KnowBe4

PHISHING BY INDUSTRY 2020

BENCHMARKING REPORT

VERIZON'S 2019 DATA BREACH INVESTIGATION REPORT SHOWS THAT **PHISHING REMAINS THE #1 THREAT ACTION** USED IN SUCCESSFUL BREACHES LINKED TO SOCIAL ENGINEERING AND MALWARE ATTACKS.

INTRODUCTION

As cybercrime continues to surge, security leaders must understand that there is no such thing as a perfect, fool-proof, impenetrable secure environment. Many organizations fall into the trap of trying to use technology as the only means of defending their networks and forgetting that the power of human awareness and intervention is paramount in arriving to a highly secured state. Every security leader faces the same conundrum: even as they increase their investment in sophisticated security orchestration, cybercrime continues to rise. Security is often presented as a race between effective technologies and clever attack methodologies. Yet there's an overlooked layer that can radically reduce an organization's vulnerability: **security awareness training and frequent simulated social engineering testing**.

Verizon's 2019 Data Breach Investigation Report shows that phishing remains the #1 threat action used in successful breaches linked to social engineering and malware attacks. These criminals successfully evade an organization's security controls by using clever phishing and social engineering tactics that often rely on employee naivete. Emails, phone calls and other outreach methods are designed to persuade staff to take steps that provide criminals with access to company data and funds.

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.

Understanding Risk by Industry

An organization's PPP indicates how many of their employees are likely to fall for social engineering or phishing scams. These are the employees who might be fooled into opening a file infected with malware or transferring company funds to a fraudulent offshore bank account. A high PPP indicates greater risk, as it points to a higher number of employees who typically fall for these scams. A low PPP is optimal, as it indicates the staff is security-savvy and understands how to recognize and shut down such attempts. In short, a low PPP means that an organization's human security layer is providing security strength rather than weakness.

The overall Phish-Prone percentage offers even more value when placed in context. After seeing their PPP, many leaders ask questions such as "How does my organization compare to others?" and "What can we do to reduce our Phish-Prone percentage?"

KnowBe4, the world's largest Security Awareness Training and Simulated Phishing platform, has helped tens of thousands of organizations reduce their vulnerability by training their staff to recognize and respond appropriately to common scams. To help companies evaluate their PPP and understand the implications of their ranking, KnowBe4 conducts an annual study to provide definitive Phish-Prone benchmarking across industries. Categorized by industry vertical, organization size, and the amount or frequency of security awareness training, the study reveals patterns that can light the way to a stronger and safer future.

2020 PHISHING BY INDUSTRY BENCHMARKING STUDY

Every company struggles to answer an essential question—"How do I compare with other organizations who look like me?" To provide a nuanced and accurate answer, the 2020 Phishing By Industry Benchmarking Study analyzed a data set of over 4 million users across 17,000 organizations with over 9.5 million simulated phishing security tests across 19 different industries.

All organizations were categorized by industry type and size. To calculate each organization's Phish-Prone percentage, we measured the number of employees that clicked a simulated phishing email link or opened an infected attachment during a testing campaign using the KnowBe4 platform.

Methodology For This Year's Study

Over the past year, we have experienced explosive growth resulting in a significantly large pool of globally diverse data. This data has become much more reflective of the current state of actual organizations. Each year we reevaluate our approach. This year we concluded that it was time to refine our processes for data-pulls and analysis so that the processes are scalable in the long term for future reporting. As a result, we adjusted our approach for the 2020 study.

To calculate each organization's **Phish-Prone percentage**, we measured the number of employees that clicked a simulated phishing email link or opened an infected attachment during a testing campaign using the KnowBe4 platform.

In the past, we looked at three benchmark phases: Baseline phishing security test results, Phishing test results at 90-Day performance, and phishing test results at One Year performance. Through our analysis, we noticed that the way organizations use our platform varies, so we adjusted our lens for a new method of benchmarking. We continue to focus on the same first phase of the initial baseline phishing security test results, but we recalibrated phases two and three to measure Phishing security test results within 90 Days after employee training, and Phishing security test results after One Year or more of ongoing employee training.

For simplification purposes, we will refer to these benchmark phases as:

- **Phase One:** 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

Analyzing Training Impact

To understand the impact of security awareness training, we measured outcomes at these three touchpoints to answer the following questions:

1. **Phase One: If you haven't 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.

2. **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 look for all simulated phishing security events up to 90 days after that training is completed.

3. **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 and look for users that completed training at least one year ago and take the performance results on their very last phishing test.

