

STOP！フィッシング詐欺

巧妙な偽メール(フィッシングメール)を使って、偽サイトに誘導します。



フィッシングメールが巧妙化！判別が非常に困難に！

メールの文面も流ちょうな日本語で、メールアドレスのドメイン(@●●●.com等)も偽装！

思わずタップしたくなる内容！

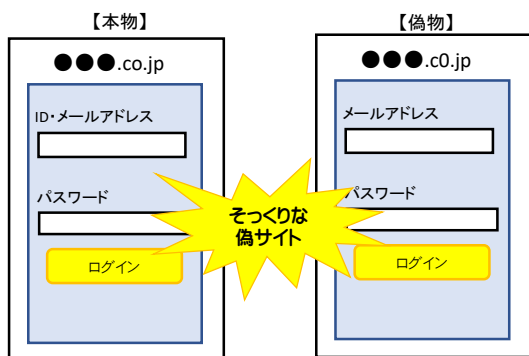
件名も「お支払方法に問題があります！」「荷物をお届けしましたが不在でした。」等つい押ししまいそうな内容！

メールだけじゃない！SNSの広告にも注意！

閲覧中のホームページに表示されるネット広告や、SNSに表示される広告等からフィッシングサイトに誘導する手口もあります。

不審なURLは絶対クリックしないで！！

精巧な偽サイトに誘導し、個人情報をだまし取る！



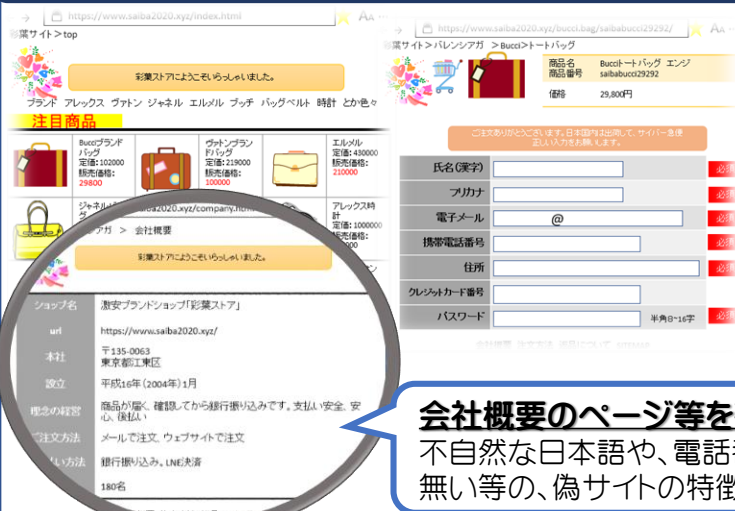
偽サイトは本物そっくり！

本物のサイトのページ構成等をそのまま転用し、個人情報やパスワードの入力を要求してきます。

URLもまぎらわしい！！

URLもセキュリティに対応した「https」で作られ、アルファベットも「1(いち)」を「l(エル)」、「o(オー)」を「0(ゼロ)」にする等、あの手、この手でだまそうとします。

盗まれた個人情報は悪用されます！！



クレジットカードの不正利用で、身に覚えのない請求書が！

偽サイト等でクレジットカード情報を入力したら、クレジットカードは不正利用されます。フィッシングサイトにクレジットカード番号を入力してしまったら、クレジットカード会社に連絡して、すぐにカードの停止措置をしましょう。

会社概要のページ等を確認！

不自然な日本語や、電話番号や会社の代表者の氏名の記載が無い等の、偽サイトの特徴が無いか確認しましょう。



STOP！パスワードの使い回し

ショッピングサイトA

ID abc-xxx@mail.ne.jp

パスワード abcxxx123

SNSサイト

ID abc-xxx@mail.ne.jp

パスワード abcxxx123

同じIDパスワードを使いまわしていると・・・

Bショッピングサイト

ID abc-xxx@mail.ne.jp

パスワード abcxxx123

サイバー攻撃により、Bショッピングサイトの顧客情報が10万件漏洩！

漏洩したBショッピングサイトのパスワードは変更したのに、ショッピングサイトAから身に覚えのない請求書が届きました。私のSNSが乗っ取られました！！

という被害に遭うかもしれません。

有名SNS

ID・メールアドレス

パスワード

ログイン

IDは公開しているメールアドレスです。

パスワードは生年月日・・・

推測しやすいパスワードを使っていると・・・

ある朝起きると、私のSNSから、身に覚えのない書き込みがされて、私のアカウントが炎上してしまいました。

という被害に遭うかもしれません。

ブログサイト

インターネットバンキング

パスワードは覚えられないので、いつも「123456」にしています。

漏洩パスワードランキングに入るパスワードを使っていると・・・

いつの間にか預金の残高が0円になっていました。

パスワードランキング上位のパスワードを手当たり次第に入力すると、誰かのアカウントに入れるぞ！

となってしまうかもしれません。

安全なパスワードの設定方法

- パスワードの文字列は長めにする。(12文字以上を推奨)
- インターネットサービスで利用できる様々な文字種(大小英字、数字、記号)を組み合わせると、より強固になる。
- 推測されやすい単語、生年月日、数字、キーボードの配列順などの単純な文字の並びやログインIDは避ける。
- 他のサービスで使用しているパスワードは使用しない。

安全なパスワードの管理方法

- 紙にメモして、人目に触れない場所で保管する。
- パスワード付きの電子ファイルでパソコン等の中に保管する。
- パスワード管理ツールを使用する。

日本人の漏洩パスワードランキング

	1位	2位	3位	4位	5位	6位	7位	8位	9位	10位
2022年	123456	password	1234	12345678	akubisa2020	xxxxxxx	sakura	303030	12345	123456789
2021年	password	123456	123456789	12345678	1qaz2wsx	member	asdfghjk	12345	password1	1234567890