ISSUE 27 - JUNE 2022



SCAMS AWARENESS UPDATE

Older Persons Scams Awareness & Aftercare Project

In this update:

Courier fraud Page 2

Top tips to avoid becoming a victim Page 3

Current frauds Page 4

Stop, think, report and talk

This month, we've worked with our partners, Cheshire East Trading Standards, and with Cheshire Police to bring you information about the Citizens Advice Scams Awareness Fortnight and courier fraud.

In their annual campaign, Citizens Advice are highlighting how the cost of living squeeze means we're all more at risk of becoming a victim of scams, as we try to make ends meet. We wholeheartedly support their messages which are:

- Stop and get advice. You can call their Scams Action Team on 0808 250 5050.
- Report scams to Action Fraud on 0300 123 2040 or @actionfrauduk on Twitter.
- Talk with friends, family and neighbours about scams you've experienced.

If you would like face-to-face 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 <u>enquiries@ageukce.org</u> to book your place.

But now, read on to find out the who, what, where and how of courier fraud and how to avoid becoming a victim...





COURIER FRAUD...

What is it?

Courier fraud is when people are tricked into handing over money or valuables to criminals posing as couriers.

Recent police data shows 3,625 people were victims of courier fraud last year, with losses totalling more than £15.2 million.

How does it happen? **Typically**, the fraudsters contact their victims, often by phone, claiming to be a police officer or a member of staff from a victim's bank. They often pressure people into making quick decisions to assist with a fictitious investigation.

Who could be a victim?

ANYONE! Criminals use our in-built respect for authority and sophisticated language to manipulate, persuade and exploit people to go along with the scam. However, victims of reported courier fraud tend to be between 70 and 89 years old.

Here are 4 common types of courier fraud to be aware of:

Bank card expiry: Fraudsters claim to be from your bank and say your card is no longer valid, so they need to collect it. They ask for the PIN and then send a "courier" to collect the card before using it to commit fraud.

Buying expensive items: Criminals pretend to be police officers. They ask for help with an undercover operation, asking you to buy items like watches, jewellery and gold (for which you'll get your money back). Once the item is bought, it's handed over to the fraudster, never to be seen again.

Counterfeit cash/bank investigation: Someone claiming to be from the police or bank persuades a victim to help with a banking corruption investigation. The victim is told to withdraw a large amount of money. They are told to lie to the bank about why they need the money. The cash is picked up later by a courier to "check for fingerprints or to identify counterfeit bank notes".

Computer takeover: Here, a fraudster telephones you, impersonating your internet service provider. They say that there's been an issue with your internet connection, so you're due compensation. The victim is persuaded to download a remote access software, giving the criminals access to their computers. The fraudster then tells the victim they have been paid too much compensation and tells them to withdraw cash to pay the money back, which is collected by a courier.



In Cheshire last year, almost £173,000 was lost to courier fraud, with victims losing almost £2,000 more than the national average. Our Scams Awareness and Aftercare Project has supported victims of courier fraud in Cheshire East to get back on their feet, as they lose their confidence as well as their money.

So, here's our top tips to avoid becoming a victim of this type of fraud:



Courier fraud usually starts with an unexpected 'phone call. **REMEMBER:** *It's okay to hang up if you don't recognise who's calling.*

The criminals typically pose as a bank official, police officer or a computer or utility engineer.

REMEMBER: Check with the genuine organisation whether they called you by phoning them on a number you already have for them.



Courier fraudsters may suggest you hang up the phone to ring the organisation to confirm their identity. But they can hold the line open and pretend to be from the genuine company, to provide false confirmation.

REMEMBER: Call the genuine organisation from a different phone, call a friend to check the line is clear, or wait a few minutes.



The criminals usually ask you to buy expensive items, withdraw cash or provide a bank card for collection from a courier.

REMEMBER: *The Police and banks will NEVER ask you to do this.*



Fraudsters will instruct victims not to tell any family or friends about what they are doing. They will ask you to lie to the bank or shop.

REMEMBER: This is financial abuse. As with any abuse, NEVER keep it a secret. Tell your bank or contact the police immediately.



The criminals will make arrangements for a courier to meet the victim and collect the item they have purchased.

REMEMBER: Banks and the Police will not ask you to do this.

If you have been approached by a courier fraudster, or if you have been a victim of courier fraud, **report it** to Action Fraud on 0300 123 2040 or at <u>www.actionfraud.police.uk</u>

If you have revealed your bank details or handed your card to a courier, **call your bank** straight away to cancel your card.

CURRENT FRAUD ALERTS



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



Fake Ofgem rebate emails

Action Fraud received over 750 reports in just 4 days of a fraudulent email

pretending to be from Ofgem. It pressures people to apply for recently announced energy rebates. People are worried about the rise in the cost of living, and confused about how any rebates will be paid. So, they may be more vulnerable to this scam.

Ofgem is the national regulator, not an energy provider, so would not be contacting customers about rebates.



New name, same scam!

Evri is the new name for Hermes parcel delivery firm. The fraudsters have

been quick to jump on this, sending out text messages asking you to pay a shipping fee to have a parcel delivered. Even though the claimed shipping fee is only a modest £1.45, it's likely that the scammers are really looking to steal and misuse your bank details.

You can report suspicious texts by forwarding them to 7726 on your mobile.

BANK ACCOUNT

Santander impersonation fraud

People have reported getting texts from

Santander bank warning of suspicious activity on their account. This can panic people. If you click on the link, it takes you to a fake log-in page. This is to harvest your online banking details. The sting in the tail is that, once you've completed the fake log-in page, it takes you to the genuine Santander website, so you don't suspect anything.

Rule of thumb - never click on links in texts.

COMING NEXT TIME



Roof insulation offers

One of our volunteers received a call from someone puporting to be from the council. They were offering roof

insulation under a "Greener and Warmer" scheme. Again, with energy bills rising, people my be tempted to response to such cold calls. But remember, it may be a scam if it's not expected and the offer is too good to be true.

You can check current local authority warmer home schemes by contacting Cheshire East Council on 03300 123 5017 (option 4) or at warm@cheshireeast.gov.uk.

Current fraud alerts

• Holiday 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

