



2024 Phishing Attack Landscape and Benchmarking

The data you need to know



Perry Carpenter
Chief Human Risk Management Strategist
KnowBe4, Inc.



Joanna Huisman
SVP Strategic Insights & Research
KnowBe4, Inc.



Perry Carpenter
Chief Human Risk Management
Strategist
KnowBe4, Inc.



Joanna Huisman
SVP Strategic Insights & Research
KnowBe4, Inc.

PHISHING BY INDUSTRY BENCHMARKING REPORT

2024 EDITION

The question every executive asks...

Agenda

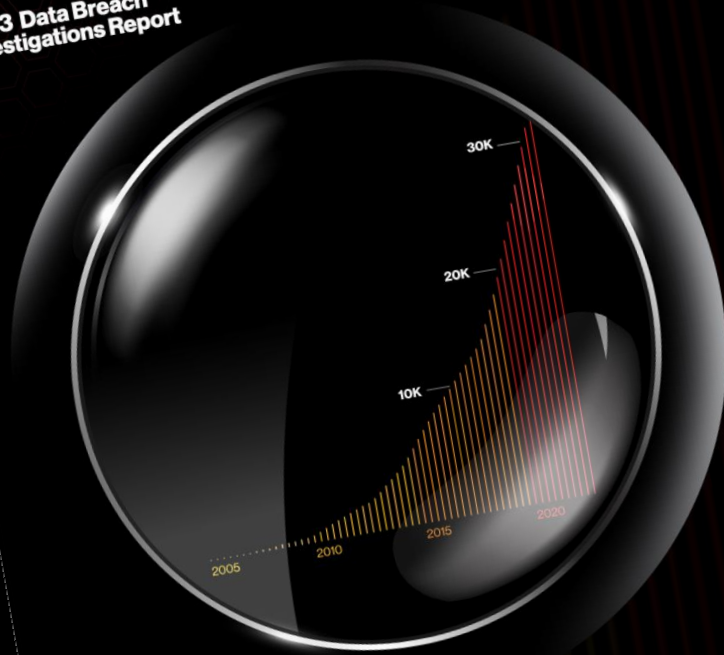
1. The phishing problem
2. Phishing benchmark data by industry
3. International phishing benchmark data by region
4. Actionable tips to strengthen your human defense layer and create a security aware culture

Agenda

1. The phishing problem
2. Phishing benchmark data by industry
3. International phishing benchmark data by region
4. Actionable tips to strengthen your human defense layer and create a security aware culture

