RESILIENCY STRATEGIES

for Battling Phishing Attacks in an AI-Driven Era

Phishing attacks are rapidly transforming and evading detection at an alarming rate. With generative AI fueling the rise of highly targeted phishing campaigns, the threat landscape demands smarter, more proactive strategies. To effectively protect your organization, your security awareness training (SAT) must be based on real and relevant threats that are bypassing perimeter defenses and landing in employee inboxes.

Resiliency, in the context of SAT, refers to an organization's ability to not only reduce susceptibility to phishing attacks but also to empower employees to recognize and report threats effectively. It shifts the focus from merely identifying vulnerabilities to building a culture of capability and preparedness.

Why is resiliency to phishing attacks so important? In today's threat landscape, where AI-generated phishing campaigns are more convincing and harder to detect, resiliency is the cornerstone of a strong defense. It ensures that employees are not just passive participants in security but active defenders who can identify and report threats before they cause harm.

Mimicking Real-Life Threats for Proactive Defense

You can't defend against what you don't train for. Yet, many organizations still rely on outdated phishing simulation templates.

Here's the issue with that approach:

1. **Lack of Relevance:** Employees quickly spot the predictability and tune out, often not even reporting because they have checked out.
2. **Under-preparedness:** Attackers are utilizing today's trends, like AI-enhanced impersonation or targeted multi-channel methods.
3. **Missed Opportunities:** Irrelevant training leads to wasted time without measurable improvement in resiliency.

To address these challenges, organizations must adopt best practices for security awareness training that not only engage employees but also equip them to recognize and report evolving threats. By focusing on relevance and adaptability, training programs can transform from routine exercises into powerful tools for building a proactive and engaged defense.

Best Practices for High-Impact Security Awareness Training

To maximize your SAT program success in the age of AI-generated phishing, Cofense™ recommends these best practices:

1. **Prioritize Relevance Over Generic Content:** Focus on simulating and educating your users on actual threats entering your organization, immersing them in a real-world experience. The threat landscape is constantly changing with evolving tactics and techniques, often impersonating top brands like Microsoft. While eCards and holiday giveaways are fun, they likely aren't the top threats to your organization.

   Connect with your Incident Response (IR) or Security Operations Center (SOC) teams to identify the top threats. Given time and budget constraints, every simulation needs to count. Ideally, when security awareness and operations teams collaborate, everyone wins. Awareness program managers have confidence that simulations are relevant, while the SOC team receives more useful reports from well-conditioned users.

   Remember, the primary goal of your phishing simulation program should be to reduce risk AND condition users to act when they encounter a real attack. Given this, you want to place a large focus of your SAT program on reporting. Recognize this positive behavior regularly. The more an employee reports during simulations, the more they'll report real threats—and build a resilient organization.

   - Customers who delivered scenarios with Cofense Reporter deployed saw a 19% decrease in susceptibility rate compared to customers who do not have Cofense Reporter deployed.

