Ju Shua Tan. Social Bot in Social Media: Detections and Impacts of Social Bot on Twitter Users. A Master's paper for the M.S. in I.S. degree. April, 2018. 107 pages. Advisor: Bradley M. Hemminger

A social bot is a computer algorithm that automatically produces content and interacts with humans on social media, trying to emulate and possibly alter their behavior. Social bots have inhabited social media platforms for the past few years. Although the initial intention of social bot might be benign, existence of social bot can also bring negative implication to society. For example, in the aftermath of Boston marathon bombing, a lot of tweets has been retweeted without people verifying its accuracy. Therefore, social bot might have the tendency to spread fake news and incite chaos in public. For example, after the Parkland, Florida school shooting, Russian propaganda bots are trying to seize on divisive issues online to sow discord in the United States.

This study describes a questionnaire survey of Twitter users about their Twitter usage, ways to detect social bots on Twitter, sentiments towards social bots, as well as how the users protect themselves against harmful social bots. The survey also uses an experimental approach where participants upload a screenshot of a social bot. The result of the survey shows that Twitter bots bring more harms than benefits to Twitter users. However, the advancement of social bots has been so great that it has been hard for human to identify real Twitter users from fake Twitter users. That's why it is very important for the computing community to engage in finding advanced methods to automatically detect social bots, or to discriminate between humans and bots. Until that process can be fully automated, we need to continue educating more Twitter users about ways to protect themselves against harmful social bots.

Headings:

Social media

Microblogs

Social bots

Artificial intelligence

Surveys

SOCIAL BOT IN SOCIAL MEDIA:
DETECTIONS AND IMPACTS OF SOCIAL BOT ON TWITTER USERS

by
Ju Shua Tan

A Master's paper submitted to the faculty
of the School of Information and Library Science
of the University of North Carolina at Chapel Hill
in partial fulfillment of the requirements
for the degree of Master of Science in
Information Science.

Chapel Hill, North Carolina

April, 2018

Approved by:

Bradley M. Hemminger

Table of Contents

Introduction

Along with the advancement of modern Internet technology and smartphone usage, we have seen the rapid development of popular social network sites such as Twitter, Facebook, Instagram, Snapchat, Vine, Tumblr and etc. People are using these popular social media sites to be able to communicate with their friends and network as well as sharing about their personal stories, interests, opinions and beliefs to the whole world. One of the most popular social media that this paper will dive deeper into is Twitter.

Twitter is an online news and social networking service on which users post and interact with messages known as "tweets". Users are restricted to only use 140 characters for each tweet. Since released publicly in 2006, Twitter has experienced initial rapid growth to rise as a mainstream social outlet for the discussion of a variety of topics through microblogging interactions. As billions of tweets are being posted every day, including by the most powerful man in the world, President Donald Trump, Twitter has gained so much interest and attention from the whole world. As Twitter has evolved from a simple microblogging social media interface into a mainstream source of communication for the discussion of current events, politics, consumer goods/services, it has become increasingly enticing for parties to manipulate the system by creating automated software to send messages to organic (human) accounts as a means for personal gain and for influence manipulation (Clark, Williams, Jones, Galbraith, Danforth, & Dodds, 2016).

Bots have been around since the early days of computers. These automated software that tries to emulate a real human who is posting contents like tweets on social media are known as social bots. One particularly popular medium for social bots is Twitter. Twitter bots are automated agents that operate in Twitter using fake accounts. Although people may straight away dismiss Twitter bots as inherently bad, they are often benign, or even useful, but some are created to harm, by tampering with, manipulating, and deceiving social media users (Ferrara, Varol, Davis, Menczer & Flammini, 2016). Often times they try to spread fake news or influence political opinions. Fake news and the way it spreads on social media is emerging as one of the greatest threats to modern society. In recent times, fake news has been used to manipulate stock markets, make people choose dangerous health-care options, and manipulate elections, including 2016 presidential election in the U.S (Bessi & Ferrara, 2017). It is thus very important for us to understand more about the existence of social bots and try to find ways to automatically detect them.

Recently being widely debated in the news, after the Parkland, Florida school shooting, we have read a lot about how Russian propaganda bots are trying to seize on divisive issues online to sow discord in the United States. This is just one of the most recent examples of how social bots can wade into our everyday lives. There are many ways that social bot can enter into a Twitter feed and impact the way how normal Twitter users interact with the bot. Often time, Twitter users do not realize that they are interacting with a bot, and might reveal information that are too much of their own personal information and thus might put their own privacy at risk. Therefore, this paper aims to investigate the many ways that social bots can appear and what are the risks that it can bring to the regular Twitter users.

Research Problem

Most of the researches that I have found are focusing on the methodologies on how to identify social bots among tweets. Even though this topic is trending in the news right now, few researches have actually studied the social impact of social bots by conducting an online survey among Twitter users. As the current events about Russian bots continue to unfold in the country right now, this topic has been increasingly popular due to the mass media attention that it received. Therefore, in this master's paper, the main research question that I want to explore are:

How do social bots impact online social media ecosystems and our society?

This is a very important question to research because social bots impact all aspects of our social lives as technology have changed the way we interact with other people. I have also decided to use survey questionnaire method to explore these four specific research questions below:

Specific Research Questions:

RQ1. By looking at existing research in this area, why do social bots appear in Twitter?

RQ2. By doing literature review to identify methods used by other researchers, what are the ways that we detect social bots in Twitter? By incorporating some experimental questions in my survey, I want to see whether my participants are able to detect social bots because one of the question in my survey asked them to provide a screenshot of what they perceived to be a social bot. If my participants do not have a lot of knowledge about social bots, I hope that my survey can raise their awareness about social bots in Twitter and better protect themselves against the negative impact of Twitter bots.

RQ3. Through the survey questionnaire to Twitter users, what are the positive and negative impacts of social bots on social media users?

RQ4. By doing a literature review, and understanding why social bots exist, identifying and incorporating users' needs and desires, what are the general best practices for automatic detection of social bots in Twitter?

These research questions will lead me to explore the various issues of social bots, not only from the perspective of the computer programmers, but also from the everyday perspective of ordinary Twitter users. I haven't seen any other surveys out there that explicitly ask Twitter users about their personal interactions with social bots yet, so hopefully this method will be yield a lot of new insights into the research of how Twitter users interact with social bots and be able to answer all my research questions above.

Literature Review

In my literature review, there are four sections that I think are very important to understand how social bots work from multiple perspectives. The first section will explore multiple ways we can detect social bots. The second section will identify the impact of social bots in our society, especially in politics since social bots have a large impact in influencing presidential election results. The third section will be explaining about the intricacies of the design of social bots and how social bots operate. Finally, for narrative summary of our literature review, we will propose several standards for social bot use.

Social Bot Detection

An area of intense research in artificial intelligence area is the detection of social bots. As Twitter users, there can be many interactions with social bots that we do not even realize. To assist human users in identifying who they are interacting with, Chu et al. focused on the classification of human, bot and cyborg accounts on Twitter. The researchers first conducted a set of large-scale measurements with a collection of over 500,000 accounts. The researchers observed the difference among human, bot and cyborg in terms of tweeting behavior, tweet content, and account properties. Based on the measurement results, the researchers proposed a classification system that includes the following four parts: (1) an entropy-based component, (2) a machine-learning-based component, (3) an account properties component, and (4) a decision maker. (Chu, Gianvecchio, Wang, & Jajodia, 2010).

A lot of the times, there were no differences in the perceptions of source credibility, communication competence, or interactional intentions between the bot and human Twitter agents. Therefore it is not unusual that we sometimes question whether is that a bot running the social media feed. Edwards et al. suggested that people will respond to a computer in a similar manner as they would to a human if the computer conforms to their expectations of an appropriate interaction (Edwards, Spence, & Shelton, 2014).

However, a majority of Sybils (machine-controlled Twitter accounts) have actually successfully integrated themselves into real social media user communities (such as Twitter and Facebook). In this study, Alarifi et al. compared the current methods used for detecting Sybil accounts. The researchers also explored the detection features of various types of Twitter Sybil accounts in order to build an effective and practical classifier. To evaluate their classifier, the researchers collected and manually labeled a dataset of Twitter accounts, including human users, bots, and hybrids (i.e., tweets posted by both human and bots). The researchers consider that this Twitter Sybils corpus will help researchers to conduct high-quality measurement studies (Alarifi, Alsaleh & Al-Salman, 2016). BotOrNot is a publicly-available service that leverages more than one thousand features to evaluate the extent to which a Twitter account exhibits similarity to the known characteristics of social bots. Since its release in May 2014, BotOrNot has served over one million requests via Davis et al.'s website and APIs (Davis, Varol, Ferrara, Flammini, & Menczer, 2016).

Gilani et al. comparatively analyzed the usage and impact of bots and humans on Twitter, by collecting a large-scale Twitter dataset and define various metrics based on tweet metadata. Using a human annotation task the researchers assigned 'bot' and 'human' ground truth labels to the dataset, and compare the annotations against an online bot detection tool for evaluation. The researchers then asked a series of questions to discern important behavioral characteristics of bots and humans using metrics within and among four popularity groups. From the comparative analysis the researchers drew differences and interesting similarities between the two entities (Gilani, Farahbakhsh, Tyson, Wang & Crowcroft, 2017).

Fake followers are those Twitter accounts specifically created to inflate the number of followers of a target account. Therefore, we would also consider fake followers as another kind of a social bot. Cresci et al. contributed along different dimensions for this problem. First, they reviewed some of the most relevant existing features and rules for anomalous Twitter accounts detection. Second, the researchers created a baseline dataset of verified human and fake follower accounts. Then, they exploited the baseline dataset to train a set of machine-learning classifiers built over the reviewed rules and features in revealing fake followers (Cresci, Di Pietro, Petrocchi, Spognardi & Tesconi, 2015).

Fake news have also been in the limelight of the media a lot, especially since the Trump administration began. Online news sites have become an internet 'staple', but we know little of the forces driving the popularity of such sites in relation to social media services. Larsson & Hallvard discussed empirical results regarding the uses of Twitter for news sharing. Specifically, they presented a comparative analysis of links emanating from the service at hand to a series of media outlets in Sweden and Norway. They then problematized the assumption that online communication involves two or more humans by directing attention to more or less automated 'bot' accounts. They then made conclusion that automated accounts need to be dealt with more explicitly by researchers as well as practitioners interested in the popularity of online news as expressed through social media activity (Larsson & Hallvard, 2015).

Ratkiewicz et al. studied astroturf political campaigns on microblogging platforms: politically-motivated individuals and organizations that use multiple centrally-controlled accounts to create the appearance of widespread support for a candidate or opinion. The researchers described a machine learning framework that combines topological, content-based and crowdsourced features of information diffusion networks on Twitter to detect the early stages of viral spreading of political misinformation (Ratkiewicz, Conover, Meiss, Gonçalves, Flammini, & Menczer, 2011).

Another technique, "Analysis Based Detection Techniques (ABDT)" is a novel technique to detect fast flux service network (FFSN) based Social Bots on social media based on presented information on user's profile. It uses geographically-dispersed set of proxy hosts to locate the position of the mothership in an abstract and dimensional space and built similarity graph (clustering) for each URL presented to validation checking for each user (Tyagi & Aghila, 2012).

Twitter has a vast source of linguistic data, rich with opinion, sentiment, and discussion. Therefore, Twitter bots can range from the benevolent (e.g., weather-update bots, help-wanted-alert bots) to the malevolent (e.g., spamming messages, advertisements, or radical opinions). Existing detection algorithms typically leverage metadata (time between tweets, number of followers, etc.) to identify robotic accounts. Clark et al. presented a powerful classification scheme that exclusively uses the natural language text from organic users to provide a criterion for identifying accounts posting automated messages (Clark, Williams, Jones, Galbraith, Danforth & Dodds, 2016).

To understand social bot behavior on end hosts, Ji et al. collected the source code, builders and execution traces of existing social bot to examine three state-of-the-art detection approaches over their collected traces. The researchers then used a new detection approach with nine new features and two new correlation mechanisms. This approach was proved to detect existing social bots with significant results (Ji, He, Jiang, Cao & Li, 2016).

Due to the development of social networks in the Internet such as Facebook, Twitter and Instagram, the programs that provide automatic users' actions imitation are able to obtain wide circulation. Common usage of these programs causes informational noise. Drevs & Svodtsev considered a possibility of fuzzy logic mathematical apparatus application for the recognition of these programs' activity in social networks (Drevs & Svodtsev, 2016).

Through different machine learning techniques, researchers have now begun to investigate ways to detect these types of malicious accounts automatically. To successfully differentiate between real accounts and bot accounts, a comprehensive analysis of the behavioral patterns of both types of accounts is required. Kaya et al. investigated ways to select the best features from a data set for automated classification of different types of social media accounts (ex. bot versus real account) via visualization. To help select better feature combinations, the researchers tried to visualize which features may be more effective for classification using self-organizing maps (Kaya, Conley & Varol, 2016).

From politicians and nation states to terrorist groups, numerous organizations reportedly conduct explicit campaigns to influence opinions on social media, posing a risk to freedom of expression. Thus, there is a need to identify and eliminate "influence bots"-realistic, automated identities that illicitly shape discussions on sites like Twitter and Facebook-before they get too influential. In response to this problem, Defense Advanced Research Projects Agency (DARPA) held a four-week competition in February and March 2015, in which multiple teams supported by DARPA’s Social Media in Strategic Communications (SMISC) program competed to identify a set of influence bots on Twitter serving as ground truth on a specific topic. From this competition, Subrahmanian et al. learned that bot detection is a semiautomated process that builds on four broad techniques: inconsistency detection and behavioral modeling, text analysis, network analysis, and machine learning (Subrahmanian, Azaria, Durst, Kagan, Galstyan, Lerman & Menczer, 2016).

The popularity of social media platforms such as Twitter has led to the proliferation of automated bots, creating both opportunities and challenges in information dissemination, user engagements, and quality of services. Past works on profiling bots had been focused largely on malicious bots, and assume that these bots should be removed. However, Oentaryo et al. found many bots that are benign, and proposed a new, broader categorization of bots based on their behaviors. This includes *broadcast*, *consumption*, and *spam* bots. To facilitate comprehensive analyses of bots and how they compare to human accounts, the researchers developed a systematic profiling framework that includes a rich set of features and classifier bank. They conducted extensive experiments to evaluate the performances of different classifiers under varying time windows, identify the key features of bots, and infer about bots in a larger Twitter population (Oentaryo, Murdopo, Prasetyo & Lim, 2016).

Gilani et al. provided some wonderful statistics and characteristics on how to detect social bots. Their work confirmed a number of noteworthy trends: (i) bots generally retweet more often, while some humans can exhibit bot-like activity; (ii) bots can post up to 5 times more URLs in their tweets; (iii) bots can upload 10 times more content with their tweets; (iv) humans can receive as much as 27 times more likes and 24 times more retweets as bots; (v) bots retweeting other bots is over 3 times more regular than bots retweeting humans, whereas humans retweeting other humans is over 2 times greater, indicating homophily; (vi) humans favorite others' tweets much more often than bots do, though newer bots are far more aggressive in favoriting tweets to replicate human behavior; (vii) humans enjoy higher levels of friendship and usually form reciprocal relationships; (viii) bots typically use many different sources for active participation on Twitter (up to 50 or more); and (ix) activity sources include basic automation and scheduling services — used abundantly by bots and seldomly by human (Gilani, Wang, Crowcroft, Almeida & Farahbakhsh, 2016).

Influence of Social Bots in Politics

Over the last several years political actors worldwide have begun harnessing the digital power of social bots — software programs designed to mimic human social media users on platforms like Facebook, Twitter, and Reddit. Increasingly, politicians, militaries, and government-contracted firms use these automated actors in online attempts to manipulate public opinion and disrupt organizational communication. Politicized social bots — here 'political bots' — are used to massively boost politicians' follower levels on social media sites in attempts to generate false impressions of popularity. They are programmed to actively and automatically flood news streams with spam during political crises, elections, and conflicts in order to interrupt the efforts of activists and political dissidents who publicize and organize online. They are used by regimes to send out sophisticated computational propaganda. Woolley conducted a content analysis of available media articles on political bots in order to build an event dataset of global political bot deployment that coded for usage, capability, and history. This information was then analyzed, generating a global outline of this phenomenon (Woolley, 2016).

After the broad overview, now we are going to explore the impact of social bots on very specific political events in different countries all across the world. Let us start with US first, especially with the highly contested 2016 presidential election. By leveraging state-of-the-art social bot detection algorithms, Bessi & Ferrara uncovered a large fraction of user population that may not be human, accounting for a significant portion of generated content. The researchers inferred political partisanships from hashtag adoption, for both humans and bots, and studied spatio-temporal communication, political support dynamics, and influence mechanisms by discovering the level of network embeddedness of the bots. The researchers' findings suggested that the presence of social media bots can indeed negatively affect democratic political discussion rather than improving it, which in turn can potentially alter public opinion and endanger the integrity of the Presidential election (Bessi & Ferrara, 2016).

This same presidential election had also been associated with the problem of fake news for a long time, and we are very interested in finding out if the fake news have actually increased the support for Trump and depress Hillary Clinton's support on Election Day. The massive spread of fake news has been identified as a major global risk and has been alleged to influence elections and threaten democracies. Shao et al. analyzed 14 million messages spreading 400 thousand claims on Twitter during and following the 2016 U.S. presidential campaign and election. They found evidence that social bots indeed played a key role in the spread of fake news. Accounts that actively spread misinformation are significantly more likely to be bots. Automated accounts are particularly active in the early spreading phases of viral claims, and tend to target influential users. Humans are vulnerable to this manipulation, retweeting bots who post false news (Shao, Ciampaglia, Varol, Flammini, & Menczer, 2017).

The same problem of social bots influencing the result of the presidential election does not only occur in the US, but also in France. Similar disinformation campaigns have been coordinated by means of bots, social media accounts controlled by computer scripts that try to disguise themselves as legitimate human users. Ferrara described one such operation occurred in the run up to the 2017 French presidential election. Ferrara collected a massive Twitter dataset of nearly 17 million posts occurred between April 27 and May 7, 2017 (Election Day) to study the MacronLeaks disinformation campaign: By leveraging a mix of machine learning and cognitive behavioral modeling techniques, the researchers separated humans from bots, and then studied the activities of the two groups taken independently, as well as their interplay. However, unlike the US presidential election, the disinformation campaign in France did not succeed and Macron still won the French presidential seat. The reasons of the scarce success of this campaign: the users who engaged with MacronLeaks are mostly foreigners with a preexisting interest in alt-right topics and alternative news media, rather than French users with diverse political views. (Ferrara, 2017).

Besides US and France, the next country that we will be focusing on is UK. Murthy et al. analyzed a high-stakes political environment, the UK general election of May 2015, asking human volunteers to tweet from purpose-made Twitter accounts-half of which had bots attached-during three events: the last Prime Minister's Question Time before Parliament was dissolved (#PMQs), the first leadership interviews of the campaign (#BattleForNumber10), and the BBC Question Time broadcast of the same evening (#BBCQT). Based on previous work, the researchers initially expected was that their intervention would make a significant difference to the evolving network, but they found that the bots they used had very little effect on the conversation network at all. There were economic, social, and temporal factors that impact how a user of bots can influence political conversations (Murthy, Powell, Tinati, Anstead, Carr, Halford & Weal, 2016).

Computational propaganda deploys social or political bots to try to shape, steer and manipulate online public discussions and influence decisions. Collective behavior of populations of social bots has not been yet widely studied, though understanding of collective patterns arising from interactions between bots would aid social bot detection.

Duh et al. showed that there were significant differences in collective behavior between population of bots and population of humans as detected from their Twitter activity. Using a large dataset of tweets they have collected during the UK EU referendum campaign, the researchers separated users into population of bots and population of humans based on the length of sequences of their high-frequency tweeting activity. The result showed that while pairwise correlations between users are weak they co-exist with collective correlated states, however the statistics of correlations and co-spiking probability differ in both populations (Duh, Rupnik & Korošak, 2017).

Our next country will be closer to us, which is Mexico. Social bots can also affect online communication among humans. Suárez-Serrato et al..studied this phenomenon by focusing on #YaMeCanse, the most active protest hashtag in the history of Twitter in Mexico. Accounts using the hashtag are classified using the BotOrNot bot detection tool. Their preliminary analysis suggests that bots played a critical role in disrupting online communication about the protest movement (Suárez-Serrato, Roberts, Davis, & Menczer, 2016).

