

Practicing Safe Surfing, or How to Survive on the Internet

Can You Survive?

This, as most people know, is a complicated subject. If the answer were simple, we wouldn't hear about computer networks at major corporations crashing when a new virus or worm is unleashed.

However, you can survive safely on the Internet. For me, the answer divides into two categories: *tools* and *behaviors*. Tools are software add-ons that you need, some of which may have been provided for you by your computer vendor, such as an anti-virus program. Behaviors are rules of the road that you never, ever violate.

Before we embark on this subject, please read my article entitled, *"What are the Internet and the World-wide Web?"*. It will give you the background you need to understand the tools and behaviors I recommend.

What are Viruses, Trojan Horses and Worms?

A ***virus*** is a piece of software that enters your computer attached to something else, such as email or a program you want to install. It may do nothing, or it may destroy your machine: once on your machine, its options are open.

A ***Trojan Horse*** is a program that appears to do one thing, but in reality is there for another purpose. For example, many popular browser add-ons claim to provide ease of use, fun features, etc. What they really do is install programs on your computer that report your activities to other web sites or add advertising to your Web browser and email; such programs are often called ***spyware***. More specifically, programs that bring unwanted advertisements to your computer are called ***adware***.

A ***worm*** is a program that, once installed on your computer, attempts to propagate itself to other computers at your home or on the Internet.

For the purposes of this article, I'll refer to any such unwanted program as a ***virus***.

How Does Your Computer Become Infected?

All these types of programs have several things in common, and many of the more serious "infections" have been caused by programs that fit into more than one category. What they have in common is that:

- Every such program must somehow be loaded onto your computer, and
- Each one must somehow be activated.

Just having a bad program sitting on your hard drive won't hurt your system; to live, it has to be launched (started).

In general, viruses are like vampires: **they can only enter your home when you let them in**. There are rare cases where serious errors in low-level programming (e.g., at least a good dozen or so by Microsoft in Windows XP) may allow your machine to be "taken over" by other computers and infected without your knowledge or action. We'll address this issue later.

How Do Viruses Spread?

These days, viruses spread over networks. In the 80's many Macintoshes were infected by people passing bad diskettes around, mostly by making illegal copies of software for friends. One infected machine led to a whole cluster of problems.

These days, virus writers spend most of their time working with the Internet communications protocols: they're fast and virtually ubiquitous. But there are two parts to propagation: entry and exit. In other words, the virus has to find its way onto your machine, and, if it behaves like a worm or spyware, must find a way to send its information from your computer to others.

Internet Traffic Basics

As far as the real Internet is concerned, every computer can both initiate outgoing communications (think "dial a phone") and accept incoming communications (think "answer a phone"). Almost all of the common, end-user programs such as email clients and web browsers only use outgoing communications; in fact, this is an important part of their design. Your email program knows what server to call up to get your email because you configured it that way; your web browser knows what computer to load pages from because of the URL (address) you typed or clicked on.

So what does this tell us? Among other things, *only certain programs on your computer should be able to talk on the Internet at all*. And almost all of those should only ever make outgoing connections, and those connections should be to well-known "hosts" (remote computers). So you need to know if your computer is communicating in ways that aren't good for you.

The basic tool in this regard is called a ***firewall***. As the name implies, it creates a barrier between your computer's actual hardware capability and the actions of the software running on it. Every time a program on your machine tries to connect to another computer or allow another computer to connect to it, the firewall is invoked and it decides if that connection is permissible.

There are several things to know about firewalls.

- Good firewalls are bidirectional: that is, they can block outgoing as well as incoming operations.

- Many cable and DSL modems have firewalls that come preconfigured for normal home use. It's difficult to know how safe you are, though, without checking with the manufacturer.
- Microsoft has a free firewall in Windows XP. But it has a serious (I'd say life-threatening) limitation: it cannot block outgoing communications. This is like having a car that can't go into reverse: you can drive for a while, but eventually you'll be stuck.
- For many home networks, it's a good idea to buy a router rather than a hub to share cable and DSL connections. Modern routers have very good firewalls built in them; hubs just split the connection to allow sharing. Even if your fast Internet modem has a firewall, a recently built router is probably better and smarter.
- You must work with software firewalls to teach them which programs should (and should not) be able to perform Internet operations. This can be tedious, but it's necessary.

