SCAMS & FRAUD

Doorstep crime

Not sure? Don't open the door!

- Keep your front and back doors locked, even when you are at home.
- Install a 'spy hole' or electronic viewer in the front door so that you can see who the caller is before opening the door. Some include audio so that you can speak to someone without having to open the door. If you don't recognise them, you don't have to open the door.
- Use a door chain or door bar so that if you do want to see who is on your doorstep, you don't have to open the door fully.
- You might have a friendly neighbour who is happy to help - if so, direct the caller to speak to your neighbour first.
- Trading Standards advise all householders to never buy goods or services from cold calling doorstep traders.
- Never leave any doorstep callers alone with your door open.

Never agree to have work done by someone just passing by. If you some work is needed, get at least two quotations from reputable traders. Your local Trading Standards Service may operate an 'approved trader scheme' - contact the consumer helpline on the next page for help.

Never sign anything on the spot, never agree to allow any work to start right away and remember that you normally have a 14 day cooling-off period during which you can cancel any work and receive a refund of money paid.

Bogus callers, sometimes called distraction burglars, may turn up on your doorstep and say that they have come to investigate a water leak or they are lost and need a drink of water. Sometimes they may say they have a child who has lost a ball in your back garden. They are probably trying to trick you to let them into your home so they can steal cash and valuable items. Don't let them in.

Here are some responses you can use to callers at the door:

"I never deal with cold callers at the door - please would you leave."
"I have a neighbour who helps me - please knock at their door first."
"I don't know who you are so would you please leave."

It isn't rude to ask someone to leave - it is your right.

If you get into difficulties with someone on your doorstep and they will not go away, call the police on 999. If you think you've been the victim of crime or want to report a suspicious incident, you can call the police on 101 or, in the case of a possible rogue trader, call Trading Standards via the consumer helpline numbers below.

For advice on doorstep selling, how to find a reputable trader and to report suspicious incidents, you can call the Citizens Advice consumer helpline on 03454 04 05 06 (English) or 03454 04 05 05 (Welsh), or visit www.adviceguide.org.uk

Safety on the telephone

- Never agree to anything over the phone. Don't be shy of just hanging up on telephone cold callers.
- Criminals may already have basic information about you. Don't assume a caller is genuine because they have these details.
- It takes two people to terminate a call. Use a different phone line to return a call or wait five minutes before returning a call.
- Never reply to unsolicited text messages, even to try and stop them. Just delete them.
- Never give any personal information over the phone unless you made the call and are certain of who you are speaking to.
- Use a password, passcode or pattern code to lock your phone.
- Don't store password reminders on your phone.
- Don't open suspicious or unsolicited messages.

Register your mobile with www.immobilise.com, using your IMEI number (15 to 17 digit code usually behind the battery - or key in *#06#).

If your phone is stolen, report it immediately to the police and your service provider to block usage, even if it's pay-as-you-go. Don't report lost phones as stolen. This is a crime.

If you have a smartphone

- Install anti-virus software specifically designed for mobile phones. Ask for advice at the store where you bought your phone.
- Avoid opening links or downloading games and apps unless you are certain of their source.
- Clear your browser history – especially if using online banking.

Remember:

- If you have a smartphone, take the same precautions as you would when accessing the internet over any other device.
- Be careful with your location settings.

If you use your phone to update social media or to upload photos, location data could be uploaded to the internet without you realising. Burglars can use this information to find out where you live and even when you are likely to be out of the house.

If you are unsure, ask a member of staff at the shop where you bought your phone to show you the location settings.

More information about smartphone safety is available at www.outofyourhands.com

Sign up to the Telephone Preference Service (www.tpsonline.org.uk or 0845 070 0707) and the Mail Preference Service (www.mpsonline.org.uk) to minimise unsolicited calls and mail.

Stay safe from scams

Remember: scammers often pretend to be from legitimate, well-known, national or global companies like banks or utilities providers. If in doubt, hang up, wait for five minutes or use a different phone line, and phone the company yourself, using a phone number from their official website, Yellow Pages or letterheaded correspondence from them.

A common scam involves someone calling you up and claiming that there is something wrong with your computer and they can fix it for you. This is a hoax.

If you think there is a problem with your computer or you want to buy or update antivirus software:

- Ask advice from the store where you bought it.
- Ask a trusted computer repair technician that you have contacted yourself.
- Never give control of your computer remotely to a third party over the telephone.

The Metropolitan Police produce a useful online booklet called **The Little Book of Big Scams**. This can be downloaded at www.met.police.uk/docs/little_book_scam.pdf and an audio version is also available (visit www.met.police.uk and type 'little book big scams' into the search box). Two websites with useful information about hoaxes are www.snopes.com and www.hoax-slayer.com.

Some scams or frauds involve online dating. Be very careful about what information you give to someone you have never met in person, and never send any money to someone you haven't met.

Scams can also revolve around job-hunting. As well as being wary of links and attachments in unsolicited emails, beware of interview, job or training 'offers' that require you to buy books or equipment, or pay a fee upfront.

The charity 'Think Jessica' has an anti-scam website, www.thinkjessica.com, with a useful poster, FAQs and information about what to look out for, as well as further materials that you can order.

Protect yourself from fraud and 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.

Criminals sometimes try to dupe innocent victims into becoming money mules and laundering money on their behalf. They normally do this by pretending to offer legitimate jobs via newspapers or the internet, and often target vulnerable groups such as migrant workers or university students who may be tempted by the lure of a seemingly easy way to make extra cash.

Be very cautious of offers to make 'easy money' - particularly job offers from people or companies based overseas. These may involve receiving money into your bank account and paying amounts out whie keeping a percentage as 'commission'. Never give your bank account details to anyone unless you know and trust them!

If you have already disclosed your bank account details or received money into your account and you think it could be a money mule scam, you should contact your bank immediately.

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.

- 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.

You can contact Trading Standards via the Citizens Advice Consumer Helpline on 03454 04 05 06 (English) or 03454 04 05 05 (Welsh), or visit www.adviceguide.org.uk

Online safety

- Make sure you have an up to date security programme and anti-virus 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.
- 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.

- 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!

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

How to bank safely online

- 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.
- Don't use open wi-fi hotspots to send private information such as bank details.
- When entering sensitive data, look for a locked padlock or unbroken key symbol in the bottom right corner of the screen. This indicates that you are on a site that has its own built-in security. This applies to buying products online as well as using online banking.
- The beginning of your bank's internet address will change from 'http' to 'https' when a secure connection is made.
- Be wary of any unexpected or suspicious-looking pop-ups that appear during your online banking session.
- Stop and think about the process you normally go through to make a payment to someone - be suspicious if it differs from the last time you used it.
- Fraudsters sometimes try to trick people into making a real payment by claiming 'it's just a test'.
- Never give anyone your login details in full either by email or over the phone - your bank will never request these in this way.
- Check the online banking security options your bank provides; some offer free anti-virus and browser security software.
- Check your bank statements regularly and contact your bank immediately if you spot any transactions that you didn't authorise.
- When sending money via your online bank account, always double check the amount you are sending as well as the account number and sort code you are sending it to.
- Make sure your bank has your up-to-date contact details.
- Browsers often come with security features built in. Make sure they are activated.

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

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