

Phishing by Industry Benchmarking Report

Asia 2026



Navigating the AI-Driven Frontier of Human Risk

Reducing phishing risk is central to effective digital workforce security.

Every successful attack relies on a person to carry out a specific action — clicking a link, downloading an attachment or surrendering credentials. If a phishing email bypasses technical defenses, the attack still fails if the recipient has the instinct to report, delete or simply ignore it.

While organizations must continue to enhance technical barriers with AI-powered email security, the data in this report proves that significant risk reduction comes from best-practice security awareness training (SAT).

As organizations expand beyond human employees to include AI agents, the attack surface grows in ways that traditional technical controls were not designed to address. SAT is not only the most effective lever for strengthening digital workforce security — it is the foundation for building the security culture and organizational vigilance required to manage the risks the human/AI workforce has introduced.

Benchmarking: Your First Step Toward Resilience

An effective risk mitigation strategy begins with a clear understanding of your organization's specific risk profile. To move the needle, you must know how your workforce compares against peers of the same industry, size and geographical region. Only by identifying who is most susceptible can you deliver the timely, personalized security interventions — such as bespoke training and real-time coaching — necessary to change behavior.

Our annual Phishing By Industry Benchmarking Report provides the essential data to take that first step. For this 2026 edition, we conducted an exhaustive analysis of 42 million phishing simulations, 14 million unique users and 64,000 organizations. Over a one-year period, we tracked the Phish-prone™ Percentage (PPP) across 19 industries and seven geographical regions.

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

How We Calculate Phish-prone Percentages

The PPP is the percentage of employees within an organization likely to fall for social engineering or phishing attacks.

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-Plus 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.

2026 International Phishing Benchmarks

At baseline, Africa records the highest regional PPP at 35.9%, followed closely by North America at 34.5% and South America at 31.5%. Asia enters with the lowest baseline at 24.9%, suggesting relatively greater prior investment in awareness training or a more homogenous threat environment at the point of first testing.

The 90-day results are notably uniform across regions, clustering between 16% and 21.4% — indicating that initial training produces broadly similar short-term behavioral change regardless of starting point.

After one year of ongoing training, South America achieves the lowest regional PPP at 3.3%, followed by North America at 4%. Africa remains the most challenging environment at 7.4%.

Organization Size	Phase 1 Initial Baseline Phishing Security Test Results				Phase 2 Phishing Security Test Results Within 90 Days of Training				Phase 3 Phishing Security Test Results After One Year-Plus of Ongoing Training			
	1-249	250-999	1000-9,999	10,000+	1-249	250-999	1000-9,999	10,000+	1-249	250-999	1000-9,999	10,000+
Region												
Africa	28.9%	30%	34.6%	39%	26.6%	28.1%	24.8%	14.7%	3.9%	15.1%	9.1%	3%
Total	35.9%				21.1%				7.4%			
Asia	23.1%	27.8%	28.4%	21.6%	18.6%	18.9%	19%	12.6%	6.6%	6.4%	5.8%	3.4%
Total	24.9%				16%				5.5%			
Australia & NZ	24.6%	28.5%	32.7%	54.5%	23.9%	24%	18.5%	16.7%	5.7%	5.5%	4.8%	4.3%
Total	33%				21%				5.3%			
Europe	23.5%	26.1%	29.6%	38.1%	20.8%	22%	21%	21.6%	4.70%	4.5%	6.6%	4.7%
Total	31.1%				21.4%				5%			
North America	25%	29.5%	35.4%	44%	21.7%	21.9%	20.3%	16.6%	4.3%	3.9%	3.8%	4.2%
Total	34.5%				20.1%				4%			
South America	26.6%	25.4%	33.6%	32.9%	23.7%	21.5%	18.4%	12.8%	7.2%	3.6%	2.2%	2.8%
Total	31.5%				17.7%				3.3%			
UK & Ireland	24.8%	26.8%	32.7%	33.1%	22.9%	23.1%	20%	14%	4.5%	5.5%	6.1%	5.8%
Total	30.3%				19.8%				5.5%			

Introduction: The Threat Landscape in Asia

Asia's cybersecurity environment is under sustained and escalating pressure. Asia is home to some of the world's fastest-growing digital economies — and, increasingly, some of its most determined cybercriminals. Rapid connectivity has unlocked immense opportunity, but uneven cybersecurity maturity across the region continues to create openings for threat actors. Rapid digital transformation and economic expansion have made [regional enterprises lucrative targets](#), and despite significant investment in technical defenses, the human element remains the most consequential variable in organizational security posture.

Threat actors are increasingly leveraging generative AI to produce flawless, localized phishing lures capable of bypassing automated email security gateways. From AI-enabled deepfake scams and industrial-scale fraud operations to ransomware and infostealer malware, the challenges facing the region are formidable. The burden of defense falls, more than ever, on the workforce.

