GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES

UNDERSTANDING SOCIAL ENGINEERING THREATS IN MASSIVELY MULTIPLAYER ONLINE ROLE-PLAYING GAMES: AN ISSUE REVIEW

Saroja Roy Grandhi, Nikhil Chopra Galimotu

MPhil Clinical Psychology, Amity Institute of Behavioural and Allied Sciences,
Amity University, Gwalior, Madhya Pradesh
sarojaroy.grandhi@gmail.com

M.Sc. Forensic Psychology, Institute of Behavioural Sciences,
Gujarat Forensic Sciences University, Gandhinagar, Gujarat
choprans3@gmail.com

Abstract

In this developing virtual era, the recreational activities like online games have turned into very intriguing tasks by giving whole new identities and avatars to individuals. This allows the individual to interact and also do anything that seemed possible as well as impossible in real lives. This virtual identification sometimes crosses into the real world, as they allow gamers to sell virtual game items for real-world money in markets and sometimes even requires use of real money to create or purchase personal property in their online world. This has created an opportunity for virtual crimes involving social and technical risks. The widespread adoptions of such Massively Multiplayer Online Role-Playing Games (MMORPGs) have not only become a dedicated activity for gamers but also act as a platform for social engineers. Social Engineering is considered as an art of collecting sensitive data/information by persuasion or manipulation of individuals and is the first step involving social risk in virtual crimes. MMORPGs were found to be highly socially interactive environments providing the opportunity to not only form relationships but also to be targeted by social engineers. In this study, we are reviewing and evaluating social interactions and psychological factors of MMORPG gamers which are making them vulnerable to social engineering threats. Various studies have assessed the psychological factors making an individual vulnerable to social engineering on social network interactions and also few studies have analysed the behaviours and relationships of gamers in online interactions. Observing such factors, in this study we analysed how the social engineers, disguised as fellow gamer, would target similar psychological vulnerabilities in the gamers by using social interaction platform on MMORPGs to gather personal and sensitive data from the targeted gamers.

Keywords: *Virtual crime, Massively Multiplayer Online Role-Playing Games, Social Engineering, Social Interaction.*

1. INTRODUCTION

Affordable high bandwidth internet connections have made lives easier, informative and entertaining in many ways along with the way video games are played, allowing a greater number of players from around the globe to connect and play[1]. Online gaming is such an activity which is the latest reiteration of the well conventional leisure occupation of video or computer gaming. It has turned into a noteworthy global phenomenon, with estimations that there are more than 217 million online gamers globally [2]. This has resulted in creation of a number of video game genres that can be played online. One of the most prevalent genres is playing of Massively Multi-player Online Role-Playing Games (MMORPGs) such as *Pub-G*, MMORPGs are complexly-developed, huge, virtual environments or worlds where masses of users interact with each other using avatars that they create inside the game on a daily basis. MMORPGs were found to be extremely socially interactive environments/platforms providing the opportunity to create strong social connections, friendships and emotional relationships [3]. Especially in MMORPGs, there has also been a significant growth in online-gaming related crimes majorly involving theft and fraud with online cheating being the most notable criminal behaviour [4]. Although, this criminal behaviour included fraud by various methods like collusion, abusing policies, exploiting bugs, misusing etc., for different targets such as gaining unauthorized access to software/game, stealing virtual properties which can be converted to real-world valued possessions etc., social engineering frauds were observed in more than 26% of cases [5].

Social Engineering, today, is one of the principal threats and considered as the entry point for most of the significant online attacks [6]. It is type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud

scheme[7]. In cyber-security, social engineering means the manipulation of individuals with intent to persuade them to carry out explicit tasks or to reveal information that can be used by an attacker. Social engineering, itself, does not necessarily involve a great amount of technical knowledge to be successful. Instead, social engineering targets on various aspects of human psychology such as gullibility, empathy, curiosity, courtesy, greed, etc [8].

