

Internet Filtering – Modern Media Committee

MM modernmedia.nrclethbridge.com/internet-filtering/



Internet Filters:

- in your home

- on your mobile devices

- everywhere

Internet filters on digital devices are changing every day. Filtering of any device (mobile or in-home) is a must-have, and even secular families and workplaces are scrambling to monitor their internet traffic. The human heart is open to any filth and distraction, and we are obligated to protect our children and ourselves against the many temptations.

As a committee, we would like to share the experience we have gained from filter trials but want to refrain from making any commercial recommendations. All filters will need to be monitored and adjusted continually.

As you perhaps know, there are both hardware filters as well as device filters, which we will try to explain below.

In-home filter (hardware filter)

The internet service provider brings the cable into the house where it is hooked up to your modem. From this modem, your computer can be plugged directly into the internet connection. Some providers supply you with an All-In-One unit (modem & router in one). The computer can be plugged into this All-In-One device by using a cable or by using a WiFi (wireless) signal. Another option is to plug-in a separate router into the modem and to 'bridge' the modem, whereby the internet signal just passes through the modem.

A filter provider can place some program (firmware) changes into the router, whereby the internet signal coming into your home is filtered. Any device (cell phone/tablet/laptop/desktops with the Wifi feature enabled or desktop/laptop connected with an ethernet cable) that are either plugged in or hooked up through WiFi will receive the filtered internet connection.

To eliminate any WiFi signal in your home, you can log into the router and turn off the WiFi signal. The only way that the internet is received after applying this procedure will be through the cable to your computer. All routers are password protected to secure the changes and avoid unwanted access.

Some loopholes are:

- Any device with WiFi capability can connect to all unlocked and possibly unsecured internet providers. Your in-home filters will not protect you outside of the home.
- Any mobile device has a potential to hook up through a data plan (with a subscription to a provider such as Bell or Telus), and by doing so, will bypass your in-home filter.
- By applying a 'lenient' filter setting, there will be inadequate protection and a greater potential to stumble over improper and unwanted internet content (further details below).

Device filter

Any device plugged into or run through the in-home filtered router receives filtered internet. But what about mobile devices? The answer is: each device needs to have a separate filter installed to filter the internet connection outside of the home. Laptops that are taken to a motel room or restaurant have Wi-Fi capability and need a filter installed on the device to protect internet access.

Mobile devices are generally run by two major operating platforms: Android and iOS (Apple/iPhone). It is relatively easy to filter the Android and install an App Monitor. It becomes a little trickier with the iOS as this platform needs to have a password protection to avoid the use of default, unfiltered browsers like Safari.

There are no filters available that can never be bypassed or uninstalled, and therefore communication with your family is of utmost importance.

Some people have the internet turned off on their children's devices, which means that there is no data plan purchased for this phone. But these devices still have the capability to connect to WiFi and browse the internet using the home router or at public locations (for example Tim Hortons or McDonald's). By having this WiFi connection, the device can download and use all types of Apps and games.

Filters

We would like to suggest some filter and accountability options which have been used with successfully by other members in the community. It is strongly recommended that an accountability or browsing report is received each week or month. Some people depend on browsing history on their computers, but these can easily be deleted and can therefore not be considered an adequate response.

Choices for filters and accountability software depend on the following aspects:

1. *Family size and ages.* A husband and wife will need a different setup, for example, then a family with (younger) children.
2. *Personal protection.* For people living on their own, we recommend to setup a filter with an accountability partner, which could be a friend or relative.
3. *Devices used.* A family with only a desktop computer which is placed in the living room will need a different filter than a family with (older) children and various mobile devices.

Filters in Alphabetical order:

Covenant Eyes

- Device filter for Internet and Apps
 - Great for adults. Fewer options for (younger) children
 - Great accountability setup
 - Easy setup and tutorials. Email and phone support.
-

DNS Thingy

- In home filter only.
 - The content filter is managed outside the home.
 - Time restriction can be set.
 - Per device restrictions and settings
 - No reporting on internet usage. A separate device filter needs to be installed to access report
 - Third party setup or online purchase of the pre-installed device. Email support only.
-

K 9 filter

- Device internet filter
 - No reporting on internet usage.
-

Net Nanny

- Device filter for Internet and Apps
 - Great for families with small children
 - Device usage reports are sent every week
 - Easy setup and tutorials. Email support only
-

Open DNS

- In home filter only.
 - The content filter is managed outside the home.
 - No reporting on internet usage. A separate device filter needs to be installed to access report
 - No support other than some only tutorials. Basic technical knowledge is required.
-

Qustodio

- Device filter for Internet and Apps
 - Great for families with small children
 - Text messages and contacts can also be monitored
 - Device usage reports are sent every week
 - Easy setup and tutorials. Email support only
 - Note: public networks like a college or university will not allow WiFi connection which results in high data usage.
-

As a committee, we strongly urge you to install device filters with usage reports on every mobile device (Laptop/tablets/cellphones). Also, install a router filter to avoid devices from using your wireless internet without a

filter.

Time restrictions for weekdays and on Sundays are also strongly recommended.

We hope that this overview is of help. May the fear of the Lord be found in our families and may He protect us and our children.

The Modern Media Committee.