WHAT IS CYBERCRIME? PROTECTION AGAINST CYBERCRIME

Mukhammatkulov Shakhrukhbek Erkin ugli
Employee of the Cybersecurity Department
of the Department for Combating Crime
in the Field of Information Technology
of the Main Department of Internal Affairs
of the city of Tashkent
+99897 463 44 43
sh.muhammatqulov@mail.ru
https://doi.org/10.5281/zenodo.8181187

Annotation.

In this article, the author will analyze the types of cybercrimes. It analyzes the most dangerous types of cybercrime, which are widely spread around the world and attract more and more people every year.

Keywords: cyberspace, cybercrime, cybersecurity, qualification of crimes.

What is cybercrime?

Cybercrime is a criminal activity in which a computer, computer network or network device is used or attacked. Most cyber attacks are carried out by cybercriminals or hackers in order to obtain financial profit[1]. However, the purpose of cyberattacks may also be to disable computers or networks – for personal or political reasons. Cybercrimes are committed by individuals and organizations – from novice hackers to well-coordinated groups that use advanced techniques and are well-tech-savvy[2]. And according to the "Law on cybersecurity": "cybercrime is the sum of crimes carried out in cyberspace using software and technical means for the purpose of capturing information, modifying it, destroying it or disabling information systems and resources"[3]. It is obvious that new and new manifestations of crime are already firmly rooted in society and States. In addition, the detrimental impact of cyber attacks, and cybercrime will not only lead to a slowdown in the economy, but will also cause unprecedented negative consequences, such as demographic changes, crises, excessive allocation of state budget funds for cybersecurity and, as a result, leaving socially vulnerable segments of the population without material support.

What are the types of cybercrimes?

Currently, there are more than 100 types of cybercrime, which are divided into a number of groups based on the style of its occurrence, the forms of

[1] Зоилбоев, Ж. (2022). Kiberxavfsizlik, raqamli huquq va raqamli gigiyena–kiberjinoyatchilikka qarshi muqobil yechim. *Общество и инновации*, *3*(6/S), 12-24.
[2] https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime
[3] "Law on cybersecurity" of The Republic of Uzbekistan// https://lex.uz/uz/docs/-5960604

participation, the level of danger, as well as the attitudes of the perpetrators towards the crime.

Here are some types of cybercrime:

- *Fraud using e-mail and the Internet*
- *Digital identity theft (theft and use of personal data)*
- *Theft of payment card data and other financial information*
- *Theft and resale of corporate data*
- *Cyberschantage (extortion of money under threat of attack)*
- *Attacks using ransomware (one of the varieties of cyber-sabotage)*
- *Cryptojacking (mining cryptocurrencies using other people's resources)*
- *Cyber Espionage (obtaining unauthorized access to government or corporate data)*
- *Disruption of systems in order to compromise the network*
- *Copyright infringement*
- *Illegal gambling*
- *Online trading of prohibited goods*
- *Harassment, production or possession of child pornography.*

Cybercrime always implies at least one of the following: Criminal activity for the purpose of attacking computers using viruses or other malware. Using computers to commit other crimes[4].

Cybercriminals, whose goal is to attack computers, can infect them with malware in order to damage or completely disable them, as well as to delete or steal data. Cybercriminals may also target a DoS attack (a denial of service attack), due to which users or customers of the company will not be able to use the website, computer network or software services.

Cybercrimes, in which computers are used to commit other crimes, may be aimed at distributing malware, prohibited information or images using computers or computer networks[5].

Cybercriminals often use and attack computers at the same time. For example, they can first attack computers with a virus, and then use them to spread malware further across the network[6]. In some countries, the classification of cybercrimes provides for another, third category: the use of a

[4] https://www.kaspersky.ru/resource-center/threats/types-of-malware

[5] https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwiZ7MOi86SAAxWjBXsKHSDNDw0YABAAGgJsZQ&ohost=www.google.com&cid=CAESauD2Qf1t2vBOvB_Taf7gx3oyInqgi5vVwo5jzecqI7WbLZa9qCKfcfiydG6CxkJs5W1Si9fgkp7LatzJwDptZn-nT9DiW8Ifb3HeInrrTT0xhMCwhVkpfFjme1oPV6Pj5Rn7BVdZa8h9xy0&sig=AOD64_3xe4UrCtJa9Hka3g9CkPIctjRiKw&q&adurl&ved=2ahUKEwiCur6i86SAAxXtHxAIHXV1BHAQ0Qx6BAgJEAE

[6] https://uniserveit.com/blog/how-computer-virus-attacks

computer as an auxiliary tool for committing a crime. An example is the storage of stolen data on a computer.

Examples of cybercrime

The following are sensational examples of various types of cyber attacks.

Malware attacks

In this case, the computer system or network is infected with a computer virus or other malware. After that, cybercriminals can use the computer to steal confidential information, damage data and other criminal activities. A well-known example of this kind of cybercrime is the global cyberattack committed in May 2017 with the help of the WannaCry ransomware. Such programs allow cybercriminals to demand ransom for data or devices taken hostage. WannaCry exploited a vulnerability of computers running Microsoft Windows[7].

