Cyber-security: Identity Deception Detection on Social Media

Alex Mathew[#1]

[#]*Professor, Dept of Cyber Security, Bethany College*
Bethany, USA

Abstract — *Social media is an essential tool that allows billions of people to share information on a different perspective in real-time and without censorship. People are less likely to lie and act more responsibly on online platforms when they can be identified. However, the freedom present in social media platforms comes at the cost of encountering cyber-attacks. Social media is characterized by anonymity and false identities; this makes it difficult to detect the source of cyber threats on such platforms. Cyber-security caused by people on social media is widespread and have generated a lot of attention. Social media has also been associated with other negative aspects such as cyberbullying and cyber-terrorism where terrorist groups use the platforms to acquire new members. Fighting deception requiresthe combined effort of both the developers and social media users; this help in detection of such cases and therefore handle them appropriately. The research below focusses identifying and detecting deception on social media.*

Keywords — *Social media, deception, detection, cyberbullying*

I. INTRODUCTION

Identity attributes provide details on who a person is or the qualities that can be used to distinguish the person from other individuals [9]. Deception refers to the act of cheating someone by misrepresenting or concealing the truth; this can also be defined as a situation where facts are represented contrary to the truth. Identity deception can be viewed from different perspectives. Deception is not something new, it exists even in nature, for example, viceroy butterflies mimic the look monarch butterflies so birds cannot eat them as the dislike monarch butterflies due to their bitter taste; this allows them to survive as long as they are not overpopulated in a specific ecosystem [8]. Similarly, humans have been using deception mainly for hostile motives.

II. TYPES OF SOCIAL MEDIA DECEPTION

There are different types of deception; the first type is content deception. In social media, this is achieved by providing false information. Social media platforms that focus on the creation and sharing of online content are the most susceptible to this kind of deception. Humans find it challenging to identify images that have been modified even in situations where the changes are reasonably substantial [5]. Technology makes it possible for users to manipulate digital files, advanced software for editing images provide excellent avenues for creating fake content.

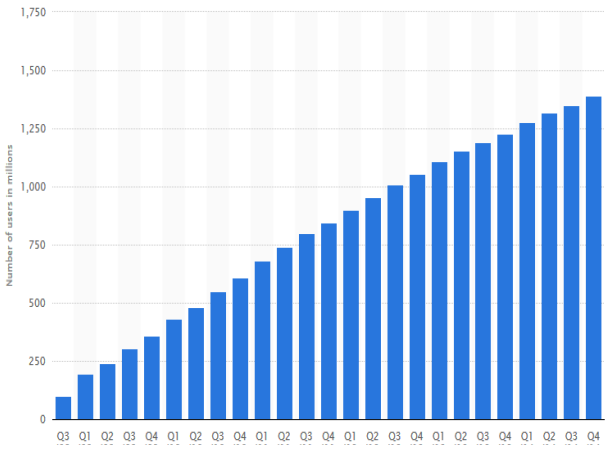

Figure 1: The growth in the number of fake accounts over the years.

For example, a person can edit pictures to appear as if the person is traveling the world and then use social media to broadcast these images. Such a strategy may help in elevating the person's status and maybe in some cases aid in gaining trust from a victim so that the victim can freely agree to the deceiver's requests.

The second type of deception is sender deception. The primary method used to achieve this is through impersonation. Social media impersonation occurs when a profile or page is created to appear as though it is a legitimate page for a business or a person's social media account [7]. Deceivers may also illegally gain access to the account of another person and use it to obtain information from the people who they interact with using the stolen identity. Lack of the ability to authenticate the sender's credential increases the chances of conducting successful deception procedures. Social media platforms such as Facebook where the names used by users are not unique as it is the case in other platforms such as Twitter and Instagram make it easier for users to get away with identity theft. However, even in platforms that implement the use of

unique usernames, it is still possible for users to deceive others by using names almost similar to those of the original user by creating usernames almostidentical to those of the original user by manipulating letter that almost look alike.

III. DETECTING DECEPTION ON ONLINE COMMUNICATION PLATFORMS

A lot of information posted on social media is not trusted. The exponential growth experienced in the social media platformsespecially in the last decade has significantly increased the volume of data generated. Social media has expanded the traditional view of a community to include groups of people that have never met before but can communicate on the online platforms to share opinions, interests, and knowledge. However, based on 2014 study by McAfee, 90 percent of the young generation do not trust information posted on social media platforms especially personal information; this is mainly attributed by the aspect that they believe it is dangerous to display such data in online communication platforms [1]. Ensuring accessibility, confidentiality, and integrity of information is a significant concern for companies, learning institution and people that use social media for different purposes.

Fake accounts are considered as one of the forms of cheating. People create fake accounts for various reasons; the most common one is that they are hackers. Such cyber-criminals use every method accessible to them to try and steal personal information from unsuspecting users [4]. Using this method, people conduct deception not only by uploading profile pictures that do not belong to them but also using usernames that belong to other people. Due to the massive popularity of social media, experts have analyzed the behavior on the platforms and proposed automatic methods of assessing the content shared on them; this also entails assessing differences between fake and real accounts to distinguish between fake and legitimate accounts or information.

