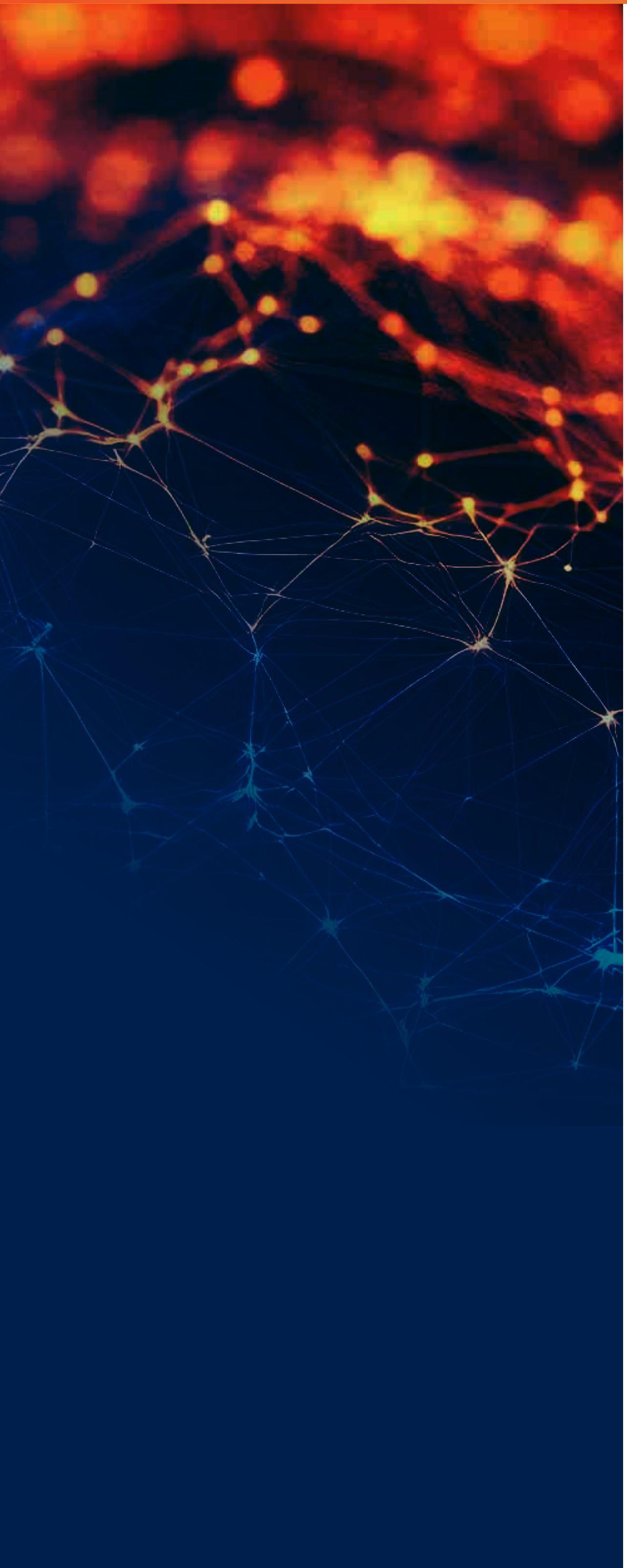
KnowBe4

Phishing Benchmarking Report

Europe 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 Europe.

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%**		

Europe | *By Martin Kraemer*

The PPP in Europe remains consistent with the results of previous years. The average initial PPP before implementing SAT is 32.5%, dropping to 20.7% after 90 days and 5% after one year.

As we've seen with wider global trends, the baseline PPP is higher in larger organizations (1,000+ employees) at 34.9%, 26.7% for midsize (250-999 employees) and 24.9% for small (1-249 employees). Predictably, larger organizations experience the greatest risk reduction. After one year-plus of training, click rates dropped to just 5.3% — an 84.8% decrease. Smaller organizations achieved marginally lower clicks after one year of training at 3.9% for those with 1-249 employees and 4.4% for those with 250 to 999.

