Keeping your family safe on the Internet

By following these guidelines, parents can significantly reduce the risk of their children accessing inappropriate content and help them maintain a safer and healthier online experience.

1. Set Up Router Parental Controls

- **Access Router Settings**: Log into your router's web interface (usually by typing 192.168.1.1 or 192.168.0.1in the browser).
- **Enable Parental Controls**: Many modern routers come with built-in parental control features that allow you to block websites, restrict internet access during certain hours, and monitor online activity.
- **Set up Content Filtering**: Block inappropriate content based on categories such as adult content, violence, or gambling.

2. Use Device-Level Parental Controls

- **For Smartphones**: Both Android and iOS have built-in parental controls (e.g., Google Family Link and Apple's Screen Time) that allow you to set limits on app usage, manage purchases, and block inappropriate content.
- **For Computers**:
  - **Windows**: Use the Family Safety feature to set up user accounts, activity reporting, screen time limits, and content restrictions.
  - **Mac**: Use Screen Time settings to set up app usage limits, content restrictions, and downtime.

3. Monitor Online Activity

- **Use Monitoring Apps**: Apps like Bark or Qustodio can help monitor texts, social media activity, and web browsing, while also blocking harmful content.
- **Review Browsing History**: Regularly check your child's browsing history to ensure they are accessing safe and age-appropriate websites.

4. Set Up Time Limits

- **Screen Time Management**: Set time limits for different activities (e.g., educational time vs. entertainment) to ensure a healthy balance between online and offline activities.
- **Scheduled Internet Access**: Use router controls or app settings to disable the internet during certain hours (e.g., bedtime or during study time).

5. Block Inappropriate Websites

- **Safe Browsing Tools**: Use tools like Google SafeSearch or DNS services (e.g., OpenDNS) that filter harmful content from web searches.
- **Create a Block List**: Add specific sites to a block list within the router or parental control software.

6. Educate and Discuss Online Safety

- **Open Communication**: Regularly talk to your child about the dangers of sharing personal information, interacting with strangers, and navigating social media.
- **Set Rules for Social Media**: Decide on which platforms are acceptable for your child, monitor their profiles, and ensure privacy settings are appropriate.

7. Use Secure Passwords

- **Strong Passwords**: Make sure all accounts (email, social media, etc.) are protected with strong, unique passwords.
- **Use Two-Factor Authentication**: Enable 2FA where possible for added security.

8. Regularly Update Devices

- **Software Updates**: Ensure that devices and apps are up-to-date with the latest security patches.
- **Antivirus Software**: Install reliable antivirus and anti-malware programs to protect against potential threats.