





令和5年6月28日発行


静岡県警察からのお知らせ

フィッシングメールの注意点

-  フィッシングメールとは、実在する企業やサービスを装い
- ▶ ログインID・パスワードの識別符号
 - ▶ 住所、氏名、銀行口座番号、クレジットカード番号等の情報を詐取するサイトへ誘導するメールのことです。

実際に届いたフィッシングメールの例

差出人 ●● カード <info@: ●.co.jp>  **差出人は簡単に偽装できます。**

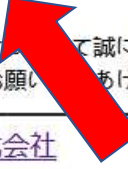
宛先  11:49

件名 【最終警告】: ●● 銀行 からの緊急の連絡 [メールコード57465]

【●● カード】利用いただき、ありがとうございます。
このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。
つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。
お客様にはご迷惑、ご心配をお掛けし、誠に申し訳ございません。
何卒ご理解いただきたくお願い申し上げます。
ご回答をいただけない場合、カードのご利用制限が継続されることもございますので、予めご了承下さい。


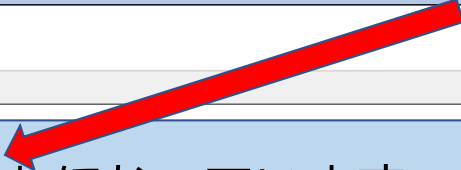
■ご利用確認はこちら

ご不便とご心配をおかけして誠に申し訳ございませんが、何とぞご理解賜りたくお願い申し上げます。

●● カード株式会社  **表示上正規サイトのアドレスが表示されていても、カーソルを合わせることによって、実際のリンク先が表示される**

■発行者■
●● カード株式会
※本メールは送信専用
※本メールは「●●」にメールアドレスをご登録いただいた方にお送りしています。

http://www.smbe-card.com.qvol2cdsvwfy12bt.shop/

(0) http://www.smbe-carb.com.qvol2cdsvwfy12bt.shop/



URLの最後が「.shop」になっています。
普段見かける「.jp」や「.com」でない場合は特に注意が必要です。
このほか、「.xyz」「.top」「.cn」などでフィッシングサイトや詐欺サイトに誘導されることが多いです。

