Dean&Francis
ISSN 2959-6149

Investigation and Research on Internet Privacy Security: Taking "Account Opening" as an Example

Yiran Chen [1],

Xinwen Liang [2, *]

[1] Beijing 21st Century International School, Beijing, China
[2] Zhuhai Oriental Yinghua International Academy, Zhuhai, China

*Corresponding author: MiniLiangXinwen@outlook.com

Abstract:

Network privacy security research is very important, it is directly related to the protection of personal privacy rights and interests, affecting social stability and trust. At the same time, it is also the foundation for the healthy development of the digital economy, which is of great significance to safeguarding national security and preventing cybercrimes and is an indispensable part of building a harmonious cyberspace. However, with the development of Internet technology, the problem of privacy leakage is becoming more and more serious, and the phenomenon of "account opening" has gradually become the focus of scholars. This study uses questionnaires to try to understand the reasons behind "opening accounts". Specifically, through the four questions set in the questionnaire, we understand the user's security awareness, the reliability of the download source, the virtual private network, and the sensitivity of private information. The results show that the privacy problem cannot be ignored at this stage. This study provides some reference value for the further development of the related theories of privacy economics.

Keywords: Privacy security; account opening; network.

1. Introduction

In today's digital age, the network has become a bridge connecting the world, and the development of information technology has greatly promoted social progress and economic prosperity. However, with the extensive and in-depth network applications, network security issues have become increasingly prominent and become a key factor restricting the healthy development of cyberspace [1]. Cyber security is not only related to the interests of individuals and enterprises, but also closely related to national security, social stability and even the global economic order. Personal privacy is a fundamental right of everyone, and it is particularly important in cyberspace. Network security measures, such as encrypted communication, anonymization, and data minimization principles, can effectively protect users' personal information from illegal collection, abuse or disclosure, enhance users' trust in network services, and promote the construction of a healthy and safe network environment [2]. The purpose of this study is to explore whether social media has a significant impact on the disclo-

ISSN 2959-6149

sure of user privacy and the negative consequences of users' weak privacy awareness. The goal is to arouse the attention of society to the issue of personal privacy and security. Through questionnaire survey, this study analyses the importance of personal privacy and gives relevant suggestions on how to prevent network security problems.

2. Survey Design

The primary aim of this survey is to investigate users' behaviour patterns related to internet usage, file downloads, software use, and privacy protection. The survey has four main objectives, as outlined in the following Table 1.

Table 1. Survey

	Title
1.	Understanding User Security Awareness: Questions focus on whether users regularly update their operating systems, check privacy settings of software, and review the scope of permissions granted to applications.
2.	Concern for Download Source Reliability: Questions assess whether users pay particular attention to the reliability of the source when browsing websites or downloading files.
3.	Awareness of VPN or Proxy Usage and Online Social Interaction Safety: This section aims to gauge users' understanding of virtual private networks (VPNs) or proxy servers and their awareness of online social interaction security, particularly in relation to protecting online privacy. These questions help evaluate users' knowledge and awareness concerning personal privacy protection.
4.	Sensitivity to Personal Privacy Information: The goal here is to collect data that will help analyse whether security vulnerabilities exist due to users' lack of concern for their own privacy.

These questions are designed to evaluate users' awareness of internet security and privacy protection. The results will provide insights into the need for promoting cybersecurity knowledge among different user groups. By examining users' habits and awareness, more targeted recommendations can be made to enhance overall internet security awareness.

3. Results

In this study, a total of 301 questionnaires were collected from September 18 to September 25, 2019. The survey results of question 1 are shown in Table 2 below.

Table 2. Survey results of question 1

Options	Subtotal	Proportion
Occasionally	90	29.9%
Frequently	87	28.9%
Always	51	16.94%
Seldom	38	12.62%
Never	35	11.63%

The largest percentage of respondents, 29.9 percent, said they update software occasionally. This may reflect a more passive approach to security, where updates are made only under certain circumstances or when prompted. Never update 11.63 percent of respondents said they never update their operating system or software. This percentage, while not high, is still cause for concern, as it means that their devices may present a serious security risk [3]. These data reveal different behaviour patterns of different users in terms of equipment maintenance and information security. Given that software updates are an important means of maintaining equipment security, it is necessary to raise public awareness and attention to regular updates. This will not only reduce potential security threats, but also improve the overall level of cybersecurity. The survey results of question 2 are shown in Table 3 below.

