Online scams

Scams online move very fast, with scammers using topical issues to attempt to draw people into sending money to them or obtaining personal information such as bank details, credit card details, national insurance numbers and addresses.

Some examples are:

- Sellers offering hugely discounted designer items or hard to come by items.
- Pop-ups online or phone calls alerting you to potential viruses or software issues that need to access your device to resolve.
- Emails or messages pretending to be from an organisation or friend, often asking you to follow a link in the messages.
- Websites charging fees to renew or process documents.
- Free trials or 'just pay for postage and packaging' deals.
- Romance or friendship scams

These can all be warning signs that someone is trying to scam you. Take steps to avoid the scammers.

- Check the website is genuine - Take a couple of minutes to watch the video provided by National Cyber Security Centre about shopping securely online
- If you do an internet search, don't assume that the top listed company is the genuine one you are looking for. Sometimes these can be adverts or a very slight change in the company name you are looking for.
- Check the domain name to get to the official page, and avoid sites that end in .net or .org - it is unusual for shopping sites to use these. There should be a geographical address to return items, with details of the returns policy.
- Search the Financial Conduct Authority register to check if a company offering investment or pension opportunities is registered. https://register.fca.org.uk/s/
- Never automatically click on a link in an unexpected email, text, or social media. Check with the person or organisation via another contact method what it is and why they have sent it to you. For example,

organisations such as the HMRC tax office will not text or email you with a link to add your bank details for a refund.

- People who contact you out of the blue via social media, who may ask for help or money. This may also happen with friends' accounts that have been hacked. Check with the person in another way.
- Don't give your bank details over until you are sure it is a genuine company/ seller and the items are genuine too.
- Check for http or https at the beginning of the weblink. The 's' means the connection is secure. More information can be found on get safe online website.
- Use a payment method that offers protection if there is a problem (such as PayPal, Apple pay, debit or credit card.)
- Check in advance of using the website or online platform what their online dispute resolution process is.
- Don't send money by bank transfer. Once you have sent a payment, it can be very difficult to trace and get it returned if there is a problem.
- Don't click on email links via text or email. Speak to the friend or organisation that has seemingly sent it to you. If this is someone that has befriended you over the internet, be very cautious about why they are sending this to you and why they need your bank details or for you to send money. Sadly, there are many reports of people being scammed by those they think are their friends or in relationships with.

You can also use the check if something might be a scam page following the instructions www.citizensadvice.org.uk/consumer/scams/check-if-something-might-be-a-scam/. To report an online scam or get further advice from Citizens Advice Scams Action Service, call 0808 2505050, or you can talk to an adviser online. www.citizensadvice.org.uk/consumer/scams/check-if-something-might-be-a-scam/

For further advice, contact Citizens Advice consumer helpline 0808 223 1133, Welsh-speaking adviser 0808 223 1144.

Relay UK - if you can't hear or speak on the phone, you can type what you want to say: 18001 then 0808 223 1133.
www.citizensadvice.org.uk/consumer/get-more-help/if-you-need-more-help-about-a-consumer-issue/