Coronavirus-related frauds **increase by 400%** in March

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 (e.g. your bank or HMRC) and the police.

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.

Social Engineering
Social Engineering is defined as "The clever manipulation of the natural human tendency to trust." It's easier to trick you into opening an infected email than it is to hack into your account. Due to this, social engineering has become much more prominent, and cyber criminals are trying more diverse ways to get people to undertake tasks, provide information or hand over money using these techniques.

Types of social engineering;

- **Phishing** – fraudulent emails sent by cyber criminals pretending to be someone else, for example a bank, NHS or government department. The aim of the email is to install malicious software on your device or obtain Personal Identifiable Information including login credentials.
- **Spoofing** – is the act of disguising a communication from an unknown source as being from a known, trusted source. This can apply to emails, phone calls and websites.
- **Smishing** – fraudulent text messages purporting to be from reputable companies in order to get individuals to reveal personal information, such as passwords or financial details.
- **Vishing** – criminals making phone calls or leaving voice messages pretending to be from reputable organisation in order to induce individuals to reveal personal information such as bank details and credit card numbers.

How to protect yourself:

- Don't assume a call, text or email is genuine.
- Never provide financial or personal details to a caller.
- Don't click on website links or download attachments in unexpected texts or emails.
- Phone numbers and emails can be changed (spoofed) and are not proof of identity.
- Challenge every request for your information, money or details.
- Double check requests for your details and verify via a trusted source.

The police can't stop crime it doesn't know is happening.
Even if you didn't lose money, you should still report every instance of fraud or cyber crime you're targeted by. Every report assists police investigations, disrupts criminals, and reduces harm. Reports are also used to identify crime trends and create awareness campaigns to help protect people against them.
Report online at www.actionfraud.police.uk or by telephone on 0300 123 2040.

Useful websites:
https://www.ncsc.gov.uk
https://www.friendsagainstscams.org.uk
https://takefive-stopfraud.org.uk
https://www.met.police.uk/littlemedia
Don't assume your friends and family know the latest scams.
Tell2 of them offline and play your part in disrupting criminals!

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Fraudsters cold call you pretending to be from your bank or from the police. They claim there is an issue with your bank account or request your assistance with an ongoing bank or police investigation.

They claim they are investigating, often saying it involves corrupt bank employees or police and ask for your help or say your account is at risk. The aim of this call is to trick you into parting with your money either in person, online, via a money service bureau or in a bank.

If they manage to convince you, they instruct you to carry out a task which ultimately involves you handing over your money. These include:

- Asking you to attend your bank branch to withdraw a large sum of money which they will then collect from you for evidence. They may claim the money may be counterfeit, or that it is going to be sent off for forensic or fingerprint analysis.
- Asking you to withdraw large amounts of foreign currency, which will similarly be collected by a courier from your home address.
- Asking you to provide details over the phone, including typing in your PIN then handing over your cards to a courier sent to your address (often after you have cut them up as instructed).
- Asking you to purchase high value items, such as expensive watches to 'clear criminal funds' which will again be collected by a courier.
- Asking to purchase other items, like gift cards or vouchers.

In all of these cases they will assure you that you will soon be reimbursed.

Fraudsters want to avoid detection, and may give you instructions to achieve this such as:

- Informing you it is an undercover operation involving bank/police corruption, so you must not tell bank staff or police anything about the phone call. They may even threaten that you could be arrested if you do.
- Give you a cover story to tell bank staff or police, e.g. the money/item is for building works, a holiday or a gift for a relative.

Criminals have developed their methods further to no longer involve the courier. They may now claim that as a result of the fraud, they are investigating your bank account and therefore ask you to transfer your money into a 'safe account'. They will provide you with the account details and may even say this is set up in your name. This is called Push Payment Fraud.

How to protect yourself

- Be extremely wary of unsolicited phone calls from your bank or the police, particularly if they are requesting personal information.
- End the call, call back on a different phone line or on a mobile. If this is not possible, wait at least one minute before calling back. Use either the telephone number on your bank card, go to the bank's website or for the police dial '101'.
- Speak to friends or family before carrying out any actions. Don't trust claims made by cold callers.
- Never hand over your money, bank cards or make purchases following an unexpected call.
- Never share your PIN with anyone.
- Watch our video on Impersonation Fraud at www.met.police.uk/littlemedia.

REMEMBER - Your bank or the police will never ask you for your PIN, bank card, or ask you to withdraw money or buy items on their behalf.

CAUTION - If you receive an unexpected call, hang up and use another phone to call back and confirm identity.

THINK - How do I know they are who they say they are?

How to report it

You can report either online at http://www.actionfraud.police.uk/ or call 0300 123 2040.
If you've given your bank details over the phone or handed your card to a courier, call your bank straight away to cancel the card.