Whittlesey
Forward Advising™

PHISHING BY INDUSTRY

BENCHMARKING REPORT | 2022 EDITION

Verizon's 2022 Data Breach Investigations Report states that "the human element continues to drive breaches. This year, 82% of breaches involved the human element. Whether it is the use of stolen credentials, phishing, misuse or simply error, people continue to play a very large role in incidents and breaches alike."

INTRODUCTION

The human layer continues to be the most enticing attack vector for cybercriminals. Sadly, most organizations continue to neglect this easily penetrable entry point. Throughout 2021, the world continued to see significant year-over-year increases in phishing attacks. No industry vertical, size of business or geography was immune. The human layer was under attack in both professional settings and personal settings. Cybercriminals do not discriminate when they consider victims, as carefully constructed attacks target humans both at work and play, day or night through various types of social engineering.

The FBI's Internet Crime Complaint Center (IC3), *continued to receive a record number of complaints from the American public: 847,376 reported complaints, which was a 7% increase from 2020, with potential losses exceeding $6.9 billion.* Additionally, business email compromise incidents accounted for *19,954 complaints with an adjusted loss of nearly $2.4 billion.* And these are just the reported incidents.

Industries are grappling with how they can better develop their human defense layer to detect, protect and report suspicious actions before it's too late and their systems are compromised.

Most organizations turn first to technology as the means to combat cybercriminals, not taking into account that investing in human awareness and intervention is equally, if not more, critical. According to the Verizon 2022 Data Breach Investigations Report, *82% of all security incidents involve a human element,* proving how susceptible humans can be.

Security leaders who continue to invest solely in sophisticated technology and security orchestration 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 not only helps raise the readiness level of humans to combat cyber crime, it lays the critical foundation necessary to drive a strong security culture throughout an organization.

As the world finally begins to emerge from the grip of the COVID-19 pandemic, social engineering attacks continue to rise. The use of email, phone calls, texts, social media and other outreach methods all work together to evade an organization's secure infrastructure as workforces and individuals remain more distracted and exposed than ever.

Distraction can easily lead to disaster. With phishing on the rise, an employee's mindset and actions are critical to the security posture of every organization. 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 warning their employer? 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.

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 clicking on a link, 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 PPP 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 and better equip our human layer?"

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, safer and more secure future.

2022 GLOBAL 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 2022 Phishing By Industry Benchmarking Study analyzed a data set of over 9.5 million users, across 30,173 organizations, with over 23.4 million simulated phishing security tests, across 19 different industries.

Methodology For This Year's Study

All organizations were categorized by industry type and size. 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 2022 report, we continue to look at the following three benchmark phases:

- **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:

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.

