KnowBe4

PHISHING BY INDUSTRY 2021

BENCHMARKING REPORT

VERIZON'S 2021 DATA BREACH INVESTIGATIONS REPORT SHOWS **THAT PHISHING CONTINUES TO BE THE TOP THREAT ACTION** USED IN SUCCESSFUL BREACHES. CYBERCRIMINALS STOLE LOGIN CREDENTIALS IN 85% OF BREACHES LINKED TO SOCIAL ENGINEERING.

INTRODUCTION

Cybercriminals never take a vacation. In fact, 2020 gave them reason and renewed motivation to ramp up their nefarious efforts. Phishing incidents nearly doubled in frequency from 2019 to 2020, from 114,702 incidents in 2019, to 241,324 incidents in 2020, according to the U.S. Federal Bureau of Investigation (FBI). Overall, phishing reigned as the most common type of cyber crime last year, according to the FBI.

The idea that technology can prevent all cyber-related incidents has never been further from the truth because cybercriminals know the easiest way in is through your humans. 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 forget that the power of human awareness and intervention is paramount in arriving at a highly secured state.

Every security leader faces the same conundrum: even as they increase their investment in sophisticated security orchestration, cyber crime continues to rise. Security is often presented as a race between effective technologies and clever attack methodologies.

Yet there's an overlooked best practice that can radically reduce an organization's vulnerability: **security awareness training and frequent simulated social engineering testing**.

As the COVID-19 pandemic continues to monopolize our lives, cybercriminals have not stopped their onslaught of manipulation campaigns. The COVID-19 pandemic proved lucrative for these criminals as the public remained continuously curious and distracted by changing news broadcasts, misinformation spread on social media, and fragmented "factual" debates in the political forum. KnowBe4 saw a 6,000% increase in COVID-19 related phishing attacks in March 2020 alone.

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 tricked into opening a file infected with malware or transferring company funds to a cybercriminal's 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 provider of 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 organizations 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 and organization size, the study reveals patterns that can light the way to a stronger and safer future.

2021 PHISHING BY INDUSTRY BENCHMARKING STUDY

Every organization struggles to answer an essential question—"How do I compare with other organizations that look like me?" To provide a nuanced and accurate answer, the 2021 Phishing By Industry Benchmarking Study analyzed a data set of over 6.6 million users across 23,400 organizations with over 15.5 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 who clicked a simulated phishing email link or opened an infected attachment during a testing campaign using the KnowBe4 platform.

Calculating Phish-Prone Percentages

To calculate each organization's Phish-Prone percentage, 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 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.

In our 2021 report, we will continue to look at these three benchmark phases. For simplification purposes, we will refer to the 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 looking for all simulated phishing security events up to 90 days after that training was 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, looked for users who completed training at least one year ago, and took the performance results on their very last phishing test.

METHODOLOGY AND DATA SET

15.5 million phishing security tests

6.6 million users

23.4 thousand organizations

ORGANIZATION SIZE RANGES

19 INDUSTRIES

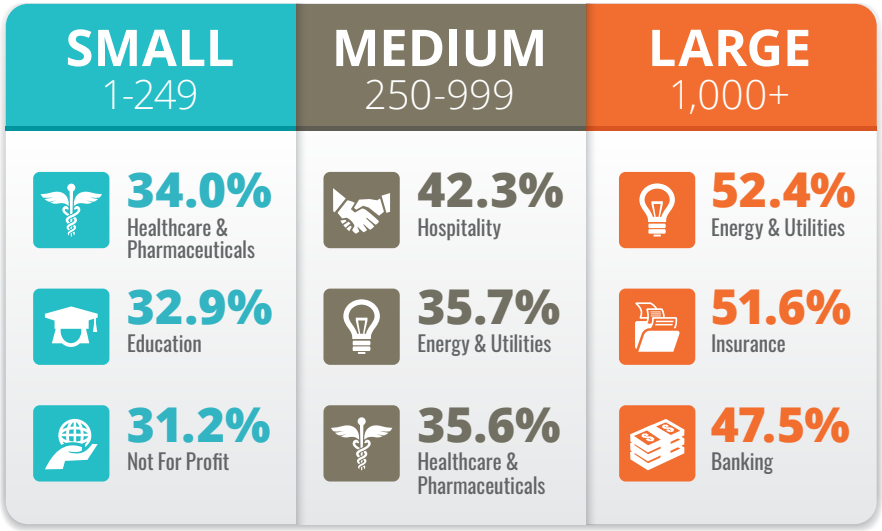
- Banking
- Business Services
- Construction
- Consulting
- Consumer Services
- Education
- Energy & Utilities
- Financial Services
- Government
- Healthcare & Pharmaceuticals
- Hospitality
- Insurance
- Legal
- Manufacturing
- Not For Profit
- Other
- Retail & Wholesale
- Technology
- Transportation

