A PARENT'S GUIDE TO

Internet Filtering & Monitoring

axis

Your ultimate goal is to raise kids who use the Internet safely and responsibly and think critically about their actions, but a little technical assistance can help. And, as your kids get older, you'll need to dial down the restrictions to help them develop their own sense of responsibility.

—Common Sense Media

Monitors and Filters Are Useful, But They Shouldn't Replace Relationships

There's no question that there's a lot of filth on the Internet. And it's pretty easy to run into it, even accidentally. Internet filters are extremely useful tools for preventing you and your children from encountering content that is harmful and disturbing.

But in the same way that sending your kids to Christian school won't automatically make them Christians, setting up an Internet filter won't in and of itself keep them from online dangers. Why? For two reasons: 1. People on the other end of the Internet are constantly developing new ways to access new people (for various reasons); and 2. If our tech-savvy kids are determined, they *will* find ways around anything we implement. Because of that, we hope that parental controls are just one part of your overall strategy for protecting your children. Don't view Internet filters as ***the*** safety net that will keep your kids safe. Instead, view them as your first line of defense. Your priority should be training your kids to think critically and discipling their hearts to ***want*** to pursue what is good and to hate what is evil.

Because Internet filters are a good resource, we want to highlight what we think are some of the most helpful solutions currently available. Keep in mind that our list is not exhaustive (if it were, we'd never stop writing!), but will hopefully help point you in the right direction.

Why aren't filters enough?

There are several reasons why filters alone are not an effective safeguard for your children. First, human beings create filters, and where a human being creates something, there is always the potential for error. No algorithm will catch everything we want it to catch. A study from the University of Oxford found that Internet filters were fairly ineffective at protecting teenagers online. It concluded "that resources would be better spent trying to develop the resilience of teenagers to such experiences." In addition, we can't filter our kids' worlds forever. They will grow up, so we need to teach them how to be responsible adults, not try to shelter them forever.

Don't get us wrong—we think Internet filters are great. But we can't fall into the trap of thinking that if we get one, we can kick back and never worry about our kids encountering graphic content. Pornography still (surprisingly) exists in print, and many scenes in non-X-rated films could be classified as soft-core porn. They could even see it at a friend's house or on a friend's device. We simply cannot control every place where they might encounter it or what might pique their curiosity. And if kids are curious and determined enough, they will find a way to get around any parental controls we install. (If you're wondering how, this article from Protect Young Minds provides a list of some of the ways kids might bypass parental controls.)

So we should put up defenses where we can, but we should also take an offensive approach to protecting our kids. Educate them on Internet safety. Talk to them about the challenges of interacting with people online versus in real life. Start the conversation with them about porn before porn starts it with them behind our backs (see our upcoming guides on pornography for more information on how to do so).

What's the difference between Internet filters, Internet monitors, and parental controls?

Good question! Though the terms are often used interchangeably, for the purposes of this guide, we'll use them to refer to different things.

Parental controls refer to the built-in controls on a device that restrict access to content. You can learn how to utilize parental controls on Android devices here. On iOS devices, Apple refers to them as "Restrictions," and you can access Apple's guide to turning them on here. (Or check out our Parent Guide bundle, "A Parent's Ultimate Guide to Smartphones," which covers both Android and iOS devices in depth.) Other devices, like gaming consoles and tablets, often come with (limited) parental controls as well.

Internet filters are third-party software or hardware that needs to be installed in order to restrict or otherwise limit access to online content.

Internet monitors are third-party software or hardware that needs to be installed in order to simply record one's Internet activity and usage, then deliver a report that details sites visited, time spent online, etc.

What's the best strategy for implementing filters and monitors?

Think about using Internet filters and monitors like teaching kids not to trust strangers. We all do it because we know that when they're young and innocent, they view people as good and the world as a safe place, so they need us to firmly make them aware of "stranger danger" while also keeping them in our sight at all times. But then as they age and become more aware and capable, we slowly let them out of our sight and trust them to be discerning until they strike out on their own.

Though Internet filtering is new territory, we should approach it similarly (if not with *more* caution, since the number of "strangers" that can be encountered exponentially increases). In an ideal situation, the best strategy for protecting our kids online would start with strict Parental Controls *and* filters *and* monitors when they're young and first using devices.

As they get older and we continue to have formative conversations with them about things like social media, cyberbullying, and pornography, we would slowly reduce the strength of our filters and Parental Controls while continuing to monitor their activity closely, as well as letting them earn more privileges and responsibilities. (But the converse would also be true: If they prove not to be trustworthy, then these privileges and responsibilities would be revoked.)

