Hi-Tech Crime

Protecting Yourself In The Computer Age

Crime and Violence Prevention Center
California Attorney General's Office

Bill Lockyer
Attorney General

Hi-Tech Crime

Protecting Yourself In The Computer Age

Crime and Violence Prevention Center
California Attorney General's Office
Bill Lockyer, Attorney General

Revised November 2000

Table of Contents

Words or phrases that appear in **bold type** can be found in the glossary and resource section.

Introduction

Imagine a world without technology. Jump back to a horse and carriage, no electricity, no telephones. Now, fast forward to the new millennium. The research firm, Odyssey, estimates that half of all U.S. homes have a personal computer and that one-third of all homes are online. They further conclude that "... the home computer is rapidly eclipsing the television as the communication and information appliance for many consumers."[1]

This is great news for consumers who can access an entire universe of information on the World Wide Web. Children and teenagers can research homework topics and engage in interactive games with a click of a button. Adults can bank, trade stocks and purchase a multitude of items while **surfing** the Web.

But danger lurks on the Web. Criminals manipulate the Web into a nightmare by distributing child pornography to unsuspecting consumers; stealing personal information such as names, addresses and credit card numbers; **hacking** confidential systems and personal home computers to obtain or delete information and planting harmful **viruses** that destroy entire systems. Unfortunately, these are just a few examples of high tech crimes which are getting more sophisticated and harder to detect as technology advances.

You can help stop criminals from threatening your children, your financial well-being and your peace of mind. This high tech crime prevention information will guide you safely through your high tech adventures.

Additionally, important information on preventing identity theft is included. Cases of identity theft have dramatically

increased with advances in technology and this guide will help you take control and prevent further victimization.

Technology is advancing at a rapid pace and printed material about cutting edge technology is almost obsolete by the time it goes to press. With this in mind, we present the basics of high tech crime prevention. This publication provides strategies on how to protect your children from child molesters who befriend potential victims on the Internet. It also covers ways to protect yourself from cyber-stalking, identity theft, fraud schemes, cellular telephone fraud and hackers.

Consumers, parents, employees and employers will find useful information to protect your families and finances. Remember, high tech crime prevention techniques must evolve as rapidly as technology.

Crime and Violence Prevention Center
California Attorney General's Office

Child Safety on the Internet

The sleepy woman glanced at the clock and reached for the ringing telephone. It was 2:00 a.m. Panic gripped her as the caller identified himself as a sheriff's deputy. He had her 14-year old daughter in his patrol car, and he needed to resolve a delicate situation. The woman thought her daughter was down the hall in her bedroom, asleep. Not so, according to the deputy. In fact, he had found her parked along a country road three or four miles from the girl's home with a 26-year old married man from a neighboring community. Shock and disbelief gripped the woman. "How" and "why" were only a few of the questions running through her mind. The answers she found in the next few hours added to her shock. Her daughter had become a victim of Internet crime.[2]

• • • • • • • • • • • • • • • • • •

As a parent, if you own a home computer and allow your children Internet access, you need to be Internet literate. If you do not know how to access the Internet, take a class, read a book or spend time with your children and let them show you the amazing world of cyberspace. Be aware of what is out there and prevent your child from gaining access to inappropriate Web sites and **chat rooms**.

Did you know that child molesters frequent chat rooms on the Internet? If you are not familiar with chat rooms, it is time you sat in on one. If your children have access to the Internet, they have access to child molesters who pose as

other "teens" or confidants trying to develop friendships with unsuspecting children. Child molesters lure their victims with promises of friendship and material goods. And, too often, it works! Many adolescent Internet users look for friends – someone who will "chat" while their unsuspecting parents are not present.

In addition to child molesters, other individuals try to glean personal information from your children, such as their name and address. Parents have also found that their child "borrowed" a credit card and gave the number to a new "friend" on the Internet. Once this information is on the Internet, parents are vulnerable to identity theft and other potentially expensive problems.

