KnowBe4
Human error. Conquered.

REPORT

2018 Phishing By Industry Benchmarking Report

Table of Contents

> According to Verizon's 2018 Data Breach Investigation Report, 93% of data breaches are linked to phishing and other social engineering incidents.

Introduction

Every security leader faces the same conundrum: even as they increase their investment in sophisticated security orchestration, cybercrime continues to rise. Often security seems to be a race between effective technology 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**.

According to Verizon's 2018 Data Breach Investigation Report, 93% of data breaches are linked to phishing and other social engineering incidents. 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 their 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 a social engineering or phishing scam. 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 staff 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.

The overall Phish-prone percentage offers even more value when placed in context. After seeing their number, 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 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 conducted a 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.

2018 Phishing By Industry Benchmarking Study

Every company wants an answer to the essential question: "How do I compare with others who look like me?" To provide a nuanced and accurate answer, the **2018 Phishing By Industry Benchmarking Study** analyzed a data set that included over six million users across 11,000 organizations and a few hundred thousand simulated phishing security tests.

All 11,000 customers were using the KnowBe4 platform according to the recommended best practices for a new-school security awareness approach:

- Running an initial baseline test
- Training their users through realistic on-demand, interactive training
- Frequent simulated testing at least once a month to reinforce the training

These organizations were broken down 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 and Data Set

6mil
Drawn from a data set over 6 million users

11k
Across nearly 11,000 organizations

241k
Over 241,000 Phishing Security Tests Segmented by industry type and organization size

INDUSTRIES	SIZE RANGES
Energy & Utilities	**1 - 249**
Financial Services	**250 - 999**
Technology	**1000+**
Manufacturing	For the study, the approxamate number of organizations in each size range were as follows:
Government	
Healthcare	
Insurance	
Not For Profit	**1 - 249 Employees 8k Organizations**
Education	**250 - 999 Employees 2k Organizations**
Retail & Wholesale	**1000+ Employees 1K Organizations**
Other	

Allowing for a 'follow-the-user result' from initial Phishing Security Test baseline, to results after 90 days of combined Computer-based Training and phishing training, to the result after one year of combined phishing and Computer-based Training.

Analyzing Training Impact

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

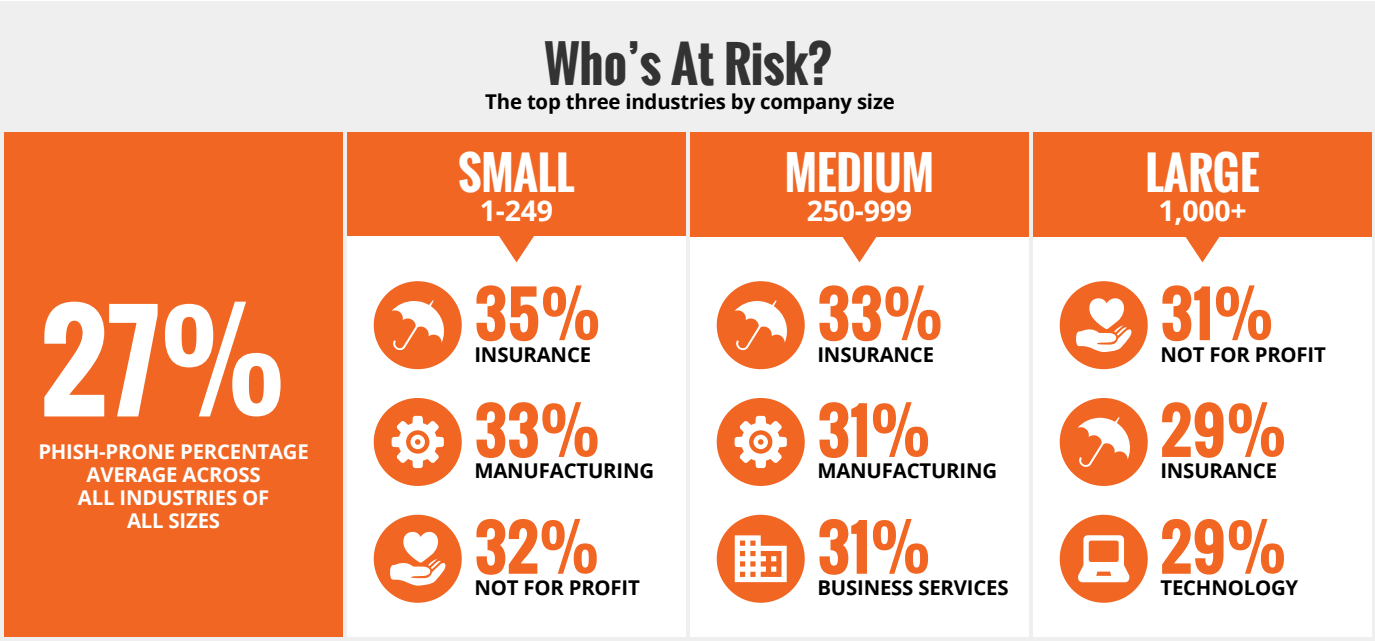
Phase One: If you haven't trained your users and you send a phishing attack, what is the resulting PPP? To do this, we monitored employee susceptibility to an initial baseline simulated phishing security test.

