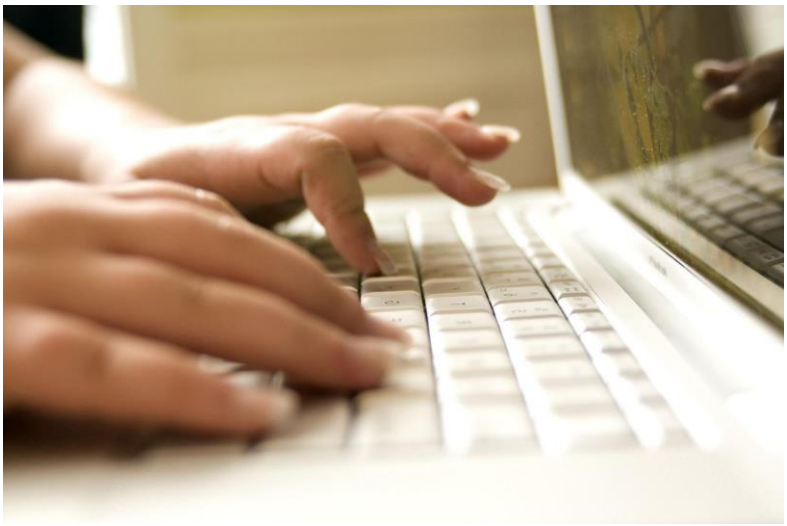
Bewick Consulting

A Simple Guide to Staying Safe Online

Note: this is an abridged version of a presentation/ workshop session put together for older adults.



Introduction:

There's one sure way to ensure your computer does not get infected by virus, and you don't receive spam, hoax emails, suspicious offers or other malicious contact.

Don't connect to the Internet.

That **highly** restrict your use of your home PC or Laptop and given that more 39% of people aged 75+ have used the internet in the last three months, this short document is assuming you want to do so to, and will look at some of the more common types of threat you may see out there, and offer some advice on how to avoid them.

The table below shows that the proportion of people aged 75+ who have used the internet in the last 3 months has nearly doubled in the last five years (from 20 per cent to 39 per cent), and increased by around a half for those aged 65 to 74 (from 52 per cent to 74 per cent). However among those aged 75+, around three-fifths (61%) are still non-users.

It's intended to be jargon-free, but some technical terms are unavoidable so I've provided a short explanation at the end of this document.

One final note: I have worked in Digital Marketing for 25+ years and sat on councils for cyber safety. I am not however a lawyer so please do not take this advice as legally binding in anyway.

A very brief A-Z.

There are many types of dangers online – but not enough that should put you off using the internet. Some are just annoying, others can be more malicious – looking to get hold of your personal data, bank details or to pay for something you don't actually want.

You may hear terms such as phishing, hoaxes, viruses, malware, scams, bots and many more. I'll try to outline simply what these terms mean and give a few examples of what you should look out for.

Anti-Virus software:

You should definitely use anti-software. When you buy your computer or laptop you may find that you get an initial free trial of one. You may also find the salesperson will recommend a certain package. Whether you buy it from them or not is completely up to you, but you should buy it – and as soon as you intend to using online services. There are many options.

They will provide different levels and services in terms of what they will protect you from and how they do it: the best ones will act in the background and require you to do very little. They will warn you if you try to use sites it thinks are a risk, and it will run checks automatically for you. It is possible to find free anti-virus programmes, but if there is one area you should be ensuring you have the best safety in it is this one. You can find advice on what the best paid and unpaid services available are on many sites: I'd suggest this one: https://www.techradar.com/uk/best/best-antivirus

Browser:

If you are looking for technical help one of the first questions you are likely to be asked is "What browser are you using?" the browser is the program your computer is using to look at and display the information on the web. You may find your computer comes with a browser ready installed. Each will make things slightly different in look and feel, and some work better depending on the type of computer you are using. Common browsers include Google Chrome, Mozilla Firefox, Microsoft Edge and Explorer. You may find you have to update your browser for safe use: but be sure that any requests to update are genuine (by checking the sender, the security level, the wording and other methods described in this document), as messages saying 'your browser needs updating' are common phishing techniques.

Passwords:

Once you have your computer you will need to start thinking about passwords. Many of the sites you will need a password for (Facebook, Amazon, your bank, your email provider etc.) are becoming stricter about how complex your password is: it's no longer enough just to use your first name, or enter '*password*'. Many sites will now require at least 8 characters, including at least one number and one special character. Five key things to remember about passwords:

1. Try not to use the same password for multiple sites. This can become difficult when you use lots of sites, but it is important to vary them.

