こんなの見たことない！

これは、斬新なサイバーセキュリティー教材だ！

最近の高度サイバー攻撃は、パスワードの窃取など人の心理的な弱みにつけこんだ騙しのテクニックによるものが多く、ひとりひとりの自覚を高める以外に防ぐ手段はありません。このコンテンツは誰でも飽きずに、興味を持って取り組むことが出来る卓越した教材です。

＜6つのテーマ＞

1 ソーシャルエンジニアリング
2 パスワード
3 モバイルデバイス
4 物理アクセス
5 メール
6 内部脅威

本教材はインターネット環境により、e-learning 教材をサブスクリプションとして提供します。

各テーマは、約 20 分程度のコースで、最後に 20 問の確認テストがあります。各社の管理者の方には受講者の進捗情報および終了された方の「修了証」を発行いたします。テレワークによりご自宅などでも実施可能です。C4E 社の得意なインタラクティブなコンテンツであり、飽きずに実施することが可能です。新入社員などの社員教育にご利用ください。

※ 2021 年 10 月リリース予定。 定価 6,000 円＠1アカウント
（人数と期間によりディスカウントあり、見積りします）

製品・サービス、見積りなどについてのお問い合わせは

株式会社 エヴァアビエーション

詳細はこちら https://www.EvaAviation.com E-mail ： sales@EvaAviation.com

データ窃取は、コンピューターをハッキングすることから始めるのではなく …

… 「人」をハッキングすることから始めます！

新しい脅威には、新しいタイプの防御が必要です。
ヒューマンファクターサイバーセキュリティです。

ヒューマンファクターサイバーセキュリティは、従業員がコンピュータネットワークを保護するための「知識と行動」と定義されます。これは、従業員が実施できるネットワークセキュリティのひとつです。

データの盗難または破壊につながるサイバー攻撃の 91%以上は、従業員から始まります。

ほとんどのサイバー攻撃は、無意識のうちにまたは故意に、攻撃者をネットワークに侵入させた従業員から始まります。コンピュータセキュリティソフトウェアが高度化するにつれて、ハッカーは、トレーニング不足、不注意な従業員、もっと悪いことに、会社のセキュリティ機能を乗り越えることができる従業員を見つければ良いと気づいています。サイバー攻撃が成功するたびに、**企業は平均3億円以上の損害が生じています。**

「人」への脅威に対抗するために、ヒューマンファクタートレーニングがあります。

Comar Cyber の創設者は、CIA ヒューミントインテリジェンス（HUMINT)の運用責任者として、さまざまなサイバーセキュリティプロジェクトに取り組んできました。彼は、ほとんどのサイバー攻撃が成功したのは、ハッキング技術が高度なためではなく、人間の知性の世界で見られるのと同じタイプの騙しのテクニックを使用するためであることを経験しました。

攻撃者は、騙せる可能性のある、または目に見えないため脅威など存在しないと考えてセキュリティを軽く見ている従業員“ターケット”を見つけます

我々は、ネットワークを脆弱にしたのはネットワークの技術的要因ではなく、人的要因であることに気づきました。新しいヒューマンファクターの脅威に対する唯一の防御策は、人間のトレーニングです。Comar Cyber のスタッフは、長年の経験からそのことを良く知っています。

https://comarcyber.com/