International Journal of Multidiscipline

TLEP – International Journal of Multidiscipline
(Technology, Language, Education, and Psychology)
ISSN: 2488-9342 (Print) | 2488-9334 (Online)

Open Access | Peer-Reviewed | Monthly Publication | Impact factor: 8.497 / 2025

Analysis Of Cybersecurity Issues In Social Networks

Murodjon Abdullayev
Department of Information Technology Implementation
and Digitalization of Education.
Academy of the Ministry of Internal Affairs
Tashkent, Uzbekistan
imronkamron17@gmail.com
ORCID: 0009-0001-9832-7575

Odil O‘rinkulov
Department of Digital Technologies and Information Security
Academy of the Ministry of Internal Affairs
Tashkent, Uzbekistan
ourinkulov@gmail.com
ORCID: 0000-0003-2392-9309

Abstract
This article analyzes the current problems of cybersecurity in social networks, their impact on society, users, and information security. In particular, risk factors such as fake accounts, phishing attacks, the spread of malware, and illegal collection and distribution of personal data are studied. Special attention is also paid to the cybersecurity culture that is being formed in the minds of users when using social networks. The article provides an analytical approach based on international experience, statistical data, and modern protective measures. As a result, proposals are put forward for the development of effective security strategies for users and responsible organizations.
Keywords: social networks, cybersecurity, phishing, malware, personal data, artificial intelligence, information security.

Introduction

Although social networks have become an integral part of human activity in recent years, the cybersecurity problems they pose are increasing. According to statistics, the number of social network users worldwide exceeded 5 billion in 2024 [3]. At the same time, phishing attacks, malware, and illegal distribution of information are becoming widespread due to the fact that most users do not pay attention to security measures [1;2].

The main purpose of the article is to analyze cybersecurity problems encountered in social networks, consider technical solutions, and highlight practical measures used in the conditions of Uzbekistan.

Main part

Today, social networks (Facebook, Instagram, Telegram, TikTok, etc.) have become the main arena for global information exchange. According to a Symantec (2024) report, more than 35% of total cyberattacks were carried out through phishing [1]. In Uzbekistan, according to CERT.UZ, more than 17% of users have encountered phishing attacks [4]. Phishing is a type of cyberattack that is carried out to deceive users over the Internet and obtain their personal information (login, password, bank card numbers, passport information, etc.) [3]. Basically, these attacks are carried out through e-mail, social networks, fake websites, messengers [7]. For example, a cybercriminal may send you a link that looks like it comes from a bank and write in it “click on this link to verify your account”. When you click on the link, you will be redirected not to the original bank page, but to the cybercriminal’s fake page, and he will

International Journal of Multidiscipline
TLEP – International Journal of Multidiscipline
(Technology, Language, Education, and Psychology)
ISSN: 2488-9342 (Print) | 2488-9334 (Online)
Open Access | Peer-Reviewed | Monthly Publication | Impact factor: 8.497 / 2025

withdraw all the money from your bank plastic card. There are 6 main types of phishing attacks: 1-Email phishing (deceiving a user through a fake email and forcing them to click on a malicious link), 2-Spear phishing (attack directed at a specific person or organization), 3-Whaling (targeting high-ranking individuals (directors, managers), 4-Smishing (phishing sent via SMS), 5-Vishing (attack carried out through phone calls), 6-Clone phishing (copying the original message, adding a malicious link to it and resending it). 1-rasm

Figure 1. Main types of phishing attacks.

These attacks are often aimed at stealing users' logins and passwords through fake pages, emails, and links.

Users should first of all increase their vigilance to avoid such attacks. It is important to carefully check the domain of any link before clicking on it, not to open letters or messages from unofficial sources, and never send passwords to strangers. Two-factor authentication (2FA) provides additional protection for the account even in the event of a phishing attack.

Malware and botnets. Social networks are an effective channel for distributing malicious programs. We can indicate malware programs as malicious programs. Malware is a program designed to damage a user's computer or network, steal information, disrupt the system, or use it for illegal purposes. There are the following main types of malware programs that are currently widespread. Worm is a type of virus that spreads quickly through various networks, often capturing file resources. Trojan (Trojan horse) – malicious code hidden inside seemingly useful programs. Spyware – secretly monitors users' activities, collects passwords and banking information. Ransomware – encrypts files on devices and demands to be unlocked in exchange for money and other resources.

Worldwide, more than 5 billion 60 million malicious programs (malware) were deployed through social networks in 2020, more than 5 billion 40 million in 2021, more than 5 billion 50 million in 2022, more than 6 billion 6 million in 2023, and more than 6 billion 50 million in 2024. Figure 2.

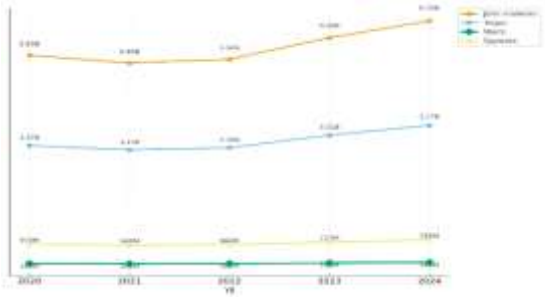

Figure 2. Statistics of malware spread through social networks

According to statistics, the most common types of malware in 2024 are Stealer (data stealer), Loader and RAT (remote control program) [5]. A botnet is a network of many computers and devices (bots) infected with malicious programs. Cybercriminals control them remotely and use them in various attacks. Botnets are one of the most dangerous tools in modern cybercrime, and their operation is based on the scheme of infection → connection to control → execution of commands. During the infection stage, the attacker places malicious programs (viruses, trojans, warm) on devices, using phishing messages, malicious applications, documents or vulnerabilities to carry out this process. During the connection to control, the malware sent turns into a "zombie" without being noticed by the user and works as part of the botnet. Each bot connects to a central server or P2P network controlled by the

attacker, through which the attacker can send commands to all bots. The bot carries out the instructions given by the attacker, i.e. DDoS attacks, spamming, password harvesting, cryptocurrency mining, and other attacks. Figure 3

