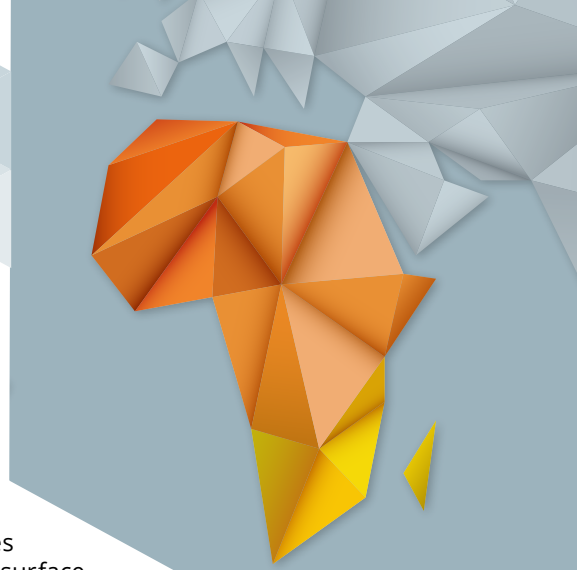
KnowBe4

2023 PHISHING BENCHMARKING

Report for Africa

*By **Anna Collard**, Senior Vice President of Content Strategy & Evangelist for KnowBe4 Africa*



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 Africa.

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 Africa

A region of growth, Africa is rapidly increasing its usage of technology and connectivity. But with growth, prosperity and digitisation comes new risks and vulnerabilities that can undermine progress.

According to the KnowBe4 and IDC Report on Cyber Extortion in Africa, nearly 60% of organisations across Southern Africa planned to increase their connectivity and IoT over the next 12 months. This growth unfortunately means a larger attack surface area. The rise of smartphone penetration, online banking mobile payment networks and cryptocurrency is providing criminals across Africa with new targets and avenues of finance. There is a linear relationship between the continent's GDP and cyber crime; as one increases, so does the other. As a result, Africa has had the most exponential growth in cyber crimes over the last few years, particularly among small and medium-sized organisations.

To address rising cyber crime, some African countries have imposed strict regulatory compliance laws, however the majority of African countries have not. Currently, only 15 of 55 African countries have ratified the African Union Malabo Convention, which is a legislative framework to foster data protection and general safeguards against cyber crime; 11 countries have partial laws; and 30 have no meaningful cyber crime laws at all. Governments frequently do not adequately monitor threats, collect digital forensic evidence, and do not prosecute computer-based crime.

As highlighted in last year's report, one of Africa's biggest cybersecurity issues remains the skills shortage. The continent faces a growing lack of certified cybersecurity professionals. Many organisations, agencies and consumers lack cyber awareness and organisations fail to implement basic cybersecurity controls.

We predict that cyber extortion groups and cyber crime syndicates will shift their attention away from the more mature nations like the U.S. towards other regions, including emerging economies like Africa where industries have a large cyber dependency but lack the resources to adequately prevent, remediate or prosecute cybercriminals.

AFRICA	BASELINE	90 DAYS	1 YEAR
1-249	30%	25.2%	9%
250-999	29.4%	22.7%	10.5%
1000+	33.3%	19.3%	5.7%
Average PPP Across All Organisation Sizes	32.8%	20.5%	6.6%

Economic Impact

It is difficult to estimate how much cyber crime really impacts the African economy as incidents and financial impact are not officially disclosed. Most cybersecurity incidents go unreported.

As stated in the 2022 research report by the Global Initiative against Transnational Crime, "The Downside of Digital Revolution," "the spread of digital technology has led to the formation of new organised cybercriminal networks, which now rank among the top threats to African enterprises and is estimated to cost the region's economy billions of dollars per year."