Finally, instead of looking at political activity in another country, we will slightly shift our focus to governmental activities online. WikiEdits bots are a class of Twitter bot that announce edits made by Wikipedia users editing under government IP addresses, with the goal of making government editing activities more transparent. Ford et al. examined the characteristics and impact of transparency bots, bots that make visible the edits of institutionally affiliated individuals by reporting them on Twitter. The researchers map WikiEdits bots and their relationships with other actors, analyzing the ways in which bot creators and journalists frame governments' participation in Wikipedia. The researchers found that, rather than providing a neutral representation of government activity on Wikipedia, WikiEdits bots and the attendant discourses of the journalists that reflect the work of such bots constructed a partial vision of government contributions to Wikipedia as negative by default. This has an impact on the public discourse about government's' role in the development of public information, a consequence that is distinct from the current discourses that characterize transparency bots (Ford, Dubois & Puschmann, 2016).

Impact of Social Bots

After going through all the negative political impact being brought by the social bots, let us now explore some of the bright side of the impact of social bots in other areas, such as tackling harassment. Munger conducted an experiment which examined the impact of group norm promotion and social sanctioning on racist online harassment. Racist online harassment de-mobilizes the minorities it targets, and the open, unopposed expression of racism in a public forum can legitimize racist viewpoints and prime ethnocentrism. Munger employed an intervention designed to reduce the use of anti-black racist slurs by white men on Twitter. Munger collecteed a sample of Twitter users who have harassed other users and use accounts Munger control ("bots") to sanction the harassers. By varying the identity of the bots between in-group (white man) and out-group (black man) and by varying the number of Twitter followers each bot has, Munger found that subjects who were sanctioned by a high-follower white male significantly reduced their use of a racist slur (Munger, 2017).

Geiger also explored the role of social bots to tackle the problem of harassment, but with a different method. Geiger introduced and discussed bot-based collective blocklists (or blockbots) in Twitter, which have been developed by volunteers to combat harassment in the social networking site. Blockbots support the curation of a shared blocklist of accounts, where subscribers to a blockbot will not receive any notifications or messages from accounts on the blocklist. Blockbots support counterpublic communities, helping people moderate their own experiences of a site. Blockbots also helps raising issues about networked publics and platform governance. Such projects involve a more reflective, intentional, transparent, collaborative, and decentralized way of using algorithmic systems to respond to issues of platform governance like harassment. The author argued that blockbots are not just technical solutions but social ones as well, a notable exception to common technologically determinist solutions that often push responsibility for issues like harassment to the individual user (Geiger, 2016).

After looking at the positive impact of social bots in overcoming harassment, we will be looking at how social bots can help academia. Haustein et al. presented preliminary findings on automated Twitter accounts distributing links to scientific articles deposited on the preprint repository arXiv. It discussed the implication of the presence of such bots from the perspective of social media metrics (altmetrics), where mentions of scholarly documents on Twitter have been suggested as a means of measuring impact that is both broader and timelier than citations. The results showed that automated Twitter accounts create a considerable amount of tweets to scientific articles and that they behave differently than common social bots, which has critical implications for the use of raw tweet counts in research evaluation and assessment (Haustein, Bowman, Holmberg, Tsou, Sugimoto & Lariviere, 2016).

Social media has also become a place for discussion and debate on controversial topics, and thus provides an opportunity to influence public opinion. This possibility has given rise to a specific behavior known as trolling. A troll is an individual who shares inflammatory, extraneous or off-topic messages in social media, with the primary intent of provoking readers into an emotional response or otherwise disrupting on-topic discussion. The analysis of trolling is based on public discussion stakeholder, including positively engaged faith-holders, negatively engaged hateholders, and fakeholders. Trolls can be considered as either hateholders (humans) or fakeholders (bots or cyborgs). Paavola et al. continued the work of sentiment analysis with automatic detection of bots, which facilitates the analysis of fakeholder communication's impact. The automatic bot detection feature is implemented in the sentiment analysis tool in order to remove the noise in a discussion (Paavola, Helo, Sartonen & Huhtinen, 2016).

Cha et al. came up with three statistics to measure the ‘influence’ of a Twitter account. The following are the three metrics:

- **Indegree**: The number of followers a user has. Represents the user's popularity.
- **Retweets**: The number of times a user's tweets have been retweeted. Represents the content value of the user's tweets.
- **Mentions**: The number of times the user has been mentioned by other users. Represents the user's name value (Cha et al., 2010).

These three metrics are included in the ‘Klout score’. This is a score between 1 and 100 that represents a user's online influence. To compute this score, Klout uses measures such as following count, follower count, retweets, unique mentions, list memberships, how many of the account's followers are spam/dead accounts and how influential the account's retweeters are.

Systems that classify influential users in social networks have been used frequently and are referenced in scientific papers and in the media as an ideal standard of evaluation of influence in the Twitter social network. Messias et al. considered such systems of evaluation to be complex and subjective, and therefore suspected that they are vulnerable and easy to manipulate. Based on this, the researchers created simple robots capable of interacting by means of Twitter accounts, and the researchers measured how influent they were. Even with this automatic and predictive behavior, the bots received significant influence score in two systems that measure influence: Klout and Twitalyzer. The results showed that it is possible to become influential through simple strategies. This suggests that the systems do not have ideal means to measure and classify influence (Messias, Schmidt, Oliveira & Benevenuto, 2013).

While much research has studied how to identify such bots in the process of spam detection, little research has looked at the other side of the question - detecting users likely to be fooled by bots. Wald et al. examined a dataset consisting of 610 users who were messaged by Twitter bots, and determine which features describing these users were most helpful in predicting whether or not they would interact with the bots (through replies or following the bot). The researchers then used six classifiers to build models for predicting whether a given user will interact with the bot, both using the selected features and using all features. They found that a users' Klout score, friends count, and followers count are most predictive of whether a user will interact with a bot, and that the Random

Forest algorithm produces the best classifier, when used in conjunction with one of the better feature ranking algorithms (Wald, Khoshgoftaar, Napolitano & Sumner, 2013).

Wagner et al. studied data from the Social Bot Challenge 2011 - an experiment conducted by the Web Ecology Project during 2011 - in which three teams implemented a number of social bots that aimed to influence user behavior on Twitter. Using this data, the researchers aimed to develop models to (i) identify susceptible users among a set of targets and (ii) predict users' level of susceptibility. The researchers explored the predictiveness of three different groups of features (network, behavioral and linguistic features) for these tasks. The results suggest that susceptible users tend to use Twitter for a conversational purpose and tend to be more open and social since they communicate with many different users, use more social words and show more affection than non-susceptible users (Wagner, Mitter, Körner & Strohmaier, 2012).

Today's social bots are sophisticated and sometimes menacing. Indeed, their presence can endanger online ecosystems as well as our society. Social bots have populate all the techno-social systems: they are often benign, or even useful, but some are created to harm, by tampering with, manipulating, and deceiving social media users. Social bots have been used to infiltrate political discourse, manipulate the stock market, steal personal information, and spread misinformation. The detection of social bots is therefore an important research endeavor (Ferrara, Varol, Davis, Menczer & Flammini, 2016).

Social bots that are legal and truthful can still behave unethically by violating strong norms that create more evil than good. Moral evils inflict “limits on human beings and contracts human life.” Developers who are coerced into doing something unethical without a choice may not be entirely culpable, but in the case of free enterprise there is always a choice. The Bot Ethics procedure serves as a starting point and guide for ethics-related discussion among various participants in a social media community, as they evaluate the actions of social bots (de Lima Salge & Berente, 2017).

Design of Social Bots

After exploring more about the positive and negative impacts of social bots in our daily lives, let's discover more into the technical aspects as how social bots are designed.

The security implications of social bots are evident in consideration of the fact that data sharing and propagation functionality are well integrated with social media sites. Existing social bots primarily use Really Simple Syndication and OSN (online social network) application program interface to communicate with OSN servers. Researchers have profiled their behaviors well and have proposed various mechanisms to defend against them. He et al. predicted that a web test automation rootkit (WTAR) is a prospective approach for designing malicious social bots. After the researchers implemented three WTAR-based bot prototypes on Facebook, Twitter, and Weibo, they validated this new threat by analyzing behaviors of the prototypes in a lab environment and on the Internet, and analyzing reports from widely-used antivirus software. Their analyses showed that WTAR-based social bots have the following features: (i) they do not connect to OSN directly, and therefore produce few network flows; (ii) they can log in to OSNs easily and perform a variety of social activities; (iii) they can mimic the behaviors of a human user on an OSN. Finally, He et al. proposed several possible mechanisms in order to defend against WTAR-based social bots (He, Zhang, Wu & Li 2016).

Since impersonation bots are trying to pretend to be someone else, impersonation bots are smart enough that they are able to generate output in one, or possibly, multiple modalities. Furthermore, rapidly advancing areas of machine learning and artificial intelligence could lead to frighteningly powerful new multi-modal social bots. Although most commonly known bots are one dimensional (i.e., chatterbot), and far from deceiving serious interrogators, however, using recent advances in machine learning, it is possible to unleash incredibly powerful, human-like armies of social bots, in potentially well-coordinated campaigns of deception and influence (Adams, 2017).

Recent innovations in social scientific methodology that aspire to address the complex, iterative and performative dimensions of method become part of a larger project that uses Speculative Design and ethnographic methods to explore energy-demand reduction, specifically considers the ways in which energy-demand reduction features in the Twitter-sphere. Developing and deploying three automated Bots whose function and communications are at best obscure, and not uncommonly nonsensical, Wilkie et al. traced some of ways in which they intervene and provoke. Heuristically, they drew on the conceptual characters' of idiot, parasite and diplomat in order to grasp how the Bots act within Twitter to evoke the instability and emergent eventuations of energy-demand reduction, community and related practice (Wilkie, Michael & Plummer-Fernandez, 2015).

How Social Bots Operate

In this section, we are exploring many literature about how social bots operate in general, to understand in depth what makes social bot so dangerous to social media users. Therefore we will be looking at some researches that were not dealing with Twitter bots but with other kind of social bots, such as Wikipedia bots and news bots.

Political actors are now deploying software programs called social bots that use social networking services such as Facebook or Twitter to communicate with users and manipulate their behavior, creating profound issues for Internet security. Current approaches in bot control continue to fail because social media platforms supply communication resources that allow bots to escape detection and enact influence. Bots become agents by harnessing profile settings, popularity measures, and automated conversation tools, along with vast amounts of user data that social media platforms make available. Guilbeault developed an ecological approach to thinking about bots that focuses on how social media environments propel bots into agency. This habitat-based model used bots to expose ripe targets of intervention and innovation at the level of interface design. It also situated bots in the context of platform providers with a vested interest in interface design, revealing a range of new political problems. Most important, it invited a hybrid ethics, wherein humans and bots act together to solve problems in bot security and Internet ethics more broadly (Guilbeault, 2016).

Development of a social bot with sophisticated human-like behavior faces three main challenges:

- (1) Producing credible and intelligent content, which is accepted as such by human consumers.

- (2) Leaving a trace of human-like metadata in social networks.
- (3) Creating an adequate (often balanced) network of friends or followers to spread information.

While the first challenge is a rather open issue in science and even the more in practice, Grimme et al. found that the second aspect can be handled to a certain extent by imitating human actions in social networks sticking to normal human temporal and behavioral patterns. This includes performing activities in a typical day–night cycle, carefully measured actions at the social media platform, as well as variability in actions and timing. Thus, at Twitter, a bot should pause between actions to simulate phases of inactivity (sleep or work), limit posting and Retweeting activities to a realistic, human-like level, and also vary these pauses and limits (Grimme, Preuss, Adam & Trautmann, 2017).

Bots are, for many Web and social media users, the source of many dangerous attacks or the carrier of unwanted messages, such as spam. Nevertheless, crawlers and software agents are a precious tool for analysts, and they are continuously executed to collect data or to test distributed applications. However, no one knows which is the real potential of a bot, whose purpose is to control a community, to manipulate consensus, or to influence user behavior. It is commonly believed that the better an agent simulates human behavior in a social network, the more it can succeed to generate an impact in that community. Ariello et al. presented the outcome of a social experiment aimed to explore the relation between trust, popularity and influence in the dynamics of online social media. They showed that popularity in social networks does not require peculiar user features or actions, since an automated agent can acquire a surprisingly high popularity just by reiterating a simple activity of "social probing". In a second phase of the experiment the researchers sent friendship suggestions from their bot to a pool of users, providing random suggestions to some and thoughtful recommendations to others. As evidence that an untrustworthy user can be very influent if popular enough, the researchers found that people more aware of the presence of the bot have been more inclined to follow its suggestions. (Aiello, Deplano, Schifanella & Ruffo, 2014).

In the early days of online social media, over one decade ago, creating a bot was not a simple task: a skilled programmer would need to sift through various platforms' documentation to create a software capable of automatically interfacing with the platform and operate functions in a human-like manner. However these days, the landscape has completely changed: indeed, it has become increasingly simpler to deploy social bots, so that, in some cases, no coding skills are required to setup accounts that perform simple automated activities: tech blogs often post tutorials and ready-to-go tools for this purposes. Various source codes for sophisticated social media bots can be found online as well, ready to be customized and optimized by the more technically-savvy users. Finally, a very recent trend is that of providing Bot-As-A-Service (BaaS): companies like RoboLike1 provide "Easy-to-use Instagram/Twitter auto bots" performing certain automatic activities for a monthly price. Advanced conversational bots powered by sophisticated Artificial Intelligence are provided by companies like ChatBots.io that allow anyone to "Add a bot to services like Twitter, Hubot, Facebook, Skype, Twilio, and more" (Ferrara, 2017).

Mønsted et al. created a botnet with a large number of followers with a network structure. They began by ensuring that the bots would appear to be human-like if subjected to a cursory inspection. They achieved this goal by having the bots generate content using simple natural language processing rules as well as ‘recycling’ popular content from other Twitter users. They also had the bots tweet at irregular intervals, but with frequencies set according to a circadian pattern. Finally, the researchers used some Twitter users’ tendency to reciprocate friendships to ensure that the bots were followed by a large number of accounts while themselves following only a few; a following/follower ratio much smaller than one is unusual in typical twitter bots. The full botnet consisted of 39 algorithmically driven Twitter accounts (Mønsted, Sapieżyński, Ferrara, & Lehmann, 2017).

Alperin et al. presented a new methodology---the Twitter bot survey---that bridges the gap between social media research and web surveys. The methodology uses the Twitter APIs to identify a target population and then uses the API to deliver a question in the form of a regular Tweet. The approach of embedding the survey into the social media environment facilitates the enrichment of user responses information about their social media behavior, obtained from the particular platform. This approach thus allows us to gain all of the advantages of social media research and to complement it with the 3 of 4 user details that can only be gleaned from a survey. By linking all of the data from the user accounts with user responses, this method provides a better and more complete understanding of the users behind the social media accounts. In the case of Twitter, we can map their tweeting behavior and tweet contents with their responses to questions about their motivations, affiliations, personality, opinions, etc. (Alperin, Hanson, Shores & Haustein, 2017).

Besides Twitter bots, let's us look at an example of a Wikipedia bot to compare how they work similarly or differently from a Twitter bot. Bots on Wikipedia are computer scripts that automatically handle repetitive and mundane tasks to develop, improve, and maintain the encyclopedia. They are easy to identify because they operate from dedicated user accounts that have been flagged and officially approved. Approval requires that the bot follows Wikipedia's bot policy. Although in quantitatively different ways, bots on Wikipedia behave and interact as unpredictably and as inefficiently as the humans. The disagreements likely arise from the bottom-up organization of the community, whereby human editors individually create and run bots, without a formal mechanism for coordination with other bot owners. Tsvetkova et al. found that most of the disagreement occurs between bots that specialize in creating and modifying links between different language editions of the encyclopedia. The lack of coordination may be due to different language editions having slightly different naming rules and conventions (Tsvetkova, García-Gavilanes, Floridi & Yasseri, 2017).

Server-side socialbot detection approaches can identify malicious accounts and spams in online social networks. However, they cannot detect socialbot processes, residing on user hosts, which control these accounts. Therefore, new approaches are needed to detect socialbots on hosts. The fundamental to design host-side detecting approaches is to gain an insight into the behaviors of socialbots on host. He et al. analyzed a series of representative socialbots in depth and summarized the typical features of socialbot behaviors. They provided several behavior features of socialbots on hosts, including network flow through which socialbots communicate with botmasters through the online social network, system calls via which socialbots conduct an activity, and process information of socialbots running on hosts. These features can be used by someone to design approaches to identifying socialbots on a host. The researchers' proposed detection approach can effectively distinguish between a socialbot and a benign application on end hosts (He, Li, Cao, Ji & Guo, 2017).

Another type of common social bots is called news bot. So-called "robot" journalism represents a shift towards the automation of journalistic tasks related to news reporting, writing, curation, and even data analysis. Lokot et al. studied the use of "news bots"-automated accounts that participate in news and information dissemination on social networks. Such bots present an intriguing development opportunity for news organizations and journalists. In particular, the researchers analyzed a sample of existing news bot accounts on Twitter to understand how news bots are currently being used and to examine how using automation and algorithms may change the modern media environment. Based on their analysis, they proposed a typology of news bots in the form of a design and editorial decision space that can guide designers in defining the intent, utility, and functionality of future bots. The proposed design space highlights the limits of news bots (e.g., automated commentary and opinion, algorithmic transparency and accountability) and areas where news bots may enable innovation, such as niche and local news (Lokot & Diakopoulos, 2016).

Finally, another way that social bots can operate fraudulently is by phishing. Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication (van der Merwe, Loock & Dabrowski, 2005). Shafahi et al. investigated how social bots can phish employees of organizations, and thus endanger corporate network security. Current literature mostly focuses on traditional phishing methods (through e-mail, phone calls, and USB sticks). However, Shafahi et al. took it one step further by addressing the serious organizational threats and security risks caused by phishing through online social media, specifically through Twitter. In their experimental development, the researchers created and deployed eight social bots on Twitter, each associated with one specific subject. For a period of four weeks, each bot published tweets about its subject and followed people with similar interests. In the final two weeks, their experiment showed that 437 unique users could have been phished, 33 of which visited their website through the network of an organization. The phisher now has a direct link to the organization's network, allowing him to spread malware and/or gather sensitive information. The risks are mitigated when the organization's cyber security infrastructure is up-to-date, but even in this scenario, zero-day attacks might be used to infiltrate the company (Shafahi, Kempers & Afsarmanesh, 2016).

Standard for Social Bot Use and Narrative Summary

Political actors are using algorithms and automation to sway public opinion, notably through the use of "bot" accounts on social networking sites. Marechal considered the responsibility of social networking sites and other platforms to respect human rights, such as freedom of expression and privacy. It then proposed a set of standards for chatbots operating on these platforms, building on the existing policies of leading social networking platforms and on the indicators laid out by Ranking Digital Rights. A good normative framework for the use of bots on social networking sites should have three components: bots should clearly be labeled as such, they should not contact other users without consent, and information collected by them should only be used for disclosed purposes (Marechal, 2016).

Based on the literature review above, we now understand that social bots can bring us a lot of convenience in social media, however the negative impacts that it bring can outweigh its positive impact, especially in politics. That's why we need to develop more advanced algorithm for us to detect social bots before it deceive even more social media users. But are Twitter users that easily deceived by social bots? Since we have understood that social bots nowadays are very easy to generate, you do not need advanced programming skills to be able to make social bots. So instead of relying on developers of social bots to always abide by the good normative framework that was addressed above, how about we educate more Twitter users to become more aware of the existence of social bots and adopt some good strategies to better protect themselves against harmful Twitter bots? In my opinion, that is a more effective approach when fighting against the harmful social bots. Therefore, in this paper, I want to investigate about the level of awareness among Twitter users about the social bots, what are the users' sentiments towards social bots and the ways that Twitter users protect themselves against harmful social bots. To achieve this objective, I decided to use online survey methodology to survey Twitter users about this topic. If my participants did not already know that they were interacting with social bots, I would like to educate them about the existence of social bots in social media and give them some helpful tips about how to protect themselves against harmful social bots, by giving them some idea about this in the checkboxes. The details of my survey methodology are included in the next section below.

Methods

This section of the paper describes the method which was used in the proposed research. It first identifies and describes the survey questionnaire method, including a discussion of why this method is particularly appropriate for this research. It then explains the sampling method and the rationale behind it. It describes the data collection procedures for the study and the sampling method being chosen. The final part of this section is the result of the survey together with the visualization of the result so that it can be easily interpreted by the readers of this paper.

Survey Questionnaire

A survey questionnaire was the primary method of data collection for this research. A survey is a set of items, formulated as statements or questions, used to generate a response to each stated item (Wildemuth, 2009, p. 257). Surveys use rating scales and open-ended questions to collect facts and measure beliefs, opinions, and attitudes; they are typically self-report instruments. They can be used to assess cognitive, affective, and physical functioning (Colton & Covert, 2007). A survey is appropriate for this research for many reasons. It enables the researcher to obtain information from a large number of people. It allows the researcher to explore relationships between variables, such as the relationship between a Twitter users' years of experience using Twitter and the ability of him or her in detecting social bots. It measures attitudes and beliefs, facilitating research into the Twitter users' perceptions of the social bots. Finally, it is easy to preserve anonymity and confidentiality with surveys (Colton & Covert, 2007). This is especially important when Twitter users might fear that if their answers to questions might be tracked back to their private activities in Twitter.

