World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-46, May-2025
ISSN: 2749-3601

CYBERCRIMES COMMITTED THROUGH PHISHING AND RANSOMWARE ATTACKS IN UZBEKISTAN: ANALYSIS AND PROTECTIVE MEASURES

Qobilov Shokir Anvarovich, Expert Advisor on Legal Issues at the Inson Social Services Center in Yangihayot District, National Agency for Social Protection under the President of the Republic of Uzbekistan.

Article history:

Received: 24th February 2025
Accepted: 20th March 2025

Abstract:

In recent years, due to the rapid development of information technologies and artificial intelligence, cybercrime has taken on new forms and content. In particular, cyberattacks carried out using artificial intelligence - phishing, ransomware, deepfake, botnets and automated attacks - pose a serious threat to the security of society and individuals. This article provides a detailed analysis of the state of modern cybercrimes in Uzbekistan, their mechanisms of implementation, the level of distribution, consequences, and measures that are being used and should be taken against them. In particular, cybercrimes such as illegal seizure of personal data, hacking of financial accounts, false information sent via e-mail (phishing), and software encryption and ransom demands (ransomware) are comprehensively analyzed. The article presents international experiences, legal mechanisms, technical and preventive approaches to ensuring cybersecurity. At the same time, the need to increase the culture of information security and raise the digital awareness of the population and organizations is emphasized. This study includes scientific and practical proposals and recommendations aimed at strengthening the fight against cybercrime and improving the state security system in Uzbekistan.

Keywords: Cybercrime, information security, artificial intelligence, phishing, ransomware, cyberthreat, personal data, information technologies, cyberprotection, legal measures, digital security, Uzbekistan, combating cybercrime, prevention, international experience, intelligent technologies, computer crimes, information protection, digital awareness.

In the modern world, information and communication technologies (ICT) have penetrated all aspects of human life. Digitalization processes have created unprecedented opportunities in the economy, education, healthcare, public administration and the private sector, but along with these processes, new and complex cybersecurity threats have also emerged. In developing countries like Uzbekistan, the rapid growth of Internet use, the expansion of e-commerce, online banking and digital services have given rise to new forms of cybercrime. In particular, types of cybercrime such as phishing (phishing attacks) and ransomware (paying programs) are emerging as a serious source of danger for individuals, business organizations, government institutions and the country's digital infrastructure as a whole. These threats lead not only to financial losses, but also to multifaceted consequences such as social distrust, theft of personal data, psychological stress and undermining of national security. Uzbekistan's efforts to develop digital infrastructure, in particular, to increase internet speed, expand e-services, and strengthen the digital economy, as part of its Digital Uzbekistan 2030 strategy, require new and comprehensive approaches to cybersecurity. This article is devoted to an in-depth analysis of the characteristics of phishing and ransomware attacks in the context of Uzbekistan, an assessment of their economic, social, legal, and technical consequences, and the proposal of effective protective measures against them. The article aims to identify the relevance of cybercrimes in the country, provide practical recommendations for their prevention, address existing problems in the field of cybersecurity, and discuss future prospects.

The global growth of cybercrime has become a major concern for global security and the economy in recent years. According to Cybersecurity Ventures' forecasts for 2025, cybercrime is expected to cost the global economy $10.5 trillion annually, which is more financial losses than drug trafficking, human trafficking, or other traditional types of crime. This growth in cybercrime is mainly due to the expansion of digital technologies, the popularization of Internet use, and the sophistication of cyberattack methods. The number of cybercrime in Uzbekistan has increased significantly in the past five years. According to statistics from the Ministry of Internal Affairs for 2024, cybercrime accounts for 6.2% of total crime, which is 10 times more

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-46, May-2025
ISSN: 2749-3601

than in 2020. In particular, the number of cyberattacks against websites in the "uz" domain exceeded 8.2 million in 2024, which clearly demonstrates the vulnerabilities in the country's digital infrastructure. The majority of these attacks are carried out using phishing and ransomware methods, which emphasizes the importance of not only technical, but also social and organizational measures in the field of cybersecurity.

Phishing attacks are the most widespread and relatively inexpensive method used by cybercriminals. These attacks are based on deceiving users through fake emails, SMS, social media messages or websites that appear to be from a trusted source. In Uzbekistan, phishing attacks are often aimed at stealing bank card details, online payment systems (e.g. Payme, Click, Uzcard) and personal identification data (passport numbers, logins and passwords). For example, through fake messages sent to users on behalf of local banks or payment systems, they are redirected to specially created websites, where they are required to enter their login and password information. The success of such attacks is often associated with the low digital literacy of users, lack of knowledge about cybersecurity and the sophistication of social engineering methods. According to Interpol, more than 1.5 million phishing messages are distributed globally every day, and in Uzbekistan, a significant portion of these messages are directed at local users, in particular, citizens who actively use banking services. In 2024, about $15 million in citizens' funds were stolen due to phishing attacks in Uzbekistan, which indicates the severity of the problem.

