



サイバーセキュリティの置き薬

2021年
第13号

サイバー犯罪被害防止・だまされないで！

違和感を覚えたら一旦停止

1 フィッシング(メール・SMS)

金融機関や通信事業者、宅配事業者、通販事業者など、様々な大手企業を騙ったメール・SMSによるフィッシング被害にご注意ください。

フィッシングでは、金融機関の口座情報やクレジットカード情報が盗まれ金銭的な被害に遭うだけでなく、不正アプリ(不正プログラム)がインストールされ、ウイルス感染や遠隔操作の被害に遭う危険性もあります。

【被害に遭わないための注意点】

- 心当たりのないメール・SMSには要注意！
- 違和感を覚えるメール・SMSには要注意！
- URL接続を急がすものには要注意！
- 金融情報やアカウント(ID・パスワード)要求には要注意！
- アプリのインストールを要求するものには要注意！



2 偽サイト(ショッピング詐欺)

インターネットショッピングにおける偽サイトに関する相談が寄せられています。

偽サイトは、無関係な複数の正規サイトから商品画像や運営会社の情報等を無断使用するなどしており、サイト構成に不自然な点が多々あります。商品価格を注視しがちですが、会社概要や振込先口座名など、よく確認してください。

【偽サイトの主な特徴】

- URL(ドメイン名)が不自然、サイト名称と一致していない
- 商品価格が、著しく値引きされている
- 銀行振込しか支払手段がない、振込先口座名が不自然
- 住所が番地まで表記されていない、連絡手段がメールのみ
- サイト内の表記が不自然な日本語や字体フォントが不自然



止まれ
STOP

Check!

※ 年末が近づき、ネットショッピングを利用する機会が多くなるかと思えます。ご利用の際は、十分にご注意ください。

受信したメール・SMSに違和感、ショッピングサイトに違和感を覚えたら直ぐに返信・クリックせず、商品購入する前に一旦立ち止まって確認したり家族や友人に相談するなどして、被害防止をお願いします。