

ますます巧妙化する サイバー犯罪に だまされるな！ あなたの情報や財産が狙われています！

フィッシング詐欺

「本物そっくり」なSMS・メールが大量に！

手口 有名企業や金融機関を装い、偽サイトへ誘導。ID・パスワードやクレジットカード情報を盗み出します。

△ URLやリンクは絶対に押さない！



サポート詐欺

突然の警告画面！「電話をかける」は詐欺！

手口 偽の警告音と画面で不安をあり、電話をかけさせます。言葉巧みに「遠隔操作ソフト」で端末を乗っ取り、嘘の修理代やサポート料金を請求します。

△ 表示された番号に電話しない！



偽ショッピングサイト

リアルなサイトデザインで油断させる！

手口 人気商品を格安で販売しているように見せかけます。代金を支払わせた後、商品を発送しない、または粗悪品を送付します。

△ 「安すぎる」は、まず疑う！



「自分は大丈夫」が一番危険。今すぐできる対策は裏面へ！→

今すぐできる! 3つの鉄壁ガード

日頃から注意し
心がけましょう



1

疑うクセをつけよう!



メール・SMS

URLやリンクは一切押さない!

「送信元」は偽装できるので信用してはいけません。

メッセージ内のURLやリンクは「詐欺の入り口」!

必ず「公式アプリ」か、あらかじめ登録した「ブックマーク」から開くルールを徹底しましょう。

偽警告

画面の番号には決して
電話しない!

「電話番号が表示される」警告は全て偽物です。

表示された番号には絶対にかけないでください。

対処法:無視して画面を閉じる。

閉じられない時は「再起動」しましょう。

パソコン:Escキーを長押ししてから画面を閉じる。

Ctrl + Alt + Deleteキーで再起動/強制終了

スマホ:電源ボタン長押しなどで「再起動」



2

防御を固めよう!



パスワード

使い回しは絶対NG!

ひとつ漏れると全て乗っ取られます。

長く複雑なパスワードをサービスごとに設定しましょう。

アップデート

弱点の「穴」をふさぐ!

OSやアプリの「更新通知」が来たら、後回しにせず速やかにアップデート。

セキュリティの穴を埋めましょう。

セキュリティソフト

自動でブロック!

人間の目では見抜けない偽ショッピングサイトやウイルスも検知します。

パソコンだけでなく、スマホにも必ず導入しましょう。



3

迷わず相談! 「あれ?」と思ったらすぐ電話

徳島県警察
サイバー犯罪相談ダイヤル



088-622-3180

188 嫌や!(いやや!)局番は必要ありません
消費者ホットライン

音声ガイダンスに従って、郵便番号を入力すれば、
お住まいの地域の消費生活センター等をご案内します。