

FREE PARENT RESOURCE



THE PARENT'S GUIDE TO KEEPING KIDS SAFE ONLINE

Practical conversations, device controls, scam awareness,
and family cybersecurity for the connected home

Patrick W. Upman, CISSP, CRISC
Founder, Home Safe Advisor

Smart solutions. Safer homes. Better living.



THE PARENT'S GUIDE TO KEEPING KIDS SAFE ONLINE

Free e-book edition | July 2026

© 2026 Patrick W. Upman. All rights reserved.

Published by Tier 1 Services LLC d/b/a Home Safe Advisor.

Smart solutions. Safer homes. Better living.

EDUCATIONAL DISCLAIMER

This guide provides general educational information, not legal, medical, mental-health, law-enforcement, or individualized cybersecurity advice. Technology and platform settings change frequently. Confirm current instructions with the manufacturer or service provider before making changes. Product names are included as examples and do not imply sponsorship or endorsement.

FAMILY PRIVACY NOTE

Monitoring should be age-appropriate, transparent, and consistent with applicable laws, school rules, service terms, and the child's developmental needs. The goal is safety and guidance, not secret surveillance. Explain what you monitor, why you monitor it, and how greater responsibility can lead to greater independence.



BEFORE YOU BEGIN

How to Use This Guide

This e-book combines three forms of protection: family communication, age-appropriate device choices, and technical safeguards. Start with the chapters that match your immediate concern, then return to the family checklist at the end.

- ☐ Read Chapters 3 through 7 with another parent, guardian, or trusted adult so the family uses consistent language and rules.
- ☐ Use Chapter 8 before purchasing or handing down a new phone, tablet, computer, console, or headset.
- ☐ Use Chapter 9 while the device is in front of you. Menu names may differ by model and software version.
- ☐ Review Chapter 10 with older children so they understand deepfakes, impersonation, and AI-assisted scams.
- ☐ Complete the family online safety plan in Chapter 12 and schedule a quarterly review.



CONTENTS

Table of Contents

Introduction: Why this guide exists

Chapter 1: The Connected Home

Chapter 2: Digital Footprints and Interconnected Life

Chapter 3: Online Communities

Chapter 4: Online Dangers

Chapter 5: The Online Money Machine

Chapter 6: Common Red Flags

Chapter 7: What Parents Can Do

Chapter 8: Choosing Devices and Platforms

Chapter 9: Technical Safeguards

Chapter 10: Artificial Intelligence and Deepfakes

Chapter 11: General Cybersecurity for Families

Chapter 12: Your Family Online Safety Plan

Resources: Reporting and official guidance

About the Author: Patrick W. Upman and Home Safe Advisor



INTRODUCTION

Why this guide exists

This book is for parents and guardians doing their best to help children use technology safely. My name is Patrick W. Upman. I have worked in information technology since 2008 and have focused on cybersecurity since 2012. I hold the CISSP and CRISC certifications, along with other advanced IT and security credentials, and I have supported security programs in large enterprise environments, including work at Tenable in Columbia, Maryland.

I grew up alongside the modern internet. I remember school computers, The Oregon Trail, a dusty DOS computer no one in my household knew how to use, and an eMachines computer connected through AOL dial-up. Web pages loaded slowly, phone calls interrupted the connection, and even a small image could take a long time to appear. Like many children of that era, I eventually gained unsupervised access and immediately searched for things I was too young to understand. The internet was slower then, but a lack of supervision still shaped what I saw and how I understood relationships.

High-speed internet changed everything. Games, chat rooms, videos, and strangers became available instantly. By about age eleven, I could spend hours online without an adult knowing whom I was talking to or what personal information I was sharing. At the time, that freedom felt exciting. As an adult and a parent, I understand how risky it was and how easily unfiltered content can shape a young person's expectations about relationships, sexuality, attention, and trust.

With the explosion of social media, I became a very different person, almost overnight. Once I realized that all my friends were online, I was on social media all the time. It was how I knew where the party was and who was dating whom. But then like many others, I developed anxiety (although I did not realize that is what it was at the time) seeing my friends hanging out and realizing I did not get an invite. I started just collecting "friends" so that I looked popular, but many of these people I barely knew, and some I didn't know at all, I just accepted a friend request, assuming we met at a party.

I also saw people misuse social media to monitor former partners, sell illegal products, and identify homes that appeared empty. Posting vacation or concert photos in real time can unintentionally tell strangers that no one is home.

Growing up with the internet was not all bad. I did get to learn things much faster, no waiting on a book to be returned from the library to complete a project. And I did make actual friends from online gaming. I discovered communities of people with similar interests, and took part in discussions, hearing perspectives I may not have heard otherwise which I believe helped me become a more open-minded person.

I wrote this guide to help parents understand the risks and opportunities that technology presents. The goal is not to frighten families away from the internet. It is to help parents create reasonable boundaries, configure common devices, recognize warning signs, and keep communication open so children can ask for help without fear.



CHAPTER 1

The Connected Home

What is online? In practical terms, almost everything. Phones, vehicles, televisions, thermostats, cameras, watches, appliances, medical devices, and toys may all connect to the internet. Some connections add real value. Others add convenience while also creating new privacy and security questions.

Every connected device uses electricity, bandwidth, an account, and usually some amount of personal data. It may also require updates and security support. Before connecting a new device, ask what benefit the connection provides, what data the manufacturer collects, how long the device will receive updates, and whether the feature can be disabled.

Think of bandwidth like a highway. A few vehicles move easily, but heavy traffic creates congestion. The same thing happens when many phones, cameras, televisions, game consoles, and smart devices use a home network at once. Wired connections can improve reliability for stationary devices, but the more important lesson is to connect only what you need and keep the network organized.

KEY TAKEAWAY

Connect only what provides a real benefit. Every connected device adds an account, data flow, update obligation, and potential point of failure.



CHAPTER 2

Digital Footprints and Interconnected Life

The largest concern with a highly connected home is the digital footprint it creates. Apps and devices may record account activity, location, viewing habits, searches, purchases, device identifiers, voice commands, and usage patterns. Individual data points may seem harmless, but together they can reveal routines and preferences.

Companies use profiles to personalize services, measure advertising, recommend products, and assess how people use a platform. Criminals can use similar information to guess passwords, impersonate family members, target scams, or determine when a home may be unoccupied. The practical response is not panic; it is data minimization. Share only what is needed, review privacy settings, and delete accounts and devices you no longer use.

Turning off a screen does not always stop network activity. Phones, tablets, computers, and smart devices may continue syncing, receiving notifications, installing updates, or reporting diagnostic information while in standby. Review background permissions and power settings, and fully shut down or disconnect devices when appropriate.

No system is perfect. Security vulnerabilities can exist in software, hardware, cloud services, and mobile apps. A previously unknown weakness is often called a zero-day vulnerability. Families cannot eliminate every risk, but they can reduce exposure by buying supported products, installing updates, removing unused apps, and avoiding devices from vendors that do not clearly explain their security practices.

Another risk is misuse by people who already have access. Employees, contractors, support technicians, and account administrators may be able to view information that customers assume is private. Use reputable providers, avoid handing an unlocked device to an unknown technician, backup sensitive data, and remove private content before a repair whenever possible.

Government agencies and private companies also collect data for public safety, analytics, fraud prevention, advertising, and other purposes. The rules and safeguards vary. Parents do not need to become privacy lawyers, but they should understand that accepting a long terms-of-service agreement can authorize significant data collection.

Automated license-plate readers and other networked surveillance systems are increasingly common in public and private spaces. These systems can support investigations and property security, but they also raise questions about retention, access, accuracy, and oversight. Families should learn what technologies operate in their community and review reliable local information before drawing conclusions.

Location and behavioral data may also influence advertising, recommendations, fraud checks, and pricing experiments. Limit unnecessary location access, choose 'while using the app' instead of 'always' when possible, and periodically review which apps can access precise location.

Navigation services estimate traffic by combining road information with signals from many devices and vehicles. This can improve travel, but it is another example of how individual device data becomes valuable when aggregated.



Some websites and apps use session-replay or analytics tools that record clicks, scrolling, errors, and other interactions. Reputable services should disclose this in their privacy notices. Treat every website and app as a service that may collect usage information, and avoid entering sensitive details on sites you do not trust.

KEY TAKEAWAY

Privacy improves when families minimize data, review permissions, delete unused accounts, and avoid posting routines in real time.



CHAPTER 3

Online Communities

Communication is one of the internet's central functions. Early online content was mostly published for people to find later: a webpage, blog post, forum entry, or wiki article. Responses were slower, audiences were smaller, and live interaction was limited.

Instant messaging, chat rooms, and online games changed that. Early chat users often asked for age, sex, and location, exactly the kind of identifying information children should not share with strangers. These tools also made it easy to talk with school friends and find communities built around hobbies and interests.

The same access created opportunities for adults to pose as children, build trust, introduce sexual conversations, request images, or arrange meetings. A person who appears to be another child in a game or chat may not be who they claim to be.

Scammers also use email, messages, social media, and malicious downloads to steal passwords, financial information, and identities. Catfishing uses a false identity to create a relationship and manipulate the victim emotionally or financially.

These scams affect ordinary families. My own mother lost \$200 after responding to a fraudulent business-loan email. Intelligence and experience do not make a person immune when a message arrives at the right emotional moment.

Online communities can also reward trolling, harassment, and outrage. I understand the temptation to post something simply to provoke a reaction, especially during heated public debates. What feels like a joke to the poster may become humiliation, fear, or coordinated abuse for the target.

Groups have used online communities to organize prank calls, raids, false reports, and harassment campaigns. Children should understand that participating in a crowd does not remove personal responsibility for harm or legal consequences.