As they continue on toward adulthood, the filtering would be reduced to minimal levels, while monitoring would be somewhat reduced and accountability would be at its highest. Then, if we've done our jobs properly, when they leave the home for the "real world" and total Internet freedom, they will be prepared for what they will face, as well as recognize the dangers and pitfalls for what they are while understanding how necessary continued submission to accountability is in our Internet-enabled world.

Sounds great, but my situation is definitely not "ideal." So what do I do?

No situation is actually ideal when it comes to the Internet and technology. We're all still trying to figure out how to navigate this ever-changing, constantly connected world in which we find ourselves, and thus far, there's no manual for how to do it. So no matter how old your children are or how much you feel like you've "messed up," it's never too late to start introducing technology accountability into your home (just like it's never too late to start teaching kids to protect themselves from physical strangers!).

If your kids are older, start by having conversations with them about what you'd like to implement. Explain why, let them ask questions, express frustrations, etc. But make it clear that the accountability will be for everyone in the home (not just them!). If necessary, point them to Scripture showing God's desire for each of us to be under authority and have accountability (Gal. 6:1-5, Jam. 5:16, Prov. 27:17, 1 Thess. 5:11, Heb. 4:13, Heb. 13:17, etc.). They may be angry at first, but if done well, they will eventually come to see that it's good for them. (If they continue to be angry and try to get out of it, it may be because there's already something they don't want you to see or know about. If that's the case, then you know you're on the right trail! Just make it clear that you're on their side and want to help them truly flourish, not be the bad guy.)

Once you've had the conversations with them, figure out what's age appropriate for each of your kids (some may still require lots of filtering, while others are older and should have monitoring and accountability instead). Then slowly begin introducing the new systems into your home.

What do I need to know before deciding on an Internet filter?

While we definitely disagree with the LDS Church's theology, their article about Internet filters is a great resource for getting a basic understanding of the different ways that filters work. It's helpful to understand the types of filters out there so that you know which are the best solutions for your family.

The majority of filtering solutions are types of **software**, meaning that you download them and install them on your devices. Software moderates the communication between your computer and the Internet. Software-based Internet filters tend to have the most variety of features and the greatest capacity for customization.

Others are **hardware** solutions. For example, you could buy a router that filters all devices connected to your Internet. The advantage of hardware solutions is that they tend to be more difficult to bypass than software. The disadvantage of hardware is that it is limited to your house and tends to be less customizable.

Another way of filtering is through a DNS (Domain Name System). Though understanding the technical sides of these things can be tricky, suffice it to say that it helps humans (who largely communicate with and understand words) interact with computers (which largely communicate using series of numbers). (Still confused? Learn everything about DNS here.) The advantage of having a DNS filter is that you can use it to filter any device in your home that connects to

your WiFi. A disadvantage is that DNS solutions are more limited (i.e. they don't filter anything using a cell network to access the Internet).

Some solutions work through a VPN (virtual private network). As you would expect, Internet filters that work through a VPN filter content through their own networks. (But beware: Just as we can use VPNs to filter content out, our teens can easily read online how to use VPNs to get around our filters...)

Before you decide which filters you need, **you should decide which devices you want to protect**. If you're concerned about devices at home, you'll probably want focus on something that filters every device through your WiFi. It's a good idea at the outset to investigate what protections are available to you through configuring your router. Be aware that if your children have smartphones, they can use cellular data to go online. So even if you set up a tool that filters through your router and covers all devices that connect to it, your kids could always switch to their phone data to bypass those restrictions.

If you go with a software solution, remember that it might not be able to protect every Internet-aware device you have in your home if your kids have iPods or gaming consoles.

Your operating system also impacts your choice of filter. While we've tried to recommend filters that work with a variety of operating systems, parental control solutions usually favor certain systems over others. (As a side note, some operating systems have protections already built into them, and it would be worth your time to explore these. For example, Apple has recently rolled out some new features for setting up parental controls on its devices, though Android is still ahead when it comes to the level of control a parent can have on a device. That may impact what device you get for your children, if you haven't decided already.)

Check out this article for good habits for protecting your privacy online. Consider using Google SafeSearch, a tool Google has created to block explicit content online. It's not infallible, but it is somewhat helpful for catching objectionable content.

When evaluating your options for Internet filtering, it's good to "consider how much time your kids spend online, how much supervision you can provide while they're online, how technically savvy they are, and whether they have a history of searching for age-inappropriate stuff."

