METHODS OF PROTECTING USER DATA FROM MALICIOUS SOFTWARE ON SOCIAL NETWORKS

Qaxramonov Elbek Quvondiq o‘g‘li,
Tashkent university of information technologies named after Muhammad al-Khwarizmi, Tashkent
e.qaxramonov@tuit.uz

Karimov Abdukodir Abdisalomovich,
Tashkent university of information technologies named after Muhammad al-Khwarizmi, Tashkent
karimovabduqodir041@gmail.com

Abstract. This article discusses the increasing threat of malware on social networks and highlights some effective ways to safeguard user data. Social media platforms have become vital channels for communication, marketing, and information exchange; therefore, they have become an easy target for cyberattacks. The preventive approach, education on cybersecurity, and the use of artificial intelligence in this regard are discussed in this research study.

Keywords. cybersecurity, malware, social networks, phishing, user protection, digital security, artificial intelligence.

Introduction. Social networks like Facebook, Instagram, X, and TikTok have transformed digital communication, making it possible for billions of users to share personal information daily. In this regard, increased connectivity has also provided different opportunities for cybercriminals. Most malware attacks on social media are designed to steal login credentials, personal data, and financial information. Protection of user data is thus among the most important challenges of modern cybersecurity [1].

Literature review and methodologya. *Social network* can be defined as any online group or community of people interested in communicating, sharing information, building friendships, posting photos and videos, or exchanging opinions.

In other words, a social network is a virtual area that unites people: one can chat with friends, read news, or share some content there. Malware is a type of software created to harm computers or mobile devices, damage or steal data, or scam users in general [2].

The protection of users' data against malware in social networks presupposes measures aimed at preventing malicious applications or scams from getting access to, stealing, modifying, or destroying any personal information of users on social platforms, including messages, photos, passwords, contacts, or even banking accounts [3].

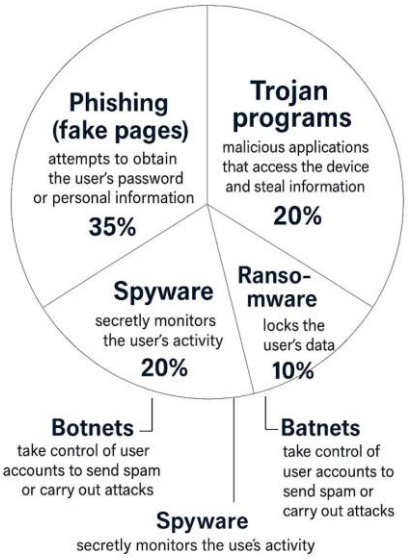

Fig 1. Main malware found on social networks

The following are some of the current work being done by scientists on ways to protect user data from malicious programs on social networks:

1. Yuval Elovici — In his “Stealing Reality” study, he analyzed how malware is able to keep

track of and compile personal information by observing users on social networks.

2. Matthew Williams - In “Digital fingerprinting for identifying malicious collusive groups on Twitter”, he proposes a technique of using digital fingerprints to detect the accounts involved in propagating malicious links on Twitter [4].
3. Grigori Sidorov - In “Cyberattack Detection in Social Network Messages Based on Convolutional Neural Networks and NLP Techniques”, he suggested using AI (NLP and CNN) to detect malicious messages on social networks.
4. Xuerong Zuo: He has also pointed out in the paper “Research on Personal Information Security Protection of Social Networks in the Era of Big Data” that it is required to raise user awareness, increase the responsibility of social network services, and enhance legal regulations for the protection of personal data [5].
5. Francesca Cerruto: In “Social network data analysis to highlight privacy threats in sharing data”, she analyzed the risk of reconstructing users' personal data on social networks and recommended improving the privacy policies.

