

Bypassing Spam Filters Using Homographs

By

Fady Mohamed Osman

www.darkmaster.tk

@fady_osman

A few days ago i discovered a new technique to bypass spam filters using homograph letters the idea is pretty simple yet very effective ,anyway before we start we should first understand how spam filters work in order to understand how to bypass them.

Understanding spam filters:

In general spam filters typically looks for three important things to determine if the message is actually a spam then start adding scores when it finds something suspicious and the final score determines whether the message is a spam or not these three things are:

1- Where the message came from : The spam filter checks if the message came from a trusted source this is done by looking for the network where the message came from in several RBL (Realtime Blackhole List) and each time the network appears in a list the spam score is increased a little this check can be bypassed by using a trusted network may be one of the public mail services.

2- Software that sent the message: Spam filters looks for clues in the message headers that the message was sent by a spam engine rather than a real mailer. If the spam engine is clever enough to simulate a real mailer this check can be bypassed also by using a real mailer it can be bypassed anyway when using a real mailer the risk of being traced is increased.

3- Contents of the message: This is actually what we are interested in in this paper. Spam filters check the contents of the message for spammy phrases like "CLICK HERE!" or "FREE! BUY NOW" and each time it finds one it adds more points to the spam score. This is a sample criteria from Spam Assassin one of the most popular spam filters:

- Talks about lots of money (.193 points)
- Describes some sort of breakthrough (.232 points)
- Looks like mortgage pitch (.297 points)
- Contains urgent matter (.288 points)
- Money back guarantee (2.051 points)
- Why Pay More? (1.249 points)

after checking all that if the total spam score exceeds a certain threshold your mail is sent to the junk folder.

In the rest of this paper we will discuss a new technique to bypass spam filters using homograph letters.

What are homographs and how can they bypass spam filters??

homoglyph is one of two or more characters with shapes that either appear identical or cannot be differentiated by quick visual inspection. Examples of homographs in english are the capital "0" and zero "0" also the number "1" the lowercase "l" and the uppercase "I". Homographs presents security risks in variety of situations see:

http://http://en.wikipedia.org/wiki/IDN_homograph_attack for an example of these attacks.

Also you can check this article i wrote a while ago about this attack:

<http://www.darkmaster.tk/index.php/articles/1-homograph-phishing-attack>

What we are interested in here is the unicode homographs in languages like cyrillic and greek they contain letters that looks exactly the same like some english letters but with different unicode since they have different unicode the spam filter will not recognize them for example if you wrote "CLICK HERE!!" with some cylliric characters the spam filter will not be able to find it even if it looks exactly the same as the one written in english letters.

homographit tool:

replacing characters manually or using "find and replace" in your favorite text editor could be pretty annoying so instead i created a tool that will replace the characters with thier homographs for you. you can download it here:

<http://www.darkmaster.tk/index.php/tools/10-homographit>

Testing against emailspamtest.com

emailspamtest.com is a website for testing spam mails. To test my new method i grabbed a copy of one of the spam mails in my spam box this is the message body and i set the subject to "make some money" with the following body:

How are you doing? Hope you have not forgotten me, I am Dr. David Mark.

I Secured the release of some money accrued from the over invoicing of a contract/inheritance that was awarded by my government some time ago during the military regime.

