AL-HIKMAH RESEARCH & PUBLICATION CENTER

Al-Hikmah International Journal of Islamic Studies and Human Sciences
Volume 4, Issue 1, January 2021
e-ISSN: 2637-0581
DOI: 10.46722/hkmh.4.1.21c
https://doi.org/10.46722/hkmh.4.1.21c

Social Media Impersonation in the Virtual World

Mohammed A Gharawi

Multi Media University, Kuala Lumpur, Malaysia

Ahmed Badawy

Corresponding Author: badawyahmed2025@gmail.com

University of Malaya, Kuala Lumpur, Malaysia

Doaa Elsayed Ramadan

Airlangga University, Surabaya, Indonesia

Shaymaa Elsayed

TOGO Digital Ltd, Dubai, UAE

Abstract

Introduction: Social media is becoming a critical part of everyone's life. Social media has numerous platforms including Facebook, Twitter, Instagram, and LinkedIn. Impersonation is a common phenomenon found nearly on all social media platforms; it is the act of attempting to deceive someone by pretending that he is another person. Impersonators always try to hide a real account by making another similar profile to spread the fake contents on social media platforms making it very difficult to know the real accounts from the fake ones. Aims: This paper aims to write a comprehensive review on the social media impersonation, impersonation types, how to identify the social media impersonation, cases of social media impersonation, how to prevent impersonation, and how to protect the security of a social media user. Besides, the article explains the position of Islam toward impersonations including social media impersonation. Method: This is a narrative review of the existed literature review on the social media impersonation in the virtual world. Con-

clusion: Social media impersonation is the act of pretending that a person is another person which usually occurs on all social media platforms.

Keywords: Social media, Impersonation, Platforms, Virtual, Media

Introduction

Recently, social media has become a very important part of people's life worldwide. The various social media platforms have an obvious effect on people's daily life affecting their structures, routines, rules, regimes, and social interactions such as business networks and friendship relations (De, Bogart, & Collins, 2012). Social media is defined as a group of internet-based applications built on technological and ideological web foundations to provide the opportunity to create and exchange contents between the geographically separated users (Kaplan & Haenlein, 2011).

Social media is considered an outstanding innovation in communication which caused a true revolution to institutions including government authorities and mass media. Social media owns a variety of online platforms such as Twitter, LinkedIn, Facebook, and Instagram which are growing very fast leading to a huge distribution of news and information (Van Dijck & Poell, 2013). A social media user can have a profile page that provides other users with his own information giving the opportunity of easier and simpler communication. A user profile can include information about the user's acquaintance relationships including colleagues, friends, relatives, and schoolmates on the social networks (De et al. , 2012).

Impersonation is a common phenomenon found nearly on all social media platforms especially on Instagram. It plays a vital role in content production and propagation on online social networks (Zarei, Farahbakhsh, & Crespi, 2019). Impersonation is the act of attempting to deceive someone by pretending that he is another person.

A social media user can assume the real identity of another user by creating a profile content that identifies the impersonated user. Impersonators always try to disguise a real account by making similar profile and spreading an in genuine content on the social media that makes it very difficult to differentiate genuine posts from the fake ones on social media networks (Zarei, Farahbakhsh, Crespi, & Tyson, 2020).

Such impersonators have the ability to be found on all main social media platforms which are utilized by numerous numbers of businessmen, public figures, influencers, celebrities with various popularity levels. They usually put obvious stable plans in which they create

untrustworthy contents, generate fake engagements, perform brand abuses, and make accounts more famous than they are (Zarei, Farahbakhsh, & Crespi, 2020).

Despite the existence of a wide range of literature on social media impersonation, there are not many articles explaining the whole aspects of social media impersonation as every article discusses a specific idea related to social media impersonation. Besides, there are very limited literature on the Islam position towards social media impersonation. That's why, the authors tried to write a comprehensive review on all aspects related to social media impersonation concept, impersonation types, how to identify the social media impersonation, cases of social media impersonation, how to prevent impersonation, and how to protect the security of a social media user. Besides, the authors discussed the position of Islam toward impersonations including social media impersonation.