Take charge of your computer. Set ground rules for Internet access and discuss with your children these crime prevention tips:

- Place the computer in a centrally located area in your home – not in a child's bedroom. This prevents "secret" communications or access and also allows all members of the family to use it.
- Talk to your children about the Internet. Explain that it is an excellent source of information, but some sites are inappropriate and they are expected to stay away from these sites.

- Establish time frames for Internet access. This will encourage your children to obtain information in a timely manner and discourage aimless wandering.
- Keep an open line of communication with your children. Discuss their Internet experiences and guide them to sites that are age-appropriate.

- ➢ If your children have Internet access at school, find out if the school has adopted an acceptable use policy. If so, obtain a copy and use it to establish additional guidelines at home. If the school does not have a policy, become involved with your child's school and encourage responsible Internet use. An acceptable use policy may limit the sites available to children based on age-appropriate material and set specific time limits for use.
- ➢ Consider using software that can block or filter Internet sites or certain words that may indicate inappropriate sites.

BACK TO THE CHAT ROOM

Many parents and law enforcement experts believe that chat rooms are a safety risk because the identities of the "chatters" cannot be confirmed. The elusive identity of chatters poses many risks to children. If you do allow your children to "chat," they should follow these important safety guidelines:

- ➢ Never give out any personal information including: name, address, city, state, school attended, telephone number, family names or other personal family information.
- ➢ Use age-appropriate chat rooms. The larger Internet Service Providers (ISP) have moderated chat rooms with appropriate themes. Contact your provider or search the Internet for more information.

- ➢ Never respond to someone who wants to meet in person or send photographs. Instruct your children to exit the chat room and notify you immediately if this happens.

- Never agree to send or receive a file without parental permission. (Receiving "blind" files may introduce your children to pornography or plant a virus in your computer.)

Most importantly, if your child visits a particular chat room, spend at least five or ten minutes monitoring the conversation to see if it is appropriate. Consider purchasing computer software products that can help you monitor and control your child's access to the Internet. It is also a good idea to have a well-known protection program if your children download files. Additionally, monitor your children's Internet activity by checking all of the sites visited. This is accomplished by accessing the Internet and pressing the "control" and "h" keys simultaneously on your keyboard. If this doesn't work, access the Internet, click on the "windows" pull down menu, and then click on "history." Either way, a window will appear that lists the "history" of all sites visited.

Finally, immediately report to your local law enforcement agency any attempts by others to meet your child or any inappropriate sexual conversations. If possible, save the conversation text for review by law enforcement. This will assist law enforcement in an investigation and possible prosecution.

When You Least Expect it ... Protect Yourself

The jilted ex-boyfriend had a plan. Using personal information from his ex-girlfriend, he sent a message over the Internet that lured men to her door who thought they were going to fulfill a rape fantasy. The information included her name, address, telephone number, physical description and detailed instructions on how to circumvent her security system. The woman was not harmed, but half a dozen men tried to visit her. Fortunately, the jilted ex-boyfriend was charged under California's cyber-stalking law.[3]

• • • • • • • • • • • • • • • • • •

The Internet is supposed to be the information super highway, not an instrument used for violence. Unfortunately, some individuals choose to turn the Internet into their personal playground of destructive messages, threats and illicit pornography. And you're probably thinking, where are the laws prohibiting threats and pornography? Defining Internet crime is a unique challenge; therefore, lawmakers are continually updating and introducing new laws relating to Internet safety.

Because the First Amendment protects freedom of speech, there is little, at this point, that law enforcement can control on the Internet. The cyber-stalking law does not inhibit free speech, it prohibits computer-based harassment. The issue for law enforcement now becomes one of jurisdiction.

Where did the crime occur? This is the first question that law enforcement asks a victim. Did the crime occur in your

home because that is where the computer is located? Or, did the crime occur where the message originated from, which could be in another state or country? This is a law enforcement dilemma. ISP often cooperate with law enforcement, but it isn't always easy to find the suspect. In fact, a hacker can compromise your Internet account and send harassing messages under your name and profile – and get away with it.