Today's internet supports many conversations at once. A child can play a game, watch a stream, join a voice chat, send direct messages, and browse another app on the same device. This makes it easy for a conversation to move beyond the space a parent originally approved.

Connection is not inherently harmful. During the COVID-19 pandemic, online tools helped families, students, workers, and isolated people maintain relationships and find support. Online communities can be especially valuable when a person cannot find a similar community locally.

The challenge is quality and context. Endless entertainment does not guarantee healthy entertainment, and a community built around a child's favorite game may include adults, advertising, pressure, misinformation, or conversations the child is not ready to handle.

Adults can make their own lawful choices, but children require additional protection because they are still developing judgment, boundaries, and an understanding of long-term consequences.

- Healthy online interaction should be honest, voluntary, age-appropriate, and free from coercion.
- It should not encourage self-harm, violence, exploitation, or abuse.



- It should not depend on secrecy from a parent or trusted adult.

Children should not be pulled into sexual, graphic, criminal, or manipulative conversations. Parents should explain these boundaries before a child encounters them and give the child a safe way to leave and ask for help.

Parents and guardians have the responsibility to understand the platforms a child uses, the people who can contact them, and the information they can share. The next chapters describe common dangers before moving into practical device and account controls.

KEY TAKEAWAY

Online communities can be valuable, but children need clear rules about strangers, private messages, moving to other apps, and sharing personal information.



CHAPTER 4

Online Dangers

The internet today is as vast as the ocean and expanding like our universe. Most people have heard by now of the dark web, the layers of the internet that require a special browser and protocols to access. While that is a danger in its own right, it is not what we will be discussing here.

When it comes to child safety, I am more concerned about the internet level that most people operate on. The public internet if you will. As we previously discussed there are plenty of social media and chat room options that predators can use to target children. However, there are many which people do not think about.

Roblox is a popular example of a user-generated platform. Children can play games, build worlds, and interact with others across phones, tablets, computers, and consoles. The creative freedom is part of its appeal, but user-generated spaces can change quickly and may include chat, purchases, frightening themes, sexualized behavior, hate speech, or attempts to move a child to another platform.

A game that looks harmless at first can include content created by other users or change after an update. Ratings and parental controls help, but they cannot predict every live interaction. Parents should review account settings, limit communication, approve purchases, and occasionally sit with the child while they play.

The same problem exists on video platforms. A channel may look child-friendly while including jump scares, disturbing edits, misleading thumbnails, or inappropriate themes. For younger children, approved-content lists and supervised viewing are safer than relying only on recommendations.

Predators may offer game currency, rare items, gifts, or attention in exchange for private conversations, photos, secrets, or risky behavior. A gift from an online stranger is not free; it may be an attempt to create obligation and control.

Trolls may also enter child-oriented spaces with offensive avatars, slurs, threats, or sexual content. Even well-configured filters cannot stop every live user, so children need a simple response: leave, block, report, and tell a trusted adult.

I have personally seen inappropriate avatars and racist language appear in a game session that otherwise seemed suitable for children. That experience reinforced an important lesson: settings reduce risk, but adult involvement is still necessary.

Video platforms face the same challenge at a much larger scale. Automated filters and age labels are useful, but they do not replace active supervision, especially for young children who may watch one recommended video after another.

Older children face different risks. Pornography, graphic violence, extremist content, self-harm material, dangerous challenges, and misinformation are easy to find. Repeated exposure can affect expectations about bodies, relationships, consent, conflict, and identity before a teenager has the experience to place the content in context.



Adult content online is often more extreme and more available than material previous generations encountered. Parents should discuss consent, respect, unrealistic performance, exploitation, and the fact that pornography is entertainment rather than relationship education.

Curiosity can also lead children to dangerous instructions involving chemicals, medications, weapons, fire, or viral challenges. Teach children to pause before copying anything that could cause injury and to ask an adult, teacher, pharmacist, or other qualified professional.

False instructions can spread quickly because they are shocking, funny, or presented with confidence. A polished video is not proof that an idea is safe.

The public internet is not a controlled classroom. Platforms, regulators, schools, and service providers all have roles, but parents and guardians remain the people best positioned to understand a child's age, maturity, needs, and behavior.

The goal is not total control. It is layered protection: clear expectations, age-appropriate access, technical safeguards, regular review, and a relationship strong enough that a child will ask for help.

KEY TAKEAWAY

Filters cannot predict every live interaction. Teach children to leave, block, report, and tell an adult whenever content or contact feels wrong.



CHAPTER 5

The Online Money Machine

Everyone that has grown up with the internet at some point in their life considers making money online. Gambling, gaming, streaming, day trading, freelancing, content creation, drop shipping, arts & crafts, and of course selling “spicy” (nude) photos or videos.

There are many ways to make money online. We see people do it all the time on platforms like YouTube, Twitch, Instagram, OnlyFans and TikTok. People turn their passions into cash generating lifestyles. The problem is we typically only see the ones who succeed and their edited products.

Content creation can be a real career, but the finished videos hide much of the work: planning, recording, editing, publishing, audience development, contracts, taxes, and constant pressure to stay relevant.

Young people of every gender may feel pressure to create provocative, dangerous, humiliating, or attention-seeking content. Some are pushed toward sexualized images; others are rewarded for pranks, rage bait, stunts, or conflict. The common risk is making a permanent decision for a temporary burst of attention.

Public attention has costs. Creators may lose privacy, receive threats or harassment, attract stalkers, or develop one-sided audience relationships that feel personal to the viewer but are not mutual.

Online content can remain searchable long after a trend ends. A post made as a teenager may later affect employment, education, licensing, relationships, or personal safety. Private organizations may make decisions based on public content even when the content is lawful.

Sexual or borderline sexual content can create lasting privacy and exploitation risks. Images may be copied, altered, redistributed, used for blackmail, or discovered years later. Children should understand that consent to create or share something once does not guarantee control over where it goes next.

Multi-level marketing, bulk-resale, and drop-shipping pitches may also be presented as easy income. The participant may pay fees, buy inventory, purchase training, or recruit others before learning whether there is real customer demand. Read the contract, calculate all costs, and avoid any opportunity that depends mainly on recruiting new sellers.

What most people do not realize is that these influencers often have different contracts from the people who sign up to sell the products. Influencers will typically have a contract as an advertiser whereas the person signing up as a reseller is often locked into a contract where they need to move a predefined number of units and or convince others to sign up as resellers to earn money. The issue is the products are often not of good quality and while the influencer was able to make a good enough pitch, the person reselling may not have the same skill level of work ethic when it comes to sales.

There is a new rise in popularity for online sports and speculative betting. People can make money from platforms such as DraftKings and PolyMarket, but most do not. Much like betting at a casino, if someone wins too much or too often, they will be banned from using the platform.



In summary, be sure to talk with your children and let them know that there is no such thing as free or easy money. The cost may not be obvious or up front, but there is always a cost be it reputation, legal or social consequence, or hard work behind the scenes.

KEY TAKEAWAY

Easy money online usually transfers risk to the person who understands the opportunity least. Slow down, verify, and never invest under pressure.



CHAPTER 6

Common Red Flags

Now that we are aware of some of the dangers lurking online, let's discuss some of the red flags to look out for. There are several things that scammers and predators look for in their victims.

Emotional Vulnerability. Victims are often people who are lonely, recently separated, depressed, isolated, grieving, or stressed and are seeking friendship, love, connection, or validation. The people who generally fall into this category are young people (Children or teens) and the elderly. Both groups are often willing to overshare information and seek out connection.

Predators seek out the lonely and isolated by sending out mass messages on dating sites and emails to hook a victim into a false relationship, a technique known as catfishing.

They often start off as innocent conversations and then they build an emotional connection around information their victim shares with them.

A romance scam may sound like this: 'We have so much in common. I want to visit you, but I need money for travel documents. Please do not tell anyone because they will not understand us.' The details change, but the pattern is the same: fast emotional intimacy, secrecy, and a financial request.

Alternatively, they may make claims that they want to come see you but cannot afford the plane ticket. The victim sends them the money; they tell the victim when they are due to arrive only for the victim to be left waiting at the airport for their "lover" to never arrive.

Then they get a message from the scammer, "Sorry my love I tried to make it, but when I arrived at customs, I did not have enough money, so I was denied entry."

The victim may then be asked to pay for another ticket or send \$10,000 to solve a new customs, medical, legal, or travel emergency. Each payment creates another reason to believe the relationship must be real, even though the scammer never intended to arrive.

Children, teenagers, and some older adults may be especially vulnerable when they are lonely, grieving, isolated, unfamiliar with technology, or eager to trust. Vulnerability is not a lack of intelligence. Scammers design messages to trigger emotion before a person has time to verify the facts.

To be clear this is not limited to these two age groups, however they are both more susceptible because of the stages of their brain development and willingness to accept information without carrying out their own due diligence.

Pressure and impersonation are common scam tools. A caller may claim to represent the IRS, a court, a police agency, a bank, a school, or a utility company and threaten immediate arrest, account closure, or another serious consequence unless payment is made at once.

The victim may comply before checking whether the agency would contact them that way, whether the phone number is genuine, or whether the requested payment method makes sense. Caller ID, official-sounding language, and personal information are not proof that the caller is legitimate.



Time sensitivity is not only used by scammers to get your bank account information, but also a technique used by salespeople and marketing firms. I remember being in my early 20s and attending a “once in a lifetime event”. A music festival that I bought VIP tickets for because it was “once in a lifetime.” The next year the same event came around with the same marketing pitch. “You don’t want to miss this once in a lifetime event” and you know what, 17 years later that event still happens every year and they still market it as a “once in a lifetime event.”

Another angle often tied to time sensitivity is limited opportunity. How many ads have you heard that say things like “limited time only” or “while supplies last”. I had a job early on in a restaurant where they would run a “limited special” on things like steak or lobster tail. Part of the gimmick was they would cook it and blow the air out of the restaurant so that people passing by would smell it.

