

## **I spend all of this money every year to protect my computer with Anti-Virus software. Why do I still get Viruses?**

Each year, computer users spend \$30 - \$100 per computer to protect against viruses. Why do they still get viruses? There are a variety of reasons, but first, it is important to know what a virus is and where it comes from. Following are excerpts we have found from published articles that describe the various types of annoyances that attack our computers every day.

### **What is a Computer Virus?**

A **computer virus** is a computer program that can copy itself and infect a computer without permission or knowledge of the user. The term "virus" is also commonly used, albeit erroneously, to refer to many different types of malware and adware programs. The original virus may modify the copies, or the copies may modify themselves, as occurs in a metamorphic virus. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user sending it over a network or the Internet, or by carrying it on a removable medium such as a floppy disk, CD, or USB drive.

### **What is Malware?**

**Malware**, a portmanteau word from the words **malicious** and **software**, is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Many computer users are unfamiliar with the term, and often use "computer virus" for all types of malware, including true viruses.

Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software. In law, malware is sometimes known as a **computer contaminant**.

Malware is not the same as defective software, that is, software which has a legitimate purpose but contains harmful bugs.

### **What is Spyware?**

**Spyware** is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.

While the term *spyware* suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as

Internet surfing habit, sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting Web browser activity, accessing websites blindly that will cause more harmful viruses, or diverting advertising revenue to a third party. Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other programs.

## What is E-mail Spam?

**E-mail spam**, also known as "bulk e-mail" or "junk e-mail," is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail. A common synonym for spam is unsolicited bulk e-mail (UBE). Definitions of spam usually include the aspects that email is unsolicited and sent in bulk.

E-mail spam slowly but exponentially grew for several decades to several billion messages a day. Spam has frustrated, confused, and annoyed e-mail users. The total volume of spam (over 100 billion emails per day as of April 2008) has leveled off slightly in recent years, and is no longer growing exponentially. The amount received by most e-mail users has decreased, mostly because of better filtering. About 80% of all spam is sent by fewer than 200 spammers.

E-mail addresses are collected from chatrooms, websites, newsgroups, and viruses which harvest users' address books, and are sold to other spammers. Much of spam is sent to invalid e-mail addresses. ISPs have attempted to recover the cost of spam through lawsuits against spammers, although they have been mostly unsuccessful in collecting damages despite winning in court

## Who creates Malware?

Programmers create malware, ***it is not accidentally created***, and the person who creates it intentionally developed the malware to do damage.

In the early days of computer viruses the people creating the viruses had extremely specialized programming skills, it took a lot of work and a lot of knowledge. You had to know how operating systems worked, what vulnerabilities were available for exploitation, and you had to know how to take advantage of those vulnerabilities. It took a lot of effort. In those days virus creators were primarily disgruntled employees lashing back at their employer by creating and releasing viruses into the company system. These people generally did not intend for the entire world to be infected, they just wanted to hit a specific person/entity, however generally speaking they didn't particularly care if others got infected, after all their computer would be safe, they knew how to protect against viruses.

Unfortunately with the growing popularity of the Internet, and increasing computer savvy by younger generations, viruses are becoming easier to create, and much easier to distribute. Now, if you know where to look, you can find programs that will help you write a virus, or worm. These programs take existing viruses and alter them so that a new virus is created. Almost anyone with minimal computer

knowledge can custom build his or her own personal virus. This new breed of virus programmers makes it much more difficult to track the explosion of new viruses, since the need for specialized training has vanished. Luckily in order to create a brand new and truly effective virus you still need to have specialized training and advanced knowledge of computer systems. This breed of virus programmers are mainly out for glory, they want to see their virus featured on the five o'clock news. Generally these are high school or sometimes college students who want to prove that they can create a virus that will spread around the world in record time.

### **Why do people create malware?**

No financial or career gain is obtained by writing viruses, and the fame achieved is usually shadowed by the fines and long prison terms one accumulates after getting caught. David L. Smith, alleged author of the Melissa virus could face up to 40 years in prison if convicted. So why do people write these viruses? Are these people crazed lunatics, possibly?

### **Reasons for the insanity**

Marshall Brain, the writer of "How Computer Viruses Work" suggests that there are at least three reasons why people write computer viruses. Marshall thinks the first reason why people write viruses is analogous to why vandals and arsonists wreak their havoc - for the pure thrill of seeing something destroyed, for example, a destroyed hard drive or computer network [Brain 2000].

The second reason is similar to the first but this reason is for the pure thrill of watching things "blow up". Remember the kid in Chemistry class who was a little bit too fascinated with watching sodium or lithium explode in water? The same fascination can come from creating a virus that spreads quickly - the virus is like a "bomb inside a computer, and the more computers that get infected, the more "fun" the explosion" [Brain 2001].

According to Sophos, most virus writers tend to be male, single, and under the age of 25. Their self-esteem relies on the acceptance from peers or their small electronic community. This leads to Brain's third reason for why virus writers do what they do: bragging rights. If a hole in a corporation's computer network has never been exploited, a virus writer may ask himself; why not exploit that hole before someone else does? I'll show them the hole!

