AJPDIS GLOBAL RESEARCH NETWORK

AMERICAN Journal of Public Diplomacy and International Studies
Volume 01, Issue 10, 2023 ISSN (E): 2993-2157

Criminalistic Features of Cybercrime Investigation

Mirazova Shchista Davron's
Daughter Graduate student of the University of Public Security of the Republic of Uzbekistan

Abstract: The article examines the criminalistic features of the practice of investigating cybercrimes, and establishes obstacles and barriers to the disclosure of such types of crimes and phishing. Based on the analysis of domestic and international practical experience, tactical methods of conducting investigative actions in the investigation of cybercrimes using information technology, the Internet, online payment systems were developed.

Keywords: phishing, cybercrime, Internet, information and communication technologies, online banking.

Cybercrimes today are a very common type of crime, the distinctive feature of which is high adaptation to existing conditions, mutability, and rapid transformation into new forms. The coverage of victims, the use of modern technology to minimize visual contact with victims, as well as the possibility of remote access to their funds has led to an increase in the number of cybercrimes, which increased 3 times over the same period in 2019, not to mention the number of victims in a single criminal case.

As E.A. Morozova rightly noted, "one of the main "disasters" of recent years associated with the widespread spread of information technology has become cybercrime. This is due to the high level of latency of this type of crime, as well as significant difficulties arising in the process of its disclosure and investigation"[1].

The danger of cybercrimes is determined by the insufficient level of their knowledge, the lack of new methods for their investigation, ignorance of how to commit them, as well as measures to prevent them, and the lack of qualified IT specialists to assist investigative units is also a problem. Thus, according to the official message of the State Unitary Authority of Uzbekistan "Cybersecurity Center"[2] dated December 28, 2020, the specialists of this center warned corporate email users about targeted phishing attacks on corporate email addresses carried out by cybercriminals, which is undoubtedly know-how in the framework of regional crime, since this kind of crime was widespread mainly only in Western countries.

A few words about targeted phishing attacks. Phishers, when trying to commit a phishing attack on a certain company or enterprise, conduct research on correspondence, business management, and also study employees and their hobbies on social media accounts. The goal is to compile a targeted phishing email, especially this method is used when the manager himself is chosen as the victim, since unlike a simple employee, access to his data can provide an opportunity to obtain more valuable information, which can subsequently bring greater profit. Therefore, it is necessary to be careful when posting private information, especially about the place of work and discuss this point (confidentiality) when drafting a contract for employment.

In the practice of countering cybercrimes and their investigation, there are some problems that require comprehensive careful consideration:

- according to the studied materials of the pre-investigation check and criminal cases concerning new types of fraud (phishing, cybercrimes), for which there is no investigation methodology, in most cases, the collection of materials of the pre-investigation check was limited only to attaching the victim's statement, requesting explanatory and available documents from him (details of calls, screenshots of correspondence on social networks, receipts for transfer cash, copies of transactions, etc.), sending requests to criminal investigation officers. With such scarce materials, the issue of refusing to initiate a criminal case was considered, rather than initiating and fully investigating it, through the production of a wider range of investigative actions that can be carried out during the preliminary investigation. Even in the case of a criminal case, the investigative actions were limited to the interrogation of the victim, the recognition of the presented documents as material evidence. Other investigative actions were not carried out in most cases.;
- these types of fraud are characterized by the absence of ideal traces of a crime, characteristic of "ordinary" frauds due to contactless fishing for necessary information and as a result of funds, being at a considerable distance from the victim of the crime (in some cases, being on the territory of another country), which makes it actually difficult to establish the identity of all participants in the crime;
- the transfer of funds is made contactless, that is, through online banking systems (Click, Payme) or electronic payment systems (UzCard, Humo), electronic money (WebMoney, QiWi, Yandex. Money);
- fraudsters, using new types of fraud, mainly use the inattention, ignorance and credulity of victims, users of virtual space;
- in some unsolved criminal cases of fraud (cybercrimes, using electronic payment systems), there were formal "on paper" plans for operational investigative measures and investigative actions on behalf of the head of the Department of Internal Affairs, which the investigator or inquirer himself compiled;
- in some cases, even if there is information about the account or profile on social networks, the persons in whose name the accounts were registered were not identified (there was not even a request to the criminal investigation department to establish such);
- in some episodes, requests were not sent to banks or organizations that carry out money transfers, interrogators and investigators referred to the need to obtain a prosecutor's sanction or the need to send it to the Central Bank of Uzbekistan, since in most cases the attackers were in another region of the country or the transfer was carried out abroad, and there is no way to claim data about the recipient of the transaction due to the lack of concluded interstate agreements and the presence of bureaucratic obstacles (a complicated procedure for sending a request to other countries);
- criminal cases were suspended, even if the identity of the criminal was established due to insufficient evidence (the person did not come into direct contact with the fraudster, the correspondence was conducted on the Telegram social network and was deleted by the attacker (Telegram has such a function of unilateral deletion of correspondence), the statement of the suspect about the ignorance of the source from where the funds came to his account);
- in some cases, there was a place of repeated redirection of criminal cases allegedly under territorial investigation, with reference to the location of the sender or recipient, the place of cash withdrawal, etc. instead of conducting a qualitative investigation.

