

テーマ

インターネット利用に 潜む犯罪

皆さんはインターネット上で買い物を したことはありますか？

オンラインショッピングはとても便利
家から一歩も出ずに、世界中の商品を購入できます。
メルカリやAmazon、楽天など、クリック一つでお気
に入りの商品がすぐ手元に届きます。



Rakuten



しかし...

この便利さには裏があり、私たちが想像している以上に**多くのリスク**を含んでいます。



POINT ①

具体的なリスクの例

実際にある例で考えてみましょう！

例その① ショッピング詐欺

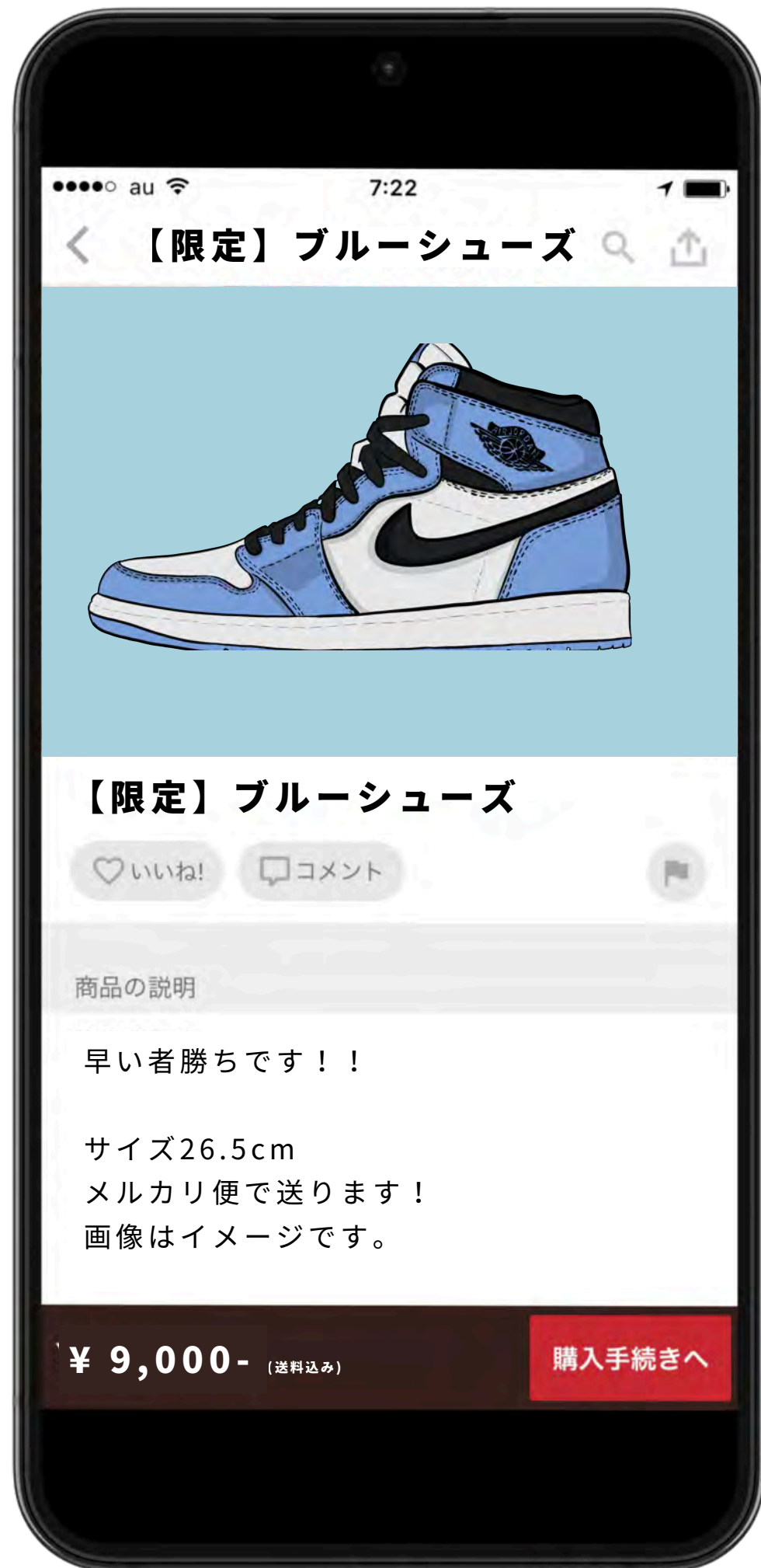
商品を注文しても、商品が届かない、または全く異なる商品が届くという詐欺もあります。



注意

これらは、特に新しいまたは評価の低い売り手から購入した場合に発生しやすい





ナイキの靴を買ったら違うものが届いた...

