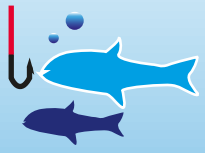
フィッシングメールから身を守るには

フィッシングメールとは?

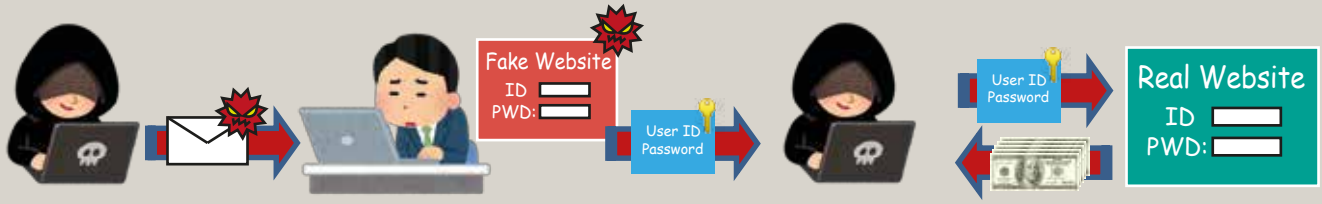
フィッシングメールとは、信頼できる機関を装った悪意のある第三者が、受信者から機密情報や個人情報などを盗み取ろうとするために送信するメールのことです。最近、特にインターネットバンキングのIDやﾊﾟｽﾜｰﾄﾞを盗み取ろうとするケースが多発しており、盗まれたアカウントは不正送金などの金融犯罪に使われています。



フィッシングメールに対しては自衛の意識を持つことがもっとも重要です。このお知らせでは、フィッシングメールの被害者とならないため、どのような事をすればよいかをご案内いたします。

フィッシングメールはどう作用するか?

1. 犯罪者は、偽のウェブサイトのリンクや添付ファイルが含まれたメールを送信します。
2. 受信者は偽のウェブサイトにログインしようと、IDやﾊﾟｽﾜｰﾄﾞを入力したり、添付ファイルを開こうとします。
3. 偽のウェブサイトや不正プログラムが、IDとパスワードを盗みます。
4. 盗んだIDとパスワードで、不正送金などの金融犯罪を実行します。



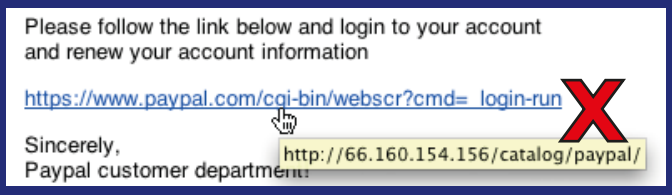
フィッシングメールから身を守るには

xxx@mizuho-cb.com ○

xxx@m1zuh0-cb.com ×

1. 送信者を注意深く見る

偽の e-mail の中には、本物に良く似ているが本物とは異 なるアドレスから送信してきているものがあります。メール を開く前に、送信者が確実に判別できるかどうかご注意ください。

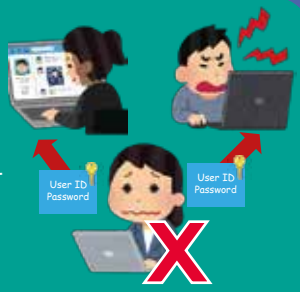


2. 不審なメールのリンクや添付ファイルを開かない

フィッシングメールのURLリンクや添付ファイル に仕掛けられたウィルスは、あなたのログイン情報を盗み取るものです。不審なメールのリンクや添付ファイルは絶対に開かないようお願い致します。

3. 他人とパスワードをシェア、開示しない

銀行スタッフは決してあなたのパスワードを問い合わせることはありません。パスワードは決して誰とも共有・開示しないようお願いします。



4. アンチウィルスソフトをインストールし、最新に保つ

アンチウィルスソフトは、情報を盗み取ろうとするウィルスなどに有効です。

5. もし不審なメールを受け取った場合は、メールを開かずにすぐに削除する。不確かなメールに対しては、送信者に電話などで直接メールについて確認する。

Mizuho Bank, Ltd. Bangkok Branch 98 Sathorn Square Office Tower 32nd - 35th Floor, North Sathorn Road, Silom, Bangrak, Bangkok 10500 Tel: 0-2163-2999
Mizuho Bank, Ltd. Eastern Seaboard Branch, 300/7 ESIE Plaza 2, Unit No. 2-05 Moo 1, Tasit, Pluakdaeng, Rayong 21140 Tel: 038-997-000