pISSN:2349-5707 Volume:13,Issue 5, May -2026 eISSN:2349-5715

CYBERCRIME IN UZBEKISTAN

Odiljon Bobomurodov
First-year student, Sorbonne University
Uzbekistan

https://doi.org/10.5281/zenodo.20200137

Abstract: This article examines cybercrime in Uzbekistan as a growing legal and social problem accompanying the rapid expansion of digital technologies. It analyzes the most common forms of cybercrime, including internet fraud, phishing, unauthorized access to digital accounts, and theft of personal data. Special attention is given to the factors that make citizens vulnerable to online threats, particularly limited digital literacy, psychological manipulation, and insufficient observance of basic cybersecurity practices. The article also reviews the legal framework of the Republic of Uzbekistan, including criminal liability for offenses in the sphere of information technologies, and considers recent state measures aimed at improving cybercrime prevention. The analysis shows that effective counteraction to cybercrime requires a combination of legal regulation, institutional response, technological protection, and public awareness.

Keywords: cybercrime, internet fraud, phishing, digital security, Uzbekistan.

Аннотация: В статье рассматривается киберпреступность в Узбекистане как актуальная правовая и социальная проблема, сопровождающая процесс цифровизации общества. Анализируются наиболее распространенные формы киберпреступлений, включая интернет-мошенничество, фишинг, несанкционированный доступ к цифровым аккаунтам и хищение персональных данных. Особое внимание уделяется факторам уязвимости граждан к онлайн-угрозам, в частности недостаточному уровню цифровой грамотности, психологическому воздействию со стороны злоумышленников и несоблюдению базовых правил кибербезопасности. В статье также рассматривается правовая база Республики Узбекистан, предусматривающая ответственность за преступления в сфере информационных технологий, и анализируются недавние государственные меры, направленные на профилактику киберпреступности. Проведенный анализ показывает, что эффективное противодействие киберпреступности возможно лишь при сочетании правового регулирования, институциональных мер, технологической защиты и повышения общественной осведомленности.

Ключевые слова: киберпреступность, интернет-мошенничество, фишинг, цифровая безопасность, Узбекистан.

Introduction

The rapid development of digital technologies has transformed communication, commerce, banking, and access to information. At the same time, it has created new opportunities for criminal activity. Cybercrime has become one of the most serious threats to the security of individuals and society in Uzbekistan.

This article aims to examine cybercrime as a contemporary phenomenon, identify its most common manifestations, and assess the legal and institutional measures being taken to combat it. Particular attention is paid to the role of public awareness and individual responsibility in reducing risks.

Cybercrime as a Problem

pISSN:2349-5707 Volume:13,Issue 5, May -2026 eISSN:2349-5715

Cybercrime refers to unlawful acts committed through computers, mobile devices, or internet-based systems. Such offenses may involve financial theft, personal data breaches, account compromise, or the unauthorized distribution of malicious software. In many cases, offenders exploit trust rather than technical complexity, using social engineering to manipulate victims into revealing confidential information.

A common misconception is that cybercriminals always possess advanced programming skills. In reality, many fraudulent schemes rely on psychological pressure, deception, and impersonation of trusted institutions.

Main Forms

The most widespread forms of cybercrime in Uzbekistan include fraudulent phone calls from persons posing as bank employees, phishing messages containing malicious links, unauthorized access to messaging or social media accounts, fake online stores, and deceptive online job offers. These schemes often imitate legitimate services and create a sense of urgency, which reduces the victim's ability to react critically.

Such crimes are particularly dangerous because they can be committed remotely and at a low cost, while causing substantial financial and emotional harm.

Vulnerability Factors

Several factors explain why citizens fall victim to cybercrime. The first is insufficient digital literacy, especially regarding the safe use of banking applications and messaging platforms. The second is fear, since fraudsters often present themselves as representatives of banks or state institutions and claim that immediate action is required.

The third factor is trust. Many victims assume that a polite voice, familiar language, or knowledge of personal details indicates legitimacy. The fourth factor is negligence, including weak passwords, absence of two-factor authentication, and failure to verify sellers or websites before making payments.

Legal and State Response

Uzbekistan has strengthened its legal response to cybercrime in recent years. The Criminal Code includes provisions on the creation and distribution of malicious software, unauthorized access to computer information, and computer fraud. In 2025 and 2026, the government introduced additional measures to reinforce accountability and improve prevention mechanisms.

These reforms show that cybercrime is being treated as a matter of public security. At the same time, enforcement remains difficult because offenders may use anonymous accounts, third-party devices, or infrastructure located outside the country.

Prevention

The most effective preventive measures include never sharing verification codes, avoiding suspicious links, using unique passwords, enabling two-factor authentication, and verifying online shops before paying. It is also important to educate family members, especially elderly users, who may be more vulnerable to deception.

Cybersecurity education should be integrated more systematically into schools, universities, and public awareness programs. A sustainable response requires not only punishment after the offense, but also prevention before harm occurs.

pISSN:2349-5707 Volume:13,Issue 5, May -2026 eISSN:2349-5715

Conclusion

Cybercrime in Uzbekistan is a serious and expanding threat linked to the growth of digital services and online financial activity. Although the state has taken important steps to improve legislation, institutional coordination, and public safety measures, these efforts must be supported by individual vigilance and digital literacy.

A comprehensive approach combining law, technology, and education is necessary to reduce the scale of cybercrime. In the digital environment, security depends not only on state institutions, but also on the informed behavior of each user.

References

1. Criminal Code of the Republic of Uzbekistan, Articles 278¹, 278³, 278⁴. — https://lex.uz/

2. Presidential Decree No. UP-38 of 10 March 2026 on the Cybersecurity Strategy of the Republic of Uzbekistan. — https://lex.uz/docs/8084828

3. Uzbekistan strengthens measures to combat cybercrime. — UzDaily

4. Government proposes tougher measures against cybercrime and financial pyramids. — Kun.uz

5. Cybercrime prevention and youth digital resilience initiatives in Uzbekistan. — UNODC/UNDP

6. Legislative and analytical materials on cybersecurity in Uzbekistan. — https://lex.uz/