



# International Institute of Security & Safety Management



*Let's professionalize the professionals...*



## Newsletter of NCR Chapter : February 2007

### Who are the stalkers?



Priyadarshani Mattoo case will be remembered for many reasons! It is a case of tenacity of frail old person who wanted to see the murderer of his daughter to be punished! It was a case of untiring efforts of a friend who left no stone unturned to seek justice! It was also a case of public resolve that made Indian justice system to have a re-look into the case.

In the law class-rooms this case will be treated as leading case of crimes of stalkers! In-spite of restraining order from the court, the convict did not relent and continued to stalk Priyadarshani! Police did not respond sufficiently and timely. As a result the convict got enough time and opportunity to commit gruesome crime.

This case has also drawn attention of security professionals and students of criminology whether stalkers are psychopaths and need treatment or they have to be treated as criminals and need to be given punishment?

**Capt S B Tyagi, FISM, CSC  
Secretary, NCR Chapter, IISSM**

### This news letter contains articles on-

- The crime of stalking
- Loss of proprietary information
- Be web-wary: Phishing hits banks
- Security precautions while transacting on line



# The Crime of Stalking

**Before implementing any intervention, it is important to have an experienced threat management team perform a risk assessment, as each stalking situation is unique.**

## About Stalkers and Stalking

A recent study by the National Institute of Justice, USA found that stalking was far more prevalent than anyone had imagined: 8% of American women and 2% of American men will be stalked in their lifetimes. That's 1.4 million American stalking victims every year. The majority of stalkers have been in relationships with their victims, but significant percentages either never met their victims, or were just acquaintances - neighbors, friends or co-workers.

## Types of Stalkers

There is tremendous confusion in the stalking research literature about how to classify stalkers. Everyone uses different terms. For the purposes of easy understanding I have broken down types of stalkers into three broad categories:

- Intimate partner stalkers
- Delusional stalkers
- Vengeful stalkers

Obviously, there is overlap. Since studies show that the overwhelming numbers of stalkers are men and the overwhelming numbers of their victims are women, we will be referring to stalkers and their victims accordingly. The excellent book '*I Know You Really Love Me*', by Doreen Orion MD, delves into much greater detail and provides extensive case histories about each of these types of stalkers.

Intimate partner stalkers are typically known as the guy who "just can't let go." These are most often men who refuse to believe that a relationship has really ended. Often, other people - even the victims - feel sorry for them. But they shouldn't. Studies show that the vast majority of these stalkers are not sympathetic, lonely people who are still hopelessly in love, but were in fact emotionally abusive and controlling during the relationship. Many have criminal histories unrelated to stalking. Well over half of stalkers fall into this "former intimate partner" category.

In these types of stalking cases, the victim may, in fact, unwittingly encourage the stalker by trying to "let him down easy," or agreeing to talk to him "just one more time." What victims need to understand is that there is no reasoning with stalkers. Just the fact that stalking - an unreasonable activity - has already begun, illustrates this fact. When the victim says, "I don't want a relationship now," the stalker hears, "She'll want me again, tomorrow." When she says, "I just need some space," he hears, "If I just let her go out with her friends, she'll come back." "It's just not working out," is heard as "we can make it work out." In other words, the only thing to say to the stalker is "no." No explanations, no time limits, no room to maneuver.



A victim should say "no" once and only once. And then, never say anything to him again. If a stalker can't have his victim's love, he'll take her hatred or her fear. The worst thing in the world for him is to be ignored. Think of little children: If they're not getting the attention they want, they'll act out and misbehave because even negative attention is better than none at all. Former intimate partner stalkers have their entire sense of self-worth caught up in the fact that, "she loves me." Therefore, any evidence to the contrary is seen as merely an inconvenience to overcome. Since giving up his victim means giving up his self-worth, he is very unlikely to do so. Don't help him hang on.

These delusional stalkers have almost always come from a background which was either emotionally barren or severely abusive. They grow up having a very poor sense of their own identities. This, coupled with a predisposition toward psychosis, leads them to strive for satisfaction through another, yearning to merge with someone who is almost always perceived to be of a higher status (doctors, lawyers, teachers) or very socially desirable (celebrities). It is as if this stalker says, "If she loves me, I must not be so bad." As Dean Martin compellingly crooned what could be considered the delusional stalker's anthem: "You're Nobody 'Til Somebody Loves You." It is not unusual for this type of stalker to "hear" the soothing voice of his victim, or believe that she is sending him cryptic messages through others.