Table 3. Survey results of question 2

Occasional consideration	81	26.91%
Most of time	77	25.58%
Always consider	62	20.6%
Little	44	14.62%
Never	37	12.29%

From the above table, it is clear that 26.91% of users only occasionally think about privacy risks when sharing information, which may mean that they do not pay enough attention to privacy systematically and only take precautions when alerted or when they encounter obvious risks. Never consider: 12.29 users indicate that they never consider privacy risks when sharing personal information, and this small group of users are highly likely to be exposed to a high risk of privacy infringement in cyberspace, possibly due to the lack of necessary knowledge or awareness of privacy protection. The data reveals a key issue: While some users continue to be highly vigilant about the privacy protection of their social media accounts, a significant number are less active in this regard, especially those who rarely or never check. This may be due to a lack of awareness of privacy protection or a perception that the act is too cumbersome. The survey results of question 3 are shown in Table 4 below.

Table 4. Survey results of question 3

Yes	208	69.1%
No	93	30.9%

Most people (83.72%) will make new friends on social networks, and 69.1% will reveal their personal information in communication. However, virtual social platforms cannot be equated with real life, and cannot map everyone's real life status in time, so you cannot determine the security of the opposite side of the social network. The survey results of question 4 are shown in Table 5 below.

Table 5. Survey results of question 4

	Obs	Proporation
Usually authorized, easy to use	93	30.9%
Little authorization, fear of privacy	69	22.92%
Security incident and response	54	17.94%
Decide whether to authorize after careful evaluation	50	16.61%
Had no idea you could manage these permissions	35	11.53%

More than half of those surveyed (60.13%) do not take the time to read the initial personal Information Access and privacy policy when downloading an app. Among the sensitive permissions required by the app to access personal location information and address books, the largest proportion is usually authorized, because it is convenient to use. Both may lead to network security incidents, so it is found in the questions later in the questionnaire that most people (66.12%) have experienced network security incidents. Only 16.61% of users will carefully evaluate the APP's requirements for sensitive permissions before deciding whether to authorize, reflecting that some users attach some importance to privacy protection. However, 30.9% of users said they usually grant permission for ease of use, while 11.63% were completely unaware that these permissions could be managed, which puts these users in a passive state when it comes to privacy protection.

4. Suggestions

4.1 Enhancing Individual Awareness of Cybersecurity and Self-Protection

The proliferation of "account opening" phenomena is largely due to individuals' neglect of personal information privacy protection. Many people, when using social networks, shopping online, or filling out online surveys and forms, often provide personal information too easi-

ISSN 2959-6149

ly. However, the information security measures of these platforms are frequently inadequate, becoming a loophole through which malicious actors can steal information. Therefore, increasing public awareness of cybersecurity, especially enhancing the understanding of personal privacy protection, is an essential step in preventing information leakage [4].

Internet users need to recognize that any form of personal information can become a potential entry point for malicious actors to acquire further details. Therefore, on any online platform, particularly those that are not verified third-party platforms, individuals should avoid entering sensitive information such as identity card numbers, home addresses, and contact details [5]. Additionally, people should be cautious of online lottery events and promotional offers, as these are often traps designed to collect personal information.

To better protect their account security, individuals should use complex and non-repetitive password combinations and regularly update their passwords. For important accounts, such as social media or bank accounts, enabling two-factor authentication (2FA) can significantly improve the security of those accounts.

During the use of online platforms, individuals should regularly check their account privacy settings and monitor for any suspicious login records or account activities. Additionally, utilizing third-party security tools and services can provide real-time monitoring and alerts regarding potential information leakage risks. This enables individuals to take immediate action to prevent further information exposure [6].

