PARENTAL
DEVICE & APP SECURITY
CHECKLIST

THE 30-MINUTE GUIDE THAT COULD PREVENT A LIFETIME OF TRAUMA

Think your parental controls are working?
Most parents do—until it's too late.

This guide gives you exactly what you need to secure every device in your home: phones, tablets, gaming consoles, smart TVs, and browsers. No technical jargon. No fluff. Just clear, actionable steps that take 30 minutes to complete.

⚠️ **WARNING:** Partial protection is false protection. Completing 7 out of 10 steps leaves the door wide open. This checklist must be completed in full, on every device, for every child.

TABLE OF CONTENTS

SECTION 1: SMARTPHONES

iPhone & Android Devices

Smartphones are the primary device used for online contact, app downloads, and image sharing. This section must be completed first—and rechecked monthly.

FOR IPHONE USERS:

Step 1: Enable Screen Time

- Go to Settings → Screen Time → Turn On Screen Time
- Tap This is My Child's iPhone
- Set a Screen Time Passcode (different from device passcode)

Step 2: Set Content & Privacy Restrictions

- In Screen Time, tap Content & Privacy Restrictions → Enable
- Under iTunes & App Store Purchases:
    - Set Installing Apps to Don't Allow
    - Set Deleting Apps to Don't Allow
    - Set In-App Purchases to Don't Allow

Step 3: Restrict Explicit Content

- Under Content Restrictions:
    - Set Music, Podcasts & News to Clean
    - Set Music Videos to Off
    - Set Movies to age-appropriate rating
    - Set TV Shows to age-appropriate rating
    - Set Books to Clean
    - Set Apps to age-appropriate rating

Step 4: Disable Web Content

- Under Content Restrictions → Web Content
- Select Limit Adult Websites
- Manually add dangerous sites to Never Allow list (see Section 8)

Step 5: Turn Off Location Services

- Go to Settings → Privacy & Security → Location Services
- Review each app individually
- Set social media apps to Never or Ask Next Time
- Keep Find My iPhone enabled for safety

Step 6: Disable AirDrop from Everyone

- Go to Settings → General → AirDrop
- Set to Contacts Only or Receiving Off

Step 7: Restrict Siri & Game Center

- In Screen Time → Content & Privacy Restrictions → Allowed Apps
- Turn off Siri & Dictation (prevents voice bypass)
- Review Game Center settings: disable Add Friends and Connect with Friends

Step 8: Set Communication Limits

- In Screen Time → Communication Limits
- Set During Screen Time to Contacts Only
- Set During Downtime to Specific Contacts (family only)

Step 9: Review App Permissions Weekly

- Go to Settings → Privacy & Security
- Review Camera, Microphone, Photos, Contacts
- Disable access for any suspicious or unnecessary apps

Step 10: Install Family Sharing

- Go to Settings → [Your Name] → Family Sharing
- Add your child as a family member
- Enable Ask to Buy so all purchases require your approval

FOR ANDROID USERS:

Step 1: Enable Parental Controls in Google Play

- Open Google Play Store
- Tap your profile icon → Settings → Family → Parental Controls
- Turn on and set a PIN (do not share with child)
- Set age-appropriate content ratings for Apps, Games, Movies, TV, Books

Step 2: Set Up Google Family Link

- Download Google Family Link on your phone and your child's phone
- Follow setup to link devices
- Enable Require Approval for Downloads
- Set screen time limits and bedtime schedules

Step 3: Restrict App Installations

- On child's device: Settings → Security → Install Unknown Apps
- Disable this for ALL apps (Chrome, Files, etc.)
- This prevents sideloading apps that bypass Google Play

Step 4: Enable SafeSearch & Restricted Mode

- Open Chrome → Settings → Search Engine → Manage Search Engines
- Ensure Google is default and SafeSearch is locked (via Family Link)
- Open YouTube → Settings → General → Enable Restricted Mode

Step 5: Disable Unknown Sources

- Settings → Apps → Special App Access → Install Unknown Apps
- Ensure every app listed is set to Not Allowed

Step 6: Turn Off Location for Apps

- Settings → Location → App Location Permissions
- Review each app individually
- Set social media apps to Deny or Ask Every Time

Step 7: Disable File Sharing & Bluetooth

- Settings → Connected Devices → Connection Preferences
- Turn off Nearby Share
- Set Bluetooth to Off when not needed
- Disable Receive Files via Bluetooth

Step 8: Lock Down Google Account Settings

- On child's device, open Settings → Google → Manage Your Google Account
- Under Data & Privacy, review Web & App Activity
- Under People & Sharing, disable contact sharing options

Step 9: Review App Permissions Weekly

- Settings → Privacy → Permission Manager
- Review Camera, Microphone, Files and Media, Contacts
- Remove access from suspicious apps immediately

Step 10: Install Device Monitoring App

- Consider installing monitoring software like:
    - Qustodio
    - Bark
    - Net Nanny
- Configure to receive alerts for flagged content or risky behavior

SECTION 2: TABLETS

iPad & Android Tablets

Tablets often fly under the radar because they're 'just for homework' or 'just for games.' Wrong. Every access point must be secured.

