CYBERSECURITY WHITEPAPER

# Deepfakes, Voice Cloning and AI-Powered Scams

A Defence Guide for Regional & Remote Australia

EmergeIT

**Artificial intelligence has made scams faster to produce, cheaper to scale and far harder to spot. This guide explains how AI-powered attacks work, why regional and remote organisations are squarely in scope, and the practical controls that make the biggest difference.**

## Introduction

Tasks that once demanded skill, time and fluent written English can now be automated and scaled, and the results are far more convincing than the scams Australian businesses learned to recognise a few years ago. For small and medium enterprises (SMEs) in Darwin, Katherine and across regional and remote Australia, this shift carries real weight. Lean teams, heavy reliance on cloud services and distance from specialist support combine to make AI-enabled fraud one of the most pressing risks of 2026. This guide sets out how these attacks work, why regional organisations are firmly in scope, and the controls that deliver the most protection for the least effort.

## The New Threat Landscape

Cybercrime in Australia is widespread and still growing. In its Annual Cyber Threat Report 2024-25, the Australian Signals Directorate (ASD) recorded more than 84,700 cybercrime reports, roughly one every six minutes, and its Australian Cyber Security Centre responded to over 1,200 serious incidents, an 11 percent increase on the previous year.[1] Over the same period, the average self-reported cost of cybercrime to business rose by around 50 percent to $80,850 per incident.[1]

What has changed is not only the volume of attacks but the method behind them. Generative AI now lets criminals write flawless phishing emails, clone a person's voice from a few seconds of audio, and generate live deepfake video on a conference call. Industry reporting through 2025 put Australian business losses to AI-enabled scams at around $2.03 billion, part of an estimated $2.18 billion lost to scams nationally across the year.[2,3] The familiar advice to watch for spelling mistakes and suspicious logos no longer offers much protection, because AI erases the very signals staff were trained to notice.

## How AI-Powered Attacks Work

Three techniques are responsible for most of the damage to Australian businesses today.

- **AI-written phishing and business email compromise (BEC).** Email compromise remains the single most reported threat to Australian businesses and accounts for roughly 15 percent of business cybercrime.[1] AI lets attackers write fluent, context-aware messages that convincingly imitate a supplier or a manager, then redirect an invoice payment to a fraudulent account.
- **Voice cloning (vishing).** With only a short audio sample, often scraped from a webinar, video or voicemail, attackers can clone a person's voice and telephone a staff member to "authorise" an urgent payment or password reset.
- **Deepfake video.** The most alarming cases involve live or recorded deepfake video of a senior leader on a call, instructing an employee to move money or share credentials. In one widely reported global case, an employee transferred millions after a video meeting in which every other participant was AI-generated.

## Why Regional and Remote Organisations Are Exposed

A persistent myth holds that attackers only pursue large city corporates. The evidence points the other way. Automated, AI-assisted attacks do not discriminate by postcode; they target whoever is reachable and underprotected. Councils, health services, not-for-profits and businesses across the Northern Territory and South Australia hold valuable data and money, frequently with leaner IT resources than their metropolitan counterparts. Smaller teams also mean fewer people available to cross-check an unusual request, while reliance on cloud platforms and external vendors widens the attack surface. That combination is exactly what opportunistic, AI-enabled criminals look for.

## Seven Practical Defences

Deepfakes cannot be un-invented, but a few disciplined controls make your organisation a much harder and far less rewarding target. The following steps map closely to the ASD Essential Eight, the baseline that local managed IT providers such as Emerge IT implement every day.

1. **Enforce multi-factor authentication (MFA) everywhere.** Phishing-resistant MFA stops most credential-based attacks even when a password has been stolen.
2. **Introduce a verbal-verification protocol for money and credentials.** Any request to change bank details, pay an unusual invoice or reset access must be confirmed through a known, separate channel, never by replying to the original message.
3. **Train your people on AI-era threats.** Regular, scenario-based user training that now includes deepfakes and voice cloning turns staff into a genuine first line of defence.
4. **Lock down email.** Modern filtering, domain protection (DMARC, DKIM and SPF) and Microsoft 365 hardening sharply reduce successful phishing and BEC.
5. **Keep systems patched and applications controlled.** Two Essential Eight pillars that close the doors attackers rely on.
6. **Maintain tested, offline backups.** If the worst happens, clean and verified backups are the difference between a bad day and a business-ending event.
7. **Have an incident response plan, and rehearse it.** Knowing who to call and what to do in the first hour limits the damage and helps meet tightening regulatory reporting obligations.

## Conclusion

AI has handed criminals a powerful new toolkit. It has not changed the fundamentals of good security, but it has raised the stakes for getting them right. Organisations that combine the Essential Eight, sensible verification habits and ongoing user training are well placed to absorb these attacks. The hardest part for a lean regional team is doing all of it consistently, which is where a local managed partner earns its place.

### How Emerge IT can help

Emerge IT is a managed IT and cybersecurity partner built for regional and remote Australia. We implement the Essential Eight, harden Microsoft 365, deliver practical user training, and stand alongside your team if an incident occurs. For a personalised Essential Eight assessment, get in touch.

**Phone** 1300 348 287 (1300 EIT AUS)

**Email** hello@emergeit.com.au · **Web** www.emergeit.com.au

**Serving** Darwin, Katherine, Northern Territory, South Australia & Regional Australia

**REFERENCES**

1. Australian Signals Directorate, Annual Cyber Threat Report 2024-25. cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025
2. SecurityBrief Australia, “Australian businesses lose AUD $2.03 billion as AI scams surge,” 2025. securitybrief.com.au
3. SBS News, “Australians are reporting fewer scams but losing more,” 2025. sbs.com.au