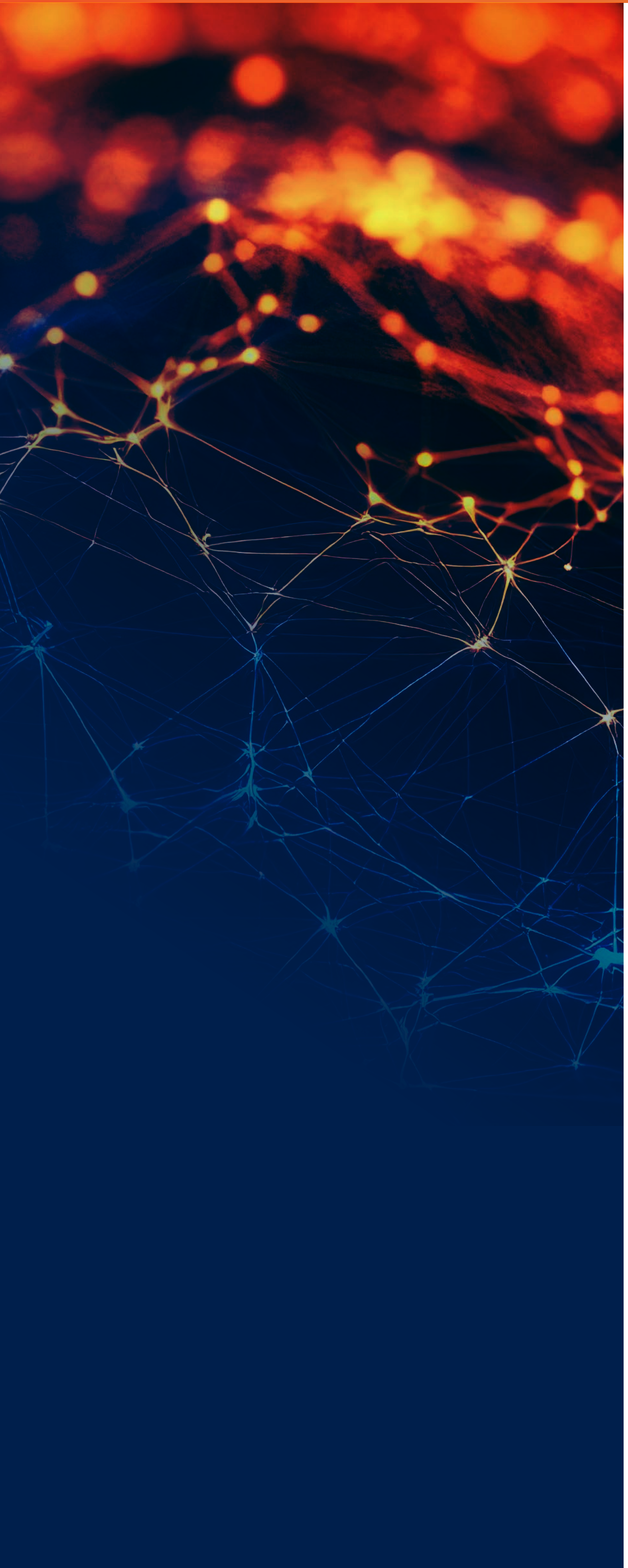
KnowBe4

Phishing Benchmarking Report

UNITED KINGDOM & IRELAND 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 United Kingdom & Ireland.

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%**		

United Kingdom & Ireland | *By Javvad Malik*

Organizations across the United Kingdom & Ireland (UK&I) that have embraced simulated phishing and training have demonstrated an impressive improvement against phishing threats. In fact, the average PPP plummeted from an initial 32.9% to a mere 4.8% after one year of sustained best-practice training. This 85.4% reduction represents a substantial improvement by any measure.

Delving into the data reveals a clear trend of improvement in phishing resilience across all organizational sizes and industries following cybersecurity training. Initially, PPPs vary widely, with small companies starting at 18-27%, medium companies at 22-44%, and large companies showing the most variability at 16-60%. Healthcare & Pharmaceuticals, Consumer Services and Hospitality tend to have higher initial vulnerabilities, especially in larger organizations.

After 90 days of training, all sectors show significant improvement, with PPPs typically reducing by 5-15%. The most dramatic changes occur after one full year of training, where the average PPP drops to 4.8%.

This demonstrates the long-term effectiveness of sustained phishing awareness programs. Notably, larger companies often start with higher vulnerability but show more substantial improvements over time, possibly due to more comprehensive training resources.
The data underscores the critical importance of ongoing cybersecurity education in substantially reducing an organization's susceptibility to phishing attacks regardless of size or industry.

Let's delve into some of the key themes that have shaped the cybersecurity scene across the UK&I over the last year.

