BE SCAM WISE

SPOT • AVOID • REPORT

Advice from Trading Standards South West on how to spot, avoid and report scams.

For more information about Trading Standards South West and our ScamWise resources, visit:

www.tssw.org.uk/scamwise

Trading Standards South West

What are scams?

Scams are crimes. They are fraudulent activities designed to cheat you out of your money or obtain your personal details for illegal purposes. They come in all shapes and sizes, from bogus lottery wins to miracle cures and chain letters.

Scammers may trick you online, by phone, by post or in person.

Scams target people of all ages, backgrounds and income levels. It's important to be alert to this type of crime so that you can protect yourself and those close to you.

This guide provides information on how to recognise a scam and what to do if you've been scammed.

For examples of current scams, visit www.tssw.org.uk/scamwise

BE SCAM WISE

Report a scam with Citizens advice
0808 223 1133

How to spot scams

One of the best ways to protect yourself from a scam is to know how a scam might look.

Criminals may target you via: the post; telephone; email; the internet; social media - or in person. Whatever the nature of the scam they all share common characteristics.

Here are some of the warning signs to look out for:

- **A request for information:** When you're asked for personal or banking details.
- **An upfront payment demand:** When you're asked to pay money in advance or send a fee, without an agreed contract.
- **A fantastic offer:** When something sounds too good to be true, or is offered on extremely attractive terms.
- **Unexpected contact:** When someone contacts you out-of-the-blue, unexpectedly and without your prior request.
- **Poor communication:** When an email or letter is oddly-written and incorrectly-formatted; perhaps addressed wrongly, or using misplaced words or out-of-date phrases.
- **A sense of urgency:** When you're told that you have limited time to respond and/or you must act quickly.

A scam may not show all of these warning signs. Just one of these factors alone should alert you to the likelihood that the offer is not legitimate.

ONLINE SCAMS

Common online scams

Scammers frequently use email, social media and the internet to con people out of money, obtain personal details, or to install harmful software. Here are some common techniques to be aware of:

You receive an email (a "phishing" email) that looks like it's from your bank, HMRC or another trusted organisation. This can include government agencies asking you to confirm your account details by replying to the email or clicking on a link.

You receive an email saying that you've won an overseas lottery or a prize, but you need to send some money first for taxes or processing fees.

You receive an email from someone overseas asking if they can transfer money into your UK bank account in return for a percentage of the money.

You receive a call out of the blue to tell you there's a problem with your computer or wireless internet. The caller offers to fix it and asks you to download remote access software which gives them access to your computer.

You receive an email or see a pop-up advert online claiming to be able to cure an incurable disease or ailment.

This list is not exhaustive and the nature of online scams is continuously changing so always be suspicious and cautious.

Warning signs

Here are some key warning signals to look out for:

The language in the email is odd and the formatting or spelling is incorrect.

You're contacted unexpectedly by a company or person you've never heard of.

You're asked to provide your personal or banking details.

The site you're purchasing from doesn't have a secure website.

Sites that provide enticing apps or pop-ups to download while you're browsing.

You're asked to download unknown software from an unfamiliar source.

SECURE WEBSITE CHECK
Look out for the https prefix and a padlock symbol in the browser window frame.

BE SCAM WISE
SPOT • AVOID • REPORT

Protect yourself from online scams

Here are a few general tips to protect yourself:

DO

- **Delete** any suspicious emails.
- **Install** genuine antivirus software on your computer and keep it updated.
- **Filter spam** by using an email account with a spam filter.
- **Contact your bank** using the telephone number printed on the back of your card, if you receive a suspicious email from them, such as one asking for your security details. You can also use the 159 service to make contact with your bank through the correct channel.
- **Check** for the padlock icon in the search bar before inserting your card details.
- **Use strong passwords** 15 characters including numbers, letters and symbols.
- **Have different passwords** for each website or app.
- **Enable a pop-up blocker** via the settings page in your browser.

DON'T

- Don't open suspicious emails.
- Don't open links or attachments in emails or text messages from someone you don't know.
- Don't reply to suspicious emails or emails from someone you don't know or those from someone you do know but with content that seems unlikely, or isn't written in their usual style.
- Don't forget to check email addresses by clicking or hovering over the display name.
- Don't give out your personal information, bank details or passwords to anyone.
- Don't respond to requests for money.
- Don't purchase items or services from unsecure websites.
- Don't download unknown apps from unfamiliar sources.
- Don't shop from your social media feeds - verify the vendor independently and visit their shop website using your browser.

