滋賀県警察

サイバーセキュリティ情報SHIG@

サイバー犯罪からあなたを守るセキュリティ情報をお届けします。

R４年度 No.２

auやau関連サービスをかたる フィッシングメールにご注意ください！

全国的に、au利用料金の「未払い金」や「au PAY」などのKDDIグループサービスからのお知らせや通知を装ったEメールやSMSにより、偽サイト(フィッシングサイト)に誘導され、IDやパスワードを入力してしまったことで、不正決済されるという被害が発生しています。

被害を防止するため、サービスを利用する際には、メールに記載されているURLを押さずに、必ず公式のアプリやブックマークからアクセスしてください。

ID・パスワードの入力は、必ず公式サイトから行いましょう。

クレジットカード・スマホ決済・キャリア決済 不正利用が発生しています。

キャッシュレス化が進む一方で、クレジットカード決済等の不正利用が多発しています。

クレジットカードは、カード番号、有効期限、セキュリティコード番号（以下、クレジットカード番号等）が流出するとショッピングサイト等で無断で登録された上、買い物をされてしまう場合があります。

特にフィッシングによるクレジットカード番号等の流出には、注意してください。

キャッシュレス決済は便利ですが、セキュリティ対策や決済状況の管理をしっかり行う必要があります。

【クレジットカード】

- クレジットカード番号等の入力を促すメールやSMSは、**フィッシングを疑ってください。**
- クレジットカード番号等の入力は、信頼できるサイト（**公式サイト**）で行ってください。
- クレジットカード利用時の**メール通知機能**を利用してください。
- **利用明細**を必ず確認して、不正利用があればすぐにカード会社に連絡してください。

CARD

【スマホ決済】

- スマホのアプリの設定で、指紋認証や顔認証等の**生体認証**が可能な場合は、利用しましょう。
- 二次元バーコードを読み取る場合は、正規のバーコードであることを確認してください。

【キャリア決済】

- キャリア決済の場合、**利用限度額**を低額に設定しましょう。
- **利用通知**の設定をしておきましょう。

（キャリア決済とは・・・携帯電話利用料金と合算して商品代金等を支払うサービス）

PAY

«サイバーコネクトSHIG@»QNAP製NASに脆弱性情報があります。すぐにアップデートを。

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）　県警Webページ→