How to spot a scam

Things you can do to protect your money.

financial planning & advice

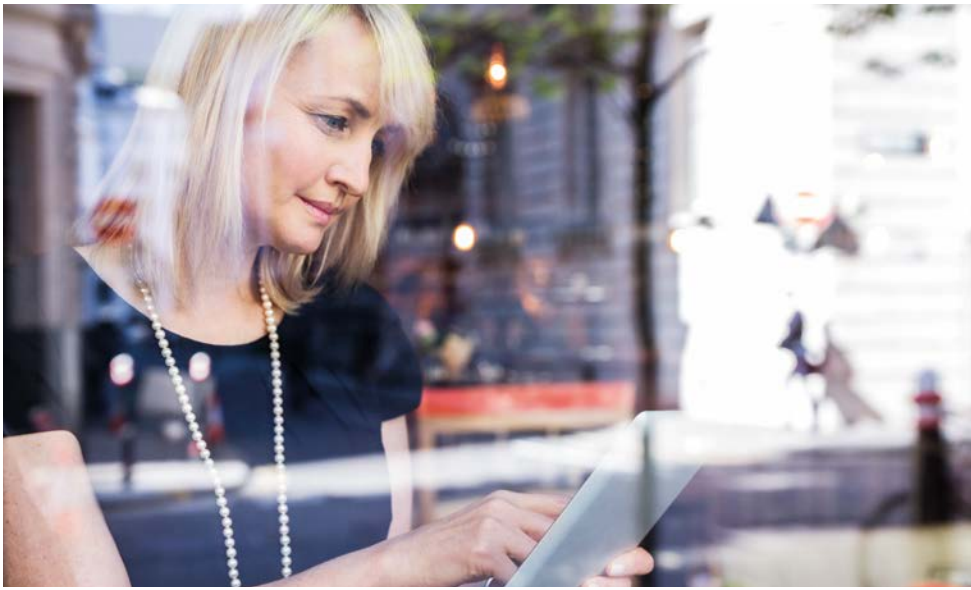
SKIPTON BUILDING SOCIETY
Since 1853

Introduction

Back in 1821, a Scotsman named Gregor MacGregor invented a fictional country he called Poyais. He persuaded hundreds of people to invest in his non-existent Central American land.

MacGregor printed adverts, fake maps and a 355-page guidebook about Poyais, and even arranged for 250 boats to sail to his imaginary country, in search of a better life. When they got there, all the travellers found was an inhospitable jungle. In total, MacGregor scammed £200,000 (about £21 million in today's money) before fleeing to France.

In these modern times, few people would be fooled by the idea of someone inventing a country and selling it as an investment opportunity. But unfortunately, the spirit of MacGregor lives on. It's a sad reality of life that there are fraudsters out there trying to fool innocent people out of their money – and the scams they employ continue to grow more sophisticated and difficult to spot.



As technology continues to rapidly change the way we live our lives – and well-intentioned initiatives like the pension freedoms give us more control over our money – there are more opportunities for fraudsters to take what doesn't belong to them. Their tactics are more cunning, and evolve very quickly.

It means it's more important than ever to be wary of the possibility of being targeted by a scammer. At Skipton Building Society, we take the wellbeing of our customers very seriously. We don't want you – or your loved ones – to fall victim to a scam.

To help you feel more prepared for that possibility, this special guide outlines some of the most common forms of scams. You'll find information on the different types to watch out for, plus guidance on what to do if you suspect you're being targeted. If you think you have been scammed, there's also a step-by-step guide on what you need to do.

About scams

When it comes to scams, it's easy to think "that will never happen to me." But with fraudsters finding new techniques and angles, the reality is that anyone could be fooled.

For example, scammers can look and sound like the real thing – employing slick salespeople, producing glossy brochures and building impressive websites. There's also been a rise in scammers using social media channels, such as Facebook and Instagram, to target people. So identifying whether they're legitimate can be difficult.

In order to see past what might appear to be a genuine and professional appearance, it's important you can spot the warning signs.

