citizens advice Tendring

SCAMS AWARENESS CAMPAIGN JUNE 2021

72 out of 100 people in the East of England have been targeted by scammers so far in 2021

72% of people in the East of England have been targeted by a scammer since January, new research* by Citizens Advice has found. 75% also say they're worried that they or a loved one could fall victim to a scam.

Fraudsters tried to trick local people in a range of ways, but the biggest scam faced by those living in the East of England was delivery text/email scams; these claim that you have missed a delivery and ask you to reschedule for a fee, thereby obtaining your bank details. 57% of people in the area said they'd been contacted about a scam of this kind.

To encourage people to report scams, share their experiences and look out for others, Citizens Advice Tendring have launched their annual Scams Awareness campaign which runs until 27th June.

What is a scam?

A scam is a scheme to try to steal money, personal information or data from a person or organisation. Other names for a scam include fraud, hoax, con, swindle and cheat. (A "Scams glossary" is at the end of this document.)

General scams advice

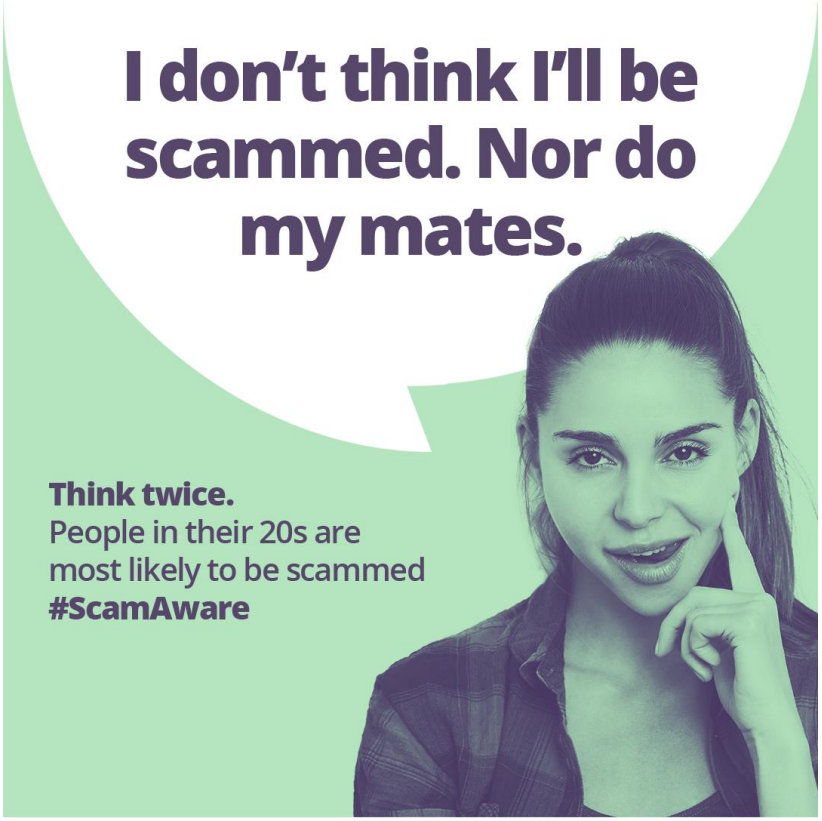
Spotting a scam

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:

*Opinium surveyed a representative sample of 2,086 adults living in the UK. The sample was weighted to be nationally representative of the UK. Fieldwork took place between 21 and 25 May 2021.

- 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
- 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 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

