**Password Recommendations**

**A full run down and guidence can be found on** https://www.ncsc.gov.uk/

Use unique password on each site.  As many accounts use your email address as the username which is always the same, then if one system is compromised then that password will be tried against other accounts. Keep different passwords at work and at home and change default ones on new things.

It is suggested passwords are at least 8 characters long, ideally more say 12 or 14 chars.

A password should be different from the user login.

Avoid simple, easy to guess passwords such as names of friends, football teams, family and pets.

Unless you think your complex password might be compromised, don't change it.(CESG

Particularly keep away from words in a dictionary (in any language including Klingon!) or commonly used passwords such as password, 123456, 12345678, football or QWERTY.

Use a mix of upper and lower case letters, numbers *and* special characters like @ ! $ % &

Hackers are onto patterns like capitalising first letters, substituting vowels for numbers and adding a number 1 or 2 at the end then incrementing the number when changing it.

Before you enter a password into a website, especially but not only on a public or free wifi, make sure it is using a secure connection beginning with https:// (it might also show a small green padlock close to the address) this means the site is using a secure link that cannot be intercepted by attackers.

Beware the "secret question”. You don't want a backup system for when you forget your password to be easier to break than your password.

Be conscious of shoulder surfing where someone is watching you enter your password (particularly relevant for cashpoints and public places like coffee shops).

Good advice is to make a memorable, unusual sentence or passphrase: “I am a 7-foot tall metal giant” is better than “My name is John”, and use the first letter of each word with punctuation: "Iaa7-ftmg”.

Two factor authentication is one of the best ways to secure your accounts.  This can involve sending a text with a code to your phone when you login in eg available with Google and Paypal or using a ‘gizmo’ to generate a number like for internet banking