There are several good firewall products on the market; there are even some free ones. I'm running **Norton Internet Security** on my laptop: it's a combination anti-virus and bidirectional firewall that seems to work fairly well. Bonnie runs **ZoneAlarm** (a free firewall) that I configured for her machine.

Behaviors, or What Can You Do?

There are many rules of the road for the Internet, and I'll summarize with a table at the end of this article. Simply put, there are certain actions you should never take without being sure of the source of the input or the expected outcome. And there's nothing you can do to make surfing "idiot proof", because some of the problems arise from differences in outlook: one person's junk email is another person's godsend.

The Next Level

Personally, I don't use the email systems provided by my Internet Service Provider. As I said in another document, an ISP selling email is like the power company selling toasters: it doesn't really make sense. **In addition, the bulk of all junk mail arises as a direct result of ISPs that sell your email information for profit.** If you don't believe me, read the fine print on your ISP contract or privacy agreement: there's always a loophole that lets them do what they want with the information.

I use email services provided by **usermail.com**. They just do email: there's no advertising, and they never sell anyone's information to anyone. For \$20 a year, you can almost guarantee that you'll never get any more junk mail.

However, after many years of using the same email name you will eventually start getting junk mail again. At that point, just change your account and notify

all your correspondents. In fact, a lot of people have two email names: a “real” one for friends and family, and a “surfing” one for general use. The “surfing” identity can easily be discarded or changed. All modern email clients support multiple simultaneous email accounts.

Internet Rules of the Road

Behavior	Explanation
Don't open email attachments unless necessary.	Most email viruses are in attachments, and the names don't always reflect the contents. Unless you expect an email from someone and know what it is, just say no. And remember: friends get infected, too.
Never install anything from the Internet unless it's essential. If you don't need it; it'll just slow you down. Don't be tempted by pretty pictures!	Regardless of the attraction, too many products are just spyware and adware : they claim to be free, but there's nothing free in this world.
Don't click on URLs in email when sensitive information is involved. Instead, use the URL you normally would to perform whatever operation must be done.	This is called "phishing". Links in emails can be forged to send you to a "look-alike" web site where your personal information is stolen.
Avoid opening email from strangers.	Most of it's junk; just delete it unopened.
Don't give your email name to anyone unless necessary. In particular, don't sign up for "newsletters".	Almost everyone sells your email name to someone else. If you want the news from an organization, visit their web site periodically and browse.
Don't give any important data (even your real name) unless you're sure of the organization and you're using a secure connection.	Look for the little padlock (for Internet Explorer) or the little key (for Netscape). In addition, the web site URL should begin with " https: ", not " http: " (note the 's').
Avoid going to web sites to ask that your name be removed from a mailing list.	This is often a ploy to verify that the email they used to reach you really works.
When you purchase on-line, check that you're really at the site you think you are.	Look at the URL (Internet address) in your browser and be sure you haven't been redirected unexpectedly.
When you purchase on-line, limit the number of sites you use.	There are quite a few "review" sites that give numerical scores for on-line retailers. Rely on only the best sites.
Be wary of "chat" programs.	They almost always contain spyware

	or adware .
Never give your Social Security Number, driver's license number or other vital information unless absolutely necessary.	Challenge any company that requires such information: they shouldn't need it. This applies to regular life as well as the Internet!

Tools and Techniques

Tool	Justification
Run an anti-virus program.	Essential to help you do safe emailing. Use Norton or McAfee or some other trusted brand.
Keep your anti-virus updated.	Without updates, an anti-virus program soon becomes useless. Most such programs will do this automatically. Let it.
Run a software or hardware firewall.	For hardware, it may be in your cable modem (find out), or you may need a good network router. For software, use products like Norton Internet Security or ZoneAlarm. Learn what they do for you.
Keep your operating system updated.	Visit the web site of your computer's operating system and update it often. For most people, this is Windows Update, and it can be launched directly from the Start menu. On new systems it runs automatically.
Get your email from a safe provider.	Forget your ISP. Pay for your email and demand better service.
Use wireless encryption	If you do wireless, use WEP or its successor.
Require logon passwords in Windows XP.	Don't default to just allowing the machine to come up logged on; use a good password.
Run SpyBot or some other adware removal software on a regular basis.	Spyware is everywhere these days. Removing their traces from your machine is important, and it requires the same sort of vigilance as virus

prevention.