見守り新鮮情報

事例1 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）

事例2 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、カード会社に連絡をすると**覚えのない決済**があり、1万2千円が使用されていた。（70歳代）

SMSやメールでのフィッシング詐欺に注意

ひとこと助言

- 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。
- 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、すぐにお住まいの自治体の**消費生活センター**等にご相談ください（消費者ホットライン 188）。

本文イラスト：黒崎 玄

見守り新鮮情報　第479号（2024年4月11日）発行：独立行政法人国民生活センター