For example:

- You're contacted out of the blue through cold-calls, text messages, emails or door-to-door salespeople.
- They attempt to pressure you to make quick decisions, or adopt pushy sales techniques.
- You're offered incredible-sounding deals, such as guaranteed investment returns or high interest rates.
- **If an offer appears too good to be true, it probably is.**

Authorised companies simply won't contact you out of the blue, unless you have provided appropriate contact preference permission for them to do so.

If you are approached in this way, the best course of action is to immediately report them to the Financial Conduct Authority (FCA) – **fca.org.uk**.

Coronavirus scams

When coronavirus hit the headlines, scammers didn't waste any time finding new ways to take advantage of people – especially their savings, investments and pensions.

Banking-related scams, insurance scams and pension fraud are amongst the most reported scam attempts since the pandemic began.

There has also been a jump in investment scams. Criminals have been targeting customers looking to earn a better return on their money amid the market falls caused by the pandemic. This usually involves scammers offering bogus investments in cryptocurrencies or currencies that do not exist.

On top of this, there's been an increase in impersonation scams – where con artists pretend to be tax officials, utility providers or bank staff, in order to seek payments and personal information.

One scam came under the guise of a text message from HMRC stating all UK residents are due a lump sum payment due to the coronavirus. To receive it, recipients must click a link and enter their card details. HMRC have since clarified they will never text, email or phone to ask for bank details or passwords.

We always stress to our customers the need to be vigilant when it comes to protecting finances from scam artists, but now more than ever we ask you to be on the lookout for potential fraudsters. Always remember, the golden rule is if it looks too good to be true – it probably is. And if you have the slightest doubt, please do contact us before proceeding with anything you're not sure with.

Pension scams

Pension scams have become increasingly common since reforms were introduced in April 2015, allowing people to access their pension pots from 55.

Defined contribution pension holders now have more options on how they access their pension from the age of 55. The reality that millions of people now have access to a significant pot of savings – and yet it's complicated to figure out how best to use it to fund retirement – is seen as a big opportunity for fraudsters.

The fraudster may offer to help you invest your pension with the promise of huge returns, but in reality steal your savings. They may even keep up the pretence they're investing your money, meaning it could take months or even years for victims to realise what has happened.

The good news is the FCA has now introduced a pension cold-calling ban. If you're contacted by a company or person you don't know regarding your pension, they're probably breaking the law. Those found to be in breach of the rules could face enforcement action from the Information Commissioner's Office, including fines of up to £500,000.

If you're contacted by a company regarding your pension out of the blue, it doesn't necessarily mean it's a scam. The organisation might be legitimate, and you may have in the past provided them with appropriate contact permission for them to speak to you. That said, you should certainly question the legitimacy of any organisation who contacts you unexpectedly about your pension.

It's absolutely right to be cautious – and to report, to the Information Commissioner's Office, anyone who you have strong reason to believe doesn't have the appropriate permission.

Early pension release schemes

It's not just people nearing retirement who are the target of scammers. If you're under 55, there's a possibility you might be approached and encouraged to access your pension early – through 'early pension release', 'pension liberation' or 'pension unlocking' scams.

Government rules state that only in rare – and extremely limited cases – would you be allowed to access your pension before 55. So if you're ever contacted by someone offering you access to your pension early, alarm bells should immediately sound.

