

Ready to soak up the sun and surf the web this summer? Before you dive into endless hours of online fun, you need to know how to stay safe online. From scrolling through social media to online gaming, Know2Protect has you covered.

- **1.** Set all apps, games, social media accounts and devices to private.
- 2. Turn off location data services on social media and all apps, except the ones your family uses to keep track of where you are. Talk to a trusted adult about which apps need location services and which don't.
- 3. Remember, anything posted online can be found later, even if it's deleted. After it's sent, you can't take it back.
- 4. Don't believe that everyone is who they say they are online.
- 5. Know who is on your friend lists. Remove strangers. Only accept friends you know in real life.
- 6. Never leave a game to chat on a different platform with someone you don't know.
- 7. Don't respond to messages or requests from people you don't know.
- 8. If something happens that makes you feel uncomfortable or you feel like something's just not right, tell an adult you trust, such as a parent, relative, teacher or family friend.
- **9. Do not** delete messages or images. Save usernames, screenshots and images as evidence.
- **10.** Don't panic. You're not alone. There are many ways you can get help.





Parents and trusted adults: Children and teens have extra time with their devices when they're not in school. Use these tips to help them stay safe online.

- **1.** Start an open, two-way conversation with your child.
- 2. Password-protect or control access to your child's app store and gaming downloads.
- 3. Set time and area limits for use of devices and set device check-in times.
- 4. Set all apps, games and devices to private.
- 5. Turn off location data services on social media and nonessential apps.
- 6. Talk about data permanency. Online data can last a lifetime.
- 7. Create a contract with your child regarding online behavior.
- 8. Know your child's friend lists. Remove strangers.
- **9.** Warn your child that they should never leave a game to chat with someone they don't know on a different platform.
- 10. Do not delete messages, images or videos from predators and do not forward any sexually explicit images or videos. Save usernames, screenshots and images or videos as evidence for law enforcement to collect directly from the device.

