Cheshire East Age UK

ISSUE 35 - FEBRUARY 2023

SCAMS AWARENESS UPDATE

Older Persons Scams Awareness & Aftercare Project

In this update:

Protecting your money

What banks are doing to combat fraud

One thing is certain with fraud - somewhere along the road, your bank account will be involved. Whether it's withdrawing cash in branch to pay a rogue trader for poor work or transferring money online to help someone out that you've met on the internet.

As fraud continues to be the most commonly experienced crime in the UK, banks have a balancing act of allowing us access to our money and protecting us from fraud. They use advancements in technology available to them, alongside educating customers and collaborating with law enforcement.

If we want to keep our money safe, we also need to do everything possible to avoid fraudulent activity on our accounts.

This month, we've teamed up with representatives from the banking industry to explore what the banks are doing to prevent fraud occurring, and what we need to do to keep our money safe.

If you are affected by issues raised in this bulletin, or any other type of fraud, you can speak to us. To book a free appointment, contact our Scams Awareness & Aftercare Team on 01625 612958 or at enquiries@ageukce.org

Banks' response to fraud

We have featured frauds directly targeting money in your banks accounts in previous editions. But, here are some other tactics fraudsters may use:

Money Muling: A money mule is someone who lets criminals use their bank account to move money. Often the mule doesn't know what's really happening. They have been manipulated into believing a cover story, such as helping out a friend or a police operation, or they are enticed by the offer of a reward payment.

Money muling is a criminal offence, leading to many years in prison and a poor credit rating.

Never let anyone put money into your bank account, without good reason.

Asking for one-time passcodes: To keep your accounts secure, banks and other organisations send one-time passcodes (OTP) to your phone for you to log into your account.

Fraudsters call people, pretending to be such organisations, saying there is an issue with your account. They ask you to log into your account and then give them the OTP that was just delivered to your phone by text or email, so they can sort out the problem. This gives them access to your account.

Never share an OTP with anyone. Your bank or any other reputable company will never ask you to share an OTP with them.

Lying to the bank: Criminals know the banks are aware of fraud. So, they often tell victims to lie to the bank when they are asked why they want to withdraw or transfer money. They even tell victims the bank is acting fraudulently, so to not tell them the truth.

Honesty is always the best policy. If someone tells you to lie or keep a secret about money, tell your bank straight away.

The safest place for your money is in your bank account. Banks have a wide range of checks in place to keep it safe from fraud.

Here are some of the ways banks are keeping our money safe in our accounts.

Banks will:

- Send letters or emails telling you how to recognise a genuine contact from your bank.
- Ask you who you are making payments to, and why.
- Give you fraud warnings, to help you stop and think before moving money.

Banks will NEVER:

- Ask you to complete a "test transaction", for example, sending money to another account.
- They will never ask for all of your password, any of your PIN or one-time passcode.

Our responsibilities to combat fraud

It's our money, so the gift of keeping it safe is in our hands. Here are some top tips from banks about how we can help to keep money safe in our accounts:

- Check with your bank how they will contact you if they suspect a fraudulent transaction on your account.
- Make sure your bank has your current contact details. Then they can contact you quickly if there is possible fraud on your account.
- Always be honest about who you are moving money to, and why. The bank isn't being nosey, they're just checking the transaction is genuine.
- Never agree to receiving money into your account, however desperate the person may appear or however tempting the offer of a reward payment may be.
- Make sure you read very carefully each of the fraud warnings with each transaction you make. The bank is giving you the opportunity to stop and think about whether the transaction is genuine.
- Never share passwords, your PIN or one-time passcodes.
- Sign your bank card as soon as you receive it, and never give to anyone else.
- Set up strong passwords - for example, using 3 random words. Avoid using pets names, football teams, birthdays etc.
- Set up 2 factor authentication for your online banking. Ask your bank to help you with this.
- If you receive a text from your bank asking you about the transaction you have just made, consider if it is genuine, then respond accordingly. If you ignore it, your account may be frozen until you contact the bank.
- Run regular virus checks on the device you use for online banking.

What to do if you have been a victim of fraud on your bank account

Contact your bank immediately if:

You think your security details, card or device (like a smartphone) has been lost, stolen, damaged or is being misused.

You think someone else can access your accounts without your permission or knows your security details.

If you have transferred money to another account and then realised it may have been fraudulent.

The bank can help secure your account and avoid losing more money.

CURRENT FRAUD ALERTS

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

Fake equity release email

Equity release is an agreement that lets you access money from the equity in your property, without having to leave your home. There are many legitimate equity release schemes.

One of our volunteers received an email offering this service out of the blue. Luckily, they checked the email address it was sent from, and found it wasn't from a legitimate equity release company. If they had been interested in equity release, they may have fallen for this scam, if they hadn't made the checks.

Fraudulent Car Parking QR codes

We highlighted a QR code scam last month. Here's another to be aware of.

Criminals are sticking fake QR codes on parking machines, to steal money from drivers using their phones to pay. If you scan the code with your phone you'll be taken to a fake version of the parking company's website, and asked to enter your card details.

Always look carefully at the QR codes to see if they have been stuck on over the legitimate code.

Election photo ID open to fraud

For the elections due on 4th May 2023, everyone will need to show photo identification in order to vote. There is more information on the Electoral Commission website or by calling 0800 328 0280. You do not need to pay to get photo ID.

Unfortunately, we believe criminals will contact people to offer them photo ID, at a cost and to steal personal and bank account details. If you receive such an offer, do not engage with it and report it to the Electoral Commission.

Give safely

Many of us will have seen the devastation the earthquake in Turkey and Syria have caused, and will want to help.

However, fraudsters will take this opportunity to pose as charities and ask people to donate money.

Instead of responding to texts, emails or calls out of the blue asking for donations, be proactive and contact the charity of choice on a phone number or website address you know to be genuine.

COMING NEXT TIME

- **Current fraud alerts**
- **How we can be vulnerable to fraud**

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

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