Literature Review

Online social media has reformed human social interactions in a manner that eliminates obstacles that historically hold strangers apart (Kambellari, 2017). Social media also plays an important role in different sectors such as economic, social, and political sectors. It is critical in shaping people's awareness during the difficult times such as COVID-19 pandemic as it helped a lot to contain the situation (Badawy, Gharawi, Bidin, & Khamis). In addition, social media has a great effect on education, including language learners by facilitating continuous and direct interactions between users which improve the capability of learning as in case of Arabic language learners. This promotes the learning and teaching skills and enforces the language vocabulary and materials (Gharawi & Bidin, 2016).

Social media always faces impersonation. Impersonation is an action of creating fake social media accounts that are similar to other's legitimate accounts (Nuakoh & Anwar, 2018). Social media impersonation may occur in two different ways; either by creating a totally in genuine social media account or by stealing another person's personal information to be able to have an easy access to his social media profile (Reznik, 2012).

The fake social media account can describe details that belongs to someone else or is entirely fictional. This versatility in assuming one's virtual identity is because of the privacy that people would enjoy in the social media world. Inability to establish adequate detection methods for the internet users is one of the main obstacles in combating and investigating crimes related to social media platforms (Hoffmeister, 2014).

Impersonators are defined as the people who are responsible for the occurrence of this undesired behavior and who create accounts pretending to be a famous person or a repre-

sentative of a well-known company, brand or an institution (Kambellari, 2017). It has been also stated that an impersonator is a person who builds a profile using the same personal information of another legitimate account and copies the actions and behaviors of that account owner (Zarei, Farahbakhsh, & Crespi, 2020).

Impersonators exist on social media websites for the intent of defrauding, bullying, harassing, or damaging another person (Kambellari, 2017). Because social media is a virtual world, a social media user can introduce himself in various personalities and many other people may introduce themselves with the same online personality (Van Dijck & Poell, 2013).

Impersonators are divided into two main types including fan impersonators and bot impersonators. Bot accounts refer to the public fraudulent accounts or social bots which appear to imitate the individual person, and typically produce the basic contents. These bots are typically easy and simple accounts using the default settings of Instagram such as; no biography, no full name, and sometimes no profile pictures. In these bots, the followers count is low, but they follow a large number of other accounts. From a similarity point of view, these bots have got poor profile similarity degree represented into low similarity in username, full name, and biography. There are no similar profile photos as well. From an activity point of view, these bots receive extremely limited engagements such as a comment or a like per post. In addition, they are lazy in publishing stories, interested in making feedbacks and interested in duplicating comments (Ferrara, Varol, Davis, Menczer, & Flammini, 2016).

In addition, fan impersonator is a semi-human-operated account which is generated and managed by a devotee or a fan. Actually, fans have more supporters than bots, and they are absolutely public accounts having a biography and using a URL. From the perspective of impersonation, the fans have higher profile similarity in profile photo, username, full name, and biography. From a behavioral point of view, fans are more efficient than the bots publishing posts and tales, receive a higher degree of participation in their posts such as a comment or a like per post and the owner never shares his self-generated content. From controlling point of view which manages the pages, fan pages are divided into two outstanding types. The first type is controlled, governed and published by a human. The second type is controlled by a human and a bot. In this type, the page owner is a person and automation and bot systems are used as well (Zarei, Farahbakhsh, Crespi, et al. , 2020).

The United states with other countries undertook several laws and regulations which considered social media impersonation is a crime. These laws include assuming a fake identity in order to defraud another person or to claim to be a representative of another person, in-

stitution, brand or agency. Impersonation may be also motivated politically (Zarei et al. , 2019). The influence of impersonation on social media platforms such as Facebook and Twitter can be undergirded by expectations of legitimacy. Impersonation identification helps to develop methods for automated detection which -in turn- affects social media companies positively (R. Page, 2014).

There are many methods, techniques, systems, and mechanisms for identifying social media impersonation of a user's profile page. Generally, impersonation can be observed by matching the elements of the impersonator's profile page including images, fields, and details with the elements of the victim's profile page. Such a contrast could offer indications that the profile page of the alleged impersonator is likely to represent the profile page of the alleged victim (De et al. , 2012). The first page of user profile is possibly the second user profile page. The user profile retrieval portion is used to recover the first information associated with the first user profile page and second information associated with the second user profile page on social media (R. Page, 2014).

