Devon and Cornwall ALERT

SIM-Swap Fraud

SIM-Swap Fraud: What You Need to Know

SIM-swap fraud is a clever and increasingly common type of crime where a criminal takes over your mobile phone number. They do this by tricking your mobile provider into switching your mobile phone number to a new SIM card that they control. Once they have your number, they can access your online accounts and steal your money and personal information.

How Does It Happen?

Scammers begin by gathering personal information about you from various sources, including social media, data breaches, and phishing attempts. With enough details, they contact your mobile provider pretending to be you. They might do this online, over the phone, or even in a store. Using your stolen information, they pass security checks and convince your mobile provider to transfer your mobile phone number to a new SIM card.

Once your number is affiliated to their SIM card, they receive all your calls and text messages. They can then try to log into your bank accounts, email, and social media. Since many of these services use one-time passwords (OTPs) sent by text message for verification, the scammer can easily receive these codes and gain access to your accounts.

How to Protect Yourself

- **Add Extra Security to Your Mobile Account:** Contact your mobile provider and ask what additional security measures you can add. Many providers allow you to set up a unique PIN or password that must be used to approve any changes to your account, whether in a store or over the phone.

- **Use Stronger Authentication:** Set up multi-factor authentication (MFA) on your email, social media, and bank accounts. While SMS-based verification is better than nothing, it's vulnerable to Sim-swap fraud. Wherever possible, choose more secure methods like passkeys or authenticator apps (like Google Authenticator or Microsoft Authenticator). Passkeys, in particular, are a great option as they are tied to a physical device rather than your phone number.

- **Review Your Online Presence:** Check your privacy settings on social media to control who can see your profile. Avoid sharing personal details like your date of birth, phone number, and information that could be used for security questions (e.g., your mother's maiden name or the name of your first school).

- **Recognize the Warning Signs:** If you suddenly lose service on your mobile phone or receive an unexpected message about a SIM transfer, act immediately. This could be a sign of a SIM-swap in progress.

- **Act Fast if You're a Victim:**

    - **Immediately contact your mobile provider.** Tell them your phone service has been hijacked.
    - **Alert your banks and financial institutions.** Call them right away to inform them of the suspected fraud so they can freeze your accounts. You can quickly reach many UK banks' fraud departments by calling **159**.
    - **Keep a close eye on all your accounts** (bank, credit card, email, social media) for any unusual activity.
    - **Change all your passwords** and, where possible, switch off SMS as an authentication method.
    - **Report the crime to Action Fraud.** You can report it online or by calling 0300 123 2040.