ActionFraud

0300 123 2040
www.actionfraud.police.uk

The UK's National Fraud and cybercrime reporting centre. Get in touch if you believe you have been the victim of fraud.

Citizens Advice & Trading Standards

03444 111 444
www.citizensadvice.org.uk
www.tradingstandards.uk

Offers free legal advice and guidance. Get in touch if you have been left in financial difficulty.

Age UK

0800 678 1602
www.ageuk.org.uk

Provides companionship, advice and support for older people who need it most.

The Financial Conduct Authority (FCA) Scams Helpline

0800 111 6768

The UK's regulator of financial services. Get in touch to find out if a firm or individual is regulated by the FCA or if a firm has any warnings.

Mind

020 8519 2122
www.mind.org.uk

Provides legal advice and support for people with mental health difficulties.

Victim Support

0808 168 9111

Helps people affected by all types of crime, providing free confidential support 24 hours a day.

Language Line

0845 310 9900

A translation service, offering language assistance.

This booklet has been produced by graduates and apprentices as part of the Financial Conduct Authority (FCA) CEO Challenge in partnership with the East London Business Alliance (ELBA) charity no. 1122173. It is a mandatory part of our Graduate and Apprentice Development Programme. The FCA sponsors the challenge to encourage colleagues to come up with innovative ideas to help members of our community. The content does not form part of any FCA policy.

www.teambravuraceochal.wixsite.com/stamponscams

STAMP ON SCAMS

Scams

and how to spot them

Contents

What is a scam?

Scams are fraudulent schemes that deceive people into giving away money or other goods.

In the UK, fraud accounts for 40% of all crime, with criminals making £609 billion in the first half of 2022.

Citizen's Advice reports that 75% of UK adults were targeted by scams in 2022, a 14% increase from the previous year. During the cost of living crisis, this figure is set to rise.

Scammers use various methods such as phone calls, text messages, emails, fake websites, and social media to obtain personal information and passwords to authorise payments.

It is crucial to recognise warning signs and know how to handle the aftermath of being scammed.

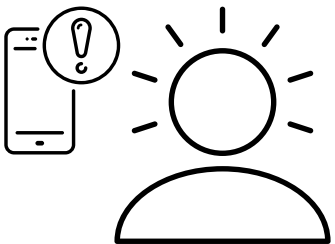
How to spot a scam

Although scammers can be crafty, there are warning signs to look out for. The general hallmarks are:

- spelling/grammatical mistakes
- promises of an aspirational lifestyle
- cold calls
- addressing you by email
- returns that seem 'too good to be true'
- asking you to share your screen
- applying time pressure

DO:

- Pause and reflect
- Verify the legitimacy of anyone who contacts you, online or in person
- Report any suspicious activity to the Financial Conduct Authority (FCA) immediately



DON'T:

- disclose information to anyone who contacts you out of the blue
- trust promises of high returns with low risk from unknown or unverified sources
- rely solely on information provided by the person contacting you
- open the door for strangers

Staying safe online

Email scams

- Scammers may send emails that appear to be from legitimate sources, such as a bank or HMRC. These might include a link for you to click on directing you to a fake website or harming your device - this is called **phishing**. You could be asked to enter personal information such as your bank details - but remember, genuine organisations will never ask you for this.

Screen sharing scams

- Scammers may ask you to download screen sharing software, enabling them access to your computer. They may claim they are from a well-known software company, such as Microsoft. Genuine software companies will never contact customers out of the blue.

Relationship scams

- Scammers often use social media platforms like Facebook, Instagram, or dating website. After building a relationship with the target, they may start asking for money. If you're beginning to suspect that someone you're talking to online might be being dishonest, it's worth asking for the opinion of a trusted friend or relative.

Doorstep Scams

What is a doorstep scammer?
Doorstep scammers will knock on your door and attempt to scam you out of your money or steal items from your home.

85% of doorstep scam victims are aged 65 and over, so it's important to stay vigilant and be aware of the warning signs.

Common types of doorstep scam

Fake officials
- A scammer will pretend to be from a gas or electricity company in an attempt to steal from your home once you let them in.

Rogue traders
- These scammers will offer you services that you may not need at extortionate or hidden prices. A common strategy is when they claim to have noticed something about your property that needs improvement, such as drainage or tiling.

Fake charity collections
- Scammers may pretend they're from a charity and ask for donations. Always ask for a **charity number,** which can be checked on the government's charity register online.

