Staying Safe Online

The first priority is to ensure your computer is kept up to date and is well protected with regularly updated anti-virus software. Also don't store your banking passwords on your computer and change passwords regularly - just in case *(e.g. for ease of remembering you can keep same password but try it in reverse, or with alternate caps. and lower case, or exchange letters for numbers such as s=2 etc.)*

Beyond that, staying safe online is largely a matter of being careful what you click on and what you plug into your computer or connect it to. **Malware** *(a general term for all kinds of 'malicious software')* can only enter a computer via:

- an email attachment,
- by being downloaded from a website
- via connection with an infected device or system - e.g. a USB stick or a compromised network such as in a public cyber cafe.

But Remember:

The internet is an amazing technology offering enjoyment, great rewards and freedom to achieve many great things. Don't feel threatened by it but just follow simple common-sense precautions to stay safe.

Email Attachments

Even if you receive an email containing an infected attachment, Malware cannot transfer to your computer unless you open the attachment. The solution is therefore clear: NEVER open an attachment on an email unless you are confident of its source.

If you receive ANY email from an unknown source and wish to check it, a simple procedure is just to copy its subject line or a few lines of its body text into Google - if it is a scam you will not be the first to have spotted it!

Be suspicious of any email which asks you for personal details. Banks etc. will never ask you to check account details by asking you to click on an email link. Emails which do are often **Phishing Scams** *(i.e. attempts to get you to disclose bank account access details etc.)*. If you are ever in doubt, then ignore the email link and log into your bank account in the normal way or contact your bank and ask. Note that the appearance of the email, the address it appears to come from and the web link offered may all appear genuine - these are VERY EASY TO FAKE.

If banks and similar institutions do email you they will always address you by name and not "Dear Valued Customer" for example.

You may even receive an odd looking email which appears to come from someone you know. But it may simply mean that someone somewhere has a compromised computer with both your email address and your friend's email address in its Contacts List. The Malware has simply pretended to be one of the contacts at random and sent emails to all others - your friend may know nothing about it!

Look out for spelling mistakes and bad grammar - sure signs of a fake email.

Be wary of any offer to unsubscribe you from a service. Many spammers use this to create a list of valid e-mail addresses. If you are in doubt just delete.

You may get emails apparently from major retailers offering you free gift cards or vouchers for being a loyal customer or invited to take part in a survey and get them after. DON'T DO IT unless you have first checked with the retailer or tested it by submitting the subject line to Google for example.

And finally, remember the old adage, if something sounds too good to be true: it probably is!

Website Downloads

Unfortunately, just visiting a dodgy website can be sufficient to compromise your computer and this is why it is so important to keep anti-virus software up to date and a Firewall switched on. These help stop Malware getting into your computer in the first place. But none *(not even paid-for ones)* are 100% effective and that is why a regular sweep with MalwareBytes is recommended as a second line of defence.

There are many occasions when you will wish to download some information or a piece of software from the internet - there are many good things there - and often for free! Look closely at the web address (URL) to make sure it is the actual supplier or manufacturer you are downloading from and not some subtle variation of it - e.g. :

- hover over the suspect web address without clicking on it and read the actual URL you are being taken to at the bottom of your screen.
- many secure website URLs start with HTTPS and the page carries a small padlock symbol - never type your financial details into a website that does not start HTTPS.
- be very wary of any URL containing the @ symbol - everything to the left of the @ symbol is ignored so http://www.argos.co.uk@10.19.32.4/ goes to a URL numbered 10.19.32.4 and has absolutely nothing to do with Argos!
- in fact there should be nothing between the known URL and the first forward slash (/) or question mark (?) - e.g. http://www.amazon.co.uk.FakeURLGoesHere.com?sometext
- check every part of the URL against the one given on the real company's web site - e.g. http://signin-ebay.com/ IS NOT THE SAME AS http://signin.ebay.com/ *(dash instead of dot)*
- always try to download printer drivers etc. direct from the manufacturer and not via 3rd party suppliers - they are unlikely to be supplying for nothing! *(although sometimes you may have no choice).*

Even legitimate websites may try to offer you add-ons and extras you haven't asked for such as:

- search toolbars
- 'customised' home pages
- free trials for paid-for full versions
- additional features or related software you don't really need

Usually, these offerings are in the form of tick-boxes and, in the most pernicious cases, the boxes are ticked by default - so look carefully at each web page in turn to make sure you are not getting more than you asked for! There is after all, no such thing as a free dinner!

Connecting with External Devices

Plugging in a USB stick, connecting to a public network or even inserting a home made CD or DVD can expose your computer to malware just as if you were visiting a dodgy web site.

You should know and trust the source of any USB stick, CD or DVD you introduce into your computer and never save personal details on any computer connected to a public network - such as a cyber cafe when on holiday for example..

Your anti-virus software and Firewall will protect you as when you visit dodgy web sites, but best to avoid the problem.

Social Networking

Applications such as FaceBook are essentially websites and so the same precautions should be observed. In fact, anti-virus software is becoming so effective that spammers and the like are increasingly turning their malevolent attentions towards these new opportunities.

G Howard March 2015