

## Citizens Advice Scams awareness campaign [13-26 Jun]

Our annual Scams Awareness campaign aims to create a network of confident, alert consumers who know what to do when they spot a scam. This year's campaign will take place 13 - 26 June.

With many people facing increased financial pressures, there is a high chance that scammers will take advantage of this.

For example, we've already seen instances of scammers pretending to be energy companies offering "too good to be true" deals and others sending out phishing emails offering fake government rebates. Anyone can fall victim to a scam. People of all ages and backgrounds get scammed. It's important to be on your guard - if you're not sure about something, take your time and get advice. If you think someone might be trying to scam you, it's important to act straight away. If you need advice and support you can call the Citizens Advice consumer service on 0808 223 1133 or visit [www.citizensadvice.org.uk](http://www.citizensadvice.org.uk). You should also report scams or suspected scams to Action Fraud.

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

### 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

### 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:
  - Use 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're 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. 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
    - 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](http://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](http://www.actionfraud.police.uk/news)