KnowBe4

Phishing by Industry Benchmarking Report

2025 EDITION

WWW.KNOWBE4.COM

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

The 21-Second Countdown...

People are still incredibly quick to click. The Verizon Data Breach Investigations Report (DBIR) revealed that the median time to click on a malicious link in a phishing email is just 21 seconds.

This means you have less than half a minute for an employee to realize what they're about to do.

The Verizon DBIR also found that when data input is needed (e.g., for credential theft), employees spend an average of another 28 seconds. So even for attacks that require a response from the target, you have just 49 seconds to influence the outcome.

Phishing Attacks are Increasing in Scale and Sophistication

The latest KnowBe4 Phishing Threat Trends Report highlighted two notable increases: an overall bump of 17.3% in the quantity of phishing emails and a 47% increase in attacks successfully evading native defenses and secure email gateways (SEGs). In other words, more attacks are being sent and traditional defenses are becoming less effective against them.

As can probably be anticipated, artificial intelligence (AI) is the primary driver in the increase of advanced phishing attacks that evade certain technical detection measures and also appear more plausible to the target. In fact, KnowBe4's Threat Research team observed that 82.6% of phishing emails sent in a six-month period utilized some form of AI. They also believe the continued use of AI in phishing campaigns will render some detection mechanisms (such as grouping malicious emails) obsolete in the next two years.

Other factors driving increased risk globally include Business Email Compromise (BEC), particularly within the supply chain; rapid, and often uneven, digital transformation creating new vulnerabilities; and the ever-present "human factor" that leaves us exposed to social engineering.

Shining a Light on Human Risk and Reducing Phishing Click Rates in 2025

Reducing phishing risk is central to effective human risk management (HRM).

Every successful phishing attack is reliant on a trusted person to carry out a specific action, such as clicking on a hyperlink. If a phishing email gets through technical defenses, it will still fail if the recipient subsequently reports, deletes or does not engage with it.

While enhancing their technical defenses with an AI-powered anti-phishing product, organizations can also significantly reduce their phishing risk through best-practice security awareness training (SAT).

The first step to any effective risk mitigation strategy is to understand your organization's risk profile and how it compares against others of the same industry, organizational size and geographical region. Next, identify how susceptible your organization actually is to phishing risk — and, in particular, who might interact with a phishing email. These insights will enable you to deliver timely and personalized security, such as bespoke training programs and real-time coaching.

Our annual Phishing By Industry Benchmarking Report provides the initial step in this strategy. For this year's report, we analyzed a total of 67,718,305 phishing simulations across 14,508,441 users in 62,460 organizations over a three-year period to show the Phish-prone™ Percentage (PPP) for organizations across 19 industries and seven geographical regions.

How We Calculate Phish-prone Percentages

67.7M
Phishing Security Tests

14.5M
Users

62.4K
Organizations

What is the Phish-prone Percentage?

The PPP is the percentage of employees within an organization likely to fall for social engineering or phishing attacks. Elsewhere, you might see it described as “phishing simulation click rate.”

Methodology

Phase One

Baseline Phishing Security Test Results

Before any KnowBe4 training takes place, we send an initial phishing simulation. This is used to identify risks and calculate an organization’s baseline PPP.

Phase Two

Phishing Security Test Results Within 90 Days of Training

Employees receive KnowBe4’s security awareness training. Another simulation is sent to recalculate the organization’s PPP and measure the effectiveness of the training program.

Phase Three

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

After 12 months of KnowBe4’s security awareness training, the PPP is calculated again to further quantify the training program’s effectiveness.

Analyzing Training Effectiveness

The Big Picture: Global Phishing Click Rates

In Phase One, before any SAT had been administered, the global average PPP was 33.1%. So, one in three employees clicked the link.

When we dig in, we find over half of industries (10 out of 19) have a PPP that's above this average. Across organizations of all sizes, these are the most at-risk industries:

1. Healthcare & Pharmaceuticals: 41.9%
2. Insurance: 39.2%
3. Retail & Wholesale: 36.5%

Only five industries have PPPs below 30%. Even then, well over one-quarter of employees are phish prone: Transportation (29.9%), Business Services (29.6%), Consumer Services (29.5%), Legal (28.5%) and Government (28.2%).

The Larger the Organization, the Greater the Risk

On average, organizations with 10,000+ employees had a PPP of 40.5%. Those with 1,000-9,999 had a PPP of 33.7%, compared to 28.7% for organizations with 250-999 employees and 24.6% for organizations with 1-250 people.

It makes sense: more people equals more mailboxes and more fingers that can click on hyperlinks. Plus, it can be harder to raise collective awareness across a greater number of people.

The risk profile shifted across different industries and organization sizes, but overall, the greatest risk lay with the larger organizations.