METHODOLOGY AND DATA SET

17 thousand organizations

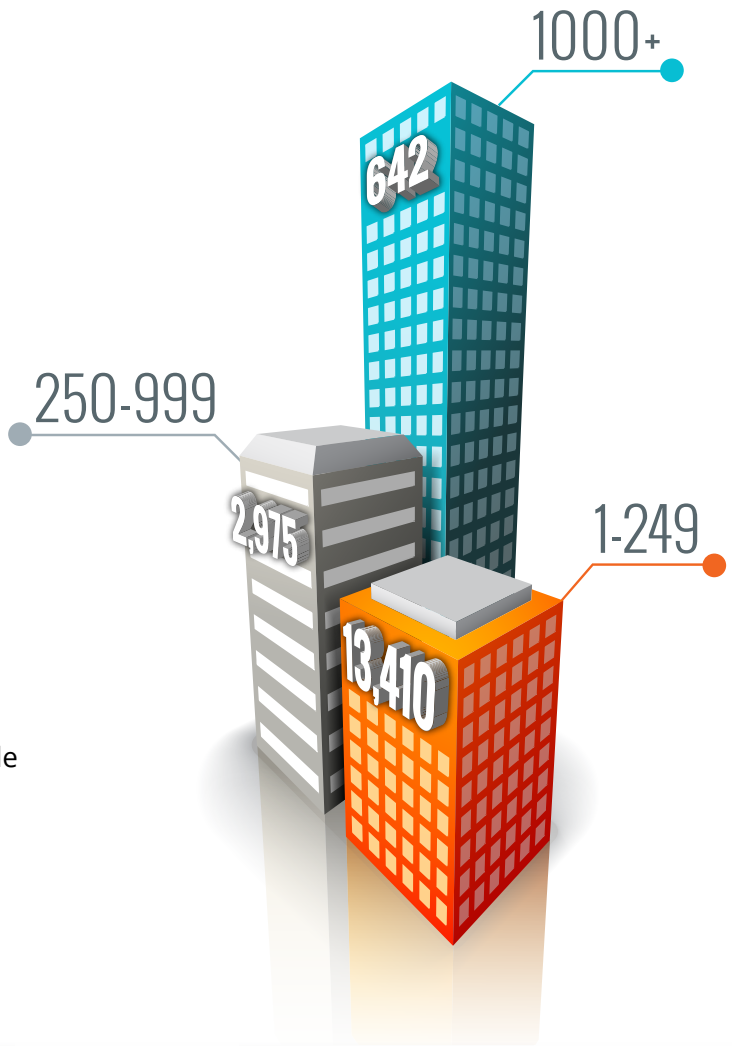
4 million users

9.5 million phishing security tests

19 INDUSTRIES

- Banking
- Business Services
- Construction
- Consulting
- Consumer Services
- Education
- Energy & Utilities
- Financial Services
- Government
- Healthcare & Pharmaceuticals
- Hospitality
- Insurance
- Legal
- Manufacturing
- Not For Profit
- Other
- Retail & Wholesale
- Technology
- Transportation

ORGANIZATION SIZE RANGES



WHO'S AT RISK: RANKING INDUSTRY VULNERABILITY

The results across the four million users highlight a sobering truth for organizations that don't feel the need or choose not to invest in security awareness training which includes phishing security tests. The Phish-Prone percentage data shows that no single industry across all-sized organizations is doing a good job at recognizing the cybercriminals phishing and social engineering tactics. When users have not been tested or trained, the initial baseline phishing security tests show how likely users in these industries are to fall victim to a phishing scam and put their companies at risk for potential compromise.

The overall PPP average across all industries and size organizations was **37.9%**. Trends varied across different industries, revealing the bleak truth that untrained users are failing as an organization's last line of defense against phishing attacks.

Specific trends show industry Phish-Prone percentages increased across almost all industries at initial baseline testing and include:

- Across small organizations, three new industries unseated 2019 leaders (Construction, Retail/Wholesale & Insurance) to take the lead in highest percentage of "Phish-Prone" employees: **Healthcare & Pharmaceutical** organizations had the **highest percentage at 44.7%**, followed by **Education at 41.1%** and **Manufacturing at 40.9%**.
- As in 2019, within mid-size organizations, **Construction companies had the highest percentage** of "Phish-Prone" employees, ranking at **49.7%**.
- Within mid-sized organizations, two new industries joined the highest percentage of "Phish-Prone" employees: **Healthcare & Pharmaceuticals at 49.2%** and **Business Services at 43.5%**.
- For the large organizations of 1,000 or more employees, **Technology companies displaced Hospitality companies leading with an astounding 55.9%**. Hospitality organizations had favorable movement in 1,000 or more employees with their PPP lowering to 39.2%.
- The winner of the lowest Phish-Prone benchmark was large **Government organizations at 26%** unseating large **Transportation organizations at 27.2%**. Although the lowest in the findings, the PPP is still a strong indicator that users are not able to recognize a simulated phishing attack and how that can translate into real malicious attacks.

CALCULATING PHISH-PRONE PERCENTAGE BY INDUSTRY

Phase One: Baseline Phishing Security Test Results

The initial baseline phishing security test was administered within organizations that hadn't conducted any security awareness training. Users received no warning and the tests were administered on untrained, unaware people going about their regular job duties.

The results indicated a high-risk level. Across all industries and all sizes, the average Phish-Prone percentage was **37.9%**. That means **1 out of 3 employees** was likely to click on a suspicious link or email or obey a fraudulent request, about the same outcome as last year.

It's interesting (and maybe scary) to see that no organization performed well without training. Very few industries were under 30% in "Phish-Prone" employees: Banking - Small and Large at 29.8% and 27.4% respectively, Business Services - Large 27%, Government - Large at 26%, Legal - Medium at 26.8% and Transportation - Large at 27.2%.

The inescapable conclusion: Absent of training, every organization regardless of size and vertical is susceptible to phishing and social engineering. Workforces in every industry represent a possible doorway to attackers, no matter how steep the investment in world-class security technology.

