

### Highlights:

#### Videos on Security - Protect yourself against viruses and worms

In previous editions we highlighted a new section on the Microsoft site devoted to the subject of Security.



This provides a number of short videos, designed to help users to get to know the major Security problems and how to avoid them. This month the focus is on defence against viruses and worms

In this video we shall show you how to reduce the risk through the use of antivirus software, firewalls and much more. Additionally, you can quickly access alerts and the personalised help of other... >>

### News:

#### How to recognise a Hoax

Hoaxes are e-mails that contain false, alarming messages designed to encourage readers to continue to divulge them....

>>



### Basic Security Principles:

#### Notions about Windows Firewall (part 1 of 3)

##### Introduction

The Windows Firewall, formerly known as the ICF or Internet Connection Firewall, is a protective

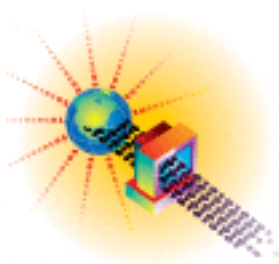


barrier that monitors and restricts information moving between the user's computer and the net or Internet... >>

### Configuring and updating software:

#### Security Updates – Security Bulletins

As you probably know, software updates are an important part of the security of your Personal Computer. Every month, on the same date, Microsoft publishes updates of its software... >>





## Highlights:

### Videos on Security - Protect yourself against viruses and worms

In previous editions we highlighted a new section on the Microsoft site devoted to the subject of Security.

This provides a number of short videos, designed to help users to get to know the major Security problems and how to avoid them.

This month the focus is on defence against viruses and worms. In this video we shall show you how to reduce the risk through the use of antivirus software, firewalls and much more. Additionally, you can quickly access alerts and the personalised help of other users.

**Type the following in the address bar of your browser and see the video to get to know more about this subject:**

[http://www.microsoft.com/athome/security/viruses/video\\_virusworm.msp](http://www.microsoft.com/athome/security/viruses/video_virusworm.msp)



## News:

### How to recognise a Hoax

Hoaxes are e-mails that contain false, alarming messages designed to encourage readers to continue to divulge them.

One of the commonest kinds of hoaxes consists of warnings about dangerous viruses, but there are also hoaxes that are intended to libel a certain company, product or brand, and those that promise easy money to be won.

Usually, the purpose of those that create hoaxes is to see how long the hoax stays around and the extent to which it is propagated. The latter is easy to see if you consider a person reading a hoax who forwards it to 10 people on his list (Group 1) and, in turn, each of the latter sends it to another 10 (Group 2), and so on. See where we soon arrive:

Group	1 <sup>o</sup>	2 <sup>o</sup>	3 <sup>o</sup>	4 <sup>o</sup>	5 <sup>o</sup>	6 <sup>o</sup>
N <sup>o</sup> of e-mails	10	100	1.000	10.000	100.000	<b>1.000.000</b>

### How to identify a hoax:

Although it is not always easy to recognise a hoax, there are characteristics that can help you in this:

- it uses technical language
- it makes reference to a well-know company or organisation
- it warns of drastic consequences of not carrying out certain actions
- it declares it is not a hoax
- it asks you to forward the e-mail to all your friends
- it contains instructions to protect your computer from a certain virus that can be detected by your anti-virus software
- it contains spelling and grammar mistakes.

There are sites that provide lists and contents of hoaxes moving around the Internet. These sites include:

Symantec

McAfee

Vmyths



## Basic Security Principles:

### Notions about Windows Firewall (part 1 of 3)

#### Introduction

The Windows Firewall, formerly known as the ICF or Internet Connection Firewall, is a protective barrier that monitors and restricts information moving between the user's computer and the net or Internet. It provides a line of defence against anyone trying to access your computer from beyond the Windows Firewall, without permission. A computer with a virus is like a person with flu - if you analyse the symptoms you can "diagnose the illness". Here are some of the signals that you should look out for to see if your computer is infected by virus.

If you have Windows XP Service Pack 2 (SP2) installed, the Windows Firewall will be activated by default. However, some computer manufacturers and network administrators may deactivate it.