The best and easiest way to prevent personal information from getting into the wrong hands is to be very selective in the information that you divulge. Use the following common-sense tips when using the Internet:

- ➢ Do not give out your name, address, telephone or credit card numbers or other personal information, such as your social security number, unless you are dealing with a reputable company and you have initiated the contact.
- ➢ Think twice before submitting your personal information profile through your ISP.
- ➢ If you decide to meet someone from online, use common sense. Meet in a busy, public place and consider taking a friend with you to the meeting.

PROTECTION AGAINST INTERNET SCAMS

The Internet has also become a vehicle for criminals to use to perpetuate tried and true scams. If it sounds too good to be true ... it probably is! Have you heard this before? Believe it! Being on the information super highway does not legitimize a get-rich opportunity. Simply type "get rich quick" in a **search engine**, and you are on your way to new-found wealth or a scam.

Many old confidence schemes, such as pyramid schemes, have resurfaced on the Internet. The scams are the same. People are contacted via e-mail or notice a Web page touting a sweet deal. They are encouraged to invest some money, and if they can convince others to do the same, they are promised a huge return. The first few people make money, but two or

three levels down, the pyramid crashes because the initiators are the ones receiving profits. Pyramid schemes focus on recruiting new members, not on selling products.

In 1999, the Federal Trade Commission (FTC) launched a sweep of the World Wide Web to locate sites that host illegal multilevel marketing scams. These sites are under ongoing investigation.

Additionally, the FTC offers the following tips to consumers to guard against illegal pyramid schemes:

- ➢ Avoid any plan that offers commissions for recruiting additional distributors.
- ➢ Beware of plans that ask new distributors to spend money on excessive amounts of high-priced inventory. These plans can collapse quickly and also may be illegal pyramid schemes in disguise.

- ➢ Be cautious of plans that claim you'll make money through continued growth of your "downline" (the commissions on sales made by the new distributors you recruit) instead of through sales you make yourself.
- ➢ Beware of "shills" – decoy references or endorsements that the promoters pay other people to describe fictional successes in earning money through the plan.
- ➢ Do your homework. Check with your local Better Business Bureau about any plan you're considering, especially if the claims about your potential earnings or the product sound too good to be true.

Pyramid schemes aren't the only scams to be wary of on the Internet. There are many and they tend to recycle periodically. Beware of "free gift offers" for completing a

simple survey or because you won a prize in a drawing – especially if you did not enter. These typically ask you for your name and credit card number to cover the nominal cost of shipping. Their real purpose is to commit credit card fraud. Other tips to keep you safe online include:

- ➢ Never send money to an unsolicited e-mail or a posting you spotted on the Web.
- ➢ Watch out for the buzzwords: *downline, matrix, network, recruitment* and *cell.* These words and their synonyms are often used to dress-up classic pyramid schemes.
- ➢ Never agree to a meeting with someone who has posted a fabulous offer. In-person meetings give the con artist a chance to turn on high-pressure sales tactics or even rob you.
- ➢ If you are setting up an online identity for e-mail, be very vague. Do not give out personal information in a profile.
- ➢ Contact your ISP or local law enforcement if you receive suspicious or threatening e-mail.
- ➢ Be alert for any responses to e-mail that you don't believe you have sent.
- ➢ Be alert to e-mail bearing a return address you recognize, but with content that does not match the personality of the sender.
- ➢ Look carefully at message headers for discrepancies between sender and provider.
- ➢ Acquire and use encryption software if you send e-mail containing confidential or sensitive information.
- ➢ Web sites whose purposes are to commit fraud appear and disappear quickly, making it difficult for them to be tracked. If you find a suspicious Web site, print the screen and any correspondence. Present this information when filing a complaint with your ISP or law enforcement.

Finally, use the Internet to find information regarding online safety. Your ISP may also provide useful prevention tips and most encourage you to report suspicious online activities.

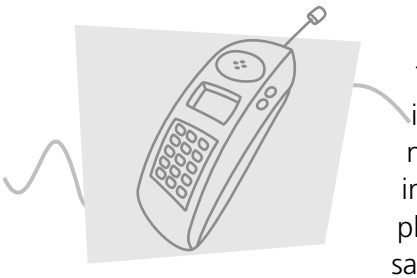
If you are a victim of online crime, contact your local law enforcement agency. Do not purge any information from your computer – law enforcement needs this documentation to assist in their investigation.

