THINGS TO AVOID OR BE WARY OF

- If you receive an unexpected call from a company, it's always best to hang up and call them back yourself using an official customer number listed on their website.

- Scammers may be able to keep your phone line open even after you've hung up, so if you hang up on a dodgy call, use a different phone to call the company back on a trusted number or wait for at least 10 to 15 minutes.

- NEVER give out any personal or financial details, emails, passwords etc no matter what you are told.

- If you're at all suspicious about a caller, end the call immediately.

- Call 159 if you receive a call claiming to be from your bank. When you call, you'll be put through to your bank's genuine customer service line. The banks involved in the scheme include Barclays, Bank of Scotland, Co-operative, First Direct, Halifax, HSBC, Lloyds, Metro Bank, Nationwide, NatWest, Royal Bank of Scotland, Santander, Starling Bank, Tide, TSB, Monzo and Ulster Bank. You can use this service if your phone contract is with BT (including EE and Plusnet), Gamma, O2 (including giffgaff), Sky, Three, Vodafone, TalkTalk or Virgin Media.

- Don't pay any attention to investment opportunities or offers that sound too good to be true. Do your own research before you part with any cash.

- Ignore texts, emails and calls from unknown contacts and invitations to WhatsApp groups that you've never heard of

- Never click links in unsolicited messages

- Ignore adverts and posts on social media which aren't from official accounts. You can verify company social media accounts by checking the links on a company's official website.

- Avoid paying for anything online via bank transfer as it's difficult to get your money back.

- The safest way is to pay by credit card for transactions over £100 or by using PayPal and its 'buyer protection programme'

- Look out for spelling and grammar mistakes as well as missing 'about us', 'contact us' and 'terms and conditions' pages.

- Stick to official ticket sellers for events or concerts.

- PLUS - see the section on QR scams