

A benefits fund office avoided a potentially costly cybersecurity incident when employees identified and reported a sophisticated phishing email before taking any action. Working with Segal, the organization built a phishing awareness program that turned its people into an early warning system, resulting in zero compromised accounts, zero exposed credentials and rapid threat containment.

Why trusted Microsoft infrastructure made this phishing attempt harder to detect

Most phishing emails reveal themselves through obvious warning signs. This attack was different.

A multiemployer benefits fund office received a highly convincing phishing email generated and delivered through legitimate Microsoft infrastructure, rather than merely disguised to look like a Microsoft message. That trusted delivery path made the message appear legitimate and harder to identify as a threat.

For an organization responsible for administering pension, health and welfare benefits, the stakes were significant. Employees routinely handle sensitive participant and financial information, and a single click could have exposed credentials or triggered a larger security incident.

As phishing attacks continue to evolve, the fund office needed more than technology alone. It needed employees who could recognize suspicious activity and know how to respond.

How a phishing awareness program prepared employees for a real-world attack

Long before the suspicious email arrived, Segal's Administration and Technology Consulting team helped the fund office strengthen its cybersecurity readiness through a practical, behavior-focused phishing awareness program.

Segal implemented quarterly phishing simulations designed to mirror the tactics employees were most likely to encounter. These exercises were paired with targeted awareness training, remediation education and clear escalation procedures that reinforced a simple expectation: if something doesn't look right, report it immediately.

The approach focused on creating habits rather than checking a training box. Through repeated exposure to realistic scenarios, employees built the muscle memory needed to recognize and

respond to emerging threats, while leadership reporting and ongoing program reviews supported continuous improvement.

How trained employees stopped a sophisticated phishing attempt

The true test of the program came when the phishing email landed in employee inboxes.

Multiple employees independently recognized that something was wrong. Rather than clicking links, opening attachments or providing credentials, they reported the message to IT immediately, allowing IT to investigate and contain the threat quickly.

The results were clear: no links were clicked, no credentials were exposed and no systems were compromised. The incident demonstrated the value of a trained workforce capable of identifying and escalating suspicious activity before damage could occur.

What could have become a damaging cybersecurity incident instead demonstrated the fund office's preparedness. By combining realistic phishing simulations, awareness training and remediation education, Segal helped transform human risk into human resilience while reinforcing a critical lesson: informed employees are often the first line of defense against evolving phishing threats.

Contact:

[Michael Stoyanovich](#)

VP, Senior Consultant

Segal's consulting services include:			
Administration & Technology Consulting	Compensation & Career Strategies	Financial Well-Being Health Benefits Consulting	Organizational Strategy and Transformation
Artificial Intelligence	Compliance Consulting	Insurance Brokerage	Property & Casualty Insurance
Benefit Audits	HR & Benefits Communications	Investment Solutions	Retirement Consulting