Journal of Criminology and Forensic Studies
ISSN: 2640-6578

Academic Strive
Researcher's perception is our reality

Editorial *Volume 5 Issue 1*

Fake Profile 'Original Vs Anonymous'

Chawla A*
Advocate, Delhi High Court, India

***Corresponding author:** Ajay Chawla, Delhi High Court, House No-44, Pocket F/19, Sector-8, Rohini, New Delhi – 110085, Delhi, India, Tel: +91-9711777033; Email: advajaychawla@gmail.com

Received Date: February 25, 2023; **Published Date:** March 13, 2023

Introduction

If you use social networks on a daily basis, you will probably have discovered fake profiles on Facebook, Instagram or Twitter more than once.

Today, OSNs (Online Social Networks) considered the most platforms common on the Internet. It plays a substantial role for users of the internet to hold out their everyday actions such as news reading, content sharing, product reviews, messages posting, and events discussing etc. Unfortunately, on the OSNs some new attacks have been recognized. Different types of spammers are existing in these OSNs. These cyber-criminals containing online fraudsters, sexual predators, catfishes, social bots, and advertising campaigners etc [1].

When cyber fraudsters create a social media profile using the identity details like name, address, mail id, photograph etc., of victim, without their knowledge, it is called a fake profile creation. The fraudsters create fake profile with an intention of causing harm to the victim. The fraudsters use the fake profile to spread false or fake information, damage the reputation of the victim, and may also send friend requests to other friends of victim to gain financial benefit. They can be created to give voice to a product of a brand, it does not inflict serious damage to the network. They can be created to impersonate someone else, stealing their identity and creating a bad reputation on them [2].

These fake social media accounts exist and it is important to identify them so that their activity is ignored or even reported.

Identity is an object attached to a human being, separate from him or her. A typical example is the name of a person. Another example is a passport that contains the name, birth date and place of the person, nationality, digitally captured fingerprints and a digitally stored and a photograph of the person. A third example is a private and public key adhering to a Public Key Infrastructure. In general, identity should be unique in the sense that each identifying object must only refer to at most one person. The same person might still have several identities, like a passport and a pair of keys above, or a social security number.

What are Fake Profiles?

A fake profile is the representation of a person, organization or company that does not truly exist, on social media. Often these accounts use names and identities that not only look real but are designed to get closer access to specific people and their target audience. The appearance of these fake profiles can range from an attractive woman, who is trying to gain access to a man's Facebook, or a business such as a bank, reaching out to you for updated account information. They usually are recently opened accounts that have few friends, anywhere from just a dozen to several hundred. The pictures they use, are usually altered versions of images stolen from actual people or organizations [3]. So, who knows? maybe someone is using your pictures for malicious purposes somewhere on the internet to deceive, gain access, and exploit your data.

Why would Anyone Create Spam Profiles?

Spammers create fake profiles for a number of nefarious purposes. Sometimes they're just a way to reach users internally on a social networking site. This is somewhat similar to the way email spam works - the point is to send your users messages or friend invites and trick them into following a link, making a purchase, or downloading malware by sending a fake or low-quality proposition.

Spammers are also using spam profiles as yet another avenue to generate web spam on otherwise good domains. They scour the web for opportunities to get their links, redirects, and malware to users. They use your site because it's no cost to them and they hope to piggyback off your good reputation.

The latter case is becoming more and more common. Some fake profiles are obvious, using popular pharmaceuticals as the profile name, for example; but we've noticed an increase in savvier spammers that try to use real names and realistic data to sneak in their bad links. To make sure their newly-minted gibberish profile shows up in searches they will also generate links on hacked sites, comment spam, and yes, other spam profiles. This results in a lot of bad content on your domain, unwanted incoming links from spam sites, and annoyed users [4].

Four Steps to Identify Fake Accounts on Social Media

Verified Account Icon

Verified accounts have a blue icon (it's green on WhatsApp) at the end of the profile handle and may even have "Verified account" written on them.

Only companies that request that icon and can give documentary proof that an official channel is theirs can receive it. In fact, Twitter and other sites prohibit handles with emojis that look like the verified account icon to avoid misleading users.

Account Activity

Official profiles can receive numerous tags and messages by the day, hour or even minute depending on their type. Check out how a profile engages with followers and be suspicious of profiles that post spam or only showcase deals that seem too good to be true.

On customer service profiles, you will likely find direct engagement with followers. Remember to send a private message and not to post personal or particular details on a message wall.

Number of Followers

Even though the number of followers can vary greatly according to the popularity of the brand, product or business, it can help you recognize if a channel is official or not.

Account History

On Twitter and other social media platforms, you can see how long a profile has been active. Be careful when interacting with profiles that haven't been open for long, since you can't know their purpose. If a profile has been open for a long time but has few posts or messages, it may no longer be in use [5].

Approaches to Dealing with Fake Profiles

- Report the account - Almost all social media platforms have a process in place for fake profiles and for profiles impersonating someone. Follow the process on each platform and the provider will investigate the account and (if found to be fake) remove the profile and its content. Use these links to report fake profiles on Facebook, Twitter, LinkedIn, Snapchat, Pinterest and Instagram. If you need help pushing the platforms to take action report it via Report Harmful Content.
- Keep a copy of the evidence - It's important to keep information about the fake profile through taking screenshots or printing out the profile pages. This may be useful if the issue continues and you need to work with the platform or the police to resolve the issue.
- Try not to monitor the content online and resulting comments - While the information is online try not to monitor the comments and feedback. This will cause more distress.
- The information is now public - As hard as it is to deal with the information shared in the fake profile is public. Get the help and support you need to come to terms with this information being in the public domain [6].