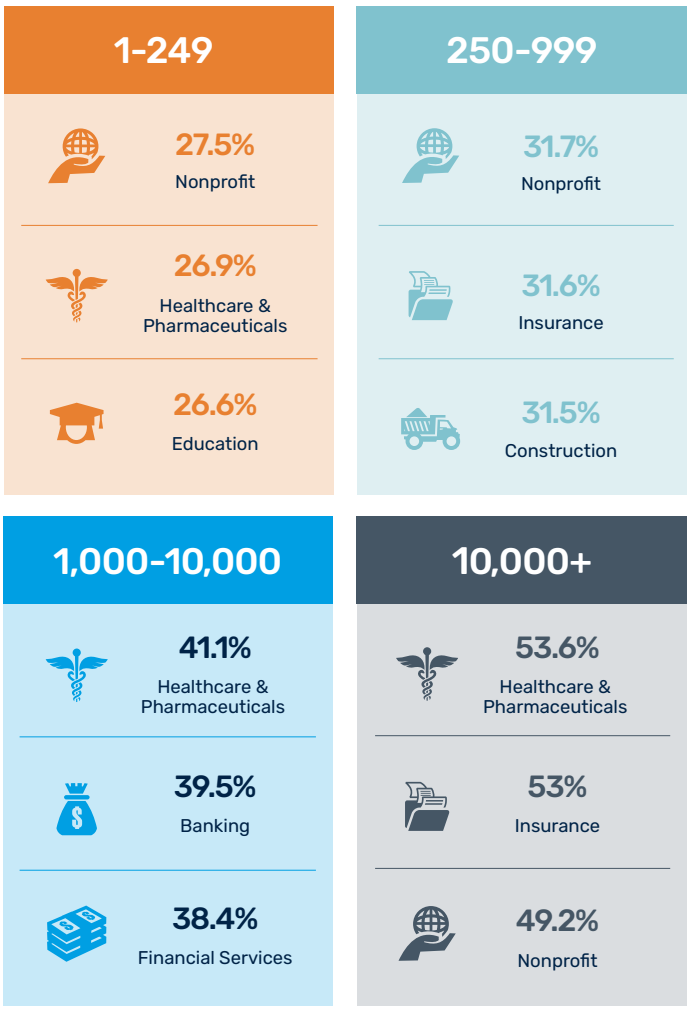
Phishing Risk Can Go Down — and Stay Down

There is good news. After just 90 days of best-practice training, every industry experienced a significant reduction in phishing risk. On average, the global PPP reduced by 40% to just under one in five employees (19.8%) clicking the link.

It keeps getting better: after 12 months, the average PPP drops 86% to 4.1% — and this reduction lasts for the long term. With ongoing training, average PPPs fell to 3.7% after two years and 3.6% after three years. This reduction was visible across every industry.

Who's At Risk

The Top Three Riskiest Industries By Organization Size



87% Average Improvement Rate for Organizations with 10,000+ Employees

The largest organizational segment (10,000+ employees) had the highest average baseline PPP at 40.5%. This initial risk was significantly elevated across multiple industries, with four seeing approximately half of their employees clicking on phishing links: Healthcare & Pharmaceuticals (53.6%), Insurance (53%), Nonprofit (49.2%), and Retail & Wholesale (47%).

These enterprises also demonstrated the greatest risk reduction, with an 86.8% average improvement rate. The hospitality sector achieved the greatest improvement, reducing their click rate by 93% to just 2.4% phish-prone employees. These sectors also achieved an average improvement rate of 90% and above: Consulting (92%), Manufacturing (92%), Financial Services (91%), Banking (91%), Retail & Wholesale (90%) and Healthcare & Pharmaceuticals (90%).

Industry	PPP Baseline	PPP 90 Days	PPP 1 Year	Improvement Rate %
Banking	43.2%	11%	4%	**91%**
Business Services	27.6%	10.5%	4.7%	**83%**
Construction	28.1%	20.1%	6.7%	**76%**
Consulting	41%	21.7%	3.4%	**92%**
Consumer Services	26.8%	11.8%	3.7%	**86%**
Education	34.2%	17.3%	4.8%	**86%**
Energy & Utilities	41%	14.7%	5.3%	**87%**
Financial Services	44.7%	16.8%	3.9%	**91%**
Government	29.9%	13.6%	3.7%	**87%**
Healthcare & Pharmaceuticals	53.6%	16.8%	5.3%	**90%**
Hospitality	33.1%	15.7%	2.4%	**93%**
Insurance	53%	17.5%	7%	**87%**
Legal	31.8%	16.7%	4.7%	**85%**
Manufacturing	43.7%	17.2%	3.6%	**92%**
Nonprofit	49.2%	21.1%	6%	**88%**
Other	31.5%	20.3%	7.2%	**77%**
Retail & Wholesale	47%	18.1%	4.7%	**90%**
Technology	40.6%	16.6%	6%	**85%**
Transportation	33.6%	18.3%	5.6%	**83%**

87% Average Improvement Rate for Organizations with 1,000-9,999 Employees

Organizations with 1,000-9,999 employees had an average baseline PPP of 33.7%, meaning one-third of employees were prone to clicking on phishing links. When compared to those with 10,000+ employees, click rates for organizations of this size showed less variety by industry. Notably, however, four industries stood out as having elevated initial risk: Healthcare & Pharmaceuticals (41.1%), Banking (39.5%), Financial Services (38.4%) and Energy & Utilities (37.2%).

