HOME CYBER DEFENSE
ARE YOU SAFE FROM CYBER CRIME?
WEEKLY

Volume #4 - Issue #160
May 18th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Should You Connect through WiFi or Ethernet

There is a lot of debate about Wi-Fi speeds and whether they can offer higher potential speeds than a cable connection, but in practice Ethernet connections turn out to be not only faster but also safer.

The era of technology we exist in leads us (and in some cases forces us) to be connected at all times. One of the consequences of this connectivity can be clearly seen in communications and in how we have gotten used to things happening instantly. Nowadays we, as users of technology, see it as only natural to be able to obtain information or communicate with another person immediately.

In this context, for the most part we have two options for getting online: The first is wireless, via Wi-Fi, and the second is through a network cable, commonly known as Ethernet. Let's analyze these two options to see the differences between them and also take a closer look at the belief that network cables are always the best option.

Naturally, the arrival of wireless connectivity was a great benefit as it allows us to keep our physical space tidier and avoid the need for lengths of cable between connected devices. But besides the convenience offered by wireless, when it comes to pure speed, a debate has been raging for some time now leading to a lot of disagreement: Which is faster, Wi-Fi or network cables? The answer is straightforward, though: cable. Although Wi-Fi is a newer protocol, there are a lot of factors in play (in fact we will only look at a few in this article) that influence whether one connection can be faster than another. Perhaps the main issue is the saturation of channels and the large number of default connections, which makes data transmission speeds less stable and generally lower.

Added to this is the effect of building structures, for example, concrete walls, swimming pools, and other building materials which cause a loss of signal and a reduction in performance, which affects the speeds achievable from a Wi-Fi connection. Generally speaking, the higher the frequency, the larger the rate of absorption by walls and floors.
Of course, it is almost impossible to notice these slight, almost imperceptible variations during normal browsing. However, the differences in performance are more obvious when it comes to activities like playing an online game, sharing files on the network, or streaming ultraHD content.

While there are different norms and standards for each type of connection, in general, a correctly installed network cable connection ends up being faster than a Wi-Fi connection. When we look at the speeds offered by each protocol, for example the 802.11ac standard, we need to understand that its stated speed of 6.5 Gb/s is the maximum theoretical speed (which is faster than Ethernet 2.5 at 6 Gb/s), but that in most cases it cannot actually reach its maximum potential as it is affected by the obstacles we just mentioned. For their part, Ethernet connections offer a more stable performance, as they are not affected by these issues or other external factors.

If we think in terms of secure communications, the argument in support of wireless connections loses immediately if we compare it to Ethernet. Numerous kinds of attacks can be carried out remotely, such as deauthenticating a device, or cracking the encryption key to get into the network. Furthermore, in the past year we have seen the emergence of vulnerabilities like KRACK, which affects WPA2 (one of the most robust and widespread protocols), and which was likely the trigger that led to the development of the new WPA3, although this has not yet been launched. As well as this, an attacker could also block wireless communications, with greater or lesser degrees of success, through the famous signal-blocking jammers.

Finally, another very common type of attack is one which uses fake access points, whereby the victim connects to an open network which was created by the attacker, who then spies on the user's traffic and steals their data. Of course, these attacks are impossible to carry out remotely through an Ethernet network, as an attacker would need physical access to do so. For these reasons, cable connections are more secure than wireless, or, in other words, they offer a lower risk of incidents if you do not make great efforts to apply some of the various security measures available.

Clearly, the need for mobility will have an impact on our decision, as will the number of ports available in our router. If you use a laptop and are constantly moving from one desk to another within the range covered by your Wi-Fi, it may be impractical to restrict yourself to a cable, which would force you to stay in the same spot. With a desktop, though, things are different. While desktops can be fitted with a wireless card, this is only recommended when connecting an Ethernet cable between the desktop and the router is not possible. For network sharing devices and media players, cable connections are also best.

While the dream of cable-free devices is already possible, in many cases it is not the best option if you love high speeds. In the end, then, it all comes down to a question of priorities.

Thank you for subscribing to our email!

Home Cyber Defense Weekly

is a service of

House of File Technologies