Organizational and Industry Profile

The Asian dataset segments organizations into four size tiers: small (1–249 employees), medium (250–999), large (1,000–9,999) and enterprise (10,000+). The distribution is heavily weighted toward small and medium enterprises, reflecting the region's vibrant business landscape, alongside a growing contingent of large enterprise environments.

Asia's regional average baseline PPP of 24.9% is the lowest of any region in the 2026 benchmark — but that headline figure masks significant sector-level variation. The three most exposed industries at baseline are Legal (44.1%), Insurance (41%) and Education (40.6%). These are high-value, data-intensive environments that combine sensitive client information with workforces that may be less accustomed to formal security training regimens. A 44.1% baseline in Legal firms means nearly half of employees in that sector would engage with a simulated phishing email before any training is introduced.

Globally, high-stress, data-heavy industries consistently show the highest baseline vulnerability, with large-scale healthcare environments reaching a peak baseline of 54%. Asian organizations in Legal, Insurance and Education should assume comparable risk profiles apply to their operations.

Benchmark Data Analysis

Asia's PPP data across all organization sizes tells a clear and encouraging story: sustained training works, and it works consistently across every tier.

At baseline, the regional average PPP is 24.9% — meaning roughly one in four employees would interact with a malicious email before any training is introduced. Exposure rises with organization size, from 23.1% in small organizations to 28.4% in large ones, before stepping down slightly to 21.6% in enterprise environments. The higher baseline among large organizations likely reflects the complexity of operating across multiple departments and geographies, where a lesser sense of shared security responsibility can take hold.

Asia

	Phase 1 Initial Baseline Phishing Security Test Results	Phase 2 Phishing Security Test Results Within 90 Days of Training	Phase 3 Phishing Security Test Results After One Year- Plus of Ongoing Training
1-249	23.1%	18.6%	6.6%
250-999	27.8%	18.9%	6.4%
1000-9,999	28.4%	19%	5.8%
10,000+	21.6%	12.6%	3.4%
Average PPP Across All Organization Sizes	24.9%	16%	5.5%

Within 90 days of training, the regional average falls to 16%, with the most pronounced early improvement occurring in enterprise environments, which drop from 21.6% to 12.6%. This mirrors the pattern observed in other regions: larger organizations with centralized, programmatic training infrastructure can mobilize quickly once a program is in place.

After one year or more of continuous training and simulated testing, the regional average converges to 5.5% — a relative reduction of 78% from baseline. Results are notably consistent across size bands at this stage: small organizations reach 6.6%, medium 6.4%, large 5.8% and enterprise 3.4%. The convergence toward a common threshold of roughly 5% after sustained training is one of the most striking patterns in the Asian data, and reinforces a finding that holds across every region in this benchmark: security awareness is a trainable, measurable capability that responds to consistent investment regardless of organizational scale.

Key Takeaways

→ Human risk is universal, but sector concentration matters

Asia's 24.9% regional average is the lowest baseline of any region, yet Legal (44.1%), Insurance (41%) and Education (40.6%) demonstrate that sector-level exposure can be severe even where the regional average appears moderate. Organizations in these sectors should treat their baseline as significantly above the regional norm.

→ Scale shapes the risk profile

Baseline PPP rises with organization size, peaking at 28.4% in large organizations. Larger environments — with more complex communications, more tools and more distributed workforces — require formalized, ongoing training programs rather than ad hoc interventions.

→ Enterprise environments show the sharpest turnaround

Enterprise organizations move from a 21.6% baseline to 3.4% after a year of training — the lowest long-term result of any size band in the region. Centralized, programmatic training at scale produces the most consistent long-term results.

→ Convergence after one year is the standout finding

Across all four size bands, one-year PPP results cluster tightly between 3.4% and 6.6%. Technical defenses alone cannot achieve this kind of consistency; it is the product of continuous simulation, immediate remediation and a sustained culture of security awareness.

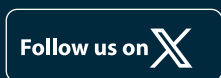
→ Move beyond annual compliance training

The distance between Phase 2 (16%) and Phase 3 (5.5%) results demonstrates that a single training cycle is insufficient. Security leaders should move from compliance-based annual programs toward localized, continuous attack simulation and training to sustain meaningful risk reduction against AI-enhanced, regionally targeted threats.

About KnowBe4

KnowBe4 empowers the modern workforce to make smarter security decisions every day. Trusted by more than 70,000 organizations worldwide, KnowBe4 is the pioneer of digital workforce security, securing both AI agents and humans. **The KnowBe4 Platform** provides attack simulation and training, collaboration security, and agent security powered by AIDA (Artificial Intelligence Defense Agents) and a proprietary Risk Score. The platform leverages 15 years of behavioral data to combat advanced threats including social engineering, prompt injection, and shadow AI. By securing humans and agents, KnowBe4 leads the industry in workforce trust and defense.

More information at www.KnowBe4.com.



KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com

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