DBIR

2023 Data Breach Investigations Report

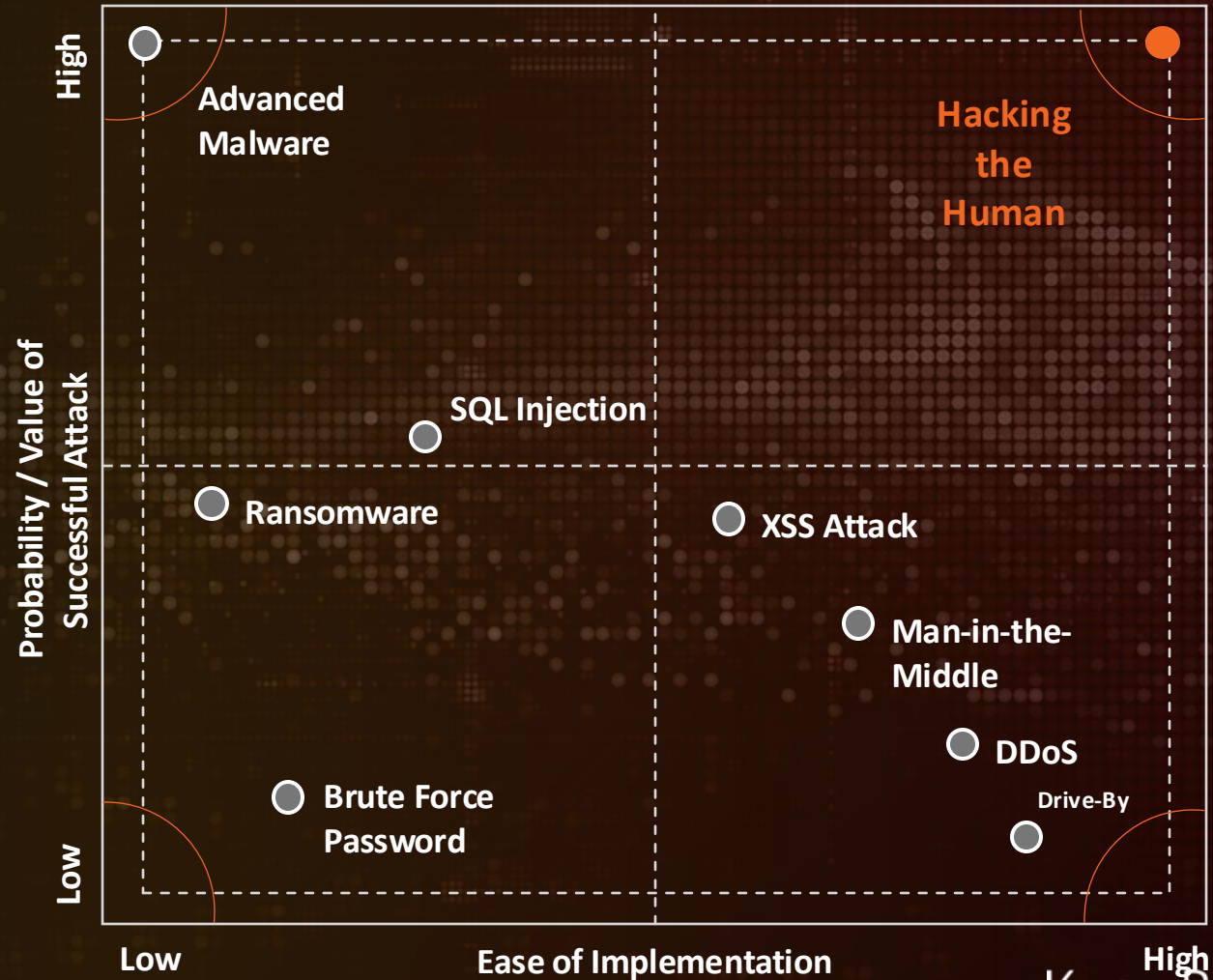


verizon

Verizon's 2024 Data Breach Investigations Report states that "68% of all breaches include the human element, with people being involved either via error, privilege misuse, use of stolen credentials or social engineering."

With favorable movement over the prior year, this renewed focus on the human element is working...but the job is not done.

Social Engineering is Popular Because it Works!



Agenda

1. The phishing problem
2. Phishing benchmark data by industry
3. International phishing benchmark data by region
4. Actionable tips to strengthen your human defense layer and create a security aware culture

Methodology & Data Set

54.1M
Phishing
Security Tests



11.9M
Users



55.7K
Organizations



42,488
Organizations

9,934
Organizations

3,253
Organizations



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

Three-Phases of Measurement



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.

Who's at Risk?

The top three riskiest industries by organization size

RISKY
BUSINESS

SMALL 1-249	MEDIUM 250-999	LARGE 1,000+
 34.7% Healthcare & Pharmaceuticals	 39.7% Hospitality	 51.4% Healthcare & Pharmaceuticals
 32.4% Education	 38.8% Healthcare & Pharmaceuticals	 48.8% Insurance
 31.2% Hospitality	 36.2% Consulting	 47.8% Energy & Utilities

