"Is Your Firewall and Virus Protection Safe Enough?"

Do You Have a Virus?

This Special Report by

http://www.richardpresents.com/

will help you identify viruses, prepare for attacks and infections, and guide you in their removal.

This Report is excerpted from the full Firewalls and Virus Protection website at: at: http//www.forewalls-and-virus-protection.com

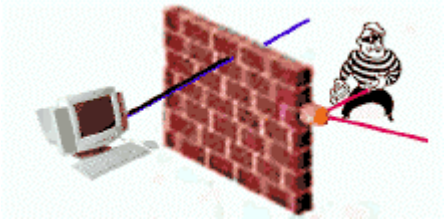
Is Your Firewall and Virus Protection Safe Enough?

First. What's a Firewall?

A **FIREWALL** is Hardware and/or software designed to keep unauthorized outsiders from tampering with a computer system or network. (The system can be a standalone computer, a small Local Area Network or a company-wide network with thousands of users).

"How Do They Work?"

They filter the information coming through your internet



connection into your computer system or private network.

If this information contains stuff that the filters judge to be suspicious, (based on rules established by the Firewall software manufacturer), they reject it and keep it from passing through to you.

"What Is A Trojan?"

A large portion of the mischief and malice done to personal computers across the Internet is performed through 'RATS', which are Remote Access Trojan programs.

Trojans are programs that contain a vicious payload. Frequently they appear to do something harmless or helpful and good. They might display a pretty animation or appear to be a utility of some sort (a famous Trojan of several years ago was an email client).

How do Trojans get on your computer?

You put them there; therefore, it is very important that you exercise caution in where you obtain software. Never take software from someone you meet in a chat room.

This is the #1 place where people get stuck with Trojans. Often people are tricked into thinking the program they are obtaining will do something for them, like help them play a game, fix a problem, or give them something for FREE.

Trojans Can Do Very Destructive Things

They do damage to your computer regardless of whether you are connected to the Internet or not. The bottom line is that if a wicked person can get you to run his or her program, it is no longer your computer.

They can make it run your printer even if you don't have a program open, make your CD tray open and close without your help, steal passwords, change your wallpaper selection to a pornographic picture, and examine and make copies of private information you may have stored on your computer.

If you haven't been Infected by a Computer Virus yet, there's a VERY Strong chance you could be soon.

FIREWALLS CAN HELP PREVENT THESE PROBLEMS

But a firewall alone can't protect your from a **computer virus.**

A Virus is a malicious, but not necessarily destructive, unauthorized, self duplicating string of code, or program, that copies itself from program to program.

Viruses are like parasites that attach themselves to various types of files (.exe and .com) and are caught and spread among infected computers by sharing floppies and files.

E-MAIL viruses probably pose the greatest threat to most of us who use the internet for communicating with family and friends, sharing photos, recipes, chat message sessions, entertainment, and just routine web surfing.

"How Can We Protect Ourselves From Viruses, Worms, and Trojans?"

Only you can protect yourself completely from a Computer Virus. Putting too much faith in virus scanners, firewalls and other software could only make you less careful.

Would you step into a busy intersection without looking both ways just because the light was in your favor?

Always think it through.

What Are Worms?"

They aren't just ordinary viruses, but they can, and do spread themselves over the Internet very rapidly.

That's why Crackers like to use them for their hateful attacks on our peace of mind. Worms spread themselves primarily in email messages, many of which they create just as soon as the email message they are attached to is opened.

They send copies of themselves to every email address in your address book.

Since they are complete programs in themselves, they can be removed from your computer by deleting these worm programs.

Best defense is to have up-to-date Firewall and anti-virus programs and -

Don't open strange emails

These 5 basic steps can go a long way toward keeping you out of trouble:

1. Never, ever, open anyone's personal floppies unless you scan them first in your anti-virus program!

2. Be fearful of any email messages from addresses (senders) that you don't recognize.

3. Be wary of any programs you download from forums, etc.

4. Don't install bootlegged copies of someone else's software.

5. Keep your anti-virus program DAT files up to date.

"What Are The Symptoms Of A Virus Infection?"

