Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Social Media Impersonation

Rajashri Tripathi[a]

[a]Amity University, Lucknow, India

Received 21 June 2022; *Accepted* 04 July 2022; *Published* 13 July 2022

Everyone's life is growing increasingly reliant on social networking. Facebook, Twitter, Instagram, and LinkedIn are just a few of the social networking networks available. Impersonation is a prevalent occurrence that can be observed on practically all social media platforms; It is the act of misleading another person by posing as somebody else. Impersonators try to hide a real account by creating a similar account to spread phony information on social networking networks, leaving it difficult to tell the difference between the two. Objectives: The goal of this paper is to provide a full overview of social media impersonation, including varieties of impersonation, how to identify impersonation on social media, cases of impersonation on social media, and how to prevent impersonation, and how to protect a social media user's security. In addition, the page covers Islam's stance on impersonations, including social media imitation. Method: This is a narrative evaluation of the existing literature on virtual world social media imitation. Conclusion: Social media impersonation is the act of pretending to be someone else on social media. It can happen on any platform.

Keywords: *social networking, impersonation, accounts, social media impersonation.*

INTRODUCTION

On social media, impersonation (identity theft) happens when a person, company, or organization's picture, name, or other identifying aspects are utilized for fraudulent reasons.

[1]The goal is to trick the victim's connections into believing that the profile is being run by a real individual. The purpose is to gain access to the personal information of those who interact with the bogus profile. Individuals and organizations impersonate one another to engage in unlawful actions. Though it was once thought to be a minor annoyance, it is now widely seen as a significant infringement of security, privacy, and secrecy. Impersonating real individuals on social media is part of a bigger category called social engineering, which includes a variety of psychological manipulation techniques. The goal is to trick victims to reveal important or crucial information or act against their better judgements. To carry out their illicit actions, malicious actors use social media platforms to impersonate individuals and organizations.

TYPES OF SOCIAL MEDIA IMPERSONATION

Here are the most common forms of social media impersonation to be on the watch for while interacting with individuals and organizations on your favourite social channels.[2]

Impersonation of a Personal Account: With so much private information regarding people around the world, it has become an easy task for cybercriminals to copy data and piece it together to construct a believable profile. They even have software that creates false profiles and posts stuff to make them appear real. As a result, their nefarious activities are easily scaled. We often hear that several accounts have been taken down and were used by hackers to trick people into digital identity theft, but it has no effect on hackers as they are creating hundreds of them every day.[3]

Hijacking of a Social Media Account: Impersonations may also occur when hackers use authentic accounts and exploit them to cultivate harmful or fraudulent information.[4] There are numerous instances of this since prominent social media profiles with large followings are

[1] 'Social Media Impersonation Definition Violations Reporting' (*Helpline Law,* 23 June 2022) <https://www.helplinelaw.com/national-and-social/SMID/social-media-impersonation-definition-violations-reporting.html> accessed 18 June 2022
[2] 'What is Social Media Impersonation? Action Tips for Cautious Users' *(Bitdefender)* <https://www.bitdefender.com/cyberpedia/what-is-social-media-impersonation/> accessed 18 June 2022
[3] *Ibid*
[4] *Ibid*

especially enticing targets. Scammers attack everybody from corporate executives to politicians and media personalities...

Fake Accounts or Bots: Bot accounts are another sort of social media imitation. A bot in general is an application that does its activities automatically. Bots provide a large no of opportunities to cyber criminals to expand their nefarious works. *"Fake accounts are dangerous because cyber-criminals use them to lure other people into different types of scams. One of the most frequently encountered scams is social network accounts run by bots that impersonate the military. This decorated war hero is fighting somewhere in Afghanistan and planning to retire. They contact senior people and try to establish some sort of a personal connection that would eventually lead to romance.*

These bots are trying to convince the victim they're real people with genuine intentions and the only thing that separates the two of them is distance and shortage of money. So, eventually, the victim ends up getting scammed for ticket money or emergency funds they need. It's such a popular and heartbreaking scam that Australia, for instance, has issued numerous warnings, particularly to senior people, to make them aware of these scams. Never engage with people who are supposedly working in the army and attempt to meet you because you're falling for a modern version of the Nigerian prince scam." Bogdan Botezatu (Director of Threat Research and Reporting, Bitdefender)[5]

Bots can:[6]

- post automatically generated content on social media sites
- disseminate malware-infected links and controversial ideas (usually disinformation, propaganda, and other types of manipulation)
- keep track of end users
- Participate in groups
- use a large number of posts to amplify messages
- create fictitious followers to give the impression that these accounts are authentic

[5] *Ibid*
[6] *Ibid*

Unfortunately, there are currently no rules or regulations in place to address the consequences of bot accounts on social media and other online platforms. As a result, their activities are practically unrestrained. For example, we've all seen (and continue to witness) the political ramifications of social media bot activity around the world in recent years.

