

# The Household CTO

April 14, 2020



Hosted by Ben Murphy



**HARVEST  
BIBLE  
CHAPEL**  
PITTSBURGH NORTH

"Making conscientious choices about technology in our families is more than just using internet filters and determining screen time limits for our children. It's about developing wisdom, character, and courage in the way we use digital media rather than accepting technology's promises of ease, instant gratification, and the world's knowledge at our fingertips. And it's definitely not just about the kids."

-Andy Crouch, Tech Wise Family

[Becoming a Tech Wise Family on Dad Tired Podcast](#)




# What is a CTO?

Sometimes known as a chief technical officer or chief technologist, is an executive-level position in a company or other entity whose occupation is focused on the scientific and technological issues within an organization.

## Chief Technology Officer 🚔

- Is aware and vigilant (responsible for research)
- Creates and enforces rules (Biblically based)
- Serves and protects (family)
- Educates and facilitates (plans and implements)

# Awareness and Vigilance

Desktops , smartphones , tablets, smart TVs , fitness devices, security cameras, smart devices like the Google Home or Amazon Alexa, and much more have dominated our culture and attention over the past decade.

It's important and biblical to be aware of everything  
that is brought into your household.

(Prov 4:23 - Keep your heart with all vigilance, for from it flow the springs of life.)

# R.U.L.E.S.

- Realistic
- Unilateral
- Locked down
- Educationally based
- Servant Hearted



Procedure



**HARVEST  
BIBLE  
CHAPEL**  
PITTSBURGH NORTH

## Technology Audit

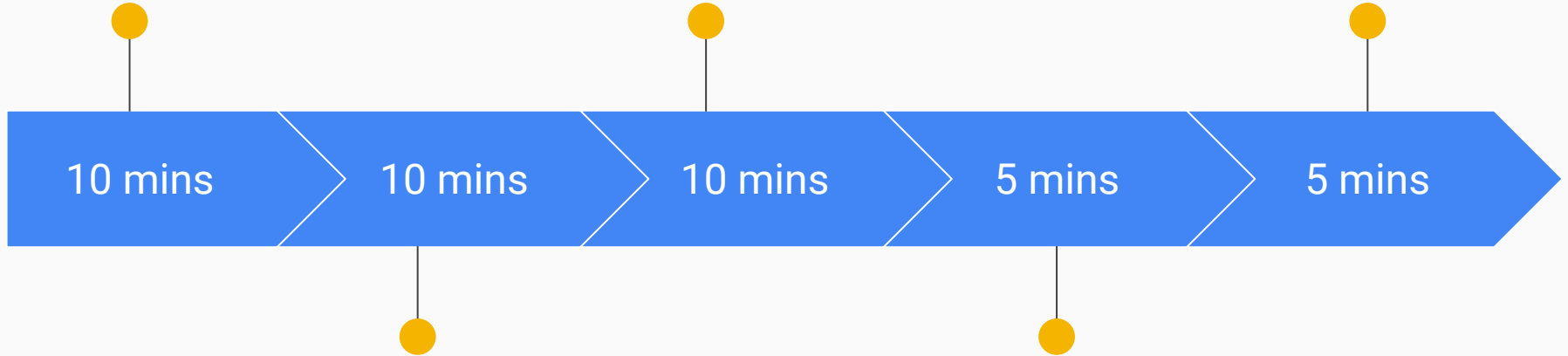
Count the number & types of devices in your home that have access to the internet

## More help needed?

Determine additional blocking, filtering, tracking & accountability needs

## Set up alerts / Homework

Optional, but helpful



## Set up DNS Filtering

Family or Home Account, set filter rules, download / install IP updater

## Set device schedules

Why allow your child to access the internet past their bedtimes?

# Network Care

If your home internet doesn't have a personal wifi router, one that's not provided by your ISP (Internet Service Provider), then I highly suggest you buy one.

Owning your own router enables you to:

1. **Save money each month!**

Most ISPs charge a monthly rental fee for their proprietary wifi routers that they "give" you upon installation of their services. I'm looking at you Comcast/Xfinity, Armstrong, Verizon FiOS, Time Warner Cable, etc.

2. **Have more flexibility to the content entering your home!** Ideally, this is what we're after today.

