Cheshire East Age UK

ISSUE 28 - JULY 2022

SCAMS AWARENESS UPDATE

Older Persons Scams Awareness & Aftercare Project

In this update:

Don't push it!

Avoiding authorised push payment fraud

Last month, we said the July edition would focus on holiday fraud. But, in the last few weeks, UK Finance has published information about the devastating impact of Authorised Push Payment fraud last year. So, that's our focus, to avoid becoming a victim statistic for 2022.

Authorised Push Payment (APP) fraud happens when a criminal tricks ("pushes") someone into sending money directly from their account to an account the criminal controls. The fraudster contacts their victims by phone, text message, email, on websites or through social media.

In 2021, individuals lost over half a billion pounds to this type of fraud. Businesses lost £77.4 million. It is a fraud that is on the increase - the number of cases rose by 27% and the amount lost rose by 39% in one year.

There are many types of Authorised Push Payment fraud. So, read on to learn how to avoid authorising any fraudulent payment.

As always, if you would like individual advice about how to protect yourself from scams, we can offer you a scams advice visit. Contact our Scams Awareness & Aftercare Team on 01625 612958 or enquiries@ageukce.org to book your place.

AUTHORISED PUSH PAYMENT FRAUD

Criminals use lots of ways to make us believe that what we're being asked to do is genuine. They prey on our natural instincts of wanting to help, not questioning authority, wanting to believe the best of everyone and not wanting to make a fuss.

There are certain situations when banks refund some of the money lost to authorised push payment fraud. But, it is not automatic - with only half of the money stolen returned to vicitms.

Remember - it's your money, so it's your right and responsibility to make sure it's used correctly.

Here are examples of authorised push payment frauds, and how to avoid them:

Purchase fraud: This is when the victim pays in advance for goods or services that are never received. These often happen online - on a website or through social media.

Last year, £64.1 million was lost to this type of fraud, with only 34% being refunded to victims.

Protect yourself - be suspicious of offers that are too good to be true. Do your research and only use secure payment methods, rather than bank transfer. Check out our November 2020 bulletin for more top tips.

Investment fraud: With this fraud, a criminal convinces the victim to move money to a fictitious account to pay for an investment that doesn't exist. This could be gold, wine, fine art, property or cryptocurrencies. We featured investment scams in our March 2022 bulletin.

In 2021, individuals lost £166.2 million, with only 44% being reimbursed.

Protect yourself - be cautious of investment opportunities and check the Financial Conduct Authority register to see if a company is genuine and licensed to offer investment advice.

Romance fraud: Here, the victim is persuaded to make a payment to a person they have met, often online, who they think they are in a friendship or relationship with.

Last year, this took £30.9 million from people. Only 41% was returned to victims, who lost their hearts as well as their money.

Protect yourself - avoid accepting friends requests or sending money to anyone you've not met in person. Research the person you're talking to. For more advice, re-read our May 2021 bulletin.

Advance fee fraud: This is when fraudsters convince victims to pay a fee to secure a much larger payment or higher value goods. Examples include overseas lotteries, prize draws and competitions, gold or jewellery waiting at customs, or inheritance due to you.

In 2021, people lost £30.8 million to advance fee fraud. Just 35% was reimbursed to the victims.

Protect yourself - remember, if an offer is too good to be true, it usually is. Research any companies that approach you. Check spelling and grammar in emails and don't believe the stories people may tell you.

Invoice and mandate fraud: Here, the victim thinks they have paid an invoice or bill to a legitimate person or company. But, the fraudster has intervened, telling the victim that the company's bank details have changed. Often, the criminals pretend to be solicitors and tradespeople.

Last year, people lost almost £20 million. Although 63% was returned to victims, this fraud can lead to people losing the dream home they're buying.

Protect yourself - always confirm bank details directly with the company by phone or in person before making a payment. Transfer a small amount first, and then check the company has received it before making full payment.

Impersonation fraud : The criminal poses as the bank, telling the victim that fraudsters are taking money from their account. They persuade the victim to transfer money to a "safe account" to protect their money. But that account is controlled by the fraudster. Or, they may say they are from the police and ask the victim to transfer money to help them with an undercover operation. A third way is for the fraudster to pose as an organisation and persuade the victim to transfer money to settle a (fictitious) fine or pay overdue tax.

These types of frauds accounted for £200 million lost by individuals. 58% was returned to victims.

Protect yourself - banks and the police will never ask you to transfer money. Organisations such as HMRC don't notify you of tax penalties or refunds by phone, text or email. If you are contacted out of the blue, don't respond - contact the organisation directly on a trusted number to check if they contacted you.

If you have been a victim of any of these frauds, **contact your bank immediately** and **report it** to Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk

CURRENT FRAUD ALERTS

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

Fake Paypal emails

Paypal is a secure way to pay for goods and services online. But, the National Trading Standards Scams Team is warning us about fraudulent emails pretending to be from Paypal.

The emails say your account is “suspended”, or “about to be suspended”, “you’ve been paid” or “you’ve been paid too much”. They then have a link to click on to sort out the issue.

Look out for these emails and never click on the links. Always access your Paypal account independently to check what’s happening.

Fraudulent Congleton Council phone call

Residents in Congleton have received a scam call, saying they are from Congleton Borough Council. They are asking to carry out an insulation survey. Congleton Town Council has advised that this is a scam. Congleton Borough Council has not existed since 2009.

This is an example of taking time to listen exactly to what is said when you’re called out of the blue. If you receive a call saying they’re from your council, you can always check by calling the council on an independent number to see if they tried to contact you.

BP fuel giveaway scam

Fraudsters are promising a £200 fuel gift card in return for answering a few questions and paying £1.78. They contact people through social media and emails. They make the offer sound plausible by playing on the Ukraine crisis and linking it to pulling out of Russia.

They ask for personal and bank details for you to pay the nominal amount.

Remember - this really is an offer that’s too good to be true.

Courier fraud

Last month, we had a focus on courier fraud. Cheshire police have asked us again to remind people that they, or any other police force, will never ask you to withdraw money to post to them or for a courier to collect.

If you receive a phone call asking you to do this - hang up, wait for the line to clear and then report the matter to Action Fraud on 0300 123 2040.

COMING NEXT TIME

- **Current fraud alerts**
- **Useful tools to fight fraud**

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

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

in partnership with