"Bots can also do other things like inciting panic or spread malware. Sometimes, bots can even be used as command-and-control servers. A few years ago, there were a couple of instances in which Twitter accounts were used to send commands to malicious software that infected victims' devices. So bots can do a lot of things, but they're mostly related to trying to deceive people in some way or misinterpret or manipulate information. Or, as we've seen recently, amplify content.

For example, imagine you have an army of bots or fake accounts. If you want to get a story trending, all you have to do is post something on one of those accounts and then use the rest to amplify it and make sure it reaches as many people as possible. If it catches on like wildfire, it's going to be difficult for people who don't do a lot of fact-checking (which we should) to identify the truth. They're going to believe the type of information that's being propagated by those bots." Liviu Arsene (Senior E-threat Analyst, Bitdefender)[7]

Executive Impersonation: Duplicating the identities of company executives is another sort of social media impersonation. Attackers and Con artists use the bogus names of CEOs of companies. Their purpose is to connect with people as a medium within the organization. The ultimate goal of scammers is to obtain crucial information from trusted workers to trick unwary individuals and make them pay money to the fraud via fake company proposals and job offers.[8] This type of threat can have long-term ramifications for both the individual and the organization as a whole. The more the executive's role, the greater the risk to his or her reputation.

Brand Impersonation: They create fake business sites, involve in discussions with actual users, and false advertising, and address customer service inquiries using trademarked material (name, logo, photos). These activities are intended to generate engagement on the phony

[7] *Ibid*
[8] *Ibid*

profile and give it a more legitimate image.[9] The main objective of the impersonators is to get as many users as possible by interacting with them and directing them to the malware-infected websites which often (ask your name, address, phone number, bank account details, pin, and credit and debit card details.)

"There are plenty of examples in the brand impersonation category because scammers usually ride on the popularity of brands. One such example would be giveaways and other raffles that use the names of supermarkets to lure customers into clicking on malicious links which leads to having their information or their online banking credentials stolen. Other types of brand impersonation can actually happen in what we call 'competing wars'. The tactic might be used by organizations to hijack a different brand and tarnish their reputation online just by posting jokes or discrediting these companies in the eyes of their current customers." Bogdan Botezatu (Director of Threat Research and Reporting, Bitdefender)[10]

WHY DOES SOCIAL MEDIA IMPERSONATION WORK SO WELL?

A number of variables make it simple for hackers for attacking and playing con games. It's not an uphill task for them to create fake accounts, and those accounts mimic the writing style of the person or organization they are impersonating from their perspective. They can hide the fake content in your feed by sandwiching it between authentic items.[11] We are hardwired to trust others as humans. We also have a strong want to be connected, which we are increasingly able to fulfill through digital exchanges. We have a proclivity for consuming content quickly, paying little attention to it, and becoming enthralled by chances that appear to match our interests or surprise us. To watch the amazing and amusing content we always take the security of our accounts secondary, which results in getting impersonated. Cybercriminals are well aware of all of this. They observe us know our psychological qualities so that they can extract that in form of information or cash or sometimes in both forms. So, social media impersonation is not an ordinary issue and cannot be avoided, because in long run it can result in big issues. Teams of researchers and cyber security experts collaborate with law

[9] *Ibid*
[10] *Ibid*
[11] *Ibid*

enforcement agencies and legal experts and academicians to develop effective methods to control and tackle this type of danger in near future.