A comparison module is done to compare the first information and the second information to identify impersonation indicators leading to identifying similarities of elements on the first user profile page and corresponding elements on the second user profile page. In addition, there is impersonation analysis component which is used to determine that the first page of user profile is likely impersonating the second page of user profile on the different social media networks based upon the identified indicators of impersonation (Li & Han, 2013). Social media impersonation can be also detected by observing the indicators of impersonation and the indicators that there is not any impersonation as concluded from analyzing and comparing the profiles of the impersonator and the victim. Different models can be used to determine the likelihood of social media impersonation; whether impersonation is probable, impersonation is certain, or impersonation is taking place (De, Bogart, & Collins, 2013).

There are different cases of impersonation occurred on social media platforms such as Twitter, Facebook, and Instagram. The first case is that a woman in New Jersey was accused for creating a fake Facebook profile to impersonate the identity of her previous husband to prove that he is a drug addict. In addition, a teenager in California stole the password of his classmate's Facebook account to post bad material about the victim. The impersonator was imprisoned one year in an adult detention center (Reznik, 2012).

Many terms and conditions are regulated for these platforms to prevent impersonation and protect security (Timm & Perez, 2010). Facebook's terms and conditions state that a user will not be able to provide any false personal information on Facebook platform, or build an account for someone other than yourself without permission. In addition, Twitter also

prevent impersonation as its terms and conditions state that any Twitter account seems to be for another user just to deceive, confuse, and cheat others will be permanently suspended under Impersonation Policy of Twitter (R. E. Page, 2013).

Protection is a requirement for online impersonation, but self-disclosure further decreases privacy by extending the measure of online data available to various clients. The linkages between these systems are influenced by essential variables such as control and confidence (Benson, Saridakis, Tennakoon, & Ezingeard, 2015). Trust is another requirement which characterized by the assumption that a user may trust individuals, meetings, or institutions. It also has an anti-protection correlation since the time people like to know about each other. It is always believed that the overall objective of trusting them is having a positive impact on online self-exposure (Senthil Kumar, Saravanakumar, & Deepa, 2016). An imperative build that can impact the mind-boggling relationship is the apparent control over data.

Islam has a clear opinion on impersonations in general, especially social media impersonation. Impersonation is an immoral activity which is against Islam principles and behaviors (Hoby & Mohamed, 2014). Impersonation is a kind of cheating on people which is totally prohibited in Islam religion (Al-Qaradawi, 2013). Islam also prohibited impersonation as it is a kind of lying, and the person who lies is an insincere person who will be punished from Allah. A true Muslim should be honest and he never lies or impersonates another person's identity generally or on social media platforms (Esposito, 1998).

Discussion

Social media platforms have been called 'networked publics', they are defined as the connecting communities created through internet-enabled connections (Boyd & Marwick, 2011). Social media has different online platforms represented into Twitter, LinkedIn, Facebook, and Instagram which are growing very fast leading to easy communication between social media users. During sharing information on social media platforms, the users have to seek for privacy and security (Boyd, 2010).

Impersonation is a common phenomenon found nearly on all social media platforms when social media users pretend as if they are other people. Impersonators exist for the intent of defrauding, bullying, harassing, and damaging another person. Impersonation can be observed by matching the elements of the impersonator's profile page details with the elements of the victim's profile page (R. Page, 2014). (De et al. , 2012).

Many terms and conditions are regulated to prevent social media impersonation and protect security (Timm & Perez, 2010). Protection is a requirement for online impersonation essential variables such as control and confidence (Benson et al. , 2015). Trust is another requirement which is characterized by the assumption that a user may trust individuals, meetings, or institutions. Trust is another requirement which characterized by the assumption that a user may trust individuals, meetings, or institutions. It is always believed that the overall objective of trust is having a positive impact on online self-exposure (Senthil Kumar et al., 2016).

