Computer Security 101

PC Lock Down

A common sense course for all PC owners

Identify – Eliminate - Defend

Against Viruses, Trojans, Worms & Backdoors,
Pop-Ups, Spam, Malware, Spyware,
Phishing, Spoofing, Identity Theft.

Only *You* Can Prevent Misuse of *Your* PC

Viruses are not the only threat to your computer.

Until a few years ago, viruses were the main threat to computers. Viruses are programs that replicate by infecting other files or applications and carry out damaging actions.

Then worms, appeared, programs that do not need to infect other files in order to replicate, and which spread by creating copies of themselves in order to collapse the networks they penetrate. To these, Trojans and backdoor Trojans can be added. These apparently harmless programs try to get into computers and steal passwords and capture keystrokes, allowing remote access to the information stored, etc.

However, recently, due to the widespread use of computers and the Internet, other threats have appeared that can be extremely destructive, redefining the concept of threat, also known as **malware**.

Malware

The word malware comes from malicious software, i.e., malignant programs. Malware includes any program, document or message that can cause damage to computers, resulting in loss of data and loss of productivity.

Therefore, as well as viruses, worms, Trojans and backdoor Trojans the following can also be defined as malware:

Dialer: A program that tries to establish a phone connection with a special rate number.

Joke: A harmless program that pretends to carry out damaging actions on the computer.

Security risk: A legal tool that can be used for malicious purposes.

Hacking tool: A tool that allows hackers to carry out damaging actions on affected computers.

Vulnerability: A programming error in an application that can be used to breach security and take control of computers.

Spy program: A program that collects data on the users Internet habits and sends it to advertising companies.

Hoax: An e-mail message warning of a virus that does not exist.

Spam: The mass mailing of unsolicited mail, which is generally commercial mail.

Viruses, Trojans, Worms and Backdoors

Along with viruses, there are three other types of damaging programs, which are the bane of all computer users worldwide. Although they have similar effects to viruses, these programs have clearly distinguishing characteristics.

Virus

A virus is a program that can enter a computer in many different ways and can cause effects ranging from the simply annoying to the highly destructive. Viruses can enter computers through e-mail, the Internet, different types of disks etc.

- They have the ability to reproduce, infecting other files and programs.
- When they are run, they are able to carry out a range of annoying or damaging actions in your computer.

Computer viruses are called viruses due to their similarities with biological viruses.

In the same way that biological viruses enter the body and infect cells, computer viruses get into computers and infect files. Both types of virus can reproduce themselves and spread, passing the infection from one infected system to another. Also, just as a biological virus is a micro-organism, computer viruses are micro-programs.

Worms

A worm is a program very similar to a virus. It can self-replicate, and can lead to negative effects on your system. Worms do not need to infect other files in order to reproduce.

Worms, unlike viruses, simply replicate themselves, damaging files, but can reproduce rapidly, saturating a network and causing it to collapse. Normally sent via e-mail, some of the most notorious include: I Love You, Navidad, Pretty Park, Happy99 and ExploreZip.

Trojans

Trojans or Trojan horses, unlike viruses do not reproduce by infecting other files nor do they self-replicate like worms.

Trojans work in a similar way to their mythological namesake, the famous wooden horse in which Greek soldiers hid so that they could enter the city of Troy undetected. They appear to be harmless programs that enter a computer through any channel. When that program is executed (they have names or characteristics which trick the user into doing so), they install other programs on the computer that can be harmful.

A Trojan may not activate its effects at first, but when it does, it can wreak havoc on your system. Trojans have the capacity to delete files, destroy information on your hard drive and open up a backdoor to your security system. This gives them complete access to your system allowing an outside user to copy and resend confidential information.

Examples of Trojans: Backdoor, Donald Dick, Crack2000, Extacis, KillCMOS, Netbus, Downloader.GK

Backdoors

A backdoor is a program that can get into computers by passing itself off as a harmless program. Once it has been run, it opens a backdoor through which it can control the affected computer. This allows a malicious user to carry out actions on the affected computer that can compromise user confidentiality or impede the operations carried out.

The actions that backdoor allow malicious users to carry out can be extremely damaging. They could allow them to delete files or destroy all the information on the hard disk, capture confidential data and send it out to an external address or open communications ports, allowing remote control of the computer.

Some examples of backdoor are: Orifice2K.sfx, Bionet.318, Antilam and Subseven.213.

What is a vulnerability?

Some programs contain security holes that make computers vulnerable to infection.

A vulnerability represents a weak point though which the security of a computer can be breached. A vulnerability is a programming error in an application that can be exploited to gain access to the computer with that program installed.