WAYS ATTACKERS GAIN CONTROL OF SOCIAL MEDIA ACCOUNTS

Breaking into social media accounts has become remarkably simple for cybercriminals. All they have to do is take advantage of the massive amount of personal data that has been exposed as a result of a breach of data[12] Now what do hackers do with personal information such as email addresses, identities, and credentials, as well as individual addresses, telephone number, and other information:

"One of the most frequently encountered methods that expose social network accounts is credential stuffing. Data breaches generate a lot of information about us, that's for sure. Some of the information includes usernames and passwords. With those credentials, cybercriminals attempt to log into different services, including social networks. They can do so at a very high rate because they have a lot of computing power (and time to spare!). If users have reused those leaked passwords, they will – sooner or later – find a matching identity on social networks that accepts those credentials and take over the account. From there on, attackers are just clicked away from conning other people into installing malware, donating money, or even going through private conversations or sending private pictures. Credential stuffing is still the number one problem associated with digital identities and it works very well even now, 20 years after the Internet boom." Bogdan Botezatu (Director of Threat Research and Reporting, Bitdefender)[13]

Credential stuffing, also known as a violent attack, is a type of attack in which a hacker tries several identities and passwords in order to obtain access to your accounts. Cybercriminals often buy databases of millions of compromised login credentials in order to improve the effectiveness of their operations and avoid raising security alarms. To boost their chances of success, they discard failed attack combinations and substitute them with fresh data leaks. They also take advantage of the time to avoid detection by social media's automated security

[12] *Ibid*
[13] *Ibid*

measures, building bogus profiles weeks before the attack. Aside from brutal attacks, phishing is a popular method for gaining control of social media profiles. This generally happens when a person received a link that says ("Hey, I found this picture of you online!"). The said link redirects you to a bogus website that requests your login information, and once you enter the information, the hacker will get all that he wants from your respective account. Social media impersonations can have long-term ramifications. Little did we know about the consequences of digital identity theft is that once the data is obtained it ends up in the hands of cybercriminals and the underground economy. Furthermore, if one tries to log in to other websites and services there are chances that criminal hackers can gain access to your login combination. Unfortunately, there seems to be no solution to stop the procedure once it has begun. Often victims have the least idea that they are impersonated and maximum times this type of identity theft is left undiscovered.

The big threat is to your non-perishable information which comprises your name, date of birth, names of family members and their contact numbers, and some other important information that is valuable and will stay the same throughout your life. *"There are various goals attackers will try to achieve when compromising a social media account. One of them is perpetuating the attack: using your contacts list to distribute other pieces of malware to your contact list or to scam them. There's the financial motivation: once they gain access to your account, you're either subjected to potential blackmail or they can gain access to your financial assets. There's the reputational damage that's connected to both blackmail and financial loss. And there's also the fact that they may use your account to spread propaganda, for instance. Granted, if your account is compromised and at some point and it starts spreading misinformation, links to fake, fraudulent campaigns, or information that is not legitimate or is misleading, your contacts will likely try to let you know that something's going on. However, most of these attacks are not that obvious. So, whenever attackers gain access to your accounts, they're usually trying to monetize that covertly, either by using the data they collect and selling it on the Dark Web or directly going for your financial assets." Liviu Arsene (Senior E-threat Analyst, Bitdefender)*[14]

[14] *Ibid*

IMPERSONATION OF BRAND OWNERS ON SOCIAL MEDIA: TRADEMARK INFRINGEMENT

Social Media allows us to remain in touch with friends and family, it also allows business owners to sell their products and services to customers. Furthermore, companies may build a portal that assists them in comprehending customer requirements and marketplace developments through participation and interactive activities. However, as corporations develop their presence on numerous the amount of fraudsters on social media sites and phony profiles has grown, leading to a surge in trademark infringement claims. As a result, huge businesses are becoming increasingly vulnerable to infringement by bogus accounts and cloned logos masquerading as originals.[15] The problems with brand impersonation extend beyond phony accounts to include a layer of financial deception. This occurs when these bogus profiles are validated and engage in 'real-looking activities,' resulting in account monetization, or when they go a step further and begin passing off items and services under the name of the copyrighted work as their own. Passing off is the act of purposefully or inadvertently misrepresenting one's own products or services as those of another party. In such circumstances, while these false identities could deliver invoices and tracking numbers following payment, you might either receive things that are not original or no products at all. More often than not, the brand bears the burden of such deceptive operations in the form of fewer followers and consumers, unfavorable reviews, reduced goodwill, diminished brand value, and so on. As a result, trademark imitation is immoral, leading to fraudulent acts that harm both the brand and the customer.

