Five Uncommon Ways to Tighten Your PC's Security

When it comes to PC protection, an ounce of prevention is worth a pound of cure.

We all know we need to protect our computers from viruses, hackers and malicious software. If you care about your digital security, you probably already have some form of protection installed - hopefully an antivirus package that can detect trojans and malware too.

However, although anti-virus software is essential, it by no means guarantees that your computer is 100% secure.

Luckily, you aren't powerless – there are several lesser-known steps you can take to make your PC's security watertight. Here are five of them.

1) Change Your Browser's Security Settings

Internet browsers such as Firefox, Internet Explorer and Google Chrome are our portals to the web. We use them every day, and most of us click on dozens of links to unfamiliar sites, largely without a second thought.

Unfortunately, viruses and malware excel at hiding in websites. If you land on an infected site, your computer will be exposed. What's more, dubious sites often disguise malware as a free utility or downloadable file, and downloading it might inadvertently infect your computer.

To protect yourself from malicious sites, change your browser's security settings. The higher the security level, the more likely your browser will be to detect infected sites or covert attempts to install malware on your computer.

You'll want to implement the highest level of security that still enables the functionality you require. To do so, navigate to the security options in your browser's 'Settings' window, and select the level of security that's right for you.

2) Don't Visit 'Dubious' Sites!

We know they're out there. The fact is, file-sharing websites, and sites in "seedier" industries have been shown to be much more highly loaded with viruses and malware than the rest of the web. Some of these sites are even constructed entirely with the intention of infecting their visitors' computers.

Seedy websites play to people's impulsive sides, and they rely on the fact that visitors will be clicking links without thinking.

The more you steer clear of unscrupulous content, the safer your device and your data will be.

3) If You Telecommute, Use a Business VPN

More and more people take their work home with them and use a remote connection to transfer files to and from their workplace.

If this is you, you absolutely need to be transferring your data via a Virtual Private Network, or 'VPN'. In short, a business VPN is a secure connection between your device - laptop, table or smartphone - and your company's private network. A VPN is typically far more secure than raw 3G or WiFi internet - this is due to advanced encryption algorithms and the direct nature of the connection.

If your boss isn't up to speed with VPNs for telecommuting, perhaps it's time to make the suggestion – a well-implemented VPN will prevent security crises, and save your company time and money in the long run.

4) Use a Limited User Account

Even with a solid antivirus program installed, malware can still slip through the net.

One effective way of rendering it harmless is to make sure you use a 'limited user account' for regular tasks with a risk of exposure, such as reading emails and browsing the internet.

If you're running Linux or Mac OS, you're in luck – these operating systems already require you to enter a password in order to allow programs to make a significant change to your computer. In Windows, you'll need to set up a designated user account that doesn't allow major changes without administrator confirmation.

With this in place, a large proportion of malware programs will be forced to reveal themselves when they ask for permission to be installed.

Of course, they're not always named honestly – so beware of browser toolbars or "speed boosters" that look too much like a free lunch.

5) Be Wary Of Public WiFi

You'd be forgiven for assuming that Public WiFi spots should be safe. After all, you're using them in a reputable business, or a public utility such an airport. Unfortunately, public Wifi is notoriously insecure - unprotected networks are often the entry-point of choice for hackers seeking to gain access to your computer.

Many websites don't encrypt your data, and many public WiFi networks aren't up to scratch on the security front. That means that if someone has hacked the WiFi network - or worse, has set it up

deliberately to steal data - then your information is readily available, and it has the potential to be harvested by those with malicious intent.

There are a couple of things you can do to mitigate public WiFi risk. Firstly use your 3G connection where possible. If you have an ample data plan associated with your smartphone or tablet, tether it to your laptop and use that to access the net. It's likely to be much safer than the WiFi in a small shop or café.

Secondly, make sure you enable the highest Wifi security settings on your device. When you connect to a new network, most computers will ask you whether it's a Home, Office or Public network. Be sure to select Public! This deactivates network file-sharing, and it shields your private documents, files and media from prying eyes.

Multiple Safety Nets – The Answer to Watertight PC Security

The more layers of security you have, the more likely you are to stop any given virus, trojan or piece of malware dead in its tracks. Make no mistake, antivirus and firewall software are your first line of defence – but remember to implement the points above to really maximise your computer's security.

If you do, you'll have a good chance of getting several years of use out of your device while avoiding the misery of a nasty virus or data theft.