消費者啓発参考情報「くらしの１１０番」トラブル情報

個人情報は渡さない！本物っぽい偽メールによるフィッシングに注意

【事例１】

「銀行口座を凍結したので再開手続きが必要」という通知がＳＭＳで届いた。口座を持っている銀行だったので慌ててＵＲＬをクリックし、現れた画面に名前、住所、電話番号、口座番号、暗証番号などの個人情報を入力した。後日、その銀行から「口座に消費者金融から１００万円が振り込まれ、すぐ出金された」と連絡があった。

【事例２】

実在する生命保険会社から「ＡＬＰＳ処理水放出による健康被害を保障します。診断により一千万円の前払いをします。定員があるので申請はお早めに」というメッセージとともに、申請先ＵＲＬが記載されたメールが届いた。最近、処理水についてよく耳にするが、本当だろうか。

実在する企業、銀行、通販サイト、通信会社、宅配業者、公的機関などを装ってＳＭＳ（ショートメッセージサービス）やメールを送り、個人情報をだまし取る「フィッシング」の相談が寄せられています。

メールの件名を【重要】【至急】としたり、「料金未納」「不正使用」といった文言で消費者の不安をあおる以外にも、話題性のあるキーワードを用いるなど次々とメールの内容を変えますが、基本的な手口は同じです。①消費者の関心を引いてメールを開かせ、②メッセージ内に仕込んだＵＲＬをクリックさせ、本物そっくりな偽サイトへ誘導し、③クレジットカード情報やＩＤ、パスワード、暗証番号などの個人情報を入力させ、④情報を不正使用して金銭をだまし取ります。なお、ＵＲＬクリック後、不正アプリをインストールさせる手口もあり、注意が必要です。

【消費者へのアドバイス】

1. 慌てず冷静に対応することが大切です。普段から取引がある、心当たりのある相手からのＳＭＳやメールであっても、開く時には注意を払いましょう。
2. 金銭のやり取りをする、個人情報の入力を促すような内容には警戒してください。メールに記載されたＵＲＬにはアクセスせず、公式サイトを調べたり、実存の店舗等に問い合わせましょう。
3. 偽サイトにアクセスしてしまった場合、個人情報は絶対に入力しない（アプリはインストールしない）で、すぐサイトを閉じてください。
4. 日ごろから、正規のＵＲＬをブックマークする、正規アプリを利用するようにしましょう。

困った時には、お近くの消費生活センター等にご相談ください。

消費生活センターへのお電話は、消費者ホットライン「188」へお掛けください。

（くらしの110番　2023年9月）