How to stay safe while using public Wi-Fi

If you are a remote worker or love travelling frequently, you will often need to rely on public Wi-Fi at airports, restaurants, hotels or libraries to get your work done on the go. However, being publicly accessible networks, these Wi-Fi hotspots come with certain risks you should be wary of. If you regularly use public Wi-Fi, here are some tips to always keep in mind.

Don't share sensitive information

Public Wi-Fi networks are usually not secure, so it is best to avoid accessing sensitive information such as banking and credit card information, social security numbers and other personal information. This runs the risk of your important information being stolen or used in malicious ways.

Turn off automatic connectivity

Your device may automatically connect to a Wi-Fi network, including public networks. You should turn off automatic connectivity in public Wi-Fi to avoid inadvertently connecting to a public network without your knowledge. This is important because public Wi-Fi networks are often unsecured, meaning that anyone on the network can potentially access your device or intercept your data.

Turn off file sharing

If you're connected to a public Wi-Fi network, it's important to be cautious about file sharing to protect your personal data. To turn off file sharing in a public Wi-Fi network, start by going to 'Control Panel'. From there, open the 'Network and Sharing Center' panel and click on 'Change advanced sharing settings' in the left-hand sidebar. You will then see the options to turn off network discovery as well as file and printer sharing - two options you should disable when using public Wi-Fi. These steps should help to ensure that your files are not shared with others on a public Wi-Fi network.

Use HTTPS on links

Websites that use HTTPS encryption are more secure, so look for the padlock icon in the URL bar before entering sensitive information. The padlock icon indicates an SSL certificate, which means it is encrypted. Accessing such sites doesn't cause the risk of your information being exposed to third parties. Conversely, accessing via HTTP instead might expose your traffic's visibility to anyone else accessing the same network.

Don't use public Wi-Fi to buy things online

Using public Wi-Fi to make online purchases is generally not recommended due to the potential security risks. Public Wi-Fi networks are typically unsecured, which means that anyone with the right tools and knowledge can intercept and read the data being transmitted over the network. To protect your personal and financial information while shopping online, it's best to use a secure, private network such as your home Wi-Fi or a cellular data connection.

Keep your security software updated

To protect against random data leaks or suspicious activities online, you should always keep your antivirus and anti-malware software updated to their latest versions. Popular antivirus software like Kaspersky, Norton, McAfee, Bitdefender and Avast are especially proficient at keeping you safe while browsing the internet in a public network. These softwares also frequently launch updates with important patches - which you should definitely stay on top of for all your online security needs.

Be aware of your surroundings

Last but not least, be careful of your surroundings when you're using your laptop or smartphone connected to public Wi-Fi. Especially when using a laptop, your screen might be privy to random passersby - who just might glance at sensitive or personal information that you don't want to share. As such, be especially aware of the environment you're in and stay alert for any notable changes in the public setting.