Intended Participants

The desired sample would be frequent users of Twitter.   For this study, "active" twitter users will be considered to be users who read or post on Twitter at least once a week. The survey was anonymous, to ease the mind of my participants about exposing their privacy. I recruited 26 participants primarily by distributing links through listserv to SILS students. The cover letter together with the link to the Qualtrics survey were sent to all SILS Master's students first. After that, I also asked Ms. Lara Bailey, the SILS Graduate Student Coordinator to forward my recruitment cover letter email to all SILS undergraduate and PhD students. I also shared the survey link on my Facebook page to invite my friends to fill it out. The reason to have two recruitment methods was to have a more diverse background, country and culture of the Twitter users that I recruited for the survey. Their population would mainly be college students, grad school students or working adults.

Designing the Survey Instrument

The survey contained 20 questions, and it took around 10-20 minutes to complete. All the questions were compulsory questions to answer except 3 questions: one which required the participant to upload a screenshot of a social bot, the second question was asking them to explain why they thought that screenshot was a social bot and the last question was asking them to provide concerns and questions if they had any after completing the survey.

First, I asked them about demographics information, including their age, gender, country and occupation. After the demographics questions, I asked a series of questions about their habit in using Twitter, such as their purpose of using Twitter, frequency of using Twitter in general and frequency of using Twitter for specific actions. I used an experimental approach in my survey to gauge my participation's prior interactions with Twitter bots, where I wanted my participants to upload a screenshot of what they think was a social bot in their Twitter interaction, although this question is optional. I was not sure if this was an infringement of their privacy or not since they might revealed their own identities through their Twitter screenshot, but luckily it ended out not be a problem at all because the users only showed the social bots in the screenshot and nothing about their personal identities in Twitter. I also asked them why they thought that screenshot was a social bot. The last part of my survey was to gauge their attitudes about social bots in general. I started this section by asking them by their sentiment towards social bots first, whether they thought that it would bring more benefits or more harms to Twitter users. Following that, I had one question asking them about the positive impacts of social bots after their interactions with Twitter bots and one question about the negative impacts of social bots. Finally I asked them about how do they identify fake Twitter accounts and how did they protect themselves from the harmful social bots. A last optional question was asking them about questions or concerns that they had after completing the survey. The complete survey questions are included in Appendix C of this paper.

The survey was set up in Qualtrics and was administered to any Twitter users online. The participants were informed about the purpose of the survey and my motivation for conducting this research through a cover letter that is included in Appendix A and Appendix B. The cover letter for email recruitment through SILS listserv were a little bit longer than the cover letter for Facebook recruitment because I also had to include my personal introduction and formal closing to the email cover letter. I tried to make my audience to get interested in participating in my survey by talking about the impact of my research in my cover letter to hopefully maximize survey response rate. After getting all the results for my survey, I used Excel and the statistical tools provided by Qualtrics for data analysis, since they were easier to use.

My sampling method would be convenience sample. Convenience sampling is a nonprobability sampling strategy where participants are selected based on their accessibility and/or proximity to the research (Bornstein et al, 2013). One of the most common examples of convenience sampling within SILS is the use of student volunteers as study participants. First, the survey will be distributed by listserv to SILS students. However, the drawback of convenience sampling is that all the participants would have similar ad-hoc demographics background, since they will have similar age and are all studying the same subjects in the same school in the United States. Convenience sampling also have the problem of typically include small numbers of underrepresented sociodemographic subgroups (e.g., ethnic minorities) resulting in insufficient power to detect subgroup differences within a sociodemographic factor or factors. Therefore, to diversify my convenience sample, I have decided to also draw samples from my Facebook friends, which had a wider range of age, gender, nationality and ethnicity. Personally, I do not use Twitter on a regular basis, and that is why I shared the survey link on my Facebook page. The survey result was collected online through Qualtrics. This method is easier, less time-consuming and the least expensive to implement.

Since this was an online survey, we could include skip logic into the design of the survey so not everyone will answer the same questions based on their previous response. However, I did not include this in my online survey because all participants should have the same set of questions to answer. The full survey questions can be found in the appendix.

Survey Administration

Before I started my survey administration, I had to obtain prior approval from my advisor, Dr. Bradley Hemminger and the campus IRB. Once I had obtained the approval from both of them, I started to send out my Qualtrics survey through SILS Masters Students Listserv. I have included my cover letter in the body of my email, followed by the link to the Qualtrics survey. This is the first wave of my survey distribution. My second wave of survey distribution was to ask SILS Graduate Student Services Coordinator, Lara Bailey, to send out my survey to the undergraduate and PhD students in SILS. When the survey responses was not very encouraging, I decided to start a third wave instead by utilizing the SILS Facebook group to reach out to even more SILS students. My third wave was to post the link and recruitment cover letter on the SILS Facebook group. Finally, my fourth wave was to post the same link and recruitment cover letter on my personal Facebook page. Informally, I also occasionally talked to my friend and casually ask them to fill out my online survey.

Ethics

To make sure that the participant remain anonymous in my research, I did not collect any personally identifying information from my participants. I also coded their answers and did not identify each answer to specific demographic information when writing my paper. When collecting Twitter screenshot from my subjects, and there was a possibility that they might include their Twitter handler or any other personal information in this screenshot. To protect my participants' privacy, I would blur out any part of their screen shot that might reveal the identities of my participants, before publishing the screenshot in the appendices of my master's paper. However, there is no personal Twitter handler information to be found in any of the 10 screenshots, so I did not have to do this step.

Results

1. Demographics

Since I could not keep track of the number of recruitment email that I have sent out (they are in Listserv), I was unable to accurately calculate the response rate of my online survey. We will look at each attribute of the demographics individually. Table 1 shows the distribution of the age group among our participants.

Age Group	**Number of Participants**	**Percentages**
21-25	15	47%
26-30	10	31%
31-35	6	19%
36-40	1	3%
Grand Total	**32**	**100%**

Table 1: Age group distribution among participants

The age range of the participants are from 21 years old to 40 years old. The mean age was 27 years old. The median age was 26 years old. The mode age were 24 and 26 years old. The distribution of the age range peaked across the age range of 21-25 year old. As the age range went up, the number of participants in that older age group subsequently went down. Similarly, the gender of the participants were not that uniformly distributed (Figure 1).

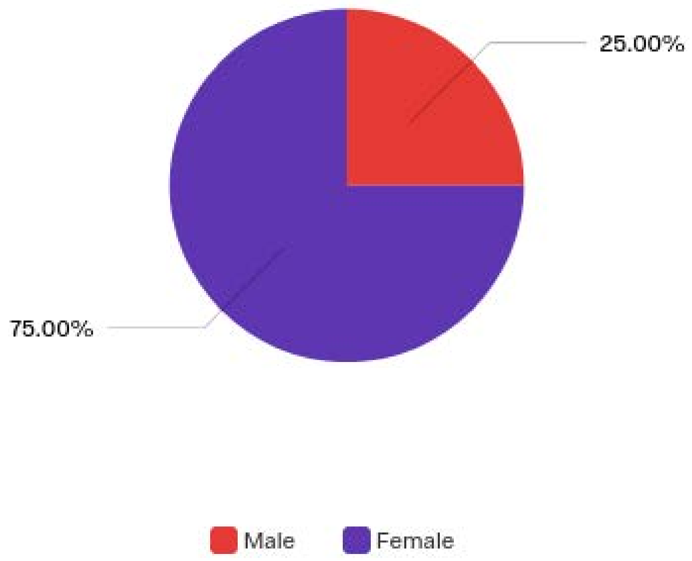


Figure 1: Gender distribution among participants

They were highly skewed towards the female, with 24 out of 32 (75%) of them female and 8 out of 32 (25%) of them being male (Figure 1). This was not a big surprise, given that the demographics of SILS students, which make up most of the participants, are highly skewed towards female. The next demographics question asked the participants about which country they were from. Table 2 shows the distribution of the country of our participants.

Country	**Number of Participants**	**Percentages**
USA	25	78%
Malaysia	4	13%
China	2	6%
Canada	1	3%
Grand Total	**32**	**100%**

Table 2: Distributions of the country of participants

Not surprisingly, we had the majority of the participants come from US (78%), followed by Malaysia (13%), China (6%) and Canada (3%). The next question asked the participants about their occupation. The majority of the participants are students (66%) (Table 3).

Occupation	**Number of Participants**	**Percentages**
Student	21	66%
Library Assistant	2	6%
Finance	2	6%
Project Manager	1	3%
Restaurant Manager	1	3%
Researcher	1	3%
Graphic Designer	1	3%
Optometrist	1	3%
Professor	1	3%
Postdoc	1	3%
Grand Total	**32**	**100%**

Table 3: Distributions of the Occupations of the participants

Therefore, we can conclude that out of the 32 people who completed the survey, their demographics were mostly biased towards young female students in their 20s. Therefore, the result of the rest of this survey questionnaires mostly reflect the viewpoint of this particular demographic group.

2. Twitter Usage

After the participants have completed the demographics questions, the second set of survey questions focus on the participants' habit in using Twitter. The first question asked about how often the participant used Twitter. Figure 2 shows the frequency of our participants' usage of Twitter:

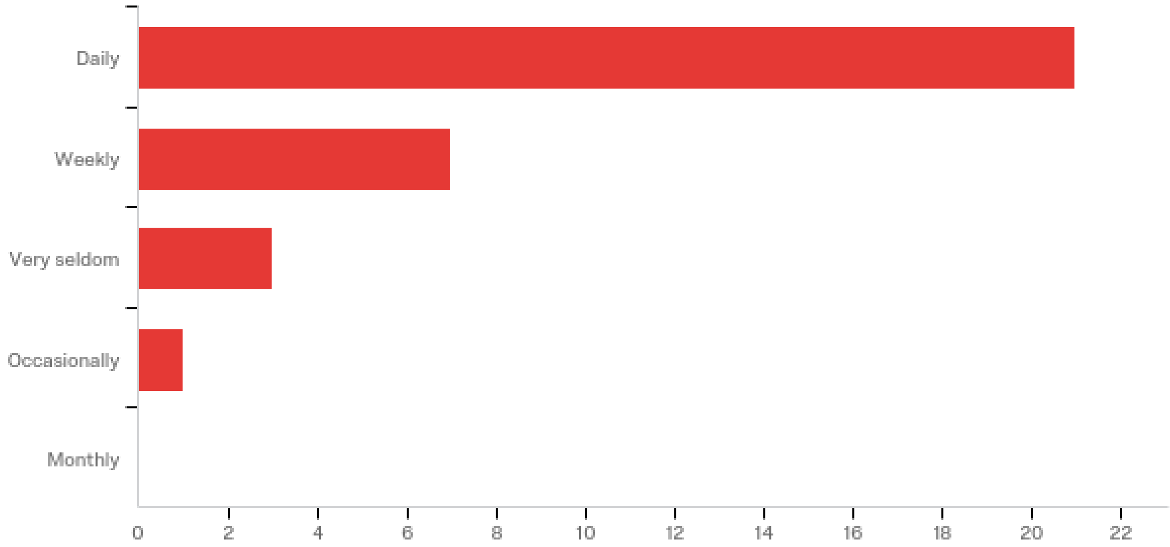


Figure 2: Frequency distribution of Twitter usage among participants

The majority of the participant used Twitter daily (63%), followed by weekly (21%), very seldom (12%) and only one who said occasionally (4%). There was no participant who use Twitter monthly, probably because I wrote in my cover letter that I required active Twitter users to participate in my survey. When asked about how long they have been using Twitter, most responded that they used Twitter between 1 to 5 years (63%), followed by 5 years or more (25%) and those who responded the shortest time were between one month and one year (12%) (Figure 3). Unlike when calculating the mean, mode and median for the age of the participants, the mean, median and mean for the duration of how long the participants have been using Twitter cannot be calculated accurately because we only had range data and did not have exact data to calculate these descriptive statistics. There was no Twitter user who have used Twitter for less than a month, which is probably too short of a time frame for them to be familiarized with the Twitter interface.

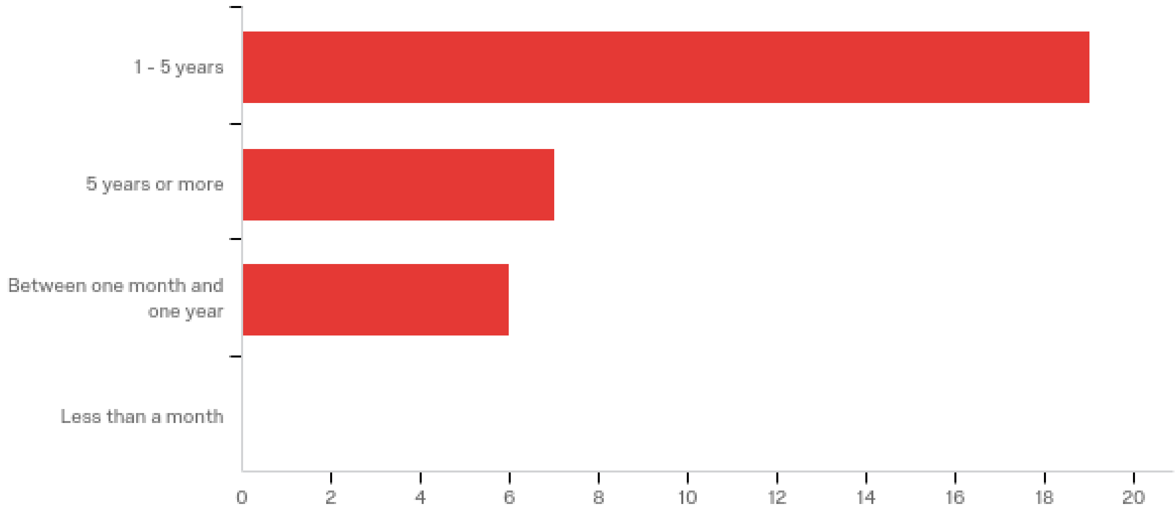


Figure 3: The duration of how long participants had been using Twitter

The next question asked about the purpose of them using Twitter. This was a checkbox question where the participant was able to check multiple boxes and also provide free flow text in the "Other" checkbox. The majority of the responses for this question was "To pass the time" (22%). Participants who answered "Other" gave answers such as "Keep up with art friends and exhibitions" and "For fun -- to see jokes etc". The rest of the responses along with their percentages breakdown can be found in Table 4 and Figure 4.

#	**Answer to "Why do you use Twitter?"**	**Count**	**%**
1	To pass the time	22	15.28%
2	To see what people are saying about live events that I am watching or interested in	20	13.89%
3	To be alerted to or find out more about breaking news	18	12.50%
4	To follow trending topics	17	11.81%
5	To keep up with the news in general	14	9.72%
6	To follow famous people	12	8.33%
7	To tell others what I am doing and thinking about	11	7.64%
8	To keep in touch with people I know	9	6.25%
9	To socially network	9	6.25%
10	To share news	7	4.86%
11	Other	5	3.47%
	Total	**144**	**100%**

Table 4: Answers to “Why do you use Twitter?” and percentages of response

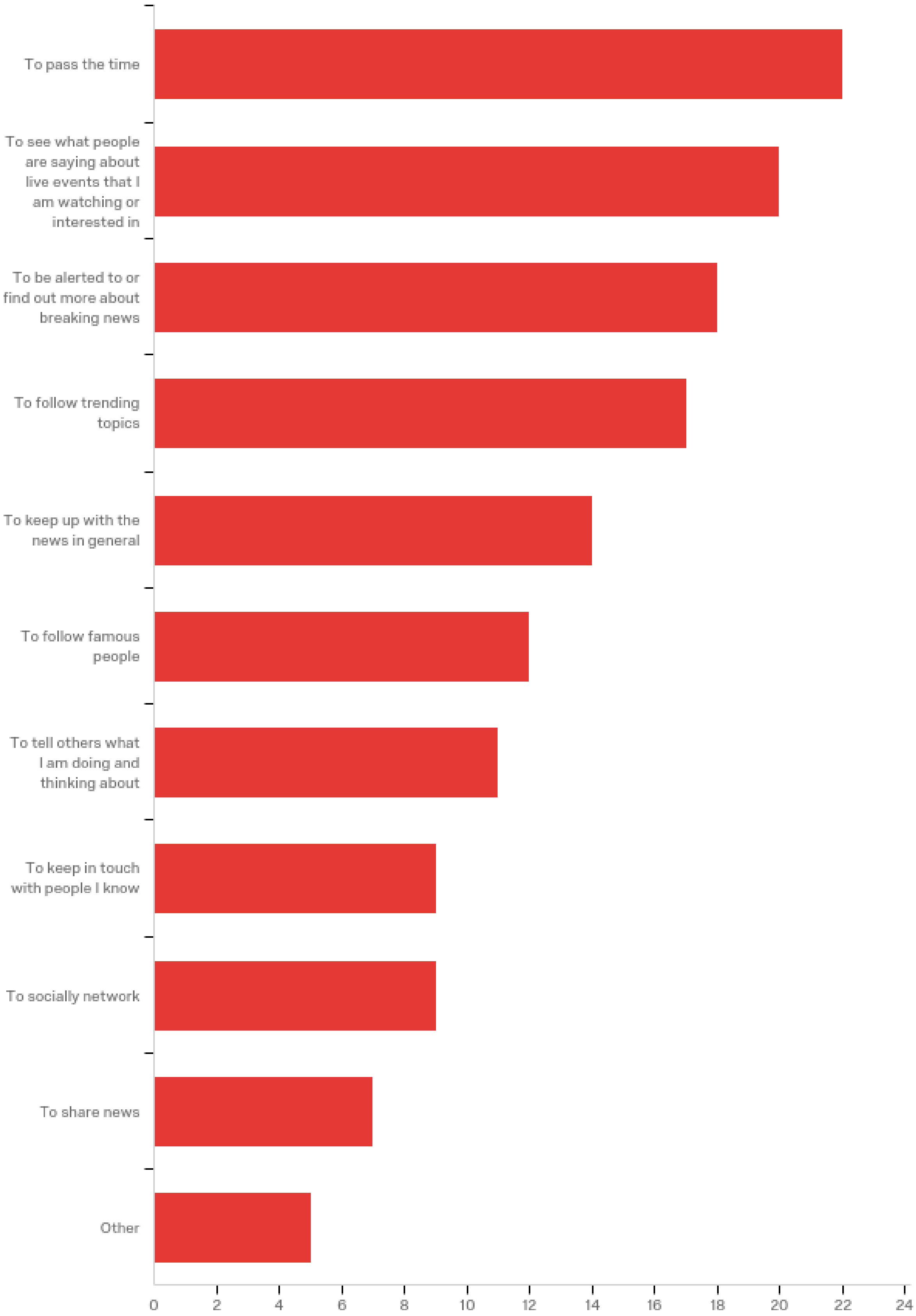

To pass the time
To see what people are saying about live events that I am watching or interested in
To be alerted to or find out more about breaking news
To follow trending topics
To keep up with the news in general
To follow famous people
To tell others what I am doing and thinking about
To keep in touch with people I know
To socially network
To share news
Other
0
2
4
6
8
10
12
14
16
18
20
22
24

Figure 4: The distribution of the reasons our participants used Twitter

The next question about Twitter usage was nested button table with Likert scale for the user to enter how frequently they did some of the specific activities on Twitter. Those activities were:

a) Post new tweets
b) Comment on tweets
c) Re-tweet
d) Follow other Twitter accounts
e) Post images
f) Like other tweets

The majority of the participant posted new tweets monthly (17%). Most of them also commented on tweets weekly (30%) and re-tweet weekly (30%). When it comes to following other Twitter accounts, most of them did it monthly (46%). Most of our participants seldom post images (50%). The majority of our participants liked other tweets daily (46%). When asked about who did they follow on Twitter,

Most of them follow their friends (19%). When the participants answered that they follow "Other" people on Twitter, they gave answers such as "News media", "Artists and scholars", "Companies/Brands", "People in my field", "Teachers", "Writers", "Journalists" and "Musicians".

The percentages breakdown of the other Twitter accounts that our participants follow are listed in Table 5 and Figure 5.

