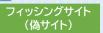
富山県警察 サイバー防犯 🎙 シンク ボランティア あなたをねらっていま

ID









③ フィッシングサイトで ID やパスワードなどの 情報を入力する

「フィッシング」とは、実在するサービスや企業をかたって 偽のウェブサイト(フィッシングサイト)へ誘導し、ID、パス

ワード、口座番号、クレジットカード番号などの重要な情報

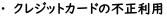
① 実在するサービスや企業を かたり、偽のメールや SMS を 送信する。

※SMS:ショートメッセージ

④ 入力された情報を だまし取り、悪用する

だまし取られた情報が悪用されると… こんな被害にあう可能性が!

アカウント乗っ取り



- ショッピングサイトの不正利用
- - ネットバンキングの不正利用



フィッシングの被害にあわないために

を入力させ、だまし取る行為です。

- ◆ 身に覚えのないメールやSMSは開かず削除しましょう。 ⇒「重要」「緊急」など、対応を急がせるような内容でも、 慌てずに一度立ち止まって確認してください。
- ▶ メールやSMSのURLをクリックしてはいけません。 ⇒ フィッシングサイトに接続してしまった場合は、情報を 入力せず、すぐに画面を閉じてください。

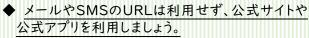
【重要】不正ログインを 検知しました。本人確認 設定をお願いします。

http://○△□

・対応を急がせる 不安をあおる

お客様が不在の為お荷 物を持ち帰りました。 至急ご確認ください。 http://○△□

不審なメールや SMS に注意!!



⇒ あらかじめ公式サイトのURLを「お気に入り」や 「ブックマーク」に登録しておくと便利です。

銀行



その URL、本当に公式?

- パスワードをしっかり管理!
 - ⇒ パスワードを複数のサービスで使い回さないでください。
- スマートフォンやパソコンのセキュリティ対策を!
 - ⇒ ウイルス対策ソフトや迷惑メールフィルタを利用しましょう。
 - ⇒ OSやアプリを更新し、常に最新の状態に。



ダイレクトログイン ログインID 実在する企業の 口座番号 ログインパスワード

「フィッシング」に釣られるな!!



困ったことがあれば、 周りの人や警察に相談を