hw11_Panchagnula_Raghava

Homework Number: HW11

Name: Raghava Vivekananda Panchagnula

ECN Login: rpanchag

Due Date: 4/11/2024

Recipe 1:

:0

^From.@.*@.*

recipe_1

This is a simple recipe that checks if there are 2 or more senders and sends it to recipe 1. It checks for more than 1 entry in the from field, and filters it out.

recipe 2:

:0

^Subject.(diploma|MBA|PHD|diploma|VerifiableDiploma|bonuses|safe|career|graduate|watches|measures|free|mock|countries|fast|single|Partner|action|protection|guaranteed|accredited|secure|quick|degree|certification)

recipe_2

I just added in words that I read or found in the subject that I thought were worthy to filter out.

Recipie 3:

:0 B:

* (Price|Poker|casino|casinos|gambling|Casino)

recipe_3

I set the recipe to search in the body only, and look for the above words in the body of the emails, and filter it out if they are found.

Recipe 4:

:0 HB:

* ^Content-Type: text/plain

* ^Content-Type: text/html

* ^Content-Type: multipart/alternative

* ^Content-Transfer-Encoding: base64

recipe_4

This checks the header and body of the email to see if there are any plain text or html text based emails and filters them out. This should catch any suspicious emails with HTML embedded into the body or if they try to force you to look at plaintext that is unformatted. All the emails in the list seem to have problematic HTML embeds and such, so looking for those seems to be the way to go.

The assumption is also that the emails with the content transfer encoding of base64 are the ones that are spam emails, since they are encoded and are not plain text. This means they are containing some sort of image or link or something that is not plain text. The ^ checks to make sure that it is the start of the line instead of being in the body.