JATAED
Journal of Appropriate Technology for Agriculture, Environment, and Development
email: jataed@lkppl.org
E-ISSN 3031-0903
Volume 3, **Number** 1, October 2025
https://doi.org/10.62671/jataed.v3i1.96

Computer Network Security: A Review And Implementation For Beginner Users

Muhammad Farhan[1*], Rudi Arif Candra[2] , Ihsan Anwar [3], Fardiansyah[4], Dina Miftahul Jannah[5], Devi Satria Saputra[6]
[1,2,3,4,5,6]Politeknik Aceh Selatan
[1*]mrfarhan1303@gmail.com, [2]rudiarifcandra@gmail.com, [3]ihsan.poltas@gmail.com, [4]fardian.poltas@gmail.com, [5]dinamiftahul55@gmail.com, [6]devisatriasaputra@gmail.com

open access

***Corresponding Author**

Article History:
Submitted: 10-12-2025
Accepted: 22-12-2025
Published: 26-12-2025

Keywords:
computer network security, cyber threats, beginner users, firewall, literature review.

ABSTRACT

Computer network security has become a crucial aspect in the digital era as users increasingly depend on network technologies for daily activities. Beginner users represent one of the most vulnerable groups to cyber security threats due to limited technical knowledge and low security awareness. This article aims to provide a comprehensive review of fundamental concepts, common threat types, and basic network security strategies that are relevant for beginner users.

The research method employed is a descriptive literature review of scientific articles and academic publications related to computer network security published between 2018 and 2025. The collected literature was analyzed to identify dominant threats and effective protection mechanisms for beginner users.

The results indicate that threats such as malware, phishing, ransomware, and unauthorized access remain major security issues. The implementation of basic security mechanisms, including strong password policies, firewalls, antivirus and anti-malware software, regular system updates, and improved user awareness, has proven effective in minimizing security risks. With adequate understanding and proper implementation of these measures, beginner users are expected to apply network security practices more safely, responsibly, and efficiently.

INTRODUCTION

The rapid development of information and communication technology has led to the widespread use of computer networks in various aspects of life, including education, business, government services, and daily communication activities (Yani & Maulana, 2020; Zhang et al., 2023). Computer networks enable fast and efficient data exchange and information sharing; however, their extensive use also introduces various cyber security threats. These threats include malware attacks, data theft, phishing, identity fraud, and unauthorized access to network systems (Galib et al., 2024; Miracle, 2024).

Beginner users, such as students and the general public, often lack sufficient understanding of the importance of computer network security. Limited technical knowledge causes users to ignore basic security practices, including the use of strong passwords, careless access to suspicious websites, and the failure to perform regular system updates (Astuti & Hidayat, 2020; Wulandari & Rahman, 2021). Consequently, user devices and personal data become more vulnerable to cyber attacks that can lead to information leakage, financial loss, and system damage.

Therefore, a comprehensive and easily understandable discussion of computer network security is necessary, especially for beginner users. This article aims to provide an overview of fundamental network security concepts, common cyber threats, and basic protection strategies that can be applied as preventive efforts to help users utilize computer networks safely and responsibly.

LITERATURE REVIEW

Computer network security refers to systematic efforts to protect the confidentiality, integrity, and availability of data transmitted across network infrastructures. These three principles, commonly known as the CIA triad, form the foundation of modern network security. Studies conducted over the past seven years indicate that network security threats have grown increasingly complex as technological innovation and internet usage continue to expand.

JATAED
Journal of Appropriate Technology for Agriculture, Environment, and Development
email: jataed@lkppl.org
E-ISSN 3031-0903
Volume 3, **Number** 1, October 2025
https://doi.org/10.62671/jataed.v3i1.96

Several studies reveal that the major threats in computer networks include malware, ransomware, phishing, and denial-of-service (DDoS) attacks (Andriansyah & Pratama, 2021; Zhang et al., 2023). Malware and ransomware are designed to disrupt systems and steal or encrypt data, while phishing exploits social engineering techniques to deceive users into revealing sensitive information. DDoS attacks aim to overload network resources, causing service disruptions. These threats typically exploit vulnerabilities in operating systems, applications, and improper network configurations.

