

Phishing by Industry Benchmarking Report

2026 Edition



Navigating the AI-Driven Frontier of Human Risk

The phishing threat landscape is maturing at an unprecedented pace. In 2026, we are witnessing the convergence of novel tactics, seasoned threat actors and classic social engineering attacks supercharged by AI at scale.

Phishing in 2026 is no longer a game of chance—it is a persistent, AI-enabled operation. According to [KnowBe4's Phishing Threat Trends Report](#), there has been a **17.1% increase** in phishing attacks since the second half of 2025. As technical defenses evolve, the human element remains the ultimate pivot point for cybercriminals.

Reducing phishing risk is central to effectively managing cyber risk. 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).

Lastly, 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 reducing human risk — 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:

- 42,000,000 phishing simulations
- 14,800,000 unique users
- 64,000 organizations

Over a one-year period, we tracked the **Phish-prone™ Percentage (PPP)** across 19 industries and seven geographical regions.

17.1%
increase
in phishing attacks
since the second
half of 2025

What's Inside

- **02** Introduction
- **04** How We Calculate Phish-prone Percentages
- **05** Analyzing Training Effectiveness
- **07** Average Improvement Rate for Organizations with 1-249 Employees
- **09** Average Improvement Rate for Organizations with 250-999 Employees
- **11** Average Improvement Rate for Organizations with 1,000-9,999 Employees
- **13** Average Improvement Rate for Organizations with 10,000+ Employees
- **15** International Phishing Benchmarks
- **16** Africa
- **21** Asia
- **24** Australia and New Zealand
- **27** Europe
- **30** North America
- **33** South America
- **36** United Kingdom & Ireland
- **39** Conclusion and Key Takeaways
- **40** Contributors/About KnowBe4

How We Calculate Phish-prone Percentages



42M

**Phishing Security
Tests**



14.8M

Users



64K

Organizations

What is Phish-prone Percentage?

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

Methodology

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.

Analyzing Training Effectiveness

The Baseline: A Persistent State of Vulnerability

Before any security awareness training (SAT) is implemented, the **global industry average PPP stands at 33.2%**. This baseline proves that technical defenses alone are insufficient; a significant portion of emails that bypass filters will be engaged with by employees.

Notably, the three most at-risk industries remain unchanged from our 2025 report:



42.7%

Healthcare & Pharmaceuticals

38.1%

Insurance

36%

Retail & Wholesale

The fact that these findings are identical to the previous year suggests that these sectors face systemic targeting and inherent cultural vulnerabilities that require sustained, long-term intervention.

The Scaling Risk: Organizational Size Matters

The data reveals a direct correlation between workforce size and initial vulnerability. As an organization grows, its attack surface expands, and centralized security culture becomes more difficult to maintain.

Organization Size (Employees)	Baseline Phish-prone Percentage (PPP)
1 – 249	24.7%
250 – 999	28.9%
1,000 – 9,999	34.1%
10,000+	39.5%

While risk profiles shift slightly across different industries, the general trend is undeniable: **the larger the organization, the greater the risk.**

The Solution: Measurable Behavioral Change

The introduction of consistent SAT triggers an immediate and dramatic shift in risk posture. Every industry analyzed experienced a significant reduction in phishing susceptibility within the first quarter.

90 Days of Training

The global average PPP drops by **40%**, falling to **20.1%**.

12 Months of Training

The reduction becomes transformative, with the average PPP plummeting **79%** to a mere **4.2%**.

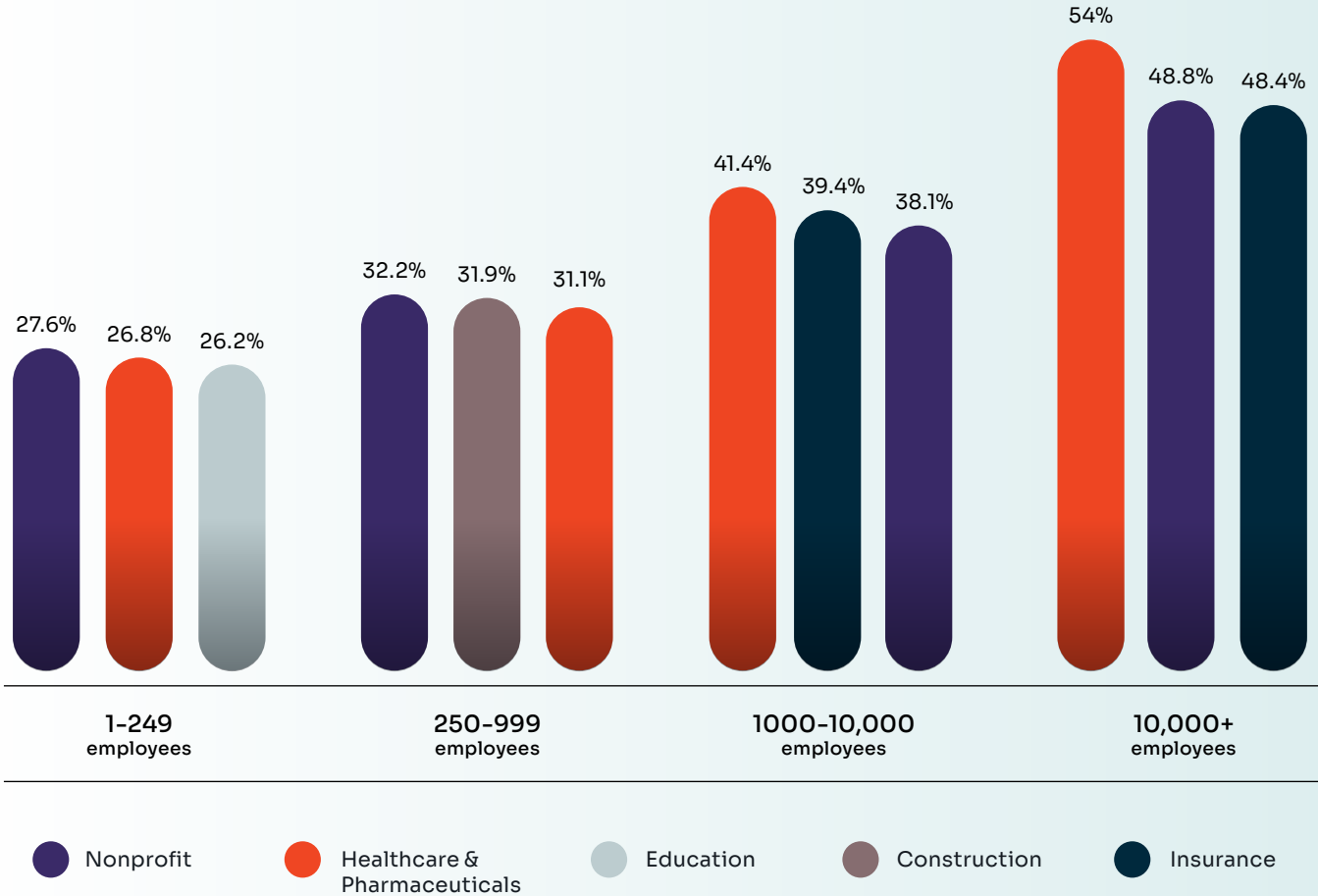
24 Months of Training

Long-term reinforcement leads to a baseline of **3.9%**.