2. Obvious passwords include relatives' names; often with their age- avoid these.

3. Don't enter your passwords on a public, unsecure Wi-Fi network.

4. Don't share your password, or tape it to your computer, or keep it on a pad next to computer…

5. You also need a password for your home broadband service: details on how to set up and store a password you'll remember will be available from your provider. DO NOT leave it publicly open.

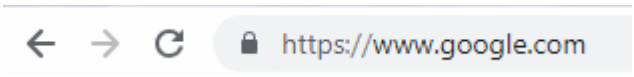
Three suggestions on how to create a difficult-to-crack password from McAfee- one of the leading anti-virus companies:

- *Make strong passwords which are easy to remember but hard to guess. Iam:)2b29! — This has 10 characters and says "I am happy to be 29!" I wish.*
- *Use the keyboard as a palette to create shapes.* ***%tgbHU8****- Follow that on the keyboard. It's a V. The letter V starting with any of the top keys. To change these periodically, you can slide them across the keyboard. Use W if you are feeling all crazy.*
- *Have fun with known short codes or sentences or phrases. 2B-or-Not_2b? —This one says "To be or not to be?*

Secure sites:

A first step to knowing whether a site is reputable or not is to check its security. You can see this easily in the address field at the top of the web page: A secure site's address will start with **https**: the 's' at the end stands for 'secure'.

So for example, Google's address looks like this:



You'll notice a locked padlock before that address. This shows it is a secure site.

Where a website does NOT have an 's' at the end of the http it indicates it is not secure. Depending on the browser you are using this may appear slightly different, but in Google Chrome it looks like this:

NOTE: the https:// and padlock do not 100% gaurentee the site is safe, but if they are NOT there, it is a big indicator that the site may have issues.

System:

You may also get asked about your system if you are requesting technical help. You may also get requested to 'upgrade your system' or elements of it by emails or messages on screen. It's possible you may have to update certain programmes. You shouldn't ever have to change your 'system', but in any case you should be wary, as it is another common phishing method. You can always check what edition system you have in Windows by clicking on the Start icon in the bottom left corner of your screen, type "msinfo32" into the search box, and you will see details about your computer appear, including 'Version' near the top of the page. This screen can be useful if you ever find yourself having tech jargon thrown at you.

Common Annoyances and Dangers:

Spam emails:

Spam emails are annoying, a waste of time, and everywhere – more than 95% of all emails sent in the world are estimated to be 'spam' (The origin of the term comes from the Monty Python sketch where the customer gets spam with everything…spam, spam, spam, spam…). Spam is normally sent out by companies to advertise. The companies will gather email details from accessible sources – some general, some sold on by sites who have collected your details and then pass them on (illegal in most cases, but difficult to prove). The legality of Spam varies from country to country. Email Providers become better and better at spotting SPAM emails and many you will never even see as they'll just go straight to your inbox. However, the Spammers also get 'better' and constantly modify their emails to hide the fact they are spam – this might be through their email address or the subject line that they use. It's very easy using software to make an email look person in its subject line.

One note: Junk folders or Spam traps used by email providers are not perfect. You may occasionally need to check yours just to make sure everything going in there IS spam. You can mark email senders as 'safe' to ensure they don't end up straight in your Spam box.

Spam emails tend to be annoying and normally irrelevant, but not, for the most part 'dangerous'.

Phishing emails:

Are more dangerous than SPAM.

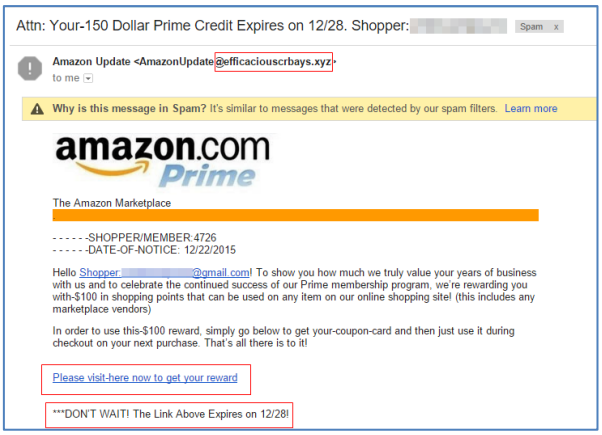
The sender will pretend to be a well-known company or a person/ group you know.

