最新個人情報漏洩事件・関連ニュース

LATEST

DATE：2022.06.17

サイバーセキュリティ.com　SecurityNEXT、jiji.com、Yahoo!NEWS

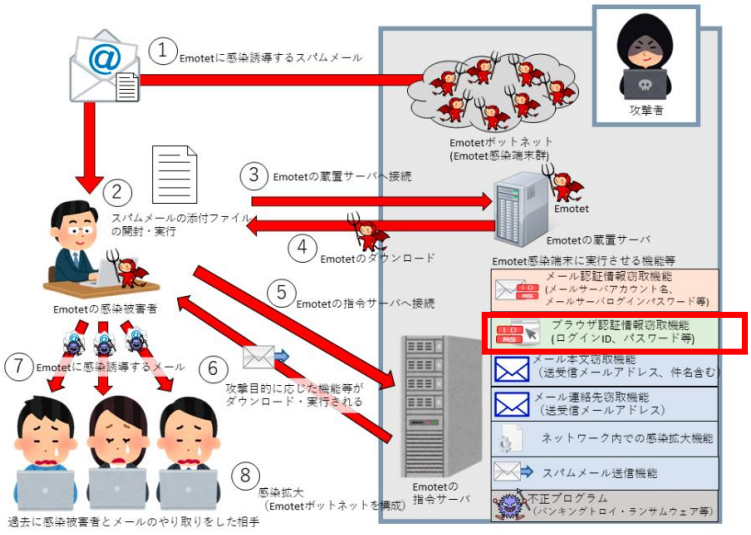
- 06月15日：スニーカーダンク、不正アクセス原因で約275万件の顧客情報流出か
- 06月15日：委託先がEmotet感染でアドレス流出か、相模原市が謝罪
- 06月15日：相次ぐ感染被害報告、砺波自動車学校でもEmotet不審メール
- 06月15日：神奈川県が偽サイトに注意喚起 － マルウェア感染のおそれ
- 06月14日：Emotet感染で不審メールや情報流出の懸念、愛三種苗株式会社
- 06月14日：ホームセンターのナフコが不正アクセス被害
- 06月14日：徳島市の偽サイトに注意 － 個人情報詐取されるおそれ
- 06月14日：ヤマト運輸を装うメールやなりすましサイトに注意を
- 06月13日：従業員がフィッシング被害で情報流出の可能性、矢野経済研究所
- 06月13日：不正アクセスでカード情報や取引データ流出か、誠和
- 06月13日：「Emotet」感染でアカウント奪われ、大量のメール送信 － 埼大
- 06月10日：脆弱性が原因で不正アクセス、カード情報や顧客情報流出か
- 06月09日：J&T環境株式会社、サイト改ざんで不審メール発生
- 06月09日：Emotet感染でChromeのクレカ情報が盗まれる。警察庁が警告
- 06月08日：高齢者支援施設名乗る不審メール出回るもマルウェア感染確認されず － 仙台市
- 06月08日：サイト改ざんで迷惑メール送信の踏み台に － リサイクル事業者
- 06月07日：勤怠システムがランサム被害、総当たり攻撃で侵入か － ヴィアックス
- 06月07日：フィッシング攻撃、地域密着の信販会社を立て続けに標的に

PICKUP!

Emotetに新機能、警察庁が警告「Google Chrome のクレカ情報標的に」

出典：2022年6月9日警察庁Emotetの解析結果について
https://www.npa.go.jp/cyberpolice/important/2020/202012111.html

ブラウザ認証情報窃取機能、追加を確認。Chromeのクレカ情報が標的に



*ウェブブラウザ「Google Chrome」に保存されたクレジットカード番号や名義人氏名、カード有効期限を盗み、外部に送信する機能が追加されたことを確認しました。Google Chromeでは個人情報を暗号化して安全に保存していますが、**Emotetの新機能は暗号データを元に戻すための鍵も同時に盗み出すため、Emotetに感染すると、お使いのクレジットカード情報が第三者に知られるおそれ**があります。*

※引用：2022年6月9日警察庁Emotetの解析結果について

Emotet再び活発化の恐れ　JPCERT/CC　EmoCheck2.3.2　リリース

PICKUP!