These figures underscore that while the “90-day win” is vital for immediate risk reduction, the true goal of SAT is a 12-month cycle of behavioral conditioning. This long-term commitment is what ultimately bridges the gap between a vulnerable workforce and a secure organization.

Who’s At Risk

The Top Three Riskiest Industries By Organization Size



Average Improvement Rate for Organizations with 1-249 Employees

Banking as the Industry Leader

The **Banking** sector demonstrates the highest level of resilience, boasting both the lowest 1-year PPP (**2.4%**) and the highest overall improvement rate (**89%**).

Nonprofits Face Highest Initial Vulnerability

The **Nonprofit** sector started with the highest baseline PPP at **27.6%**. Despite this high initial risk, they achieved a strong **84%** improvement rate over one year, proving that even the most vulnerable sectors can effectively close the security gap through structured awareness programs.

The “90-Day Lag” Phenomenon

In many industries—most notably **Healthcare & Pharmaceuticals** and **Technology**—the improvement in the first 90 days is marginal (e.g., Healthcare only dropped from **26.8%** to **24.9%**). This highlights that for smaller organizations, a single quarter of training is often insufficient to change habits; meaningful behavioral shifts require a full year of reinforcement.

Consistency in Improvement

Despite varying baselines, the improvement rate is remarkably consistent, with almost every industry landing between **80%** and **87%**. This data underscores that a standardized security awareness training program yields predictable, high-impact results regardless of the specific industry vertical.

Average Improvement Rate for Organizations with 1-249 Employees

	PPP Baseline	PPP after 90 Days	PPP after 1 Year	Improvement Rate %
Banking	21.3%	16.2%	2.4%	89%
Business Services	23.9%	22.1%	4.8%	80%
Construction	25.2%	22.7%	6.1%	75%
Consulting	24.5%	22.5%	4.2%	82%
Consumer Services	25.3%	22%	4.2%	83%
Education	26.2%	19.6%	4.4%	83%
Energy & Utilities	24.9%	20.9%	3.9%	84%
Financial Services	23.4%	19.2%	4.1%	82%
Government	25%	19.9%	3.8%	85%
Healthcare & Pharmaceuticals	26.8%	24.9%	4.7%	82%
Hospitality	26.2%	24%	3.6%	86%
Insurance	22.3%	22.1%	3.4%	85%
Legal	25.9%	21.7%	5.6%	78%
Manufacturing	24.7%	21.8%	5%	80%
Nonprofit	27.6%	25.3%	4.5%	84%
Other	24.8%	22.4%	4.7%	81%
Retail & Wholesale	25.6%	22.1%	4.7%	82%
Technology	22.5%	22%	3.9%	83%
Transportation	24.2%	21.7%	3.2%	87%

Average Improvement Rate for Organizations with 250–999 Employees

Higher Initial Vulnerability

Compared to smaller organizations, mid-sized entities generally start with a higher PPP baseline, with several sectors like **Nonprofit (32.2%)**, **Construction (31.9%)** and **Healthcare (31.1%)** exceeding the 30% mark. As headcount grows, the attack surface expands, making “human-layer” security more difficult to manage without formal training.

Energy & Utilities Leading in Efficiency

The **Energy & Utilities** sector achieved the most impressive results in this cohort, reaching a **90% improvement rate** and the lowest 1-year PPP at **3.1%**.

Accelerated 90-Day Gains in Banking

While many industries struggled to move the needle significantly in the first quarter, the **Banking** sector saw a massive **drop from 30% to 17.9%** in just 90 days. This rapid early adoption is likely due to high-stakes regulatory environments that prioritize compliance and employee vigilance.

Strong Resilience in Highly Targeted Sectors

Industries often targeted by high-volume phishing—such as **Insurance (88%)** and **Consulting (88%)**—showed above-average improvement rates.

Consistent Bottom-Line Stabilization

Regardless of the industry, the data show that 12 months of consistent testing and training brings the risk level down to a manageable **3% to 6%**. This stabilization point is critical for risk assessment, as it proves that mid-sized organizations can achieve a “new normal” of high security awareness regardless of their starting point.

Average Improvement Rate for Organizations with 250–999 Employees

	PPP Baseline	PPP after 90 Days	PPP after 1 Year	Improvement Rate %
Banking	30%	17.9%	3.9%	87%
Business Services	28.1%	23.8%	5.9%	79%
Construction	31.9%	25%	4.9%	85%
Consulting	29.7%	23.7%	3.5%	88%
Consumer Services	29.7%	23.7%	3.9%	87%
Education	29.2%	20.2%	3.7%	87%
Energy & Utilities	29.6%	22.1%	3.1%	90%
Financial Services	28.6%	20.2%	3.9%	86%
Government	27.2%	18.8%	4%	85%
Healthcare & Pharmaceuticals	31.1%	24.1%	4.6%	85%
Hospitality	29.9%	23.8%	4.4%	85%
Insurance	30.2%	24.1%	3.7%	88%
Legal	24.5%	19.6%	4.4%	82%
Manufacturing	27.5%	21.3%	4.1%	85%
Nonprofit	32.2%	24.3%	4.4%	86%
Other	28.5%	22.4%	4%	86%
Retail & Wholesale	28.4%	22.1%	4.2%	85%
Technology	27.4%	22.1%	3.7%	86%
Transportation	27.7%	23%	5.2%	81%

Average Improvement Rate for Organizations with 1,000–9,999 Employees

Extreme Initial Risk in Healthcare

The **Healthcare & Pharmaceuticals** sector faces a massive initial vulnerability with a **41.4%** PPP baseline. This underscores that in large-scale healthcare environments, nearly half of the workforce is initially susceptible to phishing.

Superior Efficiency in Insurance and Legal

The **Insurance** sector achieved a remarkable **93%** improvement rate, bringing its PPP from **39.4%** down to a mere **2.9%**. Similarly, **Legal** dropped to **2.7%** (the lowest 1-year PPP in this group). Large organizations in highly regulated industries can reduce risk via scaled, effective security awareness programs.

The “Size-to-Risk” Correlation

As organization size increases, so does the initial PPP baseline. Small and medium-sized organizations often have PPP baselines in the **20s** versus PPP baselines in the **30s or 40s** for organizations with over 1,000 employees.

Massive 90-Day Breakthroughs

Unlike the smaller cohorts where the first 90 days showed slow progress, large organizations see huge early wins. For example, **Energy & Utilities** nearly halved its risk (from **37.3%** to **19.9%**) in the first quarter.

