Queen’s Park Trust

version v1.0, dated 28th May 2026

Protect Yourself from Online Scammers

Contents

Protect Yourself from Online Scammers

Spot the warning signs

Scams can be difficult to spot. Fraudsters can be convincing and knowledgeable, with websites and materials that look identical to the real thing.

But if you've been contacted unexpectedly, or are suspicious about a call or text message, make sure you stop and check the warning signs.

- **Is it unexpected?** Scammers often call out of the blue. They may also try and contact you via email, text, post, social media, or even in person.
- **Do you feel pressured to act quickly?** Scammers might offer you a bonus or discount if you invest quickly, or they may say the opportunity is only available for a short time.
- **Does the offer sound too good to be true?** Fraudsters often promise tempting rewards, such as high returns on an investment.
- **Is the offer exclusively for you?** Scammers might claim that you've been specially chosen for an investment opportunity, and it should be kept a secret.
- **Are they trying to flatter you?** Scammers often try to build a friendship with you to put you at ease.
- **Are you feeling worried or excited?** Fraudsters may try to influence your emotions to get you to act.
- **Are they speaking with authority?** Scammers might claim that they're authorised and often appear knowledgeable about financial products.

If you answered 'yes' to any of these questions, or you're unsure if a contact is genuine, follow the steps below to protect yourself.

How to protect yourself

Do:

- Treat all unexpected calls, emails and text messages with caution. Don't assume they're genuine, even if the person knows some basic information about you.
- Hang up on calls and ignore messages if you feel pressured to act quickly. A genuine bank or business won't mind waiting if you want time to think.
- Check your bank account and credit card statements regularly.
- Consider getting independent financial advice or guidance before a big financial decision.
- Check overseas regulators if you're dealing with an overseas firm.

Don’t:

- Give out your bank account or credit card details unless you're certain who you’re dealing with.
- Share your passwords with anyone (including your social media passwords).
- Give access to your device by downloading software or an app from a source you don’t trust. Scammers may be able to take control of your device and access your bank account.

Banking and online account scams

- Banking scams can take many forms, with fraudsters using a number of tactics to steal your money. Find out what these scams are and how to protect yourself.

Telephone scams

Vishing

Vishing, or 'voice phishing', is when fraudsters call you pretending to be from your bank, HMRC, the FCA or other organisations.

These scams often use scare tactics to get you to act quickly. The fraudsters may claim your bank account is at risk, or that you owe money that must be paid immediately. They may also say that they’re calling from your bank's fraud team to check your account.

The call might be from a real person, or it might be an automated message. Either way, the scammers will try to get you to share important information, such as your account or login details.

To appear genuine, the scammers might also use number spoofing to get you to answer their call.

Number spoofing

Number spoofing is when fraudsters change the number displayed on your caller ID to look like they’re calling from a real bank or organisation. They will then try to trick you into sharing information about your account.

To protect yourself from vishing and number spoofing:

- Avoid answering calls from numbers you don’t recognise (let them go to voicemail).
- Hang up on suspicious calls.

- Never give out personal information unless you’re certain who you’re dealing with.

  Never share your bank account or credit card details unless you're certain who you're dealing with. If you've already given fraudsters this information, tell your bank immediately using the contact details on your card or statements.

Online banking scams

Phishing scams

Phishing is when fraudsters email or text you pretending to be from your bank. These messages will often ask you to verify information about yourself, including online banking passwords, your account or card details.

The message often comes with a story about why your details are needed, such as for a refund, a security check, or even to stop fraud.

Always remember that a bank will never email or text you to ask for your personal information or account details. Be especially careful if the message doesn't include your proper name or has spelling mistakes or poor grammar.

If you want to check if an email or text is from your bank, phone them to ask. Use the number on your card or bank statements, rather than any numbers in the message.

Website scams

Bank websites can be copied by criminals to get you to share personal information. These fake websites often look identical to the real thing and use addresses that are similar to the genuine bank.

As part of a phishing scam, fraudsters might try and direct you to a fake website using a link in an email or text message.

To protect yourself, make sure you carefully check the website address. Look for small differences, such as an extra letter or hyphen. It’s always better to bookmark your bank’s website address, so you know it’s the right one.

Card scams

Card details can be stolen by copying the information from the magnetic strip of a bank or credit card, usually at a cash machine or in a store. This is known as skimming.

