# AI-driven phishing attacks surge with Australia among top targeted countries in 2024



The recent release of Zscaler’s ThreatLabz 2025 Phishing Report reveals a concerning rise in sophisticated, AI-driven phishing attacks, with Australia identified as one of the top ten most targeted countries globally. Analysis of over two billion blocked phishing attempts in 2024 pinpointed a significant shift in tactics among cybercriminals. These attackers are moving away from broad, indiscriminate phishing emails to more precise assaults on critical business departments, including IT, human resources, finance, and payroll. This evolution highlights a remarkable utilisation of artificial intelligence, which enables the creation of realistic and convincing phishing lures.

While the overall volume of phishing attempts has reportedly decreased by 20% worldwide—thanks in part to stricter email authentication protocols—this decline has not deterred attackers. Instead, they have adapted by launching more targeted campaigns, particularly in digitally evolving markets with lesser investments in security measures, such as Brazil, Hong Kong, and the Netherlands. Despite these trends, Australia remains a formidable target: it was hit by over 30 million phishing attempts last year, securing the eighth position globally in phishing activity.

Heng Mok, Zscaler's CISO-in-Residence for the Asia Pacific and Japan, noted, "Australian organisations must remain vigilant to the evolving cyber threats that have become increasingly sophisticated with the support of AI." This assertion is reinforced by findings from the Australian Cyber Security Centre, which indicates that the rise of AI has not only enabled automated spear-phishing techniques but also enriched social engineering tactics through the use of deepfake technology. A notable case study included in their 2023-2024 Annual Cyber Threat Report described an incident where AI-generated deepfakes manipulated an employee into authorising a fraudulent financial transaction during a video call.

Another critical aspect of this ongoing threat is the targeting of corporate executives, who are particularly vulnerable due to their broad access and decision-making power. Attackers increasingly utilise deepfake voice and video technology to enhance their social engineering strategies, making the identification of fraud more challenging for organisations. This trend extends across various platforms as cybercriminals are not confined to traditional email avenues; they are employing social media channels like Facebook, Telegram, and Steam for impersonation, malware delivery, and information gathering.

Zscaler’s report also highlights a burgeoning trend termed "Phishing-as-a-Service," leveraging AI to generate counterfeit websites and personalised phishing messaging at an unprecedented scale. This further complicates the landscape, as attackers mimic legitimate AI tools to trick users into disclosing sensitive information. Complementing these insights, Trend Micro's findings indicate that Australia's cyber threat landscape remains both substantial and alarming, with nearly 72 million email threats identified in the first half of 2024 alone.

In response to these heightened threats, Zscaler advocates for a robust security posture involving Zero Trust architecture combined with advanced, AI-driven phishing prevention methods. This multi-layered approach aims to minimise attack surfaces, prevent initial breaches, mitigate insider threats, and safeguard sensitive data. The findings underscore an urgent call to action for Australian businesses to embrace enhanced cybersecurity measures, especially as 91% of organisations are planning to increase their cybersecurity budgets by 2025 in response to the growing prevalence of AI-powered threats.

As the battle against cybercrime intensifies, the adoption of proactive, sophisticated security strategies will be essential in defending against the rapidly evolving landscape of phishing attacks.

## Reference Map:

* Paragraph 1 – [[1]](https://itbrief.com.au/story/ai-driven-phishing-attacks-surge-against-australian-targets-in-2024), [[4]](https://www.insurancebusinessmag.com/au/news/cyber/australia-ranks-among-top-10-global-sources-of-phishing-attacks-491170.aspx)
* Paragraph 2 – [[1]](https://itbrief.com.au/story/ai-driven-phishing-attacks-surge-against-australian-targets-in-2024), [[2]](https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024), [[3]](https://www.zscaler.com/press/zscaler-research-finds-60-increase-ai-driven-phishing-attacks)
* Paragraph 3 – [[2]](https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024), [[6]](https://vitg.com.au/the-new-frontier-of-cybercrime-understanding-ai-driven-threats-and-their-impact-on-australian-organisations/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://itbrief.com.au/story/ai-driven-phishing-attacks-surge-against-australian-targets-in-2024> - Please view link - unable to able to access data
2. <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024> - The Australian Cyber Security Centre's Annual Cyber Threat Report 2023-2024 highlights the increasing use of artificial intelligence (AI) by cybercriminals, noting that AI enables more efficient and large-scale spear-phishing activities. The report also discusses the emergence of AI-driven social engineering attacks, such as deepfake voice impersonations, which can circumvent traditional network defenses. A case study within the report details a vishing scam where AI-generated deepfakes were used to deceive an employee into transferring millions of dollars during a video conference call.
3. <https://www.zscaler.com/press/zscaler-research-finds-60-increase-ai-driven-phishing-attacks> - Zscaler's press release reveals a 60% year-over-year increase in AI-driven phishing attacks, as detailed in their ThreatLabz 2024 Phishing Report. The report highlights the rise of voice phishing (vishing) and deepfake phishing, with the United States, United Kingdom, India, Canada, and Germany being the top five countries targeted. The finance and insurance industry experienced a 393% increase in phishing attacks, and Microsoft remained the most impersonated brand, with 43.1% of phishing attempts targeting it.
4. <https://www.insurancebusinessmag.com/au/news/cyber/australia-ranks-among-top-10-global-sources-of-phishing-attacks-491170.aspx> - An article from Insurance Business Australia discusses the rise in AI-driven phishing attacks, referencing Zscaler's report that Australia experienced over 29 million phishing attempts, placing it among the top ten countries targeted globally. The report also notes a 479% year-over-year surge in phishing content hosted in Australia. The finance and insurance sector saw a 393% increase in phishing attacks, and Microsoft continued to be the most impersonated brand, with 43% of incidents involving the company.
5. <https://www.trendmicro.com/en_au/about/newsroom/press-releases/2024/09-11-2024.html> - Trend Micro's mid-year roundup report for H1 2024 reveals that Australia encountered nearly 72 million email threats and ranked among the top ten countries for URL victims, with 21.6 million detections, representing 2.5% of global detections. The country also ranked eighth globally in mobile app detections, with approximately 24.3 million unique queries, including about 16,703 malicious apps. These statistics underscore the significant volume of cyber threat activity monitored in Australia.
6. <https://vitg.com.au/the-new-frontier-of-cybercrime-understanding-ai-driven-threats-and-their-impact-on-australian-organisations/> - An article from VITG discusses the impact of AI-driven cybercrime on Australian organisations, noting that in 2024, more than 50% of Australian businesses reported experiencing a cyberattack, with 36% of these being AI-generated. The surge in AI-powered phishing scams, deepfake fraud, and automated hacking has pushed cybersecurity concerns to the top of the agenda for Australian organisations. The article also highlights that 91% of businesses plan to increase cybersecurity spending by 2025 to address these evolving threats.
7. <https://www.zscaler.com/press/zscaler-threatlabz-uncovers-surge-ai-driven-cyberattacks-targeting-critical-business> - Zscaler's press release discusses the surge in AI-driven cyberattacks targeting critical business operations, as detailed in their 2025 Phishing Report. The report reveals that while global phishing volume dropped by 20% in 2024, attackers shifted strategies to focus on high-impact campaigns targeting IT, HR, finance, and payroll teams. The report also highlights the use of community-based platforms like Facebook, Telegram, Steam, and Instagram for phishing campaigns, and the rise of Phishing-as-a-Service enabled by AI technology.