E - SECURITY TIPS for -

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 softwares 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.

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.

- 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 Chart (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 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 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.**