If they get hold of these details, fraudsters can access your account or create a fake card that has your details on it.

To protect yourself against skimming:

- Never share your PIN and be careful that it's hidden when using it.
- Look for signs of tampering on ATMs.
- Check your bank statements regularly.
- Report any suspicious activity to your bank immediately.
- Tell your bank when you travel overseas.

Supplier scams

If you run a business, fraudsters may contact you pretending to be a supplier. They may say their bank details have changed and that you need to update your payments.

They may also email you pretending to be a senior member of staff and may try to persuade you to make an urgent transfer.

Remember, always check that the email address is the same as you've used before with your supplier. If you're suspicious, call them back on a number you're sure is genuine or speak with them in person.

Insurance and warranty scams

If you buy a mobile phone, a TV, or a home appliance, you may think about getting it insured. Especially if you'd struggle to get it fixed or replaced if something went wrong.

Some scammers take advantage of this by selling fake insurance.

Other fraudsters target individuals looking for cheaper car insurance. This is known as 'ghost broking', and it could leave you with no protection if you need to make a claim.

Ghost broking

Ghost brokers are criminals posing as legitimate insurance brokers. They sell fake or invalid insurance policies, often for cars, at seemingly cheap prices.

These fraudsters often use social media to target young drivers, producing fake documents that look very similar to the real thing.

They'll often ask you to use messaging apps like WhatsApp, hoping it will be harder for anyone to catch them. Once you've paid, they then disappear.

Getting caught with fake insurance can cause big problems. You could see your car seized and crushed by the police, face penalties of up to £300, and potentially face court and a driving ban.

If you have an accident, you could also have to cover the costs of any injuries or damage caused.

In some cases, contact with these fraudsters can lead to identity theft, which can seriously affect your finances and emotional wellbeing.

Warranty scams

A warranty is a guarantee to replace or repair an item if it breaks. It's usually provided by the manufacturer when you buy a product such as a washing machine.

Warranties are technically insurance contracts and because arranging and providing insurance is a regulated activity, the company offering it to you **must be authorised by FCA**.

The fraudsters may contact you unexpectedly soon after you buy an item or start a new contract.

They may claim they're linked to your provider, or the store or company where you bought the product. They may also advertise their offers on social media or on online forums, often at cheaper rates than real policies.

If you agree to the offer, the scammers may give you fake documents, or they may use fake details to buy cheaper insurance, which they then sell to you.

Unfortunately, you may only find out you don't have the cover you need when your claim is rejected.

Common warning signs

- **Not on the FCA Firm Checker**: The broker or insurance company is not listed on the Firm Checker.
- **Social media and messaging apps**: Scammers mainly use WhatsApp, Snapchat, Facebook Messenger, or Instagram rather than professional email or landline numbers.
- **No professional presence**: Scammers lack a legitimate company website, physical office address, or UK landline number.

- **Quick sell**: Scammers create artificial urgency to pressure you into purchasing quickly.
- **'Too good to be true' deals**: Often, the cost is significantly lower than quotes from reputable, mainstream insurers.
- **Unusual payment methods**: Scammers often ask for payment via direct bank transfer, cryptocurrency or cash, rather than secure, established payment systems.
- **Upfront fees**: Scammers often charge an upfront flat fee for their service.

How to protect yourself

1. **Check your policy**: You should always check the details on your insurance policy to make sure they're correct. This includes your name, address, contact details and the details of the item you need cover for.
2. **Check if they're real**: To make sure the firm or broker you're dealing with is genuine, search Firm Checker to find out if they're authorised and have permission for the service they're offering you. Only contact them using the contact details listed on the Firm Checker, to make sure you're dealing with the genuine firm. A firm or broker must be authorised and have permission for the right activities.
3. **Check your car is insured**: For car insurance, also check the Motor Insurance Database (Link is external) to confirm your vehicle is listed.
4. **Check-in**: If you're worried about a potential scam, or you think you may have been contacted by a fraudster, call FCA on 0800 111 6768.
5. **Report it**: If you've lost money to a scam, contact Report Fraud (Link is external) and then report it. If the incident involves a ghost broker, contact the Insurance Fraud Bureau via their Cheatline (Link is external) .

Loan fee fraud

Loan fee fraud or advance fee fraud is a common scam where individuals are conned into paying a fee for a loan.

The fraudsters often ask for between £25 and £450. But once the fee is paid, you'll never receive the loan you were offered.

