SOCIAL DECEPTION IN ONLINE PLATFORM:CONCEPT,ATTACKS AND ETHICAL ISSUES

Rajesh Yadav
BML Munjal University,Gurgaon,India
rycs1980@gmail.com

Abstract: Online communication through social network services has become a vital part of our life. As a result, social deception in the online platform has grown up as an important threat in this world of interconnected digital technology, specifically for that category of users who are vulnerable to different cyber-attacks and threat to privacy, monetary fraud. Hence, it is very important to analyze online social deception and build defensive measures which can work very well against it to build reliable social network services. A broad survey has been done in this paper which includes understanding the elemental meaning of social deception, its techniques, a detailed summary of attacks in online social deception with its preventive measures as well as ethical issues related to the conduct of research in this area.

***Keywords*: Cyber Attacks, online social deception, defense, online social networks**

1. Introduction

Now a days, social network services and social media plays a very important role in our life. A very large percentage of users are using social media for dif- ferent activities, this increase in usage of social media is because of the different benefits a user gets from it like staying connected with others, participating in civic as well as political activities, to search for jobs we all as presenting views and emotional support over it. Although social media offers so many benefits from its usage, but still, a large number of people are concerned about their pri- vacy and activities which can be deceptive aiming to be harmful for legitimate users[1]. In order to deceive users in many different ways, cyber criminals have used advanced social media as a platform to exploit them[2].Throughout year 2018,around 25% of users have experienced various types of social deception like theft of identity ,cyber fraud, phishing attacks and this has happened be- cause of the damage caused by attacks in online social deception[3].Due to the advancement of features in social network services, a large number of cyber- crimes have happened in addition to phishing attacks, online customer fraud
,cloning of identity, hacking into the machine as well as trafficking of hu- mans[4].Therefore, our society deeply needs to understand social deception in online platform and should work upon against different attacks so that we build a reliable cyberspace.

Key Offerings

In this paper, I have made the following key offerings:

- Thorough understanding of basic meaning of deception in online platform with its methods.
- An extensive classification of various categories of attacks in online social deception .
- A comprehensive survey of prevention mechanisms of online social decep- tion.
- An extensive discussion on ethical issues in online social deception research.

Organization of Paper

This paper is organized as follows.

- In Section 2 , I have surveyed the concept of deception along with methods of deception.
- In Section 3, different types of attacks in online social deception have been dis- cussed like misinformation, phishing, spam, sybil attack, profile cloning, crowd
-turfing as well as some human targeted attacks.
- In Section 4, a survey of present mechanisms of prevention for online social deception has been done, namely fake news prevention, identity theft preven- tion, cyber bullying prevention and social honeypots.
- In Section 5,due to the involvement of human being and their behaviors in the research of online social deception, I have discussed various ethical issues re- lated to the conduct of online social deception research.
- Finally, Section 6 provides concluding remarks and discusses future research directions in the area of online social deception.

2. Deception Concept And Techniques

2.1 Concept Of Deception

According to the Cambridge online dictionary, deception is defined as “the act of hiding the truth, especially to get an advantage”. In view of online deception, many factors should be considered like deceiver, the basic aim of deception ,social media service ,technique of deception and possible target of deception[5].

All the aspects which are related to deceivers who try to get involved in online de- ception should be taken care of like how

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

much technical knowledge they carry, their expectations and level of motivation as well as how are they related to the target . A high level of security applied to social media can impact deception suc- cess, by increasing the security level, we can bring down online deception by be-
ing cautious and implementing prevention measures against the attacks. Many techniques of online deception exist now a days which are based on Cialdini's 6 principles of influence. On the other side, the application area of deception i.e., the social media, number of users who are targets as well as deception time puts an impact on the way we choose the techniques of deception. In case we consider human factors, securing user data and information becomes much more difficult. Particularly when we talk about privacy paradox, it is about disclose of personal user information even when they consider it very seriously as a concern[6].

2.2 Deception Methods

In social media scenario, different methods of deception have been discussed in the literature that include bluffs, website mimicking, fake website creation
,evasion, redirection of webpages.The model shown in figure 1 involves sender(S), message, or content(I), communication channel(C), and receiver (R). if the model of receiver is not matching with the received model, then deception has happened[29].

