CASE STUDY

Cofense Case Study

Healthcare Data and Technology Company Builds A Complete Phishing Defense.

COFENSE

Cofense Case Study

COFENSE AND HEALTHCARE TECHNOLOGY COMPANY

Background

This company's VP of Information Security inherited a strong anti-phishing program. The organization had been a Cofense client for about a year. It used Cofense PhishMe™ and Cofense Reporter™ to condition users to recognize and report suspicious emails, then added Cofense Triage™ and Cofense Intelligence™ to shore up incident response.

Challenges

When the VP came onboard, his challenge was to take phishing defense to the next level. How could the organization make its anti-phishing more complete? How could his team refine their strategies to stay ahead of evolving threats? The answers came in a number of innovations they rolled out.

Executive Summary

Client: A national provider of healthcare data and technology serving hospitals, clinics and other medical facilities.

Challenges: Make its phishing defense as complete and advanced as possible, with tougher simulated phishes, higher reporting, and faster response.

Solutions: Cofense PhishMe, Cofense Reporter, Cofense Triage, and Cofense Intelligence.

Results:

- Keeps users on their toes with more difficult simulations, for example, an "Over your time-off limit" email, which drew a 37% click rate.
- Maintains strong reporting with a Phishing Bounty Program, paying cash to employees who report verified malicious emails.
- Respond to real threats in minutes, including a highly effective phish aimed at rerouting payroll deposits.

> "We have the kind of culture that likes to push the envelope. We want to make sure our anti-phishing tactics are challenging and relevant."
>
> **VP, Information Security**

Solutions

Cofense PhishMe and Cofense Reporter

Using Cofense PhishMe to run phishing simulations, the company mixed in harder scenarios to keep employees alert. The toughest one was an email titled "Time-Off Requests," which told recipients they had gone over their limit for personal time. It asked employees to click a link to take care of the matter.

Thirty-seven percent of recipients took the bait. When employees received a similar email a year later, the susceptibility rate dropped to 22%—still high, but a noticeable improvement.

"We have the kind of culture that likes to push the envelope," said the VP. "We want to make sure our anti-phishing tactics are challenging and relevant. So, we keep our eyes peeled for new and emerging threats."

His team sent another irresistible email during the 2016 presidential election. With emotions running high as Hillary Clinton and Donald Trump battled, the email, purportedly from HR, reminded employees of the company's policies on political activities at work, asking them to click a link to show they understood and agreed.

"It was a good reminder not to be complacent," the VP said. "A lot of people bit on that one." Other top-performing scenarios: "Package Delivery" and tax-related emails in the run-up to April 15.

A best practice the VP recommends is to keep HR and other departments in the loop. "You can't send a phish supposedly from HR without working it out with them beforehand," he said. "They need to prepare for more calls and emails when certain simulations go out. Once they're in your corner, everything goes more smoothly."

To keep email reporting rates high, the VP launched a Phishing Bounty Program. It gives rewards to employees who use Cofense Reporter to report a verified malicious email. "We're really proud of this program," said the VP. "Employees participate enthusiastically and the rewards are way cheaper than a breach or ransomware incident. Plus, we notify managers to give credit to vigilant people."

Results

Cofense Triage and Cofense Intelligence

The company uses Cofense Intelligence to feed its simulations. Intelligence on the latest threats help make the training relevant. The intel also augments the protection of the company's secure email gateway.

Cofense Managed Triage is a key defense layer, too. Before it arrived, the team had a backlog of thousands of employee-reported emails. Triage automates their analysis, allowing the Cofense Phishing Defense Center to work with the VP's team and respond to threats in real time. One incident in particular highlights the value of this partnership.

"An attacker sent an email that showed he'd really done his homework," said the VP. "The email looked and sounded exactly as though our CEO had sent it."

> "All of this was the result of a single well-crafted phishing email. If we hadn't been prepared, the damage would have been worse. We were able to retract the email in under 20 minutes."
>
> **VP, Information Security**

The link took them to a counterfeit Office365 page that asked for login credentials. The idea was to harvest passwords, gain file system access, and reroute automatic payroll deposits. The bad news: the email was so credible that many recipients clicked. The good news: a hawk-eyed employee reported it and Cofense sprang into action.

Here's how fast the company and Cofense disrupted the attack:

11:48 a.m. – Spear phishing campaign launched.

11:49 a.m. – Employees, trained through Cofense PhishMe, begin reporting the email using Cofense Reporter.

11:49 a.m. – Reported emails go to Cofense Triage for automatic analysis.

12:00 p.m. – As more evidence emerges, Cofense Phishing Defense Center escalates its investigation.

12:07 p.m. – Cofense completes the investigation and calls the company's VP of Information Security.

12:07 p.m. – The company blocks the phishing site and begins to:

- Retract the email from inboxes
- Monitor behavior coming from affected Office365 accounts
- Disrupt any lateral movement

"We removed the email quickly," said the VP, "though in the space of a few minutes a lot of people clicked. Once we contained the threat, we started on repair and recovery work, seeing who clicked and mitigating problems linked to their accounts. All of this was the result of a single well-crafted phishing email. If we hadn't been prepared, the damage would have been worse. We were able to retract the email in under 20 minutes."

Results

Next Steps

By steadily innovating, the VP of Information Security is expanding and refining his company's phishing defense. To bolster phishing awareness, his team will keep adding harder-to-identify phishing scenarios. To maintain high reporting rates, the Phishing Bounty Program will keep humming along. And the team has recently complemented Cofense Triage with capabilities to automate the retraction of malicious emails.

Attackers looking to make a quick buck—who think healthcare security is softer than in, say, financial services—will always target the company. It's one reason why an aggressive phishing defense is a must. Another reason: in healthcare, ransomware can be a matter of life or death.

"We supply data to healthcare practitioners on, for example, medication or other supplies," said the VP. "If a ransomware attack succeeded, we'd be in a difficult spot. By enlisting the entire organization in awareness and response, we can reduce this risk—and a host of other vulnerabilities, too."

For more information on Cofense phishing defense solutions, please email **info@cofense.com**. Sign up for **Cofense Threat Alerts** for updates on the latest phishing and malware threats.

COFENSE

W: cofense.com/contact **T:** 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175