How to secure your PC

In this tutorial, we have collected a number of tips aimed at raising the security level of your PC.

Protect your PC and files with secure passwords

It is essential to use secure passwords to protect the system and the files saved on the disk. As for the choice of passwords to be used to protect the PC, We recommend using access keys that are long enough, difficult to guess (therefore meaningless) and made up of numbers, letters and symbols and at least 16 characters.

Install a good antivirus

Installing a good antivirus is one of the most important steps you need to take to protect your PC.
You can download free antivirus or purchase paid antivirus. Both solutions are valid, paid antivirus offers some additional features that can always be useful: they usually allow you to activate settings that prevent cyber criminals from taking control of the webcam or microphone connected to the PC.
They offer password managers in which to keep the access keys to your accounts and much more.
You can find reviews of a good antivirus on this website
https://www.av-test.org/en/antivirus/home-users/

Use a firewall

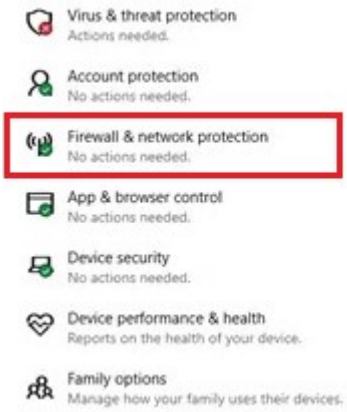
A firewall is one of the indispensable programs for the security of your computer.
A very important clarification: a firewall is not an antivirus.
An antivirus protects the system from malicious software that very often arrives by e-mail or is hidden in programs and executable codes taken from the Web.
A firewall, on the other hand, protects network connections, preventing there from being an uncontrolled or illegitimate use (via local network or Internet) of your system.

The operating systems "Windows 10", "Windows 8", "Windows 7", "Windows Vista" and "Windows XP" (with service pack 2 or higher) are already equipped with Firewall.
Therefore it is not necessary to install one.
However, keep in mind that to have a secure Windows operating system, it is highly recommended to update it to the latest version.
That said, to check if a Firewall exists and is active on your PC,
For Windows 10:

Open the Settings by clicking on Start> Settings
or, by pressing the key combination START + [I], that is, hold down the start button and press the letter I.
Click on the "Updates and security" section

Click on "Windows Security", located in the side column.

Click on "Firewall and network protection"



N.B .: if you already see a green "sticker" it means that everything is fine!

Look at the panel
If "firewall is enabled" on all three networks:
Domain network,
Private network,
Public network
It means that everything is in order.

Otherwise, follow any instructions proposed by the system.