Resilience of Professional Services

Business Services, Hospitality and **Manufacturing** all maintained high **89%–90%** improvement rates. This demonstrates that even in industries not traditionally viewed as “tech-centric,” effective security awareness programs can dramatically reduce risk.

Average Improvement Rate for Organizations with 1,000–9,999 Employees

	PPP Baseline	PPP after 90 Days	PPP after 1 Year	Improvement Rate %
Banking	35.7%	18.6%	5.7%	84%
Business Services	34.1%	22.2%	3.3%	90%
Construction	33.3%	22.9%	5.2%	84%
Consulting	33%	21.8%	4.6%	86%
Consumer Services	31.6%	21.2%	6.1%	81%
Education	33%	19.2%	5.3%	84%
Energy & Utilities	37.3%	19.9%	5%	86%
Financial Services	37.6%	20.4%	4.4%	88%
Government	29.2%	18.5%	3.8%	87%
Healthcare & Pharmaceuticals	41.4%	21.3%	5.1%	88%
Hospitality	32.7%	19.9%	3.6%	89%
Insurance	39.4%	19.1%	2.9%	93%
Legal	31.5%	17.3%	2.7%	91%
Manufacturing	32.1%	20.3%	3.6%	89%
Nonprofit	38.1%	22.6%	4.5%	88%
Other	32.2%	17.1%	3.3%	90%
Retail & Wholesale	34.7%	21.1%	5%	86%
Technology	33.3%	22%	4.1%	88%
Transportation	29.4%	19.9%	3.8%	87%

Average Improvement Rate for Organizations with 10,000+ Employees

Critical Vulnerability in Large-Scale Healthcare

The **Healthcare & Pharmaceuticals** sector shows a staggering **54%** PPP baseline. This is the highest baseline across all datasets, indicating that in massive healthcare enterprises, more than one in two employees is likely to click a malicious link before training. However, they also achieved one of the highest improvement rates (**93%**), dropping to **3.8%** after a year.

The “Massive Early Win” in Banking

Unlike smaller cohorts, **Banking** saw an incredible drop from **44.6%** to **11.4%** in the first 90 days.

Sector-Specific Challenges in Transportation

While most industries achieved an 80%+ improvement, **Transportation** is a notable outlier with an improvement rate of only **68%** and the highest 1-year PPP (**8.9%**).

Highest Overall Improvement Ceiling

This tier shows the most aggressive improvement rates across the board, with multiple industries (**Banking, Healthcare, Insurance, Legal, Manufacturing, Retail**) consistently hitting or exceeding the **90%** mark. This proves that scale is not a barrier to security.

The Power of Institutionalization

By the one-year mark, even sectors that started with near-majority vulnerability (like **Insurance** at **48.4%** or **Nonprofit** at **48.8%**) managed to stabilize at risk levels comparable to much smaller firms.

Average Improvement Rate for Organizations with 10,000+ Employees

	PPP Baseline	PPP after 90 Days	PPP after 1 Year	Improvement Rate %
Banking	44.6%	11.4%	3%	93%
Business Services	36.6%	16.2%	5%	86%
Construction	31.6%	21.8%	6.2%	80%
Consulting	36.4%	23.4%	3.3%	91%
Consumer Services	22.6%	13%	3.9%	83%
Education	34.3%	16.8%	4.6%	87%
Energy & Utilities	38.7%	17%	7.1%	82%
Financial Services	42.4%	14.8%	4%	91%
Government	30%	15%	4.3%	86%
Healthcare & Pharmaceuticals	54%	17%	3.8%	93%
Hospitality	30.5%	16%	2.6%	91%
Insurance	48.4%	17.3%	4.7%	90%
Legal	26.2%	12.4%	2.4%	91%
Manufacturing	38.8%	16.1%	3.4%	91%
Nonprofit	48.8%	21.1%	6.3%	87%
Other	40.1%	21.1%	2.9%	93%
Retail & Wholesale	46.4%	18.1%	4.3%	91%
Technology	38.8%	14%	4.6%	88%
Transportation	28.1%	16.3%	8.9%	68%

International Phishing Benchmarks

At an international level, we benchmark using the same three phases and segment our customers by industry (see regional analysis) and four organizational sizes.

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%**, driven largely by the persistently high one-year result for organizations with 250–999s.

Enterprise organizations (10,000+) show the widest variance at baseline — from **21.6% in Asia to 54.5% in Oceania** — but converge strongly after a year, reinforcing that scale is not a barrier to improvement when training is sustained.

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%			
Oceania	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%			

Phishing Benchmark Report

Africa 2026

By Anna Collard, SVP Content Strategy and CISO Advisor, KnowBe4 Africa

Introduction: The Threat Landscape in Africa

Africa's digital economy, valued at USD [\\$180 billion annually](#), is projected to reach USD \$1 trillion by 2030. This transformation is powered by the world's youngest population and fastest-growing mobile user base — but with that opportunity comes an expanded attack surface.

The scale is already significant. The United Nations estimates illicit financial flows drain [USD \\$89 billion](#) from the continent each year, and increasingly those flows move through digital channels. [INTERPOL's Africa Cyberthreat Assessment Report 2025](#) found cyber-related offenses rose to more than 30% of all reported crime in parts of Western and Eastern Africa, with cybercrime stripping roughly USD \$3 billion from African economies between 2019 and 2025.

The [World Economic Forum's Global Cybersecurity Outlook 2026](#) found sub-Saharan Africa leads the world in exposure to cyber-enabled fraud, with 82% of regional respondents targeted by digital scams. Generative AI is accelerating the threat — lowering the cost of attacks and enabling criminal networks to produce culturally convincing, localised social engineering content at scale.

The consequences are visible in the public industry. Recent attacks have hit South Africa's [Government Pensions Administration Agency](#), Kenya's [M-Tiba digital health wallet](#), and in 2026, hacktivist campaign [#OpSouthAfrica](#) exposed significant municipal under-preparedness. Law enforcement is responding: [INTERPOL's Operation Serengeti 2.0](#) resulted in 1,209 arrests and USD \$97.4 million recovered.

Africa's technology ecosystem is more innovative than it is often credited — but [90% of African countries](#) report that their cyber law enforcement capacity needs significant improvement. The pace of vulnerability outstrips the capacity to defend. Protecting the human layer is part of how that gap closes.

[Africa Center for Strategic Studies](#) analysts frame the continent's cyber risk around three principal threats:



Cyber-enabled organized crime

Phishing, ransomware, BEC and extortion dominate, with transnational networks operating at industrial scale. West African syndicates such as Nigeria's Black Axe have grown into globalized, multimillion-dollar criminal enterprises.



Attacks on critical infrastructure

Recent major incidents have hit [Morocco's National Social Security Fund](#) and [telecoms operators in Namibia](#), underscoring that essential public services are squarely in the firing line.



