Cybersecurity threats and prevention technologies

Ravshan Mallayev
Mubina Khabibullayeva
Uzbekistan State World Languages University

Abstract: *Cybersecurity threats are examined based on malicious APK files, JPG exploits, vulnerabilities in mobile devices, and user errors, which pose risks to financial and personal data. Additionally, modern technologies and practical methods to mitigate and prevent these threats are proposed.*
Keywords: *cybersecurity, mobile security, malware, APK files, JPG exploits, social networks, phishing, mobile banking, information security, cyber threats, social manipulation, cybercrime, protection technologies, permission management, authentication, sandbox, antivirus systems, Android vulnerabilities*

Introduction. In recent years, the growth of the internet, widespread use of social networks, and rapid adoption of mobile devices have heightened the importance of cybersecurity issues. In Uzbekistan and worldwide, cases involving various forms of fraud, malicious files, APK-based software attacks, and social manipulation techniques have sharply increased among users.
Particularly on platforms such as Instagram, Telegram, and Facebook, financial fraud has proliferated through malicious APK or JPG files accompanied by captions like “wedding video”, “invitation”, “I sent a photo”, or “important file”. These situations attract users’ attention but involve risky technical processes.
This article aims to elucidate modern cybersecurity threats from a scientific perspective, analyze key vulnerabilities in mobile devices, and present effective methods for their prevention.
Main Section
The Concept and Relevance of Cybersecurity:
Cybersecurity refers to the comprehensive set of processes, technologies, and practices designed to protect computer systems, networks, software, and data from unauthorized access, attacks, malware, and other digital threats.
Cybersecurity encompasses technical, organizational, and software measures aimed at safeguarding information from unauthorized access, modification, distribution, or destruction. According to experts, global annual losses due to cybercrime amount to billions of dollars. Mobile devices remain one of the most targeted platforms. Increasing public awareness and conducting preventive measures in communal spaces can significantly reduce such incidents.
The Relevance of Cybersecurity
Today, as digital technologies permeate all aspects of life, the importance of cybersecurity is paramount:
Increased Value of Data: The need to protect personal data, bank cards, and state secrets is growing.
Rise in Cyberattacks: Attacks such as hacking, phishing, and DDoS are intensifying.
Growth of the Digital Economy: As businesses digitize, their vulnerability to attacks also increases.
National Security: Cybercrime, information warfare, and cyberterrorism have become strategic threats to states.
Cybersecurity has become an integral part of the modern digital society, playing a crucial role in protecting information, systems, and personal lives.

In the context of Uzbekistan, the most common types of cyber threats prevalent in our daily digital lives include: Malicious Software (Malware, Spyware, Trojan). These harmful programs infiltrate systems without user consent to:

Steal personal data;

Gain access to banking applications, including personal bank cards, even enabling large loans to be issued in another person's name;

Corrupt personal files;

Remotely control phones and computers. This can also occur via Wi-Fi servers, allowing data to be copied, which is increasingly common today.

Currently, APK attacks rank among the most frequently used cyberattacks in Uzbekistan.

APK-Based Attacks

These are a type of cyberattack carried out through specially crafted or modified APK files designed to harm or gain unauthorized access to devices running the Android operating system.

Since the Android system has an open architecture, APK files downloaded from untrusted sources can lead to cyberattacks resulting in:

Unauthorized copying of SMS, call logs, contacts, and control over banking apps, including all personal data. To prevent this, the Ministry of Internal Affairs of Uzbekistan has issued multiple warnings to the public, contributing to a reduction in such crimes.

Enabling full device control via “Accessibility Service”, allowing fraudsters to manage mobile banking apps, read SMS codes, and withdraw all funds from user accounts.

Social Media Exploits via JPG/PNG Files

Cybercriminals also distribute hidden exploits disguised as JPG/PNG files through social networks. While appearing as ordinary images, some malicious files may contain hidden code or text that exploits device vulnerabilities to activate malware. Typically, an image itself does not directly steal money-it is supplemented with additional specialized programs.

Social Engineering

This cyberattack method relies on human psychology rather than technical tools to deceive, manipulate, and obtain confidential information. The most common tactics include:

“I sent you an invitation, open it”;

“Wedding video”;

“A complaint has been filed in your name”;

“You have won a prize”;

“Court summons”.

These methods aim not to threaten us directly but to gain our trust as users and exploit it. Unfortunately, many among us have fallen victim to such fraudsters.

