CEREBRA سيريبرا

SAUDI TECH

Human Awareness in The Age of AI Phishing

2026 REPORT

Table of Contents

01 Key Definitions

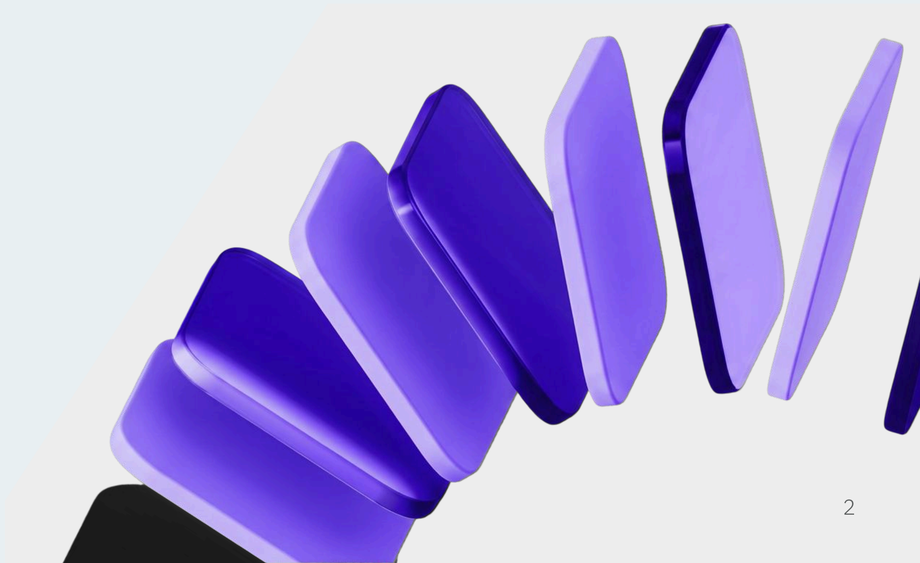
02 Executive Summary

03 Key Insights

- 3.1 Credential Submission Rate
- 3.2 Campaign Timing & Peak Activity
- 3.3 Reporting & Response Time
- 3.4 Brand, Season & Category Breakdown
- 3.5 Engagement & Active Users
- 3.6 Completion Rates & Module Progression
- 3.7 Top Topics, Course Length & Peak Activity

04 SANS Awareness Maturity Model

05 Conclusion



Key Definitions

AI-Driven Phishing	Phishing attacks that use AI to create highly convincing and personalized deceptive messages.
Why it matters in 2026 →	AI enables phishing attacks to scale, making every employee a potential target.
Click Rate	The percentage of employees who clicked on a simulated phishing link out of the total recipients.
Why it matters in 2026 →	AI-generated phishing makes attacks more convincing, increasing click rates and human risk.
Confidential Submission Rate	The percentage of users who submitted sensitive information after clicking a simulated phishing link.
Why it matters in 2026 →	Credential submission reflects the highest level of deception and potential account compromise
Reporting Time / Response Time	The time it takes for employees to report a phishing simulation to the security team after receiving it.
Why it matters in 2026 →	Faster reporting reduces the window attackers must act.
Awareness Engagement Rate	The percentage of users who actively engaged with the awareness platform by starting or completing assigned training.
Why it matters in 2026 →	Higher engagement is linked to lower phishing click rates and faster reporting.
Module Completion Rate	The percentage of assigned training modules that employees fully complete.
Why it matters in 2026 →	Incomplete training creates knowledge gaps that attackers exploit.

Executive Summary

Cybersecurity awareness is undergoing a structural shift. Generative AI has dramatically improved the quality, personalization, and scalability of phishing attacks, allowing adversaries to craft highly convincing messages with minimal effort. As a result, the distinction between real attacks and simulated ones has never been narrower, placing greater pressure on organizations to strengthen the human layer of defense.

These results indicate that while organizations are investing more heavily in awareness programs, reducing human risk remains a critical challenge in the era of AI-driven phishing.

The State of Cybersecurity Awareness — 4th Edition analyzes phishing simulation outcomes alongside employee training engagement to evaluate organizational resilience. While phishing simulation activity increased by **40%**, the click rate remains at **28%**, with AI-generated templates driving a further 2% increase. At the same time, awareness engagement rose to **85.8%**, and module completion improved from **28.2%** to **42.1%**.



The threat has gotten smarter. The question is whether your people have kept up.