Where to Report on Fake / Impersonated Social Media Accounts

Firstly, lock your profiles and below are few links that will then help you to resolve the problem, if necessary, deleting the fake account and banning the individual or the organisation responsible.

- Report the Nearest Cyber Crime Police Station or Report on National Cyber Crime Portal https://www.cybercrime.gov.in
- Facebook: https://www.facebook.com/help/contact/169486816475808
- Instagram: https://help.instagram.com/370054663112398
- Twitter: https://help.twitter.com/forms/impersonation
- LinkedIn: https://www.linkedin.com/help/linkedin/solve
- YouTube: https://support.google.com/youtube/answer/2802027#report_channel

Regulation by Social Media Platforms Against Fake Accounts

There is no specific law in place that holds accountable social

media platforms liable for the creation of fake accounts or Profiles within their network. This is because the network only acts as an intermediary or mediator and does not directly create the account. The safe-harbour immunity given under Section 79 of the Information Technology Act, 2000, protects intermediary social media networks from liability for content posted thereon by third parties. Under Section 79 of the Information Technology Act, 2000 an online portal which acts as an intermediary i.e. only receives, stores, transmits or communicates an electronic record will not be liable for any third-party information or communication that is available on it. However, the provisions state that upon receiving 'actual knowledge' that any information, data or communication link residing in the portal is used to commit an unlawful act, then the intermediary becomes liable to take such content down. Unfortunately, no clarity has been provided with regard to what constitutes 'actual knowledge'. Although the Shreya Singhal [7] case required a 'court order' to be considered as actual knowledge, the Delhi HC in MySpace [8] case removed this need with regard to removal of content.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 has incorporated various regulations intended to be helpful in combating the nuisance of fake accounts. Under these guidelines, every social media site has the responsibility to set up a grievance redressal mechanism wherein complaints can be lodged against any content available on that site. Under rule 3(2) (b) if the intermediary upon the receipt of complaint, finds that the impugned content is in the nature of impersonation in an electronic form, including artificially morphed images, then it shall take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it. These guidelines and the grievance redressal system set up under it would be supportive for users to report fake profiles. The guidelines also state that intermediaries are required to report cybersecurity incidents and share related information with the Indian Computer Emergency Response Team.

An additional responsibility is placed upon significant social media intermediaries, who have more than 50 lakh registered users in India. These websites are required to (i) appoint an additional chief compliance officer who ensures that the websites are acting in compliance with the IT act (ii) appoint a grievance officer who resides in India and (iii) publish a monthly compliance report with the necessary information.

Most platforms, within their Terms of Use, have provisions against impersonation and can take action when a profile is not being operated by the persons themselves. All major social media platforms such as Facebook, Instagram, Snapchat, etc. provide an option for users to report profiles that are fake or participating in unlawful activities. This system does not assure that all reported profiles will be removed, however investigations are launched to cross-check the authenticity of reported profiles. Furthermore, some websites such as Facebook have set up their own verification and enforcement agencies with the aim of identifying and removing fake accounts.

Social media websites are also improving their system by employing various verification methods that provide credibility to genuine and authenticated profiles. This allows users to differentiate between fake and real profiles and further allows the platform to identify potentially impersonating/fraudulent profiles.

Law Governing Fake Accounts

Every day there are several persons who become victim to various offences committed by imposters. These victims have the right to report such instances as the attackers are in violation of various provisions of the Indian Penal Code (fraudulent impersonation is a statutory offence) and the Information Technology Act, 2000.

The Most Relevant Section for Fake Accounts is Sec 66D of the IT Act which States that

"Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend up to three years and shall also be liable to a fine which may extend up to one lakh rupees". Moreover, Sec 66C of the Act states that "Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh."

In case of fake accounts that are used to cheat others by appropriating the personal information of other users without their consent or by using made-up personal details, the creator can be held liable under Section 416 of the IPC which deals with cheating by personation. The provision states that a person is said to 'cheat by personation' if he cheats by pretending to be some other person [9]. The imposter would be held guilty whether the individual personated is a real or imaginary person. Under Section 468, any person who commits forgery of an electronic record for the purpose of cheating would also be held guilty.

Warnings

- Keep an eye on your teens. Young people are the most vulnerable to building online relationships with people

who don't exist. They fall in love with an image of the perfect person and the faker is happy to oblige for their own gratification or other reasons.

- Be careful what you put online and what you tell people you don't really know. Some people act very caring until they have enough information about you and then they turn around and blackmail you with it. If you don't know the person, no matter how friendly you've become in the online context, keep back your private details and keep everything very general.
- Remember, that while a person using a fake account could be after money, property, or personal information, they could also be after you. That is why it is extremely important for your physical safety to use discretion with who you choose to interact with [10].

References

1. Ajay Chawla, Advocate Delhi High Court, India advajaychawla@gmail.com
2. https://metricool.com/fake-profiles/
3. https://www.cybintsolutions.com/detect-fake-profiles-phishing/
4. https://developers.google.com/search/blog/2009/06/spam20-fake-user-accounts-and-spam
5. https://www.santander.com/en/stories/four-steps-to-identify-fake-accounts-on-social-media
6. https://www.thecyberhelpline.com/guides/fake-profiles
7. 2013 12 SCC 73
8. MANU/DE/3411/2016(Delhi HC)
9. https://www.lexology.com/library/detail.aspx?g=1d2176fd-9833-443c-8ca6-05379a09d9e2
10. https://www.wikihow.com/Reveal-a-Fake-Facebook-Account