What are some criteria for good filters?

The best filtering solutions have many of the same features in common. One of the most essential is **content filtering**. Does the filter distinguish between different categories of content? How in-depth does it analyze the content? Some solutions go so far as to scan pages in real time, allowing certain pages on a site, but not others.

Does the solution filter or block secure (HTTPS) sites? Is it browser independent, meaning that it will filter content on any browser someone uses? Will it filter content if your child tries to use an anonymous proxy server?

What about online games, smartphone apps, videos, social media, chat, or email? Certain solutions have the ability to filter these types of content, while others don't. Some filters are so thorough that you can set them up to take periodic screenshots and record keystrokes. While this ability is impressive, when it comes to older children, we would caution against being too invasive and trying to decipher every little action they take online. It will probably be a lot more effective to implement a solid filter while focusing on setting up accountability and having good

conversations with them.

Also, **there is no Internet filter that we are aware of that is able to monitor every possible social media account or app your child might use**. Those that do monitor social media require children to give parents their login information, which means that your kids will have to buy into you overseeing their social media activity.

Another feature to look for is a detailed and clear activity log (clear as far as whose activity you are seeing). Ease of use, customization, real-time alerts, and compatibility with different operating systems are all helpful. Many solutions come with the ability to set time limits and to whitelist (allow) and blacklist (ban) specific URLs. Many Internet filtering solutions also offer a way to track and limit children's locations through geolocation and geofencing. "Geofencing" means setting up a perimeter in a certain area, and if your children go outside those boundaries, you will get an alert.

What are the top 10 filters you recommend?

In the following list, we've prioritized those that tend toward having the criteria we've just mentioned. If we included any that lack those criteria, it's because the solutions had other focuses and strengths that we felt made them at least worth mentioning. We've also prioritized those that encourage accountability through relationships. Keep in mind that Apple controls its devices more tightly than Android does, so it's normal for a solution's iOS capabilities to be more limited.

For the following seven recommendations, we've relied heavily on these reviews from *PC Mag*, as well as information from the companies themselves.

1. QUSTODIO

Qustodio is one of the most solid Internet filters on the market and appears to be highly recommended by just about everyone who reviews it.

Works with: 

Pros

- Strong content filtering: filters by category, browser independent, blocks anonymous proxies, filters HTTPS sites, evaluates web pages on a case-by-case basis
- Detailed activity log
- Extremely customizable time limits
- User-friendly: can set up and monitor activity from almost anywhere
- App blocking
- Facebook monitoring (but not Messenger)
- Location tracking
- Can read and block SMS (Android only)
- Child can press a panic button (Android only)
- Option to associate a profile or an entire device with a specific child

Cons

- Expensive
- Facebook is currently only social platform it reviews
- iOS version has more limits than Android version
- Antiquated online portal

Other info

- Free version protects one device, comes with web filtering, time quotas for activities, and records seven days of activity

Pricing

- Small Plan $54.95/year, 5 devices
- Medium Plan $96.95/year, 10 devices
- Large Plan $137.95/year, 15 devices

2. CIRCLE WITH DISNEY

Circle with Disney offers several parental control products. We recommend at least using the Circle Home device in conjunction with the companion app Circle Go. The reason is that Circle Home is a device you install that will filter all of the devices in your home, but Circle Go will protect your kids' devices when they leave the house. Note that Circle Home doesn't replace your router, but rather works with it.

Works with: 

Pros

- Content filtering by category, browser independent, blocks anonymous proxies, doesn't overblock, protects all devices in the router's network
- Circle Go protects a child's device even if using cellular data or a friend's network
- Detailed activity log
- Time limits
- User-friendly
- App blocking
- Circle Home is a good price
- Can pause the Internet
- Circle Home plus Circle Go is a unique model

Cons

- Circle Go currently only works with iOS
- Circle Go is easy to disable, but you'll be notified
- Confusing blocking messages appear when you access HTTPS sites
- No location tracking
- Circle detects all devices in your home, but it's confusing which ones it's talking about
- Assumes every device is used by one person

Other info

- Circle Go has a one-month free trial
- Can't use Circle Go without Circle Home

Pricing

- Circle Home $99 one-time fee
- Circle Go $4.99/month, 10 devices

3. KASPERSKY SAFE KIDS

Kaspersky Safe Kids is a well-rounded and highly affordable option for managing your children's Internet use.

