Cyber Security

Date No

Cyber Security Threats.

A cyber security threat is a malicious and deliberate attack by an individual or organization to gain unauthorized access to another individual's or organization's network to damage, disrupt or steal IT assets, computer networks, intellectual property or any other form of sensitive data.

Types of Cyber Security Threats.

01. Malware.
02. Phishing.
03. Spear Phishing.
04. Man in the Middle Attack.
05. Denial of Service Attack.
06. SQL Injection.

01.) Malware

* Malware attacks are the most common type of cyberattack.
* Malware is defined as malicious software, including spyware, ransomware, viruses and worms which gets installed into the system when the user clicks a dangerous link or email.
* Once inside the system, malware can block access to critical components of the network, damage the system and gather confidential information among others.

Date No

02.) Phishing.

* Cyber criminals send malicious emails that seem to come from legitimate resources.
* The user is then tricked into clicking the malicious link in the email, leading to malware installation or disclosure of sensitive information like credit card details and login credentials.

03.) Spear Phishing

* Spear Phishing is a more sophisticated form of a phishing attack in which cyber criminals target only privileged users such as system administrators and C-suite executives.

04.) Man in the Middle Attack.

* Man in the Middle (MitM) attack occurs when cyber criminals place themselves between a two-party communication.

* Once the attacker interprets the communication, they may filter and steal sensitive data and return different responses to the user.

Date No

05.) Denial of Service Attack

- Denial of Service attacks aims at flooding systems, networks, or servers with massive traffic, thereby making the system unable to fulfill legitimate requests.
- Attacks can also use several infected devices to launch an attack on the target system. This is known as a Distributed Denial of Service (DDoS) attack.

06.) SQL Injection.

- A structured Query Language (SQL) injection attack occurs when cybercriminals attempt to access the database by uploading malicious SQL scripts.
- Once successful, the malicious actor can view, change or delete data stored in the SQL database.

Sources of Cyber Security Threats.

01.) Criminal Groups.

- Criminal groups aim to infiltrate systems or networks for financial gain.
- These groups use phishing, spam, spyware, malware to conduct identity theft, online fraud and system extortion.

02.) Hackers

- Hackers explore various cyber techniques to breach defences and exploit vulnerabilities in a computer system or network.
- They're motivated by personal gain, revenge, stalking, financial gain and political activism.
- Hackers develop new types of threats for the thrill of challenge or bragging rights in the hacker community.

03.) Terrorist Groups.

- Terrorists conduct cyber attacks to destroy, infiltrate, exploit critical infrastructure to threaten national security, compromise military equipment, disrupt the economy and cause mass casualties.

04.) Hacktivists.

- Hacktivists carry out cyberattacks in support of political causes rather than financial gain.
- They target industries, organizations or individuals who don't align with their political ideas and agenda.

Best Practices to Protect From Cyber Threats.

01.) Regularly Update System and Software.

* As cyber threats are evolving rapidly, your optimized security network can become outdated within no-time, putting your organization at the risk of cyberattack.
* Therefore, regularly update the security network and the associated systems and software.

02.) Backup Data.

* Backing up data regularly helps reduce the risk of data breaches.
* Backup your website, applications, databases, emails, attachments, files, calendars and more on ongoing and consistent basis.

03.) Initiate Phishing Simulation

* Organizations must conduct phishing simulations to educate employees on how to avoid clicking malicious links or downloading attachments.
* It helps employees understand the far-reaching effects of a phishing attack on an organization.

Date No

04.) Secure site with HTTPS.

- * Organizations must encrypt and secure their website with an SSL (Secure Sockets Layer) certificate.
- * HTTPS protects the integrity and confidentiality of data between the user and the website.