

Money mules

Once scammers get a victim's money, they are far from done. They often need to move the money – and they are not going to do it themselves.

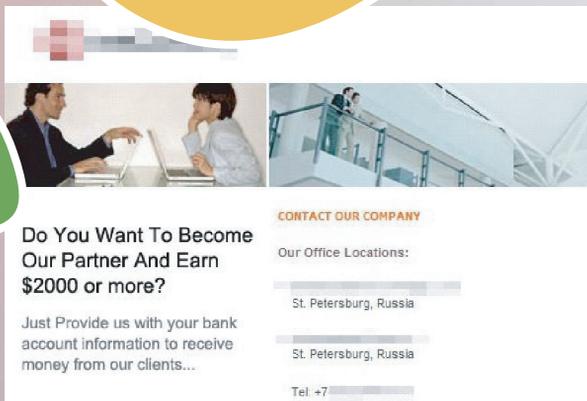
This is what you should look out for:



Receiving an unsolicited email or contact over social media promising easy money for little to no effort or requesting you to respond accordingly to an advert promising as much.

The “employer” you communicate with uses web-based email services such as Gmail, Yahoo Mail, Hotmail or Outlook.

You are asked to open a bank account in your own name or in the name of a company you form to receive and transfer money.



As an employee, you are asked to receive funds in your bank account and then “process funds” or “transfer funds” via a variety of means, such as wire/telegraphic transfer, mail, cryptocurrency or a money service business.

You can keep a portion of the money you transfer.

Your duties have no specific job description.

Your online companion, whom you have never met in person, asks you to receive money and then forward these funds to an individual you do not know.

Money mules

Action you should take:

A legitimate company will not ask you to use your own bank account to transfer their money. Do not accept any job offers that ask you to do this.

Be wary when an employer asks you to form a company to open a new bank account.

Never give your financial details to someone you do not know and trust, especially if you met them online.

Contact your bank immediately.



Stop transferring any money or valuable items.

Stop all communication with suspected criminals.

Keep all receipts, contacts, and communications, such as texts, emails or chats.

Notify the Malta Police Force immediately. It is common for money mules to never see a pay cheque or a commission they thought they would be earning. Even worse, there is the chance of being arrested for being part of a crime, even though the mule did not know what was going on.