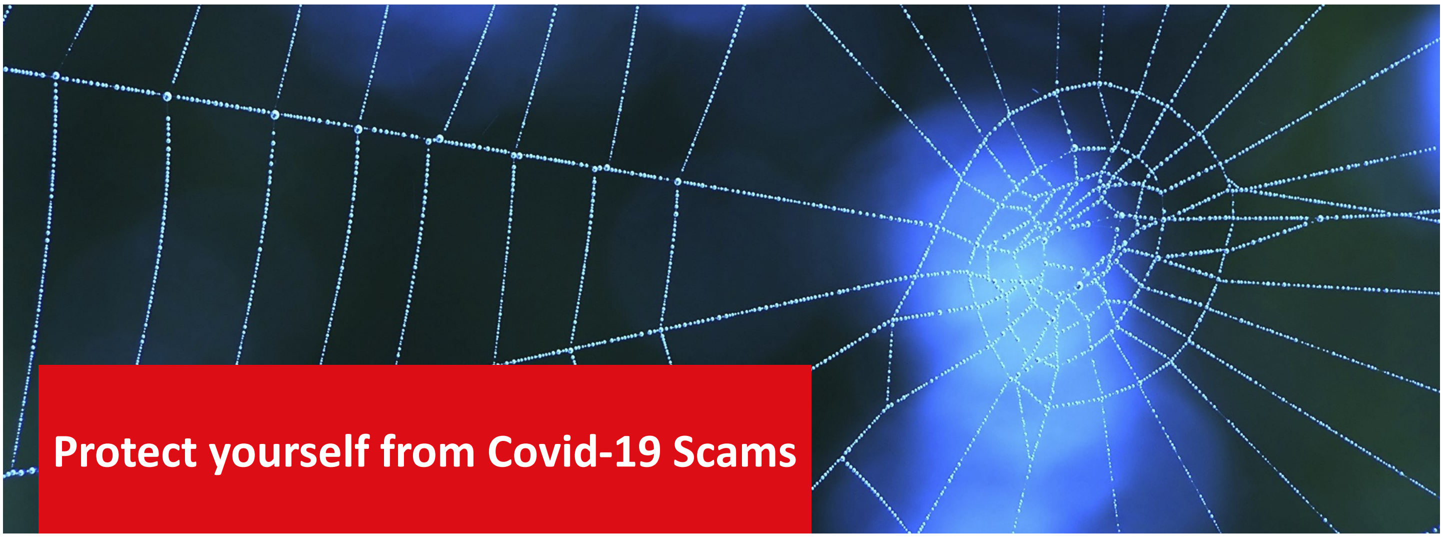

Protect yourself from Covid-19 Scams

During the pandemic there will be fraudsters who try to take advantage of us to make a profit.

This newsletter outlines some of the scams that you need to be aware of. Unfortunately Covid-19 is creating an environment for fraudsters to thrive.

Phone and Doorstep Scams

There is likely to be an increase in scam calls, with scammers pretending to be from authorities such as your bank or HMRC.

Remember—never give out any personal information or log in details over the phone and never agree to transfer any money.

Scammers are taking advantage of the vulnerable and knocking on their doors, offering to do shopping and even saying they can take your temperature.

Remember—Never hand over any money to someone you don't know and never let a stranger in to your house.

Scams selling goods

Scammers are also using email to encourage you to buy items such as face masks and hand sanitisers.

Once ordered and paid for, the items never arrive.

Remember—if you are making a purchase from a company you don't know, carry out some research first, and always use a credit card as most major credit card providers insure online purchases.

NHS Lanyards

It has been reported that Amazon and eBay are removing NHS lanyards for sale, as sales of the lanyards have increased significantly since the coronavirus outbreak. It is likely that the lanyards could be used to access NHS discounts, and protected shopping hours for NHS staff.

Remember -Keep your own lanyards and ID cards secure when you are not wearing them, as there have been incidents of them being stolen to access the current benefits for NHS staff.

Counter Fraud Services

Phishing emails

Action Fraud are reporting an increase in corona virus themed phishing emails . These emails will try to trick you to into opening malicious attachments or revealing personal or financial information.

Fraudsters are emailing potential victims purporting to be from research organisations such as the World Health Organisation (WHO) asking you to click on a link for information relating to the coronavirus. The link leads to a malicious website or you are asked to make a payment in Bitcoin.

Smishing texts

The same applies to SMS messages. Known as Smishing texts, they look they are from a reputable company, but they will try to get you to do something such as call a premium rate number or sharing confidential information.

Remember—Don't reply to a text message from someone you don't know and don't click on links that you receive in a text message.

Any apps you install should come from an official app store.

How to spot and avoid Covid-19 scams:

- Be very wary of unsolicited emails and texts
- Watch out for grammar and spelling errors
- An urgent tone which is designed to make you click on the links quickly
- Legitimate services who you have accounts with will address you by your name, not 'Dear Customer' for example.
- Fake domains. Scammers have been setting up website addresses linked to coronavirus which will be used to try to trick the public.
- Don't be rushed into doing anything. If it sounds too good to be true it probably is.

What to do if you get scammed:

Contact Action Fraud at:

www.actionfraud.police.uk or 0300 123 2040

The Action Fraud website has various useful links:

How to shop online safely:

https://www.actionfraud.police.uk/shoponlinesafely

How to protect your devices from the latest threats: https://www.ncsc.gov.uk/guidance/securing-your-devices

If you have any questions please contact:
Hayley Cobb, NHS Counter Fraud Specialist
Tel: 07580 700845 or Hayley.cobb@nhs.net