Global
Encryption
Coalition

A Parents Guide to Encryption

Encryption might seem like the stuff of spy movies, but we all rely on it to keep us safe. You might be surprised to learn how often it touches your life. In fact, you're using it right now.

How does encryption protect you and your loved ones?

Every time you type a password, scan your smartphone to pay for coffee, send your parents a photo of your kid scoring a goal, or use a fitness watch to track your personal best, encryption helps make sure nobody else can see that information.

When your data is encrypted, that means it's scrambled when it's on the move or when it's stored somewhere. This makes it more difficult for hackers to interfere with your financial life, steal your identity, or get photos you only meant for one person.

That's why it's so important to take a few simple steps to make sure your devices, apps, and services are actually using it.

You're seeing this website thanks to data that's being sent back and forth between your device, your browser, and a range of connections, servers, and computers. But because the website uses an encrypted tool called HTTPS, it makes it harder for anyone to know that you're reading up on how to use encryption.

PARENTS

Baby Monitor

Make sure those baby coos are just for you

The smartest home is an encrypted one. Learn how to choose safer baby monitors and connected home devices.

Baby monitors offer peace of mind and give you the chance to intervene quickly if your child has a health emergency or just needs comfort after a scary dream. They allow you to keep track of your baby's activity from another room or even outside the home.

But if your monitor is connected to the Internet, that "other room" could be almost anywhere, and you might not know who is in it.

When someone else can monitor your baby

Parents have been using baby monitors since the late 1930s. Even then, sometimes the radio signals would pick up nearby devices that use the same frequency. That's not a musical ghost, that's your tired neighbor singing Cocomelon songs for the 600th time at 2 am (if you know, you know).

Today's devices are more sophisticated, with high-quality video and audio, noise cancellation, and even a two-way microphone. Some can connect to your home WiFi, which means you can access them outside your house. So, when the babysitter calls to tell you they can't get your anxious kid to settle, you, too, can sing 600 crystal-clear versions of the "Yes Yes Vegetables Song," right from that date-night restaurant. But being connected to the Internet like this comes with an added risk. The emitting end is a microphone and camera inside your home, physically near your child. And it's probably on all the time.

It works by sending a signal sent over the Internet to a server from your phone. If that's not secure, it could mean someone malicious could also hear you sing "Good, good, peas are good for you." They could use this listening capability to collect your personal information, see how you move around your home, or put your baby at risk.

Should you even use a baby monitor? Maybe you shouldn't even go out to dinner. But wait! Don't cancel that table for two just yet.

Here's why you don't need to panic
Connected home devices aren't inherently dangerous, but it's important to know some ways to prevent unwanted eavesdropping. Even if your communications are flowing through the manufacturers' servers, they shouldn't be able to watch or listen to what's actually happening or see the actual data you're sending.

But to make sure of this, it's important to choose a model of baby monitor or connected home device that has end-to-end encryption technology. This protects the connection and keeps the signal—and your Cocomelon tunes—just between you and your baby (and the rest of the restaurant). And maybe when you get home, your baby will have discovered Bluey instead.