Key Insights

28% Click Rate
VIA AI TEMPLATES

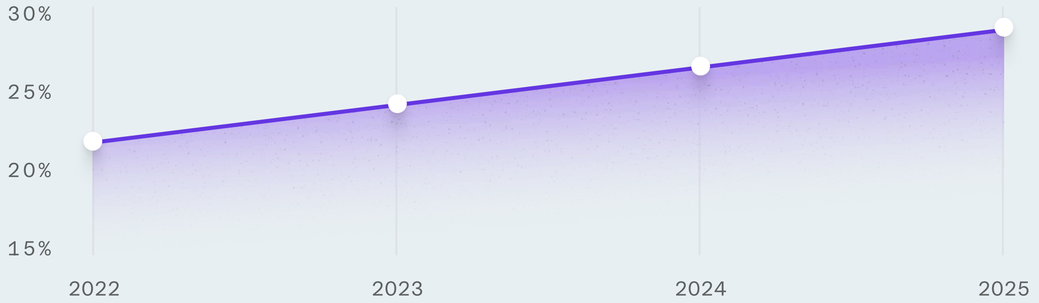
40% Simulation Activity
YEAR OVER YEAR

10+ Average Campaigns
PER ORG / YEAR

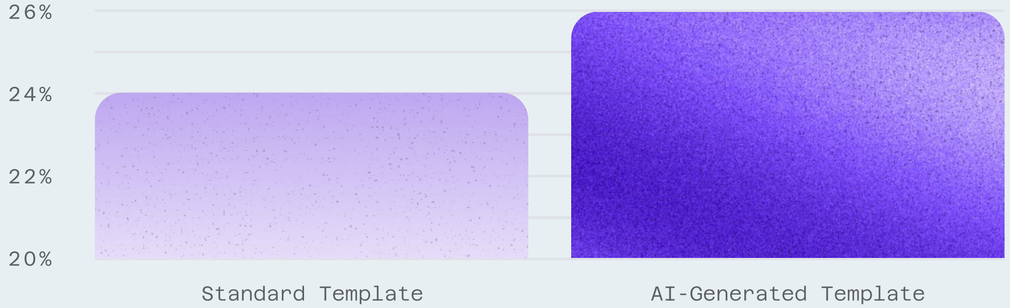
Phishing simulation activity surged by **40%** compared to the previous year, reflecting a growing consensus that regular behavioral testing is no longer optional. Organizations conduct an average of more than **10** simulation campaigns per year — a cadence that enables meaningful trend analysis and ensures employees remain alert across different scenarios. Yet despite this increased investment in testing, the overall click rate held at **28%**, indicating that simulation activity alone does not automatically translate into improved detection.

More critically, AI-generated phishing templates elevated the click rate by an additional **2%**, providing direct evidence that more convincing attack content is already degrading employee resilience at scale. Since the first edition of this report in **2022**, click rates have trended upward in correlation with AI-complexity — a trajectory that should concern every organization still relying on static, annual training.

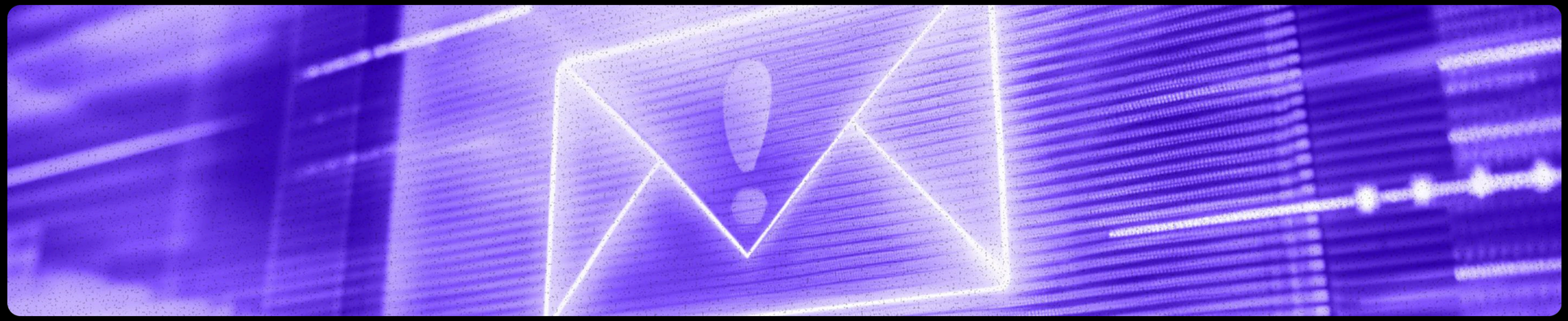
Click Rate Progression Across All Four Report Editions



AI-Generated vs. Standard Template Click Rate



1 in 4 employees clicked. AI just made that number worse. And your next simulation hasn't launched yet.



