JANAMAITHRI- A JOURNAL OF DEMOCRATIC POLICING

CONTENTS

1:CYBER STALKING

2:SPOOFING

3:OTP FRAUDS

4:Framework & Guidelines for Use of Social Media for Government Organisations

CYBER STALKING

Team Members

1. Jijimon K M, Dy Superintendent of Police,
2. Sajesh, Senior Civil Police Officer,
3. Anil Kumar N R, Senior Civil Police Officer,
4. Sujith, Civil Police Officer,
5. Ragesh, Civil Police Officer,
6. Arjun, Civil Police Officer,
7. Vishnu, Civil Police Officer,
8. Shameer A, Civil Police Officer,
9. BibinB, Civil Police Officer,
10. Aravind Krishnan G U, Civil Police Officer.

Abstract

The cyberspace is being taken up by a new form of crime that includes repetitive attempts by one person to contact another thereby causing a sense of threat in the mind of such other person. This emerging crime is popularly known as “Cyber Stalking”. Here we have made an attempt to deal with the issue of cyber stalking. Initially, we are having a discussion on what is cyber stalking and how cyber stalkers are formed and types of cyber stalkers etc. Then we focus on different types of cyber stalking and laws governing this. We have also, for the benefit of law enforcement agencies, listed the investigation steps, tips and case studies for reference. Some suggestions and preventive action to be taken are included in the concluding part. However, always remember, the age old saying “Prevention is better than cure”.

Introduction

Stalking is unwanted or repeated surveillance, by an individual or group towards another person. Stalking behaviors are interrelated to harassment and intimidation, and may include following the victim in person, or monitoring them. For example; stalking can be done in the following ways such as: to follow a person till his home or where he does his business, to cause destruction to a person's property, leaving written messages or objects, or making harassing phone calls etc. If someone monitors or follows a person, using internet, email or any other form of electronic communication that results in a fear of violence, or interferes with the mental peace of such person, he/she commits the offence of **Cyber Stalking**. Cyber stalking is a technologically-based "attack", on one person who has been targeted specifically for that attack, for reasons of anger, revenge or control as though it's a criminal practice. Cyber stalking is actually a form of cyber bullying; the terms are often used interchangeably by people.

Eight out of 10 people in India have experienced some form of online harassment, with most common forms being abuse and insults, according to a new survey by Norton by Symantec. The majority of cyber stalking victims are between 18 and 29 years of age.With India's growing population spending more time of social media platforms and mobile applications, it is important that online users take basic precautions to protect their safety and security to avoid unwanted contact. Cyber Stalking can be terribly frightening. It can destroy friendships, credit, careers, self-image, and confidence. Ultimately, it can lead the victim into far greater physical danger when combined with real-world stalking.

Why Cyber Stalking?

Why is cyber stalking increasing day by day?. One of the main reasons is, because the victims just want to avoid further legal procedures and headaches, instead of complaining they move out from the cyber space. Most of the cyber stalking cases in India are chosen to be ignored by the victim itself, instead of approaching the

police. It is usually because they are intimidated or frightened by the thought of approaching the police, or feel that the police will not help.

The cyber stalkers who are computer experts are one step above the Law enforcement agencies. Stalkers always think that they're anonymous and can hide. In other words, the cyber stalker's biggest strength is that they can rely upon the anonymity which internet provides to them that allows them to keep a check on the activities of their victim without their identity being detected. In most of the cases reported the victims had deleted the evidences like screenshots, mails, messages etc. Cyber stalkers can easily hide evidence of their online activity.

Social media, the constant presence and use of our phones, tablets, and other devices, and our 24/7 reachability and connectivity is increasing the ability to constantly message, post, or otherwise invade the mind and emotions of targets. There is a need of efficient cyber tools to investigate cybercrimes and to be prepared to defend against them and to ensure victims justice.

Physical stalking vs. Cyber stalking.

In order to discuss difference between cyber stalking and physical stalking, there is a need to understand what physical stalking means. The differences between the two are as follows.

Basis of Distinction	Physical Stalking	Cyber Stalking
Geographical proximity	The stalker and the victim are geographically close to each other. It is not easy for the stalker to instigate third party to harass or threaten the victim. Physical confrontation is necessary.	As compared to physical stalking, there is a chance that the victim and the stalker may not be in the same geographical boundaries. It is comparatively an easy task for the stalker to instigate the third party to harass or threaten the victim. Physical confrontation is not necessary to achieve the intended purpose.

Predictability	It is fairly predictable as the stalker follows the victim to his/her house, workplace, etc. It becomes easy for the investigators to track down the offender	It is not easily predictable as the stalker uses cyber platform and there is no physical confrontation. The stalker hides his/her identity making it difficult for the investigators to trace down the offender.
Familiarity with the victim	It occurs in interpersonal relationships. Generally the victim is known to the stalker such as the victim may be a celebrity, or a relative or those residing nearby to stalker.	In this case, the stalker chooses the victim randomly. E.g., where the stalker follows victim on social networking sites, the knowledge is restricted to the information available on the site.
Anonymity	It becomes difficult for the stalker to hide his/her identity in cases of physical stalking.	The cyber stalkers, comparatively, enjoys high level of anonymity. Anyone with immense knowledge of technology can hide his/her identity in virtual world.
Nature	There is personal interaction between the stalker and the victim. Thus, it prevents shy people from committing any criminal acts because they may not feel comfortable to talk to people over the phone or cause a sense of threat in their minds by using words in a letter.	The stalker does not need to confront his victim as the internet provides anonymity to him/her. In cyber stalking, it is easy for the stalker to choose how to behave.

Intimacy	It becomes easy for the victim to understand the intentions of the stalker in case of physical stalking as there is no false sense of intimacy.	Internet provides a feature of ensuring a false sense of closeness between the stalker and the victim. This results in a misunderstanding of the stalker's intention
Risk	The stalker can monitor the activities of his/her victim in the real world as well but it involves a high degree of risk that could make the stalker vulnerable to criminal action	The internet provides an opportunity for the stalkers to keep a check on the activities of his/her victims such that the stalker may get into a discussion with the victim on some discussion forum or chat rooms, or access his/her personal information by tracking their virtual movement or even get direct access to details stored in the victim's computer. The risk is comparatively less as the identity of the stalker is hidden.

How Cyber Stalkers are formed?

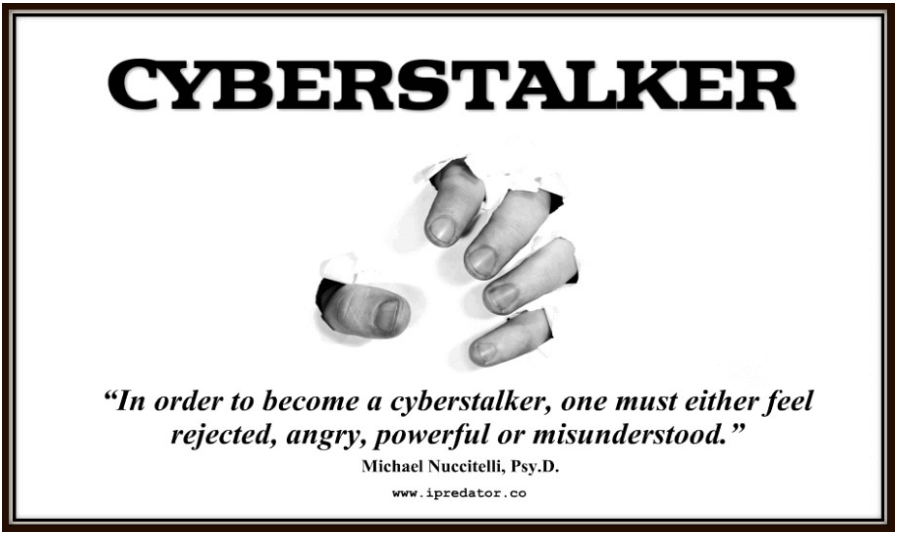
How a cyber-stalker is born? What are the reasons for a person becoming cyber stalker? As per the surveys, 3% of people are anti-socials without any reason. These people enjoy anti-social activities. Hence, this is one of the reasons for such behaviour.

There are various psychological reasons behind stalking like severe narcissism (Obsession & attraction), hatred, rage, retribution, envy, obsession, rejection, fear & distress, psychiatric dysfunction, power and control, sadomasochistic fantasies, sexual deviance(violating social norms), internet addiction or religious fanaticism. Some of the reasons are

- Jealousy: Jealousy can be a strong motive behind stalking especially when it is towards ex-partners and their current partners.

- Obsession and attraction: Another motive behind stalking could be obsession and attraction. The stalker could be attracted to victim sexually or mentally. There's a fine line between admiration and stalking.
- Erotomania: It is a kind of belief in which the stalker assumes that the victim, usually a stranger or famous person, is in love with him. It always involves sexual inclination towards someone.
- Sexual harassment: It is said to be the main motive behind cyber stalking. This is so because the internet reflects the real life.
- Revenge and hate: Sometimes the victim is not reason for the feeling of hatred and revenge in the mind of the stalker yet he/she becomes the target of the stalker. Internet appears to be the most convenient platform for the stalker to express his feeling of hatred and revenge.

Based on the above mentioned motivations behind stalking, a stalker could be an obsessed/enraged/psychopathic/deranged personality.



Type of Stalkers…

Based on the motivations behind stalking, a stalker can be categorized.

There are three categories of stalkers:

- Obsessional stalkers
- Delusional stalkers
- Vengeful stalkers

Obsessional stalkers are those stalkers whose motivation are their obsession for sexual harassment and sometimes love;

Delusional stalkers are those stalkers who feel the need to prove their power.

Vengeful stalkers are those stalkers who want to take revenge.

Against Whom..

Cyber Stalking usually happens with females, who are stalked by men, or children who are stalked by the adults. Cyberstalkers target mostly those who are internetaholic, emotionally weak or unstable in their life. Normally, the cyber stalkers victims are new on the web, and inexperienced with the rules of netiquette and internet safety. It is believed that most of the time, victims are female, but sometimes men are also stalked. As per the statistics provided by WHOA (Working to Halting Online Abuse) 74 % victim of cyber stalking are female.

Types & Characteristics of Cyber Stalking ..

Low cost of internet and ease of use motivate stalker to use information technology tool to stalk people. Cyber stalkers use different ways for stalking their target.

- Email Stalking
- Internet Stalking
- Computer Stalking
- Social Media Stalking

Email Stalking: Email or electronic mail is the most commonly and heavily used network based application. Due to the increasing use of emails, it has now become a most common way to harass, threaten or stalk any individual. In this type of stalking, stalkers basically send spontaneous email in the form of nuisance, including hatred, obscene words or threatening. Email stalkers repeatedly send mails to their target for an attempt to initiate a relationship, fix a relationship or threaten and hurt a person.

Internet Stalking: Stalkers can more widely use internet in order to abuse and jeopardize their victims. In this type of cyber stalking, stalkers are more concerned about public element than private.

Computer Stalking: The above two categories of cyber stalking can fall over the real word interaction while in this type of cyber stalking, the stalker controls its victim's computer by unauthorized access. A cyber stalker can communicate directly with their target as soon as the target computer connects in any way to the Internet. The stalker can assume control of the victim's computer and the only defensive option for the victim is to disconnect and renounce their current Internet "address".

Social Media Stalking: The stalker is using the social media platforms for threatening or harassing the victim like posting morphed photos, sending continuous messages through social media etc. The victim has to be away from the social media for escaping from this type of stalking.

The normal behavior of cyber stalking is sending electronic messaging such as classic emails, text messages, twitter, Facebook etc.

- Sending spam mails or sending threatening emails to the victim or family, friends etc.
- Posting the victim's personal information such as name, address, phone numbers, and e-mail address in social media platforms.
- Posting offensive comments in the victim's name by hacking.
- Creating and posting sexually explicit images of the victim or victim's loved ones for abusing.
- Hacking into the victim's computer, accounts and mobile devices.
- Subscribing the victim to pornography sites and unwanted advertising.
- Attaching spyware to emails or installing it on the computer.
- Setting up websites that threaten the victim or encourage others to contact, harass or harm them by using social media accounts of victims.

These are some of the methods used by stalkers.

Cyber Laws which can deal with Cyber Stalking..

Information Technology Act, 2000 and Indian Penal Code, 1860 more specifically deal with cyber stalking. In India, the laws are gender biased as the law-makers considered women as the weaker section of the society hence; every statute revolves around protecting women. There are no direct provisions that deal with the issue of cyber stalking.

- Firstly, Section 354 D of IPC defines "stalking". It reads as follows:

"(1)Any man who follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or monitors the use by a woman of the internet, email or any other form of electronic communication commits the offence of stalking;.."

The section was added by Criminal Amendment Act 2013 post Delhi gang-rape case. This section takes into account both, the physical stalking and cyber stalking. The section defines its scope in terms of activities that forms the offence of "stalking." The Section clearly mentions that if anyone tries to monitor the activities of a woman on internet, it will amount to stalking. Thus, if the stalker indulges in any of the activities defined in the section, he shall be guilty of the offence under Section 354 D of Indian Penal Code.

This section has many loopholes such as firstly; the section only considers "women" to be the victim and ignores the fact that even men can be the victim. The Section states that whoever tries to monitor the usage by a woman of internet, e-mail or any other mode of electronic communication shall be liable for committing the offence of cyber stalking. We can see that it focuses only on women. Thus, it is gender biased legislation. Secondly, the legislators have not mentioned the "method of monitoring." It might happen that the person might lack the intention but his actions amount to stalking.

- Second, Section 292 of IPC defines materials that can be termed obscene. When the stalker attempts to deprave the other person by sending "obscenity" through social networking site or through emails or messages, then it is a crime.

The offence of cyberstalking takes within its purview the act of sending obscene language, any obscene material on internet with the intention that the other person would read, see or hear the content of such material. In that case he shall be guilty of the offense under Section 292 of Indian Penal Code.

- Third, Section 507 of IPC relates to "criminal intimidation by anonymous communication."

This section states that when the stalker tries to hide his identity so that the victim remains unaware of the source from where the threat came, it amounts to an offence. Thus, it ensures the very characteristic of cyberstalking i.e., anonymous identity. The stalker shall be guilty under this section if he attempts to conceal his/her identity.

- Fourth, Section 509 of IPC relates to outraging of modesty of women which reads as follows:

"Words, gesture or act intended to insult the modesty of a woman. —Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished..."A stalker can be booked under this section if the conduct of the stalker hinders the privacy of such woman by making any gesture or through words sent by e-mails, messages or posted on social media. If he does any such activities, he shall be guilty of offence under Section 509 of Indian Penal Code.

However, Section 509 suffers from a few shortcomings. Some of them are: it is a gender biased provision as it focuses only on modesty of a woman and therefore, ignores the fact that this crime of cyber stalking is gender neutral in nature and even males can be the victim in such crimes. This section requires that the words, sound or gesture should be spoken, heard and seen respectively. Thus, cyber-stalkers can easily escape the penalty under this section as word cannot be spoken, gesture cannot be seen and sound cannot be heard on internet. Lastly, the intention of insulting the modesty of the woman cannot be assumed from communications on internet.

- Fifth, Section 67 of Information Technology Act, 2000 is a replica of Section 292 of Indian Penal Code.

This section relates to publishing obscene material in "electronic form". Thus, this section covers the online stalking. If the stalker tries to publish any obscene material about the victim on social media i.e., in electronic form so as to bully the victim, he shall be guilty of offence under Section 67 of IT Act.

- Sixth, Section 67 A of Information Technology Act, 2000 relates to a part of cyberstalking crime.

This section was added after the amendment in 2008. It states that if the stalker attempts to publish any "sexually explicit" material in electronic form i.e., through emails, messages or on social media, then he shall be guilty of an offence under Section 67 A of IT Act and shall be punished accordingly.

- Seventh, Section 67 B of Information Technology Act, 2000 is newly inserted section.

This section is newly inserted by Amendment Act 2008. The section focuses on the crime of stalker targeting children below the age of 18 years and publishing material in which children are engaged in sexual activities in order to terrorize the children.

- Eighth, Section 66 E of Information Technology Act, 2000 and Section 354 C of Indian Penal Code deals with "voyeurism."

Section 66 E reads as follows: "Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished."

- Ninth, Section 354 C IPC reads as follows:

"Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator

or by any other person at the behest of the perpetrator or disseminates such image shall be punished..."

The stalker might hack the account of the victim and post private pictures of the victim on social networking sites in order to cause depression and a sense of threat in the mind of the victim. Both the above mentioned sections aims at publishing or capturing pictures of private act of a person without the consent of such person. He shall be guilty of an offence under these sections. However, Section 66 E is more generic as it addresses the victim as "any person" whereas Section 345 C is kind of gender biased. As per section 354 C, the victim should be a "woman"

The Information Technology Act, 2000 and the Indian Penal Code, 1860 does not explicitly provide provisions for dealing with the issue of Cyber Stalking and the defamatory or threatening messages sent by the stalker during stalking the victim through messages, phone calls, e-mails or by publishing blogs under the name of the victim. It is possible to punish the offender under some of the provisions of the above mentioned Acts as mentioned in above chapters but there is no express provision that solely deals with this crime.

Investigating Steps

On the preliminary Investigation if the Investigating officer determines that this is indeed a cyber stalking case, he or she should initiate a preliminary criminal investigation. It is important to obtain from the complainant a detailed description of the harassing behavior, including any personal contacts, such as telephone calls or being followed.

- Step 1: Ask the complainant if he or she knows who is sending the harassing messages. If so, obtain the standard investigative information about the suspect: name, age, address, telephone number, vehicle information, and relationship to victim. Obtain a copy of the messages for the case file showing the e-mail address, Web site URL, nickname, screen name, and the content(s) of the message(s).

