



Message Filters
Credit card: Sel
Name on card:
Card number:
Secure Area

CRIME PREVENTION IN THE INFORMATION AGE

CRIME PREVENTION MONTH ACTION KIT
NOVEMBER 2005-OCTOBER 2006

Connect
http://
http://
http://
http://
http://

Lookies
Accept all cookies
OK

BJA Bureau of Justice Assistance
Office of Justice Programs • U.S. Department of Justice

tyco Fire & Security

ADT

NCPC
NATIONAL CRIME PREVENTION COUNCIL

CONTENTS



12-MONTH CALENDAR

COMMON SCAMS AND SCHEMES

CRIME PREVENTION COALITION OF AMERICA

NATIONAL CITIZENS' CRIME PREVENTION CAMPAIGN

SAMPLE PRESS RELEASE

A PROCLAMATION FOR CRIME PREVENTION MONTH 2006

NCPC RESOURCES

NATIONAL MCGRUFF® LICENSING PROGRAM

RESOURCES ON THE WEB

REPRODUCIBLE BROCHURES AND HANDOUTS

FEEDBACK REQUEST

CRIME PREVENTION MONTH ACTION KIT

NOVEMBER 2005–OCTOBER 2006

Dear Crime Prevention Practitioner,

We live in the age of technology. New technology allows criminals to commit traditional crimes like theft, forgery, and illegal drug sales in whole new ways. At the same time, new technology offers law enforcement state-of-the-art tools like shared databases, surveillance equipment, and crime-mapping software to help them fight crime. To be effective, today's crime prevention practitioner must combine traditional approaches (e.g., patrolling drug-infested neighborhoods, lighting dark parking lots, and cleaning up graffiti) with new approaches (e.g., educating citizens about illegal online pharmacies and telemarketing fraud).

Locks on doors and windows, for example, won't keep high-tech criminals from virtually strolling into people's homes in broad daylight via the Internet and the telephone. Hiding behind an electronic curtain, they can steal petty cash, life savings, and even personal identities. High-tech criminals won't be caught tiptoeing through backyards loaded down with stolen goods either. Their black market is virtual, not physical. In seconds, they can profit from their crimes by using the Internet to unload hot valuables like an individual's personal identifying information to anyone anywhere on the globe.

Keeping people safe in an age of technology crime is clearly a challenge for law enforcement. Patrol cars cannot cruise down the information superhighway looking for suspects. Fraudulent telemarketers don't set off security alarm systems when they call someone at home. And personal identities cannot be engraved with traceable numbers like cameras or TV sets so that thieves would have a harder time pawning or selling them.

Yet even when dealing with technology-related crime, the crime prevention practitioner can rely on two traditional techniques: (1) educating citizens on ways to stay safe and (2) asking them to be the "eyes and ears" of law enforcement by reporting criminal activity when they see it. A well-educated citizen won't let the high-tech criminal "in" in the first place. These citizens will know how to handle a fraudulent telemarketer or recognize an Internet scam when they

see one. They will spread the word and teach others in their communities about the dangers of technology fraud. And they will know how to notify law enforcement if they are scammed, so others won't also become victims.

Future technology holds great promise for crime prevention. Before long, every driver's license, credit card, and even passport will contain a "smart" chip that makes forgery difficult if not impossible. Face recognition technology will identify known terrorists in crowd situations at vulnerable events. And a completely integrated justice information system will get comprehensive data from every federal, state, and local source on criminal activity into the hands of law enforcement officers—even cops on the beat—via wireless, handheld computers in "real time."

This year's Crime Prevention Month Kit, developed on behalf of the Crime Prevention Coalition of America, will give you the tools you need to help protect citizens—and help citizens protect themselves—from technology crime. Each month offers the latest information about a technology-related crime, an organization working to address the crime, how citizens can report the crime, and reproducible brochures to educate citizens on ways to avoid victimization. The materials and resources in this kit are intended for you to use in your everyday outreach, your organization's newsletter, special planned activities, public service announcements, and targeted media campaigns.

Alfonso E. Lenhardt

President and CEO
National Crime Prevention Council

Tibby Milne

Chair, Executive Committee
Crime Prevention
Coalition of America



PROTECTING CITIZENS FROM IDENTITY THEFT

One of the most serious technology-related crimes facing Americans today is identity theft, defined as the stealing of another person's personal identifying information in order to fraudulently establish credit, run up debt, or take over existing financial accounts.

In 2003, the Federal Trade Commission (FTC) received 516,740 complaints from consumers, up from 404,000 in 2002. Of these, 214,905 (42 percent) were identity theft reports. According to the FTC's *2005 Identity Fraud Survey Report*, 9.3 million Americans have been victims of some form of identity theft in the last 12 months.¹

Identity theft has been around for a long time. Although identity thieves still use the hands-on approach like sifting through trash for credit-card statements or solicitations (dumpster diving), stealing purses and wallets, diverting a person's mail to another address, and obtaining personal numbers by looking over someone's shoulder during a transaction, technology has made it easier for them to steal someone's personal identifying information and get away with it.

Using a technique called "phishing," identity thieves send emails asking consumers to update their account information by entering it into a linked form or website that closely resembles that of a legiti-

mate company—but isn't. They also use the Internet and the telephone to encourage unsuspecting consumers to release personal information to claim phony prizes, donate to bogus charities, or transfer money for fake investments; then they steal their money and their identities. And they hack into business and personal computers to steal people's personal identifying information such as Social Security numbers and bank account information.

Raising public awareness about identity theft is the best approach to preventing this crime. If already victimized, consumers need to know how to limit the damage. The FTC recommends that consumers exercise caution when giving out personal information such as Social Security and credit card numbers, put passwords on credit card and bank accounts, and regularly inspect their credit reports.

The FTC's website, www.consumer.gov/idtheft/, is an excellent resource for identity theft prevention, with information for consumers, businesses, and law enforcement. Consumers can get advice by contacting the FTC's Identity Theft Hotline at **877-IDTHEFT (438-4338)**; they can also fill out an online complaint form on the website. The FTC enters complaints into Consumer Sentinel, an online database available to hundreds of law enforcement agencies. The FTC also offers an ID Theft Affidavit that makes it easier for consumers to dispute debts resulting from identity theft.

For additional websites with information on identity theft, see "Resources on the Web." For the handouts "Identity Theft" and "Protecting Your Private Information," see the reproducible section.

FTC's Identity Theft Hotline
877-IDTHEFT

9.3 million Americans have been victims of some form of identity theft in the last 12 months.



¹ Report available at www.javelinstrategy.com/reports/2005ReportBrochure.pdf.

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
6	7	1	2	3	4	5
13	14	8	9	10	11 Veterans' Day	12
20	21	15	16	17 Great American Smokeout American Cancer Society 800-ACS-2345	18	19
27	28	22	23	24 Thanksgiving Day	25	26
		29	30			



PUTTING A STOP TO SPAM SCAMS

To report spam
spam@uce.gov

Many people with email accounts find their inboxes flooded with unsolicited commercial email, also known as "spam." Most spam is annoying; it crowds out legitimate email, and deleting it takes time. Some spam, however, is illegal. These messages often imitate those used by fraudulent telemarketers and direct mail advertisers. They include pyramid and get-rich-quick schemes, chain letters that involve sending money and promise big returns, stock offerings for unknown start-up companies, work-at-home schemes, bogus charities, phony weight-loss claims, ads for pornographic websites, credit repair offers, and quack health products. Because spammers know people don't want these emails, they use deceptive subject lines to fool people into opening them. Spammers can also "hijack" a home computer by installing remote access software through a virus or other point of entry and then using the computer to send unsolicited email to other computers.

the email give recipients an opt-out method (a return email address must be provided that allows a recipient to request that future email messages be stopped, and this request must be honored); and it requires that commercial email be identified as an advertisement and include the sender's valid physical postal address.

Because spam marketers often harvest email addresses from the Internet, the Federal Trade Commission (FTC) advises people who wish to avoid unwanted email not to display their email address on the Internet in such places as newsgroup postings, chat rooms, or an online service's membership directory; to always check the privacy policy of any website to which they submit their email address; to use a unique email address; and to treat commercial email solicitations the same way they would treat unsolicited telemarketing calls: with skepticism and caution.

Deceptive or unwanted email can be reported to the FTC. A copy of the message should be sent to **spam@uce.gov**. The FTC uses the unsolicited emails stored in this database to pursue law enforcement actions against people who send deceptive spam email. The FTC's online complaint form at **www.ftc.gov** can be used to report spam with removal links that don't work or that do not allow the consumer to unsubscribe. This complaint will be added to the FTC's Consumer Sentinel database and made available to hundreds of law enforcement and consumer protection agencies.

For additional websites with information on spam, see pages "Resources on the Web." For the handouts "Don't Be Scammed!" and "Ten Tips To Secure Your Personal Computer," see the reproducible section.

The CAN-SPAM Act was passed in 2003 to protect people from illegal spam. This act bans false or misleading header information (the email's "from," "to," and routing must be accurate and identify the person who initiated the email); it prohibits deceptive subject lines (the subject line cannot mislead the recipient about the contents or subject matter of the message); it requires that



Most spam is annoying; it crowds out legitimate email, and deleting it takes time. Some spam, however, is illegal.

National Drunk and Drugged Driving Prevention Month
 National 3D Prevention Month Coalition
 202-452-6004

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
4	5	6	7	1	2	3
11	12	13	14	8	9	10
18	19	20	21	15	16	17
25	26	27	28	22	23	24
Hanukkah begins at sundown Christmas Day	Kwanzaa begins at sundown					
					Celebration of Life, Victim/Survivor Tribute MADD 800-438-6233	
					29	30
						31

CONFRONTING THE PROBLEM OF ELECTRONIC STALKING

The history of stalking is as old as the history of human relationships. Although the stalker's primary goal—to gain control over the victim by instilling fear and terror—has not changed over time, the techniques used by the stalker have. New technology has made it easier for stalkers to harass their victims anonymously and from a distance.

Among other techniques, the high-tech stalker uses sophisticated surveillance equipment such as global positioning systems and miniature video cameras to track or spy on the victim; obtains information such as the victim's address and place of employment over the Internet; and delivers threatening messages to the victim's computer via email. The stalker also spreads damaging rumors about the victim through Internet chat rooms, message boards, and webpages—often without the victim's knowledge.

Advances in telecommunications may have changed the nature of stalking but not its effect. The victim suffers psychological trauma

24 hours a day, seven days a week, which often results in anxiety, depression, insomnia, and even loss of employment. Whether perpetrated online or offline, stalking can have the same deadly consequences. In a significant number of cases, stalking is a precursor to lethal violence. Stalking is against the law, and most states give law enforcement the legal tools

to intervene in stalking cases before the offenders act upon their threats to harm their victims. Unlike crimes such as assault and robbery, stalking is a mix of criminal and noncriminal behaviors that can occur over a long period of time and in different police jurisdictions. As a result, several police agencies may be involved in coordinating the investigation.

One approach to preventing online harassment is to educate Internet users on how to make informed decisions online and how to document harassment and report it. Law enforcement should ensure that all victims of stalking receive consistent support services; take a collaborative approach by involving other community resources; and develop a system for sharing information and coordinating responses when stalking occurs in multiple jurisdictions.

The Stalking Resource Center, www.ncvc.org, is a program of the National Center for Victims of Crime (NCVC) that offers information on stalking such as how to make a safe plan, how to create a stalking incident and behavior log, state stalking laws, and other resources. NCVC has developed a model protocol to promote more effective anti-stalking policies by police departments across the nation.

For additional websites with information on stalking and cyberstalking, see "Resources on the Web." For the handout "How To Avoid Being Stalked in Cyberspace," see the reproducible section.

Stalking Resource Center
www.ncvc.org



Advances in telecommunications may have changed the nature of stalking but not its effect.

SM

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
1 New Year's Day	2	3	4	5	6	7
8	9	10	11	12	13	14
15 Justice Sunday National Alliance of Faith and Justice 703-765-4459	16 Martin Luther King, Jr. Birthday MLK Day Events Corporation for National and Community Service 202-606-5000	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Stalking Awareness Month
National Center for Victims of Crime
202-467-8700

Crime Stoppers Month
Crime Stoppers International, Inc.
601-987-1335



ADDRESSING TELECOMMUNICATIONS FRAUD

FCC's website
www.fcc.gov

The telecommunications industry is booming. Telephones, cell phones, and pagers make it easy to keep in touch. But fraud associated with telecommunications technology is also booming.

Here are some common scams:

- Cell phone subscription fraud occurs when a criminal obtains personal information about an individual and uses that information to sign up for service in the individual's name.
- Cell phone cloning occurs when a criminal monitors radio wave transmissions to steal a cell phone subscriber's unique electronic serial number and telephone number, and uses them to create a cloned cell phone.
- Phone "cramming" is the practice of placing unauthorized, misleading, or deceptive charges on a consumer's local or long-distance telephone bill.

- Phone "slamming" is the illegal practice of changing a consumer's long-distance telephone service without his or her permission.

- Calling-card number scams occur when a criminal poses as a telephone company representative and asks a consumer for "verification" of a calling-card number to check for unauthorized charges, then uses it to make international calls.

- Pager and voice mail scams trick the consumer into making long-distance calls by sending a message indicating a family emergency or urgent legal matter. When the consumer returns the call, he or she is charged for an international call.
- Voice mail fraud occurs when hackers use a consumer's voice mail system to make long-distance collect calls without the consumer's knowledge.
- Modem hijacking happens to people who have dial-up connections to the Internet. Victims are prompted to download a "dialer" program for free. This program redirects their phone connection, resulting in expensive long-distance charges.

The best defense against telecommunications fraud is a well-informed consumer who knows how to identify scams, how to create and protect voice mail passwords, how to check phone bills for cramming and slamming charges, and how to determine the location of an area code before making a call.

The Federal Communications Commission (FCC) website, www.fcc.gov, offers consumer fact sheets on telecommunications fraud including cell phone fraud, Internet modem switching scams, voice mail fraud, 809 phone scams, and deceptive phone bill charges. Citizens can file a complaint by email (fccinfo@fcc.gov), the Internet (www.fcc.gov/cgb/complaints.html), or telephone (888-CALL-FCC or 888-225-5322).