Phase 1- Benchmark

Phase One

34.3%

Initial Baseline
Phishing Security
Test Results

Organization Size

1-249
250-999
1000+

Initial PPP

28.7%
31.9%
37.5%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	27.8%	33.3%	42.3%
Business Services	26.7%	31.6%	33.2%
Construction	28.8%	35.0%	32%
Consulting	28.4%	36.2%	47%
Consumer Services	28.8%	31.2%	31.6%
Education	32.4%	31.2%	31.7%
Energy & Utilities	29.3%	33.3%	47.8%
Financial Services	28.1%	31%	41.6%
Government	27.9%	27.8%	28.6%
Healthcare & Pharmaceuticals	34.7%	38.8%	51.4%
Hospitality	31.2%	39.7%	31.8%
Insurance	28.6%	34.1%	48.8%
Legal	26.5%	29.2%	35.2%
Manufacturing	27.9%	31.6%	35.9%
Not-For-Profit	30.3%	33.9%	36.7%
Other	26.3%	28.9%	29.7%
Retail & Wholesale	30.7%	32%	42.4%
Technology	26.1%	30.3%	32.9%
Transportation	27%	28.6%	35.1%

Phase 2 – 90 Days

Phase Two
18.9%

Phishing Security
 Test Results Within
 90 Days of Training

Organization Size

90-Day PPP

1-249	19.9%
250-999	20.1%
1000+	18%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	13.9%	16.6%	13.8%
Business Services	20.8%	21.9%	21.3%
Construction	20.8%	21.5%	19.6%
Consulting	20%	21.8%	21.9%
Consumer Services	20.5%	20.9%	19.3%
Education	19%	19.4%	18%
Energy & Utilities	18.7%	19.5%	16.7%
Financial Services	17.4%	17.9%	18%
Government	17.7%	17.1%	15.6%
Healthcare & Pharmaceuticals	21.9%	20.8%	17.7%
Hospitality	21.9%	23.7%	15%
Insurance	20%	19.3%	15.7%
Legal	18.8%	16.7%	18%
Manufacturing	19.6%	19.8%	17.4%
Not-For-Profit	23.1%	23%	21.8%
Other	20.6%	21.5%	18.8%
Retail & Wholesale	20.6%	21.1%	18.3%
Technology	21.1%	20.8%	18.5%
Transportation	21.1%	20.4%	20.5%