Conclusion

Social media impersonation is the act of pretending that a person is another person which usually occurs on all social media platforms. It requires to be identified to differentiate real social media accounts from the fake ones. It is important to prevent the occurrence of impersonation and take care of private security. Prevention and trust are two main requirements to prevent the social media impersonation and protect the security of social media users. Islam prohibits impersonation as it is a kind of cheating and lying.

References

Al-Qaradawi, Y. (2013). *The Lawful and the Prohibited in Islam:* الحلال والحرام في الإسلام: The Other Press.

Badawy, A., Gharawi, M. A., Bidin, A., & Khamis, M. Role of Ministerial Media Arms During COVID-19 In Malaysia.

Benson, V., Saridakis, G., Tennakoon, H., & Ezingeard, J. N. (2015). The role of security notices and online consumer behaviour: An empirical study of social networking users. *International Journal of Human-Computer Studies, 80*, 36-44.

Boyd, D. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In *A networked self* (pp. 47-66): Routledge.

Boyd, D., & Marwick, A. E. (2011). *Social privacy in networked publics: Teens' attitudes, practices, and strategies.* Paper presented at the A decade in internet time: Symposium on the dynamics of the internet and society.

De, A., Bogart, C. M., & Collins, C. S. (2012). Detecting impersonation on a social network. In: Google Patents.

De, A., Bogart, C. M., & Collins, C. S. (2013). Detecting impersonation on a social network. In: Google Patents.

Esposito, J. L. (1998). *Islam: The straight path* (Vol. 165): Oxford University Press New York.

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

Gharawi, M. A., & Bidin, A. (2016). Computer assisted language learning for learning Arabic as a second language in Malaysia: Teacher perceptions. *International Journal of Information Education Technology, 6*(8), 633.

Hoby, E., & Mohamed, H. M. H. (2014). *Perception of the impersonation on facebook in the Egyption context.* Kuala Lumpur: International Islamic University Malaysia, 2014,

Hoffmeister, T. (2014). The challenges of preventing and prosecuting social media crimes. *Pace L. Rev., 35*, 115.

Kambellari, E. (2017). Online Impersonation: I Have a Right to Be Left Alone v. You Can't Mandate How I Use My Privacy Toolbox. *You Can't Mandate How I Use My Privacy Toolbox (September 2017). The University of Illinois Timely Tech online journal (September, 2017).*

Kaplan, A. M., & Haenlein, M. (2011). Two hearts in three-quarter time: How to waltz the social media/viral marketing dance. *Business horizons, 54*(3), 253-263.

Li, B., & Han, L. (2013). *Distance weighted cosine similarity measure for text classification.* Paper presented at the International Conference on Intelligent Data Engineering and Automated Learning.

Nuakoh, E. B., & Anwar, M. (2018). *Detecting Impersonation in Social Network Sites (SNS) Using Artificial Immune Systems (AIS).* Paper presented at the SoutheastCon 2018.

Page, R. (2014). Hoaxes, hacking and humour: analysing impersonated identity on social network sites. In *The language of social media* (pp. 46-64): Springer.

Page, R. E. (2013). *Stories and social media: Identities and interaction*: Routledge.

Reznik, M. (2012). Identity theft on social networking sites: developing issues of internet impersonation. *Touro L. Rev.*, *29*, 455.

Senthil Kumar, N., Saravanakumar, K., & Deepa, K. (2016). On privacy and security in social media–a comprehensive study. *Procedia Computer Science*, *78*, 114-119.

Timm, C., & Perez, R. (2010). *Seven deadliest social network attacks*: Syngress.

Van Dijck, J., & Poell, T. (2013). Understanding social media logic. *Media and communication*, *1*(1), 2-14.

Zarei, K., Farahbakhsh, R., & Crespi, N. (2019). *Typification of impersonated accounts on instagram.* Paper presented at the 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC).

Zarei, K., Farahbakhsh, R., & Crespi, N. (2020). How impersonators exploit Instagram to generate fake engagement? *arXiv preprint arXiv:2002.07173*.

Zarei, K., Farahbakhsh, R., Crespi, N., & Tyson, G. (2020). Impersonation on Social Media: A Deep Neural Approach to Identify Ingenuine Content. *arXiv preprint arXiv:2010.08438*.