Ensuring that our loved ones are safe when on the internet.

3. **Control your internet experience:** ISP routers are filled with additional ways that they can "spy" on your internet usage, why bother giving them that information?

[Why You Shouldn't Use Your ISPs Default DNS Server](#) | [DNS over HTTPS](#)



# Network - Router Care

Owning your own personal wifi router comes with some responsibility in care.

You should do the following:

1. **Change the default router management password!** This is easily the biggest security hole within your home. Anyone can walk in (or from a distance since wifi travels outside), login to your router, find all connected devices, and begin finding data on your family through your connected devices.
2. **Check for firmware updates regularly (bi-monthly)!** Router manufacturers are constantly trying to keep up with hacking exploits and the basic home router is a massive attack vector because of the valuable data available on your network. Updating your router firmware gives you better security, new features, and sometimes faster internet speeds!
3. **Turn on your Guest Network!** Don't allow just anyone to jump on your personal family network. A Guest Network allows you to share your internet but doesn't let them see other devices on your personal family network.

# Internet Content Filtering

Would we walk our children into a Strip Club?

Would we knowingly turn on some porn instead of Disney+ for them and walk away while we go back to our work of cleaning the house?

I highly doubt it and pray that's not the case!

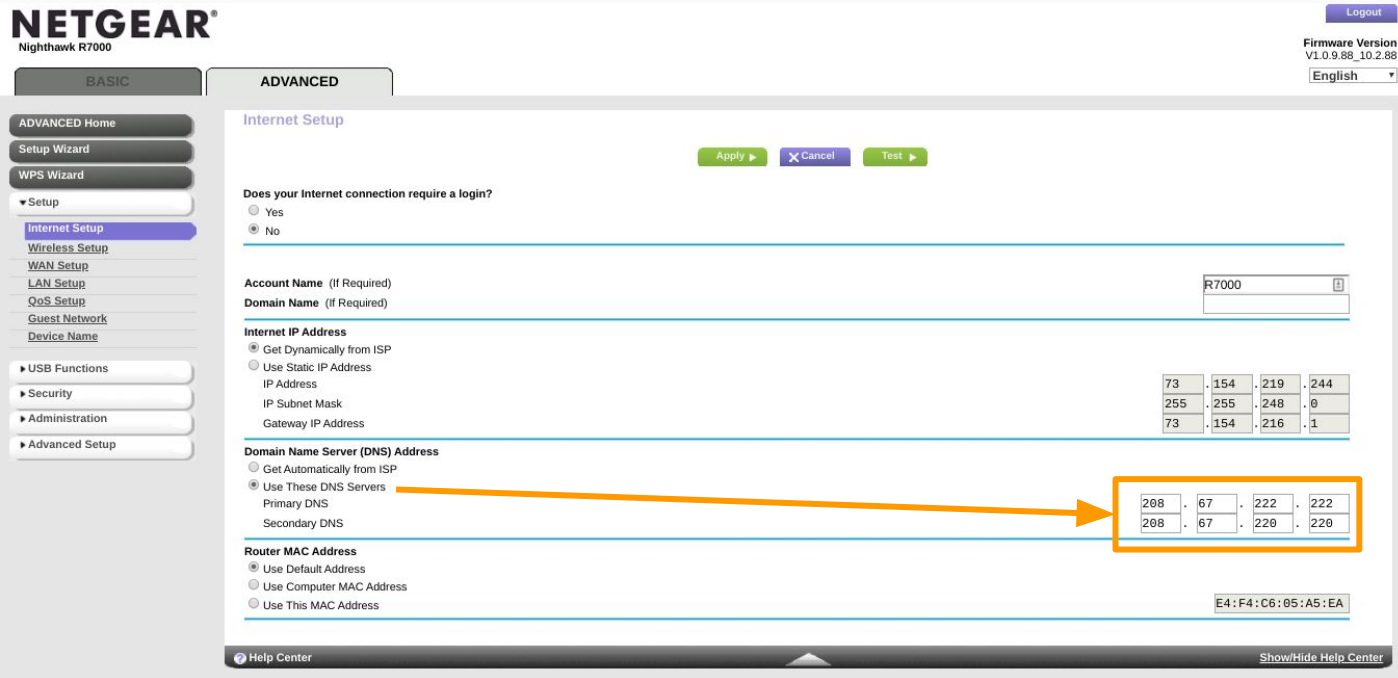
1. We should filter because we love our family and want to protect them
2. We should filter because we understand that seeing everything that they see is highly improbable and we need help
3. We should filter because God calls us to!