Step 1: Apply the Same Smartphone Steps

- Follow all iPhone or Android smartphone steps listed in Section 1
- Tablets require identical protections—no exceptions

Step 2: Disable Browser Private/Incognito Mode

- Most parental controls don't block private browsing by default
- iPad: Use Screen Time → Content Restrictions → Web Content → Allowed Websites Only
- Android: Use Family Link or third-party browser controls
- Consider removing Chrome and Safari entirely; use only supervised browsers

Step 3: Remove Social Media Apps

- Unless absolutely necessary, remove Instagram, TikTok, Snapchat from tablets
- These apps are harder to monitor on tablets than phones
- If must keep, apply strictest privacy settings (see Section 8)

Step 4: Lock Down App Store

- Require password/biometric for every download
- Enable Ask to Buy (Apple) or Require Approval (Google)
- Review download history weekly

Step 5: Disable In-App Browsers

- Many apps (TikTok, Instagram, Discord) have hidden browsers
- These bypass parental controls entirely
- Solution: Restrict or remove apps with embedded browsers
- Monitor screen time reports for unusual activity

Step 6: Set Downtime & App Limits

- Use Screen Time (iOS) or Family Link (Android)
- Set Downtime for nighttime hours (e.g., 9 PM - 7 AM)
- Limit specific app categories (Social, Games, Entertainment)
- Only allow Always Allowed apps: Messages, Phone (if applicable), and educational tools

Step 7: Secure Multi-User Settings (Android)

- Android tablets allow multiple user profiles
- Settings → System → Multiple Users
- Disable Add Users to prevent secondary unmonitored accounts
- Check for hidden guest profiles

Step 8: Disable Split-Screen & Picture-in-Picture

- These features allow hidden app usage during 'homework time'
- Android: Settings → System → Developer Options → Disable Force Activities to be Resizable
- Monitor for apps running in background

Step 9: Enable Device Location Tracking

- iPad: Find My → Enable Find My iPad
- Android: Google Find My Device → Enable
- This allows recovery if device goes missing

Step 10: Conduct Weekly Reviews

- Check Screen Time reports every Sunday
- Review app usage, web history, and downloads
- Have a 5-minute conversation about what they used the device for

SECTION 3: GAMING CONSOLES

Xbox, PlayStation, Nintendo Switch

Gaming consoles have messaging, voice chat, and browsers. Predators know this. Most parents don't monitor consoles at all—making them a primary grooming tool.

FOR XBOX:

Step 1: Create a Child Account

- Go to account.microsoft.com/family
- Add your child as a family member
- Set their correct birthdate (this determines restrictions)

Step 2: Set Privacy & Online Safety Settings

- On Xbox: Settings → Account → Privacy & Online Safety
- Set to Child Defaults or customize:
    - You can communicate outside of Xbox with voice & text: Block
    - You can communicate with voice & text: Friends Only
    - Others can communicate with voice & text: Friends Only
    - You can share content: Block

Step 3: Disable Web Browser

- Xbox has Microsoft Edge browser built-in
- Settings → Privacy & Online Safety → Xbox Privacy
- Under View details & customize → Communication & multiplayer
- Block ability to use Web Browser or restrict entirely

Step 4: Restrict Game Content

- Settings → Account → Privacy & Online Safety
- Set age-appropriate content filters for games
- Block Mature (M) and Adults Only (AO) rated games

Step 5: Disable Friend Requests from Strangers

- Privacy & Online Safety → Xbox Privacy → View Details & Customize
- Under Communication & multiplayer:
    - Others can add you as a friend: Block or Friends of Friends
    - You can add friends: Friends of Friends (prevents random adds)

Step 6: Monitor Messages & Activity Reports

- Visit account.microsoft.com/family on your device
- View weekly activity reports showing game time, communication, and content
- Review message history monthly

