FCC | CONSUMER CONNECTIONS

SIM Swapping



SIM swapping is when someone hijacks your mobile phone number to gain access to your texts and calls. Intercepting two-factor security messages can allow a thief to take over your financial and social media accounts.

Scammers gather enough personal information about their target to convince a mobile phone company to port the number to a device the scammer possesses. They may also steal a removable SIM card – which contains a unique ID that links to the account owner's phone number – from the victim's phone and use it to divert calls and texts to another device.

SIM Swapping

Increasingly, your mobile number is the key to accessing financial and social media accounts. Scammers that gain access to a victim's texts and calls can use two-factor codes to change login credentials, drain bank accounts, and sell or try to ransom social media accounts.

Loss of service on a device – the phone going dark or only allowing 911 calls – is typically the first sign of a SIM swap or port out scam.

Act Quickly

If you suspect you have been a victim of either SIM swap or port out, take immediate action:

- Contact your phone company.
- · Contact your bank and other financial institutions.
- · File a police report.

How to Protect Yourself

- Be proactive: Ask your phone company to add a PIN or a password to your account.
- Stay vigilant: Enable email and text notifications for important accounts.
- Don't overshare: Guard personal details that can be used to verify your identity, and keep that information off social media.