[Time to Talk - Family Life Podcast](#)

# Internet Content Filtering How-to

1. Setup free [Open DNS](#) / [Family Shield](#) or [Home](#) account
  - a. Cloudflare has an alternate free [Family Solution](#) as well: [Setup Instructions](#)
2. Adjust network router DNS settings to Open DNS
  - a. Log into your router settings: likely 192.168.1.1 or less likely 10.0.0.1
  - b. Find your DNS settings, typically found under the Internet Setup section
  - c. Enter the Open DNS given nameserver settings into your router DNS Address:  
**208.67.222.123** and **208.67.220.123**
3. Add the Open DNS ip updater app (for using the Open DNS Home only)
  - a. Windows IP Updater [Installer](#)
  - b. MacOS X IP Updater [Installer](#)
4. Update your browsers to resolve [DNS over HTTPs](#) (Firefox & Chrome only)

# Internet Content Filtering How-to



**NETGEAR**  
Nighthawk R7000

Logout

Firmware Version  
V1.0.9.88\_10.2.88

English

**BASIC** | **ADVANCED**

ADVANCED Home  
Setup Wizard  
WPS Wizard

Setup  
Internet Setup  
Wireless Setup  
WAN Setup  
LAN Setup  
QoS Setup  
Guest Network  
Device Name

USB Functions  
Security  
Administration  
Advanced Setup

**Internet Setup**

Apply | Cancel | Test

Does your Internet connection require a login?  
 Yes  
 No

Account Name (If Required) [R7000]

Domain Name (If Required)

**Internet IP Address**  
 Get Dynamically from ISP  
 Use Static IP Address  
 IP Address: 73 . 154 . 219 . 244  
 IP Subnet Mask: 255 . 255 . 248 . 0  
 Gateway IP Address: 73 . 154 . 216 . 1

**Domain Name Server (DNS) Address**  
 Get Automatically from ISP  
 Use These DNS Servers  
 Primary DNS: 208 . 67 . 222 . 222  
 Secondary DNS: 208 . 67 . 220 . 220

**Router MAC Address**  
 Use Default Address  
 Use Computer MAC Address  
 Use This MAC Address [E4:F4:C6:85:A5:EA]

Help Center | Show/Hide Help Center

Similar DNS settings should easily be found for all major residential wifi router brands such as:

- Asus
- Belkin
- Cisco
- D-Link
- Google
- Linksys
- Netgear
- TP-Link

# Device Assessment

**NETGEAR®**  
Nighthawk R7000

Logout

 Firmware Version  
V1.0.9.88\_10.2.88

English

BASIC

ADVANCED

Home

Internet

Wireless

Attached Devices

QoS

Parental Controls

ReadySHARE

Guest Network

NETGEAR Armor











## Attached Devices

Edit

 Access Control: Turned On  
General Rule: Allow all new devices to connect

 Go to [Access Control](#) to allow or block devices.

Refresh

	Status	Connection Type	Device Name	IP Address	MAC Address
<input type="checkbox"/>	Allowed	Wired	 Steam Link steamlink-72B8	169.254.113.34	E0:31:9E:3C:D3:BC
<input type="checkbox"/>	Allowed	Wired	 Canon DEV-AE:84:00	10.0.0.24	00:1E:8F:AE:84:00
<input type="checkbox"/>	Allowed	5G Wireless	 EX3700	10.0.0.2	02:0F:B5:D0:5B:43
<input type="checkbox"/>	Allowed	5G Wireless	 Samsung Samsung-Android-MOBILE	10.0.0.18	02:0F:B5:FB:36:F8
<input type="checkbox"/>	Allowed	Wired	 WSHX002891	10.0.0.12	F4:8C:50:7A:B7:D2
<input type="checkbox"/>	Allowed	2.4G Wireless	 Chromecast Chromecast-Audio	10.0.0.3	A4:77:33:FE:E6:90
<input type="checkbox"/>	Allowed	5G Wireless	 Chromecast Chromecast	10.0.0.4	A4:77:33:37:2F:AC
<input type="checkbox"/>	Allowed	Wired	 RX-V673 RX-V673 93BFC1	10.0.0.6	00:A0:DE:93:BF:C1
<input type="checkbox"/>	Allowed	5G Wireless	 Chromecast Chromecast-Ultra	10.0.0.7	44:07:0B:31:41:AF
<input type="checkbox"/>	Allowed	5G Wireless	 65" Roku TV 65" Roku TV	10.0.0.5	C4:98:5C:48:0E:85

