at night, even when unattended.

b. Computer files ending in: GIF, JPG, BMP, TIF, PCX, DL, GL, FLI, MPG, AVI, MOV.
These are picture or graphic image files and parents should know what they illustrate. Image files may be pictures of sexual nature and can be of very high quality, moving and even include sound.

c. Names on communications programs that seem satanic, pornographic, rude or vulgar words in nature.

d. An obsession with fantasy adventure games such as Dungeons and Dragons, and Trade Wars.

e. Use of the computer to scan or run telephone or credit card numbers.

4. What you can do to protect your children.

a Learn about computers. Take a course at your local city college or adult school so you will have at least an understanding about what your children are doing.

b Talk to your kids about their use of the computer and the dangers on-line. You are already talking about school, sex, drugs, and violence. Computers can involve all these problems and they can happen in your home without your knowledge.

c Be involved with your kids in using the computer. This is a great opportunity to spend time with your child. It also gives you the opportunity to see what they like to do. If they like games, try playing the games with them. If they do their homework, read the paper while they work. If they use a modem to call on-line systems, ask questions about what your child is doing and looking for.

d Keep the computer in a "common" area of your home. Don't use the computer as a baby sitter. Keep the computer in a family room or den. This allows you to monitor on-line activity. Virtually every case we have investigated where children were involved in computer crimes or were the victim of abuse by people met on-line, the computer was found in the child's room. Often the child could lock the door prohibiting others in the household from observing their activity.

e Control all modem activity. Monitor the times and the numbers dialed. If you have any questions about the types of services your child is calling, contact the Police Department.

f Closely monitor your long distance telephone bill for unexplained calls. With on-line services and bulletin boards all over the world, it is easy to start calling long distance for special systems.

g Check the screen of an unattended computer. If the computer is showing a series of changing numbers, the computer may be running a hacking program trying to identify calling card "pin" numbers or long distance access numbers.

h If the computer is showing a series of sixteen-digit numbers the computer may be running a program that is trying to validate credit card numbers.

The San Gabriel Police Department can be reached at (626) 308-2828.

Children and Computers The Hidden Dangers

A GUIDE FOR PARENTS

Courtesy of the
San Gabriel Police Department
Crime Prevention Office
(626) 308-2828

"Today's children are being weaned on video games and quickly move to computers. Society has high hopes for this technically literate generation, but the proliferation of microcomputers and computer literacy also means that more and more assets will be stored on computer systems and the community of potential computer criminals will increase astronomically."

Dr. Willis Ware
Rand Corporation
Santa Monica, CA

Dear Parent,

With the ever increasing development of computer technology and the increasing number of people who are computer literate, it is much more likely that our children will be victimized or exploited in a computer environment. The "Information Super Highway" which is made up of BBS services, commercial on-line services such as Prodigy, America Online, CompuServe and the Internet allow millions of people around the world to communicate anonymously in a virtually uncontrolled electronic world.

If your child has a home computer or access to a friend's computer, particularly if they have connected the computer to a phone line via a modem, please take the time to review this guide. Just as we tell our children not to talk to strangers and watch and direct where they go and whom they meet in the "real world," we need to be aware of the dangers in the electronic world and exercise these same precautions.

Parents have unknowingly allowed their children to invite criminals into their homes via the computer that resulted in the child becoming involved in criminal activities and all too often victimized by persons who would never have been allowed in the home by the parents.

1. Tip for safe computing.
Advise your children to observe the following safety rules whenever they are on-line. Remind them that no matter how safe or friendly a BBS seems (and this includes the major on-line services), there is always a potential for danger.

a. Never give out any personal information about themselves-particularly real names, addresses, phone numbers, financial information, etc. to anyone that they meet on computer bulletin boards.
The above is not meant to preclude giving your name, phone, address and credit card number to on-line services that often require them to open an account. You may also find you can order services and products via on-line services and we are not discouraging this. Making purchases online with a credit card is probably just as safe as it is in person at a store. What we are concerned about is giving personal and credit information out on-line to people you meet in chat or E-mail. It is the same as using a telephone. When you call a business and order products by phone you know whom you are calling and can feel secure in giving them your credit card. When they call you, you have no way of knowing if you are talking to a legitimate business or a crook.

b. Do not fill in the "Member Profile" section used by on-line services where you fill in you name, address, age, school, sex, interest, etc. This allows any on-line user access to personal information. If you want to put anything in here, use your handle and interests. Skip the address and other personal info.

c. Be aware of undesirable chat rooms and bulletin boards. Use the "parental discretion" options where necessary to block these areas.

d. Don't respond to anyone who leaves you obnoxious, sexual or menacing E-mail. You should not become involved in public "Flame" sessions. You have no idea who you are dealing with and what access an individual may have to your personal or on-line account information. Many services provide a "kill" file where they can automatically block messages from these persons.

e. Report all electronic harassment and/or abuse to their parents. As parents, you should notify the BBS SYSOP (system operator) of the problem. If the SYSOP does not give you satisfaction in stopping this abuse, notify the police.

f. Never set up face-to-face meetings with anyone you have met on the BBS. If anyone you meet on-line wants to meet you – tell your parents.

Notify the police of all attempts by adults to set up meetings with your children. This is by far the most dangerous situation for children and should be reported to law enforcement.

2. Warning signs of possible computer crime problems. Note: these are warning signs only and are meant as warnings of possible problems, not evidence of a problem.

a. Computer addiction. Withdraws from friends, family, and "lives on computer" may lose interest in social activities.

b. Use of new or unusual vocabulary, heavy with computer terms, satanic phrases, sexual reference or sudden interest in related hard rock or satanic oriented posters, music, etc.

Look for related doodling or writing using of words such as: Hacking, Phreaking or any words with "ph" replacing "f".

c. Lack of interest in self and appearance, grooming and hygiene or indications of lack of sleep, sudden drop in school grades and unauthorized absences from classes.

3. Other potential danger signs.

c. The computer and modem are running late