Credential Submission Rate

66% Opened the message

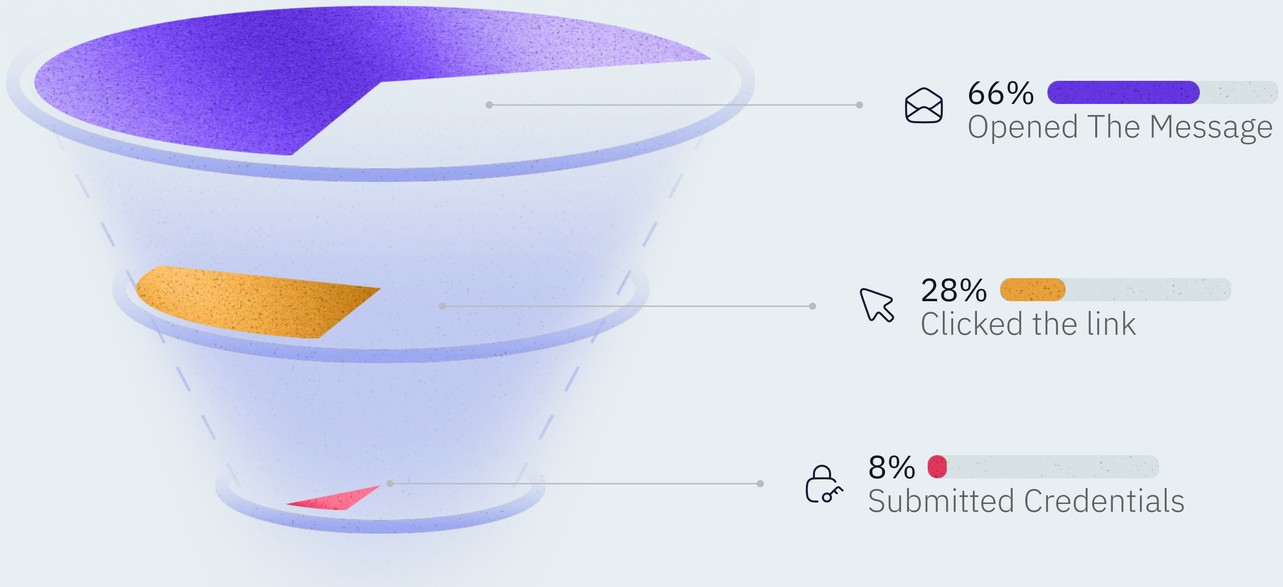
28% Clicked the link

8% Submitted credentials

OF USERS WHO CLICKED

A phishing simulation was delivered to employees, with **66%** opening the message, and a click rate of **28%** is alarming — but it is not the most dangerous number in this report. The **8%** credential submission rate reveals how far the deception ran in a subset of users: employees who not only clicked a phishing link but proceeded to enter their actual login credentials into a fraudulent page. In a real attack, this represents full account compromise — instant access to email, internal systems, or financial platforms, depending on the account targeted.

Credential harvesting remains one of the most high-value outcomes of phishing campaigns precisely because it bypasses technical defenses entirely. The **8%** figure demands specific attention to anti-credential-harvesting training: users must understand not only that phishing links are dangerous, but that the pages they lead to are designed to be convincing.

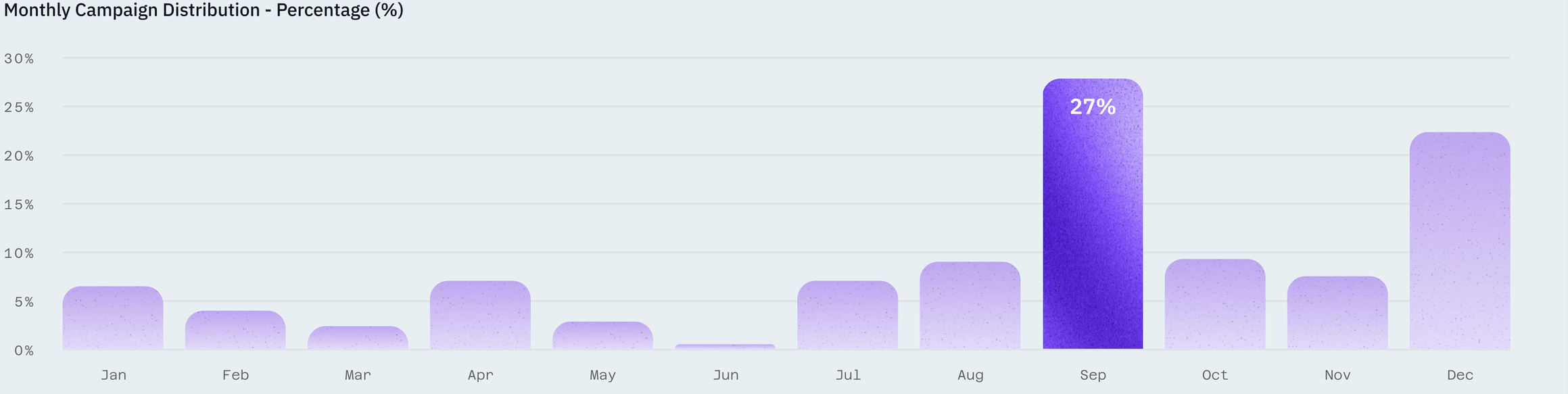


Clicking is curiosity. Submitting credentials is surrender. 8% of users crossed that line.

Campaign Timing & Peak Activity

Timing matters in phishing — both for attackers and for simulation designers. The data shows a significant concentration of campaign launches in September, which accounted for approximately **27%** of all campaigns launched across the year. This surge coincides with organizations returning from summer, meaning employees are re-engaging with full workloads, higher email volumes, and potentially diminished alertness — precisely the conditions under which threat actors operate most effectively.