Similar device settings should easily be found for all major residential wifi router brands such as:

- Asus
- Belkin
- Cisco
- D-Link
- Google
- Linksys
- Netgear
- TP-Link

# Device Control

**NETGEAR**  
Nighthawk R7000

Logout

Firmware Version  
V1.0.9.88\_10.2.88  
English

BASIC

ADVANCED

---

ADVANCED Home

Setup Wizard

WPS Wizard

▶ Setup

▶ USB Functions

▼ Security

Access Control

Block Sites

Block Services

Parental Controls

NETGEAR Armor

Schedule

E-mail

▶ Administration

▶ Advanced Setup

Access Control

Apply
X Cancel

---

You can use Access Control to allow or block computers or electronic devices from accessing your network.

Turn on Access Control

Access Rule: This is a general rule. You can also allow or block individual devices.

Allow all new devices to connect  
 Block all new devices from connecting

Allow
Block
Edit
Refresh

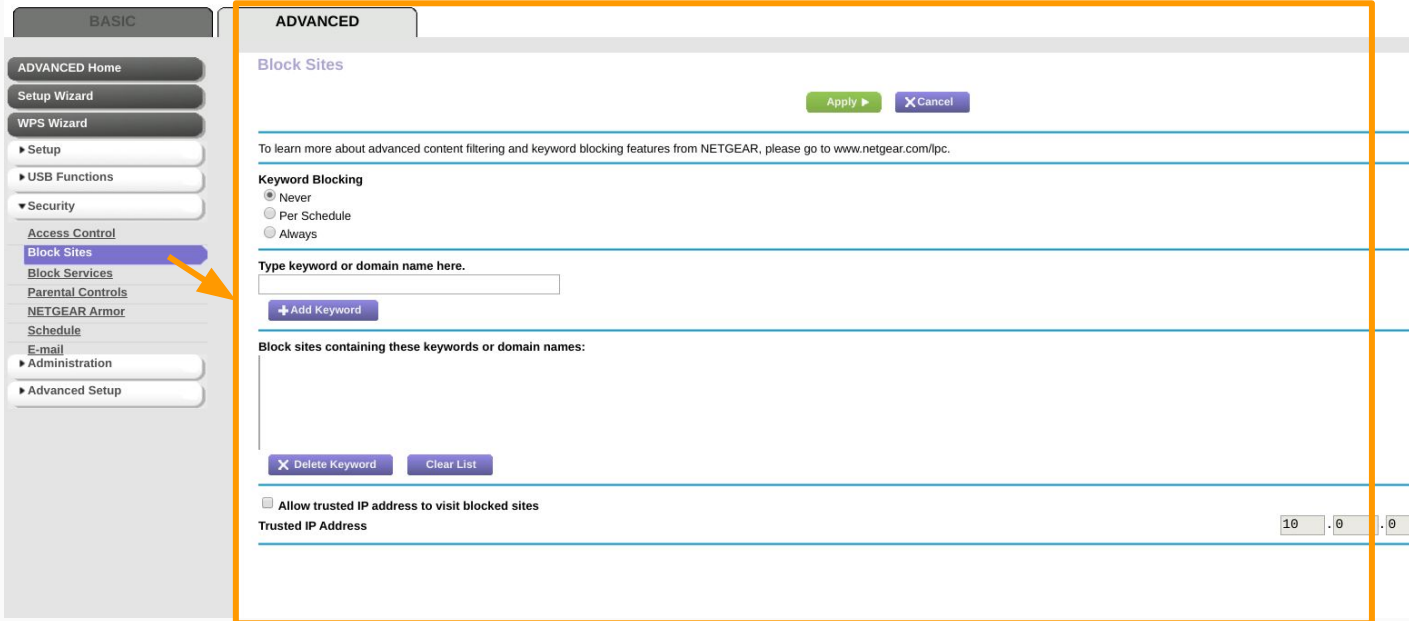
Status	Device Name	IP Address	MAC Address	Connection Type	
<input type="checkbox"/>	Allowed	EX3700	10.0.0.2	02:0F:B5:D0:5B:43	Wireless(MURPHY-5G)
<input type="checkbox"/>	Allowed	Chromecast-Audio	10.0.0.3	A4:77:33:FE:E6:90	Wireless(MURPHY)
