Keeping your money safe

We know you've worked hard for your money and trust us to look after it, so keeping your data and money safe is our priority.

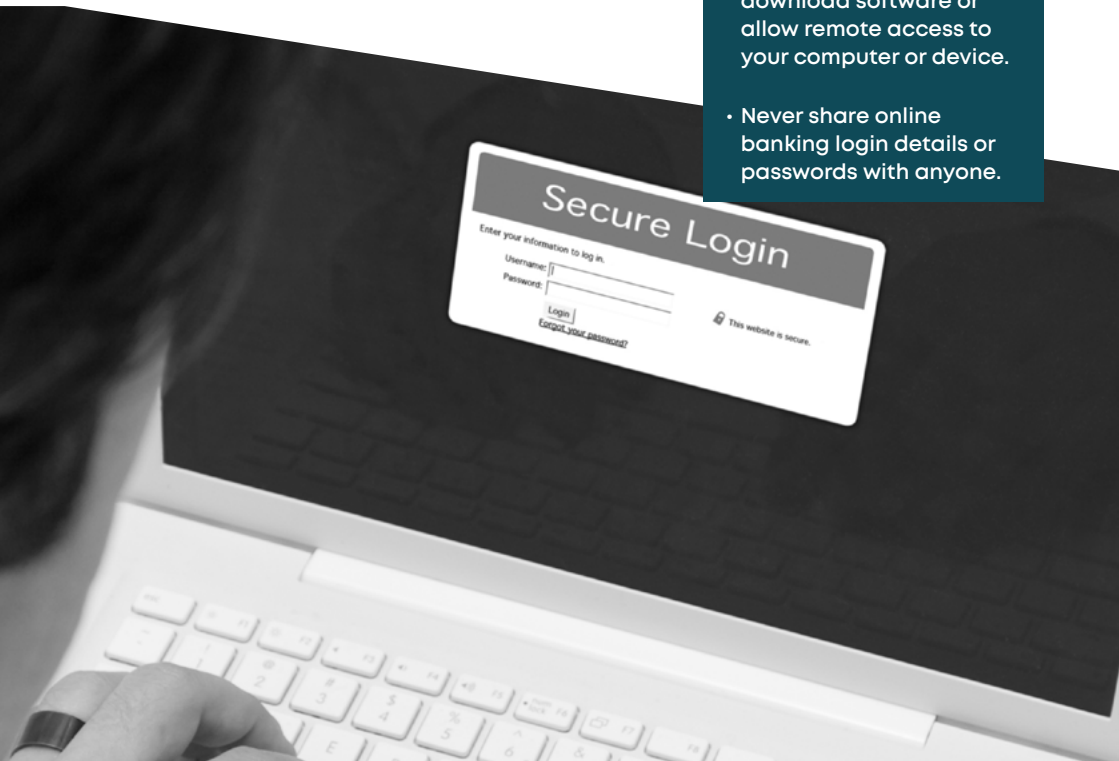
We're always on the lookout for threats from fraudsters. Understanding the latest methods that fraudsters might use to try to gain access to your savings accounts will help you to spot if something isn't quite right and take action if you think you may have fallen victim.

Latest scams and what to look out for

Remote access or computer software scams

This type of scam tries to convince you that you have a problem with your computer or internet connection. You'll be called by someone who claims to be from your telecoms or broadband provider and they'll request remote access or ask you to download software to your computer to fix a problem. By providing access or downloading the software, you're providing the scammer with access to your computer. They'll then look to compromise your security by accessing your sensitive information or financial accounts.

- Make sure that you have the most up to date security software installed on your computer, tablet and mobile, including antivirus protection.
- Never provide sensitive or personal information to an unsolicited caller.
- Don't be persuaded to download software or allow remote access to your computer or device.
- Never share online banking login details or passwords with anyone.



Safe account scam

You'll be contacted by someone claiming to be from a trusted organisation such as your bank (typically the fraud team) or the police, who'll tell you that your account has been compromised in some way and that you need to move your money to a "safe account". The details they'll give you will be fraudulent and once you move your money they'll have access to it.

- Your bank or the police will never ask you to move money to a "safe account" or send someone to your home to collect cash, cards or cheque books if you are a victim of fraud.
- If you're ever suspicious about any contact, always call the organisation back on a number you can trust (e.g. as detailed on your account statement).

Push payment fraud

Push Payment Fraud is where scammers convince you to transfer money to them. The scammers may pose as a legitimate business or individual who is known to you, typically via email, to inform you that their bank account details have changed and to make a payment to the new account. The scammer may have intercepted emails and therefore have information to make them appear convincing, such as information about who you are due to make payment to.

In an investment scam, a criminal may try to convince you to move your money to a fictitious fund or to pay for a fake investment. They'll usually promise a high return to entice you into making the transfer.

From 7th October 2024, new UK regulations will improve protection for customers affected by Authorised Push Payment (APP) fraud. These rules strengthen refund rights for payments made via Faster Payments (FPS) or CHAPS, enhance fraud detection by banks, and simplify the claims process with stricter reporting standards.

You may be eligible for a refund if:

- → You made a payment through Faster Payments or CHAPS to a UK account.
- → You submit your claim within 13 months of the final fraudulent payment.
- → The current maximum limit that can be claimed is up to £85,000.

- For Business Savings customers, if you'd like to learn more, visit our FAQ page.
- For Personal Savings customers, if you'd like to learn more, visit our FAQ page.
- For Corporate Deposit customers, if you like to learn more visit our web page.