According to Antonov I.O., Shalimova A.N., "improving the effectiveness of the preliminary investigation of criminal cases of cybercrime is impossible without identifying factors that can have a noticeable negative impact on the quality of the criminal investigation procedure. Firstly, it concerns the imperfection of the norms of domestic criminal law providing for liability for cybercrimes. Secondly, there is a lack of fully adequate forensic support for the investigation procedure of this category of criminal cases (both at the level of forensic methodology and at the levels of forensic tactics and techniques)"[3].

The solution to this problem of countering and preventing cybercrimes, in particular phishing, can be:

- development of scientifically based recommendations for the detection and investigation of phishing, the development of a new, meeting modern requirements, proven in practice methodology for investigating modern types of fraud, the development of a new algorithm for the production of investigative actions during pre-investigation and preliminary investigation, the procedure and tactics of their production;
- attracting highly qualified IT specialists (graduates of universities of information technology, hiring specialists with high skills in the IT field to work in the Ministry of Internal Affairs on a competitive basis);
- development of new issues for the production of forensic computer-technical expertise, depending on the object of research;
- raising public awareness with school-based education on protection and security measures in the virtual space, following the example of some Western countries;
- in the structure and system of the organization (corporation, LLC), when hiring new full-time employees, to instruct during the probation period on measures to counter phishing (targeted), with written notification and familiarization with the rules that in the case of a phishing attack on the company due to the fault of an employee, he is personally responsible for the losses incurred;
- establishment of a hierarchy among employees, according to which, depending on the importance and confidentiality of information, access to certain information is granted to each category, as in military institutions.

When conducting investigative actions in the investigation of phishing, we would like to focus on the actions of the investigator or investigator at the stage of pre-investigation verification in cases of cybercrime. First, it is necessary to obtain explanatory notes from the victim. The following main circumstances should be established: the method of committing fraud, how the scammers contacted the victim (social network (Telegram, Instagram, Whatsapp), e-mail (mailing letters), by phone number);

- the name and number of his account (ID), phone number, e-mail, as well as the name of the account of the attacker who sent the phishing message with a detailed description of what the site looked like, the link to which he clicked, from whom this letter was sent, what data was forced to enter, which links he clicked, the name of the link, the data of the entered plastic card or the e-mail address to which the online payment system was attached,
- for what purpose was the mailing sent, that is, the subject of fraud (purchase of goods, exchange, purchase of services, lottery winnings, Nigerian letter), as well as whether the criminal was familiar with who he introduced himself, the subject of the agreement, what actions provided for the execution of the sent letter or message, the amount of the agreement
- the method of transferring funds: if by a blitz transfer - to whose name (full name), the address of this person; if through an intermediary – at what time and place the money was transferred; a detailed description of the person to whom the money was transferred (can the victim identify him and make up a sketch); whether an intermediary by car (description of the vehicle, state number of the car); if by transfer to the account of a certain cell phone number or bank account – where, when and how the funds were credited; – other circumstances relevant to the criminal case.

Next, it is necessary to inspect the victim's profile in a registered social network, his profile, correspondence, with mandatory clarification of the date of receipt of the letter, the sender's name, the title of the message, the sender's account, his ID, the content of the correspondence, the topic of the conversation with a line-by-line indication of the entire content of the letter exactly to the point with alternate entry of messages: sender-recipient, with an attachment to the

inspection protocol of a printout of a screenshot of the victim's account profile (after the initiation of a criminal case, further recognition of it as material evidence);