Social Engineering threats or attacks in MMORPGs, in specific, is a very understudied topic. As, with large number of users or gamers on MMORPGs, that allow innovative forms of social identity and social interaction appealing to both adults and teenagers from a wide range of backgrounds, leading them to spend, on average, more than half of a working week, it became a platform of huge scope for social engineers. Research into MMORPGs has specified that the most significant reasons for engaging in such games are social i.e., to play and meet other like-minded people [1]. Being highly interactive platforms with involved and dedicated gamers, MMORPGs have attracted social engineers to get to work targeting vulnerable gamers by using different persuasion techniques for stealing virtual properties, collecting sensible information, fraudulent transactions, gaining unauthorised accesses etc.

1.1. Rationale of the Study

The focus of this study is to investigate or explore into the social engineering threats in MMORPGs by reviewing different types of aspects involved in social engineering which could be applied or used by social engineers in MMORPGs. Social interactions in MMORPGs, being one of the vital characteristics of the game design, opened up opportunity for social engineers to get into action by various attacking methods and persuasion techniques by just interacting with the players. There are no specific researches or studies on how social engineers go about in their attacks in social interactions on MMORPG platforms which can educate or create understanding in the players who mostly happen to be teenagers and adolescents, making vulnerable targets or victims.

1.2. Research Methodology

To investigate the research issue and to search for relevant studies, firstly, we have selected top notch information security, social psychology and gaming related journals. We searched for the keywords in sources such as “Social Engineering in Online Gaming,” “Vulnerability to Social Engineering,” “Impact of Massively Multi-player Online Role-Playing Games,” “Social Interactions in Massively Multi-player Online Role-Playing Games,” “Security threats in Massively Multi-player Online Role-Playing Games,” etc. All primary research studies in the English language were taken into consideration. However, studies were obligatory to have a minimum of further features in order to be included in the review. First of all, the studies had to clearly indicate social engineering attack analysis, vulnerabilities to social engineering, impacts of MMORPGs and interactions in MMORPGs was the subject of the exploration /investigation. It was very common to go through articles that looked at “social engineering” and “gaming” in general, but from which it was not possible to identify if social engineering in online gaming and MMORPGs was an element of the study. As there was not very notable literature available specifically on social engineering in MMORPGs, studies on social engineering in online social interactions, vulnerabilities to social engineering and attack scenarios, MMORPG impacts and social interactions in MMORPGs were selected for further analysing and reviewing in this paper.

2. LITERATURE REVIEW

Social Engineering vulnerabilities are as such considered and observed as a base for the cyber influential crimes, which in these current days have taken many forms to it. Evidentiary basis of this significant effect with reference to the primary studies and meta-analytic studies are yet to prove the fact that the involvement of psychological understanding and focusing on the causes for these vulnerabilities require an in-depth observation into it. Many studies have supported and tried to introduce the concept of social engineering in multiple ways, but limiting the wide online platform to gaming interaction and online gaming behaviour has formed the basis for this study’s objective.

Social Engineering was considered as a sensitive approach to gather information related to human interactions in the study done by Lohani.S. Focusing on to the Cyber Security approach he has explained the types, effects of social engineering and introduced to the preventive measures that one could follow. With strong connection points to the idea of social engineering as a way of hacking into humans, this comprehensive research study has related the psychological aspects of curiosity, courtesy, gullibility, empathy and greed to identify the vulnerabilities of a human to the attacks of social engineering. [8]

Though many researchers have studied the social engineering vulnerabilities on social media the focus to identify the predictors of victimization came into light with the study of A.Vishwanath who studied and investigated the user’s vulnerabilities on social media for such attacks have concluded that the user’s frequency of usage, lack of control over usage related behaviour and trying to maintain the online relationships have been focused to profiled to identify the victims vulnerabilities. [9]

Influenced by the similar work, Samar Abladli and Georrge R.S.Weir's had tried to work more on understanding the vulnerabilities of social engineering by giving a new perspective to the research by exploring more on why people fall victim to such attacks and studied the behavioural approach by proposing a user-centric framework to understand the user's susceptibility, relevant factors and dimensions of social engineering. The user centric framework developed in the study distribute its attributes across four dimensions that are Socio-psychological variables (Personality traits like openness, agreeableness and extroversion, demographics like age, gender, and education and the culture), Perceptual variables which are explained with the help of Workman, Bommer & Straub's protection motivation theory that suggested four cognitive approaches to evaluate the risks and vulnerabilities [10], in forms of (Perceived risk of social networking, Past experiences with social network, Perceived severity & likelihood of negative consequences, Privacy & Security awareness and Self-efficacy), Habitual variables describes the levels of engagement which classified the users as high or less active users based on many variables such as number of friends, number of subscribed groups, status level and frequency of use. The social emotional variables like fear, hedonism, anxiety and trust playing the major role in it [11].

