実在する企業や組織を装うフィッシングメール

【問】

①大手通販サイトから「登録しているクレジットカードの有効期限が切れました。クレジットカード情報を更新してください」とのメールが届いた。よく利用している通販サイトからのメールだったので不審に思わず、メールに記載されているＵＲＬをクリックし、ＩＤとパスワード、クレジットカード情報を入力してしまった。その後、クレジットカードを不正利用されてしまった。　　（４０歳代女性）

②スマートフォンに配送業者から「荷物をお届けにあがりましたが、留守のため荷物を持ち帰りました」とのショートメッセージが届いた。ちょうど通信販売で注文した商品が届く予定があったので、再配達を依頼するために、ショートメッセージに記載されていたＵＲＬをタップした。すると、画面にIDやパスワードの入力フォームが表示されたが、よく分からなかったので、画面を閉じた。冷静に考えると、配送業者からの不在連絡票が郵便受けに投函されておらず不審だ。　　（６０歳代男性）

～安易に指示に従わない～

【答】相談事例のように、実在する通販サイトや配送業者、クレジットカード会社、携帯電話会社などの企業や、時には税務署などの公共機関など実在する組織を装い、クレジットカード情報や決済に必要なＩＤ、パスワード、暗証番号等を詐取するメール（フィッシングメール）に関する相談が、依然として多く寄せられています。

フィッシングメールに記載されているＵＲＬにアクセスすると、企業の公式ホームページと見誤ってしまうようなそっくりの画面が表示され、個人情報を入力するよう求められます。しかし、この偽サイトに、指示通りに、クレジットカード情報やキャリア決済に必要なＩＤ、パスワードなどを入力してしまうと、第三者にクレジットカードやキャリア決済を不正利用されるおそれがあります。

利用したことのあるサイトや知っている企業からメールが届いても、メールの文面に記載されたＵＲＬにはアクセスせずに、まずはその企業の正規のホームページを確認し、フィッシングメールに関する注意喚起がされていないか、届いたメールの送信元のアドレスが企業のアドレスで間違いないか確認しましょう。

もし、偽サイトに入力してしまった場合は、早急にパスワードを変更し、クレジットカード会社やキャリア決済事業者に確認し、不正な決済履歴がないか確認してください。

また、スマートフォンでフィッシングメールに記載されたＵＲＬにアクセスすると、アプリをインストールするよう求められるケースもあります。うっかり指示通りにインストールしてしまうと、スマートフォンを乗っ取られたような状態になり、相談者のスマートフォンから勝手に大量のショートメッセージが送信されて、高額な通信料が発生してしまったという事例もあります。

提供元不明のアプリは、インストールしないでください。インストールしてしまった場合は、安全のためスマートフォンの初期化が必要となる可能性があります。

フィッシングメールの手口は巧妙化し、文面やＵＲＬから偽のメールと判断することが難しくなってきています。

メールが正規のものか判断に迷われる場合や少しでも不安に思われた場合は、消費生活センターにご相談ください。

筆者ひとこと

通販サイト、クレジットカード会社、官公庁などさまざまな組織を装い、本物と見誤るようなフィッシングメールが送られてきます。「変だな」と思ったら、メールを開封せず、発信元に確認するようにしましょう。発信元への連絡が難しいときなども、消費生活センターにご相談ください。（県消費生活センター）