ONLINE SCAMS

Advice from Trading Standards South West on how to stay safe from online scams.

BE SCAM WISE

SPOT • AVOID • REPORT

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 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.

Protect yourself

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 purportedly 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 application.

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 insecure 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 below.

For reporting and further advice

The Citizens Advice consumer helpline
03454 04 05 06

Action Fraud
0300 123 2040

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

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

www.tssw.org.uk/consumer

Trading Standards South West