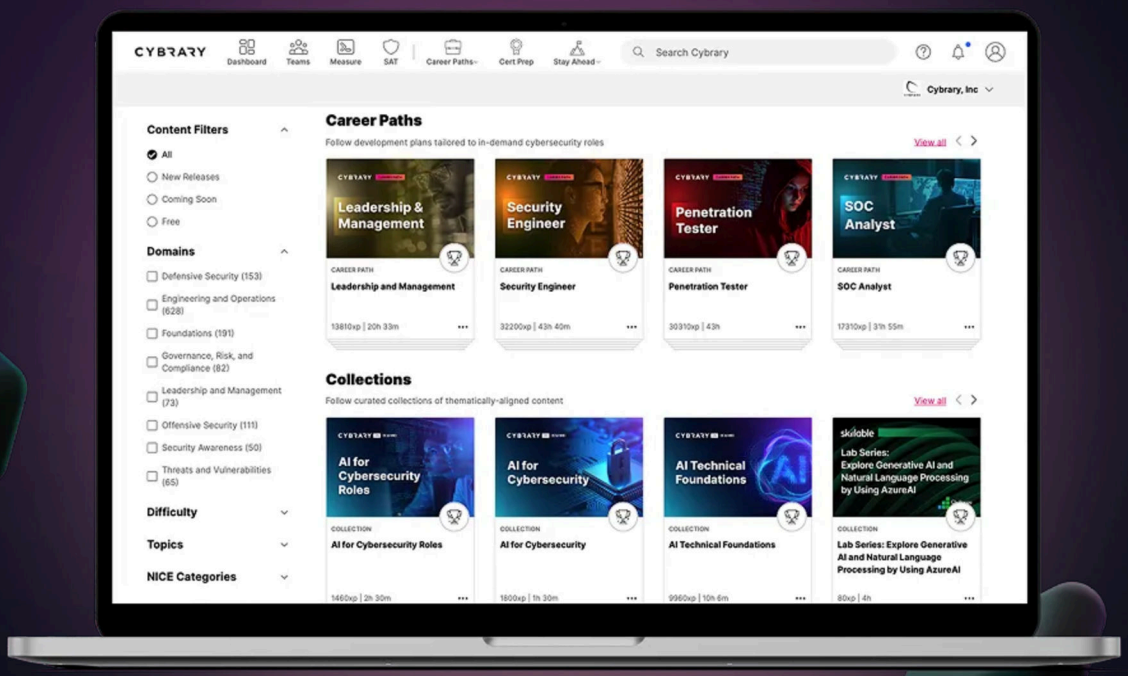
CYBRARY



Customer Story

Why Cybrary Chose CanIPhish for Next-Generation Human Security

caniphish

www.caniphish.com

ABOUT CYBRARY

Cybrary is one of the world's leading cybersecurity training platforms, trusted by millions of learners and used by the vast majority of Fortune 1000 organizations.

As the threat landscape accelerates, Cybrary continues to expand beyond awareness training into real-world skill development.

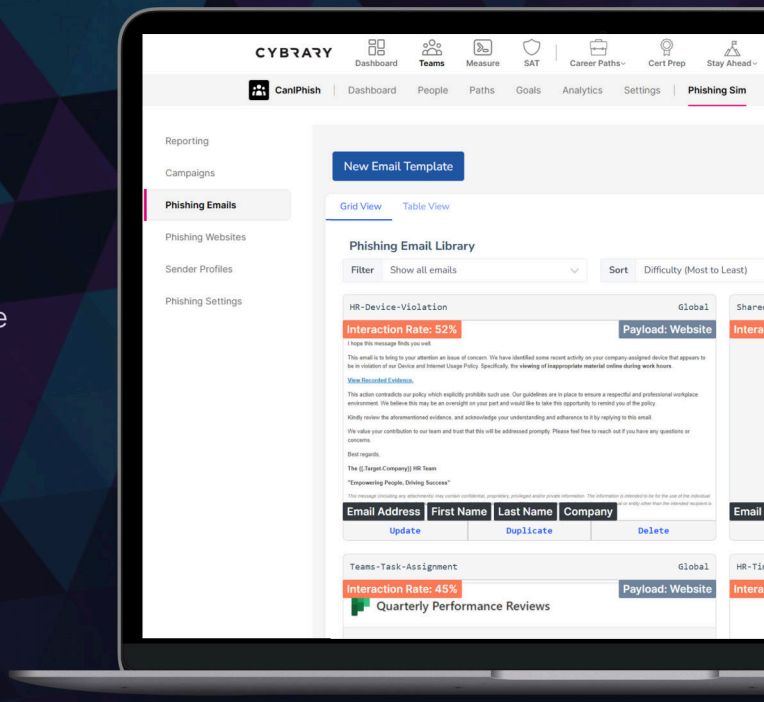
With phishing still responsible for most security incidents, and AI making attacks more convincing and scalable than ever, Cybrary recognized the need for something beyond static content.