BEWARE OF CELLULAR PHONE CLONING

The cellular telephone bill arrived and the amount due exceeded $500! Many of the numbers called were in foreign countries. When the cellular telephone carrier was contacted about the bill, the truth came out. The cellular telephone had been cloned.

• • • • • • • • • • • • • • • • • •

Cloning cellular telephones is relatively easy, and as a consumer, you won't know your cellular telephone was cloned until you get your monthly statement. Cloning is the act of making one cellular telephone "act" the same as another. This is accomplished by copying the identity and phone number of one phone and inserting it into another. The phones do not have to be the same model or even the same brand. The cloned phone is now the same as the first – it will ring when the original phone rings and any charges incurred will be billed on the original phone's monthly billing statement.



If you own an analog cellular telephone, or if your digital phone can also revert to analog, then there is a chance that your phone can be cloned. The best way to prevent your analog cellular telephone from being cloned is to keep the power off when it is not in use. When your cellular telephone is on, it sends out an electronic serial number (ESN), and there is technology available that will capture this signal. Once the

ESN is captured, it is then used in the cloning process. If your cellular telephone is off, the ESN is not transmitted.

As technology advances, cloning is likely to become obsolete. The digital cellular telephones are somewhat secure from cloning. However, with any cellular telephone, remember that your actual conversation is not private. The cellular telephone is a transmitter, and your conversation is out on the airwaves and vulnerable to interception by radio scanners.

Finally, never give out any personal or financial information over cellular telephones. If you notice unusual and excessive charges on your monthly billing statement, contact your cellular service carrier's fraud division.

Identity Theft

With interest rates at an all-time low, the Smiths decided to refinance their home. They contacted their local banking institution and started the necessary paperwork. They ordered their credit report and were shocked to find that they had three credit card accounts with delinquent balances. They had never applied for the credit cards and the outstanding balances totaled over $20,000. The nightmare started. The Smiths soon learned that they were victims of identity theft. They began the very long, tedious process of clearing their credit. Adding to their grief, the refinancing of their home was also delayed. The Smiths were, therefore, victimized again because they missed out on the lower interest rates.

• • • • • • • • • • • • • • • • • •

Sounds unbelievable, but it could happen to you! Think about your daily activities. You go to the grocery store and write a check. What type of information is on your check: name, address, telephone number, driver's license number, social security number? Wait a minute! Take that social security number off your personal checks. In fact, your social security number should be your most protected information.

If a thief has access to your name and social security number, that information can be used to open fraudulent accounts. Innocent people have discovered utility, department store and other credit accounts opened in their name and it is usually accomplished using a stolen social security number. Do not give out your social security number unless it is absolutely necessary. Many forms have an area for the social security

number, but you should question why the number is needed. A social security number is needed for loan/credit applications and certain other financial transactions. But the video store and car rental agency certainly don't need it. Be aware that your social security number is not necessary for check cashing or credit purchases. If you are asked for this information, ask to speak with the store manager to verify the need for this information.

Aside from guarding your social security number, guard all your personal information. Do you receive pre-approved credit applications in the mail? What do you do with them? Throw them in the trash? Think again. This mailer contains your name, address, and perhaps other personal information. If you carelessly toss it in the trash, a **dumpster diver** can use this information to steal your identity or pass it on or sell it to someone else.

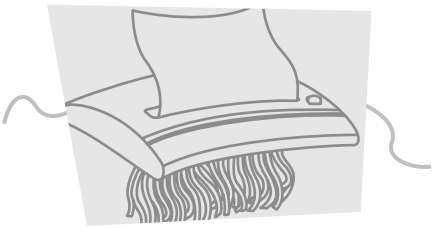
Your mailbox is an excellent source of information. Many thieves wander through neighborhoods looking for "easy" mailboxes. These are unlocked mailboxes that are usually adjacent to the curb or affixed to a house. A red flag indicating outgoing mail is an invitation to a thief. What's in your outgoing mail? A Visa payment? A card and a check for your nephew's sixteenth birthday? Checks that a thief can easily alter. Additionally, if you are mailing credit card payments, the thief now has not only your personal checks, but also your credit card account numbers. He can then fraudulently charge items to your account without your knowledge. Remember that personal information is easy to obtain.

