

フィッシングの被害拡大中!

そのメールは本物ですか?

フィッシングメール
(なりすましメール※)
のリンクをクリックして、

銀行預金を不正に送金された



クレジットカードを不正に利用された



という被害が後を絶ちません。

※なりすましのSMSも含まれます。

正規のメールと
見分けることが困難

宅配業者、金融機関、通信事業者、
ネットショップ、官公庁等
実在の企業等を装う。

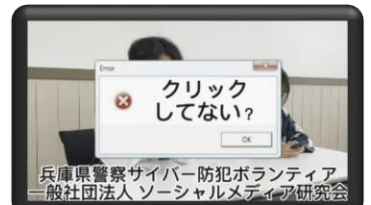
✉ フィッシングメールの特徴 ✉

【重要】 【不正アクセスを検知】 【取引を制限】
等のタイトルで不安にさせ、リンクをクリック
させようとする。

フィッシング被害に遭わないためには?

- メールやSMSに記載されたリンクをクリックしない。
- 内容を確認するときは、公式サイトやアプリを利用する。
- 携帯電話会社等の迷惑メッセージブロック機能を活用する。

《 フィッシングメール対策動画 》



制作：めじろん
おおいた見守り隊



制作：サイバー防犯
ボランティア島根大学



制作：サイバー防犯
ボランティア一般社団法人
ソーシャルメディア研究会

Twitter (サイバーセンター公式ツイッター)

兵庫県警察サイバーセンターではツイッターで、サイバー犯罪や
サイバーセキュリティの情報をいち早くお届けしています。

https://twitter.com/HPP_c3division

