citizens advice Wealden

SPECIAL EDITION

SCAMS AWARENESS 2022
13TH TO 26TH JUNE

THE COST OF LIVING AND HOW TO BE A SAVVY CONSUMER

Scams

Consumer borrowing

Energy costs Gas and Electricity

COST OF LIVING CRISIS

Food

Communications and Home entertainment

Rent, Mortgage, Council Tax

What is the difference between fraud and a scam?

What is a Scam?

A scam is a fraudulent scheme generally involving money and some sort of business transaction. Scams come in various forms. Maybe you have experienced someone telling you would win a prize if you revealed your credit card details or asking you to donate money to a charity that does not exist?
Scams can be very convincing, and anyone can get caught out.

Examples of scams include:

- Instructions to transfer money to another account (e.g. a 'safe' account')
- Fake investment opportunities
- Requests for money from a scammer who has befriended you or struck up a romance online
- 'Too good to be true' deals that much be paid for by bank transfer

What is fraud?

Fraud implies a deception. It is a breach of confidence or trust.
Fraud is a serious crime and violation of civil law.

The motivations for fraud can be many. These include monetary gain, discrediting an opponent or adversary. It can be to gain prestige as well as financial advantage.

Examples of fraud include:

- Unauthorised use of your credit or debit card
- Bank account takeover – someone accesses your account without you knowing
- Identity theft – a fraudster uses your details to open accounts in your name

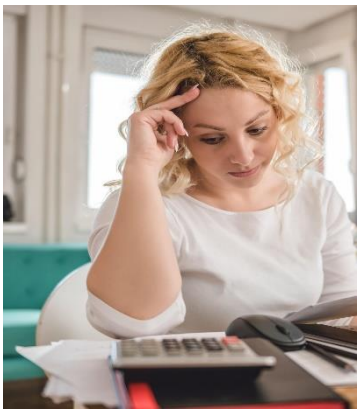
Cost-of-living crisis scams – how to spot the latest tricks from fraudsters

Financial scams are more prevalent than ever, and scammers are finding evermore ingenious ways to part you or your loved ones from your money.

The cost-of-living crisis has provided fraudsters with yet another way to try and swindle you.

Banks are now obliged to reimburse you for loss of money and the process is not easy and it can take a lot of time to recover stolen funds.

It is therefore essential to know how to protect yourself in the first place and to recognise some of the lates ways in which fraudsters try to fool us.



Cost-of-living crisis scam – Council Tax rebate

Households could be at risk of falling victim to scammers as they continue to wait for their £150 council tax rebate.

Local authorities have warned that criminals are cold-calling householders asking for bank details to receive the Government's £150 rebate.
Councils have urged residents to be alert to the scam, stressing they would never ask for bank details over the phone.

The Government announced the rebate support earlier this year in response to soaring energy bills, with payments administered by local authorities for households in certain council tax bands.

Payments are due anytime between April and September, but scammers are jumping onto the opportunity to steal from those who are still waiting to hear from their council on how and when they will be paid. Those who pay by direct debit will be paid automatically, but if you are not paying by that method, then you could become a scam target.

The Local Government Association (LGA) said anyone who unexpectedly receives a text, email or phone call seeking information or payment should not give out personal

information, including bank details, click any links or respond until they can be sure it is genuine.

How to spot a Council Tax Rebate scam

There are a number of tactics that scammers may use to get you to hand over your money.

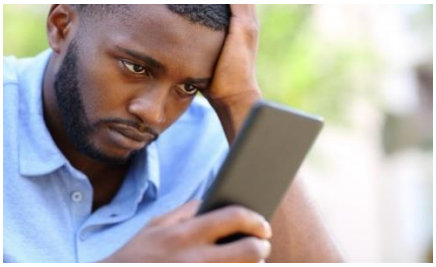
- They may ask for your bank details so they can provide a refund, then steal money from the bank account. **Although your local authority may contact you by phone, email, or text to tell you a payment is due or late, it will not ask for your bank account or personal details.**
- A scammer may insist you're in the wrong council tax band and are owed back payments on your council tax bill. Remember, you can check your council tax band by postcode yourself online and a council is unlikely to contact you about it.
- They may quote the official-sounding billing authority (BA) reference for your home to lull you into a false sense of security. **But this is public information and can be found using the online service**.
- Phone calls from scammers are often characterised by a strong sense of urgency. "You have to act now, or else it will be too late."
- Fake websites may pop up, designed to look like an application process on a genuine government website. However, these websites will have been created and designed to capture the information that you enter.
- Email and texts that are not genuine are typically riddled with spelling errors, poor grammar and, on closer inspection, nonsensical email address names and logos.
- Scammers here could pose as a local council and claim that you need to make a small payment to them so they can authorise your bank details before the rebate is paid. They will most likely claim that you will receive a refund of the payment you made at the same time as the council tax rebate.