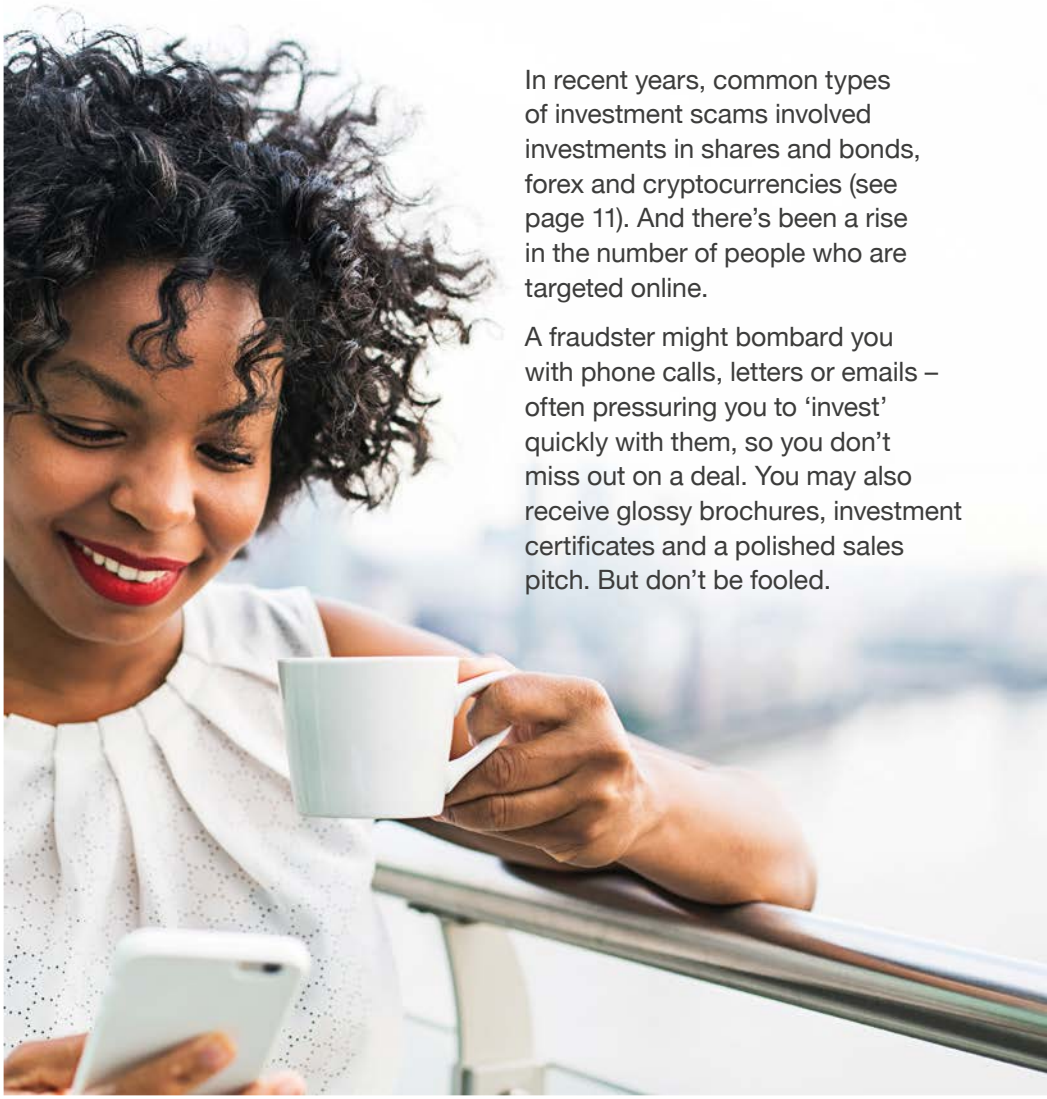
This is because early pension release schemes aren't authorised by Her Majesty's Revenue and Customs (HMRC), and funds withdrawn under this kind of scheme will suffer a tax charge of 55%.

Scammers claim they're able to release your funds in special ways, such as transferring your pension into an overseas scheme. An extortionate fee could be charged (often as much as 30%) and your money could be placed into high risk investments. Once your money is transferred into an 'early release' scheme, in some cases, the scam company will take the full amount of your pension pot. Your savings gone, just like that.

Of course, there might be circumstances where you want to consider accessing your pension before you reach 55. If that's the case, the FCA recommends you seek professional advice first. You should also check the company who has approached you is authorised and regulated by the FCA, and has a registration number you can look up on the FCA register.

Investment scams

No matter how savvy you are with your investments, you could still be caught out by a bogus financial adviser or advisory firm seemingly offering you something legitimate.



In recent years, common types of investment scams involved investments in shares and bonds, forex and cryptocurrencies (see page 11). And there's been a rise in the number of people who are targeted online.

A fraudster might bombard you with phone calls, letters or emails – often pressuring you to 'invest' quickly with them, so you don't miss out on a deal. You may also receive glossy brochures, investment certificates and a polished sales pitch. But don't be fooled.

