Cheshire East Age UK

ISSUE 38 - MAY 2023

SCAMS AWARENESS UPDATE

Older Persons Scams Awareness & Aftercare Project

In this update:

Battling identity theft and fraud

Protect yourself from both threats

Identity theft and identity fraud are two different concepts. But one often leads to the other.

Identity theft is when your personal information is stolen. Details such as your name, address, National Insurance number, bank or credit card number can be taken from you without your consent or knowledge in a lot of different ways.

Identity fraud is the use of a stolen identity in criminal activity to obtain goods and services by deception. Fraudsters can use your identity details to order goods, open new bank accounts, apply for loans or other financial services, or even obtain genuine documents such as passports and driving licences in your name.

Identity theft and fraud have risen in the past few years. We can all be vulnerable to it. So, read on to learn the different ways fraudsters can steal your identity and how to prevent this so you can avoid becoming a victim of identity fraud.

If you would like to talk about your personal situation and fraud, you can book a free appointment with a member of our Scams Awareness & Aftercare Team. Contact us on 01625 612958 or at enquiries@ageukce.org.

Proudly funded by John Dwyer Police & Crime Commissioner for Cheshire

Cheshire East Age UK in partnership with Cheshire East Council Trading Standards

Avoiding Identity Fraud…

Keeping our identity safe makes us less vulnerable to it being stolen and used for identity fraud. But, how does identity theft happen, what does identity fraud look like, and how would you know you're a victim?

How identity theft happens

Criminals steal information to build up a duplicate identity.

This is often from a range of sources and over a period of time.

Criminals can get information from:

- *Discarded paperwork - e.g. bank statements and letters in your bin*
- *Lost documents such as a passport, driving licence or bank card*
- *Data breaches at companies who you've genuinely given your data to*
- *Social media posts, photos and answers to quizzes etc.*
- *Phone calls, emails and texts you receive asking you for details or to confirm information*

What identity fraud looks like

Fraudsters will use the stolen information to:

- *Take over your existing accounts*
- *Open bank accounts in your name to use the overdraft or to launder money*
- *Obtain state benefits in your name*
- *Order goods in your name*
- *Take out credit contracts in your name that they never pay back - e.g. phone contracts, catalogue accounts, store cards, personal loans, credit cards and mortgages*
- *Obtain genuine documents such as passports and driving licences in your name*

How you know you're a victim

You may not know your identity has been stolen and used until:

- *You are refused credit when you apply for a new phone, energy supplier, loan or credit card*
- *You receive a letter from a company or organisation saying you owe money*
- *A letter arrives from the bank about a new account opened in your name*
- *A new bank card and PIN arrive for an account you've not opened*

In 2019, the credit score company Equifax reported that identity theft had risen by 17% in one year. In 2021, the CiFAS organisation reported an 11% increase in identity fraud in the first half of the year.

…by Keeping Our Identity Safe

The best way to avoid becoming a victim of identity fraud is to keep our personal and banking information safe in our everyday lives.

How to prevent identity theft

Here are some top tips we can all do:

- *Shred paperwork that is no longer needed. Alternatively, dip the confidential information in the washing up water, screw it up tightly and pop it in the bin*
- *Report lost or stolen documents and cards immediately*
- *Don't be afraid to ask why information is being requested, and only give the minimum amount of information required. For example, just one piece of contact information to get a refund*
- *Never give personal or bank details to someone who has contacted you, whoever they say they are. Say you will contact the genuine organisation on an independent number or trusted email address*
- *Avoid answering quizzes and surveys on social media*
- *On social media, set your privacy settings so only invited friends can see what you post*
- *When talking to people, especially online, be careful about the information you share about what's happening in your life, your friends, family, interests and work*
- *Sign up online to a free monthly credit score report from Equifax, Transunion or Experian. You may need to give some basic information, but this is only so your bank accounts can be linked to your credit score*

If you are a victim of identity fraud

Act immediately to minimise the impact:

- *Tell your bank and report it to the police on 101*
- *Sign up online to a free monthly credit score report (see above). Your report will show "hard searches" which is where credit has been applied for in your name*
- *Apply for protective registration from CIFAS. This places a warning flag against your name and other personal details in the CIFAS National Fraud Database. This tells organisations to pay special attention when your details are used to apply for their products or services. There is a small fee. More information can be found at https://www.cifas.org.uk/pr*
- *Monitor transactions on all your accounts. Report any that you don't recognise to the bank or company you have the account with*
- *Contact us at Age UK Cheshire East on 01625 612958 for practical and emotional support as a victim of fraud*

CURRENT FRAUD ALERTS

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

Fake "storage full" emails

People with Microsoft Hotmail email accounts have reported receiving an email saying their document storage is full and offering more storage, as a loyal customer. This leads to a fake website, which asks for personal, contact and bank details. Fraudsters can then use this information to scam you further.

It's always best to check if an email is legitimate, such as looking at the sender's email address. Genuine emails about this will come from microsoft@mail.onedrive.com.

Safe account scam phone calls

Over half of frauds reported to banks are from customers who have received a call pretending to be their bank, telling them there is fraudulent activity on their account, and they need to move money to a safe account.

Recently, we have spoken to victims of this crime in Cheshire East. They have told us how convincing the fraudsters were. They wanted to warn others about this scam.

Remember - banks NEVER ask you to move money to a new account. If you're asked to do this, hang up and dial 159 to contact your bank.

Rogue traders offering spray insulation

Trading Standards are warning people to do their research when it comes to home insulation. There have been reports of rogue traders using high pressure sales techniques to persuade home owners to agree to spray insulation being installed, regardless of if it's suitable for the property.

Never deal with anyone who cold calls on your doorstep, by phone, email or letter. Approach reputable traders independently, get a range of quotes and never be pressured in to agreeing to work.

Cost-of-living payments

Some people are entitled to further cost-of-living payments. The Department for Work and Pensions (DWP) has started to pay these out.

If you are entitled to a cost-of-living payment, it will be paid to you automatically. You do not need to apply for it.

So, if anyone contacts you asking you to apply for the payment, or asks for contact or bank details to process a claim, it's a scam.

COMING NEXT TIME

- **Current fraud alerts**
- **Phone scams**

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

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