Generally, this programming error refers to operations that cause the application to malfunction. This bug can be reproduced artificially by a malicious user in order to gain access to computers without the user's permission. Sometimes, this can be done by simply opening a specially crafted document.

This would allow a malicious user to carry out a wide range of actions on the vulnerable computer, for example, running or deleting files, inserting viruses, accessing information.

Although the most commonly known vulnerabilities are those affecting operating systems, Internet browsers and mail programs, any program can have vulnerabilities: word processing applications, databases, sound file players, etc.

A vulnerability does not pose an immediate threat to computers. However, it is a potential entry point for other threats, such as viruses, worms and Trojans, which can have destructive effects.

For this reason, it is highly advisable to keep informed about the vulnerabilities discovered in the programs you have installed and apply the latest security patches released by manufacturers of these applications, which are usually available on their websites.

Some examples of worms that exploit vulnerabilities in order to carry out their actions are: Blaster, Bugbear.B, Klez.I and Nachi.A.

Hoaxes and jokes

False virus warnings and jokes sent to confuse users.

- Hoaxes
- Jokes

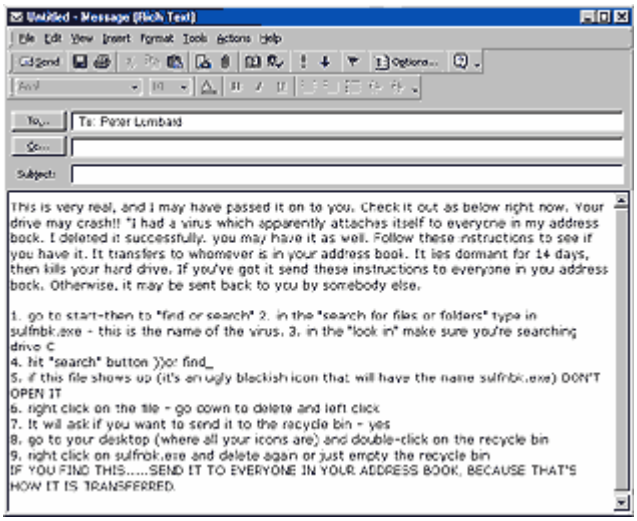
These messages are often confused with viruses but they are something else entirely. It is important to know the difference so as not to fall into the dangerous trap set by these pranks.

Hoaxes

Hoaxes are not viruses, they are false messages sent by e-mail, warning users of a non-existent virus. The intention is to spread rumors causing panic and alarm among users who receive this kind of information.

Occasionally, hoax warnings include technical terms to mislead users. On some other occasions, the names of some press agencies are mentioned in the heading of the warnings. In this way, the hoax author attempts to trick users into believing that they have received a warning about a real virus.

Users are therefore advised not to pay attention to these misleading reports.



Hoax message SULFNBK.EXE.

Jokes

Jokes are not viruses but programs designed to trick users into believing that a virus has infected them. These programs usually simulate the destructive effects of viruses - for instance the deletion of the files in the hard drive. Although more annoying than harmful,

users are strongly recommended not to open any files attached to suspicious e-mail messages.

What do viruses infect?

Where do viruses actually go when they attack a system?

The main targets of a virus are program files (files with an EXE or COM extension), which can be run to perform specific operations. Increasingly other types of files and documents can also be infected such as web pages (HTML), Word documents (DOC), Excel spreadsheets (XSL), etc.

If a file becomes infected, it may behave in a completely different way than before. The consequences of an infection to the system can therefore vary enormously.

As files are often stored on disks or drives (hard drive, CD-ROM, DVD, diskettes, etc.) the damage caused by the virus may also affect these elements.

Most common entry points

Internet

Networks

Removable disks

Viruses enter computers through the same communication channels used to exchange information. Internet, networked computers, and removable disks.

Internet

The Internet has become a widely-used form of exchanging information. Unfortunately, it also serves as the fastest way to spread a virus. What this means is that although the Internet presents us with numerous ways to send information, each one of these has its risks. Some forms of information exchange include e-mail, browsing web pages, transfer of files through FTP, downloading programs, chat and newsgroups.

Networks

A network is a group of interconnected computers (via cable, modem, routers, etc.) that makes it easier for groups of people to work together. Each computer that forms part of the network can connect to all other networked machines, making it possible to share information and resources (printers, scanners, etc) without the need for a removable disk.

This makes working in groups easier but also offers a convenient channel for viruses to spread: virus infection is more likely in networked computers than in standalone machines. If one computer in the network gets infected, others connecting to it will also become infected, causing a chain reaction that can paralyse the entire network.

