Home Computing: Seven Secure Steps

There's good news and bad news. The bad news is that it's almost impossible to prevent something nasty happening to your favourite PC, Mac, laptop, tablet or smartphone. The good news is that you can swing the odds in your favour by following a few simple steps.

1. **Stop unauthorised people using your computer**: Choose, use and keep confidential, good passwords; this will stop someone (even your children) using your device and obtaining access to your data and accounts by guessing or hacking your identity. A good password is more than eight characters and one that most people wouldn't guess, but that you can remember without writing it down. It's also worth considering fully encrypting the device, preventing anyone using it if it's lost or stolen. This is straightforward and several reputable firms offer free products. And don't leave it lying around!

2. **Update it**: Most of the important software on your device (the operating system, internet browser and protective software etc.) have automatic updating options, and most of the updates are to improve their resilience.

3. **Be suspicious**: Look for the unusual, don't click on links or attachments in emails that you weren't expecting, don't accept Facebook or other invitations from nice, honest people, but some unpleasant ones too.

4. **Make it difficult for hackers to get in:** Use a software firewall: this will prevent most common malicious software getting in. Most PCs and Macs have one installed as default, just make sure it is turned on. Even use one on your tablet and smartphone, they're usually free.

5. **Find them if they get in**: Install and run anti-virus software with automatic updating; this will help to detect and prevent most malicious software affecting you. Again most PCs and Macs often have them installed. Don't use the free ones if you can afford to buy one – these often have more protective features than the free ones. This is also available for smartphones and tablets.

6. **Keep a copy**: Back-up the documents, photos and other files that are important to you in case you have a security incident or your computer fails. An automatic backup or file copying programme is best, but you could just copy the files to a USB stick, DVD etc. once a day or week. Remember to keep this safe too.

7. **Clean it up**: when you sell or dispose of your device, either full format (do not quick format) the hard drive, or use wipe software to ensure all your information is completely gone. Wiping software can be found either in your security software or free on the internet. Also remember you might not legally be able to give away any licensed software.

© IASME Consortium 2013