Saudi National Day campaigns represented **10%** of total annual campaigns, illustrating how cultural events are weaponized as social engineering hooks that lower employees' guard through familiarity and emotional resonance. Perhaps most revealing, the majority of campaigns were launched in the **early morning hours** — a deliberate strategic choice exploiting the cognitive window in which employees are least focused, most likely to act reflexively, and least likely to apply critical scrutiny to an incoming message.



Attackers don't work bankers' hours — they work your employees' weakest ones.

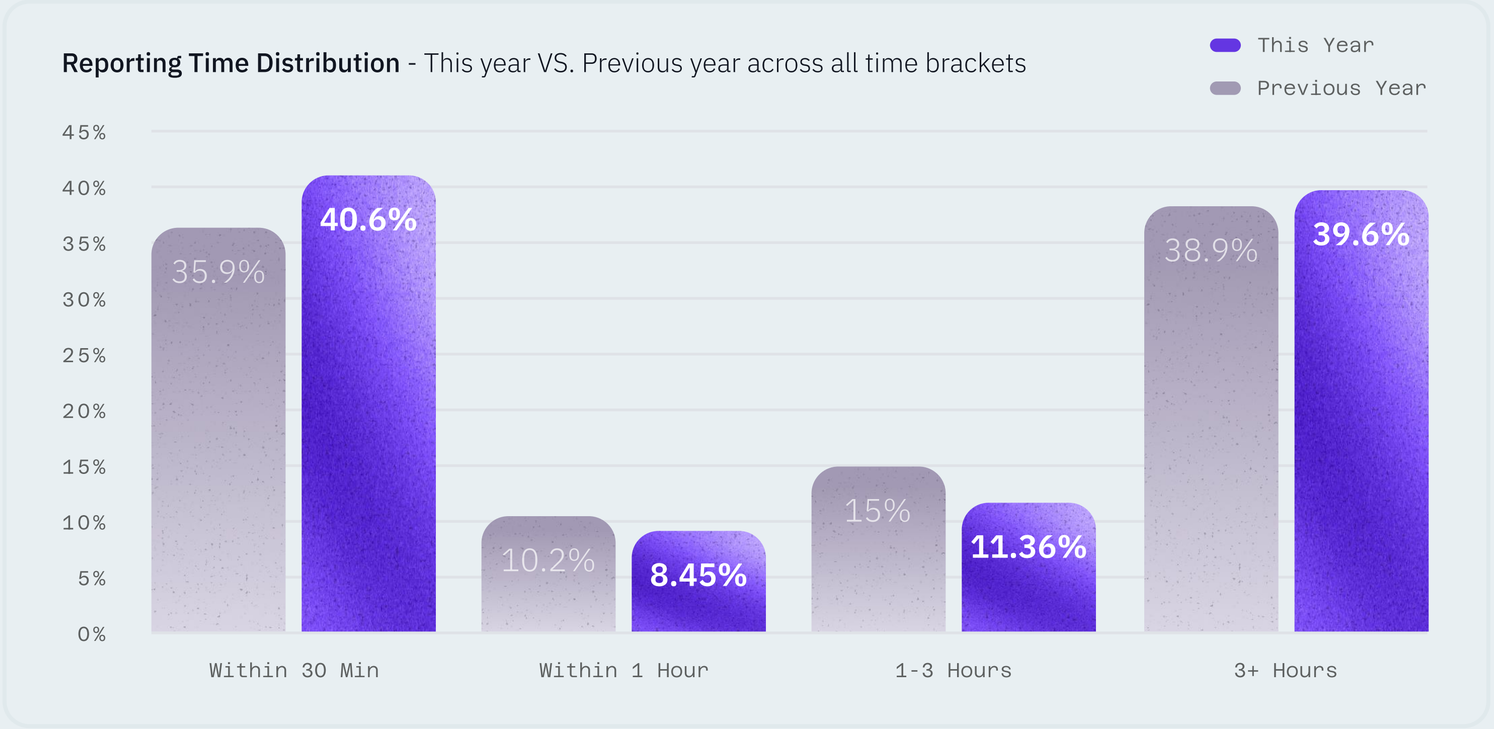


Reporting & Response Time

40.6%	8.45%	11.4%	~40%
Report within 30m	Report within 1 hour	Report within 1-3h	Report after 3h
+12.8% INCREASE	MID-RANGE DROP	-24.3% DECREASE	CONTINUED RISK WINDOW

Reporting speed is the final line of behavioral defense — and the data reveals a split picture. The proportion of employees reporting simulated phishing within **30 minutes** rose to **40.6%**, a **12.8%** improvement that reflects measurable progress in building an alert, action-oriented workforce. However, this good news coexists with a significant risk: nearly **40%** of users still reported after more than **3 hours** — a window during which a real attacker could traverse an entire network, exfiltrate data, or deploy ransomware.

The mid-range reporting window **(1–3 hours)** also contracted — down **24.3%** — suggesting that users are polarizing into two behavioral groups: rapid reporters and late reporters, with limited middle ground. This bifurcation demands a targeted intervention strategy: recognize and reinforce the early-reporting cohort while investigating the structural barriers preventing the late-reporting majority from acting promptly.