Public networks typically have lower security, and hackers can easily steal personal information through specialized means. Therefore, when using public Wi-Fi, users should avoid conducting sensitive operations and take care to prevent information from being intercepted during transmission.

By improving public awareness of cybersecurity, reducing the unnecessary provision of sensitive information, and adopting appropriate protective measures, the risk of "account opening" and personal information leakage can be effectively minimized. However, personal self-protection is only one aspect of addressing information leakage. Companies should also assume corresponding social responsibility and implement stricter privacy protection measures.

4.2 Privacy Protection and Data Management Optimization for Enterprises and Institutions

Enterprises and institutions are the primary entities responsible for storing large volumes of personal information, especially in industries such as finance, education, healthcare, and social media. Therefore, businesses must employ technological means to enhance data security and prevent information leakage [7]. First, companies should vigorously apply data encryption techniques to ensure that even if information is intercepted during transmission or storage, it cannot be directly accessed.

Enterprises should regularly audit and update their cybersecurity systems to identify potential vulnerabilities and address them promptly. As hacking techniques continue to evolve, information security systems must also be continuously updated. For vulnerabilities that have already been exposed, companies should take swift action to repair them and promptly review and remediate affected data.

Moreover, enterprises should strengthen the vetting process for third-party partners to ensure that they also possess the necessary data protection capabilities, preventing information leakage through vulnerabilities in partner systems.

Many instances of information leakage stem from poor internal management. For example, employees may access, download, or even sell customer information, representing a significant internal risk. Therefore, companies need to establish strict data access control systems and introduce access records to ensure that only authorized personnel can access sensitive data, with a clear record of data operations for auditing purposes [8].

Additionally, companies should strengthen cybersecurity training for employees to enhance their awareness and preventative skills. Training content should include how to avoid phishing emails, how to use complex passwords, and how to identify potential cyber-attacks. By continuously reinforcing employees' security consciousness, organizations can effectively reduce information leakage caused by human errors.

To address the "account opening" phenomenon, the government should enhance legal regulation of information leakage and misuse and promote the further refinement and enforcement of relevant laws. Enterprises should not only comply with data protection laws, such as the Personal Information Protection Law and the Cybersecurity Law, but also proactively cooperate with regulatory authorities to ensure transparency and legality in their data processing [9]. Governments and enterprises should collaborate to jointly combat illegal activities that involve the unauthorized acquisition and use of personal information. For detected illegal acts, legal responsibility should be pursued, and victims should receive timely compensation and assistance.

4.3 Technological Controls and Legal Management

Due to the use of virtual identities online, many internet users believe they are not accountable for their actions, leading to many infringing behaviours. To regulate "account opening" violations, real-name authentication on the internet must be established. By creating a mechanism for matching real identities, individuals can communicate online based on their true identities, significantly improving information credibility and responsibility for one's statements. Furthermore, real-name authentication enables the application of social adjustment mechanisms, such as moral and legal frameworks, in the online world. However, there are differing views on whether real-name authentication should be implemented. Proponents argue that it would enhance accountability, while opponents suggest that such a policy could undermine the freedom of expression enabled by internet technology, advocating for a "limited real-name system," where the public-facing side is anonymous, but the backend uses real names.

"Account opening" itself is merely a mechanism for obtaining information; its negative effects often arise from internet users' lack of awareness of the facts, being misled or incited, leading to emotional outbursts. This requires websites to strengthen their management, establishing reasonable online monitoring mechanisms to oversee search behaviours and information dissemination, and provide timely guidance [10]. In the event of privacy violations or signs of cyberbullying, websites should promptly clarify the facts, offer reasonable explanations, and guide users to moderate their extreme behaviours. If infringement or illegal activities occur during the "account opening" process, websites, as the platforms hosting the accounts, have an obligation to delete or block content related to personal privacy. Rational organization and guidance from websites can also help prevent the "account opening" process from leading to negative outcomes. Websites can also utilize new technologies to limit the dissemination of harmful content, fulfilling their role as gatekeepers.

