KnowBe4

2023 PHISHING BENCHMARKING

Report For Europe

By ***Jelle Wieringa***, *Security Awareness Advocate for EMEA 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 Europe.

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 Europe

The continuing conflict between Russia-Ukraine has impacted societies across Europe. The ENISA Threat Landscape Report 2022 describes an increase in hacktivist activity, its mobilisation and aid by nation-state groups during this conflict. Because of the Russia-Ukraine conflict, disinformation has become a favoured tool in cyber warfare. We've seen great technological advances in the fields of AI, such as generative AI and machine learning, which make its malicious application more accessible to bad actors. AI-enabled social engineering attacks, disinformation, and deep fakes have become de facto threats that organisations now must protect against.

The most prevalent cyber threats are still ransomware, malware and social engineering. According to the latest "What CEOs talked about" report by IOT-Analytics, economic uncertainties (inflation, recession and interest rates) still dominate what is top-of-mind with organisational leaders. And even though these are very important topics, the continuing threat of cyber crime warrants more attention from the C-suite. Ignoring this leaves the door wide open for threat actors to continue their nefarious activities on unprepared organisations.

Economic Impact

While the economic impact of cyber crime in Europe is hard to accurately determine, it is widely accepted that the impact can have financially devastating consequences.

Under the General Data Protection Regulation (GDPR), organisations that fall victim to data breaches can be forced to pay claim compensation to impacted customers. Legal fees, non-compliance fees, and cost of investigation into the incident can rise into the millions, not to mention the possible reduction in (or cessation of) production, delayed orders and reputational loss with suppliers and customers.

The economic impact of cyber crime applies to all organisations, not just ones that fall victim to a cyber attack. The rising shortage of qualified cybersecurity staff, and the widening skill gap that comes with it, forces organisations to spend more money maintaining security operations. Heavier workloads, unfilled positions and worker burnout all lead to understaffed security organisations. According to the World Economic Forum, the global cybersecurity workforce needs to grow by 65% to effectively defend an organisation's critical assets. This leads to an added pressure to the already strained IT security budgets at organisations.

EUROPE	BASELINE	90 DAYS	1 YEAR
1-249	26.5%	19.1%	6.7%
250-999	28%	19.7%	7.6%
1000+	36.2%	19.4%	6.1%
Average PPP Across All Organisation Sizes	32.9%	19.4%	6.8%

Typical Organisation Profile

Unfortunately, this year's PPP data covering Europe shows us that there are many organisations that could improve on their efforts to combat cyber crime. Overall, in Europe, smaller organisations (1–249 employees) score best, with an average PPP across industries before training of 26.5%. Followed by medium (250 – 999 employees) with an industry average PPP of 28% and then large enterprise organisations (1000+ employees) scoring an average of 36.2%.

These results are consistent with those from 2022 showing larger organisations being most vulnerable to cyber attacks. While the efforts of the governing bodies in the European Union continue to update and form new policies like the recent Network and Information Security Directive (NIS2), it does not apply to all organisations, since not all countries are member states of the EU.

Cultural Adoption and General Attitudes

The growing increase in cyber crime throughout Europe, mixed with laws, regulations and legislation put in place to protect organisations and consumers alike, forced many organisations to actively work on their cybersecurity maturity. The ISACA "State of Cybersecurity 2022" indicates that 66% of organisations are actively assessing their cybersecurity maturity level by increasing their assessments to more than once a year.

The increased cost of security, caused in part by the increase in cyber crime and the widening IT security skill gap, forces organisations to "do more with the same, or less." Technology spend alone will not provide a sufficient coverage of the security posture of an organisation. Thus, security organisations need to look for other, more efficient and cost effective ways to defend. This movement triggered an increased interest in the importance of a strong security culture, defined as the ideas, customs and social behaviours of an organisation that influence its security. Organisations have begun to actively shape their security culture and use this definition as a central and guiding principle to develop their security posture. This gives their existing workforce (e.g. the "people" element within the people-process-technology triad) a more prominent position in their security strategy.

With digital transformation still being a key focus for many European organisations, the top-of-mind approach that security culture brings to security as a business enabler proves alluring for many security organisations. A 2023 report by Deloitte Global Future of Cyber Survey shows that collaboration across cybersecurity, risk management, and business units is critical to neutralizing cyber threats, protecting business value, and sustaining customer trust. This makes security culture an ideal instrument for any organisation.

Key Takeaways

Cybersecurity remains one of the biggest concerns to the business continuity of organisations all throughout Europe. With an average PPP of 32.9%, (up from 29.9% in 2022) organisations are still vulnerable to social engineering attacks across all verticals and countries of Europe. It remains vital that we continue our efforts to further increase our resilience and lower our risk posture.

Three key takeaways are:

✓ **Intensify the efforts to increase the resilience of European organisations.** Geopolitical and economic threats have diverted our attention away from cybersecurity. And with the increase of digitization of organisation, the impact of cyber attacks is likely to increase as well.

✓ **Focus on educating audiences about the threat and impact of AI-enabled cyber attacks.** With the increased sophistication and developments in machine learning, such as deep fakes and voice biometrics, threat actors now have powerful tools to create misleading content to augment their already dangerous attacks. Because of the increased realism this brings to existing forms of attacks, it is imperative to educate people about these new attack forms.

✓ **Increase efforts to build a strong security culture.** The holistic approach it brings to combine security awareness and shape secure behaviours is a proven method to reduce risks and enable business at the same time.