Works with: 

Pros

- Content filtering by category, option to warn about content instead of just blocking it, evaluates web pages on a case-by-case basis (but only on Windows currently), blocks anonymous proxies, filters content on all the major browsers, flexible options for limiting Internet access, real-time alerts
- Activity log is in-depth
- Time limits
- User-friendly
- App monitoring and blocking (not on iOS)
- Monitors games on iOS
- Location monitoring and geofencing
- Thorough and customizable alerts
- Unlimited devices and profiles
- Inexpensive

Cons

- Good browser filtering, but failed to block off-brand browser (one the reviewer coded himself)
- Limited social media monitoring

Other info

- Free version lets you manage online activity, apps and devices

Pricing

- $14.99/year, unlimited devices and child profiles

4. MOBICIP

Mobicip has an interesting model in that it's cloud-based and that, once you determine your rules for your children's devices, an agent enforces those rules. The solution's filtering abilities are strong, and although it has some limitations, Mobicip is solid option.

Works with:

Pros

- Content filtering by category, browser independent, blocks anonymous proxies, blocks HTTPS sites, evaluates web pages on a case-by-case basis, child can request access to certain pages
- Activity log
- Time scheduling
- New apps blocked by default till parent approves (Mobicip doesn't filter their content once approved)
- Filters YouTube videos, works better than YouTube's Restricted Mode
- Ability to whitelist/blacklist specific sites
- No limit to how many profiles you add

Cons

- Could be more user-friendly
- Time limits feature is minimal
- No social media monitoring (apart from YouTube)
- No ability to cap Internet use
- Some communication issues with console and local agent who helps manage the app
- Feature that blocks specific words often overblocks

Other info

- Free version supports limited content filtering

Pricing

- $39.99/year, 5 devices, unlimited profiles

5. OPENDNS HOME

We highly recommend using OpenDNS along with a parental control software product. Used alone, OpenDNS is limited. But the free version of OpenDNS is pretty comprehensive, and because it is a DNS solution, it will filter all devices on your network. This is advantageous because it can filter gaming consoles and other Internet-aware devices, such as iPods. So if you get an Internet filtering software and use it with OpenDNS, you will get the broader range of features that the software provides while covering more devices than software can protect.

Works with: All devices

Pros

- Content filtering by category, blocks HTTPS sites and anonymous proxies (even at lowest filtering level), child has ability to request access to a site
- Activity log is detailed, but you can't break it down by device or user
- Ability to whitelist/blacklist specific sites
- Free version probably has all the features you would need

Cons

- No real-time analysis of content
- Extremely limited malware and phishing protection
- Reports show all URLs, even those that aren't websites
- Has none of the features offered by software (like real-time analysis of content, social media tracking, in-depth activity tracking, or real-time notification of problems).

Other info

- The VIP version retains activity logs for a year (vs. 2 weeks in the free version), allows your whitelists and blacklists to hold 50 URLs each (vs. 25 in the free version), and comes with a whitelist-only mode where users can only surf sites you've approved

Pricing

- Open DNS Home, Free
- Open DNS Home VIP, $19.95/year

6. NET NANNY

Net Nanny has extremely strong content filtering features. However, it is a bit expensive and its software needs to be updated.

Works with:

Pros

- Content filtering by category, option to warn about content instead of just blocking it, child can request access to blocked site, blocks HTTPS sites, blocks anonymous proxies, evaluates web pages on a case-by-case basis, customizable option for blocking profanity
- Activity log is very in-depth
- Time limits
- User-friendly
- Remote management and notifications of activity
- Ability to whitelist/blacklist specific sites

- Installing NetNanny on iOS doesn't count toward one of your licenses
- Can create child profiles (if child uses more than one device)

Cons

- Expensive
- No location monitoring
- iOS support is extremely limited
- Software needs to be updated
- No social media monitoring

Other info

- No free version
- No free trial

Pricing

- 1 device, PC or Mac, $39.99
- Family Pass (includes iOS and Android):
- $59.99/year, 5 licenses
- $89.99/year 10 licenses
- $119.99/year 15 licenses

7. SYMANTEC NORTON FAMILY PREMIER

Norton Family Premier is an affordable solution with a wide range of features. We also love that the company encourages parents to have open and ongoing conversations with their kids.

