CCS Media

KnowBe4

2023 PHISHING BENCHMARKING

Report for the United Kingdom and Ireland

*By **Javvad Malik**, Lead Security Awareness Advocate at KnowBe4*

With the root cause of the majority of data breaches being traced to the human factor, security leaders who continue to invest solely on technology-based security layers run the risk of overlooking a best practise proven to reduce their vulnerability: security awareness training coupled with frequent simulated social engineering testing. This approach both helps raise the readiness level of humans to combat cyber crime and lays the critical foundation necessary to drive a strong security culture.

With geopolitical changes affecting the dynamics of cyber crime, organisations ought to reduce their single biggest cyber risk: the human element. Cybercriminals are counting on your employees lacking the necessary knowledge, attention and energy to trick them into making bad security decisions. One over-stressed, distracted, or daydreaming employee is all you need to let the bad actors in.

Security leaders need to know what happens when their employees receive phishing emails: are they likely to click 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?

Each organisation's employee susceptibility to these phishing attacks is known as their Phish-prone™ Percentage (PPP). By translating phishing risk into measurable terms, leaders can quantify their breach likelihood and adopt training that reduces their human attack surface.

To assist geographical regions with evaluating their PPP and understanding the implications of their ranking, KnowBe4 conducts an annual study to provide definitive Phish-prone benchmarking across small, medium and large organisations by geographical regions. This guide provides an overview of the key findings for the United Kingdom and Ireland (UK&I).

2023 Global Phishing By Industry Benchmarking Study

Though every organisation would like to understand how they measure against the rest in their industry and geography, the comparison requires robust data coupled with a scientific, proven method to produce valid results. To provide a nuanced and accurate answer, the 2023 Phishing By Industry Benchmarking Study analysed a data set of over 12.5 million users, across 35,681 organisations, with over 32.1 million simulated phishing security tests, across 19 different industries and seven geographic regions.

All organisations were categorised by size and geographical region. To calculate each organisation's PPP, we measured the number of employees who clicked a simulated phishing email link or opened an infected attachment during a testing campaign using the KnowBe4 platform.

In our 2023 report, we continue to look at the following three benchmark phases:

PHASE ONE

If you have not trained your users and you send a phishing attack, what is the initial resulting PPP?

To do this, we monitored employee susceptibility to an initial baseline simulated phishing security test. From that established set of users, we look at any time a user has failed a simulated phishing security test prior to having completed any training.

PHASE TWO

What is the resulting PPP after your users complete training and receive simulated phishing security tests within 90 days after training?

We answered this question by finding when users completed their first training event and looking for all simulated phishing security events up to 90 days after that training was completed.

PHASE THREE

What is the final resulting PPP after your users take ongoing training and monthly simulated phishing tests?

To answer this, we measured security awareness skills after 12 months or more of ongoing training and simulated phishing security tests, looked for users who completed training at least one year ago, and took the performance results on their very last phishing test.

2023 International Phishing Benchmarking Results By Geographical Regions

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**	**1000+**	**1-249**	**250-999**	**1000+**	**1-249**	**250-999**	**1000+**
North America	28%	30.1%	37.1%	18.5%	19%	18.4%	4.2%	5.1%	5.7%
	TOTAL: 33.1%			**TOTAL: 18.6%**			**TOTAL: 5.1%**		
Africa	30%	29.4%	33.3%	25.2%	22.7%	19.3%	9%	10.5%	5.7%
	TOTAL: 32.8%			**TOTAL: 20.5%**			**TOTAL: 6.6%**		
Asia	32.6%	33.2%	28.8%	20.9%	19.6%	13%	7.3%	7.4%	6%
	TOTAL: 30%			**TOTAL: 14.9%**			**TOTAL: 6.5%**		
Australia & New Zealand	27.1%	30.9%	41.1%	21.1%	19.9%	15.3%	6.3%	7.7%	5.4%
	TOTAL: 34.8%			**TOTAL: 17.8%**			**TOTAL: 6.4%**		
Europe	26.5%	28%	36.2%	19.1%	19.7%	19.4%	6.7%	7.6%	6.1%
	TOTAL: 32.9%			**TOTAL: 19.4%**			**TOTAL: 6.5%**		
South America	34%	27.7%	49.5%	23%	25.8%	18.7%	6.4%	10.2%	5.1%
	TOTAL: 41.1%			**TOTAL: 21.3%**			**TOTAL: 6.9%**		
United Kingdom & Ireland	26.3%	28%	39.6%	18.5%	18.1%	17.6%	6.1%	8.1%	4.9%
	TOTAL: 35.2%			**TOTAL: 17.8%**			**TOTAL: 5.8%**		

Most Prevalent Issues Facing The United Kingdom and Ireland

The UK&I region is experiencing a challenging period as they combat multiple crises simultaneously. The global outbreak of COVID-19 has caused significant harm to both public health and the economy, leading to widespread unemployment and declining economic activity. The United Kingdom's departure from the European Union has also posed a significant challenge to the region, bringing with it supply chain issues and significant uncertainties for business owners. Additionally, the ongoing Russia-Ukraine conflict has increased cybersecurity risks and has become an issue of utmost concern to organisations operating in the region.

