

McAfee®



Protect what you value.

Protecting Your Computer against Threats and Attacks

Table of Contents

Defending against Malware and Trojan Horse Threats.....3

What Do Trojan Horses Do?.....3

How Does My PC Get a Trojan?.....3

Top 13 Ways to Defend Against Malware and Trojans.....4

Protecting Your Computer against Threats and Attacks

Using a computer for web surfing, shopping, banking, email, instant messaging (IM), and gaming can put you at high risk of being victimized. Malware—short for malicious software, which can include viruses and Trojan horses—is being used ever more frequently by cybercriminals throughout the world. A virus is a manmade program or piece of code that causes an unexpected and usually negative event; a Trojan horse program is a malicious program that pretends to be a benign application. (They are not viruses since they do not replicate, but Trojan horse programs can be just as destructive.)

Keeping yourself safe against malware, Trojans, and viruses is not difficult. Companies like McAfee provide most of the protection required, but some of the responsibility rests with the computer user as well. Follow the steps outlined in this whitepaper to protect your PC against attack.

Defending against Malware and Trojan Horse Threats

By exploiting vulnerabilities in operating systems and browsers, malware can sneak malicious Trojan horse programs onto unsecured PCs. Unsuspecting and unprotected users can also download Trojans, thinking they are legitimate game, music player, movie, and greeting card files. Trojans can also lurk in files shared between friends, family, and coworkers using peer-to-peer (P2P) file sharing networks.

Trojans have traditionally been spread by email, but they're increasingly showing up in IM, on PDAs, and on cell phones. Organized crime rings have devised insidious new ways of delivering Trojans, and consumers must stay informed of the latest tricks. Protection against these multi-faceted attacks requires integrated anti-virus, firewall, and anti-spyware technologies.

What Do Trojan Horses Do?

Today, Trojans can be spread by browser drive-bys, in which the program is downloaded in the background when you simply surf to a rigged web site. Shell code runs a Trojan that downloads additional code—various forms of bots, spyware, backdoors, and other Trojan programs. Hackers then send emails to lure users to web sites where unsuspecting victims are tricked into revealing personal information, which is known as "phishing." Hackers can also exploit security weaknesses on sites and then piggyback their Trojans onto legitimate software to be downloaded by trusting consumers.

How Does My PC Get a Trojan?

P2P networking has become a launching pad for viruses. Attackers incorporate spyware, viruses, and Trojan horses into their free downloads. One of the most dangerous features of many P2P programs is the "browse host" feature that allows others to directly connect to your computer and browse through file shares.

P2P networking can accidentally give access to logins, user IDs, and passwords; Quicken files and credit reports; personal information such as letters, chat logs, cookies, and emails; and medical records you accidentally house in accessible folders on your PC. As with email and IM, viruses in P2P files are capable of weaving their way through as many users as they can, stealing information and delivering it to cybercriminals who forge identities and commit fraud.

Top 13 Ways to Defend Against Malware and Trojans

Although hackers never stop developing new tricks to commit fraud and steal identities, you can take proactive steps to safeguard your systems. All it takes is a combination of robust security software and a commitment to following basic safety rules:

1. **Protect your computer with strong security software** and make sure to keep it up to date. The McAfee® Internet Security Suite guarantees trusted PC protection from Trojans, hackers, spyware, and more. Its integrated anti-virus, anti-spyware, firewall, anti-spam, anti-phishing, and backup technologies work together to combat today's advanced multi-faceted attacks. It scans disks, email attachments, files downloaded from the web, and documents generated by word processing and spreadsheet programs.
2. **Use a security-conscious Internet service provider (ISP)** that implements strong anti-spam and anti-phishing procedures. For example, Comcast and AOL partner with McAfee to block known phishing sites so that customers can't reach them. The SpamHaus organization lists the current top 10 worst ISPs in this category. Consider this when making your choice.
3. **Enable automatic Windows updates** or download Microsoft updates regularly to keep your operating system patched against known vulnerabilities. Install patches from other software manufacturers as soon as they are distributed. A fully patched computer behind a firewall is the best defense against Trojan and spyware installation.
4. **Use extreme caution when opening attachments.** Configure your anti-virus software to automatically scan all email and IM attachments. Make sure your email program doesn't automatically open attachments or automatically render graphics, and ensure that the preview pane is turned off. This will prevent macros from executing. Refer to your program's safety options or preferences menu for instructions. Never open unsolicited business emails, or attachments that you're not expecting—even from people you know.
5. **Be careful when engaging in P2P file-sharing.** Trojans sit within file sharing programs waiting to be downloaded. Use the same precautions when downloading shared files that you do for email and IM. Avoid downloading files with the extensions *.exe*, *.scr*, *.lnk*, *.bat*, *.vbs*, *.dll*, *.bin*, and *.cmd*. Anti-virus software and a good firewall will protect your system from malicious files.
6. **Download the latest version of your browser** to ensure that it is also fully updated and utilizes the latest technologies to identify and filter out phishing sites that can install Trojans.
7. **Use security precautions for your PDA, cell phone, and Wi-Fi devices.** Trojans arrive as an email or IM attachment, are downloaded from the Internet, or are uploaded along with other data from a desktop. Cell phone viruses are in their infancy, but will become more common as more people buy phones with advanced features. Anti-virus software is available for PDAs and cell phones. McAfee also offers trusted security solutions for Wi-Fi.
8. **Configure your IM application correctly.** Make sure it does not open automatically when you start your computer. Turn off your computer and disconnect the DSL or modem line when you're not using it. Beware of spam-based phishing schemes—don't click links in emails or IM.
9. **Be certain a web site is legitimate before you go there.** Use software that automatically checks this, such as McAfee SiteAdvisor.® You can also check the validity of individual web addresses (URLs) with a WHOIS search such as www.dnsstuff.com.
10. **Back up your hard drive or your network drive.** With CD-writers so readily available and so inexpensive, backing up has become easier and faster, and back-up software lets you automate backups, making things even easier.
11. **Get software that takes snapshots of your system.** This lets you revert to the latest snapshot when things go wrong so you can recover from a crash quickly. However, these snapshots are not backups of your system or files, so you still need to perform regular daily backups.

12. Visit McAfee at <http://us.mcafee.com> for information on how to fight the latest viruses and worms.

Often, you can download patches that will help prevent an attack. Sometimes the federal government issues suggestions about preventing virus infections. Treat these with great caution: The Department of Homeland Security suggested network administrators cut off access to ports 135, 139, and 445 to prevent infection by the Blaster worm. Network administrators who followed this advice found that the actions caused problems when people tried to use Microsoft Outlook and Exchange. It was later discovered that the Blaster worm uses port 69 to replicate itself to other PCs on a network, rather than those ports named by the government.

13. Turn your PC off. If you are using an always-on connection such as cable or DSL, turn off your PC when you are not using it. Always-on connections have what is called a static IP address, which makes it easy to locate your computer on the Internet, thus making it an easy target. Turning off your PC will prevent people from accessing it over the Internet.

McAfee, Inc.
3965 Freedom Circle,
Santa Clara, CA 95054
888.847.8766
www.mcafee.com

McAfee, VirusScan, and/or other noted McAfee related products contained herein are registered trademarks or trademarks of McAfee, Inc., and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. Any other non-McAfee related products, registered and/or unregistered trademarks contained herein is only by reference and are the sole property of their respective owners. © 2008 McAfee, Inc. All rights reserved. 6-protect-001-0308