Unit 6: Personal Cybersecurity (5 LHs)

6.1. Evaluating Cybersecurity for Home Computers

Home computers are critical as they often store sensitive data like financial information, personal documents, and login credentials. Proper evaluation ensures protection against cyber threats.

Key Areas to Evaluate:

1. **Operating System (OS) Updates and Patches**
    - Ensure the OS (Windows, macOS, Linux) is updated to the latest version.
    - Regular security patches address newly discovered vulnerabilities.
    - **Tools:** Automatic updates enabled on the OS.
2. **Antivirus and Anti-Malware Software**
    - Install and update reliable antivirus/anti-malware programs.
    - Perform regular scans for threats.
    - **Examples:** Windows Defender, Avast, Kaspersky, Malwarebytes.
3. **Firewall Configuration**
    - Enable firewalls to block unauthorized network traffic.
    - Check default firewall settings and ensure proper configuration.
    - **Types:**
        - Software Firewalls (e.g., OS built-in firewalls)
        - Hardware Firewalls (e.g., router-based firewalls).
4. **User Accounts and Passwords**
    - Use **strong, unique passwords** for all accounts.
    - Enable **multi-factor authentication (MFA)** where possible.
    - Remove unused or default user accounts.
    - Tools like **password managers** help store and manage passwords securely (e.g., LastPass, Bitwarden).
5. **Software and Application Security**
    - Remove unnecessary or outdated applications.
    - Install software only from trusted sources.
    - Enable auto-updates for software (e.g., browsers, plugins).
6. **Data Backup and Recovery**
    - Regularly back up critical data to secure locations (e.g., cloud storage or external drives).
    - Use automated backup solutions (e.g., OneDrive, Google Drive, Acronis).
7. **Network Security**
    - Use encrypted Wi-Fi connections (WPA3 or WPA2).
    - Regularly update router firmware and change default login credentials.
    - Disable remote administration on the router.
8. **Threat Monitoring**
    - Monitor for unusual activity on your system.

- Tools: Activity logs, Resource Monitor, and Security Information and Event Management (SIEM) tools.

---

2. Evaluating Cybersecurity for Mobile Devices

Mobile devices are increasingly targeted due to their widespread usage for communication, financial transactions, and accessing sensitive information.

Key Areas to Evaluate:

1. **Operating System and App Updates**
   - Regularly update the mobile OS (e.g., iOS, Android) for security patches.
   - Keep applications updated to avoid vulnerabilities.
2. **Device Access Control**
   - Enable **biometric authentication** (fingerprint, facial recognition) or strong PINs/passwords.
   - Configure automatic screen locks after inactivity.
3. **App Permissions and Privacy Settings**
   - Review and minimize app permissions (e.g., location, camera, microphone).
   - Remove unused applications.
   - **Tools:** Device settings and privacy dashboards (e.g., Android Privacy Dashboard, iOS App Tracking Transparency).
4. **Mobile Antivirus and Security Apps**
   - Install reputable mobile security software.
   - **Examples:** Norton Mobile Security, Avast Mobile Security, Lookout.
5. **Data Backup and Encryption**
   - Enable automatic backups (e.g., iCloud, Google Backup).
   - Ensure device storage is encrypted.
6. **Secure Mobile Connections**
   - Avoid public Wi-Fi or use a **VPN** (Virtual Private Network) to encrypt connections.
   - Use mobile hotspots with WPA2/WPA3 encryption.
7. **Lost Device Protection**
   - Enable device tracking and remote wipe features (e.g., Find My Device on Android, Find My iPhone on iOS).
8. **Threat Detection and Phishing Awareness**
   - Avoid clicking on unknown links and downloading files from untrusted sources.
   - Recognize phishing SMS (Smishing) and malicious apps.

---

3. Evaluating Cybersecurity for Internet of Things (IoT) Devices

IoT devices include smart home gadgets, wearables, and connected appliances. While they improve convenience, they often have weak security, making them prime targets for attacks.

Key Areas to Evaluate:

1. **Device Authentication and Password Security**
    - Change default usernames and passwords for IoT devices.
    - Use strong, unique passwords for each device.
    - Enable two-factor authentication if supported.
2. **Firmware Updates**
    - Regularly update device firmware to patch security vulnerabilities.
    - Check for updates from the manufacturer’s website or mobile app.
3. **Network Segmentation**
    - Isolate IoT devices on a separate Wi-Fi network (Guest Network or VLAN).
    - Ensure critical devices like computers are on a different network.
4. **Secure Device Connections**
    - Use encrypted protocols for device communication (e.g., HTTPS, TLS).
    - Disable Universal Plug and Play (UPnP) to prevent unauthorized device access.
5. **Monitoring Device Activity**
    - Regularly review device logs and network traffic for suspicious activity.
    - Tools: Router logs, IoT monitoring tools like Fing or IoT Inspector.
6. **Disable Unused Features**
    - Turn off unused features such as voice control, Bluetooth, or remote access.
    - Remove any devices no longer in use.
7. **Router and Gateway Security**
    - Update router firmware and enable WPA3/WPA2 encryption.
    - Use a firewall and disable unused ports.
8. **Secure IoT Management Platforms**
    - If managing multiple devices through a hub (e.g., Google Home, Amazon Alexa), enable strong authentication.
    - Regularly review and remove unnecessary connected devices.

