Fraudsters can be clever and convincing

In December 2013, Edna Oates* was contacted by someone pretending to be from her bank's fraud department. They told her that they were investigating employee fraud and asked her to get samples of money from her bank for fingerprinting.

The fraudsters stressed the secrecy of their 'investigation' and Edna was given cover stories in case anyone asked why she needed the money. Over several months, Edna withdrew over £120,000 – more than her life savings – for the fraudsters who then visited her home to collect the cash.

This is an extreme case, but did you know that last year, fraud victims aged 61-90 in Avon and Somerset lost an average of £3,500 each?

Fraudsters are known to use the same techniques again and again, whether they approach you by email, post, phone or at your door.



Report fraud to www.actionfraud.police. uk or call 0300 123 2040



Report information on crime anonymously to Crimestoppers.



Visit www.crimestoppers-uk.org or call 0800 555 111

Contact the Citizens Advice Consumer Helpline on **03454 04 05 06** or your local Trading Standards, if you are concerned about a caller

In an emergency, or if an incident is happening at the time, call the police on **999**. For non-emergencies, call **101** or contact the police via **www.avonandsomerset.police. uk/contact-us**



If you've been a victim or have been affected by a crime, Victim Support can help. Call your local office on **0300 303 1972**



Learn how to protect yourself and your family online. Visit www.getsafeonline.org and www.cyberstreetwise.com







Protect yourself

SPOTIT

- Make decisions in your own time
- Check people are who they say they are

STOP IT

- **O**Don't share your personal information
- Report fraud to 0300 123 2040 / www.actionfraud.police.uk

If you are concerned and the caller is still in the area call 999





^{*} The victim's name has been changed to protect their anonymity.



Protect your community

In Avon and Somerset last year

- there were over 5,000 reports of fraud.
 The true number of crimes is likely to be much higher
- local residents aged 61–90 lost over
 £5million as a result of fraud



Types of fraud

At the door

Be wary of cold callers or bogus tradesmen that put you under pressure to act straightaway. Genuine tradesmen won't mind waiting a day or two and will always offer cooling off periods



Through email or post

Be wary of bogus emails or letters which appear to be from legitimate organisations and request personal or financial information. Never download attachments from suspicious emails, and remember your bank will never send a link to their log-on pages

On the phone

Be wary if someone asks you to call back and verify their identity. Fraudsters can stay on your phoneline after you hang up, so that any subsequent calls you make go directly to them





You can protect yourself from fraud

SPOT IT



Make decisions in your own time

- Obtain at least three written quotes and references before having any work done
- Genuine callers won't mind coming back in a day or two so that you can make independent checks
- If a caller refuses to leave your doorstep contact the police



Check people are who they say they are

- Check a company is trustworthy by making independent checks, such as calling the National Consumer helpline or Action Fraud
- Check a caller is a genuine employee by calling the company on a number you've looked up independently. Don't use the number they provide on their ID badge
- Telephone fraudsters can stay on the line after you hang up. Wait at least 10 minutes or use a different phoneline to make any other calls

STOP IT



Don't share your personal information

- Personal information includes: financial details, your full name, date of birth, address and travel plans
- Always destroy documents containing your details



Report fraud to 0300 123 2040 www.actionfraud.police.uk

 If you are concerned and the caller is still in the area call 999



8 things your bank will NEVER ask you to do



To give you peace of mind when answering the phone or reading emails, the major banks have made a pledge to you – a list of 8 things you can be confident they will NEVER do

- Ask for your full PIN number or any online banking passwords over the phone or via email
- 2 Send someone to your home to collect cash, bank cards or anything else
- 3 Ask you to email or text personal or banking information
- Send an email with a link to a page which asks you to enter your online banking log-in details
- Ask you to authorise the transfer of funds to a new account or hand over cash
- 6 Call to advise you to buy commodities like diamonds or land
- 7 Ask you to carry out a test transaction online
- Provide banking services through any mobile app other than the bank's official apps