ビジネスメール詐欺

サプライヤーセキュリティ警告

MSD は詐欺防止と情報保護に真剣に取り組んでいます。

バーチャルコミュニケーションへの依存度が高まるにつれ、ビジネスメール詐欺（BEC）事件が増えています。BECは、電子メールその他の電子通信を使用して、役員、従業員、またはその他の権限のある人物になりすまします。
そして企業として不当に支払いを請求したり、従業員の給与計算システムやW2(米国のみ)
情報に不正にアクセスしたりします。

知っておいていただきたいこと

MSD は御社のビジネス情報と銀行情報の保護に取り組んでいます。当社では、グローバル・プライバシー・オフィス、情報テクノロジーのプロセスとガイドライン、そして地域の規則に準拠して、トレーニングを受けたスタッフが厳格なプロセスと管理の下、データを収集、検証

、取得しています。その手続きと業務については複数のチェックポイントを設け、定期的に監査を実施しています。

御社のビジネスを守るために:

- セカンダリチャネルまたは2ファクタ認証を使用して、アカウント情報の変更要求を個別に検証します。
- 電子メールに記載されているURLが、発信元とされる企業に関連付けられていることを確認します。
- 実在のドメイン名にスペルミスのあるハイパーリンクがあれば警告します。
- 特にモバイルデバイスまたはハンドヘルドデバイスを使用している場合は、電子メールの送信に使用される電子メールアドレスを確認し、送信元と照合します。
- 侵入検知システムフィルターを導入して、会社の電子メールのように見える拡張子を持つ電子メールにフラグを付けます。たとえば、正当な eo@abc_company.com というアドレスは、ceo@abc-company.com の詐欺メールとしてフラグが立てられます。
- 預金の消失などの異常がないか定期的に金融口座を監視します。
- すべてのソフトウェア・パッチを有効にして、すべてのシステムを更新します。
- 従業員の使用するコンピューターをチェックして、電子メールの拡張子がすべて表示される設定になっているか確認します。
- 地域の解決センター
  の連絡先情報を把握しておき、MerckまたはMSDに関連してBECの被害に遭ったと思われる場合に通知します。または地元の法執行機関に連絡します。