Phase Two: What is the initial resulting PPP across industries and sizes after training and monthly simulated phishing tests? We answered this question by measuring phish-prone behavior after 90 days of training and phishing security tests.

Phase Three: What is the final resulting PPP across industries and sizes after continued training and monthly simulated phishing tests? To answer this, we measured security awareness skills after 12 months of training and phishing tsecurity ests.

Who's at Risk: Ranking Industry Vulnerability

The results across the six million users highlights a drastic predicament for organizations that don't feel the need or choose not to invest in new-school 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 **27 percent**. 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 above 30 percent at initial baseline testing include:

- In both the small and mid–size organization categories, small insurance companies had the highest percentage of "Phish-prone" employees, ranking at **35 percent** and **33 percent** respectively.
- For the large organizations of 1,000 or more employees, not-for-profit companies took the lead with **31 percent**.

The winner of the lowest Phish-prone benchmark was large business services organizations at **19 percen**t which is still a significant number when considering how many users in a larger organization could put your organization in jeopardy if they click on a phishing link.

Calculating Phish-Prone Percentage by Industry

Phase One: Initial Baseline Simulated Phishing Security Test
The initial baseline phishing test was administered to organizations that hadn't conducted any security awareness training. Users weren't warned by IT staff and the tests were administered out of the gate 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 27 percent. That means more than 1 out of 4 employees was likely to click on a suspicious link or email or obey a fraudulent request. Chart A below ranks the percentages for different industries.

It's interesting (and maybe scary) to see that no organization does well without training. Industries such as energy and utilities were over 30 percent and so were technology vendors and other technology-based companies. Not-for-profit organizations also ranked over 30 percent and insurance organizations exceeded 35 percent. Even smaller organizations in industries that typically require more regulatory oversight and requirements fared badly.

The inescapable conclusion: Every organization regardless of size and vertical is susceptible to phishing and social engineering without Computer-based training (CBT)*. Workforces in every industry represent a possible doorway to attackers, no matter how steep the investment in world-class security technology.

Benchmark Phish-prone Percentage by Industry

Baseline Phish-prone Percentage (B-PPP)			
Industry	**1 – 249 employees**	**250 – 999 employees**	**1000+ employees**
Energy & Utilities	31.56	29.34	22.77
Financial Services	27.41	28.47	23.00
Business Services	29.80	31.01	19.40
Technology	30.68	30.67	28.92
Manufacturing	33.21	31.06	28.71
Government	29.32	25.12	20.84
Healthcare & Pharmaceuticals	29.80	27.85	25.60
Insurance	35.46	33.32	29.19
Not For Profit	32.63	25.94	30.97
Education	29.20	26.23	26.05
Retail & Wholesale	31.58	30.91	21.93
Other	30.41	28.90	22.85