The South African Council for Scientific and Industrial Research (CSIR) expects an increase in cyber attacks on government departments and critical infrastructure, impacting not just private sector organisations but societies and countries' economies. This was the case with the ransomware attack against South Africa's Transnet, a state-owned ports authority enterprise, in 2021. The incident impacted the country's critical maritime infrastructure and undermined South Africa's economic recovery from the COVID-19 pandemic. Attacks against critical infrastructure can result in devastating economic consequences that go beyond the direct losses experienced by the affected organisation.

Typical Organisation Profile

Africa is a region of considerable geographic, linguistic, cultural and economic diversity. When delving into the state of cybersecurity on the continent, this diversity must be taken into account and can, to some extent, explain the wide variety in the security maturity across different countries and sectors.

Africa's potential as a growth market for business remains underestimated and misunderstood. More than 400 companies in Africa earn annual revenues of $1 billion or more; and they are, on average, faster growing and more profitable than their global peers.

This year's KnowBe4 Phishing By Industry Benchmark Report is based on a total of 337,937 phishing simulation tests delivered across 412 African organisations. Of these, 58% of the organisations are small (1-249 employees), 26% are medium (250-999 employees) and 16% are large organisations (1000+ employees). Most of the data set is derived from organisations in South Africa, followed by Kenya, Nigeria and Botswana.

In Africa, the initial baseline phishing security test results are at an average of 32.8%. That means that before receiving any training, one out of three employees is likely to click on a suspicious link or email or comply with a fraudulent request. Overall PPP varied greatly across African sectors and countries.

Africa's potential as a growth market for business remains underestimated and misunderstood. **More than 400 companies in Africa earn annual revenues of $1 billion or more...**

...and they are, on average, faster growing and more profitable than their global peers.

Cultural Adoption and General Attitudes

Many African countries face unique and complex socioeconomic landscapes, and the challenges faced internationally are compounded even further on a local level.

For example, South Africa is one of the most unequal countries in the world, resulting in a high rate of poverty and unemployment rate, and increase in its crime rate.

With a **median age of just 19.7 years**, Africa has the youngest population in the world. And Africa's growing youth is demanding access to global connectivity while driving technology adoption and digitalisation: mobile smart device ownership is growing exponentially, social media use is increasing and so is the adoption of cryptocurrencies. According to the International Monetary Fund (IMF), sub-Saharan Africa is the only region in the world where nearly 10% of its gross domestic product is generated through mobile money. People across the continent depend on their mobile devices for remittances, salaries, payments, bills and shopping.

KnowBe4's Africa End User Cyber Awareness Survey 2023 uncovered that:

- 71% of the respondents from eight African countries use their mobile data to access the internet, while 63% use their mobile phone for mobile banking and payments
- 68% of the respondents were concerned about cyber crime, however, many lacked some very basic understanding of what type of threats they are exposed to
- 57% of respondents did not know what a ransomware attack is. 21% have experienced a social engineering attack over the phone (vishing) and 32% have lost money because they fell victim to a scam
- 36% said they had fallen victim to a crypto scam, and 57% knew people who had been victims of such scams

Based on a 2022 survey run by KnowBe4 and ITWeb in South Africa, the number one reason for people making security mistakes, such as clicking on a phishing email, was cited as lack of awareness or training (52%), followed by distraction, multitasking and cognitive overload (38%).

Key Takeaways

- ✓ The lack of prioritisation and investment for cybersecurity amongst both businesses and governments needs to be addressed. Raising awareness among policy makers and assisting in capacity building efforts should be prioritised.
- ✓ Public-private partnerships are needed to assist Africa in its cybersecurity challenges. Businesses in this region often cannot afford even the most basic security controls. Those that can invest struggle to find those who have cybersecurity skills. The private sector, particularly financial services sectors, possess human capital, infrastructure, capabilities, and expertise in cybersecurity that governments lack.
- ✓ Organisations training employees and their customers about security best practices remains critical. Governments and education institutions need to invest in expanding their security professional capacity as well as making cybersecurity awareness a life skill for every youth entering the workforce.