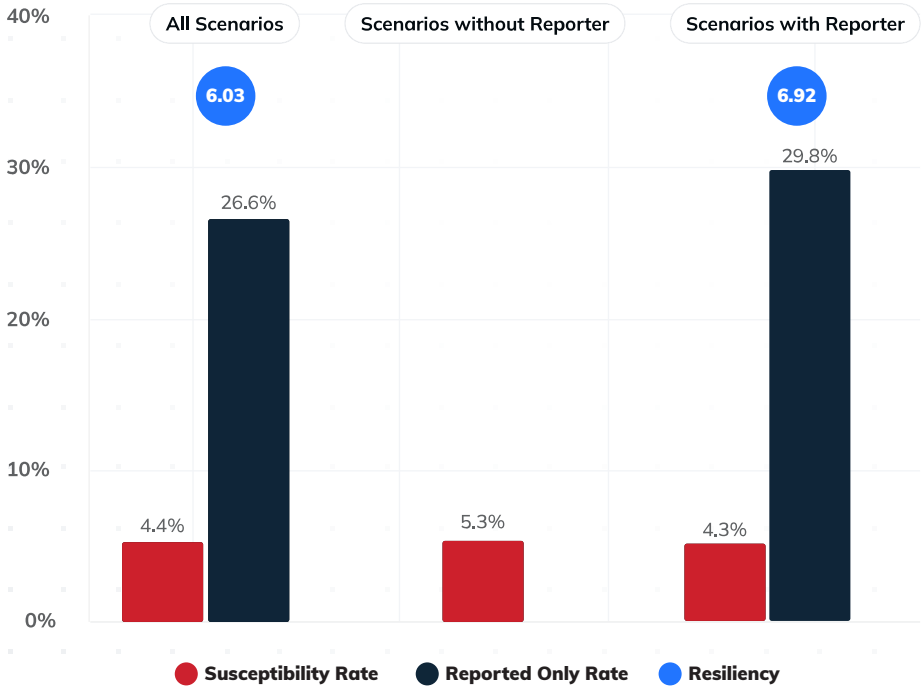

Figure 1: Impact of Cofense Reporter on Susceptibility and Resiliency (2024)

2. **Use a Variety of Training Types and Content Styles**
When training your employees, align your efforts with the mission and goals of your phishing defense program. Flexibility is key—while simulations are a valuable tool, they are just one part of a comprehensive strategy. To be effective, you'll likely need to incorporate multiple training methods beyond simulations. This could include a mix of computer-based training modules, phishing recognition games, in-person sessions, mandatory webinars, and more. Keep in mind: achieving different results requires trying different approaches. Customize your training to accommodate diverse learning styles—there's no one-size-fits-all solution.

3. **Condition Reporting Accuracy Using a Non-Punitive Approach:** Develop reward mechanisms for users who consistently report accurately while maintaining open communication to correct errors.

Customers running **non-punitive programs** observed the highest resiliency consistency due to safe environments permissive of mistakes. Employees learned without fear of HR actions or workplace stigma.

We polled our existing user base, inquiring which organizations run a punitive vs. non-punitive phishing simulation training program. With the collected sample set, we calculated an average response (weighted by size).

Result: Organizations that run a non-punitive program have a lower susceptibility rate, meaning less individuals are falling for a phishing simulation.

In addition, non-punitive programs also see a higher resiliency rate, meaning more individuals are reporting suspicious phishing activity to their response teams. We also find more engagement across the board (less unread/no response activities). Users who feel empowered and part of your company's success metrics are more open to learning and engaging in activities that help your organization's defenses.