Organisations such as Get Safe Online or Action Fraud regularly publish details of the latest scams.
You can find a list of useful contact information at the end of this booklet.

TELEPHONE SCAMS

Common telephone scams

There are many ways that scammers use the phone to try and trick people. Here are some common techniques to be aware of:

The caller says that you're entitled to compensation, a prize, or a lottery win but tells you that you need to pay some money first before you can claim it.

The caller claims to be someone from a reputable organisation, such as your bank or Microsoft, and asks you to reveal personal details and passwords or pay money.

You receive a call from an automated system that has dialled your number very briefly and left a missed call on your phone. The calls are often from premium rate numbers so if you call back, you'll be charged a high rate for making the call.

You receive a text that looks like it's been sent to you by mistake. If you call or text them back to let them know they have the wrong number, you'll be charged a high rate.

Telephone technology is changing and you may be offered fibre optic broadband or digital telephony. Always check for ID from anyone approaching you about new systems, whether they knock on your door, approach you online, or call you. Ask for callback details and end the contact if they become aggressive or evasive at any point.

Warning signs

Here are some key warning signals to look out for:

You weren't expecting the call.

You're being asked to give out your personal or banking details.

It sounds too good to be true.

You receive voicemails or texts from an unknown source. A genuine call blocker company will never cold call you.

BE SCAM WISE

0808 223 1133

Protect yourself from telephone scams

Here are a few general tips to protect yourself:

DO

- **Hang up** if you're not expecting the call.
- **Register** with the Telephone Preference Service to stop unwanted sales calls. You can register your mobile number with them too.
- **Delete** text messages from numbers or people you don't recognise.
- **Block** unwanted calls with a call blocker. If you have a smartphone you can easily block numbers through the settings on your phone. Your telephone provider can also help with this.
- **Consider** using an answerphone to screen your calls.
- **Call back via an established number**. A legitimate company (or your bank) won't mind if you hang up and safely return the call.

DON'T

- Don't give out your bank details, your PIN, or any personal information including your address.
- Don't give out your passwords.
- Don't enter into a contract over the phone.
- Don't ring the number the caller has given you to check authenticity. Look the number up yourself.
- Don't call premium rate numbers to claim a prize.
- Don't call back if you weren't expecting a call and don't recognise the number.

To report a scam please contact the Citizens Advice consumer service on **0808 223 1133**

POSTAL SCAMS

Common postal scams

Scammers regularly use postal mail to try and trick people into giving them money. Here are some common techniques to be aware of:

You receive a letter saying that you've won a prize or a lottery, but you need to send some money, or make an expensive phone call, or pay to register your winnings.

You receive a letter from someone overseas asking if they can transfer money into your UK bank account in return for a percentage of the money.

You receive a letter from a company claiming to have bought a debt from a reputable company or utility supplier with your name on it and threatening court action if you don't pay the fictitious bill or fine.

You receive an unrequested catalogue and are told that you will win a prize if you place an order.

You receive a note in the post stating that a courier has been unable to deliver a package and you need to call a premium rate number to retrieve the package.

You receive a letter telling you about a money-making scheme that involves you sending money to one address and then sending copies of the letter to several other recipients.

Warning signs

Here are some key warning signals to look out for:

You're contacted unexpectedly by a company or person you've never heard of.

The reply address is a PO Box or based abroad.

You're being asked to send money or other forms of payment.

You've been allocated winnings in a competition you never entered.

BE SCAM WISE

SPOT • AVOID • REPORT

Protect yourself from postal scams

Here are a few general tips to protect yourself:

DO

- **Ignore** letters that ask you to send money or give bank details.
- **Shred** post which has your personal details on it.
- **Register** with the Mailing Preference Service to be taken off UK direct mailing lists.
- **Recycle junk mail** - put it straight in the bin.
- **Use a credit card for purchases;** the consumer protection is stronger than with a debit card or other forms of payment.

DON'T

- Don't reply to junk mail. Your name will be added to more scam mailing lists.
- Don't send money upfront to receive a prize or other reward.
- Don't ring a premium rate number- beginning with 09, 118, 0871/2/3, or 070 - to claim a prize or receive a parcel.
- Don't give out your personal information, bank details or passwords to anyone.

