> If you need an account, go to the forum and ask for it.

Security & Home Tech

A guide to which home tech or security tech you should use for your home. Also comparisons of different products.

Phone, Tablet, and Computer Backup

> This is a setup you can do to allow for backing up all your devices into one location. Your total setup cost will vary, depending on if you already have most of the hardware. Software will only cost **$60/year** for off-site secure backup. An optional one time fee (of $120) for Plex, if you decide to use plex. Syncthing is free and open sourced!

Software Used

- Syncthing
- BackBlaze
- Plex (optional)

> Plex is optional. I use this to view all photos from all devices on any device, such as phones, tablets, and even on the Roku! However, you do not have to use this for backing up all your data.

Hardware Used

- Hard Drive - Recommend running in RAID10, but is optional
  - You can usually find a 14TB external hard drive for around $180.
- Computer - I use Windows, however, I am sure you can use Linux or even a Mac

Syncthing Setup

Synthing on Server

You will need to first setup Syncthing on your computer that will be handling the backups. In my case, I use a Windows computer with an external hard drive.

Install the latest version of SyncTrayzor from Releases · canton7/SyncTrayzor (github.com), make sure to run the 64-bit version. You can use this direct link, but it could be an old version: SyncTrayzorSetup-x64.exe

Once setup, you shouldn't need to open up a port, since Syncthing will automatically find connections locally and remotely!

I would just delete the default Folder provided. We will want to add Remote Devices, AKA your phone and tablet. So keep up the program, since we want to keep pinging out.

Make sure to pull up QR code for Android devices under Action > Show ID

Syncthing on Android

Download Syncthing - Apps on Google Play on your Android phone.

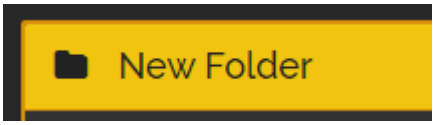
Delete existing folders

Let's add server device. Tap to devices, then tap on plus to add new device. Tap on the QR code and scan QR code from server. (On server go to actions > Show ID). Add name and save! On Server computer make sure to setup device there.

Now that the server is connected, let's setup the first folder to backup

Hit plus button to add new folder for full backup. I usually enter the folder name. Tap on directory and go to root directory (or camera directory, if you only want to backup photos and videos) for your phone. If you have an SD card, you will need to do that as a separate folder. (The new S21 phones don't have SD cards anymore). Tap on Allow Access. Now toggle ON the server to sync to. For folder type, set it as Send Only, so, you can't make changes from server. Allow watching for changes. Everything else is fine. Now save!

Go back to your server, and you should see a New Folder alert!



Click on Add, update Folder label. I either keep as is, or rename to device name (if I have another folder within device I add hyphen and the difference)

Change Folder path to the new storage hard drive. Make sure to create a folder specifically for this folder syncing and it is empty.

Optionally you can setup File versioning. This allows if a file is deleted you can restore. Simple File Versioning works well. I set "clear out after" to 0 days and keep up to 3 versions.

Under advanced, you can set folder type to receive only.

Hit save and watch the magic happen.

> If you find the remote device (The Android Device) keeps disconnecting, it could be due to it going to sleep. Make sure to change your settings to never put syncthings to sleep. Also, within Syncthing Settings > Behavior, make sure "Start service automatically on boot" is checked. In Syncthing Settings > Syncthing Options, make sure "Restart on Wakeup" is checked as well. You can go through settings and set it up the way you want.

Syncthing on iOS

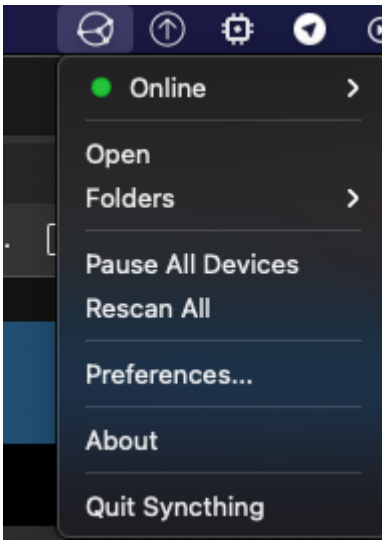
There are apps available for this, however, I have not tried it yet.
Here is the app if you want to try it out! Möbius Sync on the App Store (apple.com)

Syncthing on Windows

Same setup as the server. Should be pretty self explanatory. I usually backup the whole USER folder only.