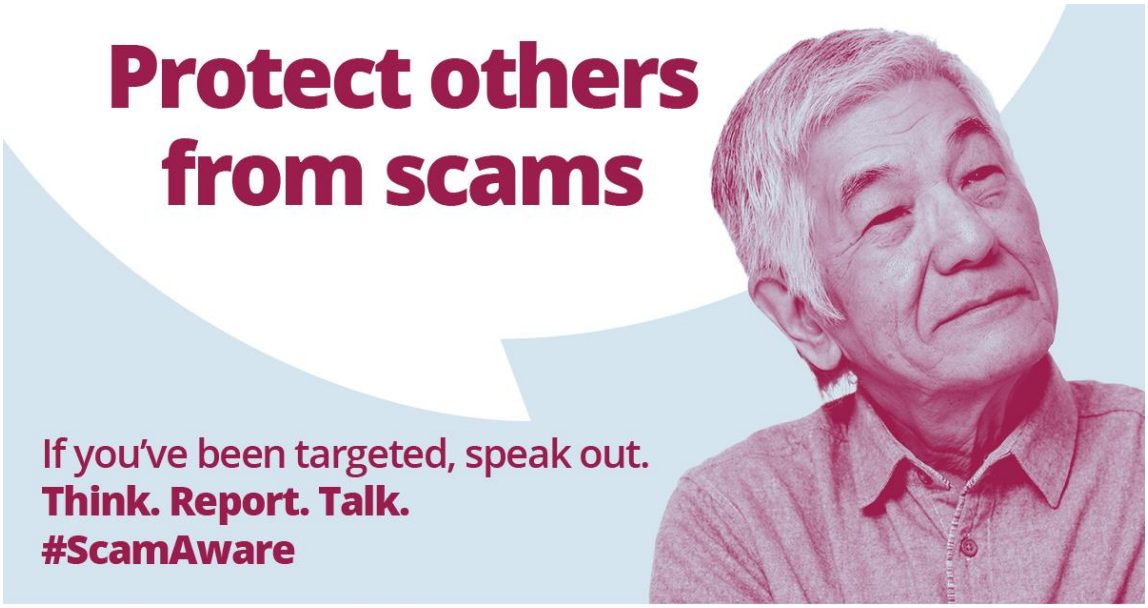
If they've lost money because of a scam, there might be ways they can get it back. Again, make sure they tell their bank what happened straight away. If they've paid for something by card, bank transfer, Direct Debit or PayPal, then depending on the circumstances the bank might be able to help them get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

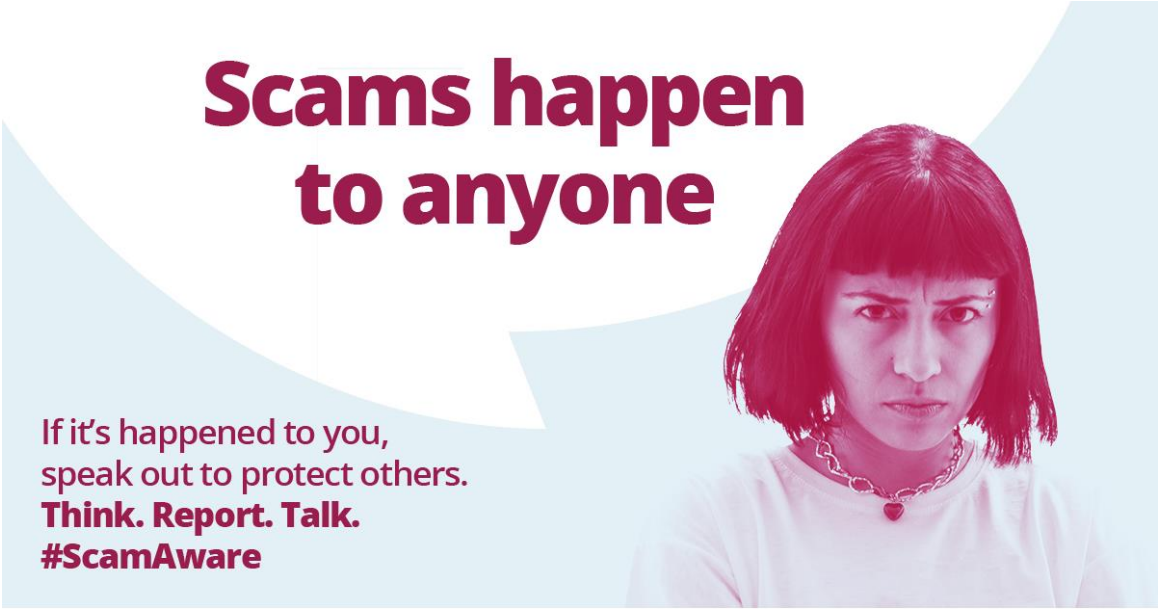
- Call the Citizens Advice consumer service on 0808 223 1133. We'll pass on details of the scam to Trading Standards, and can offer further advice.
- Report the scam to Action Fraud, the national reporting centre for fraud, on 0300 123 2040. They'll also give you a crime reference number, which can be 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. It's on this page
- There's lot of advice in the consumer section of the Citizens Advice website, 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
- You can also find out about common financial scams on the Financial Conduct Authority's website at www.fca.org.uk/consumers/protect-yourself-scams



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.
You should also report scams or suspected scams to Action Fraud - Call 0300 123 2040.