When people would start coming in, if they did not order the special, the wait staff would make comments where the customer can hear them intentionally, but the customer did not know they were meant to hear it. For example, when someone would order the lobster, they would say something like “oh you’re in luck we only have 5 left” or “let me see if we still have some because I know we are almost out.”

This way the other customers hear this interaction, and it creates a sense of urgency to order the item before it's gone. The customer has no idea that the freezer in the back has a full stock of the item the restaurant wanted to push. The Fear of missing out is real and has a real influence on people of all ages.

Financial opportunity. Many scammers and legitimate businesses take advantage of this. Ever get a speeding ticket and take it to court? Have you ever been injured and made the mistake of filling out an online questionnaire? Once your case becomes public attorneys from all over your area will start sending you letters offering to represent you. If you hire them by x date they will only charge you \$1000 instead of \$1500 to represent you.

If you have ever won a settlement, got an inheritance or won the lottery you will be bombarded with “Financial Opportunities”. People looking for you to invest in their startup, or loan them money. While some of these opportunities can be lucrative, many are not and all investments carry risk.

I know a couple who came into some money and really enjoyed traveling. They went to a beach resort and ended up in a timeshare. How did this happen? They were pitched a financial opportunity that allowed them to have “ownership” of a beachfront property where they would “save money” by paying less than what they typically would for their average vacation over the year.

Another selling point was that they could rent out their timeshare if they wanted to vacation somewhere else. The problem is they did not know that because they owned a limited portion of the share and were new “owners” their vacation dates could be bumped by other “owners” with more shares and tenure. Also, any renting of the property during their share time required board approval and access to the property could be prevented due to blackout dates for things like maintenance.

Thankfully this couple was able to get out of their timeshare when they ran into financial problems, but they did lose money to attorney costs and sold their share for pennies on the dollar, not to mention the headache of the whole process.

Another risk many do not consider when it comes to rushing into financial opportunities is they do not know the market they are getting involved with. When COVID hit, I had invested about \$500 into a cryptocurrency (digital currency privately created and regulated) called HEX. I had a friend who was heavily invested and working with a group of influencers to build brand recognition of the cryptocurrency.



It went great for a while. For months my investment grew and I was up \$2500. I was going to pull out but my friend convinced me to stay invested and “stake” my hex, which was the feature that was supposed to keep hex valuable.

Staking works kind of like a 401(k). You bank the currency, the currency gains interest while staked but if you exit early, there are penalties. I split my investments into two hex wallets. (Accounts) One was a short-term stake and the other was for 15 years.

Shortly after staking the market changed and Hex value started to dip. My \$3000 in HEX became almost worthless. By the time my short-term stake was up HEX had dipped so low that it would have cost me money to convert it back to USD, as for the \$1500 long-term stake I set in 2021 is now worth about \$3. Hopefully that will change by 2036, but I don’t have my hopes up.

Now did my friend scam me? No, neither of us knew enough about what we were getting ourselves into. The scam came from the influencers who used a technique known as “pump and dump.” This happens to people and companies alike. Someone comes along hyping up a product or opportunity. They show how “invested” they are and how if you invest you can make money with them and be just as wealthy as they are. Then what happens? They get enough people to invest, and they quietly exit holding the bag of cash.

A common example is a celebrity- or influencer-promoted digital token. Excitement and social-media attention can drive the price upward, while early holders sell quickly and later buyers absorb the losses.

This pattern is often described as a pump-and-dump scheme. The promoter may present the asset as a community opportunity, but the people with early access may have incentives that are very different from those of ordinary buyers.

The lesson for young people is simple: popularity is not due diligence. Never invest money because a creator, celebrity, friend, or online group creates urgency or promises easy returns.

Another big scamming method is to exploit the charity of others during holidays or disasters. Fake websites for fake charities, spam email chains begging for support. Influencers and companies claiming to donate a percent of proceeds to a cause, only to find that the actual amount donated is far less than you were led to believe, if it made it to anyone in need at all.

With the expansion of AI, it is becoming increasingly easy to make such scams. Websites can be built in minutes not days. Money can be laundered through crypto or sketchy offshore banks. People creating shell companies to pass the transactions through so that it is harder to identify and track the fraud.

It is important to know that IT IS NOT ALWAYS ABOUT MONEY. Some predators are out for data. They want to take over or sell peoples identities, steal intellectual property, or just stalk their victims for the thrill of it.

Some offenders seek information rather than immediate payment. Others attempt to isolate and exploit victims through identity theft, blackmail, stalking, sexual exploitation, violence, or trafficking.

Online grooming and trafficking are real, but the process is often less dramatic than people expect. Exploiters may begin with attention, gifts, transportation, housing, substances, secrecy, or a romantic relationship. They gradually isolate the victim, create dependency, collect compromising material, and use fear or shame to maintain control.

My own life experiences exposed me to people and situations that showed how coercion can work in practice. For this guide, the important point is not the graphic detail. It is that manipulation often develops step by step and may be disguised as friendship, protection, romance, or opportunity.



Most of what we covered so far are generic scams used by scammers and predators. Now let's focus on children. Children with unfettered access to the internet are exposed to a vast array of information. Images, videos, music, opinions, and echo chambers posing as communities.

Pedophile predators lurk in-games, comment sections, chat rooms, and communities. They tend to look for children who are seeking attention that they are not getting at home and are online unsupervised. They like to use anonymous chats or environments that are less likely to draw parental attention.

They will often pretend to be a minor themselves and mirror interests. They take advantages of the minor's desire to want things but lacking the money to buy them, so the pedophile will often start off by offering gifts such as in-game currency, or in-game items, sometimes they will mail the victim gifts from their online wish list.

Pedophiles often rely on secrecy, guilt, and making the victim feel special. They will say things like you're so beautiful IRL (in real life), you deserve to look just as sexy in-game. And don't tell anyone I go this for you because I don't want them to be jealous or mad.

They may offer in-game currency or real money, then ask for a private messaging account, disappearing photos, or sexual images. This is sexual exploitation, and the child is never responsible for the adult's behavior.

Predators will often build profiles on their victims. Getting their home address and school information from casual conversations. Learn their parent's names, occupation, and hours they are alone. There have been countless stories of grown men coming over to "play video games" with underage children. The most common games seem to be used by predators are Roblox, Minecraft, Fortnite, and Call of Duty, but any online game /community possesses the potential if not carefully monitored.

Another tactic these predators will use is to create chaos and time sensitivity. Claiming that they are alone, and no one understands them and they need a friend right now, even though that friend is a minor.

Alternatively, they will hype up a minor's home or emotional situation, turn the child against their parents or guardian and encourage them to run away, offering them a place to stay and the opportunity to be heard.

Other times they will simply guilt or try to extort the minor into meeting up which the minors do so that the inappropriate content or private conversations are not used against them or published publicly.

I feel I should also point out that these common red flags are often paired, and there is typically some sense of urgency. So, here is a good checklist to consider when you are faced with a potential scam or predator.

Are they:

- Rushing trust or romance
- Avoiding video calls consistently
- Asking for personal information
- Asking for photos or videos of you
- Asking for secrecy
- Creating emergencies
- Asking for money/gift cards/crypto
- Trying to isolate their target
- Using guilt or fear



- Claiming exclusive opportunities
- Creating urgency

Now that we know what to look for, what do we do? For starters have conversations with people who are at risk to falling susceptible to these techniques. Knowing the potential evils that exist and how to identify them is half the battle.

Have conversations with your children to be careful what they share when talking to people online. When on camera be careful sharing backgrounds that include sensitive information such as pictures or merch that might indicate what school they attend or where they live.

If they live near a landmark and have a window in the frame of the video, people may be able to identify their location using background clues. For example, if you live near a baseball stadium and your microphone picks up the announcer saying the team's name, that could be used to help locate you.

I will get into more technical detail in a later chapter, but uploading pictures can reveal your location if you do not remove or disable the metadata.

Joining someone private server can reveal your IP Address (internet protocol address, think of it as your identification on the internet) which can help predators find out what area you live in.

Things that many of us don't think of, such as how our Gamer or Social media tag (Username) can be used to build a profile on you if you reuse it or something similar across platforms.

Innocent conversations can provide just enough information to guess a password or reset your credentials for a service.

Sharing vacation and travel information in real time can be used by people looking to break into your home. Cyber criminals are using AI to make audio and video to trick parents, grandparents, and business professionals into sending money they shouldn't to "help family" or "pay vendors". This is a trend that is increasing daily and will only be harder to stop as AI improves.

The more information you put online, the easier it is to build a profile on you and those around you. Companies, Governments, and predators do this all the time, so be careful what you post, because the internet is about as close to forever as it gets.

To sum it all up before we move on. If it sounds too good to be true, it likely is. If you are not expecting it, it's likely a scam.

While it is possible to make friends online, trust no one and verify before making decisions. This includes trusting files, links, conversations, and meetups. I cannot stress enough that when it comes to the internet, nothing truly disappears and most of it is manufactured.

Practical habits that reduce scam risk:

Slow down decisions - If a demand cannot wait long enough for you to verify it independently, the default answer should be no.

Verify independently - Contact the organization through a number or website you already know, not the contact information supplied in the suspicious message.

Talk to a trusted person - A second person may notice pressure, contradictions, or warning signs that are difficult to see while you are emotional.



Maintain boundaries - An urgent story does not require you to abandon family rules, privacy, or financial limits.

Limit public personal information - Post travel, concert, and vacation photos after returning home rather than announcing an empty house in real time.

Learn common tactics - Review scam alerts from banks, government agencies, schools, and local law enforcement, and discuss new examples as a family.

Use multifactor authentication and passkeys - Protect email, financial, cloud-storage, gaming, and social accounts with the strongest additional sign-in method the service supports.

