digital. FUTURES

What is SIM Swap Fraud?

SIM swap fraud might sound like something out of a spy movie, but it's actually a common scam that anyone with a phone number could face. In a SIM swap, a criminal tricks your mobile carrier into transferring your phone number to a SIM card they control. **Once they have your number, they can receive your calls and texts, including One-Time Passwords (OTP) Two-Factor Authentication (2FA) security codes meant to protect your accounts.**

Imagine someone quietly "borrowing" your phone number without ever touching your phone. That's the danger of a SIM swap. With access to your number, scammers may try to break into your email, social media, or even banking apps.

The good news? Understanding how SIM swap fraud works makes it much easier to spot suspicious activity and protect yourself.

Let's break it down in a clear, friendly way so you can stay one step ahead.

Supported by Rural Action Derbyshire in partnership with Digital Support Derbyshire.

Top Tips to Stay Safe

- **Protect your personal information:** never share important info like your, telephone number, address, full name, bank account details or passwords. Ignore unexpected requests for your details.
- **Set up a PIN or password with your phone provider:** ask your provider to set up a unique PIN or password on your account, needed to approve any account changes.
- **Use social media wisely:** avoid sharing details such as your phone number, date of birth, and answers to common security questions.
- **Monitor your accounts:** regularly check your bank accounts and credit reports for strange transactions or activities. Set up alerts for any significant changes to your accounts.
- **Set up biometrics:** visit My Security Profile in the help section of our Mobile App to add an extra level of security to your account.

How to spot SIM Swapping

Contact your phone provider and bank if you spot any of these signs:

- **Sudden loss of service:** if your phone suddenly loses service and you can't make or receive calls or texts, it could be a sign that a criminal moved your number to another SIM card.
- **Notifications of suspicious activity:** if you receive log in or SIM activation notifications which wasn't you, it could be a sign that criminals are trying to move your number to a new SIM.
- **Loss of access to your accounts:** if you can't access your email, bank, or social media accounts, it could be a sign that a criminal has taken control of them.
- **Unauthorised transactions:** if you spot payments on your account that you don't remember making, it could be a sign that a criminal has accessed your account.

SIM Swap Fraud Video:

NatWest Online – Bank Accounts, Mortgages, Loans and Savings. Available at: https://www.natwest.com/fraud-and-security/fraud-guide/sim-swapping-scams.html (Accessed: 06 February 2025).