Healthcare Leader Gets Creative to **Stop Phishing Attacks**

Cofense Customer Case Study

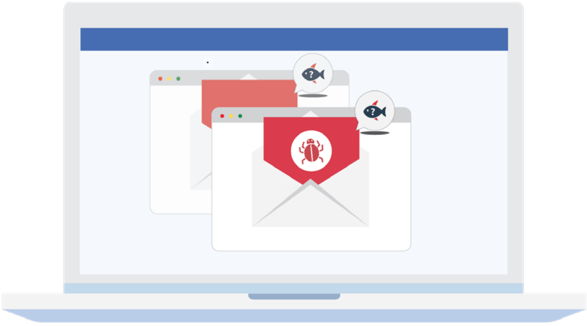
COFENSE.COM

EXECUTIVE SUMMARY

- Healthcare organization with thousands of employees across the U.S.
- **The wake-up call:** a phishing email that captured credentials from 400+ employees
- **The answer:** Cofense PhishMe™ and Cofense Reporter™ to empower employees to report phishing
- In recent phishing simulations, the reporting rate has been 3-7 times higher than the susceptibility rate
- Thanks to creative engagement tactics, employees are reporting real phish to stop attacks in their tracks: credential harvesting phish, malicious URLs, and malware campaigns to name a few

BACKGROUND & CHALLENGES

A healthcare organization with campuses across the U.S. had a rude awakening. "To see how vulnerable we were to phishing, we had a consultant send phishing emails to our senior managers," said the company's Chief Information Security Officer (CISO). "Close to fifty percent fell susceptible."



Shortly afterwards, there was more bad news. One evening, a manager saw his email account was compromised by an attacker, but failed to report the incident. The next morning, the attacker used the account to send a phish to all employees. "It had an attachment related to performance evaluations," said the CISO. "In fact, the company was in the midst of evaluating performance. We estimated that over 400 employees gave away their credentials. We had to make everyone change passwords at the same time. The organization came to a screeching halt. That was a very bad day."

SOLUTIONS & RESULTS

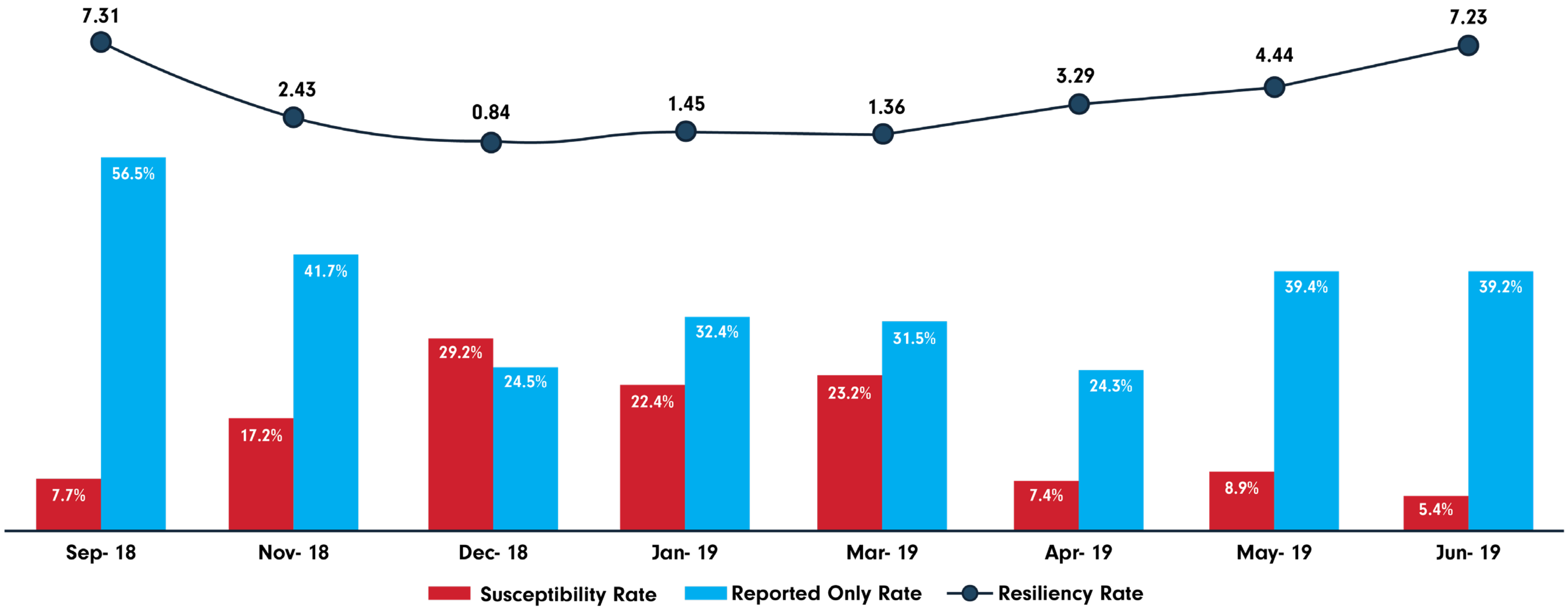
To turn things around, the CISO used Cofense PhishMe and Cofense Reporter to condition employees to recognize and report phishing. In simulated phishing attacks, employees receive real-time feedback, both positive reinforcement for a job well done and educational tips when they fall for a bogus email.