UPnP: what it is and what it is for

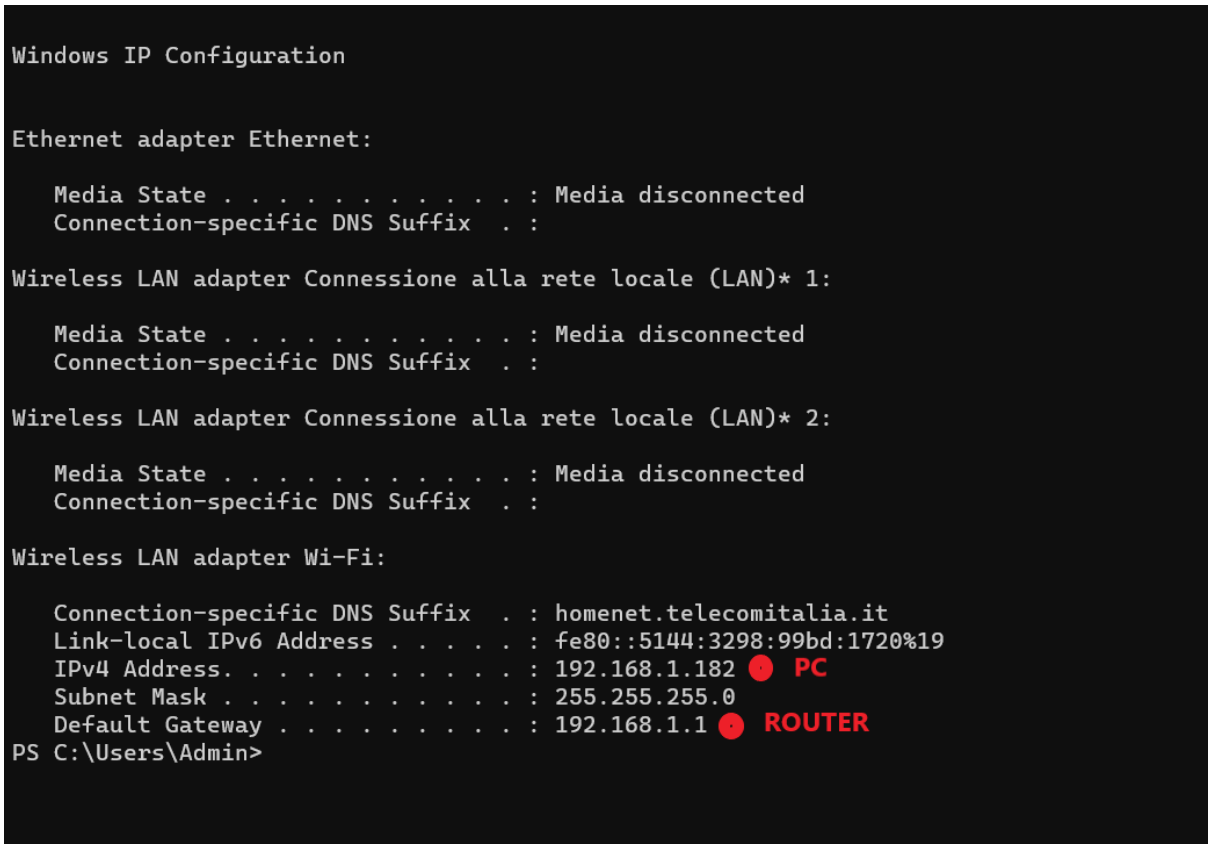
This protocol is mainly used to be able to automatically open certain ports on our router, so that there is no interference during the download. It is also possible to manually set port forwarding, using the appropriate option in the control panel of the router.

Advantages and risks of UPnP

A first real advantage of using UPnP is the fact that the connection between devices occurs automatically, without any manual intervention. This automatism, however, can be the cause, as can be easily understood, of possible cyber attacks.
Therefore the problem of safety is certainly not to be underestimated.
Another positive aspect is the total independence from the means of data transmission. In fact, the UPnP standard is compatible with most current devices, such as tablets or PCs. Other than that, you don't need any third party software for external compatibility to other devices as well. Also in this case the problem of safety returns. The fact that UPnP allows any program or device to automatically access the network is an intrinsic weakness in the protocol itself. The total absence of authentication exposes not only the connected devices but also the entire network we are using to risk.
On the other hand, UPnP allows any device to take advantage of our connection, accessing the router automatically. In practice it is as if we were giving free access to our home network.
So what to do to avoid all this? If you don't necessarily need to activate UPnP, keep it deactivated. If, on the other hand, you just can't do without it, try as much as possible to keep the security of your network under control, even if it could be of little use. Maybe try to use programs you trust or have already used without any problems.

Port forwarding

If we decide to deactivate UPnP but for example we need to open the ports to increase the number of connections of one of our wallets, it is necessary to know the concept of port forwarding.
First we identify the local IP addresses of our device and router using the "ipconfig" command in the command prompt.



That said, the first step you need to take is to start the browser you usually use to surf the Net (e.g. Chrome), type the router IP in the address bar and press the Enter key on your computer keyboard.
Furthermore, to enter the router configuration panel, you may be asked to enter your username and password. If you haven't changed your device login information, you may need to log into its admin panel using the admin / admin or admin / password combination. In any case, you should also find the login credentials in the device user manual. It is highly recommended that you change the router default credentials with your own.