How loan fee fraud works

Scammers will often try to target individuals who've applied for loans online. They may contact you unexpectedly and will offer you the money you need.

But before giving you the loan, they'll ask for an upfront payment as a deposit, administrative fee or insurance. They might claim it's because you have a bad credit history.

They'll often put pressure on you to pay the fee quickly via a bank transfer. Or they may ask you to buy a voucher, for example from Google Play, Amazon or Ebay. Scammers have even started asking for payments to be made via crypto exchanges.

The fraudsters may say the fee is refundable. But even though you make the payments they ask for, you'll never receive the loan – or a refund on the fee.

How to protect yourself

If you need to apply for a loan, you should only deal with authorised firms. If you don't, you won't be protected if things go wrong, and you could end up losing lots of money.

- Use the FCA Firm Checker to make sure a financial firm is authorised and has permission to provide the service you're looking for.
- Check that the firm's contact details match the details on the Firm Checker.
- Always use the contact details on the Firm Checker, rather than a direct line or email you've been given.
- If there are no contact details on the Firm Checker, or the firm says they're out of date, call FCA on 0800 111 6768.

How genuine loan fees work

Sometimes, genuine authorised firms will ask you to pay an upfront fee before they'll provide a loan. If they do, they must send you a notice setting out specific information.

Before you get the loan, you'll need to reply to the notice, saying you understand and agree with what it says.

The notice should include:

- The name of the firm as it appears on the Firm Checker.
- A statement that the firm is acting as a credit broker.
- A statement saying if you need to pay a charge for the firm's services.
- The amount of the charge (or how it will be calculated).
- When the firm will take payment from you and how you'll pay.

Money transfer scams

How money transfer scams work

Transferring money for someone might seem like an easy way to earn cash, but it's likely to be a scam and you could be committing a serious criminal offence.

You may be asked to accept a payment into your bank account. You're then told to forward the money to another account, or withdraw the cash, in exchange for a percentage of the payment.

The fraudsters may contact you via email or social media, or you may see an ad in a newspaper or online, offering commission on what seems like simple work.

It might be pitched as an opportunity to work from home as an 'account manager' or 'transfer manager'. You may be told that the money is for trading shares abroad, or even that you'll be helping a charity distribute funds.

But the criminals will probably use you as a 'money mule' to launder money.

Money laundering

Money is laundered to disguise where it came from. It's usually done to make the proceeds of crime look like they came from a legal source.

Once it's taken out of your bank account as cash, the money is almost impossible to trace.

By taking part in this scam, you could be helping to fund serious crime. If caught, you could be sentenced to up to 14 years in prison and receive an unlimited fine. You may also find it hard to access banking services or credit in the future.

Never share your bank account or credit card details unless you're certain who you're dealing with. If you've already given fraudsters this information, tell your bank immediately using the contact details on your card or statements.

Foreign money transfer scams

If you're contacted by someone claiming to be a foreign official who needs help transferring large sums of money, it's likely to be a scam.

Fraudsters usually say they're a government official, a doctor or a minister, and will ask for your help to transfer millions of pounds (or dollars) out of their country.

They'll often blame a recent disaster or a war for their request, and they'll promise to pay you a share of the money once you've paid a fee.

They'll claim that all you have to do is send an administration fee and your bank account details. But you may also be asked to pay for taxes, legal costs or even bribes.

The fraudsters often ask victims to send several instalments of increasing amounts, and some victims are even asked to travel overseas to complete paperwork. Once abroad, they're threatened or not allowed to leave until more money is paid to the criminals.

Transferring money upfront

There are many scams that may ask you to pay money upfront. This might be after an offer of a loan or credit, a new job or a lottery win.

You might also be contacted if you own shares in a company. The fraudster may offer to buy them, usually at a higher price than their market value. It might sound like a great deal, but they will usually ask for money upfront, as a bond or other form of security.

If you're asked to pay a fee in advance, you'll probably never hear from the fraudsters again once you've paid.

How to protect yourself

These scams are generally linked to organised crime, and you shouldn't respond in any way. Don't even reply to the fraudsters to tell them to stop contacting you. This will just confirm your identity and details.

Remember, it's highly unlikely that you've been specially chosen by someone living abroad. You're just one of many people that the scammers are trying to trick.