- Step 2: Ask the complainant if he or she knows why he or she is being harassed. If so, record the complainant's explanation in as much detail as possible in the narrative portion of the statement. Knowledge of the reason can help lead to the identification of an unknown harasser.
- Step 3: Establish when and how the harassment began. Has the contact been solely via the Internet (e-mail messages, chat rooms, mailing lists, instant messages, Web site) or has there been other harassment such as telephone calls, cell phone calls or texts, postal letters, or contacts at the complainant's workplace or other locations, and whether any of the complainant's relatives or friends have also been subjected to the harassment.
- Step 4: Determine whether the complainant has been threatened with physical harm or physically attacked. Often, the electronic messages will threaten violence, rape, and even death. The law enforcement officer will need to establish the details of how these threats were communicated. If the complainant has been attacked, it is apparent that the threat has escalated beyond electronic threats. Details of the attack and results of the subsequent investigation of that incident should become part of the case file.
- Step 5: The investigating officer needs to secure any physical evidence available and start the chain of custody to protect the evidence. The material should be saved in both paper printouts and electronic files on an electronic medium such as a disk or CD/DVD-ROM. Ask the complainant if he or she has any material evidence. Items to request include:

  E-mail messages
  Chat room messages
  Instant messages
  Web page images

Social networking messages/wall posts
Mailing list messages
Message board messages
Tele/cell phone conversations or answering machine messages
Text messages
Postal letters
Photographs

- Step 6: What communication has the complainant had with the harasser? Did the complainant respond to the messages? Copies of the responses are necessary for the investigation. The law enforcement officer needs to describe and assess the amount and nature of communication between the two parties to understand if the incident escalated or if the threats occurred without other escalating factors.
- Step 7: Although cyberstalking is a secretive, individualized crime, investigating officers always need to ask if there are any witnesses. Often the victim will alert friends and relatives to the messages received and the law enforcement officer needs to determine whether others can contribute information to the case.
- Step 8: Determine what steps, if any, the complainant has taken to stop the harassment. Has the complainant reported the harassment to anyone else, notified the ISP about the messages, filed any court actions, or sought legal advice? In order to develop a clear understanding of the case, investigating officer must make a record of any action by the complainant.
- Step 9: Assess the steps the complainant has taken to protect himself or herself. The physical protective steps of appropriate security for their person are the prime concern. In addition, recommendations provided in this article for protecting against the online abuse could be followed.

Once the initial complaint has been filed, an assessment of the case for continued investigation is appropriate. Collect all evidences from available resources and produce it in court.

Shortcuts

Many cyberstalkers who send threatening e-mail messages send them from free e-mail accounts available from such Web sites such as Yahoo!, Gmail, and Hotmail. Such e-mail service providers can supply the IP logging information, which includes IP addresses used to access the account and the dates and times of that access. The IP addresses usually resolve back to a legitimate ISP. Sometimes a law enforcement officer's telephone call to that ISP will prompt the ISP to shut down the harasser's account and send information about the harasser to the police department; other times, law enforcement will need a search warrant to get the information associated with the harasser's account or a request based on section 91 of CrPC is needed. If the harasser accesses e-mail from a location that offers free Internet access (such as libraries), identification is more difficult but not impossible.

If the investigation has uncovered more than one e-mail address associated with the harasser, the law enforcement officer could conduct a search using a search engine such as www.yahoo.com or www.google.com, www.bing.com to see if the harasser has any type of Internet presence. For example, the Maryland State Police had a case where the suspect was sending harassing e-mail messages to a female using a free e-mail account at different county libraries. The harasser's established e-mail address came from a library and therefore had no originating IP address. There seemed to be no way to determine who the harasser was. Nevertheless, a newsgroup search using the harasser's e-mail address revealed a message posted to a mountain biking group where the suspect actually gave his real first and last name and the city he lived in.

If the law enforcement officer develops an address or telephone information on the harasser, an interview with the harasser

usually ends the harassment. If the harasser is in another state, it is recommended to contact the local law enforcement agency to conduct the interview. If the harassment has escalated to cyberstalking or real-life stalking, proceed from there by filing charges, getting protective orders, or helping the victim find a lawyer to file a civil suit.

It is important to acquire as much information as possible about the Web site or message board or forum in question, including the URL. Whenever someone accesses a Web site, the Web site captures, at a minimum, the IP address used to access it at a particular date and time. So law enforcement agencies will get the IP address easily if it's inside jurisdiction.

Anonymity through the Internet:

Currently the Internet provides opportunities for anonymity that are complicating cyberstalking investigations. The cyberstalker can thwart an investigation by using different ISPs and adopting different screen names. Perhaps the most difficult situation is when the cyberstalker uses an anonymous remailer service that strips identifying information from the e-mail header and erases any transactional data from servers, thus removing the tracing evidence of a message back to the author.

Cyberstalkers using anonymous remailing services will remain virtually undetectable. Fortunately, the anonymous remailers are currently being used in only a small percentage of the cyber stalking incidents. The appropriate resolution to anonymous remailing services is the development of a technological solution that will block anonymous communication.

Tracing the Suspect:

Although the Internet eliminates some physical barriers to interaction with another person, and although it provides the perception of anonymity, it does leave evidence that can be traced to the cyber stalker.

The first identifying evidence is found in the headers. The headers contain the entire path and route the message took and is vitally needed when tracing a harasser.

Here is an example of what a person usually sees when receiving an e-mail:

To: netcrimes@netcrimes.net

From: questloans@qwest.net

Subject: FOX NEWS: End of war sure to cause rate hikes soon

Date: Wed, 30 Apr 2011 00:28:01 -1900

To determine where the message really originated, activate the full headers or show original, which will look something like this:

Received: from ns5.eleconinfotech.net [202.160.172.226] by odin.larp.com with ESMTP (SMTPD32-7.07) id ABFB80700D4; Wed, 30 Apr 2011 02:23:55 -0400

Received: from mail2.uswest.net ([211.136.104.133]) by ns5.eleconinfotech.net (8.11.6/linuxconf) with ESMTP id h3U4cij17870; Wed, 30 Apr 2011 10:08:50 +0530

Message-ID:
<000060936d3a$000072c8$00005151@gateway.attbi.com>

To: netcrimes@netcrimes.net

From: questloans@qwest.net

Subject: FOX NEWS: End of war sure to cause rate hikes soon

Date: Wed, 30 Apr 2011 00:28:01 -1900

MIME-Version: 1.0

Content-Type: text/html; charset="iso-8859-1"

Headers: Mailman v2.0.4

X-RCPT-TO:

Working from the bottom up, go to the first "Received: from line" and look at the IP address there—in this case, 211.136.104.133.

An IP address consists of four sets of numbers with one to three numerals per set. This is the server the message originated from. Once the IP address is known, the officer can find out who owns it and contact the owner for more information about the account holder.

Translating IP Addresses with WHOIS

WHOIS is the registry of all the domain names that have been registered. A good resource for translating IP addresses is available at http://www.whois.sc/. Enter the IP address or hostname in the blank text box, then click "lookup" to find out who owns that domain and their contact information.

Using the IP address from the e-mail header sample, 211.136.104.133, reveals the following about its owner:

Person: Jinxia Sun

Address: China Mobile Communications Corporation

Address: 29, Jinrong Ave., Xicheng District, Beijing, 100032

Country: CN

Phone: +86-10-66006688-1755

Fax-no: +86-10-66006012

E-mail: sunjinxia@chinamobile.com

nic-hdl: JS686-AP

Remarks: ----------

Remarks: Please send abuse e-mail to

Remarks: abuse@chinamobile.com

Remarks: Please send probe e-mail to

Remarks: security@chinamobile.com

Remarks: ----------

Other resources for a registry of domain names and translating IP addresses are http://www.whois.net/, http://network-tools.com/, and http://www.fr2.cyberabuse.org/whois/?page=whois_server.

Before using this contact information, go to the ISP contact list at http://www.haltabuse.org/cops/isplist.php (the password is cops); this is for law enforcement only and may provide better contacts. All ISPs are in alphabetical order.

If you don't find the ISP you're looking for there, then use the WHOIS information to contact the ISP.

Once the header code is identified, it will lead investigators to the ISP, then to the owner of the e-mail address, and thus the cyberstalker. At this point, standard investigative procedures are followed.

Important tips to be kept in mind for effective investigation..

1. Always ensure the presence of a woman police officer, So that the confidence of the victim or child will be maintained.
2. Take steps to record the statements of the victim/child by the Magistrate u/s 164 CrPC.
3. Appoint a victim Liaison officer for the follow up of the case, to prevent any depression happen to the victim
4. If the victim is hurt either mentally or physically, the medical help/checkup to be provided and collect any certificate thereof.
5. It is mandatory to register a case, if a woman made a complaint on such cognizable offence.
6. Always remember that the privacy of the victim should not be revealed by the Investigating Officer or Law enforcement agencies.
7. The Investigating Officer is responsible only to the court/Senior officers and to the victim.
8. Refer the relevant circulars/ Court orders regarding this.

Case Study

- India's first case of cyber stalking was registered in New Delhi and the stalker Manish Kathuria was arrested by the New Delhi Police. He was stalking, victim by illegally chatting on the Web site MIRC using her name. He used obscene and obnoxious language, and distributed her residence telephone number, inviting people to chat with her on the phone. As a result of which, victim kept getting obscene calls from everywhere, and people promptly talked dirty with her. In a state of shock, she called the Delhi police and reported the matter. The police department without waste of time swung into action, traced the culprit and slammed a case under Section 509 of the Indian Penal Code for outraging the modesty of victim.
- On 25/02/2014 in thane (Maharashtra, India), A 26 year old woman has filed a complaint against her colleague for stalking her online by downloading her photos from a social networking site and circulating them to a friend. A case was registered with the Vartak Nagar Police under Section 354D of the IPC.
- A 35-year-old man will serve three months in jail for sending obscene pictures and videos via email to a woman he met on a social networking site — the state's first conviction in a cyber-stalking case. Additional chief metropolitan magistrate convicted Yogesh Prabhu under section 509 (word, gesture or act intended to insult the modesty of a woman) of the IPC and section 66 (E) (punishment for violation of privacy) of the Information Technology Act, 2008. "Prabhu has been sentenced to three months' simple imprisonment and fined Rs10,000/- for the offence under the IT Act and Rs 5,000/- for intending to insult the modesty of a woman.

The woman initially chatted with him, but she said she started finding his behavior suspicious and stopped responding to his messages. She even removed him from her friend's list. According to the police sources, their relationship could have turned sour after the woman turned down Prabhu's proposal to get married. As the woman

is a year older than Prabhu, her parents were opposed to the marriage. The woman then stopped communicating with him. Prabhu, however, continued to keep an eye on her profile and her whereabouts. The following month, between March 3 and March 9, 2009, the woman got mails from an unknown ID. The mails contained obscene images and videos. She initially ignored them, but when they did not stop, wrote a complaint to the then crime branch chief Rakesh Maria. A case was registered at the Shivaji Park police station on April 9 and the Cyber Crime Investigation Cell (CCIC) took over the probe.

The Internet Protocol (IP) address of the computer was traced to the Vashi firm. A team headed by inspector Mukund Pawar, arrested Prabhu in April 2009. Cyber cell filed a 200-page charge sheet in September 2009, after which the trial began.Eight witnesses, including the woman, Prabhu's colleagues, cyber experts and police officials were examined by public prosecutor. When the court convicted Prabhu, it said the prosecution had proved the case beyond reasonable doubt. This is the first conviction in a cyber-stalking case in Maharashtra. Convictions in cyber frauds cases have happened earlier, but this is the first in which an accused has been convicted in a cybercrime where a woman was targeted, stalked and harassed with obscene material on the internet.

Anti Stalking tips.

Here are a few important pointers to help you thwart cyberstalking, whether it's directed at you, your PC, or your family:

- Maintain vigilance over physical access to your computer and other Web-enabled devices like cell phones. Cyber stalkers use software and hardware devices (sometimes attached to the back of your PC without you even knowing) to monitor their victims.
- Be sure you always log out of your computer programs when you step away from the computer and use a screensaver with a password. The same goes for passwords on cell phones. Your kids and your spouse should develop the same good habits.

- Make sure to practice good password management and security. Never share your passwords with others. And be sure to change your passwords frequently! This is very important.
- Do an online search for your name or your family members' now and then to see what's available about you and your kids online. Don't be shy about searching social networks (including your friends' and colleagues'), and be sure to remove anything private or inappropriate.
- Delete or make private any online calendars or itineraries--even on your social network--where you list events you plan to attend. They could let a stalker know where you're planning to be and when.
- Use the privacy settings in all your online accounts to limit your online sharing with those outside your trusted circle. You can use these settings to opt out of having your profile appear when someone searches for your name. You can block people from seeing your posts and photos, too.
- If you suspect that someone is using spyware software to track your everyday activities, and you feel as if you're in danger, then seek a professional help, only use public computers or telephones to seek help. Otherwise, your efforts to get help will be known to your cyberstalker and this may leave you in even greater danger.
- As always, use good, updated security software to prevent someone from getting spyware onto your computer via a phishing attack or an infected Web page. Check the app store for your mobile devices to see what security software is available. Or visit the Norton Mobile page to see what programs are available for your device's platform. Security software could allow you to detect spyware on your device and decrease your chances of being stalked.
- Teach Your Children; You might sound like a broken record, but keep on telling your kids they should never provide any personal information about themselves online, no matter how safe they think it might be. Tell them never to indicate their real name,

school, address, or even the city where they live. Phone numbers are not to be distributed online, and if a stranger contacts them via any method, they need to let you know right away. Encourage your kids to tell you if they're being cyberstalked. As parents, you should report cyberstalking to a teacher or school administrator and, if it seems serious, the police.

- Report if you're being cyberstalked, remember to keep a copy of any message or online image that could serve as proof. In fact, show your children how to use the "print screen" or other keyboard functions to save screenshots.
- Most important, don't be afraid to report cyberstalking to the police. Many police departments have cybercrime units and law enforcement agencies are having trained officers for dealing with cybercrimes, as cyberstalking is a crime.

Conclusion.

It is very correctly said that if you want to bring changes in the current scenario, you need to overcome the obsolete model of dealing with the situation and build a new model that is effective and efficient. At present, a system of procedures is not there for dealing with cybercrimes. Cyberstalking is a newly coined term. It has gained attention of the legislature and judiciary recently. There have been many instances where the need for effective legislation was felt as it becomes very difficult for the enforcement agencies to deal with such cases. Cyberstalking is proved to be a grave offence. It has very far-reaching impact on the mental and physical health of the victim. Through this article, the author has made an attempt to discuss the term “cyberstalking” in detail along with its nature and scope and legal remedies.

Some people argue that it is an extended version of stalking or a new form of stalking but it appears to be more than that. It is a new form of crime itself. We have seen that the intention of the stalker is to harass and threaten his/her victim. Thus, it involves a criminal activity. Information Technology Act and Indian Penal Code have a few

provisions that could be invoked against this for booking the crime stalkers. There are a very few reported cases because the police authorities do not take up the case because of the enforcement issues as the stalker and the victim possibly belong to different countries making it difficult to decide up on the course of law to be followed.

As is correctly said, "Prevention is better than cure". We should take some precautions for our safety and if after then such situation arises, we should take recourse to legislative provisions.

POLICE TRAINING COLLEGE

ADVANCED COURSE ON CYBER CRIME INVESTIGATION

PROJECT: SPOOFING

PROJECT SUBMITTED
BY

SRI. MANAF, SI OF POLICE- DCRB KOLLAM CITY
SRI. SATHIAN, ASI-CYBER CELL, KKD RURAL
SRI. SAVAD ASHRAF, CPO-CYBER CELL, KASARAGOD
SRI. ADARSH, CPO- COMPUTER CELL, KASARAGOD
SRI. AMAL, CPO-KAP 1ST BTN
SRI. RTHEESH, CPO- KOLLAM CITY
SRI. BINIL, CPO-KAP VTH BTN
SMT. JENUS CLEETUS, WCPO-CYBER CELL, TSR-R
SRI. BIJITH, CPO-POZHIYUR PS, TVPM RURAL
SRI. AKHIL, CPO-CYBER DOME

CONTENTS DISCUSSED

- What is Spoofing
- Different Types of Spoofing
- How spoofing is done
- Legal aspects of Spoofing- IPC&IT Act

I. DEFENITION OF SPOOFING:-

Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security.

OR

Spoofing is a type of scam where an intruder attempts to gain unauthorized access to a user's system or information by pretending to be the user. The main purpose is to trick the user into releasing sensitive information in order to gain access to one's bank account, computer system or to steal personal information, such as passwords.

II. DIFFERENT TYPES OF SPOOFING:-

i) e-mail Spoofing
ii) Caller ID Spoofing
iii) SMS Spoofing
iv) IP Spoofing
v) MAC Spoofing
vi) WEB Site Spoofing

III. E-MAIL SPOOFING

The word “spoof” means “falsify.” A spoofed email is one in which the sender purposely alters parts of the email to look as though it was written by someone else. Typically, the sender’s name or email address and the body of the message are formatted to appear as though they are from a legitimate source such as a bank, a newspaper, or a legitimate company on the web. Sometimes, the spoofer makes the email appear to come from a private citizen.

In many cases, the spoofed email is part of a phishing attack—a con. In other cases, a spoofed email is used to dishonestly market an online service or sell you a bogus product.

Attacks:

- Cause confusion or discrédit a Person
- Social Engineering (phishing) - An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website—nearly identical in appearance to its legitimate version—prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information is sent to the attacker

Why Would Someone Fraudulently Spoof an Email?

There are a couple of reasons people spoof the emails you receive:

The spoofer is trying to phish your passwords and login names. Phishing occurs when the dishonest sender tries to lure you into trusting the email. A false (spoofed) website may be waiting off to the side, cleverly disguised to appear to be a legitimate online bank website or paid web service such as eBay. Far too often, victims unwittingly believe the spoofed email and click through to the false website. Trusting the spoofed website, victims enter their password and login identity, only to receive a false error message that the website is unavailable. During all of this, the dishonest spoofer captures the victim's confidential info and uses it to withdraw the victim's funds or perform dishonest transactions for monetary gain.

Purpose 1: the email spoofer is trying to "phish" your passwords and login names

Phishing is where the dishonest sender hopes to lure you into trusting the email. A false (spoofed) website will be waiting off to side, cleverly disguised to appear like a legitimate online bank website or paid Web service, like eBay. Far too often, victims will unwittingly believe the spoofed email and click to the false website. Trusting the spoofed website, the victim will enter his password and login identity, only to receive a false error message that "website is unavailable". During all of this, the dishonest spoofer will capture the victim's confidential info, and proceed to withdraw the victim's funds or perform dishonest transactions for monetary gain.

Purpose 2: the email spoofer is a spammer trying to hide his true identity, while still filling your mailbox with advertising.

Using a mass-mailing software called "ratware", spammers will alter the source email address to appear as an innocent citizen, or as a legitimate company or government entity. The purpose, like phishing, is to get people to trust the email enough so that they will open it and read the spam advertising inside.

Use this site for e-mail spoofing: https://emkei.cz/

HOW DO I RECOGNIZE AND DEFEND AGAINST SPOOF EMAILS?

Like with any con game in life, your best defense is skepticism. If you don't believe that the email is truthful, or that the sender is legitimate, then simply don't click on the link and type your email address. If there is a file attachment, simply don't open it, lest it contain a virus payload. If the email seems too good to be true, then it probably is, and your skepticism will save you from divulging your banking information.

- Check the content of the email:
- Check the header of the email

IV. CALLER ID SPOOFING

What is Caller ID Spoofing?

Caller ID spoofing is technology that allows you to alter the information forwarded to your caller ID in order to hide the true origin ID.

