**Cybersecurity is briefly explained by following the steps below**

**Introduction to Cybersecurity**

Cybersecurity is the practice and method of data protection, security, and protection against unauthorized access.

Cybersecurity ensures the security of digital technologies, systems, networks, the Internet, and all elements that provide electronic information.

**Basic Concepts of Cybersecurity**

Cybersecurity primarily ensures our protection through sensitive data, proprietary software and hardware, and network and internet security.

Security of systems and networks can be enhanced by using effective cybersecurity measures, such as firewalls, antivirus software, entry point modification, data encryption, etc.

Step 3: The main way of cyber security

The key to cyber security is managing high-level network and system security. Cybersecurity integrity can then be maintained by centralizing the security of information management in the workplace, providing cybersecurity education to employees, using advanced technology with assumptions, and creating security guidelines.

**Cyber breaches and threats**

Cyber destruction is the hacker's conduct of illegal activities by illegally entering the Internet, system, or network.

In the digital age, we face certain risks of cyber attacks, such as data theft, unauthorized access, temporary blocking, permission disruption, malware propagation, etc.

Step 4: Cybersecurity Technologies and Activities

**Let's describe the cyber security technology:**

Cybersecurity Technology is a technology that is used to ensure the security of various information and various computer, mobile and laptop systems. This cyber security technology plays an important role in blocking various unauthorized accesses by data-stealing malware and hackers.

The following are the elements included in cyber security technology:

1. Firewall: It protects against unauthorized access to the network and prevents hackers from exposing it to danger.

2. Virus Scanner: It detects unfamiliar malware or virus on the computer and enables and destroys it.

3. Intrasystem Encryption: It encrypts the data so that other strangers cannot read it.

4. Identity Management: It verifies parentage and identity to grant users proper access.

5. Data Logging: It stores users' confidential data so that its collection and use are properly controlled.

These technologies ensure the security of digital materials through cybersecurity technologies and provide protection to users.

**Let's describe cyber security activities:**

Cybersecurity activities are a set of programs or activities related to protection against cyber attacks. These activities ensure security to protect users' information and protect against cyber attacks. Following are some common cybersecurity actions:

1. Network Monitoring: All events related to network connections, data changes, and accesses are monitored to detect if any anomalies exist.

2. Anti-Virus Scan: Various computer, mobile, and laptop system viruses are identified and destroyed manually by antivirus

3. Data encryption: Data encryption is a technical method that can keep data secure and confidential

Different types of cryptographic methods are used to keep information secure and confidential in different systems

Symmetric cryptography is a cryptographic method in which different data are encrypted and decrypted using the same key

Asymmetric cryptography is another cryptographic method in which data is encrypted and decrypted using a public key and a private key.

Various companies and organizations encrypt data to keep their information secure and confidential

**Malware :**

**What is malware:**

(i) Malware is a type of computer program that can perform unexpected and harmful actions. It can perform suspicious activities on the proprietary computer, which is not according to the user's knowledge. There can be different types of malware, such as viruses, trojan horses, spyware, ransomware, etc.

(ii) A virus is a piece of malware that can attach itself to a computer system and create multiple copies of itself. A Trojan horse is malware that performs a relative search for exchange and can then perform unexpected actions. Spyware is malware that monitors user resources or activity and can steal information. Ransomware is malware that encrypts information on a user's computer and demands a fee if the user does not disclose it.

(iii) Malware is usually spread unbeknownst to people and through information and services that can be collected in various areas online. Knowledge of malware needs to be acquired along with increased cybersecurity awareness and awareness. We all need to be aware of cyber security and be able to trust different potential malware types.

More about this source texture text is required for additional translation information

(iv)**Password Management**: Select and store secure and complex passwords so that no one can gain access without authorization.

(v)**Security Patchups**: Backing up data using computer and system backup software so that data is preserved in case of hardware or software damage.

These activities are conducted as part of the cybersecurity program and ensure the protection of users' information.

**Future of cyber security:**

The future of cybersecurity will be imperative that will continue to grow in importance as digital technology and the number and level of cyber attacks continue to grow. Innovative and everyday use of new technologies ensures new cyber destruction possibilities. The future of cybersecurity will consider the following opportunities and challenges:

1**. Smart City Security**: Cybersecurity Cities will continue to connect with more security technologies. It will ensure the protection of people's personal information, traffic safety, and the protection of the city's engineering projects.

**2. Enterprise Cybersecurity**: Business companies will establish a cybersecurity organization or department to ensure the security of their networks, data, and technology.

**3. Cyber Security of Smart Suburbs**: The connected environment of home, office, car, etc. needs to be secured using cyber security technology. The use of technology in smart cities will continue to be common to ensure the security of users' personal information.

4. Security of the World Bank and other financial institutions: Predictably, controversial credit and other financial institutions will adopt more proactive security measures against cyber attacks. The World Bank and financial institutions are banking initiatives with even higher estimates.

**Cyber security needs in various service sectors and MNC companies:**

Nowadays the need for cyber security management has become an important topic and the need is increasing in various service sectors and large multinational companies. The number and level of cyber attacks are increasing with new technologies, making cybersecurity programs and a marketing education system for professionals even more necessary.

Cybersecurity needs can be significant in various service sectors, such as:

**1. Bank and Financial Secto**r: Cybersecurity plays an important role in ensuring the safety of money stored by various banks and various types of financial sectors.

**2. medical field:** Cyber security is essential to protect patient personal information in the medical field

**3. Government Institutions and Departments**: Cybersecurity management is essential for government institutions and departments to ensure the security of government data and protected information.

**4. Technology companies**: Technology companies can keep their customers' data safe and add security to new technologies.

Various MNC companies use and store a lot of data so cyber security is required to protect all that data

**Step 5.Cyber Security Education**

Cyber security is an important topic, which is inextricably linked in our modern digital life. A brief introduction to various issues including cyber security dependency, privacy, cybercrime prevention, and data protection. As we are all digitally connected, we need to ensure security. Cyber Security Education With recent technological advances, we have inevitably faced more digital risks. Cybercriminals are using new technologies to challenge the assurance techniques of our security systems. This is why cyber security education becomes so important.

We can gain a lot of important knowledge through cybersecurity education. It is applicable to everyone and easy to understand and use. As we can stay safe while browsing the Internet, protect our mail account passwords, protect ourselves from cybercrime, and other ways we can let other people know how to increase their own security.

There are various training centers and institutes to get an idea of cyber security education, which can be part of our activities. We can stay protected from technological advancements and unexpected risks with cyber security training.