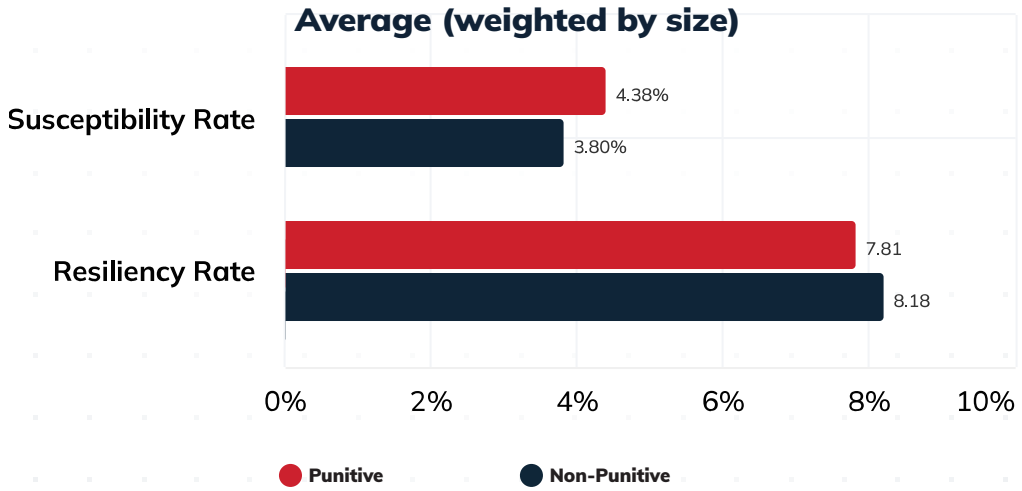

Figure 2: Punitive vs. Non-Punitive Susceptibility and Resiliency Rates

4. Ensure Training Consistency and Build Program Maturation for Increased Resiliency

Consistency is key when running an SAT program. Infrequent testing cannot keep pace with the shifting threat landscape. It's impossible to prepare users for the latest attack techniques when they only practice a few times per year. Within the Cofense PhishMe ecosystem, we have observed that continued education and training drives higher resiliency and lower susceptibility, narrowing your time to mitigate actual phishing threats (see graph below).

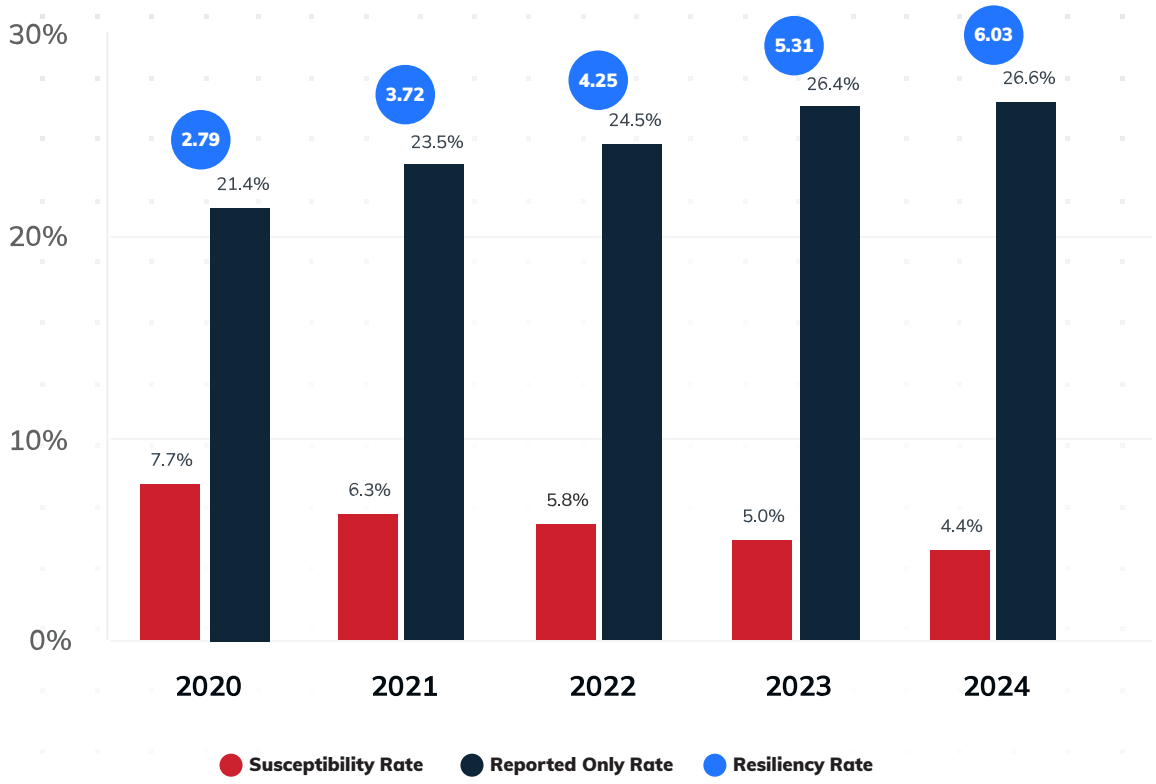

Figure 3: Year-Over-Year Resiliency for Cofense SAT Customers

What's the gold standard in terms of frequency?

