SMS やメールでのフィッシング詐欺に注意！

実在する組織をかたる SMS やメールを送信し、ID やパスワード、暗証番号、クレジットカード番号等、個人情報を詐取したうえ、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。

事例を紹介します。

・ 宅配業者名で SMS が届いた。ちょうど荷物が届く予定だったので、SMS に書かれていた URL をクリックして、記載されていた指示どおりに、ID やパスワード等を入力した。しかし、その後11万円を不正利用されていたことが分かった。（60歳代）

・ スマートフォンに「ETC カードを更新するように」とのメールが頻繁に入るようになった。所有しているクレジットカード会社発行の ETC カードの手続きが必要なのかと思い、URL を開いてメールアドレスやパスワード、クレジットカード番号等を入力した。その後、カード会社に連絡すると覚えのない決済があり、12，000円が利用されていた。（70歳代）

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や正規のアプリからアクセスするようにしましょう。

フィッシングサイトに個人の情報を入力してしまうと、クレジットカードや個人情報を不正利用されるおそれがあります。絶対に入力してはいけません。情報を入力してしまったら、同じ ID やパスワード等を使っているサービスを含め、すぐに変更し、クレジットカード会社や金融機関等に連絡しましょう。

ID やパスワード等の使い回しを避けることで被害の拡大を防ぐことができます。

困ったときは、すぐにお住いの自治体の消費生活相談窓口にご相談ください（消費者ホットライン188）。

参考：国民生活センターウェブサイト