Why should we use a VPN to protect our devices?

VPNs have evolved rapidly to satisfy the needs of users that seek security as well as anonymity online.

They were previously reserved especially for companies who wanted to have secured access to their professional network. No matter if we use a tablet, mobile phone or PC, a VPN will always protect us online.

Picture 1 of Why should we use a VPN to protect our devices?

What is a VPN?

A VPN is a tunnel, created between your machine, or your local network and an external server. The connection is encrypted from end to end using several possible protocols. Currently, the most used encryption protocols in the field are L2TP, OpenVPN, and PPTP.

The fact that the data is encrypted from end to end means that your data circulates in the tunnel, between your router and the VPN server is undecipherable. It is the VPN server that will make your requests and communicate the result to you through an encrypted tunnel. Moreover, a VPN server can be physically located anywhere in the world.

Why do people use VPNs?

VPNs are normally used by companies and allow teleworking employees especially to make a safe connection to their company's internal network in a secure manner. These types of systems are commonly considered to be an ideal solution to perform illegal downloads.

Using a VPN is not only about fraudulent downloading. It also provides a high level of security for Internet connections, especially to make online payments. The use of a VPN can be reassuring and practical to:

1. Secure your public connections when you are in a hotel or at your favorite restaurant.
2. Accessing online services which are geographically restricted.
3. Accessing restricted online services in countries such as Egypt or China that monitor communications.
4. By using a VPN, you can book cheaper fares for booking flights for different destinations, regardless of where your flight departs.

Is it possible to configure a VPN on Windows?

Absolutely, it is also possible to configure a VPN connection directly in Windows, without using any specific app downloaded from the Internet. NordVPN or Surfshark VPN for Windows are very good software for this purpose.

To set up a VPN connection, under Windows, right click on the network icon in the taskbar. Then choose **Open network and internet settings**, in the new window that opens, in the left column, choose >**VPN**. Then fill in the fields **VPN Provider**, **Connection Name**, **Server Name** or **Address**, **VPN Type**, add the connection information types, choose a username, and finally add a password.

Finish by clicking on **Save**. Once the configuration of the connection is established, you can launch it by clicking on its name in the list of your networks.

Which point should you consider when choosing a VPN?

There are some important details that you should take into consideration when you need to choose a VPN.

The Operating System

Picture 2 of Why should we use a VPN to protect our devices?

Before choosing a VPN, check that the program works on all the platforms that you use. The more you have choices, the more it will be possible to use the app differently. Most options are compatible with macOS, Windows and Linux. You should verify properly that the VPN chosen offers an app for Android or iOS. Hence, it will be effective in protecting your connections on mobile phones. If you wish to protect all your devices, the easiest option is to perform the installation of the VPN on your router.

The Price

The VPNs prices are variable and there are many promotions. Moreover, the promotions are sometimes different with offers starting for example, as from 1 month, 3 months, 1 year or 3 years. And note that you can usually benefit from one month trial offers so that you may test the VPN in real conditions. However, for most providers, you must register by giving your bank details.

No Data Recording

The greatest advantage of VPNs by far is anonymity, and this is the reason why some providers offer to keep very little or no information about the users Internet traffic. Moreover, in the interest of transparency, many ISPs order audits to obtain certification of non-data retention.

The amount of servers

The more servers the provider has, the better he will offer quality connection. The ISPs must be totally capable of offering a great range of geographical outlets. Therefore, it is necessary that the VPN provider possess servers in a lot of countries. You should also note that sometimes to access some geo-restricted services, a server will not always be enough.

Provisioning in sensitive areas

When you wish to use a VPN abroad, always check that it will work in the expected destinations and especially in certain areas that are sensitive such as UAE.

Communication and encryption protocol

Picture 3 of Why should we use a VPN to protect our devices?

Excellent encryption is an essential component of a good VPN. Therefore, it is important to make sure that the ISP uses very good quality algorithms allowing the transmission of data without any problem. In fact, if someone wants to read the encrypted data, a key will be needed to decode any information. The longer the key is, it will be more difficult to decipher it even when you use specialized software. It is usually the case as the number of combinations possible for a key will depend on its length.