CASE STUDY

Cofense Case Study

Leading University Ramps Up Phishing Defense as Global Threats Grow

COFENSE™

Cofense Case Study

COFENSE AND A MIDDLE EASTERN UNIVERSITY

Background

In 2012, a phishing email triggered one of the largest cyber-attacks ever, aimed at a large Middle Eastern oil and gas company. In the wake of the attack, organizations worldwide redoubled security investments. One such organization was a top university whose students, faculty, and administrators hail from around the world.

The school's Head of Information Security made anti-phishing a top priority. He partnered with Cofense to train his users to recognize and report suspicious emails.

Executive Summary

Client: A Middle Eastern university serving an international mix of students, faculty, and administrators.

Challenges: Reduce phishing susceptibility and increase reporting in the face of growing threats, potentially from nation-state actors.

Solutions: Cofense PhishMe™ and Cofense Reporter™. Recently added Cofense Triage™

Results: Significantly reduced the security team's time spent investigating suspected phishing emails and increased organizational resiliency to phishing attempts.

> "Fortifying the human firewall is my utmost priority. The human element is the most important part of your defense."
>
> — **Head of Information Security**

Challenges

"My mandate was to do everything necessary to protect the university community," said the Head of Information Security. "We invested in technological solutions, but with thirty years of IT experience, I know that you need to invest in people, not just processes and technology. You need to make them human firewalls."

"Look at it this way," he added. "You can put five locks on your door, but if you leave the keys under the doormat, the locks don't do much good. Fortifying the human firewall is my utmost priority. The human element is the most important part of your defense."

Cofense PhishMe and Cofense Reporter

The Head of Information Security adopted a "use it well or lose it" approach to email and Internet access. "My position is that access to online services is a privilege, like having a driver's license," he said.

"You go to the DMV to get your license and the police monitors and enforces good behavior. If your behavior is lacking, you get negative points, or possibly even lose your license for a time. I decided that the best way to encourage good user behavior was through a similar points-based system."

> “We’ve made very good progress. The Cofense solutions work beautifully.”
>
> **— Head of Information Security**

He started using Cofense PhishMe™ to send simulated phishing emails to university users. He also introduced the Cofense Reporter™ button, a one-click way for users to report suspicious emails to the incident response team.

Those who show good behavior, who recognize and report phishing, gain positive points and are eligible for gifts. Those who exhibit poor behavior accrue negative points. Too many of these could result in temporary loss of Internet access. To avoid that, users can take advantage of phishing education training, then pass a quiz to regain good standing.

“When we launched our anti-phishing program, our susceptibility rate was hovering around 55 percent,” said the Head of Information Security. “Now it’s 11 percent. And the reporting rate has gone from a pretty low number to 50 percent. We’ve made very good progress. The Cofense solutions work beautifully.”

He occasionally sends trickier simulations to keep users on their toes. “One recent scenario netted a 20 percent susceptibility rate, but the reporting rate was still at 50 percent. That’s our #1 KPI: keeping reporting well above susceptibility.”

He noted, “You need to remember certain factors to get an apples-to-apples comparison. That’s why when we benchmark our test results, we use what we call a ‘difficulty criteria model,’ which factors in the complexity of our various scenarios.”

Looking Ahead

Since the university launched its anti-phishing program, phishing attacks worldwide have grown. Researchers at the Anti-Phishing Work Group report the volume of attacks rose in 2017, targeting more organizations than ever[1]. Nation-states continue to use phishing to pursue their goals[2].

To keep its phishing defenses strong, the university is continuing its simulation training, as well as the points-based system for promoting phishing awareness. The school has also recently purchased Cofense Triage™, a platform that automates email analysis for faster threat response.

“Our team protects students and anyone else using the university’s systems,” he said. “We have users whose technical savvy and online habits vary a lot. It’s important to get everyone involved in cyber-security, especially phishing defense. We have a lot at stake.”

For more information about Cofense’s award-winning phishing defense solutions, please email info@cofense.com. Sign up for Cofense Threat Alerts for updates on the latest malware and ransomware attacks in real-time.

Sources:

1. APWG, 2017
2. Dark Reading, 2017

COFENSE

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