If you would like to help us tackle scams why not consider being a Scam Marshal – you'll receive a free regular scam prevention newsletter too. For more information please visit:
www.friendsagainstscams.org.uk/scammarshals

How to protect yourself from scams

Scammers are very clever at duping people into believing their scams are genuine. Here's how you can help protect yourself from falling victim to them:

BE SUSPICIOUS – remind yourself of the warning signs.

DELAY – don't agree to offers or deals immediately. Insist on enough time to obtain independent advice before making a decision.

REMEMBER YOUR RIGHTS – if you agree to buy goods or services and the price is £42 or more you may have cancellation rights under the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013.

HOLD PAYMENTS – never send money to someone you don't know or trust and remember that money doesn't just mean cash - it could include cryptocurrency, vouchers, bonds, or stocks and shares.

BUY SECURELY – only make payments online if there is a padlock symbol in the browser address bar and you've examined the web address for the https protocol. Also look for subtle misspellings, extra words and characters, and other irregularities.

DOUBLE CHECK – if you're unsure, contact the Citizens Advice consumer helpline for help and advice on 0808 223 1133 before you act.

SAFEGUARD YOUR DETAILS – never give your banking details or personal information to anyone you don't know or trust.

DELETE – delete any suspicious emails or throw away any junk mail.

BLOCK – contact your telephone supplier to see what call blocking options are available to you.

SEEK A TRADING STANDARDS APPROVED TRADER – if you're seeking someone to help in your home, e.g. with home improvements or gardening, we recommend using a Buy With Confidence member. Call 01392 383430 or visit www.buywithconfidence.gov.uk

PROTECT YOURSELF – use a credit card for purchases over £100 to get protection from Section 75 of the Consumer Credit Act.

STAY AWARE – keep ahead of the variety of ways in which scammers might target you - from building fraud that starts on your doorstep to cryptocurrency or investment fraud.

STOP AND HANG UP – use the 159 number to call your bank quickly and easily. Visit the following link for more information: www.stopscamsuk.org.uk/159

What to do if you've been scammed?

If you have made a payment in response to a scam, contact your bank as soon as possible as they may be able to recover some of your money and will refund you in certain circumstances. You can find more information about asking your bank for help to get your money back in the Friends Against Scams reimbursement toolkit.

If you or someone else is in immediate danger because of a scam (for example, being threatened by an aggressive doorstep caller), call the Police on 999.

REPORT A SCAM:
Contact Action Fraud

Action Fraud is the UK's national reporting centre for fraud and cyber-crime where you should report fraud if you've 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.

FOR ADVICE: Contact 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.

If you've been the victim of a scam or you know someone that has, it's important to report it. Reporting will help the authorities prevent the scammers from deceiving others.

When reporting a scam, please provide as much information as possible, e.g. company name, contact information or any documentation, as this will help the investigating team.

You should notify your bank if you think you have been a victim. This should help to protect you from future fraud and your bank may be able to support you.

If you've been scammed, it's important to remember that it isn't your fault and you've nothing to feel ashamed about. Talk to your family or a friend about your experience and don't let embarrassment prevent you from reporting a scam.

Useful resources

To get personal support following being scammed contact:

Victim Support: 0808 16 89 111
www.victimsupport.org.uk

Age UK Advice Line: 0800 678 1602
www.ageuk.org.uk

To find out more about Trading Standards South West and their resources visit:
www.tssw.org.uk

To become a Friend Against Scams:

Complete their online training course, visit: www.friendsagainstscams.org.uk/training/friends-elearning

Think Jessica
www.thinkjessica.com

To learn more and keep up with the latest online safety visit:

Get Safe Online -
www.getsafeonline.org

To safely contact your bank when in doubt or concerned that you may have been scammed:

Call 159
www.stopscamsuk.org.uk/159

You can also register with the following services:

Telephone Preference Service
0345 070 0707
www.tpsonline.org.uk

Mailing Preference Service
0207 291 3310
www.mpsonline.org.uk

To make a claim with your bank for reimbursement following a scam, visit:
www.friendsagainstscams.org.uk/shopimages/Reimbursement_toolkit.pdf

BE SCAM WISE

SPOT • AVOID • REPORT

For more information about Trading Standards South West and our ScamWise resources, visit:

www.tssw.org.uk/scamwise

Trading Standards South West