迷惑メールの見分け方

詐欺メール　見分け方の基本

脅迫、架空請求や不正サイトに誘導してID・パスワードを詐取する詐欺メールが送信されてくることがあります。
ほとんどはプロバイダーで迷惑メールとして振り分けてくれるのですが、中にはそれをすり抜けて届く場合があるので注意が必要です。
次のことを基本に詐欺メールを見分けてください。

差出人が違う

- 差出人のメールアドレスが正しいか確認します。企業からのメールであるのに個人のメールアドレスだったり、その企業とは違う組織のアドレスだったりしていないか？（ただし、差出人のメールアドレスは偽装の可能なので注意）

本文の内容がおかしい

- 本文の文章が日本語になっていなかったり、つじつまが合わなかったり、自分が覚えのない契約をしていると書かれていたりしていないか？
- システム障害が発生したというような場合、その企業のホームページを見れば本当か確認できます。

リンク先のURLが違う

- 「ここからログイン・・・」というようなことが書かれている場合、リンク先のアドレスが本当にその企業等のアドレスか確認します。

詐欺メールの例(1)

差出人が、Amazon <apikey@customeramazonservicemail.top>
で本文が次のような内容のメールが届いた。

Amazonからのメールだというのに、ドメイン名がAmazonではない


amazon.co.jp

Amazon からのお知らせ

Amazon サポート | Amazon アソシエイト

弊社のモニタリングにより。普段と違う不審なログインが見つかり。誰かがお客様のいつもお使いになった支払方法を変更しようとしていたそうです

あなたの Amaz o n のアカウント:

ログイン日時:2021/03/14 14:04:54

IP アドレス:42.148.125.73

装備:Linux; Android 8.1.0;O PM1.171019

場所:新潟県 新潟市中央区

Amazon 会員個人情報を確認する必要があります。今アカウントを確認で

続けるにはこちらをクリック

日本語の文章がおかしい

リンク先が「http://***.customeramazonservice.club/」でAmazonではない

詐欺メールの例(2)

差出人が、MyJcb <ilhd@my.jcb.co.jp>
で本文が次のような内容のメールが届いた。

ドメイン名はJCBに間違いない

JCBカードをご利用のお客さま

貴方のJCBクレジットカードでは海外交易があると発見しました。

安全性のため、そちらと連絡を取れる前に、我々はクレジットカードの一部の使用権限を制限しました。

ご了承の程、宜しくお願いします。また、返信がない場合、クレジットカードの使用は引き続き制限されます。

利用いただき、ありがとうございます。

▼海外取引確認

https://my.jcb.co.jp

▼カードの使用制限が解除される

https://my.jcb.co.jp

※一部、MyJCBを利用できないカードか

※本メールの送信アドレスは自動送信専

※本メールに心当たりのない方、お問い合わせを希望の方は、下の問い合わせ先までご連絡ください。

<本件に関するお問い合わせ>

354または355から始まるカードをお持ちの方 JCBインフォメーションセンター

https://my.jcb.co.jp.lynndon.com/

3573から始まるカードをお持ちの方 JCBデビットカードデスク

https://my.jcb.co.jp.lynndon.com/

日本語の文章がおかしい

実際のリンク先は「https://***.raymendez.com/」でJCBではない

詐欺メールの例(3)

差出人が、【三井住友信託銀行】<Mail_Direct@smtb.jp>で
本文が次のような内容のメールが届いた。

ドメイン名は、三井住友信託銀行に間違いない

実際のリンク先は「http://www.smtbjp.org/」で三井住友信託銀行ではない

最近、三井住友信託銀行はお客様の口座資金のセキュリティを高めるために、全面的にシステムのバージョンアップを行いました。すぐに口座の更新をお願いします。

こちらのURLをクリックしてください
https://direct.smtb.jp/ap1/ib/login.do

一応日本語にはなっているが、そもそもこれだけの説明で操作させようとすること自体がおかしい(「口座の更新」の説明もなし)

・本メールの送信元のアドレスは配信専用です。
・本メールにお心当たりのない方は、下記ダイヤ

■三井住友信託銀行インフォメーションデスク 0120-977-641
【受付時間】
平日 9：00～17：00　土・日・祝日 9：00～17：00
※当面の間、受付時間を17：00までとさせていただいております。

◆◇◆――――――――――――――――――――◆◇◆

詐欺メールの例(4)

情報処理推進機構への相談例から

口座からのお支払い

A [redacted]co.jp
宛先 [redacted]ne.jp

初めまして！

残念なお知らせをするために、ご連絡を差し上げております。
僕は、約2～3ヶ月前にネット閲覧用に貴方が利用しているデバイスにアクセスし、その後ずっとネット行動を追跡していました。

アクセスするまでの経緯は、
少し前にハッカーからメールアカウントへのアクセスを購入したからです(最近では、そういったものをネット上で購入するのは、かなり単純です)。
だから、貴方のメールアカウント ([redacted]ne.jp)にも簡単にログインができました。

ログインの1週間後には、既にトロイの木馬というマルウェアを、貴方のメールと繋がっている全てのデバイスのオペレーティングシステムにインストールしました。
実際、やってみると全く難しくありませんでしたよ。(受信トレイのメールのリンクを何も問題なくたどっていただき、ありがとうございました。)
巧妙な手口は意外と全て単純なのです。(^^)

そのソフトウェアによって、貴方のデバイスの操作を全て可能になりました(例えば、マイク、ビデオカメラ、キーボードの操作)。
既に、貴方の個人情報、データ、写真、ウェブ閲覧履歴を僕のサーバーにダウンロードし保存してあります。
貴方のメッセンジャー、SNS、メール、チャット履歴、連絡先一覧の全てにも僕はアクセス済みです。
僕のウイルスはドライバレベルで動作し署名を継続的に更新するため、ウイルス対策ソフトウェアでは検知されません。

同様に、この手紙がなぜウイルス対策のソフトウェアに検出されなかったのかの理由も、今ではご理解いただけていると思います・・・

貴方の情報を収集している間に、貴方はアダルトサイトの大ファンだということを発見しました。
ポルノサイトを訪問して、とてつもない快楽に耐えながら、興奮するような動画を閲覧するのが本当にお好きなようですね。
偶然にも、貴方の卑猥なシーンを録画することに成功したので、貴方の自慰行為と絶頂に達する姿を見せるような動画数本をモンタージュにしました。

もし嘘だと思うのであれば、僕のマウスを数回クリックするだけで、全ての動画が貴方の友人、同僚や親戚とシェアできることを実現いたしましょう。
僕的には、パブリックアクセスにしてしまっても問題はありません。
貴方の好きな動画の趣向を考慮しても、そんな動画を公にされたくはないはずです。(僕の言いたいことは分かるでしょう)公になったら、本当の大惨事になるかもしれませ

なので、ここで取引をしましょう。
16万円 (送金時の為替レートに応じたビットコイン相当額)を僕に送金してください。送金を受け取ると、この卑猥な動画は全て削除しましょう。
その後は、お互いのことは綺麗さっぱり忘れてしまい、貴方のデバイスにある有害なソフトウェアの機能を停止して削除することを約束します。僕は言ったことは守ります。