Proving the framework from the previous study, Abadli.S & Weir.R.S., used the factors identify and predict the individual characteristics that have influence over the vulnerabilities of a user. To address this the researchers have hypothesized that the users' level of motivation plays an important role in influencing the trust, level of involvement and the users' experiences with cyber-crimes. This also helped in developing a structural model with the identified risks factors as the considered targets in developing training and awareness programs on social engineering. The conclusion suggests that, though the characteristics have had a direct or indirect effect, Trust variable of all the factors showed a significant higher relation in predicting the individual's vulnerabilities in social networks. [12]

Shifting the focus from vulnerabilities in social networking to online gaming, many researchers have focused on what it is likely to be a part of any online game. Such behaviours and interactions of the Massively Multiplayer Online Role-Playing Games (MMORPGs) are recorded worldwide to be involved in cases like theft of Personal Identifiable Information (PII), impersonating and stealing identity for financial gains have become more famous with the incidents like that of security breech in the widely played online game Fortnite. Many such incidents have led to numerous criminal charges and developing risk behaviours in the players and also victimizing many other vulnerable players to such actions.

Developing such understanding towards online gaming securities George Yee et.al, have tried to characterize the online games security in a much more efficient and understanding way in their study by examining securing the MMORPGs to their potential threats and by giving counter measures in order to protect the game and gamers from crime that involved social engineering. They have explained the characteristics of a MMORPGs distributed into five major factors which focuses its security in terms of the Network connection, Player Authentication, Game Objectives, Number of players and the mode of payments that are being used. Restricting the area of focus have actually led them to identify the risk-oriented measures and also helped in developing counter threats protocols. [5]

The advancements in computers and internet have brought into light the new focus that is understanding role of computers in human behaviour where researchers have recently shifted their focus to the behaviours of MMORPGs as a general online behaviour. The idea of active interaction that an individual developed in the form of online avatars has become their new identities. Seung-bae Park and Namho Chung have studied this effect in there paper where they used a native approach to identify the self representation on online platforms in the forms of self-presentation theory and social identity theory. The gamers behaviour was studied on the basis of commitment and trust towards the participants of game and to the game itself. As trust was also seen as the factor of vulnerability in the social networking properties, this study has hypothesized and signified its effects in online gamers found to be exclusive for the commitment that an individual develops towards any MMORPGs. Other than identifying the significant nature of the commitment of gamers, the study also indicated that MMORPGs are not simply games, but are online communities where people express themselves and communicate with others. [13]

Though many researchers have identified the feature of social interaction as a part of the massively multiplayer online role-playing games, no study particularly looked into the type and form of interactions that were happening between the gamers. The study by Helena Cole and Mark Griffiths has targeted such interactions between the gamers where they highlighted the features like the strong bonded friendships and emotional relationships. With much of these interactions being the reason for building positive attributes they have also seen the potential of the harmful effects such as self-esteem, social inadequacy, and social anxieties. The potential of such interactions was discussed in the forms of attraction to other players, playing MMORPGs with real life friends and family, effect on relationships, online vs. offline friends, issues discussed online friends and

severity of it and such significant factors. Even though many modes of interactions have appeared to be similar in comparison to males and females, the discussion of issues with online friends was the major factor that was seen more significant in females than males. [3]

3. ANALYSIS OF SOCIAL ENGINEERING IN MMORPGs

Human beings are considered to be the weakest link in the information and cyber security domain [6]. The possible explanation to that could be that humans trust and share personal information with each other rather quickly by socialising. Online games seem to play a role in the socialization of heavy game players, predominantly for those who play MMORPGs. MMORPGs encourage social-group interactions and involvement, mastery, and flexibility, resulting in substantial friendships and personal empowerment [3]. But to what extent these interactions are being safe without victimising the players to be targeted by social engineers is in question. We analysed the predictable vulnerabilities like behavioural factors, types of attacks that are used by the social engineers in MMORPGs and theory explaining the attack scenario in MMORPG spaces.