In simpler terms, caller ID spoofing allows you to display a phone number different than the actual number from which the call was placed. With caller ID spoofing, you can send and receive outgoing or incoming phone calls or texts that appear to be from *any* phone number of your choosing.

Though spoofing offers many legitimate and useful benefits to its users, it is also one of the many ways scammers steal your personal identity and money over the phone.

Over the years, a spoofing strategy called neighbor spoofing has grown to be one of the driving factors behind nearly 3 billion spam and telemarketing calls mobile phone owners in the United States receive each month.

Neighbor spoofing works by tricking recipients into thinking they are receiving a legitimate phone call by showing a caller ID that

matches or is close to your phone number's "NPA-NXX". By matching their NPA-NXX closely to yours, spammers try to trick you into thinking the call is coming from a legitimate phone number because it looks as though it's coming from a phone number in your area code. This makes you much more likely to answer the call, and therefore even *more* likely to fall for a phone scam.

To protect yourself from neighbor-spoofed spam calls, identify your phone number's NPA-NXX following the steps below. When you receive incoming calls from similar area codes and prefixes, beware. It may be a phone scammer!

It is important to note that, though it is true that some forms of caller ID spoofing have been used as a vehicle to inflict harm on innocent victims, it is not entirely to blame for the growing robocall and phone scam problem in the United States.

Like many tools or products that have been used to cause damage or harm to others, the people *behind* the illegal (and harmful) spoofed phone calls or texts are the root cause of the problem.

To truly stop illegal caller ID spoofing phone calls, you must enlist third-party solutions such as TrapCall to address and stop the issue at the source

How to Protect Yourself Against Caller ID Spoofing:-

Don't place all your trust in the caller ID information presented to you.

Now that you know this information is easily spoofed by the use of third-party caller ID spoofing services and other tools, you won't be as trusting in the technology as you have been. This should help you in the quest to scam-proof your brain.

Never give credit card information to someone who calls you.

Don’t conduct any business over the phone when you didn't initiate the call. Get a call back number and call back if you are interested in a product or service. Use Google to reverse lookup the phone number before you call back and see if it is associated with a known scam.

V. SMS SPOOFING

- SMS Spoofing allows to change the name or number of the text messages a recipient would appear to receive. It replaces the number from which the text message is received with alphanumeric text. This type of spoofing has both legitimate and illegitimate applications.
- The legitimate manner would be setting your name or company name or the product name for or from which the text message is sent. So thereby the text message received will display the name or the company name or the product name and the purpose would thus be served.
- The illegitimate way would be when a person or a company would use the name of some other person or name or a product with the intentions of causing losses to the concerned.

VI. IP SPOOFING

- What is IP Spoofing?
- A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host
- Base for IP spoofing
- The concept of IP spoofing was discovered as a security weakness in the IP protocol which carries the Source IP

address and the TCP protocol which contains port and sequencing information.

- IP spoofing is a technique used to gain unauthorized access to computers, where by the attacker sends messages to a computer with a forging IP address indicating that the message is coming from a trusted host.
- Attacker puts an internal, or trusted, IP address as its source. The access control device sees the IP address as trusted and lets it through.

1- The creation of IP packets with counterfeit (spoofed) IP source addresses.

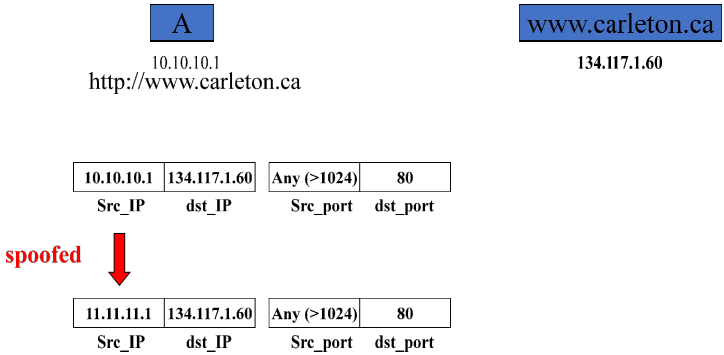
2- A method of attack used by network intruders to defeat network security measures such as authentication based on IP addresses.

There are attacks where the attacker "spoofs" the source IP address of a "trusted" IP address to slip by security measures in the network. This attack uses the trust relationships established by IP addresses that are considered trusted (usually internal) versus untrusted

- IP spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer.
- Two general techniques are used during IP spoofing:
- A hacker uses an IP address that is within the range of trusted IP addresses.
- A hacker uses an authorized external IP address that is trusted.
- Uses for IP spoofing include the following:
- Spoofing is usually limited to the injection of malicious data or commands into an existing stream of data.

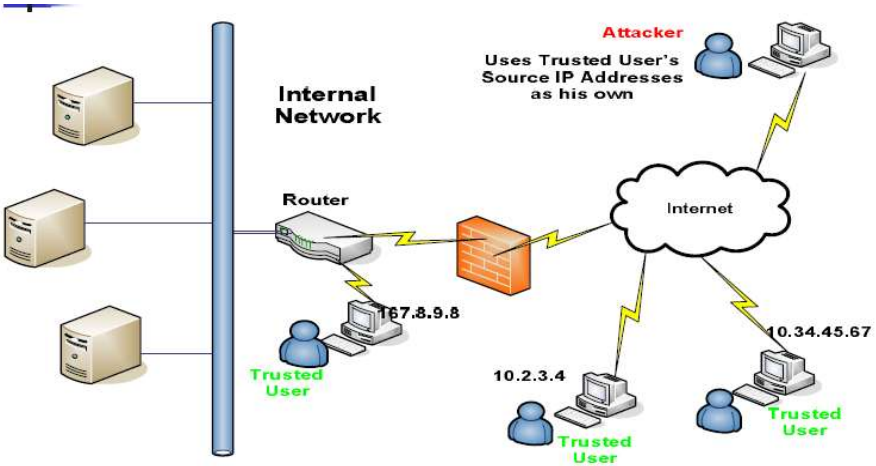
- A hacker changes the routing tables to point to the spoofed IP address, then the hacker can receive all the network packets that are addressed to the spoofed address and reply just as any trusted user can.

Basic Concept of IP Spoofing



(FIGURE - IP SPOOFING AT A GLANCE)

IP spoofing attack occurs when an attacker outside your network pretends to be a trusted user either by using an IP address that is within the range of IP addresses for your network or by using an



authorized external IP address that you trust and to which you want to provide access to specified resources on your network. Should an attacker get access to your IPsec security parameters, that attacker can masquerade as the remote user authorized to connect to the corporate network.

Why IP Spoofing is easy?

- Problem with the Routers.
- Routers look at Destination addresses only.
- Authentication based on Source addresses only.
- To change source address field in IP header field is easy.

Spoofing Attacks:

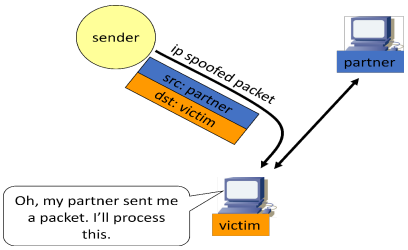
There are a few variations on the types of attacks that using IP spoofing.

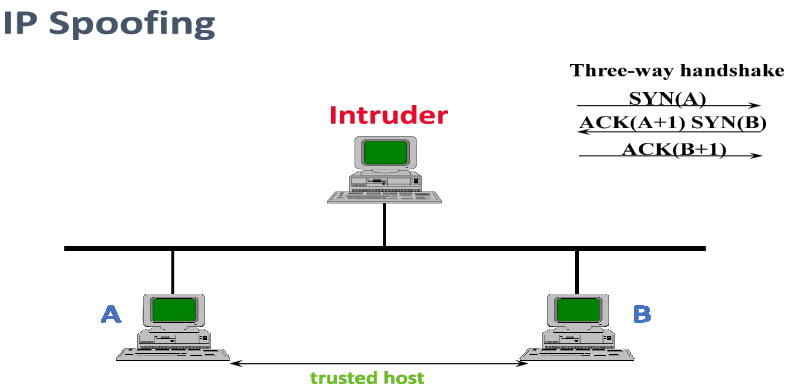
Spoofing is classified into :-

1. non-blind spoofing

This attack takes place when the attacker is on the same subnet as the target that could see sequence and acknowledgement of packets.

- Using the spoofing to interfere with a connection that sends packets along your subnet.
    - ❖ *The threat of this type of spoofing is session hijacking and an attacker could bypass any authentication measures taken place to build the connection. This is accomplished by corrupting the DataStream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine.*





(FIGURE - IP SPOOFING ATTACK AT A GLANCE)

session hijack or reset

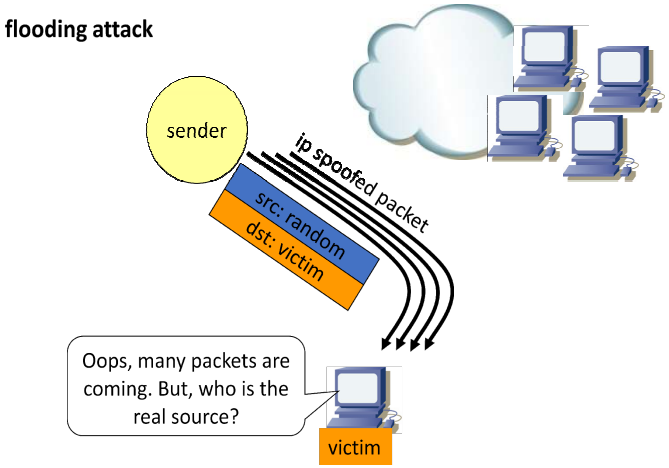
TCP SESSION HIJACKING

Send RST packet with spoofed source IP address and appropriate sequence number to one end SYN-flood that end send ACK packets to target at other end

2. Blind spoofing

This attack may take place from outside where sequence and acknowledgement numbers are unreachable. Attackers usually send several packets to the target machine in order to sample sequence numbers, which is doable in older days.

- Using the spoofing to interfere with a connection (or creating one), that does not send packets along your cable.

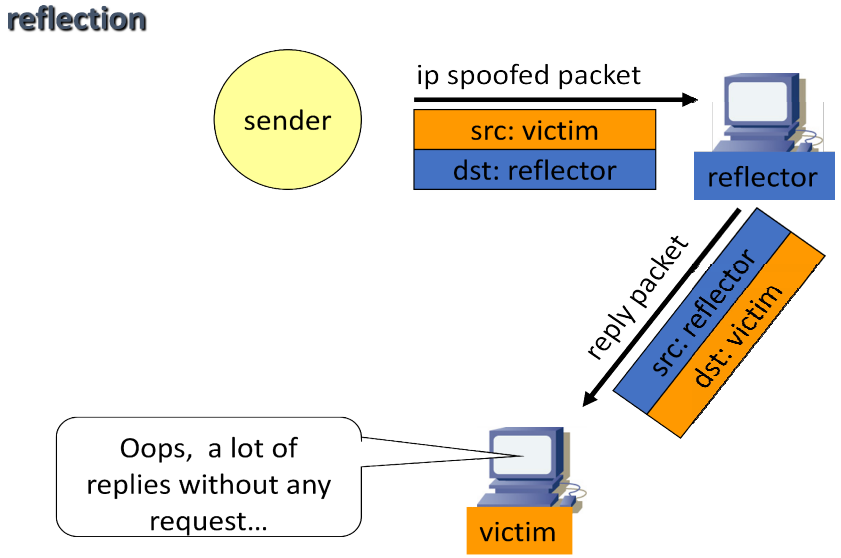


3. Man in the Middle Attack

This is also called connection hijacking. In this attacks, a malicious party intercepts a legitimate communication between two hosts to controls the flow of communication and to eliminate or alter the information sent by one of the original participants without their knowledge.

- ❖ *A type of attack where a user gets between the sender and receiver of information and sniffs any information being sent. In some cases, users may be sending unencrypted data, which means the man-in-the-middle can easily obtain any unencrypted information. In other cases, a user may be able to obtain the information from the attack but have to unencrypt the information before it can be read.*

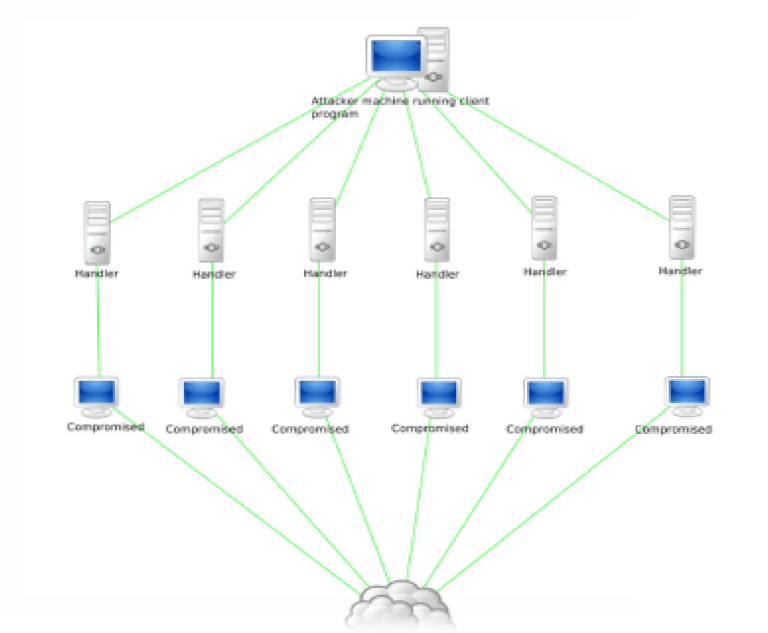
(FIGURE – SPOOFING ATTACK-REFLECTION)



4. Denial of Service Attack

- Conducting the attack, attackers spoof source IP addresses to make tracing and stopping the DoS as difficult as possible. When multiple compromised hosts are participating in the attack, all sending spoofed traffic, it is very challenging to quickly block the traffic.

- IP spoofing is almost always used in denial of service attacks (DoS), in which attackers are concerned with consuming bandwidth and resources by flooding the target with as many packets as possible in a short amount of time. To effectively



(Figure- Denial of Service Attack)

Impact:-

Current intruder activity in spoofing source IP addresses can lead to unauthorized remote root access to systems behind a filtering-router firewall. After gaining root access and taking over existing terminal and login connections, intruders can gain access to remote hosts.

VII. Detection of IP Spoofing:

1) If you monitor packets using network-monitoring software such as net log, look for a packet on your external interface that has both its source and destination IP addresses in your local domain. If you find one, you are currently under attack.

   ❖ *We can monitor packets using network-monitoring software.*

- ❖ *A packet on an external interface that has both its source and destination IP addresses in the local domain is an indication of IP spoofing.*
- ❖ *Another way to detect IP spoofing is to compare the process accounting logs between systems on your internal network. If the IP spoofing attack has succeeded on one of your systems, you may get a log entry on the victim machine showing a remote access; on the apparent source machine, there will be no corresponding entry for initiating that remote access*

2) Another way to detect IP spoofing is to compare the process accounting logs between systems on your internal network. If the IP spoofing attack has succeeded on one of your systems, you may get a log entry on the victim machine showing a remote access; on the apparent source machine, there will be no corresponding entry for initiating that remote access.

Source Address Validation :

- Check the source IP address of IP packets
  - filter invalid source address
  - filter close to the packets origin as possible
  - filter precisely as possible
- If no networks allow IP spoofing, we can eliminate these kinds of attacks

VIII. Preventing IP spoofing

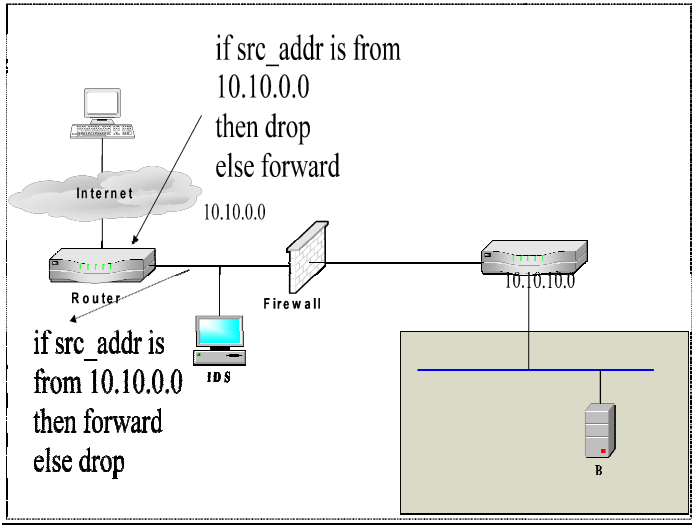
The best method of preventing the IP spoofing problem is to install a filtering router that restricts the input to your external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network. In addition, you should filter outgoing packets that have a source address different

from your internal network in order to prevent a source IP spoofing attack originating from your site.

To prevent IP spoofing happen in your network, the following are some common practices:

1. Avoid using the source address authentication. Implement cryptographic authentication system-wide.
2. Configuring your network to reject packets from the Net that claim to originate from a local address.
3. Implementing ingress and e9gress filtering on the border routers and implement an ACL (access control list) that blocks private IP addresses on your downstream interface.

If you allow outside connections from trusted hosts, enable encryption sessions at the router.



(Figure- Filtering)

IX. IP SPOOFING AT A GLANCE

Internet Protocol Address (IP Address) plays a very significant role in our day to day lives. Whether it is Cyber Security or Cyber Forensics, IP Address has a crucial role to play. IP Address is also the Starting Point for any Cyber Crime Investigation. So it is of utmost importance that an IP Address must be correctly ascertained.

Similarly, the Crackers and Cyber Criminals are interested in hiding their "Digital Footprints" through various means. IP Spoofing, use of Proxies, utilising Botnet for nefarious activities, exploiting Unsecured Wireless Access Points and Connections, etc are some of the methods that are used by Cyber Criminals.

IP Address is also the starting point to determine the "Authorship Attribution" that is a must before an accused is "Convicted" by a Court of Law. For instance, if a single Computer of Internet connection is used by multiple users, it is absolutely essential to ascertain who in fact used the Computer/Connection for the "Offending Act".

Similarly, it is absolutely essential to ensure that the owner of a Wireless Connection is actually the person who committed the Cyber Crime or Cyber Contravention. In the majority of cases, such an Unsecured Wireless Connection is misused by others and the IP Address of the owner is reflected for that activity.

Thus, Authorship Attribution is an important aspect of "Determining the Culpability" of an Offender where the means to commit the Offence are common and accessible to many people simultaneously. Data Mining and Profiling of the accused to "Attribute Culpability" to him/her alone is an emerging area of Cyber Crime Investigation.