Check how #Scam Aware you are by trying our quiz:
https://citizensadvicequiz.typeform.com/to/qglyky4y

Scams glossary

There are lots of different types of scams, and people can be targeted in many ways - whether that's phone, email, mail or even in person. Here are some common types of scams to look out for in your community.

Financial scams

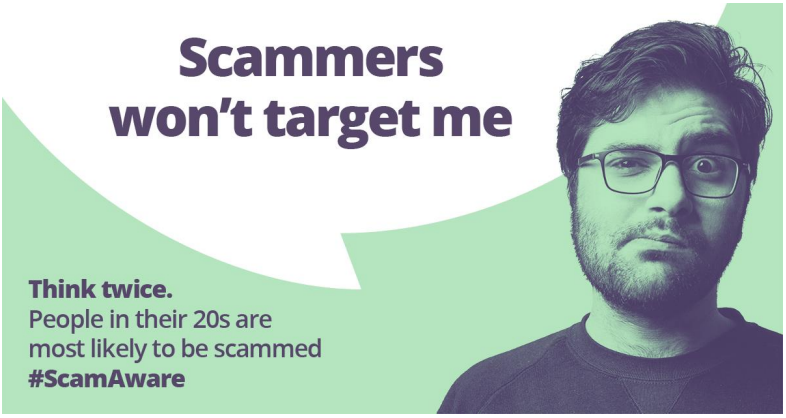
There are many new scams around at the moment as fraudsters take advantage of the ongoing economic impact of the coronavirus pandemic. Scams to look out for include:

- **Adverts offering fake "Get Rich Quick" investment schemes**
- **Phone calls, texts or emails from scammers pretending to be your bank, so they can get you to transfer money to them or give them your personal details**
- **Scam emails or automated calls pretending to be from an official organisation, like HMRC calling about a tax issue**
- **An offer of a pensions review out of the blue**

Common scams

Antivirus/computer - People are cold called and told they have a problem with their computer which, for a fee, can be fixed. Alternatively the victim might initiate the contact in response to an online advert or prompt claiming that their device has been infected with a virus. Other computer scam methods involve offering bogus virus protection or warranties

Contactless card scams - Contactless cards are 'skimmed' (where details are read or copied) by a card reader or phone nearby. While this is a relatively new crime and reporting figures are low, there has been media speculation about the rise of this type of scam



Copycat Government official service scams – Callers or websites claim to be official government departments and sell services for a 'fee'. For example, they might claim to help process passports or driver's licenses. Universal Credit scams have also been widely reported, where someone offers to apply for a Universal Credit Advance Payment on your behalf and takes some of the money as a fee. Victims can be approached both online through social media groups, direct messages and adverts, or in person by smartly dressed people claiming to be from Jobcentre Plus

Credit Card Scams - This is where customers give credit card details to buy a genuine product/service and those details are sold to a scammer. The scammer sets up a fraudulent purchase of, for example, an expensive mobile phone. They then send you something of no or little value by tracked delivery so that when you challenge the purchase they have a delivery receipt

Cryptocurrency scams - These are a type of investment scam, where someone offers a fake, but often convincing, opportunity to make a profit by investing money in cryptocurrency - virtual peer-to-peer currency that is decentralised and only exists online. These scams may involve: a fake cryptocurrency which doesn't and won't ever exist – for example if it's a fake Initial Coin Offering (ICO); a bogus investment which promises to put money in a legitimate cryptocurrency; a dangerous website link that then downloads malware onto your computer. For more information about these scams, Kaspersky has a summary of the different types of cryptocurrency scams or see Which?'s article about investment scams

Delivery text/email scams - These can be text messages or phishing emails pretending to be from a delivery courier like DPD or Royal Mail. These messages claim that you have missed a delivery and ask you to reschedule for a fee, thereby obtaining your bank details. Whilst it can start with a small fee, it can end with criminals emptying a person's entire bank account. The Guardian recently reported on this "new fraud wave sweeping the UK"

Doorstep/street selling - These all begin with the person getting an unrequested knock on their door. They are often for expensive home improvements which the victim did not want or was pressured into. Another variation of this can be where someone agrees to a service, such as having their gutters cleaned, and the trader then 'discovers' a larger problem (e.g. a roofing 'fault') which needs to be corrected at huge cost. Read more information on our website about consumer's rights if they've been missold items on the doorstep or have been pressured into signing a contract

Fake Service / invoice - This also covers a wide range of situations, but asks for payment for either a service the scam victim has never heard of or for a service which ended up being non-existent. Read more about these scams at Experian.

