



Back-to-School Online Safety Kit

30-Minute Plan for Parents

Elementary | Middle | High School

How to use this sheet

01

Pick your child's grade band and do the setup below
(10-15 min)

02

Have the talk using the short scripts
(5-10 min)

03

Post the rules on the fridge; review monthly.

Elementary (K-5)

Set up (10 min)

- 01** Turn on device controls:
 - **Apple:** **Screen Time** + **Communication Safety** (nudity detection in Messages).
 - **Android/Chromebook:** **Google Family Link** for app approvals, time limits, location.
- 02** Lock down game consoles: enable **Xbox, PlayStation, Nintendo** family controls for chat, purchases, and age ratings.

Teach (5 min)



If you didn't expect the link, don't tap it—bring it to me



If someone you don't know messages you, show me first

Red flags to watch

Pop-ups on the device, apps you didn't install, sudden "you're locked out" messages.

Follow FTC steps to
identify/report phishing

forward scam texts to **7726** (SPAM)

Practice and learn

Watch one short video/lesson together
each week

FBI Safe Online Surfing (grades 3-8)

NCMEC NetSmartz
(age-based videos/activities)

Middle School (6-8)

Set up (10-15 min)

- 01 Review **Family Link/Screen Time** limits; require approval for new apps/extensions.
- 02 On consoles, **restrict voice/text chat to friends only; disable purchases without a PIN**, set time limits.
- 03 Add a “pause-before-click” routine: kid screenshots suspicious messages and sends to you.

Talk track (5 min)



If a message feels urgent or offers free rewards, slow down and show me.



Before joining any group chat or server, ask: Do I know these people in real life?



Once you send a photo or comment, you lose control of it. Anyone can screenshot or forward it—even if you delete it.



Before you post or send, do the hallway test: would you be okay seeing it on a school screen with your name on it tomorrow?



Ask before posting someone else. Don't forward private photos or DMs.

2-minute demo

Have your child text you a harmless photo. In front of them, screenshot it and forward to your own email. Show how fast it leaves their hands.

Bullying playbook

Learn how to document, block, and report on each platform; post **StopBullying.gov - Get Help Now** by the family computer.

High School (9-12)

Hardening basics (10-15 min)

- Move to unique 16-character passwords + a password manager; enable MFA on email, school, banking, and social. (Follow [CISA Secure Our World tip sheet](#).)
- Walk through two scam examples together (job, “locked account”); practice verifying on a second channel. ([Use the FTC phishing guide](#).)

Digital footprint & permanence (2 min, monthly)

- Search their name + school together; review what’s public and tagged.
- **Reminder:** “Private accounts aren’t private to screenshots. Send only what you’re okay seeing again later.”

Reputation, money, identity

- **Quick search test:** Google their name + school; review public posts.
- **Banking/app rules:** never move money for others; no gift cards, crypto, or wire requests—ever. ([Classic scam tells per FTC](#).)
- Teens should know how to freeze a debit card in the banking app.

Isolation & radicalization (have the talk)

- Watch for withdrawal and “everyone’s against me” language. Ask what they think about the content they’re seeing (not just what it is).
- Use balanced guidance from [AACAP \(Facts for Families: Online Radicalization\)](#) and [PERIL/SPLC Parent Guide](#) to spot signs and respond.

If cyberbullying surfaces

Save screenshots with timestamps; block/mute; escalate via school policy; post [StopBullying.gov reporting steps](#) where your teen can find them.

Family Rules (post these)

- 01 Pause before you click.** If unexpected, don't open it—send me a screenshot. (Texts to **7726**; report scams at **ReportFraud.ftc.gov**.)
- 02 Ask before you download.** Apps, mods, and files must be parent-approved.
- 03 Keep it private.** No sharing full name, school, phone, or location without a parent.
- 04 Assume anything you send can be saved and shared.**
- 05 Ask before posting someone else;** never forward private photos or DMs.
- 06 When in doubt, bring it to me.** You won't lose your device for asking for help.

If Something Goes Wrong

Private photo or message was shared

- 01** Save screenshots with dates; don't retaliate.
- 02** Report in-app; ask the school to help if classmates are involved.
- 03** If an explicit image of a minor is involved, use **NCMEC's Take It Down** removal tool and file a CyberTipline report if there's pressure or threats.
- 04** Keep devices available and talk through next steps.

Clicked a bad link or download

- 01** Stop using the device.
- 02** Change the account password; turn on MFA.
- 03** If the password was reused, change it everywhere it's used.
- 04** Run updates and a malware scan; notify school if a school account is affected.
- 05** Report the **phish** (email → **reportphishing@apwg.org**; text → forward to 7726; any scam → **ReportFraud.ftc.gov**).

"Your account is locked" alerts

Don't click the message. Go to the site directly, sign in, reset if needed, review recent activity, and turn on MFA.

Lost or stolen phone

Use Find **My iPhone** / **Find My Device**; mark lost; change Apple ID/Google password; suspend service if needed.

Money requests / "help me buy gift cards"

Assume scam until verified on a second channel. No gift cards, crypto, or wires.