WE'RE ASKING THE NATION TO:

TO STOP FRAUD™

- Never assume an email, text, social media post or phone call is genuine
- Stay in control – verify the email or call using another trusted means
- Don't be rushed into clicking a link or supplying personal information
- Don't pay unexpected bills, fines or charges unless they've been verified
- Never reveal personal details such as your password or PIN

Find out more: **takefive-stopfraud.org.uk**

Secure your online accounts

Use a different strong password for each of your online accounts.
This helps to protect all your accounts if one is compromised or a data leak occurs.

You can make a strong password by combining three random words.
This method can be used to make strong memorable passwords (eg. SycamoreUrgentlyHippo).

Keep all your passwords secret.
Never reveal your passwords to anyone, even if the caller claims they are the police, or are calling or emailing on behalf of your bank, computer company, phone or Internet provider.

Protect your online accounts by enabling two-factor authentication (2FA).
This adds an extra layer of security by sending you a unique code whenever someone tries to logon using a different device. You can then use the code to confirm a valid logon attempt.

Never click links in unexpected and unverified emails, texts and messages.
These links may open phishing sites that are designed to mimic real account logons and websites to steal your passwords, personal information and payment details. Never click links in unexpected emails or texts unless you have verified them by another trusted means.

Never allow any unexpected caller to install software on your computer.
Fraudsters may try to pressure you into installing software that gives them remote access to your computer, by claiming they've detected errors or viruses that need to be fixed urgently.