Works with:   

Pros

- Content filtering by category, has customizable options
- Activity log is detailed
- Time limits
- User-friendly
- App and messaging tracking (limited on iOS)
- Tracks YouTube and Hulu videos (but not videos on other online platforms)
- Location tracking
- Good web interface, can check on activity from any computer
- Child can request access to a site
- Affordable
- Relational model

Cons

- Doesn't currently work on Macs, limited features for iOS
- Advanced web tracking only possible through limited and easily disabled plugin
- Filter failed with some HTTPS sites and an anonymous proxy
- Doesn't block profanity if it's on a site that isn't in a restricted category
- Very limited social media supervision
- Doesn't monitor online gaming

Other info

- No free version
- 30-day free trial

Pricing

- $49.99/year (currently priced at $19.99 for the first year), unlimited devices

8. COVENANT EYES

Covenant Eyes is a good solution, but does lack some of the abilities of the best Internet filters available. We really wish it had the ability to monitor browsers independently and to filter secure sites. Points in its favor, however, are its strong emphasis on accountability and the extensive resources on its blog.

Works with:

Pros

- Content filtering based on six sensitivity ratings, can customize ratings, content filtering and blocking
- New VPN monitors more activity on iOS, such as Safari/Siri, YouTube, some apps; also forces safe search across all browsers
- Activity reporting sent to an accountability partner
- Time limits
- Panic button
- Strong customer support
- Can't uninstall without admin's permission
- Ability to whitelist/blacklist specific sites
- Relational model encourages accountability

Cons

- Features limited on Android
- No HTTPS filtering
- Have to use the CE browser to filter content, issues with effectively blocking Google images
- Limited monitoring features compared to other solutions
- No chat or email monitoring
- Android version difficult to use

Other info

- Specifically created to prevent porn use
- 30-day money back guarantee

Pricing

- Personal $11.99/month, unlimited devices, filtering is an extra $1.50/month
- Family $15.99/month, unlimited devices, no extra cost for filtering

9. LOCATEGY

Locategy is another solution that is a bit lacking in the area of content filtering, and it is mobile only. But if a primary concern is tracking your child's location in case of an emergency, this app is a good choice for you.

Works with:

Pros

- Content filtering by category, effective on the browsers it filters
- Activity log is basic
- App usage blocking and scheduling, remote app locking
- User-friendly
- Strong location tracking
- Remote wipe feature (if someone steals the phone)

Cons

- Expensive compared to similar products
- No browser independent filtering, only filters Chrome and Samsung browsers
- Can't block calls and messages
- No social media monitoring
- Limited features on child app
- Good iOS design, poor Android design

Other info

- Free model gives you 3 devices and the ability to block 1 app, reporting feature saves five days of data, app defines 2 places when geofencing

Pricing

- $20 for 3 device licenses
- $35 for 5 licenses
- $70 for 10 licenses

10. BOOMERANG

Boomerang is a decent parental control solution, but not quite as impressive as some of the earlier recommendations on our list. Note also that it is mobile only.

Works with:

Pros

- Category-based content filtering (although not listed alphabetically)
- App managing and blocking
- Activity reporting
- App usage scheduling, but not for individual days
- Location tracking and geofencing
- Monitors YouTube
- Monitors calls and texts on Android (limited monitoring for MMS)
- Can set up specific actions for emergencies

Cons

- Expensive
- No browser independent tracking feature—you have to use Boomerang's browser
- Poor web interface
- Have to configure individual devices, no single child profile for all devices
- No social media activity tracking, just records time spent on platforms
- Limited features on iOS

Other info

- iOS version is free (for now) but limited
- Android version has more features, but isn't free
- 14-day free trial

Pricing

- Android $12/device/year
- iOS free for one year

What filters didn't make the list?

Following is a list of filtering software we decided not to recommend for various reasons.

Screen Time
If you're an Android user, you still might want to check out Screen Time, a time-limiting and monitoring application. It does not *filter* content. We almost included it in our recommended list above, but it's only for smartphones and tablets, and the software's ability to report on web search history and to block apps only works on Android devices. So we felt this software was too limited include in our most recommended list. However, one mom we talked to loved its ease of use (can monitor and control everything from your phone) and its capabilities for her 12-year-old son's phone. However, she was quick to mention that because it doesn't have the ability to filter, she still keeps all browsers turned off.

Bark
Bark is not a content filtering solution. It's mobile only and is strictly for monitoring your kids' smartphone use. However, it is very good at what it does. We also like that it focuses on alerting parents of potential problems like cyberbullying, as well as encouraging and coaching parents on how to talk to their kids. This seems to be a better solution for older, more mature children, while other filtering options seem better for younger kids who aren't ready to be exposed to the entire world that is the Internet.

uKnowKids Premier
uKnowKids Premier is also not a content filtering solution, but strictly a monitoring tool. It is mobile only, although it does track Facebook, Instagram, and Twitter, though it's easy to disable. Its iOS version stands out for being uncommonly strong, but costs more than the Android version.

