The OSCAR PUBLISHING Services
International Journal of Law And Criminology

VOLUME Vol.05 Issue08 2025
PAGE NO. 52-56
DOI 10.37547/ijlc/Volume05Issue08-10

Analysis of Fraud Committed Through Information Technologies

Uralov Sarbon Sardorovich
Tashkent State University of Law, Department of Criminal Procedure Law, Acting Associate Professor, PhD in Law, Uzbekistan

Received: 29 June 2025; **Accepted:** 25 July 2025; **Published:** 27 August 2025

Abstract: This article discusses the most common types of fraud committed in the era of modern information technologies. Basically, in the modern world, cases such as illegally acquiring someone else's property under the guise of social relations, giving it a legal appearance, or staging the method of committing a fraud crime as if it were civil legal relations are covered from a scientific and practical point of view. The conclusion reflects proposals and recommendations aimed at being aware of this crime and preventing becoming its victim.

Keywords: Fraud, information technology, artificial intelligence, criminal-legal relations, civil-legal relations, property transfer, property disposal and use.

Introduction: The main element in the structure of the method of fraud is the method of committing it, the purpose of which is to obtain property that is considered the subject of criminal aggression.

Fraudulent methods are carried out in such a way that the fraudster gains the trust of the victim, as a result of which he hands over property belonging to him to the fraudster. Although the fraud is committed openly for the victim, it is associated with misleading him about certain factual circumstances. Victims often do not realize the fraud immediately, but only after a considerable time. During this time, the fraudster has the opportunity not only to completely seize the property, but also to hide or destroy evidence important to the investigation [1].

Fraud methods are very diverse, but despite this, there is a consistent tendency for them to be repeated and used by the same individuals.

As technology advances, new types of fraud are emerging. The most common of these is cyber fraud. The number of crimes of this type has increased 8-fold in the last 3 years [2].

METHODS

historical, systematic, comparative-legal, analytical, logical, sociological survey, statistical data analysis, study of law enforcement practice were used in the research.

RESULTS

- the broad public views mutual relations with confidence;

- when entering into social relations, they act not within the framework of actions prescribed by law, but within the framework of customs or national traditions;

- does not have complete information about crimes that can be committed through information technologies in a dangerous world;

- This is explained by the fact that when attempts to commit such crimes are detected, the population does not contact law enforcement agencies through rapid communication, and even when they do contact them, the practice of promptly identifying such attempts as attempts to commit such crimes and holding them accountable is not sufficiently established.

DISCUSSION

Anonymous "savior". In this scheme, the fraudster calls people's mobile phones and introduces himself as an employee of the Central Bank, a commercial bank, or a payment system (for example, Click). Then, he tries to gain their trust and emotionally influence them by telling them that the mobile application has been hacked, that the bank card has been blocked, that there are attempts to illegally withdraw money from the

card, and so on, and that if immediate action is not taken, all funds may be lost.

For example, they may say, “Some money was stolen from your bank card, is it you?” [3]. The fraudster will try to confuse you with words like “quickly”, “now”, “I’ll explain later”, “I need it sooner”. In this case, never tell anyone the one-time SMS code sent to your phone related to bank cards, logins and passwords that give access to mobile applications of commercial banks, payment system operators and payment organizations. Using the information received from you (SMS code, login and password, etc.), they will be able to withdraw funds from your bank card or manage it without your permission.

“You have won the contest.” An unknown person contacts you and congratulates you on winning the contest. They then send you a link to receive the money you “won” and tell you to go to the specified website to receive the funds.[4] After you go to the website and enter the plastic card number, expiration date, phone number, and the password from the received SMS notification, all the money on the plastic card is withdrawn within seconds.

Offering gifts and asking for "additional payments," "deposits," or other forms of money transfer are also signs of fraud.

"Add a person to a group." Another type of scam that has been on the rise recently is the practice of offering rewards by adding people to Telegram groups. In this case, scammers also try to obtain phone numbers and credit card details and then withdraw money from the account.

