

フィッシング詐欺に注意！

宅配業者、通信事業者、インターネット通販サイト、金融機関など、実在する企業を装った詐欺が頻発しています。

フィッシングってなに？

宅配業者、通信事業者、金融機関などを装った電子メールやショートメッセージを送り付け、メールなどに記載されたリンク先の偽サイト（フィッシングサイト）に誘導し、ID、パスワード、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を入力させ詐取する行為です。

これらがフィッシング詐欺のショートメッセージ(SMS)の例です

ご本人様不在の為お荷物を持ち帰りました。
ご確認ください。

[http://\[redacted\].duckdns.org](http://[redacted].duckdns.org)

【●●●●】お客様がご利用の電話料金が大変高額になっております。ご確認が必要です。

[http://\[redacted\].xx.com](http://[redacted].xx.com)

お客様がご利用の〇アカウントに異常ログインの可能生がございます。下記URLで検証をお願いします。

[http://www.\[redacted\].myxxxxx.com](http://www.[redacted].myxxxxx.com)

(EC事業者名) 使用制限ポリシーの違反が検出されました、ログインして確認してください。

[https://user-\[redacted\].top](https://user-[redacted].top)

注意：ダイレクトのパスワードが翌日に失効し(金融機関名)のメンテナンスサイト[www.bk-\[redacted\].pl](http://www.bk-[redacted].pl)により、更新をお願いします。

(金融機関名)、お客様がご利用の口座が不正利用されている可能生があります。口座一時利用停止、再開手続

[http://\[redacted\].com](http://[redacted].com)

これらは、偽のショートメッセージの可能性がありますが

フィッシング詐欺の被害！

- クレジットカード情報の不正利用
インターネットショッピングされたり、偽造カードをつくられてしまう。
- インターネットバンキングにおける不正出金
取引銀行口座に入っていた預金が引き出されてしまう。
- インターネットオークションにおけるなりすまし
オークション詐欺などに利用されてしまう。
- 個人情報の不正売買
不特定多数の犯罪者に悪用されてしまう。

フィッシング詐欺に遭わないために！

- 信用しない ショートメッセージをむやみに信用しない
- 開けない ショートメッセージを慌てて開けない
- 押さない リンク(URL)を押さない(タップしない)
- 入力しない ID、パスワードやカード情報等の個人情報を安易に入力しない
公式アプリや正規サイトを登録したブラウザのブックマークからアクセスする。