

SCAMS AWARENESS UPDATE

Older Persons Scams Awareness & Aftercare Project

In this update:

Hybrid scams
Page 2

How to protect yourself
from hybrid scams
Page 3

Current frauds
Page 4



Double Trouble!

How fraudsters blend scams to trick the unwary

Now we've got your attention with the double trouble dogs, lets talk about something not so cute - the double trouble of hybrid scams. To many of us, 'hybrid' refers to cars and how we can transition from the combustion engine to electric, but in the criminal world of fraudsters, a hybrid scam is when more than one type of scam is used to steal our money.

Recent information from the Financial Ombudsman Service shows that hybrid scams are now common in romance fraud, purchase scams and 'safe account' fraud. We have featured these individual scams before. But, read on to keep safe from the double whammy of the sophisticated hybrid scam.

JOIN US for an afternoon of activities to keep you money and information safe. **"We Need to Talk About Scams"** is a session in October all about how to keep safe on the doorstep, on the phone and online.

There are sessions online, and face to face in Congleton and Crewe. There are sessions for residents and for people working with older people. They are free of charge and include light refreshments and an information pack.

Go to [Eventbrite](#) or contact us on 01625 612958 or at enquiries@ageukce.org to book your place for keeping safe.

Hybrid scams...

Being a target or victim of one type of fraud can be devastating. So imagine the impact of not only losing your heart, not receiving goods you've paid for or responding to a text message, and then also becoming a victim to a further fraud.

Here are some of the emerging hybrid frauds to look out for:



The romance and investment blend:

Scam #1 - You strike up a friendship or romance in person, on a dating site or on social media. You believe you are in a real relationship. But the other person is a fraudster.

Scam #2 - Over time, they persuade you that they're an expert in investments, often cryptocurrency. Through befriending you, the fraudster knows what to say to convince you to invest.

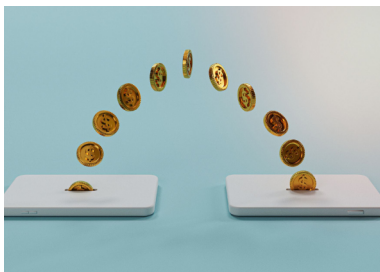
When the investment turns out to be non-existent you have lost your heart, money, confidence and trust.

The non-existent goods and bank combination:

Scam #1 - You attempt to make a bank transfer for goods or services. Unknown to you, it's a fraudster offering the goods and they don't exist. The fraudster contacts you to say that the payment has failed.

Scam #2 - You receive a text message or phone call from the fraudster impersonating your bank. They tell you to keep attempting to make the payment multiple times, as it seems to still be failing. In fact, all the payments are going through.

So, you end up without the goods you wanted (because they never existed) and without the multiple payments you made for them.



The message and 'safe account' hybrid:

Scam #1 - You receive a text message or email asking for a small amount of money e.g. to have a parcel redelivered. You click on a link and complete your bank details, for the payment to be taken. Unknown to you, this is a fake website, run by fraudsters.









Scam #2 - Later, you receive a call saying they are your bank and there is suspicious activity on your account. But it is the fraudsters, not your bank. They know everything about your account from the information you gave them on the fake website. To keep your money safe, they ask you to transfer your cash to an account they have set up for you. They may call it a 'safe account'. These may be cryptocurrency accounts.

Not only have you not received any parcel, but you have also lost your money.

...and how to protect yourself

With the evolution of hybrid scams, it's important that we keep our fraud prevention tips in the front of our minds, so that combating fraud becomes part of our routine.

Here's what we can do to keep our money and information safe:

-  **Never** take investment advice from anyone other than a Financial Conduct Authority (FCA) registered person or company. Always check they are registered for what they are giving advice on. You can check the register [online](#) or by calling 0800 111 6768.
-  **Offers** that sound too good to be true, usually are. Do your research and buy from reputable places.
-  **Don't** pay by bank transfer. Use a secure payment method such as Apple or Google Pay or Paypal. Wherever possible, pay by credit card for more protection.
-  **Be proactive** - if you are told a payment has not been successful, contact your bank independently to check transactions.
-  **Call 159** - Don't rely on a phone call saying they're your bank. If you get such a call, asking for personal or financial information, or asking you to transfer money, hang up and call 159 to check if your bank really is trying to contact you.
-  **Never** be persuaded to move money to another account. Banks will never ask you to transfer or withdraw money to combat fraud.
-  **Don't** click on links in messages and emails. Check whether the email is genuine and always log into accounts independently, instead of clicking on a link.
-  **Take** your time - don't be rushed into acting quickly. Tell the person you'll contact the organisation independently to sort out any perceived issue.

What to do if you have been a victim of a hybrid scam

If you have been a victim of a scam, single or hybrid, we understand that you may feel embarrassed, upset or frightened, but fraud can happen to anyone. It is important to get help as soon as possible.

Contact your bank immediately, on a independent number, to tell them what's happened. They can work with you to keep your money safe in your accounts.

Report what has happened to Action Fraud [online](#) or on 0300123 2040. The information you give may help to identify the fraudsters.

If you live in Cheshire East, contact our Age UK Cheshire East Scams Aftercare Team on 01625 612958 for practical and emotional support.

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

WhatsApp voice scam

There is a recent WhatsApp scam hitting community and religious groups.



Instead of a text message, the fraudster voice calls the victim and says they are sending a one-time passcode to allow them to join an upcoming group video call. The scammer then asks the victim to share this passcode with them so they can be "registered" for the video call. But, with that code, the fraudster takes over the victim's WhatsApp account and pretends to be them to ask the other group members to transfer money.

Never share your one-time password with anyone.

Rogue trader fraud increases in the bad weather

Cheshire East Trading

Standards has seen an increase in rogue traders offering roof repairs and gardening services, after the recent run of wet weather. The work they carry out is often unnecessary, of poor quality or over priced.

As mentioned in previous bulletins, Trading Standards advise not to engage with any trader who knocks on the door uninvited. Take your time to get quotes from reputable companies or recommendations from trusted friends. Contact [Citizens Advice Consumer Service](#) on 0808 223 1133 if you have any concerns about traders.



Beware of fake perfume sales

A neighbouring Trading Standards team is reminding people of the risks of buying and using counterfeit perfumes. These are often for sale on pop-up stalls and purport to be popular brands.



Worryingly, the team reported that the sellers approached people and escorted them to local cash points to withdraw money to purchase the items.

Remember, if an offer is too good to be true, it usually is, and legitimate sellers will never pressure you to part with your money.

Fraudsters cashing in on world events

Recently, we have seen the devastation caused by the wildfires in Rhodes and now the fire hurricane in Hawaii.

Fraudsters will take advantage of these disasters by contacting people by phone, email, letter and adverts online either to ask for donations to support the recovery or (in the case of Rhodes), offering to make a claim for compensation on your behalf.

Whether donating or claiming, only every deal with organisations you have checked are legitimate.



COMING NEXT TIME

- Current fraud alerts
- Money muling

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