BRUCE MEYER & ASSOCIATES

Computer & Network Support
Accounting & Manufacturing Software
Medical Billing Services & Software

Viruses, Pop–ups, and Spyware, OH MY!

I can remember when the first viruses appeared in the 1980's. We were stunned that someone would deliberately write software that would damage someone else's computer. I recommend running anti-virus software on a (gasp) quarterly basis. Soon it became monthly, then weekly.

Now, viruses appear daily and hourly. This frequency requires our vigilance, but also means that no one program or person can stop all viruses. We often hear about the spread of viruses via email. While this is the most common way to spread viruses, I want you to be aware that this is not the only way a virus can spread. You can get a virus from ANY method in which you bring data to your computer. This can include downloaded files from the internet, web pages, CDs and floppy disks, and removable hard drives and storage devices (like MP3 players and PDAs).

In addition to viruses, it is now commonplace to experience pop-up ads (some just annoying, and some quite embarrassing in nature), as well as spyware (cookies or tracking programs which reside on your computer and send information about the internet sites you visit to someone, without your permission or knowledge.)

Anti-virus and anti-spyware software is strongly recommended. Please note that these programs have "definitions" (basically, a file containing all the information known about a virus or spyware, and how to remove it). Definitions must be updated often for the program to do its job.

I apologize for the length of this document. The amount of information I need to share with you is too vast for a short email. You may want to print this for future reference.

Recently we have worked on dozens of infected computers, with these average results:

Type of Pest	Instances per PC
Virus infections:	10-100
Pop-up ads:	50-100
Spyware:	600 - 800

Below, I have described these types of "mal-ware", along with links to more information, and possible solutions that you can use. If you don't want to tackle these "monsters" alone, you can call us to come out, or bring your system in to our offices.

809 Highland Avenue, Greensburg, PA 15601-4315
Voice: 724-837-9433 Fax: 724-832-2576
Email: bmeyer@bm-a.biz Website: www.bm-a.biz

BMA Bruce Meyer & Associates

Computer & Network Support
Accounting & Manufacturing Software
Medical Billing Services & Software

Viruses, Worms and Trojans:

Viruses: Like the common cord of a flu that is passed from person to person, a computer virus is a malicious program spread from host (computer) to host. Most times does cause some problems, other times written for the pure enjoyment of the author. Frequently, the writer of a virus is not the person who launches the virus "into the wild". The author may post the virus on a web site, and wait for others to use the code (or program), and send it out via email. One recent virus, which attacked Windows XP machines, often caused the computer to crash. It is interesting that the system crash was not an intentional effect of the virus - it was merely the result of bad programming.

Worms: A worm is a program that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

Trojans: In Homer's Iliad, the Greeks give the giant wooden horse to their foes, the Trojans, as a peace offering. After the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow body and open the city gates, allowing their compatriots to pour in and capture Troy. In computer terms, a Trojan destructive program that masquerades as a benign application. Unlike a worm, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

Solutions: A good anti-virus program is the first (and best) step in defending your network and your computers against these problems. We recommend using TrendMicro's suite of products. They have some excellent solutions for all levels of business and personal use. They also have a free online scan available at: http://housecall.trendmicro.com/ .

Trend Micro: http://www.trendmicro.com
Norton: http://www.symantec.com
McAfee: http://www.mcafee.com
AVG: Available at no cost for personal (home) use:
http://www.grisoft.com/us/us_dwnl_free.php

More general information about viruses, worms and Trojans is available at
http://antivirus.about.com

809 Highland Avenue, Greensburg, PA 15601-4315
Voice: 724-837-9433 Fax: 724-832-2576
Email: bmeyer@bm-a.biz Website: www.bm-a.biz

BRUCE MEYER & ASSOCIATES

Computer & Network Support
Accounting & Manufacturing Software
Medical Billing Services & Software

Phishing:

Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

According to the Federal Trade Commission (FTC), phishers send an email or pop0up message that claims to be from a business or organization that you deal with- for example, your Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a Web site that looks just like a legitimate organization's site, but it isn't. The purpose of the bogus site? To trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

The FTC, the nation's consumer protection agency, suggests these tips to help you avoid getting hooked by a phishing scam:

1. **If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message.** Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.

2. Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:' (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

3. Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

Visit http://www.antiphishing.org for more information.