Research also emphasizes the importance of technical defense mechanisms such as firewalls and intrusion detection systems (IDS) to monitor, filter, and control network traffic (Ardiansyah & Nugroho, 2022; Siregar & Lubis, 2021). Firewalls act as a first line of defense by restricting unauthorized access, while IDS identifies suspicious activity within network environments and alerts administrators to potential intrusions.

In addition to technological aspects, the literature highlights the significant role of human factors in network security. User mistakes, such as clicking malicious links, downloading unsafe files, or using weak and repetitive passwords, remain major causes of security incidents (Prasetyo & Wijaya, 2021; Miracle, 2024). Therefore, user education, training, and awareness are considered integral components of an effective network security strategy, particularly for beginner users who are more vulnerable to cyber threats.

RESEARCH METHOD

This study employs a literature review method using a descriptive approach to analyze issues related to computer network security for beginner users. Relevant sources were obtained from scientific journals, conference proceedings, and academic publications discussing network security topics published between 2018 and 2025.

The research process consisted of several stages. First, topic identification was conducted to determine the focus of the study on network security threats and protection strategies for beginner users. Second, relevant references were collected through digital databases and journal platforms using keywords such as *computer network security*, *cyber threats*, and *user awareness*. Third, the collected literature was selected based on its relevance, credibility, and publication quality. Finally, content analysis was carried out to identify key concepts, types of threats, and appropriate network security solutions.

The results of the analysis were systematically organized and presented in narrative form to ensure clarity, coherence, and accessibility for beginner users, as well as to support academic discussion on the importance of basic network security implementation.

RESULTS AND DISCUSSION

Computer Network Security Threats

The literature review indicates that the most common security threats faced by beginner users include malware, viruses, spyware, ransomware, and phishing attacks (Yani & Maulana, 2020; Galib et al., 2024). These threats typically enter systems through email attachments, malicious websites, downloaded applications from untrusted sources, and unsecured public Wi-Fi networks.

Malware and spyware are designed to damage systems and steal personal data, while phishing attacks aim to deceive users into providing sensitive information such as usernames, passwords, and financial details. Beginner users are more vulnerable because they often cannot easily distinguish between legitimate and malicious online content. Low user awareness significantly increases the likelihood of security breaches and unauthorized access to network resources.

Sources of Vulnerabilities in Beginner User Environments

Security vulnerabilities arise not only from technical weaknesses but also from user behavior. Outdated operating systems, unpatched applications, and improper network configurations create opportunities for attackers to exploit system flaws. Public Wi-Fi networks without encryption also expose user data to interception attacks.

From the human perspective, many beginner users still use simple passwords, reuse credentials across platforms, and click unknown links without verification. Such habits increase the risk of malware infections and phishing attacks. Therefore, identifying vulnerability sources is essential to reduce security risks in computer network usage.

Basic Network Security Strategies

Basic network security strategies recommended for beginner users include the use of strong and unique passwords, enabling firewalls, installing and regularly updating antivirus software, and performing periodic operating system updates (Astuti & Hidayat, 2020; Ardiansyah & Nugroho, 2022).

JATAED
Journal of Appropriate Technology for Agriculture, Environment, and Development
email: jataed@lkppl.org
E-ISSN 3031-0903
Volume 3, **Number** 1, October 2025
https://doi.org/10.62671/jataed.v3i1.96

Strong passwords should combine letters, numbers, and symbols to prevent brute-force attacks. Firewalls function as barriers that filter incoming and outgoing traffic, protecting internal networks from unauthorized access. Antivirus software helps detect and remove malicious programs, while regular updates ensure that security patches are applied promptly. These measures are relatively easy to implement and have been shown to effectively reduce cyber security risks.

Safe User Practices in Network Utilization

Beyond technical protection, safe user behavior is critical in maintaining network security. Users should avoid opening suspicious email attachments, verify website authenticity before entering personal information, and only download software from trusted sources. Using secure HTTPS connections and being cautious of pop-up messages also help prevent attacks.