Phase 3 – 12 months

Phase Three

4.6%

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

Organization Size

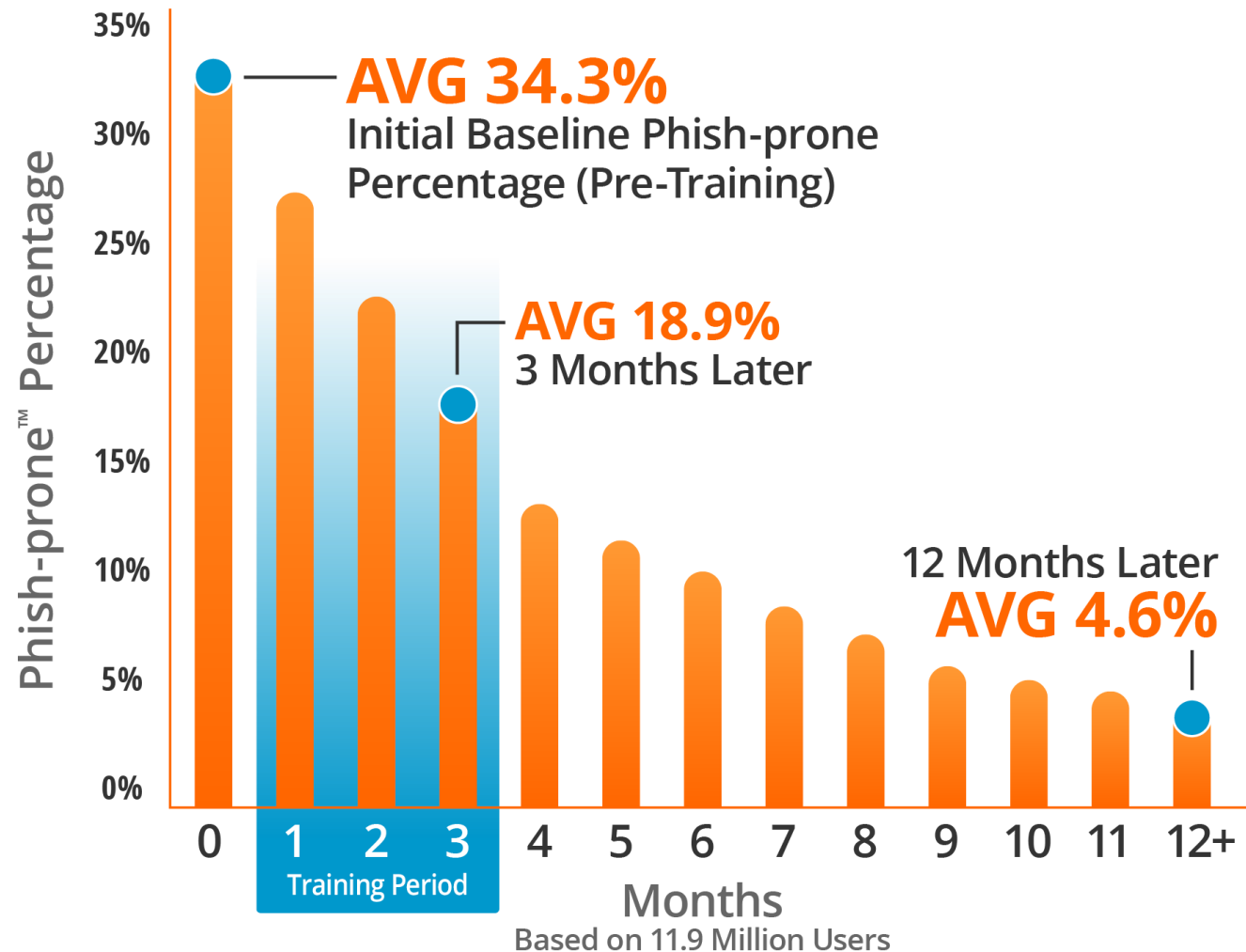
12-Month PPP

1-249	4.3%
250-999	4.6%
1000+	4.9%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	2.5%	3.3%	5.2%
Business Services	5.3%	4.7%	5.3%
Construction	4%	4.8%	4.6%
Consulting	4%	4.6%	4.4%
Consumer Services	5%	5%	4.8%
Education	3.9%	5.2%	4.9%
Energy & Utilities	3.7%	4.2%	4%
Financial Services	3.5%	4.6%	4.7%
Government	4.4%	4.3%	4.5%
Healthcare & Pharmaceuticals	5.4%	4.3%	5.5%
Hospitality	4.2%	4.4%	3.4%
Insurance	3.8%	5.2%	7.7%
Legal	5.6%	6.4%	3.7%
Manufacturing	4.1%	4.1%	4.3%
Not-For-Profit	5.6%	5.5%	4.2%
Other	4.3%	4.9%	4.3%
Retail & Wholesale	4.7%	4.5%	5.2%
Technology	4.1%	4.6%	5.3%
Transportation	4.5%	5.4%	6.7%

The Results are in:

and they are dramatic



Source: 2024 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.

“

Rather than viewing employees as inherent weaknesses, organizations should empower them as active participants in the fight against cyber crime.