RACKETS OF FAKE PROFILE

We think that fraudulent social media accounts are a small thing but we are unaware of the fake profile rackets which are operating on a global scale. This was noticed in the case of Bollywood Singer Bhumi Trivedi, where a bogus account was exploiting her reputation to get followers.[16] After the filing of the complaint, the Mumbai Police detained an employee of a

[15] Social Media Impersonation Definition Violations Reporting (n 1)
[16] *Ibid*

business that was operated by creating fake accounts and generating revenue in exchange for Instagram followers. So, whether this case falls under the purview of Section 416[17] of the Indian Penal Code? This question was answered by a learned senior associate of an esteemed law firm **''If one has to read this provision technically, this is still a somewhat simpler case because a real person was indeed being impersonated by a fake profile.''** The police were powerless to intervene during the report filed against the accused due to a lack of the corresponding statute. As the complaint was filed under Section 468 [18]of the Indian Penal Code which explains the fabrication of documents or electronic records with the intention to defraud.

"A fake account is an electronic record which can be used to mislead, for which an accused can be charged with." this was the testimony given by a Cyber Law Expert while examining the case.

USERNAME SQUATTING & CYBERSQUATTING

The illicit registration and use of Internet domain names that are identical or similar to brands, registered trademarks, corporate names, or personal names are referred to as cybersquatting. Cybersquatting registrants purchase and utilise domain names with the bad faith goal of profiting from the genuine trademark owner's goodwill. The government and the Internet Corporation for Assigned Names and Numbers have both taken steps to safeguard trademark and company owners against cybersquatting misuse.[19] Username squatting occurs when a username is used to exploit the goodwill of another individual or brand. We often see that a person's or brand's username on social media portals is analogous to the domain name of the website which indirectly exploits the goodwill of an individual or brand.[20] While rules to expressly cover username squatting have yet to be drafted, cybersquatting cases are handled

[17] Indian Penal Code, 1860, s 416
[18] Indian Penal Code, 1860, s 468
[19] Social Media Impersonation Definition Violations Reporting (n 1)
[20] Social Media Impersonation Definition Violations Reporting (n 1)

under the Trademark Act of 1999. In the case of **Satyam Infoway Ltd v Sifynet Solutions[21],** the court acknowledged the absence of an Indian cybersquatting statute.

CYBERSQUATTING CASES IN INDIA

This is because there are no regulating regulations in the social media sphere, and the burden of settling conflicts has fallen solely on the interpretation of Indian courts.[22] The case of Reddit Communication Limited v Cyberbooth[23] and And is a landmark judgement of cybersquatting. In this judgment, the court found in favour of the plaintiffs that the domain name by respondents "radiff.com" is similar to the plaintiff's domain name "rediff.com" and recognized the plaintiff's domain name as a registered trademark. In the case of Tata Sona Ltd. V, Mr. Manu Kishori ordered the defendants to surrender the plaintiff's name because it was incorrectly used as a registered domain name by them, this was done according to the World Intellectual Property Organization (WIPO) guidelines in Rediff Communication Case (supra).

HOW TO PROTECT AGAINST SOCIAL MEDIA IMPERSONATION

These are certain precautions that one must definitely take in order to avoid impersonation and the need to file a complaint is never necessary. These steps are set out below:

- **Examine your followers or following list:** Always take a look at your followers' list to confirm that you are not following any unknown account and following just those accounts that are linked to the people whom you know. Reject the requests from unknown people, they send requests to unknown people either to increase their own followers or scam you with the help of messages which might look attractive to you and they will be able to get access to your privacy, sending malicious content and try to tag original accounts so you might believe that it is a real account.
- **Take the initiative:** If one does not intend to create another account on the same portal, then this should be immediately expressed or informed to your friends or contacts, that

[21] *Satyam Infoway Ltd. v Siffynet Solutions Pvt. Ltd.,* (2004) Appeal (Civil) 3028/2004
[22] Social Media Impersonation Definition Violations Reporting (n 1)
[23] *Rediff Communication Limited v Cyberbooth & Another* (1999) 4 BomCR 278

you are not planning to open any additional account so that if they follow that person who created your fake account on the same portal, they inform you regarding it so, you can take immediate action against that person.