Cognitive warfare

Africa Center research finds 39 African countries have been targeted by information-manipulation campaigns, nearly 60% of them foreign state-sponsored — instruments of politics that in fragile environments can tip the balance between peace and conflict.

Organizational and Industry Profile

Before any training, the average African organization recorded a baseline PPP of 35.9%, meaning more than one in three employees was likely to fall for a phishing simulation. Exposure rises steadily with organization size, from 28.9% in the smallest organizations to 39.1% in the largest.

Africa	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	28.9%	26.6%	3.9%
250-999	30%	28.1%	15.1%
1000-9,999	34.6%	24.8%	9.1%
10,000+	39%	14.7%	3%
Average PPP Across All Organization Sizes	35.9%	21.1%	7.4%

By industry the spread is wider still. The table on the next page shows the industries with a sufficient sample of African organizations to be read with reasonable confidence. The most exposed at baseline were Energy & Utilities (48.0%), Retail & Wholesale (45.2%) and Consumer Services (43.6%), followed by Financial Services, Government and Banking, all clustered in the high-30s. These are data-rich, heavily targeted environments, several of which combine high transaction volumes with public-facing operations.

Africa PPP by Industry (well-sampled industries)

	Phase 1	Phase 3	Reduction
Energy & Utilities	48%	18.6%	61%
Retail & Wholesale	45.2%	5.5%	88%
Consumer Services	43.6%	25.5%	42%
Financial Services	38.6%	5.7%	85%
Government	38.4%	2%	95%
Banking	36%	6%	83%
Insurance	34.5%	5%	86%
Technology	33.5%	6.1%	82%
Business Services	29.4%	5.7%	81%
Manufacturing	27.4%	19.2%	30%

A number of other industries, Education, Healthcare & Pharmaceuticals, Hospitality, Consulting, Construction, Transportation, Legal and Nonprofit are each represented by fewer than roughly 20 African organizations, and their results should be treated as directional only. Two are worth flagging precisely because the small sample produces an eye-catching number: Education recorded the highest baseline of any industry at 57.7% (15 organizations), while Healthcare & Pharmaceuticals showed an unusually low baseline of 21.2% that barely improved after a year, to 18.8% (18 organizations). Neither should be over-interpreted on its own.

Benchmark Data Analysis

The improvement story is genuinely encouraging. Africa's average PPP fell from 35.9% at baseline to 21.2% within 90 days, and to 7.4% after a year of sustained training — a 79% reduction achieved through repeated practice, not new technology. At the industry level, most well-sampled industries fell by 80% or more, with Government (95%), Retail & Wholesale (88%), Insurance (86%) and Financial Services (85%) among the strongest performers.

Two patterns complicate that headline. The first is the mid-market anomaly. Organizations of 250–999 employees barely improved in the first 90 days (30.0% to 28.1%) and remained at 15.1% after a full year — roughly double every other size band and worse than the 9.2% this band recorded in last year's Africa report. This segment drags the continent's one-year average upward and is the primary reason Africa's Phase 3 figure (7.4%) sits above last year's (5.3%). Large enough to present a meaningful attack surface, but without the dedicated security resources of the largest enterprises, mid-sized organizations are the clearest priority for sustained intervention.

The second is residual industry risk. Consumer Services remains at 25.5% after a year (only 42% reduction) and Manufacturing at 19.2% (only 30%). These are not measurement artifacts — both rest on substantial samples (38 and 57 organizations respectively) — and they suggest that high-turnover, distributed or operational-technology-heavy workforces need reinforcement well beyond a single training cycle.

A methodological note: the organizations measured at baseline are not identical to those measured a year later. The sample falls from roughly 706 organizations across 38 countries at baseline to 351 organizations across 28 countries at the one-year mark, reflecting recent customer growth and the time new organizations need to catch up. This is inherent to the methodology and applies to every region.

Placed alongside the rest of the world, Africa’s position is sobering. The continent records the highest baseline and highest residual risk of any major region — and the gap is most revealing after training, not before. At baseline Africa sits around 8% above the global average (35.9% versus 33.2%); after a year it sits roughly 70% above it (7.4% versus 4.3%). Training works — the absolute fall of 28.5 points is among the largest anywhere — but Africa’s organizations need more sustained reinforcement to reach the residual-risk levels that North America and South America achieve. This mirrors the Forum’s wider finding of “cyber inequity”: sub-Saharan Africa reports some of the lowest resilience levels and the second-most acute cyber-skills shortage of any region, with 63% of organizations lacking the people and skills they need.

There is an economic argument for closing that gap. The World Bank, cited in the Forum’s report, estimates that reducing major cyber incidents could lift GDP per capita by 1.5% in developing economies — a reminder that security awareness training is not only a risk control but a contribution to the digital economy Africa is building.

Regional Comparison: Aggregate PPP

	Phase 1	Phase 3
Africa	35.9%	7.4%
North America	34.5%	4%
Australia & New Zealand	33%	5.2%
South America	31.5%	3.3%
Europe	31.2%	5.4%
United Kingdom & Ireland	30.4%	5.6%
Asia	24.9%	5.5%
Global average	33.2%	4.3%

Key Takeaways

→ **Training works, but Africa starts and finishes further back**

Phishing risk fell from 35.9% to 7.4% over a year of sustained training — a 79% reduction. Yet Africa retains both the highest baseline and highest residual risk of any major region, and the gap to the global average widens after training. Sustained reinforcement, not a single annual exercise, is what moves the needle.

→ **Mid-sized organizations are the priority**

The 250–999 band remains stuck at 15.1% after a year — double every other size band and worse than last year. Large enough to be targeted, rarely resourced like a large enterprise, this segment needs focused, ongoing intervention more than any other.

→ **Some industries need more than one cycle**

Consumer Services (25.5%) and Manufacturing (19.2%) retain high residual risk after a full year. High-turnover and operationally complex workforces should be treated as continuous-training environments, not one-off campaigns.

→ **AI-driven social engineering is the threat to plan for**

With sub-Saharan Africa already the world's most fraud-exposed region and generative AI lowering the cost of convincing, localized attacks, awareness programs must explicitly prepare people for AI-crafted phishing, vishing, deepfakes and disinformation — not just the generic lures of previous years.

→ **Read small samples with care**

Several striking figures — the 57.7% Education baseline, the 10,000+ band, the stalled Healthcare result — rest on small numbers of organizations. They point to where to look next, not to settled conclusions.

Asia 2026

By Dr. Kawin Boonyapreddee, CISO Advisor

Introduction: The Threat Landscape in Asia

Asia's cybersecurity environment is under sustained and escalating pressure. The Asia and South Pacific region 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.