What can you do if you are contacted by a Council Tax refund scammer?

- If you are called by anyone claiming to be from your council who is asking for bank details, hang up.
- If you get an email or text asking for personal details, then do not click on the links.
- If you want to check if a call or message is genuine, the safest thing to do is to call your council directly to double-check its authenticity. You can find your council's contact details on your council tax bill or website.
- If you realise after giving your bank details away that it was a scam you should contact your bank immediately.

You should also report any suspected scam to Action Fraud: www.actionfraud.police.uk/

Advance fee fraud



This is another rising scam and Lloyd's Bank has warned it has seen a 90% rise in instances of advanced fee fraud.

This type of fraud lead people to enter their contact details on websites which appear legitimate when looking to take out a loan or a credit card. The website will then ask for an 'advance payment', which you will never see again.

It is important to remember that a genuine loan company will never ask for an upfront payment before releasing the funds. If you are concerned in any way about your finances, there are a lot of organisations that can help, and it makes sense to speak to your bank first.

Key to spotting the signs of a scam is strange looking URLs in your internet browser, spelling mistakes or poor-quality logos on websites.

Unfortunately, scammers often mimic the official websites of normal financial firms, so being vigilant if you are looking to take on any new debt is essential.

****

Tax scams

HM Revenue and Customs (HMRC) is warning tax credit customers to be aware of scams and fraudsters who imitate the department in an attempt to steal their personal information or money.

About 2.1 million tax credits customers are expected to renew their annual claims by July 31. Criminals will mimic government messages to make them appear authentic in their phone calls, texts, and emails.

HM Revenue and Customs (HMRC) says scammers may try to threaten people about non-existent tax bills, or they may try to tempt them with tax rebates. Scammers may also claim there is an issue with the person's national insurance (NI) number or direct debit.
HMRC suggests searching gov.uk for genuine information and guidance

Fake insurance

Motorists may be tempted by supposedly cheap insurance deals – particularly young drivers, who often pay more for their insurance and may be inexperienced at buying cover. But insurance giant Aviva has warned people to watch out for offers from unsolicited or unusual sources – particularly if it's via social media or word of mouth.

'Ghost brokers' pretend to be genuine brokers offering car insurance. Policies are bought through legitimate companies but using false information. They are then doctored and sold on. It's often only when someone claims that they realise the policy isn't valid. Check a broker's status on the Financial Conduct Authority https://www.fca.org.uk/or British Insurance Brokers' Association www.biba.org.uk websites or contact insurers directly.

****

Holiday scam

Holidaymakers may be looking to cut their costs on getaways, but it's worth remembering that Action Fraud figures show victims of holiday and travel-related fraud lose £1,868 on average.
The last thing you want when you head away on holiday is to find out you haven't actually booked your flight or hotel room.

Unfortunately, there are many hotel scams, villa scams and flight scams that promise great holidays which aren't real.
Either the holiday, or parts of it, doesn't exist, or it does exist, but a fraudster has sold it to you. You might not realise you've been scammed until the flight tickets don't work. Or you might turn up at the resort, airport, or cruise terminal, only to find you've lost your money.

Ways to spot a holiday scam

As with many types of fraud, you should be suspicious of anything that looks too good to be true. Be wary of any holiday offers which are unusually cheap or ask for a high deposit.

How do you know if a holiday website is genuine?

Spend time researching holidays advertised privately to make sure they're not fake.
You can look for online reviews and recommendations to check the accommodation really exists.

How do you know if a travel agency is real?

Check that any travel agents or tour operators you're dealing with belong to a reputable trade association. This could be ABTA or the Air Travel Organiser's Licence (ATOL) scheme.

How do you book a holiday online safely?

There are ways you can safeguard your money. Try following these tips when booking your holiday:

- use safe sites when shopping online
- use safe ways to pay, such as your credit card wherever possible as there's more chance you'll get your money back if something goes wrong (however, be aware that credit cards are subject to interest and fees if you don't pay off the balance in full each month)
- check the cancellations policy before booking
- keep records of payment confirmations and receipts
- if you make an online payment, don't follow a link in an email but type in a website address you know to be correct
- make sure any payment page begins with 'https' and shows a padlock symbol, which means the communication link between you and the website is secure (but remember, the padlock doesn't guarantee an authentic site)

****

Fake jobs

The Scam

Crooks post adverts on social media offering easy ways to earn cash in a bid to snare anyone desperate for extra money.