Use a reputable password manager - Create a unique, long password for every account so one stolen password does not unlock the rest of the family's digital life.

Be comfortable saying no - You do not owe an immediate response, payment, image, explanation, or secret to someone online.

KEY TAKEAWAY

Urgency, secrecy, isolation, emotional pressure, unusual payment methods, and requests for private content are warning signs that should trigger a pause.



CHAPTER 7

What Parents Can Do

The internet is embedded in education, entertainment, friendship, and everyday life. The realistic goal is not to keep children offline forever. It is to introduce access gradually, teach judgment, and increase independence as a child demonstrates responsibility.

The first step is establishing an open line of communication. I tell my children they can always come to me with a question or a problem. There may still be consequences for unsafe choices, but asking for help and telling the truth should never make the situation worse. A child who expects only anger may hide the very information a parent needs to protect them.

Open communication helps children feel seen and gives them a trusted place to ask questions. It also makes secrecy and isolation harder for a manipulative stranger to use against the family.

Communication must be two-way. Adults need to express concern and set limits without turning every conversation into an interrogation. Listen first, gather the facts, and explain the safety reason behind a rule.

Children will test boundaries, and some rules will need to change as they mature. State expectations before problems occur, apply consequences consistently, and make a clear path for earning more freedom.

When children can talk through a situation, the family can slow down false urgency, check facts, preserve evidence, block contact, and decide what help is needed.

Parents can also help evaluate opportunities, friendships, dating situations, purchases, and requests to move a conversation to another app. Calm guidance is more useful than ridicule or an automatic ban.

Honest, age-appropriate conversations about peer pressure, substances, sexuality, violence, money, and mistakes help children recognize risk before a crisis develops.

Know your child's friends, interests, favorite games, and usual online spaces. When practical, know the adults responsible for supervision during visits, sleepovers, transportation, and shared device use.

Knowing the adults who supervise your child's friends helps families coordinate rules, transportation, sleepovers, devices, and emergency contacts.

KEY TAKEAWAY

The strongest parental control is a child who believes they can tell you the truth and ask for help.



CHAPTER 8

Choosing Devices and Platforms

Modern families have many technical safeguards available, but the options are not always simple. This chapter compares common device types and highlights the controls parents should consider before giving a child access.

Technology and threats change together. No product is impossible to bypass, and no setting replaces supervision. Choose a device that receives updates, supports child accounts, and gives the parent controls they understand and will review.

Cell Phones

Every kid wants a cellphone; it is the new driver's license. The first sense and access to freedom. You can easily connect with your friends, play games, and look up anything. However, while this is important part of growing up in a technological world, giving a cell phone to a child is like giving them their license without even going through the learner's permit stage first.

I believe a more responsible option is to give children basic (No apps, internet, or camera) phones first with important numbers saved, such as their parents, guardians and immediate family. This allows them to call and text when issues arise. They can even share their contact info with their friends if they need to be connected. Many carriers offer the ability to see what numbers were called or texted during the billing cycle.

Mobile carriers generally show call and text metadata on account records, such as the number contacted, date, and time. They typically do not provide the content of ordinary text conversations or recordings of personal calls. Use family-account tools and direct, age-appropriate conversations rather than assuming a carrier can reproduce private communications.

Smart Watches

An alternative solution I would recommend would be a smartwatch with cellular capabilities. The number of apps they can use on this style device is much more restrictive than other devices and it still allows for calls and text messages. You also have the added benefit of being able to easily track your child as most smartwatches have this option built in.

Smart Phones

Once we are ready to move onto smartphones, I personally recommend Apple iPhone for its security features that are inherent with their phone operating system and using the Apple network has built in security. Also like smartwatches, smartphones offer a tracking feature.

With that in mind other brands are fine too such as Samsung who works in a similar way, and many Android phones have security features too but require a bit more technical knowledge to set up securely as there



are many versions of android, and it is more opensource (Community built and modifiable, unlike Samsung and Apple which are more restrictive) by nature.

As I have been an iPhone user for about 10 years now, I am more familiar with Apple and will focus on them. For more information about other platforms such as Android and Samsung I would defer you to their documentation and specialists.

Apple's Lockdown Mode is designed for the small number of users who may be targeted by highly sophisticated attacks. It is not a general parental-control feature. For a child's iPhone or iPad, focus on Family Sharing, Screen Time, Communication Safety, purchase approval, content restrictions, and account recovery settings.

The names and locations of settings change over time. Use the current instructions from the device manufacturer and review the settings after major software updates.

Tablets

Tablets seem to be most children's first exposure to the internet (excluding smart TVs) that parents seem to provide. Not all tablets are the same and it is important that you get a tablet that is most appropriate for your child's age group. Many tablets also offer a tracking feature like smartwatches and smartphones.

For young children, one practical option is an Amazon Fire Kids tablet. The value is less about the brand and more about the child profile, durable case, content approval, time limits, and parent dashboard. Compare current models and subscription terms before buying.

These devices are relatively inexpensive, very durable, include a protective case with a built-in stand, and allow for easy monitoring or regulating of the content your child can access. You can set age restrictions for games and videos. You can limit screen time and see their watch history. The best part is you can do this all from an app on your phone or computer.

I use the parent dashboard to pause a device when it is time to complete a responsibility or take a break. The most effective approach is to connect the technical limit to a clear family rule rather than using it as a surprise punishment.

Another great feature of these devices is the freedom of choice it allows the children when it comes to downloading apps and games. They can see from the library apps, games, videos, and books. If they find something that piques their interest, they can send a request to download which sends my wife and me a notification in the app (or you can have it send you an email or text message) that our child would like to download something.

With the notification we see the thing they want to download, the rating it has applied, a summary of what thing they want to download is, any reviews, and if there is a cost associated. Which is worth noting that there are many free options available for download too, so you're not spending bunch of money on downloads.

The device also offers a memory expansion slot so you can buy an SD (small memory card) card to allow for the device to hold more apps, games, photos etc. It is also worth noting that the device does have a camera and the photos or videos recorded are saved locally by default. Meaning that unless you choose to upload



them, they remain on the device, adding peace of mind that your child is not accidentally uploading inappropriate photos or videos to the internet.

The last feature of note for Amazon Kids Fire Tablets is that when connected to the internet, your children can use them like a phone to call pre-approved contacts through the Alexa app. Which can be convenient when your child is on the potty upstairs and you are downstairs working, unable to hear them yelling for you to come wipe them. It is also great for connecting with the grandparents' miles away who also have the Alexa app on their phone.

For older children such as teens, you may want to consider an Android or iPad tablet. Just like with a smart phone I would suggest you set up your account as the primary and the child as a secondary. In addition to setting up email, include setting up your own PIN and biometrics such as Face ID or fingerprint reader on older models, prior to setting it up for your children.

Gaming

At a certain point every kid will almost undoubtedly go through a gaming phase. There is an entire age rating systems that parents should familiarize themselves with known as the Entertainment Software Rating Board (ESRB). This is a self-regulated body that works to help parents understand the content of a game and what age range it may be suitable for.

To find out more visit <https://www.esrb.org> however I will list a brief rating summary below:

- E (Everyone) Suitable for most ages. Minimal violence or mild themes.
- E10+ (Everyone 10+) May contain mild violence, mild language, or suggestive themes.
- T (Teen) Ages 13+. Violence, crude humor, mild blood, gambling references, or stronger language.
- M (Mature 17+) Ages 17+. Intense violence, blood and gore, sexual content, or strong language.
- AO (Adults Only 18+) Explicit sexual content or extreme violence. Rare because most retailers/platforms refuse these games.
- RP (Rating Pending) Temporary label before final review.

These ratings are generally placed on the front and back of the game case cover, typically located near the bottom left or right corner.

It is important to note that these ratings are for the US and Canada. Video games in other countries have similar rating systems but are under a different organizations purview.

Some common example games include:

Minecraft → E10+

Fortnite → T

Grand Theft Auto → M

When it comes to gaming consoles (the systems that load the data of the game for the user to play) there are currently 3 main names in the industry.



Nintendo. This is the oldest one that comes to most people's mind. Nintendo, while it does have some games for teens and adults, its main player base is young children and families. If you are looking to introduce your child to video games, this is probably the safest place to start.

The online features are much more limited than other platforms and the overall player base is younger and family oriented. While famous for its Mario franchise, it is worth paying attention to the games rating still as the Nintendo library does allow for access to games geared toward adults where there maybe violence or other content not suitable for children.

The online community is less voice chat and offers less built-in social features and is by far less competitive and many parents consider less toxic (toxic meaning people in the lobby (server or world the child is playing in) saying mean things and using inappropriate language.) than other communities. This alone makes me believe it should be every child's first gaming system.

PlayStation. This platform is owned by Sony. It started off much like Nintendo focusing on younger and family-oriented audiences, however in recent years I would argue it has shifted to the teen and adult gaming market. While it does still offer family titles such as Sonic, PlayStation is now known for titles like Grand Theft Auto and the Last of Us, games that are not suitable for children. The only community is highly competitive. With significantly more voice and social interaction capabilities built in, this platform can quickly turn toxic if your child is playing in the wrong lobby.

Xbox. Xbox was Microsoft's flagship gaming system to compete with Sony and Nintendo. Right out the gate it was famous for its shooter game titled Halo, a title, which was immediately embraced by teens and adults alike. While Xbox does also have child and family-oriented games, its online community is more geared toward competitive gaming experience.

Much like PlayStation, Xbox's online community is more player interactive focused, so this option also has voice chat and built in social options. And whenever you have voice chat and gamers, there will eventually be conversation and words spoken that are not appropriate for children.

