

The end of the year is here. We have been with you, these past 12 months, to call your attention to the real dangers that can put your computer at risk and have demonstrated for the purpose how the main weapons selected by hackers can be used. At the same time we have taught you the main weapons of defence available to you in confronting these threats.

We hope we have contributed to increasing your security mechanisms in several aspects, preventing you from being yet another victim in the cyberspace universe.

In closing we would like to wish you an excellent 2006!

Highlights:

Videos on Security – Teach your children about online security

In the wake of our previous editions we would point out a new section on the Microsoft site dedicated to Security where a number of short videos are



provided in Portuguese, designed to help users in getting to know the main Security problems and how to avoid them.

This month the focus is on Security for children and adolescents on the Internet. Children and adolescents are more likely to use the computer and the Internet during the Christmas season and holidays. In this video we shall show you how to help children and adolescents to be better protected when using the Internet.

See this video to get to know more about this issue: http://www.microsoft.com/athome/security/children/video_childsafety.mspx

News:

Electronic Cards: Beware!

The Internet has made electronic cards and simple and inexpensive alternative to traditional paper cards...>>



Basic Security Principles:

Notions about the Windows Firewall (part 3 of 3)

Using the Exceptions Tab

If you are running Windows XP Service Pack 2 (SP2), the Windows Firewall will be activated by default >>



Configuring and updating software:



Ways to protect your electronic mail (Part I)

Following our previous Newsletter in which we share a video containing a number of good practices regarding unsolicited mail (spam), this month we would like to provide practical advice in respect of possible configurations of Outlook Express... >>

News:

Electronic Cards: Beware!



The Internet has made electronic cards a simple and inexpensive alternative to traditional paper cards. There is an increasing number of electronic card companies and services, many of which are secure and easy to use. Unfortunately, computer pirates and swindlers have started to use these cards to mislead the unwary.

Nobody knows how many illegitimate electronic cards are sent, but after clicking on it or transferring it to your computer a card of good appearance can be:

- Spam, which can display undesirable images on your computer, open Web sites or invade you with pop-up advertising windows (even when not accessing the Internet).
- A computer virus that analyses your e-mail addresses and then sends a false electronic card to your personal and professional contacts, usually without your being aware of the fact. The false electronic card and the virus may even appear to have come from you.

But don't worry. With a little knowledge and prudence you can avoid false electronic cards and enjoy legitimate cards, provided you use the same precautions that you should use with all e-mail messages that you receive.

How can you avoid false electronic cards?

- Never transfer or click on something from an unknown source.
- Suspect any e-mail message or attached file from someone you don't know or seems suspicious.
- Install anti-virus software from reputable suppliers and keep it up to date.
- Examine a connection for a Web address before clicking on it. If the connection contains no address move the mouse pointer over the connection – but do not click – to see the address of the connection, which should appear in the lower bar of the Web browser.
- Do not accept an end-user agreement without first reading the small print; you may inadvertently be agreeing to install spyware or other undesirable elements.
- Use known electronic card sites or create your own electronic cards using the model electronic cards provided by Microsoft Office.

Bear in mind that exposure to risk does not depend only on technical security but also on your own

Basic Security Principles:

Notions about the Windows Firewall (part 3 of 3)

Using the Exceptions Tab

If you are running Windows XP Service Pack 2 (SP2), the Windows Firewall will be activated by default. This means that most programmes will not be

authorised to receive unsolicited messages from the Internet, unless you opt to list these programmes as exceptions. There are two programmes that, by default, have already been added to the list of exceptions and can receive unsolicited communications via the Internet: **Definitions and Files Transfer Assistant** and **File and Printer Sharing**.

Since firewalls restrict communication between the computer and the Internet, you may have to adjust the definitions in respect of other programmes that prefer an open connection. You can create an exception for these programmes so that they may communicate through the Windows Firewall.

Authorising exceptions: the risks

Each time you authorise an exception for a programme to communicate via the Windows Firewall the computer becomes more vulnerable. Authorisation of an exception is like opening a hole in the firewall. Too many holes and the protection provided by the firewall is reduced. Computer pirates often use software that searches the Internet for computers with unprotected connections. If you have a lot of exceptions and open ports, the computer may become more vulnerable.