WHO'S AT RISK: RANKING INDUSTRY VULNERABILITY

The results across the 6.6 million users highlight an all too familiar truth for organizations: failure to effectively train your users leaves them, and your organization, woefully unprepared and vulnerable to social engineering attacks. The Phish-Prone percentage data, although slightly more favorable than 2020, continues to show 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 organizations at risk for potential compromise.

The overall PPP baseline average across all industries and size organizations was **31.4%**. 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.

- Across small organizations (1-249 employees), the **Healthcare & Pharmaceuticals** industry holds the top spot for the second year in a row with a PPP of **34.0%**; while the Education industry repeats at spot number two with a PPP of 32.9%. Rounding out the third spot in small business is newcomer Not For Profit with a PPP of 31.2%, unseating the Manufacturing industry from 2020.
- With mid-sized organizations (250-999 employees), we saw Construction and Business Services exit the top three highest risk, with **Hospitality** claiming the top spot due to a PPP of **42.3%**. Another rookie to the mid-sized ranking in 2021 was **Energy & Utilities** with a PPP of **35.7%**.
- **Healthcare & Pharmaceuticals** was back in 2021 holding onto the third spot in mid-sized organizations, with a PPP of **35.6%**. Although high, they are down from a staggering 2019 PPP of 49.7%.



- For the large organizations (1,000+ employees) we see all three of 2020's riskiest industries, Technology, Healthcare & Pharmaceuticals and Manufacturing, exit their unfavorable ranking. The **Energy & Utilities** industry claims the top spot for large companies with a PPP of **52.4%**. Coming in at a close second is the **Insurance** industry with a PPP of **51.6%**. Only to be followed by the **Banking** industry, claiming spot three with a PPP of **47.5%**.
- The winner of the lowest Phish-Prone benchmark was **large Legal organizations at 23.5%,** unseating large Government organizations at 26% from our 2020 report. 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.

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 from the KnowBe4 platform. Users received no warning, and the tests were administered on untrained people going about their regular job duties. The results continue to indicate high risk levels year-over-year:

- Across all industries and all sizes, the average Phish-Prone percentage was **31.4%**. Although an improvement over 2020's 37.9%, this year's average is still much too high. **That means one out of three employees was likely to click on a suspicious link or email or comply with a fraudulent request**, about the same outcome as last year.
- The 2020 data showed very few industries with PPPs under 30% that improved with the 2021 data, especially with small organizations. The most significant improvement was seen with small **Insurance companies,** which **decreased from 39.2% to 27.7%**.
- What's most concerning are the PPPs of the following industries, which had considerable unfavorable movement from 2020 to 2021: **Large Banking** companies increased from **27.4% to 47.5%; Large Energy & Utility** companies increased from **39.2% to 52.4%; Large Insurance companies from 39.2% to 51.6%**; and **Medium Hospitality** companies went from **37.5% to 42.3%**.

The inescapable conclusion: As cyber threats grow, the communication of these threats is filtering to the masses through social/news media. In some areas, people have more information thrust at them, so their awareness is growing more organically. The question remains if that ground-level awareness will transfer to the workplace and grow with training into something more developed and instinctive. Without training and frequent reinforcement, 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

31.4% Initial Baseline Phishing Security Test Results

Organization Size	Initial PPP
1-249	28.9%
250-999	30.1%
1000+	33.6%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	24.7%	23.9%	47.5%
Business Services	28.7%	31.6%	25.8%
Construction	28.7%	33.6%	42.7%
Consulting	27.2%	30.3%	28.4%
Consumer Services	30.3%	27.2%	28.7%
Education	32.9%	29.1%	27.9%
Energy & Utilities	29.0%	35.7%	52.4%
Financial Services	26.0%	28.3%	33.2%
Government	27.9%	25.0%	24.4%
Healthcare & Pharmaceuticals	34.0%	35.6%	44.1%
Hospitality	29.7%	42.3%	23.8%
Insurance	27.7%	31.2%	51.6%
Legal	27.8%	28.8%	23.5%
Manufacturing	29.9%	29.7%	32.7%
Not For Profit	31.2%	31.5%	40.8%
Other	27.5%	29.3%	24.5%
Retail & Wholesale	31.1%	31.1%	35.8%
Technology	27.0%	29.9%	34.6%
Transportation	26.6%	33.7%	23.7%