Steps for Personal Cybersecurity Posture Evaluation

1. **Conduct a Security Audit**
    - List all devices (home computer, mobile, IoT).
    - Check for software updates, strong passwords, and unnecessary applications.
2. **Assess Network Security**

- Use tools like **Nmap** or **Wireshark** to scan for vulnerabilities on your network.
- Test encryption levels and network segmentation.

3. **Backup Critical Data**
   - Implement a **3-2-1 Backup Strategy**: 3 copies of data, 2 on different media, 1 offsite.
4. **Enable Threat Detection and Response**
   - Deploy antivirus software, intrusion detection tools, and mobile security apps.
   - Monitor logs for unusual behavior.
5. **User Awareness and Training**
   - Educate household members on phishing risks, secure device usage, and safe browsing habits.

6.2 Enhancing Physical Security

Physical security protects systems, data, and infrastructure from unauthorized physical access, theft, or damage.

Key Measures:

1. **Deterrence:**
   - Visible security systems like CCTV, warning signs, security guards, and proper lighting.
2. **Prevention:**
   - Access controls: keycards, biometrics, and PIN systems.
   - Physical barriers: secure doors, fences, locks, and cable ties for devices.
3. **Detection:**
   - Surveillance cameras, motion detectors, and alarms to identify suspicious activity.
4. **Response:**
   - On-site security personnel, emergency procedures, and incident logs to address breaches quickly.

Focus Areas:

- **Workspaces:** Lock devices and sensitive documents.
- **Server Rooms:** Restrict access with biometrics and locks.
- **Mobile Devices:** Use physical locks and remote wipe features.
- **Network Equipment:** Secure routers and switches in locked cabinets.

Best Practices:

- Conduct audits.

- Train employees.
- Use multi-layered security systems.
- Secure backup devices.

6.3 Cybersecurity Considerations When Working from Home

Working from home introduces security risks that must be addressed to protect systems, data, and networks.

---

1. Securing Home Networks

- **Change Router Defaults:** Update router username, password, and enable WPA2/WPA3 encryption.
- **Use Strong Wi-Fi Passwords.**
- **Enable Firewalls:** Use router and software firewalls.
- **Network Segmentation:** Separate work devices from personal/IoT devices.

---

2. Securing Work Devices

- **Update Systems:** Keep OS, software, and security tools up-to-date.
- **Install Antivirus:** Use tools like Norton or Malwarebytes.
- **Enable Device Encryption:** Secure data with full-disk encryption.
- **Strong Authentication:** Use strong passwords, MFA, and biometrics.
- **Automatic Locking:** Devices should lock after inactivity.
- **Regular Backups:** Use secure cloud storage or encrypted drives.

---

3. Secure Communication

- **Use VPNs:** Encrypt your internet connection.
- **Encrypted Tools:** Use secure apps like Microsoft Teams, Zoom, or Slack.
- **Avoid Phishing:** Don’t click suspicious links or emails.

---

4. Personal Device Safety

- **Install Security Tools:** Use antivirus and firewalls.
- **Keep Devices Updated:** Regular OS and software updates.
- **Separate User Accounts:** Avoid sharing devices with family.

---

5. Protect Sensitive Data

- Use company-approved cloud storage (e.g., OneDrive).
- Avoid storing sensitive data locally.
- Dispose of printed documents securely.
- Use secure file-sharing tools instead of email attachments.

---

6. Physical Security

- Lock devices and workspaces when not in use.
- Use privacy screens to prevent shoulder surfing.
- Store external drives and sensitive documents securely.

---

7. Employee Awareness

- Recognize phishing attempts and suspicious messages.
- Avoid public Wi-Fi; use VPNs when needed.
- Report incidents to IT immediately.

6.4 Securing Your Accounts and Passwords

Properly securing accounts and passwords is critical to protecting personal and sensitive information from unauthorized access.

---

1. Use Strong and Unique Passwords

- Create **long and complex passwords** (at least 12 characters).
- Use a mix of **uppercase, lowercase, numbers, and symbols**.
- Avoid common passwords (e.g., "123456," "password," or birthdays).
- **Don’t reuse passwords** across multiple accounts.

---

2. Enable Multi-Factor Authentication (MFA)

- Add an extra layer of security by enabling **MFA** on all accounts.
- Methods include:
  - **One-time codes** sent via SMS, email, or authenticator apps (e.g., Google Authenticator, Authy).
  - **Biometrics** like fingerprints or facial recognition.

---

3. Use Password Managers

- Password managers help generate, store, and autofill strong, unique passwords securely.
- Examples: LastPass, 1Password, Bitwarden.
- Benefits:
  - Reduces the need to memorize passwords.
  - Protects passwords with encryption.

---

4. Regularly Update Passwords

- Change passwords periodically, especially for sensitive accounts (e.g., banking, work emails).
- Update passwords immediately if a breach is suspected or reported.

---

5. Avoid Password Sharing

- Never share passwords through email, text, or unsecure platforms.
- Use **secure tools** for sharing passwords when absolutely necessary.

---

6. Monitor for Breaches

- Use tools like **Have I Been Pwned** to check if your accounts were part of a data breach.
- If compromised, change the password immediately and enable MFA.

---

7. Protect Password Recovery Options

- Secure your recovery email and phone number.

- Use strong passwords and MFA on recovery accounts to prevent unauthorized resets.
