What is Cyber security and Information security

Definition

Information security: Protecting information, regardless of its format, from unauthorized access, use, disclosure, disruption, modification, or destruction.

Broader: Covers all forms of information, including physical and digital.

Cybersecurity: Protecting systems, networks, and data from cyber threats, focusing on technology and digital environments.

Narrower: Focuses specifically on protecting digital systems, networks, and data.

Principles of Cybersecurity

In cybersecurity, the **CIA Triad** is a foundational model representing the three core principles of information security. These principles ensure the effective protection of data and systems.

Confidentiality: Ensures that information is accessible only to those authorized to access it.

Integrity: Ensures that data is accurate, complete, and unaltered during storage or transmission.

Availability: Ensures that information and resources are accessible to authorized users when needed.

Different types of cyber threats

- **Social Engineering**

Social engineering is a manipulation technique that exploits human nature to gain private information, access, or valuables. In cybercrime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions.

- **Malware**

Harmful software that can access a system's data, such as viruses, spyware, ransomware, and worms

- **Phishing**

A deceptive attack where cybercriminals impersonate legitimate entities to trick victims into revealing sensitive information

- **Denial-of-Service (DoS) attack**

A cyber attack that overwhelms a system's resources, making it unable to respond to legitimate service requests

- **Distributed denial-of-service (DDoS) attack**

A similar attack to a DoS attack, but initiated by many malware-infected host machines

- **SQL injection**

An attack that exploits vulnerabilities in databases by injecting malicious code into user inputs

- **Cross-Site Scripting (XSS)**

An attack that involves injecting malicious code into a website, but the code only runs in the user's browser

- **Ransomware**

A malicious form of software that encrypts a victim's files or locks them out of their computer system, demanding a ransom payment in exchange

Safe Internet and Device Usage

Verify Website Security

- Look for HTTPS in the URL.
- Avoid clicking on pop-ups or ads promising free products or rewards.

Use Strong Passwords

- Make passwords at least 8 characters long with a mix of letters, numbers, and symbols.
- Avoid using common words or phrases.
- Use a password manager to store and generate secure passwords.

Enable Multi-Factor Authentication (MFA)

- Add an extra layer of protection to your accounts by requiring a second form of verification (e.g., a code sent to your phone).

Secure Browsing

- **Keep Software Updated**: Ensure your browser and plugins are up to date to patch vulnerabilities.
- **Use a Secure Browser**: Consider browsers with built-in security features.
- **Avoid Clicking on Ads**: Block or ignore pop-ups and ads to reduce risk.
- **Use Private Browsing**: Use incognito or private modes for sensitive activities.
- **Limit Cookies**: Manage browser settings to minimize cookie tracking.
- **Avoid Public Wi-Fi**: Use a VPN when browsing on unsecured networks.
- **Log Out After Use**: Always log out of accounts, especially on shared or public devices.
- Be cautious of typosquatting domains (e.g., goggle.com instead of google.com

Tips for Public Wi-Fi Use

- **Avoid Sensitive Transactions**: Do not access banking or sensitive accounts on public Wi-Fi.
- **Use a VPN**: Encrypt your internet connection to protect your data from potential eavesdroppers.
- **Turn Off Sharing**: Disable file and printer sharing while connected to public networks.
- **Forget Networks After Use**: Ensure your device does not automatically reconnect to public Wi-Fi.
- **Verify Network Authenticity**: Confirm the network name with the provider to avoid connecting to fake networks.
- **Keep Software Updated**: Regularly update your device’s operating system and security software.

Email Security Tips

- **Think Before You Click**: Avoid clicking on suspicious links or attachments in emails.
- **Verify Senders:** Check the sender’s email address carefully for signs of spoofing.
- **Beware of Urgent Language:** Scammers often use urgency to trick you into taking action.
- **Enable Spam Filters:** Use your email provider’s spam filtering features to reduce unwanted emails.
- **Do Not Share Sensitive Information**: Avoid sending passwords, financial details, or personal information via email.
- **Use Encryption:** For highly sensitive communications, use email encryption tools.

- **Update Email Passwords Regularly:** Use strong, unique passwords and change them periodically.
- **Report Suspicious Emails**: Notify your IT team or email provider about phishing attempts.

Dos and Don’ts

- Do not change any hardware configuration, settings in the operating systems or any applications installed on their desktops.
- Do not install any software or applications on your desktops/ laptops that is not authorized by the CMES’s IT team or is not essential to CMES’s business.
- USB ports, Compact Disk (CD)/ DVD, memory card access are disabled by default. If the user needs to enable them, approval from the user’s manager and IT team shall be required.
- Take appropriate measures for physical protection of laptops such as not leaving laptops unattended in public places or while travelling.
- Do not connect removable media such as CD/ DVD, USB drives, and other portable storage media from an unknown source to a CMES system.
- Removable media containing sensitive or confidential information shall be stored in encrypted format by using CMES approved tool.
- Removable media containing sensitive information must not be left out in the open or allowed to be vulnerable to opportunistic theft.

Clear Desk and Clear Screen

- Ensure that desks and other work areas are kept clear of papers and any storage media when unattended.
- All workstations shall have password-locked screen savers enabled to activate after 5 minutes of inactivity.

Anti-virus/ Anti-malware

- Users shall not disable the installed anti-virus agent or change its settings defined during installation.
- Users shall report to the IT team for unpatched systems or any virus that is detected in the system and not cleaned by the anti-virus software.

- If you suspect any non-adherence or suspicious activities or email, kindly inform IT team at itsupport@cleanmax.com

Hardware and Software

- To prevent the introduction of malicious code and protect the integrity of CMES assets, all hardware and software shall be obtained by raising request through the IT team.
- CMES's IT team shall ensure that an approved list of authorized software is maintained.
- All employees shall abide by the software copyright law and shall not obtain, install, replicate, transfer or use software except as permitted under the licensing agreements.
- Users shall ensure that personal software are not used on CMES owned assets to protect the integrity of CMES's assets and information.

Incident Reporting

Blogging and social media

- Access to social media, blogging/ micro-blogging, and video sharing websites such as Facebook, Twitter, LinkedIn, YouTube, etc. shall be restricted to ensure productivity of the employees.
- No official matter, incidents and happenings that can align the name of CMES shall be discussed/ posted on social media platform by employees. Reporting of such an event may lead to sever consequences for the employees(s).