For additional websites with information on telecommunications fraud, see pages 36. For the handout "Protect Yourself From Telephone Fraud," see the reproducible section.

The best defense against telecommunications fraud is a well-informed consumer who knows how to identify scams.



SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
5	6	7	1	2	3	4
12	13	14	8	9	10	11
19	20	21	15	16	17	18
26	27	28	22	23	24	25

National Consumer Protection Week 5-11
www.consumer.gov/ncpw

National Child Passenger Safety Awareness Week 12-18
 National Highway Traffic Safety Administration
 202-366-9550

Presidents' Day



COMBATING ILLEGAL DRUGS ON THE INTERNET

Many Americans are turning from their local “brick-and-mortar” pharmacies to “point-and-click” pharmacies for medications. Legitimate Internet pharmacies offer many advantages over the corner drugstore, including lower prices, greater privacy, and the convenience of home delivery, while providing the same quality drugs. Just like a regular pharmacy, they require a doctor’s prescription, insurance information, and a credit card.

With hundreds of drug-dispensing websites in business, consumers often have trouble distinguishing which sites are legitimate ones, especially when it is easy to set up a site that is very professional looking and promises deep discounts. Illegal Internet pharmacies, which can operate from any part of the world, ship counterfeit, contaminated, or adulterated drug products to unsuspecting consumers. They promote unapproved drug products by making deceptive claims that these products cure arthritis, cancer, AIDS, and other diseases.

They even sell dangerous and addictive substances such as painkillers, stimulants, and depressants without a prescription—to anyone with a credit card number.

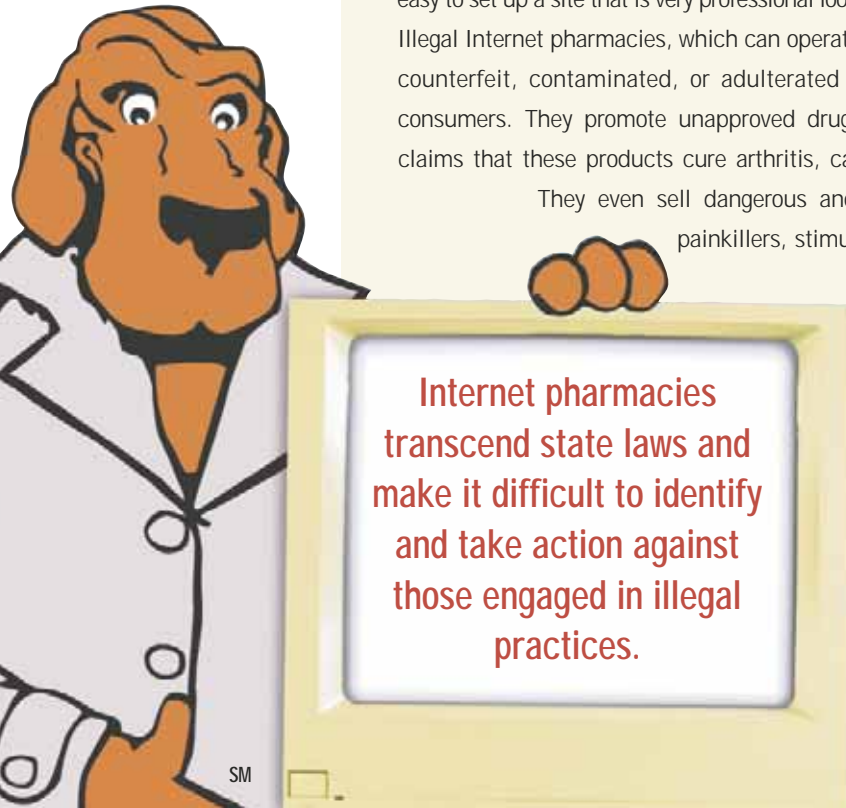
The nonmedical use of controlled pharmaceuticals is a growing problem in this country. Internet pharmacies unwittingly play a major role in the increasing illicit supply of pharmaceutical products containing narcotic drugs

and psychotropic substances. Even juveniles can purchase narcotics over the Internet by using a search engine and typing in their parents’ credit card number. Because the licensing and regulation of pharmacists traditionally take place at the state level, Internet pharmacies transcend state laws and make it difficult to identify and take action against those engaged in illegal practices.

Consumers should be advised that if they wish to purchase prescription drugs on the Internet, they should first visit their doctor and obtain a prescription to avoid serious health risks. They should look for the website of a pharmacy they’re familiar with, or for sites that display the Verified Internet Pharmacy Practice Sites seal of approval from the National Association of Boards of Pharmacy (www.nabp.net). Parents and other caregivers should be warned of the threat of Internet prescription drug pushers.

The website of the U.S. Food and Drug Administration (FDA), www.fda.gov, offers information for consumers on how to safely and legally buy medical products online. Consumers can report a suspicious Internet pharmacy by filing a report with the Drug Enforcement Administration (DEA) online at www.deadiversion.usdoj.gov/ or calling 877-Rx-Abuse (877-792-8273). If the complaint involves any pharmaceutical drug other than a controlled substance, a report should be filed on the FDA’s website at www.fda.gov/oc/buyonline/buyonlineform.htm.

For additional websites with information on illegal online pharmacies, see “Resources on the Web.” For the handout “Protecting Yourself From Counterfeit Drugs,” see the reproducible section.



Internet pharmacies transcend state laws and make it difficult to identify and take action against those engaged in illegal practices.

Report suspicious Internet pharmacies
877-RX-ABUSE

National Red Cross Month
National Red Cross
202-303-4498

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
5	6	7	1	2	3	4
12	13	14	8	9	10	11
19	20	21	15	16	17	18
26	27	28	22	23	24	25
			29	30	31	

Girl Scout Week 12-18
Girls Scouts of the USA
212-852-8100

National Inhalants and Poisons
Awareness Week 19-25
National Inhalants Prevention Coalition
800-269-4237

SECURING PERSONAL AND BUSINESS COMPUTERS

Report Cyber threats
www.us-cert.gov

Citizens must secure their computers in order to protect our nation's Internet infrastructure, according to the National Cyber Security Alliance, a public-private partnership affiliated with the U.S. Department of Homeland Security. Many people who own computers don't realize that they need to pay attention to computer security the same way they pay attention to home, business, or automobile security.

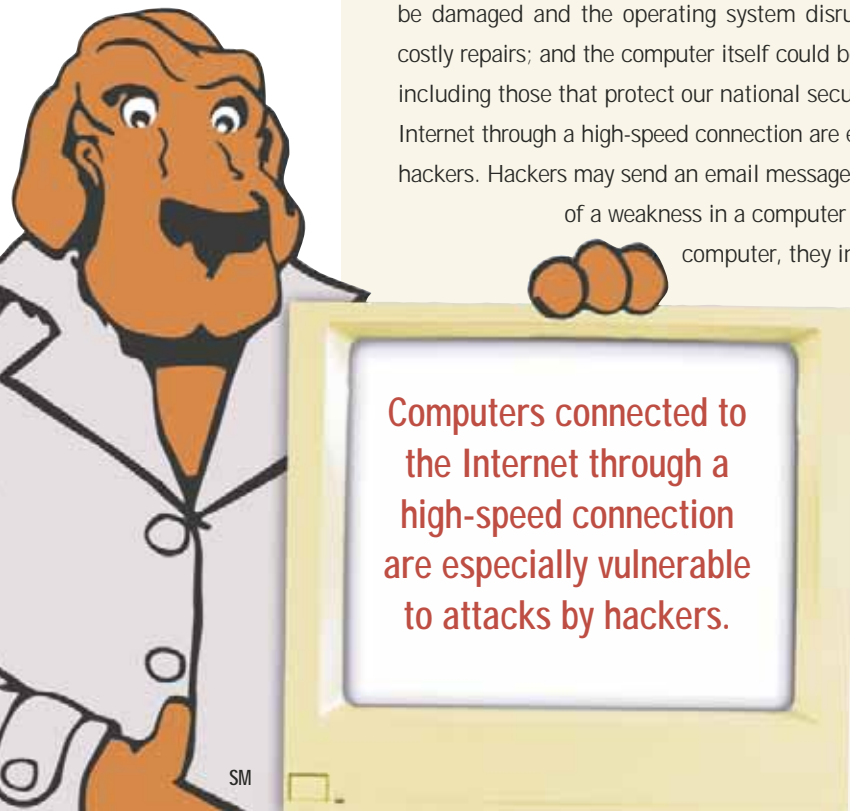
Home computers are often not very secure. If a computer is attacked by a hacker or virus, personal data such as Social Security and bank account numbers could be stolen, resulting in identity theft and other types of fraud; files could be damaged and the operating system disrupted, resulting in lost data and costly repairs; and the computer itself could be used to attack other computers, including those that protect our national security. Computers connected to the Internet through a high-speed connection are especially vulnerable to attacks by hackers. Hackers may send an email message with a virus that takes advantage of a weakness in a computer program. Once hackers get into a computer, they install new programs that let them continue to use the computer.

The best approach to prevention is to educate home and business computer owners on ways to secure their computers by using anti-virus software and keeping it up-to-date; using "firewalls" to protect the computer from intruders; installing programs to detect adware (a software

application in which advertising banners are displayed; it usually includes a code to track the user's personal information); not opening emails or attachments from unknown sources; using hard-to-guess passwords; backing up computer data on disks or CDs regularly; disabling software that permits file sharing; disconnecting the computer from the Internet when it's not in use; and downloading security updates. In addition, there are programs that erase the hard drive if a business or home user is selling, donating, or disposing of old computer equipment, but these programs are not always failsafe. Instead, instruct users to remove the hard drives and destroy them. Small businesses often end up as part of larger attacks, such as mass worm outbreaks or efforts to steal credit card numbers. The Better Business Bureau recommends that businesses teach their employees what to do if computers become infected.

The National Cyber Security Alliance (NCSA) is the U.S. Department of Homeland Security's partner for cyber security awareness and education outreach for the home user, small business, and education audiences. NCSA's website, www.staysafeonline.info, provides tools and resources to promote safe and responsible computer use including a top ten list of computer safety tips, alerts, and cyber safety checklists. This cyber security information enables users to increase their protection against online threats including viruses, worms, hacker attacks, identity theft, and spyware. To report a network intrusion or other cyber threat, consumers can file an online report with the U.S. Computer Emergency Readiness Team, www.us-cert.gov.

For additional websites with information on computer security, see pages "Resources on the Web." For the handouts "Ten Tips To Secure Your Personal Computer" and "Working Safely at Home," see the reproducible section.



Child Abuse Prevention Month
Prevent Child Abuse America
312-663-3520

Alcohol Awareness Month
National Council on Alcoholism and Drug Dependence, Inc.
212-269-7797

SUNDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
2	4	5	6	7	8
9	10	12	13	14	15
16	17	18	19	20	22
23	24	25	26	27	29
30					1

Event Details:

- 3:** National Youth Violence Prevention Week 3-7
National Youth Violence Prevention Campaign
800-99-YOUTH
- 7:** Alcohol-Free Weekend 7-9
National Council on Alcoholism and Drug Dependence, Inc.
212-269-7797
- 21:** National Youth Service Days 21-23
Youth Service America
202-296-2992
- 27:** Take Our Daughters and Sons to Work Day
Ms. Foundation for Women
800-676-7780
- 23-29:** National Volunteer Week
Points of Light Foundation
202-729-8168

KEEPING SENIORS SAFE FROM TELEMARKETING FRAUD

Technology has improved the quality of life for seniors by offering them both convenience and peace of mind. Yet this same technology—especially the telephone and the Internet—also exposes them to potential financial victimization. Criminal telemarketers are one of the top fraud threats to senior citizens, and the same scams they pitch over the telephone are showing up on the Internet. According to the National Consumers League, one of every six Americans is victimized by fraudulent telemarketers at a cost of over \$40 billion each year. AARP (formerly the American Association of Retired Persons) reports that more than half of telemarketing fraud victims are 50 or older. Seniors are more likely to receive fraudulent telephone offers because they have assets, are home alone more often, and tend to be more trusting or easily intimidated.

The top ten telemarketing frauds reported to law enforcement involve credit card offers, work-at-home plans, prizes/sweepstakes, advance fee loans, magazine sales, buyers' clubs, Nigerian money offers, telephone cramming (unauthorized charges on a phone bill), travel/vacations, and credit card loss protection plans. People who are scammed may have their names placed on sucker lists that are sold to other criminals, who then contact them hoping to scam them again by offering to recover the money they lost in the previous scam.

Seniors on the Internet may also receive spam emails pitching counterfeit drugs, "free" vacations, life insurance and other telemarketing scams. If they provide their personal information such as Social Security numbers, bank account numbers, and credit card numbers over the phone or online, they may also become victims of identity theft.

A senior's best defense against telemarketing fraud is the ability to recognize the danger signs. Seniors need to know how telemarketing works; how to identify fraudulent telemarketing calls; how to protect themselves against telemarketing by not providing bank account, credit card, or other financial information to unsolicited callers; how to get off marketing lists; and how to report an incident.

The Telemarketing Fraud Educators' Toolbox is a new resource on telemarketing fraud available at www.fraud.org/toolbox/members.htm. The Toolbox provides handouts and brochures with telemarketing fraud prevention tips, PowerPoint presentations, mat releases for newsletters, scripts for radio public service announcements, speeches, statistics from the National Fraud Information Center, advice for victims, and more. Materials are available in English and Spanish and in both PDF and HTML formats. The Toolbox was developed by the National Consumers League in partnership with the Bureau of Justice Assistance, U.S. Department of Justice.

For additional websites with information on telemarketing fraud, see "Resources on the Web." For the handouts "Use Common Sense To Spot a Con Artist," "Shopping Safely Online," "Protecting Your Private Information," and "Preventing Charity Fraud," see the reproducible section.

National Fraud Information Center
www.fraud.org



One of every six Americans is victimized by fraudulent telemarketers at a cost of over \$40 billion each year.

