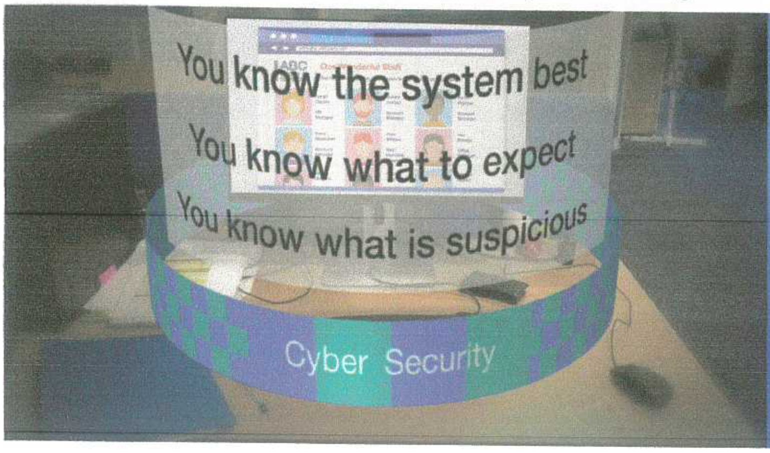
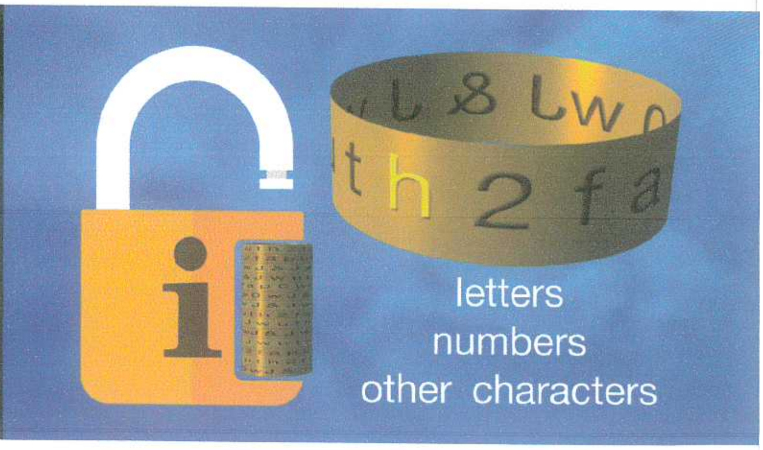
Cyber-Safety Best Practice - DOs

- Use strong passwords.
- Use different usernames and passwords for different sites.
- Read and comply with any policies or procedures your organisation has in place.
- Check unexpected emails before opening attachments or clicking on links in them.
- Set a password or code for ALL mobile phones, laptops, PCs and tablets.
- Store devices securely when not in use.
- Log off your computer at the end of the day.
- Lock your computer before leaving it unattended.
- Activate the 'lock' function on work mobile devices.
- Before using USB drives, make sure they're safe.
- Make sure your computer is getting antivirus updates and patches.
- Keep regular backups of the data stored on devices.
- Follow an 'incident management procedure' for lost/stolen devices.
- If your computer isn't performing as it normally does, report it.
- Comply with security and privacy laws, copyright and licences, non-disclosure agreements and contracts.
- Dispose of all storage devices containing restricted or sensitive data securely.
- Report anything that seems suspicious.

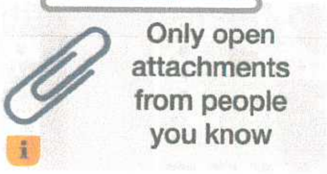
Tip: select the Windows Key + L on your keyboard to quickly lock your laptop or PC.

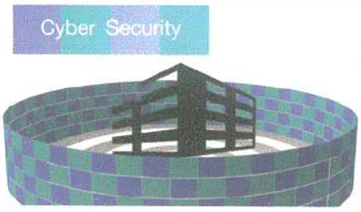
Remain vigilant and ask your manager for advice if anything's unclear!



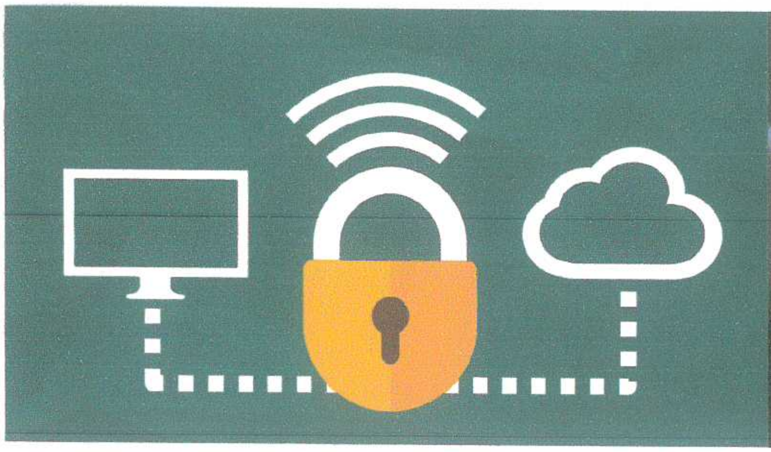


Cyber-Safety Best Practice - DON'T's





- Don't write passwords down where they can easily be seen or found.
- If in doubt, don't open any attachments, or click on any links in emails.
- Don't ignore system warnings, e.g. 'expired antivirus software'.
- Don't disable antivirus protection software.
- Don't visit a website that's 'untrusted'. A browser may display a red padlock or a warning message stating that "your connection is not private".
- Don't leave devices where a thief can easily steal them.
- Don't use your own device for work, or your work device for personal use, unless it's been authorised.
- Don't allow anyone who's not authorised, including friends or relatives, to use your work devices.
- Don't connect your work devices to untrusted networks, e.g. public WiFi hotspots.
- Don't attach unauthorised equipment of any kind to your work devices, computer or network, e.g. unauthorized USB drives and personal mobile phones.
- Don't download unauthorised software or data from the internet.
- Don't download or upload commercial software or other copyrighted material without the correct licence and permission from your manager.
- Don't use websites that could be classed as obscene, racist, offensive or illegal.



iHasco
training made simple

☎ 01344 867088 ✉ hello@iHasco.co.uk www.iHasco.co.uk
Produced to support Cyber Security Awareness. Please contact us for further information.