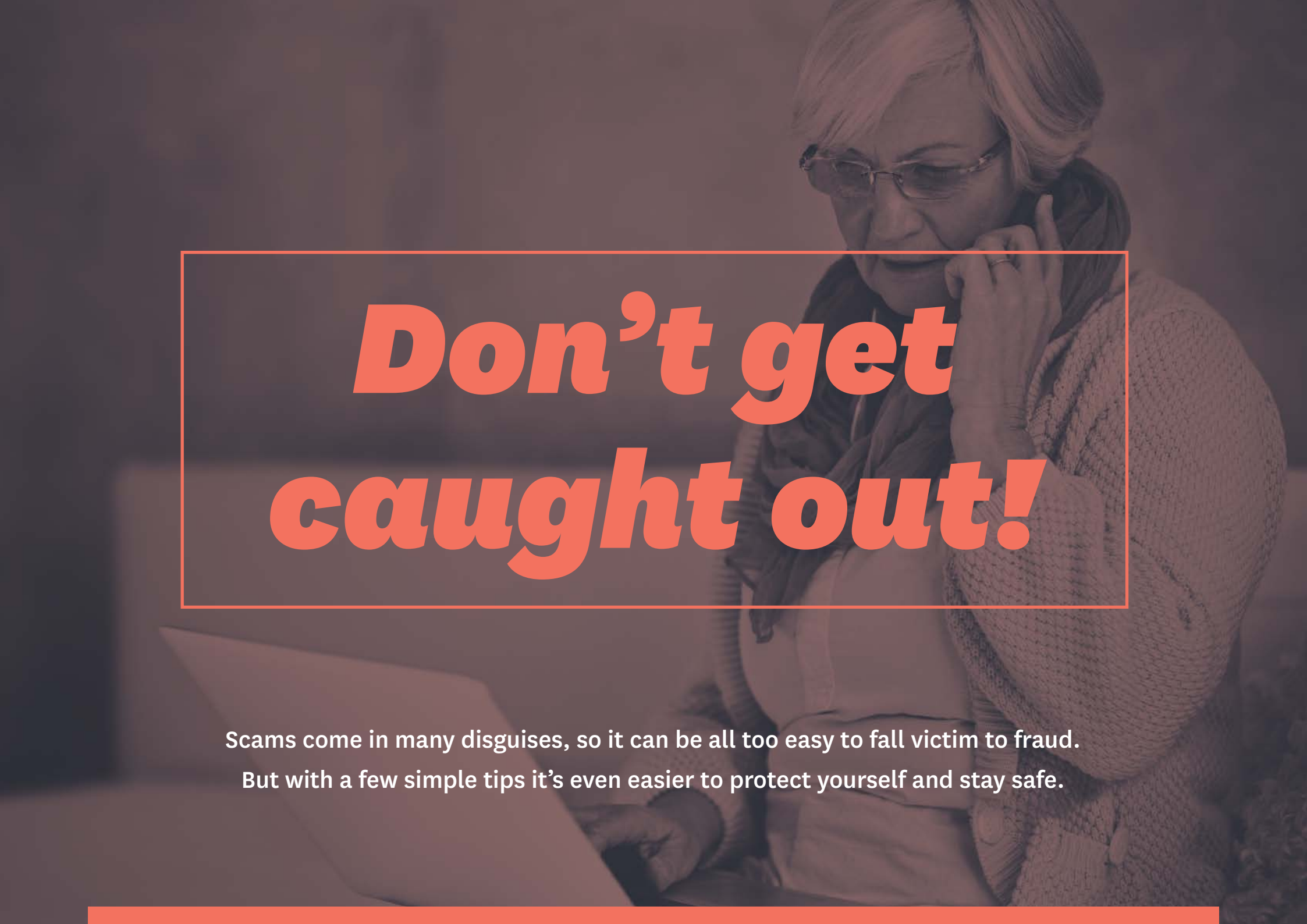
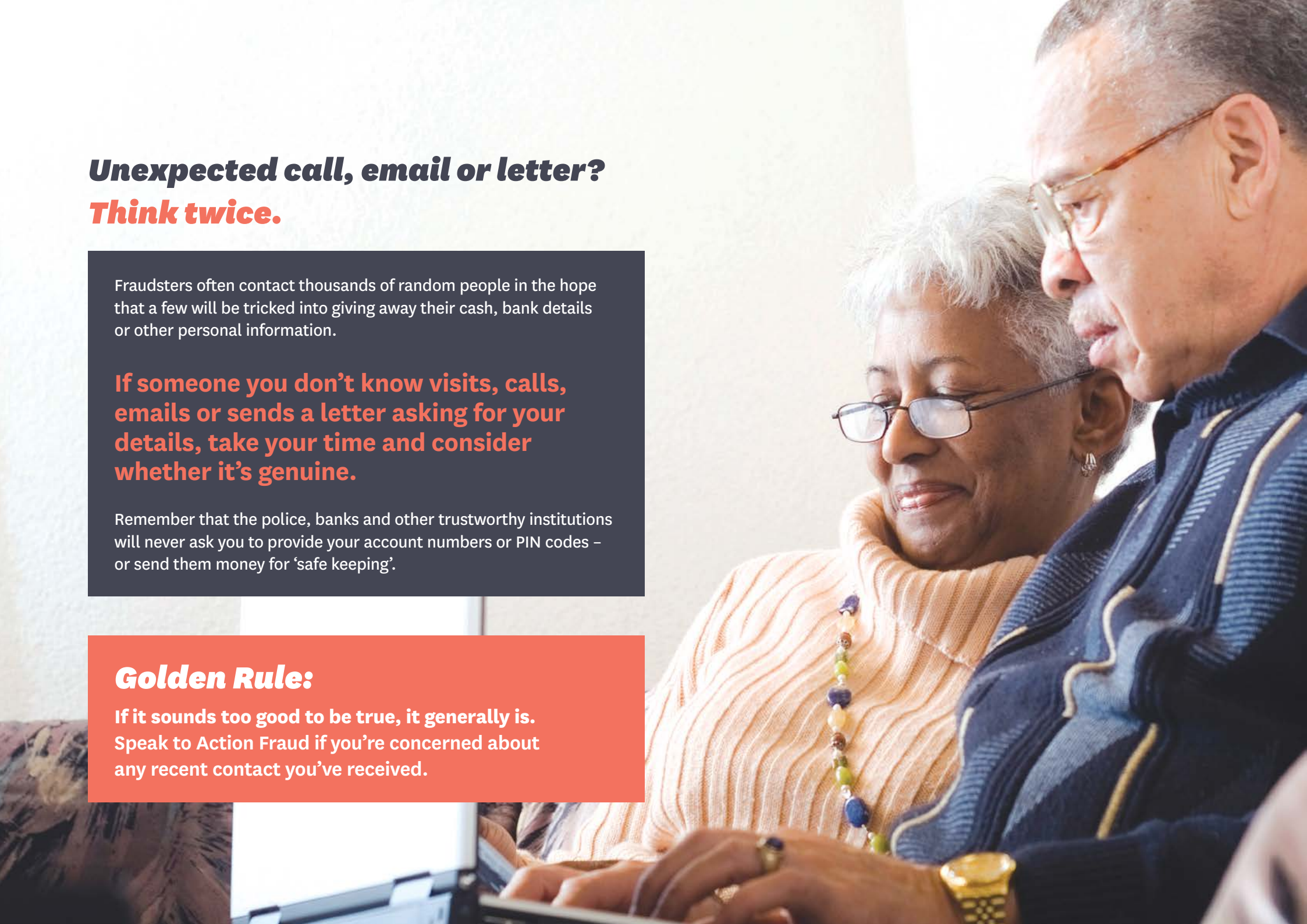


