STEALTHBLUE
CYBER

CYBERSECURITY
GUIDE FOR PARENTS

Protecting Your Family in the Digital Age

FREE CYBERSECURITY TRAINING: STEALTHBLUE.TRAINING

STUDENT EDUCATION: STEALTHBLUESCHOOL.COM

STEALTHBLUE CYBER

DETECT | DEFEND | SECURE

TABLE OF CONTENTS

Includes a Family Digital Agreement tear-out template

01 UNDERSTANDING THE DIGITAL LANDSCAPE

Your child's online world is far more complex than it appears on the surface. By 6th grade, most students are actively using platforms like Discord, Roblox, Fortnite, TikTok, Snapchat, and YouTube – many of which have age requirements of 13 or older that are routinely bypassed.

WHAT PARENTS NEED TO KNOW

- The platforms your child uses likely have chat features, direct messaging, and the ability to connect with strangers – even if they appear to be "just games"
- Age ratings don't guarantee safety. A "13+" rating means the platform has some moderation, but it doesn't prevent exposure to inappropriate content or predatory behavior
- Average screen time for this age group is 4–6 hours daily. Understanding what they're doing during that time matters more than the number itself
- Many platforms have separate ecosystems (Roblox has thousands of user-created games, Discord has millions of servers) that are impossible to fully moderate

THE REALITY CHECK

Your child likely knows more about these platforms than you do – and that's okay. The goal isn't to become an expert on every app. It's to understand the risks, set appropriate boundaries, and maintain open communication.

Visit stealthblueschool.com to see exactly what your child is learning about cybersecurity. Free training for adults is available at stealthblue.training

02 PASSWORDS & ACCOUNT SECURITY

Weak passwords remain the number one way accounts get compromised. If your child uses "password123" or their pet's name, their accounts are vulnerable.

SETTING UP STRONG SECURITY

- Use a family password manager like Bitwarden (free) or 1Password Families to generate and store strong, unique passwords for every account
- Enable two-factor authentication (2FA) on every account that supports it — especially email, social media, and gaming accounts
- Set up recovery emails and phone numbers to your own accounts so you can regain access if something goes wrong
- Teach your child that passwords are like house keys — you don't share them with friends, even best friends

WHY YOU SHOULD KNOW YOUR CHILD'S PASSWORDS

This isn't about distrust. It's about safety. Have an honest conversation: "I need to know your passwords the same way I need to know where you are after school. It's not because I don't trust you — it's because I need to be able to help if something goes wrong."

QUICK ACTION ITEMS

- [ ] Set up a family password manager this week
- [ ] Enable 2FA on your child's email and primary accounts
- [ ] Ensure recovery contacts point to a parent's email/phone
- [ ] Check that no passwords are reused across accounts

03 SOCIAL MEDIA & PRIVACY SETTINGS

Social media platforms are designed to encourage sharing. Your job is to make sure your child understands what should never be shared and how to lock down their accounts.

PLATFORM-BY-PLATFORM PRIVACY CHECKLIST

TIKTOK

- Settings > Privacy – Set account to Private
- Disable "Suggest your account to others"
- Restrict who can comment, duet, and send messages
- Enable Family Pairing for linked oversight

SNAPCHAT

- Settings > Privacy Controls – Set "Contact Me" to "My Friends" only
- Disable "Quick Add" to prevent strangers from finding your child
- Enable Family Center for oversight

INSTAGRAM

- Settings > Privacy – Switch to Private Account
- Disable "Activity Status" and restrict who can tag/mention
- Set up Supervision through Family Center

WHAT METADATA REVEALS

When your child posts a photo, it may contain hidden data including GPS coordinates, timestamps, and device information. Disable location services for camera and social media apps.

GROOMING WARNING SIGNS: Watch for an older "friend" your child mentions frequently, secretive behavior around devices, receiving gifts or game credits from someone online, or being asked to move conversations to a different platform.

04 GAMING PLATFORM SAFETY

Online gaming is one of the most common ways children interact with strangers. Voice chat, text chat, and friend requests create direct lines of communication that bypass many safety filters.

ROBLOX

- Account Settings > Privacy — Restrict chat to "Friends" or "No one"
- Enable Account PIN to prevent settings changes
- Set monthly spending limits under Billing
- Review friend list regularly — remove unknown contacts

FORTNITE / EPIC GAMES

- Parental Controls — Set a PIN, disable voice chat or restrict to "Friends Only"
- Turn off friend requests from strangers
- Disable in-app purchases or require PIN for every purchase

MINECRAFT

- Bedrock Edition: Use Xbox/Microsoft Family Settings for multiplayer and chat
- Java Edition: Stick to trusted servers with active moderation
- Review Realms membership if they play on private servers

DISCORD

- Enable "Keep Me Safe" content filter (Settings > Privacy & Safety)
- Disable "Allow DMs from server members"
- Review which servers your child has joined
- Set up Family Center for oversight of activity

IN-GAME PURCHASES: Loot boxes and microtransactions are designed to be addictive. Set spending limits, require approval for purchases, and discuss how these systems manipulate spending behavior.