If you think you've been involved in money laundering, or you've lost money in a scam, contact Report Fraud immediately on 0300 123 2040 or via the website (Link is external) .

Remember, if you've given out any of your personal information, or have made a payment, tell your bank immediately using the contact details on your card or statements.

Screen sharing scams

What are screen sharing scams

A screen sharing scam is the method someone might use to take information from you or access your accounts to transfer your money. You may be contacted out of the blue through social media or over the phone. Or when searching online for an investment opportunity or the contact details for a company.

Once a scammer has contacted you, they will try and gain your trust and convince you they can help. The type of scams may vary, whether that's help with an investment or a banking service, the scammer will typically ask you to download legitimate screen sharing software.

This could be software you have heard of or have used before with work, friends or family. This could be software such as AnyDesk, Microsoft Teams, TeamViewer or Zoom. It could be through your phone, laptop or computer.

The scam can only take place if you download the software and allow them to take control of your screen. Once they have access to your screen, they can access your personal information. This includes any financial accounts, such as your online banking.

One of the main warning signs of a potential scam is if a firm or individual contacts you out of the blue. If you're asked to share your screen or provide remote access to your phone or computer, this is a warning sign it's a scam.

How to protect yourself

Even if you have searched for a company online and contacted the firm, you should never share your screen with them. Scammers may try to build trust, friendship or a sense of security with you. Be wary of being put under pressure to make any decisions. If it sounds too good to be true, it probably is.

You should only deal with financial services firms that are authorised by FCA. Use the FCA Firm Checker to find out if a firm is authorised and has permission for the service it's offering you. If you can't find a firm on the Firm Checker, contact them on 0800 111 6768.

Always be wary if you're contacted out of the blue, pressured to invest quickly or promised returns that sound too good to be true.

If you're contacted unexpectedly by a financial business, make sure you only reply using the contact details on the Firm Checker.

Always check the FCA Warning List before dealing with a company, to find out if they are known to be operating without our authorisation.

Find out more about how to protect yourself from scams.

You should seriously consider getting financial advice or guidance before investing. MoneyHelper has information on how to find a financial adviser (Link is external) and our InvestSmart pages will help you make better investment decisions.

If you've been scammed

If you're worried about a potential scam, or you think you may have been contacted by a fraudster, report it to us. Call FCA on 0800 111 6768.

If you've already invested in a scam, fraudsters may try and target you again or sell your details to other criminals.

The follow-up scam may be completely separate or related to the previous fraud, such as an offer to get your money back or to buy back the investment after you pay a fee.

Pension scams

Pension scams often involve attractive offers that aim to persuade you to transfer your pension pot (or release funds from it).

If you're worried about money and want to use your pension to repay debts, contact a free debt adviser first to find out what your options are.

Use MoneyHelper's debt advice locator tool (Link is external) **to find free debt advice near you.**

Warning signs

Pension scams often include:

- A guaranteed better return on your pension savings.
- High-pressure sales tactics.
- Unusual investments, which tend to be unregulated and high risk.
- Complicated structures, so it isn't clear where your money will end up.
- Several groups (some of which may be based overseas) all taking a fee, which means the total amount deducted from your pension is significant.

Early pension release scams

You should be very wary of any scheme offering to help you release cash from your pension before you're 55. It's almost certainly a scam.

Generally, **you can only take money from your pension when you're 55 or older** except in certain cases, such as poor health. This will increase to 57 from 2028.

How early pension release scams work

Offers to access your pension early may be called 'pension liberation' or a 'pension loan', as the scammers often claim you can borrow money from your pension fund.

If you take up the offer, your pension funds will be transferred into a scheme set up by the scam, which will often be based abroad.

You may be 'loaned' an amount (often around half of your pension), with the company involved taking a fee, perhaps as much as 30%.

You could also face a tax bill of 55% on what you withdraw, even if:

- You didn’t realise you'd broken the tax rules.
- You put the money back in your pension.
- You've paid fees or charges to the company involved.
- You've spent all the money.

Once you’ve paid the fees and tax, any money remaining will then be invested in high-risk products or projects, like overseas property developments.

Sometimes it’s simply stolen outright.

Risks of accessing your pension early

Taking cash from your pension before you're 55 is unlikely to be in your interests.

If an FCA-authorised adviser recommends an early pension-release scheme, ask them to explain the full consequences and risks, and your other options.

