for identity theft, telephone fraud, and other criminal activities, causing individuals to suffer financial losses and tarnishing their reputations. This poses a significant threat to societal trust [1].

2.1.2. Risks of Business Information Leakage

The leakage of business information is also a perilous issue. Business information includes, but is not limited to, a company's business strategies, product designs, financial data, etc., which are critical to the company's competitive position. Once such information is leaked, it can be exploited by competitors, causing severe economic losses to the company. Such losses may also, to some extent, affect societal stability and public trust in the company.

2.2. Cyber Fraud

2.2.1. Main Forms and Harms of Cyber Fraud

Cyber fraud is a significant social problem in the internet era. It leverages the convenience and anonymity of the internet to carry out fraudulent activities, causing substantial economic and psychological harm to the public. Cyber fraud takes various forms, including but not limited to fake shopping websites, scam emails, phishing websites, and false investments.

Fake Shopping Websites: This form of fraud typically entices consumers to make purchases at extremely low prices. However, after payment, consumers may receive inferior goods or nothing at all. This type of fraud causes financial losses to consumers and damages their trust.

Scam Emails: Scammers deceive users by sending emails containing malicious links or attachments. Once users click on the links or open the attachments, sensitive information such as bank accounts and passwords may be stolen, or their computers may be infected with malicious software.

Phishing Websites: This is a very common form of cyber fraud. Scammers create phishing websites that closely resemble genuine websites to lure users into entering personal information such as usernames, passwords, and banking details, which they use for illegal activities.

False Investments: Fraudsters often attract the public to invest by promising high returns. However, these so-called investment projects either do not exist or are high-risk ventures, leading investors to lose all their investments.

Cyber fraud not only causes financial losses to the public and poses risks to public and social security but also exacerbates social conflicts and undermines the internet's security and trust environment, shaking social stability.

2.2.2. Impact of Cyber Fraud on Social Trust

The damage caused by cyber fraud to social trust is profound and widespread. In today's globalized world, the internet has become a crucial platform for human society to communicate, learn, work, and live, serving as a vital tool for various social activities. However, the rampant development of cyber fraud not only harms the economic interests of individual users but also seriously undermines the social trust system.

Firstly, cyber fraud has led the public to feel panic and distrust towards the internet. People have become skeptical and fearful of online transactions, worrying about the safety of their personal information and financial assets. This phenomenon hinders the healthy development of the internet and obstructs the widespread adoption and promotion of a range of internet services such as e-commerce, online payments, and cloud services [2].

Secondly, cyber fraud also damages trust relationships between individuals. In traditional transaction models, the parties involved can usually talk face-to-face and exchange goods, which facilitates a relatively quick establishment of trust. However, in online transactions, the parties often cannot have direct contact and can only rely on electronic information to understand each other, making trust-building more difficult. The existence of cyber fraud makes people more cautious and distrustful in online transactions, creating additional stress when dealing with the idea that the other party may be a fraudster.

Lastly, cyber fraud shakes public trust in the law and government. Although the government has implemented a series of laws and regulations to combat cyber fraud and protect public online security and rights, the concealment, complexity, and cross-border nature of cyber fraud often make it challenging for law enforcement agencies to trace and convict criminals. As a result, people begin to question whether the law and government can effectively protect their rights.

3. Constructing Social Trust: Taking Information Security as an Example

3.1. Establishing a Sound Information Security System

The establishment of an information security system is crucial for reshaping social trust. A comprehensive information security system requires not only robust legal support but also advanced technological means and widespread social education.

3.1.1. Establishment and Improvement of Cybersecurity Regulations

Cybersecurity regulations are critical to ensuring online security and preventing cybercrimes. With the development of the internet and the increase in cybercrimes, governments worldwide recognize the importance of establishing and improving cybersecurity regulations.

Firstly, governments need to provide clear legal definitions and provisions for cybersecurity, specifying what constitutes cybercrimes and what constitutes legal online behaviors. This will provide a clear legal basis for combating cybercrimes. Moreover, regulations need to be established to govern the collection, use, storage, and dissemination of online information, protecting personal privacy and preventing the misuse of personal information.

Secondly, governments should enact strict legal sanctions against cybercrimes. This includes imposing severe criminal and civil penalties to create a sufficient deterrent against cybercrimes. Additionally, for cross-border cybercrimes, international cooperation is essential. This can be achieved through the development and implementation of relevant international legal provisions to collectively combat cybercrimes.

Finally, establishing dedicated cybersecurity regulatory agencies is also crucial. These agencies can be responsible for daily cybersecurity supervision, including early warnings of cybersecurity threats, investigating cybercrimes, and collecting evidence for prosecution. Through specialized cybersecurity regulatory agencies, the enforcement of cybersecurity regulations can be strengthened, better safeguarding public online security.

3.1.2. Development and Application of Cybersecurity Technology

Technology is a crucial means to safeguard cybersecurity. With the advancement of science and technology, cybersecurity technology has also been continuously improving and plays a significant role in preventing cybercrimes and protecting online security.

Firstly, the application of fundamental cybersecurity technologies such as network encryption, firewall, and intrusion detection serves as the first line of defense against cybercrimes. These technologies can effectively prevent network attacks and protect the security of online information.