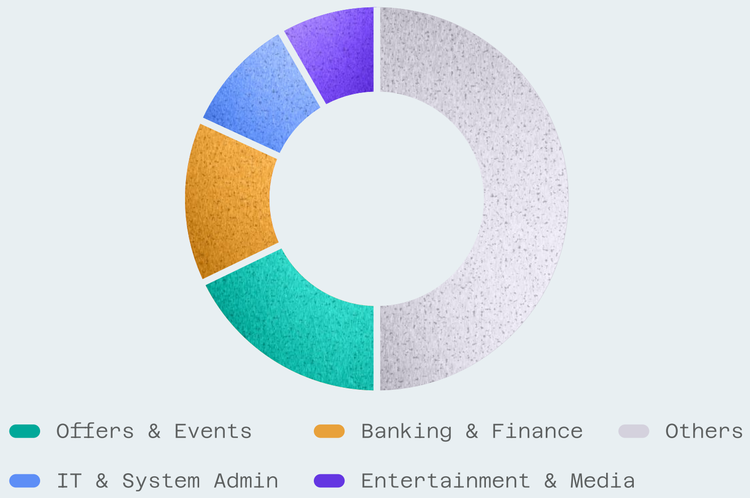
40.6% reported in 30m. 40% waited 3h or more. In a real attack, that gap is the difference between containment and crisis.

Brand, Season & Category Breakdown

The most effective phishing simulations leverage brand recognition and contextual relevance to disable critical thinking. This year's data shows that **HungerStation, AlRajhi Bank, and Microsoft** were the most frequently used brand templates — familiar brands tied to financial transactions, food ordering, and workplace productivity are trusted enough to trigger immediate action without scrutiny.

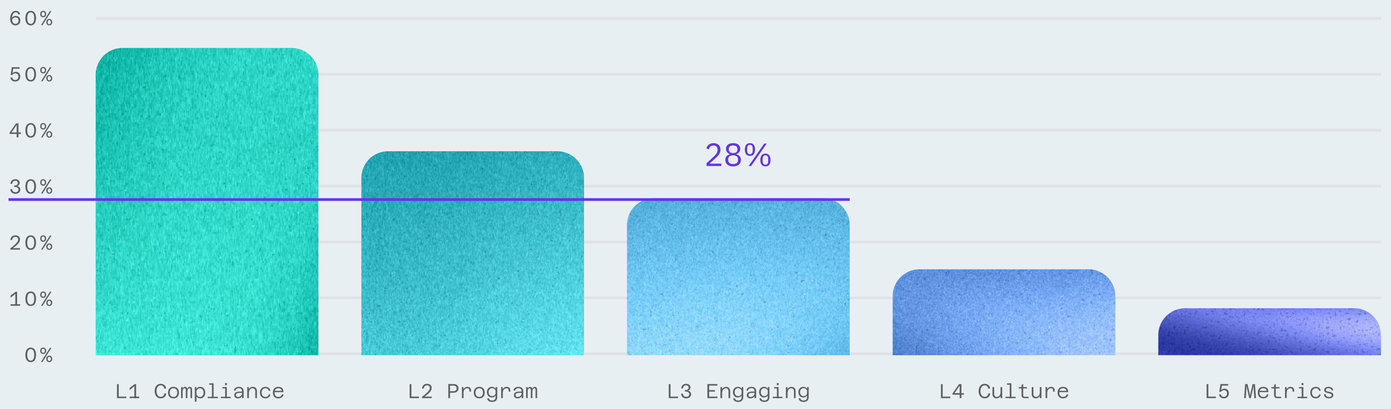
By campaign category, **Offers & Events** dominated at **20%**, and **Banking & Finance** accounted for **13%** — both categories that create urgency through monetary or reward framing. **Saudi National Day** campaigns, representing **10%** of all annual campaigns, demonstrate how national and cultural events are powerful social engineering anchors. Organizations run an average of **10+** campaigns per year, reflecting a commitment to continuous, diverse testing.

Campaign Category Breakdown



SANS Maturity Level VS. Org Click Rate

Higher maturity levels correlate with lower click rates and greater simulation frequency.



The best phishing email isn't the most suspicious-looking one — it's the one you were already expecting.

