Scam-Alert: Characterizing Work from Home Scams on Social Networks

Shaifali Gupta
IIIT Delhi

Rashi Garg
IIIT Delhi

ABSTRACT

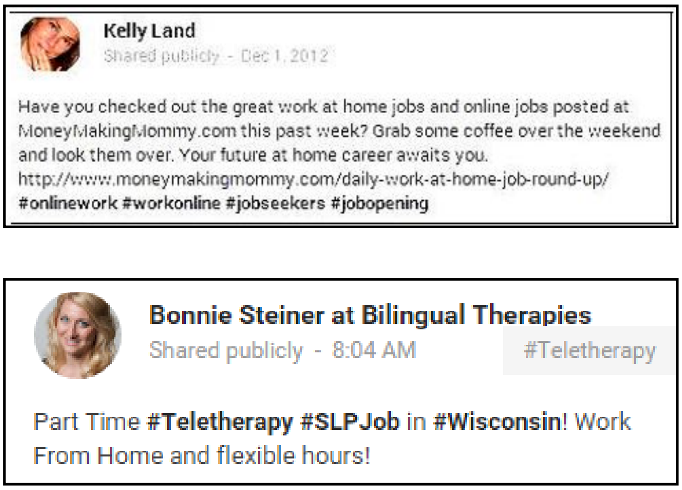
Online social networks have become a favorite platform for marketers and advertisers. Due to the wide reach of these networks and low cost of advertisement, there has been an upsurge of marketing and advertising campaigns on social media. Social networks like facebook, twitter and google+ possess the capability to quickly turn any piece of information viral, thus increasing its impact. However, there do not exist many tools which can tell whether an information circulating on social media is genuine or fraudulent. We confine ourselves to a specific section of marketing campaigns in this work, which is – “Work from home” campaigns. “Work from home” schemes are run with the intention of providing users an attractive option of working from home in return of some remuneration. Unfortunately, many of such “work-from-home” ads floating on social network are actually scams which mislead and cheat on the end user in more than one way. In this work, we present a study of online money making campaigns run on a popular social network – Google+, and propose an approach to distinguish genuine campaigns from scams.

Keywords

Work from home, online social networks, online security, scam, hashtags

1. INTRODUCTION

We often come across attractive “work from home” schemes offering home based employment. Such schemes usually lure users by offering an attractive return for doing some relatively simple task. Common targets for companies offering these schemes are generally housewives, senior citizens, unemployed or underemployed persons looking for a well-paying easy job. Some countries like Australia [1] and U.S. [2] have established enforcement agencies specifically to fight work from home scams. In this work, we focus on the activities of scammers on online social media, which has increasingly become a popular medium for advertising (See Figure-1). By analyzing different features of a “work from home” advertisement, we try to predict whether it is scam or safe. Unfortunately this problem has failed to gain enough attention from the research community. To the best of our knowledge, there is no prior work which attempts to address the problem of scams on social media. We present a study of around 10000 “work from home” and “Non work from home” posts on Google+ and their characterization on various features to distinguish safe “work from home” posts from scam “work from home” posts. We chose Google+ because unlike Twitter and Facebook, Google+ does not have any limitation of characters in a post. This makes it a suitable platform for advertisers and marketers. Our initial results are encouraging. We are able to distinguish safe posts from scam posts with around 65% accuracy. We believe that this study can be extended to build plugins or alert systems for users to warn them about suspicious posts. Such an on-the-fly alert mechanism will prove to be much more beneficial than existing systems which only focus on generating awareness and facilitating post incident reporting. In rest of the paper we refer “Safe work from home” posts simply as “Safe posts”, “Scam work from home posts” as “Scam posts” and “Non work from home” posts as “Normal posts”.



Kelly Land
Shared publicly - Dec 1, 2012

Have you checked out the great work at home jobs and online jobs posted at MoneyMakingMommy.com this past week? Grab some coffee over the weekend and look them over. Your future at home career awaits you.
http://www.moneymakingmommy.com/daily-work-at-home-job-round-up/
#onlinework #workonline #jobseekers #jobopening

Bonnie Steiner at Bilingual Therapies
Shared publicly - 8:04 AM #Teletherapy

Part Time #Teletherapy #SLPJob in #Wisconsin! Work From Home and flexible hours!