	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
	1 Law Day The American Bar Association 312-988-5000	2	3	4	5	6
SUNDAY	7	8	9	10	11	12
	13	14 National Police Week 14-20 Concerns of Police Survivors, Inc. 573-346-4911 Alcohol and Other Drug-Related Birth Defects Awareness Week 14-20 National Council on Alcoholism and Drug Dependence, Inc. 212-269-7797	15 National Peace Officers Memorial Day Concerns of Police Survivors, Inc. 573-346-4911	16	17	18
	19	20	21	22	23	24
	25 National Missing Children's Day National Center for Missing and Exploited Children 800-843-5678	26	27	28	29 Memorial Day	30
	31					

Older Americans Month
Administration on Aging
U.S. Department of Health and Human Services
202-619-0724

National Teen Pregnancy Prevention Month
Advocates for Youth
202-347-5700

PREVENTING ONLINE SEXUAL EXPLOITATION OF CHILDREN

The Internet has had a serious impact on the sexual exploitation of children, specifically the distribution of sexually exploitive images of children. According to the National Center for Missing and Exploited Children, the use of home-computer technology has revolutionized the distribution of these images by increasing the ease and decreasing the cost of production and distribution, especially across international borders. A greater number of child molesters are now using computer technology, not only to organize and maintain their collections of these illegal images, but to add to them as well.

The Internet has also dramatically increased sex offenders' access to the population they seek to victimize. Although some computer sex offenders primarily collect and trade child pornographic images over the Internet, others seek face-to-face meetings with children via online contacts. Once contact is made, child molesters may use pornography to seduce their prey, to lower the victim's inhibitions, and to serve as a kind of instruction manual—claiming to prove to the child that

sex between an adult and a child is "normal." Whether children come across pornography accidentally online or are deliberately exposed to it, viewing these images can result in devastating psychological effects.

Under federal law, it is illegal to possess, distribute, or manufacture pornographic images of children. The Innocent Images National Initiative (IINI), a compo-

nent of the FBI's Cyber Crimes Program, is a multi-agency initiative that uses new technology and sophisticated investigative techniques to identify, investigate, and prosecute sexual predators who use the Internet and online services to sexually exploit children; establish a law enforcement presence on the Internet as a deterrent to those who use it to exploit children; and identify and rescue child victims. To proactively combat this crime problem, IINI undercover operations are being conducted in FBI field offices by task forces that combine the resources of the FBI with other enforcement agencies.

The Internet Keep Safe Coalition teaches children the basic rules of Internet safety through a variety of resources including children's books, a website (www.ikeepsafe.org), and public service advertising. The website features

an animated icon/mascot named Faux Paw the Techno Cat to teach children the importance of protecting personal information and avoiding inappropriate places on the Internet. The Internet Keep Safe Coalition is a partnership of several governors' first spouses, government agencies, nonprofit organizations, and corporate sponsors. Members include the National Center for Missing and Exploited Children, the FBI Internet Crimes Taskforce, the U.S. Department of Justice, the American Medical Association, and the National Crime Prevention Council. The Coalition works to customize the program for individual states.

For additional websites with information on Internet safety, see "Resources on the Web." For the handouts "A Family Guide to Using the Internet" and "Kids: Be a Good Cyber Citizen!" see the reproducible section.

Internet Keep Safe Coalition
www.ikeepsafe.org



The use of home-computer technology has revolutionized the distribution of sexually exploitive images of children by increasing the ease and decreasing the cost.

SM

National Internet Safety Month
I-SAFE America
760-603-7911

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
4	5	6	7	1	2	3
11	12	13	14	8	9	10
18	19	20	21	15	16	17
25	26	27	28	22	23	24
				29	30	

FIGHTING FRAUD ON THE INTERNET

Fraud can occur whenever an exchange of money for goods or services takes place. Because many people are doing business online, the number of incidents involving Internet fraud is increasing. Internet fraud refers to any scheme that uses the Internet to make fraudulent solicitations, conduct fraudulent transactions, or transmit the proceeds of fraud to financial institutions or other criminals. According to the Internet Crime Complaint Center, the most frequently reported offenses in 2003 were Internet auction fraud, nondelivery of merchandise or payment, and credit/debit card fraud. Other schemes—check fraud, business fraud, identity theft, investment fraud, confidence fraud, intellectual property fraud, and Nigerian letter fraud—were also reported.

Online auctions and other retail sales are especially vulnerable to fraud because of the anonymity of buyers and sellers. Both consumers and merchants can be victims of online fraud. Fraud occurs when there is failure to deliver or pay for goods and services, misrepresentation of merchandise

(value of the items is exaggerated), fake bidding, credit card fraud, identity theft, black market goods, and hidden charges such as excessive shipping and handling fees.

Using a technique called phishing, criminals send spam emails to consumers asking them to update their account information

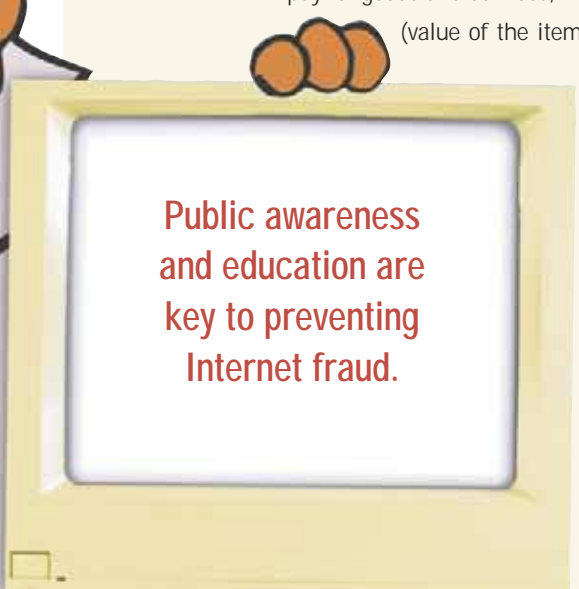
by clicking on a link to the company's website. The website looks like the real thing but is bogus and allows the criminals to steal any personal information that a consumer enters. Pharming (also called domain spoofing) is a similar technique, but it does not require the consumer to click on a link in an email. Instead, criminals redirect Web traffic from a legitimate server to their own server for the purpose of stealing personal information.

Public awareness and education are key to preventing Internet fraud. The better people are able to recognize the danger signs of fraud on the Internet, the less likely they will be scammed by criminals. It's also important for victims to report scams quickly so that law enforcement agencies can shut down the fraudulent operations.

The National Fraud Information Center was created by the National Consumers League to offer consumers advice about promotions in cyberspace. The website, www.fraud.org, provides tips on Internet fraud, telemarketing, elder fraud, scams against businesses, counterfeit drugs, phishing, and other scams. Victims of Internet fraud can file an online complaint on the website or call **800-876-7060**. Victims can also file an online complaint with the Internet Crime Complaint Center (IC3), www.ic3.gov, a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center.

For additional websites with information on Internet fraud, see "Resources on the Web." For the handouts "Don't Be Scammed!" "Online Auction Fraud," "Shopping Safely Online," "Protecting Your Private Information," and "Preventing Charity Fraud," see the reproducible section.

Internet Crime Complaint Center
www.ic3.gov



Public awareness
and education are
key to preventing
Internet fraud.

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
2	3	4	5	6	7	8
9	10	11 Independence Day	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

National Fraud Awareness Week 10-16
Association of Certified Fraud Examiners
800-245-3321

PREVENTING CREDIT CARD FRAUD

For as long as there have been credit cards, criminals have used them to commit fraud. Credit card fraud costs cardholders and issuers hundreds of millions of dollars each year. In the 1950s, technology played a major role in the development of the credit card. Now technology is being used by criminals to perpetrate credit card fraud and get away with it.

In the past, criminals relied on stolen credit cards to commit fraud. These cards had to be used quickly, before their loss was discovered and reported. Today, credit card theft is often committed without the physical card. Fraudulently obtained credit card numbers can be used until the consumer is notified by the issuer—usually through a monthly statement—that unauthorized charges have been made.

Criminals obtain credit card numbers in a variety of ways. Fraudulent telemarketers ask for credit card numbers when offering bogus prizes, goods, and services.

The same scams occur on the Internet; when consumers enter their credit card numbers in response to a fraudulent offer, the numbers are stolen.

Criminals also obtain credit card numbers by stealing mail and discarded receipts, making an extra imprint of the card during a legitimate purchase, and hacking into computer systems to steal credit card information.

The most common form of credit card fraud today involves the illegal counterfeiting of credit cards. Desktop computer systems—along with special devices such as embossers, encoders, and decoders—can produce realistic-looking credit cards in minutes. Criminals also use technology to “skim” the data contained on the magnetic strips of legitimate cards and copy the data onto blank cards that can be used or sold to other criminals.

FTC's credit card fraud line
877-FTC-HELP

Educating the public about the importance of guarding credit cards and credit card numbers is the best approach to credit card fraud prevention. Citizens who recognize fraudulent schemes, who check out merchants before ordering online, who carefully review their credit card statements, and who shred credit card and other financial statements before throwing them away are less likely to be victims of credit card fraud.

The Federal Trade Commission website, www.ftc.gov, offers information on choosing credit cards, avoiding credit and debit card fraud, using credit cards online, consumer rights, how to get a free annual credit report, and more. To report a lost or stolen credit or charge card, consumers should call the credit card issuer immediately. If the theft is fraud-related, they should file an online complaint or call toll-free **877-FTC-HELP (877-382-4357)**.

For more websites with information on credit card fraud, see “Resources on the Web.” For the handouts “Shopping Safely Online,” “Use Common Sense To Spot a Con Artist,” “Protecting Your Private Information” and “Don’t Be Scammed!” see the reproducible section.



The most common form of credit card fraud today involves the illegal counterfeiting of credit cards.

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
6	7	1 National Night Out National Association of Town Watch 610-649-7055	2	3	4	5
13	14	8	9	10	11	12
20	21	15	16	17	18	19
27	28	22	23	24	25	26
		29	30	31		



TEACHING CHILDREN CYBER ETHICS

Cyber ethics information
www.cybercrime.gov

Just as protecting children and youth from dangers on the Internet is important, so is protecting the Internet from young people who might abuse it. Almost every day there are reports of youth-perpetrated crimes such as hacking into computer networks or spreading computer viruses. Youth do not need to be highly skilled in order to commit cyber crimes. Hacker tools can be downloaded easily from the Internet. Software can be copied and shared with a few clicks of the mouse. Passwords can be stolen and misused.

Youth may know what they are doing is wrong but do not realize that it's also illegal and could result in prosecution. Those who would never think of stealing CDs from their local music store might not hesitate to use file-sharing programs to "share" copyrighted music. Pranksters who send someone a computer virus that destroys his or her hard drive may not realize that this is a crime, not a prank. Kids who threaten or spread rumors about other kids on the Internet are no different from bullies on the playground and are guilty of harassment.



The best way to prevent cyber crime is to educate children and youth about the ethical and legal rules of the Internet.

Even teachers, parents, and other caregivers might not realize the ethical and legal implications of children's criminal behavior online. Parents and caregivers may be legally liable for acts of their children on the Internet. The U.S. Department of Justice categorizes cyber crime in three ways:

- The computer as a target (using a computer to attack other computers): Children who hack into school computer networks to view or change grades, deface websites, and create computer viruses are committing cyber crimes.
- The computer as a weapon (using a computer to commit a crime): Children are committing cyber crimes when they use email and chat programs to harass others by saying things they would never say face to face or when they steal passwords in order to read other people's emails or to send emails in their name.
- The computer as an accessory (using a computer to store illegal files or information): Children who download and share copyrighted music and other programs without the permission of the owner are committing cyber crimes.

The best way to prevent cyber crime is to educate children and youth about the ethical and legal rules of the Internet, the financial and emotional cost of cyber crime to victims, and the consequences for committing cyber crimes. Parents and other caregivers should also be educated on the importance of monitoring their children's use of the Internet.

The website of the Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice, www.cybercrime.gov, has information for kids, parents, and teachers on cyber crime and cyber ethics, especially relating to intellectual property crime and hacking.

For more websites with information on Internet safety and cyber ethics, see "Resources on the Web." For the handouts "Kids: Be a Good Cyber Citizen!" and "A Family Guide to Using the Internet," see the reproducible section.

National Alcohol and Drug
 Addiction Recovery Month
 Center for Substance
 Abuse Treatment
 301-443-5052

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
3	4 Labor Day	5	6	7	8	9
10 National Suicide Awareness Week 10-16 American Association of Suicidology 202-237-2280	11	12	13	14	15	16
17	18	19	20	21	22	23 Ramadan begins
24	25	26	27	28	29	30

USING TECHNOLOGY TO FIGHT CRIME

Sixty years ago, two new technologies—the patrol car and the two-way radio—greatly improved the effectiveness of law enforcement. Today, new information and communications technologies give law enforcement even better crime-fighting tools. These technologies are expensive and often require training, but the cost and effort pay off. New crime-fighting technologies include the following:

- Computer programs that allow law enforcement officials to rapidly collect information about people who commit crimes and the places where crimes occur and to share this information with other law enforcement agencies
- Surveillance technology such as closed circuit television, mobile or fixed-site video cameras, night vision and electro-optical surveillance, and Global Positioning Systems that help deter or capture and prosecute criminals
- Detection technology such as weapon detection programs, intrusion detection, and access control

- The AMBER Alert Plan, which broadcasts the descriptions of an abducted child and the suspected abductor on radio and television stations, on electronic highway billboards, and over the Internet

- Expanded testing of DNA evidence in forensic laboratories and the development by the FBI of a national DNA database that includes samples from convicted criminals and crime scenes for use in determining guilt or innocence
- Offender-tracking technology that enables crime victims, their families and friends, and law enforcement to obtain up-to-the-minute information about an offender, such as custody status, facility where housed, release date, and upcoming court information
- Computer technology such as anti-virus programs that protect computers from worms and viruses, firewalls that protect computers from hackers and intruders, and encryption software to keep information secure as it travels over the Internet

The Office of Science and Technology within the National Institute of Justice (NIJ), www.ojp.gov/nij/sciencetech, is a focal point for research and development of new technology to support the criminal justice system. NIJ funds development of technologies to improve the safety and effectiveness of law enforcement and corrections professionals. NIJ develops new forensic science technologies and helps crime laboratories enhance their capacity to access and use new technology. Technology research areas include less than lethal weapons, critical incident prevention and response, interoperable communications, sensors and surveillance, information sharing, electronic crime, personnel protection, DNA forensics, and general forensics.

