- Get the latest anti-virus and firewall software for your device
- Keep your internet browser up-to-date
- Create a strong and easy-to-remember password
- Use a different password to the one you use for other services
- Change your password on a regular basis
- Never share your password
- Check your Privacy Markings - major websites like Facebook have privacy-enhancing settings available
- Always research online retailers, particularly if you have not bought from them before. Read feedback from trusted people or organisations, such as consumer websites. Pay securely using a credit card, which means that if your payment details are stolen your main bank account will be safe
- Consider using a payment platform, such as PayPal, Google or Apple Pay.
- When you pay, look for the closed padlock in the web address bar, meaning your connection is secure.

A Couple of Notes

- Phishing involves the attempt by backers to trick people into actions such as clicking a bad link that will download malware or direct them to a fake website. Their aim is often to make recipients visit a website which may download a virus on their computer, ask for payment or steal bank details and other sensitive information.
- You can forward suspect emails to the suspicious email reporting service at report@phishing.gov.uk. Suspicious texts should be sent on to 7726. To help HM Revenue & Customs to fight these crimes, forward suspicious texts claiming to be from HMRC to 60599 and emails to phishing@hmrc.gov.uk.
- Finally, have a look at the Digital Activities webpage here or you can contact the Digital Training Team on winorfolkdigitalhelp@gmail.com for help and advice.