Engagement & Active Users

85.8%
Engagement Rate
UP FROM 66%

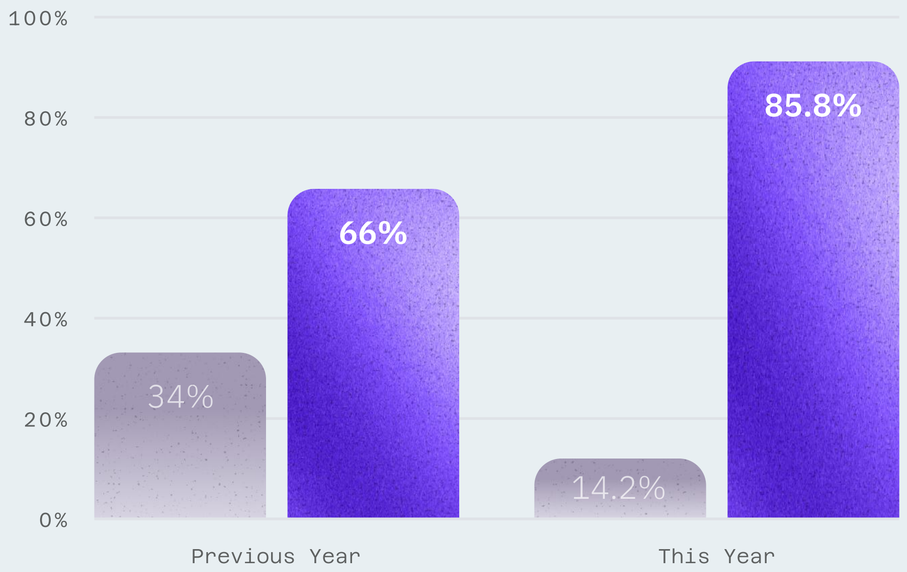
+54.8%
Active User Increase
YEAR OVER YEAR

-25.8
Inactive Users
POSITIVE TREND

The **85.8%** platform engagement rate is among the strongest signals in this year's report. Up from **66%** in the previous period, this confirms that organizations are successfully moving employees from passive recipients of security communications to active participants in their own protection. Active users grew by **54.8%**, and inactive users fell by **25.8%**.

This turnaround reflects deliberate decisions by leadership to communicate the importance of participation, integrate training into onboarding workflows, and use simulation outcomes to trigger targeted learning. The remaining **~14%** of disengaged users represent a focused intervention opportunity — and a disproportionate share of organizational risk

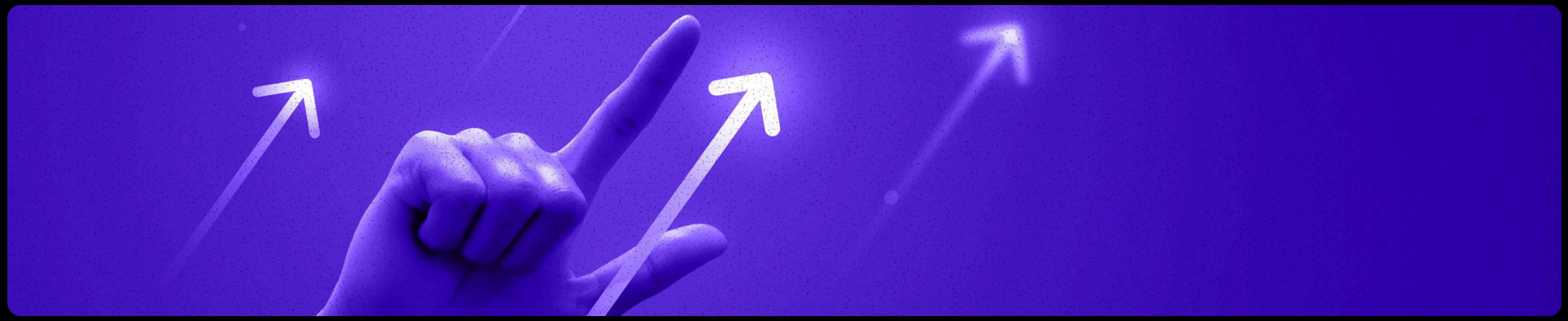
Engagement Rate - active vs. inactive user shift



PREVIOUS YEAR
Active 66%
Inactive 34%

THIS YEAR
Active 85.8%
Inactive 14.2%

Almost 86% engaged. The 14% who didn't are not just unprotected — they are the unlocked door.