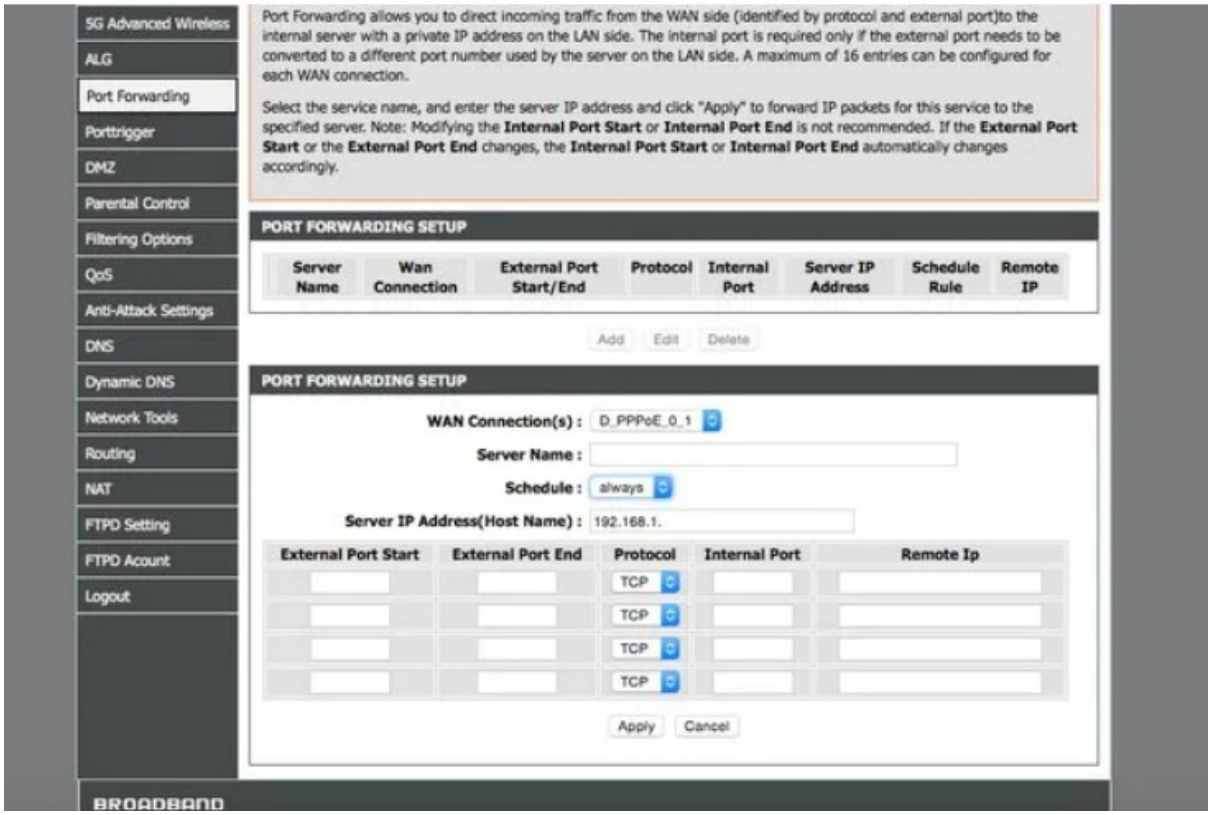
How to open the router ports

Once logged in to the router management panel, go to the Port Forwarding menu or the one dedicated to Virtual Servers, start the creation of a new rule or a new virtual server and fill in the form that is proposed to you in this way.

- **Internal port/ External port** (or **Start port/ End port**) - in these fields you must enter the number of the port to open. The same value must be entered in all fields.
- **Destination IP** (or **Server IP address**) - in this field you must type the local IP address of your PC, or rather, of the computer on which you intend to use the program that is now having connection problems.
- **Name** in this field you have to type the name you want to assign to the rule you are creating. You can type in any name (eg Wallet Sapphire).
- **Port type** (or **Protocol**) - in this field you must specify if what you are opening is a **TCP** or **UDP** port.

Once you have completed the form, click on the **Save / Apply** button to save the changes and repeat the operation for all the ports you intend to open in the router.

Each brand of router has a management panel structured in a different way. You have to identify the right options taking "cue" from what has just been illustrated.
To make the task even easier for you, below we show an example for **D-Link** routers.



If the one in your possession is a D-Link device, to open the router ports you have to go to the Advanced tab located at the top and select the Port forwarding item from the left sidebar. Then you have to click on the Add button and fill in the form that is proposed to you in this way.

- **WAN Connections** you must enter the name of the Internet connection in use, then leave the value set by default.
- **Server Name** you must enter the name to be assigned to the rule.
- **Schedule** sets this menu to always, otherwise the rule will not always be active.
- **Server IP Address** you must enter the local IP address of the computer.
- **External Port Start**, **External Port End**, and **Internal Port** you must enter the number of the port to open.
- **Protocol** you must indicate the type of port to open, choosing between **TCP** and **UDP**.

After filling out the form, click the **Apply** button to save the changes and that's it.