ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23

American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

BE AWARE! CYBER FRAUD: MODERN DECEPTION AND FINANCIAL RISK

Absamatova Zulfiya

Urgench State University

3rd-year student of Jurisprudence

Annotation: This article reveals various methods of cybercrimes that threaten people in today's technological era and explains the measures for protection against them.

Keywords: cybersecurity, fraudsters, social networks, SMS codes, information security, online scams.

In today's digital age, it is difficult to imagine human life without the Internet and modern technologies. Payments, communication, work processes, and many other activities are carried out through virtual platforms. However, alongside these conveniences, various types of cybercrimes have emerged. Modern fraudsters no longer operate in the streets but behind screens, exploiting people's inattention and trust to commit crimes.

If we look back a few decades, crimes were mostly associated with street theft, robbery, or burglary. However, in today's digital world, electronic technology–based crimes have become more prevalent. Cybercriminals often exploit people's trust by pretending to be bank employees, members of certain organizations, or by using fake lottery or prize notifications, claiming to have won prizes through green card lotteries or similar means to obtain victims' personal data.

As a result, people who are unaware of such scams or are new to using modern technologies easily believe these frauds and risk losing their plastic cards and funds from their bank accounts. In recent years, cybercriminals have even managed to access people's personal data from ID cards and passports, using this information to obtain loans and credits under the victims' names.

Across the world — and also in our country — cybercrime is recognized as a global issue. To combat it, various measures, declarations, laws, and resolutions have been adopted. For example, the UN General Assembly adopted a resolution proposed by Russia titled "Countering the use of information and communication technologies for criminal purposes." In Uzbekistan, the Law "On Cybersecurity" (No. O'RQ-764, adopted on April 15, 2022) and the Law "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with Improving Legislation in the Field of Ensuring Cybersecurity" (adopted on December 22, 2024) serve as important legal tools in preventing cybercrimes.

According to Article 3 of the Law of the Republic of Uzbekistan No. O'RQ-764 "On Cybersecurity":

- Cybercrime — is defined as the set of acts committed in cyberspace using software or technical means with the intent to unlawfully access, modify, destroy, or disable information systems or resources.

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

One of the most common methods of cybercrime today involves fraudsters using social networks such as Telegram to deceive users. They send malicious ".apk" files under misleading names like:

"Is this your picture?"

"Wedding Invitation"

"Court Decision"

"You must pay your tax debt"

When individuals who are unaware of the nature of these files open them, cybercriminals gain access to their personal data, enabling them to withdraw money from victims' bank cards and compromise their private information.

When individuals who are unaware of these malicious files open them, cybercriminals gain access to their personal data, allowing them to withdraw funds from victims' bank cards.

The existence of provisions in the Criminal Code of the Republic of Uzbekistan addressing cybercrime clearly indicates that such offenses are becoming more widespread and that combating them has become a national priority. For instance, according to Article 278^6 of the Criminal Code of the Republic of Uzbekistan:

The creation or modification of computer programs with the intent to destroy, block, modify, copy, or obtain information stored or transmitted in a computer system without authorization, as well as the intentional development, use, or dissemination of malicious virus programs, shall be punishable by a fine of one hundred to three hundred times the base calculation amount, or by restriction of liberty for up to two years, or by imprisonment for up to two years.

The same actions:

a) if they cause significant damage;

b) if committed by a group of persons by prior conspiracy;

c) if committed repeatedly or by a dangerous recidivist;

d) if committed by an organized group or in its interests —

shall be punishable by restriction of liberty for two to three years, or imprisonment for two to three years.

Unfortunately, cases where fraudsters deceive people through social networks are also becoming common. They promise unrealistic profits with phrases such as "We will triple, quintuple, or even tenfold your money," and as a result, many victims lose their hard-earned savings. Millions of people who have worked for years to earn their income lose everything due to a single act of carelessness and misplaced trust in fraudsters — a truly tragic situation.

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23

American Academic publishers, volume 05, issue 10,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

In conclusion, in today's digital world, every citizen must learn how to protect themselves and handle personal information with great caution. Let us stay vigilant, for even a moment of negligence can cause irreversible harm to our lives.

References :

1. Criminal Code of the Republic of Uzbekistan. – Tashkent: Adolat, 2024.

2. Law of the Republic of Uzbekistan "On Informatization." – Adopted on December 11, 2003 (with latest amendments).

3. Decree of the President of the Republic of Uzbekistan No. PF–6099 dated November 3, 2020 – "On Measures to Further Improve the Cybersecurity System."

4. United Nations Convention on Cybercrime (2024). – New York: United Nations, 2024.

5. Khabibullaev A. Fundamentals of Information Security. – Tashkent: TUIT Publishing, 2022.

6. Shodiyev B. Cybercrime and Measures to Combat It. – Tashkent: Legal Literature Publishing, 2023.

7. Zayniddinov M. Internet Security and the Culture of Protecting Personal Data. – Law and Society Journal, No. 4, 2023.