



Yahoo! JAPAN におけるフィッシング対策

2010年 1月 28日

R&D統括本部 セキュリティプラットフォーム技術

Project ZERO

R&D統括本部 セキュリティプラットフォーム技術

戸田 薫

Project ZERO

～全ての不正行為をゼロに～



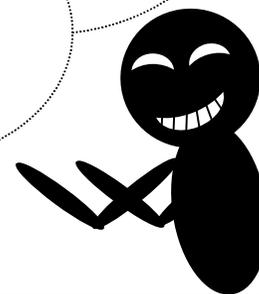
1. **フィッシングを仕掛ける動機とは？**
2. **過去から現在までのフィッシングの変遷**
3. **その手口と傾向**
4. **Yahoo! JAPAN の取り組み**
5. **今後の見通し**



1. フィッシングを仕掛ける動機とは？

Y! フィッシングを仕掛ける心理

- 悪い事をしてでも儲けたい
- ネットならではの手軽さ
- 24時間いつでもどこでも
- 数打てば当たる
- 逃げるのが簡単
- 捕まっても軽い罪



Y! Yahoo! JAPAN は格好のターゲット

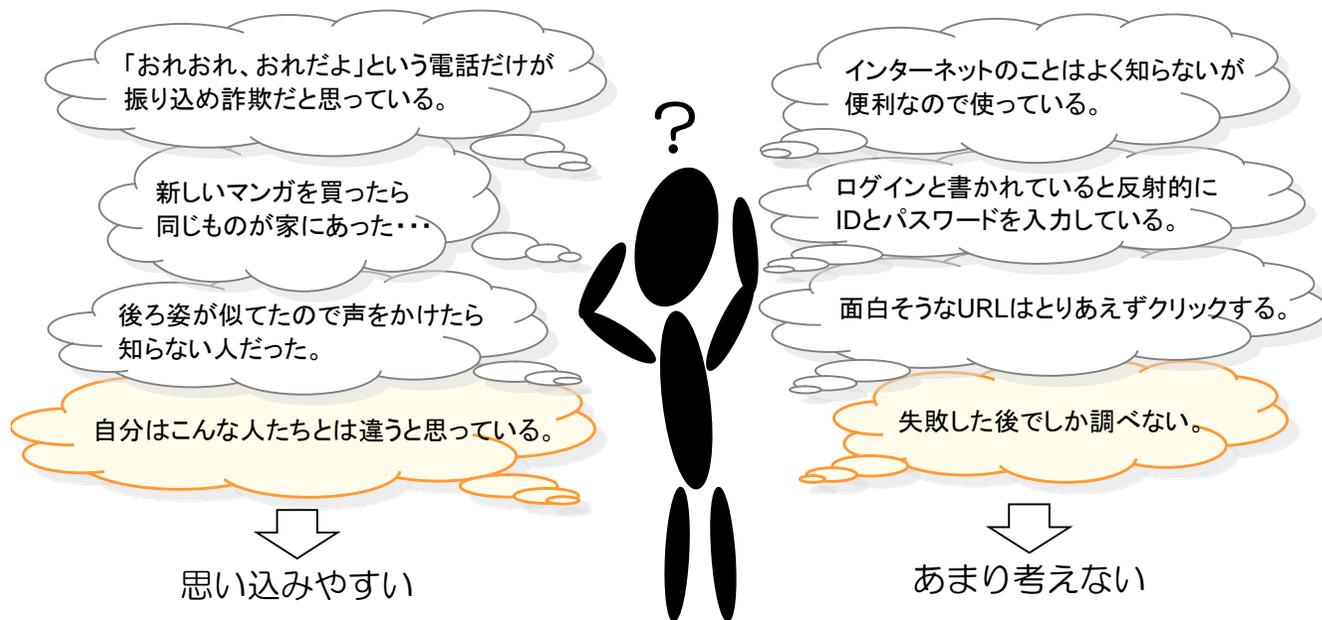
