DO's for Safety/Protection

- ✓ **Create** strong passwords that also include at least a numerical value and a symbol, such as #, to foil password-cracking software. Avoid common words, and never disclose a password online. Opt for Access code if available
- ✓ **Change** your password frequently.
- ✓ **Physically** secure your laptop/mobile/iPad etc
- ✓ **Delete** any message that refers to groups or organizations that you are not a part of.
- ✓ **Download and install** software only from online sources you trust.
- ✓ **Never** click on a link from an untrusted source.
- ✓ **Close windows** containing pop-up ads or unexpected warnings by clicking on the "X" button in the upper most right hand corner of that window, not by clicking within the window.
- ✓ **Use antivirus software**, and update it on a regular basis to recognize the latest threats especially when requested.
- ✓ **Use** a strong separate password especially for online payments e.g. shopping, eBay, Amazon and social media sites.
- ✓ **Make sure** your Firewall is turned on.

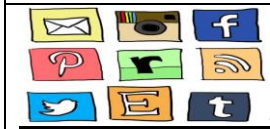
DON'Ts for Safety Protection

- **Never** write down your password. Especially on a Post-It note stuck to your computer!
- **Never** give out your password to anyone, whether you know them or not.
- **Never** select the "Remember My Password" option. Many applications do not store them securely.
- **Never** purchase anything promoted in a spam message. Even if the offer isn't a scam, you are only helping to finance and encourage spam.
- **Refrain** from opening an e-mail /text attachment, even from someone you know well, unless expecting it and never from an unknown sender.
- **Avoid** creating common passwords such as your name, pets name, birth date, home address etcetera.
- **Do not leave** your laptop/phone unattended, even for a few minutes.
- **Never** reply to e-mail(s) requesting financial or personal information. Your bank HMRC etc will never ask for these including PIN, Card Verification Code (CVC) etc
- **Refrain** from clicking on the close button within pop-up ads.
- **Never** pay by bank transfer (no protection) use PayPal or Creditcard.

Suspicious e-mail: Hover mouse over link to see country of origin (e.g. .ga Gambia .uk United Kingdom)
Suspicious link: Does the link match the e-mail given?
Mis-spelt words/incorrect use of language: **DO NOT OPEN. DELETE**.

Browsing

Look for the green padlock and https. Anything else is unsecure, not verified, and suspicious or not correct.
If possible use **Private Browsing** (Control /Shift /N - - You've become incognito) **for Internet banking** (no trail for anyone to hack into). Using this will not save: visited pages, cookies. Temp. Files or searches but will save; bookmarks, anything downloaded and anything copied. NOTE; plugins may ignore this setting (flash, Youtube will over ride Private Browsing.)



Social Media/Mobile

Don't use public WiFi – cafes, pubs ,hotels, trains etc for anything confidential including logging into any account.
Being given an access code is not necessarily secure.
Use well known commercial hotspots – BT Open Zone or T-Mobile. May be slower but is safer!
Use a unique password for each social network.
Never be too personal in what you say or photos you post.
Use the block button to avoid spam with links.

Keep your personal and financial details safe. Do not be tricked into giving away these details no matter how authentic it seems.

Don't be rushed into making a decision. A legitimate request will always give you thinking time and won't mind waiting.

Listen to your instincts.

Stay in control. If you feel 'pestered' then quote the Data Protection Act i) consent has not been given and withdraw immediately ii) state 'Right to be Forgotten' iii) contact Information Commissioners Office: https://ico.org.uk/make-a-complaint/ (this could be nuisance calls, personal information concerns, cookies, internet search results)

Hang up if on the phone. Remember you have the upper hand at all times.

If in doubt

Under no circumstances CLICK....

You should **DELETE** or **SEARCH INTERNET** for further information.

If it looks too good to be true then it probably is!

To Report or Find Information:

www.actionfraud.police.uk

www.net-aware.org

www.getsafeonline.org

www.takefive-stopfraud.org.uk

www.haveibeenpwned.com

WHITBY WHALER U3A

Whitby
"WHALER"
U3A
THE UNIVERSITY OF THE THIRD AGE

Staying safe online –

Talk given by **Mike Jackson**
Saturday 9th February 2019