# Digital Schoolbag: A Parent's Guide for the School Year

kaspersky

## Why cybersecurity matters this school year

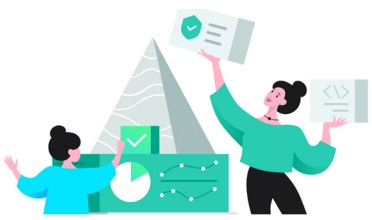
As children gear up for the new school year with sharpened pencils and fresh notebooks, there's one essential tool that often goes overlooked — cybersecurity. In an age where education is increasingly digital, students rely on laptops, tablets, messaging apps, and online learning platforms more than ever before. But along with the convenience of connected learning comes a growing range of online threats — from phishing, scams and data breaches to cyberbullying and identity theft.

For parents, this means cybersecurity is no longer optional — it's a vital part of back-to-school preparation. Just as you teach your child to safely cross the street or pack a healthy lunch, you also need to equip them with the tools and knowledge to navigate the online world with confidence and caution.

In this guide, we'll walk you through the key cybersecurity risks your child may face this school year — and how you can help prevent them. From setting up strong passwords and parental controls to identifying scams and talking about online behavior, Digital Schoolbag is here to help you stay one step ahead and ensure your child's digital safety.







# Online world

Today's students are more connected than ever, chatting with friends on messaging apps, joining class forums, using AI tools to complete assignments, and exploring the vast world of the internet for school and fun. But alongside the learning opportunities lie real risks. The online world, while exciting and full of potential, can also be a place where children are exposed to harmful content, fall victim to scams, or become targets of cyberbullying.

It's not just about screen time anymore, it's about what happens during that screen time. Children may unknowingly download malware disguised as educational tools, engage with strangers pretending to be peers, or overshare personal information that can be exploited. Even platforms designed for learning and collaboration aren't immune to threats.

Understanding these dangers is the first step toward protecting your child. In this section, we'll explore the most common online threats facing school-aged kids today from phishing and fake apps to social engineering and inappropriate content and explain how they work, why kids are vulnerable, and what you can do to help them stay safe.

# Safe searching

Search engines don't always distinguish between age-appropriate and adult content. That's why children need both technical safeguards and critical thinking skills to navigate the digital world confidently. When safe searching habits are built early, kids not only avoid online risks — they also become more thoughtful, curious, and independent learners.

## 1. Use content filters and parental control tools

Start by enabling parental controls on all devices your child uses — smartphones, tablets, computers, and smart TVs. Most operating systems (like iOS, Android, Windows, and macOS) offer built-in features that allow you to block explicit websites, restrict certain types of apps, and filter search results. Additionally, platforms like YouTube, Netflix, and TikTok allow you to activate "restricted" or "kids" modes, which limit access to mature content.  For even more control, consider using tools like Kaspersky Safe Kids, which offer real-time content filtering, screen time management, and app monitoring. This tool helps catch inappropriate content that might slip through standard filters, especially in browsers.

## 2. Turn off autoplay features

Autoplay is one of the main ways children unintentionally encounter inappropriate content. On platforms like YouTube or Netflix, one video can lead to another — and before you know it, your child is watching something far outside their age range. Disable autoplay where possible, both in settings and through browser extensions if needed. When autoplay is turned off, your child has to make a conscious choice to click the next video. This slows down content consumption, gives you a better chance to intervene, and encourages more mindful viewing habits overall.

## 3. Teach your child what to do when they see something wrong

No filter is perfect. That's why it's essential to empower your child to act when something doesn't feel right. Teach them the 3-step response: **Stop – Close the content – Tell an adult.** Let them know they won't be punished for telling you — even if they clicked something by mistake or got curious. Praise honesty and openness. You can even agree on a "digital safe word" your child can say when they've seen something they're not comfortable talking about right away.

## 4. Watch and talk together

The most effective filter isn't a piece of software — it's **you**. Make time to occasionally watch shows, play games, or browse content together. This not only helps you monitor what your child sees, but also gives you opportunities to talk about values, feelings, and real-life scenarios. Learn more about what kids search online in our latest Kids' interests report.

## 5. Check device history — and keep it open

Keep browser history, YouTube watch history, and app usage logs enabled. Don't treat this as spying, but as a shared responsibility. Most importantly, if you discover something you don't like, don't immediately start a scandal and scold the child. Try taking a break and figuring out why it happened.  The child may have heard a new word and decided to learn more about it. Over time, as your child grows older, consistently makes safe choices online, and can confidently explain why certain content is safe or unsafe, you can gradually reduce these checks. The goal is to help them build strong digital habits so that monitoring becomes unnecessary — replaced by trust, open communication, and their own ability to navigate online risks.