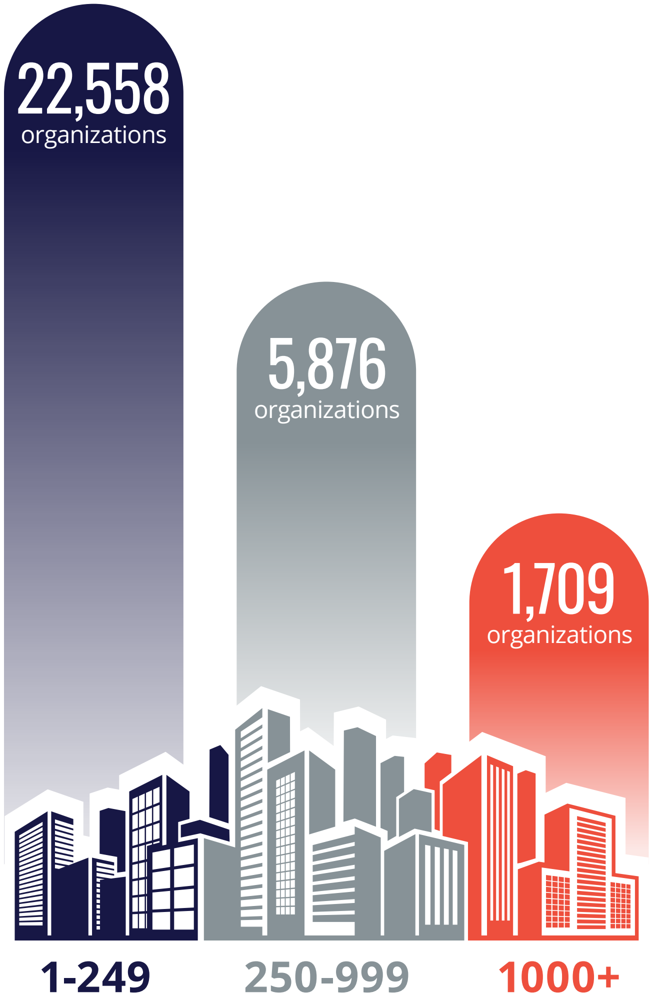
METHODOLOGY AND DATA SET

23.4 million phishing security tests

9.5 million users

30.1 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 9.5 million users highlight an all too familiar truth for organizations: failure to effectively train your users leaves them, and your organization, unprepared and vulnerable to social engineering attacks. The Phish-prone Percentage data, although slightly more favorable than 2021, 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 2022 PPP baseline average across all industries and size organizations was **32.4%**, up one point from 2021. 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 **Education Industry**, although slightly better than 2021, enters 2022 with a **PPP of 32.7%**. **Healthcare & Pharmaceuticals** is next with a **PPP of 32.5%**. Unseating Not-for-Profit for the last spot is **Retail & Wholesale** with a **PPP of 31.5%**.
- With mid-sized organizations (250-999 employees), the top three industries from 2021 remained. The **Hospitality industry** was unchanged in 2021 with a PPP of **39.4%**. **Energy & Utilities** and **Healthcare & Pharmaceuticals** swapped positions, with Healthcare & Pharmaceuticals next with a **PPP of 36.6%** and **Energy & Utilities** following with a **PPP of 34%**. It is worth noting that all three industries had stronger PPPs vs. 2021 ratings, although they remained the industries most at risk.

Who's at Risk?

The top three industries by organization size

SMALL 1-249	MEDIUM 250-999	LARGE 1,000+
32.7% Education	39.4% Hospitality	52.3% Insurance
32.5% Healthcare & Pharmaceuticals	36.6% Healthcare & Pharmaceuticals	52.2% Consulting
31.5% Retail & Wholesale	34% Energy & Utilities	50.9% Energy & Utilities

- For large organizations (1,000+ employees), we saw Energy & Utilities fall out of the top spot and be replaced by **Insurance** (second in 2021) with a **PPP of 52.3%**. The **Consulting industry**, new to the ranking, was next with a **PPP of 52.2%**, while **Energy & Utilities** rounded out the group with a **PPP of 50.9%**. Banking fell out of the top three in 2022.
- The winner of the lowest Phish-prone benchmark across small organizations (1-249 employees) was **Banking** with a **PPP of 25.4%**; across mid-sized organizations was **Government** with a **PPP of 26.4%**; and across large organizations was **Hospitality** with a **PPP of 20.4%**. Although the lowest in the findings, these PPP results strongly indicate that an untrained user base is still vulnerable to falling for phishing attacks.

PHASE ONE: BASELINE PHISHING SECURITY TEST RESULTS

The initial baseline phishing security test was administered within organizations that had not 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 **32.4%**, up 1 point from 2021. **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 2022 data showed the most significant improvement was seen with **Large Construction** companies, which positively moved from a PPP of **42.7% to 37%**. Adversely, the most significant decline was visible in **Large Consulting** companies, moving negatively from **28.4% in 2021 to 52.2% in 2022**.
- What is most concerning are the PPPs of the following industries in the Large category, which all have PPPs north of 40%: **Banking 43.5%, Healthcare & Pharmaceuticals 45%, Energy & Utilities 50.9%**, **Consulting 52.2% and Insurance 52.3%**. This means that employees in these categories are at a high risk of falling for social engineering attacks, some a staggering 50+%.

