PHONE SECURITY 2026

AI Voice Cloning and the End of It Sounded Like Him

Voice cloning has crossed the point where people can't reliably tell. That retires the oldest verification control in business.

> "I recognised their voice" was a reasonable way to verify someone for about a hundred years. **It isn't any more.** Reporting through 2025. 2026 describes voice cloning as having passed the point where people can reliably distinguish synthetic from real, built from samples as short as your own voicemail greeting, with vishing volumes surging sharply as a result. Four plays dominate here: **executive impersonation** for an urgent payment, **IT helpdesk impersonation** for a credential reset, **supplier bank-detail changes**, and **customer impersonation** aimed at your own helpful staff. Do *not* train people to spot fakes: they can't, and the false confidence makes things worse.

The short version

Play	How it runs	Why it lands	The control that stops it
Executive impersonation	Cloned owner or director rings finance with an urgent payment that must bypass approval	Hierarchy plus urgency; often aimed at a junior rather than the CFO	Callback to a held number + dual authorisation
IT helpdesk impersonation	"Support" walks a staff member through a password reset, an MFA approval, or remote access	Staff are trained to comply with IT quickly and without fuss	Absolute rule: never approve codes or credentials by voice
Supplier bank-detail change	A familiar supplier contact advises new account details before an invoice falls due	Looks like routine admin, not an emergency, so it triggers no alarm	Bank changes verified by callback, actioned by a second person
Customer impersonation	Cloned customer asks *your* staff for an address change, account detail, refund redirect or goods release	Your team is trained to be helpful, that's the vulnerability	Verification steps on outbound-facing changes too

Also worth knowing

Capability	What it actually buys you	Why it must be on beforehand
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	Reveals whether the same pretext hit three other staff, campaign vs incident	Untranscribed audio is effectively unsearchable at volume
Centralised screening & blocking	Block or flag a hostile number business-wide in one change	Per-handset blocking doesn't scale during a live campaign
Verified outbound identity	Makes your brand harder to weaponise against your own customers	Sender ID registration isn't an emergency lever
Onshore data	Evidence stays under the Privacy Act rather than in a jurisdiction you reason about mid-incident	Hosting location is decided at signup, not at 5pm on a Friday

About those figures

The percentages come from published industry and vendor reporting on 2025. 2026 attack volumes, not from our own measurement, and different sources count these incidents differently. Read them as direction rather than precision. The direction isn't disputed by anyone, and every control below is worth adopting whether the real number is 100% or 500%.

Questions the full guide answers

- [ ] Is my voice already out there for someone to clone?
- [ ] Shouldn't we train staff to recognise a fake voice?
- [ ] What is the one control that stops most of this?
- [ ] Can we trust caller ID to confirm who is calling?
- [ ] How does a cloud phone system help with this?
- [ ] What do we do in the first hour if we think it has happened?
- [ ] Doesn't Australian regulation already block scam 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 663 222** or visit **vocphone.com/about/contact-us**.