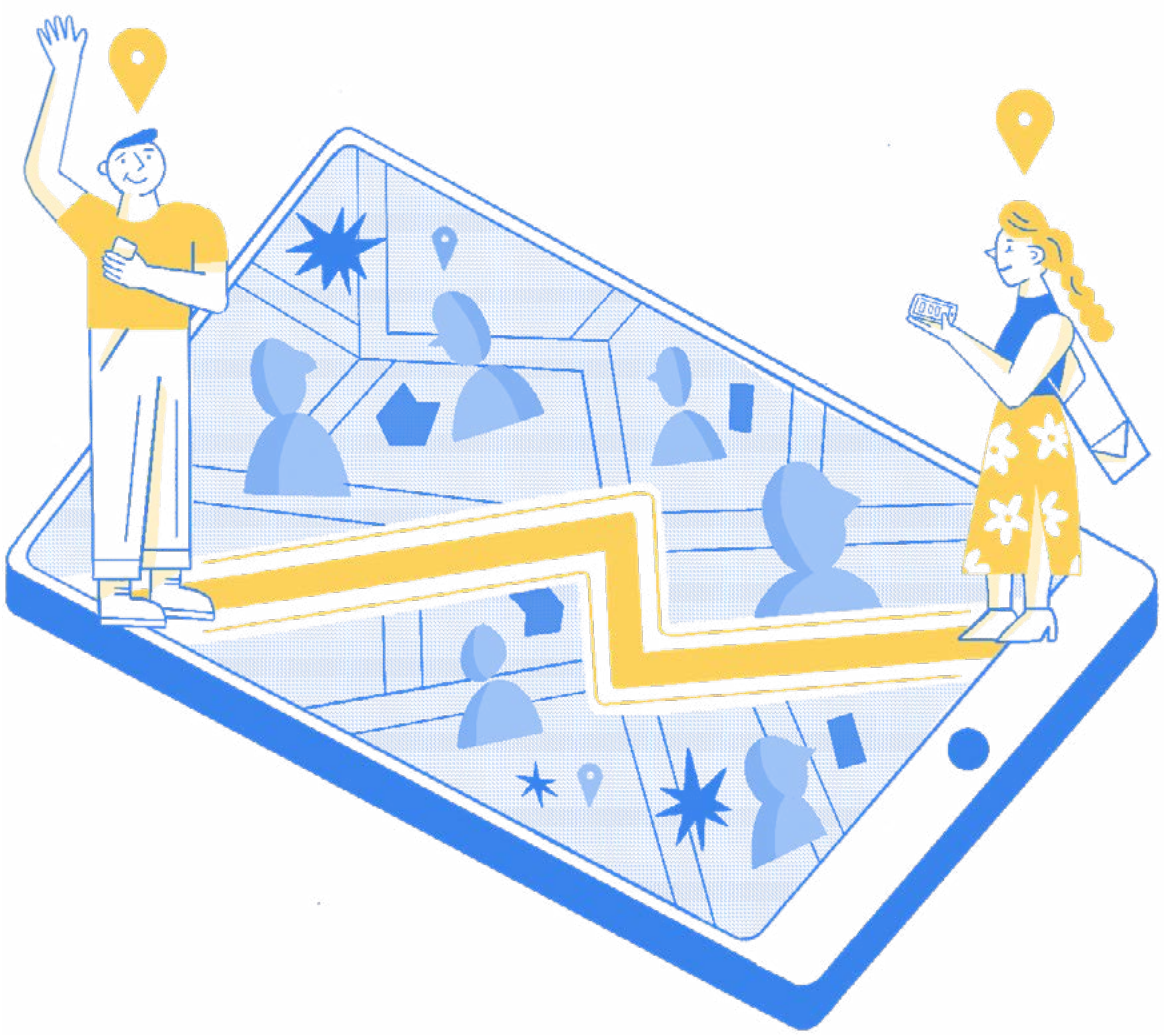
What we recommend

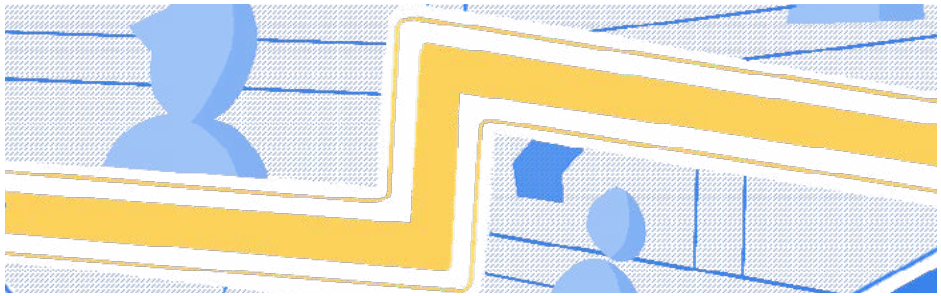
1. Choose devices that offer encryption, preferably end-to-end. Take a few minutes to review specifications in detail. If you're buying one in a physical store, ask a specialist if you can't find the technical details.
2. If the device has something called a "smart assistant," it's probably activated through a "wake" word. It's always listening for that word, which means it can be "woken up" by accident and start listening for commands. It's not usually possible to know where those voice communications are going or how they'll be stored. Turn off the voice assistant when you're not in immediate need of it. (The same goes for voice assistants like Siri and Google Home on mobile devices.)
3. Periodically check devices like Amazon Echo, Siri, or Google Home, and delete any recordings.
4. If you don't need it, consider disabling remote access.
5. Change the default password.

