Western European Journal of Historical Events and Social Science
Volume 04, Issue 06, June 2026
https://westerneuropeanstudies.com/index.php/4
ISSN (E): 2942-1926 Open Access| Peer Reviewed

CYBERCRIMES: DEFINITION AND LEGAL LIABILITY

DJUMAYEV Shokhjakhon Begimkul ugli
Senior lecturer of Training Institute for lawyers,
PhD candidate of the Law Enforcement Academy of
the Republic of Uzbekistan
E-mail: Shohjahon7474@gmail.com

ANNOTATITON
This article examines the nature and significance of cybercrime, the necessity of combating it, and the legal measures of liability imposed for such offenses. It analyzes relevant international legal instruments, considers emerging forms of cybercrime, and provides an overview of protection against one of its most widespread forms—cyber fraud—as well as the legal liability applicable to it. The article also presents international and national statistical data to highlight the relevance and importance of the topic.
Signal words: cybercrime, legal liability, cyber fraud, hacker, protection methods, statistical data.

In the 21st century, the rapid development of information technologies has brought numerous conveniences to humanity. At the same time, however, it has also given rise to new threats, particularly cybercrime. Cybercrime has become one of the most pressing challenges of the modern era, posing serious threats to national security, economic stability, and the privacy of individuals.

As technology continues to advance, methods of committing crimes are becoming increasingly sophisticated, while significant changes are occurring in people's perceptions and behavior.

Cybercrime refers to a socially dangerous act committed through information technologies, computer systems, or the Internet. **Cybercriminality**, in turn, is criminal activity carried out using computers, computer networks, or network devices. Most cybercrimes are committed by cybercriminals or hackers with the intention of obtaining illegal financial gain.

According to legal literature, the main types of cybercrime include:

- **Hacking** – unauthorized access to a computer or network;
- **Phishing** – obtaining users' personal information through fraudulent websites or deceptive messages;
- Distribution of viruses and other malicious software;

Western European Journal of Historical Events and Social Science
Volume 04, Issue 06, June 2026
https://westerneuropeanstudies.com/index.php/4
ISSN (E): 2942-1926 Open Access| Peer Reviewed

- Financial fraud committed through online payment systems;
- Theft and dissemination of personal data;
- Cyberterrorism and attacks against government information systems.

When considering statistical data, experts estimated that the total global cost of cybercrime could reach approximately **USD 10.5 trillion in 2025**.

In 2025, more than **2,000 crimes related to cryptocurrency transactions** were detected in Uzbekistan, preventing the illegal transfer of **UZS 76 billion** out of the country. During the same year, cybercriminals unlawfully misappropriated approximately **UZS 1.9 trillion** belonging to citizens. It is also noteworthy that more than **4,865 cybercrimes** were recorded nationwide in **2021**, **7,570** in **2022**, **6,455** in **2023**, and **over 50,000** in **2024**.

From the perspective of international legal instruments, computer-related fraud is also addressed in the **Convention on Cybercrime (Budapest Convention)**, adopted on **23 November 2001**. According to **Article 8** of the Convention, each Party is required to adopt such legislative and other measures as may be necessary to establish as criminal offenses, under its domestic law, the intentional and unlawful deprivation of another person's property through:

(a) any input, alteration, deletion, or suppression of computer data; or

(b) any interference with the functioning of a computer system,

when committed with fraudulent or dishonest intent to obtain an unlawful economic benefit for oneself or another person.

What legal liability applies to cyber fraud, the most common type of cybercrime?

Today, the most widespread form of cybercrime is **cyber fraud**. Under the legislation of the Republic of Uzbekistan, cyber fraud is currently prosecuted under **Article 168, Part Three, Paragraph "g" of the Criminal Code**, which applies where fraud is committed **through the use of an information system, including information technologies**. In accordance with the applicable sanction, the offender may be sentenced to **imprisonment for a term of five to eight years**.

How can individuals protect themselves against the increasingly common method of cybercrime involving APK files?

First and foremost, the most effective means of protection against cybercrime is **vigilance**. In today's digital environment, this has become an essential requirement.

For example, if a person unknowingly downloads an **APK file** received through the **Telegram** messenger, believing the accompanying persuasive message, it is important to know what steps should immediately be taken. Such malicious files are often accompanied by messages such as:

"Hi! I accidentally found your old videos. They made me laugh so much!"

or

"Congratulations! You have inherited a large amount of money. Click the link below immediately to claim it before it expires!"

Western European Journal of Historical Events and Social Science
Volume 04, Issue 06, June 2026
https://westerneuropeanstudies.com/index.php/4
ISSN (E): 2942-1926 Open Access| Peer Reviewed

These messages are intentionally designed to create urgency and manipulate recipients into acting without careful consideration. Unfortunately, many people continue to fall victim to such deceptive tactics.

