Climate Change Group

We are looking at Utilities, starting with phones, and thought this would be good to share with you.

MOBILE PHONE SCAMS

Many of us love the convenience of our mobile phones - we can message our friends; chat; shop; listen to the radio; manage our bank accounts; and so much more. However, as with everything, they come with hidden dangers, one of which is ⚡ **THE SCAMMER** ⚡ .
If we're careful, we can minimise our exposure to scams. However, as scams become more sophisticated, it is wise to keep an eye on information sites to ensure our responses to calls and messages are appropriate.
Here are a few examples of current scams. However, I urge you to read about them more thoroughly on Which - Phone Scams or Age UK - Latest Scam Alert.

Current scams: examples

- **Bank's Fraud Department:** Callers claim your account has been compromised and urge you to move funds to a new, safe account, which is controlled by the scammer.
- **HMRC/Tax Scam:** Scammers pose as HMRC officials, claiming you have underpaid tax or are due a rebate, often threatening arrest if a fine is not paid immediately via bank transfer or gift cards.
- **DWP/Winter Fuel Payment:** Fraudsters target elderly people, claiming they need to provide bank details to receive a government winter fuel payment.
- **Remote Access Scam:** Fraudsters claim your computer or phone has a virus or has been hacked. They instruct you to download remote access software to 'fix' it, allowing them to steal personal data and login credentials.
- **'Fake' QR Code Scams:** Fraudsters place fake QR codes on parking machines or in public places, directing you to a phishing website to steal payment details.
- **WhatsApp 'Friend in Need':** A message from an unknown number pretending to be a family member who has lost their phone and needs money urgently.
- **Prize Scam:** Automated calls or texts asking you to answer easy questions to win a prize, which then lead to premium-rate numbers (often starting 0906) that cost a significant amount per minute.

Avoiding Scams

There are several decisive actions you can take to avoid phone scams (from the Financial Conduct Authority website).

Do:

- Treat all unexpected calls, emails and text messages with caution. Don't assume they're genuine, even if the person knows some basic information about you.
- Hang up on calls and ignore messages if you feel pressured to act quickly. A genuine bank or business won't mind waiting if you want time to think.
- Check your bank account and credit card statements regularly.
- Set your online privacy on social media to 'private' or 'friends only'.

Don't:

- Give out your bank account or credit card details unless you're certain who you're dealing with.
- Share your passwords with anyone (including your social media passwords).
- Give access to your device by downloading software or an app from a source you don't know. Scammers may be able to take control of your device and access your bank account.

Reporting Scams

You can report phone scams officially to the National Cyber Security Centre – Reporting Phone Scams. You will also find information about scams on this site.

Gill Trickett
Climate Change Group