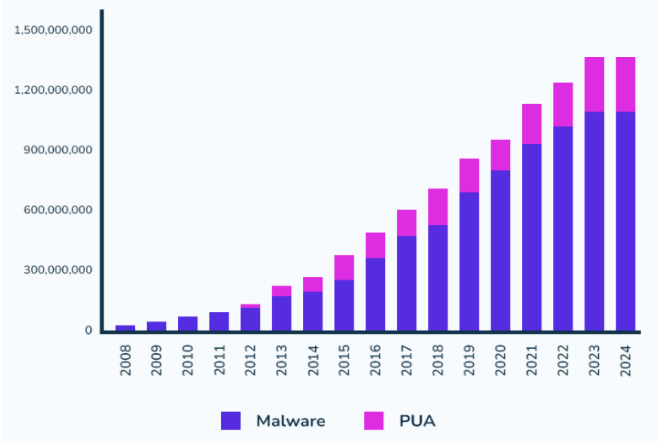

Fig 2. Total amount of malware and by year

This figure shows that the trends are growing for security threats, and it tells about the need to strengthen cybersecurity [7].

Fig 3. Security behavior change improvement

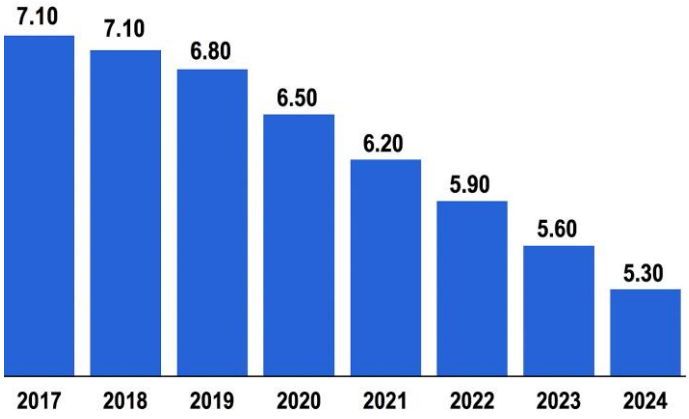

Fig 4. Uzbekistan security threats index

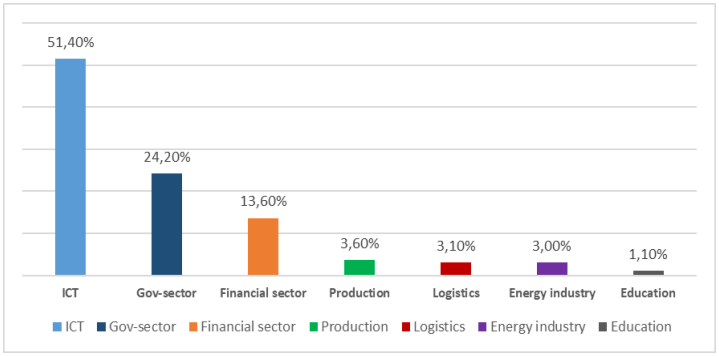

Fig 5. Analysis of the level of cybersecurity development in Uzbekistan

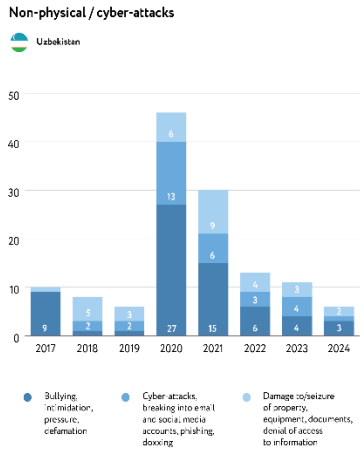

Fig 6. Attacks on media workers in uzbekistan in 2024

Results. *Methods for protecting user data:*

2FA or MFA was designed to provide an extra layer of security for user accounts. Instead of relying on a password for an account, it requires extra verification as another means to ensure the person trying to get to the account is really the account owner. The main goal is to protect accounts even if the password is stolen or compromised [8].

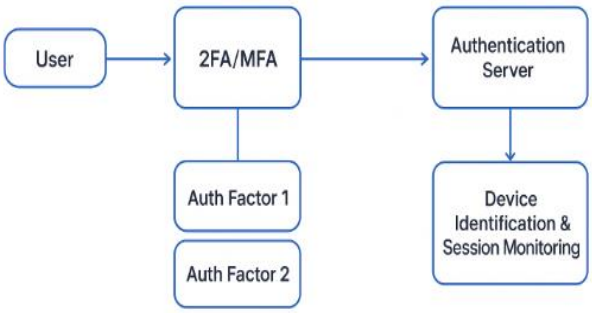

Fig 7. Strong authentication systems

Biometric authentication is a technique used to verify the user's identity based on his/her unique biological characteristics. Biometric authentication relies on physical or behavioral characteristics, rather than using a password or PIN [9].