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 measurement, results changed dramatically. We find that after users complete their first training event, the simulated phishing security results up to 90 days after that training is completed are more favorable. In those 90 days after completed training events, the average Phish-Prone percentage was cut to almost half at 16.4%, consistent with both the 2019 and 2020 studies. The dramatic drop in Phish-Prone percentages was not specific to a certain industry or organization size, but here are a few interesting data points:

- The most significant reduction was seen in the large 1,000+ organizations, where **Insurance** experienced a **67.6% decrease** within 90 days of training after recording one of the highest initial baseline PPPs at 51.6%.
- Other significant reductions were seen in the large organizations, where **Banking** experienced a **68.8% decrease; Healthcare & Pharmaceuticals** organizations experienced a **60.3% reduction**; and within the medium organizations, **Hospitality** saw a **60.3% decrease**, 90 days after training.
- The significant drop from **31.4% to 16.4%** 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.

The inescapable conclusion: After applying only 90 days of new-school security awareness training, we saw a significant improvement in employees' abilities to detect malicious emails across every industry and size organization. Think about it in terms of a weight loss plan; it takes at least 90 days to start seeing results. In that same timeframe, your newly 90-day trained employees can cut the potential of your organization experiencing a brand/revenue damaging breach by nearly half. It takes a 90-day investment to raise readiness levels and lower risk.

Phase Two

16.4% Phishing Security Test Results Within 90 Days of Training

Organization Size	90-Day PPP
1-249	16.4%
250-999	16.9%
1000+	16.1%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	11.2%	12.5%	14.8%
Business Services	16.9%	17.9%	16.0%
Construction	19.3%	18.6%	17.7%
Consulting	16.4%	18.5%	13.7%
Consumer Services	17.4%	17.8%	14.7%
Education	17.3%	18.1%	17.6%
Energy & Utilities	15.5%	16.6%	15.4%
Financial Services	13.7%	15.3%	17.3%
Government	15.3%	15.5%	14.3%
Healthcare & Pharmaceuticals	17.9%	17.8%	17.5%
Hospitality	19.0%	16.8%	13.7%
Insurance	17.2%	16.5%	16.7%
Legal	15.0%	15.0%	12.2%
Manufacturing	17.0%	16.5%	15.6%
Not For Profit	19.1%	19.6%	18.0%
Other	18.6%	18.9%	13.0%
Retail & Wholesale	16.7%	17.0%	18.2%
Technology	17.7%	17.6%	16.8%
Transportation	18.5%	15.7%	12.6%

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. We looked for users who completed training at least one year ago and analyzed the performance results on their very last phishing test. The results were dramatic for the third year running, showing that having a consistent, mature awareness training program reduced the average PPP from 31.4% all the way down to **4.8%—demonstrating significant effectiveness across all industry sizes and verticals.**

We saw remarkably low PPP results in the small organizations, where two-thirds of the industry results were below 4%; the lowest PPP going to the small **Banking** industry at **2.6%**. The Banking industry also scored the lowest PPP in the medium organizations at 2.3%, while praise goes to the **Hospitality** industry in the large organizations with a **4.0%** PPP. With Banking being one of the most attacked and regulated industries, the results are no doubt based on the head start they had with cyber crime and the diligence they have applied to training.

When we compare the entire lifecycle, the organizations that showed the greatest holistic improvement were large companies in the **Energy & Utilities industry, which went from a benchmark PPP of 52.4% to 6.5% after at least 12 months of security awareness training, a 87.6% reduction.** Energy & Utility organizations have long been desirable targets for hackers because of the universal devastation a breach can cause. Additionally, these organizations have a long history of vulnerability due to rapid growth outpacing antiquated technology, complex supply chains and large employee networks with a high number of field or remote workers.

Think of it this way, if an energy plant is breached, that could potentially deprive its service population of water, transportation, data and communications systems for a prolonged period of time, causing immeasurable chaos and uncertainty.

