

Digital Survival Skills

HANDOUTS

Released 2026

Handouts Included

AI 101

- What you need to know about GenAI
- How to use AI: A quick reference guide

Avoiding Frauds and Scams

- Recognizing and avoiding scams
- Proactive privacy and scam prevention
- What to do if you've been scammed

Finding Reliable Health Information Online

- Finding good health information online

Child and Youth Safety Online (for Caregivers)

- Keeping kids safe online: What you can control, teach and model
- Online safety by age: A guide for caregivers
- Further resources

About the Curriculum

This packet contains the take-away handouts from Pitt Cyber's Digital Survival Skills initiative which is a free curriculum developed with local community partners to help adult learners navigate life online. These handouts are designed to accompany full workshops but can also be used or shared on their own.

For the full curriculum or to bring a workshop to your organization, visit cyber.pitt.edu/initiatives/digital-survival-skills or contact cyber@pitt.edu.

Note: Each handout has a marked field for you to upload your logo if you wish. Printing the handouts will not show this field if you do not upload a logo.



University of
Pittsburgh®

Institute for Cyber Law,
Policy, and Security

What You Need To Know About GenAI



What Is Generative AI?

- Generative Artificial Intelligence (GenAI) tools produce new content—text, images, sounds, or videos—based on patterns in the data they were trained on.
- Popular GenAI examples include ChatGPT, Copilot, Gemini, and Claude.

Important:

- AI doesn't think, understand, or feel. It predicts what words or images are most likely to come next based on patterns.
- It imitates human intelligence; it does not have intelligence.

Three Things to Remember About AI

1. AI Can Be Helpful

- AI tools can process huge amounts of information quickly
- AI tools can help you brainstorm, draft, summarize, and organize
- AI tools can provide personalized recommendations
- AI tools can expand accessibility (reading text aloud, translating languages, describing images)

2. AI Can Be Harmful

- **Bias:** AI learns from data created by humans, including our biases and stereotypes. It can repeat and reinforce unfair ideas.

- **Privacy risks:** Many free AI tools store your conversations and personal information, use them for training data, and might be susceptible to leaking your information.
- **Environmental impact:** AI uses significant energy and water resources.
- **Deepfakes:** Bad actors use AI to create convincing fake videos, audio, and images.

3. AI Can Be Wrong

- When AI generates false information confidently, it's called a **hallucination**. This happens because:
 - ❑ AI predicts likely patterns, not facts
 - ❑ Training data has gaps and errors
 - ❑ AI doesn't actually "know" anything—it mimics knowledge

Using AI Responsibly

- ✓ **Check before you trust:** AI sounds confident even when wrong
- ✓ **Know the limits:** AI helps you think, it doesn't think for you
- ✓ **Remember AI is not your friend:** For real support, talk to real people
- ✓ **Think about the planet:** Consider whether you need AI for every task
- ✓ **Keep building your own skills:** Don't let AI do things you want to learn
- ✓ **Be the decision-maker:** You should make the final call, not the AI
- ✓ **Protect your privacy:** Never share sensitive personal information
- ✓ **Watch for fakes and scams:** Verify before believing or sending money

How to Use AI: A Quick Reference Guide



Popular GenAI Tools

Tool	Website	Login Required?	Cost
ChatGPT	chat.openai.com	Works without login for basic queries	Free access with usage limits; paid tiers for expanded
Claude	claude.ai	Account needed (email)	Free access with usage limits; paid tiers for expanded
Gemini	gemini.google.com	Google account needed for full features	Free access with usage limits; paid tiers for expanded
Copilot	copilot.microsoft.com	Works without login; Microsoft account unlocks more	Free with limits; also built into Windows 11 and Edge browser

How to Use Tools

1. **Prompt** → Write clear directions for the AI
2. **Refine** → Revise your prompt through conversation
3. **Verify & Personalize** → Check that the information is accurate; make it yours

Step 1: Write a Good Prompt

A strong prompt is specific, gives context, and includes examples when possible.