Step 7: Set Screen Time Limits

- In Microsoft Family Settings online or app
- Set daily time limits for Xbox usage
- Schedule gaming-free hours (e.g., school nights after 9 PM)

Step 8: Disable Purchases & Gift Cards

- Settings → Account → Privacy & Online Safety
- Under Buying & downloading:
    - Require password/approval for all purchases
    - Block gift card redemption without parent approval

Step 9: Turn Off Voice Chat by Default

- Settings → General → Volume & Audio Output → Party Chat Output
- Set mic to muted on startup
- Discuss why voice chat with strangers is dangerous

Step 10: Check for Hidden Accounts

- Confirm child is logged into their supervised account
- Look for secondary profiles on the console
- Remove any unrecognized profiles immediately

FOR PLAYSTATION:

Step 1: Create a Family Manager Account

- Go to Settings → Family and Parental Controls
- Set yourself as Family Manager
- Add child as family member with correct birthdate

Step 2: Restrict Communication Features

- Settings → Family and Parental Controls → Select child's account
- Under Communication with Other Players:
    - Set to Not Allowed or Friends Only
    - Block User-Generated Content
    - Block PlayStation Messages from Non-Friends

Step 3: Disable Web Browser & Media Features

- PlayStation has a web browser and media apps
- Under Parental Controls → Web Browser: Restrict
- Block access to PlayStation Store unless supervised
- Disable Internet Browser startup

Step 4: Set Age Restrictions for Games

- Family and Parental Controls → Child's account → Age Level for Games
- Set appropriate age restriction (e.g., 13 and under cannot play M-rated games)
- Block Use of PlayStation VR if too young

Step 5: Require Spending Limit Approvals

- Under Parental Controls → Monthly Spending Limit
- Set to $0 or very low amount
- Require parent approval for all purchases

Step 6: Disable Friend Requests

- Settings → Family and Parental Controls → Child account
- Under Communication with Other Players:
    - Friend Requests: Not Allowed or Friends of Friends Only

Step 7: Turn Off Automatic Sign-In

- Settings → Users and Accounts → Login Settings
- Disable Enable Automatic Login
- Require parent to log child in (provides checkpoint)

Step 8: Review Activity Logs

- PlayStation provides limited activity reporting
- Manually review Trophies, Recently Played, and Friends List weekly
- Ask child to show you their message inbox

Step 9: Disable Streaming & Broadcasts

- Settings → Sharing and Broadcasts
- Disable Video Clips and Screenshots sharing
- Turn off Broadcast Gameplay (prevents exposure to strangers)

Step 10: Monitor Voice Chat

- PlayStation allows voice chat through headsets
- Set rule: no voice chat with non-family members
- Consider disabling headset jack or using single-player games only

FOR NINTENDO SWITCH:

Step 1: Download Nintendo Switch Parental Controls App

- Download Nintendo Switch Parental Controls app on your smartphone
- Link to your child's Switch console via pairing code
- This gives you remote monitoring and controls

Step 2: Set Age Restrictions

- In the app: Restriction Level → Set based on child's age
- Options: Child, Pre-Teen, Teen, Adult
- This blocks games, content, and features inappropriate for age

Step 3: Restrict Social Features

- On Switch console: System Settings → Parental Controls
- Posting to Social Media: Restricted
- Communication with Others: Restricted
- Screenshot/Video Sharing: Restricted or Off

Step 4: Disable Nintendo eShop Purchases

- Parental Controls → Restriction of Nintendo eShop Purchases
- Set to Restricted
- Require password for any purchase attempt

Step 5: Enable Play Time Limits

- Use Parental Controls app to set daily time limits
- App will notify you when limit is reached
- Console can be set to suspend software when time is up

Step 6: Monitor Play Activity

- Parental Controls app shows:
  - Games played
  - Total play time
  - Daily/monthly summaries
- Review weekly and discuss with child

Step 7: Restrict Friend Codes

- Nintendo Switch uses Friend Codes for online connection
- Tell child: never share Friend Code with anyone outside family/ school friends
- Review Friends List regularly
- Delete any unknown users immediately

Step 8: Turn Off Voice Chat Apps

- Switch doesn't have built-in voice chat, but some games integrate with apps
- Do not allow Discord, Nintendo Switch Online app, or other voice services on child's device
- If necessary, use only under supervision

Step 9: Disable YouTube & Other Apps

- Switch has YouTube and Hulu available
- These can expose child to inappropriate content
- Remove these apps or use parental controls to block

Step 10: Check for Secondary User Profiles

- Switch allows multiple user profiles on one console
- System Settings → Users → Review all profiles
- Delete any unrecognized or 'guest' profiles

SECTION 4: SMART TVs & STREAMING DEVICES

Roku, Fire TV, Apple TV, Chromecast, Smart TV Apps

Smart TVs have web browsers, app stores, and social features. They also have YouTube, which is one of the most common grooming platforms. Don't ignore this section.

