# 10 RED FLAGS OF FRAUD

#### **UNSOLICITED REQUESTS**

Be cautious of unsolicited emails, phone calls, or messages asking for personal or financial information. Legitimate organizations typically don't ask for sensitive data through such channels.



#### TO GOOD TO BE TRUE OFFERS

Offers that promise unrealistically high returns on investments or products at extremely low prices could be signs of fraudulent schemes.

#### PRESSURE TO ACT QUICKLY

Scammers often create a sense of urgency to pressure individuals into making hasty decisions without proper research or thinking.



#### **UNVERIFIED CONTACTS**

Check the legitimacy of the person or organization contacting you. Look up official contact information and independently verify it before sharing any information.



## REQUESTS FOR PAYMENT UPFRONT

If you're asked to pay a fee or provide payment before receiving a service or product, especially if it's unexpected, it could be a red flag.

#### **INCONSISTENT INFORMATION**

Discrepancies between what's being presented and what you know to be true, such as mismatched logos, official names, or addresses, should raise suspicion.

### REFUSAL OF DETAILED INFORMATION

Legitimate businesses and organizations should be willing to provide clear and detailed information about their services, products, and terms.

#### **UNSECURE WEBSITES**

Always ensure the website you're dealing with has a secure connection (look for "https" and a padlock icon) when sharing personal or financial information.

# #8

# HIGH PRESSURE SALES TACTICS

Aggressive sales tactics designed to make you commit quickly without adequate research or thought are often used in fraudulent schemes.



#### **UNUSUAL PAYMENT METHODS**

Be cautious if you're asked to make payments using unconventional methods, such as wire transfers, gift cards, or cryptocurrencies, as these are often difficult to trace and can indicate a scam.

