SCAM–ALERT: CHARACTERIZING WORK FROM HOME SCAMS

Rashi Garg*
IIIT Delhi
rashi1216@iiitd.ac.in

Shaifali Gupta*
IIIT Delhi
shaifali1219@iiitd.ac.in

1. MOTIVATION

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 (See Figure 1). Some countries like Australia[1] and U.S.[2] have established enforcement agencies specifically to fight work from home scams. In this work, we instead focus on the activities of scammers on online social media, which has increasingly become a popular medium for advertising. 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 benefical 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".

Figure 1: A "work from home" post

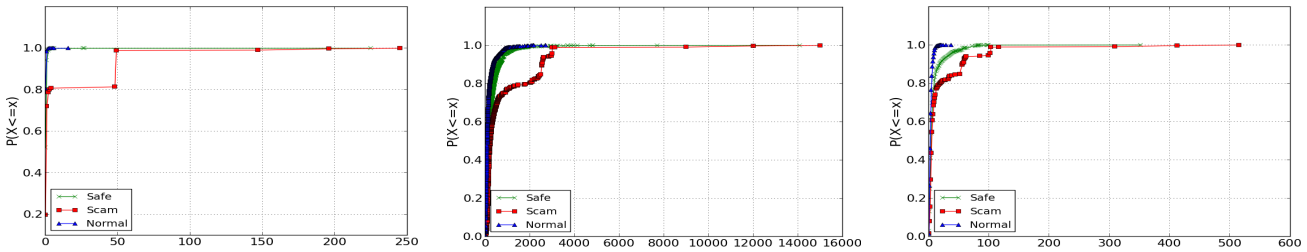
*Authors have equal contributions.

[1] http://www.scamwatch.gov.au/

[2] http://www.consumer.ftc.gov/articles/0175-work-home-businesses/

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. 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 categorize posts as safe and suspicious. For this, we followed a two pronged approach. Firstly, we used information scattered on the web to create a list 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 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 database, 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 seven 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. Our findings are



(a) URL Count (b) Content Length (c) HashTag Count

Figure 2: CDF Plots

Feature	Explanation
Resharers	#People who have reshared a post
Replies	#People who replied to a post
Plusoners	#People who 'plusoned' a post
URL Count	#URLs in the content of a post
HashTag Count	#hashtags in the content of a post
Content Length	Length of Content of a post
ChatterScore	Sum of Resharers, Replies and Plusoners

Table 1: Features

(a)Tagcloud for safe posts (b)Tagcloud for scam posts

Figure 3: Tagclouds

elaborated in the next section.

3. RESULTS

3.1 Characterization

We calculated the average values of the seven 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 Table 3.1). To check how the number of posts for each category vary with change in values of a feature, we traced CDF plots 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). It was observed that scammers have a tendency to include more hashtags and URLs in their posts. Also, Scam posts are generally lengthier than safe posts, as evident by the average content length of both types of posts.

	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
Chatter Score	0.853	0.548	13.13

Table 2: Average Values

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.

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 following Table:

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

Table 3: Naive Baye's Classifier Results

4. IMPLICATIONS OF RESULTS

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 focusses only on Google+, we hope to get similar results on Facebook and Twitter. This is due to the genericness 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. We look forward to cover these aspects in future.