Waterstons
we're with you

+44 345 094 0945
www.waterstons.com

Article

Feb 2026

The growth of attacks on Aussie charities

In July 2025, Heart Research Australia confirmed it had been the target of a cyber incident involving its online donation website.

Craig Archdeacon
Director - APAC

Email craig.archdeacon@waterstons.com

The issue wasn't discovered because systems failed or alarms went off, but because malicious code had been quietly placed on a public-facing part of the charity's site.

To donors, everything could have looked normal; the donation page still worked, the charity's name and branding were unchanged – but that was precisely the point. The attack was designed to blend in, not disrupt.

Once the issue was identified, the charity acted quickly, removing the malware notifying the relevant authorities. There was no evidence that donor data had been accessed or stolen and, from a technical perspective, the response was effective.

But the real impact of an incident rarely ends when the code is removed. And for charities, the aftermath is often quieter and longer-lasting than other sec.

Time must be spent rebuilding confidence - spent reassuring supporters, reviewing systems and answering difficult questions. Even with confirmation that no data was compromised, uncertainty lingers, donors are more cautious and volunteers ask more questions. Trust, once shaken, takes time to fully recover.

What makes this incident particularly important is what has happened since.

Although the Heart Research Australia attack was reported publicly in July, similar issues have continued to surface across the charity and not-for-profit sector in the months that followed. Email accounts have been taken over, social media pages have posted unauthorised messages, and supporters have received donation requests that just didn't quite feel right.

In many cases, organisations only became aware after someone outside the charity raised a concern.

These incidents reflect a broader shift in how cyberattacks are being carried out. Rather than locking systems or demanding ransoms, attackers are increasingly focused on impersonation and quiet access - a short window of control over a trusted charity account can be enough to redirect funds, mislead supporters, or cause reputational harm.

Charities are not being targeted because they are careless, but because they are trusted.

In many cases, access is gained in unremarkable ways; a work email address reused years earlier to sign up for an unrelated service, or a familiar password used across multiple platforms for convenience. When an external service suffers a breach, those details can be exposed and quietly tested elsewhere. If they work, the attacker doesn’t need to break in - they simply log in.

Once inside, everything they do looks legitimate, because it is coming from a real account.

The Heart Research Australia incident wasn’t an isolated event. It was an early signal of a pattern that has continued since; one where charities of all sizes are finding that their digital identity is now part of the frontline.

The good news is that many of these incidents are preventable, and prevention doesn’t require complex technology or large budgets. It comes down to a few basic habits done consistently.

Organisations should:

- Make sure work accounts are only used for work purposes – using charity credentials to sign up for unrelated platforms creates invisible links that attackers can exploit later.
- Implement MFA for important accounts such as email, social media, and donation platforms should have an extra step when logging in, which stops a large proportion of account takeovers.
- Assume that unusual messages will happen at some point and make it easy for staff, volunteers, and supporters to question them. The earlier something feels ‘off’ and is raised, the smaller the impact tends to be.

Cyberattacks on charities are no longer rare, dramatic events. They are now regular, often quiet, subtle, and human in nature. Understanding that reality - and responding to it early - is now part of protecting not just systems, but the causes and communities charities exist to serve.