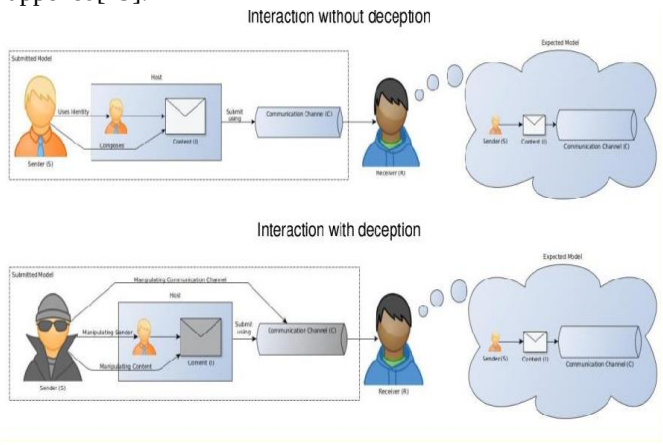

Fig. 1. Interaction without and with deception

Content Deception

The most common method to deceive others is to falsify information by changing the content. In case of social media, which is primarily based upon content like news sites, content communities, blogs are highly vulnerable to content deception[7].With the use of different tools and technologies, any person can change the multimedia files to any amount of degree. Image tampering is a very good method to fake content for example someone can represent himself as travelled to any country in the world by performing some alteration to the images
and then uploading them to social media. This is very helpful for deceivers to raise their social status and then he can win trust of a victim in order to get further information. Content deception specifically requires two parties i.e., a victim and an attacker. With respect to the social media ,goals of content deception consist of fake reviews, fake profiles etc. An attacker can perform attacks using fake profiles and fake reviews to achieve any level of success[8].

Sender Deception

One can change the identity information of sender to achieve sender deception. Impersonation attack can be performed by the attacker which results in deception of identity or theft of identity. In order to gain crucial information from their peers like address, date of birth, mobile number etc., deceivers can access victim identity and use it to achieve their goals.

Communication Channel Deception

A deceiver with good knowledge and skills can even manipulate the channel of communication.By doing so,the deceiver will be able to modify messages which are in transit,reroute the traffic as well as perfrom eavesdropping of messages. By having access to the user's IP address, multiplayer games in consoles can be hacked by the attacker[9]. If it happens,the deceiver will be able to host the game and then throw out the player and continue with deception of identity theft. Instead of getting information, deceiver might have some interest in damaging the reputation of victim. As we know that channel deception makes use of technology, so this makes it vulnerable to attacks, specifically in those environments where there is similarity of architectures and technologies.Since web servers are generally more secure, therefore social networking sites and content communities are less vulnerable to channel deception.

Hybrid Deception Techniques

A combination of host based as well as network-based techniques are used in hybrid deception. Different components like dazzling, masking, mimicking, and decoying for increasing deception effectiveness are a part of combination of network and host deception.Such deception methods are very effective in the social media platforms like blogs, social networking sites in which user identity is highlighted and one to one as well as one to many communication is provided.

3. Types of Online Social Deception Attacks

There exist a wide variety of attacks in online social deception which are used by deceivers to compromise the victims security.

3.1 Misinformation Attack

It is the false information present in web as well as social media. This belongs to the case of deception without intent because of which people's belief is mislead to the false propagated information. Misinformation can be further classified as fact- base and opinion-based. Fact-based information misleads the belief of people because of fraud from ground truth like social media fake news and hoaxes whereas in case of opinion-based,propagation happens without

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

any ground truth[11].

3.2 Phishing Attack

Phishing attack belongs to one of the most common deception techniques i.e., luring. In case of phishing attack, the attacker steals sensitive information like usernames, passwords and financial details through a fraudulent attempt.

3.3 Spam Attack

It also belongs to luring as a deception technique. Bulk emails and messages are used by malicious users to overwhelm the victims with spam which can be of dif- ferent varieties like comment scam, trackback spam, spiders and bots. Malicious users have an intention of influencing the legitimate users through spamming[12].

3.4 Sybil Attack

It belongs to the category of fake identity attacks. Attackers use many forged identities to sabotage the reputation system and enhancing as well as reducing the user's reputa- tion falsely.