Fake consumer surveys
- Scammers may ask you to complete a survey to gain personal details.

Hard luck stories
- Scammers may knock on your door and claim that they're unwell or in trouble. They might ask to use your telephone to gain access to your home.

Avoiding doorstep scams

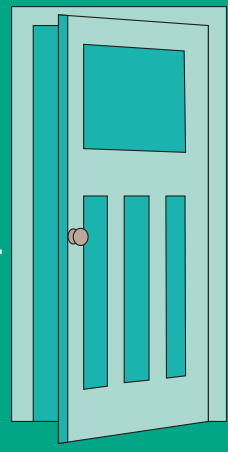
Check their credentials
- Always ask for some form of identification. If the visitor is legitimate, they won't mind being asked for identification.

Put up a deterrent sign
- Putting up a 'no cold callers' sign may deter scammers from knocking. It signals that you are aware of doorstep scams, making you a less attractive target.

Set up passwords for utilities
- You can call your utility companies and set up passwords to be used by anyone they send to your home.

Never give out personal information
- Some scammers might ask for your card and PIN number to withdraw cash on your behalf. Never disclose sensitive financial information or hand over your card.

Nominate a neighbour
- You may have a nominated neighbour scheme in place where a neighbour can help you to make sure that callers are safe. You can contact your local Neighbourhood Watch or your local Safer Neighbourhood police team to check.



Pension Scams

The number of elderly scam victims is on the rise, amounting to over 157 victims a day in 2022. As of 2022, the average pension scam victim will lose £75,000, although some have lost millions.

Scammers have become increasingly sophisticated, and their websites may look convincing.

Often targeting vulnerable consumers, scammers might persuade savers to transfer their money into pension schemes that the scammer controls. Victims can lose a lifetime's worth of savings in a matter of seconds.

If you suspect that a company isn't who they say they are, check their status on the Financial Conduct Authority's Financial Services Register
https://register.fca.org.uk/s/

Spot the signs

Do you understand what's being said?

- Adverts claiming no-obligation consultations or free pension reviews should be avoided
- Scammers may take notes on personal details to gain trust and to appear personally invested in the target
- Scammers may use phrases like **pension liberation**, l**oophole**, **savings advance**, **one-off investment**, **cashback**, **government initiatives**, or **up-front cash incentives**
- Scammers may use complicated or unusual investment structures to confuse their target
- Scammers may use the term "**fixed-term pension investments**". This indicates a long-term scam - victims often don't realise they have been scammed for years

Are you being made false promises?

- Scammers might offer you early access to your pension fund before the age of 55, with no mention of the HMRC tax bill that would be incurred
- Are there unusual underlying assets or funds? You should always ask about the underlying investment

Can you get in touch with the "firm"?

- A rogue firm may not allow you to call them back
- A firm may be rogue if their listed contact details are solely mobile phone numbers, or PO box addresses
- A scammer may use couriers to send documents to avoid being traced

Mortgage Scams

The UK has seen a steep increase in housing prices, averaging at £290,000 at the start of this year. This, coupled with the tightening of lending criteria during the cost-of-living crisis, has made getting a loan that much tougher.

Scammers are taking advantage of vulnerable borrowers; the following scams are most prevalent:

Loan modification scams

- Scammers offer existing homeowners more favourable mortgage terms, taking their ‘repayments’

Phishing schemes

- When borrowers are expecting correspondence regarding their loan, they are particularly vulnerable to phishing scams

Reverse mortgage scams

- Reverse mortgages allow homeowners aged 62 and older to borrow against the equity in their home.
- Scammers may convince the homeowner to apply for a reverse mortgage, and will attempt to steal the proceeds and/or the homeowner’s equity.

Spot the signs

Is the mortgage company taking account of your ability to pay?

- Your mortgage should not be much more than 35% of your gross monthly income. If the company or individual is not asking you for details about your finances, it may well be fraudulent.

Is the mortgage company giving you the option to buy mortgage points?

- A lender should always give you the option to purchase points, allowing you to prepay your mortgage interest.

"Bad credit doesn’t matter"

- Avoid any company that states this – they are likely predatory, targeting the financially vulnerable.