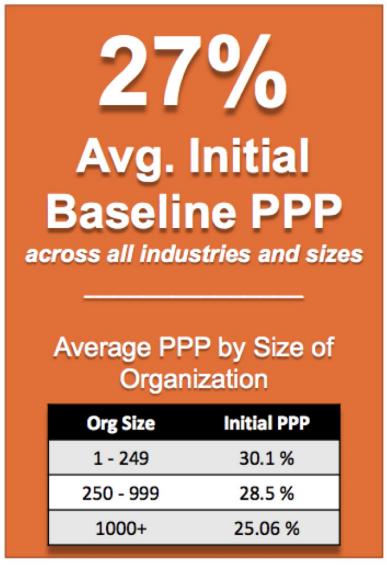


Chart A

* Computer-based training is defined as the delivery of standardized sets of interactive education and/or behavior management content to users via a laptop, desktop or tablet.

Phase Two: After 90 Days of Combined Computer-based Training and Simulated Phishing Security Testing

When organizations implemented a combination of CBT and simulated phishing security testing after their initial baseline testing, results changed dramatically. In just 90 days, the Phish-prone percentage was **cut in half**. (Chart B)

One observation: The dramatic drop in Phish-prone percentages was not specific to a certain industry or organization size. But a few trends are clear:

- The slightly higher results of some larger organizations indicate challenges with implementing a consistent program in a short period.

- Large technology companies were not doing quite as well as other smaller organizations, but still experienced a drastic reduction. After scoring a 30 percent PPP on the baseline test, they dropped down to **19.83 percent in just 90 days**.

Results after 90 Days of CBT and Phishing Testing

90 Day Phish-prone Percentage (90-PPP)			
Industry	**1 – 249 employees**	**250 – 999 employees**	**1000+ employees**
Energy & Utilities	12.53	13.31	13.40
Financial Services	10.01	9.09	14.53
Business Services	12.89	13.99	13.86
Technology	14.12	16.93	19.83
Manufacturing	13.87	14.24	9.88
Government	13.13	12.76	7.90
Healthcare & Pharmaceuticals	16.81	11.02	15.79
Insurance	13.39	16.49	13.23
Not For Profit	16.01	17.28	17.07
Education	16.95	17.16	22.56
Retail & Wholesale	13.39	10.47	10.49
Other	14.86	16.37	19.97

Chart B

The sigificant drop from 27 percent to 13.3 percent for all industries proves that a security awareness training program can pay meaningful dividends in hardening your IT security posture even within the first three months.

Phase Three: After 12 Months of Combined Computer-based Training and Simulated Phishing Security Testing

At this stage, we measured only organizations that conducted 12 months of testing while adhering to best practice recommendations to run phishing tests at least once a month. The results were dramatic, showing that having a consistent, mature awareness training program took the average PPP from **27 percent** all the way down to **2.17 percent** – regardless of industry and size of organization. (Chart C)

Results after 12 Months of CBT and Phishing Testing

365 Day Phish-prone Percentage (365-PPP)			
Industry	**1 – 249 employees**	**250 – 999 employees**	**1000+ employees**
Energy & Utilities	2.83	1.87	5.56
Financial Services	1.54	2.22	5.81
Business Services	1.89	3.09	1.27
Technology	2.02	2.42	2.69
Manufacturing	2.16	3.13	2.47
Government	1.87	1.46	1.52
Healthcare & Pharmaceuticals	2.00	1.65	2.17
Insurance	2.23	2.68	5.26
Not For Profit	2.47	2.24	3.01
Education	2.80	1.91	5.31
Retail & Wholesale	2.14	1.87	2.68
Other	1.82	3.18	4.21

*Percentages are calculated for users who experienced a combination of CBT *and* at least 10 phishing tests.*

Chart C

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. Likely this is due to the complexity of addressing different department and regional needs.

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.

