Phishing by Industry Benchmarking Report

ASSESS YOUR RISK AND IMPROVE SECURITY

Contents

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 2022, the world continued to see significant year-over-year increases in phishing attacks. No industry vertical, size of business, or geography was immune.

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.

Understanding Risk by Industry

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 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.

To help organizations evaluate their PPP and understand the implications of their ranking, 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.

23.4
million
phishing security tests

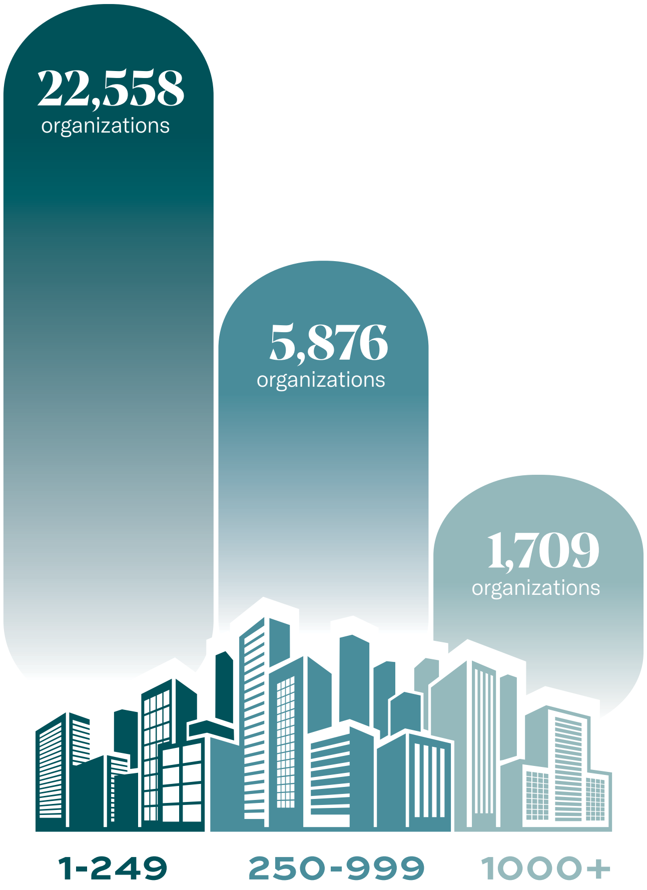
9.5
million
users

30.1
thousand
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

ORGANIZATION SIZE RANGES



Who's At Risk: Ranking Industry Vulnerability

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, revealing that untrained users are failing as an organization's last line of defense against phishing attacks.

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 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.

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

Phase One: Baseline Phishing Test Results

The initial baseline phishing security test was administered within organizations without security awareness training. Users received no warning, and the tests were administered to untrained people doing their regular job duties. Here are the results.

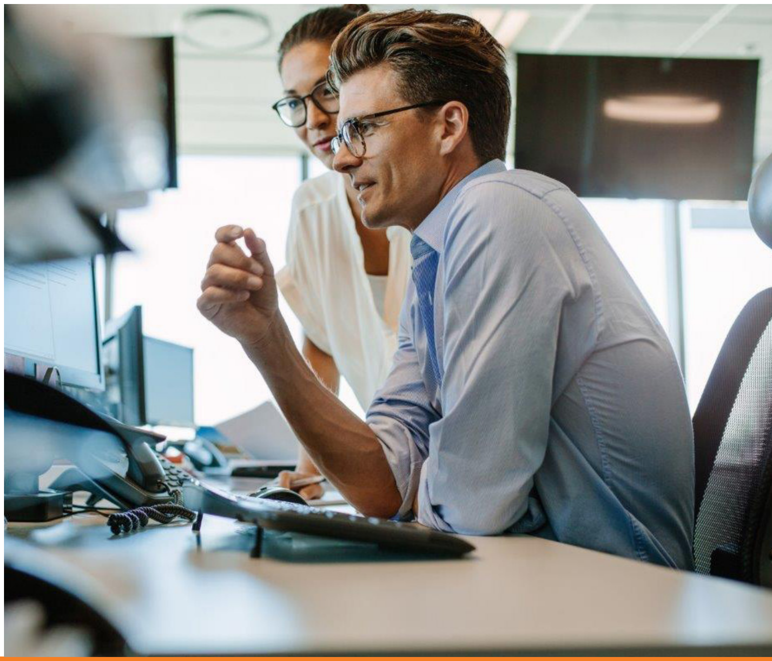
Thoughts: As cyber threats grow, the communication of these threats is filtering to the masses through social/news media. In some areas, people have more information thrust at them, so their awareness is growing more organically. The question remains if that ground-level awareness will transfer to the 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 security technology is.

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%	29.4%	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 Test Results Within 90 Days of Training

When organizations implemented a combination of training and simulated phishing security testing after their initial baseline measurement, the results changed dramatically. In those 90 days after completing 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 any industry or organization size.

Thoughts: After applying only 90 days of new-school security awareness training, organizations saw a significant improvement in employees' abilities to detect malicious emails across every industry and size of organization. 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 Test Results After One Year-Plus of Training

This stage measured security awareness skills after 12 months or more of ongoing training and simulated phishing security tests. The study looked for users who completed training at least one year ago and analyzed the performance results on their 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% down to 5%. **These results were demonstrated significantly across all industry sizes and verticals.**

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%	3.9%	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%

Key Takeaways: The Value of Security Awareness Training

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.** 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 definitive proof for gaining buy-in to establish a fully mature security awareness training program.

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.

Average Improvement

85%

Average Improvement Rate Across All Industries and Sizes

Conclusion & Contact

Jeff McCulloch

President, YYTECH

With a focus on operational efficiency and process improvement, Jeff McCulloch, President, strives to deliver maximum value to clients through right-fit technology solutions and exceptional service delivery.

Joining Yeo & Yeo in 1996 as a software specialist and holding several management positions since, Jeff has more than 25 years of experience in business development, product management, and business operations within high technology companies. Throughout his professional career, he has managed multi-scale technology engagements and support solutions for manufacturers and distributors, financial/credit unions, healthcare institutions, state and local government, retail, nonprofits, and small to mid-size businesses throughout Michigan.

Jeff is a member of Ingram Micro Trust X Alliance, serving as past secretary, Vice President, and President. He is a member of Central Michigan University's Cybersecurity Advisory Board, Saginaw Career Complex's Cybersecurity Program Advisory Committee, and is co-chair of Delta College's Advisory Information Technology Committee.

Information used in this eBook was provided by our partners at KnowBe4.

Ready to start phishing your users? We offer baseline testing to assess the phish-prone percentage of your users through a simulated attack. From there, we can provide access to the world's largest library of training content, including interactive modules, videos, games, posters, and newsletters, so you can start educating and building your human firewall. **Contact us** to get started.

Yeo & Yeo provides an abundance of information surrounding technology solutions. Check out our resources, including the latest blog articles and eBooks **here.**

Let's thrive.

We're here to help. But first, we're here to listen. No matter the need, we build a right-sized, customized path to help you get there.

VISIT
yeoandyeo.com

CALL
800.968.0010

CONNECT