Tips on How to use a Public Computer safely

Some of us will occasionally have to use a public computer for one reason or another. When using a device found in a public place, there is always the risk of exposing yourself to a number of security threats. Fortunately, there are a few simple rules when it comes to public computer safety which can be vital for your online privacy.

Read these tips on safe browsing and how to keep your work, personal, or financial information private.

How safe a public computer really is?

Most of the time, you have no prior info on the security aspects of the computer you are temporarily using, how secure the connection is and if your online actions are being recorded.

Using a public device can be quite risky for your safe browsing, or sensitive private information such as data security, password security or banking details. If you are not taking some basic computer safety measures, your private data can be at stake.

What risks of using public computers are there?

Here are some of the most common risks when using a public computer:

- Someone gaining access to your activity on the internet especially if you are using a public WiFi
- People can be indiscreet and look at your monitor
- The malware and spyware on public computers
- Access to your browsing history
- Theft of important personal information
- Passwords and log in credentials theft

However, there are ways in which you can cover your online tracks if you find yourself in the situation of using a public computer. Remember, safety first.

How to use a public computer safely?

Keep in mind that there is nothing you can do in order to make a public computer completely secure. However, there are ways in which you can significantly reduce the risks of using public computers.

Here are some public computer safety tips that you need to follow.

Delete your Browsing History

When you've finished browsing, always make sure that you delete your cookies, form data, browsing history, temporary files or saved passwords.

Don't save any passwords

We've mentioned password saving before as being extremely dangerous and this should be self-evident when using a public computer. Before logging in, make sure that the 'save password' option is not turned on by default. Also, keep an eye out for 'Keyloggers' as these tiny devices can log every key you press on your keyboard and can capture everything from passwords, personal messages, credit card details and pretty much everything you type. So, before you start using a public computer, you should always ensure that no keylogger devices have been attached.

Do not use your credit card and banking details

Always avoid actions that might reveal valuable account passwords or personal information such as credit card numbers and financial transactions details. Such actions can be extremely harmful as the information can be stolen and used.

Don't save files

Some of the files you would normally save locally can contain private or sensitive information for example an important email attachment. Best way to protect your data is by using a flash drive on which you can save files if needed.

Also, make sure to delete the temporary files associated to the use of programs other than web browsers. These files are usually supposed to be automatically deleted when you close the program or during reboot but this is not always the case.

Reboot

After using a public computer, reboot is the final step you need to make in order to erase your tracks. This will the clear the page file and also clear out everything from the physical memory (RAM).

Watch out for snoops Since you find yourself in a public place, you should always be aware of the strangers around you. You never know who's snooping behind your shoulder. Also, mind the security cameras installed in most public places as they can record your every move including password typing and screen display.