

Shelter Insurance® Prevents Fraudulent Email with Proofpoint

People-Centric Email Security Solution Halts Email Attacks, Domain-Spoofing



THE CHALLENGE

- Defend employees and agents from phishing and malware attacks
- Secure the company's brand from domain-spoofing
- Increase employee awareness of email-based scams

THE SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection
- Proofpoint Threat Response
- Proofpoint Email Fraud Defense
- Proofpoint Security Awareness Training

THE RESULTS

- Blocked virtually all malware, phishing and impostor attacks
- Protected Shelter Insurance® brand by halting domain-spoofing
- Improved employee awareness of risk and variety of attacks

The Company

Founded as a mutual insurance company in 1946 to provide affordable auto insurance to Missourians, Shelter Insurance® has grown into a full-service group of insurance companies. Shelter Insurance® supports more than two million policies in 21 states through a network of nearly 4,000 employees and agents. The company's surplus exceeded \$2 billion in 2019. The financial ability of Shelter Insurance® and long-standing reputation of providing excellent customer service have kept it growing steadily over the years. It's now one of the top 50 property and casualty insurance groups in the U.S.

The Challenge

Building a secure email infrastructure for trustworthy communications

Like many fast-growing regional companies, Shelter Insurance® was unaware that it had become a significant target for email-based attacks. These attacks were focused on business email compromise (BEC) and email account compromise (EAC). Given the explosion of phishing attacks nationwide, the Shelter Insurance® Information Security team decided to evaluate the overall security of their existing email solution. That solution was a mix of Microsoft Office 365, Lotus Notes, and Watchdog for scanning potentially dangerous attachments.

When Senior Information Security Analyst Scot Lymer joined the Shelter Insurance® Information Security team, the CIO tasked him with determining the scope of any potential issues. He was also asked to recommend possible solutions. Lymer had worked with Proofpoint at previous companies and knew the benefits Proofpoint could provide. But he had no idea of the scope of the ongoing attacks against Shelter Insurance®. After evaluating several vendors, the security team decided to hold a proof-of-concept (POC) to compare their existing solution with Proofpoint. The results, said Lymer, were "eye-opening."

Explained Lymer, "I expected Proofpoint to catch some amount of fraudulent email that was sneaking past our existing system, but I was shocked to see the sheer volume of phishing attacks. We were getting attacked far more than I expected—and the amount of bulk email and spam that Proofpoint blocked was staggering."

“Proofpoint not only blocked all of the email-based attacks, bulk mail, and spam coming to our employees and agents; it also stopped criminals from hijacking our company name. That kind of security—protecting our brand—is priceless.”

Senior Information Security Analyst Scot Lymer, Shelter Insurance®

In addition to uncovering the scope of the phishing problem, the team discovered another significant risk after turning on Domain-Based Message Authentication Reporting and Conformance (DMARC). Lymer admitted even he was shocked. “We found fraudulent messages sent from more than 100 countries using our domain name. This amount of domain fraud shocked everyone—the marketing team in particular. The potential harm to our brand was enormous.”

Given the value of the Shelter Insurance® brand, when the executive team heard the results of the trial, email security became an immediate priority for the entire company. The CIO gave the IT team the green light to move forward with Proofpoint as quickly as possible. And he gave the directive to stop 100% of both the email attacks and the fraudulent use of the Shelter Insurance® domain name.

The Solution

Creating multiple layers of intelligent protection to achieve full protection

Shelter Insurance® founded its solution on Proofpoint and its unique people-centric approach to security. With Proofpoint Email Protection and Email Fraud Defense in place, the Shelter Insurance® team now felt secure from impostor, malware, ransomware and phishing attacks. Using Targeted Attack Protection (TAP) and Threat Response Auto Pull (TRAP), the security team not stopped the barrage of phishing emails. And they dramatically reduced the time it takes to identify and address even the most sophisticated attacks. These intelligent tools identify malicious content and senders. And they reject or quarantine questionable messages for further analysis, even after delivery. If, upon analysis, a message is identified as malicious, TRAP follows that message and scrubs dangerous content from every mailbox. These features established critical layers of protection around the organization’s email system.