出典：2022年5月27日 JPCERT/CC
https://www.jpcert.or.jp/at/2022/at220006.html

マルウェア「Emotet」に新機能
JPCERT/CCが注意喚起
感染チェックツールをアップデート

図　「Emotet」v2.3.2

動作確認環境

- Windows 11 21H2 64bit 日本語版
- Windows 10 21H2 64bit 日本語版
- Windows 8.1 64bit 日本語版
- ~~Windows 7 SP1 32bit 日本語版~~
- ~~Windows 7 SP1 64bit 日本語版~~

NEW！
Emocheck最新版でチェック
してください！

JPCERT/CC 提供

感染チェックツール「EmoCheck2.3.2」

JPCERTCC/EmoCheck - GitHub
https://github.com/JPCERTCC/EmoCheck/releases

EmoCheckの使用方法や更新履歴など
https://github.com/JPCERTCC/EmoCheck/blob/master/README_ja.md

参考情報

マルウェアEmotetの感染再拡大に関する注意喚起
Emotetに関する最新動向
https://www.jpcert.or.jp/at/2022/at220006.html

5月27日更新
マルウェアEmotetの感染再拡大に
関する注意喚起

マルウエアEmotetへの対応FAQ
Emotetに関する情報、対応を確認
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

解説動画
社内周知
注意喚起に

JPCERT/CC 提供

日本中で感染が広がるマルウェアEMOTET
JPCERTCC/Emotetの解説動画
https://youtu.be/wvu9sWiB2_U

EMOTET感染の確認方法と対策
JPCERTCC/Emotetの感染確認方法と対策解説動画
https://youtu.be/nqxikr1x2ag

フィッシングURL件数が過去最多18,591件、大量の偽サイト

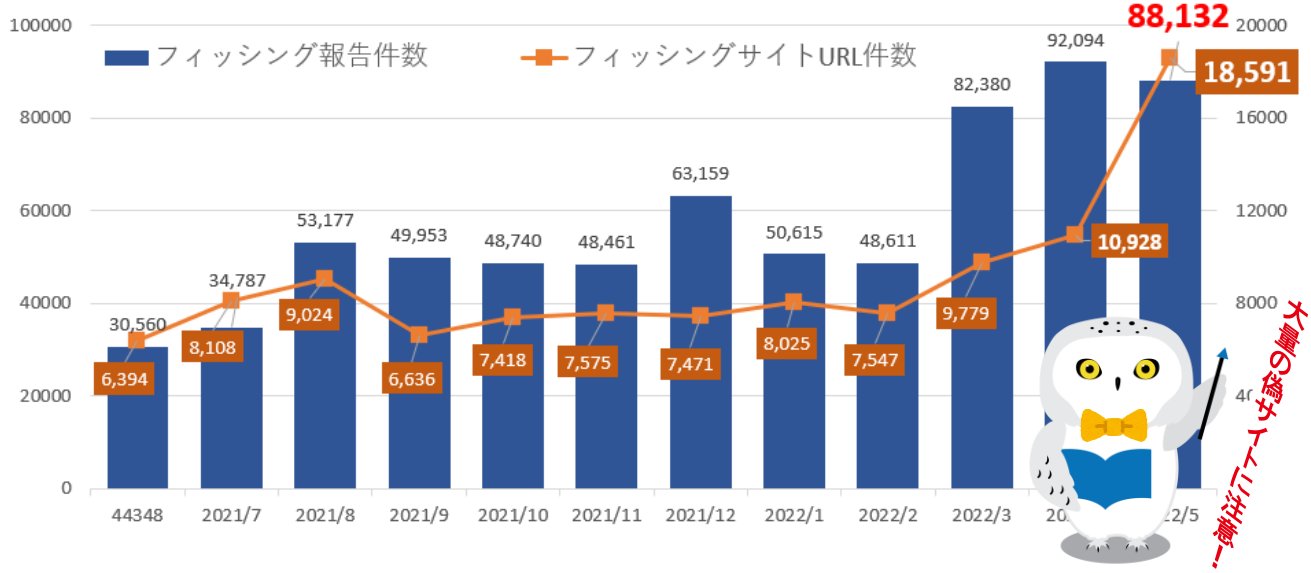
PICKUP!