For more websites with information on technology used to fight crime, see "Resources on the Web."

Office of Science and Technology
www.ojp.gov/nij/sciencetech



Today, new information and communications technologies give law enforcement even better crime-fighting tools.

SM

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
1	2	3	4	5	6	7
8	9 Columbus Day National Fire Prevention Week 9-14 National Fire Protection Association 617-984-7275	10	11	12	13	14
15 America's Safe Schools Week 15-21 National School Safety Center 605-373-9977	16 Week Without Violence 16-22 YWCA of the U.S.A. 888-992-2463	17	18	19	20	21
22	23 National Red Ribbon Week 23-31 National Family Partnership 800-705-8997	24	25	26	27	28
29	30	31 Halloween	Crime Prevention Month National Crime Prevention Council 202-466-6272 National Cyber Security Awareness Month National Cyber Security Alliance 202-331-5350	Child Health Month American Academy of Pediatrics 847-434-4000 Let's Talk Month Advocates for Youth 202-347-5700	Domestic Violence Awareness Month National Coalition Against Domestic Violence 303-839-1852 Trick or Treat for UNICEF Month U.S. Committee for UNICEF 800-FOR-KIDS	

COMMON SCAMS AND SCHEMES



Scams that appear online often mirror fraudulent scams perpetrated over the phone or through the mail. The Internet allows criminals to reach thousands of users by sending emails, posting items on auction sites, posting messages on bulletin boards, entering chat rooms, or building websites. What follows is a list of common scams that are pitched through the mail, over the phone, and on the Internet:

Telephone cramming occurs when unauthorized charges for services are put on a person's phone bill. Because phone companies now bill for legitimate services on behalf of other companies, bills have become complicated, and customers may not notice the "extra" charges.

■ **CREDIT-RELATED SCHEMES:** For payment of an advance fee, a person is promised credit cards and loans regardless of credit history, or credit card protection or credit repair services, but the cards, loans, or services are never delivered. Often the person targeted has a poor credit history or large debt.

■ **MAGAZINE SALES SCAMS:** A consumer is promised a new magazine subscription or the renewal of a subscription at a very low price by someone who claims to work for the magazine company. Often the price is misrepresented (e.g., "pennies" a day but over time the cost is high) or the magazine is never delivered. A victim who supplies credit card or bank account numbers may then become a victim of identity theft.

■ **INVESTMENT FRAUD:** A person is invited to participate in investment opportunities with the promise of spectacular profits and no risk—but the opportunities are usually bogus. In the "pump and dump" scheme, fraudulent promoters claim to have inside information about a company in order to get the stock price "pumped" up by gullible investors; then they sell or "dump" their shares quickly, causing the price of the stock to fall and the investors to lose their money.

■ **PHARMING:** Also called "domain spoofing," this technique is used by criminals to redirect Web traffic from a legitimate server to their own server, where they can steal any personal information that the user types in. Pharming is different from phishing in that it does not require the user to click on a link in an email. Instead, pharmer's poison the Domain Name Service in order to "fool" a user's browser into linking to a bogus website rather than the legitimate one when the user types in the web address.

■ **NIGERIAN MONEY SCAM:** A person is contacted by someone from Nigeria or another African country and offered millions of dollars (or a percentage of a large sum) for helping transfer money from a foreign bank to the person's bank account for safekeeping. Then the person is asked for an endless series of payments for transfer fees or legal expenses and other bogus costs, but the large sum of money is never transferred.

■ **PRIZE AND SWEEPSTAKES SCAM:** A person is told that he or she has won a fabulous prize but must buy something or pay taxes up front in order to claim it. The person may also be asked for bank account information so the prize money can be wired. It is illegal for a company to require someone to make a purchase or pay fees to enter a contest or claim a prize. A person who provides bank account numbers may also be at risk for identity theft or other fraud.

■ **FOREIGN LOTTERIES SCAM:** A person is offered tickets to enter a foreign lottery and sends money, but either the lottery doesn't exist or the tickets never arrive. It is illegal to promote a foreign lottery by telephone or mail in the United States.

■ **PYRAMIDS AND MULTILEVEL MARKETING:** Profits are promised in exchange for recruiting new members. Participation requires payment. Plans that promise profits for recruitment of members rather than for selling goods and services are illegal and inevitably collapse.

■ **OVERPAYMENT SCAMS:** A buyer will contact a seller and offer to purchase some merchandise. The buyer will send a cashier's check or money order for more than the asking price, with instructions for the seller to wire back the difference for overpayment. The check is counterfeit, but the seller doesn't discover this until after wiring the money and sending the merchandise.

■ **WORK-AT-HOME SCAMS:** Emails or other advertisements promise false profits for people who want to work at home. People pay for training or materials but then find that there are no clients to pay for their work. Some work-at-home schemes are classic illegal pyramid schemes in which participants attempt to make money solely by recruiting new participants into the program.

■ **VACATION/TRAVEL FRAUD:** A person is offered a free or very cheap travel package, but it is neither free nor cheap. There may be hidden costs, such as reservation fees or taxes, to be paid up front, or the recipient must endure high-pressure sales pitches for a timeshare or travel club membership. In some cases, fraudulent travel operators take the money and disappear.

■ **PHISHING:** A criminal copies the content of a legitimate retailer, bank, or government agency website to a newly created fraudulent website. The website address closely resembles the real name of the legitimate business. The victim receives an email that asks him or her to update or verify account information with a link to the fraudulent site. If the victim is fooled into entering Social Security, credit card, and bank account numbers, identity theft or other fraud may occur.

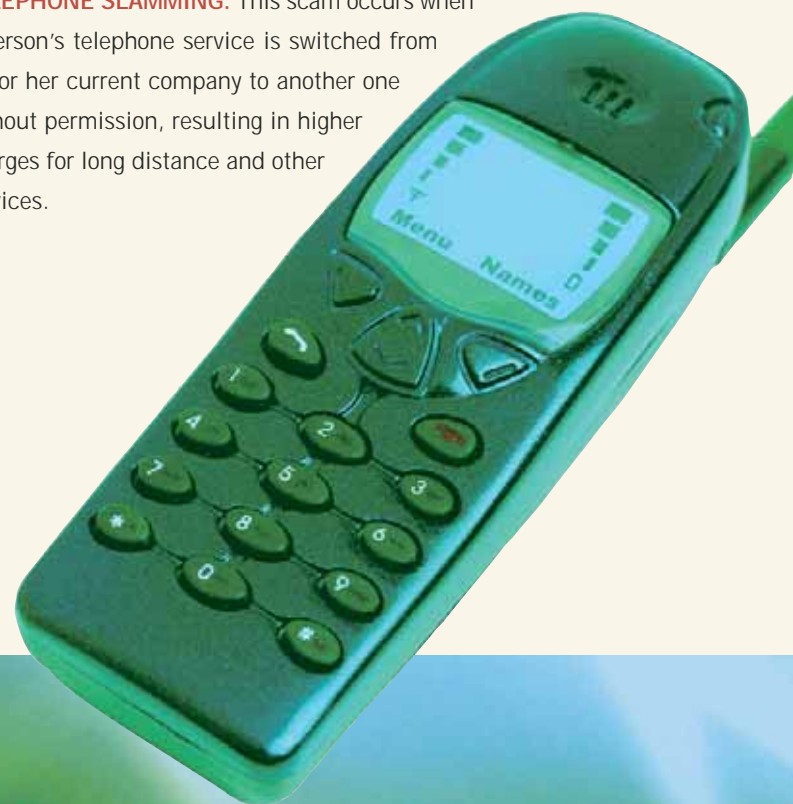
■ **CHARITY SCAMS:** Fraudulent charities often use names similar to those of well-known charities; they frequently solicit donations following a well-publicized natural or other disaster. Some charities are technically legitimate but retain a high percentage of donated funds for "administrative" costs such as salaries.

■ **BOGUS MERCHANDISE SALES:** A consumer purchases something advertised for sale on the Internet or through a telemarketing call. The customer pays for the merchandise by check, cash, or credit card but does not receive it, or receives an inferior or counterfeit product in its place. Online auction fraud sometimes involves an escrow service; the consumer pays a bogus escrow service but does not receive the merchandise.

■ **TELEPHONE CRAMMING:** This scam occurs when unauthorized charges for goods or services are put on a person's phone bill. Because phone companies now bill for legitimate services such as paging and Internet access on behalf of other companies, phone bills have become complicated, and customers may not notice the "extra" charges.

■ **TELEPHONE SLAMMING:** This scam occurs when a person's telephone service is switched from his or her current company to another one without permission, resulting in higher charges for long distance and other services.

Fraudulent charities often use names similar to those of well-known charities; they solicit donations following a natural or other disaster. Some charities are technically legitimate but retain a high percentage of donated funds for "administrative" costs such as salaries.



CRIME PREVENTION COALITION OF AMERICA

Crime prevention improves the quality of life for every citizen and every community.

EXECUTIVE COMMITTEE OFFICERS

- **Tibby Milne**, Chair, Executive Director, Utah Council for Crime Prevention
- **Bob Douglas**, Vice-chair, Executive Director, Kentucky Crime Prevention Coalition

EXECUTIVE COMMITTEE MEMBERS

- **American Society for Industrial Security**, Michael J. Stack, Executive Director
- **Boys & Girls Clubs of America**, Robbie Callaway, Senior Vice President
- **California Attorney General's Crime and Violence Prevention Center**, Paul Seave, Director
- **Corpus Christi Operation Weed and Seed**, George Hodge, Executive Director
- **Florida Attorney General's Office, Crime in the Black Community Program**, Daniel A. Gilmore, Coordinator
- **Florida Crime Prevention Association**, Ernest Long, President
- **International Association of Chiefs of Police**, Dan Rosenblatt, Executive Director
- **National Association of Blacks in Criminal Justice**, Rev. Warren H. Dolphus
- **National Criminal Justice Association**, Cabell C. Cropper, Executive Director
- **National District Attorneys Association**, Thomas J. Charron, Executive Director
- **National League of Cities**, Gwyndolen A. Clarke-Reed, Commissione
- **New York State Center for School Safety**, Felicia Watson, Marketing and Public Relations Coordinator

EX-OFFICIO

- **Hope Janke**, Counsel to the Director, Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice
- **Alfonso E. Lenhardt**, President and CEO, National Crime Prevention Council

The Crime Prevention Coalition of America (CPCA) is a nonpartisan group of national, state, federal, and community-based organizations united to encourage individual citizens and citizen groups to take action to prevent crime. Established in 1980, its members include youth development organizations, municipalities, law enforcement agencies, federal and state government representatives, state crime prevention associations, and community-based groups.

The CPCA utilizes a menu of technology tools that will enable your organization to

- Share appropriate prevention programs, presentations, and publications
- Communicate effectively with crime prevention practitioners from across the nation
- Learn more about crime prevention-related legislation and identify your representatives

For CPCA members, these resources and others are just a click away at www.ncpc.org. Please take a few minutes to review the description of membership benefits. We invite your organization to join this national movement and help prevent crime in your community.

BENEFITS OF COALITION MEMBERSHIP

All Coalition member organizations enjoy access to up-to-date information on successful crime prevention programs and innovative approaches that demonstrate the effectiveness and value of prevention. These benefits also include Internet tools to support crime prevention initiatives and improve the ability to communicate prevention messages.

State and National members: State and National members may receive a free copy of one new NCPC publication per year.

Affiliate members: Affiliate members receive discounts on new NCPC publications.

In addition, all Coalition member organizations receive the following benefits:

- *Weekly E-Bulletin*
- *Catalyst* newsletter
- Access to the Coalition members-only website containing training curricula, sample strategic plans, bylaws, membership plans and newsletters, and conference planning tools and tips
 - National and legislative tools to track crime prevention-related legislation and provide alerts and briefings
 - Reduced registration fees for the National Conference on Preventing Crime and other trainings and symposia
 - Links to Coalition member websites
 - Calendar of upcoming state and national trainings and conferences
- Training and technical assistance on organizational development, topical crime prevention, strategic planning, media relations, and resource development at little or no cost
- The opportunity to become involved in the highly successful National Citizens' Crime Prevention Campaign and benefit from its wide-reaching recognition among children as well as adults

COALITION NETWORKING

The Crime Prevention Coalition of America serves as a gathering and distribution mechanism for innovative crime, violence, and drug abuse prevention policies and programs throughout the United States. Through membership in the Coalition, organizations network with similar organizations across the country.

MOBILIZING THE NATION TO PREVENT CRIME, VIOLENCE, AND DRUG ABUSE

As part of its efforts to mobilize the nation, the Coalition collects and publishes descriptions of crime prevention programs and strategies. The Coalition would like to hear about your innovative programs and successes. Take advantage of this unique opportunity to share your work with prevention practitioners across the country. Please email your information to membership@ncpc.org or call Coalition staff at **202-466-6272**.

LEGISLATIVE AND MEDIA INFORMATION CENTER

The Legislative and Media Information Center is a password-protected section of the Coalition website. Your organization can use this service to identify key federal and state policymakers and to review the progress of legislation.

TRAINING OPPORTUNITIES

The Coalition staff arranges or provides a source of highly effective training and technical assistance at little or no cost to CPCA members. The Coalition can be a source of topical crime prevention information or a facilitator of your organization's strategic planning process. It can provide assistance in working with the media and public policy issue education and support. For more information, contact Kimberly J. Dalferes at **202-261-4173**.



NATIONAL CITIZENS' CRIME PREVENTION CAMPAIGN PSA MESSAGES TODAY

The public service advertising component of the National Citizens' Crime Prevention Campaign is one of the most visible parts of this campaign. Since 1980, McGruff the Crime Dog® and his "Take A Bite Out Of Crime®" slogan have helped adults, teens, and children learn steps they can take to ensure their own safety and to prevent crime in their communities. This year, McGruff will continue talking to citizens about personal safety and property crime, as well as new topics such as identity theft.

