PROTECT YOURSELF FROM FRAUD & IDENTITY THEFT

Don't give any personal information to anyone – either online, face to face or over the phone – before verifying their credentials.

• Never give your credit card number over the telephone unless you made the call and are certain of who you are speaking to.
• Don't let anyone take your debit or credit card out of sight when paying in a shop or restaurant.
• Shred receipts with your card details on and correspondence with your name and address on.
• Never throw away credit statements, credit cards or bank statements in a usable form. Shred them.
• Remember that your bank would never contact you to ask you for your PIN, password or other security information in full.
• Shield your PIN when withdrawing cash and when using your credit or debit card to pay for items in a shop.
• Regularly get a copy of your credit file and check it for entries you don't recognise. **Callcredit** (www.callcredit.co.uk / 0113 388 4300), **Equifax** (www.equifax.co.uk) and **Experian** (www.experian.co.uk / 0844 481 0800) can all provide your credit file.
• If you move house, contact your bank, give them your new address and arrange with the Post Office to have your mail redirected.
• Be extremely wary of post, phone calls or emails offering business deals out of the blue. If an offer seems too good to be true, it probably is.
• Reconcile your bank account monthly and notify your bank of discrepancies or unauthorised transactions immediately.
• Keep a list of telephone numbers to call to report the loss or theft of your wallet, credit cards etc.
• If you are expecting a statement, new card or cheque book by post and it does not arrive within the indicated length of time, contact your bank immediately.
• Protect mail left in communal areas of residential properties.
• When registering to vote, tick the box to opt out of the 'Edited' register.

Action Fraud is the UK's fraud and internet crime reporting centre. For advice, resources or to report suspected or attempted fraud visit www.actionfraud.police.uk or call 0300 123 2040.

You can contact Trading Standards via the Citizens Advice Consumer Helpline on 08454 04 05 06 (English) or 08454 04 05 05 (Welsh), or visit www.adviceguide.org.uk

ONLINE SAFETY

- Make sure you have an up to date security programme and antivirus software installed on your computer.
- Install updates for your operating system, web browser and other software as soon as it is available. But beware of emails about security updates; these are hoaxes.
- Make regular backups of important files.
- Be careful about clicking on links and attachments in emails. Don't click on links from an unknown sender. Remember that spammers could also gain access to a friend's account, so if you get an uncharacteristic email containing a link from a friend, do not click on it but find another way of contacting them to check that the message is genuine.
- Remember that free screensavers and games can be used to infect computers with viruses. Never download them, no matter who has sent them to you.
- Never click on a link in an email from your bank. If you want to use online banking, enter the website address in the address bar yourself, so that you know you are going to the right website and not a fake site designed to replicate the genuine article.
- Leave a website if you feel suspicious - if the site doesn't look or 'feel' right, if there is text that doesn't appear to have any purpose or doesn't tie in with the rest of the site, or if you feel uneasy for any reason.

• Don’t use open wi-fi hotspots to send private information such as bank details.
• When buying things online or otherwise entering sensitive data, look for a padlock in the bottom right corner of the screen and a web address beginning with https. This indicates that you are on a site that has its own built-in security.

If you use a wireless network at home, password-protect it.

• Make sure your passwords are strong and you use a different one for each account. As a general rule, passwords should contain a mix of numbers, symbols and upper and lowercase letters.
• Regularly check your social media privacy settings to control exactly what you’re sharing with whom.

If you’re going away on holiday, don’t advertise it on social media!

There is lots of information about staying safe online on the websites www.getsafeonline.org and www.cyberstreetwise.com

For advice about keeping children safe online, or if you want to report someone who is behaving suspiciously towards a child online, contact the Child Exploitation & Online Protection Centre at www.ceop.gov.uk or 0870 000 3344.

If a child is at immediate risk, call 999.

You can report illegal online content to the Internet Watch Foundation at: www.iwf.org.uk/report