Scammers often present offers that are exclusive, and you may be told not to discuss them with other people. They offer investments in 'unique commodities', which typically include wine, land banking, carbon credits, diamonds and graphite – with the promise of high returns of onwards sales to large multi-national companies.

Should you be fooled into this type of scam, the investments you've been promised may wind up worthless.

Share fraud and boiler room scams

This type of investment scam is where victims are sold overpriced or non-existent shares, usually with the promise of high returns.

The fraudsters, posing as salespeople, are usually highly trained and well-versed in their investment proposition; providing impressive-sounding statistics and promising high returns. They often employ high pressure sales tactics to convince you to invest with them – and give you only a very short timescale in which to make a decision. They may ask you to commit to investing immediately, or contact you again within a very short timeframe.

Some of these companies have been known to advertise in the national press and set up fake company websites/social media accounts in order to appear legitimate and credible. Others 'clone' another entirely legitimate company, using a similar name and directing you to the real company website.

Some fraudsters contact would-be victims pretending to be from authorised companies. They typically cold-call investors to promote investment opportunities that are non-tradable, worthless, overpriced or even non-existent, using the name and FCA register number of a real company, to appear genuine. They'll supply their own phone number, company address and website address to the people they target.

How to combat this potential scam

- Should you be approached by a company and are unsure if they really are who they say they are, as a first step you should check the FCA registration number they provide on the FCA register. Here, you'll also find the switchboard number of the real company.
- It's recommended you call the company back using the number on the FCA website, to verify they're the genuine company and not a clone.

Unregulated investments

It's important to note that sometimes you will be contacted by a legitimate firm, discussing investments that are unregulated but are not necessarily a scam attempt.

As the name suggests, a regulated investment means the FCA regulates the way it's sold to customers. If things were to go wrong and the regulated organisation went out of business, you would be able to complain to the Financial Ombudsman Service. You'd also have some protection from the Financial Services Compensation Scheme (the maximum amount of compensation available depends on the type of investment business and the circumstances of the claim).

With an unregulated investment, you're not covered in these ways. It's therefore really important to make sure you always understand what you're investing in.

Cryptocurrency

Over recent years there's been a huge rise in popularity of cryptocurrencies – a digital or virtual currency that investors buy and sell. The most well-known types of cryptocurrencies include Bitcoin and Ether.

As this type of investment is so new and is so far relatively lacking in legal regulation, cryptocurrency is proving to be a ripe area for scammers to target. Fraudsters typically advertise cryptocurrency investments through social media – often using fake celebrity endorsements – to attract potential victims.

The adverts link through to professional-looking websites, where you're urged to invest using cryptocurrencies or traditional currencies. The cryptocurrency may not exist, or the scammer might distort the prices and investment returns. They're also known to close users' accounts with no prior warning, and refuse to transfer the victim's funds back (or will ask for more money to release the funds).

Most types of cryptocurrency investments are not regulated investments, which means you will not be protected by the Financial Services Compensation Scheme. If you invest in cryptocurrencies you should be prepared to lose all your money.

Nevertheless, the FCA has issued guidance on how to protect yourself from scam attempts. It states to be wary of online adverts promising high returns on investments in cryptocurrencies or cryptocurrency-related products. If you're considering making an investment, make sure you do your research on the product and firm offering the opportunity. By searching online, you may discover if others have posted concerns about the organisation.

Other types of scams

Phishing and vishing

Phishing involves an email claiming to be from your bank or another trusted institution, and **vishing** is similar, but done over the phone. You should be suspicious of any emails that look to be from reputable organisations, but have small differences in the email address that don't seem accurate.

Scare tactics are often used to obtain personal information such as bank account numbers, passwords, your PIN or other details. Genuine organisations should never ask you for personal details over the phone.

Fraudsters may impersonate your bank or public services such as HMRC or the police.

Courier fraud

This is a particularly distressing type of scam as it involves fraudsters impersonating the police or the victim's own bank. It begins with a phone call from someone imitating a police officer, who will tell you they have reason to believe criminals have your bank details and are planning to empty your bank account.