Removable disks

Removable disks are storage devices on which data is stored in the form of files or documents. These disks enable documents to be created on one computer and then used on another. These types of storage devices are floppy disks, CD-ROMs, DVDs and removable disks.

If any of the programs, files or e-mails saved on a disk are infected, using this disk in another computer will spread the virus.

Before the Internet became the most popular from of communication, exchange of floppy disks was the most common form of spreading a virus. Today it is less usual for viruses to spread through disk drives but it still represents a significant risk.

Where do they hide?

Viruses can hide in a host of places without being discovered.

Most common hideouts for viruses include:

- Web pages are developed in a specific language and may contain elements known as Java applets or ActiveX controls, in which viruses can hide and infect users that visit pages containing these components.
- E-mail messages are a favourite hiding place for viruses and they represent an extremely fast way of spreading. These messages can contain attachments that harbour viruses. Simply opening these messages can lead to infection.
- The Main memory (RAM). Viruses can hide in the main memory where they wait for a program to be run (a file with an EXE or COM extension) in order to infect it. This type of virus is known as a resident virus.
- Boot sector: The boot sector of a floppy or hard disk contains information on the characteristics and contents of the disk. Some viruses, known as Boot viruses, enter this area as a means of infecting the computer.

- Files with macros make a convenient hiding place for viruses. A macro is a small program that forms part of Word documents (with DOC extensions), Excel spreadsheets (with XSL extensions) and PowerPoint presentations (PPT or PPS extensions). As these macros are programs viruses can infect them.

Symptoms and effects

How do you know if a virus has hit you?

It can be difficult to tell if a virus has infected your computer, which is why you need a reliable antivirus installed.

The following are symptoms to look for which indicate the possible presence of a virus (although the problem may not be due to a virus).

- Unusually slow processing in the normal functions of the computer with no apparent cause. This can be caused by having too many programs open, problems with the network, but also by a virus infection.
- Not being able to open certain files or work with certain programs where a virus may have erased all or part of the data necessary to open the program.
- Unexplained missing files and folders is another common side effect of viruses.
- Not being able to open certain files. Viruses can also alter files, making it impossible to view them, causing an error message to appear.
- Bogus warnings or text displayed on screen. These will often contain unusual messages (jokes, insults, obscenities etc).
- Sudden reduction in disk space or memory capacity may be an indication of viruses, as they can sometimes consume all available free space. In these cases, warnings will appear indicating that there is no disk space.
- Some viruses can affect the normal functioning of disk drives, causing problems when saving files or performing other operations involving the hard disk.

- An unexpected change to file properties is another symptom of infection. Some viruses may alter the files they infect, increasing the size, modifying the date of creation or other attributes, etc.
- If the operating system displays error messages, this can be due to genuine errors but it can also be an indication of a virus. If such messages appear when carrying out simple operations under normal conditions, it is worth being suspicious.
- If a file appears duplicated, and one of them has the extension EXE, while the other has the extension COM, it is very likely that the second is infected.
- When the name of a file unexpectedly changes, there is good reason to believe a virus may be at work.
- Problems when starting up the computer could be due to a number of causes, but infection by a boot virus is frequently the root of the problem.
- The computer may block (or freeze) when there is an excessive load, but this can also be a symptom of the presence of a virus. There is cause for suspicion if this happens when carrying out simple operations that do not put a heavy load on the computer.
- The computer shuts down suddenly for no apparent reason and then starts up again. Some viruses cause the system to do this in order to activate and ensure that they are able to function as programmed.
- If a program closes suddenly, for no apparent reason, this may also be symptomatic of the presence of a virus.
- Other strange effects, which could be indications of infection by Trojans, include the CD-ROM tray opening and closing, keyboard and mouse actions taking place automatically, windows appearing and disappearing at random, etc

What Can I Do?

Common sense *will always be one of your most valuable weapons in the protecting the security of your computer system: always treat all data entering your computer with caution.*

A Few Do's and Don'ts?

- If you receive unsolicited files from an unknown source, through chats or newsgroups for example, don't open them. Reject these messages, no matter how enticing they might seem, they could contain a virus.
- Do scan all new e-mail messages received before opening them, even if you know the sender.
- Don't download from unsafe or dubious Internet websites and when you do download from the Internet, make sure the site is backed by a respected organization, publisher or antivirus developer.
- Do be on the lookout for suspicious activity in your computer (increase in file size, unusual Windows messages, mail from unknown senders, or in foreign languages etc.).
- Don't be caught unaware, keep up-to-date on the latest developments by subscribing to security news bulletins.
- Installing pirated software or programs of dubious origin is a likely cause of infection: in brief, always use licensed software. It's the only way to guarantee the reliability of the application and be sure that you can rely on tech support services in the event of any problems

- Many widely-used applications (Internet Explorer, Outlook...etc.) have specific security options. Use them!

