KnowBe4

2023 PHISHING BENCHMARKING

Report For Germany, Austria and Switzerland

By ***Dr. Martin J. Kraemer***, *Security Awareness Advocate, 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 practice 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, organizations 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 defense layer?

Each organization'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 organizations by geographical regions. This guide provides an overview of the key findings for Germany, Austria and Switzerland (DACH) relative to the rest of the globe.

2023 Global Phishing By Industry Benchmarking Study

Though every organization would like to understand how they measure against organizations in their industry and/or throughout the world, the comparison requires robust data coupled with a scientific, proven method to produce meaningfully valid results. The struggle to answer the question "How do I compare with other organizations that look like me?" is very real. To provide a nuanced and accurate answer, the 2023 Phishing By Industry Benchmarking Study analyzed a data set of over 12.5 million users, across 35,681 organizations, with over 32.1 million simulated phishing security tests, across 19 different industries world-wide.

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 mobilization and aid by nations-state groups during this conflict. Because of the Russia-Ukraine conflict, disinformation has become a favored tool in cyber warfare. We've seen great technological advances in the fields of artificial intelligence (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 organizations now must protect against.

The most prevalent cyber threats in the region 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 business 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 organizations.

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), organizations 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 organizations, 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 organizations to spend more money maintaining security operations. Heavier workloads, unfilled positions and worker burnout all lead to understaffed security organizations. According to the World Economic Forum, the global cybersecurity workforce needs to grow by 65% to effectively defend an organization's critical assets. This leads to an added pressure to the already strained IT security budgets at organizations.

DACH	BASELINE	90 DAYS	1 YEAR
1-249	26.3%	17.4%	7.7%
250-999	26%	19.1%	7.8%
1000+	34.1%	21%	4.5%
Average PPP Across All Organisation Sizes	30.9%	20%	5.6%
Average PPP Across All Organization Sizes For Europe	32.9%	19.4%	6.8%

Typical Business Profile

Generally speaking, the DACH region scores the same or slightly better when compared to the rest of Europe. The average PPP across all organizations in DACH for Phase 1 and Phase 3 is slightly better than the average PPP across all organizations in Europe (see chart above).

Within DACH, medium organizations (250-999 employees) score best before any training has been initiated, with an average PPP across industries of 26%. This is followed by small organizations (1-249 employees) with an industry average PPP of 26.32%, and then large enterprise organizations (1000+ employees) scoring an average of 34%

Small and medium-sized enterprises represent 99% of all businesses in the EU. According to Statista, as of 2020, approximately 93.3% of enterprises in the non-financial business economy of Europe were micro-sized and employed up to nine people. In the same year, approximately 5.7% were defined as small businesses (10-49 employees), 0.9% were medium-sized (50-249) and 0.2% were large businesses that employed 250 or more people.

Key Takeaways

Three key takeaways are:

- ✓ Intensify the efforts to increase the resilience of European organizations. Geopolitical and economic threats have diverted our attention away from cybersecurity. While the region has seen relatively small increases in hacktivism, the changing geopolitical landscape is on the radar of decision makers.
- ✓ 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. Misinformation is a growing threat. 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 behaviors is a proven method to reduce risks and enable business at the same time. Security awareness professionals must continue building campaigns that seek to foster secure behaviors. Organizations must seek to foster a resilience for cybersecurity.