Because of this, it is recommended not to disclose personal account information to strangers, trusting various promotions and contests, otherwise you may become a victim of fraud.

Electronic trading platforms. You place your item for sale on an online trading platform (for example, OLX.UZ). After a while, a buyer appears on the ad and writes to you. They negotiate with you. Then they send you a link saying that they have sent the money for the goods and that they need to check the account. The sent link has a system installed that will withdraw the money from the card. After you log in, they ask for your card number to withdraw your money.

After entering the card number, no money will appear. Then the seller says that there is no money, it is not visible. After that, they send a secret code to your phone and try to withdraw all the funds from your card.

The development of online services is providing people with a number of such conveniences, but at the same time, "virtual fraud" is also on the rise. Fraudsters are now hunting their prey online.

In many cases, citizens fall into the trap of fraudsters due to their ignorance of the rules of using online payments, insufficient virtual knowledge in using bots and channels in social networks. In order not to fall into unpleasant situations, not to become a victim of lies, not to lose money, a little attention, a little diligence is required from a person.

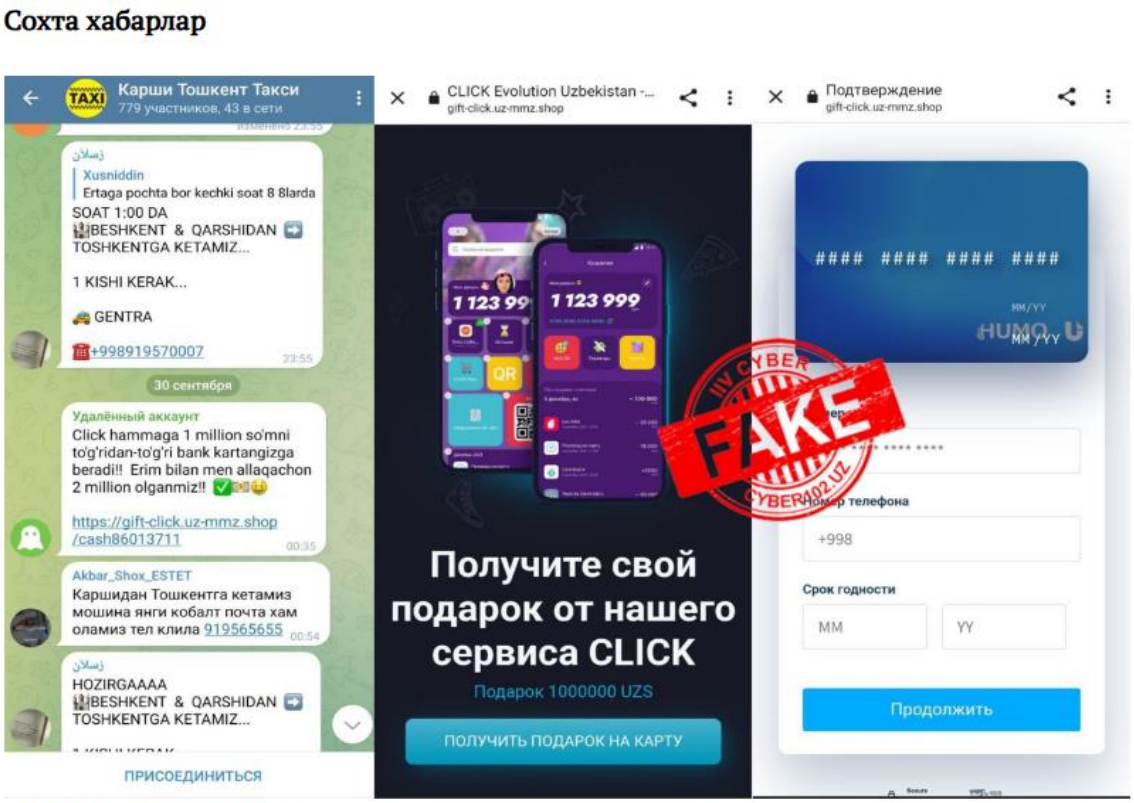
"Phishing" method. The phishing scheme is simple - fraudsters arrange to distribute a link to a fraudulent site on behalf of well-known brands, banks and delivery companies.