While all three have been building their cross platform (Playing with people who are on a different system than yours. For example, someone on Xbox can play with someone on PlayStation for certain-games) and backwards compatibility (allows you to play old games that you own from previous generation systems of the same company. For example, Xbox Series X can play some old games from the original Xbox system) so customers are not buying the same game twice to play on a newer system.

The platform that gives you the most bang for your buck in my opinion is Xbox. With Xbox you can play many of your old games and if they are tied to your account, you don't necessarily need to have the original disc to play it. Xbox offers a vast online catalog which allows for cloud play (streaming the game) or download (Saved locally) of the game. You can even buy a game pass that allows you to play almost every title, allowing players to try a game before they buy it, if they want to buy it at all.

It is important to note that backwards compatibility, online library, and game pass is not limited to Xbox. Nintendo and PlayStation offer similar services, but unlike these platforms, Xbox can stream games directly to your Windows PC natively.

Sure, there are other services that you can add on like PlayStation Remote Play or use online libraries for PC gaming (which we will discuss more shortly) but because Xbox and Windows are both built and owned by Microsoft, this feature just works clean and efficiently. You can even stream the Xbox gameplay to your computer to monitor what your child is playing.



PC Gaming. There is a joke in the gaming world that PC gaming is “the master race”. The reason for this is because with PC gaming you can do just about anything. You can find free to play games or pirate them (which is illegal so don’t do that) you can even build you own game from scratch or make mods (modifications) to a game and play it in a whole new way.

While this is the most freeing method of gaming in my opinion it is also the most dangerous. Yes, there are still rating systems for the games, but when people start customizing servers or games the ratings tend to lose their meaning.

End users also have more insight than they would on a console. Server admins can get your IP address and device information easier than they could from a server on a console, because the console limit the information that can be shared. Consoles also have more moderation (Paid administrators or game developers who monitor gameplay) from admins that can issue bans for things like hate speech, inappropriate content, and threats.

When it comes to PC gaming there is also a greater risk of downloading malicious software that could damage your device when you download unverified or unofficial game files, updates, or mods. And when it comes to social interaction and online community there are so many options that is becomes almost impossible to prevent your child from having conversations with a stranger. Laptop or desktop computers, regardless of operating system (Windows, Mac, Linux) should be one of the last devices you introduce your children to. Unlike other devices there is much more flexibility when it comes to what can be done on them as they are not typically locked down by default. However, once a child is capable, the parent or guardian has an understanding of the technology, and appropriate protections or measures are in place; children should absolutely learn how to use this technology.

Mobile Games. Think of mobile games as mini games. They are often designed for smartphones and tablets, or to be played in a web browser (like google chrome). They may or may not be rated. They often contain ads that are not filtered by age and may contain malicious code. Unless a mobile game is very well known and typically a paid (not free to download) game, I would highly advise that you monitor your child’s gameplay.

Free mobile games are often “Pay to win” and often offer one click purchase options. Many parents have discovered high phone bills from their children purchasing items from games they allowed their child to play unsupervised on their device. When it comes to these style games, I strongly encourage parents do their own due diligence for each game.

VR or AR Games (Virtual Reality or Augmented Reality). This game types are a new emerging platform. They also offer game ratings, but the online community can be all over the place. Some have active admins, some its everyone for themselves.

While there are a lot of games to play in this style of platform, the biggest feature of this platform is the social interaction. It is not uncommon to enter a VR chat where there is a full-grown man masquerading as an anime (Japanese style cartoon) girl, or a bunch of teenagers using racial slurs.

With some platforms like Facebook Meta’s Quest VR, you have the option to stream what is being displayed on the headset to your phone, tablet, or smart TV. Allowing for some parental oversight during gameplay.

I feel that I should note that VR/AR platforms can also provide great exercise and educational opportunities. There is a boxing simulator that can help kids learn how to defend themselves and burn energy.



There is a game called “Beat Saber” where you can dance to music by artists you know and have Star Wars style virtual light sabers that you slice blocks as they come toward you while you dance. It sounds weird but it is fun and a great workout. Lastly there is a huge library of educational videos and simulations. My children love to explore space or travel back in time to watch dinosaurs from the safety of our living room.

Not all games or experiences require social interaction, but it is our responsibility as parents to know what our kids are doing with their technology and who they are interacting with while online. It is important to understand the technology that you are going to allow your child to utilize prior to providing them with the access.

While you can take steps to mitigate the dangers of the internet, which we will cover in the next chapter, I cannot stress enough that technology is always changing. What is true at the time of writing this book may not be true by the time you read it.

To stay up to date you can check out the device manufacturers website, or utilize local resources such as your local library, colleges, and technical service providers in your area such as Internet service providers or IT service providers (usually referred to as Managed Service Providers) like GeekSquad.

KEY TAKEAWAY

Choose devices based on the controls your family will actually use, not only price, popularity, or technical specifications.



CHAPTER 9

Technical Safeguards

This chapter is going to be a collection of recommendations and step-by-step guidance. This is not all-encompassing and does not mean that it will be 100% effective. These techniques are meant to help enable parents to put safeguards in place to prevent their children from having free rein online. As any parent will eventually learn, children are incredibly clever and test boundaries. Once your child reaches the point that they can read and research how to achieve their goal, with enough persistence they will find a way to circumvent any measure you put in place.

As previously mentioned, I highly recommend Amazon Fire tablets for their ease of use, low cost, high durability and parental controls.

Amazon Fire Kids Setup

Official resource: [Amazon Kids setup](#)

- Turn on the Fire tablet
- Connect to Wi-Fi
- Sign in with your Amazon account
- Set a PIN/password (important for parental control protection)
- Go to Add Child Profile
- Enter child name
- Enter birthdate
- Choose avatar
- Choose Amazon Kids or Kids+
- Select Amazon Kids (free) or start Kids+ trial (optional)
- Set permissions inside the child profile
- Allow/block apps & games
- Control web browsing
- Set video/book access levels
- Restrict or approve downloads
- Set screen time limits
- Daily time limits
- Bedtime schedule
- Optional "Learn First" mode

This is wonderful for early development. They want to learn so they can play.

- Switch profiles using PIN
- Child mode = Amazon Kids app
- Adult mode = PIN required



iPhone and iPad Setup

- A. Secure the parent account
- Sign in with your Apple ID
- Go to Settings → Face ID or Touch ID & Passcode
- Turn ON:
 - Face ID or Touch ID
 - Device passcode
 - “Require Attention” (if available)
- B. Enable Screen Time (this is your control hub)
- Go to Settings → Screen Time
- Tap Turn On Screen Time
- Select “This is My Device”
- Set a Screen Time Passcode (different from device unlock PIN)

This is critical - it locks parental controls

Official resource: [Apple Family Sharing](#)

2 Create Family Sharing

- Go to Settings → Apple ID (your name)
- Tap Family Sharing
- Select Add Member
- Choose Create Child Account

3 Create the Child Apple ID (Important Step)

- Apple will guide you through:
 - Child’s name
 - Date of birth (this determines restrictions automatically)
 - Create Apple ID email for the child (example: childname@icloud.com)
 - Set password

Set recovery and oversight:

- Parent Apple ID is automatically set as:
 - Recovery contact
 - Purchase approver
 - Family organizer control point

4 Turn ON Purchase & App Controls

- Inside Family Sharing:
 - Enable Ask to Buy
 - Child must request approval for:
 - App downloads
 - Purchases
 - Subscriptions



Official resource: [Set up a child iPhone or iPad](#)

5 Set Up the Child Device (iPhone or iPad)

Sign in on the child device with the newly created Apple ID.

- Then configure:

Official resource: [Apple Screen Time for children](#)

Screen Time can be configured from the child's device or the parent's device.

- Go to Settings → Screen Time → Child's Device
- Set:
- App limits (games, social media, etc.)
- Downtime (bedtime hours)
- Content restrictions (age ratings, web filters)
- Communication limits (who they can text/call)

6 Email Setup and Parent Oversight

Email visibility varies by provider and account type. Use transparent, age-appropriate oversight and review the provider's current family-account options before enabling forwarding.

A. Create the child email account

- Use iCloud email during Apple ID set up OR add Gmail/Outlook later

B. Set up email forwarding (recommended approach)

For Gmail, use the account's forwarding settings when that feature is available:

- Log into child Gmail account
- Go to Settings → Forwarding and POP/IMAP
- Add parent email as forwarding address
- Verify confirmation code sent to parent email
- Enable:
- "Forward a copy of incoming mail to parent email"
- Keep copy in inbox

If using Outlook:

- Settings → Mail → Forwarding → Enable forwarding to parent email

C. Make parent email the recovery email

- On child Apple ID:
- Add parent email as Recovery Email
- Ensure parent is also listed in Family Sharing recovery options

7 Final Security Lockdown (Recommended)

- On child device:
- Disable app installs without approval
- Turn on content filters (web and app store)
- Disable account changes without Screen Time passcode



- Restrict Safari or use Safe Search only

Result of This Setup

You will have:

- A parent-controlled Apple ecosystem
- Face ID or Touch ID secured parent device
- Screen Time enforced restrictions
- “Ask to Buy” approval flow
- Child email with parent visibility (via forwarding)
- Parent as recovery and admin authority

Android and Google Family Link

Official resource: [Google Family Link](#)

1 Set up Parent Control First

- On parent phone, install Google Family Link
- Sign in with parent Google account
- This account becomes the family manager (admin)

2 Create Child Google Account

- Open Family Link app

Family Link can also apply supervised settings to Chrome and other Google services, giving parents one dashboard for app approval, screen time, content settings, and supported device activity.