These schemes can be illegal if you’re not told – or are misled – about the tax you’ll pay and the risks of accessing your pension early.

Pension review scams

If you’re contacted unexpectedly and offered a free pension review, it’s likely to be a scam. **Professional advice on pensions is not free**.

Most of the companies offering free pension reviews aren’t authorised, but many falsely claim they are. They may also claim that they don’t have to be authorised, as they aren’t providing the advice themselves.

How pension review scams work

Free pension reviews are designed to persuade you to move money from your pension pot into a high-risk scheme.

Your pension pot is then invested in unusual investments such as overseas property, forestry, storage units, care homes, biofuels or businesses you may not be familiar with.

You may be promised guaranteed returns or cash from your pension to tempt you to take up these offers.

Some of these investments are badly run, while others are outright scams.

As they're promoted as long-term pension investments, it could be several years before you realise something is wrong.

Protect yourself from pension scams

If you get a call out of the blue (a cold call) about your pension, the safest thing to do is hang up. It's illegal and probably a scam. If you get offers via email or text, you should simply ignore them.

Report pension cold calls to the Information Commissioner's Office (ICO) (Link is external) .

If you're thinking about changing your pension arrangements, you should get financial guidance or advice beforehand.

If you want to find an adviser, make sure they're authorised by FCA. Never take advice from the company that contacted you. This may be part of the scam.

Find out more about getting financial advice (Link is external) from MoneyHelper.

Common investment scams

Binary options scams

Binary options are a form of fixed-odds betting. Typically, a trade involves predicting whether an event will happen or not. For example, whether the price of a particular share or asset will go up or down.

If the investor is correct, they 'win' and should see a return on their investment. If they're wrong, they lose their full investment.

From 2 April 2019, the FCA banned firms from selling binary options in the UK. If you're offered binary options, it's probably a scam.

How binary options scams work

Binary options fraudsters often advertise on social media – the ads link to well-designed and professional-looking websites.

The firms running the scams tend to be based outside the UK but often claim to have a UK presence, such as a City of London address.

Scam firms may manipulate software to fake prices and pay outs. They may then suddenly close individuals' trading accounts, refusing to pay back their money.

Scammers also target people searching for investments online through search engines like Google and Bing. They may offer high returns to tempt you into investing, but some may also offer more realistic offers to appear more legitimate.

Binary options bought before the ban

Before 3 January 2018, binary options were regulated by the UK's Gambling Commission.

If you want to make a complaint against a binary option firm about a bet made before 3 January 2018, you should contact the firm in the first instance.

Carbon credit trading scams

A carbon credit is a certificate or permit representing the right to emit one tonne of carbon dioxide (CO2).

Carbon credits can be traded for money, but many investors have reported they can't sell or trade their carbon credits and so can't make any profit.

How carbon credit trading scams work

Investors are usually called out of the blue, but contact can also come by email, post, word of mouth or at a seminar or exhibition.

You may be offered carbon credit certificates, voluntary emission reductions (VERs), certified emission reductions (CERs) or an opportunity to invest directly in a 'green' scheme or project that generates carbon credits as a return on investment.

Carbon credits and VERs certificates are often ‘certified’, but this certification is voluntary and involves a wide range of bodies and different quality standards that are not recognised by any UK compensation scheme.

The scam may claim carbon credits are ‘the new big thing’ in commodity trading, that industries now have to off-set their emissions, that the Government is focusing on green developments or that it’s a growing market.

But investors have reported they can’t sell or trade their carbon credits and have lost any money they’ve invested.

Scammers also target consumers searching for investments online through search engines like Google and Bing. They may offer high returns to tempt you into investing, but some may also offer more realistic offers to appear more legitimate.

How to protect yourself

Carbon credits are not currently regulated by the FCA. This means you won’t have access to the Financial Services Compensation Scheme (FSCS) (Link is external) or Financial Ombudsman Service (Link is external) if you want to complain.

Even if an FCA-authorised firm is involved in the sale of carbon credits – for example by acting as a custodian or nominee - you have no right to compensation if something goes wrong.

Projects generating carbon credits are usually based overseas, so UK authorities have no way of controlling the quality or validity of the schemes.

Always be wary if you’re contacted out of the blue, pressured to invest quickly or promised returns that sound too good to be true.

Crypto investment scams

You should be prepared to lose all the money you invest in crypto. But if you do decide to invest, it’s important to do your own thorough research. You can read more about crypto and investing in crypto from InvestSmart.

