



ON-LINE ADVERTISING – WHAT’S THE HARM?

Why block advertising sites?

ComSifter blocks pornography, hate, gambling and many other sites not conducive to the welfare of students. But ComSifter also blocks advertising sites!

Why is this important?

Overview –

By blocking third-party on-line advertising, ComSifter™ is able to help you to better focus your students on the task at hand without a constant bombardment of online advertising.

Also significantly -

- many common sources of spyware are also blocked;
- your computers have less demand on their hard drives and memory systems;
- traffic on your shared Internet Connection is reduced.

Here’s how it works -

1. Advertising sites are more than just advertising –

Most sites that offer services or products for free make their money from advertising. Advertising sites are really tracking sites.

Let’s take an example of looking for movies by way of any of the large portal sites. When you click on the line for Movies and Entertainment you expect to go to the site showing movies and entertainment. What you don’t see is your browser is redirected to a tracking server that identifies your IP, determines that you clicked on Movies and Entertainment, gives your browser a tracking cookie (so it can identify you next time) and then prepares an advertisement relevant to what you clicked on. Then the tracking server sends your request to the real Movies and Entertainment site. This may take less than a second to accomplish and you, the user will never know it happened ---- until a few minutes later when you receive a pop-up advertisement showing the latest box office hit -- and you say – how did they know that?

The next time you visit the site, the tracking server looks at the cookie it left previously, looks the cookie up in its database and knows that you previously looked at movies and entertainment. This time you click on Clothes and Apparel. The tracking server repeats the process and this time you may receive an ad for Movies and Entertainment or you may receive an ad for Clothes and Entertainment.

Over time the tracking server builds a profile of what you like to do while online (and based on your viewing habits can determine your sex, age bracket and income level) and it shows advertisements related to your viewing habits. These advertisements may be static pictures with text, animated or annoying pop-ups.

2. Advertising sites leave artifacts on your systems –

Each ad that is displayed in your browser contains a picture (or animation) and that picture is left on your computer (this is a normal caching action of the browser so the next time it shows the ad it will not have to download the picture again).

Although each picture is small (typically less than 10K bytes) the sheer number of ads shown in a normal session may leave tens or even hundreds of these little pictures on your hard drive. Multiply this by the number of sessions per day, by the number of sessions per month/year and very quickly these little pictures begin to add to what's on your hard drive and they slow down the indexing capability of the browser. This translates to your computers slowing down.

Each time the tracking server leaves a cookie on your computer it adds to the number of cookies on your system. Although these cookies are small and may have expired, they take up space and slow down any legitimate program accessing the cookie database.

3. Some Advertising sites purposely try to infect your computer –

Most spyware and virus programs need you to download, or allow to be downloaded, an executable program. Enticing you to do so is done by many advertising sites. The come-on may be cute cursors for your mouse, a free weather service that shows the temperature in your system tray, free greeting cards or a free calendar program for your appointments. When you download the program, you get the free service, but then find that your system is inundated with pop up ads, or your home page has been changed or in the worst case - your keystrokes are being monitored and sent to an unknown site on the internet.

4. Advertising sites use your expensive Internet Bandwidth –

Even though you may not see what the advertising site is doing, it is using your Internet connection to download its advertisements. On a dial up connection (56kbps) from home your Internet connection may become useless because all it is doing is downloading ads to be shown to you at some time. At home, high-speed DSL connection (1.5mbps), with only one or at most a few computers, may cover up this issue. But a school, library or small business DSL (1.5mbps) connection, with 10s or 100s of computers accessing the Internet, will begin to see the slowdown as each of its computers tries to download advertisements.

5. Advertising is distracting –

While your students are looking at the content you have instructed them to view they will also see various advertisements for every product and service imaginable. Sometimes multiple advertisements are shown on one page (the record seen to date has been seven advertisements on one page). These advertisements are in color, may have animation, and beckon your students to click on them. They are a major distraction.

So what does ComSifter do to stop this?

ComSifter blocks advertising sites by blocking them from ever displaying in the first place. If the advertising site is blocked then:

- ✓ It cannot go to the tracking server.
- ✓ Small pictures will not be left on your system.
- ✓ Cookies will not be left on your computer.
- ✓ The page you are viewing will not have advertisements blinking in multiple places. Instead there will be a blank white spot where the advertisement was supposed to be showing.
- ✓ You will not be able to install free services because the advertising site will not be able to ask you to install the free program.

Does ComSifter block all advertising?

No. ComSifter only blocks third party advertising. If you are viewing a site and that site is advertising its own goods and services then ComSifter will not block those advertisements. But if the site receives its advertising from a third-party, by way of a redirect, and the redirect is on the block list, then ComSifter will block the advertisement.

Does ComSifter block Pop-ups?

ComSifter is not a pop-up blocker but by not allowing advertising sites to load, those trying to display pop-up ads will not be able to do so.

Since ComSifter can block sites that have viruses and spyware does that mean we no longer need anti-virus or anti-spyware programs?

ComSifter does not replace these programs but works to reduce the load they will see. ComSifter does greatly reduce the amount of spyware on a given system due to blocking the majority of sites where spyware is sourced. Comsift is constantly adding to sites that contain harmful material, but we cannot guarantee that we will block all such places on the Internet.

A case study –

Recently Comsift logged the Internet accesses for a medium-sized parochial school in San Jose, CA for 24 hours. The school has 80 computers and is connected to the Internet via a 1.5mbps DSL connection. The following is a summary of the log results.

Total requests made to the Internet -	3478	
# of access blocked due to advertising	903	26%
# of accesses blocked due to porn/gambling etc	2	<1%

As can be seen - 26% of the requests were for advertisements and these were blocked. Potentially 903 cookies and 903 small pictures were kept off computer hard drives in just one day – and the load on the Internet Connection was reduced by 26%.

Conclusion –

By blocking advertising ComSifter is able to help you better focus your students to the task at hand without the constant bombardment of online advertising. Additionally, exposure to spyware sources will be reduced, your computers will see less demand on their hard drive and memory systems, and the load on your shared Internet connection will be reduced.