Ransomware attacks are more dangerous and sophisticated than phishing, encrypting user systems, restricting access to data, and demanding payment, usually in the form of cryptocurrency (Bitcoin, Ethereum), for recovery. According to Kaspersky Lab, in 2024, the global number of ransomware attacks increased by 78% compared to 2020, and the damage exceeded $ 25 billion. In Uzbekistan, ransomware attacks are mainly aimed at the banking sector, payment systems, small and medium-sized businesses, as well as government institutions. For example, in 2023, a ransomware attack against one of the largest local banks in Tashkent encrypted customer data and forced the organization to pay a ransom of about $ 50,000. In addition, in 2024, a ransomware attack was carried out against one of the e-commerce platforms in Uzbekistan, which compromised the data of platform users and caused more than $ 30,000 in damage to the company. The majority of these attacks are directed from abroad, particularly from Russia, China, the Netherlands, India, and the United States, but there is also an active participation of local cybercriminals. A geographical analysis of the attacks shows that 92% of cyberattacks against Uzbekistan are carried out through transnational networks, which emphasizes the need for international cooperation and information exchange.

The economic and social consequences of cybercrime are particularly serious for countries developing a digital economy, such as Uzbekistan. From an economic perspective, cyberattacks can cause significant financial losses for organizations, including data recovery costs, loss of customer trust, disruption of business processes, and reputational damage. In Uzbekistan, small and medium-sized businesses suffered an average of $10,000 in losses from cyberattacks in 2024, while large organizations suffered losses of up to $100,000. For example, one local telecommunications company was forced to shut down its services for a week in 2024 due to a ransomware attack, which resulted in millions of dollars in losses and loss of customer trust. Socially, phishing and ransomware attacks compromise users' personal information, leading to psychological stress, insecurity, fear of using digital services, and a general decline in trust in the internet . leads to. Increasing internet speed, expanding digital services, developing e-commerce and e-government systems within the framework of the "Digital Uzbekistan – 2030" strategy are creating new opportunities for cybercriminals, which requires new approaches to ensuring cybersecurity. In addition, cyberattacks lead to the theft of citizens' personal data, such as passport numbers, bank card details and social network accounts, which poses a serious threat to their personal and financial security.

Uzbekistan is actively implementing legal and organizational measures to combat cybercrime. The Presidential Decree (No. PP-153) adopted on April 30, 2025, is aimed at strengthening the fight against cybercrime, and the Ministry of Internal Affairs is designated as the main authorized body in this area. According to the resolution, banks, payment system operators and payment organizations are obliged to ensure the financial security of customers. At the same time, administrative and criminal liability has been introduced for persons who allow the use of a bank card, account number or SIM card in their name to commit cybercrime. The Central Bank is introducing a special system to detect and prevent "financial pyramid" fraud schemes, which is an important step against the increase in phishing attacks. The Cybersecurity Center and the Department for Combating Cybercrime of the Ministry of Internal Affairs are also working to monitor cyberattacks, identify their sources, and respond quickly. For example, in 2024, these organizations identified and blocked more than 500 phishing websites,

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-46, May-2025
ISSN: 2749-3601

which was an important step towards strengthening cybersecurity in the country. However, despite these measures, problems with the cybersecurity infrastructure, in particular, the lack of qualified specialists and limited technical resources, further complicate the problem.

Technical measures are essential for cybersecurity. Strong encryption algorithms, such as AES-256 and RSA, have been proven to be effective in protecting sensitive data. Network security includes firewalls, intrusion detection and prevention systems (IDS/IPS), and regular software updates. Large banks and telecommunications companies in Uzbekistan are implementing SIEM (Security Information and Event Management) systems to strengthen network security, which allow them to detect and respond to cyberattacks in real time. Organizational measures include training employees on cybersecurity, implementing two-factor authentication (2FA), regularly backing up data, and developing contingency plans. For example, large banks in Uzbekistan have made 2FA mandatory for customers, which has significantly reduced the effectiveness of phishing attacks. However, the shortage of unqualified cybersecurity specialists is further exacerbating the problem. According to statistics, there are only about 3,000 cybersecurity specialists in Uzbekistan, which is completely insufficient given the growth rates of the country's digital economy and infrastructure. In addition, problems in the cybersecurity education system, namely the lack of curricula that meet modern technologies and cybersecurity standards, are slowing down the process of training specialists.