Step 1: Enable Parental Controls on Streaming Services

- Netflix: Account → Profile & Parental Controls → Set Maturity Rating → Require PIN
- Disney+: Profile → Edit Profiles → Set Content Rating
- Hulu: Account → Profiles → Kids Profile (locks mature content)
- Amazon Prime Video: Account → Parental Controls → Set Viewing Restrictions → Create PIN

Step 2: Restrict YouTube Access

- YouTube is not safe for unsupervised use—even with Restricted Mode
- Option 1: Use YouTube Kids app only (for younger children)
- Option 2: Enable Restricted Mode in YouTube settings (limited effectiveness)
- Option 3: Remove YouTube entirely and allow only on supervised devices
- Best Practice: No YouTube on Smart TV unless parent is present

Step 3: Disable Web Browsers on Smart TVs

- Most Smart TVs have built-in browsers (Samsung Internet, LG Browser)
- These bypass all parental controls
- Solution: Delete/hide browser app if possible, or restrict via device PIN
- Check TV settings under Apps or Application Manager

Step 4: Set Up Device PINs

- Roku: Settings → Parental Controls → Create PIN → Require PIN for purchases and mature content
- Fire TV: Settings → Preferences → Parental Controls → Turn On → Set PIN
- Apple TV: Settings → General → Restrictions → Enable Restrictions → Set Passcode
- Chromecast/Google TV: Limited parental controls—monitor through Family Link

Step 5: Restrict App Downloads

- Prevent installation of unapproved apps
- Require parent approval or PIN for any new app installation
- Review installed apps monthly—remove any that look suspicious or unfamiliar

Step 6: Disable Voice Assistants (Alexa, Google Assistant)

- Voice commands can bypass restrictions
- Fire TV: Settings → Alexa → Disable or restrict
- Google TV/Chromecast: Settings → Google Assistant → Turn Off or limit

Step 7: Turn Off Screen Mirroring/Casting from Unknown Devices

- Prevents others from streaming content to your TV
- Check TV network settings for Screen Mirroring, Miracast, or AirPlay
- Set to Require Permission or Off

Step 8: Review Viewing History Weekly

- Check Continue Watching or Recently Watched on streaming apps
- Look for content you didn't approve
- Ask your child what they watched and why

Step 9: Set Time Limits

- Many streaming devices lack built-in time limits
- Solution: Use router-based parental controls (see Section 5)
- Or set physical rules (e.g., TV off after 8 PM, no TV in bedrooms)

Step 10: Remove TVs from Bedrooms

- Bedrooms should not have unsupervised screen access
- Keep TVs in common areas only
- If child has TV in room, remove streaming/smart features—use for gaming console only (with restrictions)

SECTION 5: COMPUTERS & BROWSERS

Windows, Mac, Chromebook, and Browser Security

Computers are used for homework—and for everything else. If you're not monitoring browser history, downloads, and app installations, you're leaving your child completely exposed.

FOR WINDOWS COMPUTERS:

Step 1: Set Up a Child Account via Microsoft Family

- Go to account.microsoft.com/family
- Add your child as a family member
- Ensure they log in with this account (not a local account)

Step 2: Enable Activity Reporting

- In Microsoft Family settings online:
- Turn on Activity Reporting
- Review weekly reports showing:
    - Websites visited
    - Apps and games used
    - Screen time totals

Step 3: Set Screen Time Limits

- In Microsoft Family → Screen Time
- Set daily time limits for computer use
- Set schedule (e.g., no computer access after 9 PM on school nights)

Step 4: Enable Web Filtering

- Microsoft Family → Content Filters
- Turn on Filter inappropriate websites and searches
- Block specific sites manually under Blocked sites
- Only allow listed websites (if stricter control needed)

Step 5: Restrict App and Game Downloads

- Microsoft Family → Apps, games & media
- Turn on Needs approval to buy things
- Block inappropriate apps and games by age rating

Step 6: Install Antivirus Software

- Windows Defender is built-in and sufficient
- Ensure Real-time protection is enabled
- Run weekly scans for malware/spyware
- Consider additional software: Norton Family, Kaspersky Safe Kids