Don’t get caught out!

Scams come in many disguises, so it can be all too easy to fall victim to fraud.
But with a few simple tips it’s even easier to protect yourself and stay safe.



Unexpected call, email or letter?
Think twice.

Fraudsters often contact thousands of random people in the hope that a few will be tricked into giving away their cash, bank details or other personal information.

If someone you don't know visits, calls, emails or sends a letter asking for your details, take your time and consider whether it's genuine.

Remember that the police, banks and other trustworthy institutions will never ask you to provide your account numbers or PIN codes – or send them money for 'safe keeping'.

Golden Rule:

If it sounds too good to be true, it generally is. Speak to Action Fraud if you're concerned about any recent contact you've received.

Phishing fraud – don't bite!

Lots of frauds start with a *'phishing'* email. This is when the con artist sends a huge number of people a message intended to make you click on a bogus link or install a computer virus that can help them access your banking or personal information.

5 *ways to spot a phishing email*

1. They often start with a non-personal title, like *'Dear Customer'* or *'Dear Account Holder'*
2. They typically have poor spelling and grammar that you wouldn't expect from a reputable organisation
3. Usually there's an *'urgency'* to take action – with claimed consequences like account closure or a financial penalty if you don't
4. Sometimes there's an offer that you might *'miss out on'* if you don't provide a small upfront fee
5. Check the sender's email address – has it really come from the organisation being claimed?

5 *ways to protect yourself*

1. Make sure you have up-to-date anti-virus software installed with the system firewall enabled on your computer, check your browser is set to the highest level of security and monitoring
2. Don't click on links or download files from a sender you aren't sure is authentic
3. Never give away any personal information unless you are totally sure the request is genuine
4. If in doubt, ring the organisation on a contact number you already have – not the one provided in the potentially fraudulent email
5. Treat any offer with extreme caution and remember the golden rule *"if it sounds too good to be true, it generally is"*

Scam letters

As well as emails, fraudsters sometimes send their scams by post.

These letters often have non-personal titles like ‘Dear Customer’ or ‘Dear Householder’, and often this title doesn’t match the rest of the mail in style, colour or font.

Grammar and spellings are again usually poor – not what you’d expect from a reputable organisation. The post might claim that you need to take action to avoid some kind of penalty, or offer you a prize or business deal that you first have to pay a fee or share your personal information to access.

