SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107
Accredited by NAAC-UGC with 'A' Grade
Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

Department of Information Technology

19IT602 CRYPTOGRAPHY AND CYBER SECURITY
III Year / VI Semester

Cyber Security Safeguards

Cyber Security Safeguards

- In today's hyper-connected world, where we are closely connected and highly dependent on several technologies and digital platforms, protecting our digital infrastructure has become a necessity.
- Considering the threat landscape nowadays, protective sensitive information, business systems, and intellectual property must be your number 1 priority.

1. Identify Your Assets

- The first step of cyber security starts with knowing your IT infrastructure and environment. You cannot protect what you don’t know exists.
- Identify the crucial set of data that you want to protect
- Classify how the sensitive information flows through the environment

2. Train your Employees

In a research carried out by Stanford University and a top cyber security organization, it was found that approximately 88% of cyber attacks or data breaches happen due to a human mistake.

3. Keep your Endpoints Safe and Protected

Endpoint is a device that is connected to a network and exchanges information with it.

4. Keep your Software and Operating Systems Patched

If you are shocked to see this in our Cyber Security Safeguards list, then you should be. Many business owners don't take it as seriously as they should. Unpatched applications and operating systems are more vulnerable to already-known cyber attacks.

5. Restrict Admin Privileges

Almost all operating systems support different user accounts with different technical capabilities. In the case of Windows OS, you can create two types of accounts i.e. user account and administrator account.

6. Harden System Components

Whenever you set up an IT infrastructure, no matter small or large, there are several types of devices that are involved in it.

7. Divide your Network

If you run your business through a physical space, then implementing this Cyber Security Safeguard is extremely crucial. When you first set up networking equipment in your business, it is very likely that you have created a flat network.

8. Keep a Backup Copy of your Data & Test Restoration

The very first thing that you need to accept while being connected to the Internet is that cyber attacks are inevitable.

9. Use Multi-Factor Authentication

The next Cyber Security Safeguard on our list is MFA i.e. Multi-Factor Authentication. Here, a user needs to authenticate at least two of the three authentication factors in order to validate a user account.

10.Strong Passwords: Encourage the use of complex, unique passwords for each account. Consider implementing multi-factor authentication (MFA) wherever possible.

11.Regular Updates: Keep software, operating systems, and applications up to date with the latest security patches to mitigate vulnerabilities.

12.Firewalls and Antivirus Software: Install and regularly update firewalls and antivirus software to detect and prevent malware and unauthorized access.

13.Data Encryption: Encrypt sensitive data both in transit and at rest to protect it from unauthorized access.

- In conclusion, prioritizing cyber security safeguards is paramount in today's digital landscape to protect against a wide range of cyber threats.
- From implementing strong passwords and regular updates to providing comprehensive employee training and developing incident response plans, organizations must take a proactive approach to safeguarding their digital assets and sensitive information.