OFFICE OF THE COMMISSIONER OF POLICE, AURANGABAD CITY

The Information Technology Act, 2000

Note: The IT (Amendment) Act, 2008 has been passed by both the houses of parliament and received assent of the President of India on 05-02-2009.

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "Electronic Commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

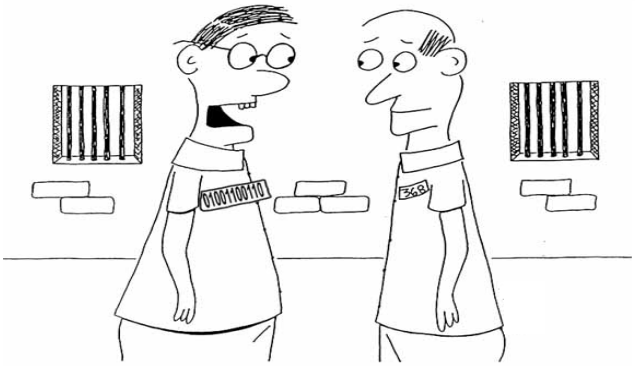
WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends, inter alia, that all States give favorable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records;

BE it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:

For ACT please refer - Information Technology Act 2000.



"How'd you know I was in for cyber crime?"

E- Security Tips

General Information:

• Don't delete harmful communications (emails, chat logs, posts etc). These may help provide vital information about the identity of the person behind these.
• Remember that all other internet users are strangers. You do not know who you are chatting with.
• Be extremely careful about how you share personal information about yourself online.
• Be extremely cautious about meeting online acquaintances in person. If you choose to meet, do so in a public place and take along a friend.
• Save all communications for evidence. Do not delete or alter them in any way.
• Be aware of all e-mails and SMS from any stranger luring you with billion dollar lottery prize, jobs in UK and huge wealth.
• Be sure that your WIFI Network secured, use a strong password.
• Never share your passwords with anyone. Change the password frequently using a combination of letters, numerical and special characters.
• Never forget to sign out of your email or any other accounts.
• Never reveal your personal information to any stranger in online chatting.
• Never make online transactions in unsecured sites. Watch for 'https' in the address bar.
• Never follow links to your banking website from another website or e-mail, type it yourself in the address bar.
• Never open spam mails as they contain either virus or spyware. Enable spam filters in your mail boxes.
• Never post sensitive information in social networking and marriage sites.
• Never be greedy for free downloads. They might infect your computers.
• Never let credit cards go out of your sight while paying.

• Never visit sites that contain pornography or terror links.

Suggestions for better security:
• Use strong passwords. Choose passwords that are difficult or impossible to guess. Give different passwords to all other accounts.
• Make regular back-up of critical data. Back-up must be made atleast once in each day. Larger organizations should perform a full back-up weekly and incremental back-up every day. Atleast once in a month the back-up media should be verified.
• Use Antivirus software and update regularly.
• Use a firewall. Firewalls are usually software products. They are essential for those who keep their computers online through the popular Broadband and cable modem connections.
• Do not keep computers online when not in use. Either shut them off or physically disconnect them from Internet connection.
• Do not open e-mail attachments from strangers, regardless of how enticing the subject line or attachment may be. Be suspicious of any unexpected e-mail attachment from someone you do know because it may have been sent without that person’s knowledge from an infected machine.
Regularly download security patches from your software vendors.

Children:
Do not give out identifying information such as Name, Home address, School Name or Telephone Number in a chat room. Do not send your photograph to anyone on the Net without first checking with your parents or guardians. Do not respond to messages or bulletin board items that are suggestive, obscene, belligerent or threatening. Never arrange a face-to-face meeting without telling parents or guardians. Remember that people online may not be who they seem to be.

Parents:
Use content filtering software's on your PC to protect children from pornography, gambling, hate speech, drugs and alcohol. There is also software to establish time controls for individual users (for example blocking usage after a particular time at night) and log surfing activities allowing parents to see which site the child has visited. Use this software to keep track of the activities of your children.

