WELCOME TO YORKSHIRE BUILDING SOCIETY

We are one of the largest building societies in the UK, with nearly 3 million members and assets of over £58 billion. Owned by and run for you, we answer only to our members, not to external shareholders. We pride ourselves on treating you as an individual and putting your needs at the heart of everything we do.

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 becoming a victim of identity theft and fraud.

What is identity theft and fraud?

Identity theft is when someone takes 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.

- Unauthorised financial fraud losses across payment cards, remote banking and cheques totalled £730.40 million in 2021*

*Source: UK finance, Fraud - the Facts 2022.

Don't ignore the problem

You may think it's unlikely you will become a victim but it isn't until you apply for credit and have an application rejected that you find out that you've had your identity stolen. Identity theft is not a victimless crime and if you don't act quickly and are blacklisted for credit, it could take years to put right, and you might have difficulty obtaining a mortgage and other credit.

How does it happen?

Criminals use many methods to obtain 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 'phishing' websites that may look similar to real websites to capture your personal information.

How can I protect myself ?

There are numerous ways you can prevent yourself from becoming a victim of 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
- ☑ 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
- ☑ Remember a bank or building society would never ask you for your PIN or whole security number or password over the phone or by email
- ☑ 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.

Offset card accounts

- If you have an Offset card account with us, don't let anyone else use your card
- Keep your card safe and the PIN secret. Don't write your PIN down
- Sign any new cards as soon as they arrive
- Keep an eye on the card expiry date. Call us if your replacement doesn't arrive
- If you lose your Offset account card or have it stolen, tell us straight away
- When entering your PIN at a cash machine use your spare hand and body to sheild the number from prying eyes and hidden cameras
- Don't use an ATM which appears to have been tampered with and report any suspicions.

Cheques

- When writing personal cheques ensure the payee details include your name (including initials) i.e 'Yorkshire Building Society a/c (your name)', and draw a line through any unused space on the payee line
- If you request a cheque payable to another institution do not make the cheque simply payable to the institution – include the payee account number and name
- 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 hacking into 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
- Remember we will only ever ask you to use three characters from your password as part of our online login process. We will NEVER ask for the WHOLE of your password, except when you want to change it
- 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 PC or laptop you are using to access our online services cannot be overlooked by another person
- When you have completed your transaction or want to take a break, logoff 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.

Third Party Providers

When accessing your accounts or making a payment using an authorised Third Party Provider (TPP), make sure you take the following steps to protect yourself:

- Check with us if your account(s) can be accessed through a TPP, before providing any personal/ account details
- Check with the relevant regulator whether the TPP is genuine before you use it. In the UK, this is the Financial Conduct Authority (FCA)
- Ensure you use the genuine TPP's website. Fraudsters often set up fake versions of websites in an attempt to obtain information
- If you receive any communication from or about a TPP regarding account access or a payment which you have not authorised, contact us as soon as possible
- If you are asked for any security details you are not normally asked for check this with the TPP before providing any information..

Phishing

Phishing is a common type of fraud where emails are sent with links to fake websites, encouraging people to enter personal, login/card details or account information. Victims may also run the risk of their computer or smartphone being infected by viruses.

Vishing

Short for 'voice phishing', vishing is a type of scam where a fraudster calls claiming to be from a bank/building society, the police or other legitimate company. The fraudster usually advises the victim that there is a problem with their account, computer or card and tries to obtain details from them. They may ask for funds to be transferred to a 'safe' account, or attempt to arrange collection of bank cards or withdrawn cash.

Smishing

Short for 'SMS phishing', smishing is when fraudsters attempt to obtain personal or security details of a victim through the use of SMS text messages.Using any of the methods listed above, fraudsters can obtain enough information to allow them to commit identity theft and bank fraud.

If you receive any emails, calls or texts asking for personal or account information unexpectedly:

DO NOT provide any information, or reply to any emails or texts.

DO NOT follow any instructions given to you, even if they suggest that action is required urgently.

NEVER click on unsolicited website links.

Call your bank, building society or Third Party Provider for help and advice, on a number YOU have verified as being genuine.

Quishing

Quishing uses a QR code to take you to a fake website where you're encouraged to enter information that can be used to steal your identity or to defraud you - for instance, personal or account information, or your login or card details. Before scanning a QR code in an email or letter make sure you trust the organisation that's sent it to you and you have an idea where the code is taking you to. If in any doubt, don't enter any personal information. If a QR code on a poster, advert or leaflet looks to have been tampered with or stuck on over the top of an original one, do not scan it.

Remember:

- We will NEVER ask for the whole of your password, only three characters from it (except when you want to change it)
- We will NEVER send you an SMS 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
- We will NEVER send you an email with a link that directs you straight through to any kind of login page
- 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/

- http://www.yorkshirebuildingsociety.co.uk/

- https://online.ybs.co.uk/

- http://email.ybs.co.uk

- http://surveys.ybs.co.uk

- http://www.ybs.jobs

- 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@emis.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.

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 or a Third Party Provider. It is important that you keep us informed if you change your number, 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
- 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 a number of failed access attempts. You will need to call us to reset your account
- After multiple 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.

FURTHER INFORMATION

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

There's lots of security advice available. The following links might be useful, but Yorkshire Building Society doesn't specifically endorse any of the advice or products offered or sold on these sites:

- www.actionfraud.police.uk
- www.fca.org.uk/consumers/scams
- www.financialfraudaction.org.uk
- www.getsafeonline.org
- www.moneyhelper.org.uk/en
- www.cifas.org.uk

CONTACT US

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**.