Cyber Security for Digital Devices

An Introduction to Cyberspace and Cyber Security

Name : Divesh Jadhwani
Institution : Pimpri Chinchwad University

Introduction to Cyberspace

- Cyberspace is the virtual environment in which communication over computer networks occurs. It encompasses the internet, computer systems, and the data they hold.

Definition of Cyberspace:

- A space in which users share information, interact with each other; engage in discussions or social media platforms, and many other activities.

- Social media platforms such as Facebook, Twitter, and LinkedIn.
- Streaming platforms like Twitch, Netflix, and Spotify.
- Metaverse projects like Sandbox and Second life .
- Cloud service providers like Google Drive.

Introduction to Cyberspace

- Overview of Computer and Web Technology:
- Computers and web technologies form the backbone of cyberspace, enabling data storage, processing, and communication.

- Historical Development of the Internet:

The internet began as a project by the US Department of Defense in the 1960s called Advanced Research Projects Agency Network (ARPANET)and has evolved into a global network connecting billions of devices as INTERNET(Interconnected Network)

Architecture of Cyberspace

- Layers of Cyberspace:
- -Physical Layer: Hardware components like servers, routers, and cables.
- - Network Layer: Protocols and technologies for data transfer.
- - Application Layer: Software applications and services.

- Communication Technologies in Cyberspace:
- - Wired and wireless communication technologies enable data transfer.
-
- - Examples include fiber optics, Wi-Fi, and cellular networks.

- Internet Infrastructure for Data Transfer:
- The internet relies on a robust infrastructure, including data centers, undersea cables, and satellite links.

Real-life Example: Phishing Attack

- Phishing attacks involve tricking individuals into revealing personal information by pretending to be a trustworthy entity.
- Example: An email pretending to be from a bank asking for account details.
- Protection: Always verify the source before providing personal information.

Case Study: Target Data Breach

- In 2013, Target Corporation suffered a massive data breach compromising the personal and credit card information of over 40 million customers.
- Cause: Hackers gained access through a third-party vendor.
- Impact: Financial loss, legal consequences, and damage to reputation.
- Lesson: Implement robust security measures and monitor third-party access.

Real-life Example: Ransomware Attack

- Ransomware is a type of malicious software that encrypts data and demands payment for the decryption key.
- Example: The WannaCry ransomware attack in 2017 affected hundreds of thousands of computers globally.
- Protection: Regular backups and updated security software can mitigate ransomware risks.

Case Study: Equifax Data Breach

- In 2017, Equifax experienced a data breach exposing sensitive information of 147 million people.
- Cause: Exploitation of a vulnerability in a web application.
- Impact: Identity theft and financial fraud risks for affected individuals.
- Lesson: Regularly update and patch systems to protect against known vulnerabilities.

Quiz: Test Your Knowledge

- 1. What is cyberspace?
- 2. Name two layers of cyberspace architecture.
- 3. What is a phishing attack? Provide an example.
- 4. Describe the impact of the Target data breach.
- 5. How can you protect against ransomware attacks?