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.

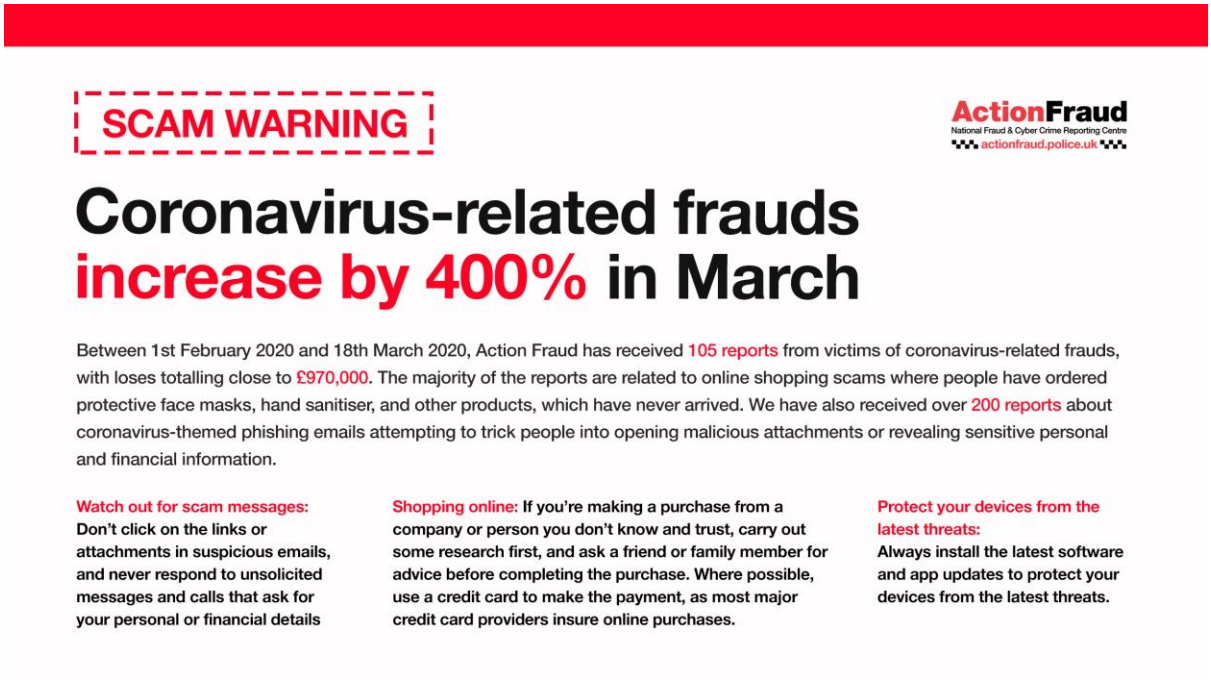
This situation is likely to continue, with criminals looking to exploit further consequences of the pandemic, such as exploiting financial concerns to ask for upfront fees for bogus loans, offering high-return investment scams, or targeting pensions.

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.

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.

If you believe or know that you have been the victim of fraud, you can report 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



Online shopping fraud

- If you're purchasing goods and services from a company or person you don't know and trust, carry out some research first. Look up reviews of the company and ask trusted friends and family members if they have heard of it before.
- Be wary of unsolicited emails and texts offering questionably good deals, and never respond to messages that ask for your personal and financial details.
- 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 service such as PayPal if possible.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Computer software service fraud

- Never install any software, or grant remote access to your computer, as a result of a cold call.
- Genuine organisations would never contact you out of the blue to ask for your financial details, such as your PIN or full banking password.
- If you need tech support, ask trusted friends or colleagues for recommendations and look for reviews online first. Don't contact companies promoting tech support services via browser pop-ups.
- If you have granted remote access to your computer seek technical support to remove unwanted software from your computer from a trusted professional. Inform your bank and monitor your bank statements for unusual activity.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Mandate fraud

- If you receive a request to move money into a new bank account, contact the supplier directly using established contact details to verfiy and corroborate the payment request.
- Establish robust internal processes for handling changes to payment details. For example, only designated employees should be able to make changes to payment arrangements.
- 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 the bank as soon as possible so they can help prevent any further losses.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040