# CYBER SECURITY PROBLEMS IN ENTERPRISES AND ORGANIZATIONS AND THEIR OCCURRENCES IN THE NEWEST TECHNOLOGIES

**Majidova Mohigul**
Faculty of Human Resources Management, Samarkand State University.
Graduate student of the Department of Digital Economy

**Annotation**
As we know, the internet is the fastest growing infrastructure of our daily life. In this article, data privacy and security are the main security measures that every organization protects. In this case, all security measures should be taken in social networks, but also in bank agreements.

**Keywords:** cyber security, cyber-crime, virtual programs, Web servers, platforms

Currently, more than 60% of financial transactions are done over the Internet, so this industry requires the best quality security for large volumes of transactions. In today's technological world, the latest technologies are changing the way people live. But due to new emerging technologies, we can't keep our information safe even in the most effective way and therefore cyber crimes are increasing day by day. The scope of cyber security is not only information protection in the information technology industry, but also many other types such as cyberspace. Cybercrime is any illegal act that uses computers as a weapon of theft and crime. Today, a person can send or receive any information via e-mail, audio or video at the click of a button, but he never thinks about how securely the information is being shared or how safely the information is reaching the other person. have you seen The answer to this question lies in cyber security. Currently, the Internet is the fastest growing infrastructure of everyday life. The US Department of Justice expands its definition and calls it: "Cybercrime is any illegal activity that uses a computer to gather evidence." The vast scale of cybercrime has expanded further through computers. For example, network intrusion, computer virus distribution, and computer-based variants of existing crimes: identity theft, violence, and terrorism have become major problems for people and nations today.

Cybercrime is widely considered to be the use of computers and the Internet to steal personal information, sell contraband, and hack transactions with malicious codes. Just as technology plays an important role in human life day by day, cyber crime is also growing with technological developments. Data privacy and security are key security measures that every organization protects. We live in a world where all information is stored in cyber or online form. Social networks provide us with sites where we can safely communicate with our family and friends. In this case, cybercriminals will continue to steal and use social networks for people's personal information. All security measures should be taken not only in social

networks, but also in banking agreements. We can also observe cyber attacks on Android operating systems, unfortunately, on a very large scale.

Desktop computers have the same operating system as smartphones, and the same weapons are used to hack these platforms. Demand for Macs continues to grow, but at a slower rate than for PCs. Windows software allows users to develop virtual applications in any application running Windows, and thus malware continues to be developed for Android and other applications, creating the expected trends in cyber security such as data extraction and malicious code injection in web applications. we can see the attacks being made through . Cybercriminals distribute malicious code through web servers they develop. But phishing attacks, which most people focus on, are also a big threat. Now we need to focus on protecting web servers and web applications.

Web servers are the most convenient platform for cybercriminals to steal data. Therefore, everyone should use secure browsers during important transactions to avoid falling prey to crime.

As we slowly enter society, companies need to find new ways to protect personal information. Information media plays an important role in cyber security and presents many private cyber attacks. The spread of information among people is accelerating and the risk of attack is increasing. Since social media and social networks are used by almost everyone, it provides a great platform for cyber criminals to steal personal and confidential information. In a world where we are quick to forget our personal information, companies must prove they are agile in detecting threats, responding in real-time and repelling cyber attacks. Because people are so addicted to social networks, hackers use them as an intermediary to get the information they need. Therefore, it is necessary for people to take appropriate measures in social networks so that they do not lose the necessary information.

A major benefit of social media to business is the ability for people to share information with millions of people. Despite the fact that social media can be used against companies in cybercrime, companies cannot stop using social media because it plays an important role in the company's popularity. On the contrary, they will need to have solutions that warn them before the real damage is done. Companies need to understand this and have enough solutions and techniques to avoid risks in social communication. Everyone should monitor social media using certain rules and the right technologies. Cyber ethics is nothing but the code of the internet. When we learn these cyber ethics, we will be able to use the Internet in a safe and appropriate way. Below are some of them:

• Use the Internet to communicate with others or share ideas. E-mail and instant messaging are the best way to stay in touch with friends and family, communicate with colleagues and exchange ideas with people in the city or around the world.

• Do not be violent on the Internet. Don't call people names, tell lies about them, share their private pictures, or do anything harmful to them.

• The Internet is the world's largest library of information in any field, so use it correctly and legally. • Do not access other people's accounts using their passwords.

• Do not share your personal information with anyone. Otherwise, they will have the opportunity to misuse your information and it can end in a fight. • Don't try to trick others with fake accounts when you're online, if the account owner has a problem, you will too.

• Always use downloaded data and download only authorized games and videos. Above are the rules of ethics that everyone should follow when using the Internet. We need to follow the same rules in life as we do in cyberspace. As the world's technology advances and networks reach important agreements, computer security is becoming more and more important. Cybercrime is developing and spreading every year, and cyber security is also developing rapidly. New platforms and technologies are required to protect the infrastructure along with the latest and modern technologies, including cyber weapons and threats. There are no perfect solutions to cybercrime, but we must try to minimize it to protect the cyberspace of the future.

**References**

1. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2020 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy

2. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2021.