By the end of the third quarter of 2004, the campaign had received \$45.5 million in donated media support—well above the national average for PSA campaigns. In addition, we reached millions of viewers with important crime prevention information. For example, one 60-second public service announcement (PSA) aired on any one of the four major networks allows the campaign to reach more than two million households with our message.

McGruff marked his 25th anniversary with the release of three new radio public service announcements focusing on easy tips for neighborhood safety. In one spot, McGruff is interviewed by Joy Behar, a co-host of ABC's *The View*. In the course of their conversation, McGruff and Behar let listeners know of ways they can "Take A Bite Out Of Crime" in their homes and neighborhoods. In the other two spots, McGruff

talks about using garden shears to attack shrubs and other plants that could provide hiding places for would-be criminals. He suggests that beginning a conversation or just saying hello to your neighbor can be a starting point for community action to reduce crime. These radio spots garnered \$1 million in donated airtime in just four months! In addition, NCPC produces outdoor advertising—billboards, posters in malls and bus shelters, and transit cards with the same messaging carried in the radio spots. NCPC is entering into a partnership with the Washington Metropolitan Area Transit Authority to provide advertising and crime prevention tips. Peak times for these messages will be July and October, but crime prevention information will be provided to riders on an ongoing basis.

McGruff media messages for children address such issues as bullying and Internet safety. The latest TV PSAs advise kids who witness bullying that they can befriend the victim and help him or her get away from the bully. The ads encourage the children to visit www.mcgruff.org for more information. While on the website, children can request new, exciting trading cards that feature McGruff, Scruff®, and friends in difficult bully situations; helpful tips on the backs of the cards offer suggestions for handling each situation. NCPC is also producing new bully prevention PSAs for parents and girls in partnership with the ABC television network. This partnership is expected to yield more than \$250,000 in donated media time from ABC.

McGruff media messages for children address such issues as bullying and Internet safety. The ads encourage children to visit www.mcgruff.org for more information.

The Internet safety initiative features print ads in which McGruff provides the basic steps to protect children while they are on the Internet. An online response piece is featured in one of the ads. The old Crime Dog is in some new threads—temporarily trading in his trench coat for a black jacket and blue trousers. McGruff encourages parents to talk with their children about being safe on the Internet and reminds parents that sometimes dangerous online predators visit chat rooms and pretend to be children.

Volunteering: Do What You Like To Do is the latest installment of award-winning PSAs for the teen audience. Many teens are getting involved in volunteer activities as a way to contribute to their communities.

However, some still haven't discovered the joy and satisfaction that come from making a difference in their own backyards. This initiative shows teens how they can take an interest they already have and use it to volunteer. The idea is simple. You don't need special skills. For example, if you enjoy talking on the phone, join a teen crisis hotline. If you like sports, volunteer to coach a local kids' team.

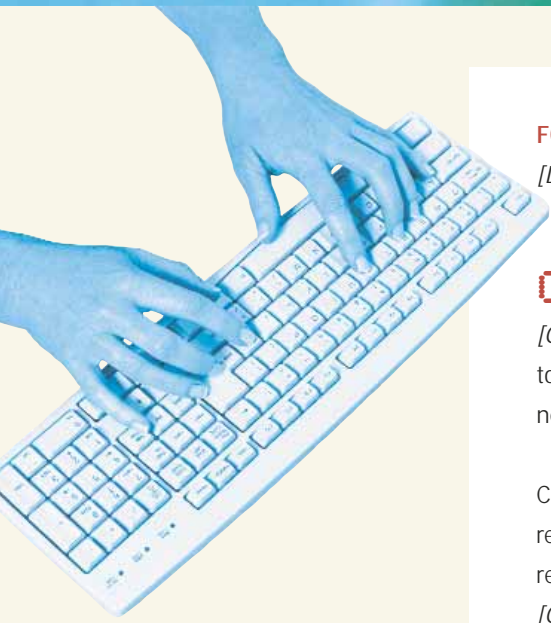
In the ads, teens are encouraged to visit www.teensvolunteer.org to search for volunteer activities in their communities and to download a free pamphlet—*Volunteering: Do What You Like To Do*. Teenagers want to make a difference in the world, and everyone benefits when teens volunteer: the teenagers gain new skills and firsthand experience, use their talents and abilities in a new way, contribute to the well-being of the community, and have fun at the same time. Individuals and communities also benefit when teenagers volunteer. Community members come to see teenagers as real assets when teens help clean up neighborhoods, tutor at-risk children, assist homebound residents, and perform other volunteer tasks.

Newspaper mat features are prewritten, ready-to-use feature articles distributed to 10,250 newspapers, 6,600 radio stations, and thousands of websites for their unlimited use. NCPC uses this as a public relations tool for the advertising messages discussed above. Survey data show that a reader is four times more likely to absorb and act on information in the media if he or she perceives that information as coming from a reliable source.

If you are interested in more information on any of the PSA initiatives or would like to help support airtime of the PSAs locally, please contact the NCPC Communications Department at 202-261-4184. Visit www.weprevent.org for the latest information on PSA campaigns and initiatives.



SAMPLE Press Release



FOR IMMEDIATE RELEASE

[Date]

FOR FURTHER INFORMATION

[Name, Phone Number]

OCTOBER MARKS CRIME PREVENTION MONTH

[Governor/Mayor/Council President] today proclaimed October as Crime Prevention Month 2006 and challenged the entire community to make crime prevention a priority. [He/she] also paid tribute to the many individuals who have taken personal responsibility for their neighborhoods and community organizations that work for the common good.

Crime Prevention Month 2006 reflects the fact that time, money, and other resources spent on prevention yield tremendous benefits in reducing crime and making communities stronger, safer, and better places to live, work, and play. We must not stop working to continue reducing crime in our country. Experience in [town or state] has proved that grassroots, collaborative action works to keep crime down. [Give examples.]

During Crime Prevention Month, government agencies, civic groups, schools, businesses, and youth organizations in [town or state] will showcase their accomplishments, reach out to educate and empower the public through educational campaigns, and explore new partnerships that build stronger communities where crime cannot survive. Events will include [list event, date, time, and place].

In 1984, the National Crime Prevention Council, the nation's focal point for preventing crime, designated October as Crime Prevention Month. Since 1980, McGruff the Crime Dog® has been around to assist communities in spreading the prevention word through trainings, mass media, conferences, publications, and media messages. The month-long celebration recognizes successful crime prevention efforts on the local, state, and national levels to generate interest and enthusiasm for prevention efforts to continue to grow even stronger and become more widespread.

Crime prevention in the age of technology is the focus of this year's Crime Prevention Month. Events throughout the year should raise public awareness of how technology crime is committed and how citizens can protect themselves from becoming victims.

A Proclamation, FOR CRIME PREVENTION MONTH 2006

An official proclamation places the power of state and local government behind crime prevention. Both as symbol and substance, the proclamation ceremony presents an excellent opportunity for a media event.

- Ask a top official (e.g., governor, mayor, city manager, council president, police chief, and sheriff) who has championed prevention as an important investment for current and future crime control to issue the proclamation.
- Schedule a press conference or photo opportunity for the last week in September to proclaim October as Crime Prevention Month. Arrange for an appearance by McGruff.
- Contact the news media and emphasize their opportunity to report on positive news about crime prevention efforts. Work with the media on ways to honor people and programs that have made outstanding contributions to community safety.
- Use this sample proclamation as a model, but adapt it to reflect state or community concerns.

Whereas, the vitality of our [city/county/state] depends on how safe we keep our homes, neighborhoods, schools, workplaces, and communities;

Whereas, crime and fear of crime destroy our trust in others and in civic institutions, threatening the community's health, prosperity, and quality of life;

Whereas, people of all ages must be made aware of what they can do to prevent themselves and their families, neighbors, and co-workers from being harmed by crime;

Whereas, people of all ages must be made aware of the dangers of technology crime and how they can protect themselves from becoming victims.

Whereas, the personal injury, financial loss, and community deterioration resulting from crime are intolerable and require investment from the whole community;

Whereas, crime prevention initiatives must include self-protection and security, but they must go beyond these to promote collaborative efforts to make neighborhoods safer for all ages and to develop positive opportunities for young people;

Whereas, adults must invest time, resources, and policy support in effective prevention and intervention strategies for youth, and teens must be engaged in driving crime from their communities;

Whereas, effective crime prevention programs excel because of partnerships among law enforcement, other government agencies, civic groups, schools, faith communities, businesses, and individuals as they help to nurture communal responsibility and instill pride;

Now, therefore, I [name of leader], [title], do hereby proclaim October 2006 as Crime Prevention Month in [name of area] and urge all citizens, government agencies, public and private institutions, and businesses to invest in the power of prevention and work together to make [city/county/state] a safer, stronger, more caring community.

NCPC RESOURCES

Here are some ways NCPC can help you.

MATERIALS

NCPC publishes high-quality educational materials on a wide range of subjects and in varied formats, including books, booklets, brochures, monographs, videos, program kits, and posters. To purchase NCPC publications, call **800-NCPC-911** or visit our secure online store at www.mcgruffstore.org. For a free catalog, call **800-NCPC-911**. For a free subscription to *Catalyst*, NCPC's newsletter, email catalyst@ncpc.org.

MCGRUFF NATIONAL LICENSING PROGRAM

If you're looking for entertaining and effective ways to reinforce crime prevention messages, our licensees offer hundreds of options. Products featuring McGruff the Crime Dog and his nephew Scruff run the gamut from pencils, stickers, lapel pins, dolls, books, and apparel to educational videos, costumes, and fully animated robots. For more information, contact our Licensing Department at **202-261-4126**.

PUBLIC SERVICE ANNOUNCEMENTS (PSAs)

We produce PSAs featuring McGruff the Crime Dog, his nephew Scruff, and the "Take A Bite Out Of Crime" slogan to promote crime prevention for television, radio, print (newspapers and magazines), out-of-home (billboards and posters), and the Web. State crime prevention programs and associations can localize these ads with their own contact information. For more information, contact the Communications Department at **202-261-4138**.

TRAINING OPPORTUNITIES

NCPC offers a variety of interactive training programs that range in scope from comprehensive crime prevention planning for whole jurisdictions to prevention strategies for teens, children, and families. For more information, visit www.ncpc.org/training/.

The National Training Center for Crime Prevention and Community Leadership is designed to meet the needs of leaders representing small, medium, and large communities. The partnership between NCPC and Fox Valley Technical College in Appleton, WI, provides training on the best in intervention and prevention practices. For more information, visit www.ncpc.org/training.

THE NATIONAL CONFERENCE

The National Conference on Preventing Crime features workshops, plenary sessions, exhibitors, the McGruff store, and plenty of inspiration to maintain the momentum for crime prevention. It attracts diverse prevention partners from across the country to learn about crime prevention trends, issues, programs, and strategies. For more information on the conference, call **202-261-4165** or visit www.ncpc.org/pop.

THE MCGRUFF STRATEGIES CENTER

This searchable online database features over 500 crime prevention programs and practices from the field. This online forum and resource center provides a platform for communities to share their crime prevention strategies, practices, and programs. To learn more, visit www.ncpc.org/strategies.

WEBSITES

NCPC's websites make a variety of helpful materials immediately available to many audiences, offering practical tips on home and family safety, the protection of children and youth, and crime prevention actions for both individuals and neighborhoods. Law enforcement, community activists, and others can download these tips for local use.

www.ncpc.org is NCPC's primary online resource center. This website offers something for everyone. Whether you are searching for information on our latest conference, purchasing a licensed product, downloading a new publication, or learning more about McGruff, this website has it all.

www.mcgruff.org, our popular children's website, offers information, activities, and links for children, families, and other adults interested in protecting children. Children can write letters to McGruff and get immediate advice on topics such as dealing with bullies, staying safe when home alone, and using the Internet responsibly. They can navigate through mazes, read comic books, and learn safety tips.

www.weprevent.org provides viewers of the National Citizens' Crime Prevention Campaign's public service advertising with follow-up information. Visitors to the site can see and listen to current PSAs.

www.nationaltcc.org offers information to teens and program managers involved in the Teens, Crime, and the Community program.

