TRUSTED FUTURE

RAISING PRIVACY CONSCIOUS CHILDREN

Access to new technologies can keep families and kids connected, enable new ways to learn, and prepare our children for jobs of the future. The Internet can quite literally put the whole universe of knowledge at their fingertips. But parents also see big challenges – especially around protecting their children's privacy. Fortunately, there are some technology tools and parenting strategies that you can use to protect your children's privacy and, as important, raise children who are privacy-conscious heading into adulthood.

The need to raise privacy-conscious kids and arm them with the tools to safeguard their personal data has never been more essential. A national survey by Trusted Future found that only 16% of American adults felt firmly in control of their online personal data. Nearly 6 in 10 said they lacked trust in the security of the technology that they use.

At the same time that adults wrestle with concerns about security, safety, and privacy, Americans under 18 are growing up digital. Digital technology has never been a more integral part of a child's life, especially after two years marked by remote learning, hybrid classes, and after-school classes, music lessons, and family gatherings streamed to laptops, tablets, and phones. One study found that half of kids already had their own smartphone by age 11. By the teen years, nearly 9 in 10 kids had a smartphone at home.

Here are some easy steps you can take to raise privacy-conscious kids:

01

BE VIGILANT ABOUT THEIR PRIVACY SETTINGS.

Before using a new device or app, take the time to review and adjust the privacy preferences. Don't assume that the default privacy settings are sufficient. If your child has a social media account, make sure you review and adjust their privacy settings. You can usually adjust the settings to prevent strangers from viewing their posts, pictures, and other sensitive parts of their profile.

02

TEACH YOUR KIDS TO REVIEW PRIVACY LABELS.

Official app stores now require detailed privacy labels for mobile apps, making it much easier to compare similar apps before downloading to your device. Make sure your kids know about privacy labels and how to use them to evaluate an app's data use policies.

03

WHEN IN DOUBT, OPT OUT.

As a general matter, it is good practice to opt out of sharing as much data as possible. This is now easier than ever – on mobile devices, for instance, Apple and Android now require apps to obtain permission before tracking your child's activity. When downloading apps to their device, challenge your kids to say out loud why they think the app is asking for access to certain data. This will get them into the habit of stopping and thinking about whether the request makes sense. Get them comfortable with saying "no" to permission requests that seem unnecessarily invasive.

04

CONDUCT REGULAR PRIVACY AUDITS—TOGETHER.

It's a good practice to regularly conduct a "privacy audit" of the apps and existing data permissions on your kid's devices. Depending on your child's age, you can and should involve them in this activity. Do they still need that game that they haven't opened in months? Do they want to continue sharing certain information with a social media app? Were they even aware that their location was being tracked "in the background"?

MEET JULIA: A PRIVACY-SAVVY TEEN

Tom's seventeen-year-old daughter, Julia, is a member of her school's robotics team. After school she is scheduled to go to her teammate Lincoln's house to work on their robot ahead of next month's district-wide competition. Although she has been to his house several times, Julia has never driven the route alone and she isn't confident that she knows the way without help, so she downloads a navigation app to her phone in order to get turn-by-turn driving directions.

When she opens the app, Julia is prompted to authorize her device to share her real-time location, which she does. But she declines to allow the app to access her contacts.

When the app asks her to "always" share her location data, even when she is not using the app, Julia stops and thinks. She recognizes that this information would be useful for advertisers, but not for Julia. She declines and configures her settings to only share her location when using the app.

At Lincoln's house, Julia downloads a robotics app to help with their project. The app asks for access to her contacts, microphone, and location data. Julia doesn't understand why she would need to grant the app access to any of those things, so she says no. Troubled by the unusual permission prompts, she goes and checks the privacy label and doesn't like what she sees, prompting her to delete and replace it with a less invasive app from a competitor.

05

DISCOURAGE OVERSHARING.

When your kids are ready for social media, take some time and talk to your kids about the impact oversharing can have on their reputation, now and in the future. A survey by Trusted Future found that 9 in 10 parents are concerned about protecting their children's identity, location data (88%), and age (85%). Protecting this data is especially important for parents concerned about the threat of cyberstalkers.

Work with your kids to set up their social media accounts to maximize their privacy by limiting the audience for their post. As a rule, young kids should never accept a follow or friend request from someone they don't know.

- *If your teen fancies himself an influencer and has a public social media profile, emphasize the importance of not sharing sensitive information that could be used by an identity thief or other malicious actor. Double check that they are being careful by monitoring their public posts—knowing that mom or dad are also watching their attempts at viral videomaking may be enough to deter kids from risky online behavior.*

ADDITIONAL RESOURCES:

TRUSTED FUTURE

8 Steps to Better Protect Your Privacy Online

9 Essential Steps to Keep Your Device Secure

5 Key Steps: How to Stop your Mobile Activity from Being Tracked

WATCH: Trust Talk: Protecting Child Safety

AMERICAN PSYCHOLOGICAL ASSOCIATION

Digital guidelines: Promoting healthy technology use for children

COMMON SENSE MEDIA

Parents' Ultimate Guide to Parental Controls

Privacy and Internet Safety

How do I decide which parental controls to use?

Should I let my tween girl use social media?

What are the basic safety rules for cellphones?

CONNECTSAFELY

Family Guide to Parental Controls

FAMILY ONLINE SAFETY INSTITUTE

How to be a Good Digital Parent Toolkit

IKEEPSAFE

Guidance for the Safe and Healthy Use of Technology – Youth/Parent Fireside Chat

CISA

Keeping Children Safe Online

Staying Safe on Social Networking Sites

Parents and Educators Tip Card

Chatting with Kids about Being Online

FBI

Keeping Children Safe Online

FTC

Kids and Mobile Phones

Talk to Your Kids

Kids and Computer Security

Parental Controls

Protecting Your Child's Privacy Online

Kids: Texting and Sexting

Kids and Socializing Online

USA.GOV

Online Safety in the Age of Digital Learning

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

12 quick online privacy tips for parents

CANADIAN CENTRE FOR CYBER SECURITY

Cyber security for kids: How parents can talk with their children

AUSTRALIA'S ESAFETY COMMISSIONER

Parents, Young People, & Kids

NATIONAL CYBERSECURITY ALLIANCE

Tips for Parents on Raising Privacy-savvy Kids

INTERNET MATTERS

Helping parents keep their children safe online

KQED

How Parents can Model Better Screen Time Behavior for their Kids

NY TIMES

How and When to Limit Kids' Tech Use

PBS

Online Safety Tips for Parents

CONSUMER REPORTS

Internet Safety for kids: How to Protect your Child from Online Danger

How to Use the Parental Controls on a Smartphone

TRUSTED FUTURE

trustedfuture.org