IP Spoofing is one of the methods used by Cyber Criminals to deny "Authorship Attribution" to them. A Cyber Crime Investigator would first ascertain the IP Address and then after analysing the E-Mail Headers/Logs, She would come to a conclusion that the IP Address reflected in the communication is a Forged or Spoofed one. Ascertaining the true and correct IP Address is required to proceed further in such case.

IP Address Spoofing requires creation of IP packets with a forged source IP Address with a purpose of concealing the real identity of the sender or impersonating another System. The most common Protocol for data exchange over Internet is the TCP/IP. The header of each IP Packet contains, among other things, the numerical source and destination address of the Packet. The source address is normally the address that the packet was sent from. By forging the header so it contains a different address, an attacker can make it appear that the packet was sent by a different Computer.

However, there is a "Limitation" to such a use. To establish a Connection, TCP uses a "Three Way Handshake" and IP Spoofing by its very nature fails to satisfy this handshake. So the purposes of IP Spoofing are limited in nature. For instance, IP Spoofing can be used for Denial of Service Attacks (DOS) as the attacker is least bothered to receive a "Response". IP Spoofing can also be a method of attack used by network intruders to defeat network security measures, such as authentication based on IP Addresses. IP Spoofing can also be used for Session Hijacking or Host Impersonation.

There are some services that are vulnerable to IP Spoofing. These include RPC (Remote Procedure Call services), any service that uses IP address authentication, the X Window System, the R services suite (rlogin, rsh, etc.), etc.

IP Spoofing can take many forms. In Non-Blind Spoofing the attacker is on the same subnet as the victim and this enables him to perform session hijacking. Using this technique, an attacker could effectively bypass any authentication measures that have taken place to build a connection.

In Blind Spoofing several packets are sent to the target machine in order to sample sequence numbers. Computers in the past used basic techniques for generating sequence numbers. It was relatively easy to discover the exact formula by studying packets and TCP sessions. Today, most Operating Systems (OSs) implement random sequence number generation, making it difficult to predict them accurately.

In Man in the Middle Attack (MITM) the attacker intercepts a legitimate communication between two Computers. The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient. In this way, an attacker can fool a victim into disclosing confidential information by "Spoofing" the identity of the original sender, who is presumably trusted by the recipient.

There is a "General Consensus" that IP Spoofing does not allow gaining Anonymous Internet Access, which is a common misconception for those unfamiliar with the practice. Any sort of Spoofing beyond simple floods is relatively advanced and used in very specific instances such as evasion and connection hijacking.

However, some believe that if a Website is not using syncookies and is using predictable initial sequence numbers, it is possible to create a live TCP connection without actually revealing the original IP Address. This may be possible as the attacker may be least

interested in getting back the "Responses". I would deal with this issue separately and in greater details subsequently.

IP Spoofing can be prevented and defended against through methods like Packet Filtering, Websites using syncookies and unpredictable initial sequence numbers, use of multiple authentication protocols so that they do not exclusively rely on the IP Address for authentication, use of Encryption, etc.

Some upper layer protocols provide their own defense against IP Spoofing attacks. For example, TCP uses sequence numbers negotiated with the remote machine to ensure that arriving packets are part of an established connection. Since the attacker normally cannot see any reply packets, the sequence number must be guessed in order to hijack the connection. The poor implementation in many older operating systems and network devices, however, means that TCP sequence numbers can be predicted.

X. MAC SPOOFING

The device that you're looking at right now has a network interface controller (NIC), the thing that's responsible for allowing you to connect to a network, like the internet. All devices capable of networking (smartphones, laptops, and routers) have one of these. Each NIC is assigned a unique hard-coded MAC addresses that cannot be changed.

However, almost all popular platform such as Windows or OS X or Linux (and hence Android) support *changing* MAC addresses and pretty easily too. Just because we cannot change the MAC address built into our NIC doesn't mean we can't make other devices think that our MAC addresses is something different. Whatever information leaves our device is in our control. And in the header of the packets

that make up our data is the address of our device, the MAC address (along with IP and a bunch of other information).

So, our operating systems allow us to instruct the NIC to ignore the built-in MAC address and instead use our own custom MAC address which could be anything we want it to be. This is called MAC spoofing.

What is MAC spoofing used for?

MAC spoofing is awesome. We're interested in MAC spoofing because it allows us to make other devices think that we are someone else. For a hacker, this opens up a variety of attack vectors:

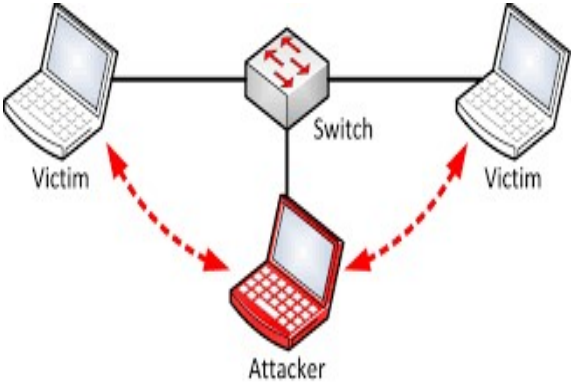
- It allows us to perform man-in-the-middle attacks
- It can help us hack Wi-Fi networks
- It lets us directly target devices connected to our Local Area Network (LAN)
- If you've been banned from using a public Wi-Fi hotspot, MAC spoofing allows you to trick the router into thinking that you are some other device.
- There are a couple of completely legitimate (read: white hat) reasons for MAC spoofing as well:
- Setting up numerous virtual machines in a corporate environment, each with a randomly assigned MAC address.
- It can be used for improving anonymity (An unsafe local network can track you using your MAC address. If your MAC address keeps changing, they can't do that anymore).

Consider an example. Say you're using Wi-Fi and you're friend is also connected to the same network. Now, when you first connect to a Wi-Fi access point (the router), you exchange some information with

the router. You request a connection from the router, enter the password and if successful, the router responds by opening a connection for you. Now the router knows who you are (your MAC address) and you know who the router is (it's MAC address).

MAC Spoofing Techniques & its Types

- There are different MAC spoofing techniques. . In general, spoofing methods are used by crackers to compromise computer systems.
- Many people mistakenly think that spoofing is an actual attack. In reality, spoofing is just one step in a process whereby an attacker tries to exploit the relationship between two hosts.
- Two spoofing techniques are discussed with some guidelines on spoofing prevention.
- Address Resolution Protocol Spoofing: The Address Resolution Protocol (ARP) provides a mechanism to resolve, or map, a known IP address to a MAC sub layer address



(*Figure*- ARP Spoofing)

XI. WEB Spoofing

- Pretending to be a legitimate site
- Attacker creates convincing but false copy of the site
- Stealing personal information such as login ID, password, credit card, bank account, and much more. aka Phishing attack
- False Web looks and feels like the real one
- Attacker controls the false web by surveillance
- Modifying integrity of the data from the victims

Here is how a spoofed web session flows.

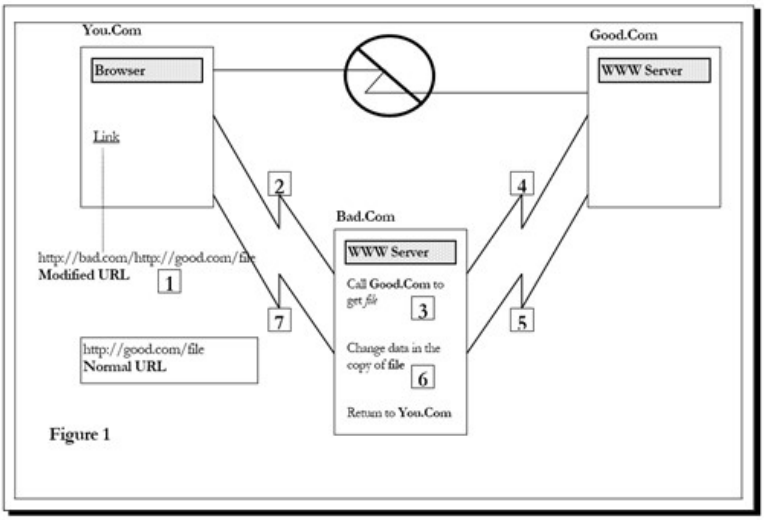


Figure 1

1. Somehow, the URL that your client browser is referencing on You.Com has been prefaced with the address of the intermediary web site – Bad.Com.
2. Your browser determines that Bad.Com should handle the URL request .
3. The web server on Bad.Com reads the URL and determines that the you are actually trying to reach a file on Good.Com.
4. The Bad.Com server calls Good.Com and asks for the specified file.
5. The Good.Com server returns the page as requested.
6. At this point, the Bad.Com server can change its copy of the page you asked for.
7. After these changes, the Bad.Com server returns the page to you.

Different types of Web Spoofing

1. DNS server spoofing attack
    - One of the most complex types of attack
    - Alter a domain name to point to different IP address
    - Redirect to a different server hosting a spoofed site
2. Content theft
    - A copy of a site can be created from the original by saving all the publicly accessible pages, images, and scripts from a site to another server. (Miguel's Demo)
    - Can be done automated by using programs called "spiders"
3. Subdomain Spoofing
    - Normal subdomain: http://subdomain.domain.com
    - Tricking internet user that they are on the correct URL
    - Make the URL long enough so that the user cannot see the entire URL

How to detect a spoofed webpage

- URL (this is the easiest way to detect the attack!)

  Triple check the spelling of the URL
  Look for small differences such as a hyphen (-) or an underscore (e.g. suntrust.com vs. sun-trust.com)
- Mouse over message (careful: this can be spoofed too!)
- Beware of pages that use server scripting such as php these tools make it easy to obtain your information.
- Beware of java scripting as well.
- Beware of longer than average load times.

XII. Legal Aspects of Spoofing

IPC

- Section 420 Cheating
- Section 463. Forgery
- [Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury], to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery. Section 464. Making a false document
- Section 468. Forgery for purpose of cheating

IT ACT

- Section 66: The account of the victim is compromised by the phisher which is not possible unless & until the fraudster fraudulently effects some changes by way of deletion or alteration of information/data electronically in the account of the victim residing in the bank server. Thus, this act is squarely covered and punishable u/s 66 IT Act
- Section 66C: In the phishing email, the fraudster disguises himself as the real banker and uses the unique identifying feature of the bank or organization say Logo, trademark etc. and thus, clearly attracts the provision of Section 66C IT Act, 2000.
- Section 66D: The fraudsters through the use of the phishing email containing the link to the fake website of the bank or organizations personates the Bank or financial institutions to

cheat upon the innocent persons, thus the offence under Section 66D too is attracted.

- Section 66E: Punishment for violation of privacy
- Section 66F: Punishment for cyber terrorism
- Section 67: Publishing obscene information in electronic form
- Section 67A: Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form
- Section 67B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in
- electronic form

Cyber Law in India

Offences	Section Under IT Act
Tampering with computer source Documents	Sec.65
Hacking with computer systems , Data Alteration	Sec.66
Dishonestly receiving stolen computer resource or communication device	Sec.66B
Identity theft	Sec.66C
Cheating by personation by using computer resource	Sec.66D
Violation of privacy	Sec.66E
Cyber terrorism	Sec.66F
Publishing or transmitting obscene material in electronic form	Sec .67
Publishing or transmitting of material containing sexually explicit act, etc. in electronic form	Sec.67A
Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form	Sec.67B
Preservation and Retention of information by intermediaries	Sec.67C
Powers to issue directions for interception or monitoring or decryption of any information through any computer resource	Sec.69
Power to issue directions for blocking for public access of any information through any computer resource	Sec.69A
Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security	Sec.69B
Un-authorized access to protected system	Sec.70
Penalty for misrepresentation	Sec.71
Breach of confidentiality and privacy	Sec.72
Publishing False digital signature certificates	Sec.73
Publication for fraudulent purpose	Sec.74

Publication for fraudulent purpose	Sec.74
Act to apply for offence or contraventions committed outside India	Sec.75
Compensation, penalties or confiscation not to interfere with other punishment	Sec.77
Compounding of Offences	Sec.77A
Offences with three years imprisonment to be cognizable	Sec.77B
Exemption from liability of intermediary in certain cases	Sec.79
Punishment for abetment of offences	Sec.84B
Punishment for attempt to commit offences	Sec.84C
Offences by Companies	Sec.85
Note : Sec.78 of I.T. Act empowers Police Inspector to investigate cases falling under this Act	

Sending threatening messages by e-mail	Sec .503 IPC
Word, gesture or act intended to insult the modesty of a woman	Sec.509 IPC
Sending defamatory messages by e-mail	Sec .499 IPC
Bogus websites , Cyber Frauds	Sec .420 IPC
E-mail Spoofing	Sec .463 IPC
Making a false document	Sec.464 IPC
Forgery for purpose of cheating	Sec.468 IPC
Forgery for purpose of harming reputation	Sec.469 IPC

Web-Jacking	Sec .383 IPC
E-mail Abuse	Sec .500 IPC
Punishment for criminal intimidation	Sec.506 IPC
Criminal intimidation by an anonymous communication	Sec.507 IPC
When copyright infringed:- Copyright in a work shall be deemed to be infringed	Sec.51
Offence of infringement of copyright or other rights conferred by this Act. Any person who knowingly infringes or abets the infringement of	Sec.63
Enhanced penalty on second and subsequent covictions	Sec.63A
Knowing use of infringing copy of computer programme to be an offence	Sec.63B
Obscenity	Sec. 292 IPC
Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail	Sec.292A IPC
Sale, etc., of obscene objects to young person	Sec .293 IPC
Obscene acts and songs	Sec.294 IPC
Theft of Computer Hardware	Sec. 378
Punishment for theft	Sec.379
Online Sale of Drugs	NDPS Act
Online Sale of Arms	Arms Act

XIII. RESOURCES:-

http://www.networkcommand.com/docs/ipspoof.txt
http://www.securityfocus.com/infocus/1674
http://www.webopedia.com/TERM/I/IP_spoofing.html
http://linuxgazette.net/issue63/sharma.html
http://www.giac.org/practical/gsec/Victor_Velasco_GSEC.pdf
http://bear.cba.ufl.edu/teets/projects/ISM6222F102/perryna/secondpage.html

A JOURNAL ON OTP FRAUDS

Team Members

1. K. MalleswaraRao, SI of Police, Chodavaram PS, AP.Ph: 8096755537
2. Jayaprakash A.U, SI of Police, Meenangadi PS, Wayanad. Ph:9747431692
3. SyamKumarK.S, SI of Police, District Crime Branch, Idukki. Ph:9495043880
4. Pradeep Kumar P, SCPO N 2474, DHQ, Pathanamthitta. Ph:9495836911
5. Sheeja A.V, WCPO 5305, Mayyil PS, Kannur. Ph:9446680032
6. Suresh V.C, CPO N2663, DHQ, Pathanamthitta. Ph:9400375617
7. Krishnakumar M, CPO 3695, RRRF,Klari. Ph:9497288359
8. Shiju N, CPO 9868, KAP IV, Mangattuparamba. Ph:9995515583

Acknowledgement

This Project report on OTP Fraud is submitted as a part of Advanced Course on Cyber Crime Investigation conducted at PTC, Thiruvananthapuram from 12.09.2018 to 25.10.2018. The Course members were divided into various groups and our 4th group was formed under the leadership of Sri.K. MalleswaraRao, SI of Police, Chodavaram PS, Vizag District, AP.

We are submitting this project report in brief span with the help of PTC authorities and also with the help of exploring vast possibilities in the web world.

We are expressing our sincere gratitude to The Principal, The Vice Principal, Course Coordinators, Indoor and Outdoor Staffs of PTC, Faculties of C-DAC, FSL, and Faculties from various establishments for making us familiar with the Cyber Crime investigation and also giving us valuable directions for completing this project.

INTRODUCTION

One Time Password

A **One-time password** (**OTP**), also known as **one-time pin**, is a password that is valid for only one login session or transaction, on a computer system or other digital device. By sending **One time password** (**OTP**) on mobile number businesses can verify users when they want to make necessary transactions.

One-Time Password (OTP) is a technological mechanism through which a single-use password is generated and sent to the registered mobile number for the user to access the website. It is also known as two-factor authentication. Products like Google for Work, PayTM, and internet banking portals often use the OTP mechanism to ensure the authenticity of the user and prevent identity thefts.

Steps in the OTP Process

User enters the username and password

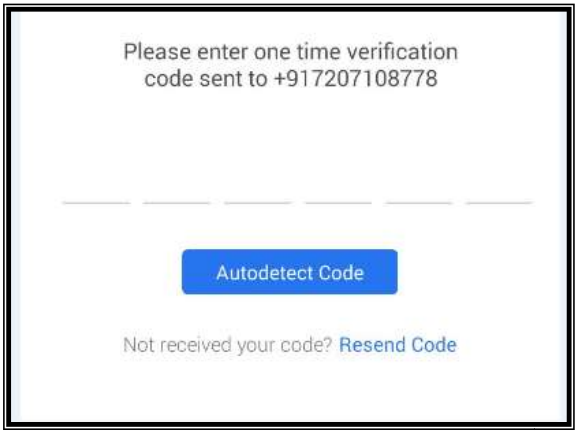
Request sent to backend

Username and password matched

User receives OTP via SMS

User enters OTP and login to the site

…that's it!



How long does OTP last

The One-Time Password (OTP) will be valid for 10 minutes from the time of generation, after which it expires. In case of One-Time Password (OTP) expiry, the transaction just needs to be cancelled by you and re-initiated where the One-Time Password (OTP) is generated again.

What is the ultimate benefit of OTP?

OTP provides another layer of online protection for you. If your user ID and password have been compromised to a fraudster, the login process will not be completed without the correct OTP that is sent to your registered mobile number. This prevents others from accessing your Online Banking account/Transaction

OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to *something a person has* (such as a small keying fob device with the OTP calculator

built into it, or a smartcard or specific cell phone) as well as *something a person knows* (such as a PIN).

The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the *previous* session, thus reducing the attack surface further.

Methods of generating the OTP

Time-synchronized

A time-synchronized OTP is usually related to a piece of hardware called a security token (e.g., each user is given a personal token that generates a one-time password). It might look like a small calculator or a keychain charm, with an LCD that shows a number that change occasionally. Inside the token is an accurate clock that has been synchronized with the clock on the proprietary authentication server. On these OTP systems, time is an important part of the password algorithm, since the generation of new passwords is based on the current time rather than, or in addition to, the previous password or a secret key. This token may be a proprietary device, or a mobile phone or similar mobile device which runs software that is proprietary, freeware, or open-source

Methods of delivering the OTP

A common technology used for the delivery of OTPs is text messaging. Because text messaging is a ubiquitous communication channel, being directly available in nearly all mobile handsets and,

through text-to-speech conversion, to any mobile or landline telephone, text messaging has a great potential to reach all consumers with a low total cost to implement. However, the cost of text messaging for each OTP may not be acceptable to some users.

