CASE STUDY

Cofense and UCB

United Community Bank Builds Phishing Defense Program with Cofense

COFENSE™

Cofense Case Study

COFENSE AND UNITED COMMUNITY BANK

Background

United Community Bank (UCB) is a $10.4 billion regional banking institution with 140-plus branches across Tennessee, Georgia, South Carolina and North Carolina. The company employs nearly 2,000 people who use email throughout the business day. Management wanted to ensure all employees use email safely and have the ability to recognize a phishing attempt when one crosses their inboxes. Phishing defenses are especially critical to banks since they are a favorite cybercrime target.

Executive Summary

Client: United Community Bank, a $10.4 billion southeast regional banking institution

Challenges: Executives and employees being bombarded with phishing attempts

Solutions: Cofense PhishMe, Cofense Reporter

Results: Fortifying the overall employee base against phishing attacks. Delivering a tailored phishing education program to lower susceptibility rates of at-risk employees.

Challenges

UCB chief executives have seen their fair share of phishing attempts in their inboxes, according to UCB Chief Information Security Officer Jim Stewart. But while an executive may have a stronger nose for sniffing out phishing emails, management worried the majority of employees may be less attuned to the threat.

"We decided we needed to condition our employees against phishing," Stewart says. Doing so wasn't without challenges because "there's a fine line between security and service." If you lean too far in one direction and block everything that looks suspicious, it could be at the expense of responding to customers. Since world-class customer service is what distinguishes UCB from larger competitors, the company needed the right vendor to provide a scalable phishing solution while saving UCB time and effort.

Solutions

Cofense PhishMe® and Cofense Reporter® Deployment

UCB chose Cofense PhishMe after reviewing a total of 11 solutions. Criteria for choosing a solution included price, scalability, ease of administration and quality of phishing education content. After UCB narrowed the choices to three, Cofense rose to the top. "We were looking for that total anti-phishing solution, and Cofense provided us with that," Stewart says.

So UCB deployed Cofense PhishMe to build a phishing defense and user education program. A cloud-based SaaS immersive learning platform, Cofense PhishMe deploys easily from all major web browsers. It instructs users on the dangers of phishing by periodically sending simulated phishes. Users have to decide whether the email is legitimate or report it as a suspected phish. Stewart compared it to picking up an iPhone for the first time saying, "No one's ever read an instruction book to an iPhone. Using Cofense is that easy and intuitive."

UCB also has deployed Cofense Reporter, which organizes and normalizes user reports of phishing attempts to improve threat detection. Reporter appears as a red fish-shaped button on email screens. It was deployed two weeks before the first company-wide simulation, which helped raise awareness about the anti-phishing campaign.

Previously employees reported suspicious emails by placing them in a mailbox labeled “Abuse.” Reporter simplified the process: With one click, users can use Cofense Reporter to send suspicious emails in their entirety into UCB’s security operations center. Those who successfully identify a real or simulated phish get a congratulatory email in response.

> “I was very pleased with our rollout of Cofense Reporter. I never would’ve dreamed we’d achieve a response rate of over 50 percent on the first campaign.”
>
> **Jim Stewart, Chief Information Security Officer, United Community Bank**

Business Results

Identifying Improvement Areas

The first simulation targeted the bank’s 14-member technology steering committee. Ramp-up time was limited because the committee was scheduled to meet two weeks after deployment, but thanks to the ease of installation, UCB completed the test successfully. “With a lot of other security solutions, we just wouldn’t have tried to run a proof of concept in that short time frame,” noted Stewart. “It’s usually impossible. But with Cofense it was just easy.”

A company-wide simulation followed. “We wound up with a 7.4 percent fail rate, which is about what I anticipated,” Stewart says. Users who click simulated phishes receive instructions on phishing and an explanation of why they failed the test. Results showed that of the 142 employees who failed, 60 spent less than 30 seconds on the instructions they received, which meant they were likely to fail the next test. “There’s not enough time to read the Cofense educational content in 30 seconds,” says Stewart.

To identify those users, Stewart’s team leverages built-in analytics that parse results by location and job title. The highest fail rate – 20 percent – was among entry-level tellers. “That told me we need to do a better job on our teller mentor program as we bring new employees into the company,” said Stewart. “It gave me very valuable information as to where I needed to target my effort to improve things. These types of insights help create actionable plans to reduce susceptibility rates.”

In the first company-wide simulation, 54 percent of employees clicked the Reporter button. “I was very pleased with that. I never would’ve dreamed we’d be over 50 percent on the first campaign,” Stewart says. When users report a suspected email, the security team gets notified through a dashboard, which keeps track of response rates, identifies users who click the button by job title and location, and the time of day. As with deployment, Stewart says, “nobody had to show me how to use the dashboard. It provided me very quickly with the information that I needed, and how I needed it.”

As simulations continued, department heads became invested in the program, even treating it as a competition. Our chief legal counsel, whose staff had scored particularly high, Hucko says, “sat everybody down, put them through extra training and really emphasized the importance of understanding the effects of a potential phishing attack on the company. Ever since that meeting, his group has had the lowest susceptibility in the company.”

Each Cofense PhishMe test generates lots of useful data. Hucko leverages it to identify which departments might need some extra attention. “We use these data to help us plot out our itinerary for one-on-one meetings, so I can say, ‘Let’s start with the 10 facilities that have higher-than-average susceptibility to phishing, and go from there,” Hucko says.

Working with Cofense

Stewart credits the Cofense team with making the implementation straightforward. Whenever he’s had a question or request, the team has responded promptly and effectively. For instance, the team obliged his request to parse users by job title and location. Per Stewart, Cofense has provided solid guidance and support, “all the way from sales and demos to contract implementation to post implementation support. Time is of the essence in everything we implement so when something’s that easy, you start out of the gate with a very positive feeling about it.”

He is confident the team will remain helpful as UCB’s anti-phishing campaign evolves. One step in the evolution was to brand the education aspect as an internal UCB endeavor, with Cofense providing the “the engine behind the scenes.”

The client wants to leverage new Cofense capabilities as they become available. “We plan to continue to stay close to the front of the line and use it to the betterment of our employees,” notes Stewart. Thanks to the solution’s scalability, Stewart says he expects no problems in adding new employees to the Cofense platform as a result of acquisitions, thanks to Cofense’s ease of administration. “Whether we’re adding 200 employees or 50, we know it’s an easy process.”

With each acquisition, Stewart says he plans to do a simulation within 60 or 90 days. The results will point the way in preparing phishing education for the new employees.

Conclusion

Stewart initially had some misgivings about an anti-phishing campaign. “It feels a little bit devious, like you’re trying to trick your employees.” Then he realized while he was thinking about the situation “with a conscience,” attackers have no such moral quandaries.

A company of 2,000 employees is a company with 2,000 potential vulnerabilities. Using a little deviousness to determine phishing susceptibility and which employees are the most likely to click suspicious emails is a small price to pay to prevent a phishing attack. Cofense, Stewart says, has helped turned those 2,000 vulnerabilities into 2,000 defenders.

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