The CISO said these solutions were "exactly what we needed." She added, "We ran our first simulation in the fall of 2018 and have done monthly simulations since then. While a few months have seen over 20 percent of employees falling susceptible, often the rate has been well under ten percent."

"People are getting the message. They know how to report and why it's important."

- Chief Information Security Officer

Only one simulation has yielded a higher rate of susceptibility than reporting—a holiday e-card phish in December. The rates fluctuate depending on the emails' difficulty. In the last three simulations, the resiliency rate (the top line in the chart below) rose steadily from over 3% to more than 7%—in other words, the reporting rate has been 3-7 times higher than the rate of susceptibility, a very encouraging trend. Resiliency is the key metric in simulation programs. It helps focus phishing defense on taking action—reporting emails—instead of looking solely at the number of people who click.



Employees are using what they learn to report malicious emails and help security teams respond faster. "The awareness program has absolutely helped to stop real phishing attacks," said the CISO. "There are days when a lot of users report the same thing in a very short period of time, so we know we have an imminent risk on our hands. Because reporting suspicious emails is now centralized through Cofense Reporter, we can see patterns that signify phishing campaigns, versus dealing with reports as one-off incidents. We now know when we've got a real threat that we need to deal with right away."

She noted that security teams respond quickly to reported emails. “We’ve got the routine down pat,” she said. “The emails are reported, we see the patterns, and can verify phishing faster. Then our network team blocks the URL, the security team looks at potential payloads, our service desk team works with our systems people to get a list of all users that received the message, and we kick off virus scans of their machines. Also, we require anyone who has interacted with a phishing email to do a password reset in case they gave away credentials.”

She said that employees are reporting all types of real phish: credential attacks, malicious URLs, malware, man in the middle attacks, and more.

> “The awareness program has absolutely helped to stop real phishing attacks.”
>
> *- Chief Information Security Officer*

The key to a successful program? “Have fun,” she said. “It’s a serious topic, but you need to be engaging.” For example, at a recent company safety fair the CISO set up a booth to promote phishing awareness with contests for spotting and reporting malicious emails.

"People are getting the message," she said. "They know how to report and why it's important." The CISO works hard to help under-performing departments, giving them extra instruction, additional training simulations, and incentives like opportunities to win Amazon gift cards. And employees companywide received pens bearing the message "Click this, not phishing links."

"For Cybersecurity Awareness Month, we're going to run a contest where people can create a scenario to phish their peers," she said. "If you were a phishing attacker, what kind of phish would you create? The winner's phish will be used in an upcoming simulation."

One person who was initially critical of the program did a total turnaround. "She told me she now looks forward to getting the simulations—she sees it as a kind of game," the CISO said. "We've 'gamified' the program and people are responding well."

The CISO has shared program results with her Chief Operating Officer (COO), who was "thrilled," she said. "The COO now wants to share results on a regular basis with the board of directors."

All in all, "Cofense is a great partner. Our professional services representative is a perfect fit for us. She helps us with every aspect of running an effective program. We have a kind of mind meld, where she'll suggest ideas and my reaction is 'I love it!'"