E-Businesses Tips to Fight Fraud:
• Develop and publish a comprehensive privacy policy.
• Ensure your employees are trained on the policy and follow it.
• Monitor the privacy policy and your compliance.
• Only ask customers for information that is absolutely necessary to complete a transaction.
• Store only absolutely necessary data elements; once a payment is complete, there is no reason to maintain payment information in readable form.
• Verify the payment system that you implement deletes temporary data files with payment records.
• Make certain server log files do not inadvertently store customer payment information.
• Limit employee access to payment systems and monitor those who have access to sensitive data or payment systems.
• Use technology tuned for the Internet to detect potential fraud.
• Follow up on suspicious transactions and immediately report any security breach or loss of computer systems to police.

Atm Frauds

Safety tips to avoid Debit or ATM Card fraud

• When you type your PIN number at an ATM, make sure that you sufficiently obscure the keypad from being viewed by an onlooker.
• NEVER let the shopkeeper take your debit card out of your sight. There is no need for him/her to do so, unless he/she intends to do something unlawful.
• Secure your debit card physically by storing it at a safe place.
• NEVER write your PIN number at a place where it can be seen by someone who you do not intend to show it to.
• ALWAYS destroy the receipts from merchants that you no longer require, especially when you have paid for using your debit card.
• If you do not receive your debit card or PIN number from the bank within a reasonable amount of time after requesting one, check with the bank when it was sent and when you should expect to receive it. It may have been picked up by someone else in transit.
• When at an ATM, make sure that no external devices are attached to the ATM machine and no wires are hanging around.
• Check your account statements carefully for transactions that you may not have made.

Using ATM machine

• Safeguard your credit cards and ATM cards at all times.
• If you notice something suspicious about the card slot on an ATM (like an attached device), do not use it and report it to the responsible authorities.
• Never disclose your ATM card and credit card PIN numbers to strangers.
• Beware of your surroundings while withdrawing money at ATM centers. Do not crumple and throw away the transaction slips or debt card memos: read them, make a mental note of the details and then, either tear them or shred them to trash.
• Periodically check your account balances on Internet or by requesting your bank or credit card company to send you statements to ensure that no transactions are happening behind your back.
• While entering any personal identification numbers, use your discretion to shield the keypad so that your hand movements are not very visible and you enter your passwords secretly.
• Be careful while withdrawing money from ATM Machine the attacker can shoulder surf to see your PIN.
• Incase any one behind you while withdrawing money just tell the ATM Security guard to ask him to wait out.
• Draw the cash only in well lit areas and secured ATMs.

What types of Credit Card Fraud are there?

Mail/Internet order fraud

• The mail and the Internet are major routes for fraud against merchants who sell and ship products, as well Internet merchants who provide online services. In this, fraudster presents stolen card information by indirect means, whether by mail, telephone or over the Internet to merchant site and orders the delivery of goods of lower value to avoid suspicion.

Skimming

• Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" by a dishonest employee of a legitimate merchant, and can be as simple as photocopying of receipts. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card out of their immediate view. The skimmer will typically use a small keypad to unobtrusively transcribe the 3 or 4 digit Card Security Code which is not present on the magnetic strip.

Carding

• Carding is a term used for a process to verify the validity of stolen card data. The thief presents the card information on a website that has real-time transaction processing. If the card is processed successfully, the thief knows that the card is still good. The specific item purchased is immaterial, and the thief does not need to purchase an actual product; a Web site subscription or charitable donation would be sufficient. The purchase is usually for a small monetary amount, both to avoid using the card's credit limit, and also to avoid attracting the bank's attention.

Safety tips to avoid Credit Card Fraud

• There is a critical 3-digit number on the back of the card called CVV (card verification value). Always erase and memories it.
• A card's magnetic strip has the basic details of the cardholder. But the card also comes with a blank space for you to sign in. You must sign on the card to avoid unauthorized use.
• Always check your monthly bank statements for any suspicious transactions.
• Shred the financial documents with care.
• Do not store your personal and credit card information on the computer.
• Do not write the PIN number down.
• During the online transactions, check if the web address starts with HTTPS, which ensures the encryption of all important data.
• Never delay to report a lost credit card as the consequences can be highly disastrous. Close the account that you suspect is being hit by the fraud.
• Thoroughly check the authenticity of the firm, the website, or any other transactional society where your money would be flowing through. Take a pause before venturing into any kind of online transaction and decide upon the authenticity of the transaction.

