SECURITY DEEP DIVE · 2026

How One Text Breached a Telco Platform

The 2022 Twilio hack as a chain of six ordinary steps, the company that got the same texts and lost nothing, and what an Australian business should change this month.

The chain, link by link

1. **A text reaches a personal mobile.** "Your password has expired." Assume it will arrive.
2. **The link opens a copy of the sign-in page** on a lookalike domain. Break it with a rule: IT never texts sign-in links.
3. **Password and code are relayed** to the real site in real time. Break it with passkeys or hardware keys.
4. **Attackers reach internal tools.** Break it by limiting who can reach admin tools.
5. **They search for specific customers.** Break it with access logs someone watches.
6. **The customers' own users are exposed.** Break it by choosing providers carefully.

The numbers

Figure	What it means
209	Twilio customer accounts accessed, out of 270,000+
93	Authy users with unauthorised devices added
~1,900	Signal users with numbers or registration codes exposed
5 days	Detection on 4 August to last activity on 9 August 2022

What Twilio got right, and worth copying

- **It noticed** within days, not months.
- **It said so publicly** three days after detection, and updated the numbers as they changed.
- **It fixed the root cause** by issuing FIDO2 hardware keys to all staff, not just more training.
- **It tightened the edges:** VPN and admin tool controls, more frequent re-authentication.

The company where nothing happened

Cloudflare got the same texts. 76 staff targeted, 3 entered credentials, **no account compromised**, because its staff used FIDO2 keys that only answer the real site. Stop measuring whether anyone clicks. Measure whether a click can do damage.

You are somebody's Signal

Signal's users never chose Twilio. Signal did. Your customers never chose your phone and SMS provider either. **If its support tools are compromised, someone may read your messages, redirect your number or text your customers as you.** Keep the chain short and ask how each link protects its own staff.

What an SMS code really proves

Assumed	Actually
The right person	Someone could read texts to this number a few minutes ago
Our real site	Nothing. A fake page can relay it
Phone in their hand	Some SIM has the number. After a SIM swap, not theirs

This month

- Brief staff: go to the site yourself, report even if you clicked.
- List systems still on SMS codes.
- Hardware keys for admins and finance.
- Send your provider the scorecard.

This quarter

- Passkeys for all staff.
- Remove SMS fallback.
- Cut phone system admin rights.
- Second check on high value customer changes.

SIM swaps and the Australian rules

ACMA rules require telcos to run multi-factor identity checks before SIM swaps, number ports and account changes. That has cut the easy attacks, not all of them. **Business numbers that receive codes for banking, accounting or domains are worth more to an attacker than a personal mobile.** Know which accounts send codes where, and move the important ones off SMS.

Score your provider, two points per clear yes

- Phishing-resistant sign-in for staff tools? Access to my data logged and limited?
- ACMA identity checks before ports and SIM changes? Named hosting country and operator?
- How many companies handle my traffic? Written incident notice timeframe?
- **Every API endpoint authenticated?** The 2024 Authy leak of ~33 million numbers came from one that was not.
- Can I restrict routing changes? Is support in-house and trained to refuse unverified urgency?