Consider the following safety tips that will help prevent you from becoming a victim of identity theft:

- Shred or tear up pre-approved credit card applications, and other mail with your social security number, bank

account and credit card account numbers before throwing them into the trash.

- ➢ Never throw mail with personal information into trash bins at post offices.
- ➢ Do not leave information with personal and financial information in your vehicle.
- ➢ Review bank and credit card statements each month for fraudulent activity. If anything is amiss, immediately report the problem to your bank or credit card company.
- ➢ If your bills do not arrive in a timely manner, contact your creditors. Your bills may have been lost in the mail or stolen.
- ➢ Before giving out any personal information to a company, ask how the information will be used and whether it will be transferred to third parties (mailing lists).
- ➢ Periodically, order your credit report from the three major credit reporting agencies and check for accuracy.
- ➢ Do not leave receipts at the ATM machine and gas pump.
- ➢ Limit the amount of credit cards and personal information that you carry in your wallet. If you have old credit accounts that you don't use, cancel the accounts and cut up the cards.
- ➢ Do not carry your social security card in your wallet. Memorize the number.
- ➢ Do not write credit account numbers on checks or the outside of envelopes when paying bills.
- ➢ Be extremely careful about divulging personal information such as place of employment, employee identification number or mother's maiden name. These are key components in identity theft.
- ➢ Buy a shredder, and use it.



If you become a victim of identity theft, take a stand! Contact law enforcement and complete a crime report. Report the theft of your credit cards or numbers to the fraud units of the three major credit reporting agencies* and ask that your accounts be flagged. Add a victim's statement to your report (up to 100 words) that includes a statement such as *" ... my ID has been used to apply for credit fraudulently. Contact me by telephone to verify any and all credit applications."* Find out how long the fraud alert is posted to your account and extend it if necessary. This fraud alert is not a guarantee that your credit is safe. It is a precaution. Continue to monitor your credit reports. If your social security number has been used in an identity theft, it is imperative that you notify the Social Security Administration Hotline as soon as possible.

Next, contact all creditors with whom your name has been used fraudulently – by phone and in writing. Send all corrspondence by registered mail. This will establish documentation of your efforts. Keep all receipts of expenses and document the amount of time that you spend clearing your name. Ask creditors for replacement cards with new account numbers for the accounts that have been used fraudulently. Ask that the old accounts be processed as "account closed at consumer's request."

Creditors may request that you fill out and notarize fraud affidavits. In California, the law does not require that a notarized affidavit be provided to creditors. A written statement and a copy of the police report may be enough.

After you have taken these steps to protect yourself or re-establish your good credit, check your credit reports again. This is the only way to determine if someone has taken your identity. Many victims have no idea how their identity was taken, but they will always remember their wasted time, the many telephone calls to creditors and police, and most of all, the invasion of their privacy.

Is it over yet? Maybe. Maybe not. Even though you may have spent hundreds of hours restoring your good name, your personal information could have been sold to someone else. Inaccurate information may still appear on your credit report in the future. That is why you need to check your credit reports on a regular basis. Don't rely on law enforcement to make this problem go away. Often, the identity of the perpetrator is unknown. Some cybercrooks do not use your personal information to commit identity theft themselves – they obtain the information and sell it to others who do. So, even if law enforcement makes an arrest in your case, your personal information may still be out there waiting for the next thief to steal your identity.

The bottom line is this: be careful with your personal information.

Additional information:
If you have had checks stolen or bank accounts set up fraudulently, report it to the check verification companies. Put stop payments on any outstanding checks that you are unsure of. Cancel your checking and savings accounts and obtain new account numbers. Give the bank a secret password for your account (not mother's maiden name).