Phase One

37.9% Initial Baseline Phishing Security Test Results

Organization Size	Initial PPP
1-249	36.8%
250-999	37.5%
1000+	39.2%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	29.8%	36.5%	27.4%
Business Services	35.8%	43.5%	27.0%
Construction	38.3%	49.7%	45.1%
Consulting	31.5%	37.6%	32.1%
Consumer Services	38.2%	30.6%	39.2%
Education	41.1%	34.4%	31.7%
Energy & Utilities	39.6%	41.2%	39.2%
Financial Services	32.1%	35.9%	43.9%
Government	33.8%	30.0%	26.0%
Healthcare & Pharmaceuticals	44.7%	49.2%	49.3%
Hospitality	32.1%	37.5%	39.2%
Insurance	39.2%	37.9%	39.2%
Legal	34.1%	26.8%	39.2%
Manufacturing	40.9%	37.7%	46.8%
Not-For-Profit	39.4%	38.1%	39.2%
Other	35.3%	41.0%	28.0%
Retail & Wholesale	40.4%	37.1%	36.5%
Technology	33.2%	30.5%	55.9%
Transportation	36.8%	43.2%	27.2%

Phase Two: Phishing Security Test Results Within 90 Days of Training

When organizations implemented a combination of training and simulated phishing security testing after their initial baseline testing, results changed dramatically. We find when users completed their first training event and look for all simulated phishing security events up to 90 days after that training is completed. In those 90 days after completed training events, the Phish-Prone percentage was **cut more than half to 14.1%**, consistent with both the 2018 and 2019 studies.

The dramatic drop in Phish-Prone percentages was not specific to a certain industry or organization size. But a few interesting data points:

- The most drastic reduction was seen in the 1,000+ organizations where **Technology** organizations experienced a **39% decrease** within 90 days of training after recording one of the highest initial baseline PPP's at 55.9%.
- Other significant reductions were seen in the 1,000+ organizations where **Manufacturing** organizations experienced a **33.3% decrease** and **Healthcare & Pharmaceuticals** organizations, who had the second highest PPP at 49.3%, experienced a **31.8% reduction** within 90 days after training.
- The **significant drop from 37.9% to 14.1%** for all industries proves that a security awareness training program can pay meaningful dividends in building a strong human firewall as part of your defense-in-depth IT security posture—even within the first three months.

Phase Two

14.1% **Phishing Security Test Results Within 90 Days of Training**

Organization Size	90-Day PPP
1-249	13.2%
250-999	14.3%
1000+	14.7%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	10.4%	10.9%	11.8%
Business Services	14.2%	13.8%	11.5%
Construction	14.2%	17.7%	16.1%
Consulting	11.1%	17.6%	11.0%
Consumer Services	15.1%	15.3%	13.2%
Education	13.6%	17.1%	18.5%
Energy & Utilities	12.5%	13.2%	14.7%
Financial Services	11.1%	12.2%	12.1%
Government	13.9%	15.1%	14.0%
Healthcare & Pharmaceuticals	15.9%	15.7%	17.5%
Hospitality	12.9%	17.4%	14.7%
Insurance	13.3%	16.0%	16.1%
Legal	13.3%	13.6%	14.7%
Manufacturing	14.3%	15.6%	13.5%
Not-For-Profit	14.9%	12.4%	15.0%
Other	13.2%	11.1%	13.6%
Retail & Wholesale	13.7%	13.2%	17.3%
Technology	12.2%	13.9%	16.8%
Transportation	10.9%	12.9%	14.7%

Phase Three: Phishing Security Test Results After One Year-Plus of Ongoing Training

At this stage, we measured security awareness skills after 12 months or more of ongoing training and simulated phishing security tests and look for users that completed training at least one year ago and take the performance results on their very last phishing test. The results were dramatic, showing that having a consistent, mature awareness training program took the average PPP from 37.9% all the way down to 4.7%—demonstrating dramatic effectiveness across all industry sizes and verticals.

Originally, we saw that large enterprise organizations scored better PPPs in their initial baseline test. In the final phase of the study, it became clear that these same organizations needed more time to turn the ship around and move in the right direction. This is likely due to the complexity of addressing different departmental and regional needs. There were two exceptions: Technology and Healthcare & Pharmaceuticals industries. These industries, representing the two highest overall baseline PPPs, experienced the most significant, favorable movement after 12 months from 55.9% to 5%, nearly a 51% reduction and 49.3% to 5.2%, a 44% reduction respectively.

A globally dispersed workforce can also introduce language differences and cultural nuances that lead to a longer roadmap for testing. Often enterprise security leaders will roll out a new security awareness training program to three or four departments first to monitor outcomes and adjust their strategies. This approach helps them incorporate lessons learned into their program, but also explains the slower response to reduction in Phish-Prone percentages.

Phase Three

4.7% **Phishing Security Test Results After One Year-Plus of Ongoing Training**

Organization Size	12-Month PPP
1-249	3.9%
250-999	4.8%
1000+	5.8%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	3.0%	4.3%	3.5%
Business Services	3.6%	5.0%	2.1%
Construction	3.9%	4.8%	3.8%
Consulting	3.4%	4.3%	5.8%
Consumer Services	5.1%	5.2%	6.9%
Education	4.0%	4.6%	4.8%
Energy & Utilities	5.4%	4.9%	5.2%
Financial Services	3.3%	4.6%	6.3%
Government	4.4%	4.2%	5.8%
Healthcare & Pharmaceuticals	4.3%	3.9%	5.2%
Hospitality	5.0%	4.1%	6.2%
Insurance	3.5%	4.0%	4.6%
Legal	4.8%	3.5%	5.4%
Manufacturing	4.2%	5.6%	5.7%
Not-For-Profit	4.8%	3.3%	6.0%
Other	4.3%	5.0%	5.8%
Retail & Wholesale	3.7%	6.5%	7.5%
Technology	3.5%	4.5%	5.0%
Transportation	3.9%	4.8%	5.4%

Average Improvement Rates Across All Industries and Organization Sizes

It's evident that after one year or more of security awareness training combined with frequent simulated phishing tests, **organizations across all sizes and industries drastically improved**. Organizations with 1-249 employees continued to achieve the **best overall improvement with eleven out of the nineteen industries coming in at 90% or more.**

Across mid-size organizations, improvement rates were good with **most industries coming in at 85% or better,** three industries fell slightly below 85%. For large organizations, we see a wider range of improvement rates with the **lowest improvement rate at 68% and the highest at 93%.**

When you look across all industries and sizes, the **87% average improvement rate** from baseline testing to One Year-Plus of ongoing training and testing is **outstanding proof for gaining buy-in to establish a fully mature security awareness training program**.