出典：2022年6月3日 フィッシング対策協議会
https://www.antiphishing.jp/report/monthly/202205.html

フィッシングURLが約1.7倍、過去最多更新
同一IPアドレス上に大量の偽サイト

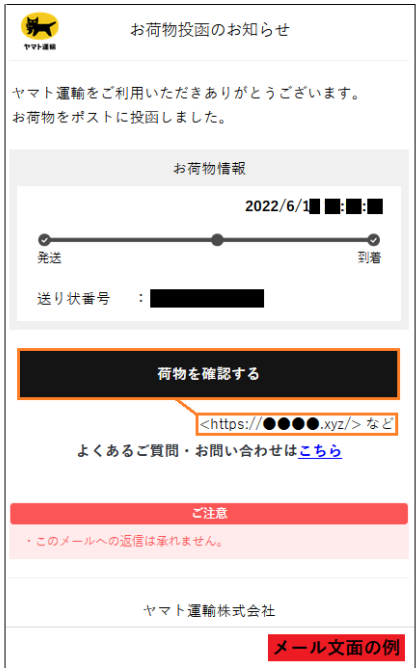
5月にフィッシング対策協議会へ報告されたフィッシングサイトのURL件数が、前月の1.7倍と急増した。悪用されたブランドとともに過去最多を更新している。

1日平均 約2843件



フィッシングサイトにご注意ください。

2022年06月15日　ヤマト運輸をかたるフィッシング
2022年06月03日　日専連ファイナンスをかたるフィッシング
2022年06月02日　東京電力をかたるフィッシング
2022年06月02日　ゆうちょ銀行をかたるフィッシング
2022年05月30日　九州カードをかたるフィッシング


お荷物投函のお知らせ

ヤマト運輸をご利用いただきありがとうございます。
お荷物をポストに投函しました。

お荷物情報

2022/6/1[redacted]

発送　到着

送り状番号　：[redacted]

荷物を確認する

<https://●●●●.xyz/> など

よくあるご質問・お問い合わせはこちら

ご注意

・このメールへの返信は承れません。

ヤマト運輸株式会社

メール文面の例


【ヤマト運輸】いつも大変お世話になっております。
重要なお荷物が届きましたが、荷物に不備があり、受取人と連絡が取れませんでした。
お客様がこの荷物の受取人であるかどうかを確認したく、ご連絡させていただきました。
そのため、下記をご覧いただき、受取情報をご確認ください。
できるだけ早く、再度の配送を手配いたします。

→確認はこちら

[redacted] の部分のリンク
<https://safeyamatoonline●●●●.top/index.php> など

お客様にはご不便、ご心配をおかけして申し訳ございませんでした。
ご理解いただきますようよろしくお願いいたします。
48時間以内に確認が取れない場合、お荷物は返却されますのでご注意ください。

電話 03-3541-3411
ヤマト運輸株式会社
YAMATO TRANSPORT CO., LTD

メール文面の例

政府機関や自治体の「偽サイト」に注意喚起

PICKUP!

出典：2022年6月15.日 内閣官房内閣サイバーセキュリティセンター：
https://www.nisc.go.jp/pdf/press/20220615NISC_press.pdf