Completion Rates & Module Progression

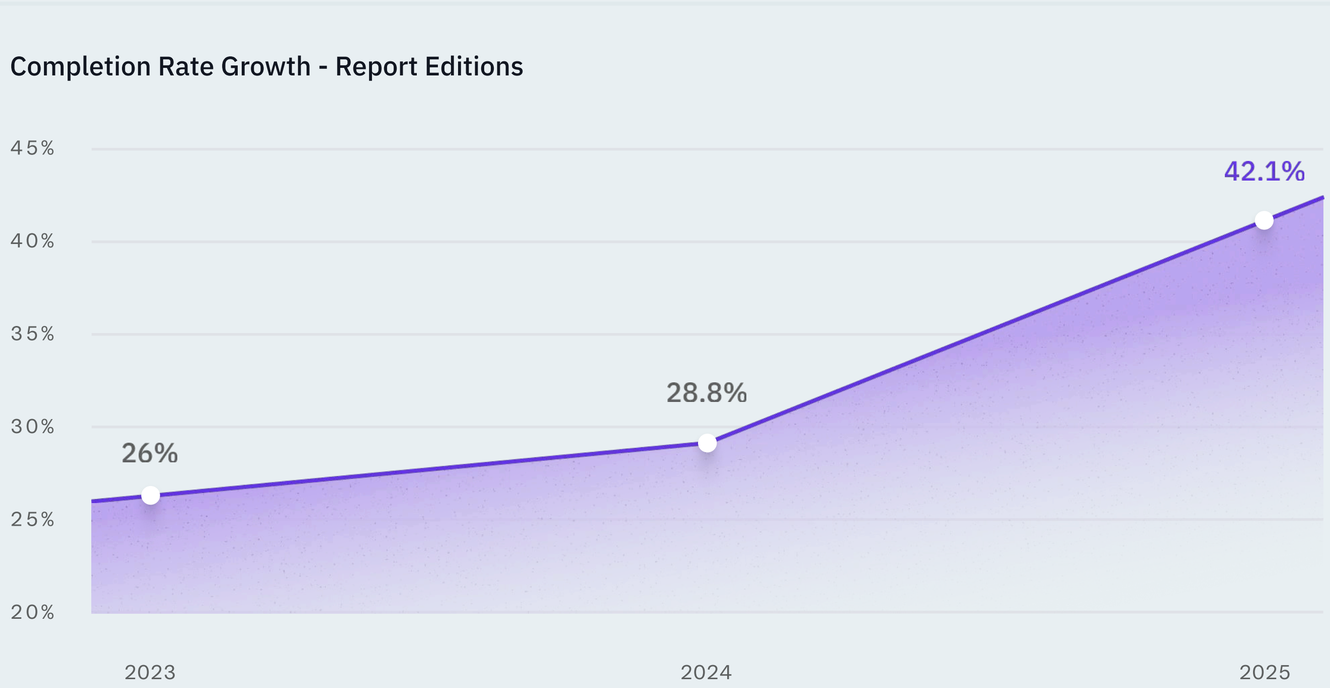
42.1% Completion Rate
UP FROM 28.2%

44.1% Users Completing Modules
YEAR OVER YEAR

5 Average Modules
PER USER

The jump from **28.2%** to **42.1%** completion rate represents the single largest year-over-year improvement in this report's three-year history — a **49.3%** relative increase that signals a structural change in how organizations are delivering and employees are consuming training. The number of users completing modules rose by **44.1%**, total modules completed increased by **12.9%**, and users actively progressing through content grew by **11.9%**.

The average user completed **5** modules a year — a figure that rises significantly in organizations with higher simulation frequency, confirming the behavioral link between testing and learning. This progress, while significant, also illuminates a remaining gap: a **42.1%** completion rate means that more than half of assigned modules are still not being finished — a gap that must close if organizations expect to reach Level 4 maturity on the SANS model.



A 49.3% improvement in completion. But an unfinished training module is an unlearned defense.

Top Topics, Course Length & Peak Activity

The topics employees complete most reveal where organizations perceive their greatest exposure. **Social Engineering, Phishing, and Malware** recorded the strongest completion rates — a clear signal that both organizations and employees understand human behavior as the primary attack surface. The courses most frequently assigned — **Phishing, Password Security, Social Media Security, Email Security, and Secure Web Browsing** — closely mirror actual attack vectors observed in the threat landscape.

A critical content design finding emerges courses with **5–7 minute** durations consistently outperformed longer modules in completion rates, confirming that concise, focused content respects employees' time and sustains engagement far better than extensive modules.

August 2025 recorded the highest month for module completions — an inflection point following the summer holiday period that organizations can deliberately exploit by scheduling high-priority training for the September return window.

5 minutes of focused training outperforms 50 minutes of ignored content. Brevity is not a compromise — it is a strategy.

SANS Awareness Maturity Model

The SANS Security Awareness Maturity Model provides a structured lens for interpreting this report's data — not as a collection of metrics, but as evidence of where organizations sit on a defined progression toward genuine security culture. The findings below map each maturity level to specific data signals from this year's report, with targeted recommendations for advancing to the next rung.