Most Computer virus infection symptoms are usually evident almost immediately after infection.

These hateful viruses cause your computer to behave in various odd ways - they can corrupt or delete program or system files or infest the computer hard drive and memory.

The loss of critical files is usually recognized almost instantly, because commonly used programs stop performing as they're supposed to. The computer operating system becomes unstable or just stops working.

If you didn't do something to cause this behavior, you can be quite certain that your computer has been infected with a computer virus.

Immediate recognition of these Symptoms gives you a chance to take action quickly when you are infected.

What are the Symptoms of a Computer Virus?

Duplication, for one-

Many implanted viruses create multiple copies of themselves on each computer, so that if one suspect is deleted, other hidden copies may carry on. Anti-virus software is programmed to recognize this, and wipe all components of a virus, including those hiding in memory.

Trojan Horse implanted computer virus symptoms:

Some computer virus symptoms are a lot harder to spot than others. The Trojan Horse implanted virus is usually the most difficult, and therefore the most dangerous virus to deal with without dedicated anti-virus software.

A Trojan Horse implanted virus often leaves very little evidence that it has infected your computer system. But, if you know what signs to watch for, you should be able to determine if you have a Trojan horse implanted virus.

Look out for these unusual activities

• If your files appear to be moving, changing size, or doing other suspicious things, it's worth getting anti-virus software to check for Trojans and open ports. The Trojan Horse implanted virus could well be the offending computer virus.

• Your computer becomes unstable

• Strange error messages pop up while you operate your computer - or while the computer is starting up

• Some computer virus symptoms may alert infected users of their presence with an on-screen message of some sort,

• Frequent lock-ups, freezing, crashing or if your computer re-starts on its own

• If you suddenly spot a dramatic decrease, or considerable slowing down of your computer terminal, it is worth scanning for viruses, as this may be a cause.

● Your anti-virus software is crashing or is not working correctly .

Worsening system performance can also appear as a sudden and apparent lack of system resources or physical RAM memory, hidden or corrupt files and executables, or an unreasonable reduction in hard drive space.

Email problems that could be Signs of Possible virus Infection

● You are receiving many "Returned Mail" or "Failure Notice" email messages and you did not send those emails

● An extremely slow Internet connection and/or frequent disconnects

● You cannot properly send or receive email

● You are receiving email from people telling you that you have a virus.

● You received an email message with a strange attachment

● When you opened an email attachment, dialog boxes appeared and your whole system seemed to slow down or nearly crash.

● WARNING: If you receive any messages about an undeliverable message that has a file attachment, do not download or execute the file. Simply delete the message.

During these periods of heightened Hacker and Cracker activity when there are so many dangerous viruses and worms being passed from person to person, it would be prudent to question any of your correspondents and friends who send you an email containing an attachment **BEFORE** you open their attachments.

If it looks suspicious, ask them to tell you what it is and if they really sent it to you.

If this sounds like a lot of extra foolery, you need only lose all of your files and data to a malicious worm ONCE, and you'll probably be just as cautious as we are.

To the Credit of nearly all ISP's who provide email services, you can obtain extensive help and guidance directly from them.

AOL publishes very detailed guidelines for your protection, as does Earthlink, Compuserve, MSN, Comcast, etc. If you take the time to read them now, you'll be that much better prepared for your safe surfing and emailing activities tomorrow.

Preparing for a Disaster

A good Disaster Plan includes preparation for securing your data before a debilitating virus attack, and recovering as much as possible of what data might still be left in your computer after restoring operation of your system.

"What's your Before and After Strategy?"

The 'BEFORE' Strategy -

1. Make sure your firewall and anti-virus programs are installed and running.

2. Get the latest virus DAT or Signature files from the maker of your anti-virus software. (If the program you are using doesn't do this automatically while you are online, schedule your computer to automatically obtain Live Updates while you are sleeping, or schedule yourself to download them regularly.)