#	**Answer to "Who do you follow on Twitter?"**	**Count**	**%**
1	Friends	26	19.26%
2	Celebrities	22	16.30%
3	People who share similar interests	20	14.81%
4	Politicians	17	12.59%
5	Co-workers	15	11.11%
6	Family	12	8.89%
7	Other	12	8.89%
8	Sports athletes	11	8.15%
	Total	**135**	**100%**

Table 5: Percentage breakdown of Twitter accounts that the participants followed

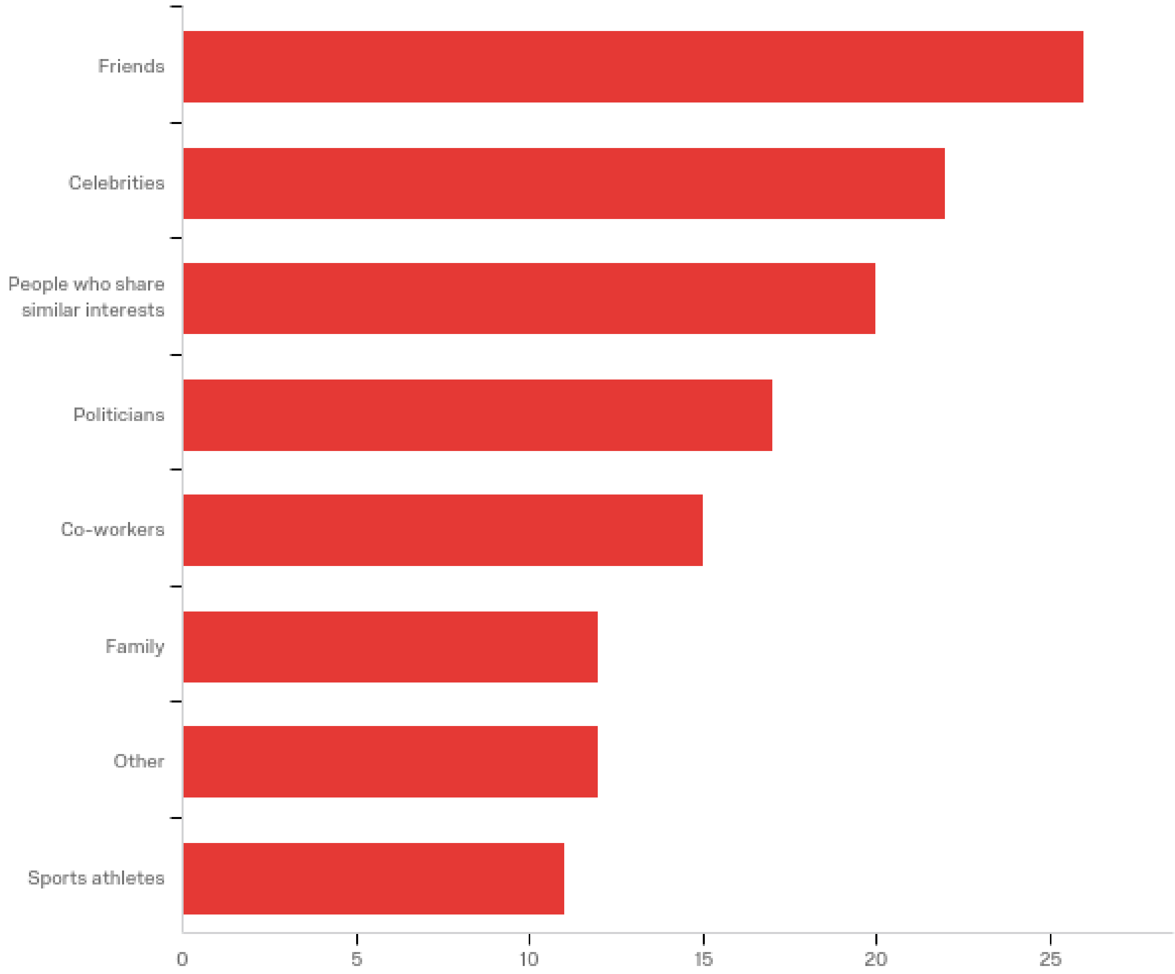


Figure 5: The distribution of Twitter accounts that our participants followed

On the other way around, when asked about who followed them on Twitter, most of them also answered “Friends” (31%). Participants who chose “Other” wrote answers such as “Artists and scholars”, “People in my field; also random people (though I block bots)” and a very special answer which is “Don't really know my followers”. The percentage breakdown of who follow our participants’ Twitter account can be found in Table 6 and Figure 6.

#	**Answer to "Who follow you in Twitter?"**	**Count**	**%**
1	Friends	28	30.77%
2	People who share similar interests	21	23.08%
3	Family	17	18.68%
4	Co-workers	16	17.58%
5	Other	5	5.49%
6	Celebrities	2	2.20%
7	Politicians	2	2.20%
8	Sports athletes	0	0.00%
	Total	**91**	**100%**

Table 6: Percentages breakdown of who followed our participants on Twitter

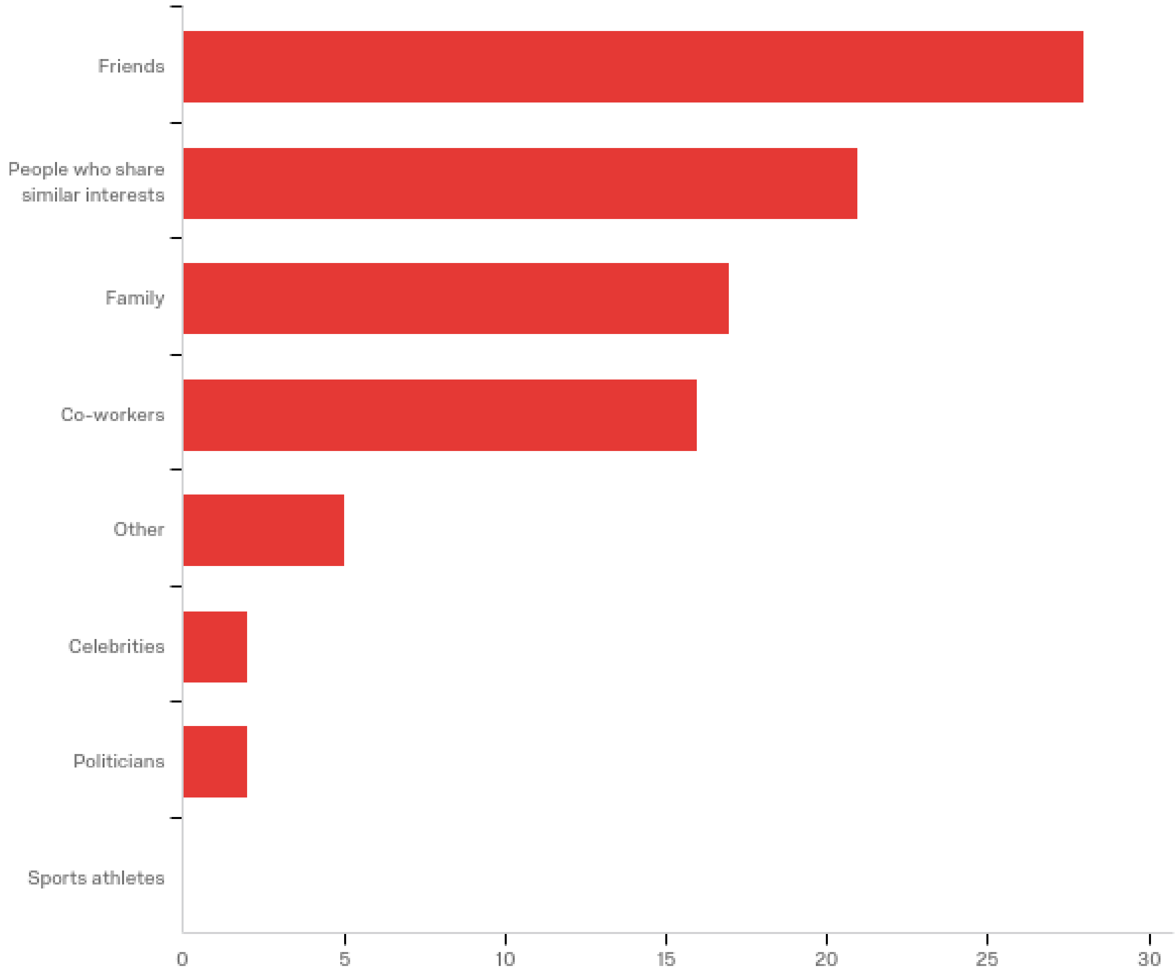


Figure 6: The distribution of Twitter accounts that followed our participants

3. Experience with Social Bots on Twitter

Now that we have already have a pretty decent understanding of how our participants use Twitter in general, I next asked the participants some questions related to their own experience with social bots on Twitter. However, since not every Twitter users were aware of what social bots are, I first asked a preliminary question to test and see how many of them were definitely aware of social bots and who were still unsure. Therefore, the first question here was "Have you seen any postings by social bot on

Twitter?" Most of them had an uncertain attitude about this question, with the majority of the participants answered "Possibly" (38%), followed by "Definitely yes" (23%), "Probably yes" (19%), "Probably not" (12%) and "Definitely not" (8%) (Figure 7).

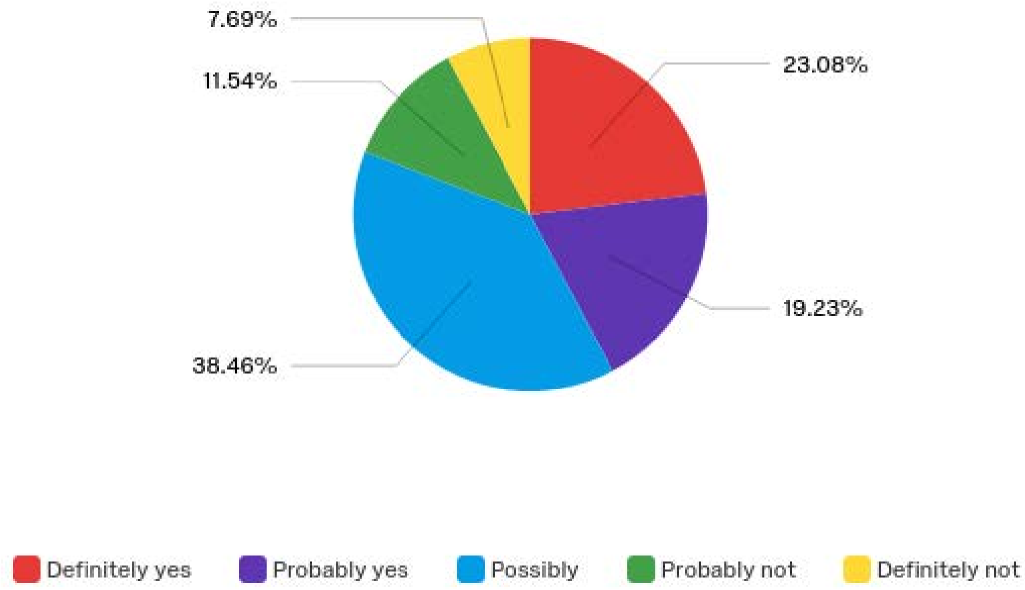


Figure 7: Breakdown of the prior experience of the participants having seen social bots on Twitter

Therefore, we can see that for participants who were more certain about their previous encounters with social bots, the majority of them knew that they have definitely seen it somewhere before.

After the warm up question, I asked them to show me proof of a real social bots that they have seen on Twitter. This is also a test question to see how skillful our participants were in detecting social bots on Twitter. However, I could not test every single participant because this was also an optional question where not every participant had to answer this question. It was not fair for me to ask someone who had never seen social bots before to come out with a screenshot of a social bot to complete this survey. Also, I did not want my participants to drop out from my survey halfway because they refused to spend extra time to actually login to their own Twitter account and do some homework to identify social bots in order to complete my survey questionnaire. In this question, I asked the participants to upload a screenshot of what they think might be an example of social bot on Twitter. For the answers for this question, I received 10 uploads, which was 31% response rate among the participants who have completed this survey. When I opened each of the 10 screenshots and looked at them, they were all coming from very different categories, ranging from @CBTS_Stream, @Angry American, @PoetryBot, @Tawasi, @Magic Realism Bot, @We Didn’t Start It, @Anti-Resistance Nate Dog, @FREEDOM NOW and @BBC News (World). Among the characteristics of the tweets common among most of the screenshots are they used many hashtags in their tweets, having the word “Bot” as its username, tweet with only a URL and nothing else, and fake news. All the 10 screenshots are included in the Appendix D from Figure 14 to Figure 23.

To follow up on the question that ask for a screenshot of social bots, I asked the participants to use their own opinion and words to explain why they thought the screenshot is a social bot. The complete answers to this question are listed in Appendix E. I have also highlighted some of the answers in Appendix E that I think were very insightful about ways that we can detect social bots. Some of main points that they shared from the highlighted comments are:

a) Lots of followers

b) Lots of hashtags

c) Using handle that a person would never choose

d) The tweet does not contribute to the ongoing conversation

e) Often retweet content

f) Text doesn’t read like a human wrote it

g) Call itself a bot

4. Perceptions towards social bots on Twitter and Protections against Harmful Twitter Bots

Now that the users had a better understanding of what a social bot was, I wanted to ask them about how were their perceptions of the impacts of social bots on them. But first, I wanted to do a little sentiment analysis to see how Twitter users generally perceive social bots. The first question in this section was “Do you think social bots are more helpful or more harmful?”. Without surprise, most of our participants replied that bots are “More harmful than helpful” (69%), followed by participants who think that bots are “Equally helpful and harmful” (23%). Only a small percentage of the participants answered that bots are “More helpful than harmful” (8%), which is still an interesting findings (Figure 8).

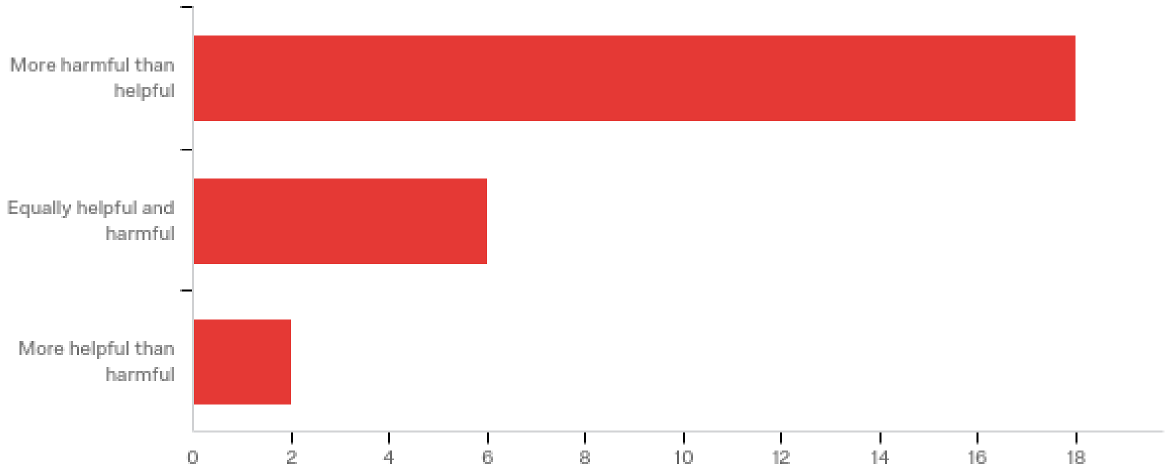


Figure 8: Perceptions of participants toward social bots

The next question made an attempt to dive deeper into the previous question. I started by asking a question from the positive side, by asking participants "What are some advantages of social bots to you on Twitter?". The majority of them responded that social bots bring "Entertainment" (26%) and "Self-promotion" (26%). There were also participants that replied "Other" and wrote "Comedy accounts where it is known that the account is a bot" and "occasionally bots exists to spread encouragement and joy". However, there are also three other participants who selected "Other" and in the free text box claimed that they see no advantage of social bots. All the other advantages are broken down in Table 7 and Figure 9.

#	**Answer to "What are some advantages of social bots to you on Twitter?"**	**Count**	**%**
1	Entertainment	9	25.71%
2	Self-promotion	9	25.71%
3	Automation	8	22.86%
4	Other	5	14.29%
6	Interactive	4	11.43%
5	Self-protection	0	0.00%
	Total	**35**	**100%**

Table 7: Advantages of social bots to participants on Twitter

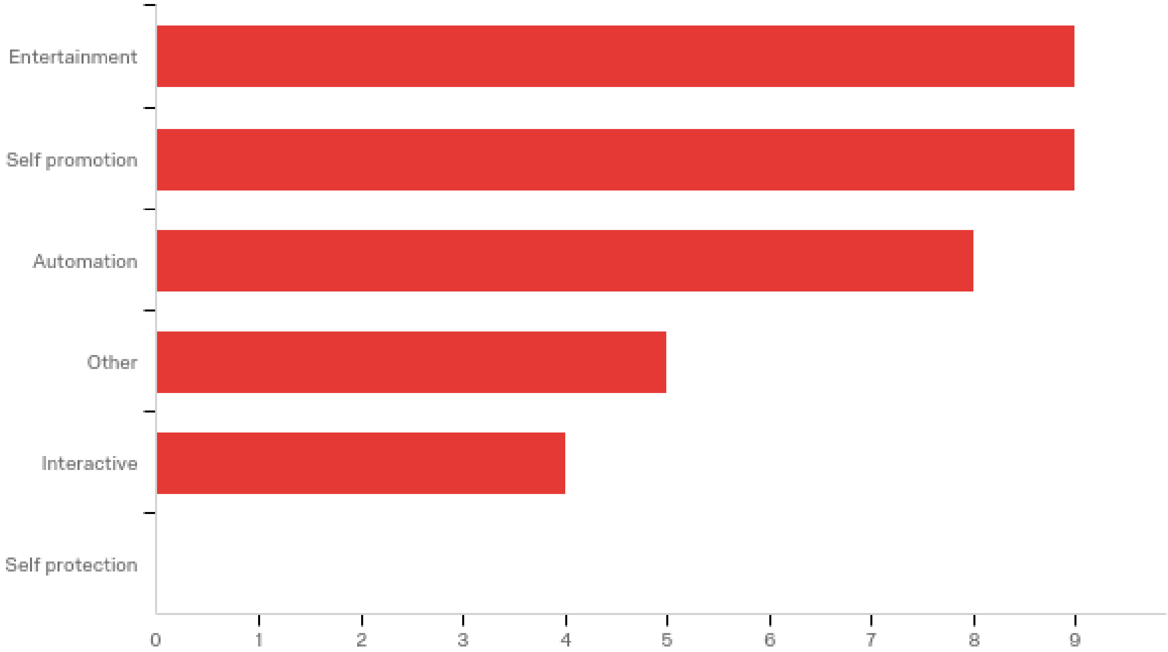


Figure 9: Advantages of social bots to participants on Twitter

This leads us to our next question, where the participants were asked about what were some disadvantages of social bots to them on Twitter. Compared to the previous question which only got 35 choice count, in this question the response rate increased tremendously to 116 choice count. The most popular choices for the disadvantages of social bots were “Spreading malicious contents” (17%), “Spreading fake news” (17%) and “Create the business of paying for Twitter followers” (13%). All the other disadvantages are summarized in Table 8 and Figure 10.

#	**Answer to "What are some disadvantages of social bots to you on Twitter?"**	**Count**	**%**
1	Spreading malicious contents	**20**	17.24%
2	Spreading fake news	20	17.24%
3	Create the business of paying for Twitter followers	15	12.93%
4	Promote hatred and hate speech	14	12.07%
5	Increase polarization	13	11.21%
6	Gaining unfair popularity	10	8.62%
7	Spreading influence	8	6.90%
8	Identity theft	8	6.90%
9	Privacy infringement	5	4.31%
10	Other	3	2.59%
	Total	**116**	**100%**

Table 8: Breakdown of “What are some disadvantages of social bots to you on Twitter?”