PARENTS

Location Sharing

Make sure nobody else can hear your pin drop





Sharing your location is a convenient way to keep kids and teens safe. Find out how to make sure you're not sharing it with the wrong people.

By the time kids are tweens or teens, you might wish they'd say more than three words to you, online or off. But mostly, you hope they really are sleeping over at that friend's house.

Location sharing is a useful way to help young people exercise their growing autonomy without cramping their style. They still want you to pick them up, just...around the corner.

But who else are they sharing their location with?

When sharing your rendezvous isn't a secret

More than anything (except unlimited data), young people want to go to parties and hang out with their friends without you hovering over them. It used to be that you'd have to hassle them for an address or get their friend's parents to give you directions. But thanks to location-sharing capabilities in your phones, they can just drop a pin, and you'll be able to find them.

They can even use location sharing with one another. We all remember—or were—the friend who storms off from a gathering and regrets it soon after. Dropping a pin helps them find each other again when all is forgiven and forgotten. This function is also common among peer groups, especially women, to share their location when going on a date with someone new.

Your teen might use location tracking when tracking cross-country running routes, playing a location-based game, or posting on social media. Without you knowing it, some of these apps might be tracking locations, creating location histories, and saving them in logs.

If that data isn't encrypted, or if it's shared publicly, it can give away regular routes between home, school, work, or friends, or inadvertently show a person's location in a sensitive location. The last thing your teen wants is for the school bully to know about where they go every week.

Used wisely, location sharing can be helpful, convenient, and safe. That's why it's important to have some tactics to prevent exposing information to malicious actors or predators.

Here's why you don't need to panic

When it comes to sharing your location, users often have quite a lot of control. You can often switch off location sharing for most of your services or use it only when the app is in use. Choosing encrypted services means only the people you want to see your location can find out where you are or where you've been.

You can still share your location, find your friends, pick up your kid, or go for an extra-long run—just directly with the people and groups you choose.

What we recommend

1. Use encrypted services that allow you to share your location safely.

2. Turn off any location-sharing features on apps that you use. Some social networks have apps that post your location publicly, but you can usually deactivate it in the settings.

3. Some fitness apps have a "private" mode, so you can still track your routes and compete with friends, but only with those you choose.

4. 4. Be mindful when "dropping a pin". Only send it to the person or group of people that should receive it.

5. You can usually select an amount of time that you want to share your location—an hour, all day, forever. Choose the smallest unit of time that's reasonable in case you forget to turn it off.

PARENTS

Instant Messaging Apps

Who’s really in your group chat?

Instant messaging is essential for many modern families. Learn how to keep your family business away from snoops and attackers.

We're so used to instant messaging that it's become natural to drop a link, a photo, a comment, or a voice note—we all have that one friend—into a chat thread.

Many of us use instant messaging services to stay in constant contact with friends and loved ones all over the world. We use it to plan playdates, parties, meetings, and weddings, and order pizza, taxis, or groceries.

But even if you're not listening to those voice notes, someone else might be.

Several people are typing...but who's reading?

Instant messaging was originally part of chat rooms and similar services and ran only on desktop computers. Even the first social media services offered only a private mailbox.

But now instant messaging is embedded in phones, gaming consoles, social media, and even movie streaming services. You can order services, get take-out, check your bank balance, and even do talk therapy over messaging apps.

