

How to Build Real-World Phishing Resilience

Measurable, human-crafted social engineering testing that gave an AI governance platform an evidence-based read on employee resilience.

INDUSTRY

AI Governance Platform

COMPLIANCE

SOC 2 Type I → Type II

SERVICE ENGAGED

Social Engineering

Goodweek is an AI management and governance platform that gives businesses a single secure place to deploy and control AI models such as ChatGPT, Claude, and Gemini across their teams. Sold through managed service providers to small and midsize businesses, the platform is built on a promise of secure, governed AI adoption, and every MSP that resells it puts its own reputation on the line.

HOW PHISHING SIMULATION MEASURED THE GAP

01

Pretexts Built With the COO

Software Secured built the campaigns directly with Goodweek's COO, who proposed pretext angles and reviewed each design before launch.

02

Two Sequenced Campaigns

An internal-survey lure set the baseline; a security-policy lure run days later tested whether employees had learned to question it.

03

An Evidence-Based Baseline

Engagement dropped, and no credentials were entered on the second test. It was a documented, measurable read on real-world resilience.

//

My objective is to genuinely assess and progressively strengthen our employees' real-world resilience against modern social engineering attacks. I wanted a program that reflects that reality, not one that creates a false sense of security.

Valérie Laffite — Chief Operating Officer, Goodweek

In under a week, Goodweek went from an untested workforce to one actively closing the gap between two campaigns — with security now an operational discipline that evolves alongside the product, its people and the threats they face.