### **What is Anti-Virus Software?**

**Antivirus software** (sometimes spelled Anti-Virus or anti-virus with the hyphen) are computer programs that attempt to identify, neutralize or eliminate malicious software. The term "antivirus" is used because the earliest examples were designed exclusively to combat computer viruses; however most modern antivirus software is now designed to combat a wide range of threats, including worms, phishing attacks, rootkit, Trojans, often described collectively as malware.

Unfortunately, since all malware is manmade, the companies that try to protect us against those threats can only do so after-the-fact. Anti-virus software

companies have huge staffs that scour the web looking for infections and they also depend on users to submit issues to be resolved. Once a problem has been identified and a way to stop it has been created, new information is downloaded to each computer that holds a valid subscription to that company's anti-virus software. Sometimes the solution arrives before a particular computer is infected so the computer is protected from it. Sometimes the solution arrives after the computer is already infected and the Anti-Virus software can clean the infected computer. Sometimes the solution arrives but the virus or malware is so severe that extraordinary measures have to be taken to clean the computer, either special software or a complete reformat

Anti-virus software companies make no guarantees. They are always one step behind the developers of this annoying problem. They do the best they can with the information that they have to work with but they can't guarantee complete protection. As long as computers are being developed by humans, there will be vulnerabilities. As long as there are vulnerabilities, there will be someone out there trying to exploit them.

### **If one Anti-Virus solution is good, will two or three work better?**

Typically not, by the very nature of how it works and the depth that it probes inside computer operating systems, Anti-virus software is looked at by other Anti-Virus software as a virus itself. There are some programs that are very specialized will work together, but for the most part, be very careful about too much protection, it will get you into trouble.

So, now that you know everything you would like to about viruses, what do you do next? Here is an article that we found that outlines what we all should be doing on a daily basis.

### **Best Practices**

Over the past few years, the internet has gone from something that "showed the average person what some nerd thinks about Star Trek" to an invaluable tool for information, entertainment, and communication. Unfortunately, with the internet's increase in popularity has come a rise in the dangers of its use. Fortunately, you can help protect yourself from the malicious aspects of the internet by following our list of best practices.

### **Protect yourself from viruses**

---

It used to be that you had to go to some effort to infect your computer with a virus. Now, it is all too easy to catch a virus. Mostly, these are spread via email, though you can also be infected through downloads from the internet or from peer-to-peer file sharing networks. Your best line of defense is to use antivirus software, such as Norton Antivirus, McAfee VirusScan, or AVG. However, we must stress that it's not enough to have the software installed—you must make

sure you keep it up to date! New viruses are discovered "in the wild" every day, and most antivirus software publishers release updates once a week, if not more often.

Antivirus software can protect you, but your best protection is going to be being an informed, aware internet user. Don't open email attachments that you are not expecting to receive, even if it comes from a known source. We will never send you an attached file, so if you receive an email claiming to be from us that has an attachment, delete it right away. Be suspicious of software downloaded from peer-to-peer networks (like Kazaa or BitTorrent) or via IRC; the allure of free software may be great, but not only are you breaking the law, you're running the risk of the software containing viruses or other malicious programs that can give others access to your computer.

### **Protect yourself from "malware"**

---

"Malware" is a generic term that's short for "malicious software." Some types of these programs are also referred to as "adware" or "spyware." These programs are typically presented to you when you visit a website. They'll promise you some free, wonderful service, but all they really do are not-so-wonderful things like monitor your internet activity and report back to them so they can force you to view advertisements. Some programs are even more malicious than that, opening up "back doors" on your computer so that spammers can use your machine as a mail relay to send millions of junk messages to other people on the internet.

Just as with viruses, your best protection is to be an informed, aware internet user. Remember the adage that there's no such thing as a free lunch. If you have to install a piece of software to use their service, it's likely that the software is going to be malware. If a website asks you to download and install something that you did not specifically request, do not install it!

There are free programs that can protect you from malware. The three most popular, and the ones that we know to be trustworthy, are Malwarebytes, Ad-Aware and Spybot S&D. These programs are similar to virus scanners, except they typically require manual scans of your system for malware, rather than monitoring your system in the background.

### **Protect yourself from software bugs**

---

Software is written by humans. Humans are fallible. Therefore, software is fallible. Sometimes, it is discovered that there are holes or errors in software that can cause problems. It is a good idea to keep abreast of updates to your operating system and any software you use, particularly if it can be used to get information from the internet. If your system runs the Windows operating system, regularly visit <http://www.windowsupdate.com> and check for updates to your computer. If your system is a Macintosh, regularly visit <http://www.apple.com/support/>. You can also find updates for your web browser or

email program from wherever you downloaded the software; if you're using Internet Explorer and Outlook Express on a Windows computer, you can get updates to these programs through Windows Update.

### **Practice common sense!**

---

There's no such thing as a free lunch. If something seems too good to be true, it probably is. If you get an email saying you did something that you didn't, it's probably a fake. Don't reply to spam emails asking to be taken off their list; all you're doing is confirming that they found a live email address to someone who looks at their messages. Be careful with the information you give out online. Only buy from trustworthy merchants.

### **Think about alternatives**

---

If you were a bad guy, looking to exploit people, would you attack where you could do the most amount of damage, or attack where no one would be affected or even notice? You'd want to do the most damage you possibly could. Your computer may have come with a web browser and email program, and they work just fine. But, there's millions of other people out there using the same software, so there's hackers out there looking to exploit security holes in that software more than some of the other web browsers or mail programs out there.