SECURITY · INCIDENT ANALYSIS 2026

The Twilio Breach, in Two Pages

In 2022 a text message pretending to be IT support got attackers inside a major communications platform. What happened, why the codes failed, and what to change in your business.

What happened

Date	Event
29 June 2022	A voice phishing call compromises one employee. Limited customer contact details viewed.
Late July	Staff get texts "from IT": password expired, schedule changed. Links to lookalike sign-in pages.
4 August	Twilio detects intruders using stolen employee credentials.
9 August	Last unauthorised activity observed.
Final count	**209 customer accounts** accessed, 93 Authy users with devices added, around 1,900 Signal users exposed.

Why the one-time codes did not help

The fake page passed each username, password and code to the attackers the moment it was typed, and they used it on the real site before it expired. **Any method where a person reads a code and types it somewhere can be relayed like this**: SMS codes, app codes and, with some variation, push prompts.

Same texts, different outcome

Cloudflare received near identical messages. 76 staff targeted, 3 typed their credentials into the fake page, **0 accounts compromised**. Its staff used FIDO2 hardware keys, which only answer the real website. People will be fooled. Whether that becomes a breach is up to you.

Why the text worked

- **A trusted sender.** Staff distrust strangers. They cooperate with IT.
- **A plausible deadline.** An expired password or a changed shift is routine and urgent.
- **A familiar address** like twilio-sso.com, half hidden on a phone screen.
- **A perfect copy** of the real sign-in page. Nothing for a careful person to notice.

The supply chain lesson

- Signal chose Twilio. **Signal's users carried the consequences.**
- Your provider holds your numbers, routing, message logs, recordings and sender identity.
- Whoever gets into its support tools can reach your customers in your name.
- Choosing a communications provider is choosing part of your own security.

Ranking sign-in methods

Method	Stops a relayed phishing page?	Use it for
SMS code	No	Low risk only. Never email, finance or admin.
Authenticator code	No	A step up from SMS, still relayable.
Push approval	Partly	Turn on number matching.
Passkey	**Yes**	Default for all staff where supported.
FIDO2 key	**Yes**	Admins, finance, phone system settings.

Three rules for staff

- **IT never texts a sign-in link.** Make it true, then say so.
- **Go to the site yourself.** Never follow the link to check.
- **Report it, even if you clicked.** Minutes matter.

Australia in 2026

- Sender ID Register mandatory from 1 July 2026.
- Scams Prevention Framework puts duties on telcos.
- ACMA identity checks before SIM swaps and ports.
- Notifiable breaches can still land on you.

Thirty days

1. **Week 1.** List every system still using SMS codes. Brief staff on the three rules.
2. **Week 2.** Hardware keys for admins and anyone with finance or phone system access. Two keys each.
3. **Week 3.** Passkeys for everyone. Remove SMS fallback. Send your provider the ten questions.
4. **Week 4.** Add a second check for high value customer changes. Confirm your sender ID is registered.

What your provider holds, and who gets hurt

Held by the provider	In an intruder's hands
Numbers and routing	Calls and codes diverted to someone who is not you
Message logs and recordings	Customer details read, and a Privacy Act problem for you
Your sender identity	Texts that look genuinely from your business

Ask your provider

How do your staff sign in? Who can see my messages and recordings, and is it logged? How do you verify me before a port? Where is my data, and how many other companies handle my calls and texts? **Does every API endpoint require authentication?** The 2024 Authy exposure of 33 million numbers came from one that did not.