How crypto investment scams work

Crypto investment scams are on the rise. In fact, reports to us about these scams have more than doubled since 2020, so it's important to know what to look out for.

Fraudsters tend to advertise on social media, often using images of celebrities to promote the fake investments. But they may also target people searching for investments online, through search engines like Google and Bing.

The scam adverts often link to professional-looking websites, where fraudsters may manipulate software to fake prices and investment returns. Once you've invested, the scammers may act quickly, closing your account and taking your money. Or they may continue the pretence, to encourage others to invest. You may not even realise you've invested in a scam until you try to sell your investment.

Most crypto-related activities aren't regulated in the UK. This means that if you invest in crypto, you generally won't have access to the Financial Ombudsman Service (Link is external) if you want to complain.

You also won't be protected by the Financial Services Compensation Scheme (FSCS) (Link is external) if the firm goes out of business. This means it's unlikely you'd get your money back.

1. **Watch out for the warning signs**
    - Have you been contacted out of the blue?
    - Are you being pressured to invest quickly?
    - Are you being promised investment returns that sound unrealistic?

    If you answer 'yes' to any of these questions, be extremely cautious. Remember, if an investment opportunity sounds too good to be true, then it probably is.

2. **Check the Financial Services Register**
    Firms offering crypto products in the UK must be registered with FCA or have permission to promote them. The FS Register will show you which firms are registered, and which firms are operating without permission.

    - Search for the firm by name, or by using its firm reference number (FRN).
    - If the firm is registered, check what activities and services it has permission for.
    - Check the firm's contact details and make sure they match the contact details you've been given.
    - If you can't find a firm on the FS Register, it's unlikely the firm has permission to offer you crypto products and **you should avoid using the firm**.

But remember, just because a firm is registered, doesn't mean you'll have access to the FSCS or the Financial Ombudsman if something goes wrong.

Forex trading scams

People are being increasingly targeted by unauthorised forex trading and brokerage firms offering the chance to trade in foreign exchange, contracts for difference, binary options, cryptoassets and other commodities.

They promise very high returns and guaranteed profits, either through a managed account where the firm makes trades on the investor's behalf, or by using the firm's trading platform.

How forex (FX) trading and brokerage scams work

Most people report that they have initially received some returns from the firm that give the impression that their trading has been a success.

They are then encouraged to invest more money, at which stage the returns stop, their account is suspended, and there's no further contact with the firm.

Scammers also target consumers searching for investments online through search engines like Google and Bing. They may offer high returns to tempt you into investing, but some may also offer more realistic offers to appear more legitimate.

Beware of clone firms

Many fake trading and brokerage firms will use the name, firm registration number (FRN) and address of firms and individuals who are FCA authorised. This is called a clone firm.

The scammers then give their own phone number, address and website details, sometimes claiming that a firm's contact details on our Financial Services Register or FCA Firm Checker are out of date.

Scammers might also claim to be overseas firms, which don't always have their full contact and website details listed on the FS Register. They may even copy the website of an authorised firm, making subtle changes such as the phone number.

Get-rich-quick, Ponzi and pyramid schemes

Get-rich-quick schemes promise investors high returns not usually available through traditional investments.

While early investors may make money from the scheme, people who invest later usually lose their money.

How get-rich-quick schemes work

The 2 most common get-rich-quick schemes are Ponzi and pyramid schemes.

Ponzi schemes are named after Charles Ponzi, who guaranteed a 50% return to investors in the US in the 1920s. Most of the money he received was used to pay dividends to early investors, and the scheme collapsed when he couldn't attract more money to pay later investors.

Pyramid schemes work in a similar way, although investors are encouraged to recruit more people and are paid commission when they do. These scams are also called franchise fraud, multi-level marketing or a chain referral scheme.

These schemes seem genuine and profitable to the early investors, which encourages them to attract more people and money. But these types of schemes collapse when the supply of new investors and money ends. Investors usually find most or all of their money is gone, and that those who set up the scheme took most of it for themselves.

These schemes often target community, religious, ethnic, older or professional groups. Leaders within a group might be targeted first, receive a high return on their investment, and promote the scheme to others before it collapses.

Scammers also target people searching for investments online through search engines like Google and Bing. They may offer high returns to tempt you into investing, but some may also offer more realistic offers to appear more legitimate.

