



Privacy, Security & Virus Information

What Virus Threats Do You Face?

Did you know that a Trojan Horse is not technically a virus?
Did you know that the first virus released was by a high school student?

The History of the Computer Virus

The computer virus has been around since the invention of the computer. The concept of the computer virus is actually not inherently bad, and they have been used by computer programs to perform tasks within their computer system. The first virus to be released and spread with ill intent was a program called “Elk Cloner”, created in 1982 by high school student Rich Skrenta, to infect Apples.

Common Types of Threats

When the public hears about computer threats, they often hear words like “Trojan Horse” or “Worm”. Yet, what do these names mean, and what dangers do they pose to your computer system?

Worm: A computer worm is a program that will duplicate itself within one computer and then send its clones through the network to infect other computer systems. One of the scariest things about worms is that they are able to work “behind the scenes”, without the computer owner’s intervention or even awareness.

A [powerful virus detection system](#) is the only way to protect your computer from worms.

Trojan Horse: A Trojan Horse is a piece of software that users install in their computer. That’s right; the user invites this dangerous program into their computer. Of course, they are tricked into doing so. Trojan Horses masquerade themselves as useful programs to gain your trust. Since users can have no way of knowing whether a program is a Trojan Horse or not, [powerful virus detection](#) is the only protection.

Increasing Virus Threats with the Internet

Email Worms: Unsuspecting targets will open an email and infect their computer with the worm. Originally, this could be prevented by not opening emails from unknown senders. Unfortunately, worm designers are now able to create worms that infect a person’s computer and send their own emails. This means that your computer worm could be using your email account to send itself to all of your contacts without your knowledge.

File Worms: Accepting a file through a chat site or instant message places you at risk for unleashing a worm into your computer. In many cases, the worm will create a file within the file, under a harmless sounding name, in order to disguise itself.



Web Security and Maintenance Services

McAfee Security



Trojan Horse Downloads and Uploads: After inviting a Trojan Horse into your computer and allowing it to live undetected, the program can start downloading other harmful programs into system, overloading it and eventually destroying your hard-drive. Worse yet, Trojan Horses are also able to upload files from your computer and send them over the internet; this is one strategy that identity thieves use to get their hands on your material.

Keystroke Logs: One variety of a Trojan Horse is a **Keystroke Logger**. This program keeps track of the strokes made on your keyboard, looking for patterns that would indicate usernames, passwords, credit card numbers, and other personal information. The program then uses the internet to send this information home, where it can be used in identity theft.

Defend your computer's internet security with McAfee anti virus software

[McAfee Internet Security Suite >](#)

[McAfee Virus Scan Plus >](#)

[McAfee Total Protection >](#)

[McAfee PC Protection Plus >](#)