#### To open the Windows Firewall

1. **Click on "Start" then on "Control Panel "**
2. **In the Control Panel, click on "Security Center"**
3. **Click on Windows Firewall**



## Security Centre

**Note:** You do not have to use the Windows Firewall; you can install and run any firewall you choose. Assess the functions of other firewalls and then decide which suits you best. If you decide to install a different firewall deactivate the Windows Firewall.

### How the Windows Firewall works

When someone on the Internet tries to access the computer of another user it gives rise to what we call an “unsolicited request”. When the computer receives an unsolicited request, Windows Firewall blocks the connection. If you execute a programme such as instant messaging or play an online game with several players that needs to receive information from the Internet or other network, the firewall asks whether you want to block it or unblock (authorise) it. A window similar to the following one should appear:



### Firewall security alert

Should you not know the name of the programme or its manufacturer you should select the “Keep Blocking” option. Some programmes could be viruses or even spyware that could affect your system or even send personal, confidential information over the Internet.

If you opt to unblock the link, Windows Firewall will create an exception so ensure the firewall does not bother you when that programme needs to receive information later on. In coming Newsletters we shall address other matters, particularly management of these exceptions.

**Suggestion:** Despite the fact that you can deactivate Windows Firewall for specific connections to the Internet, this will increase the risk as far as the computer’s security is concerned.

### What the Windows Firewall does and doesn’t do

DOES	DOESN'T
<p><b>Helps block viruses and worms</b> so that they don't reach your computer</p>	<p><b>It neither detects nor deactivates viruses and worms</b>, should they already have entered your computer. You should therefore install anti-virus software and keep it up to date to help to prevent viruses, worms and other security threats from damaging your computer or from using it to propagate viruses to other computers.</p>

<p><b>Requests your authorisation to</b> block or unblock certain connection requests</p>	<p><b>It will not stop you opening e-mail messages containing dangerous attachments.</b> Don't open e-mail attachments sent by people you don't know. Be prudent, even if you know and trust the source of the electronic message. If someone you know sends you an e-mail with an attachment take a good look at the subject line before you open the attachment. If the subject line is unintelligible or does not make sense, contact the sender before opening the attachment.</p>
<p><b>Creates a security record,</b> should you so require, that records successful and unsuccessful attempts to access your computer. This could be useful as a problem-solving</p>	<p><b>It does not block unsolicited electronic mail (Spam),</b> nor does it prevent it from appearing in your Inbox. However, some electronic mail programmes can help you to do this. To get to know more, check the documentation on the e-mail programme.</p>

**Note:** This information has been collected and adapted from the Microsoft site.

top

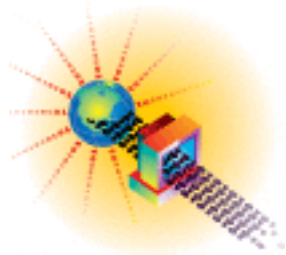


## Configuring and updating software:

### Security Updates – Security Bulletins


As you probably know, software updates are an important part of the security of your Personal Computer. Every month, on the same date, Microsoft publishes updates of its software.

The October security updates affect Microsoft Windows and Microsoft Internet Explorer, a Windows component. Users should follow the steps shown on this page to update their Windows software.





## Actions to Take Now

<b>1.</b>	 <b>Install the Updates</b> Visit the Microsoft Update Web site ( <a href="http://update.microsoft.com">http://update.microsoft.com</a> ) to check whether your computer needs updates.
<b>2.</b>	<b>Use the Windows Automatic Updates function</b> Update high priority security updates delivered automatically to your computer. See how to use the Automatic Updates: Windows XP, Windows 2000, Windows Me.
<b>3.</b>	<b>Protect your PC</b> Several basic steps can help to protect your computer and its contents. Consult the English area on the Millennium bcp Portal and see what you can do to improve the security of your PC at – "3 steps to help ensure your PC is protected".

Do not limit your updates to Microsoft's software. Don't forget to use the same procedure to update all the software you have installed on your personal computer.



"Best Consumer Internet Bank" in Portugal • "Best Online Consumer Credit" in Europe  
"Best Corporate/Institutional Internet Bank" in Portugal • "Best Information Security Initiatives" - Individuals, in Europe  
"Best Bill Payment and Presentment" in Europe • "Best Information Security Initiatives" - Corporate, in Europe