Social Media Safety Checklist (Ages 13-17)

Introduction

Social media is a powerful tool for connection, creativity, and communication, but it also comes with responsibilities. This checklist is designed specifically for teenagers (ages 13-17) to help you review your privacy settings, online habits, and overall safety on popular social media platforms. By regularly checking these points, you can ensure a safer and more positive online experience.

Your Privacy Settings: Lock It Down!

Your privacy settings are like the locks on your digital door. Make sure they are strong and only let in who you want [3].

- **Review All Privacy Settings**: Go through the settings of every social media account you use (Instagram, TikTok, Snapchat, YouTube, etc.). Make sure only people you absolutely trust can see your posts and profile [3].
    - **Action**: Set your profile to “Private” on platforms where this option is available.
- **Limit Who Can Contact You**: Check who is allowed to send you direct messages or friend requests. Restrict these to “Friends Only” or “People You Know” to avoid unwanted contact from strangers [3].
- **Turn Off Location Tracking**: Disable location services for social media apps on your phone. Avoid geotagging your posts, as this can reveal your current location or frequent hangouts to others [1].
    - **Why**: Sharing your location can make you a target for unwanted attention or even real-world risks.

- **Control Who Can Tag You**: Adjust settings so that you have to approve any tags in photos or posts before they appear on your profile. This helps prevent others from posting embarrassing or inappropriate content about you [3].
- **Manage Your Audience**: Understand who can see your stories, posts, and comments. Use features like “Close Friends” lists or custom audience settings to share content with specific groups [3].
- **Check Third-Party App Permissions**: Review which third-party apps have access to your social media accounts. Remove any apps you don’t recognize or no longer use, as they might be collecting your data [3].

Your Online Habits: Be a Smart Digital Citizen!

What you do and say online matters. Good habits protect you and others [3].

- **Think Before You Post**: Before sharing anything, ask yourself: “Is this kind? Is it true? Is it necessary? Is it helpful? Is it legal?” Once something is online, it can be very difficult to take back [3].
    - **Why**: Your digital footprint is permanent and can be seen by future colleges, employers, and others.
- **Don’t Share Sensitive Information**: Never post your full name, home address, phone number, birthdate, Social Security number, or financial details online. This information can be used for identity theft or other harmful purposes [3].
- **Be Skeptical of Links and Downloads**: Don’t click on unexpected links or attachments, even if they seem to come from a friend. They could contain viruses or lead to scams. If in doubt, ask the sender directly through a different communication method [2, 3].
- **Verify Website Legitimacy**: Malicious websites can look very similar to trusted ones. Always check the URL in the address bar for misspellings or unusual domains (e.g., `.net` instead of `.com`). If something feels off, avoid the site [3].
- **Use Strong, Unique Passwords**: Create passwords that are a mix of uppercase and lowercase letters, numbers, and symbols. Use a different password for each important account. Consider using a password manager [1, 3].
- **Enable Two-Factor Authentication (2FA)**: Turn on 2FA for all your social media accounts. This adds an extra layer of security by requiring a code from your phone in addition to your password [2].

- **Update Your Software**: Keep your phone’s operating system, apps, and web browsers updated. Updates often include important security fixes [1, 3].
- **Be Wary of “Too Good to Be True” Offers**: Free games, gift cards, or exclusive content that seems too good to be true often come at a cost to your privacy or security. Only download from trusted sources [1, 3].
- **Public Wi-Fi Caution**: Be careful when using free public Wi-Fi. These networks are often not secure and could expose your personal information. Avoid accessing sensitive accounts (like banking) on public Wi-Fi [3].
- **Respect Others**: Treat others online as you would in person. Don’t engage in cyberbullying, spread rumors, or post hurtful comments. Be an upstander, not a bystander [1].

What to Do If Something Goes Wrong: Get Help!

Even with the best precautions, sometimes things can go wrong. It’s crucial to know what to do and who to talk to [3].

- **Don’t Keep it a Secret**: If you or someone you know is being cyberbullied, harassed, or feels unsafe online, tell a trusted adult immediately. This could be a parent, guardian, teacher, counselor, or another family member [3].
- **Don’t Engage with Bullies**: If someone is being mean or sending hurtful messages, do not respond. Engaging can make the situation worse. Block the person and save the evidence [3].
- **Save Evidence**: Take screenshots of any cyberbullying, harassment, or suspicious messages. This evidence can be important if you need to report the incident to the platform or authorities [3].
- **Report to the Platform**: Most social media platforms have ways to report inappropriate content or behavior. Use these features to flag problematic posts or users [3].
- **Seek Professional Help**: If you are feeling overwhelmed, anxious, sad, or distressed because of online experiences, talk to a school counselor or mental health professional. Your well-being is the most important thing [3].
- **If in Immediate Danger**: If you feel you are in immediate danger, contact your local police or emergency services [3].

Conclusion

By actively using this checklist, you’re taking control of your online safety and becoming a more responsible digital citizen. The internet is a fantastic place, and by being smart, aware, and proactive, you can enjoy all its benefits while protecting yourself and others. Stay safe, stay smart, and keep clicking wisely!

References

[1] Internet Safety for Kids - The Annie E. Casey Foundation. (2025, March 7). *The Annie E. Casey Foundation*. https://www.aecf.org/blog/internet-safety-for-kids [2] Think Before You Click | FIU IT Security Office. (n.d.). *Florida International University*. https://security.fiu.edu/training/think-before-you-click/ [3] Online Safety Tips for Teens | NCDIT. (n.d.). *NCDIT*. https://it.nc.gov/resources/online-safety-privacy/tips-guidance/online-safety-tips-teens