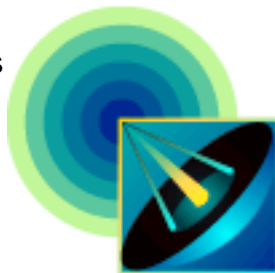


Use of secure technologies and the adoption of good practices can help to increase security when using the Internet. Spare a few moments to read this Newsletter and put our suggestions to good use.

Highlights:

Make your wireless network more secure

Use of wireless networks has increased significantly in recent years. What was, just a few years ago, a technology just for the few has now almost



become a necessity for many. It has simplified setting up a multi-point home Internet network without the hassle of connecting cables and yet more cables.

Nevertheless, its almost mass use has raised security issues . It has simplified setting up a multi-point home Internet network without the hassle of connecting cables and yet more cables.

Nevertheless, its almost mass use has raised security issues in some places, especially if the original configuration of the equipment is not altered and no additional security measures are installed ... >>

News:

If you already know about Spam, get to know about Spim

You must surely have read or heard about Spam (unsolicited e-mail). But did you know there is an even faster form of Spam? This is SpIM, or instant messaging spam ... >>



Basic Security Principles:

Videos on Security - Spyware

On our last edition we highlighted a new section on the Microsoft site dedicated to Security. A number of videos are provided, designed to help users ... >>



Configuring and updating software:

How to use the "Security alert" Dialogue box when using Windows XP Service Pack 2

Microsoft Windows XP Service Pack 2 (SP2) has several improvements to help make your system mores secure against attacks by malicious users or by virus... >>

Highlights:

Make your wireless network more secure

Use of wireless networks has increased significantly in recent years. What was, just a few years ago, a technology just for the few has now almost become a necessity for many. It has simplified setting up a multi-

point home Internet network without the hassle of connecting cables and yet more cables.

Nevertheless, its almost mass use has raised security issues in some places, especially if the original configuration of the equipment is not altered and no additional security measures are installed.

We want our customers to take full advantage of this technology, with ongoing security in their access to the Internet in general and to Homebanking in particular. We are therefore pleased to provide some advice regarding the configuration of your wireless network so as to make it more secure. To ensure proper implementation, we recommend that you read the manufacturer's instruction manual.

Alter the password of the router

To prevent strangers from accessing your equipment and altering its configurations, we recommend that you alter the router's administrator password to one that only you know.

Activate WEP/WPA

WEP (Wired Equivalent Privacy) is an optional encryption standard available on wireless devices.

Despite the fact that there are quite a lot of documented **WEP** failures, it still provides additional security, no matter how rudimentary.

If possible, you should also ensure that automatic rotation of the **WEP** key is activated. This makes it harder for certain tools to decipher the key in time.

On the other hand, **WPA** (Wi-Fi Protected Access) is already available on Windows XP, for example, and it provides a considerably higher level of security than **WEP**.

If possible, use **WPA** rather than **WEP** to encrypt traffic and to restrict access to your wireless network.

Activate MAC address filtering

MAC address is a unique address defined by the manufacturer, which identifies a given network card.

Most routers and wireless access points provide a function designated by hardware, or MAC address filtering. This function is usually not activated by the manufacturer owing to the extra work involved in its proper configuration. However, to increase the security of your wireless network we do recommend that you activate this function. After it is activated, whenever the router or wireless access point receives a request from a client to join the wireless network it will compare the client's MAC address against the list of authorised MAC addresses, so as to allow or deny access as appropriate.

The MAC address of the wireless network cards cannot be altered since it is registered on the hardware itself. However, some network cards allow the MAC address to be altered by means of software, allowing wrongdoers to take advantage of network cards of this type to configure an authorised MAC as its MAC address. Even though it is not "bullet proof", MAC address filtering continues to provide an additional security level which, together with other measures, significantly improves the security of your wireless network.

Modify the SSID

The **SSID** (Service Set Identification) is a set of alphanumeric characters that identifies a wireless network. Most wireless equipment has a factory defined **SSID**, but you should assign a personal name to your wireless network.

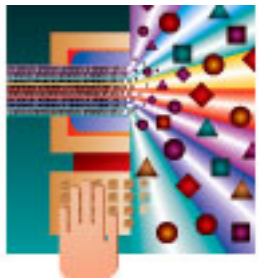
Switch off the SSID broadcasts

Most wireless devices are supplied with the SSID broadcast activated, since it is far simpler to localise your wireless network during the implementation process. After the implementation process is complete, we recommend that you deactivate SSID broadcast on your router or Access Points, preventing it from constantly announcing itself. Most hardware allows you to deactivate the SSID broadcast, allowing you to "hide"; the wireless network and making it harder for wrongdoers to discover its name.

Positioning Access Points

APs should be so positioned as to ensure that, while continuing to provide the best possible service, the signal is not propagated to the outside, that is, you should look for suitable points within the building, home or structure where the users are located. This signal should not be picked up outside the building or where there are no users.

You are also advised to check the distance the signal is propagated by simply moving away until the signal is lost.



News:

If you already know about Spam, get to know about Spim

You must surely have read or heard about Spam (unsolicited e-mail). But did you know there is an even faster form of Spam?

This is SpIM, or **instant messaging spam**.

Instant Messaging, or IM, is an online system of communication, similar to a telephone conversation, though based on text and not on voice. Used by millions of people around the world to "chat" with friends quickly, or instantly as the name suggests.

When using an IM programme it alerts you when someone on your Contact List is online, allowing you to start "talking" to that particular person.

Since it is an extremely fast and successful means of communication, particularly as far as the number of users is concerned, Instant Messaging has become a target for the propagation of malware (an abbreviation for **malicious software**) – programmes conceived to corrupt systems and to cause damage through virus, Trojans, etc. – and SPIM is already being used to a considerable extent to send electronic junk messages. It often contains messages advertising medicines, adult products or misleading messages containing schemes or virus.

Some measures to protect yourself against Spim:

- Communicate only with persons on your contact list and don't add strangers;
- Don't open attachments from people you don't know and, even if you do know them, check the origin of the messages;
- Don't accept links even if you think you know who sent the message. The sender may be "disguised" by the spimmer to look like someone you know.



Basic Security Principles:

Videos on Security - Spyware

In our last edition we highlighted a new section on the Microsoft site dedicated to Security. A number of videos in Portuguese are provided, designed to help users to get to know the more important security problems and how to avoid them.

This month's highlight is Spyware.

Spyware is a term used to designate software that executes certain actions such as: divulging advertising matter, gathering personal information or altering the configuration of your computer, generally without adequately obtaining your consent.

You may have Spyware or other undesirable software in your computer if:

- You see ads even when you are not on the Internet;
- The page that your browser opens first (the home page) or the browser's search definitions have been altered without your knowledge;
- You see a new tool bar on your browser that you do not want and find it hard to get rid of it;
- Your computer takes longer than usual to perform certain tasks; or
- Your computer suddenly hangs far more frequently than is usual.

Consult the following address on the Microsoft site and watch the video to find out more about this topic: <http://www.microsoft.com/portugal/athome/security/spyware/video1.msp>



Configuring and updating software:



How to use the "Security alert" Dialogue box when using Windows XP Service Pack 2

Microsoft Windows XP Service Pack 2 (SP2) has several improvements to help make your system more secure against attacks by malicious users or by virus. By default, the Windows Firewall is activated on

computers running Windows XP SP2. This closes doors to prevent computers hooked up to the Internet from accessing shared files and printers or other resources of your computer. When a programme tries to use the system's resources or ports that are protected by the Firewall a "**Security alert**" dialogue box opens, providing options to solve the problem in question.

The "**Security alert**" dialogue box contains information like the following:

Security alert

To help protect your computer the Windows Firewall has blocked this programme from receiving unsolicited information from the Internet or from a network.

Name: Name of the programme

Editor: Programme manufacturer

The following options are available:

- **Unblock this programme, despite the security risks;**
- **Keep the programme blocked;**
- **Keep the programme blocked, but ask again later.**

If you don't know the programme or manufacturer you should choose the option "Keep the programme blocked". Certain programmes can be virus or even spyware that could affect your system or even send personal and confidential information via the Internet.