Phase Three

4.8% **Phishing Security Test Results After One Year-Plus of Ongoing Training**

Organization Size	12-Month PPP
1-249	3.6%
250-999	4.7%
1000+	5.9%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	2.6%	2.3%	6.3%
Business Services	3.8%	4.6%	4.8%
Construction	4.0%	6.0%	7.5%
Consulting	3.8%	5.6%	5.0%
Consumer Services	4.0%	4.5%	5.2%
Education	4.8%	5.5%	4.3%
Energy & Utilities	3.2%	4.7%	6.5%
Financial Services	3.0%	4.6%	5.4%
Government	3.7%	4.4%	4.5%
Healthcare & Pharmaceuticals	3.6%	3.7%	5.0%
Hospitality	3.9%	9.4%	4.0%
Insurance	4.0%	4.6%	7.7%
Legal	3.8%	5.3%	8.6%
Manufacturing	3.3%	4.1%	7.8%
Not For Profit	4.3%	4.4%	5.1%
Other	3.3%	5.3%	5.7%
Retail & Wholesale	3.4%	5.3%	5.4%
Technology	3.3%	5.3%	7.6%
Transportation	4.5%	8.8%	4.8%

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 18 out of 19 industries coming in at 85% or above**.

Across mid-size organizations, improvement rates were good with **17 industries coming in at 80% or better**, two industries fell slightly below 80%. For large organizations, we saw **fifteen industries with improvement rates above 80%**, with the remaining four ranging from 63% to 78%.

When you look across all industries and sizes, the **84% 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 the industry-wide 31.4% of untrained users will fail a phishing test.

Once trained, only 16.4% of users failed within 90 days of completing their first KnowBe4 training. After at least a year on the KnowBe4 platform, only 4.8% of users failed a phishing test.

Average Improvement

84%

Average Improvement Rate Across All Industries and Sizes

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	89%	90%	87%
Business Services	87%	85%	81%
Construction	86%	82%	82%
Consulting	86%	81%	82%
Consumer Services	87%	84%	82%
Education	85%	81%	85%
Energy & Utilities	89%	87%	88%
Financial Services	89%	84%	84%
Government	87%	83%	82%
Healthcare & Pharmaceuticals	89%	90%	89%
Hospitality	87%	78%	83%
Insurance	86%	85%	85%
Legal	86%	82%	63%
Manufacturing	89%	86%	76%
Not For Profit	86%	86%	88%
Other	88%	82%	77%
Retail & Wholesale	89%	83%	85%
Technology	88%	82%	78%
Transportation	83%	74%	80%

2021 INTERNATIONAL PHISHING BENCHMARKS

At the international level, we used a slightly different data set that 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 that 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 significantly.

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**	26.0%	28.6%	32.1%	19.9%	23.5%	18.6%	9.9%	12.8%	5.5%
			TOTAL: 31.3%			**TOTAL: 19.3%**			**TOTAL: 6.5%**	
	APAC (Asia, Oceania & Australia)	30.8%	34.5%	42.8%	20.7%	18.8%	11.5%	4.9%	6.2%	5.2%
			TOTAL: 38.1%			**TOTAL: 15.3%**			**TOTAL: 5.5%**	
	Europe	28.4%	29.6%	29.2%	16.4%	16.6%	17.7%	4.0%	6.3%	9.6%
			TOTAL: 29.1%			**TOTAL: 17.0%**			**TOTAL: 6.9%**	
	South America	29.5%	32.6%	35.6%	19.5%	29.8%	16.3%	1.9%	9.9%	0.8%
			TOTAL: 33.7%			**TOTAL: 19.7%**			**TOTAL: 3.2%**	
	UK & Ireland	27.4%	28.4%	29.3%	15.5%	14.4%	15.2%	3.6%	4.3%	7.4%
			TOTAL: 28.4%			**TOTAL: 15.0%**			**TOTAL: 5.1%**	

AFRICA

Africa's future economic growth, productivity and prosperity all depend on its ability to adapt to an increasingly digital and technologically advanced world, a fact that has been further illuminated by the COVID-19 pandemic.

Our data shows that the Phish-Prone percentages of African organizations align with the rest of the international averages. However, organizations on the continent are faced with a couple of unique security challenges.

The major factors driving cyber crime activity in Africa are the steep increase in digitalization and growth in the user base of online consumers, vulnerabilities in digital communications networks and supply chain, a deficient cybersecurity infrastructure, lack of skilled human capital and general low level of security awareness across both private and public sectors.

Many African countries lack a cybersecurity strategy formulation, cybersecurity awareness, cyber crime legislation, cybersecurity programs and the general capability or capacity to implement all the above.

