

迷惑・詐欺メールにご注意

まごひち瓦版

ライフスタイルに関する情報をもっと知りたい
貴方にお届けする地元企業発行のかわら版です

迷惑・詐欺メール

スマートフォンやパソコン、毎日の生活でとても役に立っていますね。スマホのない生活なんて想像することできないほど、様々な情報に気軽にアクセスでき、便利な世の中になったなあって思う毎日です。でも、広告、なりすまし、詐欺、架空請求メールなどが届くことも増えていませんか。携帯・スマホ・パソコンを利用するにあたって、不審なメールは開かない、返信しない、添付ファイルを開かない、リンクをクリックしない。アプリは公式ストア以外からはインストールしない。というような注意は皆さん知っておられると思うし、明らかに詐欺っぽいタイトルや文面、不自然な日本語のメールは無視していると、思うのですが、例えば下記のような、日常からお世話になっているサイトをかたるメールだったらどうですか？

銀行、アマゾン、楽天、ヤフー、クレジットカード会社、宅配業者、国税庁、PayPay、その他よく利用しているショッピングサイトや団体名称

- さらにタイトルが不安を煽るものであったり、次のような文言があった場合はどうでしょう？
- 再配達手続きのお願い
- 入金の確認ができません
- カード情報更新のお願い
- 自動退会処理について
- 税務署からのお知らせ
- 未払いのお知らせ
- アカウント認証のお願い
- カード利用制限について
- プレゼントキャンペーン
- 〇〇が当たるプレゼント
- ☆☆円が当たりました。
- 受け取り方法は：
- アンケートに答えてポイントプレゼント
- あなたのメールアドレスが公衆トイレに書かれています
- メモリーが上限に近づいています、メール受信ができません

こういった文面のメールは必ずリンクからお客様情報を更新して下さいとか、それに類する入力を求められます。びっくりして一生懸命個人情報を入力していませんか？

ちよつと待って!!
そのメール、本当に正しい団体からのものですか？

登録済みのサイトであれば、マイページからご自身の登録情報に間違いがないか、登録カード情報、購入履歴などが確認できます。

メールの送り主、例えば税務署とか銀行を騙る場合、何故あなたのアドレスを知っているのでしょうか？登録しましたか？

「お支払いが確認できません」と書かれていた場合、あなたは注文あるいは利用をしましたか？

メールアドレスを盗み出してあなたに送るのではなく、多くの場合、文字や数字を組み合わせたアドレスに送り、届いて反応が返ってくれば（個人情報が入る）成功というわけです。



何故このメールが来たのかな？と感じたら、その差出人のメールアドレスに注目しましょう。

意味のないアルファベットの羅列であったり、本来利用登録している企業のメールアドレスとは異なるものではありませんか？！

なかにはとても巧妙に偽アドレスが作られていて本物のアドレスと区別できないものもあるかもしれません。

ヤフー、楽天、アマゾンなど大手ショッピングサイトを騙るメールのアドレスのなかには、ほとんど区別できないものもありますし、本文中のロゴやページ構成画像も実サイトそっくりです。ので要注意です。

見知らぬ宛先に向けて注文商品の発送連絡など、身に覚えのない商品購入を騙るメールが届いた場合でしたら、メールは無視して、マイページの購入履歴を確認すれば真偽の判断ができます。

疑わしいメールのリンクから、アドレスやクレジットカード情報、パスワードを打ち込んではいけません!!
ご自身に覚えのない利用に関するメールは詐欺メールだと疑うのが安全です。

プレゼントキャンペーンのメールも基本無視しましょう。本来の団体や企業のホームページ、あるいはご自身が登録済みのマイページから、キャンペーン確認が可能ですし、応募も出来ます。送られてきたメールにあるリンクからの参加はあなたの個人情報盗むための詐欺メールだと思ひます。

1件ごとに拒否設定という方法もありますが、迷惑・詐欺メールは@マーク前方のアドレスを変えて、何度でも送ってくるのでキリがありません。

@後方のドメインを拒否設定するのがお勧めです。

例：普段利用している団体のメールアドレスを試して拒否設定すると1度の設定でその後は受信しなくなります。が、詐欺・迷惑メールの場合、1つのアドレスを拒否設定しても、@の前方を変えたアドレスから同じ文面が届きます。プロバイダ、携帯会社、メールソフトなどを利用して、迷惑メールをフィルタリングしましょう。迷惑メールを拒否したり、有害情報を届かないように設定できるなど、便利な機能があります。