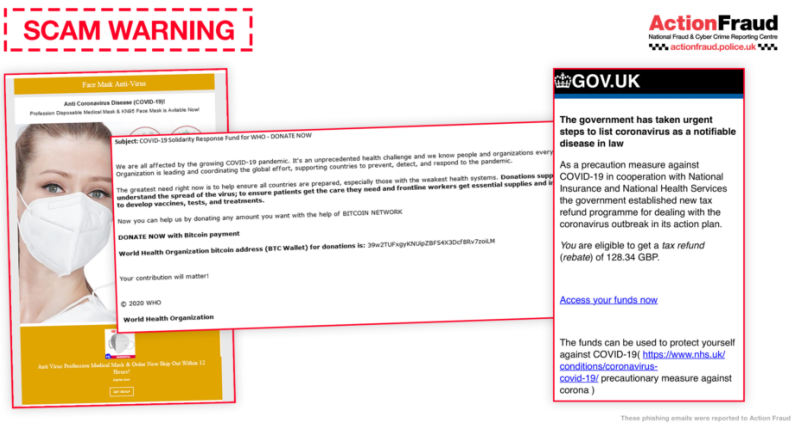
Beware fraud and scams during Covid-19 pandemic. Stay at home – stay safe on line

Posted at 08:13 on 25th March 2020 in **Forcewide News**

Following the Government's new "Stay at home – stay safe" ruling it is more important than ever to help safeguard the elderly and vulnerable and protect them from unscrupulous fraudsters and scammers.

Already there have been reports of heartless fraudsters targeting victims on the doorstep but increasingly and more worryingly, scammers are turning their attentions to targeting people on-line.



As more people stay safe at home or self-isolate from coronavirus, they are increasingly logging onto the internet to do their shopping – potentially putting themselves at risk from the unscrupulous scammers.

Since the virus took a hold in the UK more than 100 victims of coronavirus related fraud have been identified with losses of almost £1m recorded.

Arrests made …
"We have arrested two courier fraudsters in South Gloucestershire. The 17-year-old and 27-year-old had persuaded the 89-year-old victim to withdraw large sums of money from a bank in Yate. Concerned bank officials contacted us after becoming suspicious about the large withdrawals – £5000 - £7500 on each occasion – and alerted the police. The suspects have been arrested and released under investigation."

So far in the Avon and Somerset force area we are not aware of any victims and have not received any complaints or reports of people being duped by fraudsters. We are keen to keep this trend going and want to help safeguard our local communities.

We are concerned that as many people are now isolated from communities, their guard has become lowered and therefore they are potentially increasingly vulnerable to become targets – and ultimately victims – of the scammers.

The Boston Standard reported: A new heartless scam has been launched to try and exploit the coronavirus crisis. Boston Borough Council says an email claiming to be from the council has been circulating. It says that the recipient is eligible for a council tax refund due to COVID 19 - and to reply with your bank details. The council has stressed this is not from them and warn people to discard it.

Action Fraud have advised that fraudsters "will use any opportunity they can to take money from people. This includes exploiting tragedies and global emergencies and preying on the kind nature of people."

The majority of scams which have emerged relate to the online sale of protective items which may be in short supply across the country. This includes protective masks, hand sanitisers and other products associated with coronavirus.