At 87%, the average improvement rate matched that of the largest organizations. Three sectors achieved improvement rates at 91%: Healthcare & Pharmaceuticals, Hospitality and Legal. Legal organizations achieved the lowest click rate after one year of SAT (3.1%). Numerous other sectors (including Banking and Energy & Utilities, which had elevated baselines) also achieved average improvement rates in the high 80% range.

Industry	PPP Baseline	PPP 90 Days	PPP 1 Year	Improvement Rate %
Banking	39.5%	18.2%	4.1%	**89%**
Business Services	33.9%	22.2%	4.5%	**87%**
Construction	33%	21.4%	4.8%	**85%**
Consulting	33.9%	19.6%	4.2%	**87%**
Consumer Services	32%	21.7%	4%	**87%**
Education	31.7%	19%	4.6%	**85%**
Energy & Utilities	37.2%	19.4%	3.9%	**89%**
Financial Services	38.4%	19.8%	4.8%	**87%**
Government	29.1%	17.9%	4.4%	**85%**
Healthcare & Pharmaceuticals	41.1%	19.8%	3.7%	**91%**
Hospitality	36.4%	20.2%	3.3%	**91%**
Insurance	36.3%	17.8%	4.6%	**87%**
Legal	33.3%	17.3%	3.1%	**91%**
Manufacturing	31.6%	19.9%	3.8%	**88%**
Nonprofit	35.9%	21.7%	3.7%	**89%**
Other	31.4%	18.5%	4.4%	**86%**
Retail & Wholesale	34.7%	20%	4%	**88%**
Technology	32.3%	21.8%	4.4%	**86%**
Transportation	28.7%	20%	4.4%	**84%**

86% Average Improvement Rate for Organizations with 250-999 Employees

As organization size decreases, so does the global average baseline PPP, dropping to 28.7% for those with 250-999 employees. Still, however, almost one-third of employees are likely to click on a phishing link. Baseline PPP was generally consistent across industries; however, six stood out as having a PPP of 30% and above: Nonprofit (31.7%), Insurance (31.6%), Healthcare & Pharmaceuticals (31.4%), Construction (31.5%), Banking (30.4%) and Consumer Services (30.1%).

At 85.6%, the average improvement rate remained high for organizations of this size. Significantly, Banking — one of the sectors with the highest baseline PPPs — achieved the greatest risk reduction, with click rates dropping by 91.8% to just 2.5%. Risk reduction across all industries clustered close to or above the average, with the next highest rates achieved by Construction (89%), Energy & Utilities (88%), Manufacturing (87%), Transportation (87%) and Financial Services (87%).

Industry	PPP Baseline	PPP 90 Days	PPP 1 Year	Improvement Rate %
Banking	30.4%	16.9%	2.5%	**92%**
Business Services	28.7%	22.2%	4.2%	**85%**
Construction	31.5%	24%	3.5%	**89%**
Consulting	29.7%	23.2%	4%	**86%**
Consumer Services	30.1%	24%	4.9%	**83%**
Education	28.4%	19.7%	4.5%	**84%**
Energy & Utilities	28.8%	21.4%	3.6%	**88%**
Financial Services	28.9%	19.5%	3.8%	**87%**
Government	26.8%	18.6%	3.7%	**86%**
Healthcare & Pharmaceuticals	31.4%	23.7%	4.5%	**86%**
Hospitality	29.1%	23%	5.8%	**80%**
Insurance	31.6%	23.3%	5.1%	**84%**
Legal	25.1%	18.7%	4.7%	**81%**
Manufacturing	27.1%	21%	3.4%	**87%**
Nonprofit	31.7%	24.2%	4.5%	**86%**
Other	27.5%	22.1%	4%	**85%**
Retail & Wholesale	28.4%	22.7%	4.3%	**85%**
Technology	27.5%	21.8%	4.1%	**85%**
Transportation	27.1%	22.6%	3.5%	**87%**

85% Average Improvement Rate for Organizations with 1-249 Employees

The average global baseline PPP for our smallest organizational segment (1-249 employees) was the lowest, with one-quarter (24.6%) of phish-prone employees. This baseline click rate remained relatively consistent across industries, with the highest in Nonprofit (27.5%), Healthcare & Pharmaceuticals (26.9%), Education (26.6%) and Retail & Wholesale (26.5%).