Former intimate partner stalkers and delusional stalkers can become vengeful for a variety of reasons. For example, when their victims get restraining orders, or marry. Why a stalker's anger is a very bad sign is described under **what to do**.

In general, for any type of stalker, the less of a relationship that actually existed prior to the stalking, the more mentally disturbed the stalker.

### ***What to Do If You Become a Stalking Victim***

#### **Security Precautions for Stalking Victims**

Stalking victims don't like to be called victims. They will say, "I won't let myself be victimized," or "I'm not going to change my life because I'm being stalked." Sorry. Your life has changed. forever. And unless you accept that, you will actually be helping the stalker. You are a crime victim. The crime happens to be stalking. You must understand that the phrase "stalking victim" says volumes about the perpetrator, but nothing about you. It does not tell us whether you stay at home in terror with sheets over the windows, or whether you've decided to move, or to become active to change the laws in your state. On the other hand, accepting that you are a stalking victim serves to remind you that you must, from now on, take extra precautions that others do not have to take.

Here are some basics to start with. These and other safety precautions can be found in *I Know You Really Love Me*:

- Tell the stalker "no" once and only once, and then never give him the satisfaction of a reaction again. The more you respond, the more you teach him that his actions will elicit a response. This only serves to reinforce the stalking.
- Get a dog. This is "one of the least expensive but most effective alarm systems."



- *Never* give out your home address or telephone number. Get a post office box and use it on all correspondence. For those places that will not accept a post office box, change "PO Box" to "Apt." and leave the number.
- When the stalker gets your home telephone number, don't change it. Instead, always let an answering machine pick-up. Get a new, unlisted number, and give it to everyone who calls but the stalker. Gradually, only your stalker will be using your old number – it will become his private line. If it upsets you when he calls, put the machine in a room you don't use. You can even have someone else monitor the tapes. This way, the stalker will think he is still getting through to you, although you will never make the mistake of picking up when he calls. Whenever you close off one avenue for a stalker, he will find another and it could easily be worse.
- Document everything. Even if you have decided not to go the legal route, you may change your mind. Keep answering machine tapes, letters, gifts, etc. Keep a log of drive-bys or any suspicious occurrences.
- Take a self-defense class. A lot of security experts don't advise this, fearing that it gives victims a false sense of security, but we do. The best self-defense classes teach you how to become more aware of your surroundings and avoid confrontations, things that stalking victims would do well to learn.
- Have co-workers screen all calls and visitors.
- Don't accept packages unless they were personally ordered.
- Remove any name or identification from reserved parking at work or residence.
- Destroy discarded mail.
- Get a cell phone and keep it with you at all times, even inside your home, in case the stalker cuts your phone lines.
- If you think you are being followed while in your car, make four left- or right-hand turns in succession. If the car continues to follow you, drive to the nearest police station, *never* home or to a friend's house.
- Never be afraid to sound your car horn to attract attention.
- Acquaint yourself with all-night stores and other public, highly populated places in your area.
- Consider moving if your case warrants it. No, it's not fair, but nothing is fair about stalking. If you stay and fight through the legal system, you might get some justice, (although not necessarily your definition of it), but you almost certainly won't get safety: There is no possibility of life imprisonment for stalkers.
- Don't be embarrassed and think you caused this somehow. Stalkers need no encouragement. Your shame is your stalker's best weapon. It makes you more likely to engage him or agree to plea bargains, which are bound to be taken as sympathy and we know where that leads. Instead, tell everyone you know that you're being stalked, from neighbors to co-workers, so that when the stalker approaches them for information about you, they will be alerted not to divulge anything and will let you know he's been around. One young widow moved to escape her stalker, a stranger she had never really met. Yet, after finding out where she moved, he was also able to pinpoint her exact location by showing her helpful neighbors pictures he had surreptitiously taken of her and her children, telling them that he was her estranged husband and she had kidnapped the kids.



# LOSS OF PROPRIETARY INFORMATION

Courtesy: Capt A A Collaco ([acollaco@herohonda.com](mailto:acollaco@herohonda.com))

A firm believer in blending Technology and knowledge based skills; he has been contributing to various forums in the field.

At present he is **Head of Security Operations at Hero Honda, at Daruheda**, recently shifted from its plant at Gurgaon, where he was since its inception providing strategic clarity as far as the security operations goes.