On smartphones, one-time passwords can also be delivered directly through mobile apps, including dedicated authentication apps such as Authy, Duo, and Google Authenticator, or within a service's existing app, such as in the case of Steam. These systems do not share the same security vulnerabilities as SMS, and do not necessarily require a connection to a mobile network to use, as they are not internet-based.

Limitations: However, using a mobile phone as the OTPs generator has vulnerabilities to keyboard monitor attacks, memory scan attacks and software clone attacks.

What is meant by OTP FRAUDS?

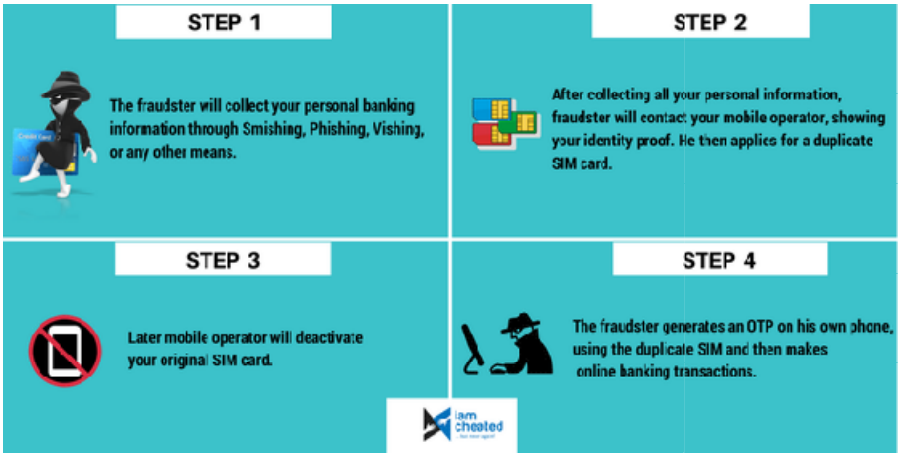
In law, **fraud** is deliberate deception to secure unfair or unlawful gain, or to deprive a victim of a legal right. Fraud itself can be a civil wrong (i.e., a fraud victim may sue the fraud perpetrator to avoid the fraud or recover monetary compensation), a criminal wrong (i.e., a fraud perpetrator may be prosecuted and imprisoned by governmental authorities). The purpose of fraud may be monetary gain or other benefits, such as obtaining a passport or travel document, driver's license or qualifying for a mortgage by way of false statements.

OTP frauds are one kind of online fraud in which attackers grabs the OTP numbers from the victim by fraudulent means and using

that OTP, attackers do e-commerce purchases using the victim's bank account, credit or debit card without the knowledge of the victim. Attackers also transfers money from victim's account to some anonymous accounts created by the attackers.

Types of OTP Fraud

1. Gozi Trojan Attack



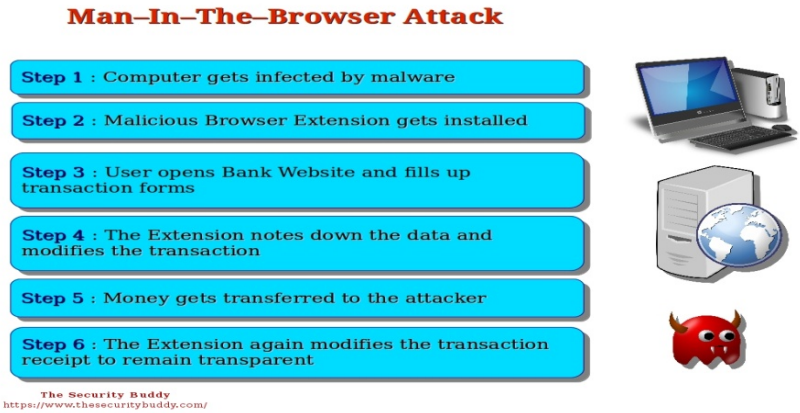
The criminals use the Gozi Trojan to steal IMEI (international mobile equipment identity) numbers from online bank account holders when they log in.

"Once they have the IMEI number, the criminals contact the victim's wireless service provider, report the mobile device as lost or stolen, and request a new SIM card.

With this new SIM card, all OTPs intended for the victim's phone are sent to the fraudster controlled device.

Gozi attacks are mainly in the U.S.

2. Man in the Browser (MitB) (Phishing attack)



This starts with a Man in the Browser (MitB) or phishing attack to obtain the victim's bank account details, including credentials, name, phone number, etc.

The criminal then goes to the local police station and uses that stolen personal information to get a police report that lists the mobile device as lost or stolen.

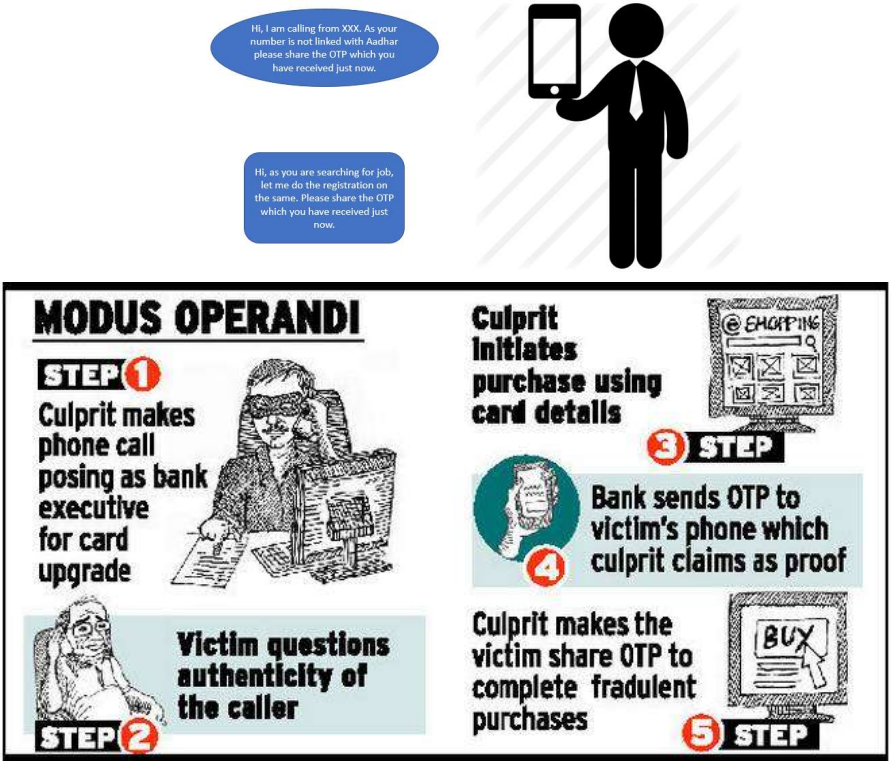
He then calls the victim to and says his mobile phone service will be interrupted for the next 12 hours.

The criminal then presents the police report at one of the wireless service provider's retail outlets. The SIM card reported as lost or stolen is deactivated by the mobile network operator, and the criminal gets a new SIM card that receives all incoming calls and OTPs sent to the victim's phone number.

3. Fraud Call Attacks

Criminal makes fraudulent phone Calls to the victim and asks for OTP pretending to be an authorized person..

Victim provides him the OTP.



Criminal uses this OTP to complete online fraudulent purchases using victims Credit/Debit card of Bank account.

How OTP FRAUD works

1. SIM SWAP

Under SIM Swap, fraudsters manage to get a new SIM card issued against your registered mobile number through the mobile service provider. With the help of this new SIM card, they get One Time Password (OTP) and alerts, required for making financial transactions through your bank account.

How do fraudsters operate?

Step – 1: Fraudsters gather customer's personal information through Phishing, Vishing, Smishing or any other means.

Step – 2: They then approach the mobile operator and get the SIM blocked. After this, they visit the mobile operator's retail outlet with the fake ID proof posing as the customer.

Step – 3: The mobile operator deactivates the genuine SIM card and issues a new one to the fraudster.

Step – 4: Fraudster then generates One Time Password (OTP) required to facilitate transactions using the stolen banking information. This OTP is received on the new SIM held by the fraudster.

How to protect yourself from SIM SWAP:

1. If your mobile no. has stopped working for a longer than usual period, enquire with your mobile operator to make sure you haven't fallen victim to the Scam.
2. Register for SMS and Email Alerts to stay informed about the activities in your bank account.
3. Regularly check your bank statements and transaction history for any irregularities.

2. VISHING

Vishing is one such attempt where fraudsters try to seek your personal information like Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.

How do fraudsters operate?

Step – 1: The fraudster poses as an employee from the bank or a Government / Financial institution and asks customers for their personal information.

Step – 2: They cite varied reasons as to why they need this information. For e.g. reactivation of account, encashing of reward points, sending a new card, linking the Account with Aadhar, etc.

Step – 3: These details thus obtained are then used to conduct fraudulent activities/ transactions on the customer's account without their knowledge.

How to protect yourself from VISHING:

Never share any personal information like Customer ID, ATM PIN, OTP etc. over the phone, SMS or email.If in doubt, call on the Phone Banking number of your Bank.

3. SMISHING

Smishing is a type of fraud that uses mobile phone text messages to lure victims into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web.

How do fraudsters operate?

Step – 1: Fraudsters send SMS intimating customer's of prize money, lottery, job offers etc. and requesting them to share their Card or Account credentials.

Step – 2: Unaware, the customer's follow instructions to visit a website, call a phone number or download malicious content.

Step – 3: Details thus shared with the person who initiated the SMS are then used to conduct fraudulent transactions on customer's account, causing them financial loss.

How to protect yourself from SMISHING:

1. Never share your personal information or financial information via SMS, call or email.
2. Do not follow the instructions as mentioned in SMS sent from un-trusted source, delete such SMS instantly.

4. PHISHING

What do you do when you come across emails that seem suspicious? Phishing is a type of fraud that involves stealing personal information such as Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc. through emails that appear to be from a legitimate source. Nowadays, phishers also use phone (voice phishing) and SMS (Smishing).

How do fraudsters operate?

Step – 1: Fraudsters pose as Bank officials and send fake emails to customers, asking them to urgently verify or update their account information by clicking on a link in the email.

Step – 2: Clicking on the link diverts the customer to a fake website that looks like the official Bank website – with a web form to fill in his/her personal information.

Step – 3: Information so acquired is then used to conduct fraudulent transactions on the customer's account.

How to identify fake Phishing website:

1. Verify the URL of the webpage. The's' at the end of 'https://' stands for 'secure' - meaning the page is secured with an encryption. Most fake web addresses start with 'http://'. Beware of such websites!

2. Check the Padlock symbol. This depicts the existence of a security certificate, also called the digital certificate for that website.

3. Establish the authenticity of the website by verifying its digital certificate. To do so, go to File > Properties > Certificates or double click on the Padlock symbol at the upper right or bottom corner of your browser window.

How to prmotect yourself from PHISHING:

1. Always check the web address carefully.
2. For logging in, always type the website address in your web browser address bar.
3. Always check for the Padlock icon at the upper or bottom right corner of the webpage to be 'On'.
4. Install the latest anti-virus/anti spyware/firewall/security patches on your computer or mobile phones.
5. Always use non-admin user ID for routine work on your computer.
6. DO NOT click on any suspicious link in your email.
7. DO NOT provide any confidential information via email, even if the request seems to be from authorities like Income Tax Department, Visa or MasterCard etc.
8. DO NOT open unexpected email attachments or instant message download links.
9. DO NOT access Net Banking or make payments using your Credit/Debit Card from computers in public places like cyber cafés or even from unprotected mobile phones.

5. MONEY MULE

Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen/illegal money via their bank account(s). When such incidents are reported, the money mule becomes the target of police investigations, due to their involvement.

How do fraudsters operate?

Step – 1: Fraudsters contact customers via emails, chat rooms, job websites or blogs, and convince them to receive money into their bank accounts, in exchange of attractive commissions.

Step – 2: The fraudsters then transfer the illegal money into the money mule's account.

Step – 3: The money mule is then directed to transfer the money to another money mule's account – starting a chain that ultimately results in the money getting transferred to the fraudster's account.

Step – 4: When such frauds are reported, the money mule becomes the target of police investigations.

How to protect yourself from MONEY MULE:

1. Do not respond to emails asking for your bank account details.
2. For any overseas job offer, first confirm the identity and contact details of the employing company.
3. Do not get carried away by attractive offers/commissions or consent to receive unauthorized money.

6. TROJAN

A Trojan is a harmful piece of software that users are typically tricked into loading and executing on their computers. After it is installed and activated, Trojan attacks the computer leading to deletion of files, data theft, or activation/spread of viruses. Trojans can also create back doors to give access to hackers.

How do fraudsters operate?

Step – 1: Fraudsters use spamming techniques to send e-mails to numerous unsuspecting people.

Step – 2: Customers who open or download the attachment in these emails get their computers infected.

Step – 3: When the customer performs account/card related transactions, the Trojan steals personal information and sends them to fraudsters.

Step – 4: These details will then be used to conduct fraudulent transactions on the customer's account.

How to protect yourself from TROJAN:

1. The first and best defense against Trojans is to never open an email attachment or run a program when you aren't 100 percent certain of the source.
2. Always keep your software up to date. This goes doubly true for important programs like your operating system and browser.
3. Keep your Internet connection as secure as possible.
4. Always keep a firewall up. Both software and hardware firewalls are excellent at controlling malicious Internet traffic, and can often stop Trojans from downloading to your computer in the first place.

Legal provisions for an OTP FRAUD case (IT Act & IPC)

How to get your money back if you fall victim to online fraud

As more and more people use online banking services, which are now reaching the unbanked under the financial inclusion programmes of the government, banking frauds are rising. Also, post demonetisation, there has been a sharp rise in online transactions.

Customer to get full refund

Banks will pay for the entire loss in the following cases.

- When a fraudulent transaction has happened due to deficiency or negligence on the part of the bank irrespective of the fact that the customer has reported it or not. "A digital transaction goes through various intermediary platforms such as the payer bank, the payee bank, the payment gateway, etc, and the transaction has to be encrypted. No data should be stored with either of the intermediaries but only transferred. Therefore, if a fraud happens during this process, the customer should not be held liable. As per RBI recommendations, the bank will have to refund to the customer," says Mehta of Deloitte Haskins and Sells.

➢ When there is a third-party breach where the deficiency lies neither with the bank nor the customer but with the system somewhere else and the customer notifies the bank regarding the transaction within three working days.

THE REFUND RULES

Time taken to report the fraudulent transaction from the date of receiving the communication	Customer's liability
Within three working days	Zero liability
Four-seven working days	The transaction amount or the amount mentioned in the maximum liability table, whichever is lower
Beyond seven working days	As per the bank's board-approved policy
Maximum liability of a customer in case the cutomer reports fraud in 4 to 7 days	
Type of account	Maximum Liability (Rs)
Basic savings bank deposit account	5,000
All other savings bank accounts	10,000
Prepaid payment instruments and gift cards	
Current and overdraft accounts of medium and small enterprises	
Individual current/overdraft accounts with annual average balance of up to Rs 25 lakh in past one year	
Credit card with limit up to Rs 5 lakh	
All other current and overdraft accounts	25,000
Credit cards with limit above Rs 5 lakh	

Legal provisions for the OTP FRAUD victims:

1. The victims who lose money through 'One Time Password (OTP) fraud' can inform The Police /Banks within an hour to prevent permanent loss of money.
2. The Banks have powers to alert banking wallet system administrators and withhold the transactions. Victims should not delete the SMS showing the money had been debited,"

Reporting OTP fraud

The procedure for reporting OTP related crimes is more or less the same as for reporting any other kind of offence. The local police stations can be approached for filing complaints just as the cyber crime cells specially designated with the jurisdiction to register complaint.

Major and Minor Law sections dealing with OTP FRAUD Cases

Sec 420 IPC

This section deals with Cheating and dishonestly inducing delivery of property. The maximum punishment which can be awarded is imprisonment for a term of 7 year and fine.

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce.

Section 66C of The Information Technology Act, 2000

Punishment for identity theft - 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.

Section 66D of The Information Technology Act, 2000

Punishment for cheating by personation by using computer resource-Whoever, by means for any communication device or computer resource cheats by personating shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Investigation of OTP FRAUD cases (Step by Step)

BASIC STEPS ON INVESTIGATING OTP Fraud cases

Step – 1: Interview the complainant

Investigator will conduct initial assessment to determine if the complaint will fall under OTP fraud.

Step –2: Complainant must file a complaint sheet with brief narrative of the incident

This may include presentation of pieces of evidence that the complainant previously secured in relation to his/her complaint.

Step – 3: Documentation of Evidence

Investigator must document the concerned complaint on the website by capturing a screenshot or save the webpage as PDF file indicating the URL. This may also include the following

- Full header in case of email
- ISP of the IP address concern
- Save all the gathered digital evidence in one folder with appropriate name.

Step – 4: Request for the conduct of the digital forensic Examination

In case that there is/are electronic evidence presented, Investigator will prepare necessary memorandum request to Digital forensic section for the conduct of forensic examination on the submitted electronic evidence.

Step – 5: Coordination ,verification and preservation with ISP/money transfer agency.

Step – 6: Coordination ,verification and preservation with website admin of the bank account.

Step – 7: Preparation of MLAT request (mutual legal assistatnce treaty) if any.

Step – 8: Preparation and application for court order to ISP to give the preserved information requested.

Step – 9: Investigation Report.

Case study

Case 1:

Narendra Pal, a government school teacher in Zirakpur near Chandigarh, got the shock of his life when he received an sms just before midnight that Rs 10,000 has been withdrawn from his account through an ATM in Surat. By the time he could realise what was happening, he got two more messages about withdrawal of Rs 10,000 and Rs 20,000. He had fallen victim to online fraud. As the first debit happened a few minutes before 12 midnight, the fraudster was able to transact again immediately as withdrawal limit for the next day set in.

Pal informed his bank about the transactions immediately by calling on the helpline number. He also wrote to the bank branch and the RBI that he had not shared details of his bank account and ATM card with anyone. He also filed a complaint with the crime branch's cyber cell. The officers took him to the petrol pump where he had last used the card but nothing came out of it. Pal says the bank staff was cooperative but still it took him more than two months and two-three visits to the branch to get his money. He had to forgo the interest.

People like Pal need not worry now. The RBI has come out with guidelines that say the bank will have to make good the entire loss if the customer notifies it about the unauthorised/fraudulent transaction within a stipulated period.

Case 2:

The latest in the list are two residents of Alangad who were almost duped of their money after they shared the One Time Password (OTP) with the fraudsters who in turn used it for making online purchase worth Rs. 69,507.