# Phishing and malicious links

Phishing is one of the most common cyberthreats children face online. It usually involves a fake message, website, or ad that tricks users into clicking a malicious link, entering personal data, or downloading harmful software. Because phishing often looks "normal" — like a prize notification, a homework file, or a game offer — children are especially vulnerable.

## 1. Teach the golden rule: "Don't click what you don't trust"

Children often click quickly, especially when they're excited about a message like "You won a prize!" or "Free skins for Roblox!" Explain that cybercriminals often pretend to be someone or something familiar to trick people — just like in real-life scams.

Give examples: fake messages from "teachers" asking for login info, pop-ups claiming their device is infected, or ads offering "free V-Bucks." Encourage them to pause and ask themselves: **Do I know this person? Does it seem too good to be true?** If yes — don't click. Always ask an adult first.

## 2. Show them what phishing looks like (safely)

Rather than simply warning them, show real examples (or safe mockups) of phishing emails, fake login pages, or scam pop-ups. Point out telltale signs:
– spelling errors
– strange URLs
– urgent tone ("You must act now!")
– requests for passwords or payment

Doing a "spot the scam" exercise together builds their visual awareness and teaches them what to avoid, just like recognizing a stranger in real life.

## 3. Use strong spam filters and safe browsing settings

Set up your child's email and browser with strong spam filters and phishing protection. Install a trusted security solution such as Kaspersky Premium that offers real-time protection against phishing attempts, malicious ads, and dangerous downloads. These tools often block harmful pages before your child can even see them.

## 4. Keep apps and systems up to date

Many phishing attacks exploit security holes in outdated browsers, apps, or operating systems. Make sure automatic updates are turned on — for your child's devices, email apps, and browsers. This helps patch vulnerabilities before attackers can take advantage of them.

## 5. Teach safe download habits

Phishing often comes in the form of malicious file downloads — especially in education and gaming contexts. For example:
– A "homework file" sent through Discord
– A "mod" for Minecraft from a random site
– A PDF from a stranger on WhatsApp

Explain that they should only download files from trusted sources — like teachers, official websites, or verified app stores. Make a rule: if they're unsure, they must ask an adult before downloading anything.

## 6. Protect payment and app store accounts

Many scams trick children into accidentally spending real money — either by asking for credit card details "to claim a prize" or by triggering unwanted in-app purchases. Make sure all app stores and payment tools require passwords, biometrics, or parental approval before any transaction. Also review which games and platforms have your payment information saved — and remove or limit it where possible.

## 7. Report and block suspicious messages and accounts

Show your child how to report fake ads, scam messages, or impersonation accounts on every platform they use. Whether it's TikTok, YouTube, Roblox, or Instagram — every major service has reporting tools. Encourage them to use them, even if the message "looks funny" or "probably isn't serious." Also teach them to block and never engage with users who send suspicious offers or links. Even replying "no thanks" can give scammers confirmation that the account is active and vulnerable.

# Oversharing

Children and teens today are growing up in a world where sharing is second nature — from posting selfies and videos to commenting on every moment of their lives. But what feels casual and fun to a child can become a serious privacy risk when sensitive information is revealed to the wrong audience.

Oversharing doesn't always look dangerous. Sometimes it's a birthday photo, a school uniform, a location tag, or a casual chat about weekend plans. But small details add up — and cybercriminals, bullies, or strangers can use that information to track, manipulate, or harm a child.

## 1. Set up accounts together — and review privacy settings regularly

Creating a social media or messaging account should always be a joint activity, especially for children under 16. Sit down with your child and walk through the sign-up process together. This helps you understand the platform, set expectations, and configure safety settings right from the start.

– Use a nickname or first name only. Avoid full names that can be linked to other personal data.
– Leave out birthdays, school names, and cities from bios and public profiles. This information can be used by strangers to locate or impersonate your child.
– Turn off location tagging in settings, and talk about never tagging current locations in posts (e.g. "At Central Park right now!").
– Restrict comments or messages to "friends only" or people you both know in real life.

## 2. Teach them what not to post

Kids often underestimate how much they're revealing in what feels like a casual post, story, or chat. Break it down into categories and explain **why** each is risky — not just "because I said so," but because it can be misused, misunderstood, or manipulated.