Average Improvement

86%

Average Improvement Rates Across All Industries and Organization Sizes

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	91%	90%	88%
Business Services	80%	85%	84%
Construction	86%	86%	86%
Consulting	86%	87%	91%
Consumer Services	83%	84%	85%
Education	88%	83%	85%
Energy & Utilities	87%	87%	92%
Financial Services	88%	85%	89%
Government	84%	85%	84%
Healthcare & Pharmaceuticals	84%	89%	89%
Hospitality	87%	89%	89%
Insurance	87%	85%	84%
Legal	79%	78%	89%
Manufacturing	85%	87%	88%
Not-For-Profit	82%	84%	89%
Other	84%	83%	86%
Retail & Wholesale	85%	86%	88%
Technology	84%	85%	84%
Transportation	83%	81%	81%

Agenda

1. The phishing problem
2. Phishing benchmark data by industry
3. International phishing benchmark data by region
4. Actionable tips to strengthen your human defense layer and create a security aware culture

2024 International Chart

Phase One

Initial 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

BASELINE

90 DAYS

1 YEAR

Organization Size

1-249

250-999

1000+

1-249

250-999

1000+

1-249

250-999

1000+

North America

29%

32.6%

39.1%

19.8%

19.9%

17.9%

4.3%

4.6%

4.6%

TOTAL: 35.1%

TOTAL: 18.9%

TOTAL: 4.5%

Africa

29.7%

32.8%

38%

23.7%

28.7%

20.2%

3.6%

5.4%

6.2%

TOTAL: 36.7%

TOTAL: 22%

TOTAL: 5.9%

Asia

31.5%

31.6%

27.4%

20.3%

17.6%

16.6%

5.4%

4.5%

5.9%

TOTAL: 28.4%

TOTAL: 17%

TOTAL: 5.5%

Australia & New Zealand

27.8%

32.5%

40.3%

21.4%

20.3%

16.5%

4.9%

5.3%

4.7%

TOTAL: 34.4%

TOTAL: 19.1%

TOTAL: 5%

Europe

26.5%

26.9%

35.6%

19.3%

20.2%

20.6%

4.1%

4.9%

5.9%

TOTAL: 32.6%

TOTAL: 20.3%

TOTAL: 5.5%

South America

32.7%

29.4%

44.9%

24.4%

22.5%

16.8%

5.2%

5.2%

3%

TOTAL: 39.2%

TOTAL: 18.7%

TOTAL: 3.9%

United Kingdom & Ireland

26.5%

30.2%

35.2%

20%

21%

16.5%

4.1%

4.3%

4.8%

TOTAL: 32.3%

TOTAL: 18.4%

TOTAL: 4.5%

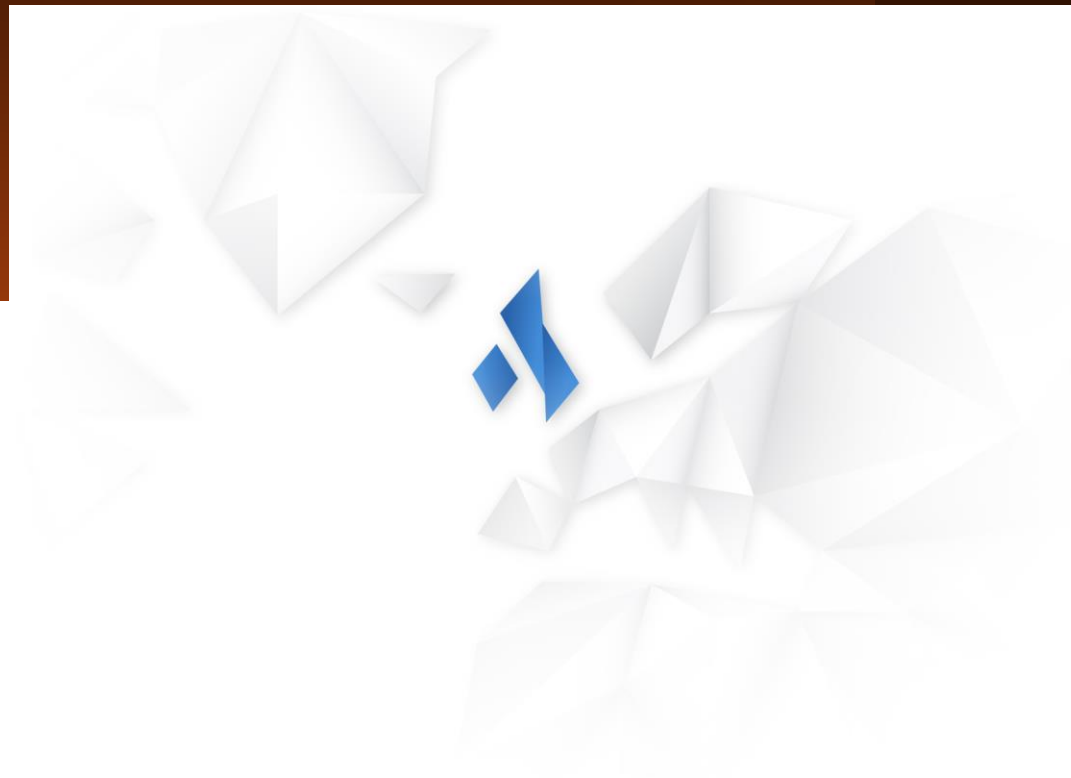
REGION

North America



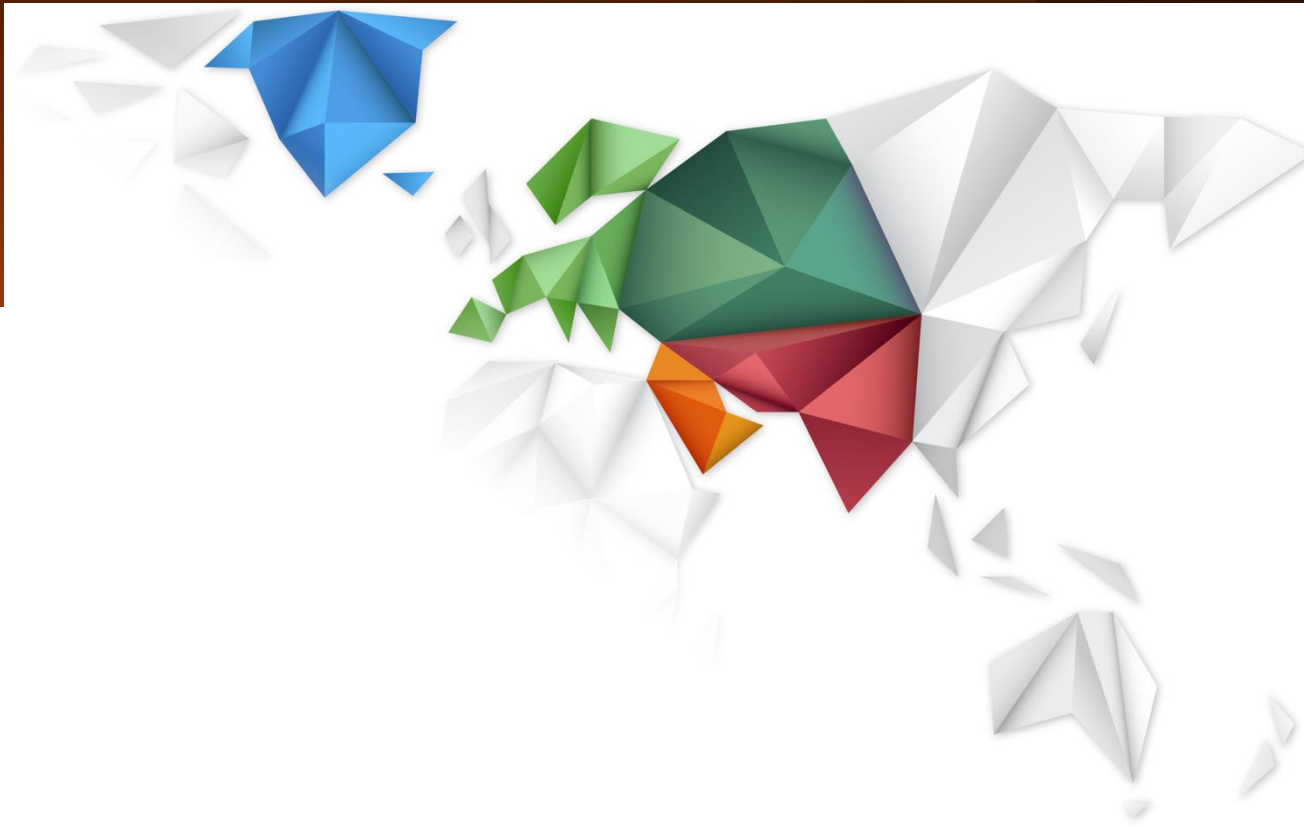
N. AMERICA	BASELINE	90 DAYS	1 YEAR
1-249	29%	19.8%	4.3%
250-999	32.6%	19.9%	4.6%
1000+	39.1%	17.9%	4.6%
Average PPP Across All Organization Sizes	35.1%	18.9%	4.5%