They will send you an email with the aim of either gathering more information about you, or encouraging you to click on a link which will take you to a fake site where they will ask you to enter more information about yourself, or potentially to download viruses to your computer. Some of these emails may look authentic, using company logos, products and may use an email address that looks like the company they are pretending to be.

Here is one example, supposedly from Amazon (image courtesy of Heimdal Security)

Things to look out for:

- The email address may look like the supposed sender but will often feature additional letters/ numbers.
- They ask you to provide personal details (which the real company would already have)
- They ask to click on a link.



HOAX emails:

Hoax emails can be cruel, malicious, financially or personally dangerous, and often a combination of all these things.

It's impossible to list all hoaxes, and new ones do spring up frequently. It's also impossible to give exact examples, as the senders will often change certain details in them to reflect their own aims or the interests they think the person they're sending to might have.

But here are some common variations:

Someone is in need of money because they've had an accident of some sort.

Often a relative or friend on holiday or business who has been hurt or attacked and desperately needs money wired/ sent to a bank account. Sometimes this will be a generic name of someone you might know (like SPAM – the sender will send so many out, even if only one person in 1,000 actually has a relative or friend named John, it will be worth it for them.) Details will be sketchy and time will be urgent so you won't have time to ask too many questions to verify the person's identity.

You've won a competition/ been left money/ been contacted by a person who wants to give you money…but just need to pay a small administration cost.

Some of these are obvious: the clichés of the Nigerian Prince, who wants to send you his rewards, or the last remaining survivor of a dead member of royalty or celebrity, are very common and easy to spot, but many are more subtle. If you don't remember entering a competition, you won't have won it. Even if you do – any competition that asks you to pay fees before getting your prize are not on the level.

Official Summons for Payment:
Often, but not always, speeding fines. This may be left on your phone or by email. It will state urgency, and you can reduce that considerably by quick payment. Don't. The police will always send by post. It might seem convincing – especially if you were on that road around that time. But again, millions of these emails are being sent out…someone had to be.

YOUR COMPUTER IS AT RISK!
This may come as an email or a pop up message. You will be told to click on a link to update to be safe. The link may even look official: Important Update for Windows the words in a link do not mean anything: this important link can go to the same place as this elephant shaped thing that doesn't mean anything

A tip*- hover your mouse over a link and you'll see the real address it is trying to take you to – you can try it with both of those links above.*

Secret Shoppers
'Survey' companies who offer money either to become a secret shopper, or to fill in surveys – which may start out very general, but will slowly start to ask you more and more personal information. These may also appear as 'free gifts' on offer

PPI
Opportunities to claim on PPI owed. These are starting to slow down and being replaced by NatWest owing you money, Travel Companies who owe you compensation etc.

Security issues on your account:

They will tell you there is a problem with your account and you need to address it now. How do they know you're a member of NatWest or whichever bank you use? They don't – but if they send out a million emails, the odds are they're going to hit some people who are. A bank will never ask you to provide PIN or other data sensitive information on line in this way. You may get similar messages saying your email account is at risk of being suspended, your PayPal account, Apple account etc.

And a final note…

It's not just while you're on your computer you may face risks – three of the most common telephone scams at the moment include:

A problem with your Windows computer:

The caller will claim to be ringing from Windows because they have picked up virus issues on your computer. They will try to get you to log on to your computer and give you complicated instructions to open up a computer log which will show you have errors. There is not a Windows support team. They will not ring you to tell you you have a problem. The screen they will show you on your computer is completely normal and does not mean there is anything wrong with your computer. Do not engage with them. Just put the phone down.

The Accident phone call:

Not strictly computer related but worth mentioning: the caller will say they are ringing about the accident which you were involved in which was not your fault. They will say they got your details from 'the public record'. They do not know anything about you: again, they are counting on the odds being that if they ring enough people someone will have had an accident and believe it is not their fault; they will then try to engage you in a claim.

5 Useful websites with detailed information:

https://www.connectsafely.org/seniors/: general safety guide for older adults

https://www.avg.com/en/signal/website-safety: a range of safety tips for using online and ensuring the sites you are using are safe.

https://www.ageuk.org.uk/information-advice/work-learning/technology-internet/internet-security/ : age UK's site offering advice on various aspects of the web.

https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/10-tips-stay-safe-online/: McAfee site, quoted from in the article.

https://www.snopes.com/ (This searchable website details thousands of rumours/ stories/ hoaxes and outlines whether they are real or not: useful for everyday life as well as online!)

Bewick Consulting

simon@bewickconsulting.com

www.bewickconsulting.com

Linkedin.com/in/simonbewick