3.5 Cloning of Profile

A duplicate of an existing user profile is done secretly by the attacker in different plat- forms of social media. Because the cloned profile looks similar to the real profile, this gives the attacker a chance to make use of friend relationship and send friends re- quests to the many contacts of cloned user. Once the trustworthy relationship is estab- lished with a victim user ; the attacker does the task of stealing sensitive data from us- er friends. Many societal threats have been exposed by profile cloning as many cybercrimes can be committed by the attacker like cyberstalking, cyberbullying, black mailing thereby introducing threats to victims[12].

3.6 Crowdturfing

Staff is hired by many public relation firms for posting comments on product on vari- ous online platforms and social networks without consuming products or services. Well coordinated attacks can be carried out by a group involving paid posters and de- sirable results can be generated which can be both positive or negative in order to grab attention and escalate the curiosity. This concept is known as crowdturfing , it also has

a second name i.e., cyber gossips. It can mislead online users and can also put busi- ness or individuals at a high level of risk.

In case of twitter networks, professional users, middleman and casual users are classi- fied as crowdturfers. Their profiles and various activities have been analyzed to crowd turfing workers detection[13].Machine learning based detection method of crowdturf- ing has been discussed in literature[14].

3.7 Human Targeted OSD Attacks Cyber Bullying

Cyberbullying is one of the human targeted attacks in which the attacker has an intention to harass someone specially the adolescents[12]. It causes fear among the victims and it is also harmful in the sense that it can lead to humiliation which can be public, malice and unwanted contact[15].

Trafficking of Human

Human trafficking is a very bad component of our society. Online social decep- tion can lead to trafficking of a large number of victims by using a variety of ad- vertise kind of services across different parts of world[16][17].

Cybergrooming

It is a type of human targeted attack in which the attacker tries to make a rela- tionship with the victims, specifically children of female gender using different platforms of social media. While doing so, they carry an intention to have sexual relationships with the victims and even involve child pornography[12][18].

Table 1 shows some of the online social deception attacks and their security breach.

Table 1. Online social deception attacks and their security breach

Social TABLE 1. Online social deception attacks and their security breach **Deception Attack**	**Security Breach**
Phishing	Account Confidentiality
Spamming	Account Confidentiality
Fake Profile	Integrity
Crowdturfing	Data Integrity, Account Integrity
Human trafficking	Safety, Confidentiality
Cyberbullying	Safety, Confidentiality
Profile Cloning	Authentication

4. Online Social Deception Prevention Technques

Social deception through online platforms can be prevented through following methods:

4.1 Prevention of fake news

In order to fight against fake news, a system based on blockchain can be used which records a blockchain transaction when a news article is posted, and authentication consensus of the record is applied[19].An authentication indicator measures the result along with the news post. The authentication indicator related to the post is shown as status verification whenever a user sees a post, the status can be successful, pending or failed. Through this method, fake prevention can be done by ensuring whether the post is trustworthy or not after determining the news authenticity by user's consensus. In addition to this, a malicious user can be traced out from the record of transaction along with deleting those posts which are false and imposing a penalty on such fake news attackers.

4.2 Prevention of Identity Theft

A very promising method of identity deception has been discussed using social network data [20].In order to establish a community's behavioral profile, data of common contribution networks is used. Those accounts which are malicious can be removed before a community is joined which is based on user behavior deviation from the community profile.

4.3 Prevention of Cyberbullying

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

A user interface which is reflective has been proposed by one of the researchers

,this dashboard interface works well for both the victims and cyberbullying attackers in the social network platforms[21].The interface has features like action delay ,integration notification as well as interactive education, it turns out to be very effective for the end user category.

4.4 Social Honeypots

In order to ensure that attackers are not able to access network/system resource, social honeypots can be utilized to detect different types of online social network attacks. Social honeypots are basically used for intrusion prevention, but they can also be used as a detection tool to work against online social deception

attacks.Fake identities of celebrities as well as common people are being used to set social honeypots for behavior analysis such as friend requests, number of friends as well as secret and public messages. Many techniques of deception have been discussed for detecting sophisticated attackers[22].

5. Ethical Issues related to Online Social Deception Research

During the conduct of social deception research, issues related to privacy may come up like fake profile creation, setting up of social honeypots as well as data collection from these types of accounts and user behavior capturing. It has been proposed to share datasets in public , therefore the researchers can avoid using methods related to any ethical issues which comes up during data collection[23].Using the publicly available data sets, many researchers can use it while conducting their research.

