サイバーセキュリティ・ニュース
CS－NEWS

令和３年２月
サイバー犯罪対策課

だまされないためには、〝知っている〟ことが大切！

「フィッシング詐欺」にご注意

「フィッシング詐欺」とは、実在する有名企業をかたるメールを使って「偽のウェブサイト（フィッシングサイト）」へ誘導し、銀行口座やクレジットカード情報などの重要な個人情報をだまし取る行為のことを言います。手口は年々巧妙化し、私たちの心理をついてくるものが多くなっています。被害に遭わないためにも、手口を知り、対策を理解することが大切です。

フィッシング詐欺の手口

1 犯罪者がフィッシングメールを不特定多数に送信

2 受信者がメールを開封し、メール内のURLにアクセス

3 偽サイトでアカウント情報やクレジットカード情報を入力させる

偽サイト（フィッシングサイト）

「フィッシング詐欺」にだまされないために

1. 身に覚えのないメールは不用意に開かない。
2. メール内のURLを安易に押さない。
   （ID・パスワードの入力や、アプリのダウンロードを促すものは要注意）
3. 正しいウェブサイトのURLは事前にブックマークに登録し、アクセスする際は必ずブックマークからアクセスする。
4. ログインの際、多要素認証※を使っているサービスを利用する。
   ※多要素認証…本人確認を強化するため、パスワードに加えて複数の種類の要素（指紋や顔、合言葉など）を使う認証方式。
5. 万一、不審なウェブサイトでパスワードなどを入力した場合は、警察安全相談電話や国民生活センター、地域の消費生活センターなどに相談する。

警察安全相談電話　☎#9110
（つながらない場合は☎059・224・9110）
相談受付：9時～17時（土日祝日・年末年始を除く）


三重県警察
マスコットキャラクター
ミーポくん

テレワークも注意しましょう！

テレワークが急速に普及する中、サイバーセキュリティ対策を怠ると、パソコンなどのウイルス感染や重要なデータの流出につながります。下記の安全確認を徹底しましょう。

- パソコンのOSやウイルス対策ソフトは、常に最新の状態に更新する
- 自宅のWi-Fiルータを使う場合は、ルータのIDを初期設定から必ず変更する
- 知人や取引先を装うメールに注意し、安易に添付ファイルを開かない

2月1日（月）から3月18日（木）は サイバーセキュリティ月間です

この月間にあたって、サイバーセキュリティ対策を見直しましょう。対策に関する詳細は、県警察本部ホームページをご覧ください。

三重県　サイバー　Q検索

問い合わせ先　県警察本部 生活安全部 サイバー犯罪対策課　☎ 059・222・0110（代表）

「県政だより みえ（令和３年２月号）から引用」

三重県警察本部　サイバー犯罪対策課