

"Understanding the Efficacy of Phishing Training in Practice," published at IEEE S&P 2025, is a fantastic bit of security science. It answers a question of great practical relevance: does phishing training actually work? The authors ran an eight-month randomized controlled study across nearly 20,000 employees at a large healthcare organization, with explicit control groups and multiple training conditions — not a small lab study or observational study. So the result is hard to argue with: annual cybersecurity awareness training shows no meaningful correlation with phishing resistance, and even embedded training — the kind where employees who click get redirected to a lesson — produces only about a 1.7% absolute reduction in failure rates. Most employees don't engage with the training material at all; more than half close it within 10 seconds.

What makes this work particularly valuable is how actionable it is. Organizations across every sector spend real money and employee time on annual security training as a compliance exercise, and this paper gives them solid empirical grounds to stop and ask whether that investment is actually helping. The one genuine signal in the data — that interactive training completed in full correlates with a 19% reduction in future failures — even points toward what might work better. The paper is also well written and honest about its limitations, which makes it more credible, not less. For the NSA's competition, this is exactly the kind of work that deserves recognition: rigorous science on a practical problem, with findings that should actually change how organizations behave.