TREND MICRO

Internet of Things Buyer's Guide for Smart Parents and Guardians

A TrendLabs Digital Life E-Guide

With the introduction of the internet of things (IoT), there are now more connected devices in homes around the world. Therefore, guidelines on how to ensure online safety for kids must adapt to the change IoT brings.

Smart devices for kids such as game consoles, smart watches, and other toys are redefining how young learners can interact and play. As a parent or guardian, it is important to find the balance of providing ways for kids to learn and have fun in a safe and secure way.

To keep your kid safe while using smart devices or toys, we will provide you with eight considerations, on online privacy—that should be considered when buying a new smart device.

Personal Data

Some smart devices require personal information about your kid–such as their name, age, birthday, gender, and home address. So when cybercriminals exploit security flaws in some smart devices, your kid's personal data can be exposed. Therefore, you have to assess what type of personal information you want your kid to share through their smart devices. Here are some ways you can keep your kid's personal information safe online:

- **Know what your kid shares online.** Remind your child that they should be cautious whenever they share anything related to their personal information. When a device stores less information (or none at all) about your kid, there is a lower chance for your kid's sensitive information to fall into the hands of the bad guys.

- **Read the device manufacturer's privacy policy.** Knowing how your kid's data are collected and where they are stored is essential to help you determine if their information is safe.

- **Review and adjust privacy settings accordingly.** Check the device's privacy settings and only enable features that won't compromise your kid's privacy. For instance, the setting that allows the device to block certain people or sites from viewing your kid's information is a good one to activate. After choosing which settings to authorize, it's important to help your kid understand why and how these settings can protect them.

Whereabouts

Monitoring your kid’s current location in real-time is easy with GPS-enabled devices. In fact, there are even some devices that allow kids to call their parents during an emergency. But what happens when your kid’s GPS-enabled device gets hacked? Recently, a GPS tracker for kids was reported to have a bug that allowed hackers to track a kid’s location and even pose as the kid’s parent. Here are a few tips on how to keep track of your kid safely:

- **Familiarize yourself with the device’s location settings.** Learn how your kid’s GPS-enabled device works and find out if there is a way for other people to know your kid’s location or usual routes.

- **Adjust how specific the location tracking is.** Devices with location-based services allow you to narrow down or broaden the geotagging feature. Manage the settings for geotagging so the tagged location of your kid will only reveal the city and not the exact address.

Visual Data

Smart devices with built-in cameras make it easy for kids to share photos and videos to other people instantly. With this, there's a chance that your kid may exchange photos or videos with people they barely know. Here are some ways to check if the camera is really turned off and if it is protected from third-party access:

- **Determine if your kid really needs a device with a camera.** If you're okay with that, help your kid understand all the positive and negative implications of using a device with a camera connected to the internet.
- **Enable camera recording only when the camera is in use.** Instead of allowing the device to record by default, activate the feature that allows you to manually enable the camera only when a photo or video needs to be taken. You can also cover the camera lens if it's not in use.
- **Supervise your kid when he/she is sharing images or videos.** Require your kid to ask for permission before downloading or posting photos and videos online. Also, remind your kid to only share data to people they know and trust.
- **Ask your kid to use avatars instead of personal photos.** Avatars are more kid-friendly (not to mention fun) to use online. Using avatars for your kid's profile photo also helps conceal your child's physical features.

Audio Data

Some smart devices function by listening to your kid's voice commands. And so, these devices usually keep those audio files to function properly. Most of the time, however, people do not know how these files are being used or how long they are being stored. Here are some tips on how to secure your kid's privacy when using devices with audio-recording features:

- **Disable default recording of audio.** If there's a microphone on your kid's smart device, make sure that the Mute button is turned on. This way, you know that the gadget is not listening in on conversations.
- **Review and/or delete audio files.** Review recordings and delete files that are unnecessary to be stored in the device.

Voice Communication

Smart devices connect and communicate with other devices through the internet. With this feature, two-way communication between your kid and family or friends is possible. Sometimes, a security flaw in your kid's device may allow strangers to talk to your child. Here are some tips on how to make sure strangers don't get into conversations with your kid:

- **Check if there's an option to disable two-way communication.** If it's not in use, disable the feature to restrict potential interactions with strangers.
- **Tell your kid to inform you of any unusual communication.** Sometimes children may feel guilty of odd activities taking place so it's important to reassure your kid that they can approach you anytime if something doesn't seem right.

Text Messages

The cyber attack against a famous toy manufacturer had been tagged as one of the worst breaches as it exposed over 190GB of photos and chat logs between parents and their kids. Such a breach helped convince a lot of parents that securing their kid’s activities on smart devices is important. Here are a few tips on how to secure your kid’s messages:

- **Filter the contact list.** Check the device settings and review your kid’s friends list. Make sure that the list only includes people your kid actually knows.
- **Manage the communication features.** See if the device allows you to filter your kid’s messaging activity by content, time, and intended recipient. That way, it will be easier for you to track strange messages your kid may read.

