

united states

global sites

products

purchase

service &amp; support

security response

downloads

about symantec

search

feedback

## The Worm Has Turned

Worms are one type of particularly malicious code that can cause major damage to the files, software, and data on your computer. They are sneaky and prolific, sometimes copying themselves until they clog your system. While these tricky intruders can be particularly difficult to detect, here is some information that may help you get the hook into that worm.

### Worms vs. Viruses

A worm's most insidious characteristic is its ability to distribute functional copies of itself to other computer systems. While viruses rely on attaching to another program to be executed, worms are free agents that can roam independently through networks, propagating and wreaking havoc (although they are not automatically executed -they must be manually opened).

### The Danger of Worms:

- **They spread easily.** Worms' ability to spread themselves without attaching to other programs makes their reproduction swift and their path of destruction wide.
- **They are deceiving.** Worms are often sent via email, disguised as a benign attachment or game. For example, the Melissa worm used email address books to send itself as an email from a friend. Recipients recognized and trusted the sender and, therefore, opened the email attachment.
- **They can cause serious damage.** In recent cases, worms have carried a malicious payload that was capable of doing serious damage to computer data. Some worms rename and hide your files so they are inaccessible, others keep the file name and path but overwrite the data. Files can even be replaced with versions of the worm. Deleted files can often be retrieved later -but not so if a worm overwrites them.
- **They are easy to create.** The code for creating worms can be found on Web pages and Usenet groups dedicated to the topic. For anyone who knows basic programming and where to look for information, creating a worm is not that difficult.

### How Worms Dig Their Way In

There are several ways that worms get into your computer. The most common is through the Internet and email. You can also get a worm through file sharing, like the online program Gnutella, used to trade MP3s. Instant messaging programs, like IRC (Internet Relay Chat), can also be an entryway for worms, as well as Web pages that offer downloads -if you accept the download.

### What do they do once they're there?

One of the things a worm does best is replicate. It hides in your computer and creates copies of itself repeatedly. If it has a payload, all the segments and copies of the worm may deliver the payload. The result can be a simple display in a text message warning you of the intrusion, or in the worst cases, all the files on your hard drive will be renamed and overwritten.

Many worms will notify you of their arrival once they have proliferated your machine. You may get a message, picture, or music from the worm program revealing its presence. More subtle indications of worms are noticeable changes in file sizes or reports of less RAM than you actually have in your computer. But many times, you won't notice the worm infection until its countless replications have clogged system resources and slowed your computer to a halt.

Some advanced worms even create back doors into your system, allowing unauthorized access. Extremely invasive worms can use instant messaging programs to send password and file information to the worm's creator. Another nasty ability of worms was evidenced by the "ILOVEYOU" worm, which spread by sending itself to all email contacts in the user's Microsoft Outlook address book, repeatedly, at scheduled intervals. This massive consumption of network resources disabled some companies until a fix was developed.

## Protection

A quality anti-virus software package, such as [Symantec's Norton AntiVirus](#), is your first line of defense in preventing an invasion of worms, and their cousins, the virus and the Trojan horse. Anti-virus software scans files regularly for unusual changes in file size, programs that match the software's database of known viruses, suspicious email attachments, and other warning signs. It's important to use your anti-virus program all the time for it to be effective -you can have it start when you boot up and continue running in the background while you surf the Web and work on your computer. You must also keep your anti-virus protection up to date because new virus definitions come out almost daily. Symantec's Norton AntiVirus offers you superior protection, and its LiveUpdate feature makes sure your virus definitions stay up to date by automatically checking each time you're online.

Good anti-virus software is your best defense against worms, but taking these preventative steps can enhance that protection:

- **Screen your email.** Don't open email from an unknown source.
- **Only open expected attachments.** Ideally, you should only open attachments you were expecting from a trusted source, and scan it with an anti-virus program before opening it. If you receive an unsolicited attachment, ask yourself if the file seems unusual, or if it is from someone you don't know. Remember that the "ILOVEYOU" worm used people's address books to send the worm to their friends. If you receive a strange attachment from someone you do trust, call them to confirm the file was sent intentionally.
- **Don't automatically open attachments.** Be sure your email program doesn't automatically download attachments. This will ensure that you can examine and scan attachments before they run. Refer to your email program's safety options or preferences menu for instructions.
- **Don't download programs from Web sites.** Unless you know and trust the source, do not download programs or software from the Internet. If you must do so, download the file into a separate folder on your hard drive and scan it with anti-virus software before running it.
- **Update virus definitions frequently.** Keep your virus definitions current by updating your anti-virus software at least every two weeks.

## Get Out.

In the event that you do get a worm, the [Symantec AntiVirus Research Center \(SARC\)](#) can help you get rid of it. Symantec regularly posts programs you can download to remove a worm from your computer. The programs scan your hard drive for unusual changes and reverse them, cleaning up the worm in the process. Prevention is better than treatment. Using proper security measures, you can avoid being infected altogether, saving your computer from the wrath of the insidious worm.

[Tell a Friend About this Article](#)

[Return to Symantec's Home Computing](#)

[article library](#)

[macintosh](#)

[small business](#)

[virus dictionary](#)