

フィッシング詐欺に注意！！

フィッシングとは、実在する組織を騙って、個人情報盗むことです。メール（SMS等）のリンクから正規サイトに似せた偽のサイト（フィッシングサイト）に誘導し、個人情報を入力させて情報を盗みます。盗まれた情報は不正に使用され、多くの場合金銭的な被害が発生します。

フィッシングメール（SMS等）に注意！！

・フィッシングメール（例）

【重要なお知らせ】 ●●銀行 ご利用確認のお願い
① ☆ 1分前 2023/06/28 水曜日 09:11 ②

いつも●●銀行をご利用いただき、ありがとうございます。

ご本人様のご利用かどうか確認したいお取引がございましたので、口座の利用を制限させていただきました。
以下からアクセスしてご確認をお願いします。

▼ <http://●●bank.co.jp> ③

フィッシングメールの特徴

- ① 「重要なお知らせ」や「至急」等と件名に入れて不安にさせ、リンク先へ誘導する
- ② 銀行・クレジットカード会社・通信販売会社等、様々な企業や団体等の名前が使われる
- ③ フィッシングサイトのリンクが貼られている（見た目だけで正しいと判断できない）

フィッシングサイトは正規サイトにとても似ています

・フィッシングサイト（例）

<http://●●bank.xyz> ①

ロゴ ●●銀行 ②

ログイン

店番号 ②③

口座番号 ②③

3桁

7桁

ログインパスワード ②③

半角英数記号32文字以内

ログイン

フィッシングサイトの特徴

- ① URLが正式なサイトと異なる
- ② ロゴは正式なものを使い、表記や項目も酷似していて正規サイトと見分けづらい
- ③ 口座番号・クレジットカード番号・ID・パスワード等個人情報に関する入力フォームがある

被害に遭わないためには

- メールリンク（URL）からウェブサイトへアクセスしない
- 条件反射でID、クレジットカード情報、パスワード等を入力しない
- 普段使用しているアプリやブックマークからサイトにアクセスする

