

# 不審なメールへの対処法

サイバー犯罪から組織を守るためには、不審なメールにどのように対処するべきかを学ぶことが不可欠です。不審なメールに正しく対処できなければ、フィッシングの被害に遭う恐れがあります。

以下のヒントを参照して、不審なメールに正しく対処できるようにしてください。

## 不信なメールには返信しない

不審なメールであっても知人から送信されているように思われる場合、つい返信して確認したくなるものです。しかし、メールに返信すると、セキュリティ上のリスクが高まる可能性があります。メールアカウントが乗っ取られている場合、返信してきたユーザーはおそらくあなたが考えている知人ではないはずです。あなたは、サイバー犯罪者とやりとりしている可能性があります。

## 不信なメールは転送しない

リンクや添付ファイルに不審な点があれば、決してクリックしたり開いたりしないことがベストプラクティスです。しかし、フィッシングメールに騙されて、悪意のあるリンクをクリックしたり、悪意のある添付ファイルを開いたりすると、リンクや添付ファイルが思わぬ動作をする場合があります。たとえば、一見画像のように見える添付ファイルを開くと、インストールウィンドウが開く場合もあります。また、悪意のあるリンクをクリックすると、偽のログインページにリダイレクトされる場合があります。

リンクや添付ファイルに不審な点がある場合には、同僚にメールを転送して相談したいと思われるかもしれませんが、同僚にそのようなメールを転送すると、リスクを拡散する恐れがあります。リンクをクリックしたり、添付ファイルを開いたりした場合に、通常とは異なる処理が実行されたら、レッドフラッグだと考えてください。通常とは異なるメールや不審なメールは他のユーザーに転送しないでください。フィッシングメールを転送すると、その同僚もフィッシングリンクをクリックする可能性があるため、セキュリティ侵害のリスクが高まります。

## 不審なメールをスパムとしてマークしない

通常、スパムメールは迷惑な広告です。スパムメールは迷惑なものですが、通常は無害です。しかし、フィッシング攻撃は、正規のメッセージを装った悪意のあるメールです。フィッシングメールには通常、リンクをクリックする、添付ファイルを開く、お金を振り込むなど、ユーザーによる行動を促す内容が含まれています。

不審なメールをスパムとしてマークすると、同じ送信者からの他のメールと共に別のフォルダに移動されます。つまり、不審なメールをスパムフォルダに移動すると、そのメールは見えなくなります。しかし、問題が解決されたわけではありません。

## 安全を維持するためのヒント

不審なメールを受け取った場合、組織のITチームに報告することが一番です。メールを報告すれば、ITチームはその脅威を評価し、その影響を回避・軽減できます。

不審なメールを受信したら、以下のヒントを参照して安全を確保してください。

- 不審なメールを報告するときには、組織のプロセスに従ってください。サイバーセキュリティ対策の所定の手続きに従うことで、すべてのユーザーの情報を安全に維持できます。
- 不審なメールを報告する方法がわからない場合は、メールを受信トレイに置いたまま、マネージャーや上司に相談してください。
- スパムかフィッシングかわからない場合は、メールを報告し、ITチームに対応を任せてください。