セキュリティ通信

2分で分かるフィッシングメール対策

身に覚えのないカード利用があるかのように思わせて、緊急性や不安を煽り、カード情報などの個人情報を盗むフィッシングメールが増加しています。
今回は代表的な事例や見分け方のポイントをお伝えします。

事例1 ご利用通知を装ったメール

偽のご利用通知を送り、
遷移先でカード情報を入力させる手口です。

事例2 不正利用検知を装ったメール

取引がご本人様のものか確認するという
内容のメールを送り、遷移先でカード情報を
入力させる手口です。

フィッシング詐欺にあわないために

２つのポイントを意識すると上記事例のようなフィッシングメールに引っかかるリスクを軽減させることができます。

1. 見分けるポイントを理解する
2. 最新事例を知っておく

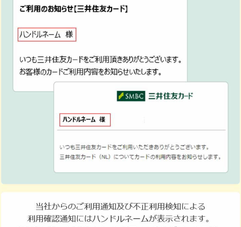
01 見分けるポイントを理解する

＼ 複数手段による通知 ／

プッシュ通知・LINEなど、ご利用通知の通知手段を複数設定している場合、同時に複数手段で通知が来るため、当社からの連絡かを見分けることができます。
メールのみでフィッシングメールかの判別は難しいため、複数設定がおすすめです。

通知手段を確認・変更する ›

＼ ハンドルネーム ／



当社からのご利用通知及び不正利用検知による
利用確認通知にはハンドルネームが表示されます。
ハンドルネームのないメールはフィッシングメールです。

ハンドルネームを確認・設定する ›

⚠ なお昨社からお送りするメールでは、お客さまのクレジットカード番号などの個人情報をお聞きすることはございません。
入力を促すメールはフィッシングメールです。

02 最新事例を知っておく

最新のフィッシングメールをホームページに随時掲載しています。定期的にご覧いただくことで最新事例が分かります。

フィッシングメールの最新事例を見る ›

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。

フィッシングは日々巧妙化していますが、見分けるポイントや最新事例を知っておくことで集らずに対処できます。
また、最近では当社のSMSや電話認証を装ったフィッシングも発生しています。次回はその手口についてご紹介します。

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！