- Tap Add Child or Create Account
- Enter:
 - Child name
 - Date of birth
 - New Gmail address for child
 - Set password
- Parent account is automatically set as:
 - Supervisor
 - Recovery or management account

3 Set Up Child Device (Android phone/tablet)

- Turn on device
- Sign in using child Google account
- When prompted, link device to Family Link

Official resource: [Google parental controls](#)

4 Enable Parental Controls (Family Link)

From parent device:

- Set:



- App install approval (parent must approve downloads)
- Screen time limits (daily limits)
- Bedtime or downtime schedules
- App usage restrictions
- Location tracking (optional)

Official resource: [Google Play parental controls](#)

5 Google Play Store Controls

On child device:

- Open Google Play Store → Settings → Family
- Enable:
- Content age restrictions (apps, games, movies)
- Purchase approval requirement

6 Web & App Filtering

- Use Family Link to restrict:
- Chrome browsing (SafeSearch enforced)
- Unapproved apps
- Age-inappropriate content

7 Monitoring (Parent Dashboard)

From Family Link app:

- View app usage reports
- See screen time by app
- Lock device instantly
- Approve/deny app requests

Official resource: [YouTube Kids help](#)

8. YouTube Kids and approved-content viewing. YouTube Kids provides child profiles and content controls, but parents should still review history, disable search for younger children when appropriate, and consider approved-content-only viewing.

- Install YouTube Kids
- Set age profile
- Restrict search and content level
- Disable or limit recommendations if needed

Important Limitation to Know (Email)

Android (Gmail) does NOT support fully automatic email mirroring of a child account to a parent inbox

Instead, use:

- Family Link activity reports
- Manual supervision
- Optional supervised Gmail filters (limited visibility)



Samsung-Specific Options

These steps are the same for both:

- Install Google Family Link on parent phone
- Sign in with parent Google account (becomes Family Manager)
- Create child Google account in Family Link
- Name, DOB, new Gmail address
- Parent becomes supervisor and recovery control
- Set up child device with child Google account
- Enable Family Link controls:
 - App install approval (Ask parent)
 - Screen time limits
 - Bedtime or downtime schedules
 - App restrictions & usage reports
 - Location tracking (optional)
- Set Google Play Store parental controls:
 - Age restrictions
 - Purchase approval required
- Monitor via Family Link:
 - App usage reports
 - Screen time
 - Remote device lock

Samsung Kids and Device Security

Official resource: [Samsung Kids and parental controls](#)

- Enable Samsung Kids Mode
- Turn on Samsung Kids from Quick Settings or Settings
- Set parent PIN
- Add allowed apps
- Enable kid-safe home screen environment
- Set time limits inside Samsung Kids
- Set up Samsung Account (optional but recommended)
- Create/sign in at account.samsung.com
- Enables Samsung device features and Find My Mobile
- Enable Samsung Security Tools
- Turn on Find My Mobile
- Remote locate device
- Remote lock
- Remote wipe if needed
- Manage dual app stores (important)
- Monitor both:
 - Google Play Store



- Galaxy Store
- Ensure all installs still require Family Link approval

Android Setup Summary

Stock Android: Uses ONLY Google Family Link (simpler set up)

Samsung: Uses Family Link and Samsung Kids and Samsung security layer (more control, more set up steps)

Result

Both set ups provide:

- Parent-controlled account
- Screen time limits
- App approval system
- Usage monitoring

Samsung adds:

- Dedicated kid mode (Samsung Kids)
- Extra device security tools
- Additional app store oversight

Microsoft Family Safety

It lets parents manage and monitor a child's device in a similar way, especially on Windows PCs, Xbox, and Microsoft accounts.

It works by linking a child's Microsoft account to a parent's account, so the parent can:

- Set screen time limits
- Approve app downloads
- Filter websites in Microsoft Edge web browser

View activity reports showing what apps and sites are being used.

Official resource: [Microsoft Family Safety](#)

Microsoft Safe Family Setup

1 Create or sign in to a parent Microsoft account

- Go to
- Sign in or create an account (this is the "parent account")

2 Open Family Safety

- Go to
- Or install the Microsoft Family Safety app (iPhone/Android)

3 Create a family group

- Click Create a family group
- Add yourself as Organizer (parent/admin)



4 Add your child

- Click Add family member
- Choose Child
- Enter child email:
- Either create a new Microsoft account for them
- Or use an existing one
- Send invite

5 Accept invite on child device

- On the child's device:
- Open email invite
- Accept joining the family group
- Sign in with child Microsoft account

6 Set up screen time limits

- On parent dashboard:
- Select child
- Go to Screen Time
- Set:
- Daily time limits
- Device-specific limits (Windows or Xbox separately)
- Bedtime schedules

7 Set content filters (web and apps)

- Go to Content Filters
- Turn on:
- Block adult websites
- SafeSearch (Bing)
- App and game age limits
- Allow or block specific apps

8 Enable activity reporting

- Turn ON:
- App usage reports
- Website history (Edge browser only)
- Search activity

9 (Optional) Install Microsoft Family Safety app

- On parent phone:
- Install app from App Store or Google Play
- Monitor:
- Screen time



- Location (if enabled)
- Activity alerts

Important notes

Works best on Windows PCs and Xbox and Microsoft Edge

Web filtering works mainly in Microsoft Edge browser

It does NOT fully control Chrome unless additional restrictions are applied, therefore if your child also uses chrome, it is still advised that you set up a Google Family Link account.

Router and DNS Filtering

Alternatively, you can make the router use a DNS (Domain Name Service, such as OpenDNS) that allows you to log into a website to select the content you want to block. For example, you can block Drugs, Guns, and Pornography using this method for all devices on your network. DNS is like the internet's phonebook that turns website names (like youtube.com) into the real address computers use. OpenDNS works by replacing your normal phonebook with one that also filters results, so it can block unsafe or inappropriate websites before your device connects to them.

OpenDNS Home Setup

Official resource: [OpenDNS setup guide](#)

OpenDNS Home Setup (Simple Short Guide)

- Find your router IP address
- On Windows systems:
 - Press Start
 - Type cmd → open it
 - Type ipconfig
 - Find Default Gateway (example: 192.168.1.1)
- On Mac systems
 - Click Apple menu
 - Go to System Settings
 - Click Network
 - Select your Wi-Fi
 - Click Details
 - Find Router (example: 192.168.1.1)
- iPhone/iPad:
 - Settings → Wi-Fi → tap (i) next to network
 - Find Router
- Android:
 - Settings → Wi-Fi → tap network
 - Find Gateway/Router

2 Log into your router

- Open a browser (Chrome/Safari)



- Type the router number (example: 192.168.1.1)
- Enter username/password (usually on router sticker)

3 Find DNS settings

- Look for:
- Internet Settings
- Network Settings
- WAN Settings
- DNS Settings

4 Enter OpenDNS

Easy Family Filter: This option is the prefiltered content geared towards families.

- 208.67.222.123
- 208.67.220.123

Full Control: This option lets you pick and choose the categories you want to block.

- 208.67.222.222
- 208.67.220.220

5 Save and restart router

- Click Save or Apply
- Restart router

6 Check it worked

Official resource: [OpenDNS test page](#)

Go to: in a web browser You should see: "You are using OpenDNS"

If you sign up for a paid OpenDNS account, you can get more information in your activity logs and more granular control of your home network.

Device-Level DNS Filtering

Maybe you just want to restrict and have visibility into limited devices instead of all devices on your network. This is how to apply OpenDNS on each device separately instead of (or in addition to) the router.

Use this if:

- You can't change router settings
- You want protection on phones using mobile data
- You want stronger control per device

1 iPhone or iPad (iOS)

Steps:

- Open Settings
- Tap Wi-Fi
- Tap (i) next to your network



- Scroll to Configure DNS
- Change from Automatic → Manual
- Remove existing DNS entries
- Add OpenDNS:
- Choose one:
- Family Filter (simple):
- 208.67.222.123
- 208.67.220.123
- Full Control:
- 208.67.222.222
- 208.67.220.220
- Tap Save

2 Android Phones or Tablets

Steps:

- Open Settings
- Tap Network & Internet (or Connections)
- Tap Private DNS (or Advanced settings)
- Select Private DNS provider hostname
- Enter one of these:
- Family Filter:
- family-filter-dns.cleanbrowsing.org
- (OR OpenDNS via app/manual Wi-Fi set up below)
- OR manual Wi-Fi method:
- Go to Wi-Fi settings
- Long press your Wi-Fi network
- Tap Modify network
- Change IP settings → Static
- Enter DNS:
- 208.67.222.123
- 208.67.220.123
- Save

3 Windows PC

Steps:

- Click Start → Settings
- Go to Network & Internet
- Click Wi-Fi or Ethernet
- Click Hardware Properties or Adapter options
- Select your connection → Properties
- Select Internet Protocol Version 4 (TCP/IPv4)



- Click Properties
- Select Use the following DNS servers
- Enter:
- Family Filter:
- 208.67.222.123
- 208.67.220.123
- Full Control:
- 208.67.222.222
- 208.67.220.220
- Click OK

4 Mac (macOS)

Steps:

- Click Apple menu ()
- Go to System Settings
- Click Network
- Select Wi-Fi
- Click Details
- Go to DNS
- Click +
- Add OpenDNS servers:
- Family Filter:
- 208.67.222.123
- 208.67.220.123
- Full Control:
- 208.67.222.222
- 208.67.220.220
- Click OK or Apply

5 How to Confirm It Works

On any browser, go to:

- You should see “You are using OpenDNS”

Important limitations

- This only protects the device you configure
- Mobile data (cellular) may bypass Wi-Fi DNS unless configured separately
- VPN apps can bypass OpenDNS

For broader coverage, configure filtering at the router and use device-level controls as an additional layer.

Alternative Home Routers

Official resource: [AmpliFi Alien](#)



AmpliFi Alien is one example of an app-managed home router with separate networks and device controls. Product features and support can change, so review the current specifications before purchase.