Our days are full of pings, bings, and vibrating devices, bringing updates and mandates from home, school, friends, and workplaces. But how private are your private messages?

Imagine someone could see into your family group chat. They might know your friend in Australia is getting married, and your friend in Vienna is getting divorced. They could learn to identify your house from photos, know your kids' pet names for each other, learn what they like on their pizza, and see that your tween needs constant reminding that it's winter—put a coat on.

Now imagine how easy it would be for someone to use that information to convince your kid they're a family friend or a long-lost cousin, and what danger that could pose. But don't delete all your messaging apps just yet. That group chat is your legacy, and it's possible to keep it safer.

In services that aren't secure, like those that don't encrypt your information, your messages can be scanned. Sometimes it's to do things like create a profile, so you can be targeted with ads. In other cases, that insecure connection could be used by attackers. They can monitor your conversations and even obtain information about your children.

Here's why you don't need to panic

It's easy to assume that all instant messaging services are the same, but some really are safer than others. You can choose the ones that offer end-to-end encryption, which means that your photos, videos, and conversations stay private. That voice note you're never going to listen to? Nobody else can hear it, either. Not even the company providing the service.

Encryption means your friend in Perth can send a wall of text about wedding plans, and your friend can send a divorce trauma dump from Austria, and only that guy looking over your shoulder on the bus can see it (you can get a screen cover for that, too).

What we recommend

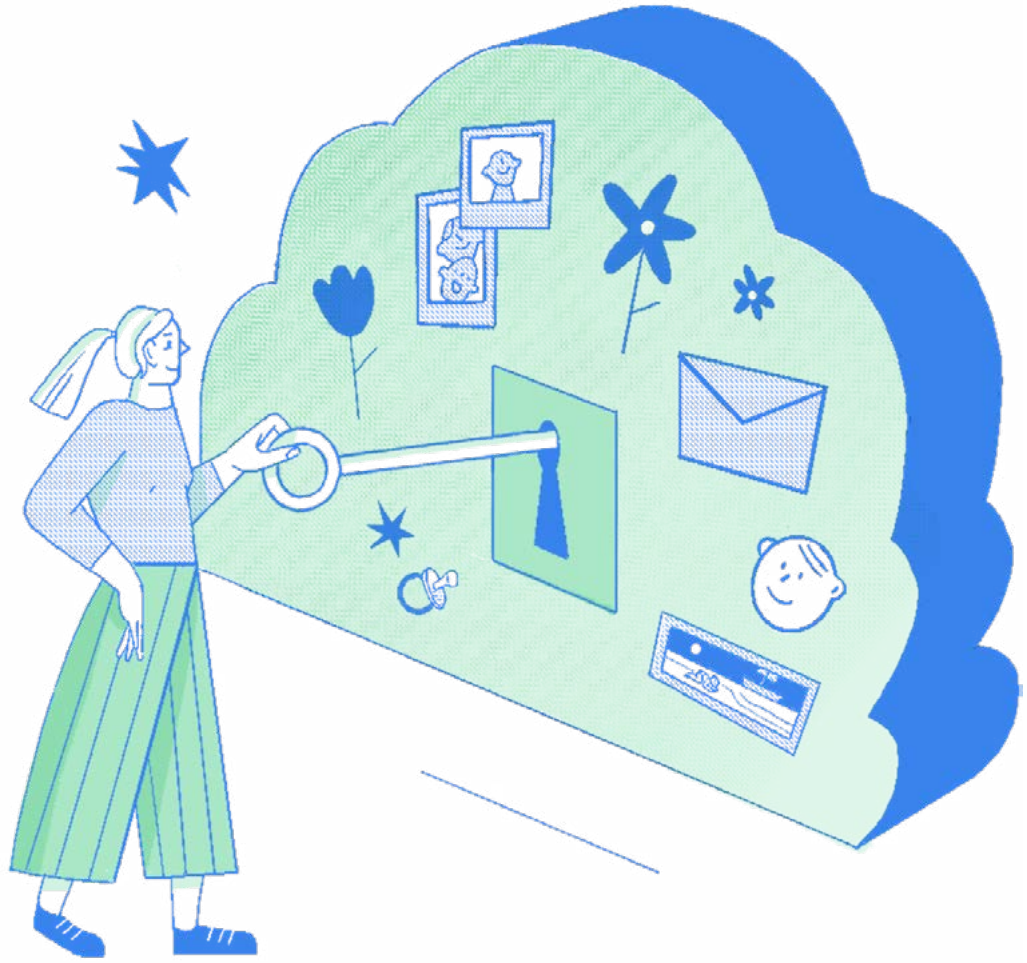
1. Find out if the instant message services your family uses offer end-to-end encryption. If it's not activated by default, make sure you turn it on.

