

そのURL

タップしないで！

それフィッシング
かもしれません

差出人： XXX @ XXX -security-update.com
宛先： ○○○○@example.com
件名： 【重要】アカウントの利用を停止します

実在する会社名
を装ってきます！

不安をあおる表現や急な対応
を促す表現は**要注意**！

お客様のアカウントに
異常なアクセスを確認しました。

24時間以内に本人確認を行わない場合、
アカウントを停止します。

▼本人確認はこちら

[https:// xxxx -security-login.com/verify](https://xxxx-security-login.com/verify)

XXX-XXX-XXX

【重要】料金のお支払いが
確認できません。

本日中に確認がない場合、
サービスの利用を停止します。

ご確認はこちら

<http://payment-check.xyz>



※金融機関がID・パスワード等をメールやSMSで問い合わせることはありません。

フィッシングとは、実在する会社等を装ったメールやメッセージを送りつけ、記載されたURLから本物そっくりの偽サイトへ誘導し、個人情報を入力させて盗み取る手口です。

被害防止対策

- ①電子メールやSMSに記載されているリンクはタップしない。
アクセスする際は、公式のURLからアクセスする。
- ②パソコンやスマートフォンのバージョンを最新にする。
- ③ID・パスワードの使いまわしはしない。



怪しいメールを受信したり、情報を入力してしまったときは、

最寄りの交番・警察署

に**通報・相談**しましょう。

フィッシングサイトを発見した場合は、

インターネット・ホットラインセンター (<https://www.internethotline.jp>)

へ通報をお願いします。

詳細は福岡県警察サイバー犯罪対策課HPをチェック

福岡県警察サイバー犯罪対策課

