Staying Safe Online – The Risks

Of course the ultimate way to stay safe online would be to ditch the computer and cancel the broadband connection, but for most of us this clearly isn't an option. The majority of people in the UK (and in deed most developed countries) now use computers or internet connected devices on a daily basis be it for work or leisure. Many of us buy products online, bank online and share personal information freely on social networking sites. This is data and information that can be very valuable both to legitimate companies looking to target marketing at you or to criminal organizations and individuals with more sinister intentions. There are many different risks in the online age but here are a few of the most prevalent:

- Malware (see separate sheet for more information)

- Phishing – By which criminals pretend to be legitimate companies. For example you might receive an email that says it is from your bank but the web links actually lead back to a clever duplicate designed to try and capture your passwords and bank details.

- Identity theft – not just an online threat (don't throw out your bank statements or utility bills without shredding them) but this can be the aim of much malware and phishing scams.

- Scam calls and emails – you may have been plagued of late as I have by calls from an Indian sounding gentleman who says he works for Microsoft (or your ISP) and wants to access your computer. Hang up they are trying to get your credit card details. Similarly I wouldn't trust any emails asking why you haven't claimed your Nigerian lottery win.

- Scam websites – if a deal seems too good to be true it probably is. If you haven't heard of a website before making a major purchase research them a bit first on google and look for reviews and recommendations from trusted sources. Goods from these websites are often fake, illegal or won't show up at all. Gigs and sporting event tickets are particularly used in this form of scam.

- Hoax virus/scam emails – sometimes you might get an email from someone you know warning about a particular virus or malware doing the rounds. Usually these are not genuine and the main purpose seems to be to create a bit of a scare. However some have included instructions on changing settings and deleting files to avoid getting infected, don't follow these instructions as they are likely to cause damage to your operating system.

- Facebook (and social networking) – love it or hate it Facebook is very popular and with 1.11 billion people having an account it's too much of a temptation for criminals and hackers not to try and scam, phish or infect you. Be wary of Apps on Facebook that want a lot of access to personal information and be wary of clicking links on posts from friends about amazing deals or giveaways.

- Email account cloning and hacking – if your email account is hacked or cloned you may find some of your contacts emailing you to say they have received spam from you. Hopefully you

should be able to recover a hacked account by contacting your email provider and resetting you password. Make sure your device is free of any malware before doing this as it may be this was how you were hacked in the first place. Cloning or Spoofing is much more annoying. It means that someone has used software to make it appear that their spam emails have come from your address. They don't necessarily need to have hacked your account for this to happen and there is not much that can be done to stop it.

- And finally, from a business perspective here are a few more things to keep you awake at night:

Hackers trying to compromise your network, Hackers trying to compromise your website, fake / scam business opportunities, complying with the data protection act, having a formal security policy.

Malware

Malware is the collective term for all malicious software that can get on to a computer, phone or tablet device. There are many different types of malware, the majority is written with the chief aim of financial gain by criminal groups or individuals. Although some malware is designed by hackers to try and attack and disrupt large corporations or governments for ideological reasons.

Below is a brief summary of the main types.

Viruses

Computer viruses are so named due to their ability to self replicate and spread around an infected machine or network. The different symptoms and signs of infection are many and varied, ranging from a crashing or frozen machine to no noticeable symptoms at all. The infection will be initiated by user interaction i.e. opening an infected email attachment. Most modern viruses are written to try and avoid detection by anti-virus software or will attempt to disable anti-virus programs completely. It is essential to keep anti-virus software up to date so that it can recognise and deal with new threats.

Worms

Similar to viruses, worms are malicious code that actively seek out new ways to spread itself from machine to machine over a network or the internet. The only real difference being that they do not need any user interaction to execute. They exploit backdoors in software or poor security to spread themselves.

Trojans

Trojans are maliciously written programs disguising themselves as or within legitimate and desirable programs. When installed they can intercept and delete data and open up backdoors to download other harmful software through such as spyware.

Rootkits

This is the collective name for viruses, worms or other harmful malware that attempts to hide itself from detection whilst taking over control of the machine. They can be particularly nasty to get rid of as they set themselves up in hidden folders or partitions and are disguised as legitimate processes or services and often overwrite key files in the operating system.