UK & Ireland



UK & IRELAND	BASELINE	90 DAYS	1 YEAR
1-249	26.5%	20%	4.1%
250-999	30.2%	21%	4.3%
1000+	35.2%	16.5%	4.8%
Average PPP Across All Organization Sizes	32.3%	18.4%	4.5%

Europe



EUROPE	BASELINE	90 DAYS	1 YEAR
1-249	26.5%	19.3%	4.1%
250-999	26.9%	20.2%	4.9%
1000+	35.6%	20.6%	5.9%
Average PPP Across All Organization Sizes	32.6%	20.3%	5.5%

Africa



...Africa has had the most exponential growth in cyber crimes over the last few years, particularly among small and medium-sized businesses.

AFRICA	BASELINE	90 DAYS	1 YEAR
1-249	29.7%	23.7%	3.6%
250-999	32.8%	28.7%	5.4%
1000+	38%	20.2%	6.2%
Average PPP Across All Organization Sizes	36.7%	22%	5.9%

South America



S. AMERICA	BASELINE	90 DAYS	1 YEAR
1-249	32.7%	24.4%	5.2%
250-999	29.4%	22.5%	5.2%
1000+	44.9%	16.8%	3%
Average PPP Across All Organization Sizes	39.2%	18.7%	3.9%

Asia



At the end of 2023, the **APAC region** accounted for nearly a quarter (23%) of global cybersecurity incidents, according to the IBM X-Force Threat Intelligence Index.



ASIA	BASELINE	90 DAYS	1 YEAR
1-249	31.5%	20.3%	5.4%
250-999	31.6%	17.6%	4.5%
1000+	27.4%	16.6%	5.9%
Average PPP Across All Organization Sizes	28.4%	17%	5.5%

Australia & New Zealand



AUSTRALIA & NEW ZEALAND	BASELINE	90 DAYS	1 YEAR
1-249	27.8%	21.4%	4.9%
250-999	32.5%	20.3%	5.3%
1000+	40.3%	16.5%	4.7%
Average PPP Across All Organization Sizes	34.4%	19.1%	5%

Agenda

1. The phishing problem
2. Phishing benchmark data by industry
3. International phishing benchmark data by region
4. Actionable tips to strengthen your human defense layer and create a security aware culture

SECURITY AND RISK MANAGEMENT EXECUTIVES CAN ENSURE THE SUCCESS OF THEIR PROGRAMS BY:



Fostering a Security Culture



Role Modeling



Engaging a Pro



Thinking Like a Marketer



Mobilizing a Security
“Culture Carrier” Program



Adding Ongoing
Simulated Phishing Tests



Increasing Frequency



Hiring the Right People



Defining Objectives



Measuring Effectively



Motivating Employees

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.

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.

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.



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.

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 33.2%, 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.

A 4-Step Security Awareness Training Program that Works!

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-school 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 PPP as possible.





Thank You

KnowBe4
Human error. Conquered.