Fraudsters pretend to be bank employees or representatives of payment systems such as Click or Payme, and state that "there is a cyberattack on your plastic card" or that there is an error in the system, or that the system needs to be updated and the number needs to be re-linked.

“You will now be sent a secret code, which you must enter immediately,” it says [5] . If they do not provide the code to connect the number, users are pressured, saying that they will be disconnected from the network, blocked from making transfers and withdrawals, or lose the money on their card. The user may also be asked for personal information: card number, login and passwords. Ordinary people, in panic and fear, believe such scams and immediately enter the SMS code that comes to their phone, losing all the money on their card.

How to protect?

Pay attention to the name of the site. In the address bar, a real site will start with https, a fake site will start with http or the site name will be changed. For example, instead of https://www.korzinka.uz, it will be http://www.korzinka.official.u...
(http://www.korzinka-online.uz and so on).



ИИВ ТКД Киберхавфсизлик маркази

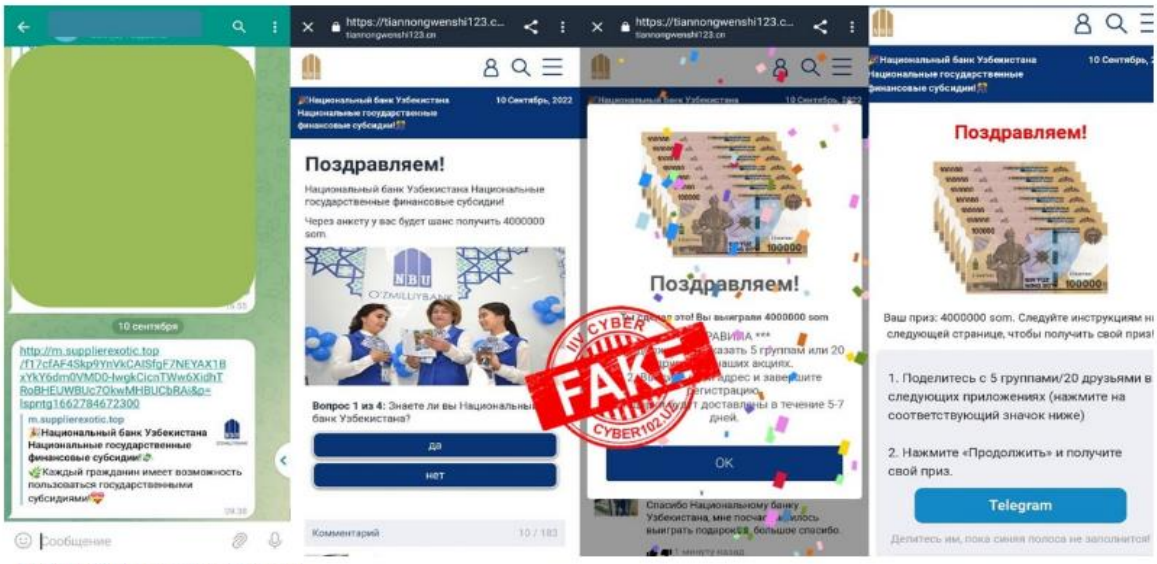
"You could win money," "You've won a prize," "You've inherited some money," or "You've been awarded money by a fund, you can get it through this link." There are also frequent cases of people being tricked into giving away their personal information through messages like ".

The most popular of these today is the promise of inheritance.

You may have also received news via email or instant messenger that a distant relative from abroad or someone with a similar last name has accidentally left you a large inheritance.

The initial costs of acquiring this inheritance will be borne by you. Naive people, believing that they have won money or unexpectedly become an "inheritor", enter their confidential data: card number, login and password through the link and pay this amount. As a result, they become not "inheritors" or "prize winners", but living food.

