CASE STUDY

Financial Services

"We stopped a phishing attack in 10 minutes. It used to take days."

COFENSE

Cofense Case Study

"WE STOPPED A PHISHING ATTACK IN 10 MINUTES. IT USED TO TAKE DAYS."

Background

A national financial services company found itself at a crossroads. Trained on Cofense PhishMe™, its users were doing a good job of recognizing phishing. The next step: report and respond to malicious emails faster.

So, the company added Cofense Reporter™ to report suspicious emails with one click, along with Cofense Triage™ to analyze them faster and accelerate mitigation.

Executive Summary

- National financial services company needed to stop phishing attacks faster and more efficiently
- Implemented Cofense Reporter and Cofense Triage
- Identified and stopped a credential phishing attack in 10 minutes
- Previously, would have taken days to find and resolve
- Blocked the phishing site BEFORE employees entered data

Solutions and Results

Two key players, the Security Awareness Manager and Threat Intelligence Analyst, work together closely on the company's phishing defense. They didn't have to wait long to see their new investments pay off.

> "The phishing email was *quite convincing*."
>
> **— Threat Intelligence Analyst**

"Within a week of implementing Cofense Reporter and Triage, we identified and stopped a phishing campaign our users reported," said the Security Awareness Manager.

Cofense Triage analyzes emails automatically. It also groups malicious emails by attributes and campaign, making it easier to find and stop attacks in progress.

"We saw a series of reported emails sent, allegedly, by a major credit card provider," said the Threat Intelligence Analyst. "It landed in over 200 inboxes and was quite convincing, using the credit card company's logo to get people to drop their guard."

The email was a classic scam. It told recipients the credit card company had noticed unusual "recent activities" in their accounts. It instructed employees to click a link to a My Account page, where they could verify and protect their personal information.

"The landing page asked for a wealth of personal data," said the Threat Intelligence Analyst. "Name, address, social security number, email, you name it." As reported by Cofense, credential phishing accounts for over half of all malicious emails.

Added the Security Awareness Manager, “Though attackers were after personal data, not company information, they could have used that data to connect a few dots and target the corporate network.”

The security team quickly blocked the landing page’s domain—before any users entered their data. “With Triage, we were able to stop the attack in minutes, not days,” said the Threat Intelligence Analyst. “Previously, that wouldn’t have been the case.”

> “Stopping the attack was a ***big win*** for our team.”
>
> **— Security Awareness Manager**

Looking Ahead

The security team can use these results to recommend further actions, like blacklisting sites or pulling malicious emails from inboxes. Said the Threat Intelligence Analyst, “There’s a balance to be struck between tightening controls and not impeding business. Email is a tool everybody uses, so before we make changes, we need to make the business case. We’re starting to have those conversations.”

As the attack unfolded, the company for the first time scooped its peers in threat intelligence. “We shared intel with the financial services security community,” said the Security Awareness Manager. “We were the first to report the campaign, including indicators of compromise, to FS-ISAC so the community would know what to look for.”

“In the past, it worked the opposite way,” he continued. “We’d get threat intelligence from FS-ISAC that came from other companies. It’s a big win for our team.” Since the attack, his team has been first to report several other times.

“Senior management is super-excited,” said the Security Awareness Manager. “We can stop attacks with a speed and efficiency we didn’t have before.”

COFENSE

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

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