Protect yourself from SIM Swap Fraud

SIM swapping is where a fraudster is able to gain control of your mobile phone number by convincing the phone provider to transfer the service to a SIM in their possession. You may notice that your mobile is no longer connecting and you are unable to make calls or texts.

The scam begins with a fraudster gathering personal details about you, either by phishing emails, social engineering, previous data breaches or reading your social media posts. The fraudster can then pretend to be you, using this information to pass any security checks requested by your phone provider. The fraudster can then instruct your phone provider to route your phone number to the fraudster's SIM card.

The fraudster will then have access to any incoming calls and text messages, including one-time-passwords to gain access to your financial and social media accounts.

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

Call your network provider immediately. 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.

Inform your banks as soon as possible. The fraudster may attempt to make a money transfer online or over the phone and therefore have been alerted for any attempt for unauthorised transactions. You can also record your details with **Cifas**, the fraud prevention service.

How to protect yourself in the future?

Contact your network provider to secure your mobile account and ask what protection they offer to prevent this from happening again.

Don't respond to unsolicited emails, texts or phone calls. These may allow fraudsters to access personal data which can then be used to convince the mobile network provider or bank that they are you.

Don't overshare personal details on social media. Avoid sharing your birth date or that of children or relatives or other common password recovery phrases such as the name of your first pet or school.

Turn on Two Step Verification (2SV). Two-step verification (2SV), which is also known as two-factor authentication (2FA) or multi-factor authentication (MFA), helps to keep cyber criminals out of your accounts, even if they know your passwords.

Use a password consisting of three random words that only you will know and which are unique. You could add uppercase letters, numbers and symbols to make it more secure.

Always keep your device's software up to date.

METROPOLITAN POLICE