**Personal Information**

Never post or message:
– Full name
– Home address or street name
– Phone number, email, or parents' contacts
– School name, classroom number, or bus route
– Student ID, grades, test scores, or passwords

This info can be used to guess security answers, find your home, or pretend to be your child online.

**Routine Details**

Avoid sharing:
– Where they are right now
– Where they go every day
– Upcoming travel plans

This can help strangers track your child's location patterns and know when they're alone or unprotected.

**Sensitive information**

Caution with photos/videos:
– In school uniform showing crests or badges
– From inside your home showing layout, valuables, or personal items
– In underwear, swimsuits, or pajamas, even if joking
– Of other children without their permission

Once shared, these can be copied, reshared, or used for bullying — and often without the child even knowing it happened.

## 3. Discuss digital footprints and long-term consequences

Even if a post disappears, the internet doesn't forget. Deleted photos can be screenshotted, copied, or archived. Future employers, schools, or sports teams may one day look at your child's online presence — or someone might try to embarrass them years later with an old post.

Frame it positively: **"You're building your digital reputation every day — try to make it something you're proud of."** Encourage them to share hobbies, accomplishments, art, or kind messages — things that reflect their values and personality in a healthy way.

# Blogging and streaming

More than 30% children say they aspire to become social media creators, with studies showing that around 32% of 12–15-year-olds already name "YouTuber" as their dream job. For kids, digital creators become role models, and their desire to shine online emerges even before adolescence. In such a situation, parental involvement becomes not just helpful, but vital. When parents take an active role, by learning how platforms work, setting up privacy and security features together, and having open conversations about boundaries, this shared digital journey turns potential risks into teachable moments and empowers kids to explore their creativity with confidence.

## 1. Be curious, not critical. Your openness builds their safety net.

When a child says, "I want to start a blog" or "I want to be a YouTuber," it can trigger worry, especially when parents think of trolls, scammers, or oversharing. But the safest first step isn't shutting it down — it's opening up a dialogue. Ask your child why they want to blog and what they want to post. This approach does two important things: first, it shows you take their interests seriously, building trust. Second, it gives you a chance to introduce safety topics naturally, like privacy settings, content boundaries, and handling attention online.

To make those conversations easier and more engaging, start with age-appropriate resources. For example, the Kaspersky's Cybersecurity Alphabet — a free, downloadable book — helps children learn the basics of digital hygiene in a fun and simple way. It introduces key cybersecurity concepts through relatable language and colorful illustrations, making it easier for kids to understand how to spot scams, protect their data, and stay safe while exploring their creativity online.

## 2. Google their alias regularly

Once your child starts posting under a screen name, it's important to stay aware of how visible and searchable they are online. A simple way to do this is to Google their alias regularly. Search their username, blog title, or social media handle, and see what comes up. Are there personal photos, location tags, or comments that reveal more than they should? Has someone copied their content or tried to impersonate them?

## 3. Warn them about scam collabs or shady offers

As young bloggers start gaining visibility, they may begin receiving messages from supposed brands or accounts offering free products, sponsorships, or collaboration opportunities. To a child, this can feel like a dream come true, but in many cases, it's a scam. Teach your child to treat every unexpected offer with caution. Fake "collabs" often come via DMs or emails and may include links that lead to phishing sites designed to steal login credentials, personal data, or even bank information. Some scammers also ask for upfront "shipping fees" for fake gifts or try to trick kids into installing malicious apps.

Help them spot red flags, such as: poor grammar or urgent tone ("act now!"), requests for personal info or passwords, suspicious links or sketchy websites, unverified accounts pretending to be real brands.

For younger children, it's best if all business-related interactions — including reading DMs, evaluating brand offers, and responding to collaboration requests — are handled by parents. Discuss together what kind of brands are appropriate to work with, and explain why some offers may not be as harmless as they seem.