Thoughts: 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

32.4% Initial Baseline Phishing Security Test Results

Organization Size	Initial PPP
1-249	28.8%
250-999	30.2%
1000+	35.2%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	25.4%	27.3%	43.5%
Business Services	27.4%	30%	29.2%
Construction	29.6%	32.9%	37%
Consulting	27.5%	30.6%	52.2%
Consumer Services	30.4%	29.1%	24.3%
Education	32.7%	29.3%	28.4%
Energy & Utilities	29.4%	34%	50.9%
Financial Services	26.4%	28.7%	35.9%
Government	28%	26.4%	24.8%
Healthcare & Pharmaceuticals	32.5%	36.6%	45%
Hospitality	28.5%	39.4%	20.4%
Insurance	26.2%	30.3%	52.3%
Legal	27.3%	27.6%	29.2%
Manufacturing	29.5%	29.5%	33.1%
Not-For-Profit	29.6%	30.8%	36.5%
Other	30.5%	31.9%	26.8%
Retail & Wholesale	31.5%	30.6%	38.6%
Technology	26.7%	28.2%	33.2%
Transportation	27%	32%	24.8%

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 found that after users complete their first training event, the simulated phishing security test 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 17.6%, consistent with the studies from the past three years. 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 following organizations: small (1-249 employees) **Education** experienced a **46% decrease** from 32.7% at baseline to 17.9% within 90 days of training; mid-size (250-999 employees) **Hospitality** experienced a **51% decrease** from 39.4% at baseline to 19.4% within 90 days of training; and large (1000+ employees) **Insurance** experienced a **67% decrease** from 52.3% at baseline to 17.3% within 90 days of training after recording one of the highest initial baseline PPPs.
- The significant drop from **32.4% to 17.6%** for all industries proves that a security awareness training program can pay meaningful dividends in building a strong human defense layer as part of your defense-in-depth IT security posture—even within the first three months.

Thoughts: 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 of 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. As with any significant change, it takes time to break old habits and create new ones. Once these new habits are formed however, they become the new normal, part of the organizational culture, and influence how others behave, especially new hires who look to others to see what is socially and culturally acceptable in the organization.

Phase Two

17.6% Phishing Security Test Results Within 90 Days of Training

Organization Size	90-Day PPP
1-249	17.5%
250-999	17.9%
1000+	17.4%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	12.3%	13.6%	15.6%
Business Services	18.3%	18.6%	17.7%
Construction	19.5%	20%	15.8%
Consulting	17.5%	20.1%	21.3%
Consumer Services	18.8%	21%	16.1%
Education	17.9%	18.5%	18.8%
Energy & Utilities	16.8%	17.2%	16.4%
Financial Services	15.1%	16%	19.1%
Government	16%	15.5%	15.2%
Healthcare & Pharmaceuticals	19.7%	19.1%	17.2%
Hospitality	19.7%	19.4%	12.2%
Insurance	17.7%	17.5%	17.3%
Legal	16.5%	15.9%	13%
Manufacturing	17.7%	17%	16.5%
Not-For-Profit	20.3%	20.8%	18.2%
Other	19%	21.4%	20.1%
Retail & Wholesale	18.3%	18.1%	18.1%
Technology	18.9%	18.8%	19.2%
Transportation	18.5%	18.7%	16.5%

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 continue to be dramatic year-over-year, showing that having a consistent, mature awareness training program reduced the average PPP from 32.4% all the way down to **5%. These results were demonstrated significantly across all industry sizes and verticals.**

For a second year, the lowest PPP in small organizations (1-249 employees) was **Banking** at **2.6%**. Also, for a second year, the **Banking** industry scored the lowest PPP in the mid-size organizations category (250-999 employees) at **3.3%**. In the category of large organizations (1000+ employees) and also for a second year, the **Hospitality** industry scored **1.3%**, a favorable decrease from their 2021 score of 4%. 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.

After comparing the data, the industries that showed the greatest holistic improvement were both in the large category (1000+ employees): **Energy & Utilities industry, which went from a benchmark PPP of 50.9% to 3.6% after at least 12 months of security awareness training, a 93% reduction and the Consulting industry which went from a benchmark PPP of 52.2% to 4.9%, a 91% reduction.** The Energy & Utilities industry, which experienced one of the largest cyber attacks on an oil infrastructure target in the history of the United States (Colonial Pipeline), continues to be a high profile and high destruction target for cybercriminals. Also highly targeted is the Consulting industry where in August 2021, one of the largest global consulting groups was hit with a massive $50 million ransomware attack by the group LockBit with help from an internal source (insider threat).

