COINJAR

Spot The Scam – Red Flag Checklist

Use this checklist to self-test yourself any time you send money or personal information.

By using this checklist, you can better protect yourself from scams and make more informed decisions about your money.

This checklist is designed to help you identify red flags when evaluating a financial opportunity. The statements are written in the first person to make it easier for you to assess your own situation and feelings.

Instructions:

1. Read this entire page before you begin.
2. Read each statement carefully.
3. Reflect on your current situation and how you are planning to use your money.
4. Tick the box next to any statement that applies to you.

Interpreting the results:

- **If you tick any statement, do not proceed** – you might be involved in a scam.
- **Ask for help from trusted people** to better understand the risks involved.
- **Still not sure? Email us** on support@coinjar.com so we can help you.

Remember:

1. Verify and research

Before sending your money anywhere, or sharing your sensitive information with someone else, it's crucial to thoroughly verify and research what you are planning to do. Doing your own research can help reduce the risk of falling victim to a scam.

- ☐ **I have not researched if the request for my money or information is genuine**
  Not verifying the source of a request for your money can leave you vulnerable to fraudulent schemes pretending to be legitimate businesses. Verify the request for money or information - if it's from a company, check their registration and licences with relevant authorities, using independent websites.

- ☐ **I have not verified the details given by the person I'm speaking with**
  Don't trust what one person tells you - scammers provide misleading or false information to lure you in and steal your money. Always do your own research. Use Google to search online and see what information is available before you send money to anyone. Never rely on the information provided by the person promoting the opportunity.

- ☐ **I have not spoken with my friends or family about this request for money**
  Keeping decisions on where to send your money or information to yourself is an easy way to fall victim to a scam – it prevents you from getting valuable second opinions that might identify potential red flags. Discuss the details with people you trust.

- ☐ **I have found the provided information to be vague or lacking in detail**
  If someone provides vague information when they request your money, be suspicious – this is a common tactic used by scammers to avoid scrutiny. Legitimate opportunities provide clear and detailed information that can be verified independently.

- ☐ **I feel the request for my money seems too good to be true**
  Offers that promise high returns with little risk are often too good to be true and a sign of potential scams. You may find that the scammer has emotionally manipulated you into urgently paying for their travel – but none of this is real; they are just trying to steal your money.

- ☐ **I have not found independent reviews from others who have sent money**
  Lack of independent reviews or testimonials can indicate that the opportunity is not well-known or is trying to avoid scrutiny. Overly positive reviews or those that lack specifics may indicate a scam – reviews of financial scams are often faked to trick you.

- ☐ **I have not researched the people involved with the request for my money**
  Unverified credentials and backgrounds can mean that the individuals promoting the opportunity are not who they claim to be.

- ☐ **I found complaints or legal issues associated with the person or company**
  Complaints and legal issues about the person or company who has requested your money are strong indicators of past fraudulent activities or unethical practices. This information can often be found through regulatory bodies, online databases or searches using Google.

2. Seek transparency and security

Ensuring that someone who requests your money or information provides clear, transparent information and secure ways to handle your information is vital in protecting yourself from scams.

- ☐ **I feel that the person asking for my money does not show transparency**
  Lack of transparency can be a sign that the person requesting your money is hiding something or is not legitimate. Ensure that all information is easy to understand and accessible, and appears on other independent websites.

- ☐ **I was asked to send sensitive information to someone I don't know well**
  Scammers often ask for sensitive information to commit identity theft or fraud. Legitimate interactions, whether commercial or personal, will never pressure you to share private information such as login details or ID documents, which can expose you to significant risks. Never send sensitive information to someone whose identity and trustworthiness you cannot independently verify.

- ☐ **I have been asked for remote access to my computer**
  Legitimate businesses will not ask for remote access to your computer. As soon as someone has access to your computer, they can take over your online accounts, including your email and bank accounts. Never provide remote access to your computer to anyone.

- ☐ **I received official-looking documentation or contracts that I can't verify**
  While legitimate entities may provide written contracts or official documents outlining the terms of an agreement, be cautious of any documents you receive – documents can be easily faked, and scammers will send fake documents to trick you. Always verify the authenticity of any paperwork independently.