KnowBe4 finds that industry-wide 37.9% of untrained users will fail a phishing test.

Only 14.1% of those same users will fail within 90 days of completing their first KnowBe4 training. After at least a year on the KnowBe4 platform only 4.7% of those users will fail a phishing test.

87%

Average Improvement Rate Across All Industries and Sizes

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	90%	88%	87%
Business Services	90%	89%	92%
Construction	90%	85%	92%
Consulting	89%	89%	64%
Consumer Services	87%	83%	71%
Education	90%	87%	85%
Energy & Utilities	86%	88%	92%
Financial Services	90%	87%	86%
Government	87%	86%	78%
Healthcare & Pharmaceuticals	90%	92%	89%
Hospitality	85%	92%	71%
Insurance	91%	89%	93%
Legal	86%	87%	91%
Manufacturing	90%	85%	88%
Not-For-Profit	88%	91%	89%
Other	88%	88%	66%
Retail & Wholesale	91%	83%	79%
Technology	90%	85%	91%
Transportation	90%	84%	80%

2020 INTERNATIONAL PHISHING BENCHMARKS

At the international level, we used a slightly different data set which does not include separate industries to determine phishing benchmarks across small, medium, and large organizations. We included organizations where a definitive country was associated with the customer account so it could be included in the international benchmark analysis. The same benchmarking phases used to measure Phish-Prone percentages across industries were used for the international data set.

Phase One: Baseline Phishing Security Test Results

The initial baseline phishing security test was administered within organizations that hadn't conducted any security awareness training.

Phase Two: Phishing Security Test Results Within 90 Days of Training

Phase two evaluates organizations who have conducted baseline testing and then progressed to using a combination of training and simulated phishing exercises within a 90-day period. The data indicates that this combination cuts the Phish-Prone percentage **more than half for most regions**.

Phase Three: Phishing Security Test Results After One Year-Plus of Ongoing Training

For phase three, we measured after 12 months or more of ongoing training and simulated phishing security tests. The results are in line with the industry benchmarking results, showing that having a consistent, mature awareness training program took the average PPP down to single digits—**demonstrating effectiveness across all organizational sizes and regions**.

		BASELINE			90 DAYS			1 YEAR		
	Organization Size	**1-249**	**250-999**	**1000+**	**1-249**	**250-999**	**1000+**	**1-249**	**250-999**	**1000+**
REGION	**Africa**	31.7%	26.9%	29.6%	23.5%	16.3%	22.2%	4.3%	2.7%	5.8%
			TOTAL: **29.2%**			TOTAL: **21.8%**			TOTAL: **5.3%**	
	UK & Ireland	28.7%	27%	22.8%	13.8%	13.6%	14.1%	3.8%	6.1%	4.1%
			TOTAL: **26.7%**			TOTAL: **13.9%**			TOTAL: **4.7%**	
	Europe	30.5%	31.9%	27.1%	17.5%	16.9%	13.4%	5.8%	7.4%	***
			TOTAL: **29.5%**			TOTAL: **15.3%**			TOTAL: ***	
	APAC (Oceanic & Australia)	28.5%	34.9%	25.1%	17.6%	18%	14%	5.2%	6.7%	***
			TOTAL: **29.1%**			TOTAL: **17%**			TOTAL: **6.2%**	

***Insufficient data to calculate accurate PPP

AFRICA

Of all the international data, African citizens appear to be the most vulnerable. As outlined in KnowBe4's African Cybersecurity Research Whitepaper, "From ransomware to phishing, to malware and credential theft, users are not protecting themselves adequately because they mistakenly believe themselves to be informed, ready, and prepared. Of Africans surveyed, 53% think that trusting emails from people they know is good enough; 28% have fallen for a phishing email and 50% have had a malware infection; 52% don't know what multifactor authentication is; and 64% don't know what ransomware is and yet believe they can easily identify a security threat."

On a continent where half a billion citizens are connected to the Internet, and with this number increasing to an estimated 1 billion by 2022 (half a billion more untrained users), this emerging economy is very attractive to cybercriminals for a number of reasons:

1. High degree of digitization of economic activities
2. High unemployment rates drive youths to illegal activities
3. Mobile connectivity, such as the pervasiveness of WhatsApp and it's use for fake news dissemination
4. Immature understanding of the current cyber situation and need
5. Talent gap

AFRICA	BASELINE	90 DAYS	1 YEAR
1-249	31.7%	23.5%	4.3%
250-999	26.9%	16.3%	2.7%
1000+	29.6%	22.2%	5.8%
Average PPP Across All Organization Sizes	29.2%	21.8%	5.3%

The good news is that when organizations adopt an ongoing security awareness and simulated phishing program for a period of 12 months or more, we see the overall PPP drop from 29.2% to 5.3%. This shows that if organizations commit to raising the readiness levels of their employees, they will have a workforce that is more effective in preventing cyberattacks.

UNITED KINGDOM & IRELAND

The latest cyberattack trend data in the UK show that the majority of data breaches in 2019 began with a phishing attack. Security consulting firm CybSafe analyzed three years of the UK's Information Commissioner's Office (ICO) cyber breach data from 2017 – 2019. Out of nearly 2,400 reported data breaches, over 1,000 – 45.5% – of attacks were initiated by a phishing attack. According to the report, phishing dominated over unauthorized access, ransomware, malware, and misconfigurations. This preponderance of phishing being the initial attack vector is consistent with the ICO's 2018 data as well, indicating that cybercriminals continue to see phishing as a staple tactic because it just works.