■ **Weak:** “Help me with a cover letter”

- ❑ **Stronger:** “I’m applying for a customer service job at a retail store. I have 5 years of experience in food service. What key points should I highlight to show my skills transfer well?”

■ **Weak:** “Give me interview tips”

- ❑ **Stronger:** “I have a job interview for an administrative assistant position next week. I’m nervous about answering questions about my weaknesses. My weaknesses are x, y, and z. Can you suggest 3 ways to answer that question honestly but positively?”

What to Include in Your Prompt: Your goal, context and audience, specific requirements or constraints, and desired format (list, paragraph, step-by-step, etc.)

Protect Your Privacy: Never share sensitive information with AI tools—no Social Security numbers, passwords, financial details, or other people’s private information.

Step 2: Refine and Revise

Don't expect perfection on the first try. Treat AI like a conversation. Keep refining until you get what you need.

Helpful phrases:

"Can you expand on the second point?"

"Make this shorter"

"Make this more casual/professional"

"Give me more examples"

"Explain this like I'm new to the topic"

"I liked X but can you change Y?"

"That's not quite what I meant. I'm looking for..."

"Can you try again, but this time..."

Tip: Not sure how to ask for what you want? Try: *"Help me craft a strong prompt about [your topic]. Ask me clarifying questions first, then generate the final prompt."*



Step 3: Verify the Output

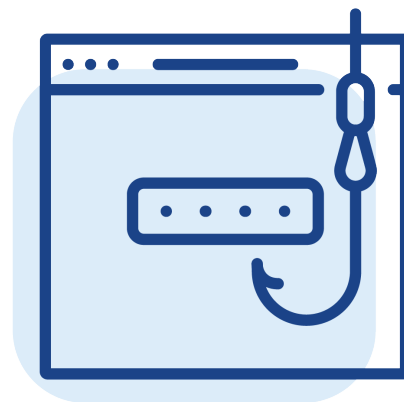
AI sounds confident even when it's wrong. Always check before you trust, share, or act on AI-generated information. **Use the SIFT method:**

- **S – Stop:** Before acting on information, ask: "What are the consequences if this is wrong?" The higher the stakes (money, health, legal issues), the more carefully you should check.
- **I – Investigate the Source:** Who created the information AI is pulling from? Is it a company trying to sell something? A news organization? A blog? Sources go through different review processes—an edited news article is more reliable than an unchecked social media post.
- **F – Find More Coverage:** Don't rely on just one source. Look for the same information in multiple trustworthy places. Remember: AI finds sources that match patterns, not necessarily the best sources.
- **T – Trace Claims to the Original:** Click through to the original source. Ask yourself: Did the AI get this right? Are these sources reliable? Is the information up to date?

Final Step: Personalize

Don't just copy and paste what the AI says. AI doesn't know your real life and often gets facts wrong. Use the AI to help you organize your thoughts, but make sure the final version is yours: based on your ideas, your voice, and conveys what *you* want to share.

Recognizing and Avoiding Scams



Psychological Tricks Scammers Use

Scammers use emotional tactics to bypass your logic and get you to act fast. **Scammers exploit your trust or kindness, your need or curiosity, and your fear or excitement.**

Watch for these common tricks:

Tactic	Goal	What They Might Say
Urgency	To make you act before you can think.	"Final warning! Act in the next hour!"
Authority	To scare you into obeying someone with authority	"This is the IRS" or "I'm Officer Smith."
Secrecy	To keep you isolated so no one can warn you.	"Don't tell your family about this."
Sympathy	To exploit your kindness and trust.	"My child is in the hospital... I'm desperate."

Common Scams to Watch For

Scams can come from texts, phone calls, emails, social media, messaging services, dating apps, gaming platforms, online ads, or through a variety of physical devices or contacts.

