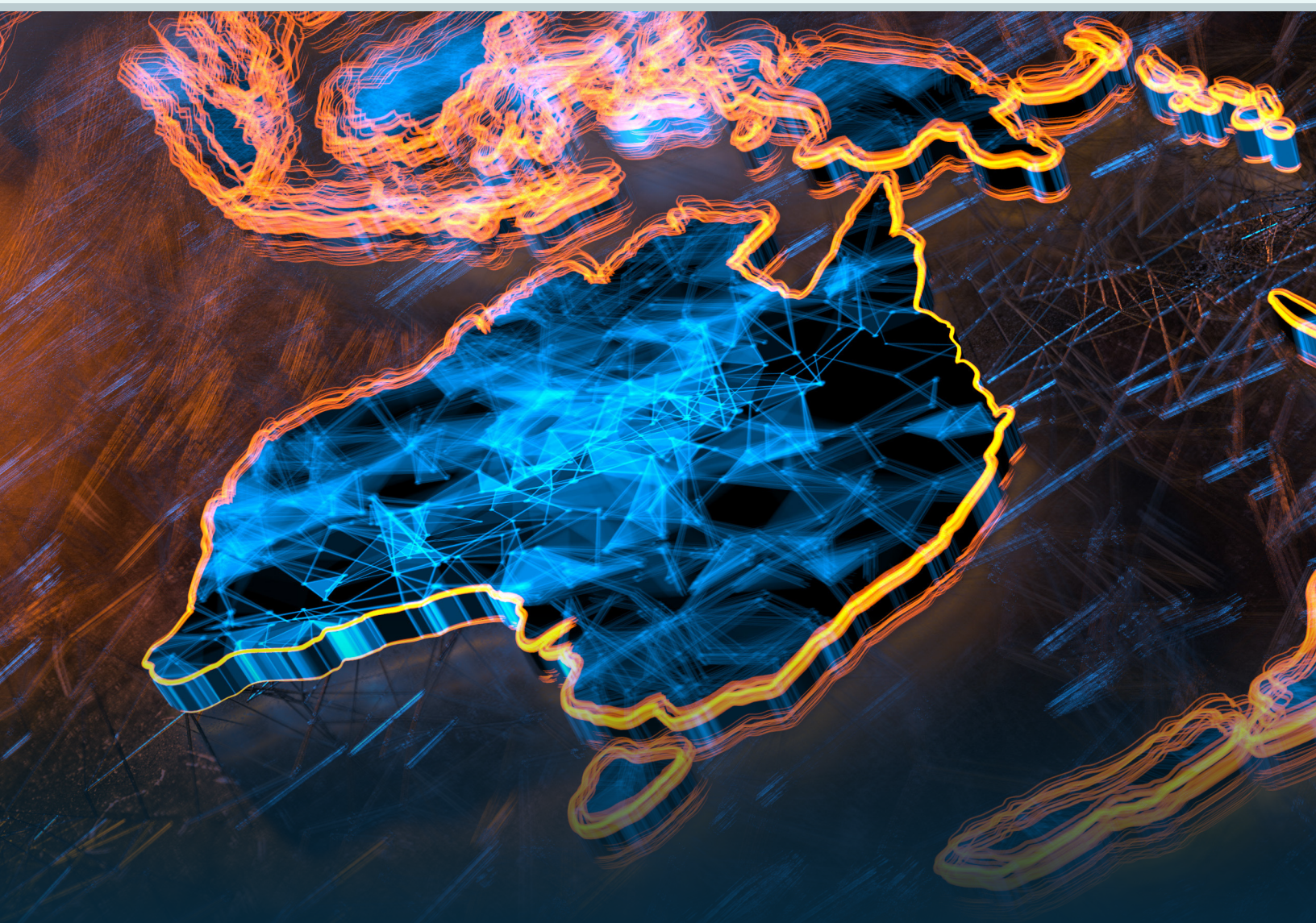
knowbe4

Australia's Cybersecurity Paradox: Strong Defences, Weak Habits

Why over reliance on tech makes Australians vulnerable



WWW.KNOWBE4.COM

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | Email: Sales@KnowBe4.com

0557 0226

53% of employed Australians put more thought and effort into protecting work accounts over personal accounts

The Complacency Crisis Beneath Australia's Cyber Defences

From a technological perspective, Australia's cybersecurity infrastructure has never been more sophisticated. However, this advanced technology appears to have lulled citizens into a false sense of security. With millions of Australians remaining passive in the face of cyber threats.

Even with a stream of headlines about data breaches affecting major organisations, according to KnowBe4 research, one in four Australians do nothing to protect themselves unless directly notified they've been compromised... and even then they may not be entirely sure as to what they need to do.

KnowBe4's lead CISO advisor, Javvad Malik, states: "People focusing on securing work accounts more than personal accounts reflects policy, not culture. True human risk management is when people take what they learn into their personal lives."