To report fraudulent use of your checks:
CheckRite: (800) 766-2748
Chexsystems: (800) 428-9623
Equifax: (800) 437-5120
National Processing Co.: (800) 526-5380 SCAN: (800) 262-7771
TeleCheck: (800) 710-9898

Other useful resources:
Federal Government Information Center: Call (800) 688-9889 for help in obtaining government agency phone numbers.

***** Information on contacting the three major credit reporting bureaus is provided in the glossary.

It's a High Tech Business

The Associated Press touted the headline, "Judge unplugs 2 teens who hacked into U.S. computers." The two teens, ages 16 and 17, hacked into government and military computers apparently just to prove that they could. The punishment – three years probation that excludes the teens from possessing a computer and modem, 100 hours of community service and $4,100 in reparations.[4]

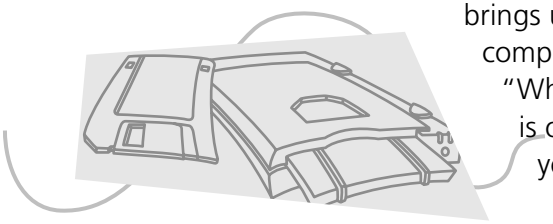
• • • • • • • • • • • • • • • • • •

The term "hacking" means breaking into a computer system or network. These two teens broke into government computers. Imagine the type of personal and financial information that our government collects! More shocking is the military information that is accessible to hackers. What happens next? Is all information stored on computers vulnerable?

Maybe. If you are connected to the Internet and have a Web page, you can be a target for hackers. Many government agencies, including the military, as well as businesses and home computer owners take great precautions to keep hackers out of their sensitive information. Encrypting files is the easiest and most common method of securing information before sending it over the Internet. Quite simply, encryption software scrambles the information. With the proper code, the intended recipient's computer can then unscramble it.

Unfortunately, for every prevention method consumers employ, there is a "genius" out there trying to defeat it. The *Back Orfice* program, for example, was created to attack online users without their knowledge. If someone is using the *Back Orfice* program, they can literally infiltrate your computer

while you are online. Once in your computer, the perpetrator can look at all your files and even delete files – again, while you have absolutely no clue that this is happening. This possibility brings up a question that every computer user should ask, "What type of information is on my hard drive?" If you have personal and financial information on your hard drive, that information may be vulnerable. Consider storing personal and financial information on disks instead. Once the information is stored on disks, put the disks in a fireproof safe.



BUSINESS SAFETY

It is wise to consider people who may work for you and have access to your company computers as potential liabilities. It isn't always the unknown people who cause irreparable damage to businesses. Often, information theft comes from within the ranks.

• • • • • • • • • • • • • • • • • • •

Fred Jones has a problem. An employee with administrative access to the company's computer system suddenly quit and went to work for a competitor. Fred suspects that this employee stole proprietary information (sensitive company information) and took it to his new employer. Did Fred's former employee commit a crime? And if he did, how can Fred, or law enforcement, prove that the former employee committed the crime of theft?

• • • • • • • • • • • • • • • • • • •

What do you think about this hypothetical situation? Did the employee commit a crime? Some say yes, some say no,

some say maybe. The big unanswered question: did Fred have any type of written company policy pertaining to computer access and the storage of data? This is key. If you own any type of business and utilize computers, you should have a solid, written policy regarding computers. Without an acknowledged policy, it would be difficult to convict an employee of theft. Additionally, theft is not the only thing you need to worry about. Should your employee steal personal information on other employees or clients and that information is used to commit crimes, you may be held liable in civil court if you did not take reasonable measures to safeguard that information.

Business owners, take note: create and implement a computer-related policy. Make sure that your employees read the policy and acknowledge it in writing.

Preventing computer crime in a business doesn't stop at creating a policy. If you own a small business and are computer-dependent, secure the information on your computers. Use the following crime prevention tips:

- Conduct thorough background checks on all employees, including temporary help. If you need assistance, contact a firm that specializes in conducting background checks.
- Do not allow temporary staff access to sensitive data.
- Require employees to use passwords that are a combination of letters and numbers. These passwords should be kept confidential and changed often.
- Initiate a company policy on backing up computers once a day. Secure all back up tapes or disks in a fireproof safe.
- Secure client and personnel information. Access to this information should be limited.
- Use surge and anti-virus protection on all computer systems.
- Remove all data from the hard drive before disposing of computers.