Step 7: Disable Private/Incognito Browsing

- Microsoft Edge: Managed via Family Safety settings (limited)
- Chrome: Use browser extensions like Incognito Killer or enforce supervised profile
- Firefox: Use parental control add-ons
- Best Solution: Regularly check history; discuss why private browsing is off-limits

Step 8: Remove Admin Privileges

- Ensure child's account is a Standard User, not Administrator
- Settings → Accounts → Family & other users
- Check account type—change to Standard if needed
- This prevents unauthorized software installation

Step 9: Review Installed Programs Monthly

- Settings → Apps → Installed Apps
- Look for unfamiliar programs, especially:
    - VPNs (can bypass filters)
    - Vault apps (Calculator+, Hide It Pro)
    - Tor Browser (dark web access)
- Uninstall immediately

Step 10: Check Browser Extensions

- Open Microsoft Edge or Chrome
- Go to Extensions page (three dots → Extensions)
- Remove any unfamiliar or suspicious extensions
- Extensions can hide activity or disable parental controls

FOR MAC COMPUTERS:

Step 1: Create a Managed User Account

- System Settings → Users & Groups
- Click the lock icon and add a new user
- Select Standard account (not Administrator)
- Enable Parental Controls

Step 2: Enable Screen Time

- System Settings → Screen Time
- Turn on Screen Time for child's account
- Set daily time limits and downtime schedules
- Use App Limits to restrict specific categories

Step 3: Set Content & Privacy Restrictions

- In Screen Time → Content & Privacy
- Restrict:
    - Explicit content in Music, Podcasts, Books
    - Web content (Limit Adult Websites or Allowed Websites Only)
    - App downloads and deletions
    - Siri web searches

Step 4: Monitor Web Activity

- Screen Time provides web history reports
- Review Most Used Websites weekly
- Check Safari history directly (do not rely solely on Screen Time)

Step 5: Restrict Safari & Browsers

- Screen Time → Content & Privacy → Allowed Apps
- Consider turning off Safari and installing only supervised browsers
- Or use Content & Privacy → Web Content → Allowed Websites Only

Step 6: Disable Private Browsing in Safari

- Screen Time → Content & Privacy → Content Restrictions → Web Content
- Set to Limit Adult Websites or Allowed Websites Only (disables private mode)
- For Chrome/Firefox: Use extensions or remove browsers entirely

Step 7: Review App Installations

- Finder → Applications
- Look for unfamiliar apps
- Check for VPNs, Tor, vault apps, or remote access software
- Delete immediately if found

Step 8: Check Login Items & Background Apps

- System Settings → General → Login Items
- Remove any suspicious apps that launch at startup
- Check Activity Monitor for unknown running processes

Step 9: Enable FileVault & Password Protection

- System Settings → Privacy & Security → FileVault
- Turn on FileVault to encrypt disk
- Require password immediately after sleep/screensaver starts

Step 10: Review Browser Extensions & Plugins

- Safari: Settings → Extensions
- Chrome/Firefox: Visit Extensions page
- Remove anything unfamiliar or that promises 'privacy' or 'ad-free browsing'

FOR CHROMEBOOKS:

Step 1: Add Child to Google Family

- Go to families.google.com
- Add your child as a supervised user
- They must log in with this Google account on the Chromebook

Step 2: Enable Family Link Supervision

- On Chromebook, child logs in with supervised Google account
- This automatically applies Family Link controls
- Manage settings via Family Link app on your phone

Step 3: Set Screen Time Limits & Bedtime

- In Family Link app → Child's device
- Set daily time limits
- Set bedtime (device locks during these hours)
- Remotely lock device anytime from your phone

Step 4: Enable SafeSearch & Site Blocking

- Family Link → Filters on Google Search → Enable
- Block specific websites manually under Manage sites
- Set Chrome to Try to block mature sites

Step 5: Restrict Chrome Extensions

- Family Link → Permissions → Chrome Extensions
- Set to Require approval for all extensions
- Review and remove any installed extensions monthly

Step 6: Monitor Activity Reports

- Family Link provides weekly activity reports
- Shows apps used, websites visited, screen time
- Review every week without fail

Step 7: Disable Guest Mode

- Chromebook allows Guest browsing (unmonitored)
- Settings → Security and Privacy → Manage other people
- Turn off Enable Guest browsing

Step 8: Restrict Android Apps (if available)

- Some Chromebooks run Android apps from Google Play
- Use same restrictions as Android devices (Section 1)
- Many Android apps bypass Chrome's parental controls

Step 9: Disable Developer Mode

- Developer Mode allows complete bypass of restrictions
- Check keyboard for suspicious key combinations being pressed
- If Developer Mode is on, device shows warning at startup—reset immediately

Step 10: Check for Linux Installation

- Chromebooks can run Linux (command line access)
- Settings → Advanced → Developers
- Ensure Linux development environment is OFF

SECTION 6: HIDDEN & VAULT APPS DETECTION

How to Find What Your Child Is Hiding

Hidden apps, vault apps, and disguised apps are specifically designed to help children hide photos, messages, and browsing activity from parents. If you find these apps, it's a red flag. Don't panic—but take action immediately.