However, their money was not lost since they had the presence of mind to alert the Ernakulam Rural Cyber Cell immediately after they received mobile alerts of money debited from their bank accounts.

The fraudsters adopted the tried and tested method of ringing up the victims posing as bank officials and asked for the OTP in the guise of renewing their expired credit card. The victims realised their folly only when they received mobile alerts about the loss of Rs.40, 000 and Rs.29, 507 respectively.

It is a usual ploy of fraudsters to ring up unsuspecting people and ask for the OTP in the name of linking Aadhaar, renewal of ATM or credit card or for redeeming reward points.

The cyber cell officials found out that the fraudsters used the money for online purchase using e-wallets. They immediately contacted the e-commerce sites concerned and directed them to cancel the order and the money was credited back to the accounts. Investigation is on to trace the fraudsters.

Following the incident, the Ernakulam Rural Police issued a public advisory warning against falling into the hands of online fraudsters by sharing OTP/ATM pin/CVV numbers with strangers.

Despite repeated alerts by banks and the police, people continue to fall victims to the most rudimentary tricks of online fraudsters.

How to protect yourself from fraud

- Never open e-mails or download attachments from unknown senders. Simply delete such emails.
- Installing antivirus helps. It scans every file you download and protects you from malicious files.
- Enable automatic OS updates or download OS patch updates regularly to keep your Operating System patched against known vulnerabilities.

- Install patches from software manufacturers as soon as they are distributed. A fully patched computer behind a firewall is the best defense against Trojan.
- Download and use the latest version of your browser.
- If your computer gets infected with a Trojan, disconnect your Internet connection and remove the files in question with an antivirus program or by reinstalling your operating system. If necessary, get your computer serviced.

Secure Net-Banking Tips

- ✓ Keep your Customer ID and password confidential and do not disclose it to anybody.
- ✓ Change your password as soon as you receive it by logging into your Net Banking account. Memorize your password; do not write it down anywhere.
- ✓ Avoid accessing internet banking from shared computer networks such as cyber cafes or public Wi-Fi network like hotel/airport etc.
- ✓ Do not click on links in the emails or sites other than the genuine net banking site of your Bank to access your Net Banking webpage.
- ✓ Always visit the Bank's Net Banking site through Bank's home page by typing the bank's website address on to the browser's address bar.
- ✓ Always verify the authenticity of the Bank's Net Banking webpage by checking its URL and the PAD Lock symbol at the bottom corner of the browser.
- ✓ Disable "Auto Complete" feature on your browser.

- ✓ Uncheck "User names and passwords on forms", click on "Clear Passwords" & Click "OK"
- ✓ Use virtual keyboard feature while logging into your internet banking account.
- ✓ Do cross check your last login information available on Net Banking upon every login to ascertain your last login and monitor any unauthorized logins.
- ✓ Always type in your confidential account information. Do not copy paste it.
- ✓ Monitor your transactions regularly. Use Bank's Alerts service and bring any fraudulent transaction to the notice of the bank.
- ✓ Always logout when you exit Net Banking. Do not directly close the browser.

Secure ATM Banking Tips

- ✓ Memorize your PIN. Do not write it down anywhere, and certainly never on the card itself.
- ✓ Do not share your PIN or card with anyone including Bank employees, not even your friends or family. Change your PIN regularly.
- ✓ Stand close to the ATM machine and use your body and hand to shield the keypad as you enter the PIN. Beware of strangers around the ATM who try to engage you in any conversation.
- ✓ Do not take help from strangers for using the ATM card or handling your cash
- ✓ Do not conduct any transaction if you find any unusual device connected to your ATM machine.

- ✓ Press the 'Cancel' key and wait for the welcome screen before moving away from the ATM. Remember to take your card and transaction slip with you.
- ✓ If you get a transaction slip, shred it immediately after use if not needed.
- ✓ If your ATM card is lost or stolen, report it to your bank immediately
- ✓ When you deposit a cheque or card into your ATM, check the credit entry in your account after a couple of days. If there is any discrepancy, report it to your bank.
- ✓ Register your mobile number with the Bank to get alerts for your transactions
- ✓ If your card gets stuck in the ATM, or if cash is not dispensed after you keying in a transaction, call your bank immediately
- ✓ If you have any complaint about your ATM/Debit/Credit card transaction at an ATM, you must take it up with the bank

Secure Phone Banking Tips

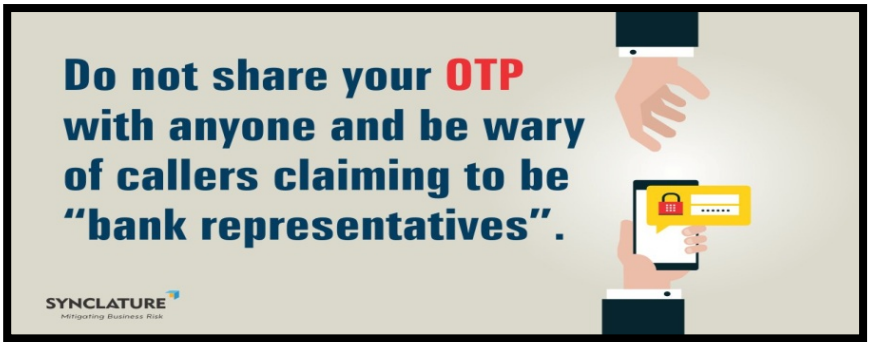
- ✓ While talking to the Phone Banking officer, never disclose the following

  (The 4 digit ATM/IVR PIN, OTP, Net Banking password & CVV (Card Verification Value))
- ✓ Ensure that no one sees you entering you PIN (personal identification number).
- ✓ Avoid giving verification details to the Phone Banking officer while in public places.
- ✓ The Phone Banking channel is meant to be used by the account holder only. Do not transfer the line or hand over the phone to any other person after you complete self-authentication.

Secure Online Shopping Tips

- ✓ Always shop or make payments through trusted/reputed websites.
- ✓ Do not click on links in emails. Always type the URL in the address bar of the browser.
- ✓ Before entering your private details, always check the URL of the site you are on!
- ✓ If you are a frequent online shopper, signup for Verify by Visa and Master Card secure code program.
- ✓ Check your account statements regularly and bring any fraudulent transaction to the notice of the bank.
- ✓ Check for PAD LOCK symbol on the webpage before starting to transact.
- ✓ Do not click on links in emails or on referral websites to visit the online shopping site. Always type the URL in the address bar.
- ✓ Do not enter your confidential account information such as Credit Card Numbers, Expiry Date, CVV values, etc. on any pop-up windows.
- ✓ Use One Time Password (OTP) received on the mobile phone instead of static Visa and Master Card secure code password as OTP are more secure.

ALWAYS KEEP IN MIND



Bibliography

- https://economictimes.indiatimes.com/wealth/plan/dont-get-cheated-by-online-fraudsters-heres-how-to-protect-yourself/articleshow/53462567.cms
- https://timesofindia.indiatimes.com/city/hyderabad/fraudsters-use-code-to-bypass-otp-cases-on-rise/articleshow/63758796.cms
- https://www.thehindu.com/news/cities/Kochi/despite-warnings-people-still-fall-prey-to-otp-fraud/article23931321.ece
- http://calert.info/details.php?id=1669
- https://www.businesstoday.in/magazine/money-today/banking/know-your-rights-in-case-you-fall-victim-to-a-fraudster/story/257827.html
- https://www.google.co.in
- http://keralapolice.gov.in/wings/training/police-training-college

****

Department of Electronics and Information Technology

Framework & Guidelines for Use of Social Media for Government Organisations

Department of Electronics and Information Technology

Ministry of Communications & Information Technology

Government of India

Executive Summary

Information Communication Technologies (ICTs) including internet and mobile based communications are increasingly becoming pervasive and integral to day-to-day functioning of our lives- whether personal or official. ICTs offer an unprecedented opportunity of connecting to each and every individual and design the communication structure accordingly to each person. Such a structure can be defined and re-defined by both initiator and receiver of communication. Such a medium of communication is referred to as Social Media and it is transforming the way in which people connect with each other and the manner in which information is shared and distributed.

While at a personal level, the uptake and usage of such media is gaining rapid popularity, use and utility of such media for official purpose remain ambiguous. Many apprehensions remain including, but not limited to issues related to authorisation to speak on behalf of department/agency, technologies and platform to be used for communication, scope of engagement, creating synergies between different channels of communication, compliance with existing legislations etc.

In order to encourage and enable government agencies to make use of this dynamic medium of interaction, a Framework and Guidelines for use of Social Media by government agencies in India has been formulated. These guidelines will enable the various agencies to create and implement their own strategy for the use of social media. The document will help them to make an informed choice about the objective, platforms, resources, etc. to meet the requirement of interaction with their varied stakeholders.

The guidelines provide an in depth review of types of social media, their characteristics and challenges in their uses. In order to assist the departments to undertake such an engagement, the document provides for a framework and detailed guidelines governing

each element of the framework. Briefly, the elements of the framework and associated guidelines are given below. The framework comprises of the following 6 elements:

- Objective: Why an agency needs to use social media
- Platform: Which platform/s to use for interaction
- Governance: What are rules of engagement
- Communication Strategy: How to interact
- Pilot: How to create and sustain a community
- Institutionalisation: How to embed social media in organisation structure Some of key caveats that the guidelines highlight and must be kept in mind include:
- All accounts must be created and operated in official capacity only
- As social media demands 24*7 interactions, some responsiveness criteria may be defined and a dedicated team may be put in place to monitor and respond
- There should be congruence between responses on social media and traditional media
- Relevant provisions of IT Act 2000 and RTI Act must be adhered to.

Detailed description and explanations are given in the Guidelines section of the document.

Social Media is being used across the world by different government agencies. The document also illustrates some examples from India as well from other countries to demonstrate the purpose and use of such media. It is believed that the Framework and Guidelines will be useful for departments and agencies in formulating their own strategies and will help them in engaging in a more fruitful manner with their respective stakeholders.

Guidelines for Use of Social Media by Government

I. Introduction

The advent of social media is transforming the way in which people connect with each other and the manner in which information is shared and distributed. It is different from traditional media such as print, radio and television in two significant ways – first, the amount of content that can be generated by the users themselves far exceeds the content generated by news/opinion makers and second, its "viral" ability for potential exponential spread of information by word of mouth and interlinking of the various social media platforms, thereby considerably reducing the control over spread of any such information.

These characteristics denote the paradigm shift from Web 1.0 technologies that enabled simple information sharing and basic two-way transactions to Web 2.0 – where literally everyone is/can be a user as well as generator of content. Social media is redefining the way people communicate with one another.

In order to encourage and enable government agencies to make use of this dynamic medium of interaction, a Framework and Guidelines for use of Social Media by government agencies in India has been formulated. These guidelines will enable the various agencies to create and implement their own strategy for the use of social media. The document will help them to make an informed choice about the objective, platforms, resources, etc. to meet the requirement of interaction with their varied stakeholders.

II. Need for Social Media Guidelines

Given its characteristics to potentially give "voice to all", immediate outreach and 24*7 engagement, Social Media offers a unique opportunity to governments to engage with their stakeholders especially citizens in real time to make policy making citizen centric. Many governments across the world as well many government agencies in India are using various social media platforms to reach out to citizens, businesses and experts to seek inputs into policy making,

get feedback on service delivery, create community based programmes etc.

However, many apprehensions remain including, but not limited to issues related to authorisation to speak on behalf of department/agency, technologies and platform to be used for communication, scope of engagement, creating synergies between different channels of communication, compliance with existing legislations etc.

It was therefore felt that Guidelines for use of Social Media were required which would enable project owners/implementers to effectively use these platforms.

III. Target Audience

The Framework and Guidelines have been developed for all government agencies including Public Sector Undertakings to help them conceptualise and evolve their Social Media interactions and strategy.

IV. Social Media

4.1 What is Social Media

Social Media in recent times has become synonymous with Social Networking sites such as Facebook or Micro Blogging sites such as Twitter. However, very broadly social media can be defined as any web or mobile based platform that enables an individual or agency to communicate interactively and enables exchange of user generated content.

4.1.1. Social Media Characteristics

Critical characteristics of social media are

- Connectedness: This attribute showcases the media's ability to connect and reconnect like-minded people or people interested in same topics and domains. Through this media, 24*7 connectedness is possible through a variety of media and

access devices including PCs, Laptops, mobile phones etc. Individuals re-tweeting & following other people's comments and status and updating their own account at all hours are examples of this attribute.

- **Collaboration:** The connections achieved on this media, enable people to collaborate and create knowledge. Such collaborations can be either open or closed. Wikipedia is an example of open collaboration which enabled creation of an open web based encyclopedia through contribution from hundreds of thousands of people. Gov Loop is an example of closed collaboration wherein experts groups contribute on specific policy matters.

- **Community:** Connectedness and collaboration helps create and sustain communities. These communities can create awareness about various issues and can be used for seeking inputs into policy making, building goodwill or even seeking feedback into delivery of public services.

Pictorially, the characteristics have been depicted below to show the inter-linkages between all characteristics and their mutual dependency.

Figure 1: Characteristics of Social Media

4.2 Need for Using Social Media

With the ever increasing diffusion of ICTs in all walks of lives, connectedness is increasingly becoming a given part of our lives. This connectedness brings with it many opportunities and also presents many challenges. From the perspective of governments, the following represent some of the reasons for using social media:

- Enhanced Outreach: As the recent world events have demonstrated, social media have emerged as a powerful platform for forming an opinion as well as generating mass support. In India, Facebook alone has over 40 million users each. Even a microblogging site Twitter has about 16 million users. These sites offer an opportunity to reach out this audience at a key stroke. Many of these facilitate access through mobile devices and withnearly 900 million mobile users in India, it offers an unprecedented outreach.

- Real Time engagement: Social Media releases the shackles of time and place for engagement. They can connect policy makers to stakeholders in real time. In recent Libyan crisis, Ministry of External Affairs used social media platforms such as Twitter to assist in locating and evacuating Indian Citizens from Libya.

- Individual Interaction: In tradition forms of media, interaction with individual user is either not possible or is very limited. Social Media platform offers the ability to connect with each and every individual. Such an interaction also enables the marginalised to participate in discussions and present their point of view, thereby improving the political position of marginalized or vulnerable groups. It is specifically useful when seeking feedback on services rendered.

- Managing Perceptions: One of the big challenges for government is to avoid propagation of unverified facts and frivolous misleading rumours with respect to government policies. Leveraging these platforms can help to counter such perceptions and present the facts to enable informed opinion making.

4.3 Types of Social Media

Kaplan and Haenlein in 2010 classified social media into six different types: collaborative projects, blogs and microblogs, content communities, social networking sites, virtual game worlds, and virtual social worlds. A brief description of some of the most common types of social media is given below:

- Social Networking : Social Networking is an online service that enables its users to create virtual networks with likeminded people akin to social networks in real life. It often offers the facilities such as chat, instant messaging, photo sharing, updates, etc. Currently, social networking sites are the most prominent version of social media. Facebook with 800 million users is one of the most well known social networking site.

- Blogs: Blogs are descriptive content pages created and maintained by individual users and may contain text, photos and links to other web sites. The main interactive feature of Blogs is the ability of readers to leave comments and the comment trail can be followed.

- MicroBlogs: Micro Blogs are similar to Blogs with a typical restriction of 140 characters or less, which allows users to write and share content. Twitter is the most well known micro blogging site.

- Vlogs and Video Sharing sites: Video Blogs or Vlogs are blogging sites that mainly use video as the main form of content supported by text. YouTube is the largest video sharing site.

- Wikis: A Wiki is a collaborative website that allows multiple users to create and update pages on particular or interlinked subjects. While single page is referred to as "wiki page" the entire related content on that topic is called a "Wiki". Wikipedia is the pioneering site of this type of platform.

A more detailed description of the different types of social media, their characteristics is given in ***Annexure I***

4.4 Core Values for Using Social Media

Unlike other traditional media, social media is more interactive, enables one-to-one conversation and demands immediacy in response. Also, on such platforms the perception of official and personal roles and boundaries is often blurred. Therefore, while using social media for official purposes, the following may be kept in mind to smoothen interaction:

- Identity: Always identify clearly who you are, what is your role in the department and publish in the first person. Disclaimer may be used when appropriate

- Authority: Do not comment and respond unless authorized to do so especially in the matters that are sub-judice, draft legislations or relating to other individuals

- Relevance: Comment on issues relevant to your area and make relevant and pertinent comments. This will make conversation productive and help take it to its logical conclusion

- Professionalism: Be Polite, Be Discrete and Be Respectful to all and do not make personal comments for or against any

individuals or agencies. Also, professional discussions should not be politicized

- Openness: Be open to comments – whether positive or negative. It is NOT necessary to respond to each and every comment
- Compliance: Be compliant to relevant rules and regulations. Do not infringe upon IPR, copyright of others
- Privacy: Do not reveal personal information about other individuals as well as do not publish your own private and personal details unless you wish for them to be made public to be used by others

4.5 Challenges in Using Social Media

a) Why to use social media: Departments sometimes find it difficult to define the need or objective to use social media. Is it for providing information, seeking feedback, generic interaction, etc. Due to this lack of clarity, departments often either choose not to use social media or attempt to be present on all platforms at once.

b) Which Platforms to use: Given the plethora of platforms and even types of social media, it is very difficult to choose the type and no. of platform on which to engage and how to create inter-linkages between these platforms.

c) Who will engage: Most departments have limited capacity to engage with traditional media itself and since social media demands a deeper and constant interaction, availability of such resources is even more limited. A closely associated question is that of authority i.e. who is authorised to respond on behalf of the department, whether such a response will be

made in personal or official capacity and from personal or official account etc.

d) How to engage: Use of social media is an ongoing process and requires long term commitment. Many have questions around rules of engagement – how to create and manage an account, what should be response time, what are the legal implications etc.

In order to help departments and government agencies to meet these challenges, Guidelines for use of Social Media have been drafted. In the following section, various elements of the Framework and the Guidelines to use the different elements of Framework have been detailed.

V. Social Media Framework & Guidelines for Government Organisations

The Social Media Framework for the Government of India has been created to enable government agencies to use these platforms more effectively and reach out to their stakeholders and understand their concerns and hear their voices. The Framework comprises of the following 6 elements:

- Objective: Why an agency needs to use social media
- Platform: Which platform/s to use for interaction
- Governance: What are rules of engagement
- Communication Strategy: How to interact
- Pilot: How to create and sustain a community
- Engagement Analysis: Who is talking about what, where and what are the main points of conversations
- Institutionalisation: How to embed social media in organisation structure

Pictorially the framework can be represented as given below:

Figure 2: Social Media Framework

(Adapted from http://www.rossdawsonblog.com/SocialMediaStrategyFrameworkv1.pdf)

The next section elaborates on each element and provides guidelines on important aspects and caveats of each element. The guidelines also use examples from India and across the world to illustrate each element.