## What is Loss of Proprietary Information?

Any loss that occurs due to loss of business information, loss of human resources, loss of competitive advantage, R&D cost could be termed as proprietary loss.

## The Nature of the Proprietary loss

Over the past few years there have been reports of loss of trade secrets and companies had to incur substantial financial loss due to this. Proprietary information differs from the other security disciplines, it differs from computer

security and network security, as the focus is on manning and protecting the intangible assets in whatever form they exist, which may or may not be limited to computerized forms. It also differs from the Physical security services even though it may involve guard services and alarm systems.

The challenge facing security professionals is to improve proprietary information protection through a systematic cooperation with the corporate legal department, compliance, human resources and the business units to address the many forms of “Non-physical” harm to the enterprise. The primary focus of these coordinated efforts should be on preventing and responding to theft, misappropriation or infringement of the company’s intellectual property rights in the physical world as well as addressing new challenges arising out from the increase electronics commerce operations in cyber space.

## Proprietary information assets

These are vital to the success of many businesses. By the end of the 21st century the importance of these assets, while often not formally valued by companies, cannot be underestimated. In today’s highly competitive world it is essential for Indian companies to recognize that the intellectual assets are the most sought after commodities. Competitive Intelligence gathering has now become an integral part of many international business houses. Many businesses feel that if they don’t protect their intellectual property they will be left behind in the race and also loose the competitive advantage they have over their rivals. This has also resulted in many companies forming their own specialized intelligence gathering units to take accurate and timely actions. There are a few Security agencies that specialize in this field and also adhere to a professional code of conduct. The loss of proprietary intellectual assets through unethical and illegal means cost business houses a significant amount of the profits and also limits business opportunities for future business success.



## **Intellectual Property Loss**

It is also important to talk about Intellectual Property Loss at this stage though they are slightly different but they go hand in glove and is like two sides of a coin. With the use of electronic communication in today's corporate environment, the ease of sending proprietary information or any kind of intellectual property in the digital format is greater than ever. When an employee decides to leave the company, they still have an easy access to all kind of information be it simple / confidential information which can be easily sent out / copied on a CD/ Floppy. It has been observed that many a time it goes unchecked.

The trend of outsourcing has also led to innumerable losses. The recent scam of a call centre employee selling information to a British company is an example as to how much information is available and it is virtually a gold mine that one is sitting on. In the same way the financial data /R&D and there are numerous examples at can go on.

### **Intellectual Property (I P) loss can include different types including.**

- Personal computer information
- Financial plans
- Product designs
- Corporate strategy
- Order history
- Personal employee information
- Material related information
- Sales reports
- New model plans

### ***The examples of Intellectual property Loss***

- ✓ Sending any of the following to an external Receipt
- ✓ Documents marked for Internal only. Confidential.
- ✓ Proprietary Research
- ✓ Financial Plans
- ✓ Product Strategy and designs
- ✓ Price list
- ✓ Patent information
- ✓ Confidential documents to an external web site
- ✓ Loss of competitive advantage
- ✓ Loss of investment opportunity
- ✓ Loss of customers
- ✓ Public embarrassment
- ✓ Loss of trust.

## **Risk factors associated with Proprietary Information (PI) and Intellectual Property Loss (I P)**

There are four major risks factors that have been observed through various studies and also by the data collected from sources –



- ✓ Former employee
- ✓ Foreign competitors
- ✓ On site contractors
- ✓ Domestic competitors

There are also other factors like computer hackers, vendor's suppliers, and current employees and offcourse intelligence sources.

## **Problems caused by PI & IP losses**

- ✓ Based on certain guidelines and some interpretation the following are the observations
- ✓ The ranking in the order of the data collected puts it as Increased legal costs
- ✓ Loss of revenue by the company. Of course it many vary from company to company
- ✓ Two problem areas could be (a) - loss of competitive edge and (b) - loss of market share.

Some commonly made Mistakes that many companies take is to overlook such losses. Many companies felt that –

- New product and service information is vital to their success;
- The internet network is a potential threat
- Information security is vital and a priority
- Physical security is required to safe guard documents
- Management should be concerned about loss of information of any kind
- Effective Information security procedure should be in place
- Vulnerability to electronic means

## **What should be done to protect Proprietary Information?**

A well-executed safe guarding proprietary information protection program should commence with an inventory of the key intellectual assets of the organization, as well as evaluation of theses assets. Once this is accomplished the organization should take a call and perform a risk assessment and determine which assets are adequately protected and which are at a risk.

