WEEK 7 – Cybersecurity, Privacy, and Ethics

I. Cybersecurity Risks

Cybersecurity refers to the practice of protecting systems, networks, and data from digital attacks. These cyber threats aim to access, alter, or destroy sensitive information, disrupt operations, or extort money from users.

Common Cybersecurity Threats:

1. **Viruses**

- A virus is a malicious program that attaches itself to legitimate files or software.
- Once activated, it can spread to other files and damage or delete data.
- *Example:* The "ILOVEYOU" virus, which originated in the Philippines, spread through email attachments and caused billions in damages globally.

2. **Worms**

- Unlike viruses, worms do not need to attach to other programs.
- They replicate themselves and spread automatically across networks.
- *Example:* The "Conficker" worm infected millions of Windows systems by exploiting network vulnerabilities.

3. **Ransomware**

- Malware that locks or encrypts files and demands payment to restore access.
- It often spreads through phishing emails or malicious downloads.
- *Example:* The "WannaCry" ransomware attack in 2017 affected hospitals and companies worldwide.

4. **Phishing**

- A social engineering technique where attackers trick users into revealing sensitive information such as passwords or credit card numbers.
- Phishing messages often appear to come from trusted organizations or banks.

5. **Social Engineering**

- The act of manipulating people into giving confidential information.
- Attackers exploit trust, fear, or curiosity.
- *Example:* A fake "IT support" call requesting your login credentials.

6. **Spyware and Adware**

- Software that secretly gathers user data (spyware) or automatically displays unwanted ads (adware).
- These programs can slow down devices and compromise privacy.

7. **Trojan Horses**

- Malware disguised as legitimate software to trick users into installing it.
- Once inside the system, it can give attackers remote access or steal data.

II. Basic Defenses and Mitigation Strategies

Defending against cybersecurity threats requires awareness and proactive habits. These basic strategies can greatly reduce risks:

1. **Use Strong and Unique Passwords**

- Combine uppercase and lowercase letters, numbers, and symbols.
- Avoid using personal information like birthdays or pet names.
- Use a **password manager** to store and generate secure passwords.

2. **Enable Multi-Factor Authentication (MFA)**

- MFA adds an extra layer of protection by requiring a second form of verification (e.g., SMS code or authentication app).
- Even if a password is stolen, unauthorized access is prevented.

3. **Install and Update Antivirus Software**

- Antivirus programs detect, quarantine, and remove malware.
- Keep your antivirus definitions and operating system up-to-date to protect against new threats.

4. **Regular Software Updates (Patching)**

- Developers release updates to fix vulnerabilities.
- Failing to update software leaves devices open to exploitation by attackers.

5. **Avoid Suspicious Links and Attachments**

- Do not open emails, links, or attachments from unknown or unverified senders.
- Hover over links to preview the actual URL before clicking.

6. **Use Firewalls**

- A firewall acts as a barrier between your device and potential threats from the internet.
- It monitors and filters incoming and outgoing network traffic.

7. **Backup Important Data**

- Store copies of critical files on external drives or cloud storage.
- Regular backups ensure data recovery in case of ransomware or hardware failure.

8. **Secure Your Wi-Fi Network**

- Change default router passwords and use WPA3 encryption.
- Avoid using public Wi-Fi for sensitive transactions.

9. **Educate Yourself and Others**

- Cybersecurity awareness training helps identify scams and suspicious behavior.
- Think before you click — user awareness is one of the strongest defenses.

III. Privacy and Data Protection

Digital privacy refers to the right to control how your personal information is collected, used, and shared. Many people unknowingly expose data through social media or unsafe websites.

Key Privacy Concerns:

- **Data Collection:** Websites and apps often track your activity through cookies, ads, or analytics tools.
- **Identity Theft:** Attackers can steal personal data like your Social Security number, bank details, or photos to impersonate you.
- **Over-sharing:** Posting too much information online can make you a target for scams or stalking.
- **Permissions:** Mobile apps sometimes request unnecessary access to contacts, location, or camera.

Best Practices for Privacy:

- Review app permissions regularly.
- Use privacy-focused browsers or extensions.
- Log out of accounts after use, especially on shared computers.
- Avoid sharing personal details on public platforms.
- Use encrypted communication apps for sensitive conversations.

IV. Ergonomics and Health Concerns

While cybersecurity protects your data, **ergonomics** protects your body. Poor posture, long screen time, and repetitive motions can cause health issues such as eye strain, carpal tunnel syndrome, or back pain.

Tips for Healthy Computing:

- Maintain proper posture: Sit upright with your back supported.
- Keep your monitor at eye level and about an arm’s length away.

- Use ergonomic keyboards and mouse devices to prevent wrist strain.
- Follow the **20-20-20 rule** — every 20 minutes, look at something 20 feet away for 20 seconds.
- Take short breaks to stretch and relax your hands and neck.
- Ensure proper lighting to reduce glare and eye fatigue.