From a cybersecurity perspective, it's a rather grim picture. Ransomware not only continues, but we are beginning to see just how much of a lasting impact ransomware has on organisations. Government departments and critical infrastructure are increasingly targeted.

Threats to the global supply chain continued to be apparent where attackers accessed target victim organisation's networks or systems via third-party vendors or suppliers. Meanwhile, disclosure of the Log4J vulnerability highlighted challenges where weaknesses in IT systems are exploited to deliver successful attacks.

Criminals upped the ante with social engineering attacks by taking advantage of issues, such as government energy grants or tax returns, and were seen to increasingly use SMS and voice-based phishing attacks (smishing and vishing).

The National Cyber Security Centre's (NCSC) annual review states, unsurprisingly, that the most significant threat facing citizens and small organisations continues to be from cyber crime such as phishing, while hacking of social media accounts also remains an issue.

Economic Impact

The true economic impact remains difficult to quantify due to inconsistent and sometimes non-existent reporting metrics. However, from what we do know, the reported costs are just a fraction of the actual figures.

Sophos reports that ransomware attacks are the most prominent, with 13% of UK organisations paying ransom at an average cost of £882,409 ($1.1 million).

But direct costs are not the only thing to consider. After suffering a ransomware attack in October 2020, Hackney Council published its accounts showing the London authority spent over £12 million ($11.7 million) to help it recover from the ransomware attack. Some of the costs included £444,000 ($553,488) on IT consultancy, £152,000 ($189,482) on recovery of the social care system, and £572,000 ($713,052) on the housing register.

UK & IRELAND	BASELINE	90 DAYS	1 YEAR
1-249	26.3%	18.5%	6.1%
250-999	28%	18.1%	8.1%
1000+	39.6%	17.6%	4.9%
Average PPP Across All Organisation Sizes	35.2%	17.8%	5.8%

Other councils have had it even worse. Gloucester City Council was hit in 2021, and as a result, its museum is unable to access its artefact database to date. While the overall attack is estimated to have cost the council £1 million ($1.2 million), the potential long-term damage to unavailable systems could be far more.

The attacks spotlight the need for the government to invest more in local services, as well as keep a close eye on critical national infrastructure.

Attacks aside, the other big economic impacts are through fines and reporting. Between January 2022 and January 2023, the UK had over 10,000 personal data breach notifications under the General Data Protection Regulation (GDPR).

According to a 2022 National Fraud and Cyber Crime Dashboard, there were 289,330 reports with total losses of £3.7 billion ($4.6 billion). Most of this was fraud as opposed to cyber crime, but the majority of attacks were cyber-enabled.

Typical Organisation Profile

Compared to last year, we see the overall PPP across all organisations has taken a jump from 30% to 35.2%. The biggest contributor to this increase are large enterprises with over 1000 employees which went from 32.7% to nearly 40%. There are probably many contributing factors to this increase, ranging from hybrid working models, to staff turnover. However, despite the initial bleak outlook - the silver lining here is that with frequent security awareness training and simulated phishing, the baseline can be drastically reduced to 17.6% in just 90 days and below 5% after a year. Highlighting how effective regular and appropriate training can be regardless of the starting point.

Cultural Adoption and General Attitudes

While threats continue to impact the UK&I, the region is becoming more vigilant about cybersecurity and the importance of educating the workforce and individuals about the role they can play in protecting themselves and their organisations.

Phishing remains the single largest threat vector and is the most popular way ransomware infiltrates organisations. While technical controls are required, the cost and time needed to make these technical changes, especially in underfunded government departments, may take too long. It is imperative that appropriate and timely security awareness and training is rolled out to reduce the risk.

The UK government has spoken about the risks of China for some time now. But with its intent to ban the likes of Huawei and apps like TikTok for official purposes, it seems as if the future of cybersecurity in the region will depend heavily on how China responds. It's also important to remember the continued digital threat Iran and North Korea pose, though admittedly not as sophisticated as China.

Key Takeaways

Cybersecurity remains a huge concern for the UK&I across many fronts. Social engineering is the biggest attack vector, and more needs to be done to promote awareness in organisations and individuals as to the role everyone plays in maintaining security.

With advancements in AI as well as deep fake technologies, we can only imagine how more sophisticated social engineering attacks will become, therefore increasing the need for all organisations across every industry to beef up their defences.

Three key takeaways are:

- ✓ While ransomware continues to be a menace, supply chain issues and the geopolitical climate make for an increasingly tricky situation for organisations to stay ahead of.
- ✓ The impact of breaches is proving to be more far-reaching in terms of cost and time than previously thought. Organisations could be paying off the debt of a breach for many years to come. Therefore, stopping attacks becomes an even greater priority.
- ✓ Although some organisations may have a poor starting point, changing the overall security culture and investing in a solid security awareness and training strategy can provide a rapid return on investment and significantly reduce risk.