THE FREECYCLE NETWORK – SPAM CONTROL TEAM

PROCEDURES FOR REVIEWING OFFER POSTS

Background

The goal of our team's work is to find and remove members who have made posts on The Freecycle Network (TFN) that are considered spam or scams. Unfortunately, there is currently no algorithm to help us find these posts, so we review posts individually. As you will soon see, there are about 50000 offers per day on the network. Our task is made more difficult because the scammers and spammers know that we are looking for them and try to conceal the purpose.

You will also see some posts that violate one or more rules of TFN that are not spam or a scam. Possible actions on those posts will be discussed toward the end of this paper.

Scanning Offers[1]

This is a safe procedure that you can start with and then modify as you see fit:

1. Check others' daily reports to see if there are any active spammers or scammers to be on the lookout for.
    a. Find out what items scammers have been offering.
    b. Note usernames, email addresses, email domains, and look for patterns.
    c. Become familiar with wording of scam posts.
    d. Daily reports are sent to a group account we refer to as our team's Webmail. The group is at: https://webmail.freecycle.org/.
2. Open the Spamtool at https://spamcontrol.freecycle.org/display_posts. This should put you in the section of the tool that you will use the most. (Note: You will probably want other sites available on tabs, such as the team webmail (see above), and an IP Address checker (see below for a reason to have this site up and running.)
3. Choose a starting point and note the time of day (all times are in UTC) and the Post ID (post IDs are in numerical order, but not sequential). In case the Spamtool loses your place, periodically write down the Post ID and time so you can navigate back there.
4. Review the subject of each post, looking for anything that seems odd (more on this below). The subject might be the first place that you will find a post that requires action. Posts in a foreign language can usually be translated using the Google translators.
5. Quickly scan usernames and email addresses, looking for any patterns you had noticed when checking the daily reports. In particular look for certain email domains sometimes used by scammers and drug dealers.

[1] This discussion assumes the reader has read the Spam Control Team Wiki.

6. If a scammer has been operating in just one geographical area (e.g., Australia), scan the group column, note anything from that area, and go back to the previous columns to determine if a post merits investigation.
7. (Note: More experienced reviewers usually use step #8 below before than this step.) If you are curious about a post, click on the Post ID, and the Spamtool will give you info on that post, including the body of the post. The body of the post is the second place that you may see something indicating that the post requires action, such as:
    a. Is it obvious – drugs for sale, etc.? (But note for non-UK reviewers, "Hardcore" in the UK is something you put in holes in the ground for construction purposes.)
    b. Does the offer seem out of place?
    c. Is the item worth a lot of money?
    d. Is the offerer offering many, many things and it doesn't make sense that they are all together?
    e. Is the subject presented in such a way that it looks commercial?
8. If you see something that looks funny in the subject of the post (i.e. you are more than curious), your best bet is usually to click on the UserID. From this view, you will see (among other things) and be most interested in: (1) IP address(es), (2) groups to which the member belongs, (3) posts the member has posted, and (4) a link to view replies to the post you are investigating.

    Look for these factors. There may be a perfectly legitimate reason for any of these, but presence of several of them typically indicates a scam or spam:
    a. Is there is more than one IP address? Are they registered in different countries? (Keep in mind that every computer/phone that a person uses has a different IP address.)
    b. Is the country in which the IP address(es) is located different from the country in which the poster's group(s) is located?
    c. Is the poster using a VPN? (This can be checked at sites such as https://www.ipqualityscore.com/free-ip-lookup-proxy-vpn-test).
    d. Is the poster using a non-VPN service that hides the sender's true IP address? E.g., protonmail, hushmail.
    e. Does the poster belong to a lot of groups? Are those groups located on different continents? (Note: the number of groups alone does not mean much. Some residents of London join up to eight groups but they are legitimate, active members. We still see a few members who joined even more groups before the limit was lowered to eight.)
    f. Is the UserID a recently issued one? (When this was published, recent UserIDs began with a "27" or "28" and had eight digits.) (Note: an asterisk next to the UserID on the "Display Posts" page means they joined the group within the last

ten days; scammers frequently, but not always, post their messages quickly after joining the group, so an asterisk in another factor.)

   g. Are the other posts made by this poster all recent? (If they have a history of clean posts, the poster is usually ok.)
   h. Are the posts to groups distant in geography?

9. When you have finished your scanning for the day note the time and the post ID of the last post that you scanned.

Possible Actions

1. Ask for Help. If you see something that you are not sure of or do not know what to do with, post your question to the group. For the next couple of months, it will likely be Chris or Patsy that will respond, but your question and the response help keep all members of the group in tune with current issues.
2. Zap the Member.
   a. There is a button on some of the pages in the Spamtool labeled “Zap Member.” This makes that user name inaccessible, and the zapped member will never again be able to use the same username or email address. Any open posts from the member are closed. However, zapping does not completely delete the member, so mods and Scam Control can still find some information about the zapped member. You will no longer be able to see the groups the member belonged to; if you want that info for your daily report, copy it to your draft report before you zap.
   b. If anyone responded to the post before you zapped the member, send the standard email warning to them.
3. Refer to the appropriate GOA. We only take direct action on spams and scams. Period. While there is general acceptance of the work we do, many groups do not welcome interference in their group from “Freecycle Headquarters.” Nevertheless, you will see posts that are inconsistent with the rules of TFN. Some of these warrant action, and we do that by sending a prepared email to the GOA (Group Outreach and Assistance) for the region in which the group is located. GOA addresses are here: https://wiki.freecycle.org/Moderator_Manual:How_to_Contact_Your_GOA

Daily Reports

1. Your final step for the day will usually be preparing and submitting your daily report. Most of this report does not have a standard format, but it should include, at a minimum, the times and post IDs of the first and last posts that you scanned, and basic information about any scams and spams that you found.

2. It helps Chris prepare his weekly report (which combines the data from all of our daily reports and is sent to TFN team coordinator) if you do the following:
    a. Send the report from your personal email account (so we can see who the report is from) to the webmail account (not the Yahoo group email account that we use to communicate with each other).
    b. Use this format in the subject line: ww-xx-yy z, where ww is the day of the month (Chris is in the UK), xx is the month of the year (in numbers), yy is the year, and z is the number of spams and scams (total) that you are reporting. Do not include any emails to GOAs, etc. in the "z" field.
    c. You can include other information in the report that you think Chris and the other team members might find useful now or later. (In webmail we can search one mailbox at a time and may do so to find info to use in deciding whether a current post is from a scammer.)
3. Daily reports show up in the webmail inbox, and after Chris has retrieved the information from them, he moves them from the inbox to a folder with your name on it. Please do not move anything from the inbox unless authorized to do so.

Conclusion

We hope that you will find the above information useful. There are other things that you need to know and figure out, and we will address them as they come up. As mentioned before, ask as many questions as you have. Chris says that your ability to spot scams and spam will improve with practice, so don't be discouraged if it is slow going at first – you will get better and faster! Thank you for your willingness to help keep TFN a useful place, and we all look forward to working with you!