KnowBe4

Phishing Benchmarking Report

AUSTRALIA AND NEW ZEALAND 2025

Shining a light on human risk and reducing phishing click rates

Reducing phishing risk is central to effective human risk management (HRM).

Every successful phishing attack relies on a trusted person to carry out a specific action, such as clicking on a hyperlink. If a phishing email gets through technical defences, it will still fail if the recipient subsequently reports, deletes or does not engage with it.

While enhancing their technical defences with an AI-powered anti-phishing product, organisations can also significantly reduce their phishing risk through best-practice security awareness training (SAT).

The first step to any effective risk mitigation strategy is to understand your organisation's risk profile and how it compares against others of the same industry, organisational size and geographical region. Next, identify how susceptible your organisation actually is to phishing risk and, in particular, who might interact with a phishing email. These insights will enable you to deliver timely and personalised security, such as bespoke training programmes and real-time coaching.

KnowBe4's Phishing by Industry Benchmarking Report provides the initial step in this strategy. For this year's report, we analysed a total of 67,718,305 phishing simulations across 14,508,441 users in 62,460 organisations over a three-year period to show the Phish-prone™ Percentage (PPP) for organisations across 19 industries and seven geographical regions.

This guide provides an overview of the key findings for Australia and New Zealand.

How we calculate the Phish-prone Percentage

The PPP is the percentage of employees within an organisation who are likely to fall for social engineering or phishing attacks. Elsewhere, you might see it described as 'phishing simulation click rate'.

Phase one

Baseline phishing security test results

Before any KnowBe4 training takes place, we send an initial phishing simulation. This is used to identify risks and calculate an organisation's baseline PPP.

Phase two

Phishing security test results within 90 days of training

Employees receive KnowBe4's security awareness training. Another simulation is sent to recalculate the organisation's PPP and measure the effectiveness of the training programme.

Phase three

Phishing security test results after one year-plus of ongoing training

After 12 months of KnowBe4's security awareness training, the PPP is calculated again to further quantify the effectiveness of the training programme.

2025 international phishing benchmarks

Across the different regions, the highest baseline PPPs were found in South America (39.1%), North America (37.1%) and Australia and New Zealand (36.8%).

Organisations with 1,000+ employees based in Australia and New Zealand were the most phish-prone globally, with 44.6% clicking on simulated phishing hyperlinks. The lowest risk was found in small organisations (1–249 employees) in both Asia and the United Kingdom and Ireland, with a quarter (24.3%) of employees clicking links.

All regions achieved average improvement rates over 80%, with North America the highest (89.5%) and South America a close second (88.9%).

		Phase one – Baseline			Phase two – 90 days			Phase three – 1 year+		
	Organisation size	**1–249 employees**	**250–999 employees**	**1,000+ employees**	**1–249 employees**	**250–999 employees**	**1,000+ employees**	**1–249 employees**	**250–999 employees**	**1,000+ employees**
Region	**North America**	26%	31.1%	42%	21.1%	21.2%	18.5%	3.7%	3.9%	4.1%
		TOTAL: 37.1%			**TOTAL: 19.6%**			**TOTAL: 3.9%**		
	Africa	27.9%	30.1%	35.8%	24.9%	28%	20%	2.2%	9.2%	5.1%
		TOTAL: 34.9%			**TOTAL: 21.1%**			**TOTAL: 5.3%**		
	Asia	24.3%	27.6%	29%	18.9%	19.1%	17.6%	5.1%	4.5%	5.4%
		TOTAL: 28.6%			**TOTAL: 17.9%**			**TOTAL: 5.2%**		
	Australia and New Zealand	25%	29.2%	44.6%	23.2%	23%	16.6%	3.9%	6.1%	4.7%
		TOTAL: 36.8%			**TOTAL: 19.9%**			**TOTAL: 4.9%**		
	Europe	24.9%	26.7%	34.9%	20.7%	21.6%	20.5%	3.9%	4.4%	5.3%
		TOTAL: 32.5%			**TOTAL: 20.7%**			**TOTAL: 5%**		
	South America	30.2%	26.3%	42.8%	23.3%	23.1%	16.9%	3.4%	5.1%	4.5%
		TOTAL: 39.1%			**TOTAL: 18.2%**			**TOTAL: 4.5%**		
	United Kingdom and Ireland	24.3%	28.5%	36%	22.1%	22.1%	17.1%	4%	4.1%	5.3%
		TOTAL: 32.9%			**TOTAL: 19%**			**TOTAL: 4.8%**		

Australia and New Zealand | *By Javvad Malik*

The PPP data across Australia and New Zealand presents a compelling narrative of improvement across industries and company sizes. Initially, large companies of 1,000+ exhibited the greatest vulnerability to phishing attacks globally, with the highest baseline PPP in 2024 at 44.6%. In particular, this risk was elevated in sectors such as banking and financial services.

Medium and small companies, while generally less vulnerable, still demonstrated significant risk, especially in consumer services and banking, with 30% or more phish-prone employees.