It is important to take into consideration the risks of Internet and digital globalization. Basic protection measures are very essential. All employees (permanent, Contractual and other staff) should be subject to background verification. Physical restrictions over visitors /vendors / service engineers and all those visiting the company for any business irrespective of their rank and designation must not be allowed to visit areas that they are not supposed to enter. There should be no soft peddling on this issue and action should be taken that is cognizance enough to act as a future deterrent.

Exit interviews should involve a proper process that the employee to whom they had access will divulge no PI & IP. Methods of communicating the company's vigilance in defending the IP & PI should be communicated. The employees should be disallowed to bring in laptops, disks and C D 'S into the company, hard copy documents, drawings and other confidential material should be kept away in lock and kept also there should be one person responsible for this activity. The Security chief should work closely with the IT head and must know all policies that affect the



Internet and intranet. The procedures should involve efforts to identify and safe guard digital excess inside the premises.

## Conclusion

Loss of proprietary information is serious threat facing all industries all over the world and specially a country like India that is on the threshold of blooming. Those with a trusted relationship with the company face a grater risk than the others. New dimensions are being added every year in this direction. The Internet and associated technologies are perceived as significant threats to the company's ability to protect the confidentiality of information.

There are regulations in India that take care of certain IT related laws like the Information technology Act 2000 and there are various sections protecting it, but the act is too wide and there are many loop holes for a person to get out and not get prosecuted.

Laws pertaining to the subject are provided in the IPC, Copyright Act, Trademark Act, Patent Act, Industrial Design Act etc. There are forums like the Information Security Technology Development Council etc. to provide direction and guidelines on the related matters. Certain government initiatives have been taken in this direction. In the end the loss of information will seriously affect business and we need to protect it.

---

## Be web wary: Phishing hits SBI, 3 other banks

The increasing use of electronic channels for payments has posed a new security problem for banks. India's largest bank, the State Bank of India (SBI), has reported an attempt at phishing (a fraudulent way of acquiring PIN numbers and bank passwords using the Internet / email by claiming to be a trusted brand) to the Indian Computer Emergency Response Team (CERT-In).

### What Is Phishing?

It's a fraudulent way of acquiring PIN numbers and bank passwords using the internet/email by claiming to be a trusted brand

### Keep Phishing at Bay

- Do not respond to misleading e-mails luring you into sharing sensitive information/transferring funds to or from your account
- Keep your password a secret and change it regularly
- Refrain from using cyber cafes to access your online accounts
- If you reveal bank account data, inform your bank customer care service

This organization is associated with the ministry of communication and information technology and acts as a referral agency to the Indian e-community for incidents related to computer security.

Banking sources indicate 1 that besides SBI, three other international banks have informed CERT-In about attempts at phishing. However, their names are still under wraps. SBI senior officials when contacted by TOI said they were aware of the attempt and their site (not the bank's website) has been hosted through Yahoo! "There has been no financial loss to the bank. We have informed the CERT-In. Probe is on and we are trying to track down the perpetrators," said the SBI official. He reiterated that this was not an attempt at hacking. This is not the first time a



bank has reported an attempt at phishing. In February, ICICI Bank filed a complaint after its customers complained about being asked to validate or confirm their account details through an innocuous email ID ([icici@icicibank.com](mailto:icici@icicibank.com)).

The cloned website was blocked in two hours. The fraudster in his phishing email addressed to the SBI net-banking customer says, "SBI's internet banking is announcing a new security upgrade. We've upgraded our new SSL servers to serve our customers for a better and secure banking service against any fraudulent activities. Due to this recent upgrade, you are requested to update your account information by following the reference below".

