Cheshire East Age UK

ISSUE 49 - APRIL 2024

SCAMS AWARENESS UPDATE

Older Persons Scams Awareness & Aftercare Project

In this update:

Stop! Think Fraud

National campaign against fraud

Fraud is everyone's problem. According to the latest statistics, fraud accounts for almost 40% of all crime in England and Wales, and in just one year 1 in 17 adults were a victim of fraud.

As a result, the government has launched a new national campaign - Stop!Think Fraud. It encourages people to take a moment and check for common signs of scams before providing personal details or payments.

If you're a regular reader of our bulletin, many of the messages may be familiar. But, none of us are immune to fraud. So, turn over to learn more about keeping our information and money safe from fraudsters.

We're taking a break! *This monthly bulletin can only run if funded by external grants. Despite significant efforts to obtain future funding we have been unsuccessful to date. So, unfortunately, the Scams Awareness Update bulletin will be suspended from May 2024. We continue to look for funding, and hope the suspension is temporary. We'll be back in touch when we're up and running again.*

Remember *- if you want to keep up to date with how to protect yourself from scams and fraud, why not book a personalised scams advice visit? If you are aged 50+ and live in Cheshire East, contact us on 01625 612958 or enquiries@ageukce.org for more information.*

Stop! Think Fraud

Criminals who commit fraud target people online and in their homes. They often manipulate their victims emotionally before they steal money or personal data.

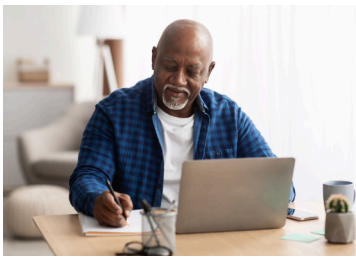
But there is always something we can do. By staying vigilant and always taking a moment to stop, think and check whenever we're approached, we can help to protect ourselves and each other from fraud.

The Stop! Think Fraud campaign asks us to consider protecting ourselves:

AT HOME: Fraudsters pose ***on the doorstep*** as traders, charity collectors or someone down on their luck. They can manipulate us into believing what they say is true, to get their hands on our money or our personal and financial information.
Through the post, fraudsters send letters to obtain money through deception. This could be the offer of a prize draw, a clairvoyant reading or goods from a catalogue. Very often they are all from the same gang of criminals. They will ask you for an upfront fee for something that, in reality, doesn't exist.
On the phone and text messages, criminals pretend to be someone we trust or have bought goods and services from and convince us to hand over confidential information, make a payment or give them access to your computer.

Stop! Think Fraud has a useful website with lots of top tips. Search for www.stopthinkfraud.campaign.gov.uk on the internet on your phone, tablet, laptop or computer.

ONLINE: Criminals send fake emails and set up fake adverts and websites. These are designed to steal your bank details and other personal information, so they can take money from your account or use your details to commit fraud elsewhere. They find out information about you from your social media profile and use this to manipulate a fake friendship with you, or use your details for a fake profile to manipulate other victims.



IN PUBLIC PLACES: Sometimes, criminals watch us entering usernames, passwords and PINs on devices in shops and at cash machines. Then, they attempt to steal the card, through distraction or using a device, so they can access your bank account.
Fraudsters manipulate our need to be online everywhere. They hack into public WiFi, or set up a similar looking wifi hotspot to be able to read everything you are doing on the web.

Top Tips to Protect Yourself

Wherever we are, whatever we're doing, to protect ourselves, the Stop! Think Fraud campaign asks us to frustrate the fraudsters by:

Stopping and checking who's contacting us: Never take calls or messages at face value – always take time to stop, think and check if the caller or sender is who they say they are.
Don't be rushed into a quick decision. If you have any doubts, hang up and do not call the number provided, as fraudsters can spoof phone numbers. This means the number that appears on your phone may not be proof of who they really are. Instead, check with the organisation directly using contact details you know are correct.

Not trusting offers or clicking on links: don't be rushed into a quick decision – always take time to stop, think and check if the message, offer or advert is genuine.
Don't automatically click a link, particularly in unexpected messages. If you're not 100% sure, don't use the link to click through – go direct to the organisation's website.
Always stay on trusted websites. Use the site's recommended payment methods and avoid paying by bank transfer or virtual currency.

Using different passwords for different accounts: Choose a different password for each account. If it's too difficult to remember them all, you can use 3 random words e.g.MoonBellowGiraffe to make them more memorable. Or, you can use a password manager.
Never choose a password that features names, places and numbers that are personal to you. Choose a different password for each account that is strong and hard to guess. But if you can't change them all at once, prioritise the password for your email account.

Using 2-step verification on at least your email and banking accounts: Even if someone has chosen strong and unique passwords for their email and bank accounts, there's always a risk – however small – that a fraudster could get hold of them. 2-step verification sends a code to your phone when you (or anyone else) attempts to sign in to your account. Only the person with your phone (you!) can use the code to access your account. Head to the settings in your email/bank/social media accounts to set up 2-step verification. If you're not sure how to, ask a trusted relative or friend to help. Alternatively, contact your local library, who have IT Buddies to help.

Stop! Think Fraud encourage us to report fraud.

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

Forward suspicious texts to 7726 and suspicious emails to report@phishing.gov.uk.

To report rogue traders, contact Citizens Advice on 0808 223 1133.

Current Fraud Alerts

Here are some recent frauds to look out for. Please share with family, friends and community.

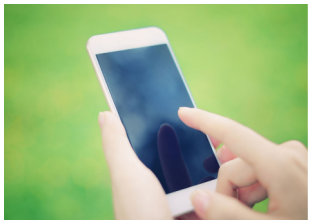
Door-to-door charity workers

We have received reports of people going door-to-door in Congleton saying they are from a range of different charities. This isn't illegal. But, fraudsters often pose as charity workers. They ask you to sign up to regular donations to get your personal or banking details to use fraudulently.

Trading Standards always advise to not deal on the doorstep. You don't need to answer the door, and it's okay to say "No thank you" to any caller you're not expecting.

If you want to donate to charity, contact them on an independent number.

Telephone digital switchover text message



The "digital switchover" is the switch to digital services for all landline phones in the UK. Your phone provider will contact you when it's your turn to "switch."

But, fraudsters are taking advantage, and contacting people by text message pretending to be a phone provider. They ask you to call a number and for an up to date phone bill for details.

Whilst this may be how your phone provider contacts you, if you receive a text out of the blue it's always best to contact your phone provider independently to check.

Fraudulent "friend" emails

People have received emails from one of their contacts asking for help. They say that they are emailing, rather than phoning, as they have laryngitis, so can't speak. But it's not their friend, it's a criminal who has hacked into the friend's email account.

If the person responds, eventually they will be asked for money in some form (bank transfer, iTunes vouchers etc.), to help them out.

Never reply to such emails. Phone the friend, to check how they are. It's likely they're not ill at all and can speak perfectly.

Fake bank websites

Last year, there were more that 2,000 reports of fake websites imitating UK banks.

As we are banking online more and more, it's important to check that the website you're using is genuine.

Never click on a link in a text message or email directing you to your bank website. Always check the website address is exactly the same as a trusted website address (which you can find on your bank card or written correspondence from your bank).

Though we don't like to see you leave, you can unsubscribe from these bulletins by emailing: enquiries@ageukce.org

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

Cheshire East ageUK *in partnership with* Cheshire East Council Trading Standards