mmu



# SCAMS AWARENESS UPDATE

#### Older Persons Scams Awareness & Aftercare Project

#### In this update:

Phone fraud tactics Page 2

Top tips for avoiding current phone frauds Page 3

FREE EVENT - We need to talk about scams Page 4

# London Calling! Or is it?

#### Unmasking the perils of phone scams

Everyone has a phone - either a landline or a mobile phone. So, we can all be vulnerable to becoming a victim of fraud over the phone.

Anyone of any age can be targeted by a fraudulent call but, in a recent Ofcom survey, 61% of over 75s had received a scam call.

Fraudulent phone calls may be computer generated, have an automated message or be a real person. The person calling may appear helpful or may sound threatening. For many, the phone is a lifeline, and we don't want people to be scared of picking up the phone.

So, this month, we aim to arm you with knowledge, strategies, and practical tips to help you to be confident to take control of conversations on the phone.

After reading this bulletin, remember to share what you've learnt with family and friends, to keep them safe too.

If you receive a lot of nuisance calls, our Scams Awareness & Aftercare Team may be able to apply for a free call blocker for you. For more information, contact us on 01625 612958 or at <u>enquiries@ageukce.org</u> to arrange an appointment.









#### **Phone Fraud Tactics to Look Out For**

Phone scams are usually a type of impersonation fraud. Criminals impersonate family, friends or trusted organisations with the sole intention of obtaining our personal or financial details, or simply our cash.

Here are some of the methods they use, along with examples of current phone scams to look out for:



**IMPERSONATION**: Criminals impersonate a trusted individual or organisation. By adopting a false identity, they gain the victim's trust and exploit it for their fraudulent purposes.

*Current examples:* calls telling you that you owe tax, or calls saying there's an issue with your broadband, so they need to install software on your computer.

**SPOOFING:** This is when fraudsters use technology to make the number they're calling from look like a local number or that of a trusted organisation. This is because we're more likely to trust a number that is familiar to us.

*Current examples:* calls pretending to be your bank, asking you to move money to avoid fraudulent activity on your account. Calls pretending to be the local council offering warm home discounts.





**URGENCY AND FEAR:** Fraudsters often create a sense of urgency or fear to pressure their targets into immediate action. This tactic aims to provoke a panicked response, preventing victims from taking a few moments to think or an opportunity to seek advice.

*Current examples:* calls offering special deals on energy or mobile phone contracts, only available for a certain time. Or,

threatening to arrest you unless you comply with a request.

**VISHING**: Similar to email phishing, fraudsters engage in "vishing" (voice phishing) by tricking victims into revealing personal information over the phone, under the guise of a legitimate organisation.

*Current examples:* Calls about the married tax allowance, asking for your National Insurance number to complete the application. Also, asking for bank card details to give you a refund because your broadband is running slowly.





**PRETEXTING:** This technique involves creating a convincing backstory or pretext to establish credibility and manipulate victims into providing sensitive information or money.

*Current examples:* calls pretending to be from a police officer, asking for help in an undercover operation (courier fraud). Also, calls from fraudsters pretending to be in a relationship with you asking you for

money to help in a medical emergency or to help out their business venture.

**EXPLOITING OUR FINANCIAL VULNERABILITY**: This is where criminals offer something that will increase our income or save us money. Remember, if an offer is too good to be true, it usually is!

*Current examples:* cold calls offering free pension reviews or investment opportunities. Calls offering free gifts, gift cards or cash in return for answering a survey.



### How to Avoid Becoming a Victim of Phone Fraud

There's lots we can do to reduce the number of nuisance calls and avoid becoming a victim of a phone scam:

- Sign up for the Telephone Preference Service on 0345 070 0707 or at <u>www.tpsonline.org.uk</u> to reduce marketing calls.
- Consider call blocking services let calls go to answer phone, ask your phone provider what they offer or consider call blocking units. Age UK Cheshire East may be able to apply for a free call blocker for you.

If you receive a suspicious call:

- 🦰 Hang up.
- Wait a few minutes for the line to clear.
- Call the genuine organisation independently to see if they have called you.
- Call 159 to contact your bank if you have sent money to the fraudsters, or if you have given any of your personal or banking details away.

### How to report Phone Fraud

You can report fraudulent phone calls to Action Fraud at <u>www.actionfraud.police.uk</u> or on 0300 123 2040.

If you have a mobile phone, text the word Call to 7726. Then text the phone number the fraudulent call came from.

## A Date for your Diary



We are pleased to announce special Scams Awareness Events in October. Please join us to talk about scams and how we can take back the power from the fraudsters to keep ourselves safe. Please invite colleagues, family and friends too.



#### **COMING NEXT TIME**

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



Older Persons Scams Awareness & Aftercare Project | page 4