**What do you mean by cyber security? What are the measures carried out to mitigate cyber threats?**

Cyber security implies to the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitations. The main target of cyber security is to prevent cyber-attacks, data loss, identity theft Etc. However, Cyber threats can take many forms, including the following:

### Malware**:** a form of malicious software in which any file or program can be used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.

### ****Ransom ware:**** A type of malware that involves an attacker locking the victim's computer system files typically through encryption and demanding a payment to decrypt and unlock them.

### Social engineering**:** A type of attack that implies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected by the means of electronic Medias.

### Phishing**:** a form of fraud in which falsified emails are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card or login information.

### Cyber security threat implies to the various mediums by which a hacker can gain access to a computer or network server to deliver a malicious outcomes. Popular attack or threats include the following:

### USB sticks and other portable storage devices

### Unsupported browser extensions

### Infected websites

### Online quizzes and tests

Cyber security measures should always be implemented to protect the data either of small or large organizations as well as of individuals. It helps to protect an organization's data assets from digital attacks that could damage the organization or individuals if placed in the wrong hands. Medical, government, corporate and financials all hold information and the main aim of cyber security is to ensure protection of these digital data and information. Security incidents can lead to losses in terms of reputation, money, theft of data, deletion of data and fraud. Some of the measures are listed below in order to reduce or protect data and information from cybercrimes:

**1. Use full-service internet securities**

Antivirus programs provide a real-time protection against existing and emerging malware including ransom ware and viruses, and helps protect your private and financial information when you go online.

**2. Use strong passwords**

Don’t make your passwords same in different sites, banking pins. Moreover change your passwords regularly and try Make them complex as far as possible.

**3. Keep your software updated**

Updated software are especially important with your operating systems and internet security software that is because Cybercriminals frequently use known exploits, or flaws, in your software to gain access to your systems.

**4. Manage your social media settings**

Social engineering cybercriminals can often get your personal information with just a few data points, so the less you share publicly, the better.

**5. Protect yourself against identity theft**

Identity theft occurs when someone wrongfully obtains your personal data in a way that involves fraud or deception, typically for economic gain. for instance, or a thief might steal your mail to access account information. That’s why it’s important to guard your personal data. A virtual private network can also help to protect the data you send and receive online, especially when accessing the internet on public Wi-Fi.

**DEFINE AND EXPLAIN:**

**1) Browser:** A web browser is a software program that allows a user to locate, access, and display web pages. In common usage, a web browser is usually shortened to "browser." Browsers are used primarily for displaying and accessing websites on the internet.

A variety of web browsers are available with different features, and are designed to run on different operating systems. Common browsers include Internet Explorer from Microsoft, Firefox from Mozilla, Google Chrome, Safari from Apple, and Opera. All major browsers have mobile versions that are lightweight versions for accessing the web on mobile devices.

# 2) Plug-In:

Plug-in is part of an array of software components known as add-ons. Programs may be changed by different kinds of add-ons in different ways. In popular technologies, like Internet browsers and audio/video applications, the ability to utilize plug-ins makes products more versatile and allows transparent and convenient customization according to the user's desired features.

Plug-ins also can enable easier software upgrades or patches or additions by project collaborators. Plug-ins also can be a strategy for dealing with complex software licensing. Users can download individual plug-ins for this free Web browser tool to promote different results on devices.

**3) The Browser cache**

The browser cache, it’s nothing more than a place on your hard disk where the browser keeps things it downloaded once in case they’re needed again.

The very first time you visit any page on websites; the browser downloads the logo, and several other items, into the cache, and then displays it as part of the page you’re viewing. For each additional page you visit, as long as the same logo is displayed, it doesn’t need to be downloaded again it’s already on your hard disk.

**4) Cookies:**

Internet cookies are small text files (255 characters or less) that are placed on your web browser or computer by web servers. A cookie is created when you first visit a site that wants to store information. This text file usually includes a name, an expiration date, a coded number, and the domain name of the visited site.

When you return to a site, the cookie tells the site that a computer with code XYZ has returned and reminds it of your activities and preferences on your previous visits. These details can include pages visited at the site, what you did when you were on the site, how many times you visited the site, language preferences, the IP address of your device, and your login information.

The information collected from cookies enables websites to offer convenient logins and authentication, personalized experience for you through preference setting and language setting, enhanced online shopping experience, ad management, and more. So in and of themselves, cookies are not bad things. Cookies, for example, do not store any of your personal information such as your email address or phone number.