Cybercrime

is a form of crime where the Internet or computers are used as a medium to commit crime. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

Don'ts:

Do not give your password to anybody. Somebody who is malicious can cause great harm to you and your reputation. It is like leaving your house open for a stranger and walking away.
When talking to somebody new on the net, do not give away personal information-like numbers of the credit card used by your parents, your home addresses/phone numbers and such other

personal information.
If you feel uncomfortable or threatened when somebody on the net feeds you an improper or indecent message inform your parents or elders.
Do not break into somebody else's computer and worse still change things; you are probably destroying a lifetime of hard work by somebody. You may be intelligent but use your intelligence for better things. Somebody else can be as ruthless and as intelligent to break into your system and destroy your creations as well.
Do not copy a program that is copyrighted on the net. It is illegal. You are actually stealing somebody else's hard work. There is a lot of illegally available material on the net. Do not use it yourself.

- Don't delete harmful communications (emails, chat logs, posts etc). These may help provide vital information about the identity of the person behind these.
- Try not to panic.
- If you feel any immediate physical danger of bodily harm, call your local police.
- Avoid getting into huge arguments online during chat or discussions with other users.
- Remember that all other internet users are strangers. You do not know who you are chatting with. So be careful and polite.
- Be extremely careful about how you share personal information about yourself online.
- Choose your chatting nickname carefully so as not to offend others.
- Do not share personal information in public spaces anywhere online, do not give it to strangers, including in e-mail or chat rooms. Do not use your real name or nickname as your screen name or user ID. Pick a name that is gender and age neutral and do not post personal information as part of any user profile.
- Be extremely cautious about meeting online acquaintances in person. If you choose to meet, do so in a public place and take along a friend.
- Make sure that your ISP and Internet Relay Chat (IRC) network have an acceptable use policy that prohibits cyber-stalking. And if your network fails to respond to your complaints, consider switching to a provider that is more responsive to user complaints.
- If a situation online becomes hostile, log off or surf elsewhere. If a situation places you in fear, contact a local law enforcement agency.
- Save all communications for evidence. Do not edit or alter them in any way. Also, keep a record of your contacts with Internet System Administrators or Law Enforcement Officials.

Suggestions for better security

- Use strong passwords. Choose passwords that are difficult or impossible to guess. Give different passwords to all other accounts.
- Make regular back-up of critical data. Back-up must be made at least once in each day. Larger organizations should perform a full back-up weekly and incremental back-up every day. At least once in a month the back-up media should be verified.
- Use virus protection software. That means three things: having it on your computer in the first place, checking daily for new virus signature updates, and then actually scanning all the files on your computer periodically.
- Use a firewall as a gatekeeper between your computer and the Internet. Firewalls are usually software products. They are essential for those who keep their computers online through the popular DSL and cable modem connections but they are also valuable for those who still dial in.
- Do not keep computers online when not in use. Either shut them off or physically disconnect them from Internet connection.
- Do not open e-mail attachments from strangers, regardless of how enticing the subject line or attachment may be. Be suspicious of any unexpected e-mail attachment from someone you do know because it may have been sent without that person's knowledge from an infected machine.
- Regularly download security patches from your software vendors

Protecting Against Credit Card Fraud

How Does Credit Card Fraud Happen?

Theft, the most obvious form of credit card fraud, can happen in a variety of ways, from low tech dumpster diving to high tech hacking. A thief might go through the trash to find discarded billing statements and then use your account information to buy things. A retail or bank website might get hacked, and your card number could be stolen and shared. Perhaps a dishonest clerk or waiter takes a photo of your credit card and uses your account to buy items or create another account. Or maybe you get a call offering a free trip or discounted travel package. But to be eligible, you

have to join a club and give your account number, say, to guarantee your place. The next thing you know, charges you didn't make are on your bill, and the trip promoters who called you are nowhere to be found.

What Can You Do?

Incorporating a few practices into your daily routine can help keep your cards and account numbers safe. For example, keep a record of your account numbers, their expiration dates and the phone number to report fraud for each company in a secure place. Don't lend your card to anyone — even your kids or roommates — and don't leave your cards, receipts, or statements around your home or office. When you no longer need them, shred them before throwing them away.

