~ Advice relating to 'On-line fraud' ~

The following advice is based on that provided by Dorset Police regarding 'on-line' fraud.

1. Stop and think. A common tactic used by fraudsters is to use manipulative techniques to get you to act against your better judgement. A bank (or any other reputable organisation) won't pressure you to act fast, or apply time limits to anything. If you feel you are being rushed to hand over information, stop! Do not let anybody make you do something you don't entirely understand, or aren't comfortable doing. If something doesn't 'feel' right, back out and take advice.

2. Remember: your bank will NOT contact you out of the blue to ask for sensitive information like your PIN or password. Nor will they ask you to move money into a new account.
Take care with emails. If you receive an unsolicited email, be wary of clicking any links or attachments. "Phishing" emails are a common tactic used to gather sensitive information from victims. Always question uninvited approaches asking for personal details, in case it's a scam.

3. If you receive an unexpected message from your bank, or a company (e.g., a utility concern), consider calling them directly using a telephone number you know and trust, rather than by calling a number in an email or text message; look at a recent statement for a contact number.

~ Advice relating to general on-line security ~

The following advice is based on that provided by Dorset Police regarding security when using the internet (via browsers, email, smart-phones etc.).

1. Think about what you're sharing: if you wouldn't share it with a stranger, then don't share on social media (e.g., Facebook, Instagram, Snapchat, Twitter). Check your privacy settings - set them to 'private' (or equivalent) which means only approved contacts, family or friends can see what you post - meaning you're safe from prying eyes. Remember! Modern software analysis programmes can 'harvest' huge quantities of data from your everyday writings - that's why you get 'targetted' adverts that might not be appropriate!

2. Don't accept 'friends requests' from people you don't know and trust: be guarded with what information you share with strangers. Do not allow anyone to pressure you into doing something you're not comfortable with.

3. Be careful what you 'click' on! Take time to check the source of any link - particularly if it it is offering something that seems 'too good to be true'! It often is!! If you hover your mouse over any link or button in an email or website, the true address should be displayed at the bottom (corner) of your screen. If the link claims to be from a reputable company (e.g., a utility concern or big-name retailer) but the address indicated using the 'mouse-hover' is wildly different - there is something wrong: don't proceed - exit the page/email and do something else!