Internet Security – some advice

The topic of computer security is similar to that of antisocial behaviour – it's continually 'in your face' as far as the media is concerned, but the reality is somewhat different. In the case of internet security, the conclusion of ***Which? Computing***'s survey (January 2011) is illuminating: ***Our verdict*** *The internet is like a big city. Stick to the areas you know and chances are you won't get into trouble. However, keep your defences up to date, just in case.*

So, what are these defences? Some of them are 'things' like anti-virus software while others are 'human factors' – how we use the system (what we do or don't do).

Antivirus software

There are a range of paid-for anti-virus packages on the market, probably the best, but most expensive, are BitDefender Internet Security 2011 (£40) and Norton Internet Security 2011 (£50). These packages charge an annual fee to keep them up-to-date.
Alternatives that cost nothing include Microsoft Security Essentials (only for recent Microsoft Windows systems) and AVG Antivirus Free Edition.

Microsoft Security Essentials	**www.microsoft.com/Security_Essentials**
AVG Anti-virus Free Edition	**http://free.avg.com**

Make sure your anti-virus software is up to date – free downloads should be enabled daily.

Antivirus scams

A number of organisations including police forces and Consumers' Association have warned of a rise in telephone scams involving initial contact by someone purporting to represent a telecoms or software company claiming to have identified viruses on your computer. Leaving aside for a moment how that could be possible, they proceed to offer advice during which the unwary can be tricked into divulging sensitive information such as credit card or bank account details. A similar issue can arise when visiting unreliable websites – a warning claiming to have identified viruses on your machine pops up. **Do not click on any icons** – even the close icon – but immediately close your web browser. Almost invariably nothing will be wrong with your computer, but just for peace of mind, run a virus scan immediately before resuming your online activities.

Firewalls

A firewall is a system that checks inbound and outbound traffic from your computer and both warns and blocks traffic that you have not previously allowed. The outbound aspect is particularly valuable since it prevents any intruder sending details out from your system – such as passwords, account details, etc.
A good, free, general purpose package is that provided by ZoneAlarm.

Zone Alarm	**www.zonealarm.com**

In the case of both AVG Free and ZoneAlarm Free, make sure you follow the free download options on their websites – they make in very easy for you to slip into one of their paid-for systems, so make sure you stay with the Free versions!

[Continued over…]

Human factors

Even with appropriate software protection, there are things that you can do to keep your defences up, some of which are:

1. Never open e-mails from sources you don't feel comfortable with; mail from banks that you've never dealt with or titled 'Dear friend' but from someone with an African-sounding name or with no subject line. All should be deleted **without opening**.
2. **NEVER pass account details, passwords to organisations in response to e-mails – no reputable bank, Building Society or utility would EVER request such information via e-mail.**
3. If you are purchasing online, check that the website's address has changed from http:// to **https://** when you get to their secure payments page.
4. Make sure your credit/debit card is protected by the extra layers of security provided by Verified by Visa or Mastercard SecureCode or similar.
5. Only make online purchases from organisation that you are comfortable with – generally those with well-known credentials or High Street presence.
6. Generally, do not pass-on those 'round robin' e-mails that arise so regularly – many have heart string tugging messages, or exhort by claiming something good if you forward it to 5, 10 or more other contacts. This is a common route by which viruses are spread, often unwittingly, or by which e-mail addresses are 'harvested'; hence the mass of unwanted advertising that follows.
7. Remember that wireless networks are particularly vulnerable to eves-dropping; someone with a laptop nearby could either listen-in or use your connection to access the internet unless you have set up all of the appropriate passwords to protect your system. If your password is still unchanged from its factory settings you will probably have the almost universal *password* as your password which any intruder could guess! Finally, switch off the wireless facility when it's not needed.
8. **Never store sensitive personal data (passwords, bank account numbers, etc) on your computer.** It is very easy to overlook this issue if you have a habit of keeping copies of correspondence on your computer. If you do, remember to delete key personal data from the copy you intend to store on your computer **before saving it.** This is a very common security loophole with serious consequences.
9. **Finally – do remember to backup your vital data at regular intervals** and make sure that you store these backups away from your computer – in the event of a theft you don't want the thief to scoop-up your backup disc/memory stick at the same time! If the data is financially important, look to store the backup(s) off-site; this could be with another family member or trusted friend or, in very important cases, a bank safe deposit box although this latter case clearly has financial implications.
   A standard backup procedure uses the grandfather/father/son approach.

Open source Software

Much of the software used during classes at our IT Group is *open source* which means it is free. The best place to access these packages – and others – is to go to our IT Group's website at:

www.cwitgroup.btck.co.uk

and go to the ***IT Links*** section.

Greg Herdman (updated 11 Feb 2012)