Bogus trades

The scam

A salesperson calls at your home and convinces you to buy something you either don't want or don't need.

How it works

They will convince you to buy goods or services that won't be real or are of poor quality. They also sometimes charge for work you didn't agree to.

Protecting yourself

Don't hand over your bank card and PIN, or agree to hand over money at the door. Take time to think about it and talk to someone you trust. Only let someone in if you're expecting them or they're a trusted friend, family member or professional.

Romance

The scam

You think you've met your perfect partner online, when really, they're fraudsters.

How it works

Once they've gained your trust, they share a problem and need financial help. They want to get an emotional response. They may even suggest meeting you face to face to ask for money. When you send money, they will often come back with reasons to send them more.

Protecting yourself

Don't send money to someone you've never met in person, particularly if you have only recently met online. Research the person you're talking to, as profile photos may not be real. Only accept friend requests from people you know and trust. Speak to your family or friends to get advice.

Could it be a scam?

Here are some common themes to look out for and help you feel more confident about identifying scams.

- Has someone contacted you unexpectedly?
- Has someone asked you to share personal and financial information?
- Has someone asked you to pay fees or provide details for competitions you haven't entered?
- Are the contact details vague or not recognised?
- Has someone asked you to keep something secret?
- Is someone asking you to deposit money for them?
- Is it too good to be true?
- Do you feel under pressure to decide?
- Are there any spelling mistakes?

If the answer is yes to any of these, there's a good chance it might be a scam so don't give them any money or personal details.

Call 999 if you feel threatened or in danger. Call the police non-emergency number 101 to report an incident if you're not in immediate danger.

Contact us immediately if:

- You think you may have disclosed confidential information to an unknown third party.
- You believe a transaction on your account is fraudulent.
- You are a victim of identity theft.
- You have any concerns about security.

Talk to our team or call us on
0345 1200 100

Useful contacts

To find out more about the latest fraud scams and how to avoid them, visit:

getsafeonline.org
Free online safety service.

takefive-stopfraud.org.uk
A national campaign by Financial Fraud Action.

friendsagainstscams.org.uk
Encouraging communities to act against scams.

cyberaware.gov.uk
A Home Office campaign to help protect businesses and individuals against cyber criminals.

actionfraud.police.uk
The UK's national fraud and cybercrime reporting centre.

fca.org.uk/scamsmart
Information on how to avoid investment and pension scams.

TO FIND OUT MORE ABOUT FRAUD SCAMS, VISIT:
YBS.CO.UK/SCAMS

Our printed material is available in alternative formats e.g. large print, Braille or audio.

Please visit us in branch or call us on **0345 1200 100**.

YBM 8546 12 06 23

YORKSHIRE BUILDING SOCIETY
Helping real life happen

Discover more ways to stay protected online at ybs.co.uk/scams

PROTECTING YOURSELF FROM SCAMS

We've been keeping our members money safe for over 150 years.

We guide you through the most common types of scams, showing how you can protect yourself and your money.

Email

The scam

You receive an email which includes links to fake websites. They will ask you to enter personal and account information like login and card details.

How it works

They use the details you provide to buy goods and set up services. This is identity theft and bank fraud. Your computer or smartphone might also have a virus.

Protecting yourself

Don't give out any personal or financial information. Don't click on links or download attachments. Make sure your systems are up to date. Install anti-virus software and keep it updated.

Fake websites

The scam

Fake websites or adverts are set up offering holidays or goods for sale at an incredibly cheap price.

How it works

You see the website or advert with pictures of places to stay and things to buy, these are not real. You get in touch and buy something. They will ask you to send the money by bank transfer, Moneywise or Western Union, rather than by debit or credit card or PayPal. This is usually a flag to say it's a scam.

Protecting yourself

Be suspicious of any "too good to be true" offers or prices. Do your research first, read reviews of the site or person and verify that the company exists. Use search engines to help.

Mortgages

The scam

When buying a house, someone could hack into emails between you and your solicitors. They divert money that's for the house sale.

How it works

You'll get an email, claiming to be the house buyer's solicitor, telling you that they have a new bank account. You then send money to the fraudster's account rather than your solicitor's.

Protecting yourself

Always question changes. Companies rarely change their bank details. Confirm bank details with the company before you make any payments to them.

Telephone

The scam

You get a call claiming to be from a bank, building society, the police, utility provider, Internet provider or IT company. They tell you there's a problem with your account or PC.

How it works

You'll be asked to do one of the following things:

- Move money to a 'safe' account. This is a scam account.
- Not to trust our branch staff due to internal fraud.
- Give your card and PIN number to a courier.
- Allow them remote access so they can log in to your internet banking.
- Give card details for a refund or payment.

Protecting yourself

Companies won't ask for financial or password details, so do not provide them. If you think a fraudster has called, or you feel pressured into doing anything, hang up. Call the main company phone line to verify it is real.

Text message (including online)

The scam

You get an unexpected text or online message which will ask you to give them your personal details.

How it works

When you provide your personal or financial information, they use it to commit fraud.

Fraudsters can also pretend to be your family member, often a son or daughter, messaging from a new number. They say they have lost or damaged their phone. They ask for money which is then paid into the fraudster's account.

Protecting yourself

Never provide your personal or financial information over text. This includes card and account numbers. If they claim to be someone you know, on a new number, contact the number you have stored to check the message is genuine.

Investment

The scam

You're convinced to invest your money into high-risk investments such as cryptocurrency, gold, property, or a high rate of interest. The investment is non-existent or worthless.

How it works

They contact you by phone, email, or private message with an investment opportunity. You may see an advert on social media and websites using celebrity images and logos to make it look real.

Protecting yourself

Check the company details on the FCA's Financial Services Register to see if it is real. If you're thinking about investing, get independent financial advice from a reputable company. Take your time, don't rush into deciding.

Advance fees

The scam

You're asked to make upfront payments for goods, services or financial rewards that aren't real.

How it works

You could apply for a loan and be asked to pay a fee before receiving the money. You're contacted to say you have won the lottery or a prize but must pay a fee before you can receive it. You're asked to pay for a background check for a new job that doesn't exist.

Protecting yourself

Question claims that you're due money for goods or services that you haven't ordered or don't recognise. If you haven't entered a competition, it's likely to be a scam. Check that the email addresses of recruiters or potential employers are real.