April 2020

Coronavirus information

Scams awareness

Are there any Coronavirus related scams that I need to be aware of?

The Covid-19 pandemic has seen truly heart-warming acts of kindness with hundreds of thousands volunteering to support the oldest and most vulnerable in their communities. Unfortunately, criminals are also using the crisis as an opportunity to devise new scams to target the public. Anyone can fall victim to a scam, so it is important that everyone remains vigilant.

The majority of Coronavirus linked fraud reports relate to online shopping for items such as face masks and hand sanitiser which never arrive. Criminals are also sending phishing emails and text messages claiming to be from the Government, HMRC and health bodies to convince you to open links or attachments and reveal personal or financial information. Fraudsters are also contacting people pretending to be from Age UK and other charities and trying to convince them to 'donate'. There have been also reports of fake Coronavirus testers coming to people's doors as well as 'rogue shoppers' that take money or bank cards to deliver essential items but never return.

How can I stay safe from scams?

Age UK has lots of information and advice on how to stay safe from different scams, whether they be on the phone, in an email or at the doorstep. The Police and Action Fraud have asked everyone to follow this key advice:

Stop: Taking a moment to stop and think before parting with your money or information could keep you safe.

Challenge: Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

Protect: Contact your bank immediately if you think you've fallen for a scam and report it Action Fraud or by calling 0300 123 2040.

Your bank or the police will NEVER ask you to transfer money or move it to a safe account.

Someone I don't know well has offered to deliver shopping to me.

If you don't the person well, ask for a way to verify who they are such as their name, address and a contact number. If they offer to deliver shopping, do not give out your bank cards or bank details. Offer to pay them back with a cheque or by telephone or online bank transfer. If there is no alternative but to pay in cash then ask for a receipt and wait until the person has delivered your shopping before handing over any money. Wash your hands for twenty seconds after handling any coins and banknotes you get back as change.

I am worried about a friend, family member or neighbour falling victim to a scam.

Criminals will often target those they perceive as

Coronavirus information

Scams awareness

more vulnerable like those that live alone, have a disability or health condition or are not comfortable at using technology. Increased loneliness and isolation can put people at risk of romance fraud approaches on social media, dating apps and by email. Those seeking companionship online may be tricked into believing that the person they are speaking to is genuine and they are convinced to transfer money. Older people unfamiliar with different forms of digital technology may be more at risk from computer service fraud, when fraudsters try and convince you to provide access to your computer so they can 'fix it' or divulge your logon details and passwords.

What are some top tips for staying safe online?

Online Shopping

Seek advice: If you're purchasing goods and services from a company or person you don't know and trust, carry out some research first, and ask friends or family for advice before completing a purchase.

Scam messages: Be wary of unsolicited emails and texts offering questionably good deals, and never respond to messages that ask for your personal or financial details.

Payment method: Avoid paying for good and services by bank transfer as that offers you little protection if you become a victim of fraud. Instead, use a credit card or payment services such as PayPal.

If you have made a payment: Inform your bank as soon as possible, they can help you prevent any further losses. Monitor your bank statements regularly for any unusual activity.

Computer Software Service Fraud

Installing software: Never install any software, or grant remote access to your computer, as a result of a cold call.

Financial details: Genuine organisations would never contact you out of the blue to ask for financial details such as your PIN or full banking password.

Tech support: If you need tech support, ask your friends or family for recommendations and look for reviews online first. Don't contact companies promoting tech support services via browser pop-ups.

If you have made a payment: Inform your bank as soon as possible, they can help you prevent any further losses. Monitor your bank statements regularly for any unusual activity.

If you granted remote access to your computer: Seek technical support to remove any unwanted software from your computer. Ask your friends or family for recommendations and look for reviews online first. Don't contact companies promoting tech support services via browser pop-ups.

If you know or suspect someone has fallen victim to a scam then get them to contact their bank immediately and report it to Action Fraud online or by calling 0300 123 2040.

If you are concerned that an older person has been targeted and they are unable to keep themselves safe due to age, injury or illness then contact your local authority, local police force, local Age UK or Age UK's Safeguarding Team.