



注意喚起情報



令和8年10月 広島県警察本部
サイバー犯罪対策課
☎082-228-0110

フィッシングメールに注意！ ～被害に遭わないために～

流出したメールアドレスに対する偽メールによって
更なる情報流出や金銭的被害に繋がるおそれがあります！

■ フィッシングの例

●●アカウントより重要なお知らせ

公式 ●●公式メール <info@●●.example>
宛先: npa.taro@example.ne.jp

商品お届けのため、
お支払方法をご確認ください。

<https://malicious-phishing.example/>



<https://malicious-phishing.example/>

お支払方法を入力

クレジットカード名義人

カード番号

送信アドレスを偽装する場合も

偽サイトで情報を窃取されます！



フィッシング対策

- ✓ メール内のリンクを安易にクリックしない
- ✓ ID・パスワードの使い回しをしない
- ✓ パスキーその他多要素認証を活用する

より詳しい対策は ⇒ 警察庁「フィッシング対策」

<https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html>



～パスキーとは？～

- ▶ パスワードを使用せず、生体情報（指紋や顔）などを使用する認証技術です。
- ▶ フィッシングサイトでは、パスキーが動作しない仕組みとなっているため、フィッシング対策として非常に有効です。

フィッシングサイト



正規のサイト



正規のサイトはパスキーで
カンタン認証！

フィッシングサイトに
パスキーは使えないので安心！



警察の取組

～サイバー空間にける安全・安心の確保のために～

警察では、民間事業者と連携して、フィッシング対策を推進しています！

警察庁「マイクロソフト・JC3と連携した犯罪インフラのテイクダウンについて」

<https://www.npa.go.jp/bureau/cyber/koho/news/20261015.html>