To help to reduce the security risk:

- Authorise an exception only if you really need it
- Never authorise an exception for a programme you don't recognise
- **Remove an exception as soon as it's no longer required**

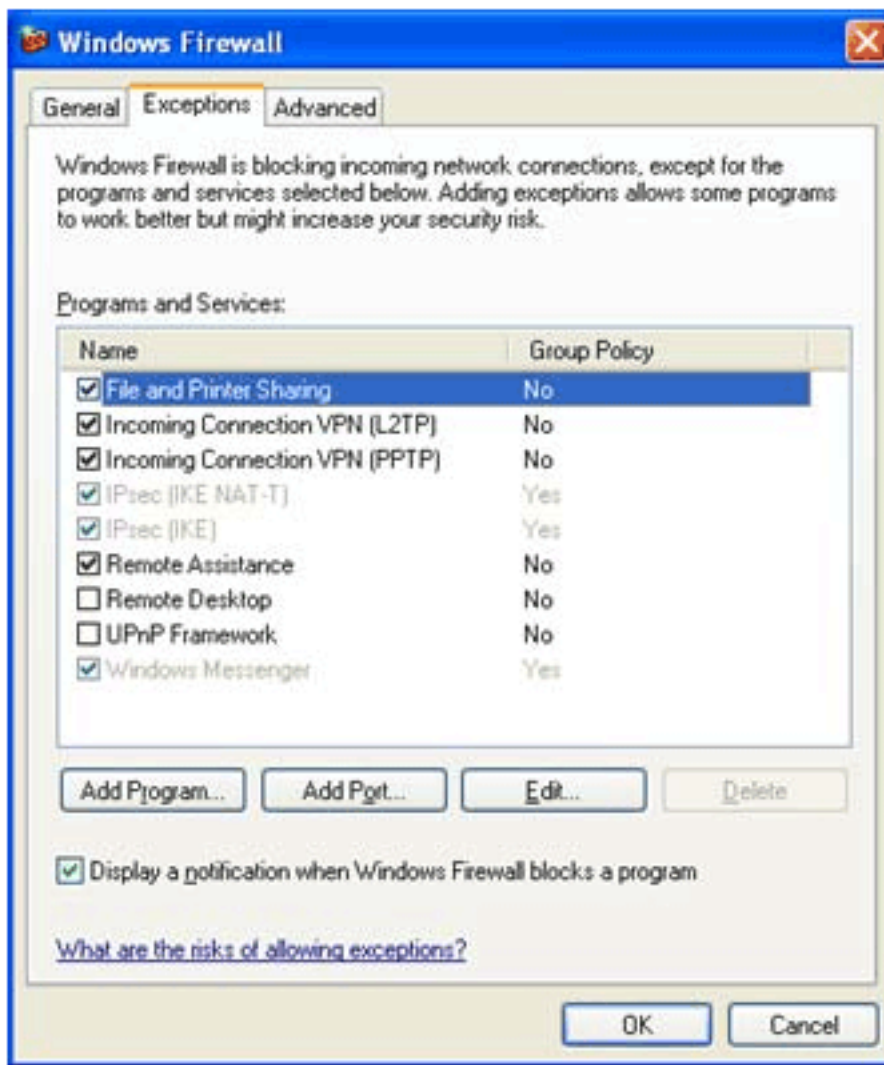
Authorising exceptions despite the risks

Despite the risk you might want someone to be able to connect you your computer: for example, when you are expecting a file to be sent through an instant messaging service or if you are playing a game with various players on the Internet.

If you are exchanging instant messages with someone wanting to send you a file (a photo for example), the Windows Firewall will ask whether you wish to unblock the connection and allow the photograph to be sent to the computer. Should you want to play an online game with several friends over the Internet, you can authorise the game as an exception so that the firewall will allow information about the game to be sent to the computer.

To add a programme to the list of exceptions:

1. Click on **Start** and then on **Control Panel**
2. In the **Control Panel**, click on **Windows Firewall**
3. In the **Exceptions Tab**, in **Programs and Services**, select the check box of the programme of service you wish to authorise and click on OK



The Windows Firewall Exceptions Tab

If the programme (or Service) you wish to authorise is not on the list:

1. Click on **Add program**
2. In the **Add a program** dialogue box, click on the programme you wish to add and then on **OK**. The programme will appear, selected in the **Exceptions Tab**, under **Programs and Services**.

Suggestion: If the programme (or Service) you wish to authorise is not on the list, in the **Add a Program** dialogue box click on **Browse**, find the programme you want to add and double click on it (the programmes are generally stored in the computer's Program Files folder). The programme will appear under **Programs**, in the **Add a Program** dialogue box.

As a last resort, open a port

If, even so, you cannot locate the programme the alternative is to open a port. A port in the firewall allows communications to pass through. To specify the port you wish to open. click on **Add Port** in the **Exceptions Tab**. (If you open a port don't forget to close it again when it's no longer required).

It's better to add an exception than to open a port because:

- It's easier
- You don't have to know the number of the port to be used
- It's more secure than opening a port since the firewall is open only while waiting for the reception of the connection.

Advanced options

Advanced users may open ports for individual connections and also to configure their scope with a view to minimising the opportunities for intruders to connect to a computer or network. To do this, open Windows Firewall, click on the Advanced Tab and use the Settings available on Network Connection Settings.