Fig 1: “Work-from-home” posts on Google+

2. METHODOLOGY

We collected a total of 4378 “work from home” posts and 5000 “non work from home” posts by doing a hashtag based search using Google+ API. Hashtags used for collecting “work from home”’ posts were: #Workfromhome, #Workathome, #Makemoneyonline, #earnmoneyonline, #workfromhomejobs, #workfromhomeopportunity and #earnmoneyfromhome. Normal trending hashtags as displayed on Google+ were used to collect “non work from home”’ posts. Figure – provides an architecture diagram of the approach we followed. All the posts were further processed to retrieve URLs and hashtags contained in each post. To establish the ground truth, we need some way to annotate posts as safe and suspicious. For this, we followed a two pronged approach. Firstly, we used information scattered on the web to create a database of popular work from home sites which are scam. There are several online forums where users report and discuss about such sites. We manually scraped a few such web pages to obtain 3000 unique URLs of websites which were reported to be indulged in work from home scams. Unfortunately, this approach proved to be of little use as there were very few scam URLs which also matched with URLs contained in Google+ posts collected by us. This indicates that such information available on the web is insufficient to conclude anything for a given website, and hence is not effective in preventing users from falling prey to such scams. As a second approach, we used a third party service - www.ScamVoid.com. ScamVoid [3] is a free online service which allows users to know whether a website is scam or reliable. It also takes in to account the reports of other well established services like MyWot, Alexa, Google Safebrowsing, Threatlog etc. along with user reports available on google search to reach any conclusion. It takes as input a URL of site and returns whether it is safe or scam. Unfortunately, the site has not exposed any webservice yet. Therefore, we sent repeated 'POST' requests to the site for every URL we had to check, and scraped the webpage to obtain the result. For every work from home post in our collection, we checked the status of URLs contained in it on ScamVoid. A post which contained at-least one scam URL was marked as 'Scam'. Rest of the posts were marked as 'Safe'. Using this technique around 661 posts were marked as 'Scam', which account for 15.09% of total "work from home" posts. We used six main features to further characterize scam and safe posts. Features used by us are listed in Table 2.

By doing some preliminary investigations using these features, we could obtain very distinguishing results for scam and safe posts. We also tried to use these features for classifying posts using Naive Bayes classification algorithm [4]. Our findings are elaborated in the next section.

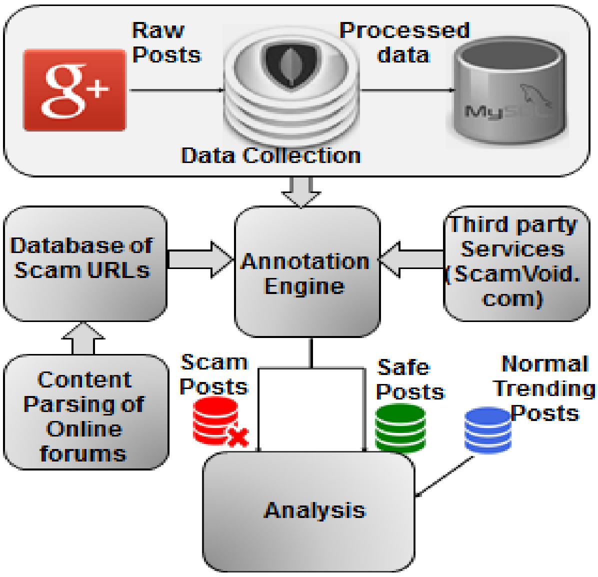


Fig 2: Methodology

3. RESULTS

3.1 Characterization

We calculated the average values of the six features listed in Table 2 for all the categories of posts (Safe, Scam and Normal). It was observed that there are three main features - URL Count, HashTag Count and Content Length which show major variation in their average values for different categories of posts (See Table1). As we can see in the table, average count of resharers, replies and plusoners do not vary much across safe, scam and normal posts. Since 'resharing' , 'replying' or upvoting/ 'plusone' is end user's action on a given post, consistency in average values of these features across different categories indicates that most of the users are unaware whether a post is safe or scam. On the other hand, the features which show most variation – URL Count, hashtag count and content length are more associated with the creator. It is evident that scammers have a tendency to write longer posts with more hashtags and URLs. Embedding a number of hashtags in each post enables easy spread of the message. They write longer content to make it more catchy and attractive. To check how the number of posts for each category varies with change in values of a feature, we traced CDF plots [5] for all the seven features. Again, URL Count, HashTag Count and Content Length were main features for which a prominent difference was observed (Figure 2). CDF plots reinforced our assumption that scammers have a tendency to include more hashtags and URLs in their posts. Also, that the Scam posts are generally lengthier than safe posts, as evident by the CDF plot for content length.