2. Choose encrypted messaging services, so you can chat safely with everyone, even that friend who uses voice notes.

PARENTS

Cloud Storage

Whose head (and eyes) are in your cloud?



Storing data in the cloud means you can keep every precious memory. Find out how to keep those photos and videos more secure.

You probably have thousands (or tens of thousands) of photos and videos of kids, pets, and family members. We take pictures of memorable meals, home decor, and social occasions.

And now, thanks to cloud storage, you can keep every video of your kids on Halloween, and every photo of your dog looking extra snuggly.

But is anyone keeping that storage space safe from prying eyes—or something worse?

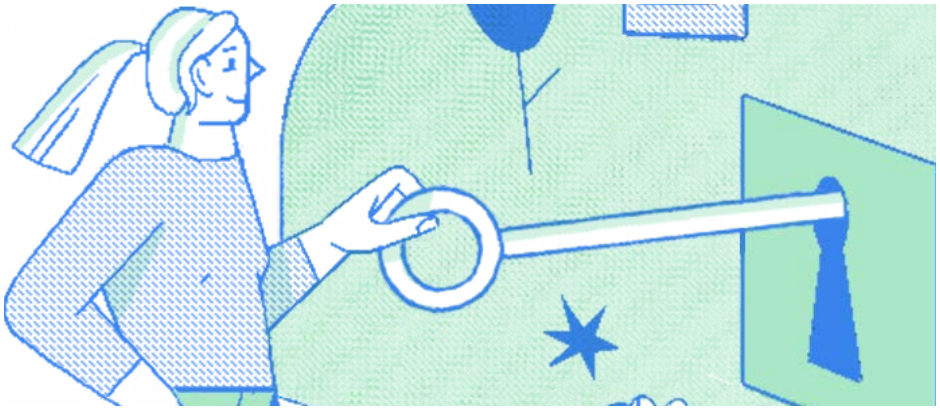
The cloud is (sort of) someone else's computer

The cameras in our mobile devices have evolved so much that they're often far better than any standalone camera we'd ever own. That camera quality is a chance for us to turn more moments than ever into high-definition memories. All those photos need to be stored somewhere, and many of us back up into cloud storage, sometimes daily.

You've probably heard the saying, "The cloud is someone else's computer." Even though that's wildly oversimplified, your data is indeed stored somewhere else, using software and hardware controlled by someone you don't know personally. So, it's a good chance to stop and ask ourselves who we would trust with our sonograms, birth videos, first birthday cake smash, or miraculously fluffy dog.

If you aren't using an encrypted service for your cloud storage, bad actors can access those images. Sure, more people really should see how cute your dog is, but you don't want any of your photos or videos to be shared beyond the circles that have permission to see them.

And you definitely don't want photos of your children to fall into the hands of truly malicious people. Those photos could be used to create other images, train AI models for purposes you didn't agree to, or shared for much worse purposes.



Here's why you don't need to panic

You don't need any more anxiety about your kids' safety, so don't worry. This can be easily prevented. Your cloud storage service might be using encryption already.

If they protect stored data (that is, data that's "at rest" in those online hard drives), it doesn't even matter if other security measures fail and someone downloads the content. The photos of your dog, the Halloween videos, and the "before" pics of your house renovation would just be a bunch of scrambled code. They wouldn't be able to use it for anything.