例その② フィッシング詐欺

ネットショッピングをした訳でもないのに
佐川急便を名乗るショートメッセージ



【佐川急便】ご本人様不在通知
為お荷物を持ち帰りました再配
達受付サービス<https://>

こんなメッセージを受け取ったことはありませんか？

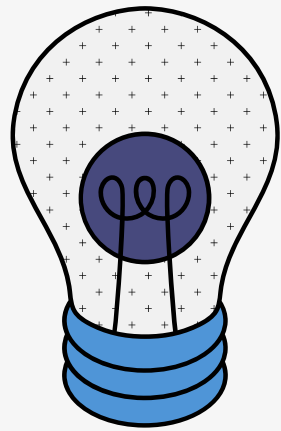
フィッシング詐欺とは？

偽の電子メールから偽のホームページに接続させたりするなどの方法で、クレジットカード番号、アカウント情報など重要な情報を盗み出す行為のこと。

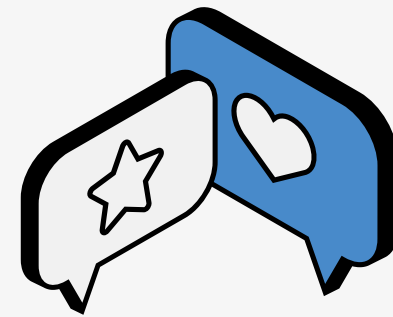


詐欺対策のポイント

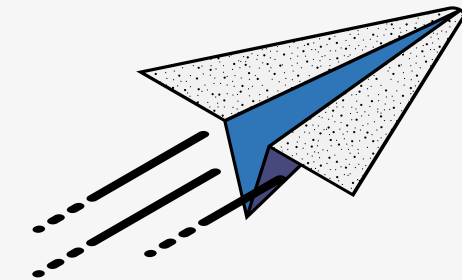
フィッシング詐欺に引っかからないためにできること



①サイトに注目



②送信元を疑う



③公式アプリの利用

注目ポイント① サイトに注目

詐欺サイトは関係のないURLに飛んだり、よく見るとURLが違ったり、日本語が不自然な場合がある。

本物	偽サイト	本物	偽サイト
 <p>本物のウェブサイトのスクリーンショット。URLは https://www.e-service.sagawa-exp... と表示されています。下部には「Web再配達受付サービス」というサービス名と「ご利用案内」のリンクがあります。下部には「https://www.e-service.sagawa-exp...」というURLが青い枠で囲われており、吹き出しで強調されています。</p>	 <p>偽サイトのスクリーンショット。URLは https://sagawa-express... と表示されています。下部には「Web再配達受付サービス」というサービス名と「ご利用案内」のリンクがあります。本物のURLと異なるURLが下部に表示されています。</p>	 <p>本物の入力画面のスクリーンショット。入力欄には「営業所番号 (半角数字)」と「お問い合わせ送り状No. (半角数字)」が表示されています。両方の入力欄は赤い枠で囲われており、右側には「入力」ボタンがあります。</p>	 <p>偽サイトの入力画面のスクリーンショット。入力欄には「お客様の電話番号を入力してください」と表示されています。入力欄には大きな赤いXが描かれており、右側には「入力」ボタンがあります。</p>

