

Scam alerts



Call Blockers

Since 2022, the City Council have installed a number of call blockers to protect residents from nuisance and scam phone calls. Scam and nuisance calls can affect people in many ways, these types of crimes often cause financial loss, emotional distress, social isolation and loss of confidence.

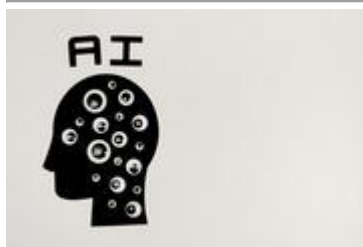


Since the call blockers were installed they have blocked 8,069 scam and nuisance calls, this was 33% of all calls received.

We still have a number of call blockers left which would be available to loan free of charge for an initial period of six months.

If you think you would benefit from a call blocker or you are aware of anyone who would, please express an interest by emailing: Public.Protection@stoke.gov.uk

Please provide the name, address and contact number of the person who is making the application. Please note that there are only a limited number of call blockers available and these will be allocated on the basis of need after an assessment has been made.



Artificial Intelligence Scams

Deep fake and AI scams use technology to manipulate information and images, making something appear real when it's not. This could include text, video, audio and images, the scammers will use chatbots, image, video and audio-generation software to create these scams. We are seeing a massive surge in scams that use AI.

Deepfake Videos

This is where a person has been digitally altered to appear a different person. Often these are used to make it seem like a celebrity is promoting an investment scheme. Deepfake videos are also used to steal people's identities, pass verification checks and access victims accounts.



Tips to spot a Deepfake Video:

- Some deepfake videos use lip-syncing, so watch the video carefully for lip-syncing that's slightly off.

- Pay attention to details in the quality – do the hair, lighting and skin tone of the person look believable? Is there any blurring in the video?
- Listen out for strange background noises or robotic voices.
- Look for unnatural expressions – it's hard to mimic natural blinking, and AI often lacks facial emotion and AI body movements can seem off.
- Where does the video come from? If it's not an official account or if it's an account you've never heard of and you haven't seen the video anywhere else, be wary.



Phishing Messages

These are usually sent by text or email as well as scam social media posts and adverts. They attempt to prompt you into following a phishing link that will ask for personal and/or financial information. Through the use of AI tools such as ChatGPT scammers can now create much more convincing messages, these messages now no longer have poor spelling and grammar which has always been a key sign it's a scam. This makes it harder to spot them but there are still things you can

look out for.

How to spot these scams:

- Most genuine companies address you by your name and also include personal account details, such as your mobile phone number or part of your account number.
- Messages asking for personal and financial data should be treated with caution.
- Be wary of messages with attachments, as most companies don't include these, and this is how scammers spread malware.
- All phishing messages contain links. Even though legitimate companies also send messages with links, you should hover over the link to see if it leads to the brand's official website.
- Brands will use their official email addresses, so always check the sender's address on emails.
- Always check the number that texts are sent from – although numbers can be spoofed, a seemingly random number is always a red flag.
- Scammers want to push you to act quickly, so be wary of a sense of urgency.
- Check the branding for blurred or pixelated images that don't use the company's latest brand colours.

Voice Cloning Scams

This is where scammers record a person's voice and then use it to create audio content of that person speaking. The scammer can then use the voice recording to make them say anything that they want them to. You may receive a call out of the blue from a loved one in distress who eventually needs you to transfer money for some made-up emergency.



How to spot and avoid these scams:

- The caller likely won't say much – perhaps they'll just say something short like 'please help me'.

- Laugh to see if they're a real person, AI has difficulty recognising and responding to laughter, so saying something off-topic could trip it up.
- Listen for unusual background noises and unexpected changes in the tone of the caller that indicate you aren't having a real-time conversation with a person.
- Ask the caller for as much detail as possible, as only the real person will know these.
- You're asked to make a payment using gift cards or cryptocurrencies, as these are typical of scams.

Reporting AI scams

- On social media, there are usually three dots in the top right-hand corner to report scam posts and ads.
- Report scam texts by forwarding them to 7726 and report emails by sending them to report@phishing.gov.uk.
- Phishing websites can be reported to [the National Cyber Security Centre \(NCSC\)](#).

If you become the victim of a scam, call your bank immediately using the number on the back of your bank card.