Land banking investment scams

Land banking companies divide land into smaller plots to sell to investors, with the expectation it will rise in value once it's available for development. But the land is often in areas of natural beauty or historical interest, with little chance of it being built on.

How landing banking scams work

Investors are usually called out of the blue, but contact can also come by email, post, word of mouth or at a seminar or exhibition.

Investors are told they will make big profits on small plots of land once planning permission is granted or development started.

But permission is often not granted or even applied for, and investors are left with land that is practically worthless.

While not all land banking schemes are a scam, it is often not made clear that there are restrictions on the development of the land or that it is protected.

There are also follow-up scams where plot-holders are asked to pay more money to settle their holding once they realise they will never turn a profit.

Scammers also target people searching for investments online through search engines like Google and Bing. They may offer high returns to tempt you into investing, but some may also offer more realistic offers to appear more legitimate.

How to protect yourself

If you're considering buying land, we strongly recommend contacting the local council where the land is located and asking them when the land will be released for development.

Just because the person promoting or operating the scheme says it's guaranteed the land will be developed does not necessarily mean it will be.

These schemes usually have small print stating that the success of the investment is subject to planning permission being granted – so you're unlikely to get any of your money back.

If the scheme is a collective investment scheme

While FCA don't regulate the sale of land, they do regulate collective investment schemes (CIS) – and a firm must be authorised by FCA to promote or operate a CIS in the UK.

They can only take action over a land banking scheme when it is being promoted or operated as a CIS without authorisation.

It is possible to sell plots of land without the scheme being a CIS, so many land banking schemes are set up to avoid looking like one on paper.

Determining whether a scheme is a CIS is often a complex legal matter. Broadly speaking, the characteristics include:

1. investors don't have day-to-day control over managing their plot
2. the scheme involves pooling investor funds
3. the operator is responsible for managing the scheme as a whole

In these cases, FCA may be able to refer it to Trading Standards, the Corporate Complaints Team at the Department for Business, Energy, Industrial Strategy (BEIS) or the police.

Online trading scams

People are being increasingly targeted by investment scams carried out via online trading platforms where fraudsters offer trades in foreign exchange, contracts for difference and cryptoassets such as bitcoin.

How online trading scams work

Investment scams using online trading platforms are often promoted online and via social media channels. They often use fake celebrity endorsements and images of luxury items to entice people to invest in their scams.

The ads then link to professional-looking websites where consumers are persuaded to invest, either through a managed account where the firm makes trades on their behalf, or by trading themselves using the firm's platform.

Most people report initially receiving some returns from the firm to give the impression that their trading has been a success. They will then be encouraged to invest more money or introduce a friend or family member. Eventually the returns stop, the customer's account is suspended and there's no further contact with the firm.

Scammers also target people searching for investments online through search engines like Google and Bing. They may offer high returns to tempt you into investing, but some may also offer more realistic offers to appear more legitimate.

Recovery room scams

People are being increasingly targeted by recovery room scams. This is where fraudsters approach investors who have been scammed or had failed investments, offering to help them get their money back for an upfront fee.

There is usually no explanation about how money will be recovered, or a false one is given. This could be by impersonating us or claiming to work with the Government, police or other regulator to recover any monies which have been lost. Generally, recovery rooms insist on being paid a fee or transaction charge before carrying out any services to recover any consumer's losses.

How recovery room scams work

Recovery room scams usually follow on from a boiler room or other type of investment scam where a consumer has lost money.

The people behind the original scam may operate the recovery room and contact the victim again pretending to be from a different firm or sell on their details to other recovery rooms. The scam tends to involve cold calling with high-pressure tactics and upfront charges described as a tax, solicitor or administrative fees, which can result in losses that can be greater than the initial loss.

The recovery rooms often have professional-looking websites to persuade visitors they are legitimate and claim to have a UK presence when they don't. These websites often make false claims to have successfully recovered money for other consumers involved in scams.

Recovery rooms generally use a web-based email address, such as gmail, Yahoo, Hotmail or Russian search engine, yandex. We never use webmail providers to contact consumers, nor does the Government, law enforcement agencies or law firms.

Beware of clone firms

Many fake firms will use the name, firm reference number (FRN), and address of firms and individuals who are FCA authorised. This is called a clone firm. Scammers may even copy legitimate websites, making subtle changes such as changing the phone number.

