Child Safety Checklist for Parents

ALL THINGS SECURED

The first step to take with your child's cyber safety is to take inventory of every device they use to communicate or access the internet. You want as much visibility and control as possible.

Device Lockdown & Monitoring

☐	Set up a family account and create separate child accounts for each child.
☐	Set all necessary adult accounts as "Parent/Legal Guardian"
☐	Ensure that the Screen Time Passcode (iOS) or Parent Access Code (Android) is different than the device PIN code.
☐	Turn on Find My (iOS) or Find My Device (Android) for all child devices
☐	Turn off unnecessary location data (Privacy & Security —> Location Services)
☐	Set up Screen Time limits and restrictions
☐	Block all new app installs & in-app purchases without approval
☐	Set Communication Limits (only messaging with contacts)
☐	Set age-appropriate content restrictions
☐	For easier-to-use controls, consider downloading Qustodio (paid)
☐	Consider purchasing camera covers for each device (paid)

Next, it's important to consider the digital footprint that your child has already created online. Do they have social profiles? Now is the time to set up privacy and protections.

Secure All Social Accounts

☐	Set all social accounts to "Private" so that only friends can see posts. This applies to Facebook, Instagram, TikTok, and others.
☐	Consider using Meta's Parental Supervisions tools to monitor your child's activity on Facebook, Instagram and Messenger.
☐	Check that your child's social login password is strong (and make changes)
☐	Create age-appropriate profiles on streaming sites like Netflix, Disney+, etc.
☐	Talk with your child about the permanence of the internet. Whatever you post, even in private DMs, can never be erased.

Most parents stop here, but there's still more you can do. While the risks of identity theft for children is low, the potential damage is really high while the solution is fairly easy.

Protect Your Child's Identity

☐	Set up a credit freeze for each child with every major credit bureau in your country (in the US, it's Experian, TransUnion and Equifax). Watch this tutorial.
☐	Set a reminder to check your child's credit report once per year (and check each adult in the family at the same time!). Watch this tutorial.
☐	If you use identity monitoring, ensure your child's information is added as well. Recommended monitoring service: Identity Guard
☐	Consider creating a private email account for your child that is only used for communication with friends and family. Recommended: free Proton account
☐	Talk with your child about a "Minimum Viable Profile" - giving over the least amount of information possible. Stress the importance of protecting your ID number (i.e. Social Security Number).

There is only so much we can do as parents to protect our children. The best thing we can do is teach them healthy habits and how to use the right tools that will serve them well throughout the rest of their lives.

Instill Healthy Cyber Safety Habits

☐	Teach your child to use a password manager. If you don't already use a password manager, set up a family plan on Proton Pass.
☐	Help your child create strong, unique passwords for each login. The same goes for their device PIN.
☐	Have your child set up 2FA on their social accounts using either an authenticator app (free) or a good security key (paid).
☐	Start a family game to see who can find fake or AI-generated videos.
☐	Next time you receive a scam or phishing email, show it to your kids and work as a family to uncover how to spot it as a scam.
☐	When new updates are released, make sure that your child updates each of their own devices.
☐	Talk to your child about the dangers of "free" - free WiFi, free games, free services. The cost usually involves your personal information.

Additional Tips for Kids & Cyber Safety

- Every family is different and each child has their own set of needs, so how you implement this checklist is up to you. It is recommended to start with strong lockdown measures and then ease it up as you discover what works best for your child. It's better to be too careful in the beginning.

- Generally speaking, it's best to keep your child in the same ecosystem that you as parents use. In other words, if you use Apple devices, it's best to have your kids do so as well. If you use Android, then kids should use the same.

- Not all internet browsers are the same. If you use Apple devices, then content restrictions only work with Safari. If you prefer to use Chrome, then you will need to set up separate restrictions through the Family Link app.

- Content filters suck. Kids are masters at finding loopholes and workarounds. Don't rely on filters alone - it's worth setting up some kind of monitoring to know what sites your kid is visiting.

- It is recommended to limit the usage of devices in a child's room, particularly at night. Kids are still developing habits and often don't have proper self-control. They will gladly stay up until the early hours of the morning watching videos and scrolling social media if you let them.

- IMPORTANT: Do NOT feel the pressure to base your decisions as a parent on what your child's peers are allowed to do. You know your child best and it is your responsibility to protect them and teach them proper cyber safety. You've got this!