What Are Vault Apps?

- Apps disguised as calculators, utilities, or games
- Store hidden photos, videos, messages
- Require secret passcodes to access
- Examples: Calculator+, Hide It Pro, Vaulty, Private Photo Vault

Step 1: Search for Common Vault App Names

- Look through all installed apps on every device
- Search for these keywords:
    - Calculator (multiple calculator apps is suspicious)
    - Vault
    - Hide
    - Private
    - Secret
    - Locker

Step 2: Look for Duplicate Apps

- Two calculator apps?
- Two photo gallery apps?
- Two file manager apps?
- One is likely a disguise

Step 3: Check for Apps with Generic Icons

- Vault apps often use generic icons (gear, folder, document)
- Apps with names like "Utilities" or "Manager" or "System"
- If you don't recognize it, investigate

Step 4: Review Recently Downloaded Apps

- iPhone: App Store → Profile → Purchased → [Child's name]
- Android: Google Play → Menu → My apps & games → Installed
- Check download dates—anything suspicious or unfamiliar?

Step 5: Search App Store for "Vault" and "Hide"

- Open App Store/Google Play on child's device
- Search "vault app" or "hide photos"
- If previously downloaded apps appear in results, they've used them before

Step 6: Check Storage Usage

- Vault apps take up storage space
- iPhone: Settings → General → iPhone Storage
- Android: Settings → Storage
- Look for apps using large amounts of data with generic names

Step 7: Look for Apps That Request Excessive Permissions

- Why does a "calculator" need access to your photos, contacts, and camera?
- Check permissions regularly (see previous sections)

Step 8: Test Suspicious Apps

- Open any suspicious app
- Try entering common vault passcodes: 0000, 1234, birthdate
- If it opens a hidden vault, you've found it

Step 9: Check for "App Hiders"

- Some apps hide other apps from the home screen
- iPhone: Search in App Library or Settings → Screen Time → See All App Activity
- Android: Settings → Apps → See all apps (shows hidden apps)

Step 10: Have a Direct Conversation

- If you find vault apps, don't yell
- Ask calmly: "I found this app. Help me understand why you felt you needed it."
- Explain why hiding things creates danger, not privacy
- Remove app together and discuss trust

Common Vault & Hidden Apps to Watch For:

- Calculator+ (and variants)
- Hide It Pro (Audio Manager icon)
- Vaulty
- Private Photo Vault
- Best Secret Folder
- KeepSafe
- Locker
- Gallery Vault
- Smart Hide Calculator
- Secret Calculator

SECTION 7: WEEKLY MONITORING ROUTINE

The 15-Minute Check That Could Save Your Child

Protection isn't a one-time setup. It's an ongoing practice. Commit to these weekly checks—they take 15 minutes and provide critical visibility into your child's digital life.

EVERY SUNDAY EVENING (or choose your day):

1. Review Screen Time Reports (5 minutes)

- iPhone: Settings → Screen Time → See All Activity
- Android: Family Link app → Child's device → Today
- Windows/Mac: Microsoft Family or Screen Time reports
- Look for:
    - Sudden spikes in usage
    - Apps you don't recognize
    - Late-night activity

2. Check Browser History (3 minutes)

- Open Safari, Chrome, Edge on all devices
- Look for:
    - Deleted history (suspicious)
    - Social media sites if not allowed
    - Chat platforms, anonymous sites
    - Search terms related to hiding apps, bypassing controls

3. Review Recently Downloaded Apps (2 minutes)

- Check App Store/Google Play purchase history
- Any new apps? Why were they downloaded?
- Delete anything unapproved immediately

4. Scroll Through Photos & Videos (2 minutes)

- Quick scroll through camera roll
- Look for:
    - Screenshots of conversations (may indicate issues)
    - Inappropriate images
    - Photos of documents (could be hiding something)