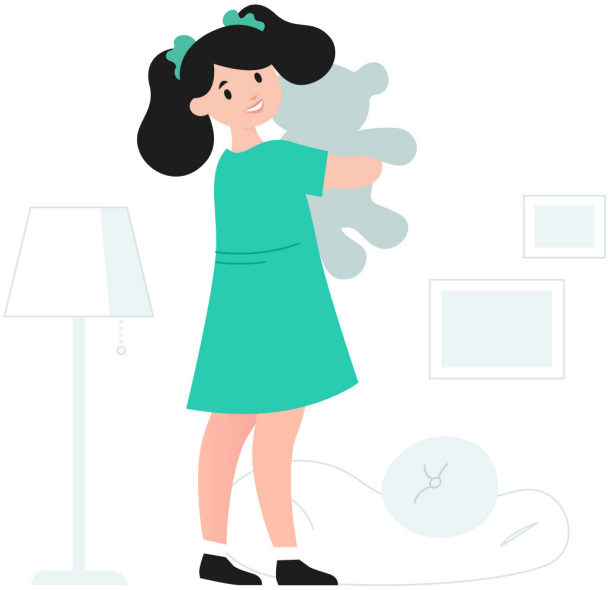
## 4. Talk about online strangers

As your child builds an audience, they may attract not only fans, but also people with inappropriate or manipulative behavior. Unfortunately, online grooming is a real threat, especially for young, open, and trusting creators who share details about their lives. Explain that not everyone who seems nice online has good intentions. Groomers often act like "supportive friends" — praising content, offering help, or pretending to have similar interests. Over time, they may ask for personal details, private photos, or try to move the conversation to less secure platforms (like private chats, video calls, or encrypted messengers).

Teach your child the warning signs:

- A stranger messaging them frequently or overly personally
- Someone who insists on secrecy ("don't tell your parents")
- Pressure to share private information or images
- Emotional manipulation — guilt, flattery, or threats

Most importantly, make sure they know: they can come to you without fear of punishment.



# AI and kids

Artificial intelligence is quickly becoming part of your child's digital world — from AI-powered chatbots and writing tools to smart toys, recommendation engines, and virtual tutors. According to Kaspersky's report, AI curiosity among kids more than doubled in 2025. While these technologies can support learning and creativity, they also raise important privacy, security, and ethical concerns. As a parent, you play a key role in guiding your child through this new reality.

## 1. Explain what AI is — and what it isn't

Children often think AI is "just a smart robot" or a friend who knows everything. Teach them that AI doesn't "think" or "feel", it generates responses based on data patterns, not emotions or intent. This is especially important for younger kids who might bond emotionally with AI avatars, chatbots, or "AI friends." Help them understand the limits: AI can be helpful for brainstorming or research, but it can also make mistakes, share biased content, or sound confident even when wrong. Encourage your child to double-check AI-generated info and never treat it as automatically true.

## 2. Talk about privacy when using AI tools

AI tools often collect large amounts of personal data — including what your child types, asks, or uploads. Make it clear that they should never share real names, school info, photos, or sensitive details with AI platforms, especially those connected to the internet. Review the privacy policies of any AI-based app or website they use. If data collection is unclear or excessive, avoid the tool altogether or find a child-safe alternative.

## 3. Set limits on unsupervised AI use

While it may seem like a safe activity, unsupervised AI use can expose children to harmful content or misinformation — especially through open-ended tools like ChatGPT, character bots, or AI art generators. Set clear rules:

- Ask permission before using new AI tools
- Use AI in shared spaces
- Avoid AI platforms that allow anonymous user interaction

Explain that some AI models are trained on the entire internet, including toxic or harmful material — so even innocent questions can sometimes trigger disturbing responses.

## 4. Encourage ethical use — no shortcuts

AI can be a tempting shortcut for homework, essays, or creative assignments. But relying on it too much can stunt critical thinking and creativity. Talk to your child about what's fair and what's cheating when using AI. A good rule: **"Use AI to support your thinking — not to replace it."** For example, it's okay to ask for ideas, definitions, or outlines — but not to copy entire answers or submit AI-written work as their own. This builds digital integrity from an early age.

## 5. Warn your child about downloading software from unofficial sources

Especially programs that claim to offer "exclusive" tools for schoolwork that promise to "instantly solve any homework problem." Cybercriminals often disguise malware as helpful study tools, using attractive names and fake educational branding to lure students into clicking suspicious links.

Explain to your child that downloading from unverified websites, file-sharing platforms, or random links in chat groups can compromise their device, steal personal data, or even lock them out of their accounts.

## 6. Watch for deepfakes and AI-generated deception

AI can now create hyper-realistic fake images, videos, or voices — known as deepfakes. Children may come across these on TikTok, YouTube, or in group chats without realizing they're fake.