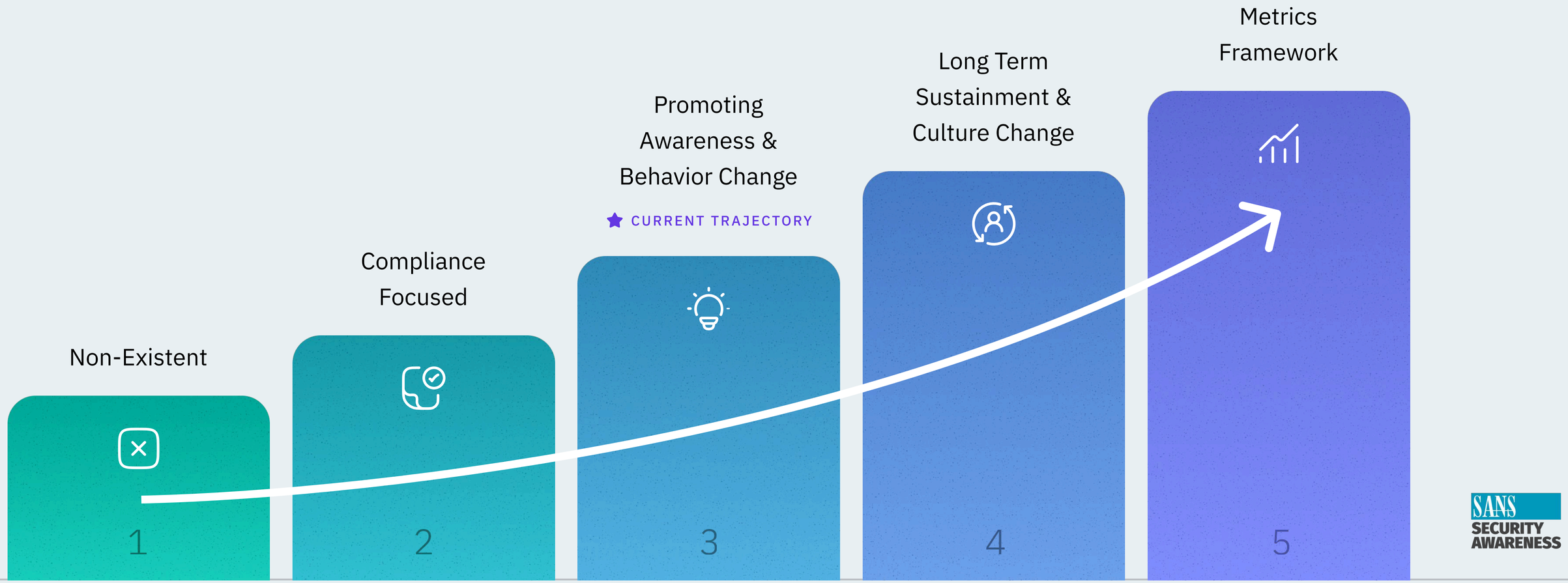
1	**Compliance focused** Training is annual and compliance-driven, with no phishing simulations. Awareness is treated as an HR requirement, not a security function. **Next step** → Introduce regular phishing simulations and shift ownership to Security.	**~65%+ click rate expected.** No simulation data.
2	**Awareness & Training Program Exists** Awareness programs and simulations are in place, but execution is inconsistent. Content is generic, engagement varies, and results are not driving improvements. **Next step** → Increase simulation frequency to 10+ campaigns/year and personalize content by role.	**28–40% click rate.** **66% engagement** (prior year baseline).
3	**Engaging Awareness Program** ★ CURRENT TRAJECTORY Training is frequent, relevant, and driving behavior changes. Engagement and completion are improving, with active phishing reporting. This is where most organizations in this report are **currently** heading. **Next step** → Formalize metrics, track performance by role, and link awareness outcomes to risk.	**28% click rate.** **85.8% engagement.** **42.1% completion.**

SANS Awareness Maturity Model

The SANS Security Awareness Maturity Model provides a structured lens for interpreting this report's data — not as a collection of metrics, but as evidence of where organizations sit on a defined progression toward genuine security culture. The findings below map each maturity level to specific data signals from this year's report, with targeted recommendations for advancing to the next rung.

4	**Long-Term Sustainment & Culture Change** Awareness is embedded in culture, with strong leadership support and continuous improvement. Reporting is encouraged and click rates are below 15%. **Next step** → Expand security champions, integrate with SOC, and report metrics at the board level.	**<15% click rate. Culture-level indicators.**
5	**Metrics Framework (Advanced)** Awareness is a measurable security control, with risk tracked across users and departments. Data is integrated to enable predictive risk insights and demonstrate ROI. **Next step** → Expand AI-driven simulations and adopt adaptive, behavior-based training.	**<8% click rate. Predictive risk scoring.**

Security Awareness Maturity Model



Every step up the maturity ladder isn't just a program upgrade — it is a measurable, auditable reduction in organizational risk that no firewall can replicate.

Conclusion

Phishing simulation activity surged by 40% compared to the previous year, reflecting a growing consensus that regular behavioral testing is no longer optional. Organizations conduct an average of more than 10 simulation campaigns per year — a cadence that enables meaningful trend analysis and ensures employees remain alert across different scenarios. Yet despite this increased investment in testing, the overall click rate held at 28%, indicating that simulation activity alone does not automatically translate into improved detection.

More critically, AI-generated phishing templates elevated the click rate by an additional 2%, providing direct evidence that more convincing attack content is already degrading employee resilience at scale. Since the first edition of this report in 2022, click rates have trended upward in correlation with AI-complexity — a trajectory that should concern every organization still relying on static, annual training.

The AI that writes tomorrow's phishing email doesn't care about your firewall

Train the one thing it cannot automate: human judgment



READY TO ELEVATE CYBERSECURITY AWARENESS IN YOUR ORGANIZATION?

Discover how Infoshield can be tailored to your environment.

If this report resonates with your challenges or has inspired new thinking about awareness and culture, we would love to hear from you.

At Cerebra, we are committed to helping organizations turn awareness into resilience.

Contact us at **hala@cerebra.sa** to explore how we can help you strengthen your human firewall, design impactful programs, and embed awareness where it matters most in daily behavior. to explore how we can help you strengthen your human firewall, design impactful programs, and embed awareness where it matters most in daily behavior.



GET IN TOUCH

Hala@cerebra.sa



OUR WEBSITE

Cerebra.sa