European International Journal of Multidisciplinary Research and Management Studies (ISSN: 2750-8587)

Received: 30 December 2025 | Accepted: 21 January 2026 | Published: 26 February 2026

DOI: 10.55640/eijmrms-06-02-08

RESEARCH ARTICLE

Immunity Against Cyberattacks and Phishing

Omanov Jasurbek Hamidulla o'g'li
Student at Urgench State University, named after Abu Raykhan Beruni, Uzbekistan

VOLUME: Vol.06 Issue02 2026

PAGE: 95-97

Abstract

This article examines modern cybersecurity issues, particularly various forms of cyber-attacks and phishing attacks. The article analyzes the latest methods of cybercrime and presents effective ways to protect against them along with practical recommendations. Contains valuable information on ensuring information security for students and teachers.

KEYWORDS

Cybersecurity, Cyber Attacks, Phishing, Information Security, Protection.

INTRODUCTION

In the modern world, information technologies have become an integral part of our daily lives. Through the Internet, social networks, and digital platforms, we communicate with each other, receive education, and work. Unfortunately, along with these opportunities, cybersecurity threats are also increasing. Cybercriminals develop new methods every day in attempts to steal users' personal information.

University students and staff are considered one of the groups particularly at high risk of becoming targets of cyberattacks. The reason is simple: the academic environment involves extensive exchange of information, and many users do not have sufficient knowledge of basic cybersecurity principles. In this article, we will discuss the most common cyber threats — cyberattacks and phishing — and examine how protection against them is possible.

Types of cyberattacks and their characteristics

A cyberattack is an attempt to gain unauthorized access to, damage, or steal computer systems, networks, or data. Cyberattacks fall into several main categories:

1. **Malware** - Viruses, Trojans, ransomware, and other malicious programs. They can infect computers and steal data, destroy data, or disrupt systems.

2. **DDoS attacks** - Distributed Denial of Service - attacks that overload servers and cause them to fail.

3. **Man-in-the-Middle (MITM) attacks** - An attacker intercepts the connection between a user and a server and reads or modifies data.

4. **SQL injection** - A method of unauthorized access to a database and stealing data.

Phishing is the most common threat

Phishing is one of the most popular and effective methods of cybercriminals. The attacker sends a fake message on behalf of a trusted source (bank, social network, university) and asks the user for personal information (login, password, card number). Phishing has several forms:

- By email - sending fake letters
- By SMS (smishing) - sending short messages
- By phone (vishing) - making fake calls

- By social networks - creating fake accounts
- Spear phishing - an attack aimed at a specific person

The most dangerous thing about phishing attacks is that they are often professionally prepared and at first glance do not differ from real messages. Attackers can offer logos, fonts and even website addresses.

Protection methods and practical recommendations

To protect yourself from cyberattacks and phishing, you should follow these basic rules:

Protective measures	Description
Strong passwords	At least 12 characters, a mix of uppercase and lowercase letters, numbers, and special characters
Two-factor authentication (2FA)	Additional verification with SMS code, app or biometric data
Ignore suspicious messages	Do not open emails and links from unknown sources.
HTTPS protocol	Use only secure connections, check the lock icon
Software update	Always keep your operating system and applications up to date

It is also recommended to take the following additional measures:

1. **Use antivirus software** - Install a reliable antivirus on your computer and keep it updated regularly.
2. **Update your operating system** - Do not delay installing new security updates.
3. **Create a backup** - Create regular backups of your important data.
4. **Report suspicious activity** - If you notice signs of a cyberattack, immediately notify IT.

Security on the university network

It is important to follow these additional rules when working on the university network:

- Avoid entering personal information when using the university Wi-Fi network
- Use your university email only for official purposes
- Download educational materials only from trusted sources
- Do not give your login and password to others
- Always close the session when you log out

CONCLUSION

Cybersecurity is an important topic for every user, not just IT professionals. Modern cyberattacks are becoming increasingly sophisticated, but by following basic security rules, you can easily protect yourself from most of them. The most important thing is to always be vigilant, not click on suspicious messages and links, and regularly update your passwords.

We remind you: cybercriminals exploit our most vulnerable part - human carelessness. Therefore, awareness is the strongest defense. Protecting yourself and your data means ensuring the safety of not only you, but also everyone around you.

REFERENCES

1. National Institute of Standards and Technology (NIST). Cybersecurity Framework Version 1.1. – U.S. Department

of Commerce, 2018. – 55 p.

2. Kaspersky Lab. IT Threat Evolution Report Q3 2024. – Moscow: Kaspersky, 2024. – 32 p.
3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. – International Organization for Standardization, 2022.
4. Symantec Corporation. Internet Security Threat Report 2024. – Mountain View, CA: Broadcom, 2024. – Vol. 29. – 78 p.
5. Agency for Informatization and Telecommunications of the Republic of Uzbekistan. Cybersecurity Guide. – Tashkent, 2023. – 45 p.
6. Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. – New York: W.W. Norton & Company, 2023. – 288 p.
7. Cisco Systems. 2024 Cisco Cybersecurity Readiness Index. – San Jose, CA: Cisco, 2024. – 24 p.
8. Anti-Phishing Working Group (APWG). Phishing Activity Trends Report, 3rd Quarter 2024. – Cambridge, MA: APWG, 2024. – 18 p.
9. Decree of the President of the Republic of Uzbekistan No. PF-123 "On measures to develop electronic government and ensure cybersecurity." - Tashkent, 2023.