Australia & New Zealand 2026

By Dr. Kawin Boonyapreddee, CISO Advisor

Introduction: The Threat Landscape in Australia and New Zealand

Australia and New Zealand (ANZ) represent high-value operating environments for threat actors — mature, digitally advanced economies operating under stringent regulatory oversight, where a successful breach can carry severe financial penalties and lasting operational disruption. According to [Arctic Wolf's 2025 Human Risk Behaviour Snapshot](#), the steepest year-on-year increases in organizational breaches were reported in Australia and New Zealand, alongside the U.K. and Ireland — with nearly two-thirds of security and IT leaders admitting to having clicked on malicious links.

Business email compromise (BEC) remained the top incident type in the region, according to [CyberCX's 2025 Threat Report](#), with espionage-related incidents taking an average of 404 days to detect — up from 390 days in 2023. Generative AI is accelerating the threat further, enabling criminal networks to produce convincing, localized phishing lures that bypass automated email gateways and place the burden of defense squarely on the workforce. Despite significant investment in technical controls, human error remains the most consequential variable in organizational security posture.

Organizational and Industry Profile

The ANZ dataset segments organizations into four size tiers: small (1–249 employees), medium (250–999), large (1,000–9,999) and enterprise (10,000+). The regional profile reflects a highly mature corporate environment with significant representation in high-risk sectors, most notably Banking and Healthcare and Pharmaceuticals.

The regional average baseline PPP of 33% sits just below the global average of 33.2% — but that figure understates the concentration of risk in specific sectors. Banking records a baseline PPP of 62%, the highest of any sector in any region in this benchmark, meaning nearly two in three banking employees would engage with a simulated phishing email before any training is introduced. Healthcare & Pharmaceuticals follows at 41%. These are precisely the sectors operating under the most stringent regulatory obligations and handling the most sensitive personal and financial data — making the gap between exposure and resilience a matter of significant institutional risk.

Globally, high-stress, data-heavy industries consistently show the highest baseline vulnerability. ANZ organizations in Banking and Healthcare should treat their sector baselines, not the regional average, as their relevant benchmark.

Benchmark Data Analysis

The ANZ data presents a stark but ultimately encouraging picture. At baseline, the regional average PPP is 33%, with exposure rising sharply by organization size: small organizations start at 24.6%, while enterprise environments begin at a striking 54.5% — the highest enterprise baseline of any region in this benchmark. The pattern reflects a well-documented dynamic: in large, sprawling organizations with fragmented communication networks and complex operational structures, phishing emails blend far more easily into the noise of daily workflows.

**Australia &
New Zealand****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	24.6%	23.9%	5.7%
250-999	28.5%	24%	5.5%
1000-9,999	32.7%	18.5%	4.8%
10,000+	54.5%	16.7%	4.3%
Average PPP Across All Organization Sizes	33%	21%	5.3%

Within 90 days of training, the regional average falls to 21%, with the most dramatic short-term improvement again occurring in enterprise environments, which drop from 54.5% to 16.7% — a reduction of 69% in under three months. This scale of early movement in the largest organizations reflects the impact of centralized, programmatic training when deployed consistently across a large workforce.

After one year or more of continuous training and simulated testing, the regional average converges to 5.3% — a relative reduction of 84% from baseline. Results tighten considerably across size bands: small organizations reach 5.7%, medium 5.5%, large 4.8% and enterprise 4.3%. The convergence is notable. Organizations that begin with vastly different risk profiles — a 24.6% small business and a 54.5% enterprise — arrive within two percentage points of each other after a year of sustained training. That is not a coincidence of sample composition; it is the measurable result of behavioral conditioning applied consistently over time.

Key Takeaways

→ **Sector concentration is the defining risk characteristic**

A 33% regional average obscures the real story. Banking's 62% baseline and Healthcare's 41% mean that ANZ's highest-risk organizations start further back than virtually any comparable sector globally. Organizations in these sectors should benchmark against their industry figure, not the regional average.

→ **Enterprise environments carry the highest initial exposure**

A 54.5% baseline PPP in organizations with 10,000 or more employees reflects the difficulty of maintaining security awareness across large, complex, geographically distributed workforces. Fragmented communication networks require formalized, centralized training infrastructure — not ad hoc campaigns.

→ **Early training delivers immediate, measurable returns**

The enterprise segment's drop from 54.5% to 16.7% within 90 days demonstrates that even the most exposed environments respond quickly to initial training. The window between baseline exposure and first intervention is where organizational risk is highest; closing it quickly is the priority.

→ **Convergence after one year is the benchmark to reach**

All four size bands land between 4.3% and 5.7% after sustained training — a range that tracks closely with the global gold standard of 3–5%. Reaching and sustaining that threshold requires continuous simulation and remediation, not annual compliance exercises.

→ **Regulatory exposure amplifies the cost of inaction**

In an environment shaped by Australia's Cyber Security Act 2024 and New Zealand's Privacy Act obligations, a successful phishing-enabled breach carries not only operational consequences but material regulatory and reputational risk. Security awareness training is both a risk control and a compliance investment.

Europe 2026

By Dr. Martin Kraemer, CISO Advisor

Introduction: The Threat Landscape in Europe

Phishing remains the single most common way attackers break into European organizations. According to the [ENISA Threat Landscape 2025](#), which analyzed 4,875 incidents between July 2024 and June 2025, phishing accounted for 60% of initial intrusions, with vulnerability exploitation following at 21%. Phishing-as-a-Service platforms, info-stealers such as Lumma, and AI-assisted lure generation have lowered the skill required to run convincing campaigns at scale. The criminal ecosystem behind these numbers has professionalized.

Geopolitics continue to be a major influence for the region. ENISA attributes roughly 80% of recorded incidents to ideology-driven hacktivism. Notably, state-aligned groups continued espionage against public administration as the most targeted sector at 38% of incidents.

Social engineering attacks attributed to Scattered Spider-linked actors, which halted Jaguar Land Rover production in its plant in Slovakia, demonstrated that a single compromised supplier or help desk can cascade across an entire sector.

[Regulation](#) continued to shape the region. DORA has applied to financial entities since January 2025, the EU AI Act's AI literacy obligation took effect in February 2025, and NIS2 transposition progressed unevenly, with only 14 member states fully transposed by mid-2025 and Germany's implementation law arriving in December 2025.

Organizational and Industry Profile

The European dataset includes 41 countries. Small organizations with 1-249 employees make up 57% of the total, followed by 27% medium organizations (250-999 employees), 14% large organizations (1,000-9,999) and 2% large enterprises with 10,000 or more employees. The enterprise segment nonetheless contributes roughly a third of all tested employees, so it meaningfully contributes to the regional average.

We observe globally, the larger the organizations the higher the baseline phishing susceptibility. This also holds true in Europe where small organizations start at a PPP of 23.5%, midsize at 26.1%, large at 29.6% and large enterprises at 38.1%. One potential reason for this difference is more complex environments in larger organizations with more departments, more tools and often a lesser sense of shared responsibility for cybersecurity.

