

フィッシング詐欺

大手通販サイトからクレジットカード番号を登録し直すようにとのメールが来たので、記載されていた URL をクリックし名前やカード番号などを入力した。その後、約 1 万円分のカード利用がされていたことが判明した。(80 歳代 男性)



●実在する組織をかたり 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など、個人情報を搾取したうえ、クレジットカードなどを不正利用するフィッシングの手口が多く発生しています。

●記載されている URL には安易にアクセスせず、事業者の正規のホームページでフィッシングに関する情報がないか確認しましょう。日ごろから公式アプリやブックマークした事業者のサイトにアクセスするようにしましょう。

●メールの URL にアクセスし、個人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 やパスワードなど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などに連絡しましょう。

湖南市消費生活センター TEL 0748-71-2360

FAX 0748-72-3788

SMSやメールでの フィッシング詐欺に注意

【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やパスワードなどを入力した。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。

【事例2】スマホに「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、クレジットカード番号などを入力した。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、1万円が使用されていた。



出典：国民生活センター