5.1. Guidelines for Using Social Media by Government Organizations

This section provides the users in government organizations, a set of guiding principles that may be used while making use of Social Media. The section will illustrate through appropriate examples, some of the critical aspects of each element.

5.1.1 Define Objectives:

The objective for the use of social media is not just to disseminate information but also to undertake public engagement for a meaningful public participation for formulation of public policy. Government organisations are exploring the use of social media for public engagements for disseminating information, policy making, recruitment, generating awareness, education etc. about public services. Therefore, Social Media may be used for:

- Seeking feedback from citizens
- Re-pronouncement of Public Policy
- Issue based as well as Generic interaction
- Brand Building or Public Relations
- Generating Awareness and education on National Action Plans and implementation strategies

In the Indian context, care must be taken so that people can communicate in their own language, and due cognizance of the views expressed in local languages is taken.

5.1.2 Choosing Platforms:

Having defined the objectives, the next step is to identify platforms and phases in which such an engagement shall be undertaken at these platforms. While social networks currently seem to be the face of social media, they are not the only platform. Some of

the other forms of social media include, Social bookmarking site – stumble upon; transaction based platforms – Amazon & eBay; self publishing media – You Tube, Picasa; Business management etc. Since the choices are many, it is essential to identify one or two key platforms from which the department may begin interaction. Based on objective and response, the basket of platforms may be enhanced.

Government departments and agencies can engage social media in any of the following manner:

- By making use of any of the existing external platforms, or
- By creating their own communication platforms
- The choice of the platform – whether owned or externally leveraged should be made based on the following factors:
- Duration of engagement - whether the engagement sought is to be an ongoing activity or created for a specific time-bound purpose
- Type of Consultation – whether the consultation is open to public or confined to a particular group of stakeholders e.g. experts
- Scope of Engagement – whether the consultation requires daily, weekly, bi-weekly or even hourly interaction
- Existing Laws – whether existing laws permit use of such platforms and the requirement under such laws regarding data protection, security, privacy, archiving etc.

5.1.3 Governance Structure:

Since use of social media is a 24*7 engagement, the extant rules and regulations of media interaction do not fully apply to them.

Two most important aspects of social media are its:

- viral characteristic – news spreads exponentially; and
- demand for instant gratification – queries, responses and counter-responses are posted instantaneously.

However, since the official pages of departments must reflect the official position, some measure of control must be included in the flexible design of communication.

Just as rules and regulations exist for interaction with traditional media, similar rules must be created for engaging with social media.

Some of the key aspects of such a governance structure include:

5.1.3.1 . Account Governance

- Account Creation: A social media account establishes an organisation's online identity. Wherever possible, the same name for the different social networking accounts may be adopted to ensure ease of search on the internet. Another important facet of online identity is the need for it to be rendered effectively in either long form e.g. website address or in 15 characters or less (this is the Twitter maximum).
- Login and passwords: Each new account requires a URL, user name and/or email address and a password. A proper record of login ids and password must be maintained. This is critical as multiple people may be authorised to post on behalf of the department.
- Account Status: It is important to define whether the engagement may be undertaken through official accounts only or the officials may be permitted to use personal accounts also

for posting official responses. It determines who says what on behalf of your organisation and in what form it is published. It also outlines how each piece of published information is presented where it is published. The most important aspect is whether the responses are in Official or Personal Capacity.

5.1.3.2. Response and Responsiveness:

Responsiveness: This indicates the how often would the pages/information be updated, in what manner would the responses be posted, what would be the turnaround time of responses etc. The major attraction of social media is the spontaneity and immediacy of response and feedback and those visiting the site would expect the some kind of response within a pre-defined time limit.

As far as possible, it is important to state upfront the scope of response – given/not given, type of response – official/unofficial, response time – 1 day/1 week etc. so that expectations are set correctly. Some of the ways to ensure timely response is Email integration i.e. email writing, list management, list building, proper lead direction so the right internal person takes actions on leads in a timely fashion and Daily management/maintenance of social media platform messages, customer contacts, etc.

Response*:* While creating a policy for responses, it may be noted that -

- Not all posts/comments need to be responded to immediately and individually. Also, wherever a response is required all posts should be kept short and to the point.
- While employees are free to post response in their personal capacity, it is mandatory that while they are doing so, they must clearly identify themselves, confidential information must not be divulged and should not be seen to represent "official view" unless authorized to do so.

- Another important aspect that needs to be addressed is the Escalation Mechanism.
    - There has to be a defined hierarchy not only of responses but also of queries. For example, the comments and queries may be classified as routine – for which a Frequently Asked Question (FAQ) and Fixed Response Format (FRF) may be applied.
    - The next level may be queries/comments related to projects/programme, for which no separate official response may be needed because all relevant information may be available in the public domain and the query may be responded accordingly.
    - The next level of query/comment may be more specific where an "official" response may be needed. Such a categorization will help organizations in streamlining their responses.
    - Finally, there should be congruence between responses posted on social media and those in traditional media.

5.1.3.3. Resource Governance

Allocation of Resources: Since using social media is a resource intensive exercise, it is important to ensure that resources and their responsibilities are clearly marked out very early. Many organisations have a dedicated team including outsourced resources to manage their engagement while others primarily uses internal resources. More often than not, it is advisable to create a dedicated team. One of the key issues that impacts the resource requirement is whether the conversation is moderated or un-moderated. In case of moderated conversation, dedicated resource/s is critical. One of the key resources is an internal champion within the system who can lead the strategy within the department. It is important to note that since the

engagement in social media requires different skill sets, the champion and other resources identified would require orientation & training specifically for the tasks assigned to them and keep abreast of the fast paced developments in this media

Roles & Responsibilities: The roles and responsibilities of the team responsible for creating, managing and responding on social media platforms must be clearly defined.

- In Indian context, they may also need to be aligned to roles and responsibilities defined for responding to RTIs.
- For most interactions, flexibility may be given to the staff to respond to regular queries or comments.
- Escalation mechanism defined in the governance structure must clearly define accountability at all levels.
- The role definition must not be limited just to responses, but also include responsibility for matters related maintenance of login ids and passwords, issues related to data security, archives, privacy, etc. For example, while the existing web content team may be assigned the responsibility for responding to usual queries; special technical expertise may be required to ensure appropriate levels of security.

Accountability: Clearance systems that distinguish between situations when an official position is required, and when open conversation is appropriate. This has to have at its heart a redefinition of accountability. The officials designated for engagement with citizen using the social media should be covered under a well defined immunity provision in consonance with the RTI Act and the IT Act and the IT Amendment Act 2008.

5.1.3.4. Content Governance:

Content Creation & Social media profiles overlap, therefore sharing consistent content on all social media platforms should form the bedrock of content policy. While the social media tools allow everyone to become a creator, for the official account, content will have to be specified and tailored to the site on which it is being published.

Accessibility: In order to enable wider participation, content creation and availability should be in Indian languages and must not be limited to text alone. The content should follow the Government of India Guidelines for Website and adequately address challenges related to accessibility in Indian Languages as well as accessibility of content for differently abled.

Moderation*:* A moderation policy should also be published if the platform permits others to add their own content; this informs people what they can post whilst protecting others who may visit your platform. The moderation policy should include matter related to copyright, rights to addition and deletion etc.

Records Management: When any information is shared or guidance given online, it is necessary to ensure that all relevant records are captured, trail is generated and records are managed appropriately. It is important that the rules regarding record keeping are states upfront so that those seeking historical data are aware of statutes and limitations. Some of the important aspects that may be kept in mind while defining record management guidelines are as under:

- The requirements for existing legislations e.g. RTI etc. need to be kept in mind and are paramount in influencing decisions regarding record keeping
- Ordinarily, if online consultations do not impact decision making, lead to or influence policy making (e.g. seeking information about nodal officers, or any other public document, or responding to generic comments such as

governance should be improved etc.) the agencies may decide that no record of such interactions will be maintained.

- However, if consultations are necessarily being undertaken on specific policy or governance issues or that may influence decision making (e.g. inputs into Plan Document, consultation on policy frameworks etc.) then all necessary records need to be maintained. If the agency is using a social media site that does not facilitate record keeping, then there are various other options that may be explored. Some of the options are given below and may be exercised based on need and resources available:
    - Records may be created agency's internal platform and records be maintained with appropriate tags e.g. creator/sender, dates, posting site etc.
    - Screenshots may be captured and stored in soft or hard (copy) format and filed at appropriate place.
    - A summary may be created of the information/ consultation and filed.

Since most of the social media platforms are based outside India and are not governed by Indian Laws, or managed and controlled by Indian regulations, specific policies may be drafted related to information security and archiving. If required the agencies may engagewith the Social Media Service Providers to work out Service Level Agreements for

- Complaint and response mechanism between the agency and the Service Provider
- Content Storage
- Shared access of the content
- Archival mechanisms

5.1.3.5. Legal Provisions: In India, the legal implications must be viewed in accordance with the law of land e.g. RTI Act, IT ACT 2000& IT Amendment Act 2008 etc as also rules and regulations made thereunder. These policies must be circulated internally to ensure uniformity of response. Some of the key sections and their implications that must be kept in mind are as under:

5.1.3.5.1. When Government department provides such social media facilities on its network, receives, stores or transmits any particular electronic record on behalf of another person or provides any service with respect to that record, they become intermediary under Section 2(1)(w) of the amended Information Technology Act, 2000. Section 79 of the amended Information Technology Act, 2000 provides the broad principle that intermediaries like Government departments providing social media facilities are generally not liable for third party data information or communication link made available by them. However this exemption from liability can only be applicable if the said Government department complies with various conditions of law as prescribed under Section 79 of the amended Information Technology Act, 2000. The said conditions which need to mandatorily complied with the Government department to claim exemption for any third party data information or communication link made available or hosted by them in connection with social media facilities made available by the said department on their network are as follows:

- The function of the Government department is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or hosted

- The Government department does not

  i) initiate the transmission,

ii) select the receiver of the transmission, and

iii) select or modify the information contained in the transmission

- The Government department observes due diligence while discharging its duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

- That the Government department as intermediary must not conspire or abet or aide or induce, whether by threats or promise or otherwise in the commission of the unlawful act.

- That the Government department must immediately after receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the Government department is being used to commit the unlawful act, must expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

- The Government department must also comply with all applicable rules, regulations and notifications in regard to their activity of providing social media facilities on its network.

- That the Government department complies with the Information Technology (reasonable security practices and procedures & sensitive personal data or information) Rules, 2011.

- That the Government department also complies with the Information Technology (Intermediary guidelines) Rules, 2011.
- That the Government department also implement reasonable security practices and procedures as envisaged under Section 43A of the amended Information Technology Act, 2000.

5.1.3.6. Data & Information Security Governance:

The Government's communication to citizens via social media should follow the same data retention policy as its communication through other electronic and non-electronic channels. Data portability compliance varies from one social media platform to another. Hence, privileged access may be mandated by the Government along the same lines "take down notices" and "information requests" currently being sent to social media and other platforms for intellectual property rights infringement and other offences.

Provisions related to Personal Information & Security: Under the Information Technology Act 2000, the Central Government has enacted various rules and regulations which impact social media. Some of the most important in this regard are as follows:

i. The Information Technology (reasonable security practices and procedures &sensitive personal data or information) Rules, 2011 define provisions for personal information & security and what constitutes sensitive personal data. Sensitive personal data or information of a person means such personal information which consists of information relating to;—

   a. password;

   b. financial information such as Bank account or credit card or debit card or other payment instrument details;

c. physical, physiological and mental health condition;

d. sexual orientation;

e. medical records and history;

f. Biometric information;

g. any detail relating to the above clauses as provided to body corporate for providing service; and

h. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

ii. For the purposes of protecting such sensitive personal data, the Government has mandated that any legal entity who is processing, dealing or handling sensitive personal data must implement reasonable security practices and procedures.

iii. The Government further stipulate that ISO 27001 is one acceptable standard of reasonable security practices and procedures. Thus, all Government departments which are providing social media facilities must comply with ISO27001.

iv. Further under the Information Technology (Intermediary guidelines) Rules,2011, since the said Government department who is provide social media facilities is an intermediary, it has to comply with the Information Technology(Intermediary guidelines) Rules, 2011. Under Rule 3(4) of the said rules, the Government department shall act within thirty six hours on

receiving the written complaint form an affected person and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2).

v. Further the Government department shall preserve such information and associated records for at least ninety days for investigation purposes.

vi. In case, if the Government department does not comply with any of the above requirements of law, then the said Government department as also the concerned head of the department who is responsible for the social media facilities and the concerned IT head would be liable for civil and criminal consequences.

vii. The civil consequences could consist of being sued for damages by way of compensation upto 5 crore Rupees under summary proceedings before the adjudicatory authorities specially constituted under the Information Technology Act, 2000. Further if person wants, they can sue the said Government department for damages beyond 5 crore Rupees in a court of competent jurisdiction.

viii. In case the concerned Government department does not comply with all the aforesaid laws, the said Government department as also the person heading the department and the concerned IT head would also be liable for criminal liability which could range from imprisonment of 3 years to life imprisonment and fine which could range from 1 lakh to 10 lakh Rupees.

Rules for Privacy and data collection: While social networking enables greater transparency, it is equally important to ensure the protection of people from exposure to inappropriate or offensive material.

- Since profiles on social network are linked more often to individuals and not organisations, for the organisation's site/page, a separate work profile may be created which can then be linked to a general email address that is accessible to anyone in the team, enabling them to administer the social networks without compromising on individual privacy.

- It is critical that social media policy for the Government is compliant with existing law governing data protection and privacy. Each department of the Government may be recommended to publish their own set of additional protections to safeguard privacy of citizens while maintaining highest levels of transparency of Government bodies.

- If the departments/agencies are collecting personal information on a social media platform, the same must be stated upfront. For example, while seeking inputs on a particular policy, it is may not be necessary to save the email id of each and every respondent and just saving the responses may suffice.

Identity Management: Identity management for the purposes of this document refers to management of identities of individual/s who seek to engage with government agencies on social media platforms. Such management relates specifically to registration mechanisms, delineation of personal identity from official identity of government officials and need to engage in a non-anonymous manner in such

consultations. Towards this end, the departments may like to use following or any other suitable mechanism to achieve the above:

- Provide for activation of registration for engagement by seeking confirmation of email addresses
- Send acknowledgement/responses to queries to registered email addresses
- Providing official email ids and accounts to each and every government official authorised to engage on behalf of the department and permit use of only official accounts for engagement However, while applying the above, The Information Technology (reasonable security practices and procedures & sensitive personal data or information) Rules, 2011 stated in the preceding paragraphs above must be complied with.

The relevant sections of the Information Technology Act 2000 are placed in Annexure III for ready reference. In addition, the users may refer to any other relevant legislations, provisions and rules notified.

5.1.4 Communication Strategy:

Some of key aspects of communication strategy include – Integration of Social Media into routine, Connection with existing networks, Sharing content across sites and Publicising use of social networking through traditional media.

- Social media can only be used by the Government to communicate existing Government information and propagate official policy to the public.
- While the social media tools allow everyone to become a creator, for the official account, content will have to be specified and tailored to the site on which it is being published.

- Great care must be taken to avoid propagation of unverified facts and frivolous misleading rumours which tend to circulate often through miscreants on social media platforms.

- It must be reiterated here that social media should only be one of the components of the overall citizen engagement strategy and government departments must desist from using only social media to communicate with their stakeholders.

- Initially, the departments may just aim to post information regularly. For example, if it is a Facebook Page, postings may be done at least a couple of times a week and on Twitter slightly more frequently.

- Ideally, none of the sites should be left more than a week or two without new content.

5.1.5 Creating Pilot:

Since social media are relatively new forms of communication, it is always better to test efficiency and efficacy of such an initiative with a pilot project. Some of principles of creating such a pilot are given below:

- Focused Objective setting: Initiate interaction for a limited objective or limited to one topic

- Begin Small: It is always better to start small and it is advisable to begin with one or two platforms.

- Multiplicity of access: The chosen platform should typically permit inputs from or linkages through multiple access devices. This will ensure wider participation.

- Content Management: It is not enough just register presence on a variety of platforms. It is essential that content provided is topical and up to date.

- Community Creation: On any social media platform, creation of a community is essential to generate buzz and sustain interaction.

A detailed guideline on creation and sustenance of community building is placed at Annexure IV

5.1.6 Engagement Analysis

Social media monitoring must be an integral part of any social media strategy. Social media data is different from other data or information because organisations have no control over its creation or dissemination on the Web and in order to understand and analyse the data a structure has to be imposed externally on it. Today a multitude of tools offer solutions for measuring conversation, sentiment, influences and other social media attributes. They help in discovering conversations about project and organisations and can be used to proactively engage with stakeholders. The Social Network Analysis (SNA) Software facilitates both quantitative as well as qualitative analysis by mining the raw data and combining it with individual and socio matrix. While some SNA software also have the features that enable them to import and/or store databases from social network, others perform preferential analysis to predict individual level or network outcome. Many social media monitoring platforms offer demographic information such as age and location. This information can be used to expand the reach of your platform by creating a geo-targeted campaign focused on areas that generate the most traffic to your social media site.

Some considerations for Data Analysis include:

- Data Definition: Selection of platforms, pages and/or organizations
- Depth and detail of analysis on each page: Areas or sections of the page to analyze (Wall, Discussion board, Pictures, etc.)
- Time-frame: Last one month etc.
- Criteria for determining the importance of the pages: notability, popularity, intentions/goals of pages, etc.

Some of challenges encountered in analysis may be related to

- Overlapping functions of posts: many comments and responses serve multiple purposes
- Difficulties in disentangling "push" messages from "pull" messages
- Inexhaustible range of topics that extend beyond your area of interest
- Unpredictable patterns of conversation and user exchange

These challenges may be mitigated by taking the following steps:

- Limit Scope of Analysis: Making a small start and defining Top 5 or 10 metrics may help organise the Data e.g. No. of mentions, No. of comments on specific posts, No. of retweets, No. of likes or shares etc.
- Creation of Dashboard: There are many free tools available that can help create a dashboard view of the data which can be pulled in through RSS feeds. This will help keep tab on latest happenings

- Connect with responders: It is a good idea to collate information/link to profiles about people who respond to queries or topics of your organisations interest, also observe their preference of response – individual mail, wall posting etc. Over a period of time this will help generate a broad profile of people who respond to your efforts

- Follow the followers/Leaders: Follow your followers and leaders on other networks/platforms to hear what is being talked about. This would help in spotting the trends in discussion.