New research by KnowBe4, drawing from a nationally representative YouGov survey of 524 Australians (October 2025), reveals a striking paradox at the heart of Australian behaviour. While three-quarters of these respondents feel knowledgeable and confident about identifying cyber threats, the survey data shows widespread risky practices persist: Two-thirds of respondents reuse passwords across multiple accounts, and the findings estimate that six million Australians never check if their personal information has been exposed in known breaches, while an estimated 4.6 million Australians are comfortable sharing login credentials for sensitive accounts with friends, family, or colleagues.

Perhaps most tellingly, employed Australians admit they put significantly more thought and effort into securing work accounts than personal ones. This reveals that security behaviours are driven by organisational policy and compliance requirements rather than internalised security culture.

This context sets the stage for the rest of the report, which examines how Australians actually respond to data breaches, how they manage passwords and account security, and the critical gap between workplace and personal cybersecurity practices. These findings highlight a critical truth: technology alone cannot secure organisations. Instead, the path forward requires comprehensive Human Risk Management (HRM) to drive genuine, culture-driven behaviour change that employees carry into their personal lives.

Key Findings from Australia

53%

Of employed Australians put more thought and effort into protecting work accounts over personal accounts

66%

Two in three Australians reuse passwords across multiple online accounts

24%

One in four Australians take no action after hearing about a major data breach unless directly notified

21%

More than one in five Australians are comfortable sharing login credentials for sensitive accounts such as email or banking

76%

Feel confident identifying phishing emails, while risky behaviours remain widespread

How Australians React to Data Breaches

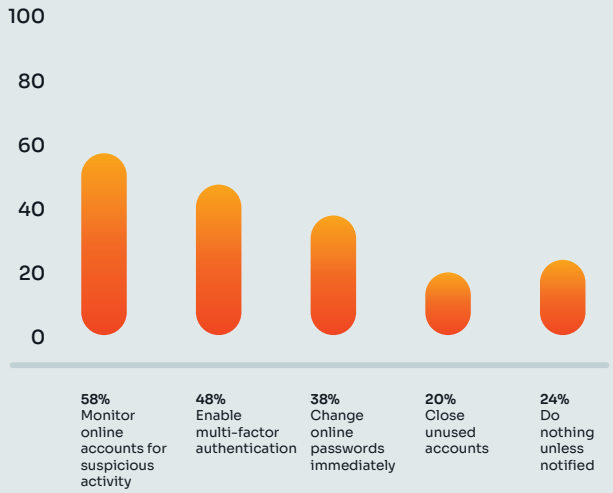
High-profile breaches have increased awareness, but not always action. When Australians hear about a major data breach affecting the public, three in four (76%) take some form of security action. The most common responses include:

- Monitoring accounts for suspicious activity (58%)
- Enabling multi-factor authentication (48%)
- Changing passwords (38%)

However, a significant minority — an estimated 5.2 million Australians — do nothing unless directly notified that they are affected. This passive response highlights a reliance on external prompts rather than proactive personal security habits.

Generational differences are stark. Baby Boomers (38%) are more than twice as likely as Gen Z (16%) to take no action unless notified, while Millennials (62%) are three times as likely as Boomers (20%) to immediately change passwords following a breach.

Actions Australians Take After Hearing About a Major Data Breach



Passwords, Convenience and Risky Normalisation

Despite years of awareness campaigns, password reuse remains deeply ingrained.

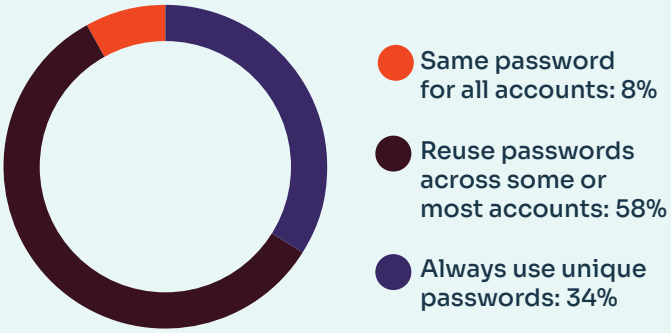
Two-thirds of Australians (66%) admit to using the same password, or a variation of it, across multiple online accounts. Approximately 1.8 million Australians use the same password for all accounts.

While Gen X is more likely than younger generations to use unique passwords, working Australians are significantly more likely to reuse passwords than retirees — a concerning signal given their exposure to corporate systems.

This normalisation of risky behaviour extends beyond passwords. One in five Australians are comfortable sharing login credentials for sensitive accounts such as email or banking, and one in three share credentials for entertainment services.

This data point is particularly telling because it highlights a significant usability gap in current security solutions. While password managers are widely available, they still remain a "black box" for many non-technical users. When security tools become too complex for users, they instinctively default to risky habits that offer immediate convenience.

