

Cofense Case Study

Global CPG Leader Accelerates
Phishing Reporting and Incident
Response with Cofense





Cofense Case Study

COFENSE AND GLOBAL CPG LEADER



Background and Challenges

In 2015, this consumer product goods (CPG) leader had no formal anti-phishing program. Knowing the threat was growing and its security team needed help, the business began using Cofense PhishMe® to measure employee's susceptibility to suspicious emails and Cofense Reporter™ to report them with one click. Later, the CPG firm deployed Cofense Triage™ to help incident responders recognize threats and remediate them faster.

According to the CPG company, 28 percent of employees, as well as third-party contractors, clicked on bad emails during initial Cofense simulations. "That was a wake-up call," said the CPG company's head of security awareness. "We knew we needed improvement, but thought we were in better shape than that." Employees needed help in spotting potential phishes – especially critical departments more heavily targeted by attackers.

Moreover, the company needed a central storehouse where suspicious emails could be forwarded and automatically prioritized. Incident responders had to spend hours sifting through 500 to 1000+ emails reported daily. Instead of focusing their efforts on dealing with real phishes – not to mention the myriad other security issues they faced – responders wasted time manually sorting through the clutter to distinguish threats from noise.



"Our leadership wants to know that we're always getting better. Cofense lets us demonstrate that."

– Head of Security Awareness, CPG leader

Solution and Results

Cofense PhishMe and Cofense Reporter

Implemented simultaneously, Cofense PhishMe and Cofense Reporter proved a powerful combination. Cofense PhishMe tested employees' susceptibility to phishing under simulated conditions. And Cofense Reporter "relieved employees of having to figure out whether and how to report a suspicious email," said the head of cybersecurity. "If they had any doubts, they could report an email with a single click and get on with their day." For that reason, the company installed Cofense Reporter on devices before deploying Cofense PhishMe.

Executive Summary

Client: A consumer product goods (CPG) business with USD 16.6B in annual net sales and 40K employees in over 100 markets

Challenges: Helping frequently targeted teams recognize and report phishing and enabling incident responders to distinguish real threats from noise

Solutions: Cofense PhishMe, Cofense Triage, Cofense Reporter

Results:

- Fewer than 1 in 10 employees now click on simulated phishes
- Up to 9 in 10 employees in some critical departments correctly report simulated phishes
- Just 20 percent of reported emails are personally triaged by incident responders – thanks to automation

Phishing Susceptibility Rates (PSR) improved strongly:



PSR in 2015



PSR in 2016, after steady conditioning and education



PSR in 2017



PSR in 2017 for some critical departments

Email Reporting Rates (ERR) have climbed:



ERR in 2016



ERR in 2017



ERR for some critical departments in 2017

While metrics continue to improve, “Our leadership wants to know that we’re always getting better. Cofense lets us demonstrate that. We can’t just do the same basic simulations over and over. With Cofense PhishMe, it’s easy to customize more complex phishing scenarios. Over time, we’ve made the exercises more advanced, personalizing emails by name and company logo, to reflect what’s happening in the real world.”



“Our incident responders are making much better use of their time now.”

— Head of Security Awareness, CPG leader

Cofense Triage™

With training and implementation help from Cofense professional services, the CPG leader now has a dedicated, purpose-built mailbox where employees can forward suspicious emails. Cofense Triage automates the process of distinguishing threats from noise. 80 percent of reported emails are resolved automatically – and just 20 percent now require active attention from responders. The service’s clustering capability helps identify larger phishing campaigns, so the incident response team can address them swiftly.

“Our incident responders are making much better use of their time now. They can recognize and respond to a real incident, instead of sifting through tons of emails before stumbling upon something important. Cofense Triage improves the quality of work our responders can do.”

80% of reported emails are resolved automatically – and just 20% now require active attention from responders

Conclusion

With susceptibility rates in the single digits and reporting rates steadily rising, the head of cybersecurity reports that “employees have become an important line of cyber defense.” And thanks to the automation and analytics of Cofense Triage, “we’re not drowning in information anymore and can act on threats right away.”

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.

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyber attacks. Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organization-wide response to the most used attack vector—phishing. Cofense serves customers of all sizes across multiple industries including financial services, energy, government, healthcare, technology and manufacturing, as well as other Global 1000 entities that understand how engaging user behavior will improve security, aid incident response and reduce the risk of compromise.



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