Home, Computer and internet security - Behaviours

- Don't forget – the internet is global, your house router (indirectly your computer) is accessible to every other computer and potential hacker/criminal on this planet
  - Don't invite them into your home and let them spoil your life
- Sadly, today, we have to be responsible for our own home, bank accounts, credit cards, purchases, medical, computer and internet security
- **ALWAYS CHECK HERE for more information** >>> https://www.actionfraud.police.uk/
- **Also here for COVID scams** >>> http://covidfraudhotline.org
- Its is as much about our behaviour as it is the technology – but it is both
- You cannot have convenience and security, to improve your security you must accept greater inconvenience – it will be 'less easy' but you will be a safer
- You cannot get 100% security/safety but you can greatly improve it with some basic steps
- Think! Don't be rushed, think first, act slowly, scammers try to make you panic/act in haste
- Microsoft wont call you about your computer or internet - its a scam
- The NHS and Police do not charge or ask for financial information – its a scam
- Callers offering pensions/investments – its a scam
- Callers saying your credit card has been compromised – its a scam
- Banks will not phone to ask you to transfer your money – its a scam
- BEWARE of fake sites REAL www.nhs.uk and here is a FAKE nhs.gov.uk
  - Criminals can make up 'real looking' websites and try to lure you to them
  - ALWAYS check and ask yourself 'is this the real site'?
- Know exactly who you get your phone and internet service from
  - Only call back to numbers **from your paperwork**
- Know exactly who you bank with and have credit cards with.
  - Only call back to numbers **from your paperwork**
- Scammers/hackers don't care, they **will take all your money** if they can or if you let them
  - They live in countries where the law can't or wont get them
  - The Banks can't or wont always give it back and worse, the criminals still get the money to make more misery for everyone

SO - DON'T let them get your money

You may need some help to add some of these protections but you can always use the behaviours

There is a lot here but I hope some of it helps

There is a second document covering additional measures you can take

Home phone calls

To greatly reduce and often completely eliminate nuisance and scam calls. Get a call screening phone. These phones answer calls and check the calling ID (the number calling you).

- If its one of your ‘known numbers’ it then rings your phone
- If its a blank number or one not one of your known numbers, it plays a message asking the caller for their name/number etc. or takes a message. Scammers give up here
- This in almost 100% of cases, stops the calls – dead
- Remember that unfortunately with modern digital calls the calling number displayed can actually be set to anything by criminals. They wont ‘spoof’ your family numbers but they might a Bank for instance
- The nuisance calls mostly come from abroad and the telephone preference service cant block them – you have to police this yourself – use a call screening phone
- Guard your phone number, limit who you give it to

In any case, don’t ever give any personal data, account / card numbers etc. to anyone that just calls you. DON’T ever transfer any money from a phone call. Don’t respond or press keypad buttons if asked. Just clear the call.

If you want to call your bank etc. use the number from your paperwork, **never** a number you have been given by a caller. Wait at least 30 minutes before using the phone again or use another phone to call your bank. Don’t get panicked into doing what **they** want. Keep control, think first.

Mobile phones

For greater privacy, turn off your bluetooth, wifi location and data when you are not using them and never use open wifi hot spots – just use your phones data it is far safer

- Never do any banking or financial transactions when you are connected to any ‘hot-spots, airport, cafe, Hotel wifi etc.
- You must be extremely careful with any ‘Apps’ you install, especially from the Android Play store. Both Google and Apple check these ‘Apps’ but bad ones do get through.
    - They can and do, collect information, show adverts which you can accidentally click on and you really don’t know what else they are doing and the Apps will never tell you. Even a ‘torch light’ app can have tracking and adverts
- Try to find and use only reputable Apps
- If in doubt – don’t install something

Better still is to install a VPN – Virtual Private Network – this is covered in the advanced document

Text messages/social media - behaviour

- Don’t give away your personal information, be careful what you disclose on social media
- Enforce your privacy – the internet is global – its your privacy
- Don’t click on any links or fall for scams given in text message – think – check elsewhere to find out what typical scams look like. The criminals always try to mimic and trap people with topical subjects – like COVID and the NHS Track and Trace procedure.
- Check known good websites, like Which, Action Fraud, the BBC and a genuine NHS or your doctors website. Sadly, you have to do this in the modern world and protect yourself.
    - The NHS vaccination notification MAY come in a text message and that is why the criminals are targeting people at the moment. You may have to click on this link BUT be extremely careful where it takes you. Check, if it asks for personal information (passwords financial etc.) it is a scam – don’t enter any details and delete the message
    - DON’T press any kepad buttons if you are asked to “to accept the vaccine appointment” for instance – the criminals then try to charge money from your phone
- Don’t click on any links or fall for scams over social media etc. – think – check elsewhere
- Delete any such messages – your life wont get worse by missing something funny or stupid but it might if you click links

