Cyber Imposter created fake profile of President of India

Introduction

The Social Networking Sites have become popular especially among the younger generation and most of the net users have their profiles in many popular networking sites among them the Face Book is the most popular and the largest social networking website. There is hardly any net savvy person in this world that does not have any idea of Face Book. The Face book started its journey as a forum meant for college students only and was available by invitation only. Now it is the favorite Social network, a phenomenon stretching across the globe and is a no. 1 social networking site though having many Privacy concerns. The Facebook currently has more than 500 million users in July 2010 and is still growing. One of the major issues concerning privacy & security recently is Fake accounts.

Fake profile of President of India on Facebook

Fake accounts of famous celebrities, personalities, politicians are created in Face Book to get a lot of audience and to spam them. The Face Book reflects the dark face of social engineering. An article from PC1News.com shows that over forty percent of Facebook profiles are actually fake one. The fake profiles in the social networking websites are doing the rounds in Face book and one can find many fake profiles in the name of celebrities, even one can find 5-7 fake profiles in the name of single Bollywood star. Now the imposter have not even spared the first citizen of India and made a fake profile in the name of the Hon'ble President her Excellency Pratibha Devi Sing Patil. The president secretariat found that there are four such fake profiles that have been created in the name of the president. The president secretariat promptly lodged a complaint with the economic offences wing of the Delhi police, the elite wing of Delhi Police which specializes in investigating economic crimes including cyber offences. The complaint of the president secretariat alleged that the Hon'ble President do not have any profile or account with any social networking site and the president house has nothing to do with the Facebook and the said fake profile is misleading the general public. The First Information Report under Sections 469 IPC and 66A Information Technology Act, 2000 was registered based on the said complaint at the police station, EOW, Delhi Police. The investigation is still going on in the said FIR and culprits are yet to be arrested. However, the fake profiles created in the name of President have since been taken down.

Similar case of fake profile of President of Guyana

It is not the first case where the fake profile has been created in the name of head of state or famous politician. Some world leaders do have genuine Facebook profile but there are many who do not simply have any Social Networking presence. Similar such incident was noticed in the year July 2008, when a fake profile of the President of Guyana Mr. Bharrat Jagdeo was found on social website www.HI5.com. Recently for the second time, another

fake profile has been discovered on Facebook in the name of Bharrat Jagdeo. A statement from Bharrat Jagdeo's office warned users of the social networking site to ignore postings purported to be from the president. The statement stated that "the impersonator is apparently using the profile to defraud supporters of the website by offering them land and other concessions."

The devastating effect of fake profiles

The problem of fake profiles on social networking sites has taken a dangerous proportion. The Annual Threat Report of the security firm Aladdin has reported against this new variant of cyber crime and warned against the increase in the incidents of "Web Identity Hijacking". According to Aladdin's report, the potential damage for this new type of identity theft will be "devastating, both on the personal level by creating difficulties in employment, ruining social and professional connections, damaging reputations; as well as on a financial level, such as stealing customers, corporate data etc." Interestingly, the security firm warns that the best method to keep your self safe is to go ahead and create your own social network profile on the major networks before someone else does. However, in the opinion of this author, this is not a solution particularly in the case of world leaders or head of the state. Do they have to mandatorily create Facebook profiles to shield themselves from imposter's fake profile and how the genuine profiles would stop imposter from opening other fake profile in some other networking sites? The Facebook or other social networking sites when creating an account in the name of such famous personalities should make proper verification, like it can take proper authorization or letter from the President office to open the account. However, the Facebook and other social networking sites do have privacy policy and other security features; however, they are so far not effective as is reflected from the numerous fake profiles coming in light and its devastating effect.

It has been found that the social networking sites are being exploited by the spammers. The spammers by using the fake Face book profiles of famous personalities persuade the users to visit the fake profile page either by sending a friend request or sending a personal message. The profile page redirects the user to a malicious malware site. In some cases, the fake profile contains the links to spam sites and other viruses.

Another devastating effect of the fake profile is the data theft. With individuals and businesses hooked on social networking sites, the imposters have leveraged them as one of the main targets for data theft and malware infiltration. The security experts around the world are of the view that the social networking sites, like facebook, myspace etc. are major security risks to corporate or personal data. One believing the friendship request received from fake profile in the name of his friend in the course of online exchange may divulge secret corporate or personal data. Thomas Ryan from a security company, Provide Security, created a fake profile for a woman named Robin Sage, who posed as a Navy cyberthreat analyst and tried to befriend around 300 real people in the US military, defence contractors, information security companies and intelligence agencies. It was a 28 day experiment to

find out how social networking sites could be used to covertly gather intelligence. The said fake profile attracted dozens of connections across sites including Facebook, LinkedIn and Twitter, including a senior intelligence official in the US marine corps, the chief of staff for a US congressman and several senior executives at defence contractors, as well as an official from the National Reconnaissance Office, which builds, launches and runs US spy satellites. Some of the friends who connected with the said fake profile shared personal and professional information and photos, which Ryan claims could have compromised corporate and possibly even national security. The experiment and its study were showcased by Thomas Ryan at the BlackHat security conference held in Las Vegas, USA. The result of the experiments shows that how easy it is to conduct social engineering for nefarious purposes like data theft.

The Legal Issues:

The Information Technology Act, 2000 and the Indian Penal Code do to some extent addresses the problems associated with the fake profiles created on the social networking sites like Facebook.