This range of 3-5% PPP has now established itself as the gold standard, and it's incredibly positive to see European organizations maintaining their averages within this bracket.

When compared to the 2024 PPPs, the performance was almost unchanged across all organizations. The baseline performance in Phase 1 was 0.1% better. After 90 days of training, the 2025 PPP was 0.4% worse than last year, and after one year-plus of training, organizations performed 0.5% better as compared to the previous year. This result shows a continued positive average performance across the board, showcasing that investments in SAT have led to a reduction in phishing susceptibility as measured by PPP. These numbers have now stabilized and can be considered the benchmark across Europe.

This ongoing and effective risk management remains an urgent priority. When we analyzed data from KnowBe4 Defend, we noted a 68% increase in phishing attacks and 137% increase in BEC globally between March 2024 and March 2025. With these increases come two heightened risks: that employees will be targeted by phishing and that malicious emails will be sent from a reputable address the recipient is likely to trust.

Europe			**Phish-prone Percentage**
Organization Size	**Phase One - Baseline**	**Phase Two - 90 Days**	**Phase Three - 1 Year+**
1-249	24.9%	20.7%	3.9%
250-999	26.7%	21.6%	4.4%
1,000+	34.9%	20.5%	5.3%
Average PPP Across All Organization Sizes	**32.5%**	**20.7%**	**5.0%**

These results emphasize the importance of sustained security awareness training in reducing cyber risk.

Training Must Match Current Trends and Developments in the Region

Organizations must ensure that phishing training is relevant, personalized and adapted to a person's job profile, personal circumstances at work and home, and individual risk profile.

Organizations that have not already done so must elevate their training regimen this way to match the quickly changing threat landscape. Denial-of-service attacks and ransomware remain the top threats in the region, with cybercriminals leveraging geopolitics as themes and motivational drivers for campaigns. KnowBe4 has also observed a sharp increase in the quantity and quality of BEC attacks in addition to leveraging reporting deadlines as extortion tactics and AI tools as co-authors of emails and malicious PowerShell scripts.

How many simulated phishing emails are tailored to these threats — and how quickly can an organization pivot to create new training content that simulates real-world threats as the attacks they face change? Without implementing this in best-practice SAT, it's not possible to fully prepare your people and reduce phishing click rates.

We Must Combine People, Process and Technology to Protect Our Organizations

Last year, the British engineering firm ARUP fell victim to a phishing scam through its Hong Kong branch. The scam notably involved an invitation to an online meeting during which urgent financial matters were discussed. The monetary loss for the organization was significant, showing that awareness of threats and good process are essential to protect organizations. The attackers had worked around both.

In another example, a senior manager at the luxury sports car manufacturer Ferrari demonstrated great knowledge of processes that safeguard payments along with quick wit. Confronted with a suspected scammer posing as the company CEO, this senior manager challenged the caller to name a personal book recommendation the real CEO would have been able to cite.

These examples show that cybersecurity must involve people, process and technology to effectively reduce the risk of falling victim to social engineering.

> Without best-practice training, almost two in five employees (39%) will automatically click on phishing links

Compliance Is Not the Same as Security, But the Market Is Largely Compliance Driven

New regulations continue to shape the cybersecurity landscape in Europe, with the Network and Infrastructure Directive (NIS 2) and the European Union Artificial Intelligence Act (EU AI Act) setting forth training requirements for SAT and AI literacy.

However, ticking compliance checkboxes once a year is not the same as improving security in day-to-day operations. Organizations that successfully increase their cybersecurity resilience also invest in better processes, such as dedicated support teams for the workforce, positive reinforcement and rewards, and metrics that encourage secure behavior.

Key Takeaways

- **Established PPP benchmark sets the standard for organizations,** with 32% as a baseline, 20% after 90 days and 5% after one year-plus of training.
- **Regulatory requirements continue to drive the need for security education and AI literacy,** increasing the adoption of SAT.
- **Email remains the number-one attack vector for social engineering,** carrying all kinds of payloads, including ransomware, QR codes and job application scams.

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-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.