Cofense Products

INNOVATION IN GOVERNMENT
TECH SPOTLIGHT SERIES

Cofense Stops Phishing Attacks at Federal Agencies

UNIQUE CHALLENGES FACED BY THE FEDERAL GOVERNMENT

Cybersecurity is the top concern for most federal agency CIOs as threats grow more numerous and more sophisticated every year. Are you confident your organization is prepared for an attack? In this "not if, but when" environment, time is of the essence. Can your agency recognize and remove a threat quickly enough? Here are two of the biggest challenges facing federal agencies today:

1. Protecting Mission Critical Information

As phishing threats rapidly evolve and increase, mission criticality must be your focus. Spear phishing is the most significant vulnerability among federal agencies. Threat actors target weaknesses such as social media, contracts, and vendors to infiltrate federal networks—and federal agencies receive billions of weaponized emails each year. Agencies need to protect their data with phishing platforms from trustworthy, FedRAMP-approved vendors.

2. Supporting Remote Workers

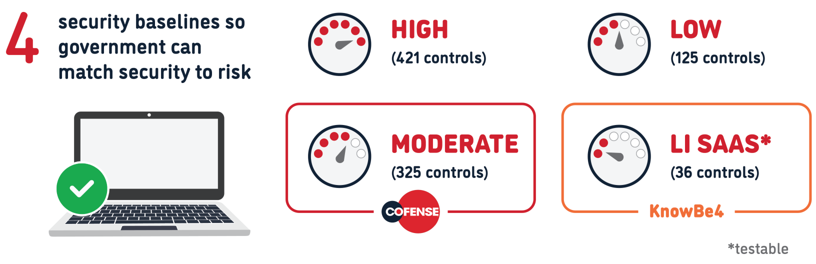
Federal agencies have rapidly scaled up the number of employees working remote to ensure continuity of operations during the Covid-19 crisis. Although VPNs can be very scalable, secure email gateways (SEGs) are not 100% secure, and phishing has become the sweet spot for constantly innovating threat actors. Remote access requires agencies to implement security solutions that educate employees and attune them to real phishing threats.

ADDRESSING CHALLENGES WITH A COMPREHENSIVE SOLUTION

To meet these challenges, federal agencies must address the risks through a comprehensive phishing defense program that not only includes industry-leading solutions but also builds up employee resilience through a positive workplace culture. Only Cofense® offers the protection your organization needs—with an end-to-end phishing defense. Cofense PhishMe™ enables federal employees to better spot and report phishing attacks, protecting the data they safeguard.

Cofense allows you to:

- Deliver simulations to users based on active, evolving threat actor tactics
- Increase program relevance based on best practice, program history and applicability
- Maximize interaction by targeting users who are active in their inbox
- Streamline template selection process and minimize time required to schedule and send across global time zones
- Easily define criteria and automatically pull recipients into defined groups
- Empower users to actively report phishing attacks and expedite SOC team analysis



*testable

Cofense increases employee awareness and delivers protection from malware threats, ransomware campaigns, and scams like sextortion which evade secure email gateways (SEGs) every day. Our solutions give federal teams the visibility and tools to stop phishing threats in minutes, not hours. We give tools to federal employees that help them recognize and stop active threats—by empowering them rather than threatening them.

RESOURCES

Real Phishing Threats Database
carah.io/Cofense-RPET

Learn More about Phishing Defense for Federal Employees
carah.io/Cofense-Federal

COFENSE | carahsoft.

HOW COFENSE SOLVES YOUR AGENCY'S PROBLEMS

Condition Employees to Report Phishing

Identifying and reporting phishing attacks is job one. Cofense enables federal users—including remote workers—to quickly and easily report the latest phishing threats without time-consuming and complicated user management processes. Our Cofense Reporter button is the easiest way for employees to report phishing, and one click sends an email for SOC investigation. Cofense PhishMe simulates active threats that evade controls and land in user mailboxes, helping users recognize threats.

Remove Phishing Campaigns with One Click

Users report suspicious emails. The SOC verifies. Then it's time to search and destroy. Cofense Vision® empowers federal security teams to find phishing campaigns across their agency and remove them with one click. You can run email searches instantly, without disrupting the mail team, while leaving an audit trail that keeps you in compliance. It's threat hunting at speed.

Analyze and Respond to Attacks in Minutes

When federal users report emails, the SOC can't spend hours finding real threats in an ocean of noise. Cofense Triage™ automates noise reduction and email analysis, sending your SOC indicators of compromise in minutes.

Plan Effective Simultions

Good simulations are based on the latest threats known to bypass SEGs. You need to engage users when they are active in their email client and accurately measure their performance—all without burdening your team with time-consuming scheduling. Cofense PhishMe lets you plan what simulations to send, to whom, and when, simulating the most relevant threats.

THE ADVANTAGES OF FEDRAMP AUTHORIZATION

Cofense PhishMe is close to achieving ATO-Moderate for the FedRAMP 'Moderate' authorization, a particularly rigorous standard to meet. FedRAMP Moderate authorization has significantly stricter security controls than FedRAMP Low-Impact authorization, and Cofense will meet the baseline for over 300 controls. Don't waste your precious time and effort in an ATO process for a non-FedRAMP authorized vendor for email phishing simulations.

Cofense is a U.S. company, with a well-established portfolio of federal government customers.

Only Cofense protects federal agencies with end-to-end phishing defense. Cofense has embraced the strict requirements of FedRAMP Moderate for Cofense PhishMe, including continuous monitoring after authorization is achieved, and is now in the final stages of the FedRAMP process. Act now to protect your organization from phishing threats and find your peace of mind with Cofense solutions.

> "We know that in the midst of any crisis, threat actors are going to try to take advantage. Within our enterprise security program, we believe that the individual employee is probably both the strongest and weakest link, and so we put a lot of emphasis on education. We added our Cofense [Reporter] button just in time. We put a lot of emphasis on making sure people are attuned to the cyber threats out there. The individual employee – it starts and ends with them."
>
> — VA CIO Jim Gfrerer in an interview with MeriTalk July 2, 2020, CIO Crossroads: Federal IT in the COVID Crisis – VA Edition

CONTACT US **Cofense@carahsoft.com** • **888-662-2724** • **www.carahsoft.com/Cofense**

COFENSE | carahsoft.