<input type="checkbox"/>	Allowed	Chromecast	10.0.0.4	A4:77:33:37:2F:AC	Wireless(MURPHY-5G)
<input type="checkbox"/>	Allowed	65" TCL Roku TV	10.0.0.5	C4:98:5C:48:0E:85	Wireless(MURPHY-5G)
<input type="checkbox"/>	Allowed	RX-V673 93BFC1	10.0.0.6	00:A0:DE:93:BF:C1	Wired
<input type="checkbox"/>	Allowed	Chromecast-Ultra	10.0.0.7	44:07:08:31:41:AF	Wireless(MURPHY-5G)
<input type="checkbox"/>	Allowed	Chromecast	10.0.0.8	D0:E7:82:BE:4E:66	Wireless(MURPHY)
<input type="checkbox"/>	Allowed	HP07010A	10.0.0.9	C8:D3:FF:07:01:0A	Wireless(MURPHY)
<input type="checkbox"/>	Allowed	FREENAS	10.0.0.10	00:11:D8:D8:9E:52	Wired
<input type="checkbox"/>	Allowed	--	10.0.0.13	F0:D7:AA:91:90:1D	Wireless(MURPHY-5G)
<input type="checkbox"/>	Allowed	VIZIOCastAudioMurphy	10.0.0.16	C4:1C:FF:6D:6A:9B	Wireless(MURPHY-5G)
<input type="checkbox"/>	Allowed	Sara	10.0.0.17	0C:8B:FD:20:D6:C7	Wireless(MURPHY-5G)
<input type="checkbox"/>	Allowed	--	10.0.0.18	02:0F:B5:F8:36:F8	Wireless(MURPHY-5G)
<input type="checkbox"/>	Allowed	DESKTOP-38AG4K8	10.0.0.20	7C:67:A2:BC:71:54	Wireless(MURPHY)
<input type="checkbox"/>	Allowed	--	10.0.0.21	A8:1D:16:1D:4E:9D	Wireless(MURPHY-5G)
<input type="checkbox"/>	Allowed	--	10.0.0.22	0C:CB:85:13:3B:5E	Wireless(MURPHY-5G)