Phase Three

5% **Phishing Security Test Results After One Year-Plus of Ongoing Training**

Organization Size	12-Month PPP
1-249	3.8%
250-999	5%
1000+	5.8%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	2.6%	3.3%	3.4%
Business Services	3.8%	5%	6%
Construction	4.1%	4.8%	4.6%
Consulting	3.8%	4.8%	4.9%
Consumer Services	4.7%	4.7%	3.3%
Education	4.1%	5.4%	6.5%
Energy & Utilities	3.4%	5%	3.6%
Financial Services	3.7%	4.9%	5.5%
Government	3.9%	3.9%	7.1%
Healthcare & Pharmaceuticals	4.1%	5.1%	5.9%
Hospitality	4.4%	5.6%	1.3%
Insurance	3.3%	4%	5.3%
Legal	4.1%	5.2%	5.6%
Manufacturing	3.3%	5.3%	6.2%
Not-For-Profit	4.1%	4.9%	4.5%
Other	3.2%	4%	6.2%
Retail & Wholesale	3.6%	5.3%	4.7%
Technology	4.7%	5.9%	7.2%
Transportation	4.1%	9.6%	4.5%

AVERAGE IMPROVEMENT RATES ACROSS ALL INDUSTRIES AND ORGANIZATION SIZES

It is clear 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 17 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 **14 industries with improvement rates above 80%**, with the remaining five ranging from 71% to 79%.

When you look across all industries and sizes, the **85% 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 32.4% of untrained users will fail a phishing test.

Once trained, only 17.6% of users failed within 90 days of completing their first KnowBe4 training. After at least a year on the KnowBe4 platform, only 5% of users failed a phishing test.

Average Improvement

85%

Average Improvement Rate Across All Industries and Sizes

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	90%	88%	92%
Business Services	86%	83%	79%
Construction	86%	85%	88%
Consulting	86%	84%	91%
Consumer Services	85%	84%	86%
Education	87%	82%	77%
Energy & Utilities	88%	85%	93%
Financial Services	86%	83%	85%
Government	86%	85%	71%
Healthcare & Pharmaceuticals	87%	86%	87%
Hospitality	84%	86%	93%
Insurance	87%	87%	90%
Legal	85%	81%	81%
Manufacturing	89%	82%	81%
Not-For-Profit	86%	84%	88%
Other	90%	87%	77%
Retail & Wholesale	89%	83%	88%
Technology	83%	79%	78%
Transportation	85%	70%	82%

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 32.4%, 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.

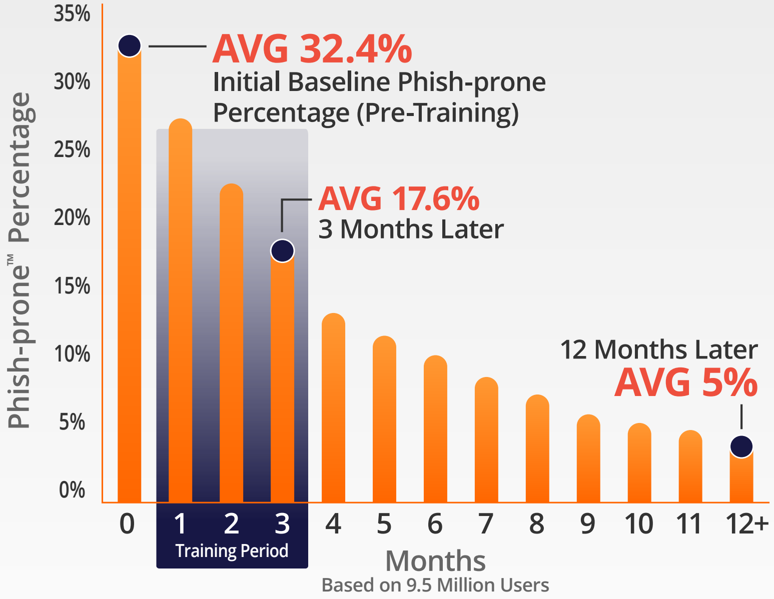
EXECUTIVE TAKEAWAYS

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 and human layer of security
- The full support of executives

Without consistent and enthusiastic executive support, raising security awareness within an organization is certain to fail.