Yahoo! JAPAN ならユーザー多いし、
色々あるから狙ってみるか！

ユーザー数・サービス数の多さ、マネタイズの
容易さがターゲット理由になってしまう・・・



Y! こんな人はフィッシングに要注意

どんな人でも被害に遭う可能性があります。



※ あくまでイメージです。

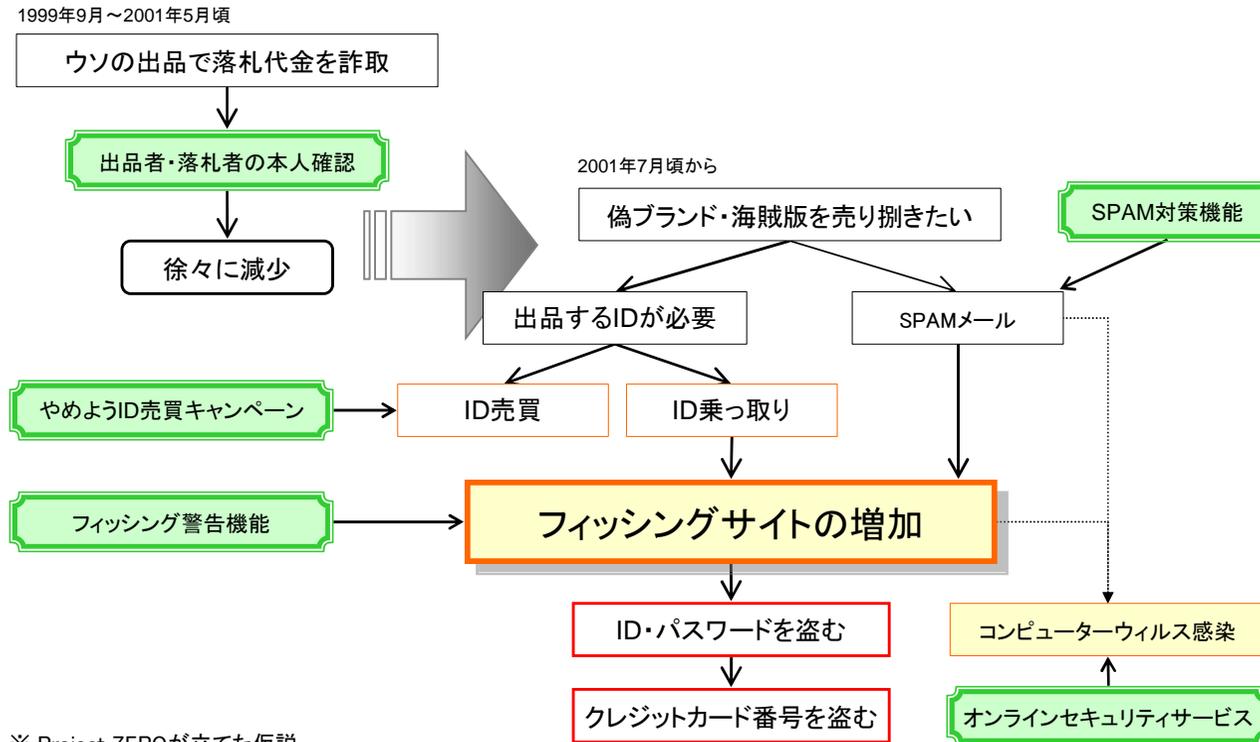


2. 過去から現在までのフィッシングの変遷

Y! (画面をご覧ください)

このページは画面のみのご提供となります。

依然としてYahoo!オークションを騙るケースが多い

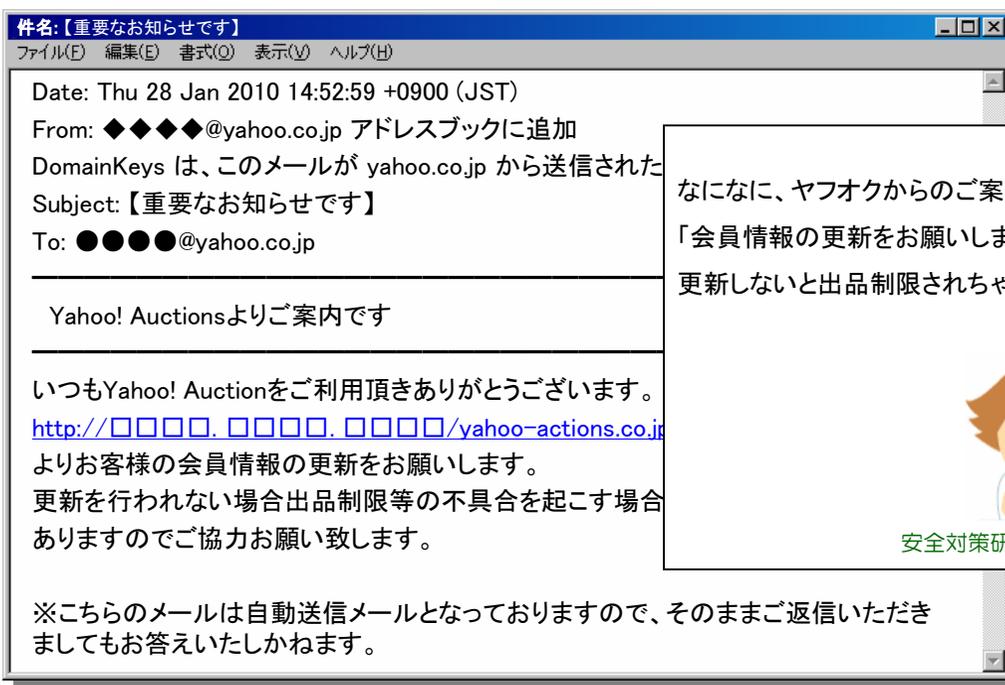


※ Project ZEROが立てた仮説



3. その手口と傾向

効果的タイミングを狙い、信憑性を高める工夫をこらす



なにに、ヤフオクからのご案内?!
「会員情報の更新をお願いします」って
更新しないと出品制限されちゃうのか...