3. Do it every few days!
During periods of high virus activity with newer variations of viruses appearing nearly every day, the safest thing you can do is to maintain current updates which are usually very easy downloads.

BE DILIGENT! THINK "COMPUTER SAFETY"

If you use the internet at all, ALWAYS BE AWARE of the damage that can be done due to one little lapse of your memory.

Backup your personal files, those that you save to your "Documents' folder, financial records, etc. Save these Backup copies somewhere other than on your computer hard drive.

Removing a Virus from your computer

Probably the most upsetting situation is when your anti-virus software cannot quarantine, disinfect or remove a virus from your computer.

In a worst case scenario, this results in the necessity of completely 'wiping' your hard drive to remove all traces of a virus, and then reinstalling your operating system and program files.

Most program files can be reinstalled using the original CD's, etc. Software programs that you downloaded to your 'C' drive will probably be lost unless you made backup copies of them after downloading.

The same could hold true for all of your Data files. Wave goodbye to them, too, unless you have them saved on some external backup device or medium like floppies, CD's, ZIP Disks or tapes.

CAUTION! Be sure you save program Serial Numbers and Passwords in a safe notebook or journal, **NOT IN YOUR COMPUTER HARD DRIVE.**

Remote Server side Data Storage can be a great DataRecovery lifesaver, especially since these services have the ability to store extremely large data files.

There's the possibility that you need only Wipe your 'C' drive, leaving other partitions intact (such as a 'D' partition or drive). Data on 'D' could still be uncompromised and not infected.

You will normally need the 'C' drive to reload your Windows 95 or 98 operating system (OS). You CAN reload your OS directly using the Emergency Start up disk or OS Program installation disk for Windows ME, NET, 2000 and XP.

--------Side Bar ---------

With so many Operating Systems and browsers available, and the hundreds of different viruses and worms floating around on the internet, it is nearly impossible to list the virus recovery and removal instructions for all of them.

There are often local computer services that provide help for removing viruses, for a fee. They are usually very up-to-date on current threats and removal techniques.

You can always contact your Virus and Firewall software manufacturers for specific help in eliminating a virus. Your Internet Service Provider could also be able to help.

--------- End Side Bar ----------

"AFTER" a Virus has been Removed

Make sure you also virus scan the backup floppies, Zip Disks, etc, **before you reload your data files**.

Immediately after reloading the OS, reinstall up-to-date firewall and virus protection software, and scan your whole system to determine if any traces of the virus remain.

When you feel confident that all traces of viruses have been removed from your computer, renew you backup data.

Evaluate your Back-up tools: What do you have?

Are they capable of storing your data now and in the future?

Should you **consider REMOTE data storage**? It is relatively cheap. For a FEW DOLLARS PER MONTH, most services provide 50 MB or greater capacities. Their Storage Servers are heavily fortified against virus attacks and infections.

Downside: you'll need a working internet connection to retrieve your 'saved data'.'

Let's Summarize

If you haven't been Infected by a Computer Virus yet, you are either very lucky, or you have done a fine job of protecting yourself from the inevitable virus attacks.

Among those 60,000 reported strains of viruses already identified, and the hundreds more appearing every month, one or more of them could penetrate your Firewall and sneak by your anti virus program.

You Must Have a good, solid FIREWALL and up-to-the-minute anti virus program for insurance against a successful hacker attack.

If you're serious about maintaining a safe and secure computer system, and avoiding the threats of system shutdown, lost files and personal data, and even the potential Identity Theft so rampant today, take heed of the cautions we've tried to bring to light in this brief article.

Although we haven't covered everything you should be alerted to, our Firewalls-and-Virus-Protection website provides much more detail, covers more on the subjects **of Spam, Spyware, Cookies, Identity Theft,** etc, and provides many tools (some Free) to help you provide for your family and computer security.

Here'e a final reminder:

In addition to having the insurance provided by up-to-date firewall and anti virus software, you should seriously consider saving all of your program Serial Numbers and Passwords in a safe notebook or journal. NOT ON YOUR COMPUTER HARD DRIVE.

Why not do it now?