Number spoofing

This is where a fraudster calls a victim pretending to be their bank.

They use a device which can copy any number – even if the one they're calling from is entirely different – meaning the number of the victim's bank will flash up on display when they call.

Authorised push payment

This type of scam sees a fraudster pose as a legitimate service provider or business, to trick the victim into authorising a payment into another account – one that is usually controlled by the scammer. Alternatively, they might pose as your bank or even the police, and potentially use a cloned email address.

One such example, reported by the BBC in June 2018, saw the fraudster pose as the victim's builder by sending an email asking for payment. The con-artist had seemingly hacked into the email account to send the message, and collected £13,000 from the victim.

Payments made using real-time payment schemes cannot be reversed once the victim realises they have been conned.

If you're approached with a request for payment, don't automatically assume it's authentic. You also shouldn't give away any of your security details, such as your PIN or banking password. If you're unsure whether the payment is legitimate, ask to delay making it – a genuine organisation won't mind waiting.

Financial abuse

It's not just complete strangers who might attempt to scam you out of your money. Even people very close to you might misuse your money or other financial assets.

Financial abuse can take many forms. The perpetrator might control the way the victim spends their money – preventing you from doing certain activities, asking you to account for every penny spent and checking your receipts or bank statements. They may spend your money or make significant financial decisions without consulting you. Other examples may include running up debts in your name, withholding child maintenance payments or damaging your possessions.

This is a very serious issue, and the Domestic Abuse Act 2020 has widened the definition of domestic abuse in order to include financial abuse. This is prosecutable under the Serious Crimes Act 2015.

If you believe you might be a victim of financial abuse, Refuge has a 24-hour national helpline you can contact – call **0808 2000 247**. The charity has also produced a practical guide with support and information – visit **www.refuge.org.uk/get-help-now/support-for-women/financial-abuse/**

Other practical tips include:

- Freeze any joint accounts
- Change your PIN and online banking passwords
- Know where important financial documents are kept – potentially keep copies yourself or with a friend.

How to protect yourself from scammers

According to the FCA, "If it sounds too good to be true, it probably is." So be cautious of anyone offering you attractive, out-of-this-world deals.

- Do not commit to any deals or offers immediately. Go away and think about it before you make your decision.
- Be wary of anyone asking you to pay money upfront. This is usually an 'upfront payment' or 'advance fee' scam, and it's likely you won't see a penny in return.
- Don't sign anything or hand over your money until you've checked the credentials of the individual or organisation.
- Never respond to a cold-call unless you know the company which has contacted you. Even if what they're claiming to be selling offers a perfect solution, you should always do your own research to make sure a firm is legitimate.
- Never be pressured into any deals offered to you. The best advice is to simply hang up the phone, close the door, delete the email or throw away the letter.
- Financial services organisations can only legally operate in the UK if they have a register number (for example, ours is 153706). You'll only be covered by the Financial Services Compensation Scheme and the Financial Ombudsman Service if you deal with companies who are authorised and regulated by the FCA.
- If you're in doubt over whether a financial advisory company is genuine, ask for their FCA register number or visit: **www.fca.org.uk/register.**
- The FCA has also published a list of unauthorised firms to avoid doing business with (although it warns their names are likely to change regularly). This list appears on the FCA website and is constantly updated. However, even if a company who has approached you isn't on the list, it doesn't mean it's a legitimate organisation (as the FCA may not yet be aware of it).

Protecting your identity

The number of identity fraud cases in the UK has continued to be very high each year, with a large amount of them taking place online.

In particular, social media sites have become a hunting ground for identity thieves. And with more of our personal information stored on our smartphones – and the growth of public WiFi access – it's really important to be careful about the information you might be sharing.

If fraudsters are able to access enough information about you, they might be able to impersonate you and steal your identity. They could either open a new account or obtain new credit cards or loans using your identity, or take over your own existing accounts by impersonating you and changing the address of your account.

Often victims don't even realise they've been targeted until a bill arrives for something they didn't buy, or they experience problems with their credit rating. By regularly checking your credit report, you can identify any suspicious credit applications which could suggest fraudsters are using your details to fraudulently obtain credit in your name.