- ➢ Ensure that every computer operation can be handled by at least two trusted employees.
- ➢ Adopt written procedures for Internet usage by employees. This discourages downloading inappropriate material and viruses.
- ➢ Purge old records and information properly. Shred or erase the information so it cannot be used by others.
- ➢ Adopt a zero tolerance approach to high tech criminals. Insist on prosecuting and pursue all civil remedies.

• • • • • • • • • • • • • • • • • •

The $400 check looked real. The bank called and notified you that it was a fake. What happened? Your employee followed all of the check acceptance procedures and you even okayed it. The check looked real...

• • • • • • • • • • • • • • • • • •

Another hypothetical situation, but businesses are being swindled out of merchandise through this means at an alarming rate. It is the world of high technology crime and the bad guys are working diligently. Computer-generated personal checks, money orders, food stamps and traveler's checks are being manufactured on home computers and being passed off to the business community. For the bad guy, start-up costs are minimal, and many times, the bad guy uses stolen credit cards or fictitious checks to purchase the computer equipment.

As a business owner, how do you know if the check is real or fake? Calling the bank to verify every single check is not an option, so it is up to you and your employees to weed out the bad ones. This can be extremely difficult since the majority of fake checks have a valid bank account number, and check verification machines will accept and endorse the document. The problem is that the account is good, but the name on the check does not go with the verified account. The account number was stolen and placed on the fake check.

Additionally, fake picture identifications are also produced on home computers that match the checks. With all of this going on, how does a business owner combat this invasion of fake documents? The following steps will help protect you and your company:

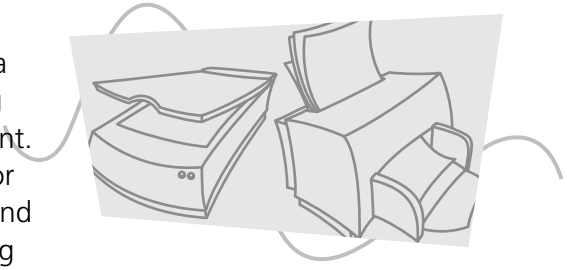
- ➢ Review your check and credit card acceptance policies. Many businesses and banks have started to require a thumb print on all checks. Some businesses feel that this practice may inconvenience their customers, and it is a controversial practice. The decision is yours.
- ➢ Train your employees to check identification when a customer is using a credit card.
- ➢ Employees should also make sure that the account number on the credit card matches the account number printed on the credit card receipt.

Obviously, you won't be able to spot every fake document, but alert employees can make a difference. Producing counterfeit or forged checks is not the only way criminals may affect your bottom line.

The bank calls to inform you that your company's account is overdrawn, but your records indicate there should be more than sufficient funds left in the account. An investigation reveals that several substantial checks have been cashed which look identical to yours with what seems to be your signature on them. However, the check numbers do not match your records.

Welcome to desktop forgery. Criminals have learned that many companies, small and large, routinely pay small billing invoices without checking their records to see if the product or service was ordered or received. If they send a fraudulent billing invoice in a small amount for some vaguely described

product or service, there is a good chance it will be paid. But they are not interested in cashing the check. They are interested in scanning the check into their computer, making a duplicate copy, changing the payee and the amount. They may make several or several hundred copies and you won't know anything until you receive a call from the bank or receive your monthly statement. Encourage your bookkeepers to track all invoices, whether large or small.



Glossary

Chat room: A site on the World Wide Web where any number of computer users can type in messages to each other in real time, thus creating an online conversation. Many chat rooms have a particular topic, but others are designed for meeting people.

Cloning: Making one cellular telephone act the same as another.

Dumpster diver: A slang term denoting an individual who rummages through trash cans and dumpsters looking for items of value, including personal information.

Hacking: Breaking into a computer system or network.

Search engine: A program that acts like a library card catalog for the Internet. Search engines attempt to help a user isolate desired information or resources by searching for key words that the user specifies.