- **Imposter Scams:** They pretend to be a trusted company (like your bank, utility provider, or a tech company).
- **Job & Investment Scams:** High pay "work from home" jobs or "guaranteed" cryptocurrency (digital money) investments.
- **Merchant & Prize Scams:** Fake websites with "too-good-to-be-true" prices or "prizes" that require a fee.
- **Romance Scams:** Fake online profiles that build a relationship with you then ask for money for "emergencies" or "travel."
- **Other:** Artificial intelligence scams (voice or video impersonation), door-to-door scams, fake QR codes, credit card stealers, Wi-Fi hacking.

“STEEL” Yourself Against Stealers

If you receive an unexpected text, email, or call, or knock on the door, use the **STEEL** method:

S – Slow Down

Don't make quick decisions. Scammers want you to rush. Pause and take a step back.

T – Think Twice

Ask yourself: Is this an unfamiliar contact? Are they using a psychological tactic like creating a sense of urgency or demanding secrecy? Does what they say actually make sense?

E – Examine The Source

- **Verify:** Contact the person/company back using an official contact from their website, your billing statement, or your own contact list. **Never** use the contact they gave you.
- **Hover:** Hold your mouse over links or email addresses to see the true destination. Only visit secure sites with the “s” in <https://>. Watch for typos (like a zero “0” instead of an “O”).
- **Search:** Use the internet to look up the official organization for contact information. You can also search for “Is X a scam?” to see what people have reported about that information, person, or contact.

E – Exit The Situation or Disengage

Many times, your best defense is to do nothing. Do not reply; do not click. Block the number, close the door, or delete the message.

L – Let Authorities Know

Report the incident to your bank, the company being impersonated, or law enforcement. Tell your friends and family so they know it's a scam if targeted.

Remember Your Resources

Identify your “Safe Person”:

Who is a friend, family member, or neighbor you can call to help you verify a suspicious message?

AARP Fraud Watch

Helpline (877-908-3360):

Free for *everyone* to get advice, help identify scams, or aid if you think you've been scammed.



University of
Pittsburgh

Institute for
Cyber Law, Policy, and Security

Proactive Privacy & Scam Prevention



You can't stop scammers from targeting you completely, but you can make yourself a harder target.

Secure Your Digital Accounts

The foundation of your security starts with how you manage your accounts across all your devices.

- **Strong, Unique Passwords:** Use long passwords that mix letters, numbers, and symbols.
- **Don't Reuse Passwords:** Use a different password for every single account.
- **Password Managers:** Use a tool like Bitwarden (which is free) to keep track of all your different logins.
- **Multi-Factor Authentication:** Turn on extra security (like a code sent to your phone or a fingerprint scan) whenever possible, especially for sensitive accounts like banking.

Guard Your Communications

Managing how you receive calls, texts, and emails can significantly reduce your exposure to scams.

Phone & Text Protection

- **National Do Not Call Registry:** Register your number at donotcall.gov or call 1-888-382-1222.
- **Carrier Blocking Apps:** Use your provider's specific app, such as AT&T ActiveArmor, T-Mobile Scam Shield, or Verizon Call Filter.

- **Manual Blocking:** Block spam numbers directly from your recent calls or messaging app.
- **Filter Unknown Senders:** Enable this in your phone settings to sort suspicious messages into a separate folder.
- **Report Spam Texts:** Forward any suspicious text messages to 7726 (SPAM).

Email Protection

- **Spam Filters:** Ensure your email spam filters are enabled (they are usually on by default).
- **Reporting:** When you receive a scam email, click "mark as spam" to report it.

Maintain Your Devices

Consistent maintenance helps ensure your hardware remains secure against modern threats.

- **Software Updates:** Keep your software updated to the latest versions.
- **Antivirus Software:** Use antivirus software and keep it current. Many computers have this built in, such as Windows Defender.
- **Antivirus Options:** Bitdefender is an example of a free option with paid upgrades.
- **Data Backups:** Back up your data regularly using an external hard drive or a secure cloud service to prevent losing files if something goes wrong.