05 HOW TO IDENTIFY CYBERBULLYING

Cyberbullying often goes undetected because it happens on devices, in private messages, and in spaces parents don't see. Knowing the warning signs is critical.

BEHAVIORAL WARNING SIGNS

- Sudden reluctance to use devices or go online
- Becoming upset, withdrawn, or angry after using their phone or computer
- Avoiding conversations about what they're doing online
- Declining grades or loss of interest in activities they used to enjoy
- Changes in friend groups or social withdrawal

PHYSICAL SIGNS

- Trouble sleeping or nightmares
- Loss of appetite or changes in eating habits
- Unexplained headaches or stomachaches
- Signs of anxiety or depression

HOW TO CHECK CHAT LOGS

- iMessage: Open Messages app or check iCloud messages if synced
- Instagram DMs: Open app > Messages icon > Review conversations
- Snapchat: Messages disappear by default – use "My Data" download (Settings > My Data)
- Discord: Review DMs and server messages directly on the device
- Roblox: Check chat history through the in-app chat window

PRESERVING EVIDENCE: Take screenshots of every message with timestamps and usernames. Do not delete anything – evidence is critical for school reports or law enforcement. Record dates and times in a written log.

06 MONITORING & OVERSIGHT TOOLS

The right level of monitoring depends on your child's age, maturity, and demonstrated responsibility. For students in this age group, active oversight is appropriate and recommended.

BUILT-IN PARENTAL CONTROLS

APPLE SCREEN TIME (IPHONE/IPAD/MAC)

- Set daily time limits per app category
- Schedule Downtime (no device use during sleep hours)
- Block specific apps or content types
- Require approval for app downloads and purchases
- Review weekly activity reports

GOOGLE FAMILY LINK (ANDROID)

- Set daily screen time limits
- Lock devices remotely at bedtime
- Approve or block app downloads
- View location and activity reports
- Filter Google Search and Chrome content

MICROSOFT FAMILY SAFETY (WINDOWS/XBOX)

- Set screen time limits across devices
- Filter web content and search results
- Manage Xbox privacy and communication settings
- Review activity summaries via email

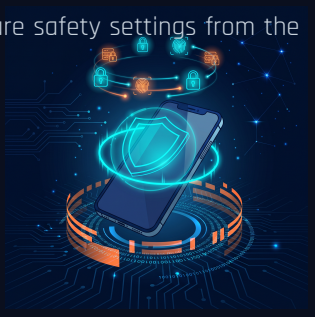
ROUTER-LEVEL FILTERING

- OpenDNS Family Shield – Free DNS-based content filtering for your entire home network
- CleanBrowsing – Family-friendly DNS that blocks adult content across all devices

THE TRUST CONVERSATION: Monitoring should be transparent, not secretive. Tell your child: "I'm using these tools because keeping you safe is my job. As you get older and show responsibility, we'll adjust the level of oversight together."

07 CELL PHONE & TABLET SAFETY

Before handing over a new device, take 30 minutes to set it up properly. It's much easier to configure safety settings from the start than to retroactively lock things down.



NEW DEVICE SETUP CHECKLIST

- [ ] Create the account using your email as the recovery address
- [ ] Enable parental controls (Screen Time / Family Link)
- [ ] Set app store to require approval for downloads
- [ ] Disable in-app purchases or require password/PIN
- [ ] Turn off location services for all apps except Find My / Family sharing
- [ ] Set up content restrictions (explicit content, web filtering)
- [ ] Configure Do Not Disturb / Focus modes for school and bedtime
- [ ] Disable Bluetooth and AirDrop from unknown contacts

LOCATION SHARING

Family location sharing (Find My iPhone, Google Family Link) can provide peace of mind without being invasive. Set it up as a two-way street — let your child see your location too. Frame it as a family safety tool, not surveillance.

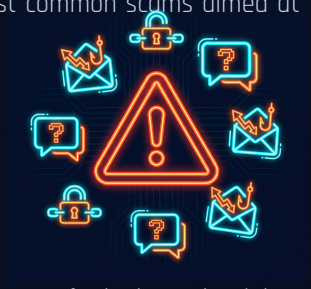
PUBLIC WIFI RISKS

When your child connects to WiFi at a friend's house, library, or coffee shop, their traffic may not be secure. Teach them to never log into important accounts on public WiFi.

BEDTIME DEVICE POLICY: Devices should charge overnight in a common area — not in the bedroom. This prevents late-night use, reduces sleep disruption, and removes the temptation to respond to messages at 2 AM.

08 PHISHING & SCAMS TARGETING FAMILIES

Scammers specifically target children because they're less likely to recognize manipulation. The most common scams aimed at this age group exploit their interests in gaming and social media.