Spy Agent
Spy Agent was another software that almost made our list because of its strong content filtering in real time. A feature that sets it apart is its ability to record activity with extreme thoroughness. It documents keystrokes and microphone/webcam usage, and it can take periodic screenshots. However, it is limited because it only works on Windows, on top of which the model skews toward being invasive rather than focusing on relational accountability (what child would feel good about parents "spying" on them?).

McAfee Safe Family
McAfee has many of the basic features of the average Internet filtering software, but we saw enough user reviews complaining about bugs to make us hesitate to recommend it.

K9 Web Protection
K9 Web Protection is free, but lacks a lot of the features that most solid parental control solutions have.

Surfie
Surfie has many of the basics of parental control features, but is only compatible with Windows.

Verity
Verity can take scheduled screenshots and record keystrokes (but not login info), but it doesn't filter content by category and doesn't work well for blocking porn sites.

Alvosenet Parental Control
Alvosecure does offer browser-independent content filtering, but fails to block obvious porn sites and has poor activity reporting.

FamilyTime
FamilyTime has no content filtering, limited activity reporting, issues with lagging, and is easy for kids to uninstall.

Clean Router
Clean Router filters all devices on your network and can block HTTPS sites, but can let inappropriate content get through and is not effective if someone uses an anonymous proxy.

SafeDNS
SafeDNS filters all devices on your network, but has some clunky or limited features and no free version. OpenDNS is a solid, free alternative.

Forcefield
Forcefield allows you to curate hundreds of sites for your kids, as well as enable the apps to "sleep" (i.e., disappear). But it has no category-based content filtering and no browser-independent filtering. Also, it is somewhat buggy and expensive.

So how do I keep the conversations about Internet safety and accountability going?

As we've already said, we think that implementing parental controls should ideally take place in the context of open and ongoing conversations with your children. Here are some suggestions for how to talk to both your younger and older kids.

Discussion Questions (for younger kids)

- Do you understand why we block certain sites so you can't see them? Do you know what might happen if we didn't?
- What would you do if you saw something online that you didn't understand or that scared you? Would you tell us about it?
- How do you think we'd react if you told us about something you didn't think you should be watching?

Make sure your children know that if they see something inappropriate online, they can and should tell you about it, knowing that you will not be angry but will be thankful they were willing to trust you.

Discussion Questions (for teens)

- Do you think having an Internet filter is a good idea?
- What do you see as the purpose of getting a filter?
- Do you think that the way we've set up the filter gives you accountability without being invasive?
- Do you feel comfortable talking to us if you run across mature content online? Is there anything we can do to help you feel more comfortable?
- What do you think Philippians 4:8 means? How does it apply to what we do on the Internet and on our devices? How do you think God wants you to apply it to your own life?

Conclusion

Internet filters are a great idea and are much more sophisticated than they used to be, even compared to a few years ago. We hope this guide helps you figure out which ones would work best for your situation. As you continue in your journey to parent your kids well in our technological world, remember that nothing can replace open and honest conversations with your kids. And never forget that, as daunting as the Internet and all its content can seem, God is infinitely greater and loves your kids with reckless abandon. He longs for their hearts to truly love and worship Him, and He's working tirelessly through you and others to make that a reality.

Additional Resources

"20 Online Review Sites for Collecting Business & Product Reviews," HubSpot

"Bypassing content filters: How to see the web they don't want you to see," PC World

"5 Myths and Truths About Kids' Internet Safety," Common Sense Media

"What are some good rules for screen names and passwords?" Common Sense Media

"How can I make sure my kid isn't sharing too much on Facebook or Instagram?" Common Sense Media

"Google Family Link (for Android)," *PC Mag*

"ESET Parental Control (for Android)," *PC Mag*

"How to use parental controls on your child's iPhone, iPad, and iPod touch," Apple Support

"Set up parental controls," Apple Support

"A Parent's Guide to Smartphones," Axis (covers a "theology of smartphones" and how to decide when to get a child a smartphone)

"A Parent's Guide to iOS," Axis (details how to set up parental controls)

"A Parent's Guide to Android," Axis (details how to set up parental controls)

We're creating more content every day! If you found this guide helpful and valuable, check out axis.org/guides each month for new Guides covering all-new topics and for other resources.