In December 2018, a survey conducted by Censuswide found that 14% of Irish office workers – approximately 185,000 people – have fallen victim to a phishing scam. Additionally, "1) millennials (17%) were most often victims of a phishing scam compared to 6% of Gen X and 7% of Baby Boomers; 2) Almost half (48%) of generation X, those aged 42-54, have been targeted by a phishing scam – with spear phishing believed to be a major contributing factor; 3) 44% of Irish office workers aged 54 and over have clicked on links or attachments from an unrecognized email sender; 4) 20% of survey respondents have never received security awareness training or simulated phishing."

UK & IRELAND	BASELINE	90 DAYS	1 YEAR
1-249	28.7%	13.8%	3.8%
250-999	27%	13.6%	6.1%
1000+	22.8%	14.1%	4.1%
Average PPP Across All Organization Sizes	26.7%	13.9%	4.7%

KnowBe4 regional benchmark data shows that by implementing a new-school approach to security awareness training, organizations in the United Kingdom and Ireland region were able to reduce their PPP from 26.7% to 4.7% in 12 months.

EUROPE

According to Europol's European Cybercrime Centre (EC3), the European Police Office which is the official intelligence agency of the European Union, in 2018, "75% of EU Member States had active investigations into phishing, while Europol stakeholders consistently highlighting phishing or related attacks as the single most common attack vector with 65% of all reported cases". Additionally, the European Payments Council reported that "social engineering attacks and phishing attempts are still increasing and they remain instrumental often in combination with malware, with a shift from consumers, retailers, Subject Matter Experts to company executives, employees (through "CEO fraud"), financial institutions and payment infrastructures and more frequently leading to authorized push payments fraud."

EUROPE	BASELINE	90 DAYS	1 YEAR
1-249	30.5%	17.5%	5.8%
250-999	31.9%	16.9%	7.4%
1000+	27.1%	13.4%	***
Average PPP Across All Organization Sizes	29.5%	15.3%	***

***Insufficient data to calculate accurate PPP

Due to KnowBe4's recent expansion into the EU, there was not enough data gathered yet to perform a statistically sound analysis for a valid 12+ month period for the 1,000+ size organizations. This additional data should be available in the next report. That being said, with the European data so closely mirroring the North American data, we anticipate the EU Large Account 12+ month data to follow that trend. We look forward to continuing to add to the volume of phishing-related data that we are able to gather from this important region.

ASIA-PACIFIC

Cybercrime continues to be an increasing risk when doing business across APAC. According to Marsh & McLennan Companies Asia Pacific Risk Center's Cyber Risk in Asia Pacific Report, "rapidly growing connectivity and the accelerating pace of digital transformation expose the APAC region, and make it particularly vulnerable to cyber exploitation." In addition, experts note that there is a lack of transparency in APAC which "results in weak cyber regulations and enforcements by authorities, as well as low cyber awareness and security investments among corporations." As a result, the report shows that organizations and individuals in APAC are 80% more likely to be targeted by hackers than other parts of the world.

Whether it's Australia, New Zealand or any other country across APAC, criminals are increasingly using social engineering to access systems and steal data and currency. The Office of the Australian Information Center shared in its Notifiable Data Breaches Scheme 12-Month Insights Report that "phishing and spear phishing continue to be the most common and highly effective methods by which entities are being compromised—whether large or small—in Australia or internationally."

APAC	BASELINE	90 DAYS	1 YEAR
1-249	28.5%	17.6%	5.2%
250-999	34.9%	18%	6.7%
1000+	25.1%	14%	***
Average PPP Across All Organization Sizes	29.1%	17%	6.2%

***Insufficient data to calculate accurate PPP

With a baseline PPP beginning at 29.1% and decreasing to 6.2% after 12+ months of ongoing new-school security awareness training and simulated phishing, we see that – as with customers in other regions – KnowBe4 APAC customers are successfully helping their employees make smarter security decisions, every day.

KEY TAKEAWAYS: THE VALUE OF NEW-SCHOOL SECURITY AWARENESS TRAINING

The results from all three phases of the study reveal several conclusions:

Every organization is at serious risk without new-school security awareness training. With an average baseline PPP of 37.9%, companies could be exposed to social engineering and phishing scams by well over a third of their workforce.

Any organization can strengthen security through end-user training in as little as three months. The power of a good training program is to set up a consistent cadence of simulated phishing and social engineering education in a rapid timeframe.

An effective security awareness training strategy can help accelerate results for all organizations. The struggle of some enterprise leaders to successfully implement security training effectively across the organization is not surprising. But it does indicate that leaders can set themselves up for success by assessing their goals and plotting an organizational strategy before rolling out training.

Average Initial Baseline Phish-Prone Percentage by Industry

Organizations across these specific industries improved their failure rate by **88% after 12 months** or more of combined security awareness training and simulated phishing using KnowBe4. (Based on weighted averages across all organization sizes. Percentages rounded.)

