STAY SAFE FROM ONLINE SCAMS

- Protect your email by using a strong and separate password, consisting of three random words.
- Don't leave your mobile devices unattended in public places. Protect them with a PIN/passcode.
- Always install the latest software and app updates on all of your devices.
- Don't use public Wi-Fi hotspots to conduct confidential activity, like banking.
- Think about what you post online and who has access to it. Configure your privacy options so that your content is only accessible to the people you want to see it.

- People aren't always who they claim to be. Fake emails and phone calls are a favourite way for fraudsters to approach their victims.

- Email addresses and phone caller ID can be faked. Never respond to emails or texts that ask for personal or financial details.

- Never automatically click on a link in an unexpected email or text. Take five minutes to consider whether it is genuine.

- Installing two-factor authentication is advised for email accounts. This is an additional process to secure your account for example using a password and a card reader to access your online banking.

- Always access internet banking sites by typing the bank's address into your web browser.

- Avoid paying for goods or services via bank transfer as it offers you little protection if you become a victim of fraud.

- If someone you've never met in person asks you for money, stop all contact.

For more advice, find the Neighbourhood Watch scams prevention kit at:
www.ourwatch.org.uk/toolkits