Cofense recommends at least monthly simulations to your entire organization, as well as quarterly spear phishing to pre-defined/highly visible groups, and targeted exercises in between to those identified users who need more conditioning - also known as "repeat clickers." You may also want to add a new joiners training track as part of your onboarding process. As someone new joins your organization, include them in a simulation to introduce them to your program. If you have a population of non-reporters, start targeting them with newsletters regarding the importance of reporting.

Over time, high-frequency simulations create "muscle memory" for quicker detection responses. Layer in more sophisticated and targeted simulations to business departments with elevated privileges. Additional tips include:

- **Remove obvious clues like grammatical errors**
- **Personalize your messages with placeholders (such as first name)**
- **Consider spoofing your domain as the sender for targeted spear groups who have heightened awareness**
- **Launch a simulation leveraging a brand imitation template**

If you are not prepared to advance your program to this level yet, you should still focus on sending a monthly campaign to your entire organization. Below, you can see that companies that run monthly campaigns have nearly a 48% increase in their resiliency. Remember, besides being frequent, phishing simulations must be relevant.

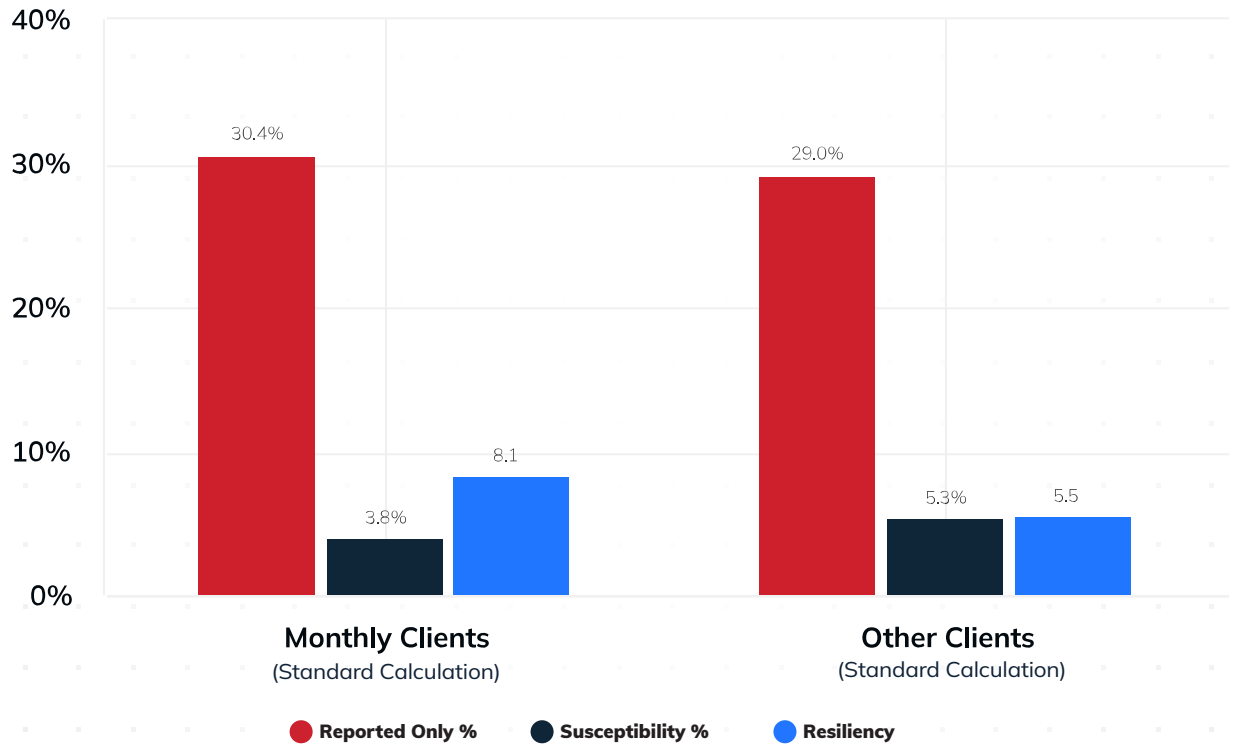

Figure 4: Comparison of clients who run monthly phishing simulation campaigns vs. those who run less frequent campaigns.

