Need for cyber security

Why Cybersecurity?

Cyber Security is important because the government, Corporate, medical organizations, collect military, financial, process, and store the unprecedented amount of data on a computer and other properties like personal information, and these private information exposure could have negative consequences.

Cyber Security proper began in 1972 with a research project on ARPANET (The Advanced Research Projects Agency Network), a precursor to the internet. ARPANET developed protocols for remote computer networking. Example – If we shop from any online shopping website and share information like email id, address, and credit card details as well as saved on that website to enable a faster and hassle-free shopping experience, then the required information is stored on a server one day we receive an email which state that the eligibility for a special discount voucher from XXXXX (hacker use famous website Name like Flipkart, Amazon, etc.) website to receive the coupon code, and we will be asked to fill the details then we will use saved card account credentials. Then our data will be shared because we think it was just an account for the verification step, then they can wipe a substantial amount of money from our account.

That is why Cyber Security provides services as a Security Gate-Way to make information more Secure; in today's time, hackers are advanced. We can't surely say whether the data stored in my Devices is safe from outside threats. With Cybercrime increasing rapidly, it's crucial to have Cyber Security in place in our personal life and our Business.

Types of Cybersecurity:

1. Network Security –
Focuses on securing computer networks from unauthorized access, data breaches, and other network-based threats. It involves technologies such as **Firewalls**, **Intrusion detection systems** (IDS), **Virtual private networks** (VPNs), and **Network segmentation**.

- Guard your internal network against outside threats with increased network security.
- Sometimes we used to utilize free Wi-Fi in public areas such as cafes, Malls, etc. With this activity, 3rd Party starts tracking your Phone over the internet. If you are using any payment gateway, then your bank account can be Empty.
- So, avoid using Free Network because free network Doesn't support Securities.

2. Application Security –

Concerned with securing software applications and preventing vulnerabilities that could be exploited by attackers. It involves secure coding practices, regular software updates and patches, and application-level firewalls.

- Most of the Apps that we use on our Cell-phone are Secured and work under the rules and regulations of the Google Play Store.
- There are 3.553 million applications in Google Play, Apple App Store has 1.642 million, while Amazon App Store has 483 million available for users to download. When we have other choices, this does not mean that all apps are safe.
- Many of the apps pretend to be safe, but after taking all information from us, the app share the user information with the 3rd-party.
- The app must be installed from a trust-worthy platform, not from some 3rd party website in the form of APK (Android Application Package).

3. Information or Data Security:

Focuses on protecting sensitive information from unauthorized access, disclosure, alteration, or destruction. It includes **Encryption**, **Access controls**, **Data classification**, and **Data loss prevention (DLP) measures**.

- Incident response refers to the process of detecting, analyzing, and responding to security incidents promptly.
- Promoting security awareness among users is essential for maintaining information security. It involves educating individuals about common security risks, best practices for handling sensitive information, and how to identify and respond to potential threats like phishing attacks or social engineering attempts.
- Encryption is the process of converting information into an unreadable format (ciphertext) to protect it from unauthorized access.

1. **Cloud Security –**

It involves securing data, applications, and infrastructure hosted on cloud platforms, and ensuring appropriate access controls, data protection, and compliance. It uses various cloud service providers such as **AWS**, **Azure**, **Google Cloud**, etc., to ensure security against multiple threats.

- Cloud base data storage has become a popular option over the last decade. It enhances privacy and saves data on the cloud, making it accessible from any device with proper authentication.
- These platforms are free to some extent if we want to save more data than we have to pay.
- AWS is also a new Technique that helps to run your business over the internet and provides security to your data

2. **Mobile Security –**

It involves securing the organizational and personal data stored on mobile devices such as cell phones, tablets, and other similar devices against various malicious threats. These threats are **Unauthorized access**, **Device loss** or **Theft**, **Malware**, etc.

- Mobile is the very common device for day to day work. Everything we access and do are from mobile phone. Ex- Online class, Personal Calls, Online Banking, UPI Payments, etc.

- Regularly backing up mobile device data is important to prevent data loss in case of theft, damage, or device failure.
- Mobile devices often connect to various networks, including public Wi-Fi, which can pose security risks. It is important to use secure networks whenever possible, such as encrypted Wi-Fi networks or cellular data connections.

3. Endpoint Security:

Refers to securing individual devices such as computers, laptops, smartphones, and IoT devices. It includes antivirus software, intrusion prevention systems (IPS), device encryption, and regular software updates.

- **Antivirus** and **Anti-malware** software that scans and detects malicious software, such as **Viruses**, **Worms**, **Trojans**, and **Ransomware**. These tools identify and eliminate or quarantine malicious files, protecting the endpoint and the network from potential harm.
- Firewalls are essential components of endpoint security. They monitor and control incoming and outgoing network traffic, filtering out potentially malicious data packets.
- Keeping software and operating systems up to date with the latest security patches and updates is crucial for endpoint security.

4. Critical Infrastructure Security-

1. All of the physical and virtual resources, systems, and networks that are necessary for a society's economics, security, or any combination of the above to run smoothly are referred to as critical infrastructure. Food and agricultural industries, as well as transportation systems, comprise critical infrastructure.
2. The infrastructure that is considered important might vary depending on a country's particular demands, resources, and level of development, even though crucial infrastructure is comparable across all nations due to basic living requirements.
3. Industrial control systems (ICS), such as supervisory control and data acquisition (SCADA) systems, which are used to automate industrial operations in critical infrastructure industries, are frequently included in critical infrastructure. SCADA and other industrial control system attacks are very concerning. They have the capacity to seriously undermine critical infrastructure, including transportation, the supply of oil and gas, electrical grids, water distribution, and wastewater collection.
4. Due to the links and interdependence between infrastructure systems and sectors, the failure or blackout of one or more functions could have an immediate, detrimental effect on a number of sectors.

5. Internet of Things (IoT) Security-

1. Devices frequently run on old software, leaving them vulnerable to recently identified security vulnerabilities. This is generally the result of connectivity problems or the requirement for end users to manually download updates from a C&C center.

2. Manufacturers frequently ship Internet of Things (IoT) devices (such as home routers) with easily crackable passwords, which may have been left in place by suppliers and end users. These devices are easy targets for attackers using automated scripts for mass exploitation when they are left exposed to remote access.
3. APIs are frequently the subject of threats such as Man in the Middle (MITM), code injections (such as SQLI), and distributed denial of service (DDoS) attacks since they serve as a gateway to a C&C center. You can read more about the effects of attacks that target APIs here.