

フィッシング詐欺

検 索

金融機関や大手通販サイトなどを装って、[パスワード][アカウントID][クレジットカード情報]などといった個人情報を盗む行為です。

多発している手口に、メール差出人に実在するサービスのメールアドレス(ドメイン)を使用した「なりすまし」フィッシングメールがあります。

メールの差出人情報は偽装できます。

そのため、差出人情報などを頼りにメールの真偽を見抜くことは難しいです。



本物のサイトにハッキリ!

だけど・・・

フィッシングサイトのURLだ!

千葉県警サイバー犯罪対策課広報キャラクター バグ

偽サイト

みんなまで
気を付けよう!



千葉ジェッツ公式マスコットキャラクター
ジャンボくん



リンクのクリックにご用心!

電子メールに記載されたリンクは偽装可能なため、見た目で見ただけでリンクの真偽を判断するのは困難です。
電子メールやSMS内のリンクを安易にクリックせず、公式サイトをブックマークしておくなど、正しいサイトに接続するようにしましょう。



モバイル端末を安全に保つ!

OSやアプリのせい弱性や不具合が悪用され、広告などからフィッシングサイトに誘導される可能性があります。
OSやアプリなどのアップデートし、端末を安全な状態にしましょう。



パスワードを使いまわさない!

複数のサイトで同じID、パスワードを登録していると、盗まれたときに全てのサービスが乗っ取られる被害にあってしまいます。
ID、パスワードはサイトごとに違うものに登録するようにしましょう。
覚えられない場合は、パスワード管理アプリなどを活用しましょう。