KnowBe4's 2020 African Cybersecurity Research Whitepaper shows that there have been some shifts in awareness from our 2019 report, presumably due to the changes in work and life behavior introduced by the global pandemic. Areas of weakness remained that should be addressed in order to ensure that people remain and become aware of the ongoing threats associated with cyber crime:

- 24% of the respondents indicated that they were affected by cyber crime while working from home.
- 52% of respondents don't know what ransomware is (64% in 2019).
- The number of people concerned about cyber crime has risen to 48% (from 38% in 2019).
- 67% percent of respondents use their mobile devices for financial transactions and mobile banking—therefore, educating consumers on how to spot social engineering attacks (often conducted via the phone, WhatsApp and SMS) and how to defend against mobile malware should be a priority of both industry and governments alike.

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 31.3% to 6.5%.

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 cyber attacks.

AFRICA	BASELINE	90 DAYS	1 YEAR
1-249	26.0%	19.9%	9.9%
250-999	28.6%	23.5%	12.8%
1000+	32.1%	18.6%	5.5%
Average PPP Across All Organization Sizes	31.3%	19.3%	6.5%

UNITED KINGDOM & IRELAND

Like most of the world, 2020 was the year where the pandemic hit the shores of the UK and Ireland. Small and medium organizations were perhaps in this instance uncharacteristically better prepared to deal with the threats that came along with the pandemic and little difference was seen in Phish-Prone percentages (PPP). In fact, in some cases, they improved.

Large organizations, hampered by inertia and the need to move large numbers of employees to remote working, saw a rise in PPP.

This rise is particularly troubling given the high volume of attacks that were seen throughout 2020. The National Cyber Security Centre (NCSC) and its partners alone took down over 15,000 COVID-19-related malicious campaigns, according to NCSC's 2020 Annual Review report. Additionally, According to a March 2021 report from the UK Department for Digital, Culture, Media and Sport (DCMS), 83% of businesses and 79% of charities reported phishing attacks over the last year, by far the most common type of cyber incident reported in the survey.

UK & IRELAND	BASELINE	90 DAYS	1 YEAR
1-249	27.4%	15.5%	3.6%
250-999	28.4%	14.4%	4.3%
1000+	29.3%	15.2%	7.4%
Average PPP Across All Organization Sizes	28.4%	15.0%	5.1%

2020 was the year that the NCSC and the City of London Police also launched the Suspicious Email Reporting Service, which received 2.3 million reports from the public in the first four months alone. Showcasing how many potentially malicious emails make their way to users' inboxes and why having an easy method to report such emails is vital.

Taking advantage of the pandemic, bad actors hijacked HM Revenue & Customs (HMRC) and the National Health Service (NHS) brands for many phishing scams. According to a Freedom of Information request, HMRC received and investigated over 10,000 scam emails, SMS messages, social media posts, and phone calls exploiting its name.

In July, the NCSC revealed Russian cyber actors, known as APT29, had been targeting organizations involved in coronavirus vaccine development. The NCSC assessed that APT29, also named "The Dukes" or "Cozy Bear", almost certainly operated as part of Russian intelligence services. An advisory published by the NCSC outlined a variety of tools and techniques, including spear phishing and custom malware known as "WellMess" and "WellMail" were being used to steal valuable intellectual property. This not only exposed the hostile action directly but also demonstrated to a wide range of pharmaceutical companies that they needed to understand more about protecting themselves.

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 28.4% to 5.1% in 12 months.

EUROPE

According to the 2020 Internet Organised Crime Threat Assessment (IOCTA) by Europol, the majority of social engineering and phishing attacks are successful due to inadequate security measures or insufficient awareness of users. Similarly, the report noted that business email compromise (BEC) continues to increase, as criminals are more carefully selecting their targets and understanding internal business processes.

Within Europe, we increased the dataset considerably compared to last year, which gave us measurable metrics for all sizes of organizations.

Much like the UK and Ireland, Europe as a whole saw small and medium-size organizations fare somewhat better than last year. Large enterprises did not see an improvement over last year. This could be attested to the larger burden they carry in adapting to remote working and serving a larger number of employees, partners, and customers. As a result, after a year, larger enterprises are almost a third more likely to fall victim to a phishing email compared to their smaller counterparts. This is concerning because according to the Europol IOCTA Report, social engineering remains an effective top threat to enable other types of cyber crime.

