

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」

※なりすましのSMSも含まれます。

「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。

！ フィッシングメールの特徴

- ✓ 正規のメールと見分けることが困難。
- ✓ **【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。**
- ✓ 宅配業者、金融機関、通信事業者、ネットショップ、官公庁等の実在の企業等を装う。

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



岩手県警察本部サイバー犯罪対策課の公式TwitterはQRコードから！
サイバー空間を悪用した犯罪の手口やサイバー犯罪の被害に遭わないための
情報をお知らせしています。

岩手県警察本部生活安全部サイバー犯罪対策課
令和5年7月21日発行



岩手県警察
Iwate Prefectural Police



警察庁
National Police Agency



@ Iwate_cyber