Official resource: [NETGEAR and UniFi](#)

NETGEAR Orbi and Ubiquiti UniFi are other examples. They differ in cost and technical complexity, but both may provide more visibility and control than a basic provider-supplied router.

Approved-Content Video Apps

Official resource: [Safe Vision setup](#)

1 Install the app

- Download Safe Vision from:
- Google Play Store (Android)
- Apple App Store (iPhone/iPad)
- Amazon Appstore (Fire tablets)

2 Create a parent account

- Open the app
- Sign up with your email
- Create a parent password (PIN)
- This password controls all settings

3 Choose your child's age

- Select your child's age range
- The app will automatically:
- Filter videos
- Block inappropriate content
- Adjust recommendations

4 Add approved content

- Search for YouTube channels or videos
- Add only what you want your child to see
- You can also remove or block channels anytime

5 Switch to Child Mode

- Tap "Switch to Child Mode"
- Hand device to your child
- Only approved content will be visible

6 (Optional) Set limits

- Limit number of channels (free version has limits)
- Set screen time limits (premium feature)
- Manage multiple child profiles (premium feature)



Separate Parent and Child Computer Accounts

If you take the time to go through all this only to let your child have administrative (elevated) access on your machine, they can easily bypass all your efforts. Let's discuss how to harden the machine so they cannot circumvent all our hard work.

As previously mentioned, you will create a separate Administrator account for parents only and ensure children use standard (non-admin) accounts.

This prevents children from:

- Installing unwanted software
- Changing system settings
- Removing security tools or parental controls

Windows 10 and 11

1 Create a Parent Admin Account

- Click Start → Settings
- Go to Accounts
- Click Family & other users
- Click Add account
- Select:
- "I don't have this person's sign-in information"
- Click:
- "Add a user without a Microsoft account"
- Create:
- Username (example: ParentAdmin)
- Password (strong password)

2 Make the account an Administrator

- Go back to Family & other users
- Click the new account
- Select Change account type
- Set to:
- Administrator
- Click OK

3 Create Child Account (Standard User)

- Go to Family & other users
- Click Add account
- Choose Add a child account (Microsoft account preferred)
- Or create local account:
- "Add a user without a Microsoft account"
- Make sure account type is:



- Standard User (NOT Administrator)

4 Confirm set up

- Parent account = Administrator
- Child account = Standard user

macOS

1 Create Parent Admin Account (if needed)

- Click Apple menu
- Go to System Settings
- Click Users & Groups
- Click Add Account
- Enter admin password
- Create new user:
- Name (ParentAdmin)
- Password
- Set:
- Administrator

2 Create Child Standard Account

- Go to System Settings → Users & Groups
- Click Add Account
- Choose:
- Standard
- NOT Administrator
- Create:
- Child username
- Password

3 Verify account roles

- In Users & Groups:
- Parent = Administrator
- Important rules for both Windows and macOS

IMPORTANT RULES (both system types)

- Never let child accounts have Administrator access
- Only parents should know admin passwords
- Use Screen Time or Family Link or Microsoft Family Safety alongside this set up
- Do NOT share admin credentials with children



Gaming Console Parental Controls

PlayStation

Official resource: [PlayStation parent safety guide](#)

Set up Family Management

- Go to Settings
- Select Family and Parental Controls
- Choose Family Management
- Sign in with a parent (adult) PlayStation Network account

Add child account

- Create or add child PSN account
- Set age (this determines restrictions automatically)

Set controls

- Game age ratings (ESRB or PEGI limits)
- Play time limits (daily/weekly)
- Spending limits (PlayStation Store)
- Online communication restrictions (chat, voice, friends)

Manage anytime

- Settings → Family Management → select child

Xbox

Official resource: [Microsoft Family Safety](#)

Set up family group

- Go to
- Create or sign in with parent Microsoft account
- Add child account

Link Xbox

- Sign into Xbox using child account
- Device automatically syncs with family settings

Set controls

- Screen time limits (daily hours)
- Content filters (game ratings)
- Online multiplayer permissions
- Friend requests and messaging controls
- Purchase approval ("Ask a parent")

Mobile control app

- Install Xbox Family Settings app (iOS/Android)
- Manage limits remotely



Nintendo Switch and Switch 2

Official resource: [Nintendo parental controls](#)

Set up app control

- Download Nintendo Switch Parental Controls app
- iOS or Android
- Link console using pairing code

Create parent control PIN

- Set 4-8 digit PIN (required to change settings)

Set restrictions

- Game age limits
- Play time limits (daily)
- Sleep time alarm (optional shutdown)
- Online communication restrictions
- Screenshot/social sharing limits

Monitor activity

- View:
- Play time per game
- Most played games
- Daily usage reports

Photo Metadata and Location

iPhone and iPad

Turn off photo location data (This stops new photos from saving GPS location data.)

- Open Settings
- Tap Privacy & Security
- Tap Location Services
- Tap Camera
- Select:
- Never
- OR Ask Next Time

Remove location before sharing

- Open the Photos app
- Select a photo
- Tap Share
- Tap Options
- Turn OFF:
- Location
- Share the photo



Android

Turn off photo location data (This stops new photos from saving GPS location data.)

- Open Camera
- Open Settings
- Find:
- Location Tags
- OR Save Location
- Turn it OFF

Remove metadata before sharing

Some Android devices remove location automatically when sharing, but not all do.

For best privacy:

- Take a screenshot before sharing OR
- Use a metadata remover app

Samsung

Turn off photo location data (This stops new photos from saving GPS location data.)

- Open Camera
- Tap Settings
- Find Location Tags
- Turn it OFF

Remove metadata before sharing

- Open Gallery
- Select photo
- Tap Share
- Tap:
- Remove location data
- OR Remove metadata
- Share the photo

It is important to know that photo metadata can contain:

- GPS location
- Date/time
- Device information

Turning off location tagging helps protect your privacy and prevents others from seeing where photos were taken or using that data to build a profile on you or your children.

Email Oversight and Forwarding

Note that you can forward email from any service provider to another. For example: Gmail to iCloud.



Gmail

Official resource: [Gmail forwarding](#)

Steps:

- Log into the child Gmail account
- Click the gear icon → See all settings
- Go to Forwarding and POP/IMAP
- Click Add a forwarding address
- Enter the parent email address
- Open the parent email and confirm the verification code
- Go back to settings and choose Forward a copy of incoming mail
- Save changes

Outlook and Hotmail

Official resource: [Outlook forwarding](#)

Steps:

- Sign in to the child Outlook/Hotmail account
- Click Settings (gear icon)
- Go to Mail → Forwarding
- Turn on Enable forwarding
- Enter the parent email address
- Save changes

Yahoo Mail

Official resource: [Yahoo forwarding](#)

Steps:

- Sign into the child Yahoo Mail account
- Click Settings (gear icon)
- Select More Settings
- Go to Mailboxes
- Select the child mailbox
- Find Forwarding
- Enter the parent email address and verify it

iCloud Mail

Official resource: [iCloud forwarding](#)

Steps:

- Sign in to iCloud Mail
- Click Settings (gear icon)
- Go to Preferences
- Select General
- Enable Forward my email to



- Enter the parent email address
- Save changes

Important note: Email services and forwarding options change. Review the provider's current help page and explain the family's oversight rules to the child.

KEY TAKEAWAY

Use layers: child accounts, separate administrator access, app approval, content filtering, updates, and regular review. No single setting is enough.



CHAPTER 10

Artificial Intelligence and Deepfakes

Artificial Intelligence (AI) works by learning patterns from large amounts of data and then using those patterns to make predictions, answer questions, generate content, or solve problems.

A simple way to think about it is:

Traditional software follows fixed instructions written by a programmer.

AI learns from examples instead of only following strict rules.

For example, an AI trained on millions of photos of cats and dogs learns the visual patterns that make a cat look different from a dog. Later, when shown a new image, it predicts which one it is based on what it learned.

Modern AI systems are usually built using “machine learning” and “neural networks,” which are computer systems designed to loosely mimic how the human brain recognizes patterns. The AI is trained by processing huge amounts of data repeatedly, adjusting itself each time to improve accuracy.

Large AI models like chatbots are trained on enormous amounts of text from books, websites, conversations, and other written material. They learn relationships between words and concepts so they can predict what response is most likely to come next in a conversation.

AI does not “think” or “understand” the world like a human does. Instead, it uses statistics, patterns, probabilities, and training data to generate responses or decisions that often appear intelligent. The quality of an AI system depends heavily on:

The data it was trained on

The design of the model

The rules and safeguards built around it

Ongoing updates and monitoring

AI technology is improving rapidly and is now used in:

Search engines

Voice assistants

Cybersecurity

Medical systems

Self-driving features

Recommendations (YouTube, Netflix, Amazon)

Image and video generation

Customer support and chatbots



Like any technology, AI can be helpful or harmful depending on how it is used, which is why understanding privacy, security, and safe usage is important.

One of the biggest dangers of AI is how easily it can be used for scams and misinformation. Criminals can use AI to create fake phone calls that sound like a family member, fake videos called “deepfakes,” or convincing phishing emails designed to steal passwords or money. AI-generated social media accounts and chatbots can also pretend to be real people to manipulate users emotionally or gain trust. As AI technology improves, these scams are becoming more believable and harder to detect.

AI-generated media can sometimes contain unnatural motion, inconsistent lighting, distorted backgrounds, mismatched lip movement, or visual details that change between frames. However, these clues are becoming less reliable. Writing style, punctuation, or the use of a particular dash is not proof that content was generated by AI.

Online accounts that post highly polished content but have very little personal history should also raise suspicion. Messages that create panic, urgency, or pressure, such as asking for money immediately or demanding personal information, should always be treated with extreme caution.