3.1. Vulnerabilities to Social Engineering in MMORPG players

Several vulnerable behaviours in humans make them fall prey for social engineering attacks. Researches have given various behavioural factors in MMORPG players which fall under the vulnerable behaviours to social engineering.

i. Involvement – People highly involved in a service tend to be relaxed and ignore cues associated with deception or fraud [12]. It can be measured by time spent on that particular service. Gaming has shown elements of compulsive and addictive behaviours, and finding it hard to resist. On MMORPGs, some players spend more than 25 hours a week, making them extremely involved [3].
ii. Commitment – When people set an aim or task for themselves, they are most likely to complete it as they take it on their self-image if not, ignoring and kind of risks [6,11]. The MMORPG players have high self-presentation desires which resulted in high interactivity and commitment to the MMORPG spaces in them [13].
iii. Trust – Humans tend to trust others easily. Social engineers first build trust and make their targets/victims do desired tasks to gain access to information [6,11,12]. Trust of game spaces and other gamers is high in MMORPG players [13].
iv. Reciprocation – In some social engineering attacks, the perpetrators offer something to the victim or target enticing them to perform what they ask for, relying on reciprocation [6,11]. MMORPG players tend to reciprocate virtual gifts as well as feelings which leads them to fall prey to social engineers.
v. Friendship – Humans have tendency to perform or do actions in favour of friends. Social engineers use this to their advantage [6]. 75% of MMPRPG players reported to have made good friends on MMORPG spaces [3]. Social engineers could be posing themselves as fellow player and start a friendly relationship with the players.

3.2. Social Engineering attacks used in MMORPG spaces

Social Engineers use various kinds of attacks like phishing, vishing, smishing, impersonation, baiting, pretexting etc [6,8]. On MMORPGs, the perpetrators, using social engineering, might want to-

i. capture your personal information,
ii. steal your identity,
iii. steal credit card information and,
iv. inappropriately contact children by pretending to be another child, setting up meetings, or tricking them into revealing personal information. [14]

To achieve the above mentioned, the attacks mostly used by social engineers are phishing and impersonation. In Phishing, the perpetrator sends the target a malware or fake page links. The targets, if install the malware or enter personal information on fake page links thinking them to be original, will either unknowingly give their system's control to the perpetrator or reveal personal information [6,8,14]. The malwares, once installed, will give total control of the victim's system to the perpetrator where he/she can monitor the victim's activities, launch attacks against other systems and even steal information from the system. The fake page links can be login pages or any personal/sensitive information seeking pages which might look exactly like the original pages, but actually are clone pages, which will send the information the victim entered to the perpetrator.
Impersonation is used by some social engineers on MMORPGs. They disguise themselves as a fellow player, built up trust and friendship, tricking the victim to reveal personal information or asking do some favours, sometimes payments for them and stealing credit/debit cards details.

3.3. Theory used in Social Engineering scenario in MMOPRG spaces

Routine Activity Theory is one the theories explaining social engineering [6], where the crime or attack is expected to occur, when –

- a motivated offender is present,

- an attractive and vulnerable target is available, and
- no guardianship is present.

This theory has been extensively cited and applied in criminology and forensic psychology studies. In understanding the perpetrators in MMORPG spaces to commit a social engineering crime, this theory clearly establishes the attack scenario.

i. According to the theory, motivated offenders are the individuals who are willing to commit the crime, besides being capable of doing so [15]. In MMORPG spaces, the perpetrators are motivated to persuade or manipulate the victims to gain unauthorised access, steal information etc., along with good skills of impersonation and phishing.

ii. MMORPGs has large number of masses from around the globe who are very much involved and committed to those spaces along with possessing other behaviours and psychological factors which make them vulnerable targets. Also, most of the players on these spaces being adolescents and young adults [2], who are still inexperienced about deception perception, makes them more attractive targets.

iii. MMORPGs are mostly played by single person using one system. Continuous play for prolonged time leaves them unsupervised and isolated. Even the perpetrators, usually, implement such attacks from their own systems using dark web disabling any supervision. This helps the crime or attack to take place without any obstacle.