Increasing the digital literacy of users is of strategic importance in the fight against cybercrime. In Uzbekistan, November of each year is declared the "Month of Promoting Cyber Culture", during which targeted advertisements, videos and educational materials are distributed on the Internet and social networks warning about cybercrime. Employees are trained to identify phishing messages, create strong passwords, and avoid dangerous websites and links. For example, in 2024, more than 50 thousand employees in large organizations in Uzbekistan underwent special training on cybersecurity, which helped reduce the success rate of phishing attacks by 30%. Studies show that if more than 80% of employees have minimal knowledge of security, the success rate of phishing and other social engineering-based attacks decreases by 60%. Despite the 3rd, an important step in developing cybersecurity education in Uzbekistan is the introduction of special cybersecurity courses in schools and universities. This initiative will serve to increase digital literacy among young people and train unskilled personnel in the cybersecurity field in the future.

Transnational cooperation plays an important role in ensuring cybersecurity. Given that the majority of cyberattacks against Uzbekistan originate from abroad, in particular from Russia, China, the Netherlands, India, and the United States, it is necessary to exchange information and develop joint strategies with international organizations, such as Interpol, Europol, and the UN Global Compact. For example, bilateral agreements on cybersecurity with Russia and China will help strengthen Uzbekistan's digital infrastructure. Uzbekistan's cooperation on cybersecurity within the Shanghai Cooperation Organization (SCO) and the Economic Cooperation Organization (ECO) will also serve to strengthen regional security. In 2024, an agreement was signed between Uzbekistan and Kazakhstan on joint measures against cyberattacks, which was an important step towards improving cybersecurity in the region.

Future prospects in the field of cybersecurity depend on the application of artificial intelligence (AI) and machine learning (ML) technologies. AI-based systems allow for real-time detection, analysis, and countermeasures against cyberattacks. For example, Palo Alto Networks' AI-based security platform is capable of detecting 95% of cyberattacks. The introduction of such technologies in Uzbekistan can significantly improve the cybersecurity infrastructure, but this process requires significant financial resources, highly qualified specialists, and long-term investments from the state. In addition, the use of blockchain technologies plays an important role in ensuring data integrity and reducing the risk of cyberattacks. For example, blockchain-based payment systems help prevent financial losses due to phishing and ransomware attacks.

In conclusion, cybercrimes committed in Uzbekistan through phishing and ransomware attacks pose a serious threat to the country's economic, social and national security against the backdrop of the rapid development of the digital economy and infrastructure. These attacks lead to multifaceted consequences, including financial losses, theft of personal data, distrust among citizens and organizations, fear of using digital services, and the weakening of the country's digital infrastructure in general. The successful implementation of the "Digital Uzbekistan - 2030" strategy depends on strengthening cybersecurity, as the expansion of the digital economy and electronic services creates new opportunities for cybercriminals. To ensure cybersecurity, legal reforms, technical innovations, organizational measures and educational

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-46, May-2025
ISSN: 2749-3601

initiatives must be introduced in an integrated manner. Increasing the digital literacy of users, in particular, expanding knowledge on how to detect and protect against phishing and ransomware attacks, is of great importance. Strengthening international cooperation, in particular, information exchange and joint measures against cyberattacks, will serve to strengthen Uzbekistan's cybersecurity infrastructure. The introduction of modern technologies such as artificial intelligence, machine learning, and blockchain will bring cybersecurity to a higher level, but this process requires long-term investments and training of unskilled personnel. These approaches and measures will serve not only to strengthen cybersecurity, but also to strengthen Uzbekistan's position in the global digital economy, reliably protect its digital future, and transform the country into a stable and resilient state against cybercrime. In the future, further investments in cybersecurity, the use of international experience, and increasing digital literacy will help increase Uzbekistan's competitiveness in the digital world and shape it as a state that meets global cybersecurity standards.

LIST OF USED LITERATURE

1. Criminal Code of the Republic of Uzbekistan. – Tashkent: Adolat, 2023. – 420 p.
2. Law of the Republic of Uzbekistan "On Electronic Government". – Tashkent: Adolat, 2021. – 35 p.
3. Resolution of the President of the Republic of Uzbekistan No. PP-3837 "On measures to further improve the cybersecurity system". – Tashkent, 2023. – 12 p.
4. Tokhtaev A.A., Karimov M.M. Fundamentals of Information Security. – Tashkent: Science and Technology, 2022. – 276 p.
5. Nazirov M., Juraev R. Cybercrime: modern mistakes and methods of protection. – Tashkent: Economics and Law, 2022. – 198 p.
6. "Cybercrimes and methods of combating them" (collection of scientific and practical articles). – Tashkent: Publishing House of the Academy of the Ministry of Internal Affairs, 2023. – 163 p.
7. Law of the Republic of Uzbekistan "On Informatization". – Tashkent: Adolat, 2022. – 27 p.
8. CERT.uz – Official website of the Computer Incident Response Service: https://www.cert.uz (accessed on May 5, 2025) .