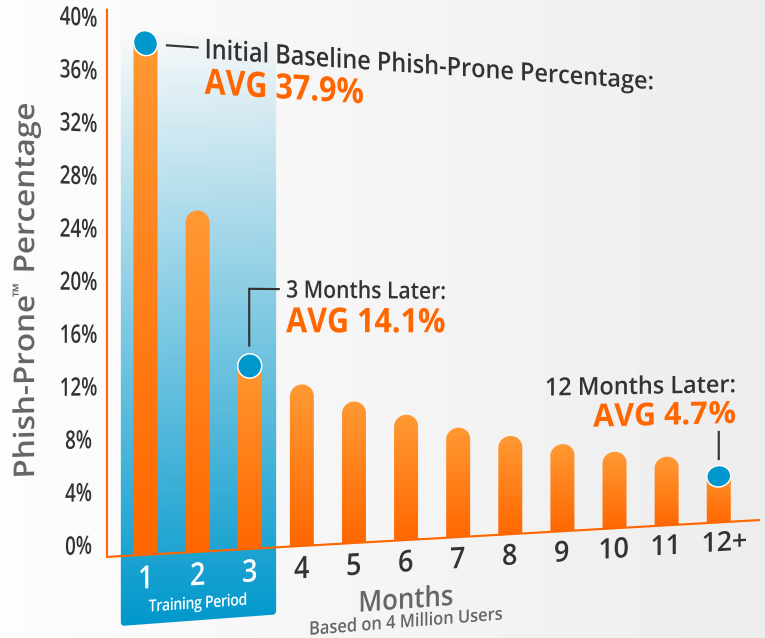
When you invest in Security Awareness Training and Phishing Security Testing you see value and ROI—fast.

When organizations understand how they stack up after doing an initial baseline phishing security test, proving value and ROI are at the top of the list to gain buy-in and budget. The results of the KnowBe4 Phishing By Industry Benchmarking Report clearly show where organizations' Phish-Prone percentages started and where they ended up after 12 months and beyond with regular testing and security awareness training.

At 37.9%, the overall industry initial Phish-Prone percentage benchmark is troubling. However, there is light at the end of the tunnel. The data showed that this 37.9% can be brought down by over half at 14.1% in only 90 days by deploying new-school security awareness training. The one year-plus results show that with continuous testing and training, the final Phish-Prone percentage can be minimized to 4.7% on average.

Another way to look at the results: Organizations improved their failure rate by an average of 87% in one year after using the KnowBe4 platform.

Visible Proof the KnowBe4 System Works



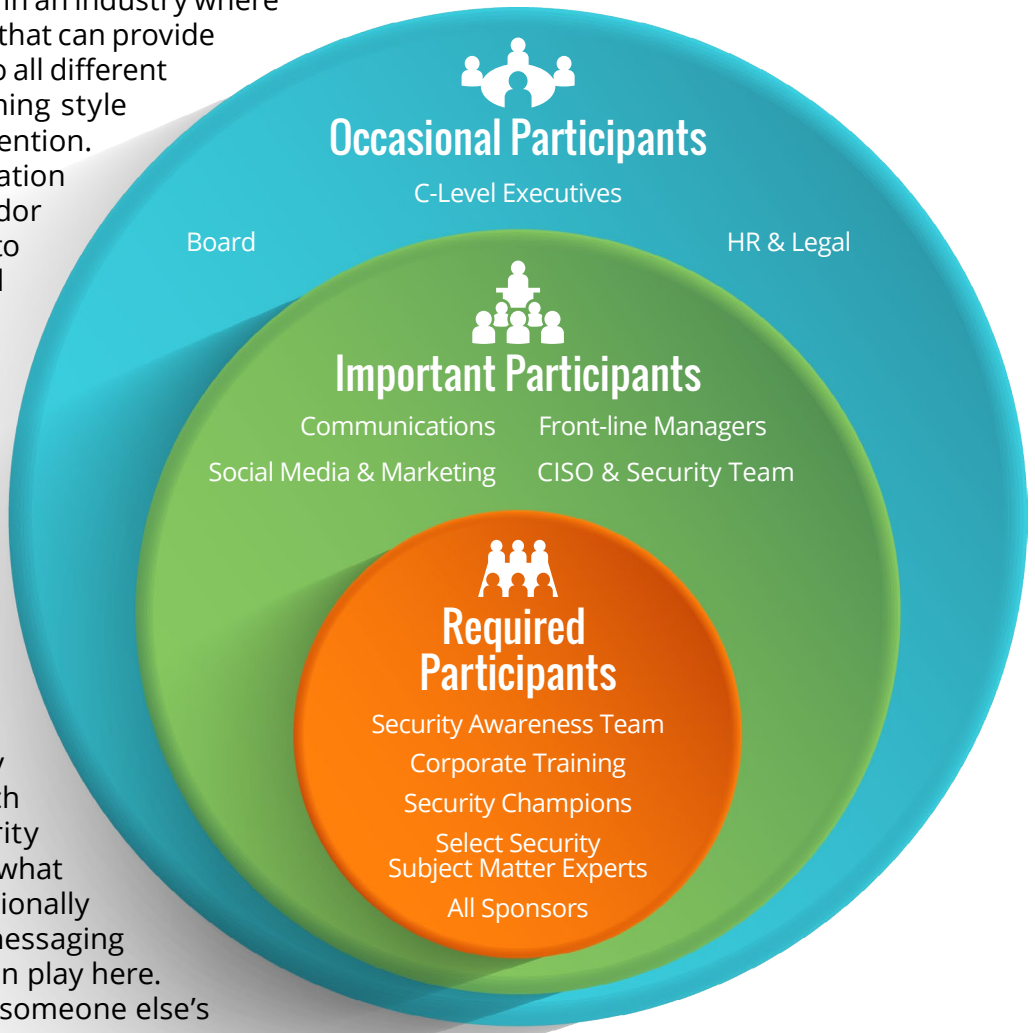
EXECUTIVE TAKEAWAYS

Security and Risk Management Leaders need to understand that in order to favorably change overall security behaviors within their organizations their programs must have a clearly defined and communicated mandate, a strong alignment with organizational security policies, be actively connected to overall security culture and have the full support of executives. Without consistent and enthusiastic executive support, raising security awareness within an organization is certain to fail.