4. CONCLUSION AND FUTURE WORK

Today's world of living in virtual environment has brought human interactions, work, entertainment, commerce and almost every possible activity to the comfort of our computers and homes with high definition experiences. This has revolutionised the gaming experience too by allowing us to present ourselves in a completely different way in an intriguing virtual environment where we can play and interact with people from all around the globe. Though, these all experiences seem so exiting, they even opened up an opportunity for cyber-crime perpetrators to commit crimes at the comfort of their homes. Virtual/cyber world, being vast and almost accessed by most of the people sharing or saving their information, offered space for the perpetrators to create a dark web space to be hidden too. But just like real world, being aware and having risk-perception can avoid ones from being targeted or falling prey to the perpetrators. Notably, the adolescents and young adults who tend to spend most time on virtual spaces and online gaming should be educated about the risks and made aware about the extent to be involved in social interactions.

Future Work: The personalities of individuals involved in social network interactions and MMORPG interactions can be different due to the characteristics of services provided in social networks and MMORPGs. And, the involvement of gamers is quite different from that of social butterflies, but yet that doesn't reduce their risk of being targeted due to their tendency to shut themselves off from real world and indulging in virtual spaces extensively. Empirical researches focusing of how the gamers can fall prey to social engineering due to confined virtual interactions and relationships must be encouraged.

REFERENCES

[1] Ghuman, D., & Griffiths, M. (2012). A cross-genre study of online gaming: Player demographics, motivation for play, and social interactions among players. International Journal of Cyber Behavior, Psychology and Learning (IJCBPL), 2(1), 13-29.

[2] Porter-Armstrong, A. P. (2013). Impact of multiplayer online role-playing games upon the psychosocial well-being of adolescents and young adults: Reviewing the evidence. Psychiatry Journal, 2013.

[3] Cole, H., & Griffiths, M. D. (2007). Social interactions in massively multiplayer online role-playing gamers. Cyberpsychology & behavior, 10(4), 575-583.

[4] Chen, Y. C., Hwang, J. J., Song, R., Yee, G., & Korba, L. (2005, April). Online gaming cheating and security issue. In International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume II (Vol. 1, pp. 518-523). IEEE.

[5] Yee, G., Korba, L., Song, R., & Chen, Y. C. (2006, April). Towards designing secure online games. In 20th International Conference on Advanced Information Networking and Applications-Volume 1 (AINA'06) (Vol. 2, pp. 44-48). IEEE.

[6] Yasin, A., Fatima, R., Liu, L., Yasin, A., & Wang, J. (2019). Contemplating social engineering studies and attack scenarios: A review study. Security and Privacy, 2(4), e73.

[7] Anderson, Ross J. *(2008).* Security engineering: a guide to building dependable distributed systems *(2nd ed.). Indianapolis, IN: Wiley. p. 1040.* ISBN 978-0-470-06852-6. Chapter 2, page 17

[8] Lohani, S. (2019). Social Engineering: Hacking into Humans. International Journal of Advanced Studies of Scientific Research, 4(1).

[9] Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. Journal of Computer-Mediated Communication, 20(1), 83-98.

[10] Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in human behavior, 24(6), 2799-2816.
[11] Albladi, S., & Weir, G. R. (2016, June). Vulnerability to social engineering in social networks: a proposed user-centric framework. In 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF) (pp. 1-6). IEEE.
[12] Albladi, S. M., & Weir, G. R. (2020). Predicting individuals' vulnerability to social engineering in social networks. Cybersecurity, 3(1), 1-19.
[13] Park, S. B., & Chung, N. (2011). Mediating roles of self-presentation desire in online game community commitment and trust behavior of Massive Multiplayer Online Role-Playing Games. Computers in Human Behavior, 27(6), 2372-2379.
[14] HAYES, E. J. (2006). Playing it safe: Avoiding online gaming risks. Retrieved from.
[15] Felson, Marcus; Cohen, Lawrence E. (1980). "Human Ecology and Crime: A routine Activity Approach". Human Ecology. 8 (4): 389-406.