# Covid-19 Scams

Scammers will play on anything in the media in order to scam people. During an already anxious and uncertain time, scammers use this to create further panic forcing victims to part with their cash.

**Pet scams** – We have received many reports of individuals buying pets online. Scammers will ask for a deposit to secure the pet but advise you cannot visit the pet yet due to lockdown, they will then either block you & keep your money, or ask for further money for things such as injections or neutering.

**Door knocking** - Action Fraud have received reports of individuals targeting the elderly & vulnerable by offering to do shopping. The individual then takes the victims cash / bank card and never returns.

**Fake websites** - Action Fraud have received reports of individuals going online to order items such as face masks & hand sanitiser. The victim pays for these items & they never arrive.

**Phishing emails / texts** – There have been many reports of fake emails / texts. Report phishing emails to the National Cyber Security Centre by forwarding them to - **report@phishing.gov.uk**

**Scam telephone calls** – Scammers continue to use the telephone to scam people, especially knowing the elderly and vulnerable are at home.

**Tips on how to work from home safely** –Many of you are working from home and you may have concerns around how to do that safely. Visit the National Cyber Security Centre for guidance: **https://www.ncsc.gov.uk/guidance/home-working**

**Test & Trace scams -** NHS Test and Trace will never ask you for financial details, PINs or passwords. They will also **never** visit your home. Contact tracers will never:

- Ask you to dial a premium rate number.
- Ask you to make any form of payment or for any bank account details.
- 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 or device.
- Ask you to access any website that does not belong to the Government or NHS.

NOTTINGHAMSHIRE POLICE
PROUD TO SERVE

Top Tips for Fraud:

1. Verify any unexpected contact is genuine by using a known number or email address to contact organisations directly – is this caller who they say they are? After hanging up, wait five minutes and make sure you can hear a dial tone before making any other calls, or use your mobile. NEVER allow an unsolicited caller remote access to your computer or devices.

2. Don't be pressurised into sending money – stop and think and check with a trusted source or person. It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you. Have confidence in yourself, if it feels wrong to you – it probably is.

3. Use someone you know and trust for shopping / other essentials. Don't hand money over to someone on the doorstep.

4. Authorities like the DWP and HMRC will never ask for banking details like your password or PIN on the phone or in person. You will NEVER be asked to move money to a 'safe account'. The Police will NEVER ask you to help in an investigation by moving money or withdrawing funds.

5. Check for ID's and get them verified – genuine officials will be more than happy to wait while you verify their ID.

Top Tips for Cyber:

1) Pick strong passwords – choose **Three Random Words** with a mixture of upper/lower case, numbers and special characters. Do not use the same password across sites. Enable Two Factor Authentication (2FA) on your accounts and devices that offer it, this provides a second layer of security.

2) Be wary of phishing scams - Don't click on any links or attachments in unexpected emails.

3) Social Media – For those of you who use social media, make sure that it is set up correctly, review your privacy settings to ensure your profile is appropriately locked down.

4) Use antivirus and ensure you are using the latest versions of software, apps and operating systems on your phones, tablets, desktops and laptops. Update these regularly or set your devices to automatically update so you don't have to worry.

5) Backups – Always back up your most important data such as your photos and key documents to an external hard drive and / or cloud storage.

NOTTINGHAMSHIRE POLICE
PROUD TO SERVE