Teach your child how to spot red flags:

- Strange eye movement or mismatched lips in videos
- Overly perfect or robotic-looking faces
- Emotional manipulation (e.g. fake news, celebrity scams)

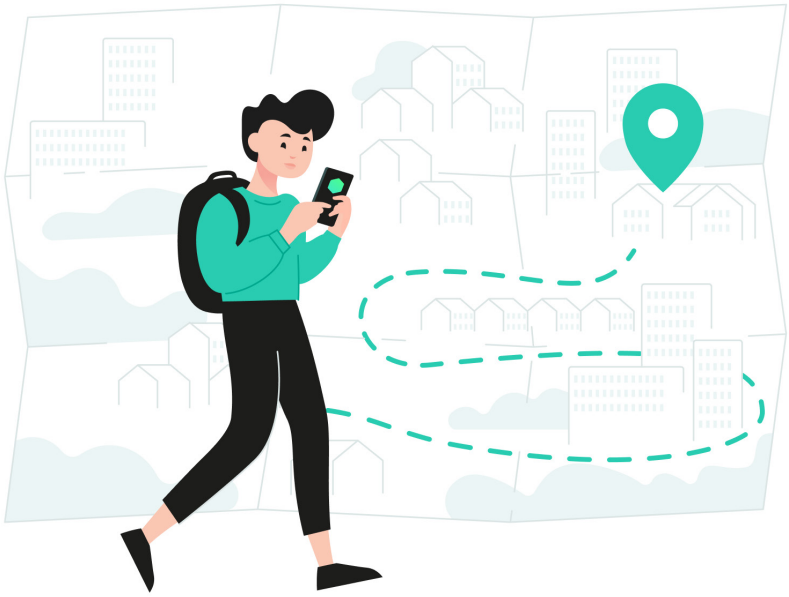
Encourage a healthy skepticism: **"Just because you see it doesn't mean it's real."** Show examples and debunk them together — turn it into a critical thinking exercise.

# Offline world

As the new school season begins, children often start spending more time on their own — walking to school, commuting on public transport, visiting after-school activities, or studying at the library. This growing independence is an exciting and important step: it helps them build confidence, develop decision-making skills, and learn how to navigate the world around them.

But as kids take on more responsibility, their exposure to real-world risks increases — and many of these risks have digital consequences. Cybersecurity isn't just something that happens online — it starts with everyday choices in the offline world. In this section, we'll explore how parents can help children build safe habits in public places, protect their digital lives on the move, and recognize that real-world awareness is just as important as screen-time rules.

From physical safety on the way to school, to smart use of public Wi-Fi, to keeping devices secure in their backpack — these lessons prepare kids to move through the world with confidence and caution.



# Physical security

While cybersecurity often focuses on apps, devices, and networks, real-world safety plays an equally important role in protecting your child. School-aged children are increasingly mobile — walking to school alone, riding public transportation, or spending time outside without adult supervision. These everyday moments carry digital implications, too: a lost device, overheard password, or unprotected smartwatch can open the door to online threats.

## 1. Teach safety rules for walking and commuting

Make sure your child knows basic street safety: always cross at designated crosswalks, follow traffic lights, walk on sidewalks, and never take shortcuts through alleys or unfamiliar areas. These rules may seem obvious, but children under 12 can easily become distracted — especially if they're wearing headphones or looking at a screen while walking.

Explain the importance of staying alert and device-free when near roads or in public. Model the same behavior yourself: put your phone away at intersections, look both ways, and remove headphones when walking with your child. When kids see adults practicing safe habits, they're more likely to copy them.

## 2. Use GPS tracking and check-in systems

Consider using GPS-enabled security tools like Kaspersky Safe Kids to monitor your child's route in real time. Many apps allow you to set up geofencing alerts — you'll get a notification if your child leaves a designated area or takes an unexpected detour.

This isn't about spying — it's about peace of mind. Be transparent: explain to your child why the tool is in place and agree on regular check-ins by call or message. Teach them how to contact you quickly in emergencies, and rehearse what to do if they feel unsafe on the way.

For parents, it's equally important to secure the tracking account: enable two-factor authentication, use a strong unique password, and review logged-in devices regularly to ensure location data stays private.

## 3. Secure devices carried outside the home

Children often carry smartphones, smartwatches, tablets, or laptops with them. These are high-value targets for theft and data exposure. Teach your child to keep devices zipped up and out of sight when not in use, and never leave them unattended — even "just for a second." Set up device lock codes, enable remote wipe features (like "Find My iPhone" or "Find My Device"), and back up schoolwork to the cloud. That way, even if a device is lost or stolen, information stays protected.