EUROPE	BASELINE	90 DAYS	1 YEAR
1-249	28.4%	16.4%	4.0%
250-999	29.6%	16.6%	6.3%
1000+	29.2%	17.7%	9.6%
Average PPP Across All Organization Sizes	29.1%	17.0%	6.9%

When looking at the Phishing Security Test results after one full year of ongoing training, it is clear that this type of investment in training does benefit organizations and the percentages of people falling victim to a phishing attack dropping quite impressively.

Therefore, it's important and beneficial for all organizations to invest in effective security awareness training to not just avoid broad phishing attacks, but also to be better able to withstand the onslaught of attacks from organized cybercriminal groups and state-sponsored actors.

ASIA-PACIFIC

According to the Trend Micro Cyber Risk Index (CRI) "One fifth (18%) of APAC organizations were hit by seven or more cyber attacks in the last year" and "Responding organizations in APAC claimed their top cyber-threat risks are: Ransomware, Man-in-the-middle attacks, Clickjacking, Phishing and social engineering and Botnets."

The Office of the Australian Information Center shared in its Notifiable Data Breaches Scheme July – December 2020 stating that the "Human factor dominates latest data breach statistics." Australian Information Commissioner and Privacy Commissioner Angelene Falk said 38% of all data breaches notified during the period were attributed to human error and added that "organizations need to reduce the risk of a data breach by addressing human error—for example, by prioritizing training staff on secure information handling practices."

APAC	BASELINE	90 DAYS	1 YEAR
1-249	30.8%	20.7%	4.9%
250-999	34.5%	18.8%	6.2%
1000+	42.8%	11.5%	5.2%
Average PPP Across All Organization Sizes	38.1%	15.3%	5.5%

On first look, the overall increase of the Phase One Phish-Prone percentage (PPP) of 9% to 38.1% PPP in 2021 is concerning until we realize that this increase is primarily driven by the 1000+ organizations with the other two small and medium organizations staying consistent year-over-year. Phase Three is the good news story with the overall PPP dropping from 6.2% in 2020 to 5.5%. KnowBe4 APAC customers are moving in a positive direction towards their employees making smarter security decisions every day.

SOUTH AMERICA

The diversity of South America is celebrated worldwide as a melting pot of cultures, languages, geographic landscapes and different economies. This region had an exponential growth of digitalization with more than 307 million users in 2020, followed by 141 million just in Brazil. The rapid, widespread adoption of digital technologies also increased the numbers of all kinds of cyber crime.

With the number of internet users growing every year, cybercriminals do not try to hide their true identities, showing that the legislation in relation to cyber crime does not keep up with this rapid evolution. Attacks like phishing, smishing, vishing and a large number of infections with ransomware are constantly detected in this region.

In Latin America, which includes the South American continent, two out of three phishing attacks are targeted against organizations. Only one in three attacks are aimed at people. Countries such as Argentina, Mexico, Colombia and Brazil lead the statistics of those who suffer most from this type of attack, mostly resulting in ransomware infections, according to the Overview of Threats in Latin America Report from Kaspersky. In 2020, due to the pandemic, attackers exploited the COVID-19 theme, promoting countless phishing campaigns focused on mobile devices, such as smishing and vishing.

S. AMERICA	BASELINE	90 DAYS	1 YEAR
1-249	29.5%	19.5%	1.9%
250-999	32.6%	29.8%	9.8%
1000+	35.6%	16.3%	0.8%
Average PPP Across All Organization Sizes	33.7%	19.7%	3.2%

The good news is that when organizations adopt an ongoing security awareness and phishing simulation program for a period of 12 months or more, we see the overall PPP drop from 33.7% to 3.2%. This shows that if organizations commit to increasing their employees' readiness levels, they will have a more effective workforce that is capable of preventing cyber attacks.