In many research papers, ethical issued related to online social deception have been discussed very well[24][25]. The researchers in these papers have discussed that it is safe for normal users if the legitimate users are not involved in any of the malicious activities. But the normal users can be indirectly influenced by social honeypots.

While conducting research in this area, one category of people thinks that research in social deception is related to privacy as an ethical issue, on the other hand, there is also another category of people who advocates this kind of research since it comes out to be helpful in safeguarding people who are vulnerable to online social deception.Therefore, they think that conducting online social deception research has relation to ethical and unethical issues. It has also been claimed by some of the researchers that fake accounts creation as social honeypots are basically for spammers and it is not related to taking advantage from legitimate users as well as buying accounts which are compromised[26][27].But it is still not clear that creation of fake accounts as social honeypots is harmful for legitimate users or not. Some of the researchers have also discussed the guidelines for protection as well as control of unethical behaviors like violation of privacy as prevention from risks from using methods of crowdsourcing[28].

6. Conclusion and Future Work

In this paper, I have discussed the fundamental meaning of social deception. Its basic purpose is to deceive the decievee by enhancing his misbelief and confusion. A deceiver can find it successful only when he gets full cooperation from the decievee and he performs actions based on the instructions provided by the deceiver. Online social deception has observed new emerging threats like human trafficking and cyberbullying which are very bad for our society. Prevention methods of online social deception are limited, and we need to think and develop

more preventive measures.We need to consider online social deception research approaches in a multidisciplinary way,since both the deceiver as well as the deceivers are human beings, who communicate through online platforms.

If we are able to figure out the way both deceiver and deceive communicates with each other then only we can think of detecting online social deception. A multidisciplinary effort is needed for the development of effective measures against online social deception attacks. People who participate in the online activities need to be made aware about different attacks which fall into the category of online deception and that they can be careful while doing anything on the online platform. As we lack effective datasets and deception cures, so it becomes a challenging task to defend human targeted attacks like human trafficking and cyberbullying.

We need to work upon such a defense system which is integrated in terms of measuring prevention, detection as well as mitigation of false information distribution and spread..

References

[1] L. Rainie,American’s Complicated Feelings About Social Media in an Ear of Privacy Concerns,available: https://pewrsr.ch/2pJczTZ(2018).

[2] J. Anderson and J. Cho, ‘‘Software defined network based virtual machine placement in cloud systems,’’ in Proc. IEEE Mil. Commun. Conf. (MIL- COM),pp. 876–881(2017).

[3] R. J. Reinhart,One in Four Americans Have Experienced Cyber- crime,available:https:// news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx(2018).

[4] S. G. A. van de Weijer, R. Leukfeldt, and W. Bernasco, ‘‘Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking,’’ Eur. J.Criminol., vol. 16, no. 4, pp. 486–508,(2019).

[5] Esma Aïmeur1, Hicham Hage2, Sabrine Amri1,” The Scourge of Online Deception in Social

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Networks",International Conference on Computational Science and Computation-al Intelligence (CSCI)(2018).

[6] P. R. Badri Satya, K. Lee, D. Lee, T. Tran, and J. J. Zhang, ''Uncovering fake likers in online social networks,'' in Proc. 25th ACM Int. Conf. Inf. Knowl. Manage.,pp. 2365– 2370(2016).

[7] M. Forelle, P. Howard, A. Monroy-Hernández, and S. Savage,''Politi- cal bots and the manipulation of public opinion in Venezuela,'', available:http://arxiv.org/abs/ 1507.07109 (2015).

[8] Michail Tsikerdekis Western Washington University Sherali Zeadally University of Kentucky," Detecting Online Content Deception"(2020).

[9] Podhradsky, A., D'Ovidio, R., Engebretson, P., and Casey, C. Xbox 360 hoaxes, social engineering, and gamertag exploits. In Proceedings of the 46th Annual Hawaii International Conference on Systems Sciences (Maui, HI, Jan. 710). IEEE, New York, 32393250(2013).

[10] Sandia National Laboratories, High-Fidelity Adaptive Deception & Emulation System (HADES), https://ip.sandia.gov/technology.do/techID=187.

[11] S. Jiang and C. Wilson, ''Linguistic signals under misinformation and fact-checking: Evidence from user comments on social media,'' in Proc. ACM Hum.-Comput. Interact. (CSCW), vol. 2, pp. 1– 23(2018).