5. Spot-Check Messages (3 minutes)

- If age-appropriate, do random message checks
- Look for:
    - Conversations with unknown contacts
    - Numbers instead of names (hidden contacts)
    - Deleted message threads (red flag)

3. Review Recently Downloaded Apps (2 minutes)

- Check App Store/Google Play purchase history
- Any new apps? Why were they downloaded?
- Delete anything unapproved immediately

MONTHLY TASKS:

1. Update All Devices & Apps

- Security updates patch vulnerabilities
- Keep parental control apps updated

2. Change Parental Control Passcodes

- Kids share passcodes with friends
- Change yours monthly

3. Review Friends Lists (Gaming, Social Media)

- Xbox, PlayStation, Switch: Check friends lists
- Social media (if allowed): Review followers/following
- Remove unknown accounts

4. Conduct a "Find the Vault App" Search

- Follow Section 6 steps
- Look for newly downloaded hiding apps

5. Have a Digital Safety Conversation

- Use questions from Appendix
- Keep it casual, non-accusatory
- Reinforce that you're here to help, not punish

SECTION 8: RED FLAG APPS REFERENCE

Apps That Put Your Child at Risk

These apps are commonly used for dangerous contact, hiding activity, or sharing inappropriate content. If you find these on your child's device, take immediate action.

🚨 HIGHEST RISK - Remove Immediately:

1. Omegle (if still operational)

- Random video chat with strangers
- No moderation, high exposure to explicit content

2. Whisper

- Anonymous secret-sharing
- Location-based, connects users nearby
- High grooming risk

3. Kik

- Messaging app not tied to phone number
- Unmoderated group chats
- Commonly used by predators

4. Yubo

- Called "Tinder for teens"
- Live streaming with strangers
- Swipe-to-connect features

5. MeetMe

- Dating/hookup features
- Location sharing
- Adult content common

6. ChatRoulette / Chatrandom

- Random video chat
- High explicit content exposure

7. Telegram

- Encrypted messaging
- Secret chats with self-destruct
- Hard to monitor, easy to hide

8. Discord (without supervision)

- Can be safe for gaming groups WITH oversight
- But also has unmoderated servers
- Private DMs not visible to parents
- Voice chat with strangers

⚠️ VAULT APPS - Designed to Hide Content:

9. Calculator+ / Calculator% / Calculator#

- Looks like calculator, hides photos/videos

10. Hide It Pro (Audio Manager icon)

- Disguised as music app
- Hides photos, videos, messages, apps

11. Vaulty

- Photo/video vault with decoy passwords

12. Private Photo Vault / Keepsafe

- Hides images behind passcode

13. Best Secret Folder

- Hides files, photos, contacts

⚠️ HIGH-RISK SOCIAL MEDIA:

14. Snapchat

- Disappearing messages create false sense of safety
- Snap Map shows location
- Easy to share images that can be screenshotted
- "My Eyes Only" feature hides content

15. Instagram

- DMs with strangers if account is public
- Anonymous question features (story boxes)
- Explore page can show inappropriate content

16. TikTok

- DMs with strangers
- Dangerous viral challenges
- Exposure to mature content via algorithm
- Live streaming features

17. Snapchat Spotlight / Instagram Reels / TikTok

- Public posting features expose kids to strangers
- Comments and DMs from unknown accounts

⚠️ ANONYMOUS APPS:

18. Yik Yak (if active in your area)

- Anonymous local messaging
- Often used for cyberbullying and threats

19. ASKfm / NGL (Anonymous Q&A)

- Anonymous question apps
- High cyberbullying and harassment risk

20. Lipsi / Sendit

- Anonymous messages via Snapchat/Instagram
- Used for bullying and inappropriate questions

⚠️ DATING & HOOKUP APPS (Should NEVER be on minor's device):

21. Tinder, Bumble, Hinge

- Dating apps with age verification that doesn't work
- Minors lie about age

22. Grindr, Scruff, Her

- LGBTQ+ dating apps
- Should never be used by minors

23. Hoop, Wink

- Snapchat integration for meeting new people
- Essentially dating apps for teens

⚠️ GAMING & CHAT PLATFORMS (Monitor Closely):

24. Roblox

- Can be safe with strict privacy settings
- But has open chat, friend requests from strangers
- Inappropriate user-generated content common

25. Fortnite, Among Us, Minecraft (online modes)

- Voice and text chat with strangers
- Friend requests from unknown players
- Safe if limited to friends-only mode

26. VRChat, Rec Room

- Virtual reality social spaces
- Voice chat, avatar interaction
- Not suitable for young children

🚨 IMMEDIATE RED FLAGS - Call for Help:

27. Tor Browser

- Access to dark web
- Why would a child need this?

