



Spriggy Mobile Porting Fraud

How we protect your child's Spriggy Mobile number from fraudulent porting

Porting is when a mobile number moves from one provider to another. Sometimes scammers try to "port" a mobile number. That's tech speak for moving a number to a different phone company. If a scammer gets your child's number, they can receive their calls and texts, including security codes for things like bank accounts.

How your number is protected

To protect you from unauthorised ports, an extra identity check is always done before any mobile number is moved to a new provider. Usually a one-time code is sent to the phone that has the number. The number can't move until the check is passed.

Once a number is ported away, the Spriggy Mobile service ends automatically.

Signs your child's number may have been ported

- Your child's phone suddenly shows no signal or "SOS only", and restarting it doesn't help
- Your child stops getting calls or texts
- Your child gets a code or message about moving their number that nobody asked for

If you think the number has been ported without your permission

Act straight away:

1. **Contact us:** contact Spriggy Member Help through in-app chat in the Spriggy app, or email support@spriggy.com.au. We're available 9am to 5pm, 7 days a week, and 10am to 4pm on NSW public holidays (AEST/AEDT).
2. **Report it to the police:** contact the Australian Federal Police or your state or territory police.
3. **Report it to support services:**
 - IDCARE, Australia's identity and cyber support service: idcare.org or 1800 595 160
 - Scamwatch: scamwatch.gov.au

You should also contact your bank and change passwords for any accounts that send security codes to your child's phone, or to yours if you've linked your number.

Handy tips to keep your child's number safe

Teach your child to never share a code sent to their phone, even if the person asking seems friendly or says they're from Spriggy. We'll never ask for it.

Keep your child's mobile number off social media and gaming profiles.

Use a strong, different password for each account, and turn on two-step verification.

Don't use your child's number as the security phone number for your own bank or email accounts.

Better safe than sorry!