Syncthing on MacOS

This has gotten much easier. Just install Releases · syncthing/syncthing-macos (github.com). Works for both M1 ARM64 and Intel x86_64. I would recommend it starting up on login within Syncthing preferences. I back up the user folder only.



Setup will be similar to other platforms.

I have setup a `.stignore` file to ignore specific folders and files:

```
**:*
**\**
**"*
/.nvm
/Library
.Trash
/Applications
Photos Library.photoslibrary
```

Backblaze

BackBlaze is super easy. Sign up here for a free month! When setting up Backblaze, make sure to backup your whole external drive, or which ever drive you have setup. Now just in case the drive goes bad, you have a backup of it secured off-site!

Plex.tv

You can then set up plex under settings > manage > libraries. under photos, or whatever you want you then point to the camera directories. This will allow viewing of all device photos and videos from one app!

DNS - Block Malware/Adult Content/Ads

> This will not explain everything, however, I will try to go through as much as I can with this.

Introduction

DNS is very important in connecting to a website. A Domain Name Server will take a domain name and then give back an IP, so your computer can connect to that server/website. A lot of domains are setup specifically for advertising, tracking, malware, adult content. This guide here is to show how you can take control of your internet connected devices.

Another concern is using the default DNS provided by your ISP. Your ISP will be able to know every website you access and sell that data to advertisers or whomever they want. This is a privacy risk.

I will explain 2 methods to help. One of which you can do RIGHT NOW. The other take a lot of setup to do.

- 1.1.1.1 Family
- Pi-Hole

1.1.1.1 Family

This is the easy one. Go into your router and change your DNS settings to:

- 1.1.1.3
- 1.0.0.3

This will block Malware and Adult Content. This will also prevent ISP from seeing any DNS queries. However, we are now trusting Cloudflare with this information. They have said they do not track or sell that data.

For more help on getting this setup go here [Router setup instructions · 1.1.1.1 docs (cloudflare.com)]

Pi-Hole

Requirements:

The first thing you need is a Raspberry Pi. You can buy one on Amazon for around $60/$70 for the board and a piSwitch. You can use these affiliated links below. I recommend the 4GB model, so that you can do other stuff with it.

- Raspberry Pi 4 Kit (4GB): https://amzn.to/3euivdP
  - Comes with everything you need, priced at $100
    - Raspberry Pi 4 4GB
    - 32GB Samsung EVO+ Micro SD Card (Class 10) Pre-loaded with NOOBS
    - USB MicroSD Card Reader
    - Raspberry Pi 4 Case with Integrated Fan Mount
    - Low Noise Bearing System Fan
    - 3.5A USB-C Raspberry Pi 4 Power Supply (US Plug) with Noise Filter
    - PiSwitch (On/Off Power Switch)
    - Set of Heat Sinks
    - Micro HDMI to HDMI Cable - 6 foot
- You could get the parts separately if you already have most of the stuff above:
  - Raspberry Pi 4 (4GB): https://amzn.to/3bD3rJ9
    - Comes with power cord and heat sinks for $60
  - 32GB MicroSD Card: https://amzn.to/3clq43Y
    - Priced at less than $10
  - Optional Case: https://amzn.to/3evqUxy
    - Priced at $11

> I recommend at least the 4GB model, so you can also install and run some other programs for your home, such as Home Assistant.

Pi Setup:

If you bought the Kit, then you already have NOOBS installed! If you bought the SD Card separately, you will need to install NOOBS. You can find out how here: NOOBS - Raspberry Pi Documentation or you can watch this video https://www.youtube.com/watch?v=y4GOG4P-4tY

> There are different ways of doing this, such as a headless setup. However, I do not want to show that. If you need that way of setting up your Pi, then I can always explain later.

I recommend connecting to the network using an ethernet cable and not wifi, however, wifi will work too.

There is no need to boot into desktop and I recommend NOOBS Lite. I nice video tutorial can be found here: Raspberry Pi OS Setup with SSH - YouTube She does very well in explaining everything you need in setting up SSH, so you can connect to the Pi from any computer on your network.