28. VPN Apps (without parent permission)

- Used to bypass parental controls and school filters
- Hides internet activity

29. Burner Phone Apps (TextNow, TextFree, Hushed)

- Gives child second phone number
- Used to hide communication

30. OnlyFans, Fansly (18+ content platforms)

- Should NEVER be on child's device
- If found, investigate immediately

WHAT TO DO IF YOU FIND THESE APPS:

1. Don't panic or yell
2. Screenshot app name and icon before deleting
3. Check app usage in Screen Time/Activity reports
4. Delete the app
5. Have a calm conversation about why it's dangerous
6. If app involved communication with strangers, see Section 9
7. If explicit content was shared, follow Emergency Response Plan (project files)

SECTION 9: WHAT TO DO IF YOU FIND SOMETHING

Emergency Response Protocol

IF YOU FIND INAPPROPRIATE CONTACT, SUSPICIOUS MESSAGES, OR EXPLICIT CONTENT:

⚠️ DO NOT:

- Delete anything yet
- Confront the other person
- Panic or accuse your child
- Post about it on social media
- Try to investigate on your own

✅ DO THIS IMMEDIATELY:

Step 1: Stay Calm

- Your child is not in trouble with you
- They may be a victim
- Your reaction determines if they'll tell you everything

Step 2: Take Screenshots (NO EXPLICIT IMAGES)

- Screenshot:
  - Usernames and account names
  - Message threads (avoid explicit images in screenshots)
  - Profile information
  - Dates and times
- DO NOT screenshot explicit images of minors (including your own child)

Step 3: Block the Person on All Platforms

- Block immediately to stop further contact
- Do not engage or threaten them

Step 4: Report to Platform

- Use built-in reporting tools on:
    - Instagram, Snapchat, TikTok, Discord, Xbox, PlayStation
- Report as: "Child safety" or "Harassment"

Step 5: Report to National Center for Missing & Exploited Children (NCMEC)

- Go to: https://report.cybertip.org
- File a CyberTipline report
- Include all screenshots (except explicit images)
- Provide as much detail as possible

Step 6: If Images Were Shared - Use Take It Down

- Go to: https://takeitdown.ncmec.org
- This stops images from being re-shared
- Creates a "hash" (digital fingerprint) without uploading the image
- Blocks image across major platforms

Step 7: Contact Your Child's School

- If incident involves classmates or school devices
- Ask to speak with school counselor or safeguarding lead
- School should follow their incident protocol (see project files: Incident_Reporting_Protocol.pdf)

Step 8: Contact Law Enforcement (If Necessary)

- Call police if:
    - Imminent danger or threats
    - Explicit images were shared or solicited
    - Suspect is adult
    - Blackmail or extortion occurred (sextortion)

Step 9: Seek Mental Health Support for Your Child

- Contact school counselor
- Find therapist specializing in digital trauma
- Call crisis lines:
    - Crisis Text Line: Text HOME to 741741
    - National Suicide Prevention Lifeline: 988
    - RAINN (sexual assault): 1-800-656-4673

Step 10: Change All Passwords & Secure Devices

- Change passwords on all accounts
- Enable two-factor authentication everywhere
- Review and apply all steps from Sections 1-5

Step 11: Have a Supportive Conversation

- Use phrases like:
    - "I'm so glad you told me."
    - "This is not your fault."
    - "We're going to handle this together."
    - "You're not in trouble."
- Ask: "Is there anything else I should know?"
- Reassure: "I'm here to protect you, not punish you."

IF YOUR CHILD IS BEING SEXTORTED:

- DO NOT PAY OR COMPLY - It won't stop
- Report immediately to FBI IC3: https://www.ic3.gov
- Report to CyberTipline: https://report.cybertip.org
- Contact local police
- Block all contact
- Use Take It Down: https://takeitdown.ncmec.org

IMPORTANT REMINDERS:

- Most children don't tell parents because they're scared of getting in trouble
- Approach with empathy, not anger
- The person who harmed your child is the problem—not your child
- You can recover from this with the right support

Key Resources:

- **CyberTipline:** https://report.cybertip.org
- **Take It Down:** https://takeitdown.ncmec.org
- **FBI IC3 (cyber crimes):** https://www.ic3.gov
- **Crisis Text Line:** Text HOME to 741741
- **988 Suicide & Crisis Lifeline:** Call or text 988
- **RAINN (sexual assault):** 1-800-656-4673