Tips, Tricks and Advice from your local "IT Guru"

This month I want to talk to you about Malware. Malware can be a Virus, Spyware, or any other nasty that gets on your PC uninvited. The intention used to be to cause some sort of disruption, wipe your hard disk, pop up adverts, that sort of thing. Now the really bad ones try and keep hidden, quietly relaying passwords you type back to home, or staying dormant until called into action in some kind of co-ordinated attack. This means it's much harder to know if you are infected. Sure, there are still the obvious ones that try to get you to pay money and slow your system down drastically, but if you have one of the more furtive ones the first you could know of it is when you get a bank statement! Clever Malware can circumvent your anti virus, block updates, fool you into thinking it has been removed and stop you visiting known security web sites. In short, once this stuff is on your PC, it's not coming off without a fight!

So, how do you make sure you don't get infected? If you are using an Apple Mac then read no further as you're safe, but otherwise read on. First make sure Windows Firewall and Update is switched on and that Update is set to download and install automatically. You can find the settings for these in the Control Panel application of Windows. The reason having Update on is a good idea is because the bad guys examine every update Microsoft issues to see what vulnerabilities they have fixed and release viruses to exploit them, knowing that either people won't update, or that it will take time to filter through to most PC's. Next, get some sort of Anti virus/Spyware program, I recommend AVG Free from www.grisoft.com. You can pay for the likes of Norton, McAfee, Etc, but AVG does as good a job and frankly, I have seen so many problems caused by the big security suites that I would steer clear of them. I would also steer clear of third party Firewall software, they just add an extra layer of complication that's not needed. Finally, make sure you are using a router to connect to the Internet. This is a clever little box that allows you to share your connection between multiple computers in your home, but as a bonus, provides an extra level of protection.

All these steps should be seen as the last line of defence, though. Modifying your behaviour is the best defence. Don't open unsolicited e-mails, even if they look as if they come from someone you know. All those jokes and pictures that turn up in your inbox? Delete them, and tell your friends that's what you do, people will soon stop sending them. Don't click on links in e-mails. Be very wary about "pop ups" saying you are infected; one of the latest scams is to put up a false message saying you have a virus. Once you click on the remove button, you really are infected. In fact, even if you click on 'No' or 'Close', you still get infected. Safest thing to do here, even though it goes against all you have been taught, is to switch the PC off by holding down the power button.

If after all this you still get hit by one of the more nasty threats, the only option is to wipe the PC clean and reload Windows. Some say you can manually remove this stuff, but I've found it's easier, quicker and safer to start from scratch. After all, you are doing regular backups aren't you?

If you have any questions or anything you would like me to cover in this column, email me at look@4-11consultants.co.uk

David runs 4-11 Consultants, a local company specialising in home and small business computer problems and can be contacted on 01206736161