At the industry level, the European pattern is consistent with the global one, with the caveat that some European industry samples are small and indicative rather than definitive. Healthcare & Pharmaceuticals organizations in Europe recorded a baseline of 33.4% which is above the regional average. Banking reported the highest baseline of the larger European industry samples at 40.8%. Globally, Healthcare & Pharmaceuticals, Nonprofit and Insurance occupy the top risk positions among organizations with more than 1,000 employees. European organizations in these sectors should assume the same risk level applies to them.

Europe

	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	23.5%	20.8%	4.7%
250-999	26.1%	22%	4.5%
1000-9,999	29.6%	21%	6.6%
10,000+	38.1%	21.6%	4.7%
Average PPP Across All Organization Sizes	31.1%	21.4%	5.4%

Benchmark Data Analysis

The 2026 results show European organizations performing slightly better than last year. The average baseline PPP across Europe is 31.1%, an improvement of 1.4 percentage points in 2025 but below the global baseline of 33.2%. Without training, almost one in three European employees would interact with a phishing email.

After 90 days of training, the regional PPP falls to 21.4%, and after one year or more of ongoing training it reaches 5.4%. The relative risk reduction of 83% against the baseline is considerable. Compared with 2025, the 90-day result and one-year result are virtually unchanged while the baseline improved. Over the last three years, European averages have moved inside narrow bands that serve as benchmarks for the region: 31-33% as baseline, 20-21% after 90 days, and 5% within a year.

The 90-day results are remarkably similar across organization sizes, ranging only from 20.8% to 21.6% but are also higher than the 16.6% global average. Large organizations with 1,000-9,999 employees reported the weakest one-year result at 6.6%. That is above the 3-5% standard range. By contrast, enterprises achieved the strongest turnaround: from 38.1% at baseline to 4.7%, an 88% reduction.

Key Takeaways

→ Europe's security awareness baseline: progress and the gap that remains

The European benchmark has stabilized over the last few years: a 31.1% baseline PPP falls to 21.4% after 90 days and 5.4% after one year-plus of training, a relative risk reduction of 83%. The gold standard for sustained training is 3-5%.

→ Phishing dominates initial access

Phishing accounts for the initial access vector of about 60% of intrusions according to ENISA. Simulations and training must reflect supply chain scenarios and address help desk social engineering.

→ Compliance Is the floor, not the ceiling

Regulation is now a primary driver of program investment. DORA, NIS2 and the EU AI Act all mandate training or literacy requirements. The organizations that beat the benchmark pair regulatory obligations with relevant, personalized and frequent training moving past compliance to shape employee behavior.

→ 1,000–9,999 employees: A region-wide vulnerability

Large organizations with 1,000–9,999 employees are the region's weak spot at 6.6% after one year. They warrant focused attention on training cadence and relevance.

North America 2026

By Erich Kron, CISO Advisor

Introduction: The Threat Landscape in North America

It should come as no surprise that cybercrime worsened again throughout 2025 and into 2026. Attack volumes have increased, and the use of AI in attacks continues to grow. According to the FBI's 2025 [Internet Crime Complaint Center \(IC3\) annual report](#), the agency received 22,364 complaints reporting AI-related attacks with adjusted losses exceeding \$893 million.

North America, and the United States specifically, remains the most frequently targeted region for cyber threats, according to [Microsoft's Digital Defense Report 2025](#). The United States topped the charts at 24.8% of attacks, with the United Kingdom next at 5.6% — a gap that underscores the scale of exposure facing North American organizations and individuals.

Political division, often amplified by disinformation and misinformation campaigns on social media, continues to weigh on North Americans alongside economic pressures — and threat actors are adept at exploiting emotionally and mentally fatigued targets through social engineering. AI and deepfakes are playing a larger role than ever in constructing convincing narratives used against organizations and individuals alike.

As organizations and employees work to improve efficiency, AI adoption within the workforce is accelerating. The rapid uptake of AI tools and agentic AI is expanding the workforce beyond humans to include a growing number of AI agents, each introducing new and novel vulnerabilities.

Organizational and Industry Profile

The North American dataset covers 31 countries, with organizations segmented into four size tiers: small (fewer than 250 employees, approximately 66%), medium (250–999 employees, approximately 23%), large (1,000–9,999 employees, approximately 10%) and enterprise (10,000 or more employees, approximately 1%). The distribution is reasonably consistent across all three phases of testing.

Testing was conducted across three phases: an initial baseline assessment, a follow-up after approximately 90 days of training and simulated phishing, and a final measurement after approximately one year of ongoing training.

The aggregate PPP for North America across all organization sizes and industries began at 34.5%, fell to 20.2% after 90 days, and reached 4% after one year — a substantial reduction across all sizes and sectors. South America recorded the lowest one-year regional PPP of any region at 3.3%. The breakdown by organization size across all three phases is as follows:

North America	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	25%	21.7%	4.3%
250-999	29%	21.9%	3.9%
1000-9,999	35.4%	20.3%	3.8%
10,000+	43.5%	16.6%	4.2%
Average PPP Across All Organization Sizes	34.5%	20.2%	4%

Benchmark Data Analysis

Industry-level results reveal how consistently and quickly organizations improve across the training timeline. As training progresses, employees become more adept at identifying phishing attempts — and the evidence suggests that improvement in simulated testing translates to better detection of real-world attacks as well.

North American Healthcare & Pharmaceuticals recorded one of the highest baseline click rates in this year's benchmark, at 44%. The risk is concentrated at the upper end of the size spectrum: large organizations with 1,000–9,999 employees started at 43.4%, while enterprise organizations with 10,000 or more employees recorded a striking 54.9% — meaning more than half of simulated phishing emails were engaged with before any training began. Insurance followed with a 39% baseline. These are significant starting points, but as the data show, they respond well to sustained intervention.

Within 90 days of training, Healthcare & Pharmaceuticals' overall PPP fell to 20.7%, with enterprise organizations in that sector dropping to 16.7% — a substantial reduction in a short period. Across all industries at the 90-day mark, Business Services recorded the lowest overall PPP in North America at 16.6%. Also notable at this stage: enterprise Banking organizations (10,000 or more employees) came in at 6.4%, and enterprise Legal firms at 4.5% — sectors where attention to detail, once activated through training, appears to take hold quickly.

After one year of ongoing training, Banking led all sectors with a one-year PPP of 2.8%. Enterprise Healthcare & Pharmaceuticals organizations closed the year at 3% — a reduction of more than 94% from their 54.9% baseline. The scale of improvement across these sectors over a 12-month period makes a compelling case for the depth of impact that sustained, continuous training can achieve.

Key Takeaways

Cybercrime shows no signs of slowing, and people remain the primary target for threat actors seeking initial network access. The data tells a compelling story: consistent workforce education produces sharp, measurable reductions in human risk regardless of organization size or industry.

