



INTERNET SECURITY AND PROTECTION OF PERSONAL DATA

Rustamova Nafosat Alijon qizi

*First-year student, Foreign Language and Literature program
Faculty of Language Teaching Guliston State Pedagogical Institute*

Phone num: +998(95)062-02-36

*Scientific Supervisor: **Berdikulova.M***

Guliston State Pedagogical Institute

Abstract. This article discusses the importance of internet security and the protection of personal data in the modern digital world. It describe common cyber threats such as phishing, hacking, and malware and highlights their negative effects on individuals. The article also provides practical ways to protect personal information online, including using strong passwords and security tools. In addition, the role of governments and organizations in ensuring cybersecurity is considered.

Key words: Internet security, personal data, cybersecurity, phishing, hacking, malware, privacy protection, online safety

Nowadays, the internet plays a crucial role in everyday life. It is widely used for communication, education, business, and entertainment. Despite its advantages, the increasing dependence on digital technologies has led to new security challenges. Therefore, ensuring internet safety and protecting personal data have become urgent global issues.

Internet security focuses on protecting digital systems and user information from unauthorized access and cyber threats. Todaay, cybercriminals use advanced



techniques to obtain confidential data. For example, phishing is a method where users are deceived into sharing their private information through fake messages or websites. In addition, malware can secretly enter devices and damage systems or steal valuable data.

Another important problem is careless user behavior. Many individuals create weak passwords or provide personal details on unreliable platforms. This makes it easier for attackers to access their accounts. As a result, users may face identity theft, financial problems, or loss of privacy.

To reduce such risks, several preventive measures should be taken. First of all, users need to create complex and unique passwords. Secondly, they should avoid clicking on suspicious links or visiting unknown websites. Keeping software updated and using security programs can also help prevent cyberattacks. Moreover, enabling two-step verification increases the level of protection.

At the same time, governments and organizations are responsible for improving cybersecurity. They establish legal frameworks and develop strategies to combat cybercrime. However, due to the rapid development of technology, security systems must constantly evolve.

Conclusion

To sum up, internet security and the protection of personal data are essential in the modern digital environment. Both individuals and institutions must take active steps to ensure online safety. By staying informed and following basic security practices, users can minimize risks and safely benefit from the internet.

References

1. Stallings, W.(2018). Network Security Essentials: Applications and Standards. Pearson Education.



2. Whitman, M.E., & Mattord, H. J. (2019). Principles of Information Security. Cengage Learning.
3. Kaspersky Security Bulletin (2024). Cyber Threat Report.
4. Norton Cyber Safety Insights Report