1. **The provisions of the Information Technology Act, 2000**
    a. **Section 66:** The Section is attracted when the imposter fraudulently and dishonestly with ulterior motive uses the fake profiles to spread spam or viruses or commit data theft. The act is punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.
    b. **Section 66A:** The section is attracted when the imposter post offensive or menacing information on the fake profile concerning the person in whose name the profile is created. Further, the Fake profile also misleads the recipient about the origin of the message posted on the fake profile. The offence is punishable with an imprisonment for a term which may extend to three years and with fine.
    c. **Section 66C**: As the imposter uses the unique identification feature of the real person like his/her photograph and other personal details to create a fake profile, the offence under Section 66C IT Act is attracted which is punishable with imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupee.
    d. **Section 66D:** If the imposter by personating the real person by means of fake profile cheats any one than the provision of Section 66D IT Act are attracted which is punishable in same manner as preceding Section 66C.
    e. **Section 67:** The Section is attracted if in the fake profile, the imposter posts something which is obscene which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. The offence is punishable with imprisonment of

either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

f. **Section 67A:** The Section is attracted if the fake profile contains sexually explicit act or conduct. The punishment is more severe which is punishable with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees. The offence is cognizable and non bailable.

g. **Section 67 B**: If the obscene fake profile is that of children below 18 years of age, the offence is punishable under Section 67 B IT Act which makes severe punishment for child pornography. There is special provision for sexual predators which makes punishable the act of enticing or luring the children for online relationship for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource. The offence is cognizable and non bailable with similar quantum of punishment as in Section 67A above.

2. The Provisions of Indian Penal Code

a. **Section 469:** The Section is attracted as the fake profile which is a forgery in electronic form is created with the intention of harming or lowering the reputation of the real persons in whose name the fake profile has been created. The offence is punishable with imprisonment for a term which may extend to three years and shall also be liable to fine.

b. **Section 499/500 IPC:** When fake profile is posted with defamatory content with an intention to defame other, the offence punishable under Section 499/500 IPC (defamation) is attracted.

The challenges

The fake profiles posted on the social networking sites poses serious problems and have become a major hurdle in efficient running of these sites. Though the social networking sites, like Face Book claims that they have efficient privacy policy and security mechanism in place, but one can wonder how the Face Book scans & identifies millions of fake profiles which appears to be impossible. Under the Facebook terms of use, the members are banned from attempting to "impersonate any person or entity". The Face Book simply deletes the fake profile on the receipt of credible complaint regarding the fake profile. However, for the legal actions against the imposter, one has to look upon the local police, who for the lack of the technical knowledge and cyber law, do not take the complaint seriously and simply do not take action on the complaint turning it down as very trivial matter which may have serious ramifications if not checked and the offenders not brought before justice. It is another matter, that the EOW, Delhi Police has very promptly register a

case invoking the provisions of Information Technology Act, 2000 on the basis of the complaint received from an official of President Secretariat against the alleged fake profile of the Hon'ble President of India, but what about many ordinary citizens of India who have been victim of this new form of cyber crime, how many FIRs have been registered by police on similar complaints by ordinary citizens, is a pertinent question one may ask. Further, on the part of the law enforcement agencies, they too face problems particularly investigating any cyber crime, that is lack of cooperation of the websites operated from the different jurisdiction or country.

What to do if victim

First of all prevention is better than cure, and it is matter of common sense, that be careful while surfing the net or making profile on the social networking sites. DO NOT REVEAL TOO MUCH OF YOUR PERSONAL IDENTIFYING INFORMATION. Never add a stranger as a friend or share personal information with him. Never click any links that come from strangers in messages or emails. More often, such links turn out to be containing malicious programs or viruses. Despite taking all the precautions, if you find fake profile of yours or your friend, there is no need to panic. You must always remember that Cyberspace is not a separate, law-free jurisdiction, particularly in view of the recent amendments made in the Information Technology Act, 2000 which gives power to the Inspector level officer to investigate the cyber crimes under newly inserted sections, few of which have been mentioned above. There are few steps you can take:-

- **Guess who the 'Culprit' is**: Make intelligent guessing, it will usually be someone you know like your classmate or your colleague or your old boyfriend or your immediate neighbor. Watch their reactions and the language used to describe you in the site and you may be able to guess who the prankster is. Tell that person to stop and threaten him/her with legal action/media publicity. However, if that person seems like a psycho then don't contact them.

- **Report to Social Networking Site**: - You may make a formal complaint giving the detail of the url of your profile and the bogus profile, then report them as bogus to the administrator of social networking website with a request to remove the objectionable content.

- **Lodge the FIR with Police**: It is advisable that you make a written complaint clearly disclosing the commission of cognizable offence invoking appropriate Sections of Information Technology Act or IPC as mentioned above to the dedicated Cyber Cell of the State Police which is well equipped and specially created to handle this type of complaints. Before making complaint ensure that the screen shot of the fake profile with objectionable content & concerned URL Link is saved by you as the same would be required for the investigation, more so it is also necessary due to the fact that the

culprit may remove the objectionable content to escape the criminal liability. Insist on the registration of the FIR as the Criminal Procedure Code clearly mandates that the FIR has to be registered on the complaint if it discloses the commission of cognizable offence (a cognizable offence is one where a police officer may arrest a person without a warrant). If the cyber cops refuse for some reason to register your FIR, then it is open to you to send the complaint in writing and by post to the concerned Superintendent of Police under Section 154 (3) of Cr.P.C. It is also open to the informant to directly approach the Court of Magistrate of the concerned Police Station with the information under Section 200 of Cr.P.C. with a prayer to direct the police to investigate the offence.