Use an antivirus correctly and make sure to update it regularly

What to look for in choosing an antivirus program

- All information entry points must of course be protected, with special emphasis on e-mail and Internet connections.
- regular updates (ideally once a day),
- technical support,
- rapid response to new virus incidents and an early warning system.

Using an antivirus program

First, read the documentation carefully and make sure you understand the basic functions of the antivirus. This will help you follow the proper procedure should any virus incident occur.

Once the program is installed, it's highly advisable to scan all data on your computer frequently to make sure your system is virus-free. This scan should include all disk drives, floppy disks, CDs and shared drives.

An antivirus is useless unless it is active: check that your permanent protection is always enabled. This will monitor all operations performed on the computer and make sure that any viruses trying to 'sneak' in will be eliminated.

Windows XP users take note:

Windows XP offers the possibility of restoring the system automatically, recovering eliminated files or the system settings accidentally modified.

For that reason, Windows XP keeps all the eliminated or modified elements inside its hidden directory, called _restore, which is protected so that its contents can't be manipulated by anybody or anything.

This feature, although sometimes advantageous, may cause the following conflict: when the antivirus performs a scan, it will detect the infected and the erased files which Windows XP stores in the _restore folder.

That is why when a new scan is performed, the antivirus will detect again the infected file in the _restore folder but it won't be able to eliminate it -- because the file is protected by the operating system and is out of it's reach.

Eliminating viruses and other threats from the Windows XP _restore folder

So what you find that even after viruses and other threats have been eliminated the antivirus is detecting it again and again in the *_restore* folde?. This is what you do:

1. Log on as the Administrator or with the details of the user that has administrator rights.
2. Click with the right button of the mouse on My Computer.
3. Select Properties.
4. Click System Restore.
5. Check the Turn off System Restore or Turn off System Restore on all drives checkbox.
6. Click Apply and then OK.
7. Restart the computer and reactivate System Restore

How to reactivate System Restore option

1. Click with the right button of the mouse on My Computer.
2. Select Properties.
3. Click System Restore.
4. Uncheck the Turn off System Restore or Turn off System Restore on all drives checkbox.
5. Click Apply and then OK.
6. After completing these steps, carry out a full scan of your computer using the antivirus program in order to ensure that it correctly disinfected.

What About a firewall?

A firewall is a software application that complements antivirus programs in order to provide maximum security when connected to the Internet. They can be used, for example, to prevent unauthorized users (hackers, etc.) from gaining access to your PC, or blocking downloads from unsafe websites. Some anti-virus programs include an effective firewall

Why use a firewall?

Hackers often 'roam' the Internet, looking for machines with open communication ports from which they can infiltrate systems. Official data suggests that some 85 percent of large enterprises have been victims of network intrusion.

Firewalls block unauthorized access to computers, as well as preventing confidential information from leaving the network.

What does a hacker aim to do?

In general, computer intruders rarely have the best intensions, they will often try to:

- Access confidential information, such as passwords to Internet services like online banking or even antivirus services.
- Gain complete control of the PC, and manipulate it like a 'zombie'. This means that a hacker could use your computer, along with numerous other 'zombies', to redirect a mass attack against a website, overloading it and causing it to crash. This is also known as a DOS (Denial of Service) attack.
- After taking over part of your hard disk, they can set up your computer as a platform for downloading and distributing pirated software.

Is there any additional risk when using ADSL or Satellite modems?

ADSL and Satellite connections create a permanent connection to the Internet; this kind of connection leaves an open door to the Internet whenever you turn on your computer (even though you are not browsing at the time).

This means that users are exposed to increased risk of hacker attacks, especially if a firewall is not installed. A similar problem applies to online connections when other computers share the same cable connection.

Back Up

If you make regular back-up copies of your information, you'll be able to restore your system in the event of virus or hacker attacks and improve your chances of saving valuable data.

What data should be backed up?

Organize and prioritise your important information. This will make it much easier and quicker to restore it .

Keep software up-to-date with manufacturer's patches

The more widely-used a software application is, the larger a target it represents for hackers.

When a vulnerability is detected in a program, software developers release updates for their clients on the Internet . You should apply these patches immediately to close off any potential security holes.

NOTES