Don't Forget Privacy & Physical Safety

Personal habits in public and at home can prevent scammers from gathering information about you.

- **Public Wi-Fi:** Avoid using public Wi-Fi for private activities like banking or shopping online.
- **Social Media:** Keep social media accounts private and do not overshare personal information (example: Do not post about traveling until you have returned home).
- **Home Security:** Put a “No Soliciting” sign on your door to stop uninvited visitors.



Resource	Contact / Link
Do Not Call Registry	Register at donotcall.gov or call 1-888-382-1222
Report Spam Texts	Forward messages to 7726 (SPAM)
Free Password Manager	bitwarden.com
Free Antivirus Software	bitdefender.com
Carrier Blocking Apps	AT&T ActiveArmor, T-Mobile Scam Shield, or Verizon Call Filter. Check with your carrier!

What To Do If You've Been Scammed

Don't be embarrassed. Scammers are professional liars, and anyone can fall for a scam. Act quickly and get help.

Don't go through this alone. Tell someone you trust like a family member or friend. **The AARP Fraud Helpline** offers free advice and support for everyone, not just seniors: **877-908-3360**

Report what happened. Even if you can't get your money back, reporting helps law enforcement shut down scams and protect others. Where you report (and what else you need to) depends on what happened. Find your situation below for specific steps:

What if I gave personal info (SSN, credit card info, bank account info, passwords, etc.) to a scammer?

- Contact your bank/credit card companies immediately and follow their instructions
- Change your passwords—use a different, strong password for each account
- Place a **fraud alert** or **credit freeze** with the major credit bureaus
 - ❑ Equifax: 800-525-6285, equifax.com
 - ❑ Experian: 888-397-3742, experian.com
 - ❑ TransUnion: 800-680-7289, transunion.com
- Visit **IdentityTheft.gov** for a personalized recovery plan from the FTC



What if I think my account has been hacked?

- Create a new, strong password (different from all your other passwords)
- Turn on two-factor authentication if available
- Report the hack to the company that runs the account
- Notify your bank if payment info was saved in the account
- Monitor your statements for unusual activity

What if I opened a harmful link or installed bad software (malware)?

- **Cut the connection immediately**—turn off Wi-Fi, enable airplane mode, or unplug ethernet
- Run an up-to-date antivirus scan and follow instructions to remove threats
- Use a **different** device to change passwords for important accounts
- If malware won't go away, you may need to wipe the device (keep backups!)

What if I gave out a password or security code?

- Change that password immediately—even if you're not sure they used it
- Change it on ALL accounts where you used the same password
- Notify the company that your credentials may be compromised

What if I lost money to a scammer?

- Report to your bank/credit card company ASAP—they may be able to stop or refund the transaction
- Report to the **FTC** at [ReportFraud.ftc.gov](https://reportfraud.ftc.gov)
- Report to **PA Attorney General**: 800-441-2555 or scams@attorneygeneral.gov
- File an **FBI report** at ic3.gov



Finding Good Health Information Online



Recommended Sources of Health Information

- **MedlinePlus:**
medlineplus.gov
- **World Health Organization:**
who.int
- **Science Feedback:**
science.feedback.org
- **American Heart Association:**
heart.org
- **American Dental Association:**
mouthhealthy.org
- **American Cancer Society:**
cancer.org
- **American Academy of Pediatrics:**
healthychildren.org
- **American Academy of Family Physicians:**
familydoctor.org
- **Academy of Nutrition and Dietetics:**
eatrightpro.org/nutritionfactcheck
- **Your healthcare provider!**

SIFT the Information You Find

When you encounter information you're unsure about, you can use the SIFT Method to help you determine whether it's accurate.

Note that you should always Stop, but the rest of the steps can be done in any order. As soon as you have enough information to decide whether the information is true, you're done!

S = Stop

Before acting on the information, pause.

I = Investigate the Source

Try to determine whether the source of the information is reliable.

F = Find Better Coverage

Have other sources confirmed, refuted, or otherwise discussed the information?