Then 230,000 computers in 150 countries were affected by the actions of the ransomware program. Victims of cybercriminals lost access to their files and received a message demanding a ransom in bitcoins for restoring access[8]. The global financial damage from the WannaCry cyberattack is estimated at $4 billion. This cybercrime still remains one of the largest in terms of infection and damage.

Phishing

A phishing attack is sending spam (in emails or through other channels) to fraudulently force users to do something that will weaken their security. Phishing messages may contain infected attachments, links to malicious sites, or a request to provide confidential information[9].

A well-known example of phishing fraud occurred in 2018 during the FIFA World Cup. As we told in the report "The World Cheating Championship 2018", scammers sent phishing emails to football fans[10]. As bait, the authors of the spam mailing list used the promise of free tickets to Moscow, the venue of the 2018 FIFA World Cup. Criminals stole personal data from users who opened phishing emails and clicked on links.

Another type of phishing campaign is targeted phishing. In this case, cybercriminals organize targeted phishing attacks in order to fraudulently force specific employees to commit actions that will violate the security of the entire organization.

[7] https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware
[8] https://www.kaspersky.ru/resource-center/definitions/what-is-bitcoin
[9] https://www.kaspersky.ru/resource-center/threats/spam-phishing
[10] https://securelist.com/2018-fraud-world-cup/85878/

Unlike mass phishing mailings with rather generalized content, letters for targeted phishing imitate messages from a trusted source in detail. For example, it may seem that the letter was sent by the director or IT manager of the company. At the same time, it can be very difficult to visually recognize such a letter as fake.

Distributed DoS attacks[11]

Distributed DoS attacks (DDoS) are aimed at disabling any system or network. Sometimes IoT (Internet of Things) devices are used to carry out DDoS attacks. Sending multiple connection requests using standard communication protocols as part of a DDoS attack leads to an overload of the system. Cybercriminals can threaten a DDoS attack as part of cyber-sabotage, extorting money. Also, a DDoS attack can be used as a distraction during another cybercrime.

One of the high–profile examples is the DDoS attack on the website of the British National Lottery in 2017. The attack completely disrupted the operation of the lottery's website and mobile application. The motives of the attack are still unknown. Presumably, the criminals tried to blackmail the lottery organizers[12].

Consequences of cybercrime

The number of cybercrimes continues to grow. According to Accenture's State of Cybersecurity Resilience report for 2021, the number of cyberattacks increased by 31% between 2020 and 2021[13]. The number of attacks per company increased from 206 to 270 in a year. Attacks on companies also affect ordinary people, as many organizations store confidential information and personal data of their customers and users.

One attack, whether it's a data leak, DDoS attack, infection with a ransomware program or other malware, costs the company an average of $200,000. And according to the insurance company Hiscox, many organizations are forced to completely stop working within six months after the cyberattack[14].

According to a study on digital identity theft fraud published in 2021 by Javelin Strategy & Research, the annual financial damage from this type of attacks amounted to $ 56 billion[15].

Thus, cybercrimes lead to serious consequences for both companies and individuals – mainly financial damage, as well as loss of trust and reputational losses.

[11] https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
[12] https://www.mirror.co.uk/news/uk-news/national-lottery-website-brought-down-11267701
[13] https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf
[14] https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf
[15] https://www.javelinstrategy.com/press-release/total-identity-fraud-losses-soar-56-billion-2020

If you have become a victim of cybercrime, it is important to detect it as soon as possible. Regularly review the transaction history and check with the bank for information on any suspicious transactions. The bank's employees will be able to investigate and determine whether the operation is fraudulent.

References:

1. Зоилбоев, Ж. (2022). Kiberxavfsizlik, raqamli huquq va raqamli gigiyena–kiberjinoyatchilikka qarshi muqobil yechim. Общество и инновации, 3(6/S), 12-24.
2. https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime
3. "Law on cybersecurity" of The Republic of Uzbekistan// https://lex.uz/uz/docs/-5960604
4. https://www.kaspersky.ru/resource-center/threats/types-of-malware
5. https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwiZ7MOi86SAAxWjBXsKHSDNDw0YABAAGgJsZQ&ohost=www.google.com&cid=CAESauD2Qf1t2vBOvB_Taf7gx3oyInqgi5vVwo5jzecqI7WbLZa9qCKfcfiydG6CxkJs5W1Si9fgkp7LatzJwDptZn-nT9DiW8Ifb3HeInrrTT0xhMCwhVkpfFjme1oPV6Pj5Rn7BVdZa8h9xy0&sig=AOD64_3xe4UrCtJa9Hka3g9CkPIctjRiKw&q&adurl&ved=2ahUKEwiCur6i86SAAxXtHxAIHXV1BHAQ0Qx6BAgJEAE
6. https://uniserveit.com/blog/how-computer-virus-attacks
7. https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware
8. https://www.kaspersky.ru/resource-center/definitions/what-is-bitcoin
9. https://www.kaspersky.ru/resource-center/threats/spam-phishing
10. https://securelist.com/2018-fraud-world-cup/85878/
11. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
12. https://www.mirror.co.uk/news/uk-news/national-lottery-website-brought-down-11267701
13. https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf
14. https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf
15. https://www.javelinstrategy.com/press-release/total-identity-fraud-losses-soar-56-billion-2020