Other fraud protection practices include:

- Don't give your account number to anyone on the phone unless you've made the call to a company you know to be reputable. If you've never done business with them before, do an online search first for reviews or complaints.
- Carry your cards separately from your wallet. It can minimize your losses if someone steals your wallet or purse. And carry only the card you need for that outing.
- During a transaction, keep your eye on your card. Make sure you get it back before you walk away.
- Never sign a blank receipt. Draw a line through any blank spaces above the total.
- Save your receipts to compare with your statement.
- Open your bills promptly — or check them online often — and reconcile them with the purchases you've made.
- Report any questionable charges to the card issuer.
- Notify your card issuer if your address changes or if you will be traveling.
- Don't write your account number on the outside of an envelope.

Report Losses and Fraud

Call the card issuer as soon as you realize your card has been lost or stolen. Many companies have toll-free numbers and 24 hour service to deal with this. Once you report the loss or theft, the law says you have no additional responsibility for charges you didn't make; in any case, your liability for each card lost or stolen is $50. If you suspect that the card was used fraudulently, you may have to sign a statement under oath that you didn't make the purchases in question

Cyber Criime Do''s & Don ''tt

Do's

1/- Install and use a firewall, pop-up blocker and spyware detector.

2/- Ensure that your virus definitions are up to date and run anti-virus and spyware detectors/cleaners regularly.

3/- Make Backups of Important Files and Folders to protect important files and records on your computer

4/- if your computer malfunctions or is destroyed by a successful attacker?

5/- Use strong passwords - Easy to remember and difficult to guess type password. Use alphanumeric and special characters in your password. The length of password should be as long as possible (More than 8 characters).

Do's continued

1/- Assignment of computer to a particular person with password protection in offices.

2/- Install the firewall and maintain the logs of firewall.

3/- Preservation of evidence (logs/received emails in question etc).

4/- Disconnect from internet when not in use.

5/- Habitually download security protection update patches & Keep your browser and operating system up to date.

6/- Never share photographs in compromise positions.

7/- Make the wireless network invisible by disabling identifier broadcasting.

8/- Encrypt the network traffic.

9/- Change administrator's password from the default password. If th wireless network does not have a default password, create one and use to protect the network.

10/- disable file sharing on computers.

11/- Turn off the network during extended periods of non-use, etc.

12/- Avoid online banking, shopping, entering credit card details, etc if the network is not properly secured.

13/- Check your online account frequently and make sure all listed transactions are valid.

14/- Use a variety of passwords, not same for all of your account.

15/- Be extremely wary of spam legitimate looking email asking for confidential information. Never ever click on the link given in the spam email.

16/- Always delete spam emails immediately and empty the trash box to Prevent accidental clicking on the same link.

17/- Be wary of websites that require your card details up front before you actually place an order.

18/- Not to believe everything you read online.

19/- Take your time - do not rush into things.

20/- Avoid posting your cell phone number online.

21/- Never respond to text messages from someone you don't know.

22/- Never let someone you don't know use your cell phone.

23/- Open email attachment carefully

24/- Be careful while downloading any free software or screensaver etc.

25/- Not delete email in question, save the email and take out the full header of the such email and report the crime.

26/- Be cautious when dealing with individuals outside of your own country.

27/- Be cautious of unsolicited offers. Never purchase anything advertised through an unsolicited email.

28/- Beware of promises to make fast profits. Be cautious of exaggerated claims of possible earnings or profits.

29/- Beware of lotteries that charge a fee prior to delivery of your prize.

30/- Contact the actual business that supposedly sent the email to verify if the Email is genuine

31/- Beware of references given by the promoter.

32/- Ensure you understand all terms and conditions of any agreement.

33/- Be leery when the job posting claims "no experience necessary".

34/- Always type in the website address yourself rather than clicking on a link provided.

Don't tell any anonymous chat friend

1/- Your real name, home address

2/- your phone number

3/- your friends' or family members' private information.

4/- your passwords

Don't

1/- Expose yourself that you are not available in town or give your details about location and itinerary when email auto responder enabled.

2/- Hand over your credit card to any person.

3/- Auto-connect to open Wi-Fi (wireless fidelity) networks.

4/- Get confused, frightened or pressured into divulging information if you receive an e-mail purporting to be from your bank or credit card provider as criminal use scare tactics .

5/- keep passwords stored on your computer.

6/- To go online without virus protection and a firewall in place.

7/- Open email attachment if you are not sure about it.

8/- Assume a company is legitimate based on "appearance" of the website.

9/- Be wary of investments that offer high returns at little or no risk.

10/- Accept packages that you didn't order.