YORKSHIRE
BUILDING
SOCIETY

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 160 years.

Here we'll guide you through the most common types of scams, showing how you can protect yourself and your money.

Calls

The scam

Scam calls may pretend to be from the police, a trusted business, or utility provider. Be cautious, as they may ask you:

- To move money to a fake "safe" account.
- Not to trust, or to lie to, our staff in person or over the phone.
- To give cash, or your card and PIN to a courier.
- To give them access or control of your device over the internet when you log into accounts.
- For your card details for a refund or payment.

Protecting yourself

Companies won't request financial or password details, so never share them. If you suspect fraud or feel pressured, hang up and contact the company directly using their official phone number.

Digital messages

The scam

You receive a message, text or email that appears to be from a trusted source but is designed to steal your information or money. It may request personal details, link to a fake form or, pose as someone you trust like a family member or service provider to convince you to send money.

Protecting yourself

- Never share personal or financial information by text, email, or social media.
- Don't click on links in unexpected messages. If someone you know contacts you from a new number or email, confirm their identity using a different method.
- Never send money based on a request from someone you've just met or a new contact.
- If someone you're expecting to pay sends new payment details, call them on a trusted number to confirm before sending money.

Fake websites

The scam

Fake websites or adverts offer cheap goods or holidays using images from genuine sites that aren't really available. Payments may be requested via bank or money transfer instead of credit or debit cards.

Protecting yourself

Be suspicious of heavily discounted prices. Do your research; read reviews of the site, verify that the company exists and that you have the genuine web address to use.

Authorised Push Payment (APP) scams

The scam

An authorised push payment scam is when you're tricked into sending money. If you send payment by Faster Payment or CHAPS there are protections in place to help you get your money back.

To qualify, you must:

- Tell us within 13 months of the last payment being made.
- Share information with us about the scam, when we ask for it.
- Make a report via Action Fraud or give us permission to report the scam to the police.

You may not get your money back if you have:

- Not taken enough care to protect yourself against scams
- Made payments to account/s outside the UK
- Committed fraud

You also need to know:

- The limit for reimbursement is £85,000
- These rules came in on 7 October 2024. Payments made before this date aren't covered.

Investment

The scam

False investment opportunities through cryptocurrency, gold, or property, may be promoted through direct contact or social media ads. These scams may use fake celebrity endorsements to appear genuine.

Protecting yourself

Verify company details on the FCA's Financial Services Register. Be wary of guaranteed returns as real investments carry risks. Seek independent financial advice before investing.

QR codes

The scam

Scammers use QR codes to link to fake sites that steal your personal or banking details.

Protecting yourself

Only scan QR codes from trusted sources. If in doubt, avoid entering personal information. Don't scan codes that appear altered, such as those stuck over an original code on posters, ads, or leaflets.

Advance fees

The scam

Scammers ask for up front payments for goods, services or financial products that aren't real. These could include prizes, jobs or money.

Protecting yourself

Be cautious of unexpected claims about money or goods you didn't order. If you haven't entered a competition, it's likely to be a scam. Always verify contact details for recruiters or potential employers.

Bogus trades

The scam

A salesperson visits your home, pressuring you to buy poor-quality or fake goods, or charge for work you didn't agree to. You may feel pressured or hurried into making a decision.

Protecting yourself

Never hand over money, your bank card or PIN at the door. If you need work to be done, do your research and check with someone you trust. Only let in expected visitors or people you know.

Romance and personal relationships

The scam

Fraudsters use fake profiles online, pretending to be partners, friends, or contacts to earn your trust. They create a relationship and make up problems to ask for money. They might suggest meeting to seem trustworthy and often keep asking for more money.

Protecting yourself

Never send money to someone you haven't met in person. Verify their identity, as profiles may be copied or faked. Only accept friend requests from people you know and trust, and seek advice from family or friends.

Could it be a scam?

Scams try to mislead you by using:

- **Unexpected contact -** a message, call or visit from someone you don't know or weren't expecting.
- **Urgency** - pressure to act quickly such as deadlines, threats or limited-time offers.
- **Emotional triggers** - panic, fear or excitement to cloud your judgment.
- **Complex or far-fetched stories** - claims that don't quite add up. Talk it over with someone you trust.
- **Missing details** - vague or unclear information.
- **Secrecy** - requests to keep things quiet to stop you from seeking advice.

If something feels off, it probably is.

Don't share money or personal details.

Call 999 if you feel threatened or in danger.

Contact us immediately if:

- You suspect someone has access to your confidential information and shouldn't.
- You believe a transaction on your account is fraudulent.
- You have been told to not tell our colleagues the truth about a payment or activity on your account.
- Someone is asking you to deposit money for them, or move money from your YBS account.

Talk to our team in branch or call us on:

0345 1200 100

Useful contacts

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

takefive-stopfraud.org.uk
A service provided by UK Finance to share information about fraud and scams.

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

LEARN MORE ABOUT FRAUD SCAMS AT:

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 15 07 25