KnowBe4

# 2023 PHISHING BENCHMARKING

## For Australia and New Zealand

*By **Jacqueline Jayne**, Security Awareness Advocate for the Asia-Pacific region for KnowBe4*

With the root cause of the majority of data breaches being traced to the human factor, security leaders who continue to invest solely on technology-based security layers run the risk of overlooking a best practise proven to reduce their vulnerability: security awareness training coupled with frequent simulated social engineering testing. This approach both helps raise the readiness level of humans to combat cyber crime and lays the critical foundation necessary to drive a strong security culture.

With geopolitical changes affecting the dynamics of cyber crime, organisations ought to reduce their single biggest cyber risk: the human element. Cybercriminals are counting on your employees lacking the necessary knowledge, attention and energy to trick them into making bad security decisions. One over-stressed, distracted, or daydreaming employee is all you need to let the bad actors in.

Security leaders need to know what happens when their employees receive phishing emails: are they likely to click the link? Get tricked into giving away credentials? Download a malware-laced attachment? Will they simply ignore the email or delete it without properly notifying their security team? Or will they report the suspected phish and play an active role in the human defence layer?

Each organisation's employee susceptibility to these phishing attacks is known as their Phish-prone™ Percentage (PPP). By translating phishing risk into measurable terms, leaders can quantify their breach likelihood and adopt training that reduces their human attack surface.

To assist geographical regions with evaluating their PPP and understanding the implications of their ranking, KnowBe4 conducts an annual study to provide definitive Phish-prone benchmarking across small, medium and large organisations by geographical regions. This guide provides an overview of the key findings for Australia and New Zealand.

### 2023 Global Phishing By Industry Benchmarking Study

Though every organisation would like to understand how they measure against the rest in their industry and geography, the comparison requires robust data coupled with a scientific, proven method to produce valid results. To provide a nuanced and accurate answer, the 2023 Phishing By Industry Benchmarking Study analysed a data set of over 12.5 million users, across 35,681 organisations, with over 32.1 million simulated phishing security tests, across 19 different industries and seven geographic regions.

All organisations were categorised by size and geographical region. To calculate each organisation's PPP, we measured the number of employees who clicked a simulated phishing email link or opened an infected attachment during a testing campaign using the KnowBe4 platform.

### In our 2023 report, we continue to look at the following three benchmark phases:

#### PHASE ONE

**If you have not trained your users and you send a phishing attack, what is the initial resulting PPP?**

To do this, we monitored employee susceptibility to an initial baseline simulated phishing security test. From that established set of users, we look at any time a user has failed a simulated phishing security test prior to having completed any training.

#### PHASE TWO

**What is the resulting PPP after your users complete training and receive simulated phishing security tests within 90 days after training?**

We answered this question by finding when users completed their first training event and looking for all simulated phishing security events up to 90 days after that training was completed.

#### PHASE THREE

**What is the final resulting PPP after your users take ongoing training and monthly simulated phishing tests?**

To answer this, we measured security awareness skills after 12 months or more of ongoing training and simulated phishing security tests, looked for users who completed training at least one year ago, and took the performance results on their very last phishing test.

## 2023 International Phishing Benchmarking Results By Geographical Regions

**Phase One**
Initial Baseline Phishing Security Test Results

**Phase Two**
Phishing Security Test Results Within 90 Days of Training

**Phase Three**
Phishing Security Test Results After One Year-Plus of Ongoing Training

| | BASELINE | | | 90 DAYS | | | 1 YEAR | | |
|---|---|---|---|---|---|---|---|---|---|
| **Organisation Size** | **1-249** | **250-999** | **1000+** | **1-249** | **250-999** | **1000+** | **1-249** | **250-999** | **1000+** |
| **North America** | 28% | 30.1% | 37.1% | 18.5% | 19% | 18.4% | 4.2% | 5.1% | 5.7% |
| | **TOTAL: 33.1%** | | | **TOTAL: 18.6%** | | | **TOTAL: 5.1%** | | |
| **Africa** | 30% | 29.4% | 33.3% | 25.2% | 22.7% | 19.3% | 9% | 10.5% | 5.7% |
| | **TOTAL: 32.8%** | | | **TOTAL: 20.5%** | | | **TOTAL: 6.6%** | | |
| **Asia** | 32.6% | 33.2% | 28.8% | 20.9% | 19.6% | 13% | 7.3% | 7.4% | 6% |
| | **TOTAL: 30%** | | | **TOTAL: 14.9%** | | | **TOTAL: 6.5%** | | |
| **Australia & New Zealand** | 27.1% | 30.9% | 41.1% | 21.1% | 19.9% | 15.3% | 6.3% | 7.7% | 5.4% |
| | **TOTAL: 34.8%** | | | **TOTAL: 17.8%** | | | **TOTAL: 6.4%** | | |
| **Europe** | 26.5% | 28% | 36.2% | 19.1% | 19.7% | 19.4% | 6.7% | 7.6% | 6.1% |
| | **TOTAL: 32.9%** | | | **TOTAL: 19.4%** | | | **TOTAL: 6.5%** | | |
| **South America** | 34% | 27.7% | 49.5% | 23% | 25.8% | 18.7% | 6.4% | 10.2% | 5.1% |
| | **TOTAL: 41.1%** | | | **TOTAL: 21.3%** | | | **TOTAL: 6.9%** | | |
| **United Kingdom & Ireland** | 26.3% | 28% | 39.6% | 18.5% | 18.1% | 17.6% | 6.1% | 8.1% | 4.9% |
| | **TOTAL: 35.2%** | | | **TOTAL: 17.8%** | | | **TOTAL: 5.8%** | | |

## Most Prevalent Issues Facing Australia and New Zealand

### *AUSTRALIA*

As with previous years, phishing reigned supreme as the most successful attack vector for cybercriminals, with their highest success using ransomware, fraud, financial and identity theft and business email compromise (BEC).

The Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report, received over 76,000 cyber crime reports, or one report every seven minutes. This is a 13% increase from the previous year, with 67,500 reports.

In the period July 1, 2022 to December 31, 2022, the Office of the Australian Information Commissioner (OAIC) shared in their notifiable data breach report that notifications were up 26%, with the top five sectors to notify data breaches being Health service providers with 71 reports, Finance (including superannuation) with 68 reports, Insurance with 42 reports, Legal, Accounting and Management Services with 37 reports and Recruitment agencies with 35 reports. Contact information remains the most common type of personal information involved in breaches.

### *NEW ZEALAND*

According to CERT NZ, in 2022, 8,160 incidents were reported, an 8% decrease from 2021. Individuals, small organisations and large organisations from all over New Zealand submitted incident reports.

When they looked at the top incidents, phishing and credential stuffing increased 16% from 2021, scams and frauds increased 15% from 2021, and unauthorised access has increased by 23% from 2021. Interestingly, malware reports decreased by a record 88% since 2021, with the primary reason being the overwhelming amount of FluBot malware reported in that year.

Privacy and data retention has emerged as a major issue with a recent high profile data breach that saw over one million New Zealand records being obtained by cybercriminals.

| AUSTRALIA & NEW ZEALAND | BASELINE | 90 DAYS | 1 YEAR |
|---|---|---|---|
| 1-249 | 27.1% | 21.1% | 6.3% |
| 250-999 | 30.9% | 19.9% | 7.7% |
| 1000+ | 41.1% | 15.3% | 5.4% |
| Average PPP Across All Organisation Sizes | 34.8% | 17.8% | 6.4% |

## Economic Impact

### *AUSTRALIA*

According to the Australian Competition and Consumer Commission (ACCC), Australians reported losses of a staggering AUD $526,292,444 to scams in 2022 (up from AUD $323 million in 2021). Remember that these are only the reported scams to the ACCC, with the potential for the total to be significantly higher.

From a business perspective, the ACSCs Annual Cyber Threat Report also noted that the average cost per cybercrime report increased to over AUD $39,000 for small businesses, AUD $88,000 for medium businesses and over AUD $62,000 for large businesses. Financial losses due to BEC increased to over AUD $98 million, with Australian businesses self-reporting an AUD $33 billion loss due to cybersecurity incidents nationwide.

### *NEW ZEALAND*

New Zealand banks report customers lost a **combined total of NZD $183.5 million to scams this year** (2022)—an increase of 40% from last year (2021).

According to the **2021/2022 Cyber Threat Report from the National Cyber Security Centre**, the National Cyber Security Centre prevented NZD $33 million worth of harm to New Zealand's nationally significant organisations. Plus, "23% of the 350 recorded incidents showed indications of a connection to criminal or financially motivated actors."

## Typical Organisation Profiles

### *AUSTRALIA*

As of June 30, 2022, 2,569,900 organisations were operating in Australia, dominated by small and medium enterprises (SMEs). Breaking down the SMEs to 97.5% small organisations (0-19 employees) and 2.3% as medium organisations (20-199 employees), with the remaining 0.2% of organisations in Australia having more than 200 employees as defined by the **Australia Bureau of Statistics**.

### *NEW ZEALAND*

As of Feb 2022, **New Zealand had 592,700 enterprises across the region**. Small enterprises hold the majority with 97.13% and have between 0 and 19 employees, 1.85% with 20 to 49 employees, 0.57% with 50 to 99 employees and 0.45% with 100+ employees.

## Cultural Adoption and General Attitudes

### *AUSTRALIA AND NEW ZEALAND*

Data breaches hit the headlines in 2022, with millions of Australians' and New Zealanders' data being caught up in significant incidents. This has seemingly had little impact on how IT decision makers view the risks to their organisations. In our most recent survey of that cohort in the region, **we found that 37% of Australian** and **32% of New Zealand IT decision makers** say they are concerned about phishing as a risk to their organisation. Considering the extremely high success rate for cybercriminals using phishing attacks to gain entry to organisations, this percentage should be much higher.

## Key Takeaways

When we consider the responses to who is responsible for cybersecurity, it's clear that IT leaders and organisations across Australia and New Zealand are looking for guidance regarding security issues. There is still much work to be achieved in relation to the following:

- ✓ Educating everyone about basic cyber hygiene must be top of the agenda to bring awareness
- ✓ Providing consistent guidance and support to all organisations regardless of their size, as they are all a target
- ✓ Implementing ongoing relevant and engaging security awareness training supported with ongoing simulated phishing emails will shift us to the desired outcomes

**Download The 2023 Phishing By Industry Benchmarking Report** DOWNLOAD