HELPING PROTECT YOURSELF FROM IDENTITY THEFT AND FRAUD HAPPEN

YORKSHIRE BUILDING SOCIETY
Helping real life happen

HOW YOU CAN PROTECT YOURSELF AND YOUR MONEY

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

Today, with the increased use of technology in financial services, the opportunities have also widened for new and different types of fraudulent activity. This leaflet aims to highlight the sorts of criminal activity you should be aware of and provides guidance on what you can do to reduce the risks of identity theft and fraud happening to you. We guide you through the most common types of scams, showing how you can protect yourself and your money.

What is identity theft and fraud?

Identity theft is when someone takes information about your identity, such as your name, address and date of birth, without your knowledge or consent. Fraud takes place when that person uses your identity to obtain goods or services by deception usually by using false or stolen documents such as a passport or bank statement.

Don't ignore the problem

You may think it's unlikely this will happen to you. You may not find out until you apply for credit and have your application rejected, that you've had your identity stolen. Act quickly if you think your identity has been stolen as you might have difficulty obtaining a mortgage and other credit which could take years to put right.

How does this happen?

Criminals use many methods to get personal information. Here are some examples of the things they may do:

- Watch for your Personal Identification Number (PIN) at an ATM
- Steal discarded bills and post from your waste bin
- Send random letters or emails
- Telephone you asking for banking details
- Request credit reports in your name
- Set up false websites that may look like real websites to capture your personal information.

How can I protect myself?

There are many ways you can prevent yourself from identity theft or fraud such as:

- Tell us when you change your name, address, telephone number or email address
- Keep personal documents in a safe place. Without this information a criminal will find it difficult to pretend to be you
- Shred important documents like bank statements, bills and mail that include personal information when you no longer need them
- If you move home, tell all the companies that send personal information to you by post so they can update your address on their database
- Redirect your post so that anyone moving in to your previous address doesn't have access to your personal details. Post is valuable in the wrong hands
- Be cautious if someone contacts you unexpectedly to confirm personal details. If you doubt the call is genuine, then arrange to call them back using a central switchboard number that you have independently obtained
- Check statements and passbooks regularly – if you see an entry is wrong then tell us straight away
- If someone asks to use your account to deposit funds on behalf of a third party (perhaps offering to pay you for your trouble) – refuse. Often these funds are the proceeds of criminal activity.

Cheques

- Never accept a cheque or bankers draft from someone unless you know and trust them – consider another form of payment especially for high value goods
- If you withdraw a cheque from your account and it is no longer required, return it immediately to be re-credited to your account so it doesn't fall into the wrong hands.

Online Protection

It is important to do everything you can to stop internet criminals from gaining access to your online building society and bank accounts. We've listed some essential precautions below and recommend you do them all as soon as possible. The more you put in place, the harder it will be for fraudsters to access your account.

- Make sure your computer is secure. Use an up-to-date firewall, anti-virus, anti-malware and anti-spyware package to keep your computer clean. Make sure you apply the latest security patches and updates
- Don't tell anyone your login information. Keep your passwords secret. If you suspect somebody else knows your password, change it immediately
- Ensure that the computer or laptop you are using to access our online services cannot be overlooked by another person
- Never let someone remote access so they can log in to your internet banking
- When you have completed your transaction or want to take a break, log off the service and close down your Internet browser
- It is best not to use a public computer to access your online accounts because you cannot be certain that the public computer is secure-it may be infected with a virus that could try to collect your password or other personal information
- Using an email account that is not shared with other family members will help keep your communications confidential.

Remember:

- We will NEVER send you a text message asking you to click on a link or provide any personal, account or security information
- Never disclose any access or authorisation codes we provide to you to another person
- Always check the URL (address) of the web page you are viewing. All Yorkshire Building Society pages start with one of the following:
  - **http://www.ybs.co.uk/**
  - **https://www.ybs.co.uk/security/latest-fraud-and-scams-updates**
  - **https://online.ybs.co.uk/**
  - **https://www.ybs.co.uk/contact-us/email**
  - **https://ybscareers.co.uk/**
- When you want to log on to our site, it's best to type the whole address yourself, or click on a link saved as a Favourite or Bookmark. This will help you to make sure that you really are visiting **ybs.co.uk** and not a fake site
- Always check the security of the site before you log on by looking for the padlock symbol. The address bar will also turn green when you are securely connected to our site.

If you receive a suspicious email, please forward it to phishing@ybs.co.uk. We won't be able to respond to each message individually, but each message we receive will be looked into and we will take steps to close down any fake websites we identify.

Could it be a scam?

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.

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, laptop or computer.

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.

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.

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.

Fake websites and QR codes

The scam

A QR code takes you to fake websites.

How it works

The website or advert shows pictures of places to stay or things to buy, but these are not real. You may be asked to enter information that can be used to steal your identity. For instance, personal or account information or your login or card details. If you do 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.

Protecting yourself

Before scanning a QR code in an email or letter make sure you trust the organisation that's sent it to you. Be suspicious of any "too good to be true" offers or prices. Do your research first, read reviews of the site and verify that the company exists.

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.

How we help to protect you online

- We will never ask you to disclose your whole password to us except when you specifically want to change it and you can only do this once you have logged into your account. When you log in we will randomly ask for three characters from your password
- All pages that display or collect personal information are encrypted. Look for the padlock symbol in your browser status bar
- A team of independent security experts regularly test our website and mobile app
- We may contact you by telephone, either to check details of changes you have requested online, or to authorise a payment you have set up using internet banking. It is important that you keep us informed if you change your contact details, and if possible provide more than one number on which you can be contacted. If you receive a call and haven't made a payment or any changes, please contact us as soon as possible
- To reassure our emails to you are genuine we will include the last 3 digits of your post code
- We do not use email to communicate confidential account information to you except where you specifically request and agree to this
- We will verify your identity before disclosing confidential information over the telephone or resetting your password
- Your session will time out after a period of keyboard inactivity
- Access to your online account will be locked out after so many failed access attempts. You will need to call us to reset your account
- After several failed biometric access attempts on a mobile app you will be required to re-register your device
- If you fail biometric login on the YBS app and then incorrectly input your password three times your account will be locked. You will need to call us to reset your account.

Financial and economic abuse

Domestic, financial or economic abuse can take a variety of different forms within different relationships, including intimate partners, family members or carers. It might be financial control, exploitation or sabotage. This can happen within partner relationships, care homes or wider family groups.

If you are suffering from domestic, financial or economic abuse, please reach out to us and we can offer you extra support.

Useful contacts

For further information on fraud scams please ask for a copy of our leaflet which is available at branches and agencies, or view the information on the security pages on our website.

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.

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 think you have had your identity stolen
- You have any concerns about security.

TO FIND OUT MORE:

TALK TO THE TEAM
CALL 0345 1200 100
YBS.CO.UK

Our printed material is available in alternative formats e.g. large print, Braille or audio. Please call us on **0345 1200 100**.

YBM 3512 (A5) 30 09 23