Vulnerabilities in Mobile Devices

Cybercriminals can exploit unpatched (or outdated) flaws in Android or iOS systems to gain access to devices. Failure to install updates promptly increases the risk.

Many users do not fully read the permissions requested by the apps they install, unaware of the consequences. While modern phones, such as new Android or iOS devices, may handle this well, owners of other mobile devices face challenges. Primarily, when installing such applications, phones or computers display notifications like “This app or program poses a risk. Install or deny?” Heeding these warnings and installing only official applications is advisable.

Unsecured Wi-Fi Networks

Public, open Wi-Fi networks without passwords can facilitate Man-in-the-Middle (MITM) attacks. As our saying goes, “Free cheese is only in a mousetrap!” Today, many have fallen into such “traps”.

Failure to install timely updates leaves devices vulnerable to exploits targeting old version flaws, making unauthorized access easier for fraudsters. Regularly updating all software is essential to mitigating cybercrime.

Consequences of Cyber Threats

Theft of funds via mobile banking. In such cases, victims should never share received SMS codes, even if requested by someone claiming to be from the bank.

Dissemination of personal photos and correspondence for illegal purposes, which may result in administrative penalties and fines under the law by the Ministry of Internal Affairs;

Sale of identification data;

Psychological harm and loss of trust.

Cybersecurity Assurance Technologies

Antivirus and Anti-Malware Systems: These help detect malicious files in real-time on mobile devices and notify users to prevent harm.

Sandbox Technologies: They run suspicious programs in an isolated environment, allowing us to test applications without risking harm to the device's internal system if they are malicious.

Two-Factor Authentication: This significantly enhances account security for banking apps and social networks. Installing it on messengers and Meta platforms like Telegram, Instagram, and Facebook is highly beneficial.

Permission Management: Android 10+ versions include mechanisms for granting limited permissions to each application.

As highlighted above, fostering cyber awareness among the population remains crucial to addressing these issues:

Avoid installing APKs from unknown sources;

Verify files before opening them;

Refrain from using public Wi-Fi for banking or financial transactions;

Regularly update passwords.

Conclusion

Cybersecurity is an inseparable part of our modern digital society and a vital skill, especially for youth and students. Cybercrimes carried out through malicious APK and JPG files pose serious risks in Uzbekistan's digital landscape. As analyzed in this article, alongside technical threats, user unawareness remains a fundamental issue. Therefore, alongside technical protection tools, enhancing public digital literacy is the most effective path to cybersecurity.

References

1. Ergashevich, E. A., & Zufar o'g'li, A. M. (2024). Components of modern information technology infrastructure. Journal of Innovation in Education and Social Research, 2(1), 154–157.

2. Ministry of Development of Information Technologies and Communications of Uzbekistan - official information.

3. Urinovich, K. A., Qobiljonovich, R. O., Baxtiyorvich, R. S., & Abdulakhatov, M. M. (2021). Modern content and concept of digital economy. ACADEMICIA An International Multidisciplinary Research Journal, 11(11), 829-832.

4. Abdullayeva, P. U. (2024). TARJIMA JARAYONIDA YUZAGA KELADIGAN MADANIY MUAMMOLAR. Экономика и социум, (11-1 (126)), 6-10.

5. Sofoyeva, F. D. (2025). SQL tili va SQL operatorlarini yozish. Science and Education, 6(12), 69-74.

6. qizi Abdusalomova, Istoraxon Ilhom, and Marjona Komiljon qizi Maxmudova. "EFFECTIVENESS OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN PERSONALIZING THE LEARNING PROCESS." International Conference Platform. No. 6. 2025.
7. Rajabov, Sherzod, and Istora Abdusalomova. "Raqamli Texnologiyalarning Makroiqtisodiy Barqarorlikka Ta'siri." Green Economy and Development 3.6: 665802.
8. qizi Abdusalomova I. I. et al. COMPLIANCE WITH ARTIFICIAL INTELLIGENCE (AI) ETHICS IN EDUCATION AND SAFETY ISSUES //International Conference Platform. – 2025. – №. 6. – С. 191-193.
9. Rajabov, Sherzod, and Shakhrizoda Sultonmurotova. "THE EVOLUTION OF TEACHING METHODS IN THE CONTEX
10. qizi Sultonmurotova, Shakhrizoda Muzaffar. "Effectiveness and development prospects of digital-pedagogical integration in English language education." Academic Journal of Science, Technology and Education 1.5 (2025): 16-20.T OF DIGITAL TRANSFORMATION." International Conference Platform. No. 6. 2025.