CASE STUDY

Cofense Case Study

Defense and Aerospace Company Reduces Susceptibility Across 8,000 Users to Less than 2%

COFENSE

Cofense Case Study

REDUCING SUSCEPTIBILITY ACROSS 8,000 USERS TO >2%

Background

A large multinational company was the target of relentless phishing attacks intended to steal intellectual property. With growing alarm, the company kept throwing more people, technology and money at the problem to little effect, until it concluded the answer lay in raising user awareness. For most multinational companies, the issue of "phishing" is an everyday occurrence. For our case study, the company concerned was investing significantly in technology to help defend itself; however, company managers concluded that without engaging end-users as the first line of defense they were undermining this investment.

Executive Summary

Client: Multinational Defense and Aerospace Company

Challenges: Creating a global anti-phishing program that engages 8,000 employees over five continents.

Solutions: Cofense PhishMe, Cofense Reporter

Results: Phishing susceptibility dropped to less than 2%

Challenges

With 8,000 users dispersed through five continents and many other international locations, getting everyone on the same page to fight phishing seemed a huge challenge. In addition to the development of a global IT Security Awareness program, a method of assessing user susceptibility to phishing email was required.

Solutions

As it happened, the company's North America division was preparing to test an enterprise phishing defense solution, Cofense PhishMe®, so the global security awareness team watched for the results. Pleased with the outcome, the security team knew it had found its phishing defense solution. "We looked at the success in North America and decided to deploy Cofense PhishMe for the rest of the user population," recalls the client's security awareness leader. In the most recent test, the company's susceptibility measured at just under 2%, a stunning drop from 21% before deploying Cofense PhishMe, including less than 1% for employees who took the simulation bait more than once.

Real-world Scenarios

The company wanted a scalable, human-driven phishing defense solution that measured results internally and had the capability to benchmark them against organizations of comparable size. So in addition to Cofense PhishMe, the client deployed Cofense Reporter® to collect relevant data. Cofense PhishMe is an enterprise SaaS solution that employs customizable simulated phishing scenarios and immediate education to reduce an organization's phishing susceptibility by conditioning users to recognize and avoid phishing threats.

After using Cofense PhishMe for two years, the client deployed Cofense Reporter, which organizes and normalizes user reports of phishing attempts (whether real or as part of a testing exercise) to strengthen threat-detection capabilities. The client set up Cofense Reporter to send suspicious emails to its global security operations center for triage and assessment.

Business Results

Rehabilitating Chronic Offenders

The company's 8,000 users include full-time employees and contractors – all subject to the same security policies. "It only takes one person to take the bait for us to have a problem. So if you miss contractors, you're missing a chunk of people," says the security awareness leader.

Since deploying Cofense PhishMe, the company has conducted four global simulations each year, although each region can run additional simulations when warranted. All users who fail a test are sent an email explaining what "red flags" they should have spotted in the test. The email encourages them to change their behavior and reminds them to re-take security awareness training.

> "We've always found [Cofense's] response to be very good in terms of speed and quality."
>
> **— Security Awareness Leader, Multinational Defense and Aerospace Company**

"We especially focus on chronic offenders. Anyone who has failed at least two of three tests gets specific attention," the company security awareness leader says. But rather than castigate them, the client nudges chronic offenders to do better. The email might say, "98% of our people passed the previous test, but unfortunately you weren't one of them. By changing your behavior you could help us improve further." It's a type of positive reinforcement. "People want to do as well as their peers," he says. "We are trying to use the carrot more than the stick."

The approach is working. The company's overall susceptibility score of 2% is remarkable considering the number of users. During the last year the average score dropped to 5% from 21%. "Our feeling is that if we are below 10%, we are doing well and certainly below average for susceptibility. Nevertheless, we recognize 2% of 8,000 is still a significant amount of people, so we can't rest on our laurels too much."

Choice of Bait

Cofense PhishMe comes with prepackaged phishing scenarios, but customization is available. This client used a package delivery scenario in its first test because receiving a package is relatable to any user regardless of location or cultural customs. "So it's quite a seductive piece of bait," says the awareness leader.

The company is mindful of cultural, religious and social considerations when choosing bait. The global security awareness team reviews the available scenarios then recommends which to use next. “I very much want my international leads to have the lead on “bait” selection. Rather than the corporate head office telling them what we are going to do, I ask them to suggest what we are going to do.”

Improved Reporting

Getting users to report suspicious emails is never easy, and this client’s experience was no different. “We had a process for them to follow. They had to follow a published process to ensure technical information within the email was preserved so that it could be examined by our experts.

The manual nature of the process discouraged people. “It’s easier to just hit delete because they may figure we’re a big organization and someone else has reported it already, or, quite frankly, they just couldn’t be bothered,” says the team leader. Cofense Reporter changed all that by giving users a one-click process to report suspicious emails. “So it’s just as easy as clicking a delete button.”

In response, users get a congratulatory message when they spot a phishing test email. If a reported email isn’t a phishing test, they receive a thank you for helping to keep the company safe. “One of the key benefits of this approach is when running a test, reported emails are not sent to the experts – reducing their workload.”

Conclusion

The client couldn’t be more pleased with Cofense. The technology has delivered as promised, and when the company has needed help with troubleshooting or usability questions, Cofense’s tech support has proven responsive and helpful. “We’ve always found their response to be very good in terms of speed and quality.”

Cofense has supported the implementation of the global IT Security awareness program in improving users’ ability to identify suspicious emails. As an added bonus, increased staff sensitivity to unusual emails has compelled the client to reevaluate its internal communications. The security team is actively working with various internal communications functions to ensure that mail sent to staff is free of “red flags” that may cause a user to ignore the content and use the Cofense Reporter button.

IT security awareness training and Cofense technology is an investment, says the awareness leader. “I was asked early in the process what is the cost of doing this. My reaction was, ‘what’s the cost of not doing it?’ This has to be seen as an investment, not a cost.” According to the awareness leader, their Cofense investment protects the company’s intellectual property and also the information stored and handled belonging to their organization and customers.

When making a case for Cofense technology, he recommends focusing on safety. “Treat any phishing investment as a safety campaign. It’s very rare that people will question how much you spend on safety.”

COFENSE

W: cofense.com/contact **T:** 703.652.0717
A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175