法人を狙った「ビジネスメール詐欺」等に注意！

取引先や自社の社長・役員・社員になりすました詐欺メールを送信し、従業員に対して送金を促す等の「ビジネスメール詐欺」が発生しています。企業・団体におかれましては、社内で詐欺手口を共有いただき、十分にご注意いただきますようお願いします。

「ビジネスメール詐欺」とは

取引先や自社の経営者(社長・役員)、自社の社員等になりすまして、偽の電子メールを送信して国内外への送金等を促し、資金を搾取する手口

【対応策】

①送金先の変更や緊急の送金を促すメールなど、送金に関するメールを受信した際には送信元への返信や相手から指定された方法では無く、相手（社長等）の真正な連絡先を自身のアドレス帳などで確認し、電話等別の方法で連絡する

②添付ファイルやリンク先を不用意に開かない

③ウイルス対策ソフト、ＯＳを最新の状態に更新する

④個人情報を送信しない

「ビジネスメール詐欺」の手口の一例

1. 法人の経理担当者宛に社長や役員を騙る人物からのメールが届き、メールにてLINEグループの作成を指示される
2. 経理担当者がLINEグループを作成すると「急いで送金するように」とのメッセージが届き、経理担当者はその指示に従い、法人インターネットバンキング等により他行法人口座宛の送金を実施

なお、上記以外にも法人を狙った詐欺が確認されていますので、今一度、手口をご確認ください。

PCサポート詐欺

1. パソコン画面にウイルス感染を装ったポップアップを表示させ警告音を鳴らす
2. パソコン画面に偽のサポート窓口の電話番号を表示させ、電話するよう誘導する
3. ウイルス除去のためと偽り、遠隔操作が可能なソフトウェアをインストールさせる
4. 「ウイルス除去費用」等と言われ、犯人が遠隔でパソコンを操作し、不正に送金させる

フィッシング詐欺

1. 銀行やクレジットカード会社などを騙り「取引制限のお知らせ」等、不安を煽るタイトルの電子メール・ショートメッセージを送り付ける
2. インターネットバンキングのログイン画面を精巧に模倣した偽ホームページに誘導
3. インターネットバンキングのIDやパスワード、カード番号等の情報を入力させ、本人が気付かないうちに不正送金される

ボイスフィッシング詐欺

1. 銀行からのサポートを騙る自動音声電話がかかり、インターネットバンキングの契約情報の更新を求める
2. ガイダンスに従い電話に応答すると、電話が自動音声から犯人に代わる
3. 犯人からメールアドレスを求められ回答するとフィッシングサイトのURLが記載されたメールが届き、契約情報の入力を指示される
4. フィッシングサイトへ情報を入力した後、犯人から電話が入り、インターネットバンキングの操作を案内され、不正に送金させる