

KnowBe4

2023 PHISHING BENCHMARKING

Report For South America

By **Rafael Silva**, Senior Director of Information Security for 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 South America.

2023 Global Phishing By Industry Benchmarking Study

Though every organization 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 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 and seven geographic regions.

All organizations were categorized by size and geographical region. To calculate each organization'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

Organization Size	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		
	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 South America

Ransomware, phishing and mobile phone theft are among the top threats of 2022 for both organizations and individuals in Latin America. A report from the [Brazilian Agency of Communication \(Anatel\)](#) revealed that in Sao Paulo, Brazil alone, 553 corporate and personal cell phones are stolen daily.

Latin American organizations experienced a significant increase in ransomware attacks in 2022; however, most organizations have not paid to regain access to their data. According to a study titled "[The State of Ransomware 2022](#)" conducted by cybersecurity firm Sophos, 55% of the 200 surveyed organizations in Brazil were targeted by ransomware attacks last year. In comparison, the reported percentage in 2020 was 38%.

In 2022, phishing attacks continued to be a major concern for Latin American organizations and individuals. The increase in remote work and back-to-office due to the COVID-19 pandemic created new opportunities for cybercriminals to exploit vulnerabilities and target unsuspecting users. Cybercriminals consistently pursue critical and sensitive data, such as login credentials, financial information, and personal identification details.

This year, they have significantly increased their focus on cryptocurrency phishing, with a 40 percent growth in just one year, as [reported by Kaspersky](#).

Account takeover attacks that are specifically focused on social media and cryptocurrency have substantially increased across Latin America. This is primarily because social media and cryptocurrencies are rapidly gaining notoriety amongst fraudsters and attackers alike. There will be a marked rise in the number of cybercriminals who attempt to gain unauthorized access to social media accounts and cryptocurrencies to use them to perpetrate further acts of fraud and deception.

Economic Impact

Ransomware continues to have a major financial impact on Latin American organizations, causing significant losses. In 2022 alone, a [Brazilian e-commerce company](#) fell victim to a ransomware attack, resulting in a staggering loss of \$183 million. This number has been on a consistent upward trend year after year.

In 2022, Brazil began imposing fines for privacy violations in order to comply with the General Data Protection Law (LGPD). It is estimated that millions of dollars will be paid to the National Data Protection Authority (ANPD) due to security breaches and privacy violations.

S. AMERICA	BASELINE	90 DAYS	1 YEAR
1-249	34%	23%	6.4%
250-999	27.7%	25.8%	10.2%
1000+	49.5%	18.7%	5.1%
Average PPP Across All Organization Sizes	41.1%	21.3%	6.9%

As the digital landscape continues to evolve, Latin American governments and organizations must prioritize investments in cybersecurity and collaborate to develop robust strategies to prevent future attacks and mitigate their financial consequences.

Typical Organization Profile

Some industries are better than others at promoting a security culture, with the Technology and Insurance industries performing better than the Healthcare & Pharmaceutical, Retail & Wholesale industries. There is significant room for improvement in South America, as indicated by the high PPP across the board. In particular, both small organizations (1-249 employees) and enterprise organizations (1000+ employees) have high baseline PPP compared to most other regions around the world.

Alongside its yearly phishing statistics per industry, [KnowBe4 also puts together an annual security culture report](#). This data provides interesting viewpoints and context about different sectors. The Hospitality, Education, and Construction industries recorded the lowest scores, only reaching (70), indicating less developed security cultures. The Retail and Wholesale sectors didn't fare much better, registering a slightly higher score of (71). However, industries such as Technology and Insurance, each scoring (76), showcased more advanced and evolving security cultures.

South America with a (73) overall score, has been facing a significant challenge in terms of security culture. However, it is noteworthy that Chile (71), Colombia (77), and Brazil (72) stand out with high scores, indicating a much higher level of security culture than the other countries.

Organizations operating in South America must take proactive measures to improve their security culture, given the prevailing low scores in most countries. It is crucial to prioritize security measures to ensure the safety and protection of people and assets, as security threats evolve and become more sophisticated.

Cultural Adoption and General Attitudes

Cultural adoption and general attitudes play a critical role in cybersecurity in Latin America. In recent years, the region has experienced a significant increase in cyber attacks. This increase highlights the importance of fostering a positive security culture to increase the security posture for both organizations and individuals.

Cultural adoption refers to the degree to which people and organizations adopt and use cybersecurity practices and technologies. In Latin America, there is a general lack of awareness and understanding of cybersecurity threats, which has resulted in a low level of cultural adoption.

However, attitudes toward cybersecurity are changing in the region, as more people become aware of the risks associated with cyber attacks. Governments and businesses are starting to invest more in cybersecurity initiatives, and individuals are beginning to take steps to protect themselves online.

Sound and useful initiatives are being created, like the national [legislation of Costa Rica](#), which has been revised to provide legal protection for its cyber society, thereby enabling individuals to report violations that were previously not addressed by the law.

Key Takeaways

- ✓ The growing issue of mobile phone theft in Latin America in 2022 underscores the need to protect sensitive data stored on mobile devices. Individuals should use strong passwords or biometric authentication, enable remote wiping capabilities, and install security apps to safeguard their devices. Moreover, governments and law enforcement agencies should work together to tackle organized crime related to mobile phone theft and create public awareness campaigns to inform citizens about the risks and preventive measures.
- ✓ Implementing advanced cryptographic techniques, two-factor authentication (2FA), and hardware keys significantly bolster the protection of your digital assets to make it increasingly difficult for cybercriminals to succeed. As a convenient and easy-to-use option, hardware keys can be easily integrated into a variety of systems and platforms, making it an accessible choice for users of all technical backgrounds.
- ✓ Investing in security awareness is crucial for organizations as it helps foster a strong security culture, empowering employees with knowledge and tools to identify, avoid, and report potential cyber threats, ultimately minimizing the risk of security breaches. By providing comprehensive training and ongoing education, organizations can significantly reduce the likelihood of human error or negligence.