HMRC/National Insurance (NI) Scam - These often involve receiving a call (often automated) saying you have committed tax fraud and you should press one to make a payment to avoid a prison sentence. Another variation includes a call stating that your NI number has been compromised and you should press 1 to obtain a new one and you are connected to a premium cost number

Investment - Often conducted either online or over the phone, these can result in people losing thousands of pounds for non-existent stocks, shares and other investments such as rare wine or art. These will sometimes involve scammers 'wining and dining' investors to convince them it's genuine. Average losses are very high - the BBC reports that victims last year lost an average of £45,000

Job scams – Scams include taking money to write CVs or carrying out security checks. Some ask for bank details to pay (non-existent) wages, others offer expensive training programmes that don't exist. Some even offer jobs that don't exist!

Online shopping and auction sites - Items are advertised for sale, often at a bargain price with pictures to make it appear more genuine. The buyer may be pressured into paying via bank transfer instead of a third party payment service. Once the payment is made the item is either not received or is counterfeit. The BBC recently reported that online shopping scams and pet scams (where scammers use social media and other channels to advertise pets, often with attractive pictures, that never arrive after a deposit or full price is paid) surged during the pandemic

Pension scams – Pension freedoms introduced in April 2015 give consumers added flexibility but it's essential they make informed decisions using trusted sources. The Citizens Advice report 'Too good to be true' calculates that 8.4 million people have been offered unsolicited pension advice or reviews since April 2015. The report also showed that 88% of consumers selected a pension offer containing scam warning signs, including out of the blue offers promising high returns, pressure to sign paperwork, and offers to access pensions before the age of 55

Phishing – Emails and harmful links designed to deceive people into revealing personal/financial details. By spoofing emails, email addresses, websites and payment services, scammers can trick people into believing they are dealing with genuine banks, traders and/or authorities

Premium Rate Number Scams - You look for the number of a government department online and see an advert for the phone number of the relevant government advice line that looks genuine. It does put you through to the right department but it is actually a premium rate switching number that charges you a high connection fee – in some cases, as much as £20 or £30 a call. It's always best instead to look for the number directly from the official government website - that way you'll always be able to find the right number to call directly for the service you want.

Refund Scam - Often involves getting a letter or email from a utilities company saying you are entitled to a 'refund' and asking you to confirm bank details to receive the repayment. This has also been a common HMRC scam in the past, with scammers using emails and texts to trick people into thinking they are owed a tax rebate, resulting in people handing over their account and personal details

Romance Scams - Romance scammers create fake profiles on dating sites and apps, or contact their targets through popular social media sites like Instagram, Facebook, or Google Hangouts. The scammers strike up a relationship with their targets to build their trust, sometimes talking or chatting several times a day. Then, they make up a story and ask for money - usually a 'disaster story', like needing to pay for medical treatment urgently or claiming to be kidnapped. The scam can take place over a long period of time and cause significant financial loss and emotional distress. Read our blog on how to avoid romance scams

Remote Access Scam - This involves the scammer convincing people to allow them remote access of their computer to fix something, but this allows them access to personal data and even direct access to people's bank accounts if they have stored the login information

Smishing – Text messages used to lure people into scam websites or inviting them to call premium rate numbers or download malicious content

Subscription traps or free trial scams – Some unscrupulous companies use subscription traps, and in particular continuous payment authority (CPA), to help themselves to consumers' accounts. Common ones include those offering health and beauty-related products such as slimming pills or skin creams. The government has reaffirmed their commitment to tackle subscription traps and empower consumers, but in the meantime, consumers still need to take care

Telephone Preference Service (TPS) or call blocking scams – Scammers demand payment for the free TPS or sell call blockers which either do not work properly or are part of an expensive subscription service.

Ticket scams – Consumers buy tickets for an event that is already sold out or the tickets haven't yet gone on sale. The tickets then either do not arrive or are fake. Consumers should use credit cards or secure payments and ensure purveyors are members of STAR – Society of Ticket Agents and Retailers.

Upfront payment/fee scams - This covers a wide range of situations and scam delivery channels, but they usually ask for an upfront payment to unlock either a cash prize, a PPI claim amount or for initiating a service. This also includes loan fee fraud: scammers prey on individuals who have a bad credit rating or who need a loan quickly are asked to hand over a fee – usually between £25 and £450 – when applying for a loan or credit that they ultimately never receive.

Vishing – This is where the consumer received a cold call aimed at extracting personal information and details from them. Scammers impersonate someone from a trusted organisation, such as a bank, to manipulate people into transferring money or pass on financial/ personal details