我が国の公的機関や企業等の偽サイトにご注意ください（注意喚起）

続出する公的機関の偽サイト
検索エンジン経由でも偽サイトに誘導されてしまうこともある
「必ずドメインを確認して」

長野市や神奈川県などの自治体が注意喚起しているほか、金融庁や文部科学省、総務省、デジタル庁などの省庁も偽サイトに注意を促している。

令和４年６月１５日
内閣官房内閣サイバーセキュリティセンター

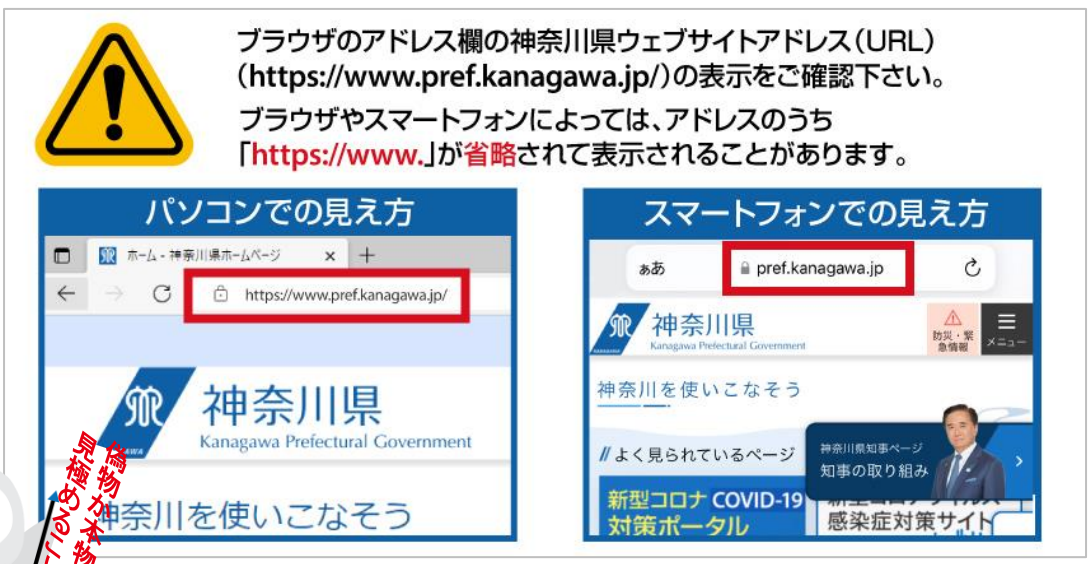
我が国の公的機関や企業等の偽サイトにご注意ください（注意喚起）

我が国の政府機関や地方公共団体などの公的機関、企業・団体等の本物の Web サイトと同じ内容を表示する偽サイトの存在が確認されています。これらの偽サイトのうちには、クリック先が悪質なサイトへのリンクに置き換えられているものがあり、サイバー犯罪等に用いられる可能性があります。

URL リンクから他の Web サイトに行くなど普段と異なる方法で利用する際は特に、リンクにポインタを置く、アドレス欄をよく見る等により、URL のドメイン名を必ず確認してからにしてください。

ドメイン名が正規の公的機関等と無関係なものであるなど不審と思われる場合には、別の検索エンジンを利用するなどの方法で本物の Web サイトの URL を確認してください。不審な場合には、安易にアクセスしたり、当該 Web サイト上の何かをクリックしたり絶対にしないでください。

政府においては、サイバーセキュリティ関係機関等とも連携しながら、引き続き被害の拡大防止に努めてまいります。



出典：神奈川県Webサイトより

従業員がフィッシング被害で情報流出の可能性、矢野経済研究所

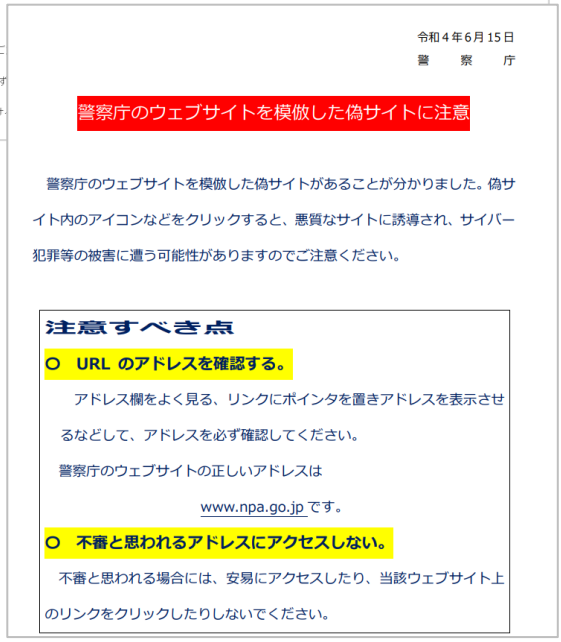
PICKUP!