## 4. Be careful with public Wi-Fi

Public Wi-Fi networks — at schools, cafés, airports, or on public transportation — may seem convenient, but they often come with serious security risks. These networks are rarely encrypted, which means cybercriminals can intercept the data your child sends and receives, including login details, messages, and even photos.

Teach your child a simple rule: never log into personal accounts (like email, banking, or cloud storage) over public Wi-Fi unless they're using a trusted VPN. A VPN encrypts the data being transferred, making it much harder for outsiders to spy on it.

## 5. Set up alerts for suspicious logins or activity

Enable **login alerts** so you're notified if their account is accessed from an unusual location or device. These alerts can help detect if someone has gained access to their credentials through an insecure Wi-Fi session. Encourage your child to report anything unusual — like being logged out unexpectedly or seeing strange pop-ups — even if they're not sure what happened. Better safe than sorry.

## 6. Practice safe conversations in public

Remind your child not to talk loudly about personal information (like home address, passwords, or travel plans) in public places. If they're on a phone or messaging app, make sure they're not sharing private details where others can easily overhear or glance at their screen. This is especially important when kids are traveling alone on buses, in malls, or at after-school activities. Digital privacy begins with awareness of surroundings.

## 7. Plan for emergencies — and rehearse the steps

Equip your child with emergency contact information and make sure they know how to act in a crisis. Who should they call? Where should they go if they feel unsafe or get lost? Role-play simple scenarios: lost phone, locked out, missed bus, or seeing suspicious behavior. Practice calm response routines, not panic. The goal is to build confidence and preparation — not fear.

# Financial security

As children gain more independence, their financial habits often start forming alongside their digital habits. From buying lunch to making in-game purchases, kids today manage real money through apps, cards, and online platforms — often before they fully understand the risks involved.

## 1. Set clear spending limits

Start by establishing a basic budget structure for your child's typical expenses:
– School supplies
– Food or lunch money
– Sports or hobby-related purchases
– Entertainment (apps, games, subscriptions)

Rather than micromanaging every purchase, talk about percentages. For example: "70% for school-related spending, 20% for entertainment, 10% for saving." Use this opportunity to introduce digital money literacy: explain how in-app purchases, microtransactions, or hidden fees can drain their balance if they're not careful.

## 2. Use secure payment methods

Instead of giving your child cash (which can be lost or stolen), opt for child-friendly bank cards or digital wallets with parental controls. Many banking apps offer features like:
– Spending limits
– Purchase notifications
– Real-time transaction history
– Blocking certain categories (e.g., games, online marketplaces)

In parallel, install a cybersecurity solution that includes safe browsing and secure payment protection. This ensures that when your child shops online (for school materials, games, or subscriptions), their banking data is encrypted and protected from keyloggers, fake checkout pages, and man-in-the-middle attacks.

## 3. Secure Devices and Financial Accounts

Children may not fully understand the importance of account security — but one weak password or stolen device can expose all their financial tools. As a parent, you can help by:
– Enabling two-factor authentication (2FA) for every app that involves money
– Using a password manager, which stores credentials securely and allows family access if something goes wrong
– Teaching the basics of strong passwords: at least 12 characters, avoid names or birthdays, no reusing across platforms

## 4. Discuss cyberthreats that target young users

Kids may think scams only happen to adults — but in reality, cybercriminals often target children and teens, who are more trusting and less experienced.

Explain the common forms of financial scams:
– Phishing emails pretending to be from their bank or favorite store
– Fake giveaways asking for card info
– "Friend in need" scams where someone asks for money through a hacked account
– In-game scams offering "free" items in exchange for login details

Teach them to be skeptical of links, offers, and DMs that create a sense of urgency ("Do this now or lose your account!"). Encourage them to check with you before entering payment details anywhere online.

## 5. Keep track of subscriptions and recurring charges

Many apps and platforms — especially games, learning tools, and streaming services — now use subscription models instead of one-time purchases. It's easy for kids to sign up for a "free trial" that later turns into monthly charges without them noticing.

Teach your child to:
– Always ask before starting a free trial
– Look for "auto-renew" settings and learn how to cancel them
– Set calendar reminders for trial end dates

As a parent, review app store purchase history monthly, and regularly check email for hidden renewal notifications. You can also use tools that flag recurring charges or send alerts for every transaction.

