サイバーセキュリティパートナーシップだより

No.14

令和3年9月3日　山口県警察本部生活環境課

NTTドコモを装ったフィッシング詐欺に注意!

現在、ドコモを装ったSMS（ショートメッセージサービス）やメールが不特定多数のユーザに発信され、リンク先の偽サイト（フィッシングサイト）で入力したｄアカウント情報が盗まれる被害が相次いで発生しています。

フィッシングの手口及び被害防止対策について紹介しますので、被害に遭わないよう十分注意してください。

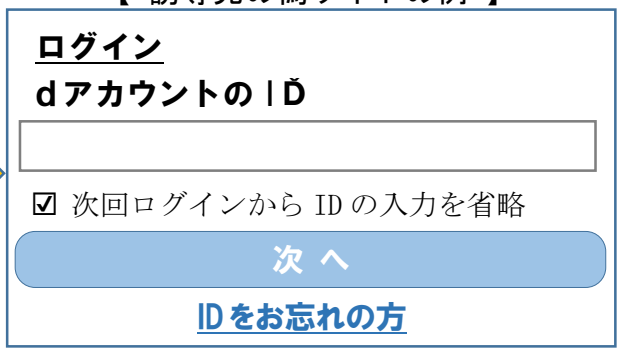
【 SMS・メールの例 】

ドコモお客様センターです。ご利用料金のお支払い確認が取れておりません。ご確認が必要です。
https://bit.ly/〇〇〇〇〇〇〇

【NTT】お客様がご利用の電話料金が大変高額となっております。ご確認が必要です。
http://nttdocomobn.duckdns.〇〇

差出人：docomo
アカウントがdocomoIDの利用規約に違反しており、アカウントが停止されています。
ログインアクティビティを確認する。

【 誘導先の偽サイトの例 】



※SMSやメールのリンク先にアクセスすると本物と見分けのつかない不正なサイトに誘導され、ログインに必要なID・パスワード、暗証番号等の入力を求められる。入力すると情報が盗み取られ、不正ログインに利用される。不正ログインに成功すると、キャリア決済や登録クレジットカードが悪用され、金銭被害に発展!

ドコモの他、au（KDDI）・ソフトバンク・楽天モバイルをかたるSMS等にも要注意！

・不安を煽るような内容のSMSやメールを受信しても安易にリンク先URLをクリックしない！
・内容を確認する場合は、普段利用しているブックマークやアプリを経由して正規サイトにアクセスのうえ、利用状況などを確認すること。
・ウィルス対策ソフトの利用を検討すること。

山口県警察サイバー犯罪相談窓口
TEL　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

詳しくはこちら
一般財団法人日本サイバー犯罪対策センター（JC3）ホームページ
（通信事業者を装ったフィッシングの注意喚起）