They pose as marketing companies that will pay you for simple tasks such as liking posts or watching videos.

You are asked to pay a deposit and told you will make your money back and much more. But you don't earn a thing and the criminals steal your cash.

TSB said that, in one recent scam, victims were asked to sign up to an app called Pinterest Task Mall, which was made to look like the real social media app, but in reality, it was a sham.

Victims were asked to make a series of deposits of £100 or more in order to be assigned tasks. But after completing the work, they tried to log in to withdraw their earnings and found the app had been shut down and their deposits stolen.

How much could you lose?

TSB said victims have lost up to £4,230, but the average is £1,399.

How to avoid it:

TSB director of fraud prevention Paul Davis said: "Steer clear of any offer of work that asks you to put money down before you can earn.
"Any offer of big returns for minimal effort is likely to be a fraud. Only ever download apps from official app stores and even then, remain wary and check reviews first."

****

Shopping swindle

The Scam

Criminals know many families are facing a choice between heating and eating as energy and grocery bills surge.

They turn this to their advantage by sending offers by email or text, offering the chance to get £50 as a refund on your shopping or vouchers for a particular supermarket by clicking on a link and filling out a survey.

You click on the link, and you are asked to hand over bank details or card details so that you can receive payment from the survey.

These details are often sold to other crooks who will either try to spend money on your card or phone you up pretending to be your bank, internet company or the police and trick you into transferring money to them.

How much could you lose?

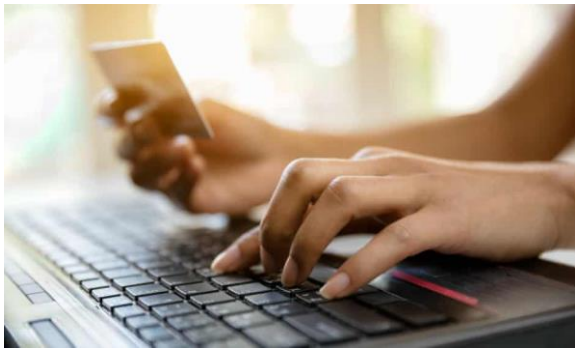
Criminals who steal your card details will typically spend £80-£200, according to analysis by data security firm Rightly.
In bank transfer scams, the average loss is £1,945, after taking into account any money that is refunded by the bank, UK Finance found.

How to avoid it:

“Never trust a link in a text or email,” said James Walker, chief executive of data management company Rightly.
“There are legitimate firms that will pay you to do surveys. Read online reviews first and contact them rather than responding to a message.”

****

Dodgy discounts



The Scam

Scammers prey on shoppers as they try to beat price hikes by hunting for deals online. They advertise heavily discounted branded items like trainers and gadgets on social media or sites such as eBay.
You are typically asked to transfer money to a bank account rather than paying by card.
Purchase frauds are one of the most common scams that Lloyds Bank sees.

How much could you lose?

Victims lose an average of £190.

How to avoid it:

Lloyds Bank fraud prevention director Liz Ziegler said: “When shopping, the best way to stay safe is to buy from a trusted retailer, and always pay by card for the greatest protection.

"If you're unable to do those two things, that should be a big red flag that you may be about to get scammed."

An eBay spokesman said: "The eBay Money Back Guarantee means that if a user buys something that doesn't arrive or isn't as advertised, we'll make sure they get their money back, if the seller doesn't resolve the issue for them first."

****

Lotto scam

The Scam

With bills mounting, many of us dream of a windfall to get our finances back on track. In this cruel con, crooks will phone or write telling you that you have won a lottery or prize draw. You will be told that you need to pay a fee to get your cash. The criminals will then steal your money and you will never get the prize you were promised.

How much could you lose

Losses to lottery scams have totalled £3.3million in the year to February, or an average of £2,696 per victim, according to Action Fraud.

How to avoid it:

Craig Mullish, of the City of London Police, said: "Remember, you can't win a draw that you haven't entered.
"If you're contacted out of the blue claiming you've won a prize draw but can only access these winnings by paying an advance fee, it's likely to be a scam."

****

Inheritance Scam

The Scam

You receive an email or a letter claiming to be from a lawyer informing you that someone very rich has died and you are in line for a big inheritance.