## 6. Watch for identity theft warning signs

If your child's personal or financial information has been exposed, you might notice:
– Unexpected purchases
– Account lockouts or password reset emails
– Strange notifications from platforms they don't use

Use monitoring tools or credit alerts (where available) to flag suspicious activity early. Teach older kids to recognize these red flags and report them immediately — not just ignore them out of fear.

# IoT and smart devices

Smart speakers, interactive toys, smartwatches, home assistants, learning tablets — the Internet of Things (IoT) is quickly becoming part of everyday life for children. These devices make learning more interactive, entertainment more immersive, and everyday tasks more convenient. But they also introduce new privacy and cybersecurity risks that many families overlook. Unlike traditional screens, IoT devices are always on, always connected, and often listening — creating a unique need for ongoing digital awareness and control.

## 1. Supervise usage and choose secure devices

At the beginning, it's essential to monitor how your child interacts with smart devices. Whether it's a voice assistant, a smart toy, or a connected learning tablet, stay involved in how it's being used and what features are enabled.

**When choosing a device, look for:**
– Built-in parental controls
– Privacy-focused settings
– Clear user data policies
– Ability to mute microphones or disable listening when not in use
– Manual approval of new features, apps, or contacts

Where possible, place smart devices in common areas like the kitchen or living room — not in bedrooms — and consider limiting usage when unsupervised.

## 2. Teach core safety rules for smart interactions

Children may anthropomorphize voice assistants or smart toys and begin talking to them like trusted friends. That's why it's crucial to teach them the boundaries of safe communication, especially when the device is connected to the internet.

Teach your child:
– Never share full names, phone numbers, addresses, or school details
– Don't talk about family routines, passwords, or personal problems
– Voice assistants may "seem nice," but they are not people, and not private

Practice together by role-playing "what's okay and what's not" to say aloud. Explain how some smart toys record interactions to improve performance — and why it's important to treat them like digital strangers.

## 3. Adjust privacy settings and disable unnecessary features

Many smart devices come with default settings that favor convenience over security. As a parent, take time to review the settings carefully.

Key actions:
– Disable auto-uploading of voice recordings or cloud sync if possible
– Turn off location tracking unless absolutely necessary
– Regularly delete interaction history or voice logs
– Choose manual updates over automatic when available, so you can review changes
– Check if third-party skills or features are activated without your consent

## 4. Update firmware and monitor device access

Outdated smart devices are more vulnerable to cyberattacks. Ensure that firmware and software are always updated — either manually or with trusted auto-update settings.

Also:
– Limit which accounts and apps are connected to the device
– Use strong, unique passwords for smart hubs and app accounts
– Regularly check login history or access logs if the platform provides them
– Turn off microphones/cameras when not in use

For example, smart TVs, speakers, and tablets can all be endpoints for unauthorized access if not properly secured.

## 5. Keep the conversation going

As smart devices evolve, so do the risks. What feels safe today might be exploited tomorrow. Create a home culture where asking questions and reporting weird behavior is always encouraged.

Ask:
– “Did anything strange happen when you were using the device?”
– “Did it ask you to say or do something?”
– “Did it respond in a way that surprised or scared you?”

These questions keep your child alert — and help you catch potential issues early.

# Additional asset: First Gadget checklist

Sooner or later (most) parents inevitably get round to buying their kids their own electronic device. According to Kaspersky's research, 61 percent of children get their first device between the ages of eight and 12, and, perhaps surprisingly, in 11 percent of cases, they're given their own cellphone or tablet before they turn five. It's essential for parents to know the guidelines for introducing a device into their kids' lives for the first time.

Together with clinical psychologist Dr. Saliha Afridi, Kaspersky is presenting cybersecurity and psychological considerations that parents would do well to be aware of before giving their kids their very first tech gadgets.

## What to do before giving a gadget to a child?

**Set up a Child Account** before giving your offspring their first gadget. Whether it's a phone or a tablet, it's crucial to ensure the age-appropriateness and safety of the gadget. Even if it's a brand-new gift, prioritize setting up this feature. A Child Account acts as a safeguard on the device, preventing things like downloads of mature content or songs with explicit content. For detailed guidance on creating a kid's account, refer to our guide for Android or the one for iOS.

**Install all the basic applications** that support either communication or geo-location (like messenger and map apps), plus learning applications. And don't forget to set up the privacy and confidentiality settings in each of the installed applications, so that the child, for example, isn't discoverable via their phone number by unknown individuals. Tools like Privacy Checker can assist you in tailoring the optimal protection settings for various devices and platforms.