Similar device settings should easily be found for all major residential wifi router brands such as:

- Asus
- Belkin
- Cisco
- D-Link
- Google
- Linksys
- Netgear
- TP-Link

# Additional Filtering/Blocking

**NETGEAR**  
Nighthawk R7000



**BASIC**

- ADVANCED Home
- Setup Wizard
- WPS Wizard
- Setup
- USB Functions
- Security
- Access Control
  - Block Sites**
  - Block Services
  - Parental Controls
  - NETGEAR Armor
  - Schedule
  - E-mail
  - Administration
  - Advanced Setup

**ADVANCED**

### Block Sites

Apply Cancel

To learn more about advanced content filtering and keyword blocking features from NETGEAR, please go to [www.netgear.com/pc](http://www.netgear.com/pc).

#### Keyword Blocking

Never  
 Per Schedule  
 Always

Type keyword or domain name here.

+ Add Keyword

Block sites containing these keywords or domain names:

X Delete Keyword Clear List

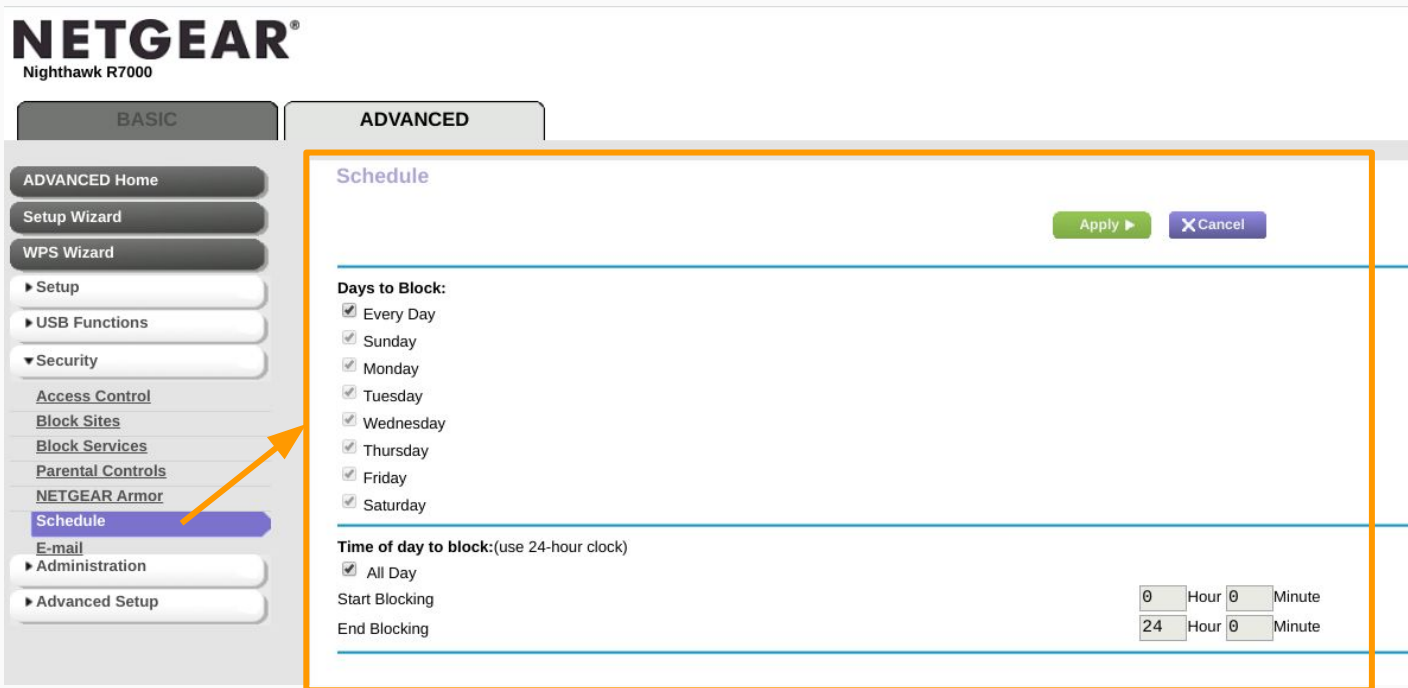
Allow trusted IP address to visit blocked sites

Trusted IP Address .10 .0 .0

Similar filtering settings should easily be found for all major residential wifi router brands such as:

- Asus
- Belkin
- Cisco
- D-Link
- Google
- Linksys
- Netgear
- TP-Link

# Schedule Internet Blocking



**NETGEAR**  
Nighthawk R7000

**BASIC** | **ADVANCED**

ADVANCED Home  
Setup Wizard  
WPS Wizard

► Setup  
► USB Functions  
▼ Security

Access Control  
Block Sites  
Block Services  
Parental Controls  
NETGEAR Armor  
**Schedule**  
E-mail  
► Administration  
► Advanced Setup

**Schedule**

Apply ► | X Cancel

**Days to Block:**

- Every Day
- Sunday
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

**Time of day to block:**(use 24-hour clock)

- All Day

Start Blocking: 0 Hour 0 Minute  
End Blocking: 24 Hour 0 Minute

Similar scheduling blocking settings should easily be found for all major residential wifi router brands such as:

- Asus
- Belkin
- Cisco
- D-Link
- Google
- Linksys
- Netgear
- TP-Link



# Ad Blocking

Ad Blocking plugins and applications should be used on all browsers. [opinion]  
Isn't this immoral?