5. Offer Multi-Channel Attack Training

While email is still the #1 phishing attack vector–don't count out other communication channels–especially those targeting an individual's personal devices. In 2023 and 2024, Cofense saw a spike in QR code attacks in the workplace. Individuals were more susceptible to this threat tactic as it was not unusual for them to engage with a QR code in their daily life outside of work. As this attack method started to decline, the Cofense Phishing Defense Center (PDC) saw a rise in call-back and text phishing throughout 2024 and into 2025. When it comes to these attack methods, it is important to note that AI tools accelerate the speed of delivery and relevance of these threats. For example, threat actors use AI voice cloning/deepfake technology to impersonate trusted colleagues and AI chatbots can make interactions feel more conversational. AI can also be leveraged for automatic dialing capabilities which allows for a quick spray attack. Many industries are directly impacted by call-back phishing, yet the PDC has noticed that Healthcare is the most targeted.

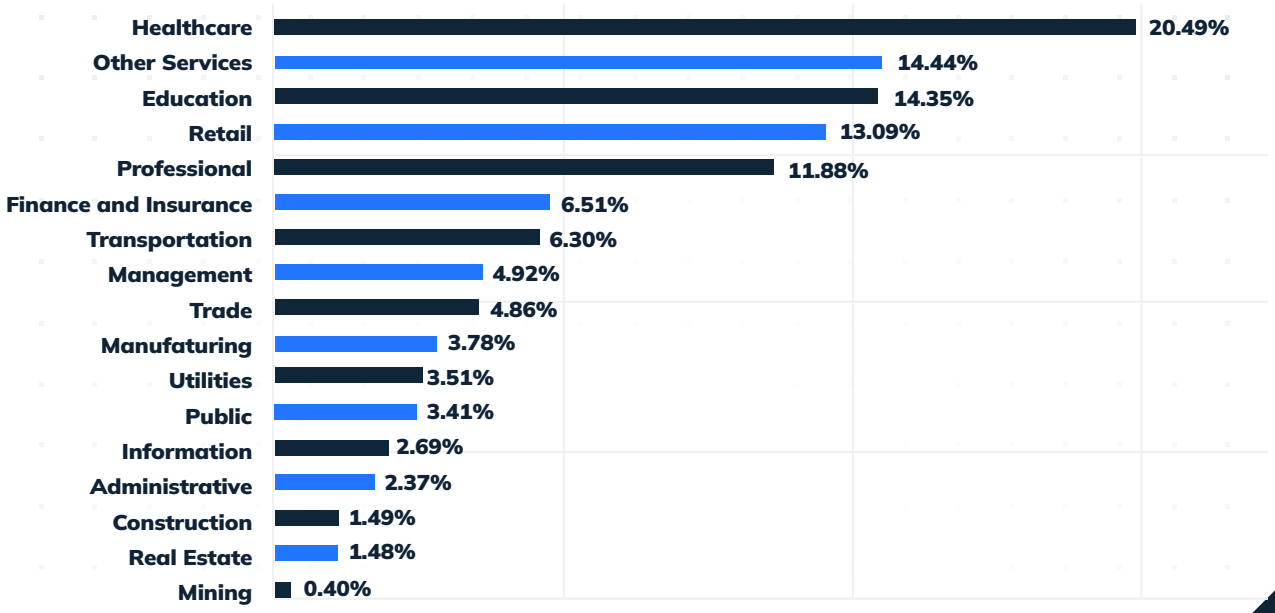

Figure 5: Cofense PDC Phone Scams as % of Total Malicious Emails

6. Employ a Multi-Layered Defense

While training prepares employees for escalating waves of phishing attacks, relying solely on awareness programs isn't enough. A multi-layered email security strategy, incorporating both awareness training and active detection/response systems, ensures maximum risk reduction.