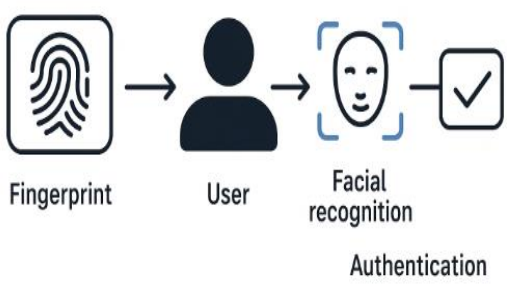

Fig 8. Biometric authentication
Device Identification

Fingerprinting definition: The method based on the principle of uniqueness of a device's (computer, phone, tablet) “fingerprint”.

Session monitoring definition: It is the way a user is tracked after he or she logs into a system.

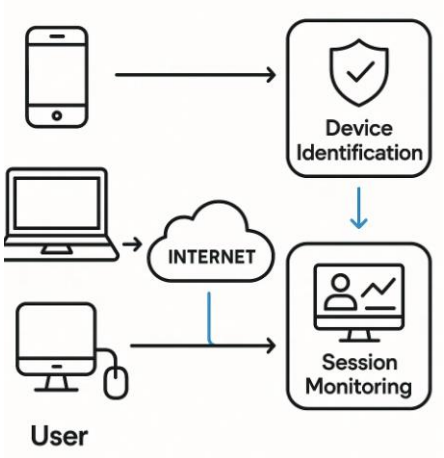

Fig 9. Device identification and session monitoring

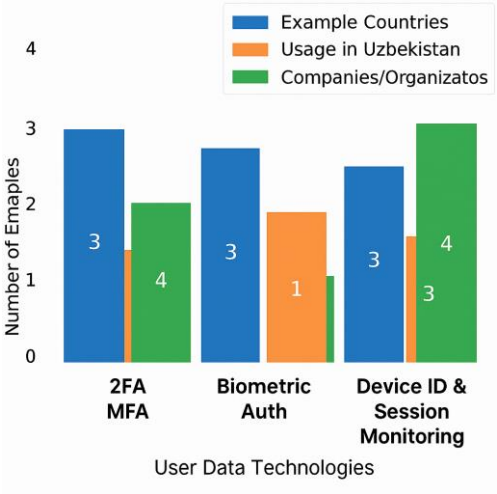

Fig 10. Comparison of user data protection technologies in social networks

AES-256 is symmetric, meaning that there is a single key for encryption and decryption. It utilizes a 256-bit key, which makes it highly secure. It's very quick and mainly works wonders for large data or files being transferred. For instance, it may be used in cloud storage to keep the files safe, or it can be used to keep data flowing across HTTPS secure. Only the person having the correct key will be able to decrypt the data; in case any third party gets hands on the encrypted data without the key, they will not be able to read it [10].

RSA is an asymmetric encryption algorithm, meaning that it relies on two keys: one for encryption, which can be public, and another for decryption, which should be private. Any person is allowed to use the public key to encrypt a message, while only the owner of the private key may decrypt it. RSA is normally used to transmit small pieces of sensitive information, such as passwords or keys, and in digital signatures.

TLS 1.3 is a protocol at the transport layer, with the basic purpose of safely transmitting data across the internet. The most important tasks of TLS 1.3 are encryption, authentication between parties-that is, verifying the legitimacy of the server and client-and integrity at the level of the data, so that it is not changed during the process [11].

This implies that the storage of personal files in cloud systems in encrypted form ensures that your data is saved on remote servers in such a way that only you or other authorized users will be able to read it. Before the files leave your device, they are encrypted with strong algorithms such as AES-256, meaning that even when somebody accesses the cloud server, they cannot read your data without the encryption key. It also ensures that your files remain private and secure from unauthorized access but allows you to access the same files from anywhere using your credentials [12].