How to protect yourself

Be wary of websites, phone calls, and online or social media adverts promising to recover any money you may have lost from investments or fraud.

If you get a phone call offering to recover your losses, ask how the caller has information about your lost money. Any report of fraud can only be shared between other law enforcement agencies. It cannot be shared with a private business operating a recovery room.

If you've been asked to pay a fee or provide your bank account, card or other financial details, end all contact immediately and do not pay any money or provide any banking details.

Share, bond and boiler room scams

Share and bond scams are often run from 'boiler rooms' where fraudsters cold-call investors offering them worthless, overpriced or even non-existent shares or bonds.

Boiler rooms use increasingly sophisticated tactics to approach investors, offering to buy or sell shares in a way that will bring a huge return.

But victims are often left out of pocket – sometimes losing all of their savings or even their family home.

Even experienced investors have been caught out, with the biggest individual loss recorded by the police being £6m.

How share and bond scams work

Share and bond fraud usually comes out of the blue, with scammers cold-calling investors after taking their phone numbers from publicly available shareholder lists.

The high-pressure sales tactics can also come by email, post, word of mouth or at a seminar.

These scams are sometimes advertised in newspapers, magazines or online as genuine investment opportunities. They may even offer a free research report into a company, or a free gift or discount on their dealing charges.

Scammers also target people searching for investments online through search engines like Google and Bing. They may offer high returns to tempt you into investing, but some may also offer more realistic offers to appear more legitimate.

You will often be told that you need to make a quick decision or miss out on the deal.

The scammers might also try to sell you shares or bonds in a company that doesn't exist.

If you already own shares in a company, you may receive a call from someone offering to buy them at a higher price than their market value.

The scam will request the money upfront as a bond or other form of security, which they say they'll pay back if the sale doesn't go ahead – but you'll never hear from them again.

Investment scams often involve products not regulated could include:

- bamboo
- diamonds

- fine art
- gold
- graphene
- hotels
- international forestry
- land for development
- land overseas
- overseas agriculture
- parking
- precious metals
- storage
- student accommodation
- sustainable energy
- UK forestry
- whisky/whiskey
- wine

But even if the offer isn’t a scam, you should still be cautious about investing in any products we don't regulate. If you do, you won't be protected if something goes wrong and you could lose all your money.

Task Scams

Task scams are fraudulent job offers that promise easy money for completing simple online tasks. These scams often lure victims with the idea of making quick cash by performing tasks like liking videos or rating products.

How task scams work

1. Initial Contact: Scammers typically reach out through unexpected messages on platforms like text, WhatsApp, or social media, offering seemingly legitimate online work.
2. Gamified Experience: Victims are led to believe they are earning money through a gamified system that tracks their supposed earnings. Initially, they may receive small payments to build trust.
3. Deposit Requirement: To access their "earnings" or continue working, victims are asked to deposit their own money, often in cryptocurrency. This deposit is a key indicator of a scam.

Key Characteristics of Task Scams

• Fake Earnings: The earnings displayed in the app are not real; only the scammers profit.

- Deposit Requests: Legitimate jobs do not require you to pay to start working or to access your earnings.
- Impersonation: Scammers may impersonate real companies or create professional-looking websites to appear credible.

How to Avoid Task Scams

To protect yourself from falling victim to task scams, follow these guidelines:

- Ignore Unexpected Offers: Do not respond to unsolicited job offers, especially those that require upfront payments.
- Verify Companies: Always check the official website of the company or contact their HR department directly.
- Trust Your Instincts: If a job offer sounds too good to be true, it probably is.
- Use Reputable Job Platforms: Stick to established job sites that have measures in place to filter out scams.

By staying vigilant and informed, you can protect yourself from the risks associated with task scams.

What to do if you've been scammed

Report it

If you're worried about a potential scam, or you think you may have been contacted by a fraudster, report it to us. This could help prevent others falling victim to the same criminal.

Call FCA on **0800 111 6768** or use their contact form to get in touch.

For anything they don't regulate, or if you've lost money to a scam, contact Report Fraud on 0300 123 2040 or via their website (Link is external)

Be wary of future scams

It's important to be extra careful if you've already been scammed. Fraudsters could try and target you again, or they may sell your details to other criminals.

The new scam might be completely different, or it could be related to the previous scam. For example, you could be contacted with an offer to get your money back or to buy back an investment after you pay a fee. These are known as recovery room scams.