KnowBe4

2024 PHISHING BENCHMARKING REPORT FOR THE UNITED KINGDOM AND IRELAND (UK&I)

INTRODUCTION

Year after year, cybercrime increases, casting its net wider and ensnaring more victims in both professional and personal spheres. Cybercriminals show no bias, targeting anyone at any time and anywhere. While cyber defences continue to evolve, perpetrators are shifting focus towards exploiting the softer, easier human targets. Human susceptibility remains a perennial attraction, drawing criminals to individuals across all walks of life and different roles in an organisation. Many organisations invest disproportionately in technological safeguards, often neglecting the crucial role of human-risk management.

As artificial intelligence (AI) integrates further into all aspects of technology, cybersecurity vigilance becomes increasingly important. AI systems possess the capability to rapidly analyse extensive data sets and identify patterns far beyond human capacity. This ability presents a double-edged sword; while it can significantly enhance cybersecurity measures, it also equips hackers with sophisticated tools to exploit vulnerabilities.

Cyber adversaries blend established tactics with advanced techniques to breach digital domains and undermine human-centric security measures. Effective protection requires employees to be equipped with awareness, refined habits and behaviours that support a robust security culture. Each member of an organisation must perceive themselves as integral to the defence against cyberattacks, understanding the impact of their actions on overall security.

Cybercriminals capitalise on human vulnerabilities. They exploit lapses in knowledge, prey on emotional responses, and take advantage of distractions and complacency. These human-centric tactics have proven to be highly effective as even the most robust technical security measures can be undermined by a single employee's mistake or lack of awareness.

Security leaders need to know what happens when their employees receive phishing emails: are they likely to click on the link? Get tricked into giving away credentials? Download a malware-laced attachment? Will they simply ignore the email or delete it without properly notifying their security team? Or will they report the suspected phish and play an active role in the human defence layer? By providing the knowledge, skills and tools that they need to identify and respond to potential threats, organisations can transform their people from a liability into a powerful asset.

UNDERSTANDING RISK BY INDUSTRY

The metric representing each organisation's vulnerability to phishing attempts is termed Phish-prone Percentage (PPP). By expressing phishing susceptibility in quantifiable terms, leaders are empowered to assess their potential risk of a breach and implement targeted training to diminish their workforce's susceptibility to cyber threats.

An organisation's PPP indicates the percentage of employees likely to fall for social engineering or phishing scams at any given time. As such, it is a good indicator of an organisation's risk of and resilience against such attacks.

A high PPP indicates greater risk, as it points to a higher number of employees who are likely to fall for these scams. Conversely, a low PPP means that an organisation's human layer of security is providing security strength rather than weakness. A low PPP is optimal, as it indicates that the staff is security savvy and understands how to recognise and shut down such attempts.

To help organisations evaluate their PPP and understand the implications of their ranking, KnowBe4 conducts an annual study to provide Phish-prone benchmarking across industries, organisational size and by geographical regions. This guide provides an overview of the key findings for the United Kingdom and Ireland.

2024 GLOBAL PHISHING BY INDUSTRY BENCHMARKING STUDY

While every organisation aspires to gauge its performance relative to peers within its industry, achieving a meaningful comparison requires comprehensive data and the application of a scientifically validated approach to yield credible outcomes. For many organisations, 'How do I stack up against similar organisations?' is a difficult question to answer.

That's where our annual Phishing by Industry Benchmarking Study comes in. To provide a nuanced and accurate answer, the 2024 study analysed a data set covering over 54 million simulated phishing tests across more than 11.9 million users from 55,675 organisations in 19 different industries.

Methodology for this year's study

All organisations were categorised by industry type and size. Each organisation's PPP was calculated by measuring the percentage of employees who clicked on a simulated phishing link or opened a simulated malware attachment during a KnowBe4 testing campaign.

In our 2024 report, we continue to look at the following benchmark phases:

- **Phase one:** Baseline phishing security test results
- **Phase two:** Phishing security test results within 90 days of training
- **Phase three:** Phishing security test results after one year plus of ongoing training

2024 INTERNATIONAL PHISHING BENCHMARKS

Phase one
Initial baseline phishing security test results

Phase two
Phishing security test results within 90 days of training

Phase three
Phishing security test results after one year plus of ongoing training

		BASELINE			90 DAYS			1 YEAR		
	Organisation size	1–249	250–999	1,000+	1–249	250–999	1,000+	1–249	250–999	1,000+
REGION	North America	29%	32.6%	39.1%	19.8%	19.9%	17.9%	4.3%	4.6%	4.6%
			TOTAL: 35.1%			TOTAL: 18.9%			TOTAL: 4.5%	
	Africa	29.7%	32.8%	38%	23.7%	28.7%	20.2%	3.6%	5.4%	6.2%
			TOTAL: 36.7%			TOTAL: 22%			TOTAL: 5.9%	
	Asia	31.5%	31.6%	27.4%	20.3%	17.6%	16.6%	5.4%	4.5%	5.9%
			TOTAL: 28.4%			TOTAL: 17%			TOTAL: 5.5%	
	Australia and New Zealand	27.8%	32.5%	40.3%	21.4%	20.3%	16.5%	4.9%	5.3%	4.7%
			TOTAL: 34.4%			TOTAL: 19.1%			TOTAL: 5%	
	Europe	26.5%	26.9%	35.6%	19.3%	20.2%	20.6%	4.1%	4.9%	5.9%
			TOTAL: 32.6%			TOTAL: 20.3%			TOTAL: 5.5%	
	South America	32.7%	29.4%	44.9%	24.4%	22.5%	16.8%	5.2%	5.2%	3%
			TOTAL: 39.2%			TOTAL: 18.7%			TOTAL: 3.9%	
	United Kingdom and Ireland	26.5%	30.2%	35.2%	20%	21%	16.5%	4.1%	4.3%	4.8%
			TOTAL: 32.3%			TOTAL: 18.4%			TOTAL: 4.5%	

UNITED KINGDOM AND IRELAND (UK&I)

By Javvad Malik

Benchmark data

Compared to last year, overall PPP across all organisations dropped from 35.2% to 32.3%. While small organisations remained the same, mid-sized organisations performed slightly more poorly compared to last year, with a 2% increase in PPP. However, large organisations improved the most, dropping nearly 5% from 39.6% last year to 35.2% this year.