Password Reuse Among Australians



Confidence vs. Reality: The Phishing Gap

Although most Australians believe they can spot a phishing attack, their actual practices show a gap between confidence and security.

Three in four Australians (76%) say they are confident in identifying phishing emails, and 70% say the same for phishing via social media.

Yet KnowBe4's research shows that email remains the primary attack vector globally, with phishing responsible for the majority of account takeover incidents. In Australia and New Zealand, sustained security awareness training has been shown to reduce phishing susceptibility by up to 78% over time.

This disconnect underscores a core Human Risk Management challenge: perceived competence can mask real behavioural risk.

24%

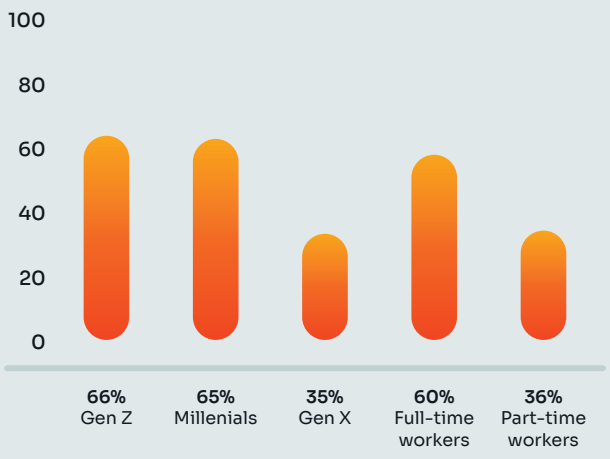
After hearing about a major data breach that affects Australians, 1 in 4 Aussies say they do nothing unless directly notified.

Work Accounts vs. Personal Accounts: A Policy-Driven Divide

The most revealing finding in this research is how Australians prioritise security differently depending on context.

Among employed respondents, 53% say they put more thought and effort into protecting work accounts over personal ones. This rises to 66% among Gen Z and 65% among Millennials, and to 60% among full-time workers.

Australians Who Prioritise Securing Work Accounts Over Personal Accounts



This behaviour suggests that security actions are driven by organisational policy, training mandates and enforcement, not by internalised security values. When those structures disappear outside the workplace, secure behaviours often disappear with them.

From Awareness to Human Risk Management

KnowBe4's State of Human Risk report consistently shows that organisations struggle not with awareness, but with behaviour. Globally, 96% of cybersecurity leaders say they find it challenging to secure the human element, and only 16% have a well-established Human Risk Management program.

HRM represents a shift from one-size-fits-all training to a data-driven, personalised approach that measures individual risk, delivers just-in-time coaching, and reinforces secure behaviour at the moment of action.

For Australian organisations, the message is clear; if security behaviours only exist at work, they are fragile. True resilience is achieved when employees carry secure habits into their personal digital lives, reducing risk everywhere.

Building a Security Culture That Travels Home

Australians are not indifferent to cybersecurity. They respond to breaches, express confidence in spotting threats, and demonstrate strong security behaviours — when policy demands it.

The challenge for organisations is to convert policy-driven compliance into culture-driven behaviour. This requires making security personal to them, so they take it home and share those secure habits with others.

Human Risk Management provides the framework to do exactly that: aligning security with how people actually behave, and ensuring that lessons learned at work protect individuals and organisations everywhere. By personalising risk and celebrating secure decisions, an HRM approach transforms policy into a genuine, internalised security culture that extends naturally into an employee's personal digital life; where they not only adopt secure practices themselves, but also share with their family and friends.

Methodology

This report is based on an independent online survey conducted by YouGov between 17–20 October 2025 among 524 Australians aged 18 and over. Data was weighted by age, gender and region to reflect ABS population estimates. The study was conducted in accordance with ISO 20252:2019 standards.

Free Phishing Security Test

Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Email Exposure Check

Find out which of your users emails are exposed before bad actors do

Free Automated Security Awareness Program

Create a customized Security Awareness Program for your organization

Free Domain Spoof Test

Find out if hackers can spoof an email address of your own domain

Free Phish Alert Button

Your employees now have a safe way to report phishing attacks with one click

About KnowBe4

KnowBe4 empowers workforces to make smarter security decisions every day. Trusted by over 70,000 organisations worldwide, KnowBe4 helps to strengthen security culture and manage human risk. KnowBe4 offers a comprehensive AI-driven "best-of-suite" platform for Human Risk Management, creating an adaptive defence layer that fortifies user behaviour against the latest cybersecurity threats. The HRM+ platform includes modules for awareness and compliance training, cloud email security, real-time coaching, crowdsourced anti-phishing, AI Defence Agents and more. As the only global security platform of its kind, KnowBe4 utilises personalised and relevant cybersecurity protection content, tools and techniques to mobilise workforces to transform from the largest attack surface to an organisation's biggest asset. For more information, please visit www.KnowBe4.com.

knowbe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com