1. This may be a gray area due to the nature of how online publications make money off of advertisements. However, the content of these ads tell me that it's worth ditching them in favor of my family's health. You've all seen them at the bottom of a typical "listicle" type article or even shoved into the middle of the article for all to see, a very predatory practice.
2. Alternate browsers such as Brave or Dissenter have ad-blocking on by default. Brave even lets you donate to give money back to the content providers.
3. Why not block Ads even further than what OpenDNS provides at the network router level? I agree, this is the ideal scenario to protect your young innocent eyes! But it gets a bit more technical, however achievable by anyone that's patient: Check out <https://pi-hole.net/>

# Ad Blocking - How-to

Install ad blocking browsers and extensions (per device):

1. Simple: Install the [Brave](#) or [Dissenter](#) browser
  - If you want to keep using Chrome, Firefox, or Safari:
    - Install the [uBlock Origin](#) (free browser plugin or extension)
2. Advanced: If you really want to block everything at the network level check out the more advanced: <https://pi-hole.net/>

# Monitoring

Phone, Tablets, Computers, and TVs should all be monitored in both usage (time spent) and content (what we are consuming).

## Software doesn't replace parenting!

<https://conquerseries.com/how-to-safeguard-your-family-online/>

### Why? Because God tells us so!

1. Time Spent - [Phil 4:8](#)
2. Consumption - [Prov 23:7](#)
3. Accountability - [Gal 6:1-2](#)
  - a. Setup [Covenant Eyes](#), [X3 Watch](#), [Accountable2You](#), or [Net Nanny](#) tools for additional needs by device
  - b. Share your link with those you trust to hold you accountable

# Homework

Here are some quick and easy things you can do to get started after tonight's talk.

1. **Discuss and Plan:**

Parents should talk about how you are currently dealing with the internet and devices in your home. Discuss how you'd like to change current behaviors going forward.

2. **Learn:** Listen to some sound advice on technology and the family when dealing with kids. Here are a few to get you started:

[Becoming a Tech Wise Family on Dad Tired Podcast](#)

[Technology, the Gospel, and your Kids on Dad Tired Podcast](#)

[Time to Talk - Family Life](#)

3. **Audit:** Walk around and assess the number of devices that regularly connect to your home network. Do they all need to? Should they be restricted by time (schedules)? Should certain sites be blacklisted (blocked) completely based on the apps being used, games played, or sites visited?

# Homework - Continued

Here are some quick and easy things you can do to get started after tonight's talk.

4. **Discuss**: Don't just cut your kids off cold turkey without warning! Have a biblically based discussion about how God doesn't want us feeding our minds and hearts with garbage. You must guide them to an understanding of what is considered good or bad content to be consumed by them on the internet / devices. This is subjective and solely up to you as parents and for your situational needs!
5. **Implement**: Put your agreed-upon Family Technology Plan into action, whatever that looks like for you in the short and long term.
6. **Reassess**: Technology is constantly evolving and so should you! Plan to re-evaluate your current plan as parents bi-yearly or whatever works best for you. As your kids grow they will find new technology obsessions and this may require adjusting your filtering, scheduling, and blocking requirements.

Thank You and  
Keep Your Family  
Safe Online!

---



**HARVEST  
BIBLE  
CHAPEL**  
PITTSBURGH NORTH



# Extra Credit

Blocking Individual Apps can be challenging due to the nature of how many networks they use for their service(s). Check out [this how-to](#) for blocking just the TikTok app. It's the same process that we've gone over tonight, however you would need to block this full list of domains for that one app:

- [v16a.tiktokcdn.com](https://v16a.tiktokcdn.com)
- [p16-tiktokcdn-com.akamaized.net](https://p16-tiktokcdn-com.akamaized.net)
- [log.tiktokv.com](https://log.tiktokv.com)
- [ib.tiktokv.com](https://ib.tiktokv.com)
- [api-h2.tiktokv.com](https://api-h2.tiktokv.com)
- [v16m.tiktokcdn.com](https://v16m.tiktokcdn.com)
- [api.tiktokv.com](https://api.tiktokv.com)
- [v19.tiktokcdn.com](https://v19.tiktokcdn.com)
- [mon.musical.ly](https://mon.musical.ly)
- [api2-16-h2.musical.ly](https://api2-16-h2.musical.ly)
- [api2.musical.ly](https://api2.musical.ly)
- [log2.musical.ly](https://log2.musical.ly)
- [api2-21-h2.musical.ly](https://api2-21-h2.musical.ly)