What we recommend

1. Check the settings and features in your cloud storage. If it offers encryption, but it's not active by default, turn it on.

2. If you haven't chosen a service yet, take your time to find the right one—the resources in this guide can help.

3. If it turns out your cloud service doesn't offer encryption, consider changing to one that does. Yes, it's painful to move your things, but you really will be safer.

4. When sharing links to pictures or files, check the settings so they're only shared with the intended recipient and they can only see the content you choose.

CHILDREN

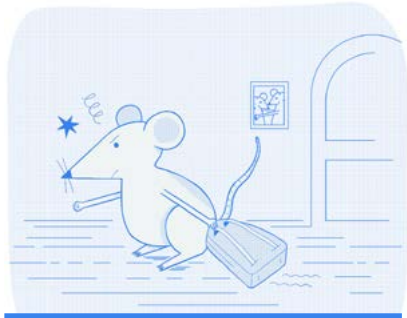
Talking to your kids about encryption

You already talk to your kids about safety and privacy. So you know it's vital to do it in a way that helps them grasp the urgency without scaring them or making them feel they can't do anything fun. Our comics can help you kick off that conversation.

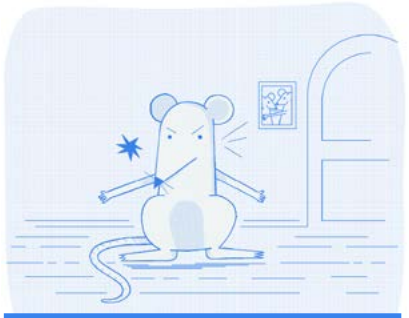
CHILDREN

Monty´s Bad Privacy

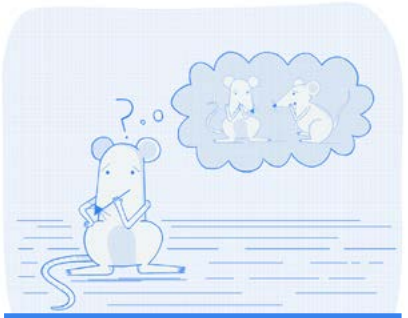
When Monty gets home from school, he is usually in a good mood. Not today.



What's up, Monty?



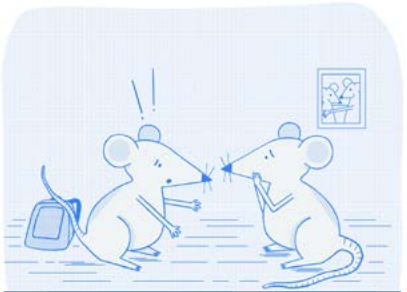
You told your best friend your biggest secret, and they told everyone else? How do you feel about them now?



Did you talk to your friend about how it made you feel? No?

Maybe that would be a good thing to do. After all, they've been your best friend for a long time...

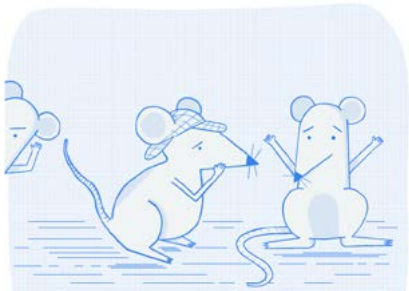
The next day, at school, Monty tells Laura he's not happy about what happened.



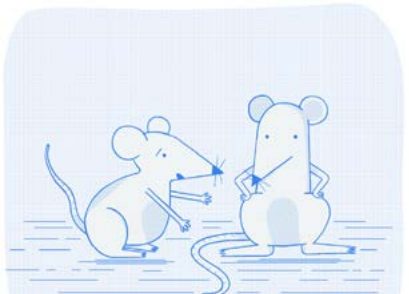
But Laura promises she didn't tell a single person..

The mystery is—who told Monty's secret?

Monty asks around...



"I heard it from Nico!" says Bella. "Nico was listening to your conversation with Laura."