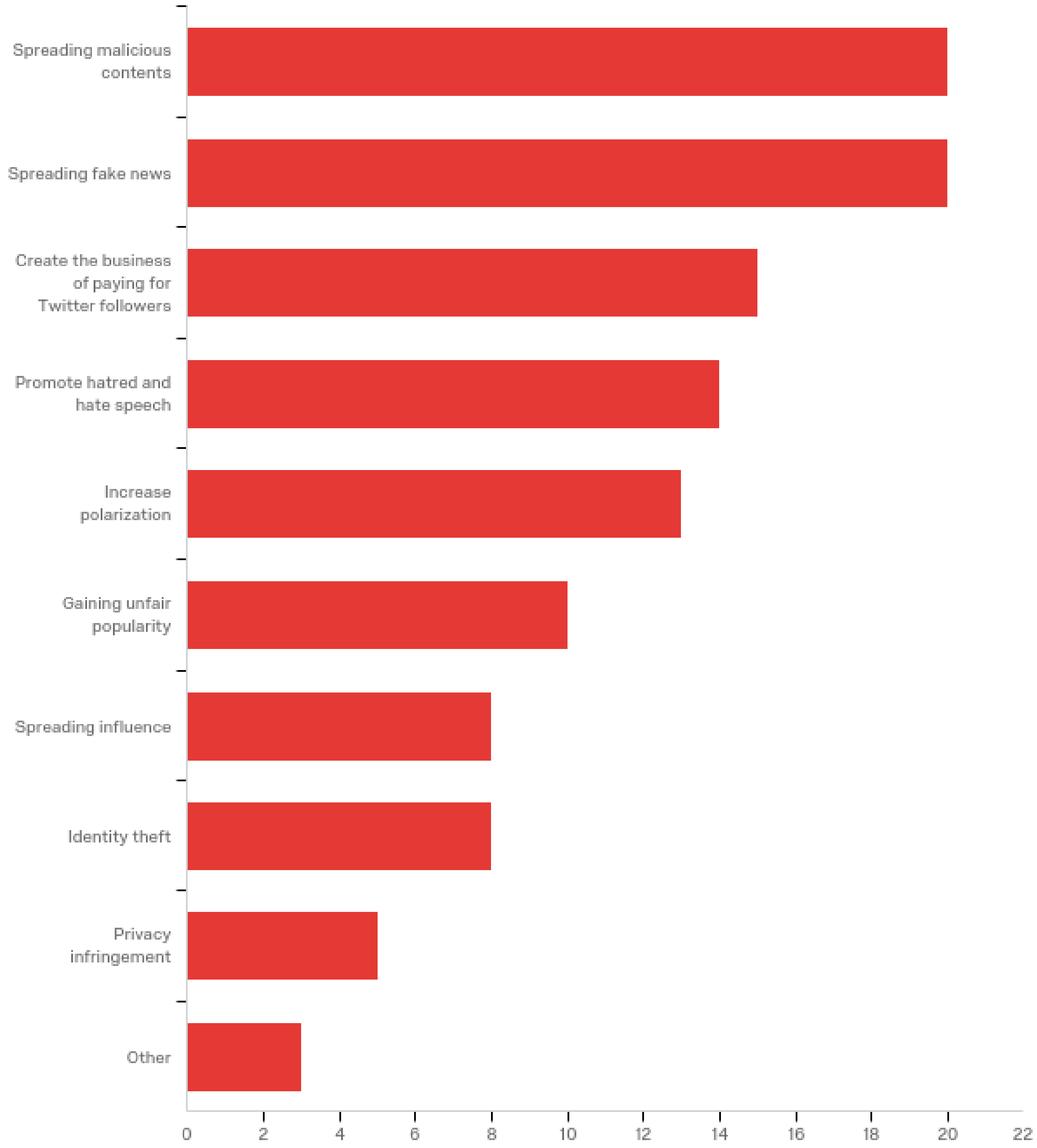


Figure 10: Disadvantages of social bots to participants on Twitter

Now that we have already identified that there are more disadvantages than advantages of social bots on Twitter, the next question would be aiming to educate survey participants about the various ways that we could protect ourselves against social bots. To do that, I asked the question “How do you identify fake Twitter accounts?” This question is very similar to the question right after the participants had attached their screenshot of a social bot on Twitter. These two questions differed only by the format of the question being asked: the previous one was a free flow text question, while this question is a multiple choice checkbox question. Another difference was the scope of the question being asked, whereas the previous question specifically asked the participants about why they perceived the tweet in the screenshot as being posted by a social bot, while this question was a more general way of asking the question. The reason I had the free flow question appeared before the multiple choice checkbox question was to really measure how much knowledge our participants had about social bots prior to reading all the answer choices presented in this question. The answer choices also served another important role: to educate the participants about some of the ways they could identify social bots using some techniques that they did not previously known. When analyzing the result, this question had a total of 106 choice count, meaning that on average, each participant had 3 ways to identify fake Twitter accounts. At the top of the results, we had a tie here: “Tweet large sequences that are often promotional and repetitive” and “Content of post sounds more machine generated than by a person” both occupied 16% of the total count. Table 9 and Figure 11 show the distribution of the answer choices:

#	**Answers to "How do you identify fake Twitter accounts?"**	**Choice Count**	**Percentage**
1	Tweet large sequences that are often promotional and repetitive	17	16%
2	Content of post sounds more machine generated than by a person	17	16%
3	Have a disproportionate follower and following count	13	12%
4	Username sounds fake	12	11%
5	Biography text is not properly written	11	10%
6	Very spectacular photos with attractive men or women	8	8%
7	The lack of a verified account blue checkmark	7	7%
8	Twitter Counter	4	4%
9	Inactive for a long time	4	4%
10	Detect them by using automated tools e.g. BotOrNot	4	4%
11	Twitter Audit etc.	4	4%
12	Tendency to be politically motivated, reply often to celebrity posts	1	1%
13	Tweets contain more links than messages	1	1%
14	No photo; or seem to have been created recently	1	1%
15	No personalization of the account (no banner photo, or generic profile photo)	1	1%
16	Other	1	1%
	Grand Total	**106**	**100%**

Table 9: Breakdown of “How do you identify fake Twitter accounts?”

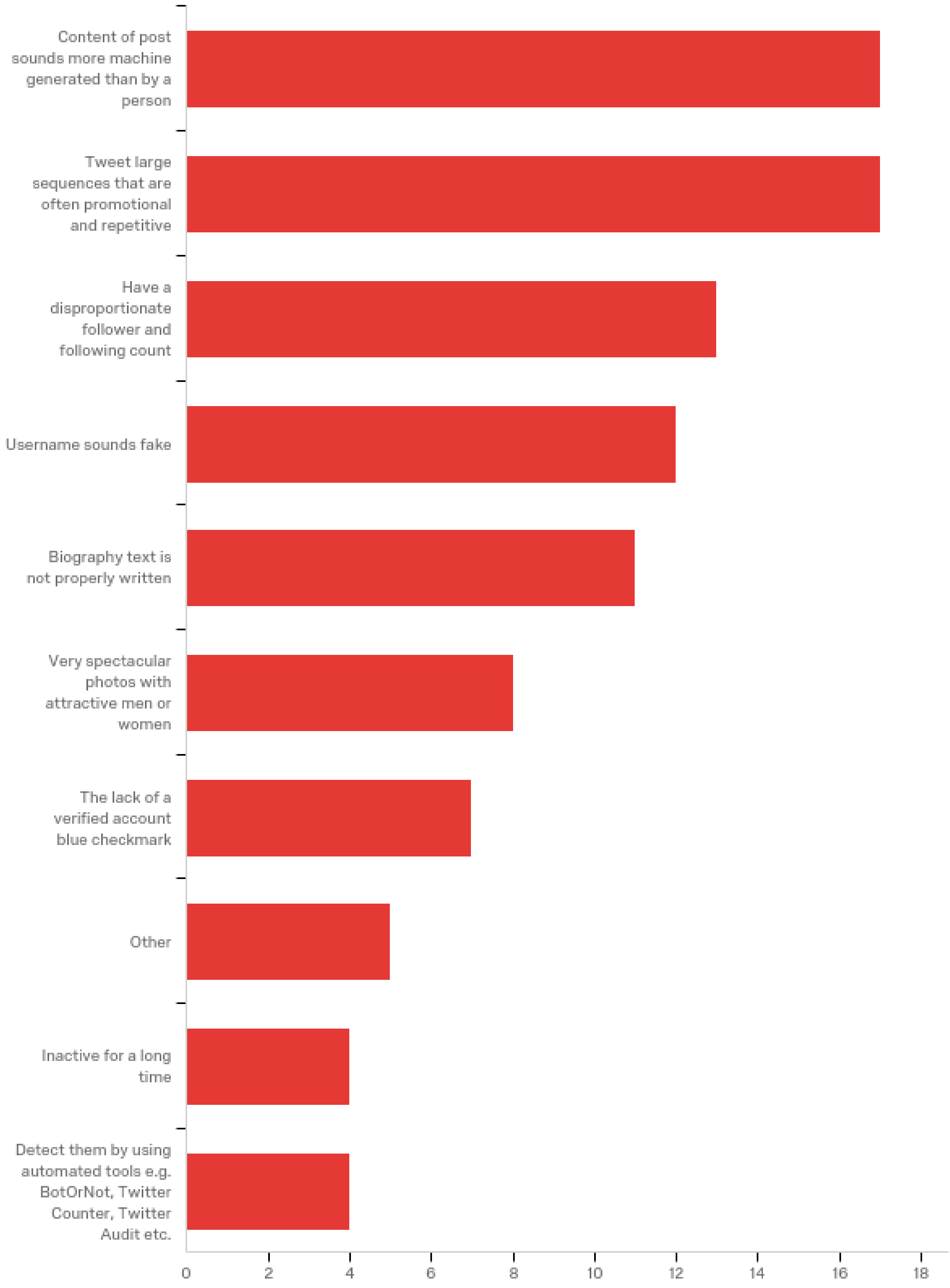

Content of post sounds more machine generated than by a person
Tweet large sequences that are often promotional and repetitive
Have a disproportionate follower and following count
Username sounds fake
Biography text is not properly written
Very spectacular photos with attractive men or women
The lack of a verified account blue checkmark
Other
Inactive for a long time
Detect them by using automated tools e.g. BotOrNot, Twitter Counter, Twitter Audit etc.
0
2
4
6
8
10
12
14
16
18

Figure 11: “How do you identify fake Twitter accounts?” answer distributions by participants

The next question was a very simple and direct question, yet it brought us a very important revelation regarding our users’ behavior when using Twitter. When asked “Do you protect yourself from harmful Twitter bots?”, only 10 out of 24 (42%) of our participants protect themselves against harmful Twitter bots, as opposed to the majority of them, 14 out of 24 (58%) of them taking no action at all to protect themselves against harmful social bots. This was an alarming discovery!

To dig deeper into what were the ways that our participants protected themselves against harmful social bots, I asked the next question “What action(s) do you do to protect yourself against harmful Twitter bots?”. Table 10 shows the breakdown of the answer choices:

#	**Answer for “What action(s) do you do to protect yourself against harmful Twitter bots?”**	**Count**	**%**
1	Block certain people from following me on Twitter	11	25.58%
2	None	10	23.26%
3	Reporting spam on Twitter	9	20.93%
4	Get rid of followers on Twitter	7	16.28%
5	Enable Twitter's "Protect my tweets" option	4	9.30%
6	Other	2	4.65%
	Total	**43**	**100%**

Table 10: Actions that the participants took to protect themselves against harmful Twitter bots

However, there are some inconsistencies in the answer to this question as opposed to the answer to the previous question. In the previous question, we had only 10 participants who took any actions to protect themselves against social bots, but in this question, we had 11 participants “block certain people from following me on Twitter”. I then looked at the individual survey responses and found one anomaly. One participant answered “No” for the previous question to indicate that she did not protect herself from harmful Twitter bots, but in this question, she chose “Block certain people from following me on Twitter” and “Reporting spam on Twitter” as the answers to this question of what actions she took to protect herself against harmful Twitter bots. The only explanation I can think of was that this participant blocked certain people from following her on Twitter and reporting spam on Twitter, but these actions were done because of other reasons other than protection against social bots. It could also be the she answered the previous “Yes/No” question in a hurry and made a mistake. Back to the data analysis as a whole, “Block certain people from following me on Twitter” (11 out of 43, or 26%) top the list among all actions that most participants protected themselves against harmful social bots. Participants who took no action at all came in at second place (10 out of 43, or 23%). For those that take action, the second most taken action was “Reporting spam on Twitter” (9 out of 43, or 21%) (Figure 12). One free text answer provided by the “Other” answer was “Ad blockers, only those I follow can follow me”.

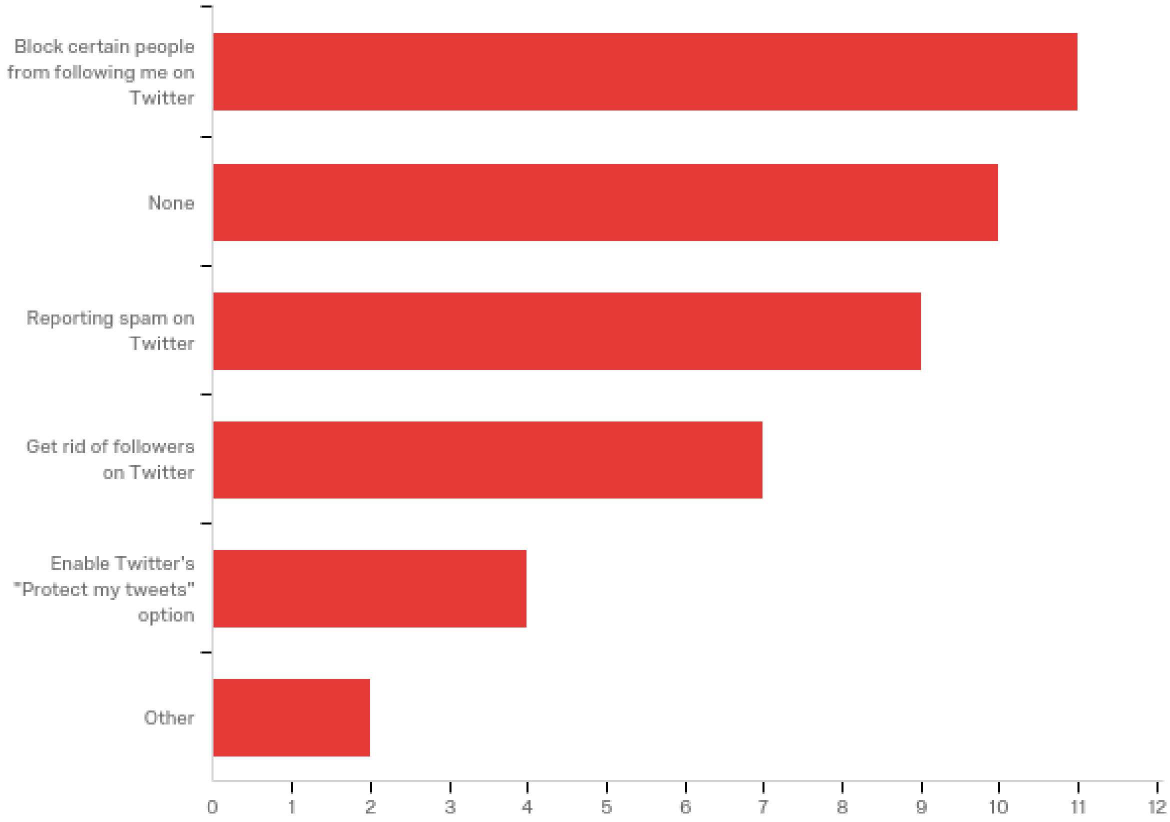


Figure 12: "What action(s) do you do to protect yourself against harmful Twitter bots?" answer distributions by participants

Finally, the last question on my survey was just for the participants to write down any comments or questions if they had any after finishing my survey. I had only 2 responses for this question. The first one was:

It was a little difficult for me to find a bot tweet on demand for an earlier question.

However, the second one was a much more insightful comment:

I check for bots regularly, but I don't know anyone else who does. I just don't want them in my twittersphere. You never know what they want and it's false through and through. I *wish more people were vigilant about them. I've considered starting to report them to Twitter rather than just blocking them from my stuff.*

From reading this comment, I wish more Twitter users can behave just like this participant, who was well aware of the detrimental impacts that Twitter bots can bring into Twittersphere and even took it one step further than blocking bots but also to report them to Twitter so that Twitter can take the appropriate action against these social bots.

The methods and procedures for data analysis

First, I performed quantitative data analysis on the survey result to use descriptive statistics on my subject population as a whole. I predicted that the age group to be skewed to the left instead of perfectly normal since Twitter users are usually young people instead of the older generation. I also did a descriptive statistics (mean, median, and mode) on the age of the participants and how long they have been using Twitter.

Then, I downloaded the Excel spreadsheet being generated by Qualtrics Data & Analysis tab to see the details of each participant's answers. However, looking for answers for 20 questions (20 columns) and 32 participants (32 rows) could be pretty tedious. I found it easier if I can aggregate the data so that readers can see the summarized data at a higher level. I tried to create pivot tables for each of the questions. But before that, I needed to clean up all the data before I can start to aggregate my data. For example, when I asked the participants to give me the country that they came from, I gave them a free flow text box to answer this question. Therefore, there would be many ways for the participants to spell USA, such as US, U.S., United States and U.S.A. Therefore, I need to clean and standardize the spelling of each version of the spelling of the same country before aggregating the data into a pivot table. The same case happened to the Occupation question.

Creating many pivot tables has become more of a hassle when I came down to the questions which allowed the participants to pick more than one answer. Qualtrics csv file will automatically concatenate the multiple answers selected by the same participant with comma. Thus, when I tried to separate each of the answer choices, I need to use Excel Data tab Text to Column function to delimit the cell into multiple columns separated by commas. This proves to be too much hassle if I continue to do my data analysis in Excel.

Therefore, I explored the Report tab in Qualtrics and discovered that this is a very powerful tab which provided me with visualizations of the answers for each question. By default, Qualtrics will generate a horizontal bar chart for the answers of each question with multiple choices. If I thought that a bar chart is not the most appropriate way to visualize the data in a question, I would edit the visualization to create something like a pie chart. From these visualizations, I could easily identify the top patterns and trends of my participants in answering various questions about social bots.

For the qualitative parts where the participant's provided free text answer, I coded their answers into 7 specific categories of their statement type when writing my paper. I also highlighted those 7 categories of answers which are insightful when analyzing the text included in Appendix E. Furthermore, I also analyzed the screenshot and coded what I can find from the screenshot and find the unifying theme across every screenshot that I got. Was there a particular Twitter account that is well known to be bot? Using grounded theory, I aggregated the common themes that I coded about how my participants encounter social bots to summarize the social bot phenomenon in this paper. I also measured the sentiment of my participants toward social bots, by analyzing the final questions about the positive and negative impacts of social bots for them.

There were some limitations of the study methods. Since this was more like an experimental approach than regular survey questions, I got my advisor’s feedback on how to handle or design this part, and how to present it to my participants to make sure that this method is effective in getting the results that I anticipate. In my literature review, I had not seen any researchers using this kind of research methods to study social bots before, so this could be the first time that a survey like this had been created to study social bot detection among real Twitter users and their sentiments towards bot.

Discussion

Demographics

As mentioned in the result section, the sampling of our survey participants were not diverse. Since I was using a convenience sampling method to get participants with the least amount of time and the least cost, those samples end to be highly skewed towards female students in the United States. Compared to the larger demographics of Twitter users out there, this sample was definitely not a realistic representation of the Twitter users' population. Since my sample were largely graduate students at SILS, this was a much more highly educated group of Twitter users, compared to the general public out there. However, according to Pew Research Center, younger Americans are more likely than older Americans to be on Twitter. Twitter is also somewhat more popular among the highly educated: 29% of internet users with college degrees use Twitter, compared with 20% of those with high school degrees or less (Greenwood, Perrin, Duggan, 2016). Therefore, the credibility of the sample sizes seemed to be increasing back.

Sample Size

This survey questionnaire also had another problem, which is the low number of sample size. As mentioned in the "Survey Administration" section, I have already realized this problem at the halfway of my sample period, I then took action to send follow up reminder via SILS Facebook Group to recruit even more participants to take my survey. This sample of 32 participants was the result of the four waves of my survey distributions. It would be too time consuming for me to individually message each of my friends to take the survey for me, thus I didn't do that at a large scale.

Besides low sample size, another problem with my sample size was that the sample size at the beginning of the survey was different from the sample size at the end of the survey. This survey had 32 participants in total. However, when we got to the question "Do you protect yourself from harmful Twitter bots?", our sample size dropped down to only 24 participants. I then tried to find out what happened to those 8 people in my sample size, and it turned out that those people drop out halfway during the survey and did not complete the survey. I then faced with a dilemma: Should I eliminate the survey responses of those 8 participants who only provided partial response to my survey? After discussing with my advisor, I decided to retain the number of the sample size to 32 participants in total, but made it clear in questions in the result section when the number of participants dropped to only 24 people. This is because I had a low sample size and thus any decrease in my sample size to my already meager sample size would be detrimental to the credibility of my research.

The primary goal of this study is to answer these questions that this paper is trying to solve at the beginning of this paper. So, we will now start to look at each research question one by one.

RQ1. By looking at existing research in this area, why do social bots appear in Twitter?

There are many reasons why social bots appear in Twitter. The first reason is popularity. Some celebrities and politicians are buying fake accounts on Twitter in order to look more popular. To boost the number of followers, they might also buy fake Twitter followers so that they appear much more popular even without the original organic Twitter followers. Having a high number of followers and retweets has become the currency of social media. It helps people get jobs and endorsements, and users are more likely to engage with content that looks more popular. The social media platform's algorithms use the numbers to determine whether to promote the message to more users. Bots like Twitter Money Bot is a really glorious software that applies these Twitter Marketing methods “automatically” so that a Twitter account can increase their twitter followers easily on Twitter

The second reason that people create social bots on Twitter is to make money. There are a number of different services out there for monetized short links. When people find your tweet, either because they follow you or because of the hashtags or search terms you use, they will want to click the link. When they click the link, they see your ads, and may click them. This gets you paid. The more people who do this, the more you earn. Therefore, a Twitter user need traffic and targeted visitors to promote their stuff (product as an affiliate, your own product, website, cpa offers etc.) on the internet. If there is no traffic, no one is going to be interested in their offer or service or product, people won’t even notice the Twitter account’s offer. And the social media, especially Twitter is a great traffic source for internet marketers. Twitter Bot will find and scrape targeted twitter users for any Twitter users, and it will follow them automatically, some of them are going to follow the user back and the user will gain new followers on an autopilot. So the Twitter user will be able to advertise their offer to new followers. This is the main idea of Twitter Marketing.