T = Trace the Claims

If you still want to know more, you can locate the original video, quote, or image to see if the information has been taken out of context or described inaccurately.

LEARN MORE ABOUT SIFT:

- lib.lavc.edu/information-evaluation/siftmethod
- bbc.com/future/article/20240509-the-sift-strategy-a-four-step-method-for-spotting-misinformation
- clark.libguides.com/evaluating-information/SIFT



University of
Pittsburgh

Institute for
Cyber Law, Policy, and Security

Keeping Children and Youth Safe Online

What you can control, teach, and model



Control

Your biggest influence is what devices your kids access. Remember that they may have access to devices through school, so be aware of what protections the school district implements.

Reality check: Kids can find workarounds to all of the technical safeguards listed here. Settings/controls often change, and age verification is easy to bypass. Think about oversight and controls as speed bumps, not walls for children. And consider loosening controls as kids get older to teach them responsible use.

Technical safeguards

- Parental controls (limit content, contacts, chats, purchases)
- Set screen time limits (limit how long kids can spend on smartphones, tablets, or games)
- Safe search settings (limit explicit, mature, or graphic content on browsers)
- App permissions (limit what information apps can access: location, photos, contacts, camera/mic)
- Privacy settings on accounts/profiles (limit who can see content on a user's profile)
- Home Wi-Fi Settings (limit content and how long users can access the internet)

Implementing Technical Safeguards	
Where to look	Built-in settings like "Screen Time" (Apple), "Digital Wellbeing" / "Family Link" (Android), or within the specific app, game, console, or router itself.
Can't find it?	Search "[device or app name] + screen time limits" (or "parental controls," "safe search," etc.). Companies publish their own guides; ConnectSafely, Internet Matters, and Common Sense Media post tutorials.
Check every device	Check all devices, apps, and browsers. Don't forget school issued devices.
Lock it down	Set a PIN or passcode your child doesn't know, so settings can't be changed without you.
Revisit often	Companies change settings and menus, and kids pick up new hacks. Recheck regularly.

Monitoring apps like Bark, Qustodio, and Aura exist and can help caregivers oversee their children's devices. To decide if they are right for your family consider cost, whether it collects/sells data, and if there is a risk of damaging trust with the children that are being monitored.

Teach

Teach about good habits of digital citizenship and create household tech agreements together—shared rules for screen time, contacts, sharing, device use, and passwords.

Common Sense Media: [Family Media Agreement](#); [Family Device Agreement](#); [Family Tech Planner](#)

Connect Safely: [Family Contracts and Pledges](#)

Internet Matters: [Digital Family Agreement](#)

...or search online for many more examples and templates to inspire your own!

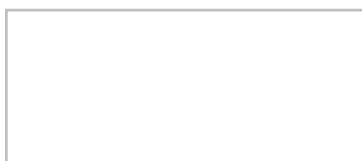
Digital citizenship habit	What it means
Treat others well	Words hurt online too. Don't share others' photos or info without consent.
Represent yourself responsibly	Posts are permanent, even if deleted.
Protect privacy	Create strong passwords, maintain private profiles, and keep ID info private. Know grooming red flags: secrecy, requests for photos/info, isolation from friends/family, escalating conversation, threats.
Evaluate what you see	Feeds run on engagement, not accuracy. Ask: Who made this, and why? Can I confirm it elsewhere? What is it trying to make me feel or do?
Know when to ask for help	Confide in a trusted adult when something feels uncomfortable, scary, or suspicious.

The Attention Economy

Teach kids that platforms profit from keeping them scrolling, so infinite scroll, autoplay, and likes/badges are design choices by companies to trigger dopamine and remove natural stopping points. Kids' developing brains are especially vulnerable, with real effects on attention, memory, and sleep. Understanding the design can help kids recognize its harms.