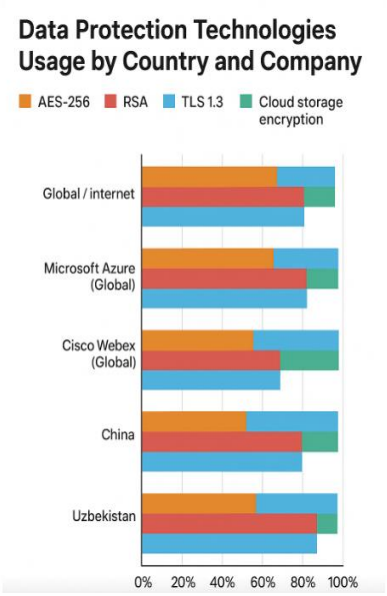

Fig 11. Data protection technologies usage by country and cpmpany

Download social media applications from official sources only: for instance, from Google Play, the Apple App Store, or an official website of the application. This can guarantee that the downloaded app is genuine, secure, and not containing malware or other kinds of malicious modifications. Using official sources ensures your personal data and device are not jeopardized by fake or other types of malicious apps [13].

It means regularly checking through the permissions to see which of these applications on your device have access to things such as your camera, microphone, contacts, location, or storage. You will be able to ensure that apps use no more permissions than they actually need and that your personal data is kept safe.

Steer clear of suspicious ads, links, or bots, as this implies one should not click on advertisements, URLs, or automated accounts that appear to be suspicious, unfamiliar, or untrusted. These often carry malware, phishing attempts, or scams that would compromise personal information or infect a device. You minimize the risk of data theft and fraud by ignoring or blocking them. In other words, avoiding suspicious adverts, links, and bots protects your personal data and device from harm.

Real-time scanning of malicious links means that any link you click or receive is immediately checked by some kind of security system or software to see if it's dangerous. It helps in the detection of phishing sites, malware, or harmful downloads and stops them before they actually harm your device or leak personal information.

IP and DNS filtering involve the use of network security measures to block access to websites that are either known or suspected to be malicious. IP filtering blocks traffic coming from certain IP addresses, while DNS filtering prevents your device from resolving the domain name of dangerous sites. It helps prevent users from accessing phishing websites, scam web pages, or malware-hosting sites to protect personal data and devices.

Keeping firewalls and antivirus software up to date means updating these security tools periodically to the latest version. Firewalls monitor and control network traffic going in and out to block unauthorized access, while antivirus programs scan, detect, and remove malware and viruses, among other threats [13].

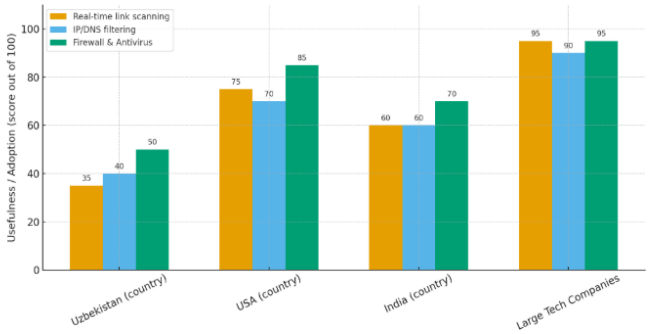

Fig 12. Comparative usefulness/adoption of security measures

It involves the design and delivery of educational programs meant to interactively teach users (employees, students, or the general user) about cybersecurity principles, threats, and safe practices. Such a program is hands-on, engaging, and practical rather than theoretical [14].

Giving instructions on recognizing phishing and malicious files involves telling users to be wary of any emails or messages that may seem fake, not to click on suspicious links, not to open unknown files, and never to give out sensitive personal or financial information to unknown sources. Users should also keep antivirus and system updates up to date, not enable macros in documents from unknown senders, and report any suspicious messages or files to the IT department. These guidelines are for assisting them in real-world cyber-attack protection.

Regular notification of cybersecurity rules and current or new threats serves to remind users. It keeps them from forgetting safe practices, what to do in risky situations, and reinforces the overall security culture of an organization. Examples of these are updating passwords, two-factor authentication, not clicking on suspicious links, and keeping antivirus and system updates current.

