Extra security for your PC.

General

Hackers, viruses, Trojans, iframes… it can get pretty dangerous on the web at times, and it pays to protect yourself as much as possible. Here are a few basic tips you should follow, to help keep your PC Clean:

- ALWAYS use a good, commercial antivirus program, such as McAffee or Symantec/Norton (or PCAV).
    - Make sure that the software is updated at least weekly
    - Make sure the virus definitions are updated at least weekly
    - Make sure you run a full scan at least weekly, and **after** the software is updated.

- ALWAYS Make sure you are using the latest patch of your browser.
    - Most browsers issue hot patches at least quarterly to close security holes that have been discovered
    - Firefox and IE both have 'check for updates' routines built in, that usually take < 2 minutes to run. Again, do this at least weekly.

- Watch for 'known bad' sites lists, and get the domains onto your hosts file
    - This document will discuss the hosts file, and show how to edit it.

The hosts file

What is it?

Let's start with an explanation of DNS, and then the hosts file will make a little more sense. On the internet, every computer has a 'number' called an "IP Address". When you browse to a site (say, http://vs-trex.com for example), your computer needs to know the 'IP Address' of that domain (67.201.47.60). To find the number, given the name, your computer goes through a set of searches using the Domain Name System (DNS for short).

If you've ever registered a domain, then you may know that you are putting your information into a huge database, controlled by ICANN (the *Internet Corporation for Assigned Names and Numbers*) and in the US by Network Solutions. That DNS registration says to the world "this website (vs-trex.com) is located on this server (67.201.47.60)".

So, ultimately, your computer will go to the World Wide Web database (or a local copy), and search for a domain, and get that address back. This is called "DNS retrieval". The problem is that with literally

billions of surfers, there could be huge lags between requesting and getting information. As a result, most operating systems have developed two short cuts:

1. They create a 'cache' of recently searched-for domains, so that they don't have to look up the address every time. This cache is in RAM, and clears when you restart your computer.
2. They keep a local table of addresses, usually in a file called HOSTS, for addresses that never change.

When your computer needs to find the IP Address for a particular domain name:

1. It checks the cache to see if it's been there before. If not found
2. It checks the HOSTS file to see if the domain name is pre-defined. If not found
3. It checks your ISP's domain table to see if THEY know of the domain. If not found
4. It goes to an 'upstream DNS table'… ultimately to the Network Solutions database. If not found
5. You get an error 'cannot locate this domain'.

Based on this, we could define the "HOSTS" file as "a shortcut to DNS, to tell the computer where a domain is".

How does this relate to security?

There is a neat little trick with the HOSTS file: There is a 'loopback' or 'self-test' address (127.0.0.1), that will PREVENT your computer from going anywhere.

The way most hackers operate: They deface hundreds of sites, adding script that tricks your browser into going to a 'bad site'. This could be done by an iframe, with some javascript, or a few other ways. The bottom line is that if your computer visits certain domains, there is code their waiting to attack your browser. You can try to block javascript, but if it works, many legitimate sites won't work. You can try and not view iframes, but that's only part of the problem. The best solution is to NEVER visit the problem sites.

If you KNOW that certain sites are specifically used to host viruses, Trojans, spyware, et cetera, then you can use the HOSTS file to prevent your computer from ever going to that domain. All you need to do is tell the computer, in the hosts file, that the bad domain should 'loop back' to your computer. That way, even if a script runs, or an iframe gets loaded, your computer can't get to the bad site, and the script/virus/Trojan/whatever never gets loaded.

The rest of this document is dedicated to explaining how to edit the HOSTS file, and to provide a short list of sites (updated as of May, 2009) that are known bad sites. By making the change we recommend, you are taking 'one more step' to making sure your computer doesn't get attacked.

Modifying the HOSTS file

These instructions are specifically for Windows-based PC's. There is a similar file on Macintosh computers, as well as on Linux-based PC's, but I don't have access to either to make screen shots.

The HOSTS file is a text file, so in this example we will show editing the file in Notepad.

