City of London Police
National Fraud Intelligence Bureau

Coronavirus fraud core script – update 1

This script has been approved by the National Economic Crime Centre, Home Office and National Cyber Security Centre.

Key messages

1) Criminals will use every opportunity they can to defraud innocent people. They will continue to exploit every angle of this national crisis and we want people to be prepared.

2) We are not trying to scare people at a time when they are already anxious. We simply want people to be aware of the very simple steps they can take to protect themselves from handing over their money, or personal details, to criminals.

3) Law enforcement, government and industry are working together to protect people, raise awareness, take down fraudulent websites and email addresses, and ultimately bring those responsible to justice.

4) If you think you've been a victim of a scam, contact your bank immediately and report it to Action Fraud on 0300 123 2040 or via actionfraud.police.uk.

Key protection advice

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you hoping you'll let your guard down for just a moment.

They can contact you by phone, email, text, on social media, or in person. They will try to trick you into parting with your money, personal information, or buying goods or services that don't exist.

If you are approached unexpectedly remember to:

- **Stop:** Taking a moment to 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 victim to a scam and report it to Action Fraud.
- You can also report suspicious texts by forwarding the original message to 7726, which spells SPAM on your keypad.
- The police, or your bank, will never ask you to withdraw money or transfer it to a different account. They will also never ask you to reveal your full banking password or PIN.
- Do not click on links or attachments in unexpected or suspicious texts or emails.
- Confirm requests are genuine by using a known number or email address to contact organisations directly.

To keep yourself secure online, ensure you are using the latest software, apps and operating systems on your phones, tablets and laptops. Update these regularly or set your devices to automatically update so you don't have to worry.

Additional protection advice for businesses:

Stop: If you receive a request to make an urgent payment, change supplier bank details, or provide financial information, take a moment to stop and think.

Challenge: Could it be fake? Verify all payments and supplier details directly with the company on a known phone number or in person first.

Protect: Contact your business's bank immediately if you think you've been scammed and report it to Action Fraud.

To keep your business secure online read the National Cyber Security Centre's Small Business Guide: Cyber Security.

When issuing press releases, please include the following in Notes to Editor:

Detailed counter fraud advice is available online, including from Scamsmart, CIFAS, TakeFive, Citizens Advice, Trading Standards and the National Cyber Security Centre. There is bespoke advice about COVID-19 fraud on the Action Fraud website.

Reporting to Action Fraud can be done online at https://www.actionfraud.police.uk or by calling 0300 123 2040. For up-to-date information on COVID-19 fraud please follow Action Fraud on Twitter.

To report offers of financial assistance from HMRC contact phishing@hmrc.gov.uk.

Agreed lines on specific issues

What is happening to fraud levels in general?

While fraud reporting levels into Action Fraud and the Financial Conduct Authority have not increased, we have seen a number of different scams circulating relating to COVID-19. This includes people falling victim to online shopping scams such as believing they are purchasing protective face masks or hand sanitiser that, in reality, do not exist. Criminals are also using Government branding to try to trick people, including using HMRC branding to make spurious offers of financial support through unsolicited emails, phone calls and text messages. We have also seen fake websites and emails purporting to be genuine companies.

This situation is likely to continue, with criminals looking to take advantage of the pandemic such as exploiting people's financial concerns to ask for upfront fees fraudulently applied to bogus loans; offer high-return investment scams; or target pensions.

Huge increases in the number of people working remotely presents an opportunity for criminals to commit computer software service fraud, which involves offers of help to fix devices. As IT systems are under increased pressure, making them work more slowly, such offers of help may seem more believable. In reality, criminals are trying to gain access to your computer or get you to divulge your login details and passwords. Visit the NCSC website for home working guidance and suspicious email advice.

It is also anticipated that there will be new phishing scams or calls claiming to be from government departments offering grants, tax rebates, or compensation.

What do you expect to see in the next few weeks? Months? Next year?

Fraud is incredibly hard to predict and while we are monitoring crime trends carefully, the most important thing is to get the message out there to the general public to be aware, be alert, and think twice before parting with their money or personal details.

The government, law enforcement, security agencies, regulators and the private sector are continuing to work together to protect the public and businesses from all types of fraud.

Government smishing

The Government has only sent one text message to the public regarding new rules about staying at home to prevent the spread of COVID-19. Any others claiming to be from UK Government are false.

Criminals are able to use spoofing technology to send texts and emails impersonating organisations that you know and trust. We would remind anyone who receives an unexpected text or email asking for personal or financial details not click on the links or attachments, and don't respond to any messages that ask for your personal or financial details.

The public can report any type of SMS scams by forwarding the original message to 7726, which spells SPAM on your keypad.

Universal Credit scam

Secretary of State for Work and Pensions Therese Coffey:

"We know cyber criminals and fraudsters are despicably attempting to exploit opportunities around coronavirus. DWP will never text or email asking for your personal information or bank details. Anyone who thinks they have been a victim of fraud should report it to Action Fraud, and notify DWP, as soon as possible."

Additional Information:

- For latest information on Universal Credit go to https://www.understandinguniversalcredit.gov.uk/.
- We urge people not to click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for personal or financial details.
- We continue to work with Action Fraud and the National Fraud Intelligence Bureau to shut down sites and posts which promote this type of fraud.

To what extent are the government support schemes vulnerable to abuse by criminals?