From the reason above, we know that Twitter bots occur to build up traffic to see the content that the marketers want to share. However, the traffic not necessarily mean that all bots are malicious; many organizational and institutional Twitter accounts, including Quartz's, are in effect bots automatically tweeting the latest published stories (Gorwa, 2017). Another example of useful bots are @CongressEdits and @parliamentedits, which post whenever someone makes edits to Wikipedia from the US Congress and UK Parliament IP addresses, respectively.

Twitter bots can also be a source of fun and entertainment for many Twitter users. For example, @DBZNappa replied with "WHAT!? NINE THOUSAND?" to anyone on Twitter that used the internet meme phrase "over 9000". @Maskchievous tweets a random meme with a random emoticon ("Twitter bot," n.d.). One participant even answered that "occasionally bots exists to spread encouragement and joy". Bots are doing a good job when they can spread some positive emotions to Twitter users.

Many non-malignant Twitter bots can also provide positive social impact. As technology and the creativity of bot-makers improves, so does the potential for Twitterbots that fill social needs. @tinycarebot is a Twitterbot that encourages followers to practice self-care, and brands are increasingly using automated Twitterbots to engage with customers in interactive ways. One anti-bullying organization has created

@TheNiceBot, which attempts to combat the prevalence of mean tweets by automatically tweeting kind messages.

RQ2. What are the ways that we detect social bots in Twitter?

In recent years, Twitter bots have become increasingly sophisticated, making their detection more difficult. The boundary between human-like and bot-like behavior is now fuzzier. For example, social bots can search the Web for information and media to fill their profiles, and post collected material at predetermined times, emulating the human temporal signature of content production and consumption—including circadian patterns of daily activity and temporal spikes of information generation ((Ferrara, Varol, Davis, Menczer & Flammini, 2016).

Instead of conducting a survey with just asking questions to the participants and expecting answers, I was also asking my participants to show whether they can successfully detect social bots or not by asking them to provide a screenshot of what they perceived to be a social bot. If my participants did not have a lot of knowledge about social bots, I hoped that my survey could raise their awareness about social bots in Twitter and better protect themselves against the negative impact of Twitter bots. Although the survey result showed that not every Twitter users have a very amount of knowledge detecting social bots as well as protecting themselves against social bots, I saw some very good suggestions among the techniques that the participants have used to detect the social bots that they attached with the survey. These are the features provided by my participants after attaching the social bots:

a) Lots of followers

b) Lots of hashtags

c) Using handle that a person would never choose

d) The tweet does not contribute to the ongoing conversation

e) Often retweet content

f) Text doesn't read like a human wrote it

g) Call itself a bot

In the literature review, we also saw many researchers in the academia have extracted many features from the social bots and use machine learning or mathematical logic to come out with ways to detect social bots, thus the way that my participants are using to detect the social bots are simplification of the ways that the researchers have been using to detect social bots, however the methods posted by the researchers are probably more robust and can detect way more social bots in a shorter time frame. In one of the literature, these are the more specific ways that we can detect social bots:

(i) bots generally retweet more often, while some humans can exhibit bot-like activity;

(ii) bots can post up to 5 times more URLs in their tweets;

(iii) bots can upload 10 times more content with their tweets;

(iv) humans can receive as much as 27 times more likes and 24 times more retweets as bots;

(v) bots retweeting other bots is over 3 times more regular than bots retweeting humans, whereas humans retweeting other humans is over 2 times greater, indicating homophily;

(vi) humans favorite others' tweets much more often than bots do, though newer bots are far more aggressive in favoriting tweets to replicate human behavior;

(vii) humans enjoy higher levels of friendship and usually form reciprocal relationships;

(viii) bots typically use many different sources for active participation on Twitter (up to 50 or more); and

(ix) activity sources include basic automation and scheduling services (Gilani, Wang, Crowcroft, Almeida & Farahbakhsh, 2016)

RQ3. What are the positive and negative impacts of social bots on social media users?

Social bots have long been associated with the negative impacts to society such as infiltrate political discourse, manipulate the stock market, steal personal information, and spread misinformation. Most of my literature review centered on the influence of social media in politics. Politicized social bots are used to massively boost politicians' follower levels on social media sites in attempts to generate false impressions of popularity. They are programmed to actively and automatically flood news streams with spam during political crises, elections, and conflicts in order to interrupt the efforts of activists and political dissidents who publicize and organize online. Computational propaganda deploys social or political bots to try to shape, steer and manipulate online public discussions and influence decisions (Duh, Rupnik & Korošak, 2017). This can be done to influence election results, as what happened in the 2016 presidential election, where material has been stolen from prominent Americans by Russian hackers that would reverberate through the presidential election campaign and into the Trump presidency. With Russia's experimentation on social bots with Twitter, the American company that essentially invented the tools of social media and, in this case, did not stop them from being turned into engines of deception and propaganda.

In terms of everyday Twitter users, they would usually associate bots with providing them with unwanted information, or more commonly known as spam. Twitter users are inundated with many advertisements, scam, and fake news so they are no longer able to distinguish between correct information and biased information on Twitter anymore. Marketers are actively searching for ways to increase their popularity on Twitter so that they can reach out to more people to be able to market their products to them.

But in a more dangerous way, social bots have the capability of stealing personal information in a method called phishing. Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication (van der Merwe, Loock & Dabrowski, 2005). When the Twitter users innocently entered the website through the network of an organization, the phishers can now spread malware and/or gather sensitive information. Therefore, the online security of a Twitter users are in great danger right now if they are being attacked.

In my survey questionnaire, I have asked my participants about the positive and negative impacts of social bots on them when using Twitter. Not surprisingly, most of them agreed that social bots bring more harm than benefits to them. My participants mostly agreed that Twitter bots spread malicious contents and spread fake news, consistent with the results from the literature review.

However, social bots are not all harm and bring no goods to the humanities. When used in the right way, Twitter bots can bring a lot of positive results such as spreading job and encouragement, preventing harassments in Twitter and helping to make previously repetitive actions now seem easier and more automated. For example, in the Geiger article, Blockbots can be used to counter harassment in Twitter, where subscribers to a blockbot will not receive any notifications or messages from accounts on the blocklist. In doing online search, search engines create bots to crawl websites, and return information on a site's content to help shape how those websites are prioritized in search results. Due to the creativity and ingenuity of many Twitter users, bots that are hilarious, witty, and fun have been created by all sorts of people. For example, @Nice_tips_bot shares life advice from Wikihow to brighten Twitter user's day.

RQ4. What are the general best practices for automatic detection of social bots in Twitter?

Social bots have become significantly more advanced today since its early day. They search social networks for popular and influential people, follow them and capture their attention by sending them messages. These bots can identify keywords and find content accordingly and some can even answer inquiries using natural language algorithms. Therefore, has detecting social bots become a much harder tasks nowadays? Looking at the result of our survey where our participants were able to distinguish social bots correctly, we can conclude that bot detection is a simple task for humans, whose ability to evaluate conversational nuances like sarcasm or persuasive language, or to observe emerging patterns and anomalies, is yet unparalleled by machines. Using data from Facebook and Renren (a popular Chinese online social network), Wang et al. tested the efficacy of humans, both expert annotators and workers hired online, at detecting social bot accounts simply from the information on their profiles. The authors observed that the detection rate for hired workers drops off over time, although it remains good enough to be used in a majority voting protocol: the same profile is shown to multiple workers and the opinion of the majority determines the final verdict. This strategy exhibits a near-zero false positive rate, a very desirable feature for a service provider (Wang, Mohanlal, Wilson, Wang, Metzger, Zheng, & Zhao, 2012).

However, the method above comes with its own drawback because detecting social bots through crowdsourcing is not feasible in the long run because it is not cost effective. Therefore, Emilio Ferrara and pals at Indiana University in Bloomington, said they have developed a way to spot sophisticated social bots and distinguish them from ordinary human users. The technique is relatively straightforward. The researchers created an algorithm called Bot or Not? to mine the social bots data looking for significant differences between the properties of human users and social bots. The algorithm looked at over 1,000 features associated with these accounts, such as the number of tweets and retweets each user posted, the number of replies, mentions and retweets each received, the username length, and even the age of the account. It turns out that there are significant differences between human accounts and bot accounts. Bots tend to retweet far more often than humans and they also have longer usernames and younger accounts. By contrast, humans receive more replies, mentions, and retweets. Together these factors create a kind of fingerprint that can be used to detect bots. "*Bot or Not?"* achieves very promising detection accuracy (Ferrara, Varol, Davis, Menczer, & Flammini, 2016).

Conclusion

Bot behaviors are already quite sophisticated: they can build realistic social networks and produce credible content with human-like temporal patterns. As the researchers build better detection systems for social bots, we as regular Twitter users need to educate ourselves of the characteristics of social bots and develop more effective strategy for mitigating the spread of online misinformation spread by social bot. Although the results of the survey shows that social bots bring both benefits and harms to Twitter users, it is undeniable that the cost of its harm far outweigh the benefits of its pro. There need to be better way for Twitter users to be aware of this and take it one step further by protecting themselves and educating others about the impact of social bots in society. Each Twitter user should be taking a more active approach in blocking Twitter bots and reporting spams to Twitter so that Twitter is able to get rid of the undesirable social bots that could make the twittersphere unsafe for us all.

References

Clark, E. M., Williams, J. R., Jones, C. A., Galbraith, R. A., Danforth, C. M., & Dodds, P. S. (2016). Sifting robotic from organic text: a natural language approach for detecting automation on Twitter. *Journal of Computational Science*, *16*, 1-7.

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. Communications of the ACM, 59(7), 96-104.

Bessi, A., & Ferrara, E. (2016). Social bots distort the 2016 US Presidential election online discussion.

Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2010, December). Who is tweeting on Twitter: human, bot, or cyborg?. In *Proceedings of the 26th annual computer security applications conference* (pp. 21-30). ACM.

Edwards, C., Edwards, A., Spence, P. R., & Shelton, A. K. (2014). Is that a bot running the social media feed? Testing the differences in perceptions of communication quality for a human agent and a bot agent on Twitter. Computers in Human Behavior, 33, 372-376.

Alarifi, A., Alsaleh, M., & Al-Salman, A. (2016). Twitter turing test: Identifying social machines. *Information Sciences*, *372*, 332-346.

Gilani, Z., Farahbakhsh, R., Tyson, G., Wang, L., & Crowcroft, J. (2017). Of Bots and Humans (on Twitter). In *Proceedings of the 9th IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM'17). https://doi. org/10.1145/3110025.3110090.*

Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2015). Fame for sale: efficient detection of fake Twitter followers. *Decision Support Systems*, *80*, 56-71.

Larsson, A. O., & Hallvard, M. (2015). Bots or journalists? news sharing on twitter.*Communications, 40*(3), 361-370. doi:10.1515/commun-2015-0014

Ratkiewicz, J., Conover, M., Meiss, M. R., Gonçalves, B., Flammini, A., & Menczer, F. (2011). Detecting and Tracking Political Abuse in Social Media. ICWSM, 11, 297-304.

Tyagi, A. K., & Aghila, G. (2012, July). Detection of fast flux network based social bot using analysis based techniques. In Data Science & Engineering (ICDSE), 2012 International Conference on (pp. 23-26). IEEE.
Ji, Y., He, Y., Jiang, X., Cao, J., & Li, Q. (2016). Combating the evasion mechanisms of social bots. Computers & Security, 58, 230-249. doi:10.1016/j.cose.2016.01.007

Drevs, Y., & Svodtsev, A. (2016). Formalization of criteria for social bots detection systems.*Procedia - Social and Behavioral Sciences, 236*, 9-13. doi:10.1016/j.sbspro.2016.12.003

Kaya, M., Conley, S., & Varol, A. (2016, April). Visualization of the social bot's fingerprints. In *Digital Forensic and Security (ISDFS), 2016 4th International Symposium on* (pp. 161-166). IEEE.

Subrahmanian, V. S., Azaria, A., Durst, S., Kagan, V., Galstyan, A., Lerman, K., ... & Menczer, F. (2016). The DARPA Twitter bot challenge. *Computer*, *49*(6), 38-46.

Oentaryo, R. J., Murdopo, A., Prasetyo, P. K., & Lim, E. (2016). On profiling bots in social media. Paper presented at the *, 10046* 92-109. doi:10.1007/978-3-319-47880-7_6

Gilani, Z., Wang, L., Crowcroft, J., Almeida, M., & Farahbakhsh, R. (2016, April). Stweeler: A framework for twitter bot analysis. In *Proceedings of the 25th International Conference Companion on World Wide Web* (pp. 37-38). International World Wide Web Conferences Steering Committee.

Woolley, S. C. (2016). Automating power: Social bot interference in global politics. *First Monday*, *21*(4).

Shao, C., Ciampaglia, G. L., Varol, O., Flammini, A., & Menczer, F. (2017). The spread of fake news by social bots.

Ferrara, E. (2017). Disinformation and social bot operations in the run up to the 2017 french presidential election.

Murthy, D., Powell, A. B., Tinati, R., Anstead, N., Carr, L., Halford, S. J., & Weal, M. (2016). Automation, algorithms, and politics| bots and political influence: a sociotechnical investigation of social network capital. *International Journal of Communication*, *10*, 20.

Duh, A., Rupnik, M. S., & Korošak, D. (2017). Collective behaviour of social bots is encoded in their temporal twitter activity.

Suárez-Serrato, P., Roberts, M. E., Davis, C., & Menczer, F. (2016). On the influence of social bots in online protests: Preliminary findings of a mexican case study. Paper presented at the *, 10047* 269-278. doi:10.1007/978-3-319-47874-6_19

Ford, H., Dubois, E., & Puschmann, C. (2016). Keeping ottawa honest-one tweet at a time? politicians, journalists, wikipedians, and their twitter bots. *International Journal of Communication, 10*, 4891-4914.

Munger, K. (2017). Tweetment effects on the tweeted: Experimentally reducing racist harassment. *Political Behavior*, *39*(3), 629-649.

Geiger, R. S. (2016). Bot-based collective blocklists in twitter: The counterpublic moderation of harassment in a networked public space. *Information, Communication & Society, 19*(6), 787-803. doi:10.1080/1369118X.2016.1153700

Haustein, S., Bowman, T., Holmberg, K., Tsou, A., Sugimoto, C., & Lariviere, V. (2016). Tweets as impact indicators: Examining the implications of automated "bot" accounts on twitter. *Journal of the Association for Information Science and Technology, 67*(1), 232-238. doi:10.1002/asi.23456

Paavola, J., Helo, T., Sartonen, H. J. M., & Huhtinen, A. M. (2016, June). The Automated Detection of Trolling Bots and Cyborgs and the Analysis of Their Impact in the Social Media. In ECCWS2016-Proceedings fo the 15th European Conference on Cyber Warfare and Security (p. 237). Academic Conferences and publishing limited.

Cha, M., Haddadi, H., Benevenuto, F., & Gummadi, P. K. (2010). Measuring user influence in twitter: The million follower fallacy. *Icwsm*, *10*(10-17), 30.

Messias, J., Schmidt, L., Oliveira, R., & Benevenuto, F. (2013). You followed my bot! Transforming robots into influential users in Twitter. *First Monday*, *18*(7)..

Wald, R., Khoshgoftaar, T. M., Napolitano, A., & Sumner, C. (2013, August). Predicting susceptibility to social bots on twitter. In *Information Reuse and Integration (IRI), 2013 IEEE 14th International Conference on* (pp. 6-13). IEEE.

Wagner, C., Mitter, S., Körner, C., & Strohmaier, M. (2012). When social bots attack: Modeling susceptibility of users in online social networks. *Making Sense of Microposts (# MSM2012)*, *2*(4), 1951-1959.

de Lima Salge, C. A., & Berente, N. (2017). Is that social bot behaving unethically?. *Communications of the ACM*, *60*(9), 29-31.

He, Y., Zhang, G., Wu, J., & Li, Q. (2016). Understanding a prospective approach to designing malicious social bots. *Security and Communication Networks*, *9*(13), 2157-2172.

Adams, T. (2017). AI-powered social bots.

Wilkie, A., Michael, M., & Plummer-Fernandez, M. (2015). Speculative method and twitter: Bots, energy and three conceptual characters. *The Sociological Review, 63*(1), 79-101. doi:10.1111/1467-954X.12168

Guilbeault, D. (2016). Growing bot security: An ecological view of bot agency. *International Journal of Communication, 10*, 5003-5021.

Grimme, C., Preuss, M., Adam, L., & Trautmann, H. (2017). Social Bots: Human-Like by Means of Human Control?. *arXiv preprint arXiv:1706.07624*.

Aiello, L. M., Deplano, M., Schifanella, R., & Ruffo, G. (2014). People are strange when you're a stranger: Impact and influence of bots on social networks.

Ferrara, E. (2017). Measuring social spam and the effect of bots on information diffusion in social media.
Mønsted, B., Sapieżyński, P., Ferrara, E., & Lehmann, S. (2017). Evidence of complex contagion of information in social media: An experiment using twitter bots.

Alperin, J. P., Hanson, E. W., Shores, K., & Haustein, S. (2017, July). Twitter bot surveys: A discrete choice experiment to increase response rates. In Proceedings of the 8th International Conference on Social Media & Society (p. 27). ACM.

Tsvetkova, M., García-Gavilanes, R., Floridi, L., & Yasseri, T. (2017). Even good bots fight: The case of Wikipedia. PloS one, 12(2), e0171774.

He, Y., Li, Q., Cao, J., Ji, Y., & Guo, D. (2017). Understanding socialbot behavior on end hosts. *International Journal of Distributed Sensor Networks*, *13*(2), 1550147717694170.

Lokot, T., & Diakopoulos, N. (2016). News bots: Automating news and information dissemination on twitter. *Digital Journalism, 4*(6), 682-699. doi:10.1080/21670811.2015.1081822

Shafahi, M., Kempers, L., & Afsarmanesh, H. (2016, December). Phishing through social bots on Twitter. In *Big Data (Big Data), 2016 IEEE International Conference on* (pp. 3703-3712). IEEE.

Marechal, N. (2016). When bots tweet: Toward a normative framework for bots on social networking sites. *International Journal of Communication, 10*, 5022-5031.

Wildemuth, B. M. (2009). Applications of social research methods to questions in information and library science. Westport, CT: Libraries Unlimited.

Colton, D., & Covert, R. W. (2007). Designing and constructing instruments for social research and evaluation. San Francisco, CA: Jossey-Bass Publishing

Bornstein, M. H., Jager, J., & Putnick, D. L. (2013). Sampling in developmental science: Situations, shortcomings, solutions, and standards. *Developmental Review*, *33*(4), 357-370.

Gorwa, R. (2017). Twitter has a serious bot problem, and Wikipedia might have the solution. Quartz. Retrieved from https://qz.com/1108092/twitter-has-a-serious-bot-problem-and-wikipedia-might-have-the-solution/

Twitter bot. (n.d.). In *Wikipedia*. Retrieved April 12, 2018, from https://en.wikipedia.org/wiki/Twitter_bot

van der Merwe, A., Loock, M., & Dabrowski, M. (2005, January). Characteristics and responsibilities involved in a Phishing attack. In *Proceedings of the 4th international symposium on Information and communication technologies*(pp. 249-254). Trinity College Dublin.

Wang, G., Mohanlal, M., Wilson, C., Wang, X., Metzger, M., Zheng, H., & Zhao, B. Y. (2012). Social turing tests: Crowdsourcing sybil detection. *arXiv preprint arXiv:1205.3856*.

Appendices

Appendix A: Cover Letter for Email and Listserv Recruitment

My name is Ju Shua Tan and I am a final year Masters student in Information Science at the University of North Carolina, Chapel Hill. As a part of research for my master's paper, I am conducting a research study to investigate how Twitter users detect social bots and what are the perceptions of Twitter users about the advantages and disadvantages of social bots. The participants must be over 18 years of age and are active Twitter users. The study involves one online questionnaire.

If you meet all of the above requirements and are willing to contribute to the study, please take the survey here - https://unc.az1.qualtrics.com/jfe/form/SV_4Z46lDk35njXugl. The survey consists of 20 questions and will take about 10-20 minutes to complete.

Your participation in this survey can help us gain valuable insight and try to identify and possibly improve the way Twitter users interact with social bots. Participation in the research is voluntary and the participant may choose to drop out at any time without penalty. This research has been reviewed by the UNC Institutional Review Board, IRB Study #17-3156.

If you have any questions about the survey or the research, please email me at jushua@live.unc.edu.

