# Cofense Reporter™

ECHTE BEDROHUNGEN IN ECHTZEIT VON MITARBEITERN GEMELDET

Cofense Simulator sensibilisiert Ihre Mitarbeiter zwar für Phishing-Angriffe, aber es reicht trotzdem nicht aus, einfach „nicht zu klicken". Bei einem Phishing-Angriff ist frühzeitige Erkennung entscheidend. Damit Security-Operations-Teams und Incident Response-Teams Sicherheitsmaßnahmen ergreifen und den Angriff auf Ihr Netzwerk schnellstmöglich abwenden können, müssen sie sich der Gefahr zunächst bewusst sein. Mit Cofense Reporter™ erhalten Unternehmen eine einfache, kostengünstige Möglichkeit, Mitarbeiter in die Lage zu versetzen, verdächtige E-Mails zu melden, die auf einen Cyberangriff hindeuten könnten.

## Warum sollten Sie sich für Cofense Reporter™ entscheiden?

Cofense reduziert erwiesenermaßen die Gefahr, dass Mitarbeiter Opfer raffinierter Cyberangriffe werden, um bis zu 95 %. Ihre letzte Verteidigungslinie wird so ermächtigt, trickreiche Phishing-Angriffe zu erkennen und zu umgehen.

### Wichtigste Vorteile

- ✓ Standardisierung und Organisation des Meldeprozesses für Benutzer
- ✓ Schnellere Erkennung von und Reaktion auf E-Mail-basierte Bedrohungen dank benutzergenerierter Berichte
- ✓ Analyse von URL- und Malware-Anhängen durch die Integration von Programmen von Drittanbietern
- ✓ Minimierung der Auswirkungen von Sicherheitslücken dank proaktiver Reaktionsfähigkeit und erhöhter Transparenz
- ✓ Anpassbares Benutzer-Feedback zur Einbindung von Mitarbeitern in Sicherheitsprozesse


## Was ist Cofense Reporter™?

Wenn technische Schutzmechanismen wie Proxy-Filterung, URL-Rewriting und DLP versagen, bilden die Benutzer selbst die letzte Verteidigungslinie gegen Angriffe aus dem Cyberspace. Durch entsprechendes Training sind Ihre Mitarbeiter in der Lage, zeitnah wertvolle Hinweise zu verdächtigen E-Mails zu liefern, da sie diese leichter erkennen und sofort melden können. Da die meisten Unternehmen ihre Mitarbeiter bislang kaum als wertvolle Informationsquelle für Cyberattacken nutzen können, bleiben böswillige Aktivitäten im Netzwerk häufig mehrere Wochen oder Monate lang unentdeckt.

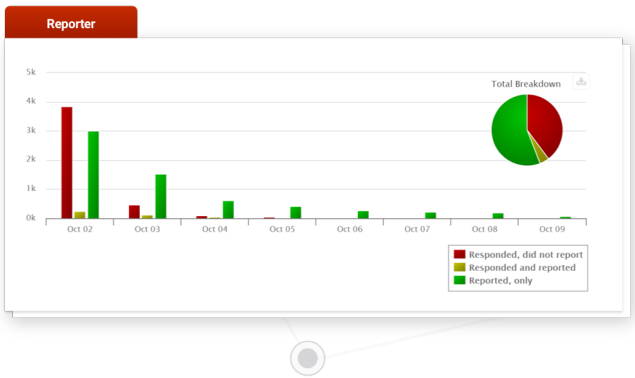
Cofense Reporter ermöglicht verbesserte Meldeprozesse durch die Installation eines Add-ins in der E-Mail-Symbolleiste des Benutzers. Damit kann eine verdächtige E-Mail einschließlich aller erforderlichen Informationen für die Analyse und Reaktion per Mausklick an das Sicherheitsteam weitergeleitet werden.