安全対策研究所・助手くん

Y! セキュリティ対策は万全に

ブラウザの脆弱性が狙われる可能性も・・・

氏名と住所とクレジット番号と・・・
これでいいのかな。それからえーっと、
「http 通信であることを確認」って何？！



Yahoo! JAPAN – Yahoo! JAPAN ID登録

http://□□□□. □□□□. □□□□/yahoo-actions.co.jp/index.htm

Yahoo! JAPANプレミアム

重要なお知らせ Yahoo! JAPANを装ったメール、偽の情報
れています。**http通信であることを確認**

お客様情報とお支払い方法を入力して、画面下の「登録」ボタンを押してください。【必須】は入力必須項目です。
※Yahoo! JAPAN IDに登録されている情報は、下記のフォームに自動入力されています。内容が正しくない場合は、修正のうえ、ご登録ください。

登録手順	お客様情報の登録
1. お支払い情報の登録	郵便物をお送りする場合がありますので、ビル、マンション名まで含め、正確に入力してください。
2. 登録内容の確認	名前【必須】: 姓 <input type="text"/> 名 <input type="text"/>
3. 登録完了	フリガナ【必須】: セイ <input type="text"/> メイ <input type="text"/> (全角) 郵便番号【必須】: <input type="text"/> (半角数字) 例) 1110001, 111-0001
	都道府県【必須】: <input type="text"/> (以下より選択してください)
	住所1【必須】: <input type="text"/>
	住所2【必須】: <input type="text"/>
	ビル、マンション名等: <input type="text"/>
	電話番号【必須】: <input type="text"/> - <input type="text"/> - <input type="text"/> (半角数字)

お支払い方法の登録
必要な項目を入力してください。
銀行口座振替をご希望の方は、右のヒントをご覧ください。

お支払い方法【必須】

お客様情報の登録
ヒント
・海外在住の場合はこちらをご覧ください。
・郵便番号から住所検索できない方は、こちらをご覧ください。
・住所2には住所検索した結果の続きを入力してください。

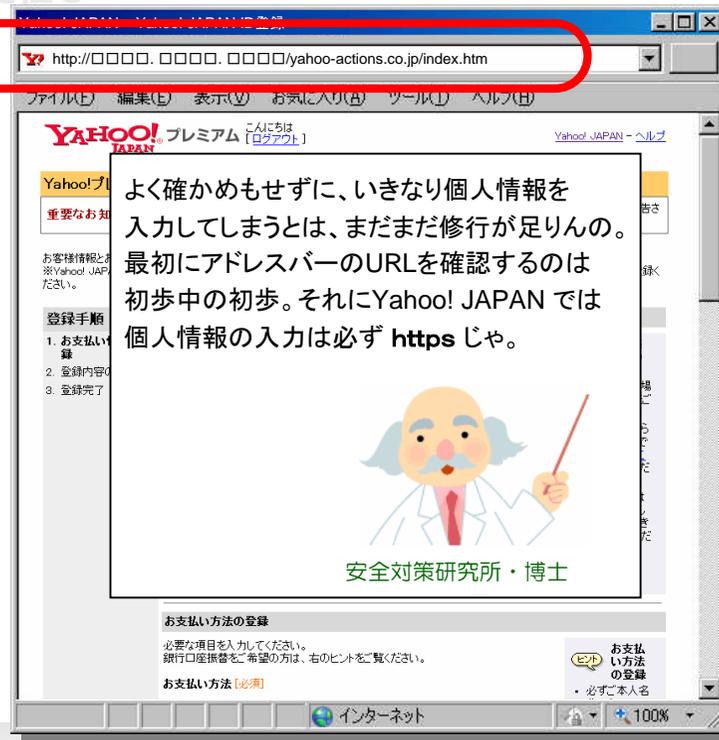
お支払い方法の登録
ヒント
・必ずご本人名

インターネット 100%

Y! セキュリティ対策は万全に

ブラウザの脆弱性が狙われる可能性も・・・

氏名と住所とクレジット番号と・・・
これでいいのかな。それからえーっと、
「**http** 通信であることを確認」って何？！



よく確かめもせずに、いきなり個人情報を
入力してしまうとは、まだまだ修行が足りんの。
最初にアドレスバーのURLを確認するのは
初歩中の初歩。それにYahoo! JAPAN では
個人情報の入力は必ず **https** じゃ。