The AI-powered Cyber Arms Race

AI has emerged as a game-changer in the cybersecurity arena, presenting both challenges and opportunities. At the end of 2023, the UK's National Cyber Security Centre (NCSC) released its guidelines on the secure development of AI systems, highlighting the growing importance of AI in cybersecurity.

United Kingdom & Ireland	Phish-prone Percentage		
Organization Size	**Phase One - Baseline**	**Phase Two - 90 Days**	**Phase Three - 1 Year+**
1-249	24.3%	22.1%	4.0%
250-999	28.5%	22.1%	4.1%
1,000+	36.0%	17.1%	5.3%
Average PPP Across All Organization Sizes	**32.9%**	**19.0%**	**4.8%**

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

The UK government's AI Cyber Security Survey, published in May 2024, further underscores the growing effect of AI on the cybersecurity landscape. The survey revealed that 45% of organizations are already using AI for cybersecurity purposes, with another 32% planning to do so in the future. Notably, 69% of organizations reported that AI has improved their ability to detect and respond to cyber threats. However, the survey also highlighted concerns, with 41% of businesses worried about potential vulnerabilities in AI systems themselves.

This data illustrates the dual nature of AI in cybersecurity: while it offers powerful tools for defense, it also introduces new vulnerabilities that organizations must address.

The Ripple Effect of Supply Chain Vulnerabilities

The interconnected nature of modern business has thrust supply chain security into the spotlight.

One notable incident was the MOVEit file transfer software breach, which affected numerous organizations across the region. The NCSC issued an urgent warning, urging businesses to patch the vulnerability immediately. This attack didn't just compromise individual companies; it exposed the web of dependencies underpinning our digital economy.

A study by SecurityScorecard in May 2024 analyzing UK FTSE 100 companies revealed alarming vulnerabilities in supply chain cybersecurity. The research found that 97% of these top companies had at least one supplier with a C, D or F rating in their cybersecurity posture. Even more concerning, 80% of FTSE 100 companies had at least one supplier who had already suffered a data breach. These findings highlight the significant risks that even the largest and most resourceful companies face due to weaknesses in their supply chain's cybersecurity, underscoring the critical need for robust vendor risk management and continuous monitoring of third-party security practices.

The ripple effect of supply chain vulnerabilities has extended beyond immediate security concerns. There has been increased tie-in with geopolitical issues, such as continued cyber threats related to the Russia and Ukraine conflict. There has also been an increase in state-sponsored attacks targeting UK infrastructure. All of this combined has led to an increased focus on supply chain security with increased global tensions.

Humans Being Human

Perhaps the most intriguing development in recent months has been the transformation of the human element in cybersecurity. Historically many organizations have exhibited dismissive attitudes, often referring to people as the weakest link. However, employees are now being recognized as a crucial line of defense against cyber threats.

This shift is exemplified by the UK Government's Cyber Aware campaign, which has moved beyond basic password advice to focus on cultivating a "cyber aware" mindset among citizens. The campaign's success lies in its ability to translate complex cybersecurity concepts into relatable, everyday behaviors.

In the corporate world, we're seeing a move away from punitive approaches to security training. Organizations are fostering a culture of cybersecurity awareness, where employees are empowered to make security decisions and report potential threats without fear of reprimand. This cultural shift is reflected in the dramatic improvement in phishing test results, particularly in larger organizations that initially struggled with higher vulnerability rates.

That's not to say that all is rosy, however. Several economic factors, such as the cost of living crisis, are leading to increased threats of insiders and social engineering susceptibility. We've also seen rising cyber insurance premiums and organizations forced to invest in cybersecurity in the face of economic pressures.

This is why it is important that security awareness activities adapt to the ever-changing threats and become integrated into the technology stack to be more personalized and relevant, providing the right awareness and training at the right time to those who need it most.

> Now, employees are being recognized
> as a crucial line of defense
> against cyber threats

Key Takeaways

- **AI is reshaping the cybersecurity battlefield, demanding** more personalized, relevant and adaptive training approaches to stay ahead of evolving threats.

- **Supply chain vulnerabilities have exposed the ever-increasing interconnected nature of cyber risks,** prompting a holistic approach to security that extends beyond organizational boundaries.

- **The human element in cybersecurity is evolving from a liability to an asset,** with cultural changes and empowerment strategies driving significant improvements in phishing resistance.

As we look to the future, it's clear that the cybersecurity landscape in the UK&I will continue to evolve. However, as the phishing results show, change doesn't happen overnight, and it needs a sustained effort to achieve and maintain improvement.

For More Information Visit KnowBe4.com →

> We need more personalized, relevant and adaptive training approaches to stay ahead of evolving threats

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.