Cheshire East ageUK

ISSUE 30 - SEPTEMBER 2022

SCAMS AWARENESS UPDATE

Older Persons Scams Awareness & Aftercare Project

In this update:

Banking Fraud

Bank safely to keep the fraudsters at bay

Along with our health, keeping our money safe is very important to us. Unfortunately, fraudsters play on our natural instinct to protect what is important to us.

These days, we don't only bank on the high street. We can bank in branch or through a telephone banking service. We may bank online on a smartphone, tablet or iPad or computer, using a website or a specialist banking app.

However we bank, we can be at risk of becoming a victim of fraud when it comes to our bank and credit card accounts. Last year, £730.4 million was lost to fraud.
Of this, £321 million was lost through authorised push payments (featured in our July bulletin) and £292 million through payment card fraud. Remote banking accounted for only 15%, with cheque fraud making up less than 1% of the total.

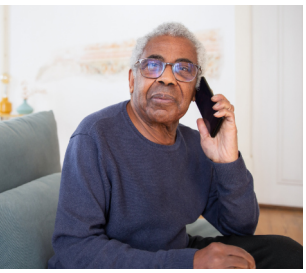
Read on to find out about current, common banking frauds, and the simple things we can do to avoid becoming a victim.

We believe the best way to protect yourself from fraud is to have a personalised scams advice session. That way, we can talk about what's important to ***you***. To book a free appointment, contact our Scams Awareness & Aftercare Team on 01625 612958 or at enquiries@ageukce.org

BANKING FRAUDS…

Criminals will use many tactics to get access to the money in our accounts. They may act with authority by pretending to be from the police, the bank or an official organisation. They may ask you to act quickly (so you don't have chance to think if it is genuine).
Others may use technology or distraction techniques to get the information they need to take money from your account.

Here are some of the most common banking scams to look out for…



Safe account: This happens when you receive a phone call from someone saying they're from your bank. Through conversation, they persuade you that there is fraudulent activity on your account, so you need to move money immediately to a safe account. They put pressure on you and create a sense of urgency, claiming they are helping you to save your money. In this "hot state" they create, with no time to think, it is easy to be drawn into this fraud.

Courier fraud: Featured in our June bulletin, this type of fraud is still happening in Cheshire East. Another fraud that happens on the phone, the criminals pretend to be from your bank or the police. With a made up story of helping an investigation, they persuade you to withdraw cash or buy goods, which a courier will collect. Alternatively, they may tell you there's a problem with your bank card and a courier will collect it before a new one is issued.

Card not received: This happens when a bank sends out a new or replacement card to a customer, but it is intercepted along the way.

If the card is new, the PIN code should be sent in a separate letter, but this won't stop a scammer from using the card for online purchases. They may also intercept the letter containing the PIN.

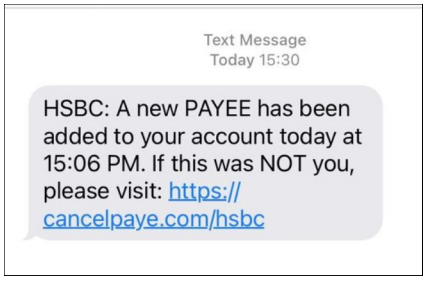
This type of fraud can be harder to detect because you might not notice the card is missing at first, thinking it's just stuck in the post.

Emails asking to update details: Criminals send emails which are very convincing, with a copy of a bank's logo, correct contact details and even fraud warnings. The email asks you to click on a link to update your personal or online banking details. A recent example was shared with our project, pretending to be from Santander. It bamboozled the customer with jargon, talking about new regulations and One Time Passwords to hurry them into clicking on a link to update personal details, so they can continue banking.

Skimming: This is the illegal process of duplicating the information found on the magnetic strip of an account card. Criminals tamper with cash machines (ATMs) and use a miniature camera to clone your card and steal your PIN.

The fraudster then "skims" the data located in the magnetic strip to make an illegal card or use the card details online or over the phone.

New payee/device text messages: You may receive a message to say a new payee has been set up or a new device has been detected on your online banking. It says if you didn't arrange this, to click on a link. These messages can look as though they are coming from your bank and are set to panic you into clicking on the link to stop fraudulent activity. In reality, following the link could give fraudsters access to you account.



…and top tips to stop you becoming a victim:

Remember that banks and the police will NEVER call you to ask you to move or withdraw money from your account.

Never click on links in emails or text messages asking you to update your security or details.

Always keep your PIN details, account cards and cheque books safe, and check ATM machines for anything unusual.

Regularly check your bank statements and report any irregular transactions to the bank straight away.

Tell your bank immediately if your bank card is lost or stolen.

Make a note of when new bank cards are due to arrive, so you can report it if they are late.

If you bank online (on your computer, phone or tablet), ask your bank to show you all the features, so you bank online safely.

Remember to log out of your online banking. Just clicking on the X at the top of the page may not log you out.

Look for the Visa Secure or Mastercard Identity Check logos on websites when buying online. These make online shopping more secure by protecting against unauthorised use of your Mastercard or Visa card. When you check out, you may be guided through an additional check on your identity.

If you have given money, personal or financial information to someone who you think is not genuine, tell your bank immediately and report it to Action Fraud online or on 0300 123 2040

CURRENT FRAUD ALERTS

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

Apple Pay fraudulent text message

iPhone users are being targeted by this scam.

People are receiving messages to say their Apple Pay account has been suspended and to click on a link to reinstate it. This takes you to a fraudulent website, asking for your bank account details to reinstate your account.

If you receive such a message, do not click on the link. Log in to your account independently to check its status and contact Apple on a trusted number/source if there is anything suspicious.

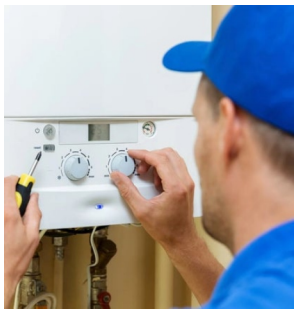
Energy rebate scam emails

In just 2 weeks, Action Fraud received over 1,560 reports of suspicious emails pretending to be from Ofgem, offering a rebate on energy bills.

With announcements being made all the time about the energy crisis, if you have any doubts about a message, contact the organisation directly.

Remember, official organisations will never ask you to supply personal or banking information via email.

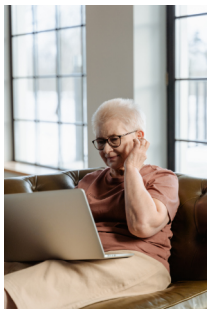
ECO4 boiler replacement scheme cold calls



One of our Age UK partners has told us about cold callers offering a free boiler replacement under the government's ECO4 scheme. The scheme is legitimate (running until 2026), but many of the companies are abandoning boiler installations halfway through, claiming that funding for the project has ran out.

If you are looking for a new boiler, research, get several quotes and use a reputable company. If you experience a company abandoning work, contact Citizens Advice on 0808 223 1133.

Gift card purchase scam



Fraudsters are playing on our human trait of wanting to help. They contact you by email or text pretending to be someone you know. They say they want to buy a gift card for a relative, but can't get to the shops. So, they ask you to buy the gift card and then share the serial number with them, so they can pass it on to the relative, in time for their birthday, exam results etc.

If you are contacted in this way, always call the person to check if they have sent the message.

COMING NEXT TIME

- **Current fraud alerts**
- **Cost of living frauds**