**Remember to install a digital parenting app as well**. This will empower you to curate content, monitor the amount of time your kid spends on specific apps (and set limits if needed), and track their current location.

## How to introduce a new device into a child's life?

**Walk them through the device's functionalities as well as the potential dangers when** gifting them a new gadget. This is an opportune moment to explore its features and understand its potential pitfalls.

**Craft a set of family usage rules together**. In this conversation, it's important to foster an understanding and consensus about the responsibilities and expectations tied to device ownership. To ensure a healthy balance, establish tech-free zones and times — perhaps during dinner or the hours leading up to bedtime. Designate moments for non-tech hobbies like reading, outdoor games, or puzzles, which can act as beneficial alternatives to screen time. Periodically revisiting and refining these rules as your kid grows and technology advances is key.

And remember — unless a kid shows a healthy level of engagement with real-life activities and in-person socializing, don't introduce a smartphone or social media. One way they can earn a device is by showing that they're capable of doing the "non-negotiables" regularly and consistently. These include sleep, exercise, homework, socializing, eating healthily, and wakeful resting periods.

## How to talk to a child about online safety?

**Encourage open communication from the outset**. Engage junior in conversations about their online experiences — ensuring they feel safe to share both the good and the bad experiences.

**Stay up to date with the latest digital trends** and threats as well as high-profile cyberbullying or data breaches. Share this information with your child in a way they understand. You can learn the latest cybersecurity news via our blog.

**Bring up the permanence of online actions**. This includes how things shared online stay there forever and can affect their reputation and future opportunities. Kids should be especially careful about information they share about themselves: never giving out their address, geolocation or login credentials and passwords. Additionally, they should avoid using their real names as user IDs, as these can be potential clues for attackers to discover their other social media accounts. Help them understand the concept of privacy and the potential risks of sharing too much information.

**Teach your kid that accepting friend requests from unfamiliar individuals in real life should be avoided**. It's crucial to explain that if someone they don't know is persistently trying to find out personal information about them or their parents, it's a cause for concern. Your child shouldn't feel they're being rude or impolite if they don't respond to a request for friendship. In social networks, just like in life, there needs to be privacy.

By having such conversations and educating your children about online risks in a non-confrontational manner, you raise your kids being more likely to approach you when they encounter something questionable online. You should make sure they maintain a stance of curiosity — not judgment or fear. Your reactions will determine how open they feel about sharing in the future.

And a **digital parenting app** serves here as a valuable tool to enable you to monitor your kids' online searches and activity, ensuring a safer online experience.

## What are the main risks I should tell my child about?

In our digital age, kids are vulnerable to cybercriminals, often because they're unfamiliar with essential cybersecurity principles and common scam tactics. It's our duty as guardians to educate them on these matters before they inadvertently fall prey to them.

For instance, guide your kid in identifying deceptive commercials, bogus survey requests, counterfeit lotteries, and other schemes that can jeopardize their personal data. Help them grasp the reality that, while it might be tempting to download a Barbie movie ahead of its official release, offers like these could be ploys by cybercriminals aimed at pilfering data or even siphoning money from their parents' cards. A reliable security solution can detect and block any phishing websites or any malicious software.

**Instill in your child the habit of being critical and cautious when online**. Teach them to pause before clicking when it comes to dubious links, unfamiliar email attachments, or messages from unknown entities. Discuss the appropriate permissions apps should have on their devices. For example, there's no valid reason for a Calculator app to request geolocation access.

**Make conversations about cybersecurity more enjoyable and interesting** by discussing the topic through games and other entertaining formats. Most importantly, instill confidence in them to approach a trusted adult when faced with unsettling or suspicious situations online.

## How to check that you're prepared?

Once a gadget appears, your family's life will inevitably undergo a transformation, as your kid will be drawn into the realm of the internet. Rather than forbidding it, it's advisable to guide them on proper online behavior — if used correctly, a gadget can really help kids learn and grow. However, this can only happen if they know when and how to alert their parents about any online threats they come across – whether they're receiving strange messages from adults, requests for personal information, or stumbling upon phishing sites.

Learning, however, is a gradual process, and it doesn't guarantee perfection from the start. Mistakes will naturally occur, such as your kid accidentally downloading malware or engaging with suspicious individuals or struggling with screen time management. Nonetheless, your role as a parent is to provide support and assistance in their learning process. Only this way can you help your child be safe online.