Model

- Be curious (not judgmental) about your child's online life: ask what they're into and who they follow
- Make sure kids know they can come to you with problems and not get punished
- Mind your own posting: ask permission before posting about your kids
- Narrate your own choices ("I'm putting my phone away at dinner because I want to talk to you")



Online Safety By Age: A Guide For Caregivers

Keeping Children and Youth Safe Online



There's no one-size-fits-all approach to online safety. Every child develops differently, so use these recommendations as a guide and adapt them to your child's maturity and your family's needs. Start with more support when children are young, then gradually increase their independence as they age.

These recommendations are based on guidance from experts like the American Academy of Pediatrics and Common Sense Media. They're meant to be helpful starting points, not sources of guilt.

The One Thing That Doesn't Change

No matter your child's age, they need to know they can come to you with anything they encounter online without fear of losing privileges or getting a lecture. That trust matters more than any settings you configure.

Ages 9 and Under (Little Kids and Big Kids)

Young kids are curious and quick to click, but they don't yet have the brain development to recognize danger or evaluate what they're seeing. This is the age where you have the most control. Use it.

What to control	What to teach
■ Whether (or how) your child accesses devices or the internet at all ■ Choose curated environments: YouTube Kids instead of regular YouTube, gaming without chat features ■ Keep devices in shared family spaces, not bedrooms ■ Disable chat features and in-app purchases ■ Co-view and co-play whenever possible, so you can react/explain things ■ Approve every online contact when you can (apps like Facebook Messenger Kids let you do this)	■ Tell a trusted adult if something feels "weird" or scary ■ Keep personal information (name, address, school) private ■ Be kind to others, in person and online ■ People online aren't always who they say they are, so be careful who you talk to ■ Ads are designed to make you want things



Ages 10–12 (Tweens)

Tweens can think more logically and grasp abstract ideas like “digital footprint.” Peer influence is growing, exposure to inappropriate content increases, and this is often when kids start asking for a smartphone.

What to control	What to teach
■ Delay smartphones as long as possible; you could consider a basic phone or smartwatch first, or a smartphone stripped of apps like social media or internet browsing ■ Keep tweens off social media; most platforms officially require users to be 13 ■ Co-create your household tech agreement, with tween’s input ■ Keep devices out of bedrooms overnight ■ Approve every app or game before download ■ Maintain parental controls, but expect tweens to test and push against them	■ What cyberbullying looks like (as a target and as a participant) and the practical steps: don’t engage, screenshot, block, report, tell an adult ■ How to ask critical questions about content: Who made this? Why? Are they trying to sell me something? ■ How to recognize sponsored content, influencers, and manipulation and that algorithms decide what shows up in a feed (it isn’t neutral or random) ■ The warning signs of grooming (tweens often miss these because the behavior can feel flattering) ■ That people online often look “perfect” (and that’s an illusion) ■ Open conversations about AI companions, deepfakes, and what’s real online

Ages 13+ (Teens)

Legally, 13 is the minimum age for most social media, though many experts suggest delaying further (some recommend 16). Teens are forming their own identity, pulling away from family, leaning into peer relationships, and wanting more privacy. They’re capable of more critical thinking but are also highly susceptible to peer pressure.

What to control	What to teach
■ Stay informed about what platforms teens use and who they follow ■ Keep a few non-negotiables: tech-free meals, phones out of the bedroom overnight (lack of sleep is one of the most consistent harms linked to teen phone use) ■ If you monitor, be transparent about what and why as heavy-handed or secret monitoring can backfire and damage trust at this age ■ Delay social media as long as is realistic for your family	■ How to manage their own privacy settings (show them how the first time) ■ The warning signs of unhealthy relationships, on and offline ■ That image-based harm is serious and sharing a private photo, even of themselves, can have legal and lasting consequences ■ To notice how being online makes them feel, and that it’s okay to log off ■ That algorithms shape what they see and how that can influence mood and thinking ■ Continue conversations about AI companions, deepfakes, and what’s real online