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

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

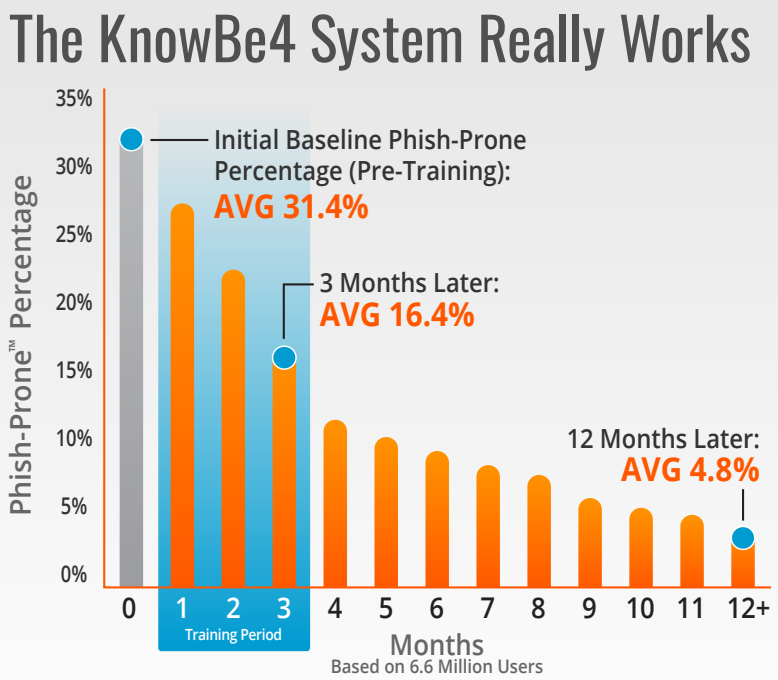
- **Every organization is at serious risk without new-school security awareness training.** With an average industry baseline PPP of 31.4%, organizations could be exposed to social engineering and phishing scams by a third of their workforce at any given time.
- **Any organization can strengthen security 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. Leaders can set themselves up for success by assessing their goals and plotting an organizational strategy before rolling out training.

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 comprehensive and continuous testing and security awareness training.

At 31.4%, 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 31.4% can be brought down by approximately half to 16.4% in only 90 days by deploying new-school security awareness training. The one year-plus results are dramatic and show that on average, with continuous testing and training, the final Phish-Prone percentage can be reduced to 4.8%.

Another way to look at the results: Organizations improved their susceptibility to phishing attacks by an average of 84% in one year after using the KnowBe4 platform.



Source: 2021 KnowBe4 Phishing by Industry Benchmarking Report

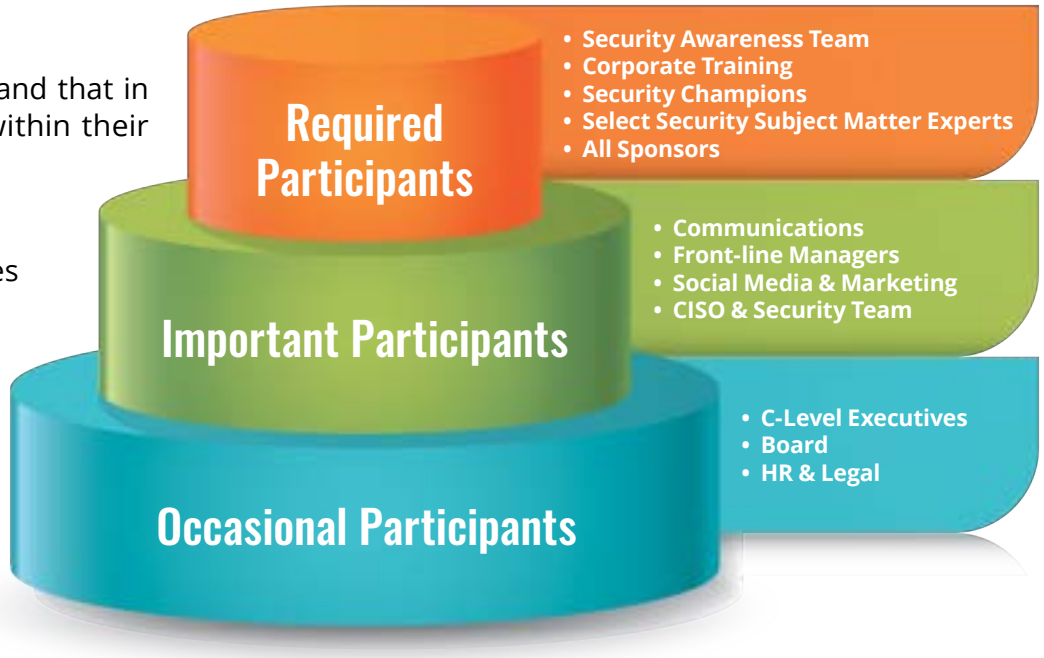
Note: The initial Phish-Prone percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-Prone percentages for the subset of users who received training with the KnowBe4 console.

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
- An active connection to overall security culture
- 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 takeaways. 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 to properly engage a global organization. Security "culture carrier" programs go by many different names, such as "Security Champions," "Security Ambassadors," "Security Liaisons," "Security Influencers," and more. Regardless of what you call it, a culture carrier program provides an organizationally dispersed team of advocates who 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 who 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 suspicious 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 who were either chosen to take on the task no one wanted 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 who 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 help protect systems, employees and data. Don't fall into the trap of selecting too many measurement criteria; that only leads to measuring irrelevant areas and/or underdelivering 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.