- **Examine every social media profile:** It is important to keep a regular watch on the social media profiles for any fraudulent behaviour and if you see any such behaviour report it to the recommended authority of the respective platform or portal as soon as possible.
- **Avoid following accounts of a stranger:** We all know that we follow random accounts just to enjoy their reels, amusing content, or memes or we follow our favourite celebrities' fan page which is frequently maintained by an unknown person behind a computer. We know that it is unavoidable to not follow them but we must be careful regarding their activities. We should immediately unfollow those accounts which look suspicious.

LEGAL FRAMEWORKS FOR SOCIAL MEDIA IMPERSONATION IN INDIA

It is significant to note that Social Media Companies in India[24] do not take any responsibility for the creation of fraudulent accounts and profiles. Owing to the fact that social media sites operate as intermediaries and have no influence over account creation. This exception was granted under Section 79[25] of the Information Technology Act of 2000. That an online platform only receives and communicates digitally, so the companies are not responsible for the third-party communication or sharing of information on the respective platform or portal which is used to commit a crime. Following that, the material must be deleted from the platform. Keeping this in mind, we must also note that, while social media impersonation is not officially defined or covered by any legislation, India does have measures in place that, implicitly, may take cognizance of such complaints/cases whenever they are submitted. Although if you take efforts to prevent being impersonated, you might become a victim. It is critical to remember the regulations that apply when filing an impersonation case. These laws are discussed below.

[24] Social Media Impersonation Definition Violations Reporting (n 1)
[25] Information Technology Act, 2000, s 79

The Information Technology Act

- ***Section 66C:*** This provision clearly states that any dishonest use and fraudulent creation of social media accounts is punishable for a period which may extend to 3 years and a fine up to Rs.1 lakh. The provision starts with, *" Whoever, fraudulently or dishonestly make use of the electronic signature, password, or any other unique identification feature of any other person" …"*[26] which makes this section applicable to Social Media Impersonation
- **Section 66D:** It clearly states that the use of any computer source or communication device to cheat people will be punishable under this section for a period of 3 years and a fine up to Rs.1 lakh. The provision starts with, *"Whoever, by means of any communication device or computer resource, cheats by personation…"*[27] which makes this section applicable to Social Media Impersonation.[28]

The Indian Penal Code (IPC)

IPC Frameworks for Social Media Impersonation are:

Section 415: Section 415[29] is defined as 'Cheating' in the Indian Penal Code. Social media impersonation will be punishable under Section 415 as creating fake accounts, it is trying to cheat people. There is less distinction between conventional cheating and online imitation cheating. Both use dishonest and deceptive ways to persuade their victims to provide 'property' that the individual would not divulge if he had not been duped. The conduct is likely to cause injury or suffering to the individual in question. The fraudulent work involves cheating so social media impersonation will be fully covered under Section 415.[30]

[26] Information Technology Act, 2001, s 66D
[27] Information Technology Act, 2001, s 66D
[28] Social Media Impersonation Definition Violations Reporting (n 1)
[29] Indian Penal Code, 1860, s 415
[30] Social Media Impersonation Definition Violations Reporting (n 1)

Section 416[31]: This section clearly states, 'cheating by personation'. Whenever one pretends to be someone else than his real self by word, sign, act, or dress. So, social media impersonation surely comes under Section 416 of IPC [32]

Forgery: It is defined in Section 468[33] which makes forgery punishable for the purpose of cheating. Section 469[34] states that a person forges a document for the purpose of damaging the reputation of another person. Section 470 defines forged documents or electronic records. Forgery of papers, including electronic documents, is covered by Section 66C[35] of the Information Technology Act of 2000, which was previously explored. Both clauses can be used in combination to prosecute any online forgery. Section 417[36] mentions punishment for cheating.

Section 499: Section 499[37] of IPC defines Defamation. Defamation has been made an offence without any reference to its tendency to cause acts of illegal violence. Mental suffering caused to the person defamed is the gist of the offence. Social media impersonation also defames people by creating fraudulent accounts.[38]

[31] Indian Penal Code, 1860, s 416
[32] Social Media Impersonation Definition Violations Reporting (n 1)
[33] Indian Penal Code, 1860, s 468
[34] Indian Penal Code, 1860, s 469
[35] Information Technology Act, 2000, s 66C
[36] Indian Penal Code, 1860, s 417
[37] Indian Penal Code, 1860, s 499
[38] Social Media Impersonation Definition Violations Reporting (n 1)