国民生活センター相談情報部

第48回

通販サイトなどをかたる フィッシングの手口にご注意！

相談事例

通販サイトから「支払い方法に問題がある」とのSMSがスマートフォンに届いた。疑いもせず指示どおりに添付のURLをタップし、クレジットカード番号や住所を入力した。その後、クレジットカードの請求明細を確認したら、合計約4万円の身に覚えのない決済があった。クレジットカード会社には状況を伝えたが、今後どうしたらよいか。（30歳代　男性）

●問題点とアドバイス

通販サイト、クレジットカード会社、宅配便業者などの実在する組織をかたる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等の個人情報を詐取するフィッシングに関する相談が寄せられています。

フィッシングの手口では、「支払い方法に問題がある」といった、消費者の不安をあおるメールやSMSが送られてきます。普段よく利用する事業者からのメッセージに見えても、実は危険なフィッシングの手口かもしれません。

(1) メールやSMSに記載されたURLには安易にアクセスしない！

消費者の不安をあおるフィッシングの手口には、焦らず冷静に対応することが大切です。SMSやメールに記載されたURLはフィッシングサイトにつながる可能性があるため、安易にアクセスしないでください。

フィッシングサイトにアクセスしてしまった場合、パスワードやID、暗証番号、クレジットカード情報、認証コード等の個人情報の入力を求められるケースがあります。こうした情報をフィッシングサイトで入力してしまうと、クレジットカードやキャリア決済などを不正利用されるおそれがあります。万が一こうしたサイトにアクセスしてしまった場合でも、個人情報は絶対に入力しないでください。

(2) フィッシングサイトにID・パスワード等を入力してしまったら……

フィッシングサイトにパスワードやID、暗証番号、クレジットカード情報等を入力したまま放置すると、クレジットカードやキャリア決済などを不正利用されてしまう状態が続きます。こうした重要な情報をフィッシングサイトに入力したと気づいた場合には、すぐにID・パスワード、暗証番号等を変更し、クレジットカード会社や携帯電話会社などにも連絡しましょう。

(3) ブックマークした正規のURLや正規のアプリからアクセスしましょう

フィッシングの被害にあわないために、ブックマークした正規のURLや正規のアプリからアクセスすることを日頃からの習慣にしましょう。また、定期的にブックマークが正しいものかを確認しましょう。

参考：国民生活センター「通販サイト、カード会社、宅配便事業者などをかたる偽SMS・メールに警戒を！－身近な事業者からの不安なメッセージ、じつは危険な“フィッシング”かも－」（2022年12月21日公表）https://www.kokusen.go.jp/news/data/n-20221221_2.html