NATIONAL MCGRUFF LICENSING PROGRAM

■ **AIMS Multimedia**: Live McGruff educational videos for children on crime prevention topics, including bullying, drug awareness, personal safety, and child abuse prevention. Numerous titles available in Spanish. **800-367-2467** or **818-773-4300**; www.aims-multimedia.com

■ **Boerner-Arfmann Marketing, Inc.**: Co-branded with a sponsor's name and contact information—McGruff Safe Kids Total Identification System kit (a fingerprinting and educational kit available in print or through a computerized system), also available in Spanish; Internet safety kit; and senior citizen safety kit. **800-288-3344** or **952-473-7322**; www.mcgruff-safe-kids.com or www.totalidsystem.mcgruff-safe-kids.com

■ **BoomerangIT, Inc.**: Personal property and bicycle identification and registration kits (National Bike Registry); McGruff ID Armor kit protects sensitive personal information. **800-848-BIKE** or **510-614-2400**; www.boomerangit.com or www.nationalbikeregistry.com

■ **Brodin Studios, Inc.**: Unique bronze sculptures, recognition awards, bas-reliefs, paperweights, medallions, and plaques featuring law enforcement and McGruff. **800-274-5194** or **320-593-1495**; www.brodinstudios.com

■ **Coastal Concepts**: New retro T-shirt apparel sold through retail stores. **760-598-2501**; www.coastalconcepts.com

■ **Create-A-Book**: McGruff and Me personalized book; Scruff sticker book, Scruff Summer Camp Adventure. **800-732-3009** or **850-934-1599**; www.create-a-book.com

■ **Data Management, Inc.**: Visitor Pass is a visitor sign-in system that enables companies, schools, and other organizations to raise the level of security and privacy in their facilities. **800-243-1969**; www.datamanage.com

■ **Ellison Educational Equipment, Inc.**: McGruff and Scruff and "Take A Bite Out Of Crime" die cuts and paper shapes for schools and other facilities. **800-253-2238** or **949-488-0344, ext. 164**; www.ellison.com

■ **Geiger Cribbins**: McGruff and Scruff beanbag dolls and key chains; activity/coloring books; T-shirts; golf tournament products; and McGruff flags, pens, pencils, and coffee mugs. **877-441-5650, ext. 262** or **206-441-5650, ext. 262**; www.McGruffgear.com or randyg@cribbins.com

■ **Grafeeties/WRS Group**: Grafeeties (bumper stickers for sneakers) and temporary tattoos. **800-299-3366, ext. 250** or **254-776-6461, ext. 167**; www.grafeeties.com

■ **KidSational, Inc.**: Cutting-edge thematic children's educational products and programming, Guardian Safety Game. **912-352-8100**; www.kidsationalinc.com or www.safetygame.com

■ **MagnetStreet**: McGruff magnets and other magnetic items including rulers, calendars, notepads, and schedules. **800-778-8633** or **763-786-9400**; www.magnetstreet.com

■ **McGruff Specialty Products Office (agent of NCPC)**: McGruff and Scruff plush and beanbag dolls, Halloween and litter bags, coloring and activity books, and crime prevention brochures with personalized imprints; reflective apparel, accessories, etc. **888-776-7763** or **518-842-4388**; www.mcgruffspo.com

■ **Northern Products, Inc.**: McGruff glow sticks, lightstick bracelets and hoop earrings, and party favor lightstick "six-packs." **978-840-3383**; www.northernlightsticks.com

■ **Robotronics, Inc.**: McGruff and Scruff costumes, animated costume, McGruff puppet program, stand-up McGruff robot, mobile McGruff driving a law enforcement vehicle. Coming soon: remote-control animated Scruff. **800-762-6876** or **801-489-4466**; www.robotronics.com

■ **RODOG Productions, Inc.**: Cassette tape and CD (McGruff and Scruff and the Crime Dogs) with crime prevention songs addressing bicycle safety, conflict management, family safety, and Internet safety. **800-915-4653** or **850-434-0500**; www.crimedog.com

■ **Rose City Label**: A variety of McGruff custom-printed stickers and labels. **800-547-9920** or **503-777-4711**; www.rclabel.com

■ **Signs and Shapes International, Inc.**: McGruff inflatable "walk-around" costume. **402-331-3181**; www.signsandshapes.com

■ **Sparta Pewter**: Pewter pins, dog chains, key chains, McGruff thermal mugs, and zipper pulls. **888-254-2002** or **514-363-5674**; www.spartapewter.com

■ **Stoffel Seals Corporation**: McGruff "Crime Fighter" badges, shields, key chains, lapel pins, and patriotic McGruff pins; badge design available for police, sheriffs, and troopers. **800-344-4772** or **845-353-3800**; www.stoffel.com

■ **Symbol Arts, Inc.**: McGruff and flag patriotic lapel pins and key chains; coins for good-deed rewards. Minimum orders of 300 pieces. **801-475-6000**; www.symbolarts.com

■ **Tee's Plus**: Sports apparel and accessories featuring McGruff and Scruff including T-shirts, golf shirts, baseball caps, jean jackets, and nylon jackets. **800-782-8337**; www.teesplus.com

You can always find a complete, updated list of licensees on www.ncpc.org.



Order your Halloween bags in early spring or summer!

RESOURCES ON THE WEB

Be sure to visit www.ncpc.org—your crime prevention toolbox—for tips, checklists, information, strategies, and more. The websites listed here can help you locate additional information. Although we have selected these links with care, NCPC is not responsible for the material posted.

IDENTITY THEFT

Identity Theft Resource Center	www.idtheftcenter.org/index.shtml
Justice Department Identity Theft	www.usdoj.gov/criminal/fraud/idtheft.html
National Criminal Justice Reference Service	www.ncjrs.org/spotlight/identity_theft/summary.html
Office for Victims of Crime	www.ojp.usdoj.gov/ovc/
Privacy Rights Clearinghouse	www.privacyrights.org

SENIORS AND TELEMARKETING FRAUD

AARP	www.aarp.org
Administration on Aging	www.aoa.gov
National Consumers League	www.natlconsumersleague.org/
National Fraud Information Center	www.fraud.org/elderfraud/
SeniorCitizens.com	www.seniorcitizens.com
SeniorJournal.com	www.seniorjournal.com
Telemarketing Toolbox	www.fraud.org/toolbox/members.htm
TodaysSeniorsNetwork.com	www.todayseniornetwork.com

TO GET OFF MARKETING LISTS

The Direct Marketing Association	www.dmaconsumers.org
The National Do Not Call Registry	www.donotcall.gov/

STALKING AND ONLINE HARASSMENT

Crime Library	www.crimelibrary.com/criminology/cyberstalking/
CyberAngels	www.cyberangels.org
GetNetWise	www.getnetwise.org
National Center for Victims of Crime	www.ncvc.org
Office for Victims of Crime	www.ojp.usdoj.gov/ovc/help/stalk.htm
Report on Cyberstalking	www.usdoj.gov/criminal/cybercrime/cyberstalking.htm
WHOA (Working to Halt Online Abuse)	www.haltabuse.org
Wired Safety	www.wiredpatrol.org/

TELECOMMUNICATIONS FRAUD

Federal Communications Commission	www.fcc.gov
Federal Trade Commission	www.ftc.gov
National Fraud Information Center	www.fraud.org

ILLEGAL ONLINE PHARMACIES

National Association of Boards of Pharmacy	www.nabp.net
National Drug Intelligence Center	www.usdoj.gov/ndic/pubs2/2161/index.htm
U.S. Drug Enforcement Administration	www.dea.gov
U.S. Food and Drug Administration	www.fda.gov

COMPUTER SECURITY

Better Business Bureau	www.bbb.org
Business Software Alliance	www.bsa.org
CyberAngels	www.cyberangels.org
GetNetWise	www.getnetwise.org
National Cyber Security Alliance	www.staysafeonline.info
Symantec	http://securityresponse.symantec.com/
U.S. Computer Emergency Readiness Team	www.us-cert.gov

INTERNET SAFETY AND ETHICS

Business Software Alliance	www.playitcybersafe.org
Cyber Smart Company	www.cybersmart.org
CyberAngels	www.cyberangels.org
CyberCitizenship.org	www.cybercitizenship.org
Cyberkids	www.cyberkids.com
Direct Marketing Organization	www.cybersavvy.org/
GetNetWise	www.getnetwise.org
Internet Keep Safe Coalition	www.ikeepSAFE.org
i-SAFE	www.isafe.org
McGruff.org's Milstein Child Safety Center	www.mcgruff.org
Netsmartz Workshop	www.netsmartz.org
Safe Kids.com	www.safekids.com
SafeTeens.com	www.safeteens.com
U.S. Department of Justice Kids' Page	www.usdoj.gov/kidspage
Web Wise Kids	www.webwisekids.com
Wired Safety	www.wiredpatrol.org/

INTERNET FRAUD

Better Business Bureau	www.bbb.org
Federal Trade Commission	www.ftc.gov
Internet Crime Complaint Center	www.ic3.gov
National Fraud Information Center	www.fraud.org
U.S. Department of Justice	www.cybercrime.gov

SCHOOL SAFETY

ADT Security Services, Inc.	www.adt.org
Afterschool Alliance	www.afterschoolalliance.org
American School Counselor Association	www.schoolcounselor.org
Be Safe and Sound Campaign	www.ncpc.org/besafe
Keep Schools Safe	www.keeperschoolssafe.org
National Association of Elementary School Principals	www.naesp.org
National Association of School Psychologists	www.naspcenter.org
National School Safety Center	www.nssc1.org
Office of Safe and Drug-Free Schools	www.ed.gov/offices/OESE/SDFS/

COMMUNITY PREPAREDNESS

American Red Cross	www.redcross.org
Centers for Disease Control and Prevention	www.cdc.gov
Federal Emergency Management Agency	www.fema.gov
National Sheriffs' Association	www.usaonwatch.org
Operation Safe America	www.safeamerica.org
United for a Stronger America Campaign	www.weprevent.org/usa
U.S. Citizen Corps	www.citizencorps.gov
U.S. Department of Homeland Security	www.ready.gov
USA Freedom Corps	www.usafreedomcorps.gov
The White House	www.whitehouse.gov
Youth Crime Watch of America	www.ycwa.org

FOR LAW ENFORCEMENT

Community Policing Consortium	www.communitypolicing.org
COPS—Community Oriented Policing Services	www.cops.usdoj.gov/
G.R.E.A.T.	www.atf.gov/great/
International Association of Chiefs of Police	www.theiacp.org
Justice Technology Information Network	www.nlectc.org
National Association of School Resource Officers	www.nasro.org
National Sheriffs' Association	www.sheriffs.org
Police Executive Research Forum	www.policeforum.org

GOVERNMENT

U.S. Department of Justice	www.usdoj.gov
Office of Justice Programs	www.ojp.usdoj.gov
Bureau of Justice Assistance	www.ojp.usdoj.gov/bja/
Bureau of Justice Statistics	www.ojp.usdoj.gov/bjs/
National Institute of Justice	www.ojp.usdoj.gov/nij
Office for Victims of Crime	www.ojp.usdoj.gov/ovc/
Office of Juvenile Justice and Delinquency Prevention	www.ojjdp.ncjrs.org

SUPPORT AND INFORMATION

American Youth Policy Forum	www.aypf.org
America's Promise	www.americaspromise.org
Child Welfare League of America	www.cwla.org
Crime Prevention Coalition of America	www.ncpc.org
Drug Strategies	www.drugstrategies.org
Drug-Free Resource Net	www.drugfreeamerica.org
Join Together Online	www.jointogether.org
Keep Schools Safe	www.keeperschoolssafe.org
National Association of Town Watch	www.nationaltownwatch.org
National Citizens' Crime Prevention Campaign	www.weprevent.org
National Collaboration for Youth	www.nydic.org/nydic/
National Crime Prevention Centre (Canada)	www.crime-prevention.org
Office of National Drug Control Policy	www.whitehousedrugpolicy.gov
Public Education Network	www.publiceducation.org
Stand for Children	www.stand.org
Street Law, Inc.	www.streetlaw.org
Violence Policy Center	www.vpc.org

RESEARCH/STATISTICS

Bureau of Justice Statistics	www.ojp.usdoj.gov/bjs
FBI Uniform Crime Reports	www.fbi.gov/ucr/ucr.htm
National Center for Health Statistics	www.cdc.gov/nchs/
National Center for Juvenile Justice	www.ncjj.org
National Clearinghouse for Alcohol and Drug Information	www.health.org
National Clearinghouse on Child Abuse and Neglect Information	http://nccanch.acf.hhs.gov/index.cfm
National Consortium on Violence Research	www.ncovr.org
National Criminal Justice Reference Service	www.ncjrs.org
Search Institute	www.search-institute.org
Sourcebook of Criminal Justice Statistics	www.albany.edu/sourcebook/



REPRODUCIBLE BROCHURES AND HANDOUTS

To help you celebrate Crime Prevention Month, this calendar contains a selection of camera-ready materials designed to be printed, photocopied, or offset. Most have space for sponsors, local phone numbers, and addresses.

Although these materials are copyrighted to protect their integrity, you may produce as many copies as you like for free distribution as long as you do not change the text or delete NCPC's credit line without written approval from NCPC. Some printers will need to see written proof that you have permission to print or copy these materials before they will proceed with the job; this page serves as that permission. You may add your local group's name, address, phone number, and website where space is provided.

If you wish to change the text or if you wish to use McGruff or Scruff in locally produced materials or settings, contact the Trademark Control and Quality Review Committee at NCPC, 1000 Connecticut Avenue, NW, Thirteenth Floor, Washington, DC 20036-5325; 202-466-6272. Call the NCPC Fulfillment Center at 800-NCPC-911 for a free copy of *Guidelines for McGruff® and Related Marks*.



Here are some ways to use these brochures:

- **Hand out brochures** at McGruff's anniversary celebrations, civic meetings, and school assemblies. Ask libraries, recreation centers, medical offices, mall kiosks, and local businesses to display and distribute materials. Ask social service agencies and doctors' offices to display brochures in their waiting areas. Enlist members of your Neighborhood Watch groups to pass them along to other residents.
- **Organize a Crime Prevention Month parade** in October and have McGruff help distribute materials to the crowd. Set up a crime prevention booth at a local mall. Hold a crime prevention fair during October.
- **Look for a match between an issue and an organization.** Youth centers and clubs, school guidance offices, and health clinics would be excellent places to leave the youth-related brochures in this kit.
- **Link your crime prevention website** to NCPC's website for downloadable brochures.

Credit Cards

If you shop online or over the phone, you may pay by credit card. Because you cannot use the physical card, you will probably give your credit card number, including the expiration date, over the phone or Internet. If these numbers fall into the wrong hands, you may find unauthorized charges on your next credit card statement.

- **Do business only with companies you know;** do not give out your credit card number to make a purchase or reservation unless you initiated the transaction.
- **Shop only at secure websites** that use encryption software to transfer data from your computer to the merchant and that have strong privacy and security policies.
- **Do not respond to emails** asking you to "update" your credit card information even if they appear to be from the company that issued you the credit card. Call the company directly to verify what information is needed.
- **If you received preapproved credit card offers** in the mail, do not throw them in the trash without shredding them first.
- **If you are expecting new credit cards in the mail** and they do not arrive, or you do not receive your bills at the expected time, call the credit card issuer immediately.
- **Check your credit card bills carefully** for several months after purchasing on the Internet. If you find purchases you did not make, immediately contact the credit card company and file a dispute claim.
- **Get a copy of your credit report once a year** and review it for any unexpected activity.

Reporting a Problem

If there are unauthorized charges on your credit card statement or withdrawals from your bank account, notify the police and the financial institution immediately. If you are a victim of identity theft, file a police report; file an online complaint with the Federal Trade Commission at www.consumer.gov/idtheft/; notify the three major credit card bureaus: Equifax (www.equifax.com), Experian (www.experian.com), and Trans Union (www.transunion.com); and close your account.



