



Internet Security Basics 101

by: Niall Roche

The explosive growth of the Internet has meant that thousands of people are today experiencing the joys of being online for the first time. With growth there always comes pain. Be it your growing pains as a child or the growth and development of this part of our culture called the Internet.

Firstly we need to quickly explain what the Internet is and where it came from. The Internet is the offspring of a military project called Arpanet. Arpanet was designed to provide reliable communication during global nuclear war. A vast network of interconnected computers was set up all over the world to allow the various branches of US and NATO forces to communicate with each other.

Nuclear war never came (thankfully) and the world was left with a massive network of computers all connected together with nothing to do. Colleges and universities started to use these computers for sharing research internationally. From there it grew and spread outside colleges to local homes and businesses. The World Wide Web was born and its father was a guy called Tim Berners Lee.

When you're connected to the Internet you're sharing a vast network with hundreds of millions of other users. This shared network provides resources that 15 years ago were never thought possible. Unfortunately when something is shared its open to abuse. On the Internet this abuse comes from hackers and virus creators. Their sole intent is to cause chaos and/or harm to your computer system and millions of other computer systems all over the world.

How do you combat this? You need an Internet security system. This might sound complicated but your Internet security system will be quite straightforward being comprised of just 2 - 3 Internet security products. We'll look at each of these products in more detail now:

AntiVirus Software

The first and most critical element of your Internet security system is antivirus software. If you don't have up-to-date antivirus software on your PC you're asking for trouble. 300 new viruses appear each month and if you're not constantly protecting your system against this threat your computer will become infected with at least one virus - it's only a matter of time.

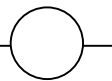
Antivirus software scans your PC for signatures of a virus. A virus signature is the unique part of that virus. It can be a file name, how the virus behaves or the size of the virus file itself. Good antivirus software will find viruses that haven't yet infected your PC and eliminate the ones that have.

Antivirus software can only protect your computer from viruses trying to infect it via email, CD-Rom, floppy disk, Word documents or other types of computer files. Antivirus software alone will not keep your computer 100% safe. You also need to use firewall software.

Firewall Software

The use of firewall software by home computer users is a relatively new occurrence. All Internet connections are a two way process. Data must be sent and received by your computer. This data is sent through something called ports. These are not physical things rather aspects of the way your computer communicates online.

Firewall software watches these ports to make sure that only safe communication is happening



between your computer and other computers online. If it sees something dangerous happening it blocks that port on your computer to make sure your computer stays safe from the person who is trying to hack into your system.

An easier way to understand a firewall would be to picture your computer as an apartment complex. At the front door of this complex there is a security guard. Every person who enters the complex must pass this security guard. If the security guard recognizes the person entering as a resident he allows them to pass without saying anything. If, however, the person entering the complex is unknown to him then he will stop that person and ask for identification. If they have no business being at the apartment complex he escorts them from the building.

If you are not currently using firewall software your computer will get hacked into - that's a guarantee.

PopUP Blocker

You can get a good popup blocker at no cost. An easy way to do this is to install either the Google or Yahoo toolbar. Both of these come with popup blockers built in. Popups are not necessarily dangerous but are a nuisance and using either of these toolbars will make your life that bit easier.

A simple rule for practicing online security is: "If in doubt then don't". If you don't recognize the file, the email address, the website or if your gut feeling says "no" then don't click that button.

About the author:

This article was submitted courtesy of the Spyware & Malware Guide. This site is dedicated to [spyware removal](#) and just generally helping users keep their PCs spyware free.

This book may be given to a third person as a gift but cannot be modified in any manner.

This rule have been established to protect the rights and ownership of the authors and to ensure that their work is upheld as their own