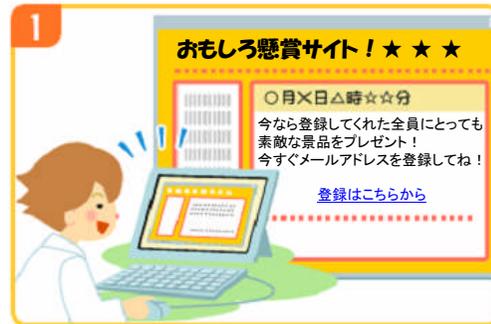
安全対策研究所・博士

お支払い方法の登録
必要な項目を入力してください。
銀行口座振替をご希望の方は、右のヒントをご覧ください。
お支払い方法 **[必須]**

お支払い方法の登録
必ずご本人名

Y! 外部で盗んでYahoo! JAPANで悪用する

1. 「A」という懸賞サイトにYahoo! JAPANと同じパスワードとYahoo!メールのメールアドレスを登録した。
2. 実はその懸賞サイト「A」は犯罪者が運営するサイトだった！



3. 犯罪者は、Yahoo!メールアドレスの@より前の文字列 (Yahoo! JAPAN IDと同じ文字列)と、懸賞サイトに登録されたパスワードでYahoo! JAPANにログインを試した。
4. Yahoo! JAPAN IDのパスワードと懸賞サイトに登録されたパスワードが同一 のためログインに成功し、Yahoo! JAPAN IDを不正利用してオークションに出品されてしまった。

Y! 日本国内のフィッシング詐欺グループ逮捕

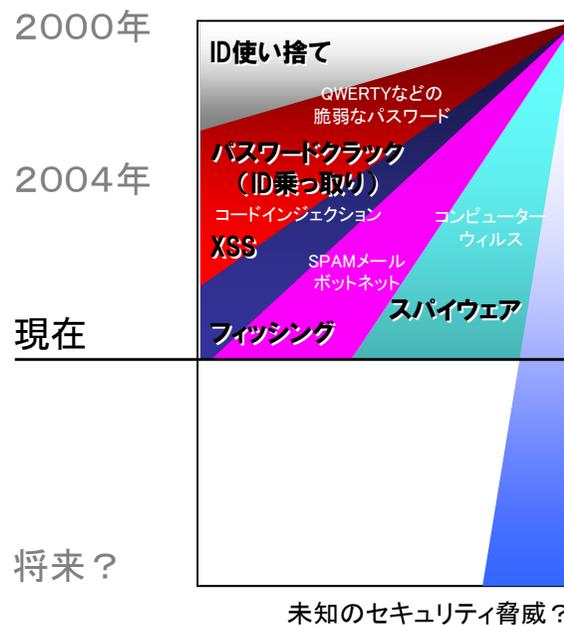
犯人グループの手口

1. 大量のメールアドレスを入手してフィッシングメールを送信
2. フィッシングサイトに誘導してクレジットカード番号を盗み出す
3. 盗み出したクレジット番号でショッピングサイトから家電製品を購入
4. 私設の私書箱に商品を送らせ秋葉原などで転売



Y! 複雑化するコンピューターセキュリティへの脅威

セキュリティの仕事を通して見えてきた手口の移り変わりとは・・・



単純な手口を試行錯誤

サービス提供側を攻撃

利用者側の脆弱性を攻撃

油断していると誰もが被害にあう時代



4. Yahoo! JAPAN の取り組み

Y! Yahoo! JAPANのログインページ

ログインページには様々な機能があります。

重要なお知らせ

さらに使いやすく便利になった「**ログインアラート**」があなたのYahoo! JAPAN IDを守ります！いつでもどこでも不正ログインを検知できるようにケータイのメールアドレスを設定しよう！



Yahoo! ツールバーのフィッシング警告機能は、Yahoo! JAPANであるかのように装い、Yahoo! JAPAN IDやパスワードなどを不正に取得しようとするサイトを表示すると、警告画面を出して注意を促します。

PR



最新のiPhoneを
驚きのプライスで。

iPhone for everybody.
12月から、iPhone 3GS (16GB)
新規ご購入実質負担 **0***
キャンペーン期間 1/31まで。

Yahoo! 携帯ショップなら、
24時間申込受付、送料無料!