URL・入力内容にも疑いの目を持つようにして下さい

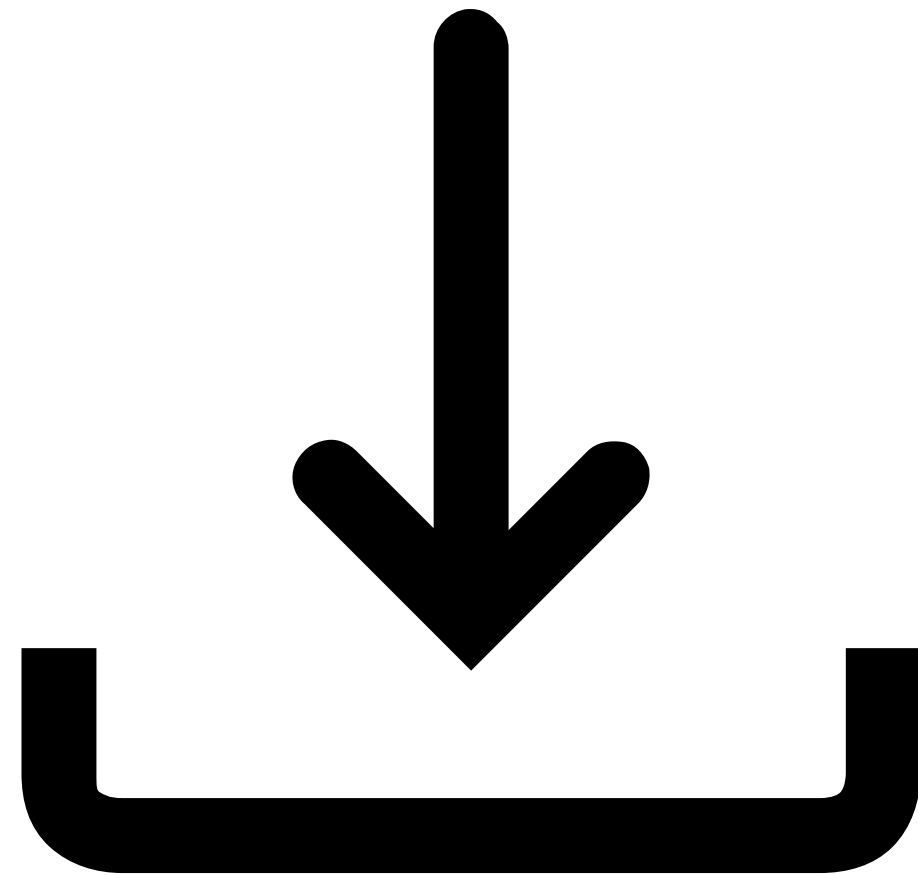
注目ポイント② 送信元を疑う

何の前触れもなくいきなり情報を聞いてくることはありません。
個人情報やクレジットカード番号等の入力を促す電子メールには注意しましょう



注目ポイント③ 公式アプリの利用

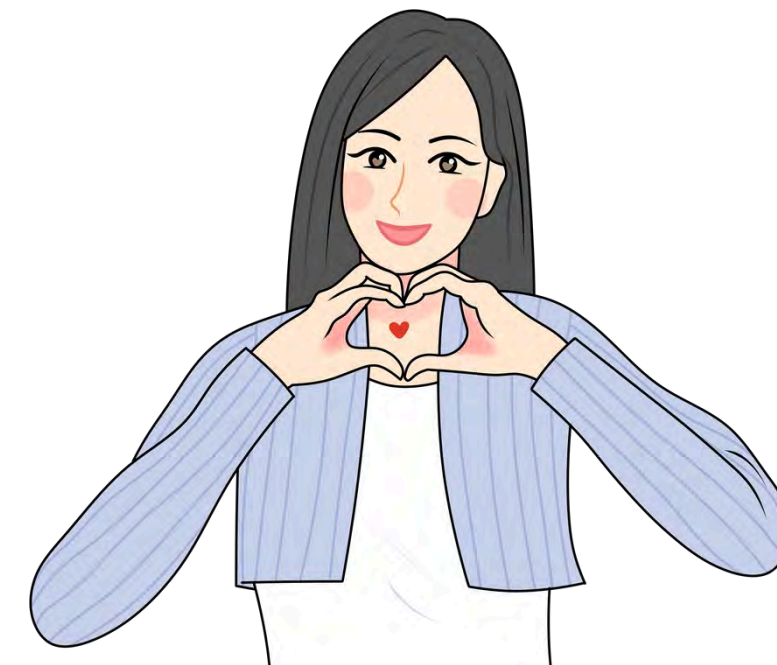
ご自身がよく公式アプリをスマホに入れておく、または、ブックマークから遷移することが重要です。



