Coronavirus Scams

There has been a 400% increase in coronavirus-related scams, with victim losses totalling almost £970,000.

Recently the National Fraud Intelligence Bureau (NFIB) reported a new trend in fraud related to Coronavirus, or COVID-19.

Updated figures show there have been 105 reports to Action Fraud since 1 February 2020, with total losses reaching nearly £970,000.

The first report relating to Coronavirus, or COVID-19, was received on 9 February. There were 20 more reports that month. Since then, there have been 46 reports between the 1 March and 13 March, and 38 reports in just four days (14 March – 18 March).

What scams are we seeing?

The majority of reports are related to online shopping scams where people have ordered protective face masks, hand sanitiser, and other products, which have never arrived.

Other frauds being reported include ticket fraud, romance fraud, charity fraud and lender loan fraud.

Phishing emails

We have also received over 200 reports of coronavirus-themed phishing emails. These attempt to trick people into opening malicious attachments which could lead to fraudsters stealing people's personal information, email logins and passwords, and banking details.

Some of the tactics being used in phishing emails include:

• Fraudsters purporting to be from a research group that mimic the Centre for Disease Control and Prevention (CDC) and World Health Organisation (WHO). They claim to provide the victim with a list of active infections in their area but to access this information the victim needs to either: click on a link which redirects them to a credential-stealing page; or make a donation of support in the form of a payment into a Bitcoin account.

• Fraudsters providing articles about the virus outbreak with a link to a fake company website where victims are encouraged to click to subscribe to a daily newsletter for further updates.

• Fraudsters sending investment scheme and trading advice encouraging people to take advantage of the coronavirus downturn.

• Fraudsters purporting to be from HMRC offering a tax refund and directing victims to a

fake website to harvest their personal and financial details. The emails often display the HMRC logo making it look reasonably genuine and convincing.

Superintendent Sanjay Andersen, Head of the National Fraud Intelligence Bureau, said:

"Fraudsters will use any opportunity they can to take money from innocent people. This includes exploiting tragedies and global emergencies.

"The majority of scams we are seeing relate to the online sale of protective items, and items that are in short supply across the country, due to the COVID-19 outbreak. We're advising people not to panic and to think about the purchase they are making. When you're online shopping it's important to do your research and look at reviews of the site you are buying from."

Graeme Biggar, Director General of the National Economic Crime Centre, said:

"We have already seen fraudsters using the COVID-19 pandemic to scam people looking to buy medical supplies online, sending emails offering fake medical support and targeting people who may be vulnerable or increasingly isolated at home.

"These frauds try to lure you in with offers that look too good to be true, such as high return investments and 'healthcare opportunities', or appeals for you to support those who are ill or bogus charities.

"The advice is simple, think very carefully before you hand over your money, and don't give out your personal details unless you are sure who you are dealing with.

"We are working together across law enforcement, government and the private sector to combat this criminal activity and protect the public. If you think you have been a victim please report to Action Fraud."

Protect yourself

1) Watch out for scam messages
Don't click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for your personal or financial details.

2) Shopping online:
If you're making a purchase from a company or person you don't know and trust, carry out some research first, and ask a friend or family member for advice before completing the purchase. If you decide to go ahead with the purchase, use a credit card if you have one, as most major credit card providers insure online purchases.

For more information on how to shop online safely, please visit: https://www.actionfraud.police.uk/shoponlinesafely

3) Protect your devices from the latest threats:

Always install the latest software and app updates to protect your devices from the latest threats.

For information on how to update your devices, please visit: https://www.ncsc.gov.uk/guidance/securing-your-devices

For the latest health information and advice about COVID-19 please visit the NHS website.

Please be aware, there are unverified reports of fraudsters going door to door claiming to be NHS staff conducting coronavirus tests or welfare visits.

NHS staff are **not** going door to door.

Call the police if someone knocks on your door claiming to be conducting coronavirus tests. Do NOT let them in to your house.

We have also had reports of flyers offering coronavirus tests being left on car windows. DO NOT take them up on the offer!