### **Cyber Awareness and Hygiene Tips for Elderly People**

1. **Secure Your Online Accounts**
   * Use **strong, unique passwords** for each online account.
   * Enable **two-factor authentication (2FA)** wherever possible for added security.
2. **Be Cautious with Emails and Messages**
   * Do not open **emails**, **attachments**, or **links** from unknown senders.
   * Be wary of emails asking for **personal information** or **bank details**—they may be phishing scams.
3. **Protect Your Personal Information**
   * Avoid sharing **personal details** like your **address**, **phone number**, or **bank information** on social media or unknown websites.
   * Never share **PINs**, **passwords**, or **OTP codes** with anyone, even if they claim to be from a trusted organization.
4. **Recognize Common Scams**
   * Be aware of **lottery scams**, **fake investment offers**, and **technical support scams**.
   * If someone claims you’ve won a prize or requests payment for a service you didn’t request, it’s likely a scam.
5. **Use Secure Devices and Networks**
   * Ensure your **computer** and **smartphone** have **updated antivirus software**.
   * Use **trusted Wi-Fi networks** at home, and avoid using **public Wi-Fi** for sensitive activities like online banking.
6. **Protect Your Financial Information**
   * Do online banking only through **official bank websites** or **verified apps**.
   * Regularly check your **bank statements** for unauthorized transactions.
7. **Be Careful on Social Media**
   * Be selective when **accepting friend requests**, especially from people you don’t know personally.
   * Adjust your **privacy settings** to control who can see your posts and personal information.
8. **Recognize Fake Calls and Messages**
   * Beware of phone calls claiming to be from **banks**, **government agencies**, or **tech support** asking for your personal information.
   * Legitimate organizations will **never** ask for sensitive details over the phone or through unsolicited messages.
9. **Keep Your Devices Updated**
   * Regularly **update your smartphone, tablet, or computer** to install the latest **security patches**.
   * Only download apps from **trusted sources** like the Google Play Store or Apple App Store.
10. **Safeguard Your Devices**
    * Lock your phone or computer with a **password**, **PIN**, or **fingerprint**.
    * Never leave your devices **unattended** in public places.
11. **Backup Your Data Regularly**
    * Keep **backups** of important documents, photos, and files on an **external hard drive** or a **trusted cloud service**.
    * This will help recover your data in case of a cyberattack or device failure.
12. **Report Suspicious Activity**
    * If you suspect any **fraud** or **cybercrime**, report it to the **nearest police station** or the **Cyber Crime Reporting Portal** ([www.cybercrime.gov.in](http://www.cybercrime.gov.in/)).
    * Consult with trusted **family members** or **friends** if you're unsure about an