YAHOO! 携帯ショップ
JAPAN

Yahoo! JAPANへ
ログインしてください



Yahoo! JAPAN ID:

パスワード:

次回からIDの入力を省略

共用のパソコンではチェックを外してください。



ログイン

Yahoo! JAPAN IDを
お持ちでない方

[Yahoo! JAPAN IDを取得](#)

Y! ログインアラート: ログインをメール通知

認証されたメールアドレスへログインされたことを通知します。

重要なお知らせ さらに使いやすく便利になった「**ログインアラート**」があなたのYahoo! JAPAN IDを守ります！いつでもどこでも不正ログインを知らせてくれるメールアラートのメールアドレスを設定しよう！

Yahoo! ツールバー
Yahoo! ツールバーのフィッシング
ように装い、Yahoo! JAPAN ID
の取得しようとする
警告画面を表示すると、警告画
面が表示されます。

PR

最新のiPhoneを
驚きのプライスで。
iPhone for everybody.
12月から、iPhone 3GS (16GB)
新規ご購入実質負担 **0***
キャンペーン期間 1/31まで。

Yahoo! 携帯ショップなら、
24時間申込受付、送料無料!

YAHOO! JAPAN 携帯ショップ

Yahoo! JAPANへ
ログインしてください

Yahoo! JAPAN ID:
パスワード:

次回からIDの入力を省略
共用のパソコンではチェックを外してください。

 ログイン

Yahoo! JAPAN IDを
お持ちでない方
[Yahoo! JAPAN IDを取得](#)

Y! ログイン履歴

登録情報ページからログイン履歴を見ることができます。

The screenshot shows the Yahoo! JAPAN account management interface. At the top, there is a notification banner for 'Login Alerts' (ログインアラート) with a red circle around the text. Below this, there are several informational boxes, including one about the Yahoo! toolbar and another about login alerts. A red circle highlights a link labeled 'ログイン履歴' (Login History) in the navigation area. Below the navigation, the 'Registration Information Confirmation' (登録情報の確認) section is visible, with a red circle around the 'ログイン履歴' link. The page also shows a user profile picture of a white cat and various settings options.

Y! ログイン履歴：不審なログインの発見手段

身に覚えの無い日時・IPアドレスなどをチェックできます。

YAHOO! JAPAN こんにちは ●●●●さん [\[ログアウト\]](#) Yahoo! JAPAN - [ヘルプ](#)

●●●●さんのログイン履歴 最終更新日時: 2010年01月28日(木曜日) 17時06分

[サービスへ戻る](#)

ログイン履歴ページは、お客様が最近Yahoo! JAPANにログインを試みた履歴を、過去60件分表示しています。
詳細は[ヘルプ](#)をご覧ください。認証形式、IPアドレスなど各項目の意味については「[ログイン履歴ページの見方](#)」をご覧ください。

60件中1~30件を表示しています。 [前の30件 | [次の30件](#)]

Yahoo! JAPAN ID / ニックネーム	日時	サービス	認証形式	認証結果	IPアドレス	端末情報
●●●●	2010年01月28日(木) 17時06分53秒	トップページ	パスワード再確認	成功	192.168.8.248	パソコン
●●●●	2010年01月28日(木) 17時06分45秒	トップページ	ログイン	成功	192.168.8.248	パソコン
●●●●	2010年01月28日(木) 16時56分52秒	トップページ	パスワード再確認	成功	192.168.8.248	パソコン
●●●●	2010年01月28日(木) 16時56分36秒	トップページ	ログイン	成功	192.168.8.248	パソコン
●●●●	2010年01月28日(木) 10時07分54秒	トップページ	ログイン	成功	192.168.8.248	パソコン
●●●●	2010年01月27日(水) 13時38分24秒	トップページ	パスワード再確認	成功	192.168.8.248	パソコン
●●●●	2010年01月27日(水) 11時23分03秒	トップページ	ログイン	成功	192.168.8.248	パソコン
●●●●	2010年01月26日(火) 08時44分54秒	トップページ	ログイン	成功	192.168.8.248	パソコン
●●●●	2010年01月22日(金) 13時39分33秒	トップページ	ログイン	成功	192.168.8.248	パソコン