Staying safe online requires a combination of awareness, critical thinking, and good security habits. People should avoid trusting information immediately just because it looks professional or emotional. Important claims should be verified using reliable sources, and suspicious phone calls, emails, or messages should be double-checked before responding. Personal information, passwords, and financial details should never be shared with unknown individuals online. Using strong passwords, password managers, enabling multi-factor authentication (MFA), and keeping devices updated with security patches also helps reduce risk.

Parents and schools also play an important role in teaching children how to safely use technology and recognize online manipulation. Open conversations about scams, fake content, cyberbullying, and online predators are becoming increasingly important as AI tools continue to evolve. Technology, apps, and online threats are constantly changing, which means learning about online safety must be an ongoing process rather than a one-time lesson.

AI itself is not automatically good or bad. Like most technology, its impact depends on how people choose to use it. Understanding how AI works, recognizing its risks, and developing safe online habits are some of the best ways to protect yourself and others in an increasingly digital world.

When a message, call, image, or video may be synthetic, do not rely on a single visual trick. Use independent verification:

- Contact the person through a phone number or account you already know, rather than replying through the suspicious message.
- Ask a private question or use a family verification phrase that a stranger would not know. Avoid questions whose answers are posted publicly.
- For money requests or emergencies, pause and confirm with another trusted person. Assume that voices, caller ID, screenshots, and video can be faked.

KEY TAKEAWAY

Treat voices, images, videos, messages, and caller ID as evidence to verify, not proof by themselves.



CHAPTER 11

General Cybersecurity for Families

Good online safety habits are important for everyone because most cyberattacks target normal everyday users, not just large companies. Scammers and hackers often try to trick people into clicking fake links, downloading harmful files, or giving away passwords and personal information. One of the easiest ways to stay safer online is by using antivirus software.

On Windows, Microsoft Defender and the built-in security features are appropriate for many families when the system is updated and used safely. Phones and tablets also include built-in protections. Additional reputable security software may help in some situations, but no app can make unsafe behavior harmless.

It is also important to use the correct type of account on computers and devices. Parents should create a separate administrator account as discussed in previous chapters and use a standard user account for everyday activities like browsing the internet, gaming, schoolwork, and email. This helps prevent harmful software from making major changes to the device without permission.

Families can also use services such as Microsoft Family Safety and Google Family Link to help manage screen time, app downloads, and online activity.

Browsers are a common path for scams and unwanted downloads. Built-in tracking protection, safe-browsing warnings, and a reputable content blocker can reduce exposure. Advanced script-blocking tools can provide more control but may break websites and are usually best for experienced users.

People should also avoid scanning random QR codes, clicking suspicious links, or opening attachments from unknown sources because scammers often use these methods to spread malware or steal information.

Strong passwords are another important part of online safety. Each account should have its own unique password, and users should consider using a password manager (an app that securely stores passwords) to help keep track of them.

Devices should also be locked using a password, PIN, or biometrics (fingerprint, facial recognition, etc) so that strangers cannot access them if they are lost or stolen. It is also a good idea to encrypt your device or any drives you may attach containing sensitive files to prevent them from being accessed if lost or stolen. As this is devices or operating system or software specific process we will not cover how to do this here. If you require assistance with encrypting your device, I advise checking with your local IT support (GeekSquad, an MSP, or even your internet or phone carrier) for assistance.

Multi-factor authentication, also called MFA (an extra security step such as a text message code or authentication app), should be turned on whenever possible because it helps protect accounts even if someone steals a password.

Keeping devices updated is also extremely important. Software updates often fix newly discovered security problems before hackers can take advantage of them.

Protect home Wi-Fi with a strong administrator password, a separate Wi-Fi password, and WPA2 or WPA3 encryption. On public Wi-Fi, verify the network name, keep file sharing off, and avoid sensitive activity on



devices that are not updated. Most modern websites encrypt traffic with HTTPS; a reputable VPN can add privacy in some situations, but it does not protect against phishing or unsafe downloads.

It is also worth backing up your data to an external drive or using a service such as Microsoft OneDrive, Google Drive, or iCloud. As these steps are specific to the method and vendor you choose, I will not outline how to do this here and would advise checking with your local IT (GeekSquad, an MSP, or even your internet or phone carrier) for assistance.

However, I will say that the cloud-based backup solutions are usually rather simple. You typically just sign into your account and on the first-time login you select the file locations you want to backup to the cloud and it just backs them up for you. Then, should you ever need to recover from a catastrophic event such as your laptop hard drive crashes, becomes encrypted by ransomware (a method used by hackers to digitally lock all of your files and ransom them back to you.) or the device is stolen, you simply log back into your cloud backup service and it will resync (copy and update) all of your data back to your new drive or device.

Technology changes quickly, and online threats constantly evolve along with it. Staying safe online is not something you do once and forget about. The best protection comes from staying informed, thinking carefully before clicking or downloading anything, using security tools properly, and practicing safe online habits every day.

KEY TAKEAWAY

Strong passwords, MFA, updates, backups, standard user accounts, and careful clicking prevent a large share of ordinary household security problems.



CHAPTER 12

Your Family Online Safety Plan

Use this chapter to turn the ideas in the guide into a short, repeatable household routine.

- ☐ Every family member knows they can report an uncomfortable message, image, request, or mistake without losing access before an adult understands what happened.
- ☐ Children use individual child accounts rather than a parent account or an administrator account.
- ☐ App downloads, purchases, and subscriptions require approval.
- ☐ Screen-time, downtime, communication, and content settings match each child's age and maturity.
- ☐ Location sharing, photo metadata, contacts, microphones, cameras, and notification previews are reviewed.
- ☐ Email, gaming, and social accounts use unique passwords and multifactor authentication where available.
- ☐ Devices and apps install security updates automatically.
- ☐ The family has a private verification phrase for urgent calls or messages requesting money or secrecy.
- ☐ Parents know how to block and report users on the games and platforms their children use.
- ☐ Important family files and photos are backed up.

QUARTERLY REVIEW

Review the plan every three months and whenever the family adds a new device, app, game, online friend group, or payment method.

The internet gives children incredible opportunities to learn, communicate, and explore, but it also exposes them to risks that change constantly. Parents must remain actively involved in their children's digital lives because online threats, apps, devices, games, and communication platforms evolve faster than most families realize. What was considered safe a year ago may no longer be safe today.

Parental controls, screen time settings, DNS filtering, content restrictions, and child accounts are all important tools, but no technology solution is perfect on its own. Children often learn new apps, workarounds, and online trends quickly, while predators, scammers, cyberbullies, and malicious content creators continuously adapt their methods to target younger users. New social media platforms, games,



chat systems, AI tools, and encrypted messaging apps appear regularly, creating new risks that many parents may not immediately recognize.

Because of this, parents should approach online safety as an ongoing process rather than a one-time set up. Devices should be configured with separate child accounts that do not have administrator access, parental controls should be enabled on phones, tablets, gaming consoles, and computers, and home internet filtering solutions such as OpenDNS should be considered. Parents should also regularly review privacy settings, monitor app installations, understand the games and platforms their children use, and keep all devices updated with the latest security patches.

Most importantly, technology should support, not replace, communication and trust. Children must feel comfortable talking to parents and guardians about uncomfortable online experiences, suspicious messages, cyberbullying, scams, or inappropriate content. Open conversations combined with consistent supervision, education, and layered security controls provide the strongest protection.

Online safety is not a “set it and forget it” task. Systems, technology, apps, and online threats are always changing, which means parents must stay informed, adaptable, and engaged in order to help keep their children safe in today’s digital world.

KEY TAKEAWAY

Online safety is a routine, not a one-time setup. Review the family plan after new devices, new apps, major updates, or changes in a child's maturity.



RESOURCES

Reporting and Official Guidance

Save these resources before an incident occurs. In an emergency or when a child is in immediate danger, contact 911 or local emergency services.

Resource	How it helps
NCMEC CyberTipline	Report suspected online enticement, child sexual exploitation, trafficking, or child sexual abuse material.
FBI Internet Crime Complaint Center (IC3)	Report cyber-enabled fraud, scams, account compromise, and other internet crime.
Federal Trade Commission ReportFraud	Report fraud, scams, deceptive businesses, and unwanted calls or messages.
CISA Secure Our World	Family-friendly guidance on phishing, passwords, multifactor authentication, updates, and safer digital habits.
Apple Family and Screen Time	Current Apple guidance for child accounts, Family Sharing, Screen Time, and parental controls.
Google Family Link	Current Google guidance for supervised child accounts, app controls, screen time, and content settings.
Microsoft Family Safety	Current Microsoft guidance for Windows, Xbox, activity reporting, screen time, and content filters.
PlayStation Parent Safety Guide	Family accounts, playtime, communication, content, and spending controls.
Nintendo Parental Controls	App-based playtime, age-rating, communication, and activity controls for Nintendo systems.

Resource links and menu names were reviewed for this July 2026 edition. Services can change without notice.



ABOUT THE AUTHOR

Patrick W. Upman

Patrick W. Upman is the founder of Home Safe Advisor and a parent who grew up alongside the modern internet. He has worked in information technology since 2008 and has focused on cybersecurity since 2012. His professional background includes enterprise security, vulnerability management, technical support, infrastructure, and risk-focused work. He holds the CISSP and CRISC certifications, along with additional IT and security credentials.

Patrick created this guide to give families practical language, realistic expectations, and step-by-step starting points. Home Safe Advisor provides home safety, security, technology guidance, online-safety education, routine household support, and referrals for specialized services. Home Safe Advisor is not a caregiver, medical provider, law-enforcement agency, or substitute for a licensed contractor or qualified professional.

WEBSITE RESOURCE

This e-book may be downloaded free from the Home Safe Advisor website. Share the original download page with other parents, schools, HOAs, and community organizations so they receive the newest edition.

[Visit Home Safe Advisor](#)

Tier 1 Services LLC d/b/a Home Safe Advisor