The improvement in large organisations could be attributed to the maturity of hybrid working and mechanisms for promoting a strong security culture.

One of the key findings this year is that after a year of frequent and continuous security awareness training and simulated phishing, the average baseline has dropped to 4.3%, a significant improvement from the 5.8% of last year's report. This result underscores the effectiveness of regular and appropriate training, regardless of where an organisation starts.

Most prevalent issues

With the continued conflicts in Ukraine and the Middle East and increasing cyber tensions with China, the UK&I region faces an ever-increasing threat from nation-states and other global actors. The last year has seen an increase in nation-state actors targeting critical national infrastructure (CNI). The UK's National Cyber Security Centre (NCSC) specifically identifies China, Russia, Iran and the Democratic People's Republic of Korea (DPRK) as posing the biggest threats.

Ransomware persists as one of the most prevalent threats facing the UK&I, and phishing remains the most utilised initial access vector. This serves as a reminder that the human factor should not be ignored and that a strong security culture is imperative to protecting organisations.

With a general election upcoming, there is a risk of disruption and disinformation campaigns being used to influence the outcome and/or divide the population. While not purely a cybersecurity issue, it is one that's considerably enabled through cyber activity.

Finally, we are seeing an increase in attacks not just against organisations, but also high-risk individuals, with an ongoing trend of persistently targeting those people who may hold sensitive information. Therefore, cybersecurity is not limited to securing corporate accounts, but also personal and social media accounts and devices.

Economic impact

The economic impact of security breaches has always been tough to determine. Even for a single organisation, it can be difficult to quantify all the direct and indirect costs of a security breach.

According to the National Fraud and Cyber Crime Dashboard, over the year, there were just under 400,000 reports, with reported losses of £2.3 billion, equating to an average loss of £5,750. But it is important to note that the majority of reported cases are from individuals and not organisations. The Cyber Security Breaches Survey from the Department of Culture, Media and Sport puts the average annual cybercrime cost for businesses at approximately £15,300 per victim.

However, the larger the organisation, the more severe the consequences. Costs related to the ransomware attack on the British Library were estimated at £7 million. Royal Mail spent over £12 million on recovery costs after it was attacked, and the attack on Capita cost the British outsourcing company £20 million.

Cultural adoption/General attitudes

General attitudes vary greatly across organisations in the UK&I. Most have an understanding of security awareness. However, an increasing number of organisations, particularly large ones, are moving beyond awareness to focus on behavioural change and security culture.

According to the UK government, around 71% of organisations report that cybersecurity is a high priority for their senior management. However, in the shadow of a tough economy, many organisations, particularly smaller ones, are often sacrificing cybersecurity in favour of keeping the show on the road.

We have seen some organisations shift their approach to building a strong cybersecurity culture by moving the departments responsible for cybersecurity awareness and culture out of the CISO organisation, which often prioritises technical issues. Aligning with more people-centric objectives, some are hiring leaders with marketing backgrounds to better understand how to promote cybersecurity messaging.

While this is still rare, it is a positive sign that organisations are looking to move beyond security awareness as a mere compliance effort and to use it as a tool to make a real difference.

AI influences

Like most of the world, the UK&I are paying close attention to AI and its impact on cybersecurity.

From a criminal perspective, AI is lowering the barrier of entry to novice criminals, allowing relatively unskilled threat actors to carry out more effective access and information-gathering operations.

The near-term impact of AI on the cyber threat assessment, published by the NCSC, concludes that AI is already being used in malicious cyber activity and will almost certainly increase the volume and impact of cyberattacks – including ransomware – in the near term.

Analysis from the National Crime Agency (NCA) suggests that cybercriminals have already started to develop criminal generative AI (GenAI) and to offer GenAI-as-a-service. But these are still in the early stages of development.

Bear in mind, though, that from a cybersecurity perspective, AI does not represent a revolution. It is more of an evolution; it can introduce some efficiencies into the process, but the underlying principles remain the same. Criminals using phishing or other social engineering techniques will continue to rely on convincing victims to make poor decisions. The same principles of healthy scepticism and active reporting of suspicious interactions can maintain the security of organisations even in the case of AI-led attacks.

Key messages

- ✓ **Global threats are on the rise. Organisations of all sizes – but especially critical national infrastructure** – and individuals with access to high-risk information need to look at their defences, particularly against phishing and similar social engineering attacks.
- ✓ **Threats powered by AI will continue to rise.** These will prey on humans in the form of social engineering attacks or through disinformation campaigns. Having appropriate knowledge and spreading awareness of the issue is key.
- ✓ **Some organisations have begun to mature their awareness to work on driving behaviour change and building a strong security culture.** These organisations will fare much better in the near future when it comes to reducing risk and having a workforce that makes smarter security decisions.

UK & IRELAND	BASELINE	90 DAYS	1 YEAR
1–249	26.5%	20%	4.1%
250–999	30.2%	21%	4.3%
1,000+	35.2%	16.5%	4.8%
Average PPP across all organisation sizes	32.3%	18.4%	4.5%

Read the full report →