Dear clients, we ask you to take attention to the main types of the Internet fraud :

1) *Calls on behalf of employees of security departments of the banks or law enforcement bodies* - during the conversation, the attackers notify about allegedly carried out unauthorized , fraudulent transactions using bank accounts or registration the loans on behalf of potential victims to people , whom called the attackers.

In this case, you must interrupt the conversation and report it to the police. Do not panish during that situations, since scammers will try to instill fear and misdirect the interlocutor, obtain all possible information about bank accounts and incoming SMS messages. Do not install any applications, especially for remote control of your devices (**AnyDesk, RustDesk, TeamViewer** and etc.),

2) *Selling goods and services on social networks and trading platforms* - this type involves the imaginary sale of various types of goods and services. As a rule, these are cars, household appliances, furniture, wearable items, accessories, consumer goods, food, etc. The goal of the attackers is to gain profit. They will let you down in every possible way and ask you to transfer funds as an advance payment. It is better to refuse such transactions until you see the product with your own eyes, otherwise you may be left without your savings;

3) *And the use of phishing sites* — this type of fraud is aimed at collecting personal and banking data information. Such sites identical with real sites.

For example : You posted an ad on one of sites, and a previously unfamiliar person contacts you and asks you to arrange delivery, after which he sends you a link for ordering. By clicking on the specified link, you will be asked to enter your data, that is, full name, year of birth, bank card number, expiration date and CVV - code. After filling out, the debiting of funds begins from bank account cards;

4) *Investment in cryptocurrency, valuable paper and etc.* - with the advent of new opportunities and technologies, the cryptocurrency movement is actively developing. Many understanding people have good income from this. But there are also ill-wishers who make money fraudulently, taking advantage of illiteracy in this area.

For example : On social networks You know advertising that offers to make money by buying and selling shares or cryptocurrencies. An attacker calls you and introduces himself as an employee of the National Company or another organizations that allegedly provides brokerage services. They lure you with lucrative offers and persuade you to deposit money, small amounts to begin with. After a few days, the invested funds are returned with the supposedly earned benefits. After which they ask to deposit larger amounts . Many of those who fell for the tricks of scammers say that the attackers behave confidently, convincingly and in their arsenal they have well-developed Internet sites in which you register and in your personal account you watch the increase your savings, but it's all fake

5) *calls to senior citizens* - attackers introduce themselves employees law enforcement authorities and report that their close people were involved in a criminal case - scammers in during the dialogue, they convince their interlocutors that an incident has occurred for which their loved ones (children, relatives, friends) may find themselves in the orbit of a criminal persecution. In this regard , in order to release from criminal responsibility necessary monetary funds that supposedly their employee will have to collect. In turn, they send so-called "drops" or couriers who carry out private labor activity on various Internet platforms. And heading along a given route, they receive money from the victims" and transfer it to the attackers or transfer on front bank accounts.

Also I wanted to take your attention on these *"drops"* - person assisting criminals by transfers their banking card and personal data for carrying out illegal financial transactions or laundering money obtained by criminal means.

The most common "drops" are : young citizens, students, the unemployed and people looking for easy money.

We address to people who are involved in activities related to cashing out proceeds of

crime using bank cards from third parties. Such behavior provides for criminal liability *(not long ago, a citizen of the Russian Federation was prosecuted and sentenced to 6 years for cashing out money obtained by criminal means using bank cards of third parties; investigative actions are also being carried out against 79 droppers who We have not cashed out funds).*