Nowadays more and more people are using a computer. A lot of them use it at their work place, but an increasing number of computer users have also discovered the need to have a computer at home. At the same time the number of Internet surfers increased. This is a good thing because people are realizing the advantages offered by the world of technology. As soon as they discover this, they start using computers and the Internet more and more, but at the same time not considering the threats that are coming in from all sides. They should know that if you don't protect yourself, nobody will. These threats are now coming from everywhere and they are growing in number and complexity. First threats of this kind were the viruses. At first, viruses were not that harmful. They were designed to perform a simple task, like flashing a single message onto the user's computer screen. Also the spread rate was slow, because not many people were connected to the Internet. But now the majority of viruses are programs intentionally written to obstruct with, or harm other programs or computer systems. And they are spreading very fast.

Many companies and people have had a lot of troubles because of these viruses. And so the need for antivirus software was born. At first one very simple antivirus appeared and this was enough. Now, as the threat is growing antivirus software are becoming a lot more complex. Some of them have also included a firewall so to better protect the users. In order to increase the competition, other antivirus software producers have also come up with a wonderful idea: to offer free scan online. This was a big help for people that are frequently using a computer mostly for their personal use, meaning it is not attached to a network and uses the Internet only from time to time. Now, they don't have to spend a lot of money to buy antivirus software that will be used very rarely.

Most of these antivirus programs have to be bought in order for you to use them at their full capacity. Also you have the option to test a so called "free trial version". These trial versions include all or most of the software's features, and are available to be checked out by the user for a short period of time, usually 30 days. After these 30 days, the program can no longer be used. Other antivirus software producers use another method; they offer a free trial version that you can keep forever. But it is not fully operational, meaning some of the options of the program cannot be used as they are not activated. After you have tried a program and you consider it is fit for your need, then you'll have to buy it to protect your computer at its full capacity.

Lately, viruses are mostly spread through e-mails because this is the most common use of the Internet. Also, e-mail viruses are easier to develop. E-mail viruses make use of the ability of having macros or scripts implanted in word documents, spreadsheets, HTML pages, and are programmed to run when the document is opened. But how does an e-mail virus works? When

an e-mail with an infected document or program is received, the user unknowingly opens a document/program, which in turn executes a code to open the e-mail directory and to send a copy of itself as an e-mail attachment to a certain number of addresses. Some of the recipients of the e-mail open its attachment and the process repeats itself.

This is where the antivirus program comes in. This program is set to check all incoming and outgoing messages and their attachments. If an e-mail is detected to have a document or program infected with a virus the program offers several possibilities to deal with the threat: delete the e-mail, put it in quarantine or try to disinfect it. Most of the times, these choices are left to the user's decision. It is up to the user to set the program in such manner to best fit his needs. But not all viruses are coming by e-mail. A few of them use security errors in the operating system or your Internet browser to be launched automatically. But if you keep your antivirus and all the other programs updated, there will be a small chance of being infected via this route.

Nowadays, most viruses are spread in the form of e-mail attachments. This is because some of the worst recent viruses relay on recipients that throw away common sense and launch a deadly e-mail attachment. Commonly the attachments are with extensions that include .bat, .com, .exe, .pif, .scr, and .vbs. Sometimes to avoid the filters of antivirus software, virus creators enclose their malicious code in a .zip or .rar archive file. The file might even have a password to full antivirus programs that scan inside archives. And obviously, the password is included in the message as an image for the convenience of the naive user. As a simple but reliable rule, you should never open an attachment that you didn't expect to receive, even if it came from someone you know. Also, make sure your e-mail software is configured so it will not automatically open attachments.

Another common way of spreading viruses is file sharing. Many viruses spread themselves throughout open network shares. You can protect your computer not sharing files or directories over the network. But if you don't have a choice and you have to share your files, you are still able to reduce the risk of being infected by installing antivirus software and keeping it updated. Other ways to become infected with viruses are downloading files or software from the Internet, instant messaging or even web pages.

If the file you are downloading or the computer you are downloading it from is infected with a virus, there is a big chance that your computer will also become infected with the virus. As for the instant messaging, the major risk comes from accepting files from other users on the network. This risk can be minimized by configuring your antivirus software to scan all incoming files and also configure your other programs not to automatically accept files, and not to

automatically execute the files you accept. Certain viruses are known to infect web servers. If you visit a website from an infected server, your computer could be infected with the same virus, but this is a very rare method of infection.

There are many different threats that are targeting the computers. Although they are very different, all of them are popularly called viruses. A virus by definition is a self-replicating file, not considering whether it is malicious or not. Another type of the so called viruses are worms; they circulate mainly through e-mail but also spread through a network. A worm is aware he is located in a network and uses it for replicating itself. Trojan horses (or trojans) are mostly used to insert some remote tools into a system in order to give the attacker free access to that system, without the user's knowledge. Most Trojan horses cannot replicate automatically.

With the increased number of Internet users, the existing threats are also raising as now there are many more computers to attack and more people that don't know to stay away from these threats. But the antivirus software producers are making it easier for us. There is a lot of antivirus software which cover a lot of threats. All we have to do is install one.