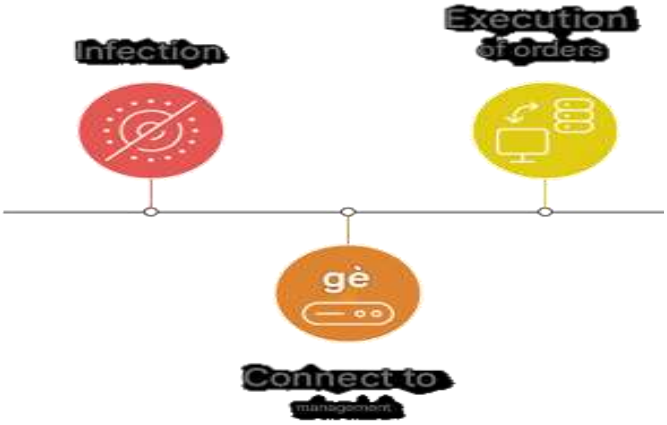

Figure 3. Botnet workflow

We can also see fake accounts on social networks as one of the cybersecurity problems. Fake accounts pose a threat not only to individual users, but also to society as a whole. What is a fake account? What kind of threat does it pose? We will answer similar questions. A fake account is an account on social networks that does not belong to a real person, opened based on false information, which is often used for manipulation, fraud or the dissemination of false information. Currently, the most common types of fake accounts on social networks include bot accounts, impersonation (impersonating someone else), troll accounts, and phishing accounts [8]. The number of fake accounts on social networks is a complex problem that is increasing year by year. While billions of accounts have been removed on Facebook and Instagram, hundreds of thousands of fake or malicious accounts have also been detected on Telegram and TikTok. While official figures are not available for some years, available open sources indicate that: Facebook — more than 1.3 billion fake accounts were removed in 2020, and hundreds of millions of accounts have been removed in subsequent years [9]. Instagram — in some years (for example, in 2024) tens of thousands of fake accounts (especially on sextortion networks) were exposed [9]. On the social network Telegram, tens of thousands of channels and accounts were reported as fake or cloned in 2021 [10].

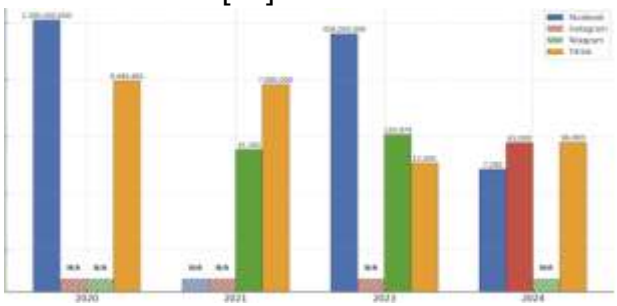

Figure 4. Statistics of fake accounts on social networks.

(N/A - official/annual number not available in open sources)

These indicators show that fake accounts pose a serious threat not only to the information space, but also to political, economic and social security. Therefore, it is urgent for platforms to strengthen their detection and rapid removal mechanisms.

Conclusion

Fake accounts, phishing and malware on social networks remain one of the most serious risk factors for users. There is no single way to protect against them, but it is necessary to apply various measures together: namely, to increase the culture of using social networks among users, to implement basic actions such as strong passwords and two-factor authentication (2FA), and to strengthen cooperation at the state and international levels.

In my opinion, ensuring cybersecurity is not only a technological problem, but also a social and cultural issue. If the cultural actions of users using social networks, the responsibility of social network platforms and strict policies of states are combined, social networks can become a safer and more reliable space for humanity.

References:

Symantec. Internet Security Threat Report. NortonLifeLock, 2023.

Kaspersky Lab. Cybersecurity Report on Social Media Threats, 2023.

Statista. Social Media Users and Fake Accounts Statistics, 2024.

CERT Uzbekistan. O‘zbekiston Respublikasida kiberxavfsizlik holati bo‘yicha hisobot, 2022–2023.

https://any.run/cybersecurity-blog/malware-trends-2024

Jalilov A. “Ijtimoiy tarmoqlarda axborot xavfsizligi muammolari”. Axborot texnologiyalari jurnali, 2023.

Oxford Dictionary of Cyber Security, 2024

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. Communications of the ACM, 59(7), 96–104.

Meta Transparency Center. (2020–2024). Community Standards Enforcement Reports & Coordinated Inauthentic Behavior Reports. Meta Platforms, Inc.

TikTok Transparency Reports. (2020–2024). Community Guidelines Enforcement. TikTok Pte. Ltd.

Urinkulov, O., & Abdullayev, M. (2023, July). Models and algorithms for optimizing legal information retrieval in the corporate network of academic libraries. In SOCIETY. INTEGRATION. EDUCATION. Proceedings of the International Scientific Conference (Vol. 1, pp. 254-263).

Urinkulov, O. CREATION OF INTELLIGENCE SYSTEMS RELATED TO INFORMATION-LIBRARY ACTIVITIES. (2024). DTAI – 2024, 1(DTAI), 388-390. https://dtai.tsue.uz/index.php/DTAI2024/article/view/urinkulovd