Financial Conduct Authority (FCA) Scams

impersonating firms

"Hello, this is Joe Bloggs from the Financial Conduct Authority (FCA). We've noticed that you've lost money on crypto trading apps, and we can help you get it back. Just pay a small upfront fee for paperwork and administrative costs, and we'll begin the recovery process. We have helped thousands of people recover their funds. If you cooperate with us and act fast, we can help you too."

over-promising

time pressure

This is a typical example of a financial scam where someone impersonates the FCA.

It is important to remember a few things if someone contacts you in a similar way:

- The FCA will never contact you out of the blue
- The FCA will never ask you for your money, bank details, or other sensitive financial information
- The FCA will never promise to recover your money
- The scammer may already know some of your personal information, such as your full name, number, email address. This does not legitimise them!
- The FCA is based in the UK, so callers from any other country will be scammers
- The FCA does not use WhatsApp as a means of communication

Investment Scams

Possibly the most well-known type of investment scam is a Ponzi scheme, which arises when money is collected from new investors to pay previous investors. Eventually, the amount of money owed is greater than the amount being collected, and the scheme collapses.

Typical signs include unregistered investments, issues with paperwork and the use of technical jargon, which is designed to impress you. Real investment advisers will use simple language to ensure the investor fully understands their investment.

Boiler Room Scams

Stockbrokers will cold-call investors and force them into buying shares. They often target middle-aged people who have previously bought shares, obtaining their names from public share registers.

This type of scam can be difficult to avoid as the scammers are often knowledgeable, well spoken and experienced, and may build a rapport with their targets to increase trust. However, if you spot any of the general hallmarks, it can indicate a potential scam.

Crypto Scams

Crypto asset investment scams are becoming more common. In 2021, 27.5% of all investment scam victims who mentioned social media in their report were aged 19-25. Almost half of all reports that mentioned social media were related to cryptocurrency investments.

Crypto scams generally fall into two different categories:

- Scammers attempting to obtain access to your digital wallet or private information. Once access is obtained, often people's online accounts are closed suddenly, and the fraudsters refuse to pay back money invested.
- Transfers of cryptocurrency to scammers as a result of impersonation, or fraudulent investment and business opportunities.

If you have been scammed, fraudsters may approach you afterwards offering to help you get your money back for an upfront fee. This is known as a **recovery room scam** and is often operated by the people behind the original scam pretending to be from a different firm.

AI Scams

Recent developments in AI (Artificial Intelligence) have made it harder to distinguish between AI and human content. Unfortunately, scammers have already taken advantage of this technology, using short voice samples to generate voice cloning to make scam targets believe a loved one is calling in distress.

Hi Granny, I've been held in jail overnight. I don't have access to my wallet and phone, and I really need cash for bail. Please help me!

This is a depiction of a real phone call received by Ruth Card, who would have lost 3,000 Canadian dollars if her bank hadn't intervened.

- If a family member or friend calls you asking for money, ask them a question that only they would know the answer to in order to confirm their identity.
- Create a code word with your family that can be used to verify the identity of the caller.
- If you're able to, put the call on hold and attempt to call your friend or family member separately.
- Be vigilant if the caller asks you to pay in an alternative currency, such as Bitcoin or by using gift cards. These are hard to trace, and often will not be recoverable if lost.

Aftermath of being scammed

If you think you have been scammed, it is important that you take action as soon as possible to not only limit the chance of losing your money for good, but also to prevent further attempts that may be made by the scammer.

You should always:

1. Contact your bank immediately. They will try to recover any money lost, and will also secure your bank account to prevent further fraudulent transactions from your account.
2. Report the incident to ActionFraud.
3. Block all calls/texts/messages from the suspicious individual or firm.
4. Contact the FCA and detail your interaction with the firm (details on the back of the pamphlet). Give as much detail as possible.
5. Contact the local police and file a report if you think you have been a victim of a boiler room scam.
6. Have your device looked at by an expert if you have downloaded any apps as instructed by the scammer. An expert will be able to ensure that the scammer does not still have access to your device through these apps.

What are the signs that a friend or relative has been scammed?

- An unusual amount of letters or post in their home
- A sudden lack of ability to pay for things
- An unusual amount of phone calls from strangers or companies
- Evidence of large cash withdrawals or multiple cheque payments

The emotional impact of a scam

- Don't be embarrassed to report a scam. Millions of people fall victim to scammers each year. Remember that the victim is never to blame.
- It is normal to feel anxious after you have been scammed. Get free, confidential help from Victim Support.
- If you are elderly, or concerned about an older person, you can get free, confidential advice about scams from Age UK, either on the phone or in person.