THE CHALLENGE

Phishing has changed faster than traditional training, and the old approach to phishing awareness training is no longer enough.

Attackers now use AI to launch highly adaptive social engineering campaigns at scale. Employees aren't just clicking links, they're being drawn into realistic conversations designed to build trust over time.

Cybrary's customers needed more than compliance training. They needed practice against modern threats.



THE PARTNERSHIP

Cybrary chose CanIPhish to bring the industry's first AI-powered phishing simulator directly into its platform.

This integration transforms phishing defense from passive learning into active skill development, allowing organizations to train employees through realistic simulations that mirror how today's attackers actually operate.

For Cybrary, this partnership represents a major step forward in delivering next-generation human security at enterprise scale.

By embedding CanIPhish directly into Cybrary, customers can deliver phishing readiness as part of a unified training experience, without adding complexity or separate tools.

As Cybrary COO Nick Misner explains:
"With CanIPhish embedded in Cybrary, our customers don't just train. They practice."

caniphish

THE IMPACT

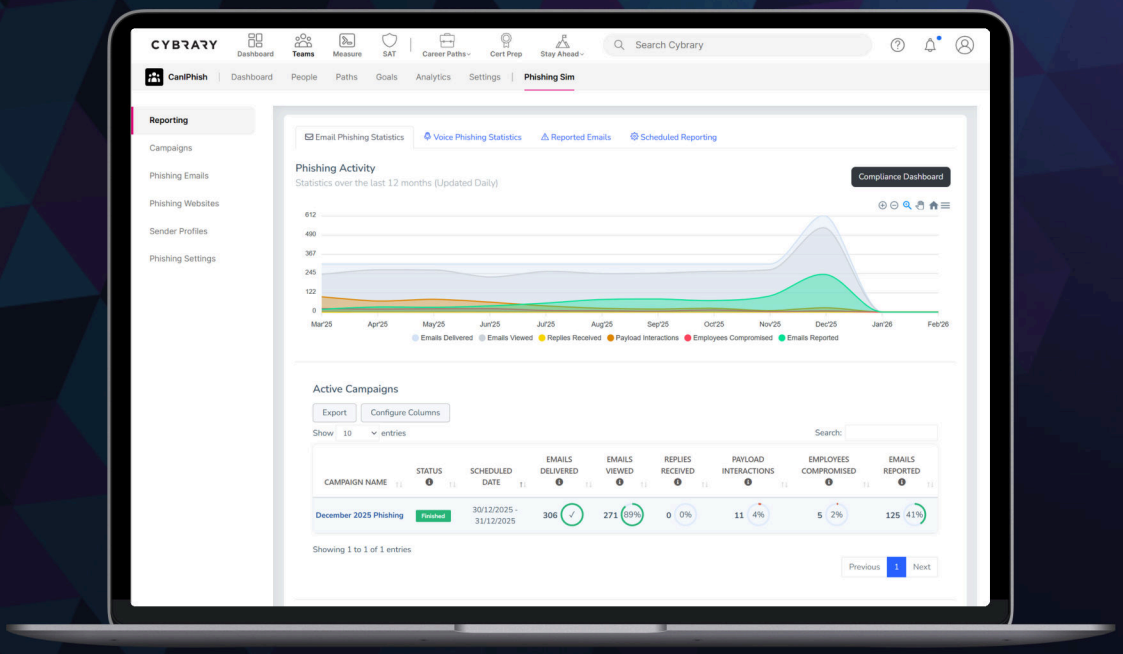
By integrating CanIPhish, Cybrary is giving enterprises a way to build measurable human resilience against the most rapidly evolving attack vector in cybersecurity.

Instead of generic inbox tests, employees now experience real-time conversational phishing, dynamic scenarios, and simulations that adapt as quickly as attackers do.

This creates something traditional training cannot deliver: Practical instinct under pressure.

Security teams gain clearer visibility into human risk, and employees build readiness through practice, not theory.

The result is a shift from awareness training to real-world readiness.



A SHARED VISION FOR CYBER RESILIENCE

CanIPhish CEO Sebastian Salla summarized the partnership clearly:

“Static training cannot hope to keep up. Employees need realistic practice that evolves with the threat landscape.”

Together, Cybrary and CanIPhish are leading the way toward a new category of integrated human risk platforms, combining expert-led learning with AI-driven phishing simulations.

THE BOTTOM LINE

When an industry leader like Cybrary chooses to innovate with CanIPhish, it signals something important: The future of cybersecurity training is not passive.

It is practical, adaptive, and built for the AI threat era.

caniphish