The fraudsters will often say that they can't reveal the identity of your benefactor and if you don't act quickly, the Government will get your money. In order to receive your payout, they say you first have to pay a fee to cover tax and legal fees. In reality, the wealthy benefactor doesn't exist, and you're left much poorer.

How much could you lose?

TSB says that the average loss is £11,500

How to avoid it:

Paul Davis said: "Never hand over money on the promise that you're entitled to a large sum. If it sounds unlikely, trust your instincts – it's almost certainly a con. Speak to friends and family, do your research, and don't act in a hurry."

****

citizens advice Wealden

We've seen time and again that scammers seek to exploit vulnerability - from the coronavirus pandemic to recessions, times of difficulty often see a corresponding increase in related scams. From early data, the cost-of-living crisis seems to be no different.

The increased financial pressure many will be facing has put more people into difficult situations, with many facing issues with debt and being unable to afford essential goods and services. Scammers are likely to exploit these issues, so empowering the public to protect themselves and others from scams will have heightened importance.

There are lots of different types of scams emerging. Some examples to look out for include:

- Scammers pretending to be energy companies, luring people with "too good to be true" deals in order to steal their money
- Fake sales representatives selling counterfeit shopping vouchers
- Fraudsters sending out phishing emails pretending to offer an energy rebate or government support to steal people's personal information.

The stats on scams

Estimates from the Crime Survey for England and Wales (CSEW) suggest there were 5.1 million fraud offences in the year ending Sept 2021. This is a 36% increase compared to the year ending Sept 2019.

Citizens Advice found in the first 5 months of 2021 more than two thirds of adults (36 million) had been targeted by a scam.

- Within this, while over 55s were most likely to be targeted, those 34 and under were almost 5 times more likely to fall victim to a scam than their older counterparts.

In the first half of 2021, criminals stole a total of £753.9 million through fraud, an increase of 30% compared to the year before.

- In the first half of 2021, criminals focused their activity on authorised push payment (APP) fraud, where the customer is tricked into authorising a payment to an account controlled by a criminal. They use things like scam calls, texts, emails, social media, and fake websites to trick people into handing over personal details, which is then used to target victims and convince them to authorise payments.
- There were significant increases in impersonation scams and purchase scams, and investment scams were also highlighted as of concern.
- What often unites these scams is the use of online platforms - UK Finance analysis found 70% of APP scams originated on an online platform.

The CSEW suggests that only 1 in 6 (17%) of incidents of fraud either come to the attention of the police or are reported by the victim to Action Fraud.

General scams advice on spotting a scam

It's important to always keep an eye out for scams. They can and do affect anyone. Here are some of the main warning signs of scams to look out for:

- It seems too good to be true – like an email saying you've won a competition you don't remember entering
- Someone you don't know contacts you unexpectedly
- You're being urged to respond quickly so you don't get time to think about it or talk to family and friends
- You've been asked to pay for something urgently or in an unusual way – for example by bank transfer or gift vouchers
- You've been asked to give away personal information

If someone thinks they might be being scammed, they should get advice immediately. They can contact the Citizens Advice consumer service for help with what to do next, and report scams or suspected scams to Action Fraud.

How to protect yourself from scams

There are some simple steps people can take to help protect themselves from scams:

- Don't be rushed into making any quick decisions. It's okay to take your time
- Never give money or personal details, like passwords or bank details, to anyone you don't know, trust or have only met online. If someone pressures you for these, it's most likely a scam

● Before you buy anything, check the company or website you're using. Read reviews from different websites, search for the company's details on Companies House, and take a look at their terms and conditions
● Pay by debit or credit card. This gives you extra protection if things go wrong
● Be suspicious. Scammers can be very smart. They can appear like a trusted business or government official, have a professional website, and say all the right things. Take your time to work out if this is a real organisation. Ask them for ID or contact the organisation on a number you know and trust
● Don't click on or download anything you don't trust
● Make sure your antivirus software is up to date
● Keep your online accounts secure by using a strong password for email accounts that you don't use anywhere else. Choosing three random words is a good way to create a strong and easy to remember password. You can also add in numbers and symbols.
If you are worried about remembering lots of different passwords, you can use a password manager. Some websites let you add a second step when you log in to your account - this is known as 'two-factor authentication'. This makes it harder for scammers to access your accounts.
● If you're not sure about something, get advice from a trusted source.

What to do if someone has been scammed

If someone has been scammed, there are 3 steps they need to take:

1. **Protect themselves from further risks**

There are things they can do to stop things getting worse. They should contact their bank immediately to let them know what's happened. They should also change any relevant log-in details, and check for viruses if they were scammed on a computer.