Debt Scams

If you receive a letter, call, email, text or doorstep visit demanding a debt payment it can be an alarming and worrying experience. If you do not recognise the debt then you need to be very wary before you agree to pay, not all such demands are genuine. There has been a reported rise in scammers posing as debt collectors and in some cases bailiffs, trying to trick consumers to pay for debts they do not owe.

Bailiff's more properly known as enforcement agents work to enforce court orders demanding payments for unpaid debts. They do have some legal powers to collect debts or goods to the value of the debts. If you are contacted by an enforcement agent and you are in any doubt that the debt is not genuine there are a number of ways you can verify if it is genuine, you should not agree to pay until you have separately verified it is a legitimate debt.

- If the demand claims to come from an HMCTS bailiff (Her Majesty's Courts and Tribunals Service), contact your local county court using the details at [Gov.uk](#)
- If you are worried or unsure, contact the [High Court Enforcement Officers Association](#) and [the Civil Enforcement Officers Association](#), who may be able to help.

It is important to remember that debt collectors do not work for the courts, they may contact you regarding a debt but they have no special powers and must leave if asked. Debt collection agencies work on behalf of companies to collect debts, or debt they have purchased. The principle is the same if you are unsure whether a demand is genuine, don't pay. Instead, try to verify it using trusted contact details.

Some things to look out for which are red flags in debt letter or notices appearing to come from enforcement agents:

- Domains ending in '.legal' – these could be a scam and you should look for a UK domain.

- References to 'bailiffs' in the body of a letter – other than in a company name, firms refer to 'enforcement agents', not bailiffs.
- Threats of Home Office attendance at a removal action – the Home Office does not attend enforcement visits.
- References to appointments for a removal action – enforcement agents do not make appointments after notice has been given.
- Threats of police attendance at a removal action – police do not attend unless there has been a breach of the peace.
- References to a High Court Enforcement Officer and/or Writ of Control re unpaid penalty charges – PCNs are not collected by High Court Enforcement Officers.
- Threats of locksmith attendance/forced entry re unpaid penalty charges – agents cannot force entry for PCNs or council tax debts.
- References to a 'Parking Charge Notice' – parking charge notices are not collected under the Taking Control of Goods Regulations 2013.
- Limited payment options – if bank transfer is the only option, that's likely to be a scam.
- Typos and grammatical errors – a genuine letter is unlikely to contain spelling or grammatical errors.

Scam Marshalls



The National Trading Standards Scams Team are looking to recruit more Scam Marshalls. A Scam Marshall is anyone who has been targeted by a scam and wants to fight back. Scam Marshalls do this by sending any scam mail that they receive to the National Trading Standards Scams Team so that it can be used as evidence in future investigative and enforcement work. The work by Scam Marshalls plays a huge role in helping to stop scam mail.

You can find more information here: www.friendsagainstscams.org.uk/scammarshalls

Illegal Money Lending

The England Illegal Money Lending Team investigates and prosecutes illegal money lenders and provides support for those who have borrowed money from a loan shark. If you have been a victim of a loan shark or know someone who may have been a victim then you can find more information here: www.stoploansharks.co.uk

Take control of who contacts you

- Register with the Telephone Preference Services (TPS) to reduce unwanted sales calls. You can register for free on 0345 070 0707 or go to www.tpsonline.org.uk
- Register with the Mailing Preference Service (MPS) to reduce unwanted mail. You can register for free on 0207 291 3310 or go to www.mpsonline.org.uk
- Register with the Fundraising Preference Service (FPS) to reduce unwanted charity contacts. You can register for free on 0300 303 3517 or go to www.fundraisingregulator.org.uk/the-fundraising-preference-service

Fakes Hotline Number

If you think someone is selling fake goods you can report it by ringing the Trading Standards hotline number: 01782 238444.

When leaving a message please include as much information as you can such as:

- What types of products are being sold and how much they are being sold for.
- The name and address of the seller, if you know it.
- Where the items are being sold, any vehicle being used or a description of where the goods are stored.
- Where the seller can be found.
- Details of any printed advertising, online advertising or social media posts.

If you need advice or want to report a scam to Stoke-on-Trent Trading Standards, please contact the Citizens Advice consumer helpline on: 0808 223 1133