Crime Prevention Tips From

NATIONAL CRIME PREVENTION COUNCIL

1000 Connecticut Avenue, NW
Thirteenth Floor
Washington, DC 20036-5325
202-466-6272
www.ncpc.org

and



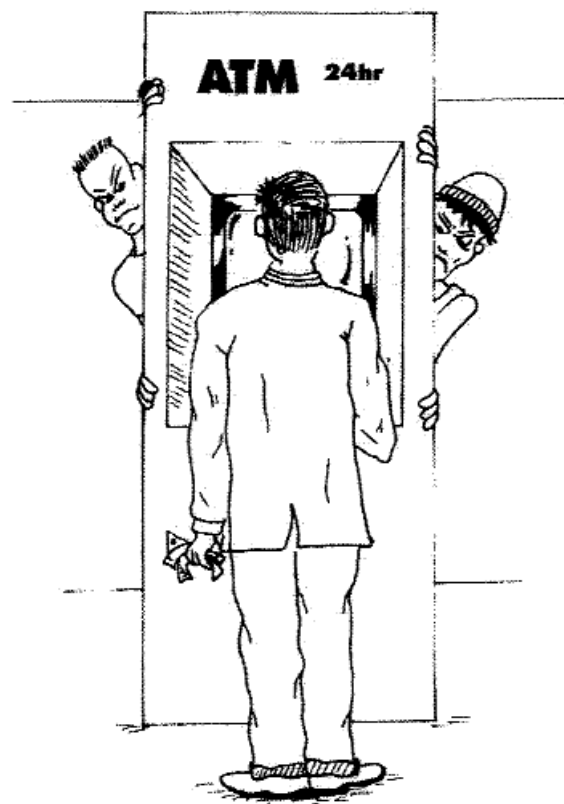
The National Citizens' Crime Prevention Campaign, sponsored by the Crime Prevention Coalition of America, is substantially funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.

tyco Fire & Security



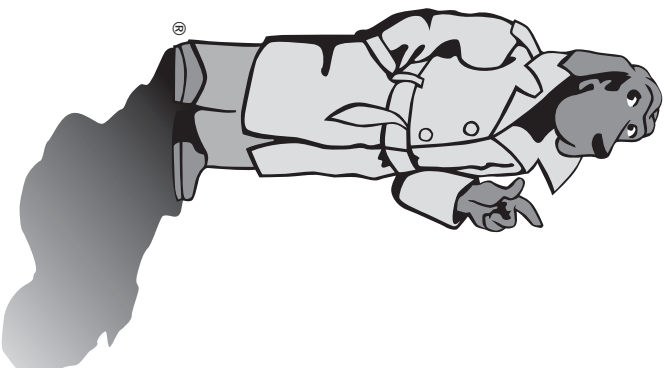
Production made possible by a grant from ADT Security Services, Inc., a unit of Tyco Fire & Security Services.

Protecting Your Private Information



NATIONAL CRIME PREVENTION COUNCIL

Ten Tips To Secure Your Personal Computer



1. **Use “anti-virus software” and keep it up-to-date.** Anti-virus software is designed to protect your computer against known viruses. But with new viruses emerging daily, anti-virus programs need regular updates. Check with the web site of your anti-virus software company to see some sample descriptions of viruses and to get regular updates for your software.
2. **Don't open emails or attachments from unknown sources.** Be suspicious of any unexpected email attachments even if they appear to be from someone you know. Should you receive a suspicious email, the best thing to do is to delete the entire message, including any attachment.
3. **Protect your computer from Internet intruders—use “firewalls.”** Firewalls create a protective wall between your computer and the outside world. They come in two forms, software firewalls that run on your personal computer and hardware firewalls that protect a number of computers at the same time. Firewalls also ensure that unauthorized persons can't gain access to your computer while you're connected to the Internet.
4. **Regularly download security updates and “patches” for operating systems and other software.** Most major software companies today release updates and patches to close newly discovered vulnerabilities in their software. Check your software vendors' web sites regularly for new security patches or use the automated patching features that some companies offer.
5. **Use hard-to-guess passwords.** Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long. Don't share your password, and don't use the same password in more than one place.
6. **Back up your computer data on disks or CDs regularly.** Back up small amounts of data on floppy disks and larger amounts on CDs. If you have access to a network, save copies of your data on another computer in the network.
7. **Don't share access to your computers with strangers.** Learn about file sharing risks. Your computer operating system may allow other computers on a network, including the Internet, to access the hard-drive of your computer in order to “share files.” This ability to share files can be used to infect your computer or look at the files on your computer. Check your operating system and your other program help files to learn how to disable file sharing.
8. **Disconnect your computer from the Internet when not in use.** Disconnecting from the Internet when you're not online lessens the chance that someone will be able to access your computer. And if you haven't kept your anti-virus software up-to-date, or don't have a firewall in place, someone could infect your computer or use it to harm someone else on the Internet.
9. **Check your security on a regular basis.** You should evaluate your computer security at least twice a year—do it when you change the clocks for daylight savings! Make sure you have the security level appropriate for you.
10. **Make sure your family members and/or your employees know what to do if your computer becomes infected.** People should know how to update virus protection software, how to download security patches from software vendors, and how to create a proper password.

These tips were adapted from the “Top Ten Cyber Security Tips” on the National Cyber Security Alliance website, www.staysafeonline.info. The National Security Alliance is a public-private partnership focused on promoting cyber security and safe behavior online.

Report hacking incidents to the FBI at www.ic3.gov.



NATIONAL CRIME
PREVENTION COUNCIL

National Crime Prevention Council
1000 Connecticut Avenue, NW • 13th Floor • Washington, DC 20036 • www.ncpc.org

Email, the Internet, automated teller machines (ATMs), online banking, cell phones, long-distance carriers, and credit cards make our lives more efficient. However, as our lives become more integrated with technology, keeping our private information confidential becomes more difficult. Electronic transactions can leave you vulnerable to identity theft and other types of fraud. Following a few simple tips can help you keep your private information safe.

Passwords are often required to access information from financial, medical, and other institutions. Hackers have sophisticated tools for cracking passwords. Here are some tips for creating and protecting your passwords.

- **Select at least eight characters**, including a combination of letters, numbers, and symbols that you can remember but that others won't easily guess.
- **Do not use your mother's maiden name**, spouse's name, last four digits of your Social Security number, pet's or children's names, or date of birth.
- **Do not use a word** that can be found in the dictionary in any language.

- **Create a new password** for every website or login that requests one. If that is impractical, create a few hard-to-guess passwords and use those at sites you want to keep most secure. Create easier-to-remember passwords to use at less important sites.
- **Change your passwords regularly**—at least once a month.
- **Memorize your passwords**, if you must write them down, don't carry them in your wallet or leave them in an unprotected place, including a computer file.

- **If you have the option of letting your computer remember a password for you**, don't do it.
- **Do not share your passwords** with family members, friends, or colleagues.
- **If you are logging into an ATM or other computer**, make sure no one is looking over your shoulder as you enter your password.

The personal identification number (PIN) is one method used by banks and phone companies to protect your account from unauthorized access. A PIN is a confidential code issued to the cardholder to permit access to that account. You can protect your PIN number by following these tips:

- **Memorize your PIN number** and do not give it to anyone, including family members or bank employees.
- **Never write your PIN** on ATM or long-distance calling cards; do not carry your PIN number in your purse or wallet.
- **When using an ATM machine or public telephone**, position yourself in front of the ATM keyboard or phone to prevent anyone from observing your PIN as you enter it.
- **Do not leave your receipt behind** when you use an ATM machine; criminals can use them to get your account number.

- **If a bank or other institution assigns you a PIN number** that is the last four digits of your Social Security number, have it changed to a new number.

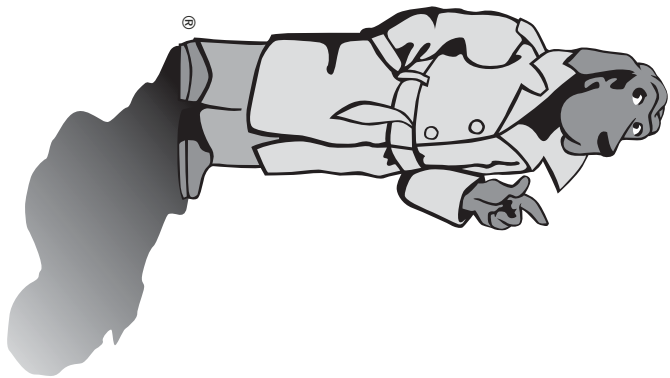
Some businesses and government agencies believe that using your Social Security number (SSN) is the most accurate way to store and retrieve information. But your Social Security number is also the prime target of criminals interested in committing identity theft and other crimes. Therefore, it is essential that you protect your SSN.

- **Release your SSN only when it is absolutely necessary.** Employers need your SSN to report your earnings to the IRS, but law enforcement does not need it to issue you a parking permit.
- **Do not carry your Social Security card** in your wallet or purse unless you need it for a specific situation, such as the first day of a new job.
- **Do not print your SSN** on checks or business cards.
- **If possible**, do not put your SSN on job applications.
- **If asked to provide your SSN online**, look for the closed padlock symbol on the bottom of the page, and read the company's privacy policy on how it safeguards your personal information.
- **Do not respond to unsolicited electronic mail messages** in which your SSN and other personal information are requested. No reputable company or government agency sends unsolicited email messages to request sensitive personal data.
- **If a private business requests your SSN**, suggest alternatives like your driver's license number (unless your driver's license number is your SSN).
- **If your state's Department of Motor Vehicles** uses the SSN as the driver's license number, ask for an alternate number.

Social Security Numbers

Working Safely at Home

Increasingly, businesses are allowing their employees to telecommute, and entrepreneurs are running businesses from their homes. Offices are standard in many homes today and are equipped with the latest in computers, scanners, printers, faxes, and other expensive equipment. Remember, it is as important to secure your equipment from burglars when you're working from home as it is to secure your computers from hackers.



It is as important to secure your equipment from burglars when you're working from home as it is to secure your computers from hackers.

- **Install solid doors and good deadbolt locks** on all exterior doors—and use them.
- **Hang window treatments** that obstruct the view of your office. You don't want to advertise what equipment you have.
- **Consider installing motion-sensored lighting** that will come on if someone is walking around your yard.
- **Keep bushes and trees trimmed** so that you can see into your yard and neighbors can see your house.
- **Install a wide-angle viewer** in the door of your home office if it is detached from the main house.
- **Look into a home alarm system.** A basic system can be purchased for less than \$100 plus a monthly monitoring fee.
- **When meeting a client for the first time,** arrange to meet in a public place, such as a coffee shop or library—not your home.
- **Let someone know** when and with whom you have appointments.
- **Review your insurance policy**—almost all policies require an extra rider to cover a home office. In the event something does happen, you want to be covered.
- **Mark your equipment with identification numbers,** and keep an updated inventory list (with photos, if possible) in a home safe or a bank safe deposit box.
- **Use the same caution with deliveries** as businesses do. Anyone making a delivery to your home office should be properly identified before you open the door.
- **Use a password-protection system** on your computer with passwords that combine numbers and upper and lowercase letters.
- **Install virus protection software** on all your computers, and scan your computer systems for viruses on a regular basis.
- **Equip your computers with firewalls,** which will protect a computer network by shutting out unauthorized people or allowing them only into certain areas.
- **Download and install security patches** from your software vendor's website on a regular basis.
- **Back up your computer data** on CDs or floppy disks on a regular basis, and store these in another location.



NATIONAL CRIME PREVENTION COUNCIL

National Crime Prevention Council
1000 Connecticut Avenue, NW • 13th Floor • Washington, DC 20036 • www.ncpc.org

Online Auction Fraud

Reporting Online Auction Fraud

- **File a complaint** with the online auction company.
- **Notify** your local and state law enforcement officials.
- **Notify** law enforcement officials in the perpetrator's town and state.
- **File a complaint** with the Better Business Bureau in the seller's area (www.bbb.org).
- **Fill out the online complaint form** at www.fraud.org, or call the Fraud Hotline at **800-876-7060**, 9 a.m. to 5 p.m., Eastern Standard Time, Monday through Friday.
- **File a complaint** with the Federal Trade Commission (FTC) Bureau of Consumer Protection, www.consumer.gov/sentinel/.
- **File a complaint** with the Internet Fraud Complaint Center (IFCC), a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI), www1.ifccfbi.gov/index.asp.

For More Information

National Consumers League: www.nclnet.org
 National Fraud Information: www.fraud.org
 Federal Trade Commission: www.ftc.gov
 Consumer Sentinel: www.consumer.gov/sentinel/
 National White Collar Crime Center: www.nw3c.org
 United States Department of Justice:
www.internetfraud.usdoj.gov/



Crime Prevention Tips From

NATIONAL CRIME PREVENTION COUNCIL
 1000 Connecticut Avenue, NW
 Thirteenth Floor
 Washington, DC 20036-5325
 202-466-6272
www.ncpc.org

and



The National Citizens' Crime Prevention Campaign, sponsored by the Crime Prevention Coalition of America, is substantially funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.



Production made possible by a grant from ADT Security Services, Inc., a unit of Tyco Fire & Security Services.



NATIONAL CRIME PREVENTION COUNCIL

Both consumers and merchants can be victims of online auction fraud. Here are some ways that fraud occurs during or after an online auction.

Failure to deliver goods. The seller places an item up for bidding that does not exist or fails to deliver merchandise after the buyer purchases it.

Nonpayment for delivered goods. The seller sends the merchandise to the highest bidder in good faith but fails to receive payment.

Misrepresentation of merchandise. The seller gives false information about the item, or attempts to deceive the buyer concerning its true value.

How Auction Fraud Occurs

In an online format that resembles a real-life auction, people offer cameras, computers, artwork, jewelry, and dozens of other products, usually in a set time frame for bidding to take place. Prospective buyers examine the descriptions and photos and decide whether (and for how much) to place bids. As in a live auction, the highest bidder wins. Upon winning, the buyer sends payment for the auction item, possibly to an online escrow service that holds payment until the buyer receives the goods.