Y! Yahoo!ツールバー ver.7.3: フィッシング警告機能

Yahoo!ツールバー ver.7.3以降でフィッシング警告機能が強化されました。



SSLで保護されたYahoo! JAPANのページを表示したときは緑色に変わります。

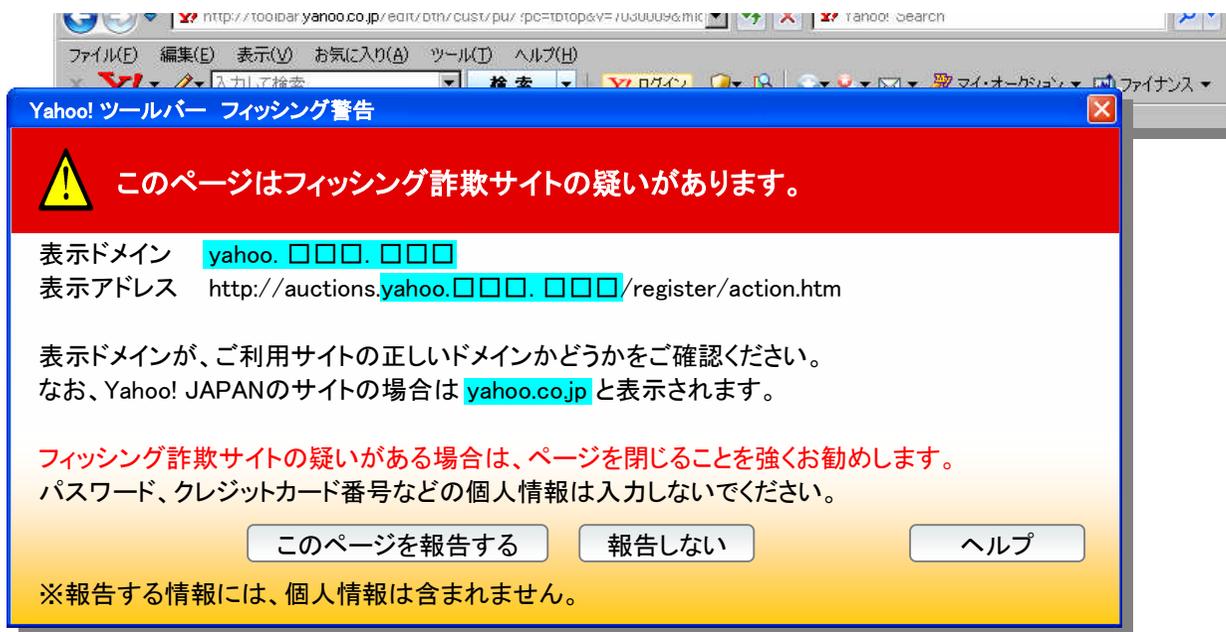


個人情報の入力に注意が必要なときは、ボタンの色がオレンジに変わってお知らせします。

Windows版 Yahoo!ツールバーVer.7.3以降

Yahoo!ツールバー: フィッシングサイトを警告

Yahoo!あんしんねっと からフィッシングサイト情報を取得してお知らせします。



Yahoo! ツールバー フィッシング警告

 このページはフィッシング詐欺サイトの疑いがあります。

表示ドメイン yahoo. □□□. □□□
表示アドレス http://auctions.yahoo.□□□. □□□/register/action.htm

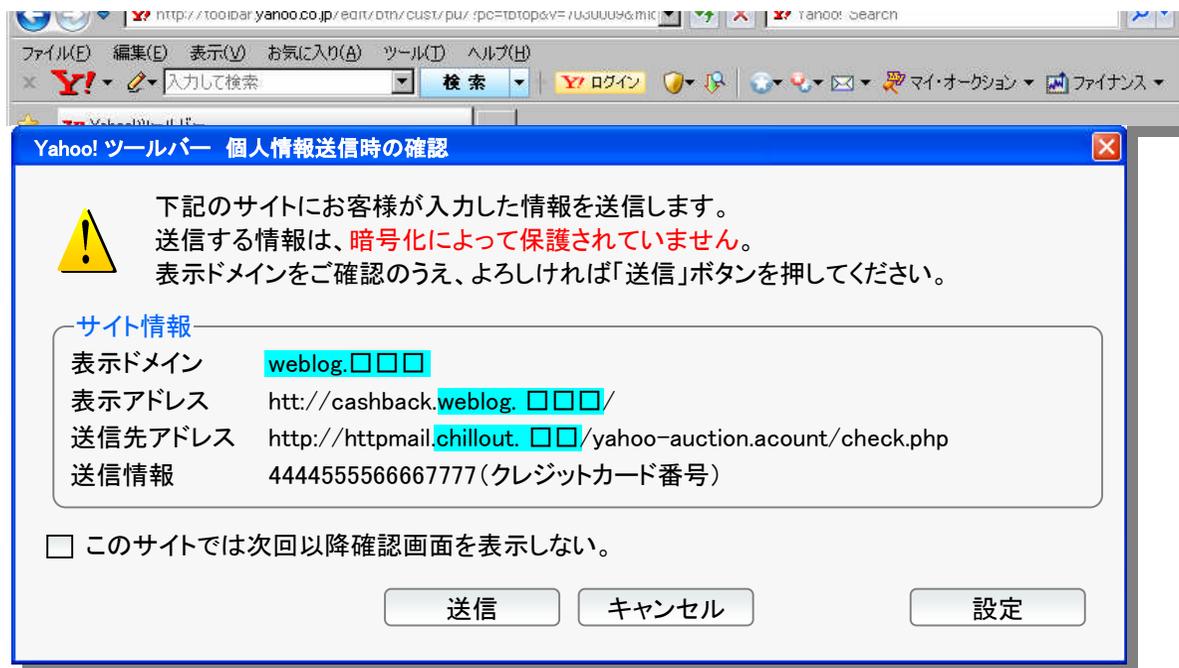
表示ドメインが、ご利用サイトの正しいドメインかどうかをご確認ください。
なお、Yahoo! JAPANのサイトの場合は yahoo.co.jp と表示されます。

