



EMERALD CITY COMPUTER SOLUTIONS, INC.

QUESTIONS ABOUT MALWARE

Source: Microsoft's website

Q: What are malware, viruses, spyware, and cookies, and what differentiates them?

A: Let us take the easy one first. "Malware" is short for malicious software and is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network, whether it's a virus, spyware, et al.

Q. What exactly is a virus? Is a "worm" also a virus?

Viruses are computer programs or scripts that attempt to spread from one file to another on a single computer and/or from one computer to another, using a variety of methods, without the knowledge and consent of the computer user. A worm is a specific type of virus that propagates itself across many computers, usually by creating copies of itself in each computer's memory.

Many users define viruses simply as trick programs designed to delete or move hard drive data, which, strictly speaking, is not correct. From a technical viewpoint, what makes a virus a virus is that it spreads itself. The damage it does is often incidental when making a diagnosis. Obviously, any incidental damage is important, even when authors do not intend to create problems with their viruses; they can still cause harm unintentionally because the author did not anticipate the full effect or unintentional side effects. The most common method used for

spreading a virus is through e-mail attachment. Sending a virus, even if designed to be harmless, can cause unforeseen damage.

Q. How can I prevent a virus from infecting my computer?

A virus scanner is the most common tool for prevention. This utility attempts to scan a computer program before it runs, and if it recognizes the signature of a malicious code, it shuts it down. Many scanners also evaluate programs to determine if it contains any virus-related characteristics.

The best way to stop viruses is to use common sense. If an executable computer program is attached to your e-mail and you are unsure of the source, then it should be deleted immediately. Do not download any applications or executable files from unknown sources, and be careful when trading files with other users.

Q. What is a "Trojan Horse"? Isn't this a virus by any other name?

I have heard some arguments that Trojan Horse malware is a virus subset (and vice versa) but there are differences worth mentioning.

A Trojan Horse meets the definition of virus that most people use, in the sense that it attempts to infiltrate a computer without the user's knowledge or consent. A Trojan Horse, similar to its Greek mythological counterpart, often presents itself as one form while it is actually another. A recent example of malware acting as a Trojan horse is the recent e-mail version of the "Swen" virus, which falsely claimed to be a Microsoft update application.

Trojans typically do one of two things: they either destroy or modify data the moment they launch, such as erase a hard drive, or they attempt to ferret out and steal passwords, credit card numbers, and other such confidential information.

Trojan Horses can be a bigger problem than other types of viruses as they are design to be destructive or disruptive, as opposed to viruses and worms where the coder may not intend to do any harm at all. Essentially this distinction does not matter in the real world. You can lump viruses, Trojans, and worms together as "things I don't want on my computer or my network".

Q. How do I prevent a Trojan Horse attack?

The methods for dealing with Trojans are generally the same as for those for dealing with viruses. Most virus scanners attempt to deal with some of the common Trojans with varying degrees of success. There are also specific "anti-Trojan" scanners available, and your best weapon is common sense yet again. Score another point for safe computing!

Q. What are cookies and spyware? How are they different?

A cookie is just a bit of text in a file on your computer, containing a small amount of information that identifies you to a particular website, and whatever information that site wanted to retain about the user when they are visiting.

Cookies are a legitimate tool used by many websites to track visitor information. As an example, I might go to an online computer store and place an item in the basket, but decide not to buy it right away because I want to compare prices. The store can choose to put the information about what products I put into my basket in a cookie stored on my computer. This is an example of a good use of cookies to help the user experience.

The only websites that are supposed to be able to retrieve the information stored in a cookie are the websites that wrote the information in that particular cookie. This should ensure your privacy

by stopping anyone other than the site you are visiting from being able to read any cookies left by that site.

Q. Do some websites use cookies to exploit user information?

A. Unfortunately, yes. Some may deceive users or omit their policies. For example, they may track your Web surfing habits across many different websites without informing you, and then use this data to customize the advertisements you see on websites, etc., typically considered as an invasion of privacy.

It is difficult to identify this and other forms of "cookie abuse," which makes it difficult to decide if, when, and how to block them from ones system. In addition, the acceptable level of shared information varies between users, so it is difficult to create an "anti-cookie" program to meet the needs of everyone.

Q. How does spyware exploit user information?

The spyware problem is similar to the cookie problem from the point of view that both are an invasion of privacy, although spyware is different from cookies, technically speaking. Spyware is a program that runs on your computer and, again, tracks your habits and tailors these patterns for advertisements, etc. Because it is a computer program rather than just a bit of text in a cookie, spyware can also do some nasty things to ensure that the spyware keeps running and keeps influencing what you see.

Q. How do I know if spyware is running on my computer?

You can use detection programs such as Ad Aware and others. Similar to antivirus software, these programs compare a list of known spyware with files on your computer and can remove any that it detects. But

again, what some consider unacceptable is perfectly acceptable to others.

Q. How does spyware install itself on computers?

Common tactics for surreptitious installation include rolling up advertising programs into "free" shareware program downloads, and once the spyware is installed it can download advertisements 24 hours a day and overlay them on websites and programs you are using. Anti-spyware programs can combat spyware from being installed, but the best strategy is to discriminate what you choose to download and install.

Q. Can spyware send tracked information to other people?

Some forms of spyware monitor a target's Web use or even general computer use and sends this information back to the spyware program's authors for use as they see fit. To fight this kind of problem, a spyware removal tool is obviously helpful, as is a firewall that monitors outgoing connections from your computer. Other forms of spyware take over parts of your Web browsing interface, forcing you to use their own search engines, where they can track your browsing habits and send pop-up advertisements to you at will.

The biggest concern regarding spyware is that most of them are poorly written or designed. Many people first realize their computer is running spyware when it noticeably slows down or stops responding, especially when doing certain tasks such as browsing websites or retrieving e-mail. In addition, poorly written spyware can often cause your computer to function incorrectly even *after* it has been removed.

Q. Do you have a quick summary of how to prevent malware problems?

A: Yes — see below.

Two of the biggest concerns for computer users today are viruses and spyware. In both cases, we have seen that while these can be a problem, you can defend yourself against them easily enough with just a little bit of planning:

- Keep your computer's software patched and current. Both your operating system and your anti-virus application must be updated on a regular basis.
- Only download updates from reputable sources. For Windows operating systems, always go to <http://update.microsoft.com/microsoftupdate/> and for other software always use the legitimate websites of the company or person who produces it.
- Always think before you install something, weigh the risks and benefits, and be aware of the fine print. Does the lengthy license agreement that you don't want to read conceal a warning that you are about to install spyware?
- Install and use a firewall. If you are running Windows XP you can use the built-in software firewall under Control Panel, and there are free versions of firewalls that work on all versions of Windows.
- Prevention is always better than cure.