SCAMS TARGETING STUDENTS

- "Free V-Bucks / Robux Generators" — Fake websites that promise free in-game currency in exchange for login credentials
- "You Won a Gift Card!" — Pop-ups or messages claiming they've won prizes that require clicking a link
- Fake giveaways from accounts impersonating YouTubers or streamers
- "Verify your account" emails that mimic legitimate platforms
- Friend requests from accounts that seem too good to be true

IF YOUR CHILD CLICKED A BAD LINK

Don't panic — and don't punish them for telling you. Take these steps immediately:

- Change passwords for any accounts that may be compromised
- Run a malware scan on the device
- Check for unauthorized purchases or account changes
- Enable 2FA on all accounts if not already active
- Monitor accounts for unusual activity over the next few weeks

CHILD IDENTITY THEFT: Children's Social Security numbers are valuable to criminals because theft often goes undetected for years. Consider placing a free credit freeze on your child's credit file through Equifax, Experian, and TransUnion.

09 HAVING THE CONVERSATION

The most powerful cybersecurity tool isn't software — it's communication. Children who feel safe talking to their parents about online problems are far more likely to report issues early.

CREATING A SAFE REPORTING ENVIRONMENT

- Establish a "no punishment for reporting" policy. If your child tells you about something scary online, your first response should be gratitude, not anger
- Avoid overreacting. If you take away their device every time they report a problem, they'll stop reporting
- Ask open-ended questions: "What's the most interesting thing you saw online today?" rather than "Were you on your phone again?"
- Share your own experiences — "I got a phishing email today, let me show you what it looked like"

REGULAR CHECK-INS

Schedule casual, low-pressure conversations about their online life. During car rides, at dinner, or during walks — not formal sit-downs that feel like interrogations. Ask about their favorite games, who they talk to online, and what's trending on their platforms.

FAMILY DIGITAL AGREEMENT

Create a written agreement together that covers which apps are approved, screen time limits, what information is never shared online, what to do if something makes them uncomfortable, and consequences for violations. Both parents and children should sign it. Review every 6 months.

A tear-out Family Digital Agreement template is included on page 14 of this guide.

10 EMERGENCY RESPONSE PLAN

When something goes wrong online, having a clear plan prevents panic and ensures the right steps are taken quickly.

IF YOUR CHILD IS BEING CYBERBULLIED

- Listen without judgment – let them tell you what happened
- Document everything – screenshots, messages, dates, usernames
- Do not respond to the bully or confront their parents directly
- Report to the school counselor and administration
- Report and block the bully on the platform
- If threats of violence are made, contact local law enforcement

IF YOUR CHILD SHARED INFO WITH A STRANGER

- Determine exactly what was shared (name, school, address, photos)
- Change all passwords immediately
- Block and report the individual on the platform
- If location information was shared, increase awareness of surroundings
- Report to local law enforcement if the interaction was predatory

IF YOU SUSPECT GROOMING

- Do not confront the individual – this may cause them to destroy evidence
- Preserve all messages and communications
- Contact local law enforcement immediately
- Seek professional support for your child

11 RESOURCES FOR PARENTS

FREE CYBERSECURITY TRAINING

stealthblue.training

Free cybersecurity awareness training for adults from StealthBlue Cyber. Learn to protect yourself and your family with the same expertise trusted by businesses nationwide.

STUDENT CYBERSECURITY EDUCATION

stealthblueschool.com

Interactive cybersecurity training designed specifically for students. 9 chapters, quizzes, and hands-on tools to build digital safety skills.

REPORTING & CRISIS RESOURCES

- Cyberbullying Hotline: 1-800-420-1479
- Crisis Text Line: Text HOME to 741741
- StopBullying.gov – Federal resources for bullying prevention
- FBI Internet Crime Complaint Center: IC3.gov

EDUCATIONAL RESOURCES

- Common Sense Media (commonsensemedia.org) – Age-based reviews and ratings
- ConnectSafely (connectsafely.org) – Parent guides and tip sheets
- Family Online Safety Institute (fosi.org) – Research and best practices
- Cyberbullying Research Center (cyberbullying.org) – Evidence-based resources

FAMILY DIGITAL AGREEMENT

Our family agrees to the following rules for safe and responsible technology use.

APPROVED PLATFORMS & APPS

_____

_____

_____

SCREEN TIME LIMITS

School days: _____ hours | Weekends: _____ hours

Device-free times: _____

Device-free zones: _____

WE AGREE TO

- [ ] Never share personal information online (address, school name, phone number)
- [ ] Tell a parent immediately if something online makes us uncomfortable
- [ ] Not download apps without parent approval
- [ ] Keep passwords private (shared only with parents)
- [ ] Be kind and respectful in all online interactions
- [ ] Not meet anyone in person that we only know online
- [ ] Follow the screen time limits we've agreed upon
- [ ] Charge devices in a common area overnight

PARENTS AGREE TO

- [ ] Listen without judgment when our child reports an online problem
- [ ] Not punish our child for honestly reporting a mistake or concern
- [ ] Respect our child's growing need for privacy as they demonstrate responsibility
- [ ] Review and update this agreement together every 6 months
- [ ] Model good digital behavior ourselves

_____ _____

Student Signature / Date Parent Signature / Date

STEALTHBLUE

CYBER

DETECT | DEFEND | SECURE

stealthblue.com

For all your cybersecurity needs

stealthblue.training

Free cybersecurity training for adults

stealthblueschool.com

Cybersecurity education for students