However, the implementation of robust SAT programmes yielded significant results. After just 90 days, most sectors observed substantial reductions in their PPP, with banking showcasing a particularly dramatic improvement of 90.4%. The most striking changes occurred after a year or more of training, where the majority of industries across all company sizes achieved single-digit PPP rates. This finding underscores the long-term effectiveness of sustained cybersecurity education.

Notably, the data highlighted interesting industry-specific trends and anomalies. The legal sector, for instance, maintained a consistently low PPP throughout all phases, while consumer services persistently showed higher vulnerability. Some sectors, such as technology and government, exhibited slight increases in PPP for large companies in the final phase, suggesting potential areas for focused training.

The overall trend, however, was clear: ongoing cybersecurity awareness programmes significantly enhanced an organisation's resilience against phishing attacks, regardless of its size or industry. This improvement was particularly pronounced in larger companies, which, despite starting with higher vulnerability, often demonstrated the most substantial risk reduction over time.

Australia and New Zealand	Phish-prone Percentage		
Organisation size	**Phase one – Baseline**	**Phase two – 90 days**	**Phase three – 1 year+**
1–249	25%	23.2%	3.9%
250–999	29.2%	23%	5.3%
1,000+	44.6%	5.3%	4.7%
Average PPP across all organisation size ranges	**36.8%**	**19.9%**	**4.9%**

Evolving threat trends in Australia and New Zealand

Australia and New Zealand have emerged as focal points for significant trends and challenges that underscore the evolving nature of cyber threats and defence mechanisms. The Australian Cyber Security Centre (ACSC) and New Zealand's National Cyber Security Centre (NCSC) have been at the forefront of addressing these challenges, providing critical insights into the cybersecurity posture of the region.

A PPP between 3–5% after one year of SAT is the gold standard.

The expanding attack surface in Australia

One of the most pronounced trends observed in 2024 was the increasing sophistication and frequency of cyberattacks targeting critical infrastructure. These sectors, including electricity, gas, water and waste services, alongside education and training, and transport, postal and warehousing, were identified as particularly vulnerable.

The ACSC's engagement, having answered over 36,700 calls through the Australian Cyber Security Hotline, underscored the heightened concern and proactive measures being adopted by organisations across the spectrum. This proactive stance was further evidenced by the response to over 1,100 cybersecurity incidents, with a notable increase in ransomware attacks, signalling a shift in tactics by cyber adversaries.

The introduction of the Cyber Security Act 2024 in Australia marked an important step forward by setting new benchmarks for smart device security and establishing mandatory reporting mechanisms for ransomware payments. This legislative action demonstrated the government's commitment to addressing the evolving cyber-threat landscape and protecting critical infrastructure.

The Australian government's dedication to enhancing cybersecurity awareness through the Cyber Security Awareness Support for Vulnerable Groups grants programme signalled a significant milestone in the nation's approach to digital safety. By allocating nearly AUD $7 million to over 200 recipients, the government demonstrated a profound understanding of the critical role that community-level education plays in building a resilient cyber ecosystem.

Collaboration works to combat threats

Across the Tasman Sea, New Zealand's cybersecurity challenges largely mirrored those of Australia. A report by CERT NZ (Computer Emergency Response Team) revealed that over 3,500 cyber incidents were reported in the first three-quarters of the year alone, marking a 15% increase from the previous year. These incidents encompassed a range of attacks – from phishing and ransomware to more sophisticated advanced persistent threats (APTs).

Both countries have recognised the importance of international collaboration in addressing cyber threats. The Five Eyes intelligence alliance, comprising Australia, New Zealand, the United States, the United Kingdom and Canada, has played a crucial role in sharing threat intelligence and coordinating responses to global cyber incidents. This collaborative approach has proven essential in tackling sophisticated state-sponsored attacks and transnational cybercrime networks.

How quickly can an organisation pivot to create new training content that simulates real-word threats as the attacks that they face change?

Closing the cyber skills gap

Australia and New Zealand have both intensified their efforts to build a skilled cybersecurity workforce to meet the growing demand for expertise in this field. Initiatives such as the 2023–2030 Australian Cyber Security Strategy and New Zealand's Cyber Security Strategy 2019 have emphasised the need for developing talent pipelines, promoting cyber education in schools and supporting reskilling programmes for professionals who are transitioning into cybersecurity roles.

Ticking compliance boxes once a year is not the same as improving security in day-to-day operations.

Key lessons

- **Sustained cybersecurity training significantly reduces phishing vulnerability across all industries and company sizes**, with large companies showing the most dramatic improvements over time.
- **Critical infrastructure sectors face increasingly sophisticated cyberattacks,** prompting legislative action and increased government support for cybersecurity awareness and defence mechanisms.
- **International collaboration, particularly through the Five Eyes alliance, and investments in building a skilled cybersecurity workforce are crucial strategies** adopted by both countries to address evolving cyber threats and build long-term resilience.

For more information, visit KnowBe4.com

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 Australia and New Zealand | Part Level 1, 95 Coventry Street, Southbank, VIC, 3006 Australia
+61 (1800) 577568 | www.KnowBe4.com | Sales@KnowBe4.com

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Copyright © 2025 KnowBe4 All rights reserved.