General Scam Advice

- Criminals will use every opportunity they can to defraud innocent people. They will continue to exploit every angle of this national crisis and we want people to be prepared.
- We are not trying to scare people at a time when they are already anxious. We simply want people to be aware of the very simple steps they can take to protect themselves from handing over their money, or personal details, to criminals.
- Law enforcement, government and industry are working together to protect people, raise awareness, take down fraudulent websites and email addresses, and ultimately bring those responsible to justice.
- If you think you've fallen for a scam, contact your bank immediately and report it to Action Fraud on **0300 123 2040** or via https://www.actionfraud.police.uk/ If you are in Scotland, please report to Police Scotland directly by calling 101.
- You can report suspicious texts by forwarding the original message to **7726**, which spells SPAM on your keypad. You can report suspicious emails by forwarding the original message to report@phishing.gov.uk An automated system will scan the email and if malicious links are found, the associated website will be taken down.

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you hoping you'll let your guard down for just a moment.
They can contact you by phone, email, text, on social media, or in person. They will try to trick you into parting with your money, personal information, or buying goods or services that don't exist.

If you are approached unexpectedly remember to:

- **Stop:** Taking a moment to 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 victim to a scam and report it to Action Fraud.
- The police, or your bank, will never ask you to withdraw money or transfer it to a different account. They will also never ask you to reveal your full banking password or PIN.
- Do not click on links or attachments in unexpected or suspicious texts or emails.
- Confirm requests are genuine by using a known number or email address to contact organisations directly.
- To keep yourself secure online, ensure you are using the latest software, apps and operating systems on your phones, tablets and laptops. Update these regularly or set your devices to automatically update so you don't have to worry.

The National Cyber Security Centre (NCSC) has launched the **Cyber Aware** campaign with six actionable steps to protect yourself.
By implementing the six 'Cyber Aware' tips and flagging threats to the NCSC, you will keep yourself and others secure from the vast majority of threats.
These tips are;

1. Create a separate password for your email
2. Create a strong password using three random words
3. Save your passwords in your browser
4. Turn on two-factor authentication
5. Update your devices
6. Turn on backup

To find out more, please visit CyberAware.gov.uk