Nottinghamshire County Council

With many people using computers and smart phones daily, they are becoming more and more vulnerable to cybercriminals and hackers. It can potentially affect all types of computers.

There are some good articles, but we have adapted one which we hope simplifies things a little.

**1. Do you need to be connected to the internet all the time?**

If you have a computer running for long periods of time and you don't need to be connected to the internet, then it's a good idea to switch your internet router off. Hackers tend to prefer to exploit "always on" connections, and if your internet connection is more sporadic, you'll be less attractive to them.

**2. Make sure your router has a decent firewall**

A firewall is a piece of software or hardware that (simply speaking) lets the good stuff in and the bad stuff out. Most internet service providers offer a free router and modem when you sign up with them. Make sure that it has a decent firewall.

**3. Make sure your Computer or Device has a decent firewall**

Most computers these days have an integrated firewall built in to the operating system. For example, Windows has "Windows Firewall"

**4. Install Decent Anti-Virus Software**

Anti-virus software is a must for almost everyone. Yes, they may slow down your computer a little, but it will prevent being infected by a virus. You don't necessarily need to spend any money on it either.

These anti-virus applications have to be updated regularly. Also, if you use USB thumb drives or external hard drives, scan them for viruses- particularly if the drive belongs to someone else.

**5. Keep Your Computer Up to Date**

Make sure you check your computer for updates! These can be important security patches and you may be compromised if you don't install them.

**6. Be careful which sites you visit**

Some sites are there to deliberately get you. Be careful where you're browsing.


**7. Keep Your Password Safe and Hard to Guess.**

It's best to use a different password for each website your sign up to and be careful about saving passwords on applications on your computer.

**8. Use a Decent Web Browser**

Most people still use Internet Explorer or Safari for browsing. Google Chrome is highly recommended as your browser as it's been hailed as the most secure of browsers again and again.

**9. Don’t Trust Public Wi-Fi**

Did you know that a lot of your internet connection (web browsing and email) is being sent over the public connection unencrypted? Anyone in the coffee shop could potentially be listening in and stealing your passwords. If you have a 3G connection then use that, but if not, you’ll need to secure your connection. Websites that use https (Facebook and Twitter for example) encrypt your data, but most websites won’t. For this, you’ll need to use a VPN or virtual private network. This encrypts your connection by connecting to a secure server in the middle.

**10. Never Leave Your Computer Unattended**

I know this is obvious, but don’t leave your computer on if you’re not around.

Taken from and adapted from the original article 10 Tips to Make Your Computer More Secure By Ian Anderson Gray

https://iag.me/tech/10-tips-to-make-your-computer-more-secure/