BE SCAM WISE

SPOT • AVOID • REPORT

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

www.tssw.org.uk/scamwise

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

SPOT • AVOID • REPORT

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 post, the telephone, email, the internet or even on your doorstep. Whatever the nature of the scam they all share common characteristics.

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

- **A cold call** – someone contacts you about something that you didn't request or expect.
- **Fantastic offer** – the offer sounds very attractive yet too good to be true.
- **A sense of urgency** – you're told that the offer is only available for a limited time or that you must act quickly.
- **Odd language** – the wording in the email or letter doesn't sound right, or it has bad spelling and grammar.
- **Secrecy** – you're told not to tell anyone.
- **Upfront payment request** – you're asked to pay money upfront or send a fee without an agreed contract.
- **Information request** – you're asked to give personal information or banking details.

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

ONLINE SCAMS

Common online scams

Scammers increasingly use email 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 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 strange or has spelling and grammatical errors.

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

You're being 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.

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** antivirus software on your computer and keep it updated.
- **Filter spam** by using an email account with a spam filter.
- **Contact your bank** by telephone if you receive an email from them asking for your security details.
- **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.

DON'T

- Don't open suspicious emails.
- Don't open links or attachments in emails from someone you don't know.
- Don't reply to suspicious emails or emails from someone you don't know.
- 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 apps from unknown, unfamiliar websites.

SECURE WEBSITE CHECK

Look out for the https prefix or a padlock symbol in the browser window frame.

Organisations such as Get Safe Online and Action Fraud regularly publish details of the latest scams. You'll find their contact details 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.

The caller offers you the opportunity to buy shares or invest money claiming that you'll receive high returns.

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.

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.

A genuine call blocker company will never cold call you.

BE SCAM WISE

SPOT • AVOID • REPORT

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.
- **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.

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.

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 to claim 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.

You receive a scratch card in the mail, but have to pay to register your win.

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.

It sounds too good to be true.

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.

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 to claim a prize or receive a parcel.
- Don't give out your personal information, bank details or passwords to anyone.

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.

BUY SECURELY – only make payments online if there is a padlock symbol in the browser window frame and you've carefully checked the web address for subtle misspellings, additional words and characters and other irregularities.

DOUBLE CHECK – if you're unsure, contact the Citizens Advice consumer helpline for help and advice on 03454 04 05 06 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

What to do if you've been scammed?

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.

To report and ask for advice about a scam contact:

The Citizens Advice consumer helpline

03454 04 05 06

www.citizensadvice.org.uk/consumer/get-more-help/if-you-need-more-help-about-a-consumer-issue

Action Fraud

0300 123 2040

www.actionfraud.police.uk/report_fraud

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 learn more and keep up with the latest online safety information, visit:
Get Safe Online - www.getsafeonline.org

To register with the Telephone Preference Service, visit:
www.tpsonline.org.uk or call 0345 070 0707

To register with the Mailing Preference Service, visit:
www.mpsonline.org.uk or call 0207 291 3310

To find a Trading Standards approved trader, visit:
www.buywithconfidence.gov.uk or call 01392 383430

To become a Friend Against Scams and complete their online training course, visit: www.friendsagainstscams.org.uk/training/friends-elearning

Recommended call blockers:

CPR call blocker
www.cprcallblocker.com

Truecall
www.truecall.co.uk

Speak to your telephone provider as they may be able to offer you a call blocking service.

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