IJIAET International Journal of Innovative Analyses and Emerging Technology

| e-ISSN: 2792-4025 | http://openaccessjournals.eu | Volume: 3 Issue: 3

Measures to Combat Society Cyber Attacks

Akhmedova Zebikhan Siddigovna

Lecturer at the Kokand State Pedagogical Institute

Abstract: The article covers cybercrime, cyberattack, their types, distribution methods and their prevention as a global problem, as well as the distribution of illegal and morally corrupt information through the Internet.

Keywords: Cyber crime, cyber security, cyber attack, DDoS attacks, Brute Force attacks, hacking.

It has been a long time since cybercrime, which is being mentioned in new forms, entered the list of global problems of our century. It is known to us to distribute virus programs, hack passwords, embezzle funds from credit cards and other bank details, as well as illegal information over the Internet, in particular, defamation, moral We can't ignore the fact that spreading misinformation is putting the lives of humanity at great risk.

The concept of "cybercrime" is the use of information and communication technology tools to terrorize the virtual network, create and distribute viruses and other malicious programs, illegal information, mass distribution of e-mails (spam), hacking, illegal access to websites, fraud, information integrity and copyright violations, theft of credit card numbers and bank details (phishing and pharming) and various other offenses. At this point, it should be noted that the scale of cyber terrorism and its threat to the life of the society is also increasing. Cyber-terrorist act (cyber-attack) - carried out with the help of computers and information communication tools, which poses a direct threat to human life and health or may pose a potential threat, causes significant damage to material objects or causes it is a political cause that is the origin or purpose of possible, socially dangerous consequences. The attractiveness of using cyberspace for modern terrorists is due to the fact that carrying out a cyberattack does not require large financial costs.

According to experts, this is done by supporting the development of developing countries, influencing the minds of citizens under the guise of establishing universal democratic principles, subjugating them to their goals in various ways. Unfortunately, in this process, attempts to organize cyber-attacks and to "effectively" use the unparalleled opportunities of the global network of the Internet are becoming more and more frequent. Because the role of "interference" in the internal affairs of the sovereign state of social networks, their producers and sponsors has not been fully studied, it has not yet been recognized that such "interference" is sometimes against this state. There are no international legal grounds for holding the owners of social networks accountable for inciting the overthrow of the state system on the pages of these networks. However, every criminal act or inaction should not go unpunished by nature.

Types of cyber attacks and their prevention.

There are many methods of cyber-attacks, from malware to social engineering to internal data theft. Other advanced but common forms are DDoS attacks, Brute Force attacks, hacking, direct hacking of a computer system (or website) or holding it for ransom using Ransomware.

1. Gaining or attempting to gain unauthorized access to a computer system or its data.

Published under an exclusive license by open access journals under Volume: 3 Issue: 3 in Mar-2023

2. Denial of Service (DDoS) attacks.

3. Tampering with the website or disrespecting the site.

4. Installation of virus or malware.

5. Unauthorized use of computer for data processing.

6. Improper use of computers or software by company employees in a way that harms the company.

Finally, improper use of computers or applications by employees can be intentional or due to lack of knowledge. For example, it is necessary to determine the real reason why an employee tried to enter incorrect information or accessed a certain data record that he was not authorized to change.

Social engineering can also cause an employee to deliberately try to hack a database just to help a friend! That is, the employee is friends with the criminal and emotionally has to get some innocent information for his new friend.

Response to cyber attacks.

Prevention is always better than cure. You must have heard this many times. The same is true for the IT industry when it comes to protecting against cyber attacks. However, even after taking all precautions, if you suspect your computer or websites have been attacked, there are some common responses:

1. Did the attack actually happen or did someone call for a prank;
2. If you still have access to your data, back it up;
3. If you cannot access your data and the hacker demands payment, you may consider contacting legal authorities;
4. Negotiate with the hacker and recover the data;
5. In cases of social engineering and employee abuse of privileges, investigations should be conducted to verify the employee's innocence or intentionality;
6. In case of DDoS attacks, the load on other servers should be reduced so that the website is back online as soon as possible. You can rent servers for a period of time or use a cloud application, so that the costs are minimal.