→ Awareness Is the antidote, not intelligence

Susceptibility to social engineering is not a reflection of intelligence or general education — it reflects a lack of awareness. Baseline click rates are high because employees are not yet conditioned to look for the threat. Through education and regular simulated phishing, they develop the ability to spot and report suspicious activity quickly and reliably. That capability matters more than ever as threat actors leverage AI to produce attacks that are more numerous, more convincing and harder to distinguish from legitimate communications.

→ The most targeted region can't afford complacency

With North America the most targeted region globally, and with workforces expanding to include AI agents, building a strong security culture has never been more important. Organizations must ensure that awareness extends beyond the human workforce to encompass the risks introduced by new and rapidly adopted technologies.

→ No organization is off the radar

From small medical practices to large manufacturers and government agencies, no organization is too small, too large or too specialized to be a target. The threat actors behind these attacks are skilled, well-resourced and persistent — and the cost of complacency continues to rise.

South America 2026

By Rafael Peruch Blauth, Sales Architect

Introduction: The Threat Landscape in Latin America

Latin America's cybersecurity landscape is at a critical inflection point. As organizations across the region undergo rapid digital transformation, they are simultaneously exposed to an increasingly aggressive and sophisticated threat environment. Security research consistently identifies Latin America as one of the most targeted regions globally, driven primarily by the monetization potential of mobile banking fraud, ransomware and business email compromise (BEC). Latin America became the most targeted region for ransomware globally in 2025, with 8.1% of organizations experiencing attacks, according to [Kaspersky's State of Ransomware in 2026](#) study. That risk is compounded by the weaponization of artificial intelligence, which enables even non-technical criminals to launch realistic, personalized phishing campaigns at scale.

While organizations have traditionally focused their defenses on technical layers — firewalls, endpoint detection and secure email gateways — threat actors have adapted by shifting focus to the human element. Social engineering, specifically phishing, remains the primary mechanism for initial access in Latin America. Attackers exploit regional economic anxieties, organizational changes and cultural tendencies toward helpfulness to bypass technical controls.

Compared with mature markets like North America or Western Europe, Latin American enterprises face a compounding vulnerability: a shortage of specialized cybersecurity personnel coupled with historically lower budgets for behavioral risk management. The human factor is no longer an ancillary concern — it is the frontline of modern cybersecurity, where a single employee's click can circumvent millions of dollars in hardware and software defenses.

Organizational and Industry Profile

KnowBe4's 2026 Phishing By Industry Benchmarking Report analyzes regional data, segmenting the South American market into four organizational cohorts based on workforce size: small (1–249 employees), medium (250–999), large (1,000–9,999) and enterprise (10,000+).

An organization's scale meaningfully shapes its risk profile. In smaller businesses, a lack of dedicated security staff means employees often handle multiple roles, creating distraction vectors that attackers exploit. In large and enterprise environments, the volume of daily communications allows phishing emails to blend into standard workflows.

Globally, high-stress, data-heavy industries carry the highest inherent risk. The Healthcare & Pharmaceuticals, Nonprofit, Education and Insurance sectors consistently show the highest baseline vulnerability, with large-scale healthcare environments reaching a peak baseline of 54%. In Latin America, sectors dealing with critical infrastructure, financial services and retail face continuous social engineering pressure from actors seeking maximum operational disruption.

Benchmark Data Analysis

Data from South American organizations provides a clear, measurable picture of both the threat landscape and the impact of continuous security awareness training. The analysis tracks vulnerability across three phases: Phase 1 (initial baseline, prior to training), Phase 2 (within 90 days of training) and Phase 3 (after one year or more of ongoing training).

South America	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	26.6%	23.7%	7.2%
250-999	25.4%	21.5%	3.6%
1000-9,999	33.6%	18.4%	2.2%
10,000+	32.9%	12.8%	2.8%
Average PPP Across All Organization Sizes	31.5%	17.7%	3.3%

Without training, South American organizations average a 31.5% PPP — nearly one in three employees will engage with a malicious email. Large organizations (33.6%) and enterprise environments (32.9%) exhibit the highest baseline risk, reflecting the broader attack surface of larger employee pools.

Within 90 days of introducing training, the regional average drops sharply to 17.7%. The most pronounced short-term improvement occurs in enterprise environments, falling from 32.9% to 12.8%, demonstrating that awareness responds quickly to initial education.

After one year or more of continuous training and simulated testing, the regional average PPP falls to 3.3% — a reduction of roughly 89% relative to the initial baseline. Large organizations achieve the lowest long-term result at 2.2%. The data makes a clear case: sustained behavioral training is the most effective lever for reducing human-centric risk.

Key Takeaways

→ **Technical controls alone are insufficient**

A baseline PPP of 31.5% demonstrates that technical perimeters cannot compensate for human vulnerability. If one in three employees is susceptible, a breach is a matter of when, not if.

→ **Scale demands a systematic approach**

Large and enterprise environments present the highest initial vulnerability (33.6% and 32.9%). As organizations grow, decentralized communications require a formalized, ongoing training program to maintain consistent security baselines.

→ **One-time training is not enough**

The improvement from Phase 2 (17.7%) to Phase 3 (3.3%) demonstrates that annual or compliance-only training is insufficient. Continuous conditioning turns security vigilance into habit rather than policy.

→ **Employees are a defensive asset**

Reducing long-term regional risk to 3.3% validates the concept of the human firewall. Regular simulation and training shift employees from a liability into an effective first line of defense.

→ **The return on investment is measurable**

An approximately 89% reduction in phishing vulnerability over 12 months provides a clear business case for security-awareness investment, directly reducing the risk of ransomware, operational downtime, compliance penalties and reputational damage.

United Kingdom & Ireland 2026

By Javvad Malik, Lead CISO Advisor

Introduction

Over the past year, phishing has retained its position as the defining cyber threat facing organizations across the United Kingdom (UK) and Ireland. The government’s [Cyber Security Breaches Survey 2025/2026](#) found that phishing remained the most prevalent type of breach or attack by a wide margin, experienced by 38% of all businesses, and it was named the most disruptive form of attack by 69% of those affected. Phishing now accounts for 93% of all cyber crime against UK businesses. Tellingly, the proportion of breached organizations that experienced phishing and nothing else rose from 45% to 51% in a single year, and interviewees consistently reported that phishing had become easier to carry out, a trend many linked to the growing availability of generative AI tools and to rising attack volumes.

This was not a theoretical risk. In April and May 2025, Marks & Spencer (M&S), Co-op and Harrods were all hit in quick succession. The attackers, linked to the group known as Scattered Spider, did not break through technology. They talked their way past it, impersonating staff to IT help desks and persuading them to reset passwords, which allowed them access to internal systems. The [NCSC responded](#) by urging organizations to rethink how help desks verify the identity of the people they assist.

For M&S, the disruption was estimated to cost around £300 million (about \$402 million). Fraud told a similar story, with [City of London Police reporting](#) that investment fraud alone stripped £879.8 million (about \$1.2 billion) from UK victims during 2025. The common thread is people. Attackers are targeting human judgement and business processes, not just technology.

