

フィッシング詐欺にご注意ください

金融機関を騙り、「セキュリティ強化」等の名目でショートメッセージ等を送り付け、フィッシングサイトへ誘導し、「ID、パスワード」等を入力させる手口が急増しています。

お客さまにおかれましては、以下の点にご注意いただきますようお願いいたします。

1. SMSに記載されているリンクへのアクセスにより、フィッシングサイトに誘導される危険性がある。
2. SMSに記載されているリンクからアクセスした先のサイトでは ID やパスワード等を入力しない。
3. インターネットバンキングのアクセスは、普段使っているブラウザの「ブックマーク（お気に入り）」に登録している URL や正規のアプリからアクセスする。

銀行をかたるフィッシング詐欺が急増

銀行をかたり、「セキュリティ強化」等の名目でショートメッセージ（SMS）等を送り付け、偽サイトへ誘導した後、「口座番号」等を入力させる手口が確認されています。

① それらしいショートメッセージで偽サイトへ誘導



本文に「お客様の【○○銀行の口座】セキュリティ強化、カード・通帳一時利用停止、再開のお手続きの設定: <http://xxxx.xx>」等の名目でメールを送りつけ、本文に記載のURLから偽サイトに誘導する！

タップしてしまうと...

② 銀行のサイトを模倣した偽サイトに移動

口座番号、暗証番号、ワンタイムパスワード等は絶対に入力しない！

店番号	<input type="text"/>	口座番号	<input type="text"/>
契約者番号	<input type="text"/>	-	<input type="text"/>
暗証番号	<input type="text"/>		
ワンタイムパスワード	<input type="text"/>		<input type="button" value="ログイン"/>

対策

- 記載されたリンク先には絶対にアクセスせず、いつも利用しているアプリやブラウザのブックマーク（お気に入り）からアクセスすること
- 誤ってアクセスしても口座番号、暗証番号、ワンタイムパスワード等は絶対に入力しないこと
- 不審点は、銀行や警察に確認すること