Spyware

Spyware is software that will attempt to gather information and data about the user without their knowledge or consent. i.e monitoring your internet browsing history and keystrokes to attempt to get bank or credit card details. Spyware is often downloaded from the internet bundled in with other legitimate software.

Adware and Browser Hijackers

Annoying software which, like spyware is often bundled with other legitimate software. Sometimes it is even legitimate software itself and will pop up to tell you it is about to install, they seem to rely on confusing tick or untick options in the setup to get installed.

Once this has happened they monitor you web browsing and pop up annoying adverts, change your home screen and hijack your search results. The legitimate kind are usually very easy to get rid of. The other kind is trickier and is normally a sign of another infection such as a virus or rootkit.

Ransom Ware

Malicious software that can pose as anti-virus software and tell you that you have an infection or could even lock up your computer completely. They then say they will remove the virus or unlock the machine if you pay them a fee. One big example of this was the Metropolitan Police scam which completely locked up a computer and displayed a webpage claiming your computer had been used for criminal activity and you needed to pay a fee to reactivate it.

Botnets

Refers to a network of infected machines (often called zombie machines) that can be controlled by hackers or criminals to send spam email or overload web servers with traffic causing them to crash.

Phishing

Not malware in itself but worth mentioning. These are websites posing as legitimate sites, such as your bank or a trusted retailer, they to try and steal your login and/or financial details. If you find you are regularly coming across phishing sites it could be a sign that your computer has another form of malware infecting it.

Staying Safe Online – Top Tips

- Install Anti-Virus Software. Good examples of paid for anti-virus include Kaspersky, Bitdefender and Norton. There are also free options available two of the best known are AVG free and Avast which offer good basic protection but without some of the extras you get with the paid for programs. (Microsoft also offers its own free protection called Microsoft Security Essentials or Windows Defender depending on your version of windows, although not as well regarded in the industry as AVG or Avast the new windows 8 only version is pretty good)

- Make sure you have an active Firewall (Windows and Mac have their own built in firewalls, some antivirus packages include their own firewall as part of the package)

- If using a free antivirus program pay attention when installing as some may try and install optional extras that are often not helpful. Un-tick the box or decline the service when installing.

- Don't assume you don't need Anti-Virus if you have a Mac. Apple actually advertised this as fact until last year but was forced to change its policy after the "Flashback" botnet struck hundreds of thousands of machines. More Mac specific viruses are appearing and as they get more popular more and more hackers will target it.

- Don't install more than one anti-virus program that feature active monitoring – they will conflict and slow down or even crash your computer. For peace of mind there are other anti malware programs (such as malwarebytes free edition) that can offer good on demand scanning options without conflicting with your existing protection.

- Use strong passwords (the best passwords use a combination of upper and lowercase letters with numbers or allowed punctuation – for extra security don't use dictionary words). Also it is advised by some to use a different password for every website and services you use.

- Stay up to date (make sure the operating system ie Mac or Windows is set to receive automatic updates. This is also applicable for mobile devices like phones and tablets as more viruses are appearing for these devices)

- Have a regular back-up policy for all your important data.

- Turn on system restore in Windows and time machine on Mac

- Make sure other software is up to date, especially make sure the antivirus program is set to receive automatic updates to the virus definitions database. (other software to keep up to date include Flash, Acrobat Reader, Java, Skype – hackers regularly target out dated versions of applications that have security issues)

- Use an up to date web browser (Internet Explorer is the most commonly targeted and least secure but Chrome and Firefox are not immune)

- There are many useful plugins for Chrome and Firefox such as Ad-Blocker that can help you stay safer online as well as eliminating annoying pop ups.

- Take advantage of private browsing and do not track options in the browser.

- If using public wi-fi consider using VPN software (this encrypts your connection and makes it much harder for hackers to try and snoop on your connection)

- As far as possible make sure you trust sites before giving out credit card details or download software from them. (look for a pad lock symbol and/or an https:// addess in the address bar – this shows the site is using encryption)

- If in doubt about a site, link or email attachment don't click it.

- If you think you have malware on your device do not use it for sensitive tasks like online banking etc.

- If you think you may have malware and haven't got an antivirus program installed then you can try and run an online scanner through your web browser. Housecall by Trend Micro is a good example of this.

- Don't leave paper printouts of online account details lying around and shred them before disposing of.