Organizational and Industry Profile

The UK&I dataset shows that exposure to phishing at the outset varies considerably by both size and sector. Looking at baseline tests taken before any training, the smallest organizations of up to 249 employees started at a 24.8% Phish-prone Percentage (PPP), rising steadily with size to 26.8% for those with 250 to 999 employees, 32.7% for organizations up to 9,999, and 33.1% for the largest organizations of 10,000 or more. Larger organizations begin more exposed, which reflects both their wider attack surface and the sheer number of people an attacker can attempt to reach.

United Kingdom & Ireland	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	24.8%	22.9%	4.5%
250-999	26.8%	23.1%	5%
1000-9,999	32.7%	20%	6.1%
10,000+	33.1%	14%	5.8%
Average PPP Across All Organization Sizes	30.3%	19.8%	5.5%

By industry the spread is wider still. The most exposed sectors at baseline were Healthcare & Pharmaceuticals at 43.9%, Hospitality at 38%, Construction at 34.1%, Financial Services at 30.7% and Energy and Utilities at 29.3%. These are sectors that either hold highly sensitive data, deal with constant customer turnover or sit high on attackers' target lists. A handful of sectors, including Banking and Insurance, are represented by smaller UK&I samples and should be read with that caveat in mind, but the overall pattern is consistent across the region. The government survey reinforces the point from a governance angle. Finance and insurance firms are among the most likely to have board-level responsibility for cyber security, while retail, construction and transport are among the least likely, and an organization's exposure tends to track that maturity gap.

Regional Comparison: Aggregate Phish-prone Percentage

	Phase 1	Phase 3	Reduction
Consumer Services	45.6%	2.3%	95%
Healthcare & Pharma	43.9%	8.7%	80%
Hospitality	38.0%	3.0%	92%
Banking	37.5%	4.3%	88%
Construction	34.1%	7.0%	80%
Financial Services	30.7%	7.5%	75%
Energy & Utilities	29.3%	6.3%	79%
Insurance	29.3%	3.2%	89%
Education	26.2%	4.6%	82%
Business Services	24.2%	6.8%	72%
Government	22.2%	3.1%	86%
Consulting	19.4%	4.0%	79%

Benchmark Data Analysis

The improvement story is where the data becomes encouraging. Across all organization sizes, the average UK&I Phish-prone Percentage fell from a baseline of 30.3% to 19.8% within 90 days of training, and then to 5.5% after a year or more of sustained activity. That is a reduction of just under 82%, achieved not through new technology but through repeated, structured practice.

The pattern by size is revealing. The largest organizations started most exposed at 33.1% but improved fastest, dropping to 14% within 90 days. The smallest organizations started lower at 24.8% but moved more slowly in the early phase, reaching only 22.9% at the 90-day mark. By one year, however, the gap had all but closed, with every size band converging into a narrow range between 4.5% and 6.1%. Sustained training appears to level the playing field regardless of where an organization begins.

Every industry followed the same downward path, with reductions ranging from roughly 70% to 95%. Several of the worst starters became the biggest movers. Hospitality fell from 38% to 3%, and Insurance from 29.3% to 3.2%. Two sectors, though, retained comparatively higher residual risk even after a year of training: Healthcare & Pharmaceuticals at 8.7% and Financial Services at 7.5%. These remain the most heavily targeted, data-rich environments, and the figures suggest they need continued reinforcement rather than a single concentrated effort.

Key Takeaways

→ **The human target: Why technology alone isn't enough**

Phishing and social engineering are the dominant threat to UK&I organizations, and they are becoming easier for attackers to launch. The attacks on M&S, Co-op and Harrods showed that adversaries increasingly aim at people and process, talking their way past technical controls rather than defeating them. Technology alone cannot close that gap.

→ **From 30% to 5%: rewriting the weakest link narrative**

The benchmark data offers a clear answer. The human layer is not a fixed weakness but a measurable, improvable line of defense. A reduction from 30.3% to 5.5% across the region, and the convergence of organizations of every size into a tight band, shows that the long-standing habit of calling people the weakest link is both inaccurate and unhelpful.

→ **Compliance is a starting point, not a destination**

What makes the difference is sustained, relevant training delivered over time rather than an annual compliance exercise. The persistence matters more than any single phase, and the sectors that remain most targeted, such as Healthcare and Financial Services, benefit most from ongoing reinforcement. Organizations that treat security awareness as a route to behavior change and a stronger culture, rather than a box to tick, will be the ones whose people make smarter decisions when the next well-crafted message lands in their inbox.

Conclusion and Key Takeaways

→ Scale is the greatest multiplier of risk

There is a direct, linear correlation between organizational headcount and phishing susceptibility. Large enterprises (10,000+) face a baseline risk nearly **15% higher** than small businesses.

→ A state of emergency

For the second year running, Healthcare & Pharmaceuticals, Insurance and Retail remain the most vulnerable sectors. In large healthcare enterprises, initial susceptibility is as high as **54%**.

→ The “12-month maturity” rule

The data proves that the 90-day mark is only the beginning of behavioral change. While initial gains are encouraging (a 40% reduction), the most significant “cliff” in risk occurs between three months and one year, where the PPP drops from **20.1%** to **4.2%**.

→ Security awareness training is the foundation of a secure digital workforce

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. Security awareness training is not only the most effective lever for reducing human risk — it is the foundation for building the security culture and organizational vigilance required to manage the risks introduced by an AI-augmented workforce.

→ SAT keys to success

In 2026, AI is not just a threat—it is the engine behind modern, effective training. Organizations using AI-powered security awareness training are seeing a “force multiplier” effect in their resilience.

- **Hyper-personalization at scale**

Traditional generic templates no longer work. AI analyzes employee roles, past simulation performance and even “human risk scores” to deliver bespoke phishing simulations that mirror the highly targeted attacks seen in the wild.

- **Adaptive learning paths**

AI-driven systems move away from “one-size-fits-all” modules. If an employee in Finance struggles with wire-transfer simulations but excels at password security, the AI automatically adjusts their curriculum to focus on Business Email Compromise (BEC) and deepfake social engineering tactics.

- **Real-time threat synchronization**

As new AI-generated phishing tactics emerge (such as “quishing” or QR code phishing), AI-native SAT can instantly scrape these trends and deploy updated simulations, ensuring employees are trained on *today’s* threats rather than last year’s.

Contributors

Colin Beasty, Director, Content Marketing at KnowBe4

Rafael Peruch Blauth, Snr. Sales Architect at KnowBe4

Dr. Kavin Boonyapreddee, CISO Advisor at KnowBe4

Anna Collard, Senior Vice President of Content Strategy & CISO Advisor at KnowBe4

Dr. Martin J. Kraemer, CISO Advisor at KnowBe4

Erich Kron, CISO Advisor at KnowBe4

Javvad Malik, Lead CISO Advisor at KnowBe4

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.