“We occasionally let questionable emails through that require further investigation, because we don’t want to block legitimate email,” Lymer explained. “What used to take two to three days to investigate now takes less than an hour. If we find malicious messages, TRAP removes them from every recipient’s mailbox. TRAP even follows distribution lists.”

The team next turned to halt illegal use of their valuable domain names. The use of fraudulent domains has become increasingly common, particularly internationally. Organized criminals use display-name spoofing, domain spoofing, and lookalike domains to “trick” the receiver of a message into believing a message is coming from a known and trusted source. DMARC establishes end-to-end email authenticity by keeping a list of approved users, credentials, and valid domains at each endpoint. To achieve this, DMARC requires both the sending and receiving email systems to implement the feature. Once all of the Shelter Insurance® offices and agents installed DMARC, the team had complete visibility into the details of domain-based fraud on a global level. It could then stop domain-based attacks aimed at employees, agents, and business partners.

To implement DMARC across its base of some 7,000 users, the five-person Shelter Insurance® team turned to Proofpoint Professional Services. “Implementing DMARC can be a heavy lift,” said Lymer. “With the number of offices and agents we have at Shelter Insurance®, putting DMARC in place took time. Proofpoint Professional Services helped us out, bearing the bulk of the weight in implementing a major rollout.”

The final piece of the puzzle was Proofpoint Security Awareness Training for the company’s employees and agents. If even one malicious email gets through, it can expose the company to significant financial or reputational risk. To prevent this, Security Awareness Training teaches employees what to look out for and provides them with ways to report suspicious content. This helps improve the overall security of the organization. Proofpoint also shares the latest attack methods among its customer base. This increases overall awareness and improves every customer’s security.

The Results

Email fraud eliminated while protecting Shelter Insurance® brand

The automated threat remediation provided by Proofpoint had an immediate impact. Proofpoint Email Protection and Email Fraud Defense, including TAP and TRAP, automatically blocked 99% of phishing and malware attacks. And they blocked more than 95% of email sent from malicious URLs. Proofpoint also significantly reduced the email load on employees. This increased overall company productivity. During a recent two-month span, the Proofpoint system stopped over 6.8M malicious emails. These included phishing attacks, ransomware, zero-hour threats, viruses and spam.

Equally important, the implementation of DMARC allowed Shelter Insurance® to take back control of their domains. This protects their valuable brand and reputation. DMARC discovered over 8,000 unique IP addresses sending on behalf of “shelterinsurance.com” from more than 100 countries. The team also uncovered 10 fraudulent lookalike domains sending messages under the Shelter Insurance® name.

“Our experience with domain fraud has helped increase awareness about security across the company,” said Lymer. “I recently received an email from a marketing director about the latest developments in DMARC. It was great to see that company leaders are aware of the security risks we face and understand the value of investing in Email Fraud Defense.”

The email security team also credits Security Awareness Training with helping them to strengthen their last line of defense: their employees. The security team conducts quarterly testing using simulations of actual phishing campaigns. This educates employees about what to watch for and whom to call if they suspect a message may be malicious. Before the training, almost one-third of employees clicked on a fake phishing link embedded in the test email. In the next quarter, after initial training, only half as many employees took the bait: some 16%. And after a full year of tests and training, just 7% clicked the test link. Also, during the same period, five times as many employees reported the simulated phishing attacks. And reports of suspected actual attacks tripled, from approximately 500 to 1,500 per quarter.

The security team plans to continue regular testing and training sessions for new and existing employees. This helps reduce the number of clicks. And it educates employees regarding new and devious threats they may encounter. With regular employee training, the email security team can also refine its rules. And they can separate legitimate messages from increasingly sophisticated attacks.

Concluded Lymer, “People across the company now see that security is part of everyone’s job.”

LEARN MORE

For more information, visit [proofpoint.com](https://www.proofpoint.com).

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. [Proofpoint.com](https://www.proofpoint.com)