2. **Check if they can get their money back**

If they've lost money because of a scam, there might be ways they can get it back. Again, make sure they tell their bank what happened straight away. If they've paid for something by card, bank transfer, Direct Debit or PayPal, then depending on the circumstances they might be able to help them get their money back.

3. **Report the scam**

Reporting scams helps authorities stop the criminals responsible and protects others from being scammed. Anyone who's been scammed should:

● Call the Citizens Advice consumer service on 0808 223 1133, or on 0808 223 1144 for a Welsh-speaking adviser. We'll pass on details of the scam to Trading Standards, and can offer further advice
● Report the scam to Action Fraud, the national reporting centre for fraud. They'll also give them a crime reference number, which can be helpful if you need to tell your bank you've been scammed.

It's also important for us to all talk about our experiences with family and friends. By letting them know what's happened they can be prepared, and together we can put a stop to scams.

Where to go for more help

- If someone has been scammed, or thinks they've been scammed, they can contact the consumer service by calling 0808 223 1133 (or 0808 223 1144 for a Welsh speaking advisor)
- If they've been scammed online, they can also get advice from a Scams Action adviser (Monday to Friday 9am to 5pm) on 0808 250 5050 or via webchat.
- You can also use our online scams helper to work out if something is a scam and see the next steps to take.

There's lot of advice on the Citizens Advice website at www.citizensadvice.org.uk/scamsadvice, including how to:

- Check if something might be a scam
- Check if you can get your money back after a scam
- What to do if you've been scammed
- Report a scam
- Get emotional support if you've been scammed
- Get help with online scams

- You can check recent scams on Action Fraud's website, and sign up for email alerts to find out about scams in your area at www.actionfraud.police.uk/news

****

REPORT: Action Fraud

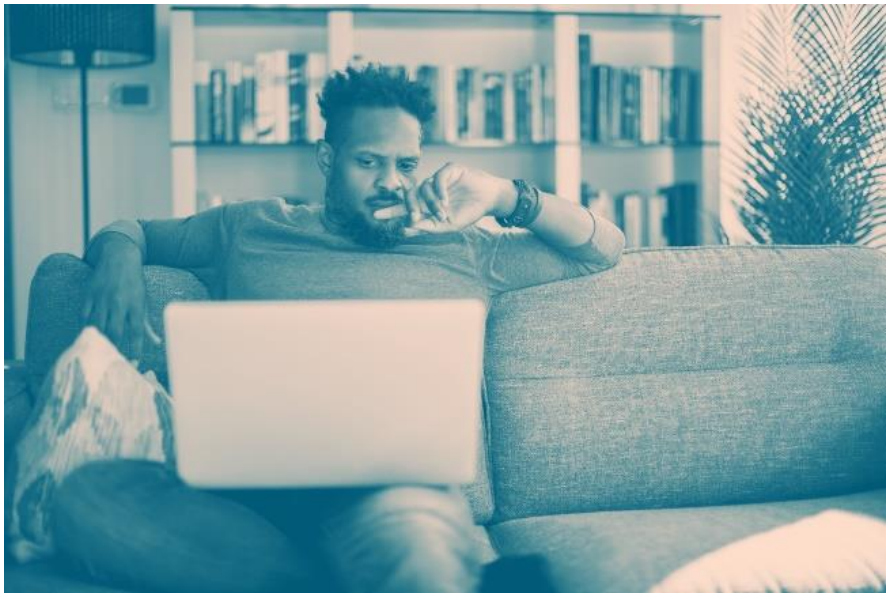
Action Fraud is the UK's national reporting centre for fraud and cyber-crime where you should report fraud if you have spotted a scam or have been scammed, defrauded, or experienced cyber-crime.

You can visit the website (www.actionfraud.police.uk) or call Action Fraud on 0300 123 20 40.

ADVICE: Citizens Advice Consumer Service
Citizens Advice Consumer Service can offer support if you or someone you know has been scammed. They will give you advice on what to do next.
You can visit the website (www.citizensadvice.org.uk) or call Citizens Advice Consumer Service on 0808 223 1133 or 0808 223 1144 for a Welsh-speaking advisor

****

Take Five to protect yourself
Stop, Challenge and Protect



Be Scam Aware Scammers are clever. We're all worried about money - don't let them take yours. Find out how to spot scams, report them and get help at citizensadvice.org.uk/ScamsAdvice

If you've been scammed: Call Citizen Advice Consumer Service on 0808 223 1133 for support Report it to Action Fraud on 0300 123 2040