How Online Auctions Work

Millions of people take part in Internet auctions every day, bidding on items from around the world. Buyers and sellers alike benefit from the great opportunities that online auctions provide, but these auctions also give criminals the opportunity to perpetrate fraud. According to the National Consumers League, online auction fraud is the number one fraud committed over the Internet.

- **Understand how an online auction works** before you bid on merchandise. What are your obligations as a buyer? What are the seller's obligations? Does the auction site provide insurance that covers buyers up to a certain amount? How would the auction site handle a dispute between buyer and seller?
- **Don't judge by initial appearances.** It can be hard to validate a seller's claims about the value of an item, and descriptions or photographs on websites can be misleading. Know as much as you can about the item you wish to purchase.

Preventing Online Auction Fraud

- **Consider using an escrow service** or alternate payment service if purchases on your credit card are not disputable or the goods are not covered by insurance. Make sure the escrow service is licensed and bonded; fraudulent escrow services might pocket your money and disappear.
- **Protect yourself from identity theft** by not giving out such personal information as your Social Security number, driver's license number, or bank account numbers, as sellers do not need this information.
- **Do not send your credit card numbers** electronically unless you know for sure that the website is secure and encrypted.
- **Try to pay the seller directly** with a credit card, so you can dispute the charges if the merchandise does not arrive or was misrepresented. If possible, avoid paying by check or money order.
- **Investigate the seller as much as possible.** Be wary of sellers who provide only an email or post office box address. Check the seller's feedback rating if available on the auction site. Call the seller to see if the phone number is working, or send an email to see if the email address is active. If the seller is a business, check it out with the Better Business Bureau.
- **Contact the seller** before bidding to find out what type of payment is required, when you can expect delivery, what the return policy is, if the merchandise is covered by warranty, and if shipping and delivery are included in the price.
- **Try to pay the seller directly** with a credit card, so you can dispute the charges if the merchandise does not arrive or was misrepresented. If possible, avoid paying by check or money order.

- **Bogus escrow services.** After the auction, the bogus escrow service receives payment from the buyer but pockets the money and disappears rather than transmitting it to the seller.
- **Black market goods.** The seller offers goods that are stolen and/or copied (e.g., software, music CDs, and videos). Often they arrive with no warranty, instructions, or box.
- **Credit card fraud.** The seller uses the buyer's name and credit card number for fraudulent purposes, or the buyer uses a fraudulent credit card when purchasing an item.
- **Fake bidding.** The seller bids on his or her own item, or has someone else bid, in an attempt to drive up the price.
- **Hidden charges.** Instead of a flat rate for postage and handling, the seller adds separate charges for postage, handling, and the shipping container, causing the buyer to pay more than anticipated.

Hidden charges. Instead of a flat rate for postage and handling, the seller adds separate charges for postage, handling, and the shipping container, causing the buyer to pay more than anticipated.

Fake bidding. The seller bids on his or her own item, or has someone else bid, in an attempt to drive up the price.

Credit card fraud. The seller uses the buyer's name and credit card number for fraudulent purposes, or the buyer uses a fraudulent credit card when purchasing an item.

Black market goods. The seller offers goods that are stolen and/or copied (e.g., software, music CDs, and videos). Often they arrive with no warranty, instructions, or box.

Bogus escrow services. After the auction, the bogus escrow service receives payment from the buyer but pockets the money and disappears rather than transmitting it to the seller.

Understand how an online auction works before you bid on merchandise. What are your obligations as a buyer? What are the seller's obligations? Does the auction site provide insurance that covers buyers up to a certain amount? How would the auction site handle a dispute between buyer and seller?

Don't judge by initial appearances. It can be hard to validate a seller's claims about the value of an item, and descriptions or photographs on websites can be misleading. Know as much as you can about the item you wish to purchase.

Do not send your credit card numbers electronically unless you know for sure that the website is secure and encrypted.

Protect yourself from identity theft by not giving out such personal information as your Social Security number, driver's license number, or bank account numbers, as sellers do not need this information.

Consider using an escrow service or alternate payment service if purchases on your credit card are not disputable or the goods are not covered by insurance. Make sure the escrow service is licensed and bonded; fraudulent escrow services might pocket your money and disappear.

Try to pay the seller directly with a credit card, so you can dispute the charges if the merchandise does not arrive or was misrepresented. If possible, avoid paying by check or money order.

Investigate the seller as much as possible. Be wary of sellers who provide only an email or post office box address. Check the seller's feedback rating if available on the auction site. Call the seller to see if the phone number is working, or send an email to see if the email address is active. If the seller is a business, check it out with the Better Business Bureau.

Contact the seller before bidding to find out what type of payment is required, when you can expect delivery, what the return policy is, if the merchandise is covered by warranty, and if shipping and delivery are included in the price.

Try to pay the seller directly with a credit card, so you can dispute the charges if the merchandise does not arrive or was misrepresented. If possible, avoid paying by check or money order.

Do not send your credit card numbers electronically unless you know for sure that the website is secure and encrypted.

Protect yourself from identity theft by not giving out such personal information as your Social Security number, driver's license number, or bank account numbers, as sellers do not need this information.

Consider using an escrow service or alternate payment service if purchases on your credit card are not disputable or the goods are not covered by insurance. Make sure the escrow service is licensed and bonded; fraudulent escrow services might pocket your money and disappear.

Try to pay the seller directly with a credit card, so you can dispute the charges if the merchandise does not arrive or was misrepresented. If possible, avoid paying by check or money order.

Investigate the seller as much as possible. Be wary of sellers who provide only an email or post office box address. Check the seller's feedback rating if available on the auction site. Call the seller to see if the phone number is working, or send an email to see if the email address is active. If the seller is a business, check it out with the Better Business Bureau.

Downloading From the Internet

The Internet has changed the way children do schoolwork. But they need to realize that information they find on the Internet is not all free. Be sure they understand the following:

- **Teachers can easily determine** if an assignment—or even one paragraph of an assignment—has been downloaded from the Internet instead of written by the student.
- **Children must rewrite and paraphrase**, not just copy material from the Internet. They must always include proper citations when they are using other people's work.
- **It is against the law to copy or download** some types of information or music from the Internet without permission.

Problems? Report Them!

Internet-related crime should be reported. Consult the following authorities:

- CyberTipline, National Center for Missing and Exploited Children, **800-843-5678**, www.missingkids.org
- Local or state police
- Federal Trade Commission (www.ftc.gov) for consumer fraud, auction fraud, etc.
- U.S. Department of Justice, www.usdoj.gov/criminal/cybercrime/reporting.htm
- Porn spam: contact your U.S. Attorney's office; complain to your Internet Service Provider.



Crime Prevention Tips From

NATIONAL CRIME PREVENTION COUNCIL
1000 Connecticut Avenue, NW
Thirteenth Floor
Washington, DC 20036-5325
202-466-6272
www.ncpc.org

and

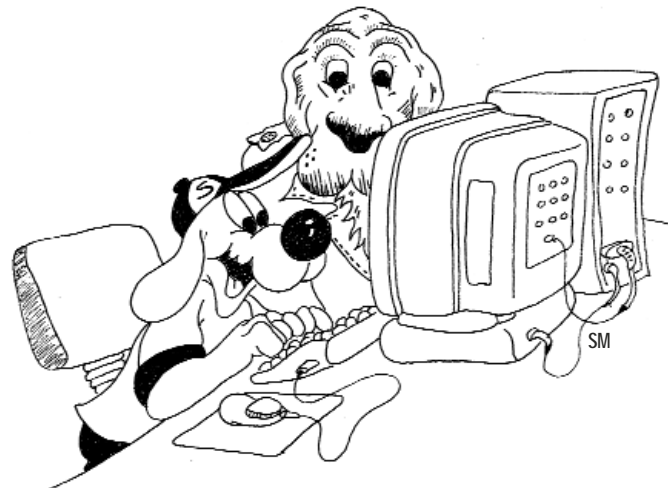


The National Citizens' Crime Prevention Campaign, sponsored by the Crime Prevention Coalition of America, is substantially funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.



Production made possible by a grant from ADT Security Services, Inc. a unit of Tyco Fire & Security Services.

A Family Guide to Using the Internet



NATIONAL CRIME PREVENTION COUNCIL

The Internet can be a wonderful tool for children and youth

• **Homework:** Kids can use the most current news, encyclopedias, and other source materials to find information for research projects.

• **Communication:** Kids can use email and public message boards to keep in touch with family and friends.

• **Entertainment and education:** Kids can use the Internet to make a virtual visit to a museum, take a college course, play games, etc.

• **Talk to your kids.** Keep the lines of communication open, and never blame the victim! If a child tells you about an upsetting event experienced online, don't blame him or her. How you react will affect how much he or she shares with you in the future.

• **Agree on a list of rules and post it by the computer:** The rules should cover how long children can spend on the Internet, how late they can surf the Web, what they may and may not visit on the Web, and whether or not they are allowed to make purchases over the Web. Have everyone in the household sign an Internet pledge (see www.safekids.com/kidsrules.htm).

• **Using the Computer Is a Family Affair**

But the Internet can also be dangerous. Here are some things families can do to encourage today's computer-savvy young people to be computer-safe.

Meeting People Online

• **As a general rule, children should never plan to meet anybody in person whom they have encountered online.** Explain that people met online may not be who they say they are.

• **When face-to-face meetings seem appropriate—the person is a student from a nearby school, for example—the meeting should be arranged only with your approval.** It should be in a safe public place, and you or another responsible adult should be present.

• **Children should never give out personal information over the Internet.** They should use an online name (not their real name) and never reveal their address, telephone number, or any identifying information.

• **No pictures, letters, or telephone calls should be exchanged** with online acquaintances without your approval. Monitor such communications.

• **If online acquaintances send your children email** that makes them uncomfortable or that they know is obscene, they should inform you at once. The same applies to information they see on message boards or chat rooms.

Making Online Purchases

• **Children need to learn to be savvy consumers.** The term "free" doesn't always mean free. Con artists use the term to attract more business. The children should ask you before signing up for anything over the Internet, even when signing up does not require a credit card number.

• **Encourage an attitude of healthy skepticism toward websites that offer prizes or giveaways.** Chances are, all the child has "won" is the opportunity to buy something he or she didn't want in the first place.

• **Establish explicit rules for getting clearance for online purchases, including documentation to be kept.**

• **Consider using a family-safe or child-safe search engine or a filter, blocking, or ratings system.** Some services have a "kids only" section so you can be sure the children won't have access to questionable material.

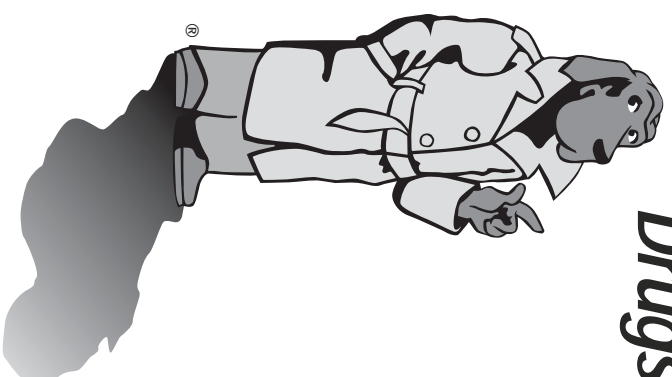
• **Encourage your children** to ask you to check out new sites with them.

• **Be responsive and nonjudgmental** if they tell you about an inappropriate site they found accidentally.

Following Links

Protecting Yourself From Counterfeit

Drugs



If you don't know for sure if the seller you're dealing with is legitimate, you may be at risk of receiving products that are contaminated, counterfeit, or not approved by the FDA.

You have lots of choices for buying prescription drugs these days. Among them are online pharmacies. Many online pharmacies offer greater convenience and lower prices than the corner drugstore, but if you don't know for sure if the seller you're dealing with is legitimate, you may be at risk of receiving products that are contaminated, counterfeit, or not approved by the FDA—or you may pay and receive nothing at all.

Counterfeit drugs can be dangerous to your health. Counterfeit medicine may be ineffective or cause serious side effects such as an allergic reaction. Drugs that are legitimate but not correctly prescribed (for example, those prescribed by an online doctor who has not examined you) can also be harmful or ineffective.

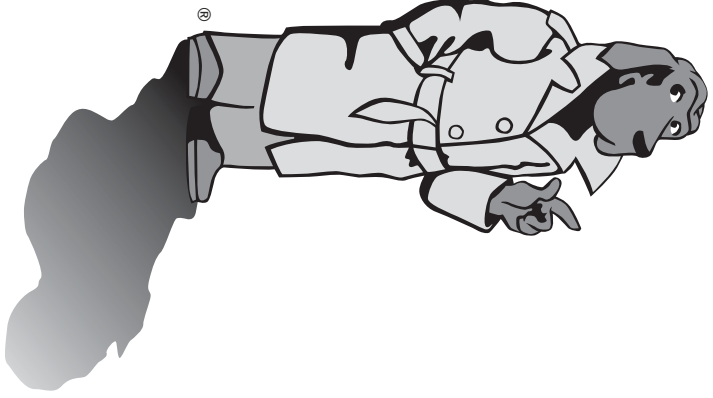
Here are some tips for buying prescription drugs online:

1. **Never purchase prescription drugs without your doctor's prescription.** Some online pharmacies will sell you drugs without one or only require that you fill out a short questionnaire. Taking drugs without the advice of a healthcare professional may put you at risk for drug interactions and other serious consequences.
2. **Be familiar with the medications you take,** including the color, size, shape, taste, and side effects. If you receive a counterfeit medication, you may be able to identify it more easily.
3. **Make sure the package or container** the medication comes in has not been altered or the label changed.
4. **Only buy prescription medications from a licensed pharmacy,** online or offline. To determine if a website is a licensed pharmacy in good standing, check with the National Association of Boards of Pharmacy (www.nabp.net, 847-698-6227).
5. **Do not purchase drugs from a foreign website.** It may be illegal to import the drugs