

【消費生活の窓口から】

その URL のクリック、ちょっと待って！

～SMS やメールでの“フィッシング詐欺”の相談が依然高水準！～

全国的に、事業者や組織をかたる SMS（ショートメッセージサービス）やメールを送信し、パスワードや ID、暗証番号、クレジットカード番号などの個人情報を詐取した上、クレジットカード等を不正利用するフィッシングに関する相談が多く寄せられています。フィッシング対策には日頃からの心構えが重要です。以下のチェックリストを活用し、より一層気を付けましょう。

フィッシング対策のチェックリスト

<事業者や公的機関などのSMSやメールを見るときは>

- ★日頃利用している事業者等からでも、まずフィッシングを疑う
- ★記載されている URL にはアクセスせず、事前にブックマークした正規のサイトの URL や、正規のアプリからアクセスする
- ★事前のブックマークがない場合や、少しでも不安に思う点があれば、事業者等の正規のサイトでフィッシングに関する情報がないか確認する

<フィッシングサイトにアクセスしたと気づいたら>

- ★ID・パスワード、クレジットカード番号等は絶対に入力しない
- ★フィッシングサイト上のアプリをダウンロードしない

<フィッシングサイトに情報を入力してしまったら>

- ★同じ ID・パスワード等を使い回しているサービスを含め、すぐに変更する
- ★クレジットカード会社や金融機関などに連絡する

<日ごろからの事前対策>

- ★セキュリティソフトや携帯電話会社の対策サービス等を活用する
- ★ID・パスワード等の使い回しをしない
- ★クレジットカードやキャリア決済、インターネットバンキングの利用明細はこまめに確認する
- ★あわせて、利用限度額を確認し必要最低限の金額に設定する

〈事例〉・大手通販サイトから携帯電話にメールが届き、月会費 550 円が引き落としにならなかったと書いてあった。「会員ログイン」という記載があったのでタップして遷移したところ、切り替わったページにはクレジットカード番号を入力する欄があったので入力した。しばらくして、クレジットカード会社から連絡があり、第三者に 5 万円不正利用されたことがわかった。（年代不明 女性）

・宅配業者から不在通知の SMS が届き、詳細を確認するために記載されていたリンク先の URL からログインしてパスワード等を入力した。その後、キャリア決済で身に覚えのない 15,000 円が課金されていたことが分かった。（50 歳代 女性）

- ・自分が利用している銀行からスマートフォンにメールが届いた。利用制限を告げる内容やリンク先の URL が記載されていたので、フィッシングメールとは気付かずに URL をタップし、本物の画面と思って契約番号、パスワードを入力した。その後、銀行の残高が 0 円になっていて驚いた。別の口座に 20 万円の送金履歴があるとのことだった。
(40 歳代 女性)

【アドバイス】

◆不安に思った場合は、消費生活相談窓口か消費者ホットライン^{い や や}188（局番なし）に相談しましょう。

※詳しくは、国民生活センターホームページ「[その URL のクリック、ちょっと待って！－SMS やメールでの“フィッシング詐欺”の相談が依然高水準！－](#)」をご覧ください。

※ご相談・お問い合わせ先

中山町消費生活相談窓口（住民税務課 住民G内） ☎ 6 6 2 - 2 5 9 3