

Mobile Phone Porting

Unauthorised Mobile Porting/SIM Swap

Criminals attempt to gain ownership of mobile numbers in order to access online accounts such as banking, email, superannuation, and government portals such as MyGov etc. Criminals do this in order to gain access to SMS codes (2-step verification) that we often have sent to our mobiles.

This may happen one of two ways:

- > 1. Unauthorised Mobile Porting – porting is a legitimate service that allows customers to transfer a mobile number from one telecommunication provider (telco) to another without changing or losing the original number. An Unauthorised Port occurs when a criminal contacts a different telephone provider, sets up an account with them and requests to have your number bought over from your provider.
- > 2. SIM Swap – the criminal will contact your existing provider and request to activate a new SIM card with your number.

Either way, once a mobile number has been successfully taken over, criminals will receive text messages containing password reset/verification codes (often referred to as 2SA or 2FA). This gives them access to your existing online accounts - banking and email accounts are major targets for such attacks.

Detection








A typical indicator of an Unauthorised Port/SIM Swap is the loss of phone coverage or reception of the affected mobile phone. SOS in this instance means that your network provider is no longer providing service to your device. Other common indicators in addition to your phone SOS display includes being locked out of accounts such as Internet banking, emails, or other services that rely on password reset/verification codes.

If you are connected to wifi at the time of the porting/SIM swap, emails from your financial institution referencing updates to your list of payees or funds transfers may indicate your number has been ported.







Please Note: If you receive a text from your mobile provider (or another telco) that your number is about to be ported, respond ASAP to the company who have sent the text as you may be able to stop the port.

Mobile Phone Porting

Prevention

-  Consider downloading your banking App onto your mobile device. Most bank Apps provide the ability to temporarily freeze your debit/credit cards.
-  See if your financial institution will provide you with a 'token' (a two-step authentication device) replacing the need to use your mobile number for security codes.
-  Make a list of accounts that send text messages to your mobile for security purposes. In the event of a port you will know which accounts to temporarily deactivate the affected number.
-  Do not treat your email account as data storage – periodically clean out your emails (inbox/outbox/sent and other folders).
-  Never provide personal details over the phone to unsolicited callers.
-  Do not click on links in emails or text messages until you verify validity.
-  Do not click on links in emails or text messages until you verify validity.

Responding to the scam

-  Freeze your online banking App or call your financial institution(s) immediately and alert them of the risk
-  Temporarily disable SMS as a password reset/verification code recovery method (or temporarily change the number) for online accounts. Start with email account.
-  Contact your telecommunication provider and find out if your number has been ported to another provider or if there has been a fraudulent SIM Swap.
-  If the number was ported, request your telco submit a 'reversal of an unauthorised port'
-  If you experienced a SIM Swap tell your provider to shut down the active SIM and provide you with a replacement SIM, then tighten security as a prevention.
-  Repeated attempts - Use a separate prepaid SIM card to set up all of your online accounts with that is not attached to your main phone number.

Disclaimer © 2018 Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this FACT SHEET, IDCARE disclaims any liability to any person in respect to any actions performed or not performed as a result of the contents of the alert or any accompanying data provided. Note our service is free to the community and our Counsellors will never ask you to provide your personal information and credentials if we make contact with you.