Go to start/all programs/accessories/notepad

If you use Vista or Windows 2003/2005, don't click on notepad… right-click and pick 'run as administrator'

For XP or NT, just click on the notepad application

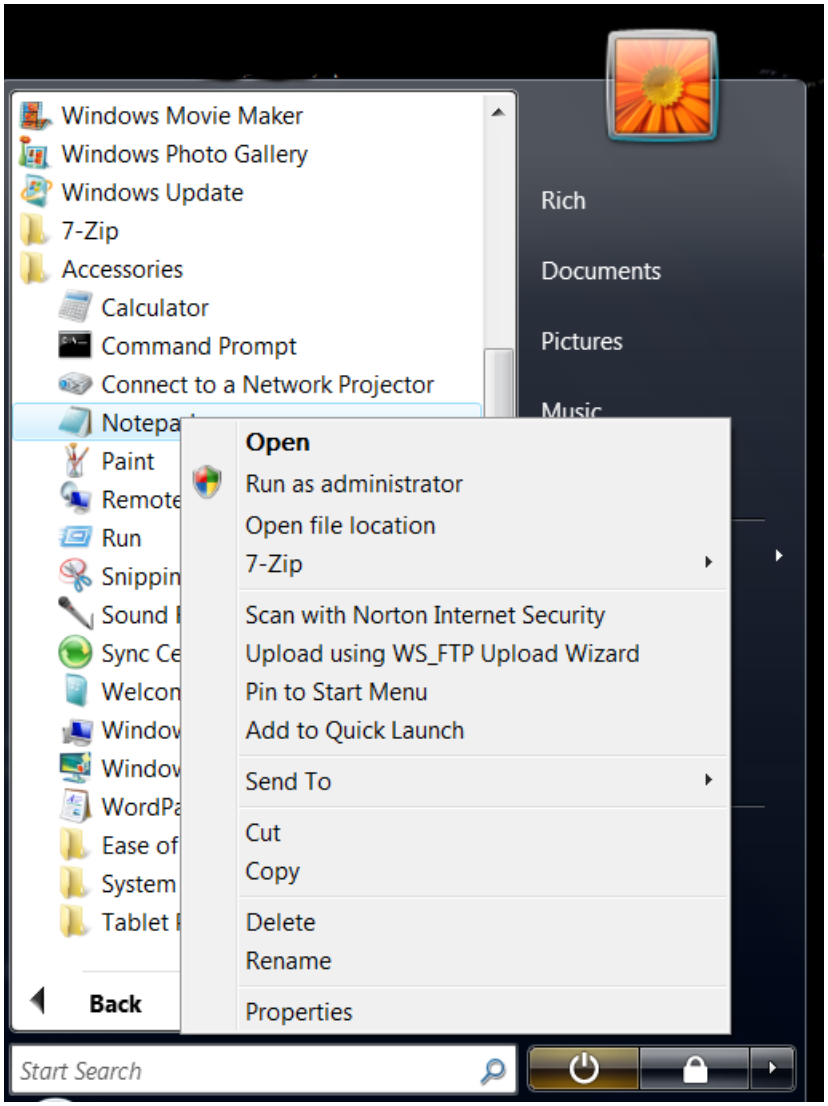

Figure 1: Example of right-clicking notepad under all programs/accessories.

With notepad open, you want to use ‘file open’ and go to c:/windows/system32/drivers/etc and load the hosts file.

In Vista, use the ‘my computer’ to get to ‘c’. Most other operating systems show the C (boot) drive automatically.

If your file-selector filter is on, switch it to “*.* all files” as shown below.

