





Spot the red flags of Mobile Phone Porting

Beat the scammers by knowing the scam

Mobile phone porting is when your mobile phone number is ported (transferred to a new telecommunications provider (telco') without your permission. Criminals may try to take control of your phone number by porting it to a new provider. They'll then be able to receive SMS authentication codes sent by your bank and other service providers. This allows them to authorize online banking transfers or change account details without your knowledge. Criminals can also use phone porting to gain control of email accounts, superannuation or government accounts, so they can access more personal information of transfer funds.

You can protect yourself by looking out for the signs below:

Spot the red flags

-  **Unexpected text messages.** Your mobile provider sends you a text message advising that “you” have requested your number be ported to a different network provider. This could indicate a criminal is trying to port your phone.
-  **SOS only.** Your mobile phone service is suddenly disconnected and may show “SOS only” where the carrier name usually appears on the screen. This could be a warning that your phone has been transferred to another provider without your authorization.



more
than
money



Stop, Check, Protect

to minimise your chance of being scammed



Stop before you act

If someone sends you a link, QR code or attachment – even if it looks like they're from someone you trust - **stop** to consider, could this be a scam?

If your phone service doesn't return in a short period, contact your mobile phone provider immediately to confirm why.

If your mobile has been transferred to another provider without your permission, contact your bank immediately.



Check before you share

If you're unsure if a message or call is legitimate, **check** the identity of the person who contacted before sharing any information. You can do this by contacting the organization directly using a publicly listed phone number.

Remove or hide personal information such as your date of birth, address and mobile number from social media accounts to protect your identity.



Protect if you suspect

Acting quickly if something doesn't feel right goes a long way in helping to **protect** your money and information. If you think you've been scammed or your banking details have been compromised, call us on **13 22 65** and ask for our Fraud team.

Find out more

Visit nab.com.au/security

For more tips on protecting yourself, visit nab.com.au/phoneporting

