通信事業者を装った フィッシング に注意！

県警察には、電子メールやSMS（ショートメッセージサービス）を利用して、通信事業者を装ったフィッシングサイトに誘導する手口に関する相談が多く寄せられています。

誘導されたフィッシングサイトは、当該通信事業者や配送業者のホームページなどを模倣して作られており、一目では判別が難しく、様々な被害へと発展する危険性があります。

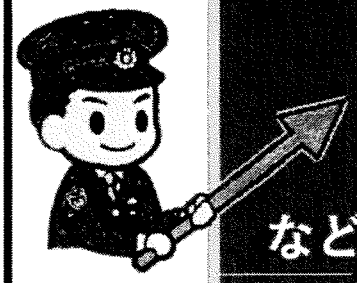
WARNING 具体的には このような危険性があるよ

メールに含まれるリンク先をクリックしてしまうと当該通信事業者を装ったフィッシングサイトに誘導され・・・

- ID・パスワード等の情報が詐取される
- 詐取された情報を悪用されて・・・
  - 商品を勝手に購入される
  - 不正送金される
- 不正アプリをインストールさせ・・・
  - 自分の携帯電話からSMSを大量に送信される

などの被害に遭うおそれがあります。

注目

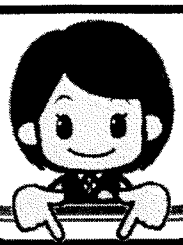


事業者を装うフィッシングメールには
- ✓ 通信事業者
- ✓ 運送系企業
- ✓ ネットショッピング事業者
- ✓ 金融機関

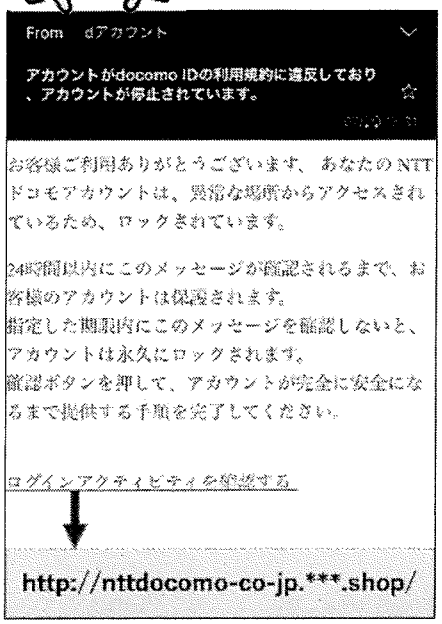
などさまざまなものがあるので要注意！！

裏面につづく

神奈川県警察サイバー犯罪捜査課



フィッシングメールの事例はこちら
似たようなメールが届いたら注意が必要です



通信事業者を装った電子メールの例

不正なアクティビティが検知されました為、au idの利用が制限されております。必ずご確認ください。 au.[illegible].xyz

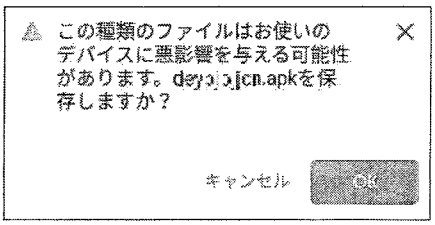
ドコモお客様センターです。ご利用料金のお支払い確認が取れておりません。ご確認が必要です。
https://bit.[illegible]

通信事業者を装ったSMSの例

[illegible]よりお荷物のお届けに上がりましたが宛先不明の為持ち帰りました。
http://[illegible].org

[illegible]よりお荷物を発送しましたが、宛先不明です、下記よりご確認ください。http://[illegible].org

運送系企業を装ったSMSの例



不正アプリダウンロードの例

重要 POINT 被害に遭わないために、次のことに注意しましょう。

- **電子メールやSMSのメッセージに含まれているリンク先を安易にクリックしない。**
- **通信事業者からの通知内容を確認するときは、公式サイト等から確認する。**
- **あらかじめ通信事業者のホームページを確認し、公式サイトのURLをブックマークに登録しておき、ブックマークからアクセスする。**
- **アプリのインストールは、正規のアプリ配信サイト等、信頼できるサイトから行う。**
- **ID、パスワードを入力する際は、公式サイトであることを確認した上で入力する。**
- **迷惑メールフィルタやウイルス対策ソフトの利用を検討する。**
- **通信事業者の公式サイトにおいてフィッシングに関する注意及び対策内容を確認する。**

「出典：一般財団法人日本サイバー犯罪対策センター（JC3）」

一般財団法人日本サイバー犯罪対策センター（JC3）のホームページでは、フィッシング等の手口についての注意喚起を、画像や動画により分かりやすく公開されていますので、併せてご参照ください。
https://www.jc3.or.jp/threats/topics/article-382.html
（脅威情報：通信事業者を装ったフィッシングの注意喚起）

ご自身だけでなく、ご家族、ご友人、職場の方々へもお声掛けしていただき、被害防止に努めましょう。

浦賀警察署防犯特報

本人特定事項の確認をかたる

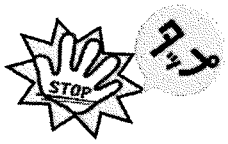
フィッシング（スミッシング）に

ひっかかかっては「イカ」んよ

大事な情報が釣られちゃうよ！！（盗まれ）

インターネットバンキングやインターネットショッピングサイト等、様々なWebサイトをかたり、各種アカウント設定における**「本人特定事項の確認」等と称して**フィッシングサイトへと誘導する

「フィッシングメール（SMS含む）」が多発



しています。

- メールに書かれたURLは安易に開かない
- 送信元（企業等）の正規ホームページ等でメール送信の真偽を確認する

などして、被害の防止を図りましょう！