City of London Police
National Fraud Intelligence Bureau

Coronavirus fraud briefing – updated 24 March 2020.

CITY OF LONDON POLICE: OFFICIAL - RECIPIENT ONLY

Latest picture from Action Fraud/NFIB

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, 38 reports in just four days (14 March – 18 March) and 84 reports between 19 March and 22 March. In total this is 189 reports but includes reports from people who have lost money and also 'information reports' where people have seen a scam but not suffered a financial loss.

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 1,000 reports of coronavirus-themed phishing attempts – the majority of which are emails. These communications try 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. We have also had reports of people receiving similar text messages.

You can see examples of these phishing emails here: https://twitter.com/actionfrauduk/status/1240911363167391744

CITY OF LONDON POLICE: OFFICIAL - RECIPIENT ONLY

What are we expecting to see going forward?

Any number of frauds could increase as more people work from home and vulnerable, elderly people self-isolate.

The NFIB have suggested, based on the MO of fraudsters, that the following fraud types could increase during the COVID-19 outbreak:

- Online Shopping and Auction Fraud – more people at home socially distancing increases the number of people online shopping through necessity but also the fact they have more time on their hands to browse the internet.
- Computer Software Service Fraud – more people working from home will increase demand on IT systems causing slower responses and making some scripts seem more believable.
- Lender Loan Fraud – there are already media reports circulating about parents concerned that they may not be able to feed their children if they are not at school and those who will be made redundant or self-employed receiving a much reduced income with potentially the same or increased living costs. This may mean people look to quick loans to see them through.
- Mandate Fraud – with more people working at home, it may be easier for fraudsters to impersonate senior decision makers, with seemingly valid reasons why they cannot be contacted, and request a change in direct debit or standing order payments.
- Investment Fraud including Pension Liberation Fraud – fraudsters could take the opportunity to create bogus investments in commodities in high demand, for example oxygen, and if people are worried that they might not have enough money to see them through this financially uncertain time, they may be more prepared to invest.

Protection advice

Detailed counter fraud advice is available online, including from Scamsmart, ActionFraud, CIFAS, TakeFive, Citizens Advice, Trading Standards and the National Cyber Security Centre.

Reporting to Action Fraud can be done online at https://www.actionfraud.police.uk or by calling 0300 123 2040.

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

Individuals

Online Shopping and Auction Fraud

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.

Lender Loan Fraud

Seek advice first: Speak with a trusted friend or family members first if you're using a loan company you're unfamiliar with, or if the lender requires an up-front fee.

Scam messages: Don't click on the links or attachments in suspicious emails, and never respond to messages that ask for your personal or financial details.

FCA register: Use the Financial Conduct Authority's (FCA) register to check if the company is regulated by the FCA. If you deal with a firm (or individual) that isn't regulated, you may not be covered by the Financial Ombudsman Service (FOS) if things go wrong and you lose your money.

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.

Pension Liberation fraud

Investment opportunities: Don't be rushed into making an investment. Remember, legitimate organisations will never pressure you into making a transaction on the spot.

Seek advice first: Before making significant financial decisions, speak with trusted friends or family members, or seek professional independent advice. The Pension Advisory Service (PAS) also provides free independent and impartial information and guidance.

FCA register: Use the Financial Conduct Authority's (FCA) register to check if the company is regulated by the FCA. If you deal with a firm (or individual) that isn't regulated, you may not be covered by the Financial Ombudsman Service (FOS) if things go wrong and you lose your money.

Tax charges: Ensure sure you are aware of any tax charges (up to 70%), plus other fees, that will be deducted from the amount you withdraw before making any decisions.

Investment Fraud

Investment opportunities: Don't be rushed into making an investment. Remember, legitimate organisations will never pressure you into making a transaction on the spot.

Seek advice first: Speak with a trusted friend or family members, and seek independent professional advice before making significant financial decisions.

FCA register: Use the Financial Conduct Authority's (FCA) register to check if the company is regulated by the FCA. If you deal with a firm (or individual) that isn't regulated, you may not be covered by the Financial Ombudsman Service (FOS) if things go wrong and you lose your money.

Advice for businesses

Mandate Fraud

Verify: If you receive a request to move money into a new bank account, contact the supplier directly using established contact details, to verify and corroborate the payment request.

Internal processes: Establish robust internal processes for handling changes to payment details. For example, only designated employees should be able to make changes to payment arrangements.

Sensitive information: Invoices, payment mandates, and other documents containing sensitive financial information should be stored securely and only be accessible to those staff that need them to perform their duties. Sensitive documents should be shredded before they are disposed of.

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.

Suggested social media posts

1) More people may fall victim to #onlineshopping fraud as they self-isolate due to #COVID19. You are a victim of online shopping fraud if you buy goods from an online seller that never arrive.

Find out more at: https://www.actionfraud.police.uk/a-z-of-fraud/online-shopping-fraud
[Online shopping graphic]

2) People may be worrying about their finances during the #COVID19 outbreak. Lender loan fraudsters will use the opportunity to:

- approve your application for a fast loan regardless of your credit history

- ask you to pay an upfront fee

- take your payment and never provide the loan

Find out more at https://www.actionfraud.police.uk/a-z-of-fraud/loan-scams
[Lender loan graphic]

3) As more people work from home due to #COVID19, fraudsters may try to get you to change a direct debit, standing order or bank transfer mandate, to divert funds to their bank account, by purporting to be an organisation you make regular payments to.

https://www.actionfraud.police.uk/a-z-of-fraud/mandate-fraud
[Mandate fraud graphic]

4) As more people work from home due to #COVID19, fraudsters may capitalise on slow networks and IT problems, to commit computer software service fraud. Be wary of cold calls or unsolicited emails offering you help with your device or to fix a problem

https://www.actionfraud.police.uk/a-z-of-fraud/computer-software-service-frauds

[Computer software service fraud graphic]

5) Fraudsters could try to take advantage of the financial uncertainty surrounding #COVID19 by offering people sham investment opportunities. If you get a cold call or unsolicited email offering you a deal that sounds too good to be true, it probably is.

https://www.actionfraud.police.uk/a-z-of-fraud/investment-fraud
[Investment fraud graphic]

6) Action Fraud have received reports of #COVID19 related scams. The majority relate to the online sale of protective items such as facemasks, and other items in short supply due to the outbreak, that don't exist.
https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march
[CV19 related scams graphic]

7) A number of #COVID19 related phishing emails have been reported to Action Fraud. These emails attempt to trick you into opening malicious attachments which could lead to fraudsters stealing your personal information, logins, passwords, or banking details.
https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march
[CV19 phishing emails graphic]

Useful protection videos for social media here:
https://www.youtube.com/watch?v=uyKPDlPxrTY&list=PLoWZUquVJo4SLWKD5A96znBNi23UzOjiG&index=1