Thank you,

Ju Shua Tan

Appendix B: Facebook Recruitment Cover Letter

As a part of research for my master's paper at the University of North Carolina, Chapel Hill, I am conducting a research study to investigate how Twitter users detect social bots and what are the perceptions of Twitter users about the advantages and disadvantages of social bots. The participants must be over 18 years of age and are active Twitter users. The study involves one online questionnaire.

If you meet all of the above requirements and are willing to contribute to the study, please take the survey here - https://unc.az1.qualtrics.com/jfe/form/SV_4Z46lDk35njXugl. The survey consists of 20 questions and will take about 10-20 minutes to complete.

Your participation in this survey can help us gain valuable insight and try to identify and possibly improve the way Twitter users interact with social bots. Participation in the research is voluntary and the participant may choose to drop out at any time without penalty. This research has been reviewed by the UNC Institutional Review Board, IRB Study #17-3156.

If you have any questions about the survey or the research, please email me at jushua@live.unc.edu.

Appendix C: Survey Questions

Survey about Social Bot in Using Twitter

A social bot is a type of bot that controls a social media account. Like all bots, a social bot is automated software that spreads by convincing other users that the social bot is a real person.

Social bots are most common in Twitter, though there also have been experiments with Facebook bots. Given the design of Twitter with short messages, re-tweeting, following etc., it's actually not too difficult for a social bot to appear human. Social bots might try to get you to click on (affiliate) links, or simply just try to get you to follow them for fun.

This is a study about how Twitter users interact with social bots. I hope that my survey can raise your awareness about social bots in Twitter and better protect yourself against the negative impact of Twitter bots.

Thanks for participating in my survey. I appreciate your feedback. This survey will have 20 questions and it will takes approximately 10-20 minutes to complete.
Click the next button to get started!

Figure 13: Illustration of Twitter bot included in survey questions

(* denotes required questions)

Q1* What is your age?

____

Q2* What is your sex?

- ○ Male
- ○ Female

Q3* Which country are you from?

____

Q4* What is your occupation?

____

Q5* How often do you use Twitter? (pick the closest)

○ Daily

○ Weekly

○ Monthly

○ Occasionally

○ Very seldom

Q6* How long have you been using Twitter?

○ Less than a month

○ Between one month and one year

○ 1 - 5 years

○ 5 years or more

Q7* Why do you use Twitter?

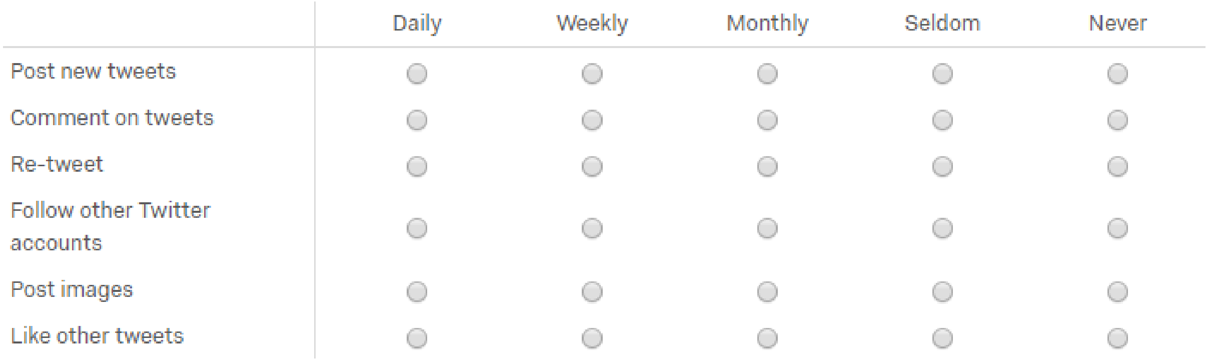
❑ To be alerted to or find out more about breaking news

❑ To keep up with the news in general

❑ To pass the time

- ❑ To tell others what I am doing and thinking about
- ❑ To see what people are saying about live events that I am watching or interested in
- ❑ To keep in touch with people I know
- ❑ To follow famous people
- ❑ To share news
- ❑ To socially network
- ❑ To follow trending topics
- ❑ Other ____

Q8* How frequently do you do these things on Twitter?



	Daily	Weekly	Monthly	Seldom	Never
Post new tweets	○	○	○	○	○
Comment on tweets	○	○	○	○	○
Re-tweet	○	○	○	○	○
Follow other Twitter accounts	○	○	○	○	○
Post images	○	○	○	○	○
Like other tweets	○	○	○	○	○

Q9* Who do you follow on Twitter?

- ❑ Family
- ❑ Friends
- ❑ Celebrities
- ❑ Sports athletes

❏ Politicians

❏ Co-workers

❏ People who share similar interests

❏ Other ____

Q10* Who follow you on Twitter?

❏ Family

❏ Friends

❏ Celebrities

❏ Sports athletes

❏ Politicians

❏ Co-workers

❏ People who share similar interests

❏ Other ____

Q11* Have you seen any postings by social bots on Twitter?

○ Definitely yes

○ Probably yes

○ Possibly

○ Probably not

○ Definitely not

Q12 Please upload a screenshot of what you think might be an example of social bot on Twitter.

Q13 Why do you think they are social bots?

____

Q14* Do you think they are more helpful or more harmful?

○ More helpful than harmful

○ More harmful than helpful

○ Equally helpful and harmful

Q15* What are some advantages of social bots to you on Twitter?

❏ Entertainment

❏ Automation

❏ Interactive

❏ Self protection

❏ Self promotion

❏ Other ____

Q16* What are some disadvantages of social bots to you on Twitter?

❏ Spreading malicious contents

❏ Spreading fake news

❏ Increase polarization

❑ Spreading influence

❑ Promote hatred and hate speech

❑ Gaining unfair popularity

❑ Create the business of paying for Twitter followers

❑ Privacy infringement

❑ Identity theft

❑ Other ____

Q17* How do you identify fake Twitter accounts?

❑ Username sounds fake

❑ Content of post sounds more machine generated than by a person

❑ Tweet large sequences that are often promotional and repetitive

❑ Have a disproportionate follower and following count

❑ Inactive for a long time

❑ Detect them by using automated tools e.g. BotOrNot, Twitter Counter, Twitter Audit etc.

❑ The lack of a verified account blue checkmark

❑ Very spectacular photos with attractive men or women

❑ Biography text is not properly written

❑ Other ____

Q18* Do you protect yourself from harmful Twitter bots?

- ○ Yes
- ○ No

Q19* What action(s) do you do to protect yourself against harmful Twitter bots?

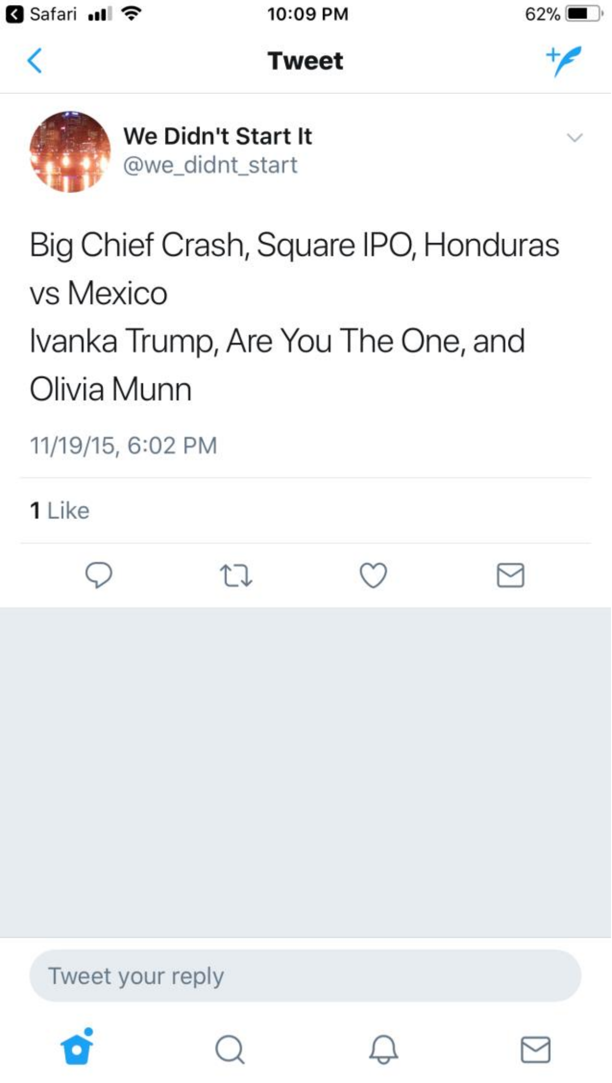
- ❑ Enable Twitter's "Protect my tweets" option
- ❑ Block certain people from following me on Twitter
- ❑ Get rid of followers on Twitter
- ❑ Reporting spam on Twitter
- ❑ Other ____

Q20 If you have any additional comments or questions, please feel free to write them here.

____

Appendix D

Screenshot attachments for the question "Please upload a screenshot of what you think might be an example of social bot on Twitter."



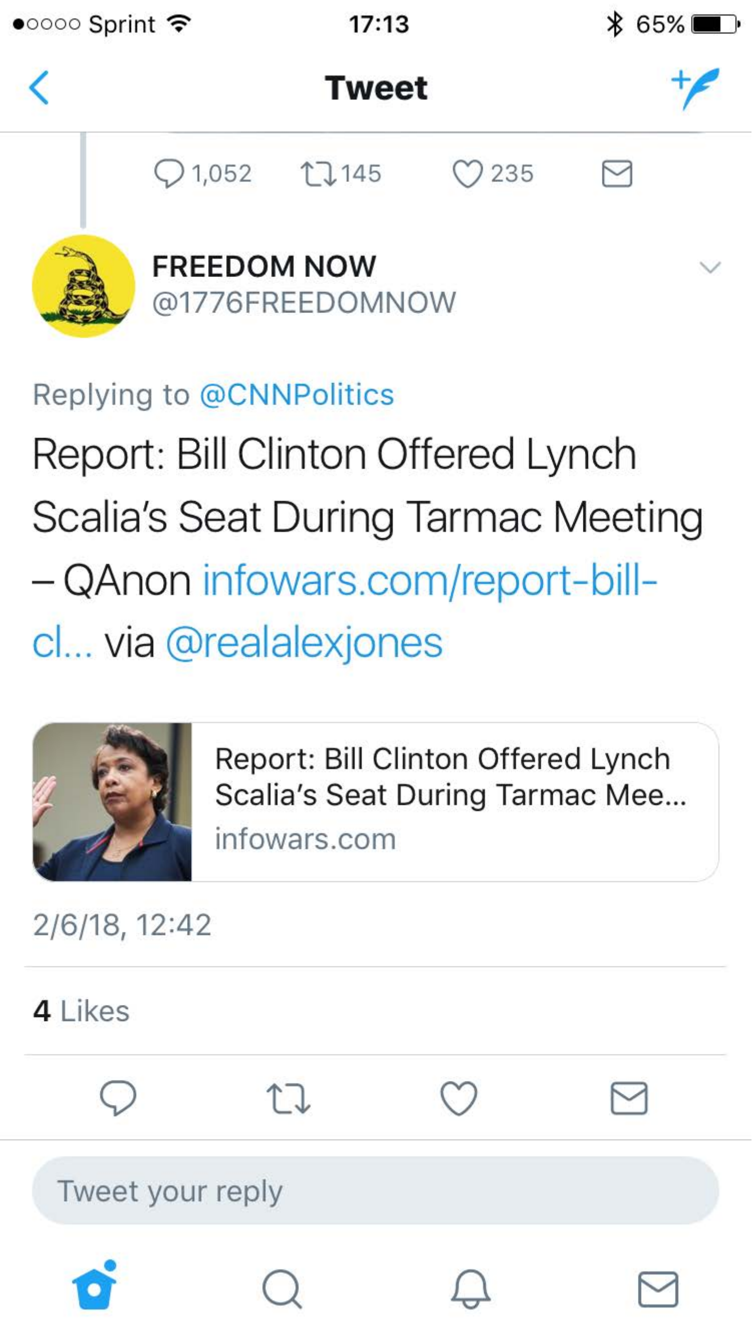
We Didn't Start It
@we_didnt_start

Big Chief Crash, Square IPO, Honduras vs Mexico
Ivanka Trump, Are You The One, and Olivia Munn

11/19/15, 6:02 PM

1 Like

Figure 14: Attachment of social bot 1



FREEDOM NOW
@1776FREEDOMNOW

Replying to @CNNPolitics

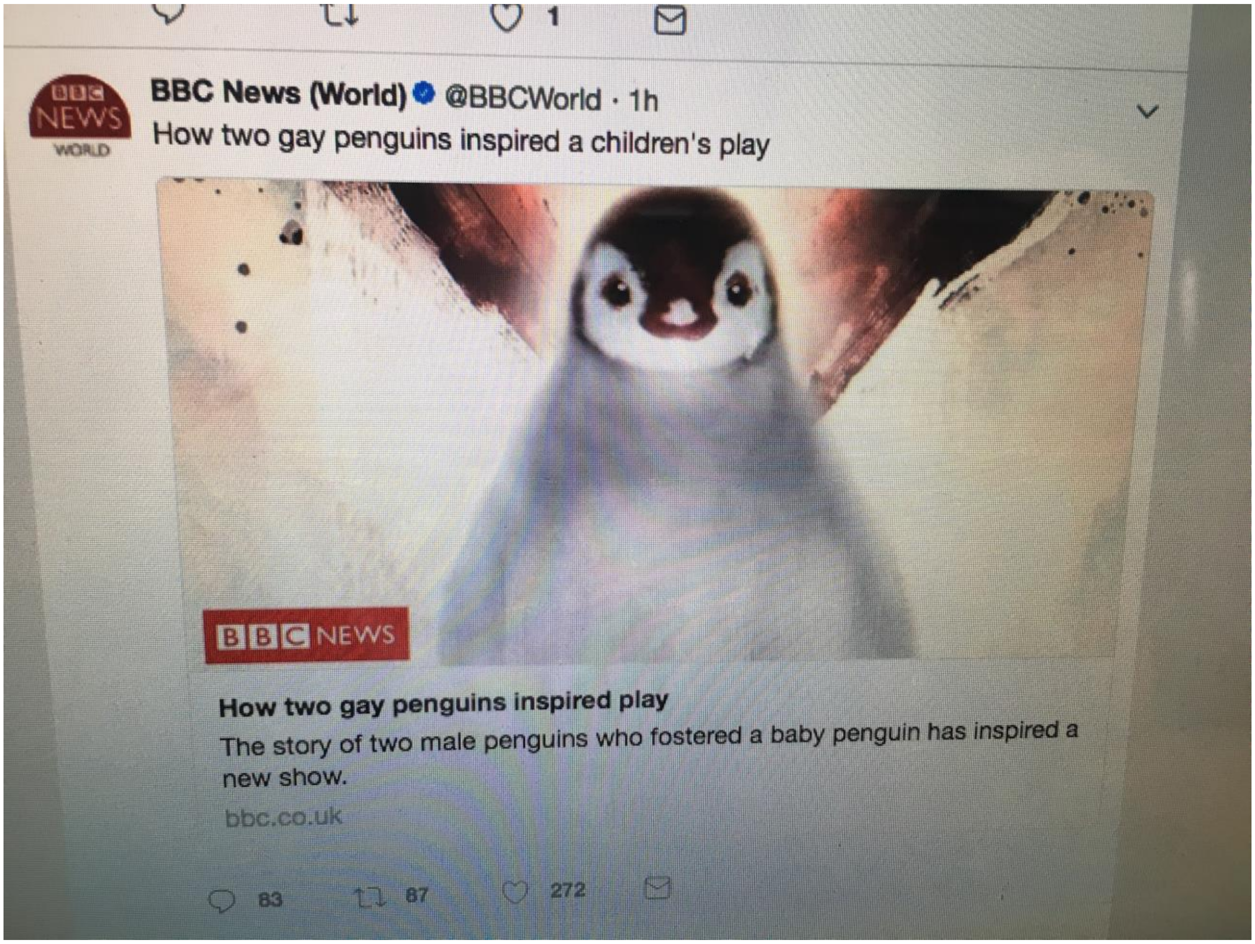
Report: Bill Clinton Offered Lynch Scalia's Seat During Tarmac Meeting – QAnon infowars.com/report-bill-cl... via @realalexjones

Report: Bill Clinton Offered Lynch Scalia's Seat During Tarmac Mee...
infowars.com

2/6/18, 12:42

4 Likes

Figure 15: Attachment of Social Bot 2



BBC News (World) @BBCWorld · 1h

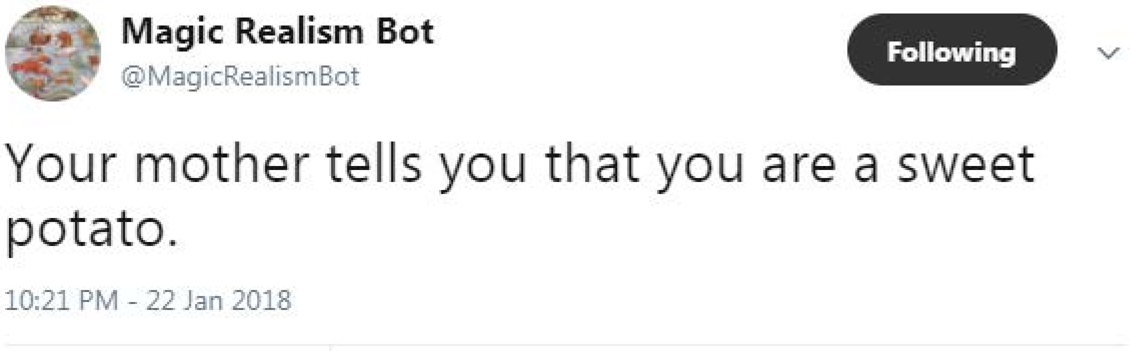
How two gay penguins inspired a children's play

How two gay penguins inspired play

The story of two male penguins who fostered a baby penguin has inspired a new show.

bbc.co.uk

Figure 16: Attachment of Social Bot 3

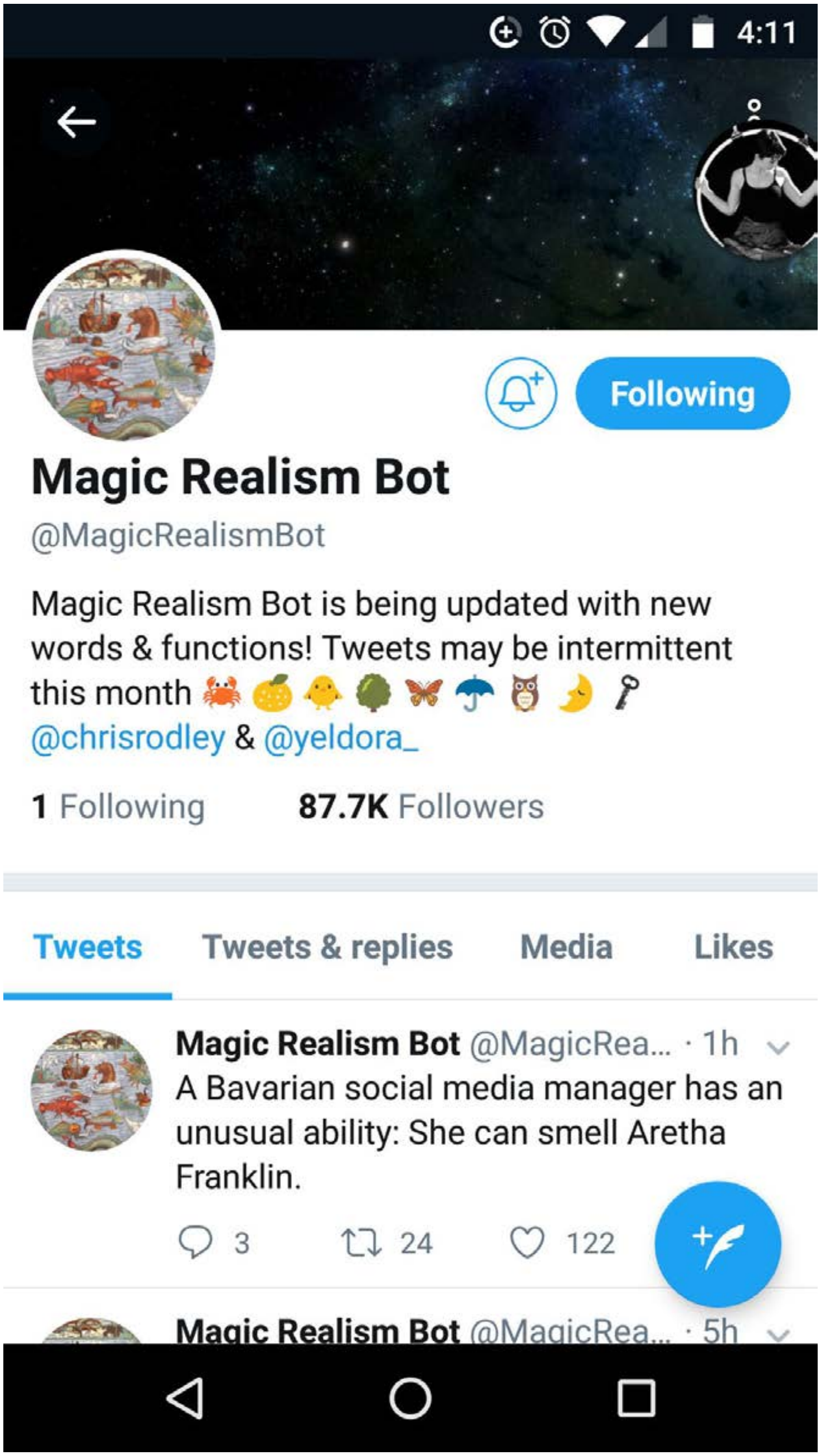


Magic Realism Bot
@MagicRealismBot

Your mother tells you that you are a sweet potato.