Though it not a requirement, the ability to recognize deception helps in improving trustworthiness on social media platforms [6]. One of the ways that can be used to achieve this is by evaluating the source, determining the intent and being careful when online. The source of information is the biggest clue in helping a person identify whether the person who posted or shared the data is an actual owner of the identity or a person without any real connections. Determining the intent of the post entails evaluating what the post aims at accomplishing. The purpose behind specific content can help identify whether the information is legitimate or strategically trying to deceive.

Lastly, being careful is an action that all social media users should take. It is necessary that people be cautious with who they share personal information while on the internet even in cases where it feels safe. The tactics used for online deception continues to evolve making it essential for every user to familiarize with them. It is essential to understand that it is not only individual users that are at risk of deception but also businesses that use social media for purposes such as advertising. All users of social media should, therefore, protect themselves while online. Also, in case a person has already been deceived, the individual should learn how to deal with it to prevent further damage.

IV. DISCUSSION

The tendency towards violence and aggression is higher when people are anonymous than when they can be identified [10]. However, anonymity in some cases, especially on social media, is essential. For example, posting legitimate information on such platforms such as addresses helps in easing the work of criminal such as kidnappers as they can track the physical location of a person by gathering information posted by the individual online. However, for social media platforms to continue expanding as a communication medium, it is crucial for the information shared on the avenues to be trustworthy.

When using social media for activities such as deceiving people into downloading and installing malicious software, the deceivers usually use destructive codes and attach them to what is considered permissible content in social media platforms. One of the ways that users can reduce the chances of them falling victim of such risk is by refraining from clicking links or opening attachment from unknown sources. Some of these links might appear appealing, for example, a person might be provided with a link offering vacation packages, but after clicking it, malicious software is deployed on the device of the user [2]. When such malicious codes successful install into the user's device, they can be used to collect information such as credit card details and other personal information.

Another essential factor to consider is ensuring the operating system and applications of devices used to access social media platforms are up-to-date whether smartphone or computers. Updated applications and operating system significantly reduce the chances of devices getting hacked by deceivers on social media platforms; this is because software developers continually look for loopholes in the programs that

hackers might use to gain unauthorized access. In most cases, vicious attacks targeting different users on the internet are as a result of malware taking advantage of vulnerabilities found in typical applications such especially browsers [3]. When developers realize any weak-points, they reinforce them and provide patches which are installed into the existing software in the form of updates; this helps to protect the users.

Social media forms an essential platform for advertising. Customers who wish to buy goods or services after seeing advertisement can be redirected to the website of firms where they can make purchases or in some cases, they can do it on the social media platforms. However, whenever users receive requests via social media for transactions or even buying virtual points, they should verify the identity of the sender and the validity of the request to ensure they do not make payments to online criminals. Users should also be cautious when making friends online and should remain vigilant at all times.

CONCLUSION

Social media has experienced exponential growth in the last few decades. It allows people from different parts of the world who share common interests to connect virtually and share ideas, information, andviews. Social media also provide a cheap method for friends or family members to communicate in real-time regardless of the distance between them. However, the continued expansion of social media has been some extent hindered by various shortcoming present on the platforms. For example, deception is a significant challenge on social media avenues and ranges from people using fake accounts, people spreading and creating misleading content and also tricking people into download malicious software that can be used to gather information from their devices. To help avoid being deceived when using online platforms, users should assess the source of the data, its aim and should remain cautious so that they do not fall victims to tricks used by deceivers present on social media platforms. Other technical safe online practices include making sure that the devices that the users use to access the internet are up-to-date. Taking advantage of outdated operating systems or software such as browsers is one of the leading methods used by deceivers to gain unauthorized access to the devices of the users they target.

REFERENCES

[1] Alowibdi, Jalal S., et al. "Detecting deception in online social networks." 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014). IEEE, 2014.

[2] Calyptix. "Social Media Threats: Facebook Malware, Twitter Phishing, and More." *Security* (2017): N.p., Web. 6 Apr. 2019.

[3] Davis, Gary. "Why Software Updates Are So Important." *McAfee* (2017): N.p., Web. 6 Apr. 2019.

[4] Holtz, Mordecai. "Fake Social Media Accounts." *Social Media Club* (2018): N.p., Web. 6 Apr. 2019.

[5] Horaczek, Stan. "Spot faked photos using digital forensic techniques." *Popular Science* (2017): N.p., Web. 6 Apr. 2019.

[6] Sciberras, Elena. "Deception on Social Media – how to protect yourself." *Social Media Buzz* (2014): N.p., Web. 6 Apr. 2019.

[7] SiteTakeDown. "SOCIAL MEDIA IMPERSONATION." *SiteTakeDown* (2016): N.p., Web. 6 Apr. 2019.

[8] Alowibdi, Jalal S., et al. "Detecting deception in online social networks." 2014 Communications of the ACM 57.9 (2014): 72.

[9] Van der Walt, Estée, and Jan HP Eloff. "Identity Deception Detection on Social Media Platforms." ICISSP. 2017.

[10] Zhang, Kaiping, and René F. Kizilcec. "Anonymity in social media: Effects of content controversiality and social endorsement on sharing behavior." Eighth International AAAI Conference on Weblogs and Social Media. 2014.