- ☐ **I have not verified that the requester has an address or contact information**
  A legitimate person or business who is asking for your money will have verifiable contact information and a physical address. Lack of these can indicate a scam, however be wary – scams sometimes use fake contact information and addresses to trick you.

3. Be aware of scam tactics

Ensuring you are aware of common scam tactics when someone requests your money or information can help you identify red flags and protect yourself from potential scams.

- ☐ **I was contacted by a stranger about sending my money**
  Scammers will often contact you unexpectedly and claim to be someone who can help you make a lot of money. Do not trust strangers who ask for your money. If you make a new friend online and they eventually start talking about how to make money online, be suspicious.

- ☐ **I am feeling pressured or feel a sense of urgency to send money**
  Scammers often create a sense of urgency to rush your decision-making process, preventing you from thoroughly evaluating the opportunity. Scammers may be pressuring you to invest in an online business, or to pay for their travel costs because they pretend they need urgent help.

- ☐ **I was promised high returns on my money with little or no risk**
  Promises of high returns with minimal risk are classic signs of a scam. Legitimate investments always carry some level of risk, including the risk that you may lose all of your money.

- ☐ **I was told not to tell my friends or family about sending money**
  Scammers may try to isolate you to prevent you from seeking advice that might reveal the scam. Always consult friends and family before you send money to another person you care about, or an investment – friends and family can help to confirm you are making the right decision with your money.

- ☐ **I don't feel I've had enough time to understand why I should send my money**
  If you feel rushed and haven't had the time to fully understand the investment, it's a sign that you should slow down and gather more information. Scammers will try to make you feel like there is a deadline or time constraint, or make you feel like you might miss out if you don't act fast.

- ☐ **I haven't asked detailed questions about why I should send my money**
  Asking detailed questions and receiving clear, satisfactory answers is crucial. Evasive or unclear responses can be a sign of a scam. You should always ask the recipient detailed questions when sending your money.

- ☐ **I have responded to unsolicited offers requesting my money**
  A large number of scams begin from an unsolicited call, text or email. Always be suspicious and cautious of unsolicited offers and unexpected communications. Scammers use these methods to reach potential victims.

3. Be aware of scam tactics (cont.)

- [ ] **I have been asked to purchase gift cards and give someone the codes**
  Scammers commonly ask for payment via gift cards because they can remain anonymous and it's impossible to get your money back. Legitimate people and businesses will never accept payment in gift cards.

- [ ] **I have been asked to use a wire transfer or cryptocurrency for a payment**
  These payment methods are favoured by scammers due to the difficulty in tracing and reversing the transactions.

- [ ] **I have been asked to donate to a charity that I haven't verified independently**
  Scammers exploit natural disasters and crises to set up fake charities and solicit donations. If you want to donate, you should search for the official website of the charity and double check it is a registered charity.

- [ ] **I have received a job offer that requires me to pay for training, equipment, or certifications before starting**
  Job or employment scams often ask for money upfront under the guise of training or other fees, promising employment that never materialises. Be sceptical of people advertising jobs outside of official channels such as well-known job websites.

- [ ] **I am interacting with someone romantically who needs financial assistance**
  Romance scams often involve fabricated stories about emergencies or financial struggles to solicit money from their victims. Do not send your money to a romance you have online - they are almost always trying to steal your money from you.

- [ ] **I have received a phone call asking for my money or personal information**
  Businesses typically do not request personal information or make threats over the phone; such calls are likely attempts to trick you into providing sensitive information about yourself, or an attempt to convince you that you must pay a fine or fee to the government. You should always call or email the person, business, or government agency using their official details and verify the request is genuine.

- [ ] **I received a payment and was asked to send a portion of it elsewhere**
  Never trust someone who asks you to make a payment on their behalf using your identity or account. This is called money muling and you are an accomplice. The person who asked you to send money in exchange for a commission is attempting to hide their identity, and setting you up to take the blame. You should never make payments on behalf of someone else.