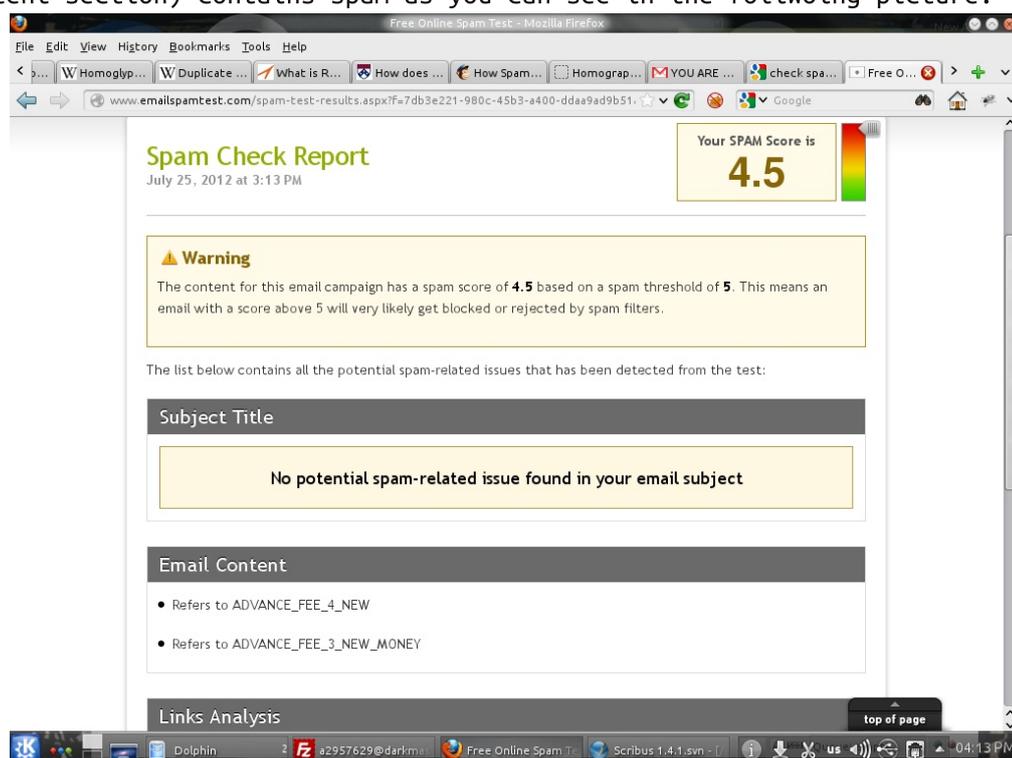
Though you were not able to assist me conclude the transaction, I'm happy to inform you about my success in getting those funds transferred under the assistance and cooperation of a new partner from Brazil . Presently I'm in London-United Kingdom for investment projects with my own share of the total sum. Meanwhile, I didn't forget your past efforts and attempts to assist me in Transferring those funds, I made sure you are not left out the benefit of the Transaction hence I kept aside for you sum of Nine Hundred And Fifty Thousand United States Dollars (\$950,000.00).

I and my new partner agreed to compensate you with that amount for all Your past efforts and attempt to assist me in this matter. I appreciated your efforts at that time very much, so feel free and get in touch with the paying bank Mr. Santiago Jimenez and instruct him on how to send wire your funds to you.

Please do let me know immediately you receive wire transfer so that we can share the Joy together after all the suffer at that time. In this moment, I'm very busy here Because of the investment projects which I and my partner are having at hand, so you Need to contact the paying bank, i have instructed PNC bank to remit the payment to you In your own method.

Below is the contact of the paying bank:

emailspamtest.com results shows that there's nothing wrong with the subject but the body(email content section) contains spam as you can see in the following picture:

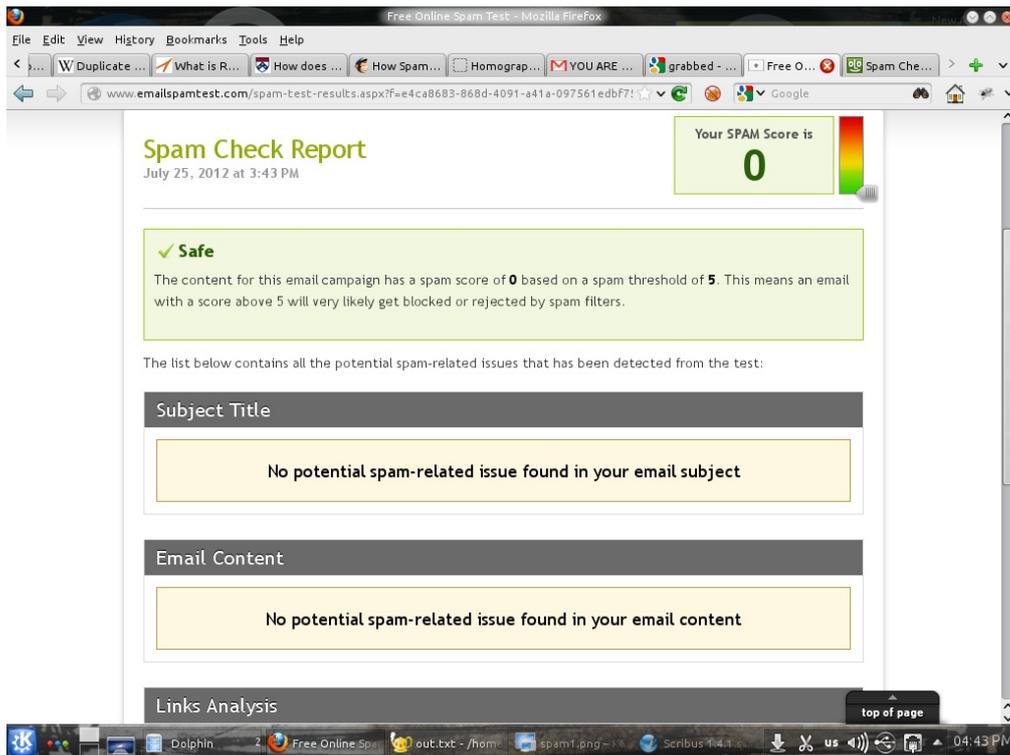


The screenshot shows a web browser window displaying the 'Free Online Spam Test' results. The page title is 'Spam Check Report' and it was generated on July 25, 2012, at 3:13 PM. A prominent yellow box displays 'Your SPAM Score is 4.5' with a corresponding color scale. Below this, a warning message states: 'The content for this email campaign has a spam score of 4.5 based on a spam threshold of 5. This means an email with a score above 5 will very likely get blocked or rejected by spam filters.' The report lists potential spam-related issues detected from the test:

- Subject Title:** No potential spam-related issue found in your email subject.
- Email Content:**
 - Refers to ADVANCE_FEE_4_NEW
 - Refers to ADVANCE_FEE_3_NEW_MONEY

The bottom of the screenshot shows the Windows taskbar with various open applications like Dolphin, Scribus, and the Free Online Spam Test tool.

now let's save our message into file and give it to homographit tool and use the output of the tool instead of the original message to see if the emailspamtest will still complain:



as you can see the spam score dropped from 4.5 to 0 and now it says that the message is safe.

Case study : Apache spamassassin

spamassassin is a popular spam filter from apache foundation. I decided to test my tool against it so i used the same email when passing it to spamassassin it gave the following results (you can ignore the complains about missing headers since i didn't put them in the test file for simplicity) the score of the message was 8.6 and considered a spam with the following problems:

1.2 MISSING_HEADERS	Missing To: header
0.1 MISSING_MID	Missing Message-Id: header
1.8 MISSING_SUBJECT	Missing Subject: header
1.4 MISSING_DATE	Missing Date: header
1.4 ADVANCE_FEE_3_NEW	Appears to be advance fee fraud (Nigerian 419)
1.0 ADVANCE_FEE_3_NEW_MONEY	Advance Fee fraud and lots of money
0.6 ADVANCE_FEE_2_NEW_MONEY	Advance Fee fraud and lots of money
1.2 MONEY_FRAUD_3	Lots of money and several fraud phrases

The last four ones is what's important for us now. Feed the message to homographit tool and then pass the output file to spamassassin the result is pretty amazing with all these missing headers the mail is not considered a spam since it have a score of 4.5 and the required score is 5!!!. You will also notice that the last four rules have no scores which means spamassassin can't see any problems with the contents of the email.

Fixing the issue:

The problem can be fixed by replacing any homographs before checking the mail for spam ,anyway this may cause a problem in situation where these homographs were added in a legitimate way.

Another way to fix this is by adding all the variations of each test with homographs.

References:

<http://en.wikipedia.org/wiki/Homoglyph>

<http://www.gordano.com/kb.htm?q=264>

<http://www.seas.upenn.edu/cets/answers/spamblock-filter.html>

<http://kb.mailchimp.com/article/how-spam-filters-think/>

<http://www.darkmaster.tk/index.php/articles/1-homograph-phishing-attack>