Conclusion. To put it all together, the protection of user data from malware on social networks relies fundamentally on technical, organizational, and educational measures. The availability of strong authentication methods increases-because of two-factor or multi-factor authentication and biometric verification-the difficulty of unauthorized access to accounts. AES-256, RSA, and TLS 1.3 encryption protocols protect the data at rest and in motion, while real-time link scanning, IP/DNS filtering, and up-to-date antivirus/firewall systems provide security against malware. Downloading applications only from official sources, keeping an eye on permissions given to applications, and avoiding suspicious links and ads are also very important practices to minimize risks.

Of equal importance is user awareness and training, allowing them to identify phishing attempts, malware, and other types of cyber threats. Continuous education, along with straightforward security policies and notifications, fortifies a proactive cybersecurity culture. Ultimately, highly advanced cryptographic protocols integrated with AI behavioral analysis and adaptive lightweight security ensure a strong defense framework for social network users. Given the continually changing nature of cyber threats, innovation and continuous user education are imperative for retaining privacy and data integrity and overall cybersecurity.

REFERENCES

1. European Network and Information Security Agency (ENISA). Threat Landscape 2021. Available from: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202021.pdf [Accessed 4 November 2025].

2. European Network and Information Security Agency (ENISA). Threat Landscape. Available from: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape [Accessed 4 November 2025].

3. OWASP. Web Security Testing Guide (WSTG). Available from: https://owasp.org/www-project-web-security-testing-guide/ [Accessed 4 November 2025].

4. FIDO Alliance. Passkeys / Passwordless Authentication. Available from: https://fidoalliance.org/passkeys/ [Accessed 4 November 2025].

5. Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. Available from: https://datatracker.ietf.org/doc/html/rfc8446 [Accessed 4 November 2025].

6. National Institute of Standards and Technology (NIST). FIPS 197: Advanced Encryption Standard (AES). Available from: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf [Accessed 4 November 2025].

7. RSA Laboratories. PKCS #1: RSA Cryptography Specifications. RFC 2313. Available from: https://datatracker.ietf.org/doc/html/rfc2313 [Accessed 4 November 2025].

8. Cloudflare Blog. A Detailed Look at RFC 8446 (TLS 1.3). Available from: https://blog.cloudflare.com/rfc-8446-aka-tls-1-3/ [Accessed 4 November 2025].

9. Malicious Phishing Detection in Social Networking Sites: A Systematic Review. ResearchGate. Available from: https://www.researchgate.net/publication/392680217_Multimodal_Phishing_Detection_on_Social_Networking_Sites_A_Systematic_Review [Accessed 4 November 2025].

10. Herath T. B. G., Khanna P., Ahmed M. “Cybersecurity Practices for Social Media Users: A Systematic Literature Review.” *Journal of Cybersecurity and Privacy*, 2022;2:1–18. DOI:10.3390/jcp2010001. Available from: https://doi.org/10.3390/jcp2010001 [Accessed 4 November 2025].

11. Albulayhi M. S., El Khediri S. “A Comprehensive Study on Privacy and Security on Social Media.” *iJIM – International Journal of Interactive Mobile Technologies*, 2022;16(01). DOI:10.3991/ijim.v16i01.27761. Available from: https://doi.org/10.3991/ijim.v16i01.27761 [Accessed 4 November 2025].

12. Koohang A., Floyd K., Yerby J., Paliszkiewicz J. “Social Media Privacy Concerns, Security Concerns, Trust, and Awareness: Empirical Validation of an Instrument.” *Issues in Information Systems*, 2021;22(2):133-145. DOI:10.48009/2_iis_2021_136-149. Available from: https://doi.org/10.48009/2_iis_2021_136-149 [Accessed 4 November 2025].

13. Efe A., Suliman H. “How Privacy Is Threatened from Social Media Communication?” *Online Social Networks and Media*, 2021;6(1):32-45. Available from: https://dergipark.org.tr/en/pub/bbd/issue/59753/817542 [Accessed 4 November 2025].

14. Ahmed L. K. “The Application: Social Media and Their Security.” *ITM Conferences (ICACS 2024)*, 2024. Available from: https://www.itm-conferences.org/articles/itmconf/pdf/2024/07/itmconf_icacs2024_01006.pdf [Accessed 4 November 2025].