Security and Risk Management Executives can ensure the success of their programs by:

- **Role Modeling:** If you expect your organization to do the right thing, you must lead them accordingly. Executives should be active participants in all aspects of driving security awareness throughout their organizations, which includes participating in the same security awareness training requirements that the rest of their employees are expected to complete.

- **Engaging a Pro:** Security Awareness content is unlike any other. Expertise goes into not only the design of the content, but also ensuring that the content leads to a positive learning experience and ultimately favorable secure behavior change. In an industry where content is king, the recommendation is to align with a vendor that can provide you with multiple flavors, versions and varieties that appeal to all different learning styles. Forcing your audience into a singular learning style limits the experience, material consumption and overall retention. It may be tempting to leverage your internal training organization to lead this program development, or to partner with a vendor that provides a one-size-fits-all approach, but that will lead to a long-term inability to shape your audience's security-related thoughts and actions.
- **Thinking Like a Marketer:** In parallel with content and simulated phishing campaigns, add frequent and relevant messaging in the form of ancillary supporting materials (posters, digital signage, newsletters, etc.) and find opportunities during cross-business meetings and presentations to reinforce the big take-aways. Holding 'lunch and learns' for employees and table-top exercises during leadership meetings provide an engaging way to disseminate information and engage directly with your audience.
- **Mobilizing a Security "Culture Carrier" Program:** Most security and risk programs lack the necessary resources in order to properly engage a global organization. Security "culture carrier" programs go by a lot of different names, such as "Security Champions," "Security Ambassadors," "Security Liaisons," "Security Influencers," and more; but regardless what you call it, a culture carrier program provides an organizationally dispersed team of advocates that can reinforce security messaging and learning at local levels. The responsibility factor is also in play here. Many employees believe that driving security awareness is someone else's responsibility. By enrolling local influencers either through manager nomination or volunteering, you essentially create a network of security go-to-people that can relate with local communities and start to help shape the overall security culture.



- **Adding Simulated Phishing Tests:** As we've shared through this research, by adding frequent simulated phishing campaigns to your overall security awareness program, you will increase your employee's resilience to being compromised, and also raise their ability to spot a mischievous email.
- **Increasing Frequency:** At all times, you are either building strength or allowing atrophy. The data indicates that most organizations not seeing favorable behavior change were limiting the frequency of their program (both content and simulated phishing) to annual, twice annual or quarterly. By testing so infrequently, you are essentially conducting moment in time baseline tests that you cannot meaningfully compare. The recommendation is to provide your audience monthly content and simulated phishing campaigns (twice monthly for high risk targets). There needs to be a regular cadence for the appropriate conditioning to take place and for behavior change to take hold. Security and Risk Management Executives may fear that this frequency is too much, but in actuality, it is helping build the right level of security muscle memory to combat the aggressive and ever-changing attack strategies of today and tomorrow.
- **Hiring the Right People:** Security awareness programs are often led by security practitioners that either drew the shortest straw or had extra time to deal with this "training" stuff. But, there is a certain level of experience and expertise necessary to manage a program like this. Target creative candidates that are aware and well versed in how to drive organizational development and behavior change through learning.
- **Defining Objectives:** Determine upfront what the success criteria of your program are and how you will measure against them, otherwise it is impossible to measure your program's effectiveness and determine inherent value.
- **Measuring Effectively:** The use of metrics that reinforce desired behaviors is important to protecting systems, employees and data. Don't try to boil the ocean by selecting too many measurement criteria; that only leads to measuring irrelevant areas and/or under delivering on promised organizational outcomes. It is paramount to utilize measurable data and training that can be frequently quantified and qualified. Also, ensure that program metrics are connected not only to overall organizational security objectives, but corporate objectives.
- **Motivating Employees:** Be intentional and consistent in how you use positive and negative reinforcement to encourage your audience to complete required training, adhere to security policies and demonstrate ongoing favorable secure behavior. Using motivators increases accountability and the employees overall role in driving a more secure culture.

GETTING STARTED

KnowBe4 is helping tens of thousands of IT pros like you to improve their network security in fields like finance, energy, healthcare, government, insurance and many more.

With KnowBe4, you have the best-in-class phishing simulation and training platform to improve your organization's last line of defense: **Your Human Firewall**.

We enable your employees to make smarter security decisions, every day. We help you deliver a data-driven IT security defense plan that starts with the most likely "successful" threats within your organization—your employees. The KnowBe4 methodology really works. Ready to get started?

4 Steps for Phishing Your Users

It's clear that organizations can radically reduce vulnerability and change end-user behavior through testing and training. Take these steps to get your organization on the right track to developing your human firewall.

1. **Conduct Baseline Testing:** Conducting a baseline test is the first step in demonstrating the need for security awareness training to your senior leadership. This baseline test will assess the Phish-Prone percentage of your users. It's also the necessary data to measure future success.

2. **Train Your Users:** Use on-demand, interactive, and engaging computer-based training instead of old-style PowerPoint slides. Awareness modules and videos should educate users on how a phishing or social engineering attempt could happen to them.

3. **Phish Your Users:** At least once a month, test your staff to reinforce the training and continue the learning process. You are trying to train a mindset and create new habits. It takes a while to set that in motion. Simulated social engineering tests at least once a month are effective at changing behavior.

4. **Measure Results:** Track how your workforce responds to both training and phishing. Your goal is to get as close to zero percent Phish-Prone as possible.