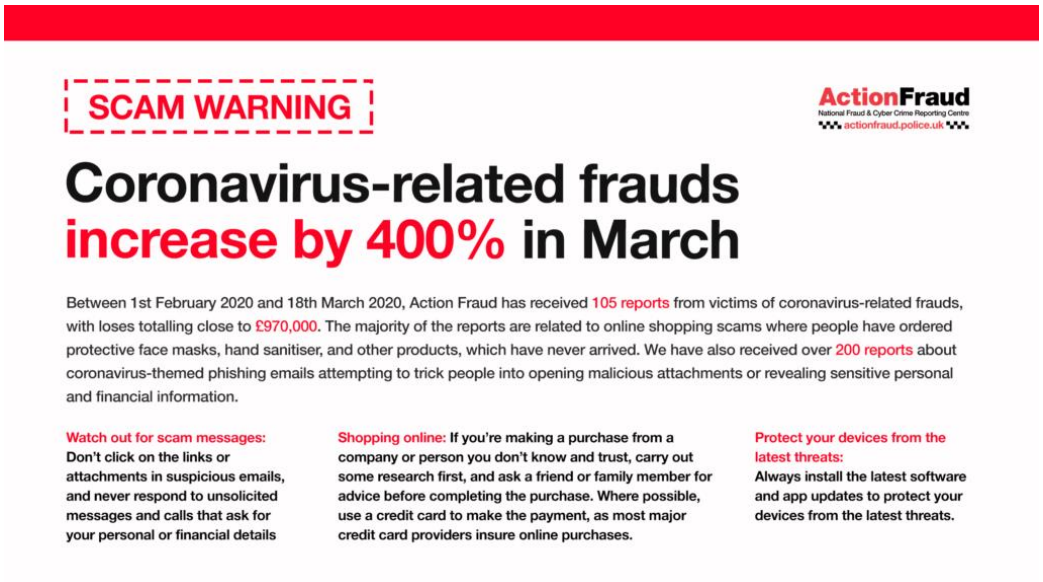
There have also been emails sent offering fake medical support, targeting people who may be vulnerable or increasingly isolated at home.

The Scottish Sun newspaper highlighted: Cyber-criminals have been impersonating the World Health Organisation in an attempt to take advantage of the coronavirus outbreak. Experts have picked up on scams that involve phishing emails with fake links to COVID-19 information. These links actually contain malware that could infect your computer. Researchers at IBM X-Force found 'HawkEye' malware being spread under the disguise of a WHO email alert from is director general Tedros Adhanom Ghebreyesus. This is a type of malware used to steal information from computers. Recipients of the email are encouraged to open an attachment for "drug advice". Once downloaded this malware can track everything you type once it's uploaded to your computer.

Manager of the Avon and Somerset Police Complex Crime Unit, Dr Kirstie Cogram said:

"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.

"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. There are also 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. Where possible – especially if buying goods – do some background research and look for reviews on the site where you intend buying from.

Guidance

- Watch out for scam messages – don’t click on the links or attachments in suspicious emails and never respond to unsolicited messages and telephone calls that ask for your personal or financial details. Apply caution if receiving cold calls, stay safe on-line and do not click on any links that you don’t know are from a tested source.

- 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 the matter to Action Fraud.

- 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.

- Don’t be duped by organisations offering to arrange to collect money from your home to pay for goods.

- Don’t buy goods from the doorstep

- Protect your devices from the latest threats – always install the latest software and app updates to protect your devices from the latest threats.

Law enforcement, government and private sectors partners are working together to encourage members of the public to be more vigilant against fraud, particularly about sharing their financial and personal information, as criminals seek to capitalise on the Covid-19 pandemic.

Criminals are using government branding to try to trick people, including reports of using HMRC branding to make spurious offers of financial support through unsolicited emails, phone calls and text messages.

This situation is likely to continue, with criminals looking to exploit further consequences of the pandemic, such as exploiting financial concerns to ask for upfront fees for bogus loans, offering high-return investment scams, or targeting pensions.

Huge increases in the number of people working remotely mean that significantly more people will be vulnerable to computer service fraud where criminals will try and convince you to provide access to your computer or divulge your logon details and passwords. It is also anticipated that there will be a surge in phishing scams or calls claiming to be from government departments offering grants, tax rebates, or compensation.

Graeme Biggar, Director General of the National Economic Crime Centre (NECC), said: "Criminals are exploiting the COVID-19 pandemic to scam people in a variety of ways and this is only likely to increase. We need individuals and businesses to be fully aware and prepared.

"There is a wealth of advice available from dedicated counter fraud professionals, but in general you should always think very carefully before you hand over your money or your personal details.

"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 fallen for a scam contact your bank immediately and please report to Action Fraud – **https://www.actionfraud.police.uk** or by calling 0300 123 2040."

Further guidance:

- Please only call 999 in an emergency. If you need to call our 101 service, please consider whether you can report online instead via our **online reporting tools**.
- Visit our dedicated **COVID-19 page** for links to all the latest news on policing services.
- Visit GOV.UK to read the **Government's advice on COVID-19**.
- See Government advice for **staying at home, for households with possible COVID-19 infection** and **social distancing to protect vulnerable groups**.
- Visit the NHS website for **hygiene advice and advice on calling 111**.
- For advice on mental health, visit the **Every Mind Matters website**.