

Introduction

Criminals attempt to gain ownership of mobile numbers in order to receive SMS codes (two-factor authentication) to facilitate password resets and gain access to online accounts such as banking, email, superannuation, and myGov. **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 to another. An unauthorised port occurs when a criminal contacts a different telephone provider, sets up an account with them and requests to have your number brought over from your current provider to the new provider they have established an account with.
2. **SIM swap** – the criminal contacts your existing provider and requests the activation of a new SIM card with your number. This transfers your number to the criminal's device without needing to change the telco provider (unlike porting).

Once a mobile number has been successfully taken over, criminals will receive your text messages, including those containing password resets and verification codes. Banking and email accounts tend to be major targets.

Prevention checklist

- ☐ Use multi-factor authentication wherever possible, including using authenticator apps, touch ID, Face ID or biometrics as part of account access requirements.
- ☐ Consider downloading your banking App onto your mobile device. Most banking apps provide the ability to temporarily freeze your accounts and cards.
- ☐ Check if your financial institution has multi-factor authentication options that do not rely on using your mobile number for security codes.
- ☐ Make a list of accounts that send text messages to your mobile for security purposes.
- ☐ 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.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Detection checklist

- ☐ A typical indicator of an unauthorised port or SIM swap is an SOS message on your mobile phone, indicating a loss of phone coverage or reception. SOS in this instance means that your network provider is no longer providing service to your device. Other common indicators include being locked out of accounts such as Internet banking, emails, social media, or other services that rely on password reset or verification codes.
- ☐ You may also begin to receive emails welcoming you to your new telecommunications provider, or from financial institutions notifying you of updates to your contact details or other account details. Or you may find that you are no longer able to access your email, banking or other online accounts as the passwords have been changed.

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

Response checklist

- ☐ Freeze access to your bank accounts via your banking app and call your financial institution(s) immediately to alert them to the risk, and request increased security on your accounts.
- ☐ Disable SMS as a password reset or verification code recovery method (or change the contact 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 telecommunication provider 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.
- ☐ Request from the telecommunication provider what credentials were used by the criminal to allow the port or SIM swap to occur.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Response Checklist cont.

Notify the relevant document issuing organisations for any of the credentials that the scammer may have accessed. Common credentials include:

- ☐
 - Driver licence
 - Passport (Australian passports contact [DFAT](#) on 131 232, for NZ passports contact [DIA](#) on 0800 22 50 50)
 - Medicare card (Contact the Scams and Identity Theft Helpdesk on 1800 941 126, Monday to Friday, 8am to 5pm or email reportascam@servicesaustralia.gov.au)
 - ATO details (Australian residents call 1800 467 033) or IRD details (NZ residents call 0800 257 777)
 - RealMe details (NZ residents call 0800 664 774 or online at [RealMe](#))
 - Bank account details, including login information

- ☐ Contact all [Credit Reporting Agencies](#) for your free credit reports and to arrange credit bans.

- ☐ Update or add passwords to all accounts, apps, and websites requiring logins.

- ☐ Check if forwarding rules have been changed on your email accounts.

Report any fraud that has occurred as a result of the port or SIM swap to the police. You can alert police through:

- ☐
 - [ReportCyber](#) (in Australia)
 - Call 105 or submit a report [online](#) and choose "Report a Police non-emergency" (in New Zealand)

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 160 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.