- **If you're expecting to make a payment online or over the phone, always check the details with the person or business you're paying, via an independently verified source, before you send your money.**
- **Chances are, any offer you receive out of the blue is likely to be a scam. If you're considering an investment, always make sure that you do some research before carrying out a transaction. The Financial Conduct Authority's (FCA) warning list details firms and individuals that the FCA knows are operating without the correct level of authorisation.**

How could a fraudster contact you?

Email Scams (Phishing)

Email fraud is commonly referred to as ‘phishing’. Always be suspicious of unsolicited emails that are supposedly from your bank or some other trusted organisation because the address can be easily faked. The email will typically encourage you to click a link and log into your account, by telling you your account has been locked or that there’s been an unauthorised login attempt. In reality, the link in the email goes to a fake website which collects your information or targets your computer with a computer virus.

Another version of this scam involves an email attachment, which is in fact a computer virus.

- Be sceptical when it comes to your emails – if one looks even remotely suspicious, don’t open it or click on any links.
- Look at how you’re addressed. Scammers will often use a general greeting such as Dear Sir, Dear Madam or Dear Customer. Poor spelling or formatting can also be giveaways, but you cannot always count on that.

Phone Scams (Vishing)

Vishing ("voice phishing") is the same as phishing, but you'll be contacted by telephone rather than email. You'll get an unsolicited phone call encouraging you to give out your personal details, such as sensitive financial information. The fraudsters might call you on your mobile phone or landline pretending to be calling from your bank or another mainstream provider offering a 'one time deal' or an unsolicited upgrade. They may already have some of your personal information such as your name, address, or phone number to make them sound genuine.

- Never give remote access to any of your devices while on a phone call as criminals may then be able to log in to your online banking.
- Never give out your personal details (such as your online banking login details) over the phone, even to a caller claiming to be from your bank or the police.
- If you get a call asking for this information, end the call immediately, wait at least 5 minutes and contact your bank on a trusted number. Never call back on a number that the caller has given you.

Text Message Scams (Smishing)

A text message might not be from who you think – Smishing is when scammers pretend a message is from your bank or another organisation you trust. They will usually tell you there's been fraud on your account and will ask you to deal with it by calling a number or accessing a hyperlink. Please take a moment to stop and think if the message has come from a legitimate source.

You can find out more about email, phone and text message scams, and tips on how to spot if something isn't quite what it seems, on the security pages on our website at aldermore.co.uk

- **Don't click on any of the links, and check the number with your bank or financial institution to ensure that it is genuine.**
- **If you click on the link by mistake, run a scan with your antivirus software to check for any malicious software.**

Protecting your identity

Usually, identity thieves work online, looking for snippets of information about your life in social media posts and profiles, and unprotected email accounts.

They exploit the fact that people like to share personal information with their online friends – and can be lax with security. Equally, they can find confidential information like National Insurance and bank account numbers in un-shredded rubbish.

It doesn't take many of these snippets for them to successfully steal your identity and wreak havoc with your life.

Protection Registration

If you feel that you've had your identity compromised, you can request Protective Registration with an organisation known as Cifas. They'll add a warning flag against your name and other personal details in their National Fraud Database. This tells any organisation that uses Cifas data to pay closer attention when your details are used to apply for their products or services. Knowing you're at risk, they'll carry out extra checks to make sure it's really you applying, and not a fraudster using your details.

You can find out more at **cifas.org.uk/pr**

- Never share account details or other information that you use to prove your identity with friends, family or other people.
- Think about what you share on social media, such as date of birth and family members' or pets' names you also use in your passwords. Don't post details or images of your driver's licence, passport, NI number or other confidential items.
- Never reveal private information in response to an email, text, letter or phone call unless you're certain that the request is authentic. Call to check, on the number you know to be correct.
- Install the latest software, app and operating system updates on your computer and mobile devices. Better still, set them to update automatically.
- Make sure all your passwords are strong and keep them safe. Don't use the same password for more than one account. Use a strong and separate password for your email accounts.
- Don't connect to public Wi-Fi hotspots when doing anything confidential online.
- File sensitive documents securely, and shred those you no longer need.
- The minimum a fraudster needs to steal your identity is your name, date of birth and address. However, the more information they can harvest the better their chances of success. Other valuable information is your bank account details, NI number, email address, phone numbers, place of work and job title.

Contact us

If you're ever in any doubt about whether a communication you've received from us is genuine, or you suspect fraudsters might be trying to gain access to your money, please call us straight away on:

0345 604 2678

Our UK based call centre is open:

Monday to Thursday 8.00am - 8.00pm

Friday 8.00am - 6.30pm

Saturday 9.00am - 5.00pm

Sunday 10.00am - 4.00pm

Closed Bank Holidays

Other useful contacts

Action Fraud

Action Fraud is the National Fraud & Cyber Crime Reporting Centre in the UK where you should report fraud if you have been scammed, defrauded or experienced cyber-crime.

Call **0300 123 2040** or visit **actionfraud.police.uk**

Get Safe Online

The Get Safe Online website provides practical advice on how to protect yourself, your computers and mobile devices against fraud, identity theft, and viruses.

Visit **getsafeonline.org**

Visit **fca.org.uk/scamsmart**

Things to remember

We've joined other UK financial services providers in Take Five, an initiative led by UK Finance. Its aim is to encourage people to stop and take time to think before they act.

You can find out more at **takefive-stopfraud.org.uk**, but always remember these five rules:

1. **Never disclose security details, such as your PIN or full banking password**
2. **Don't assume an email, text or phone call is authentic**
3. **Don't be rushed – a genuine organisation won't mind waiting**
4. **Listen to your instincts – you know if something doesn't feel right**
5. **Stay in control – don't panic and make a decision you'll regret**

TAKE FIVE TO STOP FRAUD™

Aldermore

Aldermore Savings' documentation is available in Braille, large print and audio versions.

ASV0516-1024