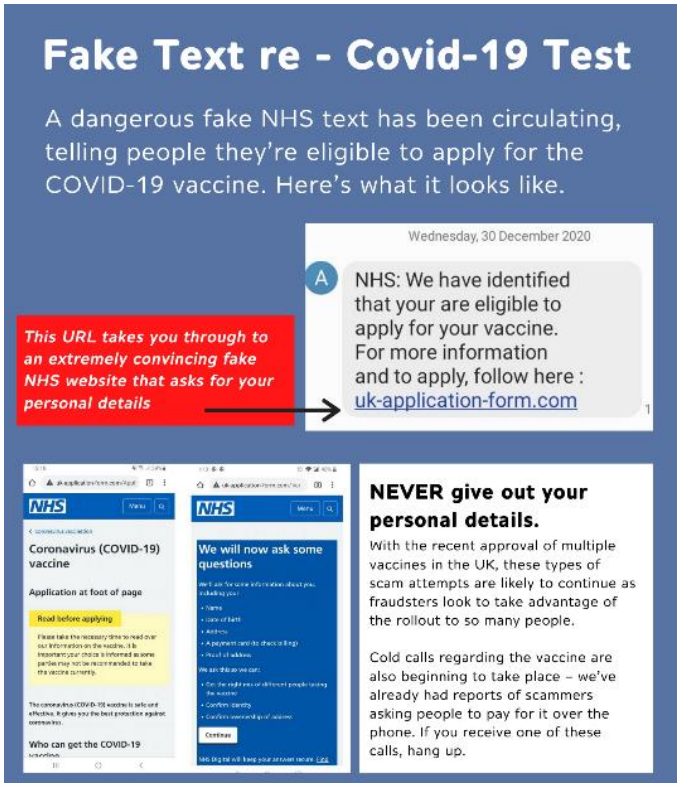
A brief guide to fraud prevention

During the COVID 19 Pandemic criminals have tried to make financial gain for themselves by targeting the public with a number of frauds that relate to the current situation

Fraudsters are using phishing email claiming to be from a trusted organisation providing assistance or requiring people to take some sort of action. They generally state or imply the need for your urgent action to either avoid an issue or take advantage of an offer including the following:



nhs.test.and.trace.covid19.app@notifications.service.gov.uk ''Public Health Message: NHS COVID-19 App'. Offer of download of track and trace app. It's important to remember that NHS Test and Trace will never ask you for financial details, PINs or banking passwords. They will also never visit your home.

Whilst it is possible for criminals to fake official phone numbers, they cannot fake official website addresses. We would encourage anyone with concerns about a phone call, text message or email they have received, in relation to Test and Trace, to check the website address being provided to you carefully. If possible, type the official address, which will be https://contact-tracing.phe.gov.uk followed by unique characters given to you, directly into your browser.

Contact tracers will never:

- Ask you to dial a premium rate number to speak to us (for example, those starting 09 or 087)
- Ask you to make any form of payment
- Ask for any details about your bank account
- Ask for your social media identities or login details, or those of your contacts
- Ask you for any passwords or PINs, or ask you to set up any passwords or PINs over the phone
- Ask you to purchase a product
- Ask you to download any software to your device or ask you to hand over control of your PC, smartphone or tablet
- Ask you to access any website that does not belong to the Government or NHS

Other phishing emails that are being seen at this time include the following:

- From s-nishimura@dc-international.co.jp - 'Covid-19 relief grant' - 'We have determined you are eligible - please submit a request' (malicious)
- From eligible-HMRC@magenta.de - 'Covid19_Relief (HMRC) - You are eligible for a grant ' - Email includes a link offering loans up to£7.5k (malicious)
- From hello@bebiboom.com- '[COVID 19] Notifications DHL Package' - link to enable the package to be delivered (suspicious)
- From various email addresses beginning notification@... - 'Important coronavirus treatment research studies seeking 18+' –contains a link to read about the research studies (suspicious)
- From various email addresses ending in @actualbestdeals.com – 'COVID-19 vaccine research studies'- links to details
- From various email addresses– 'Corona is not "controllable" ' - link to video with protection advice

If you receive an email from a "government department" offering you a council tax reduction then take a moment to Stop, Challenge, Protect. Criminals are using official government branding in emails to convince you they're genuine and to trick you into giving them your money or information. Emails received often contain links which, when clicked on, lead to an "official looking" webpage designed to access your personal information. In some cases, this could lead to criminals using your identity to commit fraud. Below is an example of a council tax reduction fraud email:

GOV.UK

Council Tax Reduction

You have a new message from GOV.UK about your Council Tax

Hi customer,

Working out your Council Tax

You'll need to know 3 things:

- the valuation band for your home in England and Wales or in Scotland
- how much your local council charges for that band
- whether you can get a discount or exemption from the full bill

You are getting a Council Tax Reduction (this used to be called Council Tax Benefit) considering you're on a low income or get benefits.

