Course Name : O Level(B3-Ist sem.)
Topic : Cyber security and Smart Phone security

Subject : ITT&NB
Date : 24-06-20

Cyber security

Cyber security is the way or process of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. The main objective of Cyber security is to reduce the risk of cyber attacks, and protect against unauthorized exploitation of systems, networks and technologies. It is also known as information technology security or electronic information security.

Need of Cyber Security

Cyber security is needed for following reasons:

- The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit to authorized users. Information security includes those measures necessary to detect, document, and counter threats to digital and non-digital information. Information security processes and policies typically involve physical and digital security measures to protect data from unauthorized access.
- **Security:** It can be considered a state of freedom from a danger or risk. For example, a nation experiences security when it's military has the strength to protect its citizens.
- **Information:** It is an asset to all individuals and businesses. Information Security refers to the protection of these assets in order to achieve **Confidentiality, Integrity and Availability (CIA).**
- To make the system secure, optimum level of confidentiality, availability and integrity is to be maintained.

Meaning of Confidentiality, Integrity and Availability *(CIA):*

- **Confidentiality:** Protecting information from being disclosed to unauthorized parties.
- **Integrity:** Protecting information from being changed by unauthorized parties.
- **Availability:** To the availability of information to authorized parties only when requested.

Three main goals of Information security are:

- **Detection:** The most important element of this strategy is timely detection and notification of a compromise. Intrusion detection systems (IDS) are utilized for this purpose.
- **Prevention:** Security measures must be taken to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional.
- **Response:** Making important decisions or developing policy while under attack is a recipe for disaster.

Securing Personal Computer(PC)

Personal Computer security is the process of preventing and detecting unauthorized use of personal computer. Prevention measures help user to stop unauthorized users (hackers) from accessing any part of their computer system. Detection helps user to determine whether or not someone attempted to break security into their system.

PC security is considered to be more important for the following reasons:

- To prevent data theft.
- To prevent theft or destruction to hardware.
- To prevent any software or service getting disrupted.

Process of Securing Personal Computer(PC)

Personal Computer(PC) can be kept secure by implementing following processes:

- Keep up with system and software security updates.
- Install antivirus and anti spyware software.
- Back up your system.
- Enable a firewall.
- Use a standard user account.
- Keep your User Account Control enabled.
- Using Password to protect your software and lock your device.
- Secure your web browser before going online.
- Use an encryption software tool for your hard drive.
- Be careful online and don't click on suspicious links.

Securing Smart Phone

Phone security is the practice of defending mobile devices against a wide range of cyber attack vectors that threaten user's privacy, network login credentials, finance and safety.

Smart Phone can be kept secure by implementing following processes:

- **Smart Phone login account**

  All smart phones require user account for providing different cloud services like android phone provide Play store service and IOS devices provide app store service for their customer. Always use own account while logging in for the first time in their smart phone. This makes the user secure from theft or loss of the mobile, user could lock their phone using their account. Also user can find their mobile if they misplace it.

- **Always download apps from Play store (Android) or App Store (Apple)**

Always download apps from their service provider like play store or app store. Don't install any app in device by using "Unknown Sources".

- **Security on install App's or application**

  Security of application installed in mobile is also necessary job. Application like social media facebook, WhatsApp and Instragram etc, has some personal information or sensitive data. For securing this type of application use "***App lock*** "application available in Play store.

- Lock apps with App lock application.
- Use pattern lock, PIN lock or finger print scanning lock.
- Avoid answering spam calls.
- Turn your Bluetooth and Wi-Fi off when not in use.
- Update your phone's software regularly.
- Encrypt hotspots from being used by other devices.
- Store passwords in encrypted files.
- Use a VPN(Virtual Private Networks) .

Exercise:

1. Write short notes on followings:

   a. Cyber Security
   b. Security of smart phones