Cyber Security Checklist

1. Password Security:
   - Use strong, unique passwords for each account.
   - Enable multi-factor authentication (MFA) whenever possible.
   - Regularly update and change passwords.

2. Software Updates:
   - Keep operating systems, applications, and antivirus software up to date.
   - Enable automatic updates whenever possible.

3. Secure Network:
   - Use a firewall to protect your network.
   - Change default router passwords and use strong encryption (WPA2 or higher) for Wi-Fi networks.
   - Disable guest networks if not needed.

4. Data Backup:
   - Regularly backup important data to an external hard drive, cloud storage, or other secure locations.
   - Test data restoration process periodically to ensure backups are working properly.

5. Phishing Awareness:
   - Be cautious of suspicious emails, links, and attachments.
   - Verify the authenticity of emails from unknown senders.
   - Avoid clicking on suspicious links or providing personal information in response to unsolicited requests.

6. Social Media and Online Privacy:
   - Review and adjust privacy settings on social media accounts.
   - Be mindful of the information you share online.
   - Avoid accepting friend requests or connections from unknown individuals.

7. Secure Web Browsing:
   - Use secure and up-to-date web browsers.
   - Enable pop-up blockers and disable unnecessary browser plugins.
   - Avoid visiting suspicious or untrusted websites.

8. Mobile Security:
   - Use a passcode or biometric authentication on your mobile devices.
   - Install apps only from trusted sources (official app stores).
   - Regularly update mobile operating systems and apps.

9. Physical Security:
   - Keep devices physically secure, especially laptops and mobile devices.
   - Lock your computer or mobile device when not in use.
   - Do not leave sensitive documents unattended.

10. Employee Education:
    - Conduct regular cyber security awareness training for employees.

Cyber Security Checklist

- Teach employees about common threats like phishing and social engineering.

- Encourage reporting of suspicious activities or incidents.

Remember, this checklist is just a starting point, and cybersecurity is an ongoing effort. It's important to stay updated on the latest security practices and adapt them to your specific needs.