[12] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, ''Social network security: Issues, challenges, threats, and solutions,'' Inf. Sci., vol. 421, pp. 43– 69(2017).

[13] K. Lee, P. Tamilarasan, and J. Caverlee, ''Crowdturfers, campaigns, and social media: Tracking and revealing crowdsourced manipulation of social media,'' in Proc. 7th Int. AAAI Conf. Weblogs Social Media,pp. 331–340(2013).

[14] G. Wang, T. Wang, H. Zheng, and B. Y. Zhao, ''Man vs. machine: Practical adversarial detection of malicious crowdsourcing work- ers,'' in Proc. 23rd USENIX Secur. Symp. (USENIX Security), pp. 239–254(2014).

[15] A. N. Doane, S. Ehlke, and M. L. Kelley, ''Bystanders against cyberbul- lying: A video program for college students,'' Int. J. Bullying Prevention, vol. 2, no. 1, pp. 41– 52(2020).

[16] V. Greiman and C. Bain, ''The emergence of cyber activity as a gateway to human trafficking,'' J. Inf. Warfare, vol. 12, no. 2, pp. 41–49(2013).

[17] M. Latonero, ''Human trafficking online: The role of social net- working sites and online classifieds,'' SSRN, Tech. Rep., doi: 10.2139/ssrn.2045851(2011).

[18] P. Zambrano, J. Torres, L. Tello-Oquendo, R. Jácome, M. E. Benalcázar,R. Andrade, and W. Fuertes, ''Technical mapping of the grooming anatomy using machine learning paradigms: An information security approach,'' IEEE Access, vol. 7, pp. 142129–142146 (2019).

[19] M. Saad, A. Ahmad, and A. Mohaisen, ''Fighting fake news propagation with blockchains,'' in Proc. IEEE Conf. Commun. Netw. Secur. (CNS),pp. 1– 4(2019).

[20] M. Tsikerdekis, ''Identity deception prevention using common contribu- tion network data,'' IEEE Trans. Inf. Forensics Security, vol. 12, no. 1, pp. 188–199(2017).

[21] K. Dinakar, B. Jones, C. Havasi, H. Lieberman, and R. Picard, ''Common sense reasoning for detection, prevention, and mitigation of cyberbully- ing,'' ACM Trans. Interact. Intell. Syst., vol. 2, no. 3, pp. 1–30(2012).

[22] N. Virvilis, B. Vanautgaerden, and O. S. Serrano, ''Changing the game: The art of deceiving sophisticated attackers,'' in Proc. 6th Int. Conf. Cyber Conflict (CyCon),pp. 87–97(2014).

[23] Y. Elovici, M. Fire, A. Herzberg, and H. Shulman, ''Ethical considerations when employing fake identities in online social networks for research,'' Sci. Eng. Ethics, vol. 20, no. 4, pp. 1027– 1043(2014).

[24] A. Paradise, A. Shabtai, R. Puzis, A. Elyashar, Y. Elovici, M. Roshandel, and C. Peylo, ''Creation and management of social network honeypots for detecting targeted cyber-attacks,'' IEEE Trans. Comput. Social Syst., vol. 4, no. 3, pp. 65– 79(2017).

[25] C. Yang, J. Zhang, and G. Gu, ''A taste of tweets: Reverse engineering Twitter spammers,'' in Proc. 30th Annu. Comput. Secur. Appl. Conf.,pp. 86– 95(2014).

[26] G. A. Kamhoua, N. Pissinou, S. S. Iyengar, J. Beltran, C. Kamhoua,B. L. Hernandez,L. Njilla, and A. P. Makki, ''Preventing colluding iden- tity clone attacks in online social networks,'' in Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW), pp. 187–192(2017).

[27] H. Zhu, ''Fighting against social spammers on Twitter by using active honeypots,'' Ph.D. dissertation, Dept. Elect. Comput. Eng., McGill Univ. Libraries, Montreal, QC, Canada(2015).

[28] A. Onuchowska and G.-J. de Vreede, ''Disruption and deception in crowdsourcing: Towards a

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

crowdsourcing risk framework,'' AIS eLibrary, Tech. Rep.(2018).

[29] Tsikerdekis, Michail and Zeadally, Sherali, "Online Deception in Social Media", Information Science Faculty Publications(2014)

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731