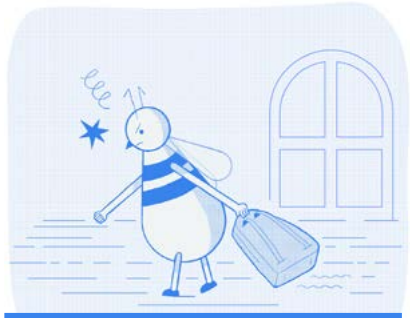
"I'm sorry, Laura," says Monty, "I should have trusted you—I know you're my best friend."

"I don't like other people listening to our conversations. Here's a code we can use for private messages."

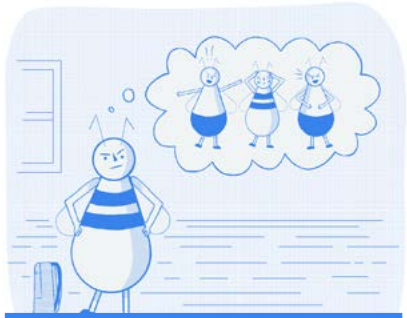
CHILDREN

Tico´s Bad Privacy

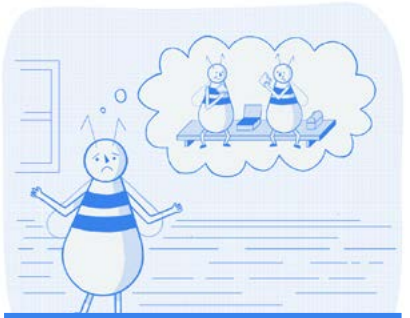
Hey, Tico, what's up? You don't look your usual, cheerful self.



"People were saying stupid things at school."



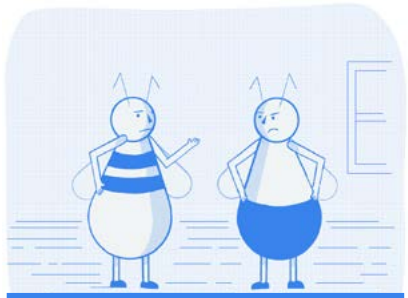
"They were making up stuff about me and my friend Minty."



"Minty and I agreed to go to the park on the weekend and have a picnic. Minty's my best friend."

"But the others found out about it, and they were singing that stupid song about 'sitting in a tree, K.I.S.S.I.N.G.' It was really embarrassing."

The next day, Tico speaks to the kids who were teasing him.



"You shouldn't have listened in when Minty and I were talking. That was private. And you shouldn't make up stuff that isn't true."

Tico and Minty agree to use a secret code to keep their conversations private.

FAMILY ACTIVITY

Do an Encryption Audit

Many companies that make devices and services have put a lot of effort into making security and encryption easy to use. But it's important to make sure it's activated and that devices are kept up-to-date. One smart way to get on top of things is to gather the family and run a household encryption audit.

You'll need 2-3 hours in total, so divide the missions by family attention span.

Mission 1

Smart Device Scramble

Find all the connected things

You probably have more connected devices than you realize, even if you're not the sort of family that gets emails from the "smart" refrigerator.

The first step is to find them all. Divide your home into zones and send everyone out to find anything that seems like it might be connected to the Internet. If something is too big to carry, get a photo of the brand and model. If you have little kids, get them to bring you any toys and devices that make sounds or move. You can look together to see which ones are smart/connected.

Create a catalog

Make a list of everything that connects to the Internet. Include names, types of devices, and the model.

Then, go online and find their user manuals to find out what specifications they use. Also, see if there's a help center for the device. You should be able to learn if they use encryption.

Whether or not they're using encryption, the first thing you should ask is: do we need this device to be connected to the Internet? Some of these things offer plenty of functionality in offline mode. You might want to connect to the Internet only when you need to update the firmware or other settings.

For encrypted devices:

- What type of encryption does it use?
- Is your firmware up to date?

For devices that aren't encrypted:

- Is there some type of encryption we can enable for it?
- Can we replace this device with one that does offer encryption?
- Have you changed the default password?

