

## How do viruses and worms spread on email?

Here are two examples to help you understand how email viruses work, based on Symantec's information.

**TipsMake.com** - There are many things you can find in your inbox. The negative entries of the email attachments include:

- Trojan horses
- Worms
- Viruses



In many cases, email viruses are not true viruses because they cannot function without human impact. However, they still affect your email system.

A Trojan horse, hearing its name does not seem to be harmful, but it can actually destroy software in plain wrappers. Plain wrapper is an email attachment from someone you don't know. This file is very misleading. When you run this attachment, it can do a lot of things, from deleting all files to changing your desktop. After that, it will send it to the people on your list to be able to spread it.

Here are two examples to help you understand how email viruses work, based on Symantec's information.

**Worm.ExploreZip** is a computer worm containing malicious code. This computer worm uses Microsoft Outlook, Outlook Express, and Exchange to manually send them to unread emails in your inbox. It also searches

for drivers and other computers on the network to copy them to the Windows directory of other computers and edit WIN.INI.

This worm will destroy all file formats such as .h, .c, .cpp, asm, .doc, .ppt, or .xls on your hard drive, as well as other hard drives on the same network if these The machine accidentally let them run. This will continue until this computer worm is removed.

You can get this computer deep through an attachment called **zipped\_files.exe** , **disguising** them as a normal zip file. However, when running, it will copy itself to Windows operating system with the file name as **Explore.exe** or **setup.exe** . This computer worm modifies WIN.INI or the registry, from which the Explore.exe file will be run every time you start Windows.

Symantec also provides additional information about the technology and explains what you need to know if you suspect there is Worm.ExploreZip in your operating system.

In some special cases, email attachments may work on your own without your impact. Based on information from Symantec.

**VBS.BubbleBoy** is a computer worm that works on Windows 98 and Windows 2000 operating systems. It can also work on Windows 95 operating systems if Windows Scripting Host is installed. This computer worm only works with the English and Spanish versions of the operating system.

Microsoft Outlook (or Express) with Internet Explorer 5 needs to be installed so that they can copy themselves.

This computer worm took advantage of the security vulnerability in Microsoft Outlook / IE5 to fill the UPDATE.HTA file every time the email was displayed without having to split the file and run the attachment. UPDATE.HTA is located at the Program-StartUp in the Start menu. From there, the infection will not work until you start the computer. UPDATE.HTA is a script file that uses MS Outlook to send messages containing deep email to everyone on the MS Outlook list. By fixing security holes in Microsoft Outlook / IE5, this computer worm will no longer work.

Microsoft also added information about this computer pest.

Keep your antivirus software up to date with the latest viruses from antivirus software vendors that cannot prevent new viruses when not being updated. If you use Norton AntiVirus, turn on Auto-Protect. Norton AntiVirus antivirus software will automatically alert you when your virus update is older than 30 days. Norton's LiveUpdate will also automatically update.

If you think the virus has spread to your computer via email sent from friends on your list, notify this person and tell them not to open mail or attachments. That will be the only effective way to prevent their spread.

You finished reading the article "**How do viruses and worms spread on email?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.