1. **When organizations leverage the entire Cofense platform and implement both SAT and Phishing Detection and Response (PDR), our customers find:** Reporting rates increase significantly, giving incident response teams better clarity and agility when addressing potentially malicious activity.
2. **Customers using Cofense Managed PDR services reduce dwell times from days to mere minutes as professional analysts deliver rapid threat analysis and remediation.**

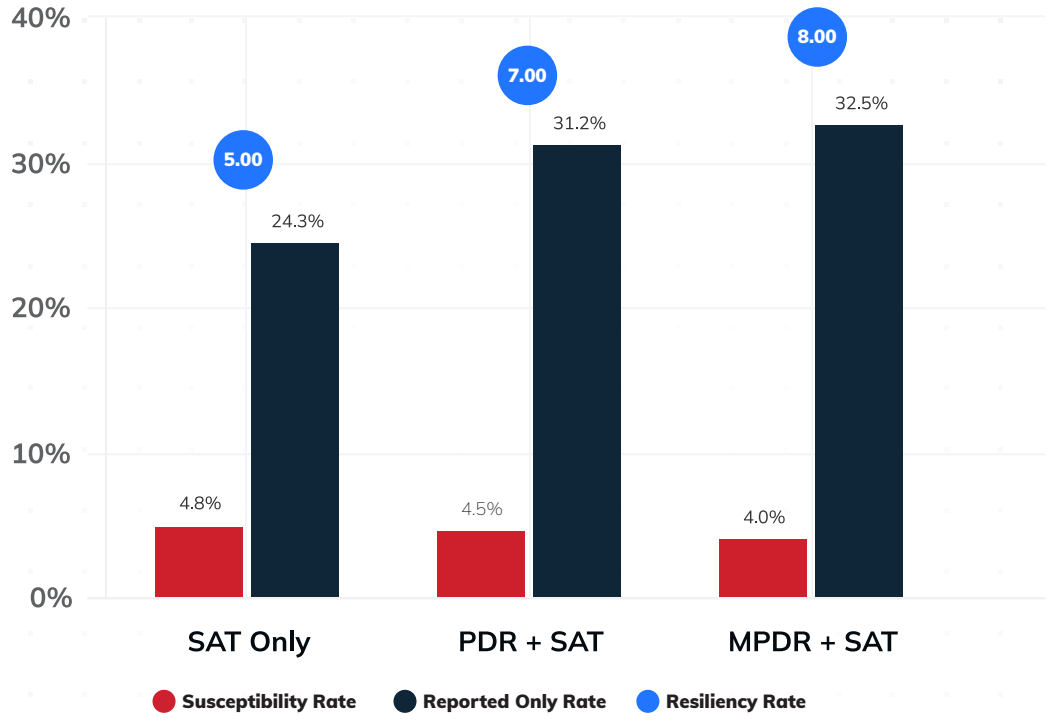

Figure 6: The effect of a multi-layered phishing defense strategy on susceptibility and resiliency.

When customers integrate phishing threat detection with proactive reporting, it creates a holistic security network capable of identifying, isolating, and neutralizing malicious activity before it spreads.

SAT Industry & Usage Comparison

We understand an important metric for many organizations is how your company compares to others within your industry vertical and how your industry compares to other industries. No surprise here, industries with more stringent regulations continue to show higher resilience. These industries usually have more guidelines, controls, and standardized processes in place.

To see where your company fits among your peers, review the chart below:

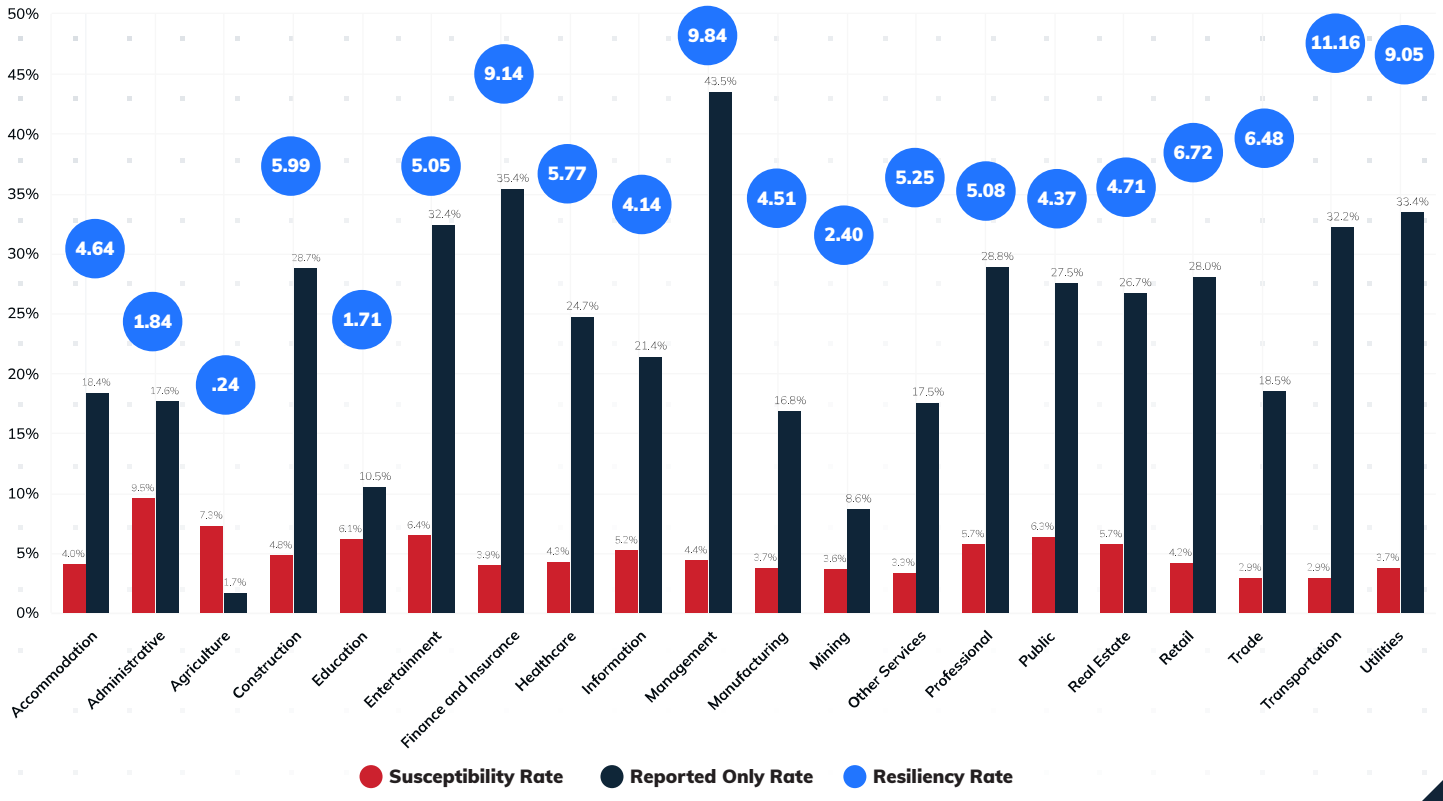

Figure 7: Comparison of susceptibility and resiliency rates by industry.

Why Companies Trust Cofense

With over one billion verified global deployments, Cofense leads SAT innovation by placing **active detection** over passive training. Our solutions go far beyond simply filtering suspected threats. Our platform teaches employees to become sharper, enables SOC teams to become faster, and empowers your workforce to become resilient—to anything the next phishing wave may bring.

Secure Your Organization's Inboxes

Don't wait until AI-powered phishing campaigns test your human firewall. Protect your organization by simulating, analyzing, and practicing using real threats. Equip your employees with what they need to recognize and report phishing today!

Interested in learning more about Cofense phishing defense solutions?
Contact us today.

Scan the QR code or visit cofense.com to learn how to catch more phish with Cofense.

PHISHME COFENSE