Secondly, with the development of artificial intelligence and big data, data analysis and machine learning technologies are becoming increasingly widespread in the field of cybersecurity. By analyzing vast amounts of network data, machine learning models can effectively identify and predict cybercriminal behavior, providing essential technical support in preventing cybercrimes.

Finally, emerging cybersecurity technologies such as blockchain and quantum encryption are also gradually being applied. These technologies can provide higher levels of network security protection and offer effective solutions to future cybersecurity challenges.

3.1.3. Conducting Cybersecurity Education

Cybersecurity education is a vital means to enhance public awareness of online security and prevent cybercrimes.

Firstly, educational institutions need to incorporate cybersecurity education into the basic education system, ensuring that students at all levels, from elementary to higher education, receive systematic cybersecurity education. Through learning, students can understand the dangers of cybercrimes, acquire fundamental cybersecurity knowledge and skills, and develop good online behavioral habits.

Secondly, for adults, the government can raise public awareness of cybersecurity through public service advertisements, cybersecurity awareness months, and other activities. Additionally, various cybersecurity training programs can be conducted to enhance public cybersecurity skills.

Finally, for businesses, the government can promote cybersecurity education and training through policy guidance, raising employees' awareness and skills to prevent enterprise-level cybercrimes.

In conclusion, cybersecurity regulations, cybersecurity technology, and cybersecurity education are the three critical means to prevent cybercrimes and protect online security. Continued efforts in these areas are necessary to enhance cybersecurity and maintain social trust.

3.2. Responsibilities and Response Strategies of the Government, Businesses, and Individuals

Information security is not only a technical issue but also a societal problem. Therefore, the government, businesses, and individuals all need to shoulder their respective responsibilities and adopt effective strategies to address the challenges of information security and rebuild social trust.

3.2.1. Government Responsibilities and Response Strategies

The government bears significant responsibilities in maintaining cybersecurity. Firstly, the government needs to establish and enforce comprehensive and strict cybersecurity regulations, imposing severe penalties for cybercrimes, and providing legal safeguards for cybersecurity through judicial means. This includes defining cybercrimes, setting standards for conviction and sentencing, establishing comprehensive cybersecurity regulatory agencies and systems, and formulating and implementing cybersecurity regulatory policies and action plans.

Secondly, the government needs to actively promote research and application of cybersecurity technology. The government can encourage and support the development of cybersecurity technology through providing research and development funding, setting up research projects, and promoting public-private cooperation. At the same time, an effective technology promotion mechanism should be established to encourage widespread application of cybersecurity technology throughout society.

Lastly, the government needs to take responsibility for cybersecurity education, utilizing various methods to raise public awareness of cybersecurity. This can be achieved through educational institutions, public awareness campaigns, training, etc., to help the public understand the importance of cybersecurity and acquire necessary knowledge and skills. [3]

3.2.2. Business Responsibilities and Response Strategies

As providers of online services and products, businesses also bear significant responsibilities for cybersecurity. Firstly, businesses need to establish and improve their own cybersecurity systems, including cybersecurity management systems, technical protection measures, emergency response mechanisms, etc., to ensure the security and reliability of their online services and products.

Secondly, businesses need to provide cybersecurity training to their employees, raising their awareness and skills in cybersecurity to prevent cybersecurity incidents caused by employee errors. Additionally, businesses should formulate and enforce strict information security policies to protect users' personal information and trade secrets, safeguarding users' legitimate rights and interests.

Lastly, businesses need to actively cooperate with government cybersecurity oversight. This includes conducting regular cybersecurity audits, promptly reporting cybersecurity incidents, and supporting strict measures against cybercrime.

3.2.3. Individual Responsibilities and Response Strategies

Individuals are users of online services and the last line of defense for cybersecurity. Firstly, individuals need to enhance their cybersecurity awareness, understand common cybercrime methods, use online services correctly, and prevent themselves from becoming victims of cybercrime.

Secondly, individuals need to learn and master cybersecurity knowledge and skills. For example, knowing how to set strong passwords, recognizing and avoiding online scams, protecting personal information, etc., to enhance their own cybersecurity protection capabilities.

Lastly, individuals need to actively cooperate with government and business efforts in cybersecurity. This includes complying with online usage regulations, promptly reporting cybercrimes, and safeguarding the security and stability of the internet.

4. Conclusion

Information security is an essential component of societal trust in the internet era. Faced with challenges such as information leakage and online fraud, it is the responsibility of the government, businesses, and individuals to jointly establish and improve an information security system, enhance public trust in the internet, and promote the construction of social trust.

References

[1] Wu, J. M., & Wang, Y. W. (2023). Analysis of Trust Crisis Governance Path from the Perspective of Social Inclusive Development. Zhongzhou Journal, (07), 96-103.

[2] Zhu, P. (2021). Legal Regulation of Personal Information Security Risks under the Background of Big Data. Legal System and Society, (15), 109-111.

[3] Yan, H., & Han, X. (2019). Personal Information Security Risks and Legal Prevention in Internet Targeted Advertising. Science, Technology and Law, (01), 55-60.