出典：2022年6月8.日 矢野経済研究所弊社アドレスからの不審メールに関するお詫びとお知らせ
https://www.yano.co.jp/announce/778

弊社アドレスからの不審メールに関するお詫びとお知らせ

この度、２０２２年６月３日に、弊社の従業員（１名）のパソコンで、誤ってフィッシングサイトにアクセスしたことにより、同従業員のMicrosoft 365のIDとパスワードが窃取されました。その結果、６月７日に、同従業員のメールアカウントから、不審なメールが複数の方へ発信されている事実を確認いたしました。（確認後、直ちに当該アカウントのパスワードを変更し、以降の不正アクセスができないよう措置を済ませております。）

フィッシングサイトが急増で政府機関も注意喚起
フィッシングからの被害にご注意ください



メルカリを装う偽サイト出現、公式が注意喚起

PICKUP!

出典：2022年6月14日 【重要】メルカリを装った不審なサイトにご注意ください：
https://jp-news.mercari.com/articles/2022/06/14/security/

メルカリを装う偽サイト出現、公式が注意喚起
「手口が巧妙化し本物と区別がつきにくい」

https://jp-news.mercari.com/articles/2022/06/14/security/

【重要】メルカリを装った不審なサイトにご注意ください

公開日：2022-06-14

重要なお知らせ

お客さまの安全のため、継続してご案内しております。

現在、メルカリを装った不審なサイトを確認しております。

詐欺の手口は非常に巧妙になっており、メルカリ公式サイトとの区別がつきにくくなっています。

以下に該当する場合には、メルカリの公式サイトではございません。フィッシングサイトの可能性がございますのでご注意ください。

最新のフィッシング詐欺の手口例

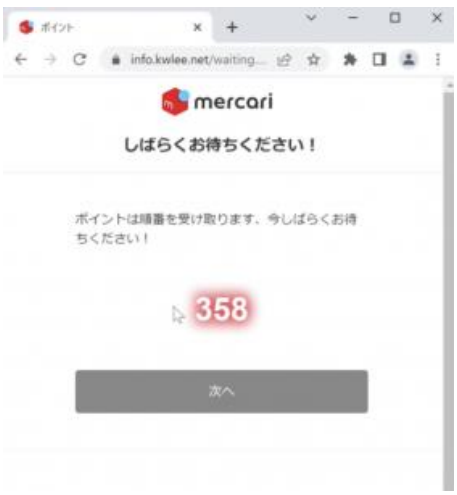
■ログイン情報や認証番号を入力後、画面上にカウントダウンが表示される（または、一定時間待たされる）

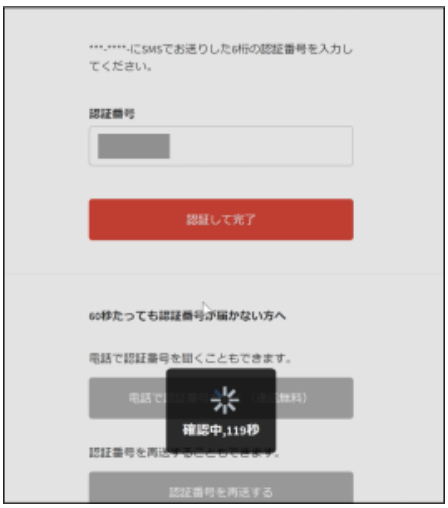
悪意のある第三者が入力情報を確認し、実際にメルカリのアカウントへのログイン等を試すための時間稼ぎとして、ログイン情報や認証番号を入力後にカウントダウン表示を出す場合があります。

*フィッシングサイト画面

最新のフィッシング詐欺の手口例

■ログイン情報や認証番号を入力後、画面上にカウントダウンが表示される（または、一定時間待たされる）
悪意のある第三者が入力情報を確認し、実際にメルカリのアカウントへのログイン等を試すための時間稼ぎとして、ログイン情報や認証番号を入力後にカウントダウン表示を出す場合があります。





その他の手口、被害にあった場合の対処など
https://help.jp.mercari.com/guide/categories/550/