5.1.7 Institutionalise Social Media:

The final step in ensuring that the pilot is scaled and integrated is to link it to existing administrative and communication structure. An indicative list includes:

- rules may be established that all policy announcements will be undertaken simultaneously on traditional as well as social media;

- all important occasions as far as possible may be broadcasted using social media;

- all documents seeking public opinion must be posted on social media sites;

- all updates from the website would automatically be updated on social media sites and;

- all traditional communications will publicise the social media presence.

VI. Conclusion

The Framework and Guidelines in this document have been formulated with a view to help government ministries, departments and agencies to make use of social media platforms to engage more meaningfully with their various stakeholders. Social media's characteristics of connectedness, collaboration and community have the potential of ensuring broad based consultation, and can help agencies reduce the duration of consultation process and receive immediate feedback on services delivered. In order to effectively utilise this media, the agencies must define very clearly the objective of such an engagement, select platforms that will be used for engagement, rules of engagement, communication strategy for ensuring broad basing such an engagement, and finally if found effective and efficient institutionalise such social media with mainstream engagement process. Both in India as well as across the world, various government departments and agencies at federal, state and local government level are using this media. However, this is a dynamic and evolving area and continuous engagement and nimbleness of response to such an evolving scenario will determine the success of such efforts.

ANNEXURES

Annexure-I

Social Media Types

Kaplan and Haenlein in 2010 classified social media into six different types: collaborative projects, blogs and microblogs, content communities, social networking sites, virtual game worlds, and virtual social worlds. A brief description of various types of platforms is given below to help the agencies understand their main characteristics and also lists some of the currently popular sites in each of the categories as well as examples of use of such platform by Indian or other governments across the world.

Social Networking: Currently, social networking sites are the most prominent platform of social media. It is an online service that enables its users to create virtual networks with like minded people akin to social networks in real life. It often offers the facilities such as chat, instant messaging, photo sharing, updates, etc. Facebook with over 800 million users is one of the most well known social networking site. A few Indian government departments and agencies are using Facebook including, Prime Minister's Office, Planning Commission, Ministry of External Affairs and a few Municipal Corporations and Police Departments, etc.

Blogs: Blogs are descriptive content created and maintained by individual users and may contain text, photos and links to other web sites. The main interactive feature of Blogs is the ability of readers to leave comments and the comment trail can be followed. A community of Blogs is referred to as Blogosphere and can be used very effectively to gauge public opinion. While many websites offer free space for blogging, this activity can also be undertaken on the existing government websites. Many government officials blog in their personal capacity on various issues. The Digital Engagement Blog of the UK

government is an initiative to use the Blog format to for consultation on as well for pronouncement related to existing and proposed policies.

Micro Blogs: Micro Blogs are similar to Blogs with a typical restriction of 140 characters or less, which allows users to write and share content. It can be done in the form of text message, instant message or even email. Twitter is a micro blogging site that enables its users to send and read text based messages or "tweets" of upto 140 character length. These Tweets are posted on the user's account and the site allows others to "Follow" the user. While Tweets are public by default, they can also be restricted to just the followers. Tweets can be generated via web, smart phone or even through SMS on some mobile phones. Due to limitation of characters, url shortening and content hosting services are often used accommodate posts that are normally longer. Twitter collects personally identifiable information of users and shares it with third party users. Twitter is estimated to have over 200 million users. Twitter is useful for short and crisp messaging and being used by Ministry of External Affairs, Chief Ministers of many states, Members of Parliament and Prime Minister's Office

Vlogs and Video Sharing sites: Video Blogs or Vlogs are blogging sites that mainly use video as the main form of content supported by text. Such sites especially enable those who may have limited knowledge of English to also share their experiences over internet. Vlogs are an important category of content over YouTube – the largest video sharing site. YouTube is a video Live Casting and video sharing site where users can view, upload and share videos and even leave comments about videos. However, for upload and sharing registration is required. YouTube is a subsidiary of Google Inc. Since a picture/or in this case a video speaks a thousand words, it is an excellent platform for sharing progress about projects. Many government departments

including DeitY and Prime Minister's Office have uploaded their promotional video content on YouTube.

Wikis: A Wiki is a collaborative website that allows multiple users to create and update pages on particular or interlinked subjects. While single page is referred to as "wiki page" the entire related content on that topic is called a "Wiki" These multiple pages are linked through hyperlinks and allow users to interact in a complex and non-linear manner. Many wiki communities are "private" and are used for deliberating upon internal policies and for knowledge sharing. Currently, based on the information available, no official wiki on any Indian government policy exists. Wikis are a good option for undertaking "close" web based interactions. Normally the content on wikis are created as part of "Creative Commons" and are more inclined towards copy left rather than copyright.

Some of the other popular social media sites include

- Slide Share – Similar to YouTube, here only presentations in PDF, PPT, KeyNote or Open Office format can be uploaded
- Orkut and LinkedIn – These are two other popular social networking site. While the former is an open site, the latter is primarily a business networking site
- Picasa and Flickr – These are photo sharing sites

Annexure II:

Use of Social Media by Government Agencies

Social media is used by several government organisations to engage with various stakeholders for the purposes of disseminating information, seeking inputs into policy making, recruitment, providing access to services, educating stakeholders, etc. In this section, a brief description of use of social media by different governments across the world and some examples from India has been presented to demonstrate the varied use of social media by government agencies.

International Experiences

Across the world, various government agencies at Federal, state and local government level are using the various social media platforms to interact with their stakeholders. While many local government agencies including Mayor's offices of many cities in United States use social media for community building and even recruitment, most state and federal agencies use social media for either seeking expert opinion or creating/influencing public opinion. Many agencies at federal level are also using this platform to gauge public reactions on upcoming/proposed policy measures. Given below are a few examples from across the world.

United States of America

Many federal and state government agencies are actively engaging with their stakeholders using social media. Some examples of use of social media are

- The White House Facebook Page and The White House Twitter profile –WhiteHouse.gov
- State Department Facebook Page

- U.S. Department of Housing and Urban Development Facebook Page
- US Army Facebook Page

In addition to established platforms created by private organisations, US government has also created its own platforms. A social network Web site called GovLoop.com was created within the US *Department of Homeland Security* to share experiences and best practices.

Australia

The Australian Public Service Commission in 2008 announced a set of interim protocols to agencies that are using or planning to use online media, including blogs, as a means of communication with clients and stakeholders and the Federal Government has established a *Government 2.0 Taskforce*. The Taskforce has submitted its report and its work related to increasing the openness of government and encouraging online engagement. It will be able to fund initiatives and incentives which may achieve or demonstrate how to accomplish government 2.0 objectives (Source: http://gov2.net.au/about/index.html last visited on August 29, 2011) The Task Force has released a set of guidelines and Toolkit to provide guidance to Australian government agencies to leverage Web 2.0 tools(http://gov2.net.au/projects/project-8/comment-page1/index.html#comment-14888 last visited on April 27, 2012). In addition, The Australian Government Information Management Office (AGIMO), amongst other information, collates and publishes list of Australian government use of social media (http://agimo.govspace.gov.au/page/gov2register/ last visited on April 27, 2012)

New Zealand

The New Zealand Government has been using Social Media to consult on varied topics including consultation on how and why online channels are used to achieve better service experience and increased strategic agility (http://www.ict.govt.nz/programme/rethink-onlinelast visited on April 27, 2012) The New Zealand government had even piloted an online discussion forum with supporting data during 2010 to test an approach of supplying publicly available data online to experts and the public for improved public consultation (http://www.goodpracticeparticipate.govt.nz/techniques/lessons-learnt-from-open-dataengagement-pilot.html last viewed on April 27, 2012) It also runs a dedicated website as a learning tool to consolidate learning and best practices from all such initiatives (http://www.goodpracticeparticipate.govt.nz/techniques/online-participation.html last visited on April 27, 2012) In November 2011, the ICT strategy group of the government approved social media guidance which includes High Level Guidance and Hands-on Toolbox (http://webstandards.govt.nz/guides/strategy-and-operations/socialmedia/ last viewed on April 27,2012)

United Kingdom

The Government Digital Service has been created within Cabinet Office of the United Kingdom government to transform government digital services. It works on multiple projects to ensure provisioning of projects and services that would improve digital experience of citizens and businesses. Some of their projects include – Directgov, Digital Engagement Blog, Assisted Digital etc. (http://digital.cabinetoffice.gov.uk/projects/ last viewed on April 27, 2012)

India

Social Media is being used by Indian government agencies in a limited way. However, recently many agencies have taken steps to engage with their service seekers on social media. Some of the examples from India are given below:

Prime Minister's Office

The Prime Minister's office launched its social media initiatives from January 2012. The PMO currently uses Twitter (http://twitter.com /#!/pmoindia Last visited on April 27, 2012), FaceBook (http://www.facebook.com/pages/Indian-Prime-Ministers-Office/1079 34225 905981 last visited on April 27, 2012) and YouTube (http://www.youtube.com/user/PMOfficeIndia?ob=0&feature=results_main last visited on April 27,2012) as its platforms for engagement

Police

- The Delhi Traffic Police has joined Facebook and Twitter to ease handling of traffic related issues (http://www.facebook.com/pages/Delhi-Traffic-Police/117817371573308).
- The Indore Police Department (http://www.indorepolice.org) has been using a blog, Twitter, online and mobile complaint forms, a Google map of police stations and a digital crime mapper to track criminal activities in the region.
- The Maharashtra Police Department (http://mahapolice.gov.in/) launched an SMS based complaint tracking system (CTS), called "TurantChovis", which promised to quickly redress citizen complaints by sending a first response within 24 hours and resolving the issue within 30 days.

Ministry of External Affairs

The Public Diplomacy (PD) division of the Ministry of External Affairs saw merit in leveraging social media to connect with the masses. It made its debut on Twitter with the user id "Indian diplomacy". It was used very successfully in the recent crisis in Libya. (http://twitter.com/#!/Indiandiplomacy) Post Office

World's largest postal network has started using Twitter to intercat with its users and public. The site is used even for status tracking and grievance Redressal (http://twitter.com/#!/PostOfficeIndia last viewed on April 27, 2012)

Municipal Corporation

The Municipal Corporation of Delhi launched a Facebook page last year and created a forum for better interaction with citizens (http://www.facebook.com/pages/Municipal-Corporation-of-Delhi/106030789427235).

Annexure III

Relevant section of Information Technology Act 2000

The Government departments need to realize that the moment they provide social media platforms/websites/portals/ facilities on their existing websites, portals and platforms, they become a network service provider as they provide the services of providing such social media facilities on the network. As such, the relevant Government department becomes network service provider and hence intermediary under the Information Technology Act, 2000. Further when the said Government department provides such social media facilities on its network, it receives, stores or transmits any particular electronic record on behalf of another person or provides any service with respect to that record. As such they become intermediary under Section 2(1) (w) of the amended Information Technology Act, 2000.

The moment the Government department becomes an intermediary, it is governed by its liability under Section 79 of the amended Information Technology Act, 2000.

Section 79 of the amended Information Technology Act, 2000 provides the broad principle that intermediaries like Government departments providing social media facilities are generally not liable for third party data information or communication link made available by them. However this exemption from liability can only be applicable if the said Government department complies with various conditions of law as prescribed under Section 79 of the amended Information Technology Act, 2000.

The said conditions which need to mandatorily complied with the Government department to claim exemption for any third party data information or communication link made available or hosted by

them in connection with social media facilities made available by the said department on their network are as follows:

1) The function of the Government department is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or hosted

2) The Government department does not-

(i) initiate the transmission,
(ii) select the receiver of the transmission, and
(iii) select or modify the information contained in the transmission

3) The Government department observes due diligence while discharging its duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

4) That the Government department as intermediary must not conspire or abet or aide or induce, whether by threats or promise or otherwise in the commission of the unlawful act.

5) That the Government department must immediately after receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the Government department is being used to commit the unlawful act, must expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

6) The Government department must also comply with all applicable rules, regulations and notifications in regard to their activity of providing social media facilities on its network.

7) That the Government department complies with the Information Technology (reasonable security practices and procedures & sensitive personal data or information) Rules, 2011.

8) That the Government department also complies with the Information Technology (Intermediary guidelines) Rules, 2011.

9) That the Government department also implement reasonable security practices and procedures as envisaged under Section 43A of the amended Information Technology Act, 2000.

Under the Information Technology Act 2000, the Central Government has enacted various rules and regulations which impact social media. Some of the most important in this regard are as follows:

i. The Information Technology (reasonable security practices and procedures &sensitive personal data or information) Rules, 2011 – These rules define for the first time in independent India what constitutes sensitive personal data. Sensitive personal data or information of a person means such personal information which consists of informal on regaling to;—
    a. password;
    b. financial information such as Bank account or credit card or debit card or other payment instrument details;
    c. physical, physiological and mental health condition;
    d. sexual orientation;
    e. medical records and history;
    f. Biometric information;
    g. any detail relating to the above clauses as provided to body corporate for providing service; and
    h. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

ii. For the purposes of protecting such sensitive personal data, the Government has mandated that any legal entity who is processing, dealing or handling sensitive personal data must implement reasonable security practices and procedures.

iii. The Government further stipulate that ISO 27001 is one acceptable standard of reasonable security practices and procedures. Thus, all Government departments which are providing social media facilities must comply with ISO 27001. In case the Government departments do not comply with ISO 27001 and provides social media facilities on which network sensitive personal data is going to be stored, processed or handled or dealt, the said Government department could be in breach of the law and could face legal consequences.

iv. Further under the Information Technology (Intermediary guidelines) Rules, 2011,since the said Government department who is provide social media facilities is an intermediary, it has to comply with the Information Technology (Intermediary guidelines) Rules, 2011. Under Rule 3(4) of the said rules, the Government department shall act within thirty six hours on receiving the written complaint form an affected person and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2).

v. Further the Government department shall preserve such information and associated records for at least ninety days for investigation purposes.

vi. In case, if the Government department does not comply with any of the above requirements of law, then the said Government department as also the concerned head of the department who is responsible for the social media facilities and the concerned IT head would be liable for civil and criminal consequences.

vii. The civil consequences could consist of being sued for damages by way of compensation upto 5 crore Rupees under summary proceedings before the adjudicatory authorities specially constituted under the Information Technology Act, 2000. Further if person wants, they can sue the said Government department for damages beyond 5 crore Rupees in a court of competent jurisdiction.

viii. In case the concerned Government department does not comply with all the aforesaid laws, the said Government department as also the person heading the department and the concerned IT head would also be liable for criminal liability which could range from imprisonment of 3 years to life imprisonment and fine which could range from 1 lakh to 10 lakh Rupees.

The aforesaid is the current legal position in India which impacts Government departments providing social media facilities on their network. In the light of the stringent provisions of the law and the subsequent legal consequences for non-compliance of the law, it is therefore absolutely essential that the relevant Government department providing social media facilities must completely comply

with all the above mentioned legal parameters as mandatorily stipulated by the Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 and various rules, regulations and notifications issued there under.

The specific legal provisions referred to above as extracted below:-

- Section 2(1)(w) of the amended Information Technology Act, 2000 states as follows:
- "Intermediary with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes."
- Section 79 of the amended Information Technology Act, 2000: Once the Government becomes an "[intermediary", its liability for third party data or information is specifically stipulated under Section 79 of the amended Information Technology Act, 2000. Section 79 of the amended Information Technology Act, 2000 states as follows:-

"Section -79 Exemption from liability of intermediary in certain cases

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or hosted

(b) The intermediary does not-

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if-

(a) The intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act.

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

> ”Explanation- For the purpose of this section, the expression “third party information” means any information dealt with by an intermediary in his capacity asan intermediary.”

Section 43 A of the Information Technology Act, 2000 also has a bearing upon the subject at hand. The said provision states as follows:-

“Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation.—For the purposes of this section,—

(i) “body corporate” means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) “reasonable security practices and procedures” means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;”

Further the Information Technology (reasonable practices and procedures and sensitive personal data and information) Rules, 2011 define what is sensitive personal data in the following manner:-

"3. Sensitive personal data or information.— Sensitive personal data or information of a person means such personal information which consists of information relating to;—

(i) password;

(ii) financial information such as Bank account or credit card or debit card or other payment instrument details;

(iii) physical, physiological and mental health condition;

(iv) sexual orientation;

(v) medical records and history;

(vi) Biometric information;

(vii) any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules."

- The exposure for damages by way of compensation is upto Rupees Five Crores under the IT Act, 2000 and further criminal exposure ranges from imprisonment of 3 years to life imprisonment.

Annexure IV:

Community Creation & Sustenance

Creating & Managing Community: The utility of social media is in its innate ability to create community of geographically dispersed individuals. However, efforts are required on a continuous basis to create and sustain this community. Some the steps that may be taken to ensure the same are:

Connect with existing networks – Existing networks refer to websites, official publications etc. The department may also like to connect it to some blogs or pages of willing individuals and/or employees. The method of establishing such connections should ensure that update on any one should automatically be seen on the other e.g. through RSS Feeds etc.

Publicise use of social networking: Existing forms of communications can be used to tell stakeholders about the department's endeavour on social media. Some of the ways in which it can be achieved include – Add social network links to leaflets, newsletters, email signatures and website, send emails all stakeholders, mention use of social networks at meetings, events and seminars and encourage people to join in, ensure any service seeker can find out about, and join in with, your social networks through posters etc. at points of service access, use TV, Radio and search engines to generate awareness about the site.

Sustaining Community: Creation of a community perhaps easier when compared to challenges related to sustenance of a community. Some of the steps involved in sustaining a community include the following:

Integrating Social Media into routine: Ideally, social networking should eventually become part of department's day-to-day work and not be an extra workload external to the routine functioning of the department. It should be seen as another way of communicating e.g. while sending an email, create a tweet simultaneously or update the Facebook page.

Linking with similar communities: Most people join pages from the links of friends or communities where they are already connected. One way of sustaining community is to link to these extended communities and provide update at least once a week. Some social media sites such as Twitter allow the user to not only schedule tweets but also create an automated message that is sent any new followers on Twitter. These methods may also be used for keep the stakeholders engaged. Social networks depend on users following each other. Networks can be built by actively following others and encouraging them to follow you. People or organisations tend to start following you if you publish posts that are useful or interesting to them. It is important to identify the influencers within these communities and build mutually beneficial relationships with them.

Sharing of content: People visit social networking sites not just for news but also content that they find useful. This includes textual content – copies of government orders, toolkits, links to forms, presentations etc. as well as visual content – photos, video, podcasts. These often serve as both a ice-breakers as well as inputs for more meaningful conversation.

Managing Expectations: Each Government Ministry/ Department/Official should publicly manage expectations for their social media presences in the form of an explicit, published "social media" policy in which expectations surrounding integral aspects of

communication with the public such as public comments, speed of response and procedure for escalation are clearly documented. This will ensure that citizens have fewer undue expectations from the social media presence of a particular Government authority.