

お取引様 各位

2022年2月10日

株式会社タカトリ

弊社社員を装った不審メールについて

平素は格別のご高配を賜り、厚く御礼申し上げます。

この度、弊社従業員を装った不審メールが、複数の方へ発信されている事実を確認いたしました。

現在、本件について、地元警察の協力を得ながら詳細な調査を行っております。

当該不審メールに添付されたファイルを開くことによりコンピュータウイルスへの感染や不正アクセスの恐れがございます。

疑わしいメールが届きました際は、以下の見分け方を参考にいただき、添付ファイルの開封をせず、メールごと削除していただきますようお願い申し上げます。

もし、誤って ZIP ファイルの解凍、エクセルファイルを開けてしまった場合には、速やかにネットワークを切断していただき、アンチウイルスソフトによる全ドライブのスキャンの実施をお願い致します。アンチウイルスソフトのバージョンによっては、ウイルスの検知・隔離ができない場合もありますので、PCの初期化を推奨させていただきます。

※アンチウイルスソフトがインストールされていない場合にもPCの初期化を推奨致します。

【不審メールの見分け方】

弊社で確認しております、不審メールは以下の内容です。

- ・差出人(from:)の表示が弊社社員名ですが、メールアドレスが異なります。
- ・送信元のドメインが takatori-g.co.jp の場合は、弊社からの正規のメールとなります。
- ・添付ファイルは、.xls、.zip が確認されております。
- ・件名(subject:)が受信者名になっているケースが多く発生しております。
- ・これ以外のパターンも存在する可能性があります。

不審メールの例

From: <弊社社員名(役職名の場合もあります)> <メールアドレス:mailto以下が本来のアドレスとは異なります>
Sent: Thursday, February 3, 2022 11:23 AM
To: <受信者名>
Subject: <RE:, FWD: などの件名>

以下メールの添付ファイルの解凍パスワードをお知らせします。
添付ファイル名: 2022-02-03_1223.zip
解凍パスワード: MIUxI ■

ご確認をお願いします。

<署名: 差出人と同じ名前になってます>
Tel 044-405-7777 Fax 044-324-7777
Mobile 090-4469-7777
Mail <メールアドレス: 差出人の正規のアドレスです>

※メールソフトにより、表示は異なります。

ご迷惑をお掛け致しますが、よろしくお願い申し上げます。