



Cofense PhishMe は従業員が phishing 攻撃に侵されないよう条件付けしますが、「クリックしない」だけでは不十分です。phishing 攻撃では、早期発見が物を言います。セキュリティ運用およびインシデント応答チームにとって、攻撃者がネットワーク上にいる時間を最小にするために、可視性は決定的に重要です。Cofense Reporter™ は、組織に対し、サイバー攻撃の初期段階を示すものかもしれない不審メールについてユーザーがレポートを作成する、シンプルで費用対効果の高い方法を提供します。

## 「なぜ Cofense Reporter™ を選ぶか

Cofense は、従業員が高度サイバー攻撃の手に陥る脅威を最大 95%軽減し、巧妙な phishing 攻撃を認識して抵抗するための最後の防衛ラインとなることを証明しています。

### 主な利点

- ✓ ユーザーレポートの作成プロセスを標準化し体系化する
- ✓ ユーザーからの報告を使って、電子メールベースの脅威をより迅速に検出し、対応する
- ✓ サードパーティ製品との統合を使用して URL とマルウェアの添付ファイルを分析する
- ✓ 先を見越した対応と可視性の向上によって違反の影響を最小限に抑える
- ✓ カスタマイズ可能なユーザーへのフィードバックが、従業員にセキュリティプロセスの一部となることを促す



## 「Cofense Reporter™ って何?

プロキシフィルタリングや URL 書き換え、DLP のような技術的防御が失敗したとき、防衛の最後のとりではユーザー自身です。適切な訓練を受けて武装したユーザーは、不審メールを認識して報告するだけで、タイムリーで価値ある脅威インテリジェンスを提供することができます。組織はこのリソースの活用ができずに苦勞しており、その結果、悪意のある行為はしばしば、ネットワーク上で数週間から時には数か月にわたって活動することもあります。

Cofense Reporter は、ユーザーの電子メールツールバーに電子メールアドインをインストールすることで、報告プロセスを簡素化します。すなわち、クリックするだけで、分析と対

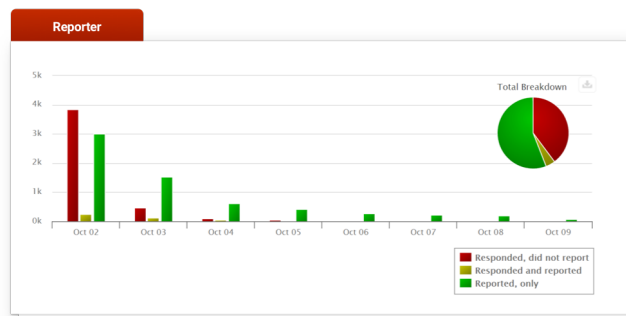
応に必要な関連情報を含む不審な電子メールがセキュリティチームに送信されます。

Reporter は、Cofense PhishMe のシナリオから報告された電子メールと、未知のソースから報告された電子メールを自動的に識別し、悪意のある可能性のある電子メールの報告だけが、適切なセキュリティスタッフまたは Cofense Triage に分析のため配信されることを確実にします。

## 拡張レポート

社内に報告プロセスが整っているか否かにかかわらず、Reporter は次の方法で改善に役立ちます：

- 報告された電子メールの完全なヘッダーを保存すると共に、応答者が同様の電子メールをブロックして削除できるようにする。
- 添付ファイルやURLが含まれているか確実にする。
- Simulator キャンペーンを補完し、ユーザーの応答と組織の応答時間を追跡する。



## このメールは Cofense のシナリオですか？

はい。そうです。

Cofenseのユーザーレポートに記録する

「ありがとう」ダイアログユーザーを表示する



「ボタンを押すとどうなるだろうか...?」

いいえ。本物です。

IRIにメールを報告する

「ありがとう」ダイアログユーザーを表示する

分析と対応決定のため、TRIAGEか社内セキュリティチームに送信する

## PhishMe Simulator メール

Reporter は、PhishMe から送信された電子メールの報告を収集し、どのユーザーが報告したかを記録し、達成した報告のカスタマイズ可能な受取確認をユーザーに提供します。フィードバックループでの陽性強化によって、サイバー攻撃を正確に識別する従業員の能力はさらに強化されます。この情報は追跡され、Cofense ソリューションの包括的なレポートメトリックに統合されます。

## 不審な不明メール

出所の分からない不審メールの報告は、指定された場所または Triage に転送され、そこで組織の内部セキュリティチームによって分析されます。不審メールには、迅速な分析のために元のヘッダーとコンテキスト情報が添付されます。インシデント対応およびセキュリティ運用チームは、Triageを使用する際に、他の特性の中から phishing の企てを正確に特定するというユーザーの信頼性に基づいて、分析の優先順位をつけることができます。

Cofense(旧PhishMe)は、人間主導型のフィッシング防御ソリューションを全世界的に提供する大手プロバイダーです。私たちは、能動的な電子メールの脅威に対する組織を挙げた取り組みを可能にすることで、サイバーセキュリティに対する協調して対応するアプローチを提供します。

当社の集成的防御スイートは、最上級のインシデント対応技術を、従業員からもたらされたタイムリーな攻撃情報と組み合わせます。Cofenseのソリューションは、スパイフィッシング、ランサムウェア、マルウェア、および業務電子メール漏洩の影響を素早く軽減します。今やこれは、国際的組織、企業にとってすべて現実となっています。より詳しくは、www.cofense.comをご覧ください。



W: [cofense.com/contact](https://www.cofense.com/contact) T: 703.652.0717

A: 1602 Village Market Blvd, SE #400  
Leesburg, VA 20175