The Law "On Cyber Security" adopted by the Oliy Majlis of the Republic of Uzbekistan and entered into force on July 17, 2022 consists of 8 chapters and 40 articles. The purpose of this Law is to regulate relations in the field of cyber security.

Prevention of cyber attacks. The official channel of the Cyber Security Center of the Ministry of Internal Affairs of the Republic of Uzbekistan warns citizens against cyber attacks through Telegram messengers.

In it,

#I will not give the SMS code of my bank card to anyone.

Hashtags like #stop_fake_cybercrime are helping citizens fight cyberattacks.

In addition, the UN General Assembly adopted the resolution "Combating the use of information and communication technologies for criminal purposes" proposed by Russia.

"The resolution gives an incentive to start looking for an answer to the problem of cybercrime, which is one of the most urgent global threats," said the Permanent Mission of Russia to the UN. caught". According to the Russian side, the resolution was co-authored by 36 countries. "The Russian initiative was widely supported by the CSTO and SCO, African, Latin American and Asian countries.

In short, the Internet is becoming an integral part of our lives day by day. Citizens, corporations, governments communicate with each other on the Internet. Communication, commerce, cooperation are related to the global network. Today, there are many opportunities for criminals. Cyber attacks are often not reported to law enforcement agencies. For companies, it's a business decision. They are afraid that if they say it openly, there will be negative publicity, that is, in a word, if citizens become immune to cyber-attacks during the measures - activities, that is, if we can instill legal awareness in citizens in this regard, this type of crime will also be severe. decreases. Such obstacles will not be a problem in the development of our society.

References:

1. Karimov I.A. Uzbekistan on the threshold of the 21st century: threats to security, conditions of stability and guarantees of development. T.: "Uzbekistan", 1997.
2. Ganiev.S.K. Fundamentals of Cyber Security. T.: "Tashkent", 2020.
3. Karimov I.A. On the way to security and sustainable development. - T.: "Uzbekistan", 1998.
4. Akhmedova, Z., and Sodiqjon Muminjonovich Turdaliyev. "ORGANIZATION OF COMPUTER SCIENCE BASED ON MODULE TECHNOLOGY." Galaxy International Interdisciplinary Research Journal 10.11 (2022): 671-675

5. Akhmedova, Z., and S. Turdaliyev. "THEORETICAL FOUNDATIONS FOR THE CREATION OF ELECTRONIC INTERACTIVE EDUCATIONAL AND PROGRAMMING IN THE TOPIC" COMPUTER SCIENCE AND INFORMATION TECHNOLOGY"." Galaxy International Interdisciplinary Research Journal 10.12 (2022): 1047-1050.
6. Ahmedova, Z. S. "Informatika va axborot texnologiyalari fanidan elektron interfaol o'quv-uslubiy majmualar yaratishning nazariy asoslari." *Namangan davlat universiteti ilmiy axborotnomasi* 22.4 (2022): 935-938.
7. Marasulova, Zulaykho, and Zebixon Ahmedova. "Problems of continuity and incessancy in informatics and information technology in the continuous education system." *Scientific Bulletin of Namangan State University* 1.6 (2019): 399-406.
8. Marasulova, Z. A., Z. S. Akhmedova, and S. M. Turdaliyev. "Continuity and succession in teaching computer science and information technology in secondary and higher education." *International Journal for Innovative Engineering and Management Research* 10.3 (2021): 201-204.
9. Siddikovna, Ahmedova Zebikhon, Marasulova Zulayho Abdullayevna, and Yuldashev Abdurauf Rozmatjonovich. "Innovations and Advanced Foreign Experiences in Teaching Informatics in Higher Education in Interdisciplinary Relations." *JournalNX* (2021): 371-374.

Internet sources:

1. www.iiv.uz
2. www.community.uzbekcoders.uz
3. www.lex.uz
4. https.//t.me/cyber_102