The KnowBe4 System Really Works



Source: 2022 KnowBe4 Phishing by Industry Benchmarking Report

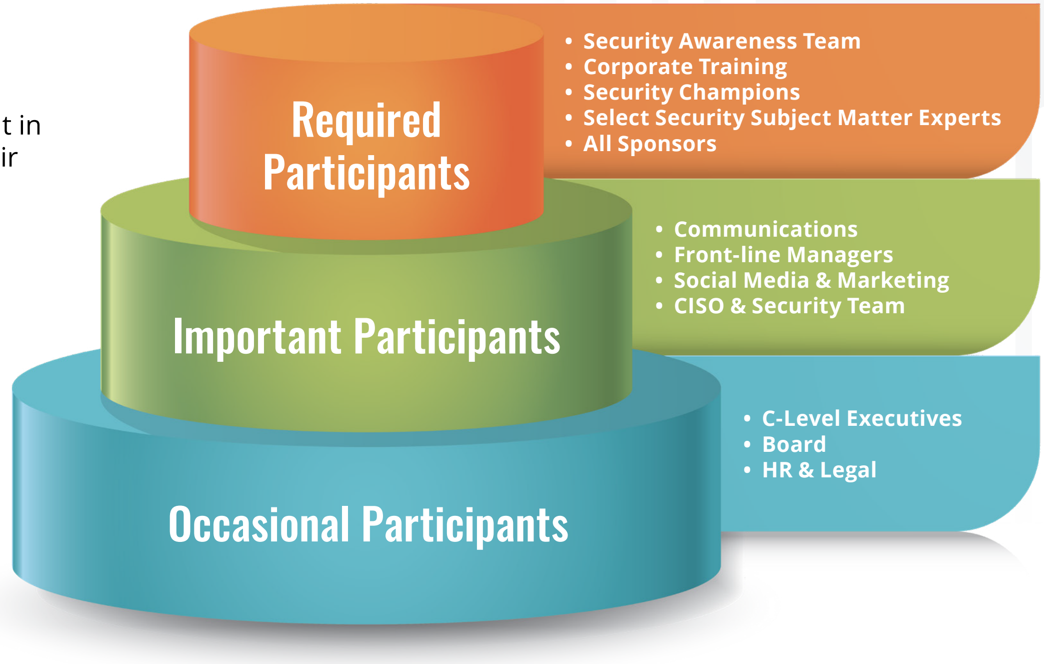
Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4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

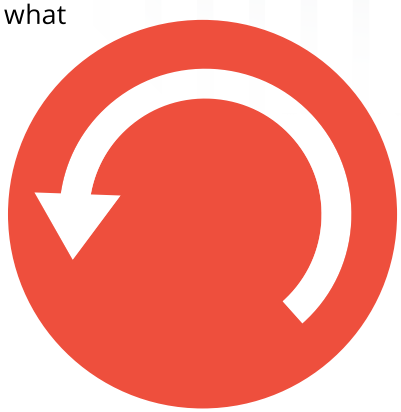
Without consistent and enthusiastic executive support, raising security awareness within an organization is certain to fail.



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

- **Fostering a Security Culture:** The human element is the most critical part of an organization's security infrastructure. All employees should understand what their role and responsibility is to protect the organization and themselves from a cyber attack. Security culture, as defined by KnowBe4, is the ideas, customs and social behaviors of an organization that influence their security. Executives need to ensure they are fostering an environment that is security ready by investing in both the focus of their security awareness and training program and the readiness level of their humans.
- **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. Both options 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 provides 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 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. Our research shows 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. However, managing a program like this requires a certain level of experience and expertise. 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. Employing measurable data and training that can be frequently quantified and qualified is paramount. 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 cybersecurity 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.

01 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.

02 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.

03 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.

04 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.

05 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 security reflexes so your workforce becomes an effective last line of defense.

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!

Mark R. Torello, CPA, CFE, CISA, CRISC, CITP
Partner-in-Charge, Technology

860.524.4433
mtorello@WAdvising.com

Whittlesey
Technology

Headquarters
280 Trumbull Street, 24th Floor
Hartford, CT 06103
860.522.3111

One Hamden Center
2319 Whitney Avenue, Suite 2A
Hamden, CT 06518
203.397.2525

14 Bobala Road, 3rd floor
Holyoke, MA 01040
413.536.3970

WAdvising.com