Surfing: A slang term that means looking or browsing at Web sites.

Virus: A program or part of a program that is loaded into a computer and runs against your wishes. A simple virus may use all available memory and bring the system to a halt. More dangerous viruses can delete or change data on your hard drive.

Resources

Major credit reporting bureaus

Equifax
P.O. Box 740250
Atlanta, GA 30374-0250
Report fraud: Call (800) 525-6285 and write to the address above.
Order credit report: (800) 685-1111
Web site: *www.equifax.com*

Experian
P.O. Box 1010
Allen, TX 75013
Report fraud: Call (888) EXPERIAN or (888) 397-3742 and write to the address above.
Order credit report: same telephone numbers as above.
Web site: *www.experian.com*

Trans Union
P.O. Box 6790
Fullerton, CA 92634
Report fraud: Call (800) 680-7289 and write to the address above.
Order credit report: (800) 888-4213
Web site: *www.tuc.com*

You are entitled to a free credit report if you are a victim of identity theft (you may be asked to provide a copy or the number from a police crime report). If you want to check your credit report, you may have to pay a fee. Contact each bureau for a fee schedule.

U.S. Federal Trade Commission (FTC)

The FTC oversees the operation of the major credit reporting bureaus. The FTC Web site includes a copy of the Fair Credit Reporting Act. The FTC also provides assistance to identity theft victims and you can also access a complaint form on this Web site.

The FTC Consumer Response Center can be reached at:
(202) FTC-HELP
E-mail: crc@ftc.gov
Web site: *www.ftc.gov*

U.S. Social Security Administration

Report fraud: (800) 269-0271
Web site: *www.ssa.gov*

To remove your name from mail and phone lists, contact:
Direct Marketing Association
Mail Preference Service
P.O. Box 9008
Farmingdale, NY 11735
or
Telephone Preference Service
P.O. Box 9014
Farmingdale, NY 11735
Web site: www.the-dma.org

California Bureau of Investigation

Department of Justice
4949 Broadway
Sacramento, CA 95820
(916) 227-4061

High Tech Task Forces

Northern California:
Sacramento Valley Hi-Tech Crimes Task Force
c/o Sacramento County Sheriff's Department
711 G Street
Sacramento, CA 95814
(916) 874-3002
Web site: *www.sna.com/htct*

Silicon Valley/Bay Area:
Rapid Enforcement Allied Computer Team (REACT)
950 S. Bascom Avenue
San Jose, CA 95128
(408) 998-5633

Southern California:
High Tech Crime Task Force
c/o Los Angeles County Sheriff's Department
11515 Colima Road - M104
Whittier, CA 90604
(562) 946-7914

End notes:

1. *Use of the Internet, home PCs surging.* Stephanie Miles. CNET News.com. March 23, 1999.
2. *Sick, sneaky – and on the Web.* Diana Griego Erwin. Sacramento Bee. January 14, 1999.
3. *Online Crimes - Net exposure can be risky.* Raoul V. Mowatt. San Jose Mercury News. January 19, 1999.
4. *Judge unplugs 2 teens who hacked into U.S. computers.* Associated Press. Sacramento Bee. November 6, 1998.

Acknowledgments

The Attorney General's Office would like to thank the following individuals for their time, comments and expertise to ensure the accuracy of this publication:

Tony West	Special Assistant Attorney General
Robert Morgester	Deputy Attorney General, Criminal Law Division
Sergeant Michael Tsuchida	Supervisor, Sacramento Valley High Tech Task Force
Detective Michael Menz	Sacramento Valley High Tech Task Force
Lieutenant Stephen Ronco	San Jose Police Department and REACT (Rapid Enforcement Allied Computer Team)
Jack Skadsem	Executive Officer, Los Angeles/Orange Counties High Tech Crimes Task Force

Crime and Violence Prevention Center

Paul Seave	Director
Nancy Matson	Assistant Director
Vicki Wright	Crime Prevention Specialist
Gary Ensign	Art Director
Margaret Bengs	Editor
Oscar Estrella	Graphic Artist