The Banking sector reduced its click rate by the greatest amount, achieving a 2% PPP after one year of training and marking a 90% improvement. The next highest average improvement rates of 87% were achieved by Energy & Utilities, Transportation, Construction and Education.

Industry	PPP Baseline	PPP 90 Days	PPP 1 Year	Improvement Rate %
Banking	21.1%	15.3%	2%	**90%**
Business Services	23.8%	22.2%	3.8%	**84%**
Construction	25%	21.7%	3.2%	**87%**
Consulting	24.4%	21.9%	3.4%	**86%**
Consumer Services	24.8%	21.7%	3.8%	**85%**
Education	26.6%	19.8%	3.5%	**87%**
Energy & Utilities	24.9%	19.9%	3.1%	**87%**
Financial Services	23.1%	18.8%	3.1%	**86%**
Government	25.1%	19.3%	4%	**84%**
Healthcare & Pharmaceuticals	26.9%	24.1%	4.5%	**83%**
Hospitality	24.8%	23.4%	3.7%	**85%**
Insurance	22.7%	21.5%	3.4%	**85%**
Legal	25.3%	20.8%	4.2%	**83%**
Manufacturing	24.8%	21.2%	3.6%	**85%**
Nonprofit	27.5%	25.2%	4.3%	**84%**
Other	24.4%	22%	4%	**83%**
Retail & Wholesale	26.5%	22%	3.9%	**85%**
Technology	22.6%	22%	3.6%	**84%**
Transportation	23.2%	21.6%	2.9%	**87%**

Key Takeaways

The Power of AI

Across all geographical regions, AI-powered social engineering and phishing attacks represent the biggest cybersecurity threat targeting employees, demanding more personalized, relevant and adaptive SAT

Every Organization is at Serious Risk Without Security Awareness Training

With an average industry baseline PPP of 33.1%, a third of an organization's workforce is exposed to social engineering and phishing attacks

Security Awareness Training Changes Behavior and Reduces Risk in as Little as Three Months

Just 90 days of SAT can reduce your organization's PPP by over 40%; 12 months of training reduces it by 86% to just 4.1%

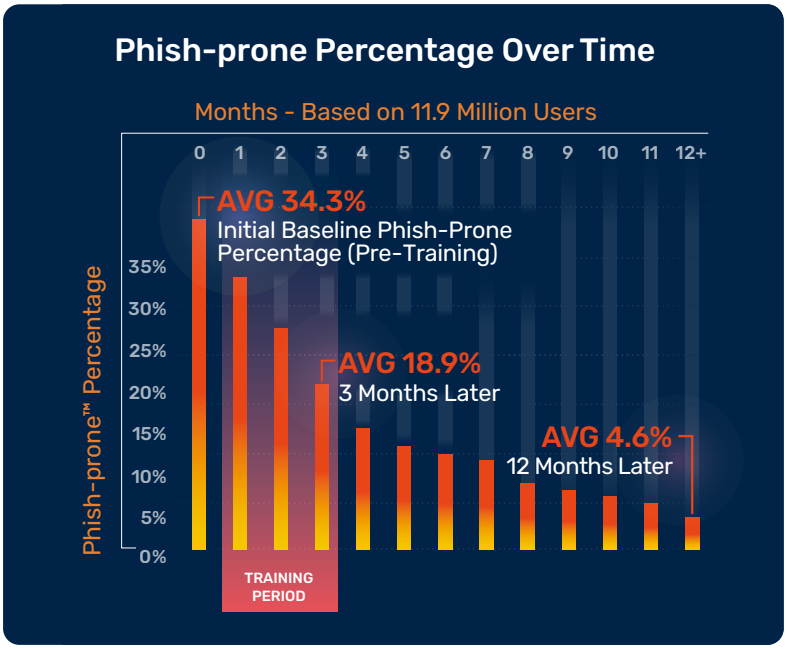
Keys to Success

To favorably change security behaviors and reduce risk, a security awareness training program must have:

- Clearly defined and communicated mandates
- Strong alignment with organizational security policies and threats
- An active connection to overall security culture
- Full executive support

Security Awareness Training is the Foundation for a Successful Human Risk Management Strategy

Human risk management represents the next phase in the evolution of employee education and engagement. HRM takes a data-driven approach to assessing individual risk by analyzing everything from phishing tests and training scores to real-world security incidents and behavioral trends. Leveraging this data, organizations can deliver highly relevant and personalized SAT and adaptive security controls to positively influence security decision making at the point of risk.



About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk.

For more information, please visit **www.KnowBe4.com**

Read Our Regional Analysis of the Phishing By Industry Benchmarking Report

- North America
- Africa
- Asia
- Europe
- Oceania
- South America
- United Kingdom and Ireland

KnowBe4

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