サイバーニュース

R 1 年 第 8 号
奈良県警察本部
サイバー犯罪対策課

ドコモを装ったフィッシングSMSに注意!!

SMS(ショートメッセージサービス)で、ドコモを装ったフィッシングSMSの送信が確認されています。当該SMSに記載されているURLにアクセスすると、dアカウントのID/パスワード等を入力する画面に移動し、入力したデータが搾取され上、dカードやキャリア決済の不正利用被害が発生しています。

ドコモ公式SMSと同じ
NTT DOCOMOとなっている

【偽物】ドコモ公式メッセージに紛れてフィッシングメッセージが表示されます。

フィッシングSMSの送信元が、ドコモ公式SMSと全く同じになっているため、同じスレッド内に表示され、フィッシングサイトへ誘導されてしまいます。

フィッシングSMS本文例

1	お客さまがご利用のキャリア決裁が不正利用の可能性があります。ウェブページで二段階認証お願いします。 www.mydocomo-***.com
2	お客さまがご利用のdカードが不正利用の可能性があります。本人認証設定をお願いします。 http://www.nttdocomo-***.com
3	お客さまのdアカウントに異常ログインの可能性がございます。下記URLで検証お願いします。 http://www.mydocomo-***.com
4	【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。下記URLでご確認が必要です。 http://medocomo**.com
5	【iD】お客様がご利用のiDアプリが不正利用の可能性があります。下記URLでご確認が必要です。 http://id-***.com/id
6	【NTT】お客様がご利用のアカウントが外部によるアクセスを検知しました。下記より必ずご確認ください。 www.mydocomo**.com

今後、他の携帯電話事業者のみならずLINEやGoogle等の他の事業者を騙る同種の事案の被害が全国的に多発するおそれがあると予想されます！！

- **このようなSMSを受信した際は、リンクを開かずに無視するようにして下さい。**
- **リンクへアクセスする前に、当該URLが公式のものであるかの確認を確実に行って下さい。**
- **万が一フィッシングサイトを表示した場合は、dアカウントのID・パスワード等の情報や個人情報を絶対に入力しないように注意して下さい。**