Note: this information has been received from the Microsoft site and adapted.



Configuring and updating software:

Ways to protect your electronic mail (Part I)

Following our previous Newsletter in which we share a video containing a number of good practices regarding unsolicited mail (spam), this month we would like to provide practical advice in respect of possible configurations of Outlook Express.

With Windows XP SP2, Outlook Express has been altered and improvements introduced insofar as Security is concerned. These new definitions provide greater help in avoiding viewing offensive contents of electronic messages, in reducing the amount of unsolicited advertising mail and in reducing the risk of receiving dangerous contents through an electronic mail message.

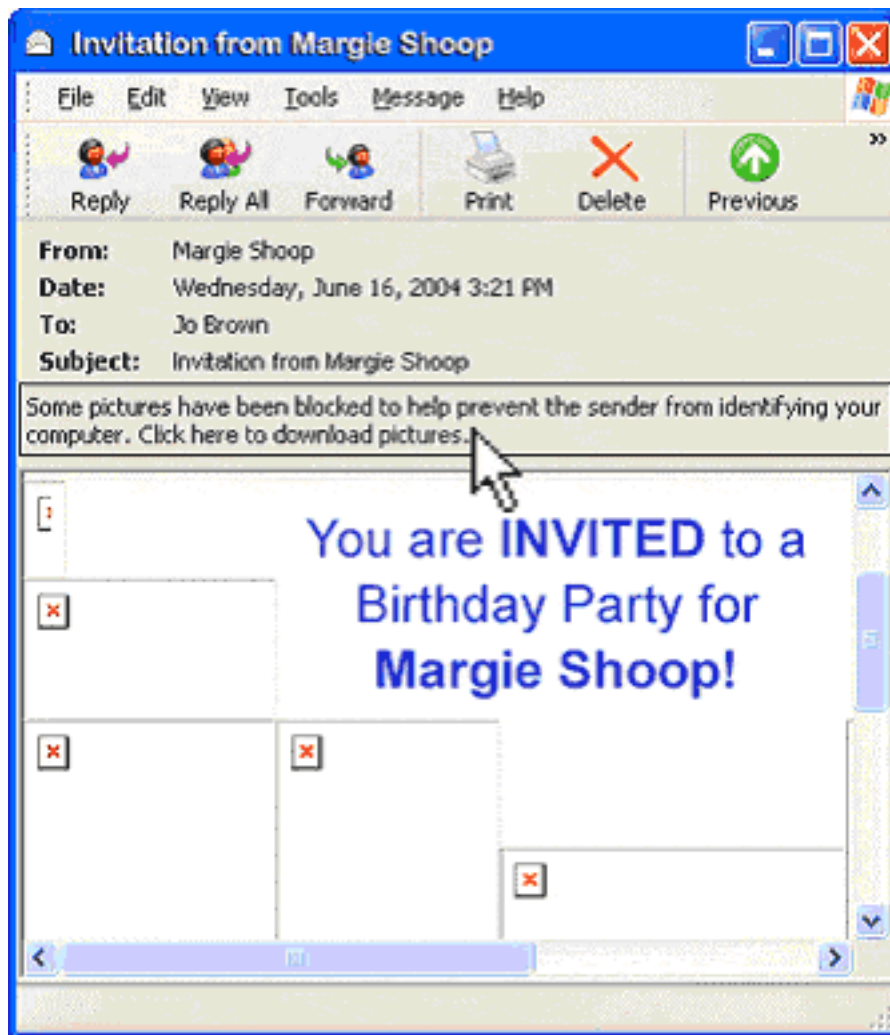
Protection against unsolicited mail (SPAM)

One of the new functions introduced into Outlook Express helps to prevent spam since it hinders the ability of wrongdoers to access your e-mail address. You may have noticed that spam often contains images. Sometimes, when an image is present a message is sent to the sender stating that the addressee's e-mail address is valid. This may mean that the user may receive spam in the future.

By default, Outlook Express now prevents external images from being loaded until the user grants permission. We advise you to block all images you receive unless you know and trust the source.

To view images in an electronic message received from a reliable source:

1. Open **Outlook Express** and open the e-mail in question.
2. If the message contains blocked images you will see a message saying **Some images have been blocked to help prevent the sender from identifying your computer. Click here to transfer the images.**
3. Click on the message bar. The image will be loaded so you can see it.



For further information consult the "Security" area in Millennium bcp's Portal

top



"Best Consumer Internet Bank" em Portugal • "Best Online Consumer Credit" na Europa
"Best Corporate/Institutional Internet Bank" em Portugal • "Best Information Security Initiatives" - Particulares, na Europa
"Best Bill Payment and Presentment" na Europa • "Best Information Security Initiatives" - Empresas, na Europa