Table 1: Average count of features for different categories of posts

Feature	Safe	Scam	Normal
#Resharers	0.059	0.026	1.576
#Replies	0.185	0.113	1.623
#Plusoners	0.609	0.408	10.348
#Content Length	301.595	854.978	168.787
#URL Count	0.632	11.767	0.215
#HashTag Count	8.432	20.407	3.419

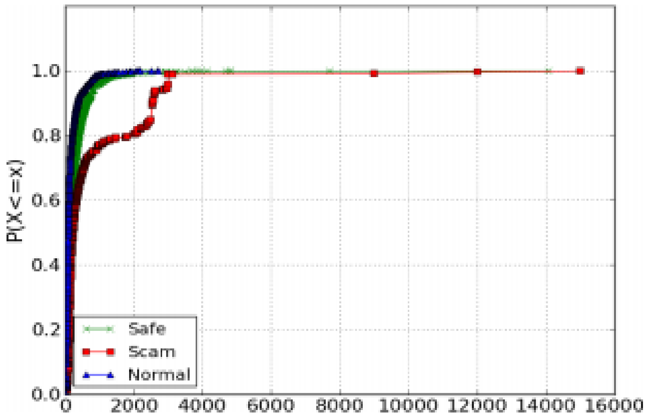


Fig 4: CDF plot for Content length

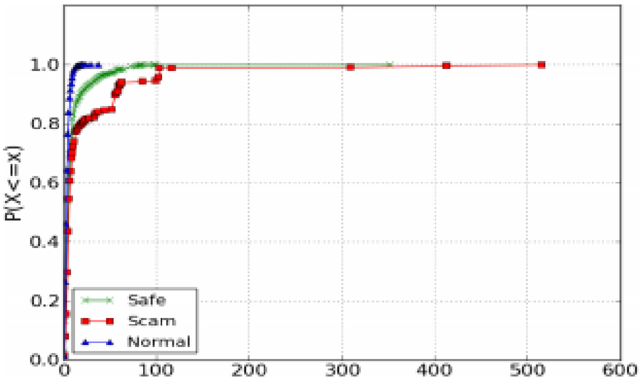


Fig 5: CDF plot for Hashtag count

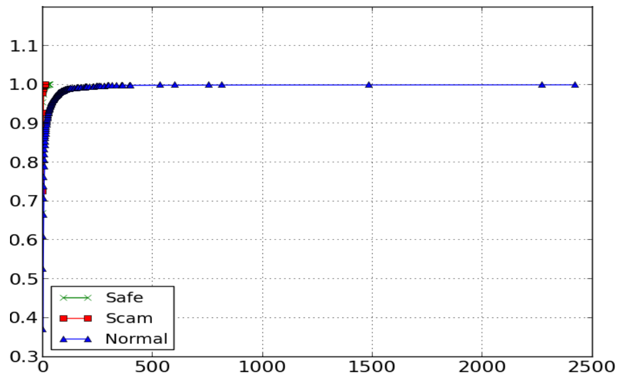
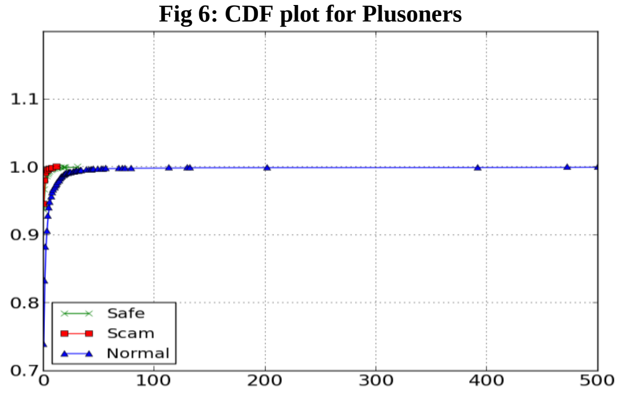