- Total amount of benefits: **GBP 385.50**
- The refund amount will be transferred directly on your Debit/Credit Card.

Apply now to claim the reductions made over your past 2 years of Council tax payments.

Claim your Council Tax Reduction Now ->

The information in this electronic e.Mail message is private and confidential, and only intended for the addressee.

Thanks

The Government Digital Service Team

Crown Copyright 2020

If you receive an email, text or WhatsApp message purporting to be from the government, HMRC, the World Health Organisation (WHO) or a coronavirus-related charity, then **take a moment to think** before you part with your money or information.

Never click on links or download attachments as criminals may infect your devices with malware or ask you to enter your personal or financial information into fake websites. In some cases this can lead to your identity being stolen.

This is not an exhaustive list of all fraudulent emails, text messages, phone calls etc. It is important to be on your guard at all times and remember to: TAKE FIVE TO STOP FRAUD

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.

TOP TIPS TO PREVENT YOURSELF FROM BECOMING A VICTIM OF FRAUD

NEVER DISCLOSE SECURITY DETAILS A genuine bank or organisation will never ask you for details such as your PIN or card number over the phone or in writing. Before you share anything with anyone, stop and think. Unless you're 100% sure who you're talking to, don't disclose any personal or financial details. Instead, hang up and contact the organisation yourself using the number on the back of your bank card or on their website.

DON'T ASSUME AN EMAIL OR PHONE CALL IS AUTHENTIC Just because someone knows your basic details (such as your name and address or even your mother's maiden name), it doesn't mean they are genuine. Criminals will use a range of techniques to get your details and may even say you've been a victim of fraud to scare you into action.

DON'T BE RUSHED OR PRESSURED Under no circumstances would a genuine bank or another trusted organisation force you to make a financial transaction on the spot; they would never ask you to transfer money into another account, even if they say it is for fraud reasons. They will always let you call them back on a number you know is real – if they try and stop you doing this, it's a fraudster and you should hang up.

LISTEN TO YOUR INSTINCTS If something feels wrong then it is usually right to question it. Criminals may lull you into a false sense of security when you're out and about or rely on your defences being down when you're in the comfort of your own home. If your gut-feeling is telling you something is wrong, take the time to make choices and keep your details safe.

STAY IN CONTROL Have the confidence to refuse unusual requests for personal or financial information. It's easy to feel overwhelmed when faced with unexpected or complex conversations. Remember that it's ok to stop the discussion if you don't feel in control of it. If you've taken all these steps and still feel unsure about what you're being asked, never hesitate to contact your bank or financial service provider on a number you trust, such as the one listed on their website or on the back of your payment card.

TOP 10 TIPS TO TAKE A STAND AGAINST FRAUD

1. **Say no** – To unwanted callers
2. **Be wise to rogue traders** – Too good to be true offers probably are
3. **Don't feel pressurized to make a decision** – Say "NO" or say you need advice first
4. **Be wise to postal fraud** – No legal company will ask for money to claim a prize
5. **Keep personal details safe** – They could be used fraudulently in the wrong hands
6. **Be Online Savvy** – Check who you are communicating with online
7. **Research the credentials of the company** – Be certain they are not bogus
8. **Talk to someone you trust** – If you are suspicious
9. **Report a fraud** – Help expose the criminals
10. **Know you are not alone** – Anyone can be victim, report it and get the right support

WHAT TO DO IF YOU BECOME A VICTIM OF FRAUD

GET HELP AND REPORT A FRAUD

If you think you have uncovered a fraud, have been targeted by a fraudster or fallen victim, there are many authorities you can contact for advice or to make a report.
Reporting crime, including fraud, is important. If you don't tell the authorities, how do they know it has happened and how can they do anything about it? Remember that if you are a victim of a fraud or an attempted fraud, however minor, there may be hundreds or thousands of others in a similar position. Your information may form part of one big jigsaw and may be vital to completing the picture.

Reporting fraud
All fraud should be reported directly to Action Fraud.
Action Fraud Reporting online: www.actionfraud.police.uk
Telephone reporting: 0300 123 2040
Unless
A crime is in progress or about to be committed. The suspect is known or can be easily identified. The crime involves a vulnerable victim. If this is the case you should contact police directly either by dialing 999 in an emergency, dialing 101 in a non-emergency or visiting your local police station. If you have information on any crime and you would prefer not to speak to police, you can call Crimestoppers anonymously on 0800 555 111 or visit www.crimestoppers-uk.org Crimestoppers is an independent charity.

For More information follow one of these links to websites that have lots of information on how to prevent fraud

Take Five - https://takefive-stopfraud.org.uk/
Friends Against Scams - https://www.friendsagainstscams.org.uk/training/friends-elearning

Together we can take a stand against fraudsters and together we can make a difference