Nicklaus Children's Hospital

SAFE+SOUND
The Digital Safety Alliance

KIDS AND ONLINE PRIVACY

A Quick Guide for Parents

Smartphones offer kids great opportunities to learn, connect, and explore. They also come with significant privacy risks.

Companies collect user information via apps and social media, while cybercriminals and predators exploit security loopholes and kids' trust.

By taking a proactive role in your kids' online safety, you can help keep them safe.

Online Privacy Risks for Kids

- Kids can accidentally share personal information on social media, gaming platforms, or other websites. This information can be exploited by cybercriminals or predators.
- Many apps and websites collect user data — including browsing habits, location, and device information — which can leave children vulnerable.
- Children can fall victim to scammers "phishing" or tricking them into revealing private information through fake emails, links, or messages.
- Using public WiFi or unsecured websites can expose their personal information to hackers.
- Bad actors can coerce them into sharing personal data, photos, or videos by building their trust.

EACH YEAR

1 in 43 kids

HAS THEIR PERSONAL INFORMATION EXPOSED OR COMPROMISED.

Tips for Protecting Your Kids' Online Privacy

1. Talk regularly with your kids to understand what they're doing and sharing online. Remind them that posts aren't always private, and they should think before they click or connect with others.
2. Teach your child to use strong, unique passwords and never share them. Consider using a password manager.
3. Encourage the use of secure, private WiFi networks and websites that begin with "https" (indicating they're secure). Remind them to avoid public WiFi.
4. Enable privacy settings on devices, apps, and websites. Teach them how their posts could be used by others.
5. Be careful with downloads and links. Spyware, malware, and other harmful software can be embedded in what seem like regular downloads. Use antivirus software to keep your devices safe.
6. Educate your child on how to recognize and avoid phishing attempts, suspicious links, fake profiles, and scams. Make sure they exercise caution before sharing any personal details.
7. Regularly check your child's online activities using parental controls or monitoring tools to spot risks. Keep the conversation open to understand experiences and build trust, reassuring them you can help if they make a mistake.
8. Set a good example by following the above recommendations, as well as by not sharing any of your kids' personal information or sensitive photos.

Use this QR code to access useful tools and resources to keep your kids safe online!

If your child is experiencing symptoms of depression, anxiety, or other behavioral disorders, it may be time to seek professional help. Contact the Nicklaus Children's Psychology Team at: 305-669-6503