email - behaviours

- Remember **all email is insecure**
- It is <u>not</u> checked for who it came from or where its going or that it arrived
- It is just a very simple, text based ‘electronic post’ system
- The FROM address can be changed by <u>anyone to anything</u>. So it might not actually be from your bank, a company your Son, Daughter, Mother, Father etc.
- Scammers copy Bank/company looking emails so because it ‘looks like’ a Lloyds Bank email, it might not be. Never respond with ANY personal details
- Never transfer money to accounts given in an email, especially from estate agents and solicitors during a house purchase or builders or any purchase. Always check the account numbers by phone to a number on your paperwork – not one given in the email
- DON’T ever login to a company or a bank from an email link because it is highly likely to be a criminal one. Logon to your bank/company/doctors directly from your browser and a Password Manager is even better (see advanced document)

<u>DO NOT EVER CLICK ON LINKS IN EMAILS</u>

<u>This is probably the single most common way people get scammed/hacked</u>

If your Son sent a funny email with a link, **phone** them first, but realise that even if it did come from them, it may still be **BAD**. If its a youtube video for instance, ask them what you should search for using youtube

The internet – browser

Together with email, this is your main connection to the internet for email, banking and shopping and it is therefore a primary target for scammers and hackers as are all the web-sites.

- Google chrome, Apple Safari, Microsoft Edge, Mozilla firefox
  - These are all good browsers, the companies try to keep them secure but they do all have weaknesses that can be and are exploited all the time
- When you search for something, you must be very careful what you click on, look carefully first.
  - If the link is in a sponsored advert section – don't click
  - If the text does not look right – don't click

DON'T allow your browser to remember passwords or other 'auto-fill' personal data. This is because browsers can be tricked into releasing this information by bad web sites. If a 'good' web site can get it – then so obviously can a bad one!

Can you see the difference below

lloydsparmacy.co.uk

l1oydspharmacy.co.uk this one will steal your credit card data

lloydsbank.co.uk

l1oydsbank.co.uk this one will steal your money

This is just a simple example, much more crafty methods are used to get you to go to a criminals website, it will look exactly like the legitimate one if the criminals are good at it - and most are. Its their day job and they scam millions of pounds from people in the UK

- Don't store passwords in any browsers – use a good (non-cloud) password manager
- Don't store any 'auto-fill' data in any browsers (i.e. your address credit card numbers etc.)
- Find the setup/preferences/options and try to find the section on 'store passwords'
  Set this to off/no/never
- Find the setup/preferences/options and try to find the section on 'cookies'
  Set this to delete cookies on exit
  Set block 3rd party cookies if there is an option for this
- Find the setup/preferences/options and try to find the section auto-fill
  Set this to off/none/no

- Find the setup/preferences/options and try to find the section on ‘search’
    - Set this to DuckDuckGo and remove the others. DuckDuckGo does not keep or use your searches and therefore reduces tracking and spying on your searches

Passwords

These are a modern scourge – but they are the most common and important method to access an account.

- Don’t forget – your house / computer is available to the planet and so are all the web sites you visit – therefore our devices and website are targets of hackers and criminals
- YOU MUST HAVE A SEPARATE PASSWORD FOR EVERY ACCOUNT
- NEVER RE-USE A PASSWORD ANYWHERE
- THEY MUST ALL BE at least 12 (more is better) characters with a mix of upper, lower case, numbers and 1 or 2 of the basic symbols (like # * & $ % @ etc.)
- THEY MUST BE RANDOM no names, words, numbers used as letters etc.
- In my opinion to manage this you <u>should</u> use a good password manager, but a spreadsheet or word document with a password is ok. BUT it wont generate high quality passwords for you
    - it must not be ‘on the internet’/cloud or whatever
    - you must store all your (correct) web site addresses (the login page) and corresponding usernames and passwords in the password manager (or spreadsheet / document)
    - storing the login page address of each web site (called the URL) in the manager means it will only ever take you to the <u>correct address</u> and therefore avoid the l1oydsbank trap
- Passwords for say any non-purchasing account (like the BBC) that has no personal data can be simpler but even then these do get hacked and the email addresses taken and used to target people. Make it 8 to 10 memorable of at least characters and numbers

Finally

It is difficult but its better to keep yourself informed about typical and current scams on the internet, email and phones. If you are aware and prepared – then you are much less likely to fall victim to the criminals. Being aware of what they do, what is possible, how they trick people is key to keeping safe.

The internet was not originally designed for what we use it for today and so it makes it very difficult for the government to control bad websites – they are trying all the time but it will always be ‘after the fact’.