A government spokesperson said:

"We take fraud against the public sector seriously.

"Sadly, the government's stimulus packages are at risk of fraud, from those who would seek to take advantage in these circumstances.

"Public servants across government are looking for ways to reduce the instances of fraud, and take action against those who do try and commit fraud. To support this, the Cabinet Office has established a COVID-19 Counter Fraud Response Team. This team is working with departments to identify fraud risks and put in place measures to reduce the impact and harm of fraud against the government.

"The government wants to keep fraud as low as it can to make sure the stimulus funding is as effective as possible.

"The team are also working collaboratively to understand wider threats of fraud, and to take action, with the NECC, NCA, City of London Police and partners."

Advice for businesses in regards to people working from home

Many organisations are either moving to working remotely for the first time or significantly increasing it, and this presents a number of cyber security challenges. Advice on how to respond to those challenges is set out in the NCSC's working from home guidance.

There are a number of practical steps organisations can take to reduce the risk including:

- Supporting people to use stronger passwords and setting up two factor authentication.
- Ensuring staff know how to report problems, especially those related to security.
- Creating 'How do I' guides for new software and tools staff may be using.
- Using VPNs to allow users to securely access the organisation's IT services.
- Ensuring devices encrypt data whilst at rest.

Some organisations may be allowing staff to use their own devices to work remotely. In this case, please refer to the NCSC's Bring Your Own Device (BYOD) guidance.

In addition to following the guidance set out above, it is worth being aware of phishing emails which trick users into clicking on a bad link. Once clicked, the user is sent to a website which could download malware onto your computer, or steal passwords. We know that cyber criminals are opportunistic and will look to take advantage of people's fears, and there is evidence that the coronavirus outbreak is being exploited in this way.

Those who do fall victim shouldn't feel bad – these scams can be extremely convincing – but what they should do as quickly as possible is report it to their IT department when the incident is work-related or Action Fraud when it is personal. They can also open their antivirus (AV) software if installed, and run a full scan, following any instructions given. If they've been tricked into providing password, they should change their passwords on all their other accounts.

The NCSC's guidance on suspicious emails provides more tips on this.

As a further resource, the Global Cyber Alliance has created a 'Work From Home Community Forum' support group where subject matter experts are on hand to answer specific questions about security issues related to working from home.

Latest update from NFIB
As of 23.59hrs on Thursday 02 April 2020

Total reports to Action Fraud = 509
Total losses = £1,583,023
Total reports of phishing to Action Fraud = 2,192

COVID-19 related fraud makes up 3-5% of all fraud reports received to Action Fraud at the moment.

What scams are we seeing?

The majority of reports are still related to online shopping scams where people have ordered protective face masks, hand sanitiser, COVID-19 testing kits, and other products, which have never arrived.

Other frequently reported scams include:

- Suspect impersonating the government and notifying the victim they were due a payment/rebate.
- Suspect incorporating the COVID-19 epidemic into push payment frauds.
- Suspect asking for a donation to tackle COVID-19, normally via email or pretending to be from a charity which is assisting vulnerable people during the outbreak.
- Suspect calling purporting to be victim's bank, saying account was compromised/there had been unusual activity. Victim advised to open new account/transfer money there and then. Victim told they should not visit their branch because of COVID-19.
- Suspect persuades victim to make an advanced payment for a rental property. The suspect uses the outbreak as the reason for the victim being unable to view the property. The property does not exist or the suspect is not in a position to rent it.
- Suspect uses COVID-19 as a hook for offering employment. Victim is persuaded to pay an advanced fee for vetting/qualifications to get them the job which ultimately does not exist.

New trends

Courier Fraud

We are now monitoring the number of courier frauds which have occurred during lockdown. This currently stands at 35 with losses of £193,464. Obviously, this is a worrying statistic and it is possible these numbers will increase. To help in getting protect messaging out, we will uploading a number of social media assets to the resources section of the Action Fraud website next week for forces to utilise.

Phishing/smishing

Some of the tactics being used in phishing emails and texts 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 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. We have also had reports of people receiving similar text messages. Another MO involves emails purporting to be from HMRC asking them to check their entitlement and make a claim by a specific date to receive any possible repayments. Recipients are asked to click on a link to start a claim.

• Smishing scams claiming to be from .gov.uk. Again, different MOs but examples we've seen include advising the victim their phone data has shown they have left their home more than once and they should phone a number to pay a fine or risk further punishment. In others reports, text messages were sent informing victims they can claim £458 of coronavirus aid. This text features a link to a fake government website, which urges users to enter their postcode to apply for COVID-19 relief.

• Emails stating that Virgin Media is cancelling subscription charges in light of COVID-19. Recipients are asked to click on a link to prevent them from being charged. We've also seen several reports relating to phishing abuse in other brands, for example TV licencing phishing attempts, BT Sport and Amazon phishing emails.

In addition, fraudsters are sending emails:-

• Selling or giving away face masks, loo roll, immunity oils etc.

• Shipping or selling COVID-19 testing kits and emergency medical and survival kits at a reduced rate

• Providing health alerts and advice with links on receiving updates and how to avoid the virus

• Encouraging recipients to invest in bitcoin or other financial schemes due to the pandemic's effect on the economy

• Asking recipients to contribute to various COVID-19 related charitable funds e.g. WHO 'solidarity response fund' / Centre for Disaster Philanthropy response fund.