

SCAMS AWARENESS UPDATE

Older Persons Scams Awareness & Aftercare Project

In this update:

Online shopping scams
Page 2

The 12 scam saves of
Christmas
Page 3

Current scams
Page 4



Shop Scam Savvy this Christmas

Whether you're reading this as a regular subscriber, because a friend has passed it to you, or as a result of National Safeguarding Adults Week - WELCOME!

We're pleased to be supporting Cheshire East Council's Adult Safeguarding Team, to raise awareness of adult abuse, including grooming through romance fraud (featured in our July issue) and online scams - this month's feature. For more information about adult safeguarding week, head to www.stopadultabuse.org.uk/NSA2020.

This bulletin is part of our Older Persons Scams Awareness & Aftercare Project, run in partnership with Cheshire East Council's Trading Standards Team. Information about the project and further resources can be found on our [Age UK Cheshire East website](http://AgeUKCheshireEast.org.uk) or by contacting Sally Wilson at sally.wilson@ageukce.org or on 07932 999902.

Now, let's read on to see how to spot, avoid and report scams, as we're online more in the run up to Christmas.



Shopping online can save time and gives a wide choice of goods from around the world. It has become even more popular during the COVID-19 pandemic, and will continue to be in the run up to this very different Christmas.

While most buyers and sellers are genuine, fraudsters use online shopping scams because they can hide their identity, and target many victims at the same time.

In the first half of 2020 over 40,000 cases of online shopping and auction fraud were reported, totalling over £29 million*.

*FOI request from Action Fraud

Online shopping scams are one of many cybercrimes. The scams come in many forms - on websites, social media or through emails and texts. All are designed to get you to part with your money, or trick you into disclosing personal or bank details.

Here are some to look out for:



Free vouchers, gift cards or offers too good to be true – The majority of these are scams. They ask for personal details that scammers use to access your bank accounts, or install viruses to steal information from your device. You may also unknowingly have signed up to a monthly subscription.

Fake goods or fake websites - The festive period is a popular time for fraudsters to sell counterfeit goods - from designer clothing to electronic appliances and gadgets. The items may be of poor quality, unsafe (even dangerous), or never arrive.



Social media scams - Fraudsters use sites such as Facebook and Instagram to advertise offers and bargains, to get you to click on the advert, and be redirected to a bogus website that can be full of viruses and scams.













Fake delivery notifications – Fraudsters send emails pretending to be from the Post Office, Royal Mail or other delivery companies saying you have a parcel to collect. They ask you to click on a link and enter personal information to verify the delivery. This gives the scammer your details. They can also put malware on to your electronic device.



Payment scams - You may receive a message saying there's an issue with your payment account (e.g. Paypal, ApplePay, GooglePay) and asking you to click a link to verify your personal details. If you sell goods online, you may receive an email tricking you into believing payment has been made, so you send the goods (to the criminal).

“Tis the season to save lolly!” - It may seem that there’s too much to go wrong in cyberspace to bother shopping online; but fear not - with these 12 scam saves of Christmas you can enjoy the benefits for online shopping whilst avoiding scams too:

REMEMBER:

-  **If it’s too** good to be true it usually is. Don’t fall for it!
-  **Always use reputable** websites when shopping or searching online.
-  **Research a website** or company as much as possible before buying goods from them.
-  **Create a different**, strong password for each of your online accounts. A recommended method is to use 3 random words together. For extra security, set up ‘two-factor authentication’ which means you get a code sent to your phone to use.
-  **Type in the** website address (the ‘URL’) in full into Google or other search engines. Avoid clicking on a link in an email, text or post, as this may take you to the fraudster’s site instead.
-  **Pay securely** - check the address bar at the top left of the screen to make sure that the website address begins “https”. The ‘S’ stands for secure. There should also be a closed padlock image in front of the ‘https’.
-  **Don’t be ‘click-happy’!** NEVER rush in to making a purchase.
-  **Don’t pay for** anything by transferring money directly to people or companies you don’t know. Use secure payment methods such as Paypal, ApplePay etc.
-  **When you’ve finished** paying, make sure you log out of the page or app. Simply closing it may not log you out automatically.
-  **Check URL’s of** emails to ensure they are genuine. Scam emails are usually littered with spelling and grammar mistakes.
-  **Avoid ‘free’ or ‘low-cost’** trials – whether slimming pills or the latest tech. Without thoroughly reading the small print and trusted reviews, you could be signing up for large monthly direct debits which are difficult to cancel.
-  **Check your bank** account regularly for any unknown transactions.

If you have been a victim of an online scam, report it to Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk.

If you are having issues with something you have ordered online, call Citizens Advice on 0808 223 1133.

Always contact your bank immediately if you have transferred money to the scammer in the last 24 hours or you think your account details or PIN have been stolen.

Not all scams happen online. Here are some recent postal, doorstep and phone scams:

Fake COVID-19 Marshals

The Chartered Trading Standards



Institute has received reports of people pretending to be COVID marshals to gain access to people's homes. COVID-19 marshals will never come to your door unannounced and don't have the right of entry, or the right to issue fines.

Cheshire East Council are not employing COVID-19 Marshals.

Report any strangers on your doorstep to the Police on **101**.



Ongoing scams

There are still many 'old' scams going around.

These include calls and emails pretending to be from HMRC, Amazon, BT Openreach and Microsoft. They threaten legal action, ask for remote access to your broadband, offer a refund or ask you to verify personal/bank details.

Don't be fooled by the urgency of these messages. Contact the companies independently to check if they genuinely tried to contact you.

Green Homes Grant cold calls

We've had reports of calls claiming to be from the Energy Saving Advice Service, offering a free survey. They sometimes claim to be linked to the Green Homes Grant.



Remember, only approved traders carry out the Green Homes work and must meet certain criteria. The REAL Energy Saving Advice Service can be contacted on 0300 123 1234.



Council tax rebanding scam

Some people have received letters from companies offering to apply for a council tax re-band, which may include a refund. They then charge a fee for the application.

You can apply for a FREE review of your council tax band at any time. Just contact your local council. For Cheshire East the number is 0300 123 5013.

COMING NEXT TIME...

- Current scams
- Focus on social media scams

Though we don't like to see you go, you can unsubscribe from these bulletins by emailing sally.wilson@ageukce.org

The Older Persons Scams Awareness & Aftercare Project is brought to you by