皆さんは好きな「アイドル」「推し」はいますか？

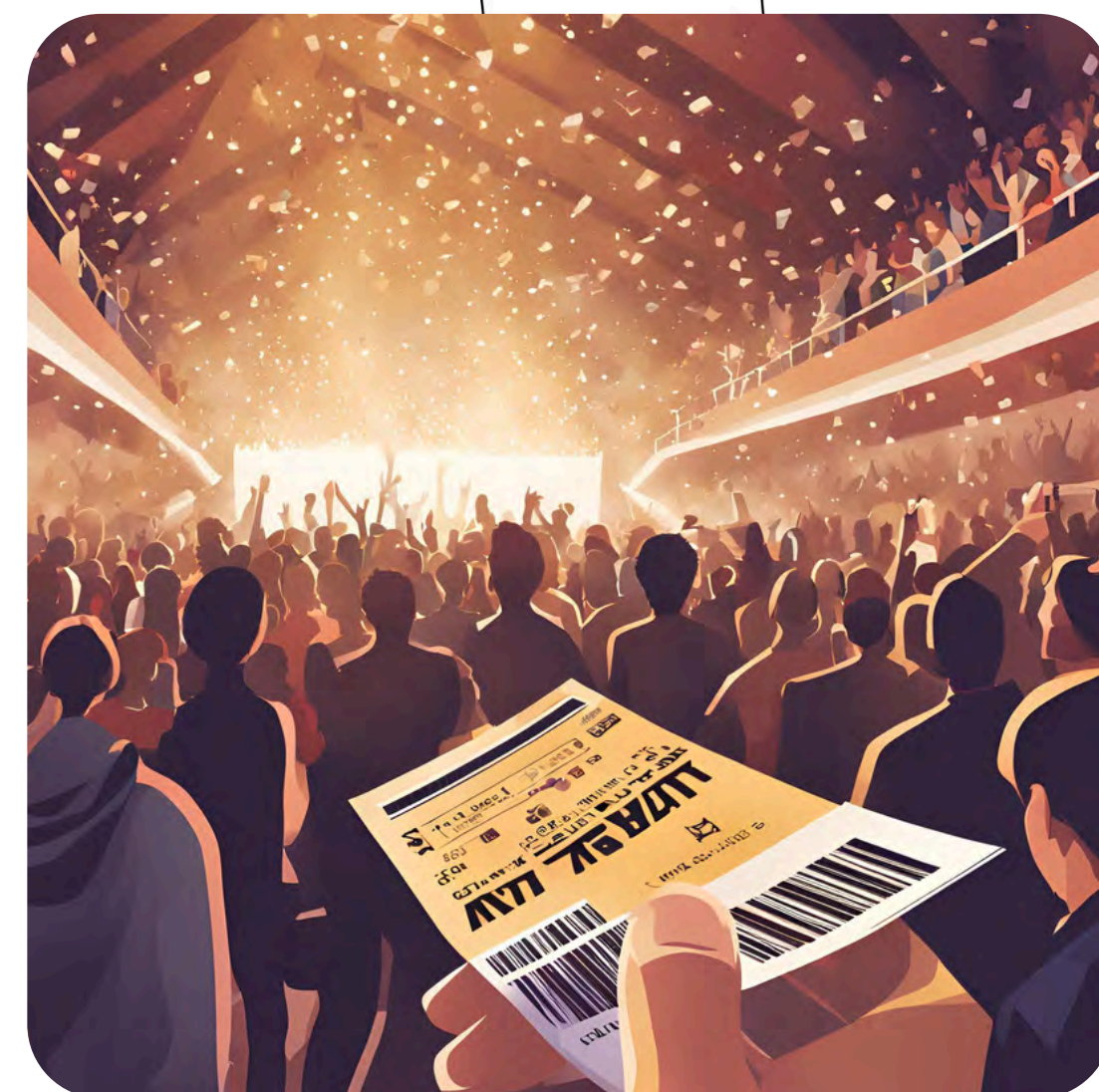


例その③ チケット詐欺



コンサート・舞台・スポーツチケット
などの抽選に外れてしまった時に
Twitter等のSNS上で取引をしていませんか？

⚠ 令和元年6月14日からチケット不正転売禁止法が施行。
不正転売、不正転売目的のチケット受け取りは
法律で禁止されています。



実際にチケット詐欺で逮捕されるケースも

スマートフォンの決済アプリで現金9220円を送金させ、だまし取った疑い

2025年1月

歌手のコンサートチケット詐欺疑いで 無職の男が逮捕



<https://news.yahoo.co.jp/articles/6eb7cf7e1c9aa47ebc46661848c7989f4de32261>

2025年1月23日Yahooニュース掲載

POINT ②

安全にネットを 利用するためのルール

SNS上の犯罪について理解できましたか？

インターネット上の情報を信じることなく、
疑うことが大切です。

「フィッシング詐欺を見分けることはできない」
という前提でいてください。

その上で、**少しでもリスクが低い行動を取ることを**
心がけることが大切です。

最後にこれだけは覚えて帰って下さい！

安全なネット利用のためにできること

守る

差出人がよく分からないメールに書かれているURLをクリックしない。すぐにサイトに個人情報を登録しない。