Please make note of your IP address. I would recommend setting the IP as static within your router. (Search for how to by your router model)

Connect to the pi using SSH. Once you get to this point, you are all setup and ready to install pi-hole!

Install Pi-Hole:

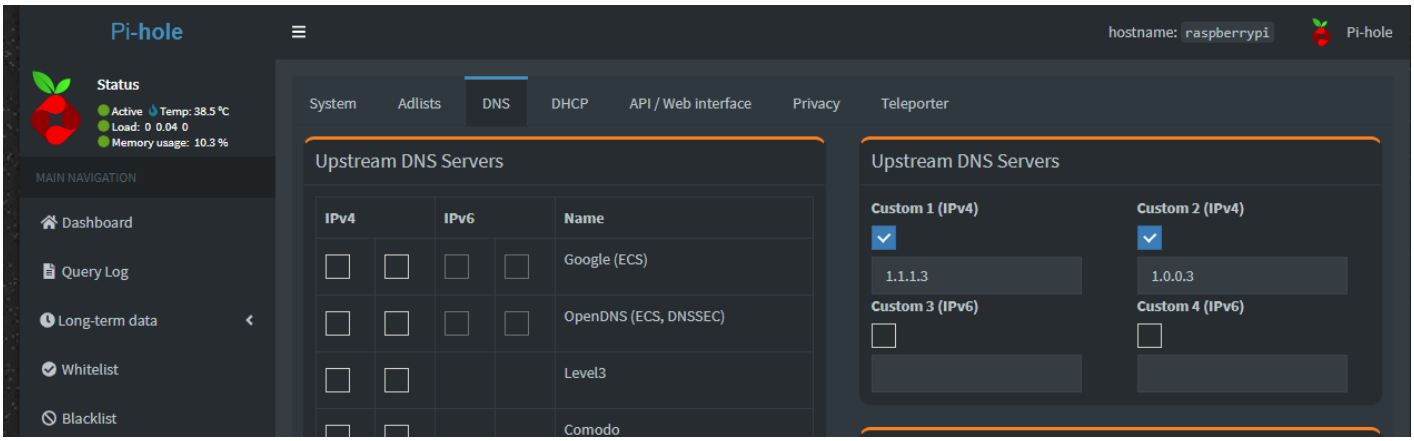
Now enter in these commands:

```
cd ~
curl -sSL https://install.pi-hole.net | bash
```

The first command goes to your home directory, the second command installs pi-hole. Follow the on screen instructions. Note: do not install DHCP, we want your router to handle that.

You can now access your Pi-Hole admin by going here `http://<IP_ADDPRESS_OF_YOUR_PI_HOLE>/admin/`

Once there, go into Settings > DNS and change your Upstream DNS Servers to the 1.1.1.3 and 1.0.0.3



Now go to Group Management > Adlists and add some of these lists, if you desire:

- https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts
- http://sysctl.org/cameleon/hosts
- https://s3.amazonaws.com/lists.disconnect.me/simple_tracking.txt
- https://s3.amazonaws.com/lists.disconnect.me/simple_ad.txt
- https://raw.githubusercontent.com/chadmayfield/my-pihole-blocklists/master/lists/pi_blocklist_porn_all.list
- https://zerodot1.gitlab.io/CoinBlockerLists/hosts_browser
- https://raw.githubusercontent.com/evankrob/hosts-filenetrehost/master/ad_servers.txt
- https://raw.githubusercontent.com/chadmayfield/pihole-blocklists/master/lists/pi_blocklist_porn_top1m.list

To find more you can subscribe to, you can go here: Blocklist Collection ¦ Firebog

Do note, that the more website you block the more of a possibility you can have false positives.

Once the installer has been run and you have made the necessary changes in admin, you will need to configure your router to have DHCP clients use Pi-hole as their DNS server which ensures that all devices connecting to your network will have content blocked without any further intervention.

Set your routers DNS to point to the static IP of your raspberry pi. Use the same IP for both fields.

Done:

You are all done. Now just wait for your devices to start pinging your Pi-Hole for DNS information. You can log into your admin page to see how many domains are being blocked!