Fake winnings on behalf of banks. Fraudsters write to users through fake accounts, fake websites, and attract them through various advertisements. They send messages confirming that money has been allocated by banks or that they have won a winning game, and claim that it can be received via a link.



ИИВ ТКД Киберхавфсизлик маркази

However, before believing such messages, you should check the user's account and pay attention to the name and domain of the site. All payment systems, banks, and official sites in Uzbekistan use only " .uz" The account that sent the message usually has one picture and no phone number.

Fraud on online shopping sites. Fraudsters introduce themselves as buyers of items for sale on online shopping sites. They simply say that they live far away, in another region, and ask you to send them the goods by mail. Then they create fake websites of various banks (for example, “anorbank.uz-derart.com” instead of “anorbank.uz”) and say, “Enter your card details on this website and receive the money.” You enter your details without thinking on the website that looks legitimate, and suddenly all the money on your card is withdrawn.

The opposite can also happen. That is, scammers not only deceive buyers, but also deceive many people as sellers: for example,

they advertise a laptop worth 6 million soums at half the price and post it on the site. After convincing those who want to buy it that the goods are in good condition, everything continues according to the scammer's plan. Who wouldn't want to buy at a big discount? Buyers start saying, "Please, don't sell it to anyone, I'll buy it," and the scammer says to each of them, "There are a lot of buyers, if you want, give me half the money right now, I won't sell it to anyone else," and then collects a small amount of money and "disappears."

To transfer money, you sometimes need a bank card number, the owner's PIN, and a social security number. However , CVV codes, PIN codes, and one-time verification codes sent via SMS are never required. If you don't trust the seller, don't make a payment in advance.

Investment, charity offer. Fraudsters also deceive people by introducing themselves as representatives of a trading or construction company and saying, "You can earn a lot of money by investing a certain amount in us." Unfortunately, there are many among us who believe such simple lies.

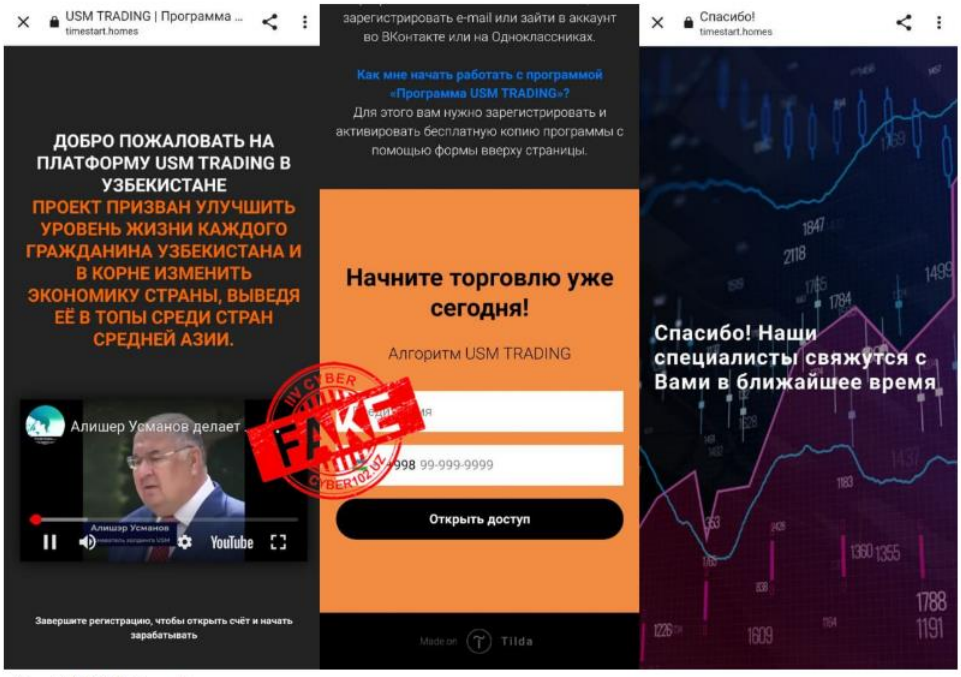


Фото: ИИВ ТКД Киберхавфсизлик маркази

Virtual fraudsters are also using famous images to scam people.