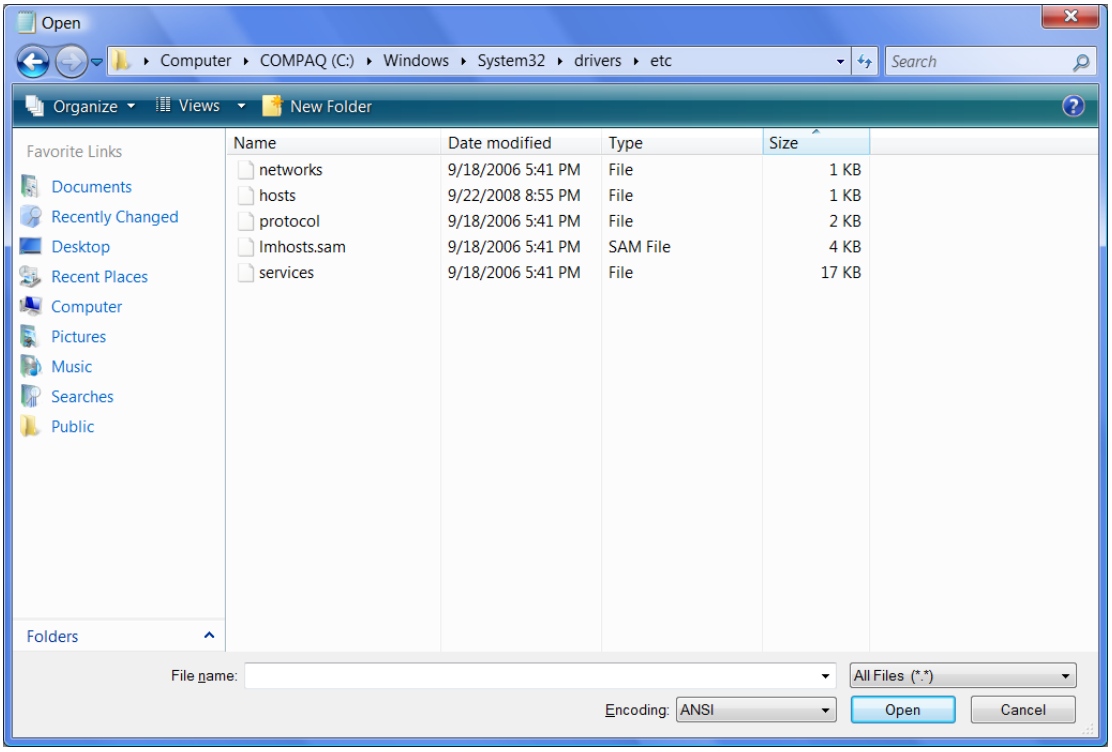

Figure 2: Navigating to the hosts file in Windows

Once you have located the hosts file, open it. Something similar to the following figure (3) should show:

