SIM-Swap Fraud: Criminals Could Take Over Your Phone Number

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 number to a SIM card they control. Once they have your number, they can gain unauthorised access to 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 the provider to transfer your mobile phone number to a new SIM card.

Once your number is transferred to their SIM card, they receive your calls and text messages. They can then attempt to log in to your bank accounts, email accounts and social media profiles. Because many services use one-time passcodes (OTPs) sent by text message for security, criminals can intercept these codes and gain unauthorised 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, password or account passcode that must be provided before any changes can be made to your account.

Use Stronger Authentication

Enable multi-factor authentication (MFA) on your email, social media and financial accounts. Text message security codes can be vulnerable to SIM-swap fraud. Where available, consider using an authenticator app, such as Microsoft Authenticator or Google Authenticator, or even better, passkeys, which are linked to your device rather than your phone number.

Review Your Online Presence

Check your privacy settings on social media and limit the personal information you share publicly. Avoid posting information such as your date of birth, phone number, mother's maiden name, first school, or anything commonly used in security questions.

Recognise the Warning Signs

Be alert to:

- Unexpected notifications from your mobile provider about a SIM change or account update.
- A sudden loss of mobile signal or service.
- Being unable to make or receive calls or text messages.
- Unexpected requests to reset passwords.
- Losing access to accounts that usually verify your identity by text message.

If your mobile phone suddenly loses signal and does not recover after restarting your device, contact your mobile network provider immediately using another phone.

Act Fast if You Think You're a Victim

1. **Contact your mobile provider immediately.** Tell them you believe your phone number has been taken over or transferred without your permission.
2. **Alert your bank and financial institutions.** Ask them to place additional security measures on your accounts and monitor for suspicious activity. Many UK banks can be contacted through the **159** anti-fraud service.
3. **Check all of your accounts** including banking, email, social media and online shopping accounts for unusual activity.
4. **Change your passwords immediately** and, where possible, switch from SMS-based authentication to an authenticator app or passkeys.

Report the crime to Report Fraud, the UK's national reporting centre for fraud and cybercrime. Report online **UK's Home for Reporting Cyber Crime & Fraud - Report Fraud** or call **0300 123 2040**.

Remember

Your mobile phone number is often used as a key part of account security. Protecting it is just as important as protecting your passwords. If you unexpectedly lose mobile service or receive a notification about a SIM change that you did not request, act immediately. A fast response can help prevent criminals from gaining access to your accounts and personal information.

Reply Share Rate



Message Sent By
Mick Harrison
(Devon & Cornwall Police, Cyber Protect Officer, Devon & Cornwall)

Your Devon and Cornwall Community Messaging account...

My Local Area Message Preferences System Support Login Unsubscribe

---

You are receiving this message because you are registered on Devon and Cornwall Community Messaging. Various Information Providers (organisations) are licensed to send messages via this system. This message was sent by Devon and Cornwall Police and Devon and Cornwall Police does not necessarily represent the views of Devon and Cornwall Community Messaging or other Information Providers.

You can review the messages you receive, configure which Information Providers can see your information, or unsubscribe. You can also review our Terms and Conditions and Privacy Policy.

This email communication makes use of a "Clear Image"(gif) to track results of the email campaign. If you wish to turn off this tracking for future emails, you can do so by not downloading the images in the e-mail itself. All links in the body of this email are shortened to allow click through monitoring.

VISAV Limited is the company which built and owns the Neighbourhood Alert platform that powers this system. VISAV's authorised staff can see your data and is registered with the Information Commissioner's Office as the national Data Controller for the entire database. VISAV needs to see your data to manage the system and provide support; it cannot use it for commercial or promotional purposes.