Currently, using the likenesses of Alisher Usmanov, Ravshan Ermatov, and Zafar Khoshimov to gain people's trust is a "trend" method for fraudsters.

Fraudsters are doing this by manipulating videos of celebrities with artificial intelligence software and forging audio recordings. As a result, gullible people are trusting fake "celebrities" and handing over large sums of money to virtual fraudsters.

There are also frequent cases of messages being sent through social networks and messengers on behalf of the head of state about money being allocated to the population, youth, and families, as well as about interest-free loans.

Before believing such news, one should pay attention to the name and domain of the site. For example, let's take the news about "Payment of 850 thousand soums to each family with children."

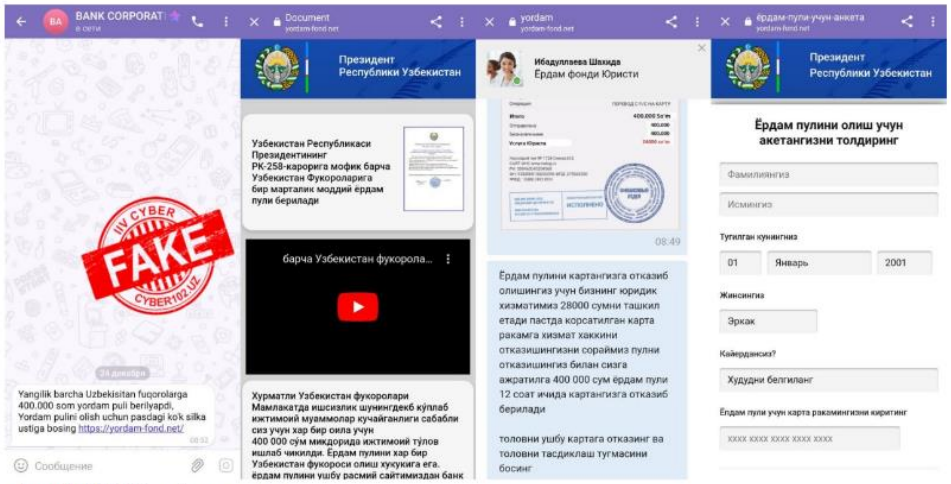


Фото: ИИВ ТКД Киберхавфсизлик маркази

Фото: ИИВ ТКД Киберхавфсизлик маркази

the money can be obtained from the website helpchildren.coqsecu.com [6]. The falsity of such messages can also be determined by the confusion, vagueness and spelling errors in the domain address: scammers mainly write with simple, grammatical errors or words are not connected correctly. This may prove that they were written based on a translation from another language into Uzbek. Unfortunately, there are those who know that these are false, and those who do not.

It's no wonder if you're reading this and saying, "I've been in the same situation," because the number of people who fall into the trap of virtual fraudsters is increasing day by day.

CONCLUSION

According to data, every second 5-7 citizens around the world become victims of virtual fraud using payment cards.

Phishing is a type of fraud, the purpose of which is to obtain confidential user information - logins and passwords.

5 common mistakes that can lead to phishing:

- not using antiviruses;
- open unknown messages received in e-mail;
- not checking the address bar of the site;
- making payments through non-secure pages;
- using one bank card for all payments.

Avoiding these mistakes can help prevent fraud.

What is the legal liability for online fraud?

Article 168 of the Criminal Code establishes liability and punishment for fraud and its types. According to it, fraud committed using information systems, including information technologies, is punishable by a fine of 300 to 400 times the basic calculation amount, or correctional labor for a term of 2 to 3 years, or restriction of liberty with deprivation of certain rights for a term of 5 to 8 years.

REFERENCES

www.pepper.uz

www.stat.uz

www.youtube.com

www.click.uz

www.proacademy.uz

www.ziyonet.uz