

Protecting Your Money

How to Spot a Scam



Penrith
building society

How to spot a scam

At Penrith Building Society, keeping you and your money safe really matters to us. Sadly, scams are becoming more common—and more convincing. The good news is that with a few simple steps, you can protect yourself.

We've put together this handy guide to help you spot the warning signs of common scams, understand what to do if something doesn't feel right, and learn how to stay safe.

We're committed to protecting your money and personal information - but staying safe is a team effort. That's why we've also included some top tips to help you stay ahead of scammers.

Stay one step ahead of scammers

Scammers try to trick people into giving away personal or financial information, often through phone calls, emails or text messages. But if you know what to look out for, you can spot the warning signs and protect your money.

A little caution goes a long way. If something doesn't feel right, it's always okay to double-check. Staying alert is the best way to stay safe.

Be cautious if you're ever asked to...

...take a call from someone claiming to be from our building society or another trusted organisation.

We'll never ask you to share one-time passcodes or personal details over the phone. And we'll never tell you to move your money to a 'safe account'. No genuine bank, building society, the police, or government department would ever ask you to do that.

...click on a link in a text or email to log in or update your details.

Whether you manage your account online or in-branch with your passbook, we'll never ask you to log in or give personal information by clicking on a link in an email or text. If something doesn't feel right, it's always best to contact us directly or pop into your branch.



Online Purchase Scams

You find a real bargain online, like a car, mobile, or concert tickets. The seller wants you to use a different, less secure payment method, than the one the website advises. It's a method that won't protect you if things go wrong.

You've been emailing the seller all along, so you believe everything should be fine. But as soon as you've moved the money from your account, the emails from the seller stop. And that bargain you set your heart on never turns up.



Always use a reputable website or app to buy goods. For more expensive purchases, make sure you see what you're buying before parting with any money.

Phone, Text or Email Scams

Fraudsters use fake emails (phishing), texts (smishing) or phone calls (vishing) to pretend to be a genuine company like your bank or building society, the HMRC or sometimes even the police. They will quite often ask for bank details or for you to follow the "link" which can download malicious software or call a premium number.



If you are ever in any doubt, contact the company directly using a trusted contact number for them to confirm they have been trying to get in touch.

Rogue Trader / Doorstep Scams

Someone who looks like a tradesperson comes to your home and tells you urgent work needs to be done (like to your roof or driveway). This work may not even be necessary.

Typical scam outcomes are they:

- Overcharge you for their work.
- Convince you to make full payment for partially completed work or materials.

You pay them and never see them, or your money, again.



Don't feel rushed to get work done by someone knocking on your door. Take your time, do your research, and get several quotes before making any decision.

Refund Overpayment Scams

Someone calls saying they're from a broadband or telecoms provider. You may even hold an account with them. They say there's an issue with your computer and can fix it if you give them remote access (access your computer from their location).

They'll tell you there's compensation for the inconvenience and will ask you to log in to your internet bank.

At this point, they claim to have made a mistake and paid you too much. What they actually do is transfer money from your savings account to your current account. It looks like a refund has been credited to your current account. You won't know this, though, and they'll ask you to transfer the overpayment of the 'refund' back to them.

Next thing you know, they're using your security details to send your money to them. And just like that, a large sum of your money is gone.



Don't get rushed into allowing remote access. Be sure who you are dealing with. Never log in to your internet bank account while someone has remote access to your device.

Investment Scams

These are usually initiated with an unexpected phone call, letter, email or social media message. They may offer opportunities that sound too good to be true and they probably are too good to be true.

These types of scams are extremely dangerous because the losses are potentially huge. Always consider your options carefully before you make a decision. Try using the 'How to spot a Scam' questions below.

Report Suspicious Activity and Fraud

If you notice anything unusual or unfamiliar on your account, please contact us straight away. If you've been a victim of fraud, cyber crime, or suspect an attempt, it's important to report it as soon as possible:

Email - enquiries@penrithbs.co.uk

By phone - 01768 863675

Report Fraud

The UK's national fraud and cyber crime reporting service is now Report Fraud.

Online: reportfraud.police.uk

Phone: 0300 123 2040

Report Fraud aims to provide a better experience for victims and improve the response from law enforcement. If you are in Scotland, fraud should be reported to Police Scotland by calling 101.

For more information, visit reportfraud.police.uk.

If you've been a victim of fraud, cyber crime, or suspect an attempt, report it as soon as possible.

Report Fraud is the UK's national fraud and cyber crime reporting centre.

Rental Scams

You find an advert for an attractive property or room with below market rent. When you contact them for a viewing, you may be asked to pay the deposit immediately before viewing. They tell you the deposit is to prevent 'time wasters', it's a 'holding deposit' or that it's refundable if you decide not to rent the property.

You send them your money and try to set up a viewing, but they never get back to you. You can't reach them, and just like that, your money's gone.



If the rent being advertised is a bargain and looks too good to be true, it's probably a scam. Never pay a deposit before even seeing the property and no contracts should be signed until you've seen it in person.

If the property is advertised as being let through a local agency, then a call or visit the agency's registered office to confirm whether it's genuine.

Romance Scams

You meet someone new online. But can you be sure they are genuine?

Maybe they're in another country and say they need financial help to:

- Care for someone close to them.
- Avoid persecution.
- Cover travel expenses to visit you.

They've earned your trust. You've developed strong feelings. What's to stop you transferring large sums of money to them? And how would you feel if you never heard from them again immediately afterwards?



Keep conversations through a reputable dating agency. Never send money to or receive money from someone you've only ever met online.

WhatsApp Scams

Fraudsters use messaging apps like WhatsApp to pretend to be someone you know. They won't know your name, so a message could begin with 'Hi mum' or 'Hi mate'.

They'll tell you about a problem and ask you to pay money to a bank account you've never paid before. Usually, they'll say it's to help pay a bill but watch out for other excuses too.



If you get a message like this - out of the blue from an unknown number - don't reply, just delete it.

Talk to your family member or friend first - to check if it's real. Call them on a number you trust, like the one saved on your phone. Never call the number from the message.

Courier Scams

Someone calls you claiming to be from your building society or bank, or the police. They might claim there's an issue with your bank account or ask for your help with a bank or police investigation.

As part of a fake investigation, you may be asked to take out money or to buy something. The person is just tricking you into giving them money or goods.



Your bank, building society or the police would never contact and ask you to do this. Never take out money or buy goods if you are asked to as part of an 'investigation'.

Spotting a scam can be difficult and fraudsters can be very convincing; below are some common signs of a scam. Remember to ask yourself these questions before handing over any details or carrying out a transaction from your bank or savings account.

If the answer is YES to any of these, say NO.

- Did they contact you out of the blue?
- Are you asked to share personal details?
- Are their contact details vague?
- Did they ask you to keep it quiet?
- Is the deal too good to be true?
- Have you been pressurised to respond quickly?
- Are there any spelling or grammatical mistakes?

Please share this information with family or friends. By staying alert and informed, we all play a part in keeping our community safe.

A member of the Building Societies Association. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Financial Services Reg No 164473.



www.penrithbs.co.uk



7 King Street, Penrith, Cumbria CA11 7AR



01768 863675



enquiries@penrithbs.co.uk