Key Takeaways: The Value of New-school Security Awareness Training

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

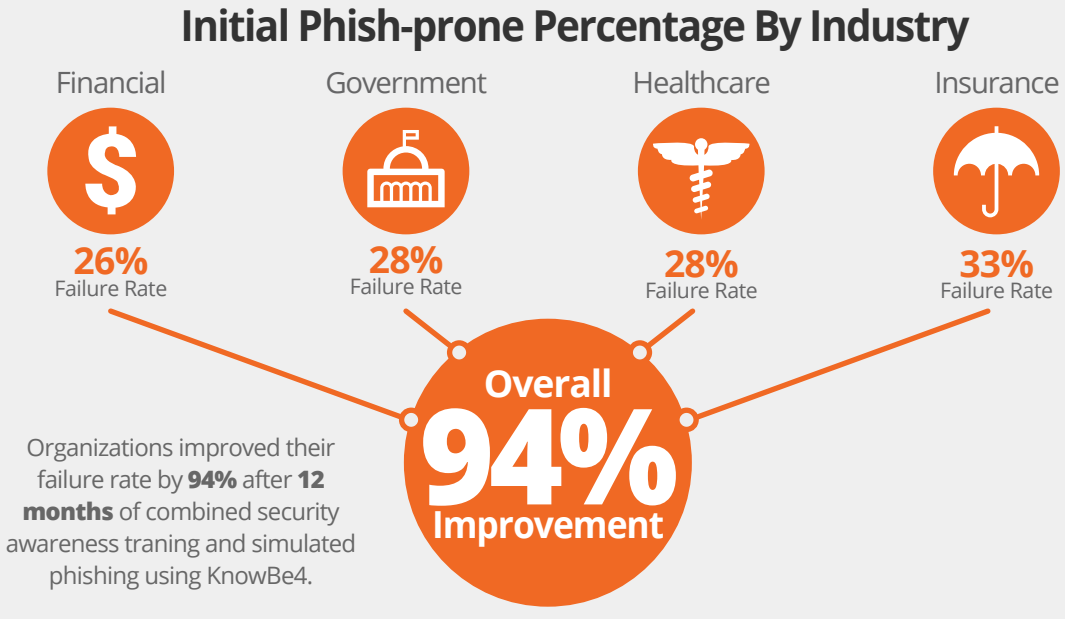
Every organization is at serious risk without new-school security awareness training. With an average baseline PPP of 27 percent, companies could be exposed to social engineering and phishing scams by more than a quarter of their workforce.

Any organization can strengthen security through staff training in as little as three months. The power of a good training program is to instill anti-phishing behavior management and social engineering education in a rapid timeframe.

An effective security awareness training strategy can help accelerate results, especially for large 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.

When you invest in Security Awareness Training and Phishing Security Testing you see value and ROI - fast. Once organizations understand where 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 Industry Benchmarking Report clearly show where organizations' Phish-prone percentages started and where they ended up after 12 months of regular testing and security awareness training.

The overall industry initial Phish-prone percentage benchmark turned out to be a troubling 27 percent. However, there is light at the end of the tunnel. Fortunately, the data showed that this 27 percent can be brought down **more than half to just 13 percent in only 90 days** by deploying new-school security awareness training. The 12-month results show that by following these best practices, the final Phish-prone percentage **can be minimized to 2.17 percent on average**. Another way to look at the results: Organizations improved their failure rate by an **astounding 94 percent in one year** after using the KnowBe4 platform.

