TRUSTED FUTURE

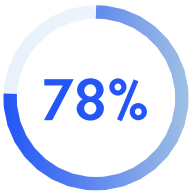
LEVERAGE CHILD SAFETY FEATURES TO PROTECT CHILDREN'S SAFETY AND PRIVACY

Today's technologies offer children endless new ways to learn, play, and communicate. But parents need to know that their children's privacy and safety will be protected online. Trusted Future's survey found that parents want to play an active role in protecting their children's privacy, safety, and security when using internet-connected devices. They also are often turning to the parental controls that have been built into their smartphones and tablets to help keep their kids safe.

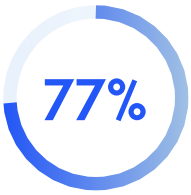
Parents strongly support the parental safety and privacy tools that companies have built into their mobile device app stores, including:

The ability to restrict children's in-app purchases

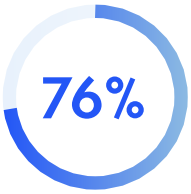
The ability to block mature content



The ability to limit targeting and tracking of kids



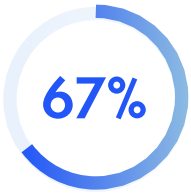
The ability to see what data may be collected about their children



The ability to restrict children's app downloads

A carefully curated kids app store that is age appropriate

The ability to set a specific time, like bedtime, when apps and notifications are blocked



The ability to keep track of how much time their kids spend using different apps

By making use of the range of features and controls now available to parents, you can better protect the safety, security and privacy of your kids even as they engage with technology with increasing independence. Here are some practical expert-curated steps you can take right now to better protect your children's safety and privacy:

01

DO YOUR HOMEWORK.

Just because a website, app, or game appears aimed at kids, doesn't mean it is safe or appropriate. Read reviews. Better yet, try it out yourself first. Make sure you understand how your data will be used and handled. The official app stores now require detailed privacy labels, making it much easier to compare similar apps.

02

MAKE SURE THEIR DEVICES AND ACCOUNTS *REMAIN* SECURE.

Cybersecurity is not a one-and-done proposition. Parents should regularly check to confirm that their child's device is secure and free of malicious software. One of the easiest ways to do this is to always install official security updates from your device or software supplier. Criminals are constantly finding new ways to try to access your device or information, and technology companies are constantly updating your protections. A security update means your provider is plugging another hole—but you must install the update to get that protection! If offered, turn on the function that automatically updates your device.

Just as they do with adults, cyberthieves can obtain the login credentials for your kids' email, social media, and other online accounts, either through a targeted social engineering attack or from a large data leak. In addition to helping you create unique passwords for each account, which can isolate the threat from an attack to just one account, password manager programs can notify you if a password is found in a data leak.

03

TAKE ADVANTAGE OF APPROPRIATE PARENTAL CONTROLS.

Parental controls are increasingly sophisticated and can help support parents in their efforts to ensure that their children's Internet experience is safe, educational, and productive. There are a wide array of parental controls now available. They can allow a parent to manage a child's ability to download apps or make in-app purchases without their permission. Content filters and "safe search" settings can be used to limit access to adult and other inappropriate content. You can also set screen time limits to encourage balance, including restricting access to certain apps and websites on school nights or during the night when your child should be asleep. For these older kids, experts indicate that when they feel like they are trusted, they will often make better decisions than if they don't feel trusted.

Devorah Heitner, a parent educator and the author of *Screenwise*, says,

"When our kids feel trusted, they often will make better decisions than if they don't feel trusted, because we're not encouraging them to feel like they need to lie or be deceptive."

Source: NPR

- *A recent Trusted Future survey found that 68% of respondents strongly support the ability to stop apps from tracking their digital activity. Don't forget you can adjust ad settings to prevent you and your family's activities from being tracked across apps and websites and limit the volume of age-inappropriate ads your kids see.*

04

ADD A SECOND LAYER OF DEFENSE BY LIMITING YOUR KIDS' ABILITY TO DOWNLOAD MOBILE MALWARE BY MISTAKE.

Bad actors have become more sophisticated about the use of social engineering to manipulate users into clicking on dangerous links via emails or text messages, some of which prompt users to download a malicious app containing malware. As a result, millions of *adults* get tricked into clicking on malicious links every year. But you can greatly increase the likelihood that your child's device and accounts will remain secure *even if* they fall prey to a social engineering scam by limiting their ability to "sideload" apps from unofficial app stores and third-party websites. Devices that have been configured to allow sideloading can easily fall victim to "smishing" attacks (social engineering attacks that use SMS messaging as the vector to get you to download a malicious app) or other social engineering tricks (like web pages 'offering' free cool apps that, once downloaded, facilitate third-party control of your device, its functions, and access to your data). You can protect their device by only allowing app downloads from official app stores, such as Android's Google Play and Apple's App Store, which invest considerable resources into vetting apps.

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

trustedfuture.org