フィッシング詐欺サイトの疑いがある場合は、ページを閉じることを強くお勧めします。
パスワード、クレジットカード番号などの個人情報は入力しないでください。

※報告する情報には、個人情報は含まれません。

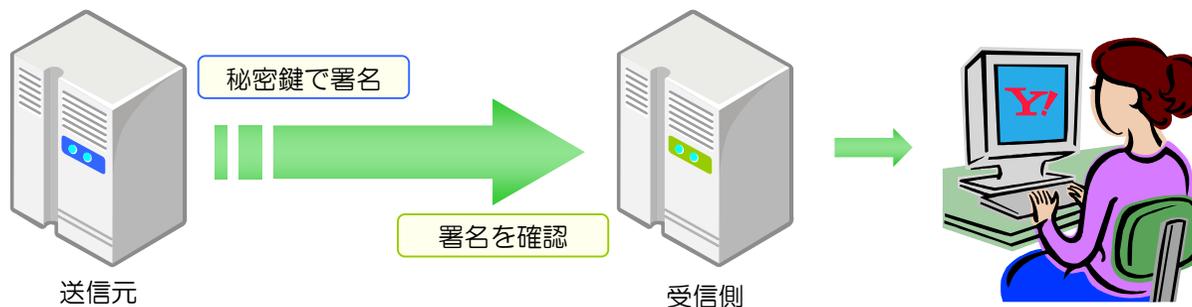
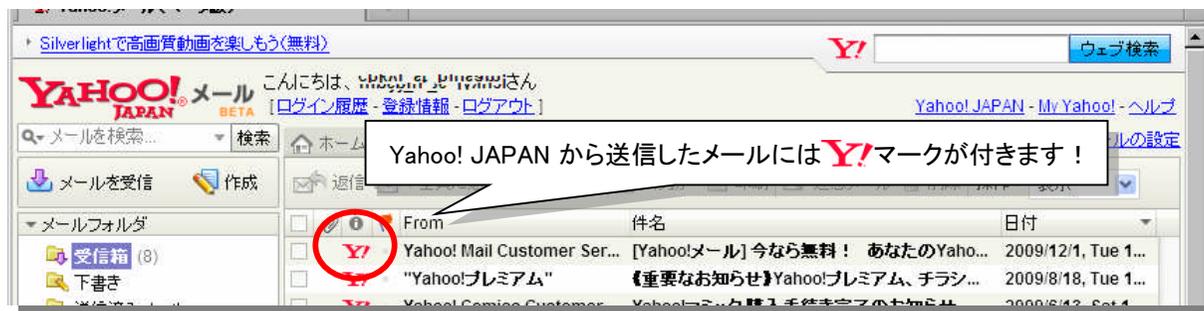
Y! Yahoo!ツールバー ver.7.3: 個人情報の送信を確認

クレジットカード番号などの重要情報送信を判定してお知らせします。



Y! Yahoo!メールのフィッシング対策機能

Yahoo!メールを使うと、Yahoo! JAPANからのお知らせが一目でわかります。



Y! 啓蒙活動への取り組み

多くの人を訪れるYahoo! JAPANだからできる取り組み

The screenshot displays the Yahoo! JAPAN homepage with several security-focused banners and articles. At the top, a banner reads "セキュリティ特集 2009 秋" (Security Special 2009 Autumn) and "Yahoo! JAPANはインターネットの安全な利用と健全な発展を目指しています。" (Yahoo! JAPAN aims for safe use and healthy development of the internet). Below this, a large banner for "Yahoo!オークション 安全対策研究所" (Yahoo! Auctions Security Research Institute) features an illustration of a doctor and an assistant. The doctor says, "よくあるトラブルを4つのケースで紹介しているぞ。興味のあるものから見ていくのじゃ。" (I'm introducing common troubles in 4 cases. Let's look at the ones you're interested in). The assistant asks, "どんな手口があるんですか?" (What kind of methods are there?). To the left, a "Yahoo! JAPAN IDガイド" (Yahoo! JAPAN ID Guide) article is highlighted, listing topics like "利用開始ガイド" (Getting started guide) and "おすすめの使用法" (Recommended usage). At the bottom, a "STOP 警察庁による検挙数最新データ" (STOP: Latest arrest statistics by the National Police Agency) banner states that cyber-crime cases have increased 3 times in the past 5 years and that 98% of cases are related to mobile phones. Other smaller banners mention "ボイズニング、検索結果の上位に不正リンク" (Boyznig, illegal links in top search results) and "PCのエラー修復やリカバリなどでできるユーティリティソフト(BGN)" (Utility software for PC error repair and recovery).