Fig 6: CDF plot for Plusoners



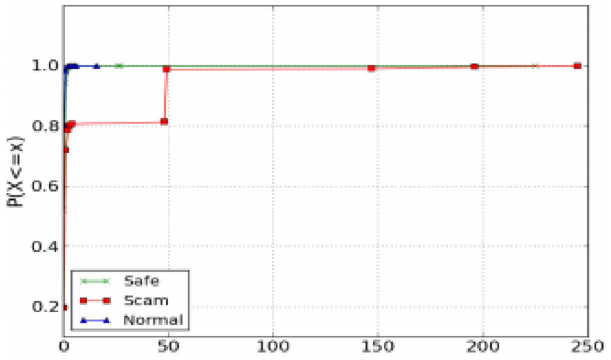


Fig 7: CDF plot for Replies

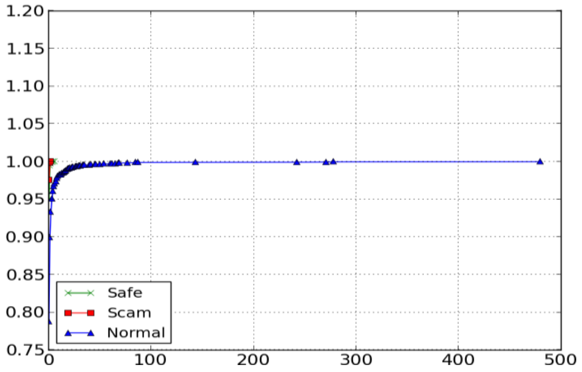


Fig 8: CDF plot for Resharers

We also built tag-clouds (Figure 3) for the hashtags used in safe and scam posts to check if there is any difference in the types of words used in these posts. Interestingly, we observed that while safe posts used more professional words like Entrepreneur, Homebusiness, Affiliate marketing etc; on the other hand scam posts laid more emphasis on tempting words like Love, Money, Marriage and sometimes even on profane words like sex. This again indicates that scammer tend to use all sorts of tricks to make their posts more eyecatchy.

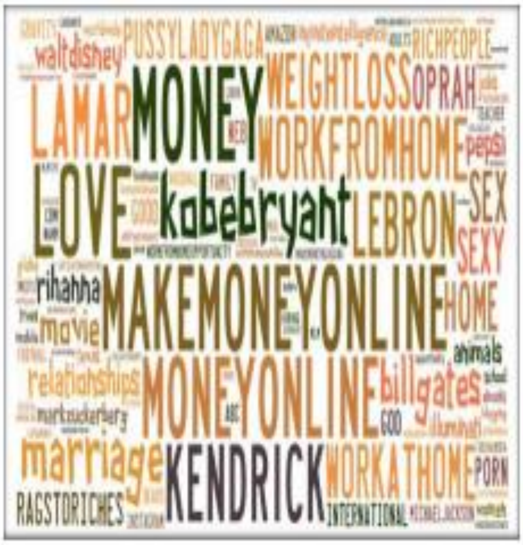


Fig 7: Tag cloud for scam posts

Next, we did a who-is lookup [6] of websites referred by top work from-home campaigns in our collection. This helped us gain useful insights about the domain registered by these campaigners. One interesting observation was regarding the creation date of these domains. We observed that most of the suspicious campaigns have a fairly recent creation date, whereas most of the safe campaigns were running since many years, hence had older creation dates. This gave way to the conclusion that scammers have a tendency to put up the show for a shorter duration of time in which they can make maximum profits without having to face any risks of getting caught due to growing suspicion. Safe campaigns, on the other hand, gradually establish their reputation and win the trust of users. Table 2 lists the creation dates of some of the campaigns from our database.

Table 2: Creation date of various campaigns

Campaign	Creation Date
Makemoneywithmeghan	21-jul-2013
Moneymakingmommy	29-jun-1999
Earningfreemoney	29-dec-2008
Badasscontent	08-apr-2013
925killers	14-nov-2012
Mumandworking	20-Jul-2005
Virtualvocations	31-jan-2007

3.2 Classification

We used Naive Baye's Classification Algorithm with the seven features listed in Table 2. To avoid biasing, we kept equal number of scam and safe posts in our initial training set. Our classifier showed an overall accuracy of 65%. Precision and Recall for scam and safe posts are listed in the Table 3:

Table 3: Precision and Recall

	Precision	Recall
Safe	66.2%	60.7%
Scam	59.6%	65.1%

4. CONCLUSION AND FUTURE WORK

Problem of fraudulent marketing and scams on online social media has not gained enough attention from research community. We believe that this work is the first step in that direction. It can be used to build intelligent systems that can identify fraudulent "work from home" campaigns and alert the user well in time. Although this study focuses only on Google+, we hope to get similar results on Facebook and Twitter. This is due to the generalness of our feature set. Every feature has a corresponding mapping on Facebook/Twitter. For example, 'Plusone'/'Reshare' on Google+ is equivalent to 'like'/'Share' on Facebook and 'Favorite'/'Retweet' on Twitter. We have observed existence of similar 'work from home' campaigns on Twitter. It will be interesting to study the characteristics of scammers on different networks and draw linkages if there are any. Another important area to focus can be study of network these campaigners form online. We believe that interesting inferences can be drawn on observing social network of scammers on social media platform. We look forward to cover these aspects in future.

5. REFERENCES

[1] ScamWatch Australia, http://www.scamwatch.gov.au/

[2] US government webpage, http://www.consumer.ftc.gov/articles/0175-work-home-usinesses/

[3] ScamVoid, http://www.scamvoid.com/

[4] Naïve Bayes Classifier, http://en.wikipedia.org/wiki/Naive_Bayes_classifier

[5] Cumulative distribution function, http://en.wikipedia.org/wiki/Cumulative_distribution_function

[6] Who Is Lookup,s http://www.whois.com/whois/