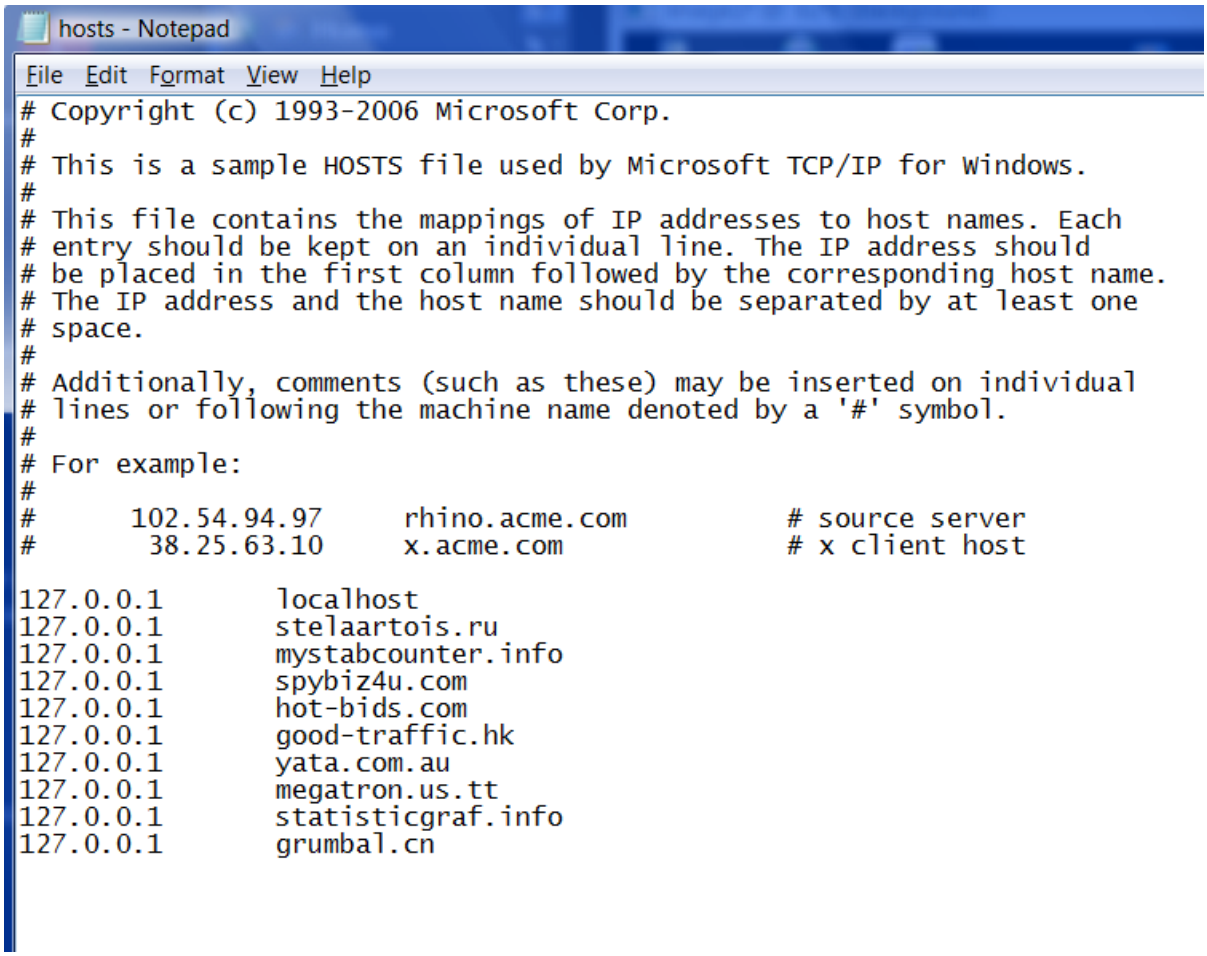

Figure 3: Notepad with a hosts file loaded

Any line that starts with a pound sign (#) is a comment, and has no impact. Blank lines have no impact.

The way this file reads, the official feedback address (or 'localhost' domain) is 127.0.0.1. That is the default for all internet computers. (And on windows machines, only the localhost line is there by default.)

The list of domains below the 'localhost' entries will always cause a loop-back on the computer, just like localhost does. That means, no matter what the hackers do, your browsers will NOT be able to go to these sites. Iframes will be blank, javascript references won't connect or load, even bad .img/.pdf/.jpg files won't run, if they have any reference to the list of domains.

Once you have edited your file and added the known bad domains, save it in the same location you found it, and then restart your computer. It's that simple.

Warning

Be very careful of what you do and don't add to this list!

The list shown above in figure 3 is a 'short list' of the worst known (to us) sites. You may find much longer lists of domains on other web sites.

Remember that anything on the list (marked as 127.0.0.1 in the hosts file) will be unreachable, so you wouldn't want to put google.com, mcaffee.com, symantec.com, mozilla.com or microsoft.com on the list, because that would make those sites unreachable as well, and could break functionality of browsers or other websites.

Remember that domains should be in all lower case (i.e.: spybiz4u.com not SpyBiz4U.com). While mixed or proper case MAY work, lower case ALWAYS works.

How we came up with this short list:

At Varisearch, we have had quite a few customers over the years, and an unfortunate percentage do get hacked. Whether through back doors, insecure servers, or flaws in software, the bad guys do get in. (Even yahoo, facebook, and myspace have been defaced at times). When it's one of our customers, we will help to remove the defacement. When we remove the defacement, we note the 'payload' domain… the web server where the actual virus/Trojan code is housed. If we can't contact the domain owner, or we see the virus stays there for a significant period of time, we put the domain on the list.

I hope this helps you understand why and how to secure your computer from these "known bad " sites. If you have feedback on how to improve this document, or you'd like to suggest another domain for us to check and add to the list, you can reach me (Rich Parker) at richp@varisearch-llc.com, or through the 'contact us' form at Varisearch-LLC corporate website. Either way, put HOSTS in either the subject line, or near the top of the message.