Plan Like a Marketer, Test Like an Attacker

While every leader can reduce risk by targeting employee PPP, there are several best practices that can bring about lasting change.

1

Use real-world attack methods

Your simulated phishing exercises must mimic real attacks and methodologies. Otherwise, your "training" will simply give your organization a false sense of security.

2

Don't do this alone

Involve other teams and executives, including Human Resources and IT and even Marketing. Create a positive, company-wide culture of security.

3

Don't try to train on everything

Decide what behaviors you want to shape and then prioritize the top two or three. Focus on modifying those behaviors for 12-18 months.

4

Make it relevant

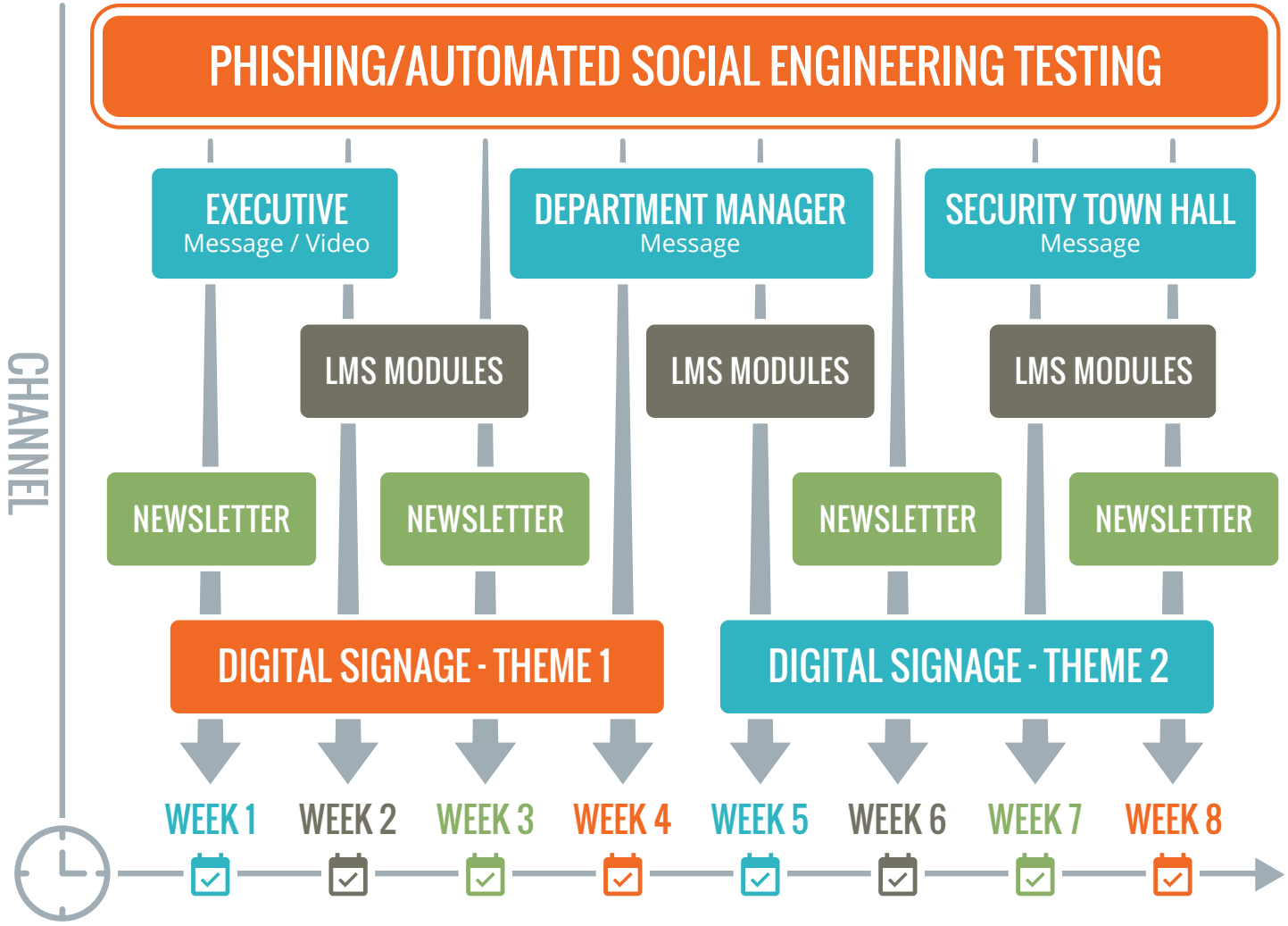
People care about things that are meaningful to them. Make sure your simulated attacks impact an employee's day-to-day activities.

5

Treat your program like a marketing campaign

To strengthen security, you must focus on changing behavior, rather than just telling staff what you'd like them to know. Give them the critical information they need, but stay focused on conditioning their secure reflexes so your workforce becomes an effective last line of defense.

To Move Employee Mindset, Lead with Clear Direction and Reinforcement



Run your security awareness program like a marketing campaign

Continuous testing while delivering targeted educational messages, training modules, and internal newsletters and digital signage will reinforce new behavior so your users become an effective last line of defense.

CREATE YOUR HUMAN FIREWALL

Free Phishing Security Test

Ready to start phishing your users? Find out what percentage of your employees are Phish-prone with your free phishing security test. Plus, see how you stack up against your peers with the phishing Industry Benchmarks! You can accomplish the same dramatic end results of the study with KnowBe4's Phishing Security Test.

ADDITIONAL RESOURCES

Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

ABOUT KNOWBE4

KnowBe4 is the world's largest integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make better security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: info@KnowBe4.com