If you’re unsure about any post you’ve received, seek advice from someone you trust. Speak to a family member or call the **Citizens Advice Bureau** on **03444 111 444** before responding to the post in any way.

You can have your name removed from direct mailing lists in the UK by contacting the **Mail Preference Service** on **0207 291 3310** or visiting **www.mpsonline.org.uk/mpsr**.

Make sure you also shred any post that contains your name, address or other personal information before you throw it away – this will help prevent it from falling into the hands of scammers.

Telephone scams

If you take an unexpected call from someone you don't know, asking yourself a few simple questions can help keep your information and money safe.

- **Is the caller asking you to send any money anywhere?**
- **Do they want my bank or personal details?**
- **Are they after my money for safekeeping or to help catch a criminal?**

If the answer to any of those questions is yes, the call is probably a con.

Seek a second opinion from a trusted source like a friend, family member or advice organisation before you do or say anything.

Sometimes scam callers will claim to be from real organisations. If you're uncertain about such a call, put the phone down and make sure you have ended the call. Ring the organisation on a number you already have – not one the caller just gave you – and they'll be able to tell you whether the call was legitimate.

Tips and hints:

Sometimes fraudsters stay on the line and play a dial tone to make you think they have hung up, so it's worth checking an unexpected call has ended by ringing a friend or the **Action Fraud automated switchboard** on **0300 123 2040**.

You can make your phone number ex-directory so that it doesn't appear in any directories or 118 enquiry services. Simply visit **www.tpsonline.org.uk** or call **0845 070 0707** to record your preference to not receive unsolicited sales or marketing calls.

To make a formal complaint about nuisance calls, speak to the **Information Commissioners Office (ICO)** on **01625 545 745** or go to **www.ico.org.uk**.

Remember –

banks and the police will never ring you to ask for money or personal details.

You can report suspected fraud calls to **Action Fraud** on **0300 123 2040**. Visit **www.actionfraud.police.uk** for more information.

On the doorstep

Some scammers prefer to work face-to-face, so always be alert when someone knocks on the door – and always keep your doors and windows locked.

Distraction burglars often try to persuade you to let them in by claiming there is a water leak or similar problem, or by asking for a glass of water or to use your phone. Whatever their claim, they may be trying to con their way inside to steal from you.

If a **potential rogue trader** tries to tell you that you need to have work done, politely refuse and explain you don't buy anything at the door. Alternatively, you could ask them to leave a quote and their contact details so you can get more quotes while seeking a second opinion.

Not sure? Don't open the door!

Tips and hints:

Always get more than one written quote for work and use trusted trades people. You can check by asking for recommendations from friends or speaking to organisations like **Age UK**, who are contactable on **www.ageuk.org.uk** or on **0800 169 8787**.

Staying safe at the door

1. Put on the chain before opening the door
2. Ask the caller what they want
3. Make sure they're legitimate before letting them in
4. Never agree to have work done by an unknown trader without getting a second opinion

How to check a caller's identity

1. If they say they're from an organisation, find your own number – not one they've given you – and ring it to confirm their story with the company. Legitimate callers won't mind waiting outside while you do this
2. Most companies use a password scheme so callers can prove they are genuine
3. Look at any ID card – does the photo match the caller and does it look real?
4. If the caller appears genuine and you still feel uncomfortable, ask them to make an appointment so you can arrange to have a friend with you during their visit

Easy ways to stay safe

- Remember that the bank is always the safest place to keep your money. Never keep large amounts of cash at home and keep what you do have hidden away
- If someone asks for money or personal information, or encourages you to let a complete stranger into your home, stop and think *'is this a con?'*
- If you're in doubt over something, seek a second opinion from someone you trust
- Regularly check your bank statements and report anything suspicious to your bank in branch or using a phone number that you know is genuine
- If you've already been a victim of fraud, be aware of scammers targeting you again – they could pretend to be a lawyer or police officer who can help recover your money

Identifying your property

Could the police identify your property if it was stolen and they found it?

You need to be able to describe it uniquely, telling them makes, models and serial numbers. Keep your property records safe and enter them on the free police-approved property recording website **www.immobilise.com**.

With the Immobilise website, all UK police forces and registered second-hand dealers will be able to see when you highlight an item of property as stolen and can return it should it come into their hands and be checked.

Don't get caught out!

Further advice and reporting fraud

If you need more advice about fraud, visit www.actionfraud.police.uk or call **Action Fraud** on **0300 123 2040** and speak to a specialist advisor.

You can report a fraud online at **www.reportlite.actionfraud.police.uk** or by making a report on **0300 123 2040**.

In association with:

Humberside Police
Protecting Communities, Targeting Criminals, Making a Difference

WHEN IT'S LESS URGENT THAN 999 101 IN AN EMERGENCY ALWAYS CALL 999

CRIMESTOPPERS 0800 555 111
Call anonymously with information about crime

designed by diva • divacreative.com • Printed on paper from sustainable forests • 9552