## Some steps you can take while transacting online to ensure security

While all banks have made all efforts to ensure security for the customer's interest, listed below are some tips to ensure maximum security:

### 1. TIPS WHILE USING YOUR H-PIN

- **Change your HPIN** after your first login and change it at least once a month
- **Change your HPIN** after you access Citibank Online Internet Banking **using shared PCs**
- **Destroy the HPIN** mailer after memorizing it
- **Keep your HPIN a secret** and don't disclose it to anyone (including bank employees)
- **Do not write the HPIN** on your ATM/Debit Card or Citibank Credit Card.
- **Do not hand over** your ATM/Debit Card or Credit Card to anyone.
- **Do not use common names as HPINs** - choose passwords that are difficult for others to guess
- **Use a different password** for each of your accounts.
- **Use both letters and numbers** and a combination of lower case and capital letters if the passwords or HPINS are case sensitive

### 2. SCAM E-MAILS AND WEBSITES

- **If you believe that someone is trying to commit fraud** by pretending to be a concerned banks' business associate and such activities raise doubts, please contact the concerned bank immediately.
- **Be alert for scam e-mails.** These are designed to trick you into downloading a virus or jumping to a fraudulent website and disclosing sensitive information.
- **Beware!** Phony "look alike" websites are designed to trick consumers and collect your personal information. Make sure that websites on which you transact business post privacy and security statements and review them carefully.
- **Verify the address of every website, known as the URL.**
- **Make sure that the URL you want appears in the "address" or "location" box on your browser window.** Some websites may appear to be legitimate but actually are counterfeits. Take a few extra seconds and type the URL yourself.
- **Don't reply to any e-mail that requests your personal information.** Be very suspicious of any business or person who asks for your password, passport details, other banks details or some other highly sensitive information.



- **Open e-mails only when you know the sender.** Be especially careful about opening an e-mail with an attachment. Even a friend may accidentally send an e-mail with a virus.

### 3. TIPS WHILE USING E-COMMERCE WEBSITES

Many e-commerce websites utilize state-of-the-art encryption and other security procedures to give you a convenient and secure shopping and banking experience.

- **If you suspect a website** is not what it purports to be, leave the site. Do not follow any of the instructions it may present you.
- **Ask yourself if the information you are asked to provide makes sense** for the activity you are engaged in. For example, an online auction site should not ask for your driver's license number or the PIN for your credit card. If a site or e-mail asks for information that doesn't feel right, do not respond.
- **Keep a Paper Trail.** Print out the "address" of the company site you are on-it's Uniform Resource Locator (URL). The URL ensures that you are dealing with the right company. It's also a good idea to print out a copy of your order and confirmation number for your records.

### 4. GENERAL PRECAUTIONS

- **Look for the padlock symbol at the bottom right of a web page** to ensure the site is running in secure mode BEFORE you input sensitive information.
- **Make sure your home computer has the most current anti-virus software.** Anti-virus software needs frequent updates to guard against new viruses.
- **Install a personal firewall to help prevent unauthorized access to your home computer,** especially if you connect through a cable or DSL modem.
- **Log off. Do not just close your browser.** Follow the secure area exit instructions to ensure your protection.
- **Do not keep computers online when not in use.** Either shut them off or physically disconnect them from Internet connection.
- **Monitor your transactions.** Review your order confirmations, credit card, and bank statements as soon as you receive them to make sure that you are being charged only for transactions you made. Immediately report any irregularities.
- **Regularly download security patches** from your software vendors.

## There once was a man who had nothing for his family to eat ...

He had an old shotgun and three bullets.

So, he decided that he would go out and kill something for dinner.

As he went down the road, he saw a rabbit and he shot at the rabbit and missed it. Then he saw a squirrel and fired a shot at the squirrel and missed it. As he went further, he saw a wild turkey in



the tree and he had only one bullet, but a voice came to him and said, "Pray first, aim high, and stay focused."

However, at the same time, he saw deer which was a better kill. He brought the gun down and aimed at the deer. But, then he saw a rattle snake between his legs about to bite him, so he naturally brought the gun down further to shoot the rattle snake.

Still, the voice said again to him, "I said 'pray, aim high and stay focused.'" So, the man decided to listen to the voice. He prayed, then aimed the gun high up in the tree and shot the wild turkey.

The bullet bounced off the turkey and killed the deer. The handle fell off the gun and hit the snake in the head and killed it. And, when the gun had gone off, it knocked him into a pond. When he stood to look around, he had fish in all his pockets, a dead deer and a turkey to eat. The snake (Satan) was dead simply because the man listened to God.

**Bottom line:**

Pray first before you do anything, aim and shoot high in your goals, and stay focused on God. Never let others discourage you concerning your past. The past is exactly that - "the past." Live every day one day at a time.



---

**Suggestions & feedback may be sent to us on e-mail: [captstbyagi@yahoo.co.in](mailto:captstbyagi@yahoo.co.in)**

---