サイバーセキュリティパートナーシップだより

No.11

令和3年7月28日　山口県警察本部生活環境課

個人情報を守るためのフィッシング詐欺対策！

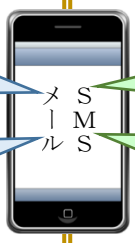
山口県内では、依然としてフィッシング行為によりクレジットカード情報やアカウントＩＤ、パスワード等の個人情報がだまし取られるといった被害が多発しています。

フィッシング行為から個人情報を守るため、増加中のフィッシング手口やその対策等を紹介しますので、参考にしてください。

フィッシングとは？

実在する組織をかたったメール、ＳＭＳから偽サイト等へ誘導し、ユーザーネーム、パスワード、アカウントＩＤ、口座番号、クレジットカード番号等の個人情報をだまし取る行為

増加中のフィッシング手口



～　ＮＴＴドコモをかたった手口　～

ｄアカウントを生体認証の利用を中止されています、解除してください
https://〇〇〇.〇〇〇

【重要】安全のためお客様のｄアカウントは一時的に停止されております。
https://〇〇〇.〇〇〇

リンク先にアクセスすると、**ｄアカウントＩＤ、パスワード、クレジットカード情報等の個人情報**の入力を求められる

～　Ａｍａｚｏｎをかたった手口　～

プライム会費のお支払い方法に問題があります。詳細はこちら https://〇〇.〇〇〇

ご利用の Amazon アカウントを一時保留しました。解決するには、https://〇〇〇.〇〇

リンク先にアクセスすると、**Amazon のアカウントＩＤ、パスワード、クレジットカード情報等の個人情報**の入力を求められる

フィッシング被害に遭わないために！！

送られてきたメールやＳＭＳに記載されたリンクに安易にアクセスしないことが大前提！！

→　**メール中のリンクからアクセスするのではなく、公式のアプリやブックマークした正規のＵＲＬからサービスにログイン**し、情報を確認！

→　メールやＳＭＳを送ってきた会社名をネットで検索し、**注意喚起状況や似たようなフィッシング・詐欺の事例がないか**を確認！！

→　**セキュリティ対策ソフト**を積極的に利用し、危険なサイトへのアクセスを回避！！！

山口県警察サイバー犯罪相談窓口
℡　０８３－９２２－８９８３
mail cyber.soudan@police.pref.yamaguchi.lg.jp
～研修会の依頼は警察署又は警察本部生活環境課まで～

サイバー防犯広報
https://www.police.pref.yamaguchi.lg.jp/kurashi/page