CYBERCRIME AND ITS CURRENT PROBLEMS

Abdusamatova Shakhodat Khojiakbar qizi
Teacher of Informatics and information technologies of the academic Lyceum under the Olmalik branch of TDTU named after Islam Karimov, tel: +998(93) 375 – 42 - 15 e-mail: abdusamatovashahodat@gmail.com
Mannonov Asliddin Akbar og'li
AL Khorezimi TATU cybersecurity faculty student tel: +998(97) 960- 03 - 02, e-mail: asliddinmannonov0980@gmail.com .

Annotation: *This article presents the dolzar challenges of cyber security, cyber crimes and strategies to prevent them.*

Keywords: *cybercrime, cybersecurity, hacking, digital information security*

Every year, different levels of crime occur around the world, and this is followed by members of the state and society. Nowadays there are many types of crime such as crime in the digital world and cyber crime are also among them. Cybercrime refers to any form of crime involving a computer or other electronic device.

While most cybercriminals are carried out with the aim of benefiting cybercriminals, some cybercriminals are carried out directly to damage or disable computers or devices. Others use computers or networks to distribute malware , illegal data, images, or other material. Some cybercriminals target both, that is, computers, to infect a computer virus, which then spreads to other machines, and sometimes entire networks.

The main effect of cybercrime is financial. Cybercriminals can include many types of income-based criminal activity, including anti-payment attacks, email and internet fraud, and personal information fraud, as well as attempts to steal financial account, credit card, or other payment card information.

Cybercriminals can target a person's personal information or corporate information for theft and resale. Recent cybercriminals cover the use of Trojan to control illegal activities, such as online banking. Cybercriminals may also involve demanding a extortion fee after infecting the affected organization's computers with a payment program or disrupting its activities through a distributed denial-of-service (DDoS) attack.

Cybercrime attacks can begin where there is digital information, opportunity, and motivation. Cybercriminals include everyone from a lone user engaged in cyberbullying to state-sponsored actors such as Chinese intelligence services.

Cybercriminals use different attack vectors to carry out their cyber attacks and are constantly looking for new ways and techniques to achieve their goals, while avoiding detection and arrest.

Cybercriminals are classified into the main three categories these are as follows:

– ***computing device targeted crimes*** - for example, for network access;

– ***crimes used as computer weapons*** - for example, to initiate a denial-of-service (DoS) attack ; and

– ***crimes in which a computer is used as an additional tool for crime*** - for example, the use of a computer to store information received illegally.

Some of the frequent cybercrime attacks include distributed DoS (DDoS) attacks that are used to shut down systems and networks. This type of attack uses the network's own communication protocol against it, increasing the network's ability to respond to connection requests. DDoS attacks are sometimes carried out simply for malicious reasons or as part of a cybersecurity scheme, but they can also be used to divert a victim organization from another attack or exploit carried out at the same time.

Infecting systems and networks with malware is an example of an attack used to damage the system or harm users. This can be done by damaging the system, software, or data stored in the system. Ransomware attacks are similar, but malware acts by encrypting or deactivating victim systems until payment is made .

Cybercriminals often carry out their activities using malware and other types of software, but social engineering is often an important component for the implementation of many types of cybercrime. Phishing emails are another important component of many cybercriminals, but especially for targeted attacks, such as a business email agreement (BEC), in which an attacker tries to position himself as a business owner by email to convince employees to pay fake invoices. .

In order to prevent the above-mentioned cybercrime, experts recommend:

– Uniform implementation of basic security measures such as regular software updates and patches.

– Expansion of international cooperation in the field of law enforcement

– In a number of countries, cybersecurity laws are stricter

– Penalties for countries that store cybercriminals

USED LITERATURE:

1. Das. M., What T., “2013) " the effects of cybercrime: problems and challenges”, International Journal of Engineering Sciences & Emerging Technologies, Volume 6

2. Raj Sinha Jayoti Vidyapeeth women's University, Niraj Kumar Vedpuria " the social impact of cybercrime: a sociological analysis”