KnowBe4

2023 PHISHING BENCHMARKING

Report for Asia

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 Asia.

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 Asia

The 2023 IBM X-Force Threat Intelligence Index reported that "the Asia-Pacific region faced the most cyber attacks during 2022 and that the region accounted for 31% of all incidents monitored in 2022."

Japan was the frontrunner with Emotet malware attacks in 2022. The Japanese National Police Agency reported that the number of cyber crimes hit an all time high in 2022 with 12,369 cases (up from 160 in 2021).

Reports across the region involving extortion are on the rise via business email compromise (BEC) and distributed denial-of-service attacks (DDOS).

According to the 2022 Thales Data Threat Report, APAC Edition, 45% of respondents reported an increase in the number of attacks and interestingly, 77% said they would trust their organisation with their own personal data. As with the rest of the world, data breaches are prevalent with 50% of respondents reported that they have experienced a data breach and 32% of those breaches occurred in 2022.

As we can see the overall Phish-prone Percentage across all organisation sizes is close to the global percentages. It is encouraging to see the larger organisations with 1000+ employees leading the way by scoring better than the overall regional percentages. This could be attributed to the fact that the larger organisations have an IT department and more than likely a cybersecurity team. These two factors tend to result in a greater understanding of the cyber threat landscape and therefore more of a focus on the need to upskill end users to make better decisions.

Economic Impact

In The State of Financial Crime 2022: Key Takeaways for Asia Pacific Firms, the UN Office on Drugs and Crime (UNODC) reported a 600% rise in cyber crimes in the region.

From a Southeast Asia perspective (Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam), PWCs Global Economic Crime and Fraud Survey 2022 reported that two thirds of incidents involved employees and of those, 34% had lost less than $50,000, 10% lost between $1 million and $5 million, while 9% lost more than $5 million.

ASIA	BASELINE	90 DAYS	1 YEAR
1-249	32.6%	20.9%	7.3%
250-999	33.2%	19.6%	7.4%
1000+	28.8%	13%	6%
Average PPP Across All Organisation Sizes	30%	14.9%	6.5%

Typical Organisation Profile

The Asia-Pacific region has a population of 4.3 billion. With over 10 countries, it is one of the world's most diverse regions and home to economies that are at the top of digital and societal developments worldwide. Organisational profiles will be shared across sole ownership, small to medium organisations and enterprise organisations all with the same challenges as every organisation globally.

Cultural Adoption and General Attitudes

We have looked for general observations across the entire Asian region and found, via the 2022 Thales Data Threat Report, APAC Edition, that the era of remote working will continue, as will the risks associated with it. Security risks of remote employees continued in 2022 with 33% of respondents "very concerned" and 47% "somewhat concerned."

Key Takeaways

There is still much work to be achieved in relation to the following:

- ✓ There is strength in numbers, and the private and public sectors will need to collaborate across the region
- ✓ All organisations need consistent guidance and support 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 help bring the desired outcomes

Download The 2023 Phishing By Industry Benchmarking Report ▸ DOWNLOAD