Biometric Data

Biometric data in smart devices can be used to get your kid's physical and behavioral characteristics. For instance, experts flagged a well-known doll brand for using a speech recognition system that processes data via the internet. Parents raised concerns about how conversations between their kids and the doll could be recorded and shared without permission. Here are a few ways you can keep your kid's biometric data secure online:

- **Make sure that the device manufacturer requires your written consent before any biometric data is collected or shared.** Even if the device manufacturer already has your consent, it is still their responsibility to provide information about how and what type of biometric data is collected, analyzed, and/or shared.

- **Find out if there's an option to refuse data collection at any given time.** Biometric data, such as a fingerprint, is unique to every individual. If compromised, the data can be used to identify your kid. So if privacy concerns over your kid's device will be raised in the future, having the option to exclude your kid's data from being collected will help protect their privacy.

Cloud Storage

Smart device manufacturers can use cloud storage to control and process data. With data stored in the cloud, parents must know that there is a chance that their kid's data may be compromised. Here are some tips on how you can secure your kid's data in the cloud:

- **Learn all there is to know about how the device stores data in the cloud.** Check the device's website if it has information on how they store data and how collected data is being used.
- **Pick a device that has security software, from a known and trusted security provider, installed.** A smart device that works with a credible security provider means that it prioritizes your kid's security and privacy.
- **Check if there's an option for your kid's device not to store information in the cloud.** In case a privacy issue surrounding your kid's device is raised, having the choice to opt out of the data collection any time will help keep your kid safe online.

Best practices for using internet-connected devices for kids:

- **Discuss the importance of practicing online safety.** Help your kid understand the public nature of the internet and its potential dangers. Teach your kid how to behave responsibly online by telling them to be careful of sharing too much information about themselves.

- **Research on the smart device.** Check reviews made about the device. Also, learn more about the manufacturer’s history in handling user data.

- **Make use of parental controls and safe-search filters.** Such features on smart devices can help you manage what content your kid can see or access. But even with such features, parental supervision is still the best way to keep your kid safe online.

- **Set up appropriate security for the device.** Install security software, if available, on the smart device and make sure it is always updated.

- **Review the privacy settings of the connected device.** Check if there is an option to change the settings and delete information or files you do not want your kid’s device to collect. A “reset” option is also nice to have since it will let you wipe any, and even all, information that the device has on your kid.

Navigating today’s ever-changing digital world provides opportunities and challenges for parents and guardians. As more smart toys make their way into homes, the risks to a kid’s privacy have also increased. But despite all the risks and privacy considerations listed in this guide, parents shouldn’t worry too much about buying a smart device for their kid. By reading through this guide and learning about all the potential issues surrounding IoT devices, parents are armed with details that can guide them to make informed decisions in choosing the right smart device. And in doing so, parents can also help their kid explore the digital world in a safe and secure way.

For more information and tips on how to keep your kid safe online, visit:

http://www.trendmicro.com/us/home/internet-safety/

http://internetsafety.trendmicro.com/

Related data protection laws for kids and IoT:

*The **Children's Online Privacy Protection Act (COPPA)** is a United States federal law that encompasses all internet users younger than 13 years old. The law sets up rules regarding privacy policies that entail seeking permission from children's parents or guardians before collecting or giving out their personal data. Without parental consent, a child's geolocation data, photos, videos, and audio recordings cannot be collected. The **EU General Data Protection Regulation (GDPR)** is also expected to adopt similar requirements regarding parental consent for data collection and processing—with 16 years old as the consenting age. However, Member States are allowed to set a lower age not below 13 years.*

Glossary

Avatar	An icon or cartoon that represents a person online (e.g. in computer games, chat rooms, and online forums)
Biometrics	The measurement and analysis of the physical attributes and behavioral characteristics that can be used to distinguish a person (e.g. fingerprints, retina and iris patterns, and voice waves)
Cloud	Refers to the delivery of hosted services via the internet
Geotag	Geographical identification used to associate where a photo or video was taken
GPS (Global Positioning System)	A global navigation satellite system used to provide location and time information (e.g. in-car or hand-held device navigation)
Internet of things (IoT)	The system of connected computing devices, or smart devices, that communicates and interacts with each other
Parental controls	Tools that help parents protect their kid’s online activity (e.g. filtering websites that can be visited or from whom the child can receive a message)
Privacy settings	Tools provided by websites or devices that help maintain privacy online by limiting access to and sharing of information

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.