



そのメール大丈夫？

フィッシングメールが出回っています!!

フィッシングとは、金融機関(銀行やクレジット会社)などを装った電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為のことを言います。

これまでは、金融機関を装ったフィッシングメールが多かったのですが、

Amazon、LINE、セゾンNetアンサー、Apple

を装ったフィッシングメールが最近出回っています。

これらのメールには、

- メール本文の日本語の表記がおかしい
- メール本文には、「アカウントにいくつかの情報がない」「アカウントに異常ログインされた」「アカウント情報の一部が誤っている」などと記載されている
- メール本文には、実際のアドレスに似たURLが記載されているほか、そのURLからログインなどするようにも記載されている
- 入力画面などには、その会社のロゴなどが使用されており、本物と見間違える
- 入力画面などでは、アカウント情報(ID、パスワードなど)の入力を求められるほか、クレジットカード情報(クレジットカード番号、有効期限、セキュリティコードなど)を求められる場合もある

などの特徴があります。

アカウント情報やクレジット情報は、絶対に入力しない!!

今後も通信販売会社などを装ったフィッシングメールが出回る可能性がありますので、

- 慌てずに対応する
- メールを送信者欄は偽装できたり、本物に似たメールアドレスが使用されている場合があることに注意する
- フィッシング対策機能を備えたウイルス対策ソフトを導入する
- メールに記載されたURLからアクセスせず、正規のURLからアクセスする
- アカウント情報やクレジットカード情報を入力させるような依頼がメールで来ることは考えにくいので、必ずホームページなどで確認する

などを心掛けて被害に遭わないようにしてください。



サイバー犯罪(インターネットに関する犯罪)の通報やご相談は...

石川県警察本部生活環境課サイバー犯罪対策室



076-225-0110



cyber@police.pref.ishikawa.lg.jp