# Checking an Email for Scams

# Using the TFSM Method

## **T**o Address:

Who is the Email Addressed To? Is it my email address and others I don’t know or just mine?

Occasionally the phishing or spoofing messages contain multiple addressee names. If it contains multiple names and you don’t know the other names, this could be a sign of a scam.

## **F**rom Address:

Who is the email from? Check the entire from name.

In the sample message, it appears to be from someone named Vectoria at Indeed.com. Indeed.com is an actual company, however upon closer look at the from address it shows it is on behalf of Victoria at Chatur.com. This is a major signal that this is a scam. The company Indeed.com first would not misspell an employee’s name (Vectoria vs Victoria and neither is capitalized). Second, they would not have an address “on behalf of”.

## **S**ubject:

What is the subject of the email?

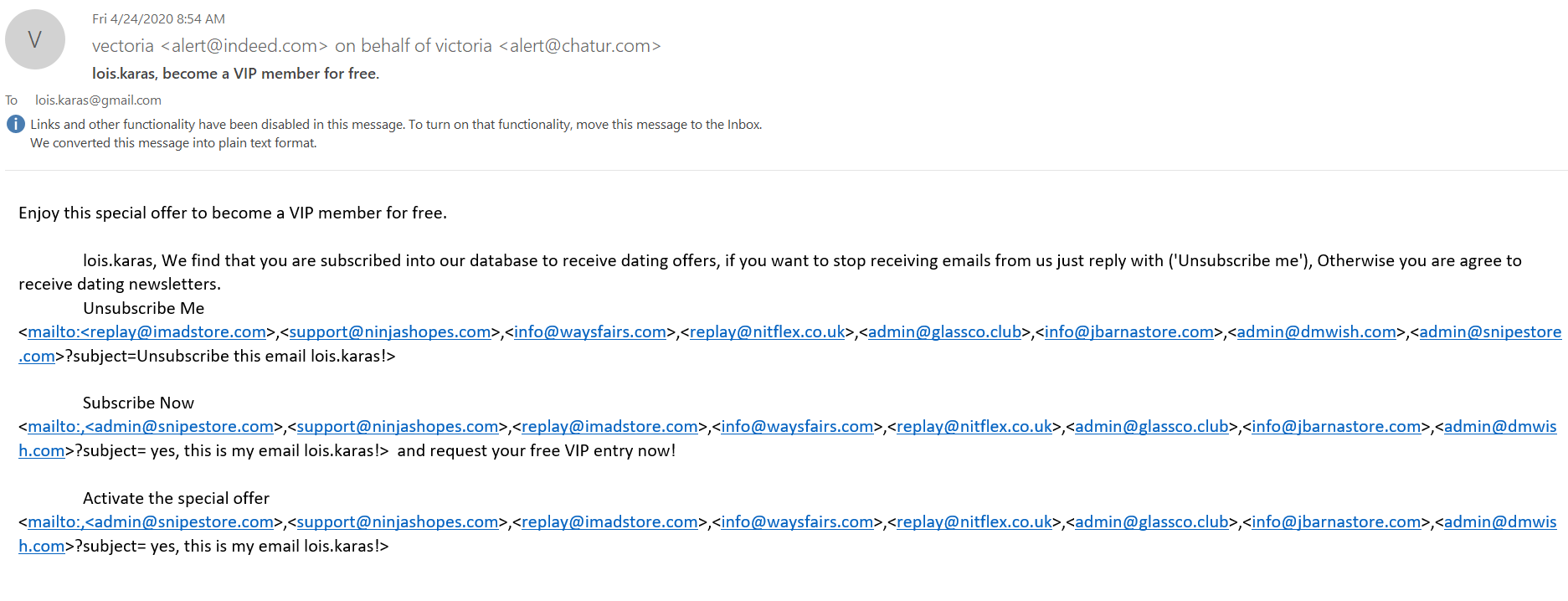
The subject of the sample message has my name listed the same as my email address. This is another sign of a scam. A real company would have my first and last name.

## Message:

Does the message include links?

In the sample message, it clearly shows the links and no images. This is because my email application (in this case Outlook) blocked the images since I have not received a message from this email address before and have not accepted it as a known sender. Since I suspect this is a phishing (or scam) email, I would delete it without clicking on any of the links. DO NOT even click on the Unsubscribe link as this would just let the scammers know your email address is real and active and they will just send more messages.

## Sample Phishing Message:



From Address

Subject

To Address

Email Message Body