10:21 PM - 22 Jan 2018

Figure 17: Attachment of Social Bot 4



Magic Realism Bot

@MagicRealismBot

Magic Realism Bot is being updated with new words & functions! Tweets may be intermittent this month 🦀 🍊 🐥 🌳 🦋 ☂ 🦉 🌛 🗝 @chrisrodley & @yeldora_

1 Following **87.7K** Followers

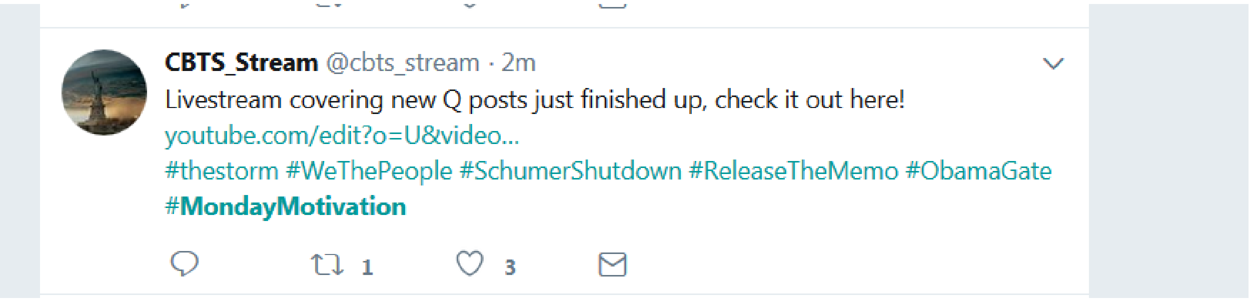
Magic Realism Bot @MagicRea... · 1h

A Bavarian social media manager has an unusual ability: She can smell Aretha Franklin.

3 24 122

Magic Realism Bot @MagicRea... · 5h

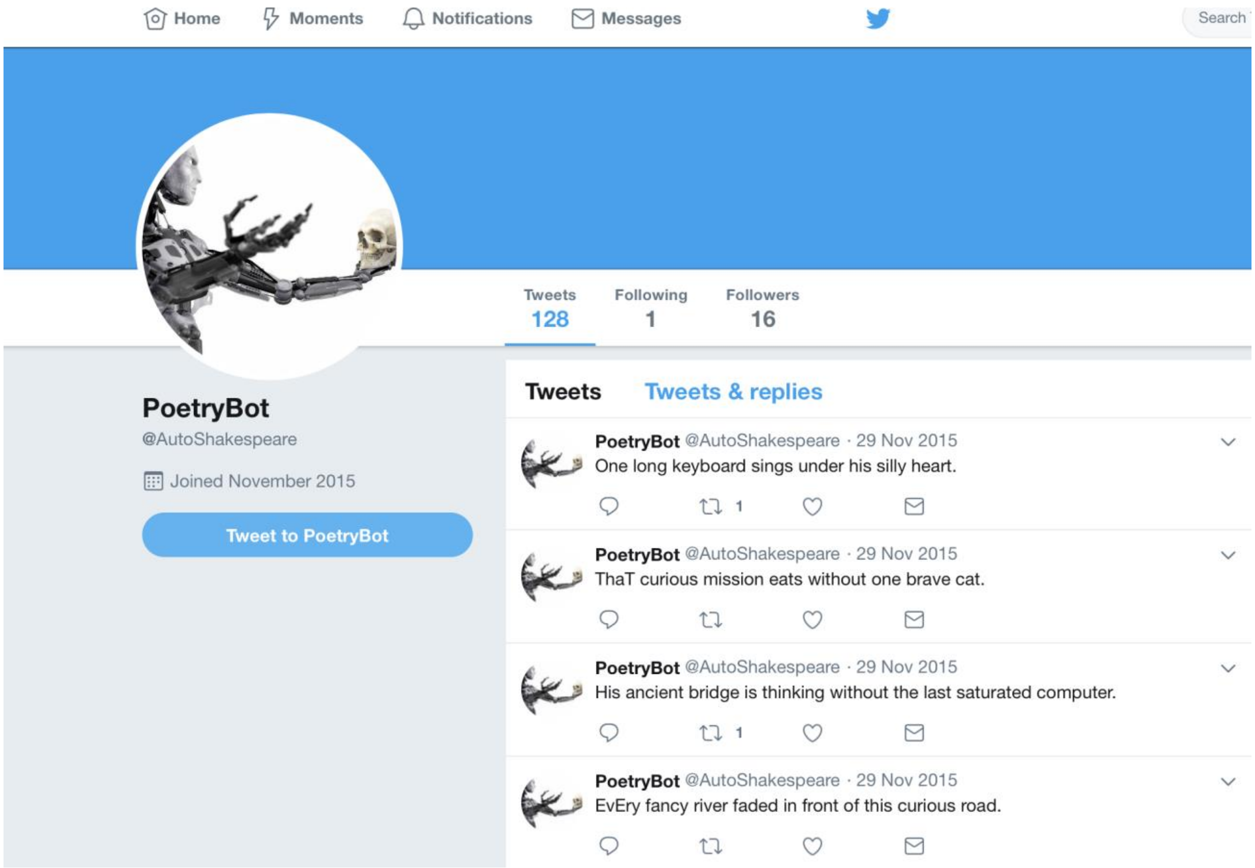
Figure 18: Attachment of Social Bot 5



CBTS_Stream @cbts_stream · 2m

Livestream covering new Q posts just finished up, check it out here! youtube.com/edit?o=U&video... #thestorm #WeThePeople #SchumerShutdown #ReleaseTheMemo #ObamaGate **#MondayMotivation**

Figure 19: Attachment of Social Bot 6



PoetryBot
@AutoShakespeare
Joined November 2015

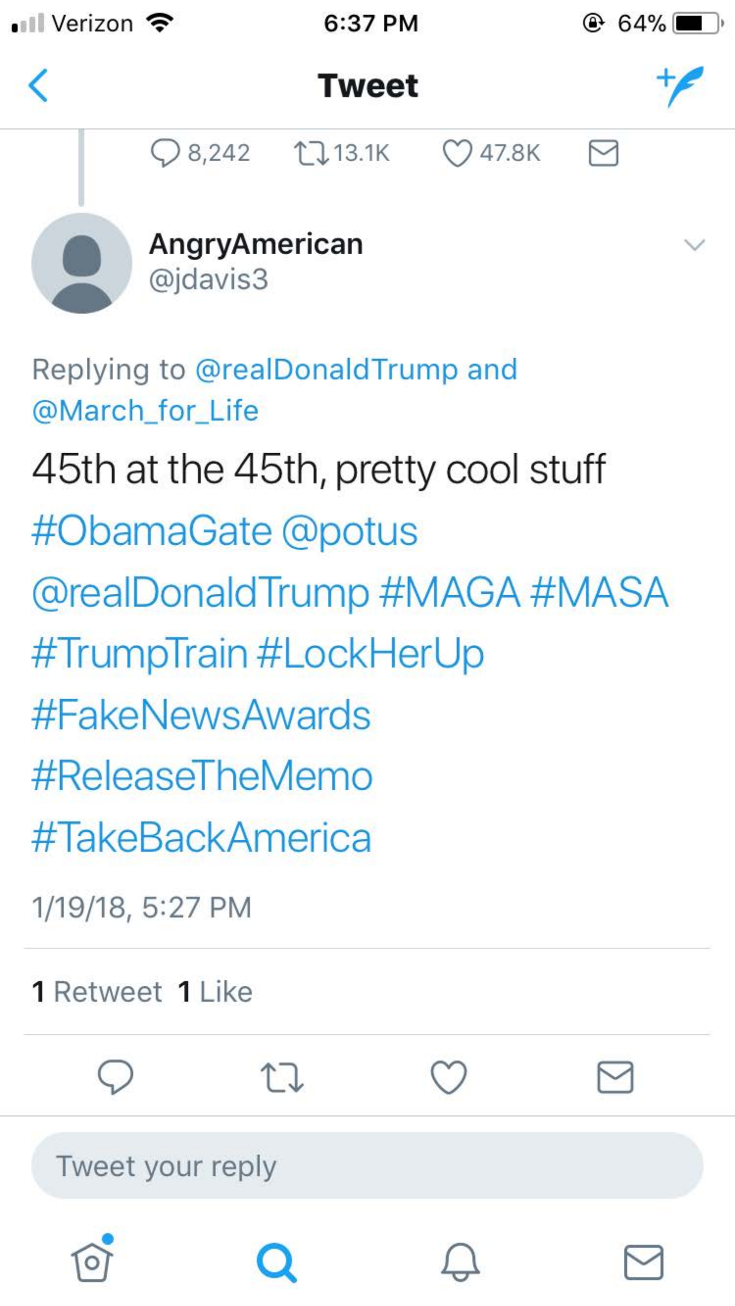
PoetryBot @AutoShakespeare · 29 Nov 2015
One long keyboard sings under his silly heart.

PoetryBot @AutoShakespeare · 29 Nov 2015
ThaT curious mission eats without one brave cat.

PoetryBot @AutoShakespeare · 29 Nov 2015
His ancient bridge is thinking without the last saturated computer.

PoetryBot @AutoShakespeare · 29 Nov 2015
EvEry fancy river faded in front of this curious road.

Figure 20: Attachment of Social Bot 7



AngryAmerican
@jdavis3

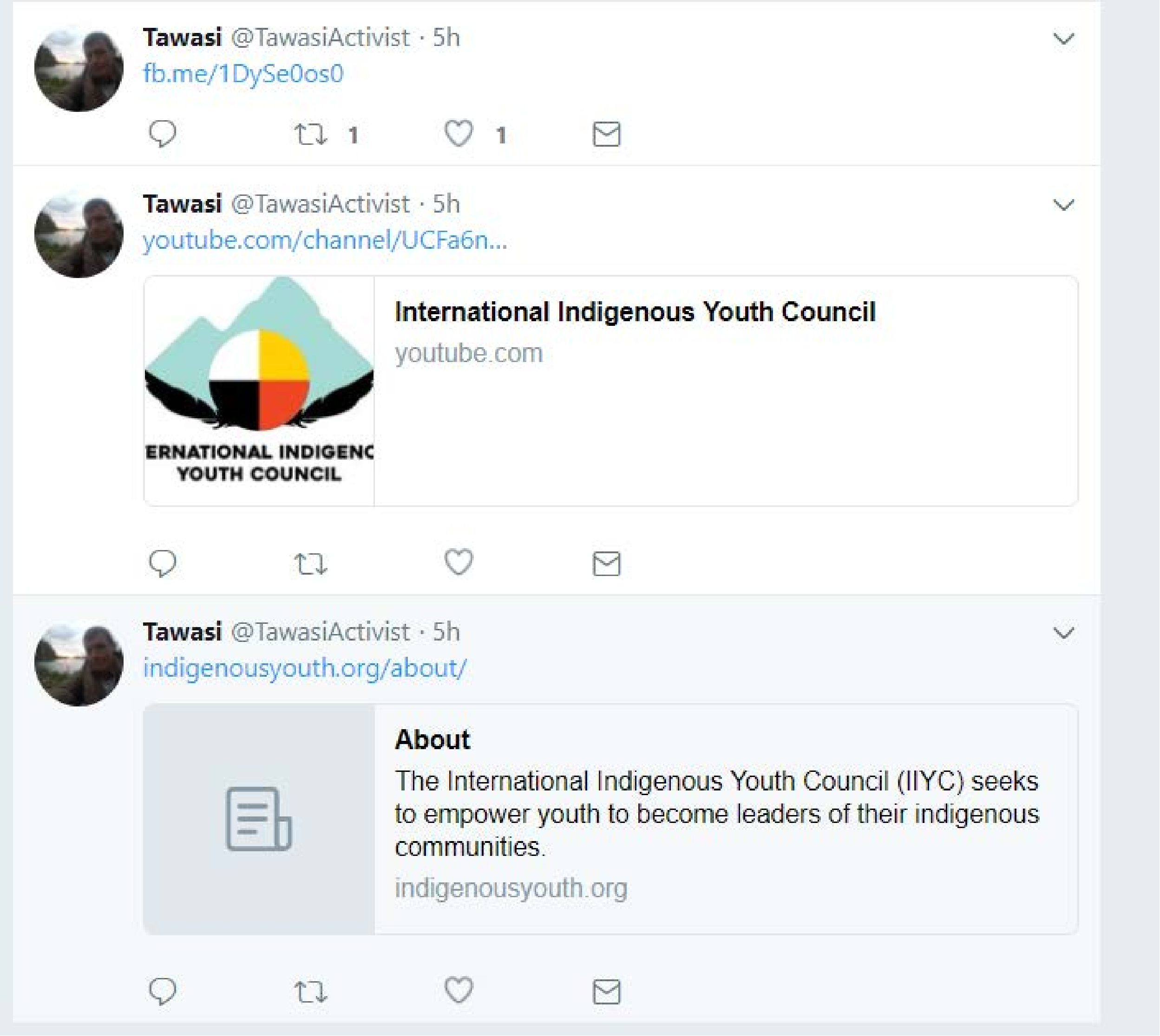
Replying to @realDonaldTrump and @March_for_Life

45th at the 45th, pretty cool stuff #ObamaGate @potus @realDonaldTrump #MAGA #MASA #TrumpTrain #LockHerUp #FakeNewsAwards #ReleaseTheMemo #TakeBackAmerica

1/19/18, 5:27 PM

1 Retweet **1** Like

Figure 21: Attachment of Social Bot 8



Tawasi @TawasiActivist · 5h
fb.me/1DySe0os0

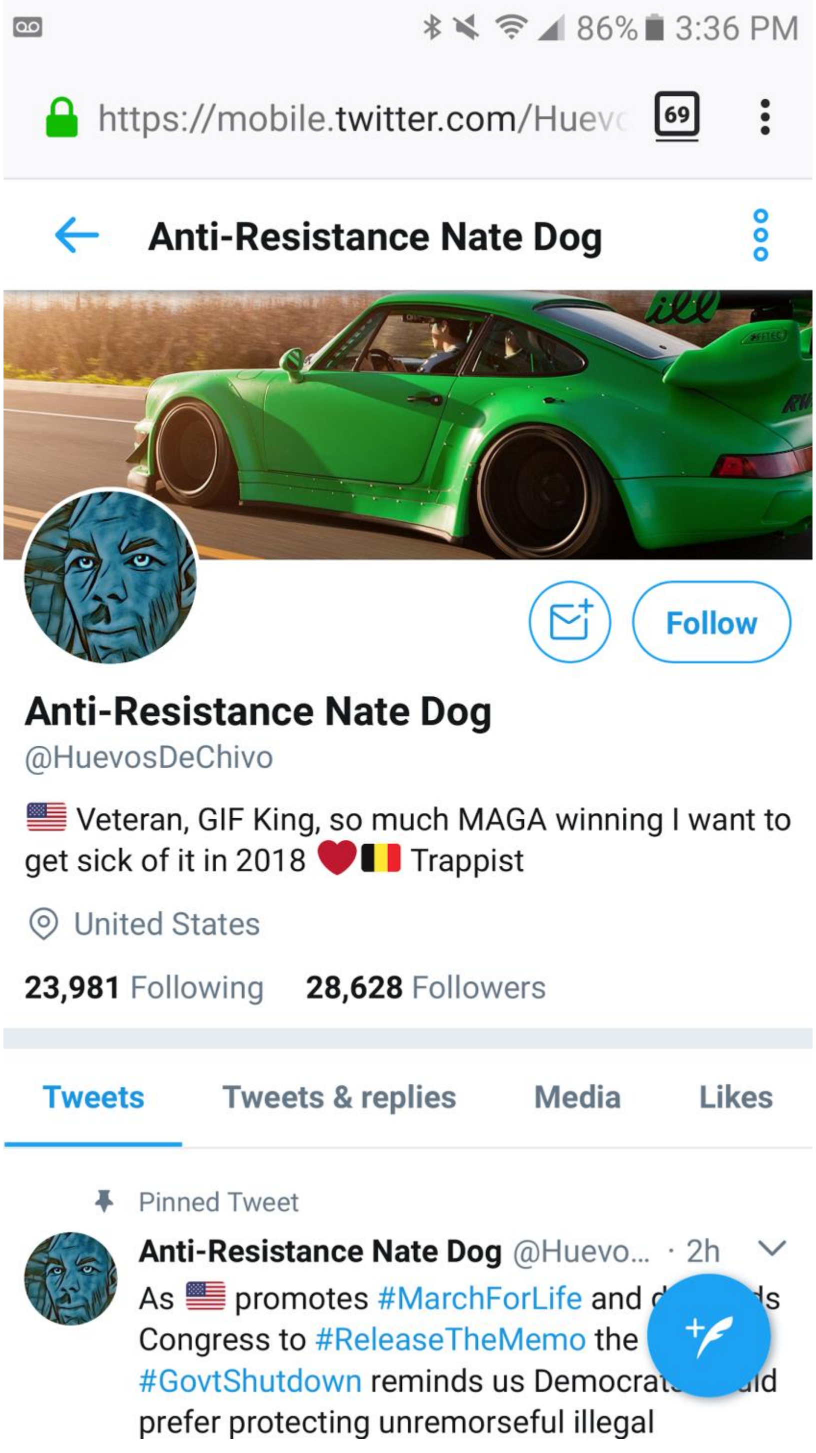
Tawasi @TawasiActivist · 5h
youtube.com/channel/UCFa6n...

International Indigenous Youth Council
youtube.com

Tawasi @TawasiActivist · 5h
indigenousyouth.org/about/

About
The International Indigenous Youth Council (IIYC) seeks to empower youth to become leaders of their indigenous communities.
indigenousyouth.org

Figure 22: Attachment of Social Bot 9



Anti-Resistance Nate Dog

@HuevosDeChivo

🇺🇸 Veteran, GIF King, so much MAGA winning I want to get sick of it in 2018 ❤️🇧🇪 Trappist

United States

23,981 Following 28,628 Followers

Anti-Resistance Nate Dog @Huevo... · 2h

As 🇺🇸 promotes #MarchForLife and d ds Congress to #ReleaseTheMemo the #GovtShutdown reminds us Democrat uld prefer protecting unremorseful illegal

Figure 23: Attachment of Social Bot 10

Appendix E

"Why do you think they are social bots?" free text answers

(Highlighted answers are those that I coded as more insightful answers and were summarized in the Result section)

Randomized language; nonsensical.
I don't have a screen shot
The tweet does not directly contribute to the conversation that is going on and the account seems to exist just to spread conspiracy theories
They are sharing
Catchy title
Text doesn't read like a human wrote it
I am not sure
I think accounts that only tweet outgoing links and accounts that only retweet famous people are probably bots.
I rarely find or recognize social bots on twitter.
--
To spread information quicker to a large amount of people/users. So that other users receive the false perception that a brand or product or person is interacting directly with them.

They have the word bot in the name
It's called Magical Realism Bot
Lots of hashtags including the use of the trending (and as far as I can tell, unrelated) hashtag #mondaymotivation. It's also a link. The use of multiple, disparate hashtags to link to a youtube video make me think it's a bot.
Aside from the fact that it calls itself a bot, the spelling of the tweets is why I think this is a bot.
Sorry, I can't think of a specific example for a screenshot!
No profile picture, lots of hashtags, page is full of political tweets
I look for bots following me on Twitter every week. For some reason I pick up a lot (aka they follow me). I don't know if this guy is actually a bot, but he has a lot of warning signs. Some signs I look for include lots of followers/following (like in the 10K level) when the person isn't verified, they often retweet content, their original content sounds like a bot wrote, all the images they post are stock photo like, if you look at there likes they don't make sense (super sporadic), or they have a handle that a person would never choose (like with a bunch of numbers).
Because they are posting on behalf of a company; I cannot attach a photo however because I have disabled ad posts and posts by twitter accounts that I do not follow.
can't find one, i feel like the social bots i find are not on my main page/feed