Mission 2

Find the Messengers

Collect your channels

There are user-to-user messaging services built into more devices and services than you probably think. Some are essential—imagine playing Among Us without chatting—but others are either less useful or might even pose a risk.

Every family member will list their apps, games, platforms, and other services. Smaller kids might be using games you don't know much about. Those might have messengers or inboxes you weren't aware of, so get them to add theirs, too.

Make your list

Have everyone write down everything that uses a messenger service and note whose device(s) each is on.

For each one, list whether or not they use encryption. If it's offered, but it's not on by default, it should be possible to turn it on. If you're not sure, find information online, either in the company's help center or in user forums.

With each service, start with the question: do I really need to use this? Can I chat with these same people on another platform?

Messengers are perfectly safe, but more channels for chatting with others means more potential points of entry for malicious people, even if the service is encrypted.

For encrypted messaging services:

- Can you tell what type of encryption it uses?
- Are you using the latest version of the app?
- Do you need to use this service?

For messaging services that aren't encrypted:

- Is it possible to turn on some type of encryption?
- Is the messaging feature in this service essential?
- Can you chat with these same people using an encrypted service instead?

Mission 3

Update and Delete

Spruce up your home screens

Everyone grabs their mobile devices—phones, tablets, watches, hand-held gaming consoles—and goes through all the apps.

Start your updates

Go into the Play or App Store and download every update that's offered. If you need to update the operating system, do that, too. These updates often include essential security features, patches, and upgrades.

As you're doing that, stop and think about apps you're not using, and have no intention of using again. Consider deleting them, and maybe even delete the account associated with it. There's a need for a company to have your data if they don't need to.

For encrypted services:

- Can you tell what type of encryption it uses?
- Do you need to use this service?

For apps that aren't encrypted:

- Is it possible to turn on some type of encryption?
- Can you delete both your user account and the app?

Mission 4

Cover Your Tracks

Locate the location trackers

Now that you've pruned your home screens, make a list of all the apps that are left. Add columns for who is using them and on which device(s). Then go online and use your favorite (HTTPS!) search engine to find out which of these apps is sharing your location. Is it encrypting that data? Most will offer a tutorial or an easy guide to turn that off. So, do that.

It's also good to go into your device settings and see what your device is sharing about your location, maybe without you knowing. Some of it is fairly general, like your weather app, but others could be way more specific than you realize.

For encrypted services:

- Can you turn off location tracking entirely?
- Can you turn it on selectively?.

If location services are not encrypted:

- Can I turn the tracking on and off?
- Can I replace this app with one that’s encrypted?
- If I can’t limit location tracking, can I re-download it when I need to use it?

Enjoy Your New Level of Protection.

You're done!

It's time to relax (a little). After all, encryption isn't perfect. Teens and kids will still keep us up at night worrying. Cocomelon songs will live in your head forever. And that one friend will keep leaving voice notes.

It's good to do an audit like this every few months, but even once a year will make a difference. Over time, your whole family will develop better habits: choosing encrypted services, adjusting location tracking, and keeping apps and devices up to date. Even kids can learn to do it. They might even tell their friends.

You can tell your friends, too. Share this guide on social media, drop it into your group chat, or kickstart a local campaign with our campaign-in-a-box toolkit.

Get the Campaign Toolkit

Recommended Reading and Resources

Keep Your Data Secure With a Personalized Plan

Mapping Online Child Safety in Asia-Pacific

When You Should (and Shouldn't) Share Your Location Using a Smartphone

Location history: How your location is tracked and how you can limit sharing it

Privacy and Protection: A children's rights approach to encryption

How to Secure Your Kid's Android Device

Make smart choices to protect your privacy. Search for products. Read expert reviews. Get tips and tricks.

Keep it secure

Chat control: 10 principles to defend children in the digital age

Global Encryption Coalition

The Global Encryption Coalition promotes and defends encryption in key countries and multilateral fora where it is under threat. It also supports efforts by companies to offer encrypted services to their users.