809 Highland Avenue, Greensburg, PA 15601-4315
Voice: 724-837-9433 Fax: 724-832-2576
Email: bmeyer@bm-a.biz Website: www.bm-a.biz

Hackers:

A hacker is a person who delights in having an intimate understanding of the internal workings of a system, computers, software, and computer networks in particular. Among professional programmers, the term hacker implies an amateur or a programmer who lacks formal training. It is more common these days for "hacker" to be a derogatory term. The press now uses the term to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data. Hackers, themselves, maintain that the proper term for such individuals is cracker. What ever term is used, you will want to protect yourself and your data from the outside world.

A good firewall will go a long way in preventing attacks from hackers who are outside your network. There are numerous commercial firewalls that you can purchase, but unless they are properly configured, they can leave security holes in your network. A firewall which is too stringent can prevent the flow of normal network traffic. Please look at this page for an in-depth look at the benefits of having a firewall in place. http://www.faqs.org/faqs/firewalls-faq/

Pop-ups

Visitors to some web sites may have advertisements display over the site they are viewing, in a pop-up window. Some of these ads may be placed there by the owner of the site. Unfortunately, these advertisements are more often created by an AdWare application that was loaded on the visitor's system or a control that was installed into the visitor's browser.

Some adware shows random ads while you browse the web. Other adware applications try to target the advertising based on the page you are viewing. For example, some students signing their Perkins Loan Promissory Note have seen popup ads for "loans with no credit check", "loan consolidation", "get rid of debt quick" schemes, and many other supposedly "helpful" advertisements relating to loans.

There are many free and low cost applications which help stop popup ads. Many of the major anti-virus manufacturers are adding popup blockers in their software. One of the easiest free applications to install and use is the google toolbar. It adds the functionality of a Google search to your web browser, while it blocks pop up advertising. Google does not add any spyware to your system. You can download it at http://toolbar.google.com . More information is available at http://www.search.com/search?q=block%20pop%20up

809 Highland Avenue, Greensburg, PA 15601-4315
Voice: 724-837-9433 Fax: 724-832-2576
Email: bmeyer@bm-a.biz Website: www.bm-a.biz

BRUCE MEYER & ASSOCIATES

Computer & Network Support
Accounting & Manufacturing Software
Medical Billing Services & Software

Spyware and Adware

Spyware and adware are technologies that assist in gathering information about a person or organization without their knowledge. Most spyware programs are installed on your computer by YOU (or your children). The program that you download may seem helpful or fun, but is really there to secretly gather information about the use and relay it to advertiser or other interested parties. As such, spyware is cause for public concern about privacy on the Internet.

Take care when clicking to get rid of popup windows that may appear on your computer. Read the warning messages that appear before you click "OK" or "Yes". By doing so, you may be agreeing to download a spyware program to your computer. Do not randomly download programs that look like fun or advertise themselves as something you can't live without. Try to get programs from reputable sources such as C/Net's www.download.com, or and be sure to read the **EULA** (**E**nd **U**ser **L**icense **A**greement) when installing software. We know people rarely do th is, but it is one of the best ways to protect yourself and your computer.

There are many programs, some available at no cost, which can help get rid of spyware once it is on your computer. In our experience, for the initial removal of spyware, it takes several programs. We recommend both SpySweeper and Ad-Aware. Once the system is cleaned,, use of Ad-Aware, which is free and allows updates of spyware definitions, should keep things running smoothly. See http://www.spywareguide.com for more information.

Ad-aware: http://www.download.com/3120-20-0.html?qt=ad-aware&tg=dl-2001
SpySweeper: http://www.spysweeper.com (Click on Free Download)

Scare tactics?
So often when I write about this stuff, I feel like a tabloid journalist hyping up the latest crisis. Unfortunately, this is all true, and at least one of these "nasties" is probably in your computer right now getting ready to spread.
If you **think** that you might have a virus or other mal-ware, you probably do. (If you do not think you have a virus or mal-ware, it would be a safe bet that you have at least one "Data Miner" or "tracking Cookie" on your system). If you can prevent a virus from spreading, you could be saving yourself (and your friends, relatives, vendors and clients) from similar or worse damage and expense.

Thanks,

Bruce D. Meyer

809 Highland Avenue, Greensburg, PA 15601-4315
Voice: 724-837-9433 Fax: 724-832-2576
Email: bmeyer@bm-a.biz Website: www.bm-a.biz