Cofense Reporter erkennt automatisch E-Mails, die im Rahmen von Cofense Simulator-Szenarien oder von unbekannten Quellen gemeldet wurden. Damit wird sichergestellt, dass nur potenziell schädliche E-Mails an die entsprechenden Sicherheitsverantwortlichen bzw. an Cofense Triage zur Analyse weitergeleitet werden.

## Verbessertes Reporting

Ganz gleich, ob Sie bereits über einen Reporting-Prozess verfügen – der Cofense Reporter bietet folgende Vorteile:

- Speicherung der vollständigen Kopfzeile verdächtiger E-Mails für künftiges Blockieren und Entfernen ähnlicher E-Mails.
- Berücksichtigung von Anhängen und URLs.
- Ergänzung zu Simulator-Kampagnen, Erfassung von Benutzerreaktionen und Reaktionszeiten im Unternehmen.




## Ist diese E-Mail Teil eines Cofense-Szenarios?

**Ja.**

**Benutzerbericht wird in Cofense erfasst**

**„Vielen Dank!"-Dialog wird angezeigt**

**Klicken!**

***Was passiert, wenn ich auf die Schaltflache klicke?***

**Nein.**

**E-Mail wird an IR berichtet**

**„Vielen Dank!"-Dialog wird angezeigt**

**E-Mail wird an Triage oder internes Sicherheitsteam zur Analyse und Bestimmung von Maßnahmen versendet**

## Cofense Simulator-E-Mails

Cofense Reporter erfasst die Berichte zu E-Mails, die von Cofense Simulator versendet werden, und die Namen der Benutzer, die die E-Mails gemeldet haben. So erhalten die Benutzer individuelle Bestätigungen für eine erfolgreiche Meldung. Positive Verstärkung bei der Kommunikation von Feedback trägt auch dazu bei, dass die Mitarbeiter Cyberangriffe besser erkennen können. Die Informationen werden erfasst und in die umfassenden Reporting-Kennzahlen der Cofense-Lösung integriert.

## Verdächtige E-Mails

Berichte zu verdächtigen E-Mails werden an die entsprechende Stelle oder an Cofense Triage gesendet, wo sie dann von einem unternehmensinternen Sicherheitsteam analysiert werden können. Dabei werden die verdächtigen E-Mails mit ihrer ursprünglichen Kopfzeile sowie kontextbezogenen Informationen für eine rasche Analyse als Anhang weitergeleitet. Beim Einsatz von Cofense Triage können Incident Response- und Security Operations-Teams ihre Analysen basierend auf der Reputation eines Benutzers zusätzlich zu anderen Attributen priorisieren um Phishing-Versuche besser zu erkennen.

Cofense™, ehemals PhishMe®, ist der weltweit führende Anbieter von Anti-Phishing-Lösungen. Wir bieten einen auf Zusammenarbeit basierenden Cybersicherheitsansatz, mit dem wir es ermöglichen, unternehmensweit gegen aktive E-Mail Bedrohungen vorzugehen. Unsere Verteidigungslösungen kombinieren marktführende Technologien und aktuelle Angriffsintelligenz von Mitarbeitern um laufende Angriffe schneller zu stoppen und weitere Sicherheitsverstöße früh zu erkennen.
Von der Sensibilisierung der Mitarbeiter bis zur Sicherheitsautomatisierung und Integration sind unsere Lösungen darauf ausgelegt, die Angriffskette zu unterbrechen um die Auswirkungen von Spear Phishing, Ransomware, Malware und Business Email Compromise E-Mails schnell einzudämmen.
Tausende globale Unternehmen im Bereich Verteidigung, Energie, Finanzen, Gesundheitswesen und Fertigung profitieren bereits durch angepasstes Mitarbeiterverhalten von der Möglichkeit, schneller auf Vorfälle reagieren zu können und das Risiko von Sicherheitsverstössen zu vermindern.

COFENSE

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

Weitere Informationen finden Sie unter **www.cofense.com.**