Organisations need to legitimately verify an identity before opening an account or issuing goods or services. They need to ensure the person applying for credit is who they say they are – and lives where they claim to live. In the UK, there is no single document used to prove identity.

At the moment, organisations use various methods to verify an identity, including personal details such as:

- Name
- Date of birth
- Address
- National Insurance number
- Appearance on various database (eg eligibility to vote)
- Mother's maiden name

And also a mix of documents and records, including:

- Passport
- Driving licence
- Birth or marriage certificate
- Bank statement
- Payslips
- Utility bills
- Educational qualifications
- Benefits/tax document

If any of these documents fall into the wrong hands you could end up being the victim of identity fraud. You should never send any of these original documents in the post, or email them unsecured. For personal documents like bank statements and utility bills, it's good practice to shred them when you no longer need them.

It's more important than ever to protect yourself against identity theft. Don't respond to unsolicited emails and phone calls asking for personal information or passwords, and always look to use different passwords for different accounts – especially with online banking. Stronger passwords will also help to reduce the chances of enduring identity theft.

The procedures used by organisations to check the information supplied by customers helps detect and prevent most identity fraud. However, some fraudulent applications are accepted due to the sophisticated techniques used by the fraudsters.

What to do if you've been scammed

If you're worried you've been duped:

1. **Stop sending your money (providing it's not too late)**
   If the scammers have your bank account details, contact your bank immediately to notify them. They may be able to help stop the payment.

2. **Report the scam to the FCA**
   Call **0800 111 6768**, providing as much information as possible about your investment and what's happened.

3. **Report it to the police**
   Call the Action Fraud line on **0300 123 2040**.

4. **Contact us**
   If you're worried you're being targeted by a scam company in relation to your Skipton savings or investments, you can contact us on **0800 055 6898*** to discuss your concerns. Whilst it's often difficult for us to establish whether an investment opportunity is legitimate, we're always on hand to offer help and advice if we can.

5. **Beware of ongoing and recovery scams**
   If you've lost money or have been contacted by a fraudster, you're likely to be targeted again. This could be someone offering to help you recoup your stolen money by charging you a fee in return for their help.

   If you provide any personal details over the phone or online, these scammers will then have access to your details and be able to extract money from your accounts.

6. **Don't be embarrassed – speak up**
   Victims often feel ashamed that they've been fooled. But don't be. Scammers are extremely cunning and can deceive anyone, regardless of their age or experience.

For more details, please visit:
fca.org.uk/consumers/scams/what-to-do-if-you-are-scammed

Useful websites

www.fca.org.uk/scamsmart

The regulatory body has a dedicated section on its website devoted to helping people avoid investment and pension scams. This includes a handy tool to help you check if an investment opportunity you have received might really be a scam.

www.cifas.org.uk

Cifas offers fraud prevention advice and identity protection for individuals and vulnerable groups of people. See the Cifas leaflet 'Don't be fooled'.

www.skipton.co.uk/security-centre/fraud-awareness

Visit our website for further information on scams.

www.takefive-stopfraud.org.uk/about/take-five

Take Five is a national campaign that offers straightforward and impartial advice – to help people protect themselves from preventable financial fraud.

www.actionfraud.police.uk

Run by the National Fraud & Cyber Crime Reporting Centre, you'll find lots of useful information about types of fraud and ways to prevent it. You can also use the site to report a scam.

www.refuge.org.uk

The domestic abuse charity provides information on types of financial abuse, including the steps you can take if you are a victim.

www.citizensadvice.org.uk/consumer/scams/scams/

Citizens Advice provides free, independent and confidential advice about your rights and responsibilities – the organisation can also help you to report a scam.

Get in touch, contact your adviser at your **local branch**
go to **skipton.co.uk** call **0800 055 6898***

If you'd like this booklet in large print, braille or audio please ask in branch or call 0800 055 6898.

*To help maintain service and quality, some calls may be recorded and monitored. Calls to 0800 numbers are free from BT landlines and mobiles.