- if the funds were transferred to the attacker by the user himself, requesting a printout of transactions from the victim and receiving a letter from the UzCard, HUMO, OSON, UPay payment systems and Click, Payme online banking systems, or sending a request by the authorities conducting a pre-investigation check (it is necessary to clarify for what purpose he sent the funds). It is necessary to inspect these receipts and indicate in the protocol: when and to which account the funds were transferred, who was the recipient (usually written last name, the recipient's bank account, through which payment system or online banking the funds were transferred), the amount of funds transferred, whether the transaction was successful and additional data with the receipt attached to the protocol as evidence. Having established the surname, first name, patronymic of the recipient of funds, the owner of the bank card, it is necessary to check it against the database form No. 1, available in all investigative departments of the structure. If several persons matching this description are found, send a request to the criminal investigation departments. In the future, this inspection protocol will be the basis for sending a request to banking institutions to seize a bank account in order to further prevent embezzlement of funds.

Next, it is necessary to inspect electronic evidence (directly user accounts or e-mail), directly computer equipment or the phone from which the login to these profiles was carried out, as well as to request documents from the victim (certificate of banking transactions) and inspect them. In the case of money transfer through post offices or international payment systems (Unistream, Zolotaya Korona), a receipt is required, as well as the recipient's passport data.

It is mandatory to send a request to online advertising platforms for the purchase and sale or exchange of goods, provision of services, such as OLX, UyBor, Olcha.uz , bulavka.uz , mediapark.uz to establish the phone number attached to the account, the presence of the user's ads, the area in which he registered (Tashkent, Syrdarya and etc.), access to his account and correspondence to identify possible victims. It is also necessary to resolve the issue of blocking the attacker's account, after establishing the identity of the account owner, printing out all mailing messages from this user, identifying the owners of the recipients of these mailings by phone number in an operational way (call, invite to the department of internal affairs, request explanatory notes to establish whether they have become victims of intruders). These measures can be carried out jointly with the staff of the criminal investigation department by sending an operational task or by the investigator or inquirer himself.

If during the pre-investigation check it is established that the attackers gained access to social network accounts or e-mail to which the online payment system (Yandex.Money or Webmoney), then together with the victim, inspect this page or account with the participation of witnesses with logging with photos, video recordings or attaching screenshots of the actions performed, with mandatory identification when the attacker hacked the account, what actions he performed by hacking or gaining access to it, whether money was transferred from online payment systems, if so, for what purposes they were spent (transferred to pay for services, purchase goods or to another bank account). It is necessary to contact the administration of these payment systems to identify the recipient, sender and all necessary data. Although it should be noted that there are no concluded contracts or agreements regarding the provision of information about registered users by court decision, which creates difficulties during the investigation of cases.

Requesting documents from the victim about the banking transactions performed from his account or, after the initiation of a criminal case, sending a request to the bank to establish information about banking transactions from the victim's account, as well as establishing the data of the recipient of funds from the sender's bank account at the time of the fraud in order to further establish his identity and suspend all transactions from this bank account for preventing embezzlement and cashing out of funds.

In case of identification of the owner of the phone number or the owner of the plastic card to which the funds were transferred, send a summons, summon the internal affairs body and demand an explanatory note. It is necessary to establish the identity, type of activity, whether IT is related to the IT sphere, whether he has an account on social networks or online platforms for the purchase and sale of property or other goods and services. If so, with whom, when he corresponded, his bank card number, for what purpose he received funds to his account on a certain day, what goods he sold or bought on online platforms, from what period he was registered there. For what purpose did he enter into correspondence with the victim, what is the purpose and motive of the correspondence, who created the phishing message, how the link was created, are there any accomplices to whom else he sent this message, what is the scheme of phishing, how a third-party site was created, to which number the account was attached, his nickname, how much money he received through phishing attacks how he was selling money (by withdrawing funds through ATMs or paying for goods).

Cyberspace has become an integral part of society, which is both a means of communication and a source of information. However, along with its obvious advantages, it has become a threat carrier not only for an individual State, but also for the international community as a whole. In the modern world, there is a global problem of the spread of cybercrime, in particular cybercrime. In addition to the difficulties of investigating cybercrimes due to the specifics of cyberspace, there is no legal regulation of criminal liability for their commission and the specifics of their investigation. In this regard, it is necessary to make appropriate changes to the current criminal and criminal procedure legislation.

Bibliography

1. Морозова Е.А. Мошенничество в киберпространстве: уголовно-правовая характеристика. - Белгород. 2019. С. 3
2. https://tace.uz/
3. Антонов И.А., Шалимов А.Н. Актуальные проблемы расследования мошенничества с использованием компьютерной информации. Ученые записки Казанского университета. Казань. 2015. С. 214