KnowBe4

Phishing Benchmarking Report

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

While enhancing their technical defenses with an AI-powered anti-phishing product, organizations 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 organization's risk profile and how it compares against others of the same industry, organizational size and geographical region. Next, identify how susceptible your organization actually is to phishing risk — and, in particular, who might interact with a phishing email. These insights will enable you to deliver timely and personalized security, such as bespoke training programs and real-time coaching.

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

This guide provides an overview of the key findings for Asia.

How We Calculate Phish-prone Percentage

The PPP is the percentage of employees within an organization 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 organization’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 organization’s PPP and measure the effectiveness of the training program.

Phase Three

Phishing Security Test Results After One Year+ of Ongoing Training

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

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 & New Zealand (36.8%).

Organizations 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 organizations (1-249 employees) in both Asia and the United Kingdom & Ireland, with one-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+		
	Organization 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 & 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 & 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%**		

Asia | *By Caroline Soo and Bex Bailey*

Organizations in Asia that invest in best-practice security awareness training and phishing simulations reduce their click rate by an impressive 81.8%. This is a welcome trend in a region that experiences a higher rate and cost of breaches. In its 2024 Breach Benchmarks By Region report, Forrester highlights that organizations in Asia Pacific (APAC) experienced an average of 3.5 breaches within a 12-month period versus a global average of 2.8. They also experienced a cumulative cost of US$2.8 million against the global mean of US$2.7 million.

As phishing is so often the gateway for cybercriminals, driving down this risk is key to organizational security.

Before taking part in security training, 28.6% of employees in Asia clicked on a simulated phishing link. In keeping with the global trend, this risk increased based on organizational size. Those with 1-249 employees had the lowest risk (24.3%), which increased to 27.6% for 250-999 employees and 29% for 1,000+ employees.

After 90 days of training, this risk reduces considerably — dropping to an average of 17.9%. Larger organizations see the greatest improvement at this stage, with those having 1,000+ employees obtaining an average click rate of 17.6%. After one year of training, this risk hits its lowest level at an average 5.4%.

Insurance organizations experience the highest initial click rate in the region at 43.6% — 15% above the regional average. Other sectors with elevated risk include Banking (39.1%), Education (37.9%), Hospitality (36.7%) and Nonprofits (33%).

Of these industries, Hospitality experiences the most significant risk reduction after one year of best-practice training, with click rates decreasing by 94.8%. The decrease in risk is similarly impressive for the other sectors: Nonprofits (88.5%), Education (82.8%), Banking (79.8%) and Insurance (63.8%).

Asia	Phish-prone Percentage		
Organization Size	**Phase One - Baseline**	**Phase Two - 90 Days**	**Phase Three - 1 Year+**
1-249	24.3%	18.9%	5.1%
250-999	27.6%	19.1%	4.5%
1,000+	29.0%	17.6%	5.4%
Average PPP Across All Organization Sizes	**28.6%**	**17.9%**	**5.2%**

Cyber Trends That Impact Human Risk in Asia

Asia has a complex map of digitalization. The World Economic Forum describes the Association of Southeast Asian Nations (ASEAN) as "the fastest growing Internet market in the world" and predicts the growth in its digital economy will add an estimated US$1 trillion to regional GDP in the next 10 years.

After a year of sustained training, the majority of industries across all company sizes achieved single-digit PPP rates, with an average reduction of 78% from initial levels

Elsewhere, both China and Japan have large digital footprints. In particular, Japan has a highly connected infrastructure and advanced technology landscape and is increasingly focusing on its security. Its new Active Cyber Defense Bill, for example, provides greater governmental powers to stop cyberattacks before they escalate.

Throughout the region, this combination of rapid digital transformation and mature technology ecosystems opens people and their employers to a wide array of threats. Let's take a look at some of the factors influencing human risk across the region.

"Ground Zero" for Cybercrime

The United Nations Office on Drugs and Crime (UNODC) reports that cyber-enabled fraud in Southeast Asia has continued to intensify, with a predominant proportion of losses attributed to cybercriminal gangs located in the region. The UNODC states that these countries, particularly those in the Mekong, are a "key testing ground" for transnational criminal networks looking to diversify, labeling it "ground zero for the scamming industry."

People and infrastructure in Asia are more likely to be targeted by novel and emerging threats as cybercriminals look to scale attacks globally.

Rapid Digitalization in the Supply Chain

PriceWaterhouseCoopers (PWC) reveals that 63% organizations in APAC believe they have an overreliance on third-party suppliers, which can increase their risk exposure from related threats.

This is further amplified by the rapid and uneven pace of digital transformation, aging infrastructure in some countries and sectors, and new implementations. PWC's report confirms the top cybersecurity concerns directly correlate to third-party ecosystems, including software security, exploiting zero-day vulnerabilities and breaches of the suppliers themselves.

GenAI Enables Cybercriminals to Localize Phishing Campaigns

Before the GenAI revolution, English was the predominant language for global phishing campaigns. As a study published by USENIX demonstrates, non-native English speakers are more skeptical of the emails they receive that are written in English and more likely to ignore any instructions they contain.

Previously, the expertise required to create or translate phishing emails in local languages was a high barrier for scaling successful attacks internationally. However, as with other regions globally, large language models (LLMs) have enabled the rapid and highly accurate creation of phishing emails in local languages, with further applications for AI found in the personalization and automation of attacks.

Key Takeaways

- **Asia sits at the epicenter of cybercrime,** with individuals and organizations forming a test bed for attacks
- **Organizations in APAC are breached more frequently versus the global average,** signaling an elevated need to stop initial attacks, which are so often delivered by phishing emails
- **GenAI has increased phishing risk,** making it easier to target people in their local languages and increasing the likelihood that they will interact with these threats
- **With cybersecurity training, organizations can reduce their phishing click rates by 81.8%,** demonstrating the value that best-practice programs can deliver

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 & compliance training, cloud email security, real-time coaching, crowdsourced anti-phishing, AI Defense 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-KN0WBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com