疑う

常に、リスクが高いか低いかを考え、少しでもリスクが低い行動を取ることを心がけてほしいと思います。

相談する

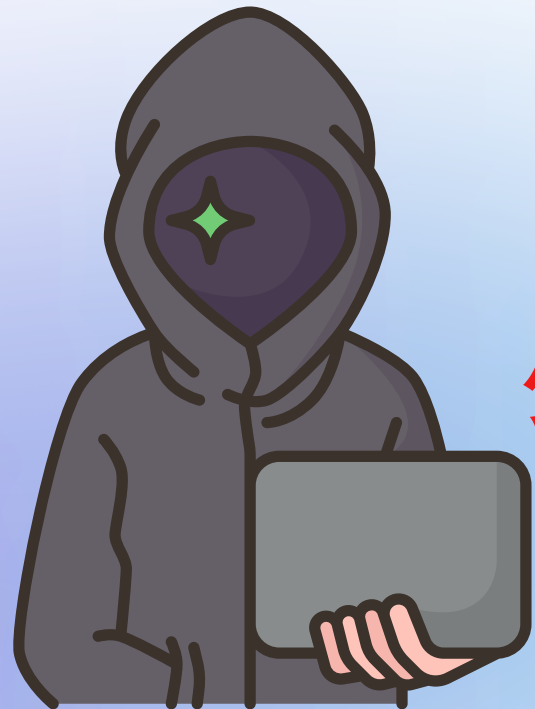
みなさんの周りには頼れる大人の方がたくさんいます。すぐに相談することで被害は最低限に抑えられます。

この電話、このサイト怪しくない???

「不自然な日本語」

「不審な連絡先」

「いきなりお金や個人情報を聞いてくる言葉」



少しでも怪しいと感じたら、そのままにしないで相談しよう



「これって詐欺かも？」といった時、相談できる場所があります

9110

警察相談窓口

188

**消費生活センター
相談窓口**



クイズタイム

クイズ①

偽のメールから偽のHPに接続させたりするなどの方法で、
クレカ番号、アカウント情報など重要な情報を盗み出す行為のこのことを
なんと言うか？

- ① フィッシング詐欺
- ② ワンクリック詐欺
- ③ スミッシング詐欺

答え：① フィッシング詐欺

クイズ②

「これって詐欺かも？」と相談したい時、
電話する番号は
次のうちどれでしょう

① #9110

② #110

③ #911

答え：①#9110

Thank you

インターネットは正しく使えば非常に便利
で楽しいツールですが、
常に安全を意識することが重要です。
今日話したことを覚えて、学校生活を
有意義に過ごしてください！

何か質問がある人は気軽に声
をかけてください！

