

PHONE SECURITY 2026

AI Voice Cloning: Protecting Your Business Phones

Voice cloning has crossed the point where people can no longer reliably tell. That retires the oldest verification control in business. Here is what replaces it, in language you can hand to your finance team this afternoon.

For a century, "I recognised their voice" was a perfectly reasonable way to verify who you were talking to. **That control is now retired.** Industry reporting through 2025 and 2026 describes voice cloning as having crossed the point where human listeners cannot dependably distinguish synthetic from real, from samples as short as a voicemail greeting or a few sentences of a webinar. Vishing volumes reportedly surged sharply through 2025 as a result. Four patterns dominate in Australia: **executive impersonation** for urgent payments, **IT helpdesk impersonation** for credential resets, **supplier bank-detail changes**, and **customer impersonation** aimed at your own staff. Do not train people to detect fakes, they can't, and false confidence is worse than none.

■ The short version

Capability	What it does for you	Why it has to be in place first
Call recording	Turns "I think he said.." into an artefact your bank, insurer and investigators can act on	You cannot retrospectively record a call that already happened
AI transcription & search	Lets you check whether the same pretext was attempted on other staff, how you spot a campaign, not an incident	Untranscribed audio is effectively unsearchable at volume
Centralised number screening & blocking	Block or flag a hostile number for the whole business in one change, rather than device by device	Per-handset blocking does not scale during a live campaign
Verified business identity outbound	Makes it harder for your brand to be used against your own customers	Sender identity registration is not an emergency lever

■ Key points

- 1. Executive impersonation
- 2. IT helpdesk impersonation
- 3. Supplier bank-detail change
- 4. Customer impersonation

A note on the figures in this article

The percentages above come from published industry and vendor reporting on 2025, 2026 attack volumes rather than from our own measurement, and different sources define and count these incidents differently. Treat them as indicative of a clear direction rather than precise. The direction is not in dispute, and the controls in this article are worth adopting whether the true figure is 100% or 500%.

■ Questions the full guide answers

- ☐ How much of someone's voice does an attacker need to clone it?
- ☐ Can staff be trained to detect a cloned voice?
- ☐ What is the single most effective control against voice cloning fraud?
- ☐ Why do these attacks work on sensible people?
- ☐ How does a business phone system help defend against vishing?
- ☐ What should we do in the first hour after a suspected voice-cloning attack?
- ☐ Does the Scams Prevention Framework mean our telco will stop these calls?

This is the summary. The guide has the detail.

Every point above is worked through in full on our site, with the Australian context, the numbers and the exceptions. If you would rather talk it through, call **1300 881 662** or visit **unidenvoice.com/get-started**.