Y! やめようID売買(啓蒙活動のご紹介)



Yahoo! JAPANでは、Yahoo! JAPAN IDの第三者への譲渡、貸与などを禁止しておりますが、残念ながら売買されるケースが確認されています。売買されたYahoo! JAPAN IDは、詐欺などの不正行為を行う第三者に渡り、悪用されていますので絶対にやめましょう。

権利譲渡および商用目的使用の禁止 ([Yahoo!オークションガイドライン](#)より)

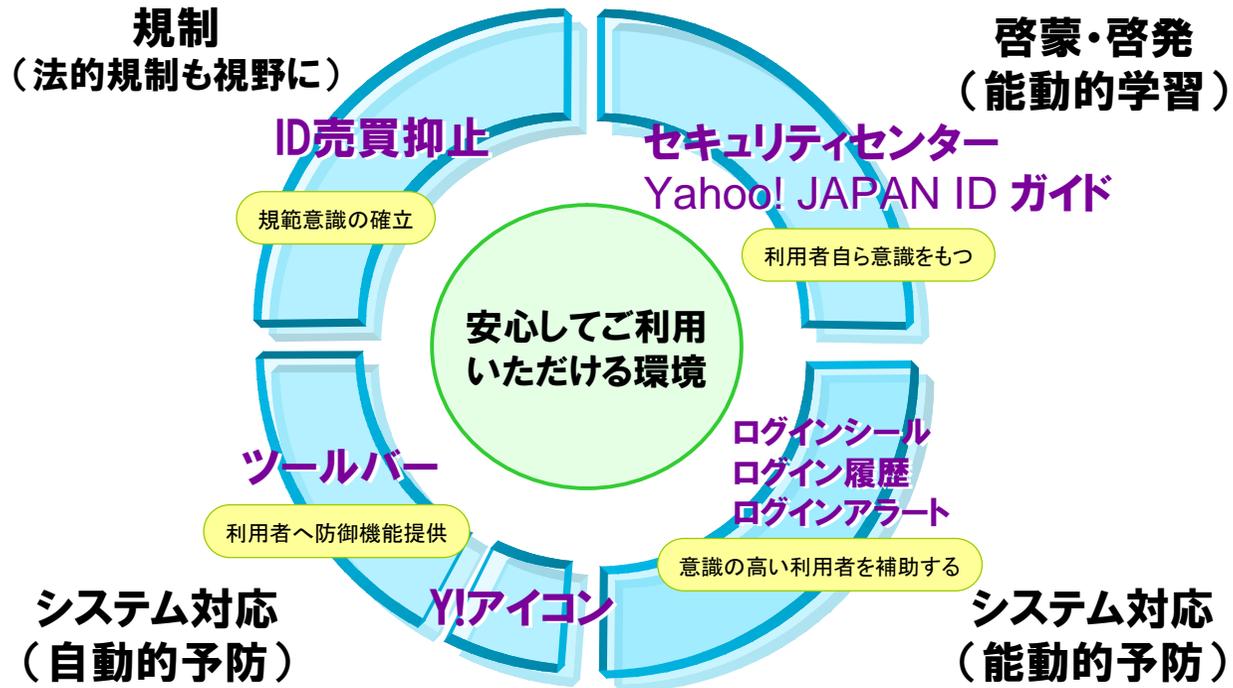
利用者は、このガイドラインの定めに従って取得した権利義務およびYahoo! JAPAN IDを第三者に譲渡、貸与等してはならないものとします。また利用者はYahoo!オークションをYahoo! JAPANのガイドラインで定める使用範囲、使用方法を超えて、Yahoo! JAPANの許可なく商用の目的で使用してはならないものとします。

みなさんをお願いしたいこと

Yahoo! JAPAN IDの第三者への譲渡、貸与等は有償、無償を問わず一切行わないでください。また、売買を持ちかけるメールやウェブサイトなどを発見した場合には Yahoo!オークションまでご報告ください。皆さまのご協力が安全なYahoo!オークションの礎になります。



Y! 安心して利用できるインターネット環境へ





5. 今後の見通し

Y! (画面をご覧ください)

このページは画面のみのご提供となります。



LIFE ENGINE™

ありがとうございました。