Further Resources

Keeping Children and Youth Safe Online



General Hubs & Organizations

Link	Description
AAP Center of Excellence on Social Media and Youth Mental Health	The American Academy of Pediatrics' hub of research-backed online safety resources for families, organized by age and topic.
ConnectSafely	Nonprofit with parent guides, quick-guides, and app-specific safety tips, covering everything from social media to generative AI.
Internet Matters	UK-based nonprofit offering age-specific advice, guides, and tools to help children stay safe online.
Common Sense Media	Independent nonprofit reviewing movies, apps, and games for age-appropriateness, plus parenting articles on nearly every digital safety topic.
HealthyChildren.org	The American Academy of Pediatrics' consumer parenting site, with articles on media use, development, and family health.

Device & Platform Setup Guides

Apple Screen Time	Apple's official instructions for setting up Screen Time limits and content restrictions on iPhone and iPad.
Roblox: Managing Screen Time	Roblox's official guide to setting time limits and parental controls within the platform.
Nintendo Switch Parental Controls	Nintendo's official walkthrough for setting play-time limits and restrictions on the Switch.
How to Check Screen Time on Android	A step-by-step guide to finding and using Android's built-in Digital Wellbeing screen-time tools.
Setting Up Parental Controls on Your Wi-Fi Router (CNET)	A walkthrough for setting network-wide controls directly on your home router — scheduling internet access, filtering content, and pausing connections for every device at once.

Family Tech Agreements & Contracts

Common Sense Media Family Media Agreement (PDF)	A printable, fill-in agreement covering screen time, sharing, and online behavior for the whole family.
Center for Online Safety: Technology Contracts	A practical guide to introducing a family tech agreement, including tips on non-negotiable vs. flexible rules.
ConnectSafely Family Contract for Smartphone Use	A customizable pledge for parents and kids to sign when a child gets their first smartphone.

AI Companions & Generative AI

Link	Description
Common Sense Media: Social AI Companions	A risk assessment of popular AI companion apps and what parents should know before their kids use them.
Talk, Trust, and Trade-Offs (PDF)	Common Sense Media's research report on how teens are actually using AI companions and chatbots.
What I Want My Kids to Know About GenAI	A non-technical conversation guide from Pitt Cyber to help caregivers talk with preteens and teens about generative AI.

Privacy & Product Safety

Mozilla *Privacy Not Included	A buyer's guide rating the privacy and security of connected toys, apps, and devices, including many made for kids.
--------------------------------------	---

Platform-Specific Guidance

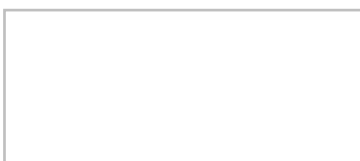
The Keys: A Guide to Digital Safety (Snapchat)	An interactive course from Snap, developed with Common Sense Media, teaching teens and families to recognize and respond to bullying, illicit drug activity, image-based harm, and sextortion on Snapchat.
---	--

Government & Public Health Resources

SAMHSA: Online Health and Safety for Children and Youth	Federal resources on the mental health dimensions of kids' online safety, from the Substance Abuse and Mental Health Services Administration.
FTC: Protecting Kids Online	The Federal Trade Commission's consumer guidance on parental controls, kids' privacy rights (COPPA), cell phones, video games, and image-based abuse.

Additional Guides & Research

AAP: The 5 Cs of Media Use	A research-based framework (Child, Content, Calm, Crowding Out, Communication) with free age-based handouts for talking about media use.
UNESCO: Growing Up in a Connected World	A global family guide to media and information literacy, covering social media, algorithms, AI, and digital wellbeing.
Stanford Social Media Lab: A Parent's Guide to Digital Safety	A guidebook for parents of tweens and teens navigating social media, messaging apps, and AI chatbots.
SANS: Secure the Generations	A cybersecurity-focused toolkit with age-specific fact sheets covering online threats from childhood through older adulthood.



University of
Pittsburgh

Institute for
Cyber Law, Policy, and Security