

SCREEN TIME TALKS



A Layered Approach to Screen Safety

*Controls you already have,
and where to find them.*

A guide to the parental controls built into your home internet,
your child's devices, their carrier, and the apps they use.

A Layered Approach to Screen Safety

Take Control.

Most parents don't know how much control they already have. Your home internet provider, your child's device manufacturer, their cell carrier, and many of the apps they use every day already have tools built in for exactly this – most families have just never been told they're there.

Two layers, in the order they're worth tackling:

- **Your Home Internet:** the shared pipe covering every device in the house, whether it's a phone or not – page 3.
- **Your Devices & Apps:** the phone itself, the cellular connection that follows it anywhere, and what runs on it – page 4.

Controls set the default, so good habits don't depend on willpower at the end of a long day.



Managing Your Home Internet

Tied to the house, not the child — covers every device on the home network, including consoles, TVs, and tablets that don't have their own phone line.

Provider	App	What It Covers
Spectrum ↗	My Spectrum App	pause WiFi per device and set schedules; Security Suite adds browsing protection.
AT&T ↗	Smart Home Manager	same app for AT&T Fiber or Internet Air (their fixed wireless); separate from Secure Family. Profiles, schedules, content filters, pause WiFi.
Verizon ↗	Verizon Home	covers Fios, 5G Home, and LTE Home the same way; separate from Verizon Family (mobile, next page). Content filters, SafeSearch, YouTube Restricted Mode, scheduled downtime.
Comcast / Xfinity ↗	Family Settings	pause WiFi per device, or set a named schedule (bedtime, homework, dinner, and more) that pauses automatically. Comcast's own data found "pause device" is the most-used feature, most often triggered right at dinnertime — the same no-screens-at-the-table habit from the full toolkit.
T-Mobile Home Internet ↗	(gateway app)	if this is your home internet, not just your phone plan — offers only basic pause-and-schedule controls, lighter than the paid FamilyMode most people associate with T-Mobile.
Frontier ↗	Secure by Frontier	parental controls bundled into their security add-on; Fiber customers with the included eero router can also use eero Secure.
Astound ↗	eero app (Whole Home WiFi)	profiles with scheduled pauses, plus pause for any single device. eero Plus (\$9.99/mo extra) adds finer site, app and content controls. Whole Home WiFi is included with 1 Gig and faster plans.
Surf Internet ↗	eero app	Surf installs eero WiFi; parental controls live in the eero app — profiles, schedules and pausing. Using your own router? Surf supports eero Pro, Google WiFi and Orbi.
NITCO ↗	WiFi+ (HomePass app)	\$12.95/mo add-on: a profile for each family member, access and usage limits, and a content manager that blocks unwanted sites and ads.

Availability varies by address. Many regional providers supply an eero router or their own app — look for "parental controls" or "WiFi management" on your provider's support site.

Managing Your Devices & Apps

Your Devices

ON THE DEVICE ITSELF — THE HARDEST LAYER TO BYPASS

Maker	App	What It Covers
Apple ↗	Screen Time	built into iOS — hardest for kids to bypass on an iPhone or iPad.
Google ↗	Family Link	the cross-device equivalent for Android — works on Samsung, Pixel, and other Android phones and tablets.
Samsung ↗	Samsung Kids	a more restrictive layer on top of Android for younger children — a locked-down space with only parent-approved apps, best for kids under 7.
Motorola ↗	Family Space	turns a parent's own phone into a temporary walled garden of approved apps before handing it over — not just a child's own device. Also includes Family Hub for screen time and location across up to 5 family members.

ON THE CELLULAR CONNECTION — FOLLOWS THE DEVICE ANYWHERE

Carrier	App	What It Covers
Verizon ↗	Verizon Family	(recently renamed from Verizon Smart Family) location, content filters, internet pause.
T-Mobile ↗	FamilyMode	usage, location, and content filtering across a child's devices (fees may apply — \$10/mo).
AT&T ↗	Secure Family	similar controls; works across carriers, not just AT&T.

If your plan is a reseller (Mint, Spectrum Mobile, and others): these apps require being a direct customer of that carrier brand, not just using their network. Mint (on T-Mobile's towers) and Spectrum Mobile (on Verizon's) don't automatically get the host's app. Spectrum Mobile has its own separate controls; Mint's "kids" plan has none and just points to Google Family Link. Check your specific provider, not the network it runs on.

Your Apps

Built into TikTok, Instagram, Snapchat, and others — useful as a backup, not a foundation. These safety features fail at least half the time. Full breakdown on the next page.

Platforms pushing your family around? Push back — every layer here is already in your hands, the same guardrails Meta was just forced to add by court order.

Parental Controls & App Risk

A June 2026 study by the Cybersafety Research Center (NYU and Northeastern University) tested 86 advertised child-safety features across Instagram, Snapchat, TikTok, and YouTube. Every platform failed at least half the time:



Platform	Risk	Available Controls
YouTube ↗	Algorithm can escalate toward harmful content	Family Link — content restrictions, watch history, screen time limits
TikTok ↗	Personal data collection, escalating algorithm	Family Pairing (strongest available) — limits, DM restrictions, Restricted Mode
Instagram ↗	Encourages sharing personal info; algorithm can push harmful content	Teen Accounts (default under 18) — private by default, DM restrictions, Family Center
Snapchat ↗	Disappearing content is a common vector for cyberbullying/sexting	Family Center — friend lists, time breakdowns; can't see message content
Discord ↗	Per-channel rules vary; some allow cybercrime/adult content	Family Center shows who a teen talks to; can't see message/call content
Roblox	User-generated games may be inappropriate; allows DMs with strangers	Limited platform-wide parental tools; varies by experience
WhatsApp	Scams, malware, cyberbullying common	Very limited — parent-managed only for new under-13 accounts
WeChat / Kik / Whisper	Anonymity and location features raise grooming/stranger-contact risk	Minimal to none
X (Twitter) / Reddit	General platform risk	No dedicated parental supervision system

Structural limitation worth naming: nearly every one of these tools requires the teen's active participation, and the teen can typically disable it unilaterally — only a notification is sent back to the parent.

A new layer: Instagram now alerts supervising parents if a teen repeatedly searches suicide or self-harm terms — only for accounts already enrolled in supervision, and without revealing the exact terms. Worth deciding in advance how you'd want to respond if you ever received one.

Whatever mix of controls you choose, write it down. The Find Your Focus exercise is also where your family can set its own usage guidelines, together — before you need to enforce them. This is also the last stop before the close: everything up to here has been about understanding and habits — this page, and the one before it, are the technical backstop.