Corporate Phishing Attack Stopped Cold: IT Security That Just Works

OVERVIEW

In the world of high-stakes insurance and complex merger-and-acquisition deals, one wrong click can cause chaos. This national insurance provider—serving some of the largest M&A deals in the country—faced just such a moment when an employee fell for a convincing phishing scam. But thanks to proactive protections built into their IT environment, the attack failed before it ever started. This is the story of how smart security planning protected a $500M firm from disaster.

Introduction

Industry

This client is a Southeast-headquartered insurance group with national reach, known for insuring high-value corporate transactions and M&A activity. Their team of 700+ users operates across multiple U.S. offices, coordinating sensitive negotiations and managing vast amounts of confidential information daily. As their business expanded, so did the need for an IT foundation that could scale securely—with protections that didn't rely solely on user behavior. With the volume and complexity of their work, leadership knew it was a matter of when—not if—a phishing attempt would slip through. Their goal was simple: stop it from going any further.

Goals

1 OBJECTIVES

- Protect sensitive client and M&A deal data across a national user base
- Prevent unauthorized access—even in the event of credential theft
- Maintain secure, uninterrupted access to Microsoft 365 and core systems

2 BUSINESS PRIORITIES

- Enable growth without increasing exposure to cybersecurity threats
- Keep operations running smoothly, even when users make mistakes
- Adopt cloud-first, scalable IT strategies that work organization-wide

3 LEADERSHIP OPPORTUNITIES

- Demonstrate proactive risk management to clients and stakeholders
- Build organizational confidence in IT systems and leadership decisions
- Position the company as a forward-thinking, security-conscious firm

Problem

EMAIL WAS A GROWING RISK VECTOR

As their business scaled, email volume skyrocketed. Negotiations, contracts, data requests—everything moved through Microsoft 365. That made inboxes a prime target for phishing attempts. The volume alone made it impossible to guarantee that every user would spot every threat.

MISTAKES WERE INEVITABLE

Even the best-trained teams can slip up. This wasn't a matter of if someone would click on the wrong link—it was about what would happen when they did. A single compromised credential could expose sensitive deal information or give an attacker access to systems with company-wide impact.

LEGACY PROTECTIONS WEREN'T BUILT FOR THIS

Traditional login security—usernames, passwords, and even basic MFA—couldn't provide the guarantees the leadership team needed. They had too many devices, too many users, and too much on the line to hope for the best. They needed controls that would stop an attack even when a user made a mistake.

Solution

Stringfellow took a proactive approach from day one. As part of our onboarding, we implemented a secure access model that prioritized conditional access across the organization. This meant that logins were no longer just about having the right password—they were also about using the right device, in the right place, at the right time. If someone tried to log in from a device not issued or approved by the company, access would be blocked automatically—no support tickets, no alerts, no escalation needed. The protections worked in the background, giving leadership peace of mind and users a seamless experience.

This wasn't a custom fix or a special project. This is how we do business with every client. Security isn't a checkbox—it's a built-in part of the Stringfellow Playbook.

Results

When the phishing email arrived, the user didn't realize anything was wrong. The Microsoft login screen looked real. They entered their credentials and submitted the form. Within minutes, an attacker halfway across the world had their username and password—and tried to use them.

But they were blocked.

Because the login came from an unapproved device in an unknown location, the system didn't allow access. The attacker never got in. The user didn't lose any data. The IT team didn't scramble to clean anything up. There was no breach, no notification to legal, no board-level emergency meeting. It was a total non-event—because the right protections were already in place.

Conclusion

Security shouldn't rely on every employee making perfect decisions every day. This story proves that the right IT strategy doesn't just respond to threats—it prevents them entirely. By building smart protections into the way their business operates, this firm avoided what could have been a catastrophic data breach with zero disruption to their business.

That's what success looks like when you work with Stringfellow.

Stringfellow Technology
Group 214 Centerview Drive
Suite 340
Brentwood, TN 37027
1.866.883.6010