

SCAMS AWARENESS UPDATE

Older Persons Scams Awareness & Aftercare Project

In this update:

Impersonation scams
and how to avoid them
Pages 2 & 3

Current scams
Page 4

Just say “No”!

...but 92% of us don't find it that easy.

In [recent research](#) carried out for the Take Five to Stop Fraud organisation, 92 per cent of people admitted to saying 'yes' to requests for personal or financial information because they don't want to appear rude. Instead, we use all sorts of phrases to avoid saying 'no', such as 'I'm not sure', 'I don't think so', 'Let me think about it', and 'I can't at the moment'.

Unfortunately, this can leave us at risk of becoming a victim of impersonation scams. Information from UK Finance show the number of impersonation scam cases more than doubled in the first half of 2021 to 33,115. This resulted in criminals stealing £129.4 million through this type of fraud alone in just six months.

Read on to find out about impersonation scams and how to avoid them, to keep yourself and loved ones safe.

Remember, in addition to this bulletin, our Scams Awareness and Aftercare Project offers scams awareness talks to older people's groups and support for individuals who have been scammed. If you would benefit from these, please get in touch to find out more. You can head to [our website](#) or contact our project manager, Sally Wilson, on 01625 612958 / 07932 999902 or at sally.wilson@ageukce.org.

An **impersonation scam** is when a criminal pretends to be from a trusted organisation such as a bank, the police, a government department, service provider or company. They may even pretend to be a family member, friend or partner. The criminal then tricks the victim into transferring money using a range of cover stories.

Anyone could be caught out by an impersonation scam, as the criminals use technology and sophisticated tactics to reel in their victims. The most dangerous thing we can do is think it won't happen to us.

They use all ways to contact potential victims. Here are a few examples to look out for and how to avoid becoming a victim.

Scammers may:

Make their number look like the genuine company's number (spoofing).

Impersonate your bank, the police or a genuine company.

Tell you to act immediately to safeguard your money or details.

Pretend they know some information about you, then ask for more.

Give you a number for you to call to verify their identity.

Impersonate a relative or friend, texting or emailing with a new number or email address.

Ask for money for an emergency or to buy something quickly.

Impersonate an organisation or company saying there's a problem with your account.

Send links to click on to sort out a problem or receive money or a prize.



You can:

Avoid sharing personal or banking information when someone has called you.

Say "No thank you" and hang up.

Call 159 - the new service to be connected to your bank to check if the call is genuine.

Contact the genuine company to check if they tried to get in touch.

Never agree to transfer or send money to a "safe" account or take part in an undercover operation.

Stay calm.

Contact relatives and friends on the number or email address you already have for them.

Avoid clicking on links in texts and emails.

Hover over the sender's email address to see if it's from a genuine company.

Check your account independently to look for any issues.

OUT OF THE BLUE

SPEAKS WITH AUTHORITY

KEEP SECRET

TOLD TO ACT NOW!

IT'S A SCAM!!

CURRENT EVENTS

Fraudsters may:

Impersonate a police officer coming to collect money, items or bank cards as part of an undercover operation.

Pretend they are selling door-to-door as part of an offenders rehabilitation scheme.

Impersonate someone from a utility company come to read the meter or carry out some work.

Ask you to complete a questionnaire (but this is a way to get your personal information).

Impersonate independent financial advisers, offering a great return on investments or to invest your pension lump sum.

Pay to have their listing at the top of search results online.

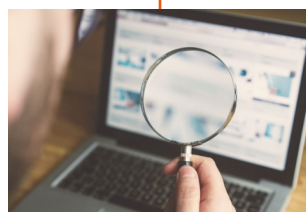
Claim to have a celebrity that has benefited from their product.

Pretend to have items for sale from pets to games consoles, using images from genuine sellers.

Use webpages that look very similar to genuine providers but have slightly different website addresses.

Steal someone's identity to impersonate someone to strike up a friendship with you before asking for money.

Search the information in your profile online to see if you're vulnerable to befriending or romance fraud.



So it's best to:

Avoid trading on the doorstep.

Say "No thank you" and close the door.

Ask the caller to wait while you call the genuine company on an independent number to check their identity. Genuine callers really don't mind if you do.

Set up passwords with utility companies by asking to go on their priority services register.

Never give out personal or financial information on the doorstep.

Think "If it's too good to be true, it probably is!"

Call the FCA on 0300 500 8082 to check ALL financial companies are genuine.

Don't believe celebrity endorsements are genuine.

Be wary of sellers asking for deposits by bank transfer for items you've not seen.

Check website addresses very carefully.

Never send money to someone you've been chatting to but you haven't met in person.

Keep your information online private by controlling your settings on social media.

Don't share too much about yourself on social media and in chat rooms, as this can make you a target for scammers.

REPORT IT!: If you have been a victim of an impersonation scam, report it to Action Fraud at www.actionfraud.police.uk or on 0300 1232040 and contact your bank immediately.

Here are a few of the current scams our volunteers, partners and readers have alerted us to:



Fake family and friends texts

It starts with a message that they've changed their number. You reply and the conversation continues. But it's a criminal pretending to be a friend who then

asks for money quickly for an emergency or for a purchase such as a car.

Luckily, the brave people who have reported this realised it was an impersonation scam before parting with any money.

You can report these scams by forwarding the original message to 7726.



Personal information used on social media for romance fraud

Criminals look for personal

information on Facebook profiles to target people looking for love. To keep your information private, follow the instructions about [controlling who can see what you share](#) page. It's best to change the settings so only you or your friends can see your information. Be careful of friends requests too. Be very cautious accepting any request from someone you don't know in person.



Survey scams

We've had reports of emails inviting people to click links to complete a survey to win a fuel gift card.

Which? recently [reported on similar scams](#) pretending to be from supermarkets.

Take care with emails out of the blue offering something for (almost) nothing. Check the sender's email address to check if it's genuine. Remember - if an offer is too good to be true, it probably is.

You can forward suspicious emails to report@phishing.gov.uk. To date, this has helped to remove over 64,000 scams.



Bank impersonation fraud alert

There have been reports of people receiving calls from scammers

impersonating banks demanding money is transferred to a "safe" account or withdrawn and posted, in order to keep your money safe. The criminals are very persuasive and anyone can be taken in by this in a vulnerable moment.

Remember, your bank or the police will never ask you to withdraw or move money. If you have been a victim of such a scam, don't be embarrassed. Share the information with your bank and the police so it can be investigated.

COMING NEXT TIME

• Current scams

• Scams and financial abuse

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