ランサムウェアによる不正アクセス、身代金要求、情報流出…
貴社を狙ったサイバー攻撃の多くは「標的型メール」から始まります。

MS&AD

標的型メール訓練サービス のご案内

訓練を受けたことがない社員は、不審なメール・興味を引くメールを安易に開封してしまいがちです！
海外現法を踏み台にして日本本社や取引先を攻撃する手口が増えており、対策を強くお勧めします！

＜標的型メールとは＞
機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃です。巧妙に業務関連のメールを装ったウイルス付きメール（標的型メール）を、組織の担当者に送付する手口が知られています。標的型メールによる被害を防止するためには、メールを受信する社員への教育（典型的な手口、万一開封してしまった際の対応）が欠かせません。

★本サービスのあらまし

- 疑似的な標的型メールを貴社の社員に送信し、受信者がメール本文にあるURLをクリックしたかどうかを集計します。
- 訓練で用いるメールは、中国でよく使われる手口を参考に、**騙されやすい巧妙な文章**を**中国語**で作成します。
- メール文案は、お客様毎にカスタマイズ可能です。社内用語を用いて社内関係者を偽装することも可能です。
- 開封率は、貴社のご要望に応じて部署別・役職別等で集計し、事後の社員教育に活用いただきます。
- サービス実施後には、評価レポートを**日本語・中国語**でご提出します。
- お預かりする社員情報（メールアドレス等）は万全のセキュリティ体制で管理し、サービス提供後は速やかに廃棄します。
- メール送信、集計等のサービスサイトは、**京セラ信息系統（上海）**の協力を得て構築しています。

★実施フロー

申し込み	訓練準備	訓練メール発信	集計・分析	評価レポートご提出
	・メール文案の作成 ・送信対象者の確定 ・対象者メアドの受領			・開封者の特定 ・開封率分析（部門・役職別等） ・事後対策のご提案

★ご利用にあたっての注意点

- 貴社メールシステム上、本サービスによる訓練メールが迷惑メールフィルタ等で遮断される場合、個別のシステム対応（ホワイトリスト機能等がある場合には予め訓練メールアドレスを追加等）をお願いするケースがあります。
  また、メール文中のURLに自動的にアクセスするようなセキュリティ機能（サンドボックスなど）がお使いのメール製品に組み込まれているか、個別に導入している場合、訓練結果を正しく集計できない場合があります。
  （**貴社メール環境等によっては、本サービスによる訓練が実施できないことがありますので、あらかじめご了承ください。**）

★ご利用料金

- 送信先**500**名まで、**15,000元～**（＋税）／回　（送信先が500名を超える場合は個別にお見積します）

★お問合せ・お申込み先

瑛得管理咨詢（上海）有限公司（インターリスク上海）
☎ 021-6841-0611　担当：阿部、張若亭（日本語可）
✉ inquiry@inter-shanghai.com.cn

【合作公司】 KYOCERA
京瓷信息系統（上海）有限公司