When accessing public Wi-Fi networks, users should limit activities involving sensitive data such as online banking and account logins. Logging out from shared devices and backing up important files regularly can further reduce potential damage if a security incident occurs. Developing safe habits strengthens overall network protection for beginner users.

User Awareness and Education

The literature consistently demonstrates that human factors play a significant role in computer network security. Users who possess fundamental knowledge of threats and preventive measures tend to be more cautious when using network services (Prasetyo & Wijaya, 2021; Wulandari & Rahman, 2021).

Continuous education and awareness programs are essential, particularly for beginner users. Training sessions, workshops, and simple security guidelines can help users recognize cyber threats and respond appropriately. By increasing awareness and responsibility, network security can be enhanced not only through technology but also through safer user behavior.

CONCLUSION

Computer network security is a critical aspect that should not be overlooked, especially by beginner users in the digital era. Based on the literature review, it can be concluded that network security threats are still predominantly caused by malware, phishing, ransomware, and unauthorized access, which are largely influenced by low levels of user awareness and inadequate security practices.

The implementation of basic security measures, such as the use of strong and unique passwords, firewalls, antivirus and anti-malware software, as well as regular operating system and application updates, significantly enhances network protection and reduces potential cyber security risks. These technical measures provide an essential foundation for safeguarding user devices and network resources.

Furthermore, user education and awareness play a vital role in establishing a secure network environment. Users who understand common threats and prevention strategies tend to behave more cautiously and responsibly when utilizing network services. Therefore, continuous education programs and the development of safe digital habits are necessary to ensure that beginner users are able to utilize computer networks securely, effectively, and sustainably.

REFERENCES

Andriansyah, R., & Pratama, A. (2021). A literature review of network security. *Jurnal Jaringan Komputer dan Keamanan, 3*(2), 45–54.

Ardiansyah, D., & Nugroho, Y. (2022). Implementation of network security systems using firewalls and intrusion detection systems. *Jurnal Mumin Informatika, 4*(2), 112–120. https://ejournal.sisfokomtek.org/index.php/jumin/article/view/6763

Astuti, S., & Hidayat, R. (2020). Computer network security protection in educational environments. *International Journal of Natural Science and Engineering, 4*(1), 23–30. https://ejournal.undiksha.ac.id/index.php/IJNSE/article/view/22175

Galib, A., Bahri, S., & Rahman, A. (2024). Latest challenges and trends in network security: Facing cyber threats in the digital era. *Journal of Cyber Security Studies, 6*(1), 1–12.

Miracle, N. O. (2024). The importance of network security in protecting sensitive data and information. *International Journal of Research and Innovation in Applied Science, 9*(3), 15–22.

JATAED
Journal of Appropriate Technology for Agriculture, Environment, and Development
email: jataed@lkppl.org
E-ISSN
3031-0903
Volume 3, **Number** 1, October 2025
https://doi.org/10.62671/jataed.v3i1.96

Prasetyo, A., & Wijaya, D. (2021). User data security in wireless networks using passwords, MAC filtering, and two-factor authentication. *Jurnal Jupiter, 13*(2), 89–97. https://jurnal.polsri.ac.id/index.php/jupiter/article/view/4385

Siregar, M., & Lubis, R. (2021). Network security implementation using intrusion detection systems. *Jurnal Ilmu Komputer dan Multimedia, 3*(1), 34–42. https://journal.dcircle.org/index.php/jikum/article/view/184

Wulandari, D., & Rahman, A. (2021). Wireless computer network management security analysis. *Jurnal Ilmu dan Teknologi Komputer, 6*(2), 101–109. https://ejournal.nusamandiri.ac.id/index.php/jitk/article/view/2786

Yani, S., & Maulana, I. (2020). Computer network security analysis. *Jurnal Nasional Komputasi dan Teknologi Informasi, 3*(1), 1–8. https://ojs.serambimekkah.ac.id/jnkti/article/download/3106/pdf

Zhang, Y., Chen, X., & Li, H. (2023). Cyber security: State of the art, challenges, and future directions. *Computers & Security, 122*, 102115. https://doi.org/10.1016/j.cose.2022.102115