A handy guide on how to keep your home Wi-Fi safe

AHM MOHSIN

The pandemic has shown us how vital the internet is in our daily lives. As access to the internet has become more of a necessity over time, we are constantly remaining connected through our devices. Sometimes, it becomes the only way to stay connected to our loved ones. Online access is also necessary for our work, education and entertainment purposes. Even so, there is a growing dependence on Wi-Fi networks to provide internet access for everyone, be it in a household or an office setting.

However, the internet can become a breeding ground for criminals with harmful intentions. As cybercrimes continue to rise across the globe, private wireless networks are susceptible to interventions as many people may have access to it through their smartphones, laptops, PCs, and even tablets. A small vulnerability in a home Wi-Fi network can give widespread access to hackers. They can breach the privacy barriers of all the devices connected to the wireless network by capitalising on it. Hence, it is essential to secure your home WiFi network against unwarranted access.

HERE ARE SOME TIPS TO KEEP YOUR HOME WI-FI SAFE:

Tip 1: Keep Your Router's Software Updated

We often hear that Internet Service Providers (ISP) offer users a router as a part of a package deal. At times, the users update the software by themselves. What often happens is that people tend to forget about firmware updates to routers. If your router is more than seven years old, you need to patch it immediately. In case you are unable to update it, it is strongly recommended that a new router be purchased. This minimises the chances of criminals breaching your network.

Tip 2: Check Your Encryption Settings

Most wireless routers come with preinstalled encryption features. However, they remain turned off by default. A common tendency among many users is that they assume their wireless home networks to be safe, and put off encrypting the router. This could lead to catastrophic implications on their data. Hence, ensuring network encryption is the safest option to prevent hackers from accessing personal and sensitive information. It is recommended to use at least WPA2-PSK (AES) encryption, also known as WPA2-CCMP.

Tip 3: Pick A Proper Password

It is necessary to update your router's password, as most routers come with preset passwords upon purchase. These basic passwords can be breached easily. So, it is imperative to change them with a suitable alternative to secure the wireless network. While it might be tempting to use a short and simple password that is easy to recall, users need to understand that these make the wireless network vulnerable to hackers. Thus, it is vital to choose a strong password that is complex and lengthy to keep criminals away.

Tip 4: Review Your IoT Devices

External devices, such as webcams and wireless speakers that can connect to routers, should be reviewed frequently. These smart devices, which can operate independently, should be only connected when necessary. Additionally, these gadgets should be updated and configured regularly.

As simple as it may seem, these tips can go a long way in securing your wireless networks and promoting a safe environment for easy internet access.

AHM Mohsin *is the Country Manager of Sophos in Bangladesh.*