

フィッシングメール被害 にあわないために (1/4)

フィッシングメールとは

差出人 ●●銀行

件名 アカウント利用停止

本文

お客様のアカウントで不正なアクセスが多数検出されましたので、アカウント利用を停止しました。

利用開始するためには、アカウント情報を再設定してください。

<https://www.●●bank.co.jp>

フィッシングメール

URL <https://www.●●bank.xyz>

偽サイト ●●銀行ログイン画面

ログイン ID

パスワード

ログイン

クリック

フィッシングメールは、不安をおおるウソのメールから偽サイトなどにアクセスさせ、個人情報などを不正に入手するものです。



フィッシングメール被害 にあわないために (2/4)

特に注意すべきメールの内容

- ・危険度をおおるパスワードの変更依頼
- ・即時パスワード確認依頼
- ・パスワード再設定のお願い
- ・アカウント利用停止
- ・アカウントが閉鎖(ロック)されました
- ・新しいデバイスのログイン

など



フィッシングメール被害 にあわないために (3/4)

対応策 (確認すべき事項)

- **メールの宛先や件名を確認する**
宛先 (メールアドレス) の文字列がおかしくないですか?
緊急度をおおる内容でも慌てず、冷静に!
- **メール内のリンクの URL を確認する**
表示のURLとそれをクリックして実際にアクセスするURL
は同一とは限らない
リンクのURLが正規のURLに似せたものである場合もある
- **リンク先で個人情報の入力を求められたら
要注意**
安易に個人情報やパスワード、クレジットカード情報
などを入力しない
- **メールの内容をインターネット検索してみる**
同様のフィッシングメールの事例があるかも



フィッシングメール被害 にあわないために (4/4)

対応策 (普段からやるべきこと)

- ・サイバァちゃんのLINE (タイムライン)
をこまめにチェックする

あなたやあなたの身近な人がサイバー犯罪の被害者にならないように、サイバァちゃんのLINEをチェックしよう！

あなたのお友達でサイバァちゃんのLINEを知らない人がいたら、お友達に紹介してあげてね！

<https://lin.ee/nIE29u0>

- ・日本サイバー犯罪対策センター (JC3)
のホームページをこまめにチェックする

最新の情報が掲載されているよ！

<https://www.jc3.or.jp/>

