令和８年１月

お客さま 各位

諏訪信用金庫

社長や役員になりすました詐欺メールにご注意ください

現在、企業の社長や役員になりすました詐欺メール（いわゆる CEO 詐欺※）が全国で多発しており、実際の被害も発生しております。

この詐欺は、経営者や上司を装って従業員に対し、金銭の振込、機密情報の提供、SNS グループの作成などを指示するものです。企業だけでなく、個人のお客さまに対しても同様の詐欺メールが送信されていることが確認されています。

不審なメールを受け取った場合は、十分にご注意いただきますようお願い申し上げます。

※社長など最高経営責任者である「チーフ・エグゼクティブ・オフィサー（Chief Executive Officer）」になりすまして、従業員や取引先を騙し、金銭や機密情報を詐取する詐欺手口

1. 詐欺メールの主な手口

・経営者や上司になりすまし、「至急対応が必要」として振込や情報提供を求める
・本物に似たメールアドレスを使用し、正規の連絡に見せかける
・LINE などの SNS グループ作成を指示し、外部サービスへ誘導する

2. 具体的な事例

【事例１：振込を指示する詐欺】
件名：至急振込してください
差出人：社長を装った偽アドレス
内容：商談に必要なため、至急振込をお願いします。手続きは後回しで構いません。戻ったら説明します。振込先：〇〇株式会社 金額：〇〇,〇〇〇,〇〇〇円

※「至急」「会社に戻ったら説明する」などは詐欺メールでよく使われる言い回しです。

【事例 2：LINE グループ作成を依頼する詐欺】
件名：社名を記載した偽メール
差出人：社長を装った偽アカウント
内容：お疲れ様です。業務利用のため、新しい LINE グループを作成してください。完了したら招待 QR コードを返信願います。代表取締役社長 〇〇

※会社で通常使用しない外部 SNS への誘導は要注意です。
※QR コードを通じて LINE グループに侵入後、マルウェアを仕込んだサイトへの誘導、不審なソフトのダウンロード、個人情報や口座情報の詐取、インターネットバンキングによる不正送金などが行われます。

3. 被害に遭わないためのポイント
・差出人のメールアドレスを必ず確認する
・内容に不自然な点があれば、正当な相手（自社の社長等）に直接電話で確認する
・メール本文の URL や添付ファイルを不用意に開かない
・LINE など SNS グループの作成指示には安易に従わない
・不審なメールには返信しない
・口座情報や個人情報を安易に教えない

万一、QR コードの送信やメール・LINE のやり取りを始めてしまった場合は、直ちに中止してください。不審な点がございましたら、最寄りの当金庫店舗または下記までご連絡ください。

本件のお問合せ先
諏訪信用金庫
総務部コンプライアンス課
TEL：0266-23-4572

諏訪信用金庫
SUWA SHINKIN BANK