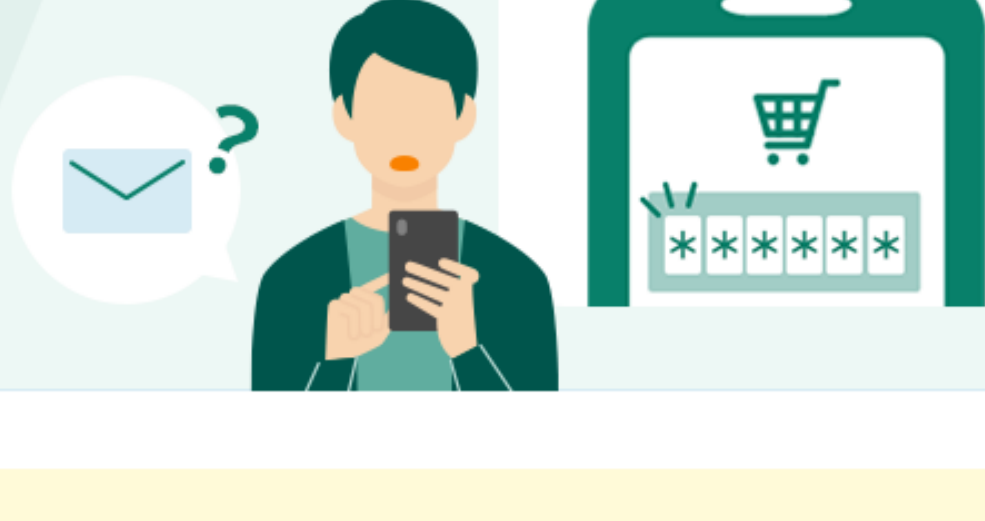


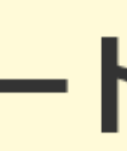
身に覚えのない

認証コードが届いたことはありませんか？



当社からお送りする認証コード（ワンタイムパスワード）をフィッシングサイトに入力してしまい、カードを不正利用されるケースが増加しています。

今回は認証コードを盗まれないための注意点をお伝えします。



認証コードを盗む フィッシング詐欺にあわないために


インターネットショッピングをご利用の際、カード情報に加えて

認証コードの入力が必要な場合があります。

認証コードは登録しているメールアドレス宛に届き、認証画面へ

入力すると決済が完了します。

[ネットショッピング認証サービスの詳細を確認する >](#)

 **当社から「認証コードのご案内」のメールが届いたら**

POINT

ご利用店名・利用金額を確認する

メールや認証画面には、ご利用店名・利用金額を表示しています。

ご自身が利用した内容であるかを確認のうえ、認証コードをご入力ください。

メール

認証画面



⚠ 取引に身に覚えがない場合は、認証コードを入力しないでください。入力した場合、不正な取引が決済されてしまいます。

⚠ 認証コードの入力を求めるメールは、フィッシングメールです

[認証コードを盗むフィッシング詐欺の手口とは？ >](#)



不審なメールにご注意を！

弊社からお送りするメールでは、カード番号等の個人情報をお聞きすることはありません。入力を促すメールはフィッシングメールです。

不審なメールを見分ける3つのポイント



[見分け方の詳細を確認する >](#)

セキュリティ通信編集部員より

最後までお読みいただきありがとうございます。

2023年度のフィッシング詐欺届け出件数は、過去最高の100万件を超え、手口も巧妙化しています。最近では、メールのアカウント情報を盗まれる事案が確認されています。不審なメール・サイトへ、個人情報を入力しないようご注意ください。

[カードのセキュリティ対策 詳しくはこちら >](#)

セキュリティ通信では、今後も会員の皆さまの安心安全なカードライフに役立つ情報をお届けしていきます。

引き続きチェックください！