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.

Don't do this alone

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

Don't try to train on everything

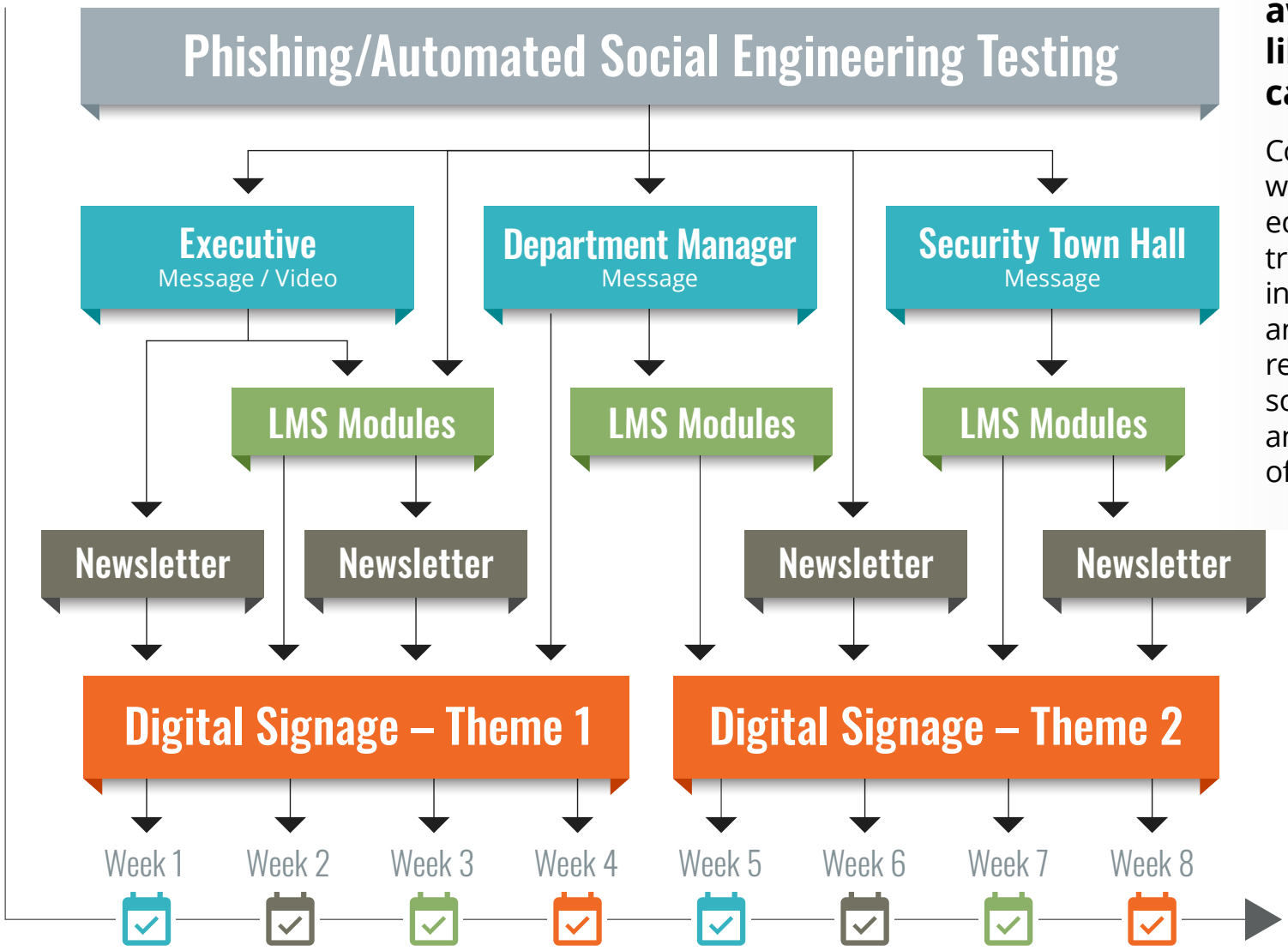
Decide what behaviors you want to shape and then prioritize the top two or three. Focus on modifying those behaviors for 12-18 months.

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.

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.



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 security 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 smarter 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

01RPRB25R01