Beware fraud and scams during Covid-19 pandemic fraud

Criminals are using the Covid-19 pandemic to scam the public – don't become a victim.

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 experts at impersonating people, organisations and the police.

They spend hours researching you for their scams, hoping you'll let your guard down for just a moment.

Stop: Taking a moment to stop and 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 for a scam and report it to Action Fraud*.

Your bank or the police will NEVER ask you to transfer money or move it to a safe account.

Criminals are targeting people looking to buy medical supplies online, sending emails offering fake medical support and scamming 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 make appeals for you to support bogus charities or those who are ill.

Reports from the public have already included online shopping scams where people have ordered protective face masks, hand sanitiser, and other products, which have never arrived and a number of cases have been identified where fake testing kits have been offered for sale.

Criminals are also 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, 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*."

Security Minister James Brokenshire said:

"Fraudsters are callous criminals who ruin victims' lives while lining their own pockets. To take advantage of vulnerable people at this difficult time is particularly reprehensible.

"The Government is committed to working with the NCA and all law enforcement partners to tackle this and protect the public."

Commander Karen Baxter, City of London Police, National Co-ordinator of Economic Crime, said:

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

"As more people stay indoors and work from computers and laptops at home, there is more opportunity for criminals to try and trick people into parting with their money at a time when they are anxious and uncertain about the future. This is especially relevant as older, more vulnerable people self-isolate and may be targeted over the phone, or even in person, by despicable criminals.

"It is important that we continue to raise awareness of fraud and protect ourselves, and the vulnerable people in our communities, the best we can."

Notes to editors

1. For interviews with Graeme Biggar contact NCA press office on 020 7979 5835 orpressoffice@nca.gov.uk
2. To request an interview with City of London Police contact 020 7601 2218 or media@cityoflondon.police.uk
3. * In Scotland reports should be made to Police Scotland 101, not Action Fraud
4. Figures in fraud related to Coronavirus, or COVID-19 (Friday 20 March 2020) show 105 victims have reported to Action Fraud since 1 February 2020, with total losses reaching nearly £1million.
5. Detailed counter fraud advice is available online, including from Scamsmart, ActionFraud, CIFAS, Take Five to Stop Fraud, Citizens Advice, Trading Standards and the National Cyber Security Centre.
6. **Take Five to Stop Fraud** is a national campaign that offers advice to help everyone protect themselves from preventable financial fraud. Led by UK Finance, the campaign is being delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector organisations.

   Consumers are urged to:

   Stop: Taking a moment to stop and 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 for a scam and report it to Action Fraud.

7. 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

Fraud types and advice - 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.