4.4 Technical Aspects of Website Security

Technical defenses represent the first line of defence in cybersecurity, focusing on identifying and resisting potential threats through advanced technological means. Strengthening perimeter defences involves deploying high-performance firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and content filtering systems to ensure that only authorized data flows in and out of the network. Security hardening should include auditing code, vulnerability scanning, and penetration testing for critical business systems, addressing known vulnerabilities in a timely manner, and implementing access control and data encryption measures [11]. Multi-factor authentication (MFA) should also be employed, incorporating passwords, biometric features, and physical tokens to improve account security and prevent unauthorized access.

In addition to technical protections, reinforcing internal management and processes is equally critical to reducing human errors and security gaps. Security training and education are essential, with regular cybersecurity awareness training for employees to increase their ability to recognize and prevent common attack methods, such as phishing emails and malware. Role-based access control (RBAC) should be implemented to ensure that employees are granted only the minimum necessary access for their duties, thereby reducing internal misuse risks.

In conclusion, solving cybersecurity challenges requires both technological and managerial efforts. By building a robust technical defence system, improving internal management and processes, establishing efficient emergency response mechanisms, and implementing scientific vulnerability and risk management strategies, organizations can significantly enhance their cybersecurity capabilities, ensuring business continuity and data security.

5. Conclusion

The issue of Internet privacy security is very important, because it is directly related to the disclosure of personal privacy, so it will affect social stability and trust. At the same time, Internet privacy security is the foundation of the healthy development of the digital economy, is of great significance for safeguarding national security and preventing cybercrimes and is an indispensable part of building a harmonious cyberspace. However, with the rapid development of Internet technology, the problem of privacy leakage is becoming more and more serious, and the phenomenon of "account opening" has gradually become the focus of academic attention. The purpose of this study is to explore the reasons behind the "account opening" phenomenon through a questionnaire survey. Specifically, through the four main questions in the questionnaire, the survey users' security awareness, the reliability of the download source, the use of virtual private networks, and the sensitivity of private information. The results show that the current privacy issues need to be paid attention to. This study provides a useful reference for the further development of the related theories of privacy economics.

Author Contribution

All the authors contributed equally, and their names were listed in alphabetical order.

ISSN 2959-6149

References

[1] Chen Xiuzhen, Zheng Qinghua, Guan Xiaohong, et al. Hierarchical network security threat situation of quantitative evaluation method. Journal of software, 2006, 17 (4): 13.

[2] Bryan. Data processing of legal regulation. Journal of chongqing university of posts and telecommunications: social science edition, 2017, 29 (6): 7.

[3] Wang Gang, Wei Feng. Discusses the problems about computer system security patch management. Journal of henan science and technology, 2013 (7): 3.

[4] Luo Bingmei. Information Ethics and Its Construction in the Network Environment Modern Intelligence, 2005 (7).

[5] Liu Chang. Research on Civil legal Issues of online transaction third-party payment platform. Thesis for master's degree. Southwestern University of Finance and Economics, 2012.

[6] Amber Minjie Li Hongwei Chen. Student Information Security and Privacy Protection: Concerns in the era of Big Data. Digital Communications World, 2024 (10).

[7] Zheng Zhiling. Analysis of data encryption technology application in computer network security countermeasures. Journal of network security technology and applications, 2015 (1): 2.

[8] Gao Zhaoqin. The multilevel security information system level protection technology research. Thesis for master's degree, Beijing university of technology, 2024.

[9] Chen Lu. On the new enlightenment of "Network Security Law" to the protection of Personal Information in Criminal Law -- from the perspective of the latest judicial interpretation of two high levels. Rule of Law Research, 2017, (4): 9.

[10] Song Jiageng, Zhao Lumin, Zhang Yuer. Network supervision mechanism under the network governance perspectives analysis. Journal of published research, 2020 (5): 7.

[11] Liang Yeyu, Xu Tan, Ning Jianchuang, et al. Code audit work of important value in the whole security system. Computer security, 2013, (12): 4.