If a malicious APK application has already been installed, the following measures are recommended:

1. **Delete your Telegram account immediately.** To prevent cybercriminals from taking control of your Telegram account, deceiving your contacts, or requesting money from them under false pretenses, log in to **my.telegram.org** and deactivate your Telegram account.
2. **Block unauthorized loan applications.** In addition to stealing funds from bank cards, cybercriminals may fraudulently obtain loans in the victim's name. Therefore, visit **my.gov.uz** and use the service **"Prohibit or Remove the Prohibition on Concluding a Credit Agreement"** to temporarily block the issuance of loans in your name.
3. **Immediately notify law enforcement authorities.** In every case of cyber fraud, victims should promptly contact the competent law enforcement agencies, including the Prosecutor's Office or the Internal Affairs bodies, through their emergency or hotline telephone numbers and report the incident without delay.
4. **Install the official "SamCyber102" application.** Download the official **SamCyber102** application from **Google Play** or the **App Store**. Within the application, select the **"Scan Applications"** feature, which will detect malicious applications installed on your device. Afterwards, open your phone's **Settings**, locate the malicious application in the list of installed apps, and uninstall it. Taking these steps will help eliminate malicious software that may lead to cyber fraud.

On **30 April 2025**, the **President of the Republic of Uzbekistan** adopted **Presidential Resolution No. PQ-153, "On Measures to Further Strengthen Efforts to Combat Crimes Committed through Information Technologies."** This Resolution represents an important step toward introducing modern mechanisms for combating cybercrime.

According to the Resolution, the following measures were envisaged:

- The **Ministry of Internal Affairs** was designated as the authorized body responsible for establishing a unified national approach to combating cybercrime in the Republic of Uzbekistan, coordinating the activities of all relevant state authorities and institutions, and ensuring effective inter-agency cooperation in this field.
- Strict responsibility was assigned to the relevant state authorities, organizations, banks, payment system operators, and payment service providers for taking all necessary measures to prevent cybercrime and to enhance the cyber awareness and digital culture of the population.
- Banks, payment system operators, and payment service providers were required to treat the protection of their customers' interests and financial security as a top priority in their day-to-day operations.

Western European Journal of Historical Events and Social Science
Volume 04, Issue 06, June 2026
https://westerneuropeanstudies.com/index.php/4
ISSN (E): 2942-1926 Open Access| Peer Reviewed

- By the end of **2025**, the **Ministry of Internal Affairs**, in cooperation with the relevant ministries and agencies, was tasked with conducting a comprehensive review of existing practices, current technological developments, and advanced international experience, and, on that basis, preparing a draft Law **"On Combating Crimes Committed through the Use of Information Technologies."** The draft law is intended to define the priority areas and operational mechanisms in this field, as well as clearly establish the responsibilities of state authorities, banks, payment system operators, and payment service providers in preventing, detecting, and investigating cybercrime.

Furthermore, within the **General Prosecutor's Office**, a **Department for Ensuring Legality in Combating Cybercrime**, consisting of **six staff positions**, is to be established as part of the Directorate for Supervision over the Implementation of Legislation within the Internal Affairs Bodies. In addition, **44 staff positions** are to be allocated for the establishment of corresponding units within the departments responsible for supervising the implementation of legislation in the Internal Affairs bodies of the territorial prosecutor's offices and the **Transport Prosecutor's Office**. These structural units will exercise prosecutorial supervision over compliance with the law during the investigation and detection of cybercrimes conducted by the Internal Affairs bodies.

Conclusion

In conclusion, cybercrime constitutes one of the most serious forms of transnational crime, posing significant threats to the security of the state, society, and individual citizens in the modern digital era. Preventing cybercrime requires not only strengthening criminal liability but also improving information security mechanisms and cybersecurity infrastructure. At the same time, effective efforts to combat cybercrime require close cooperation among law enforcement agencies, state institutions, and the public. Enhancing digital literacy and strengthening preventive measures remain essential factors in protecting society against cybercrime.

REFERENCES

1. Resolution of the President of the Republic of Uzbekistan No. PR–3723 dated May 14, 2018, **“On Measures to Radically Improve the System of Criminal and Criminal Procedural Legislation”** // National Database of Legislation of the Republic of Uzbekistan.
   URL: https://lex.uz/docs/55471975
2. **Criminal Code of the Republic of Uzbekistan**, adopted on September 22, 1994 // National Database of Legislation of the Republic of Uzbekistan. URL: https://lex.uz/docs/6750126
3. Kudryavtsev, V.N. **General Theory of Crime Qualification**. Moscow, 2007. p. 313.
4. Usmonaliev, M., Bakunov, P. **Criminal Law. General Part**: Textbook for Higher Educational Institutions. Tashkent: Nasaf Publishing House, 2010. p. 553.

Western European Journal of Historical Events and Social Science
Volume 04, Issue 06, June 2026
https://westerneuropeanstudies.com/index.php/4
ISSN (E): 2942-1926 Open Access| Peer Reviewed

5. Xudaykulov, F.X. **The Relationship between the Concepts of Crime and Corpus Delicti and Their Objective and Subjective Elements: Instrumental Analysis and Proposals** // *Journal of Legal Research*, 2021, Vol. 6, No. 11. Also published in: *Oriental Renaissance: Innovative, Educational, Natural and Social Sciences*, Vol. 2, Issue 3, 2022. ISSN 2181-1784.
6. **The Criminal Procedure Code of the Republic of Uzbekistan.** URL: https://lex.uz/docs/-111460