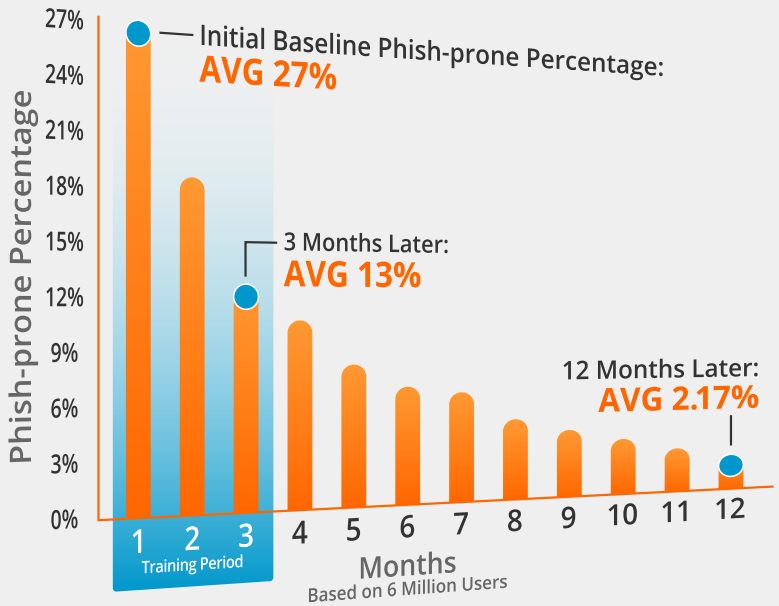


Today, reducing the Phish-prone percentage of your employees through new-school security awareness training is one the most cost-effective network protection measure organizations can take. Two common goals of security awareness training are risk reduction and compliance. Risk reduction is the most important one and has by far the biggest Security ROI. Forrester Research assessed the performance of the KnowBe4 platform in their 2017 Total Economic Impact (TEI™) Study and found a **127 percent return-on-investment with a one-month payback**.

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 organiztion 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.

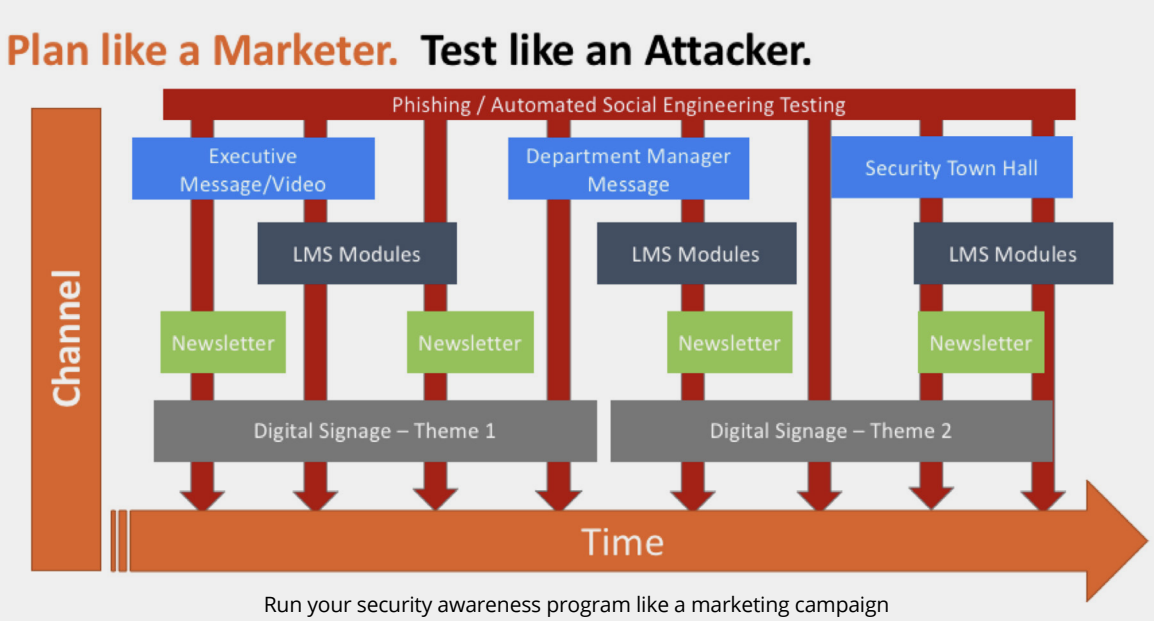
1. Use real-world attack methods. Your simulated phishing exercises must mimic real attacks and methodologies. Otherwise, your "training" will simply give your organization a false sense of security.

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.



Run your security awareness program like a marketing campaign

Train Your Staff Today

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 (PST).

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 adress 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.

KnowBe4
Human error. Conquered.

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