POLICE WARNING

We are seeing an increase in reports of network provider accounts being hacked, these incidents lead to mobile numbers being taken over by Sim Swapping.

SAFEGUARD YOUR MOBILE PHONE NOW! DON'T LET HACKERS DIAL IN

SIM swapping is a type of fraud where criminals trick your mobile provider into transferring your phone number to a SIM card they control.
Once they have access to your number, they can intercept calls and messages, including 2-step verification (2SV) codes used to secure your online accounts leading to reset passwords, access your email, bank, social media accounts and make credit applications in your name.

Act now to secure your mobile and email accounts. Use your network and email provider settings to enable strong protection before it's too late.

What to do if you think your SIM card has been swapped?

Call your network provider. If you receive unsolicited texts or emails about your SIM being ported or a PAC request, or you unexpectedly lose phone service, you will need to notify your provider immediately.

Inform your banks as soon as possible. The criminals may attempt to steal your money by making a money transfer either online or over the phone. You can also record your details with Cifas, the fraud prevention service.

Protect your mobile number now:

1. **Create a strong separate password using 3 random words:**
Strong random password example = Read421-Plants-!Treasure

2. **Turn on 2-Step Verification (2SV):**
2SV adds a second layer of protection, therefore even if hackers have your password, they can't access your email or linked accounts.

For example, once enabled, you might get a code sent to your phone when signing in on a new device or changing your password, but you won't need to do this every time you use the account or app its active on.

3. **Contact your network provider** to ensure all available protections against this type of attack are in place.

For more information:
www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/