

The computer, nowadays, is almost essential to the daily lives of many people, and the Internet plays a fundamental role. It may seem difficult, but a little care and keeping informed are all that is required to ensure that security is not compromised.

Highlights:

Activate WPA and protect your wireless network!

Wireless technology is increasingly used in our homes to access the Internet. It is more convenient in that wires don't have to be connected



around the house to be able to use the various computers.

Wireless devices use radio waves to communicate and these waves are often sufficiently strong to be received outside the house. Our privacy could well be compromised if the wireless network we use is not protected.

Knowing this, many intruders carry out what is known as 'wardriving', or driving around areas where they detect wireless network signals... >>

News:

"Online friends"... are they really?

The skipping rope, the top and the marble have given way to the computer, and friends are often on the other end of the line... or of the world...>>



Basic Security Principles:

Videos on Security - Computer updates and maintenance

The first line of defence to keep your computer as secure as possible is to regularly update the software and to carry out system maintenance... >>



Configuring and updating software:

Managing the security definitions of the computer from a single location

Windows XP Service Pack 2 (SP2) contains a number of new technologies conceived to help you to keep your PC and your personal information more secure... >>



Highlights:

Activate WPA and protect your wireless network!

Wireless technology is increasingly used in our homes to access the Internet. It is more convenient in that wires don't have to be connected around the house to be able to use the various computers.

Wireless devices use radio waves to communicate and these waves are often sufficiently strong to be received outside the house. Our privacy could well be compromised if the wireless network we use is not protected.

Knowing this, many intruders carry out what is known as 'wardriving', or driving around areas where they detect wireless network signals. If these aren't properly protected, they can access your network, your computers and even your files. In most cases the goal is simply to make use of your Internet connection.

In our last Newsletter we provided advice on the configuration of your wireless network to make it more secure.

In this edition we shall detail the process of WPA activation (Wi-Fi Protected Access).

We shall see how this can easily be done, using the SpeedTouch 580⁽¹⁾ router for the purpose. This is just an example. For other routers consult the supplier's user manual.

A) To access the SpeedTouch router configuration pages and to customise the router

Most browsers are configured using a browser such as Internet Explorer. Using the Internet browser, you then type the IP address of your wireless router to provide access. The router's IP address can easily be found in the user manual provided by the manufacturer.

To prevent loss of connection with the router, we recommend that the configurations be performed using the network cable supplied with the equipment, rather than using the wireless network for the purpose.

After accessing the router you can then configure it for the use of WPA encryption, for example.

Take the following steps:

1. Start the Internet browser;
2. Access SpeedTouch using the IP 10.0.0.138 address⁽²⁾;
3. An authentication window will open if you have defined a password on the system. Insert the system username and password to be able to access the home page of the SpeedTouch. The **System Information** page will appear;
4. Select the **Wireless** option on the menu on the left, followed by the **Security** option in the centre;
5. **5. Activate the WPA as follows:**

a) Select **Security level 2 WPA-PSK**, which allows you to move on to the next window:

The screenshot shows a web-based configuration interface for an access point. It has three main tabs: 'Access Point Settings', 'Security', and 'Associated Stations'. The 'Security' tab is active, and within it, the 'Security Mode' sub-tab is selected. Below the tabs, there is a table for 'Security Configuration' with three rows: 'Security Level 0 - no encryption' (Active: yes), 'Security Level 1 - WEP' (Active: no), and 'Security Level 2 - WPA-PSK (WPA Personal)' (Active: no). Below the table is the 'WPA-PSK Security Parameters' section, which includes a text field for 'WPA passphrase' containing 'FFA22E9CCA', a dropdown menu for 'Encryption' set to 'TKIP', and a text field for 'Rekeying interval (sec.)' set to '0'. At the bottom, there are three buttons: 'Apply', 'Cancel', and 'Help'. A red warning message is displayed above the buttons: 'Please note that changing the wireless settings may cause loss of wireless connectivity. You may need to reconfigure your wireless stations to restore connectivity. Consult your user guide for further information.'

b) Define your **Network key**, which must have between 8 and 64 ASCII characters. Make sure the key is not obvious, that is, make it alphanumeric, preferably using both upper and lower case letters.

c) Select a cryptography method ⁽³⁾.

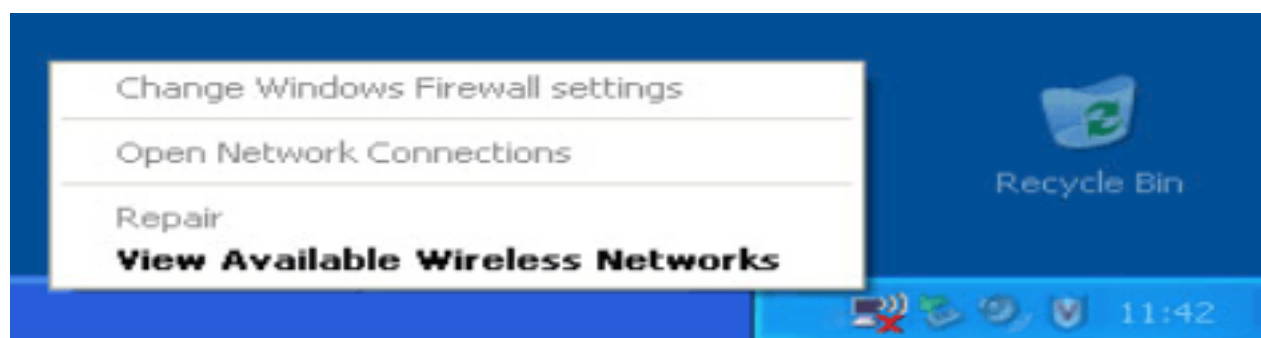
d) Click on **Apply** to apply the WPA-PSK configurations. The colour of the WLAN LED changes to green

e) Click on **Save all** to save the alterations to the permanent memory.

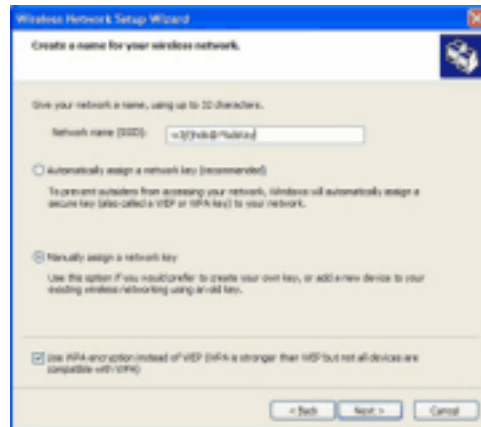
f) Reconfigure the wireless clients (the various computers having wireless devices), as shown hereunder.

B) To configure a wireless client having the Microsoft Windows XP SP2 operating system we recommend the following steps:

1. Use the right button of the mouse to click on the wireless connection and View Available Wireless Network;



2. On the **Network Tasks** menu, click on **Set up a wireless network for a home or small Office**;
3. We have to indicate the name of our wireless network (SSID), which must be the same as the one defined on the wireless router side;



4. **Click on Manually** assign a network key;
5. Select the option **Use WPA encryption instead of WEP**, and then click on **Next** ;
6. Next, introduce the WPA **Network key** defined for our router when the WPA was configured. Then click on **Next** and the process is finished.



This concludes the process. Your wireless connections will have greater protection. Don't forget all the other security recommendation, however.

- (1) This model comes with WPA. If you use a model that only uses WEP activate it preferably using the 128-bit key.
- (2) Note: 10.0.0.138 is the standard SpeedTouch IP address in most cases. If it is not, contact the Internet Service Provider (ISP) or check the manufacturer's user manual to obtain more information..
- (3) TKIP is the cryptography specified in the WPA Standard. AES cryptography provides greater security, but it does not come with WPA (it will be a part of the future standard, the WPA2) .

News:

"Online friends"... are they really?

The Internet provides an immense "sea of information" with educational potential. The skipping rope, the top and the marble have given way to the computer, and friends are often on the other end of the line... or of the world.

Chat rooms and instant messaging programmes have come to be a means of communication much appreciated by children. They communicate through a different language, using new expressions and abbreviations. You will find it hard, at first, to understand what they mean.

Children are quick to learn these technologies and they will always be one "click" ahead. Unfortunately, there may be evil-minded people on the other end of the line. Parents and teachers should take care and take part in their inline activities, transposing to the "virtual world" the advice given in the real world.

"Don't talk to strangers" :

- Get to know your children's "online friends" just as you know the others;
- Make them understand that they shouldn't send photos of themselves to people they get to know through chat rooms;
- Tell your children never to provide personal information such as address, phone number or the name of their school;

"If you get lost ask a policeman for help" :

- Tell your children that if anything upsets them or if they receive an "improper" message in a chat room, they must immediately sign off and tell you what happened;
- Insist that they only use those chat rooms supervised by monitors: these are responsible for sorting messages, eliminating those they consider improper.

Teach your children to recognise the dangers that could be posed by an "online friend" so that they can use make good use of these communication.

top



Basic Security Principles:

Videos on Security - Computer updates and maintenance

The new section on the Microsoft site dedicated to Security provides a number of short videos in Portuguese that we have divulged in recent



This month, the focus is on updating and maintaining your computer. The first line of defence to keep your computer as secure as possible is to regularly update the software and to carry out system maintenance operations on a regular basis to avoid losing data and to protect against new viruses and other potential hazards.

Consult the following address on the Microsoft site and watch the video to find out more about this topic:

<http://www.microsoft.com/athome/security/update/default.msp>



Configuring and updating software:

Managing the security definitions of the Computer from a Single Location



Microsoft Windows XP Service Pack 2 (SP2) contains a number of new technologies conceived to help you to keep your PC and your personal information more secure. SP2 also simplifies the monitoring of these definitions using the Windows Security Center, accessible through the Control Panel.

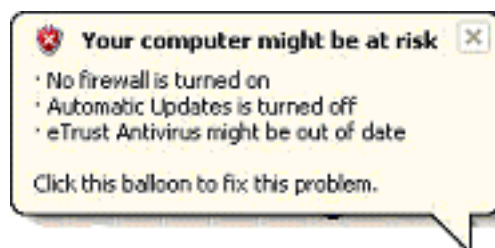
The Security Center allows you to check the status of the essential security definitions. You can also use it to locate information on more recent viruses and other security threats, or to obtain technical support from Microsoft in security-related problems.

To open the Security Centre:

1. Click on **Start** and then on Control Panel;
2. Double click on **Security Center**.

The Security Center will check whether the user has:

- Firewall software.
- Up-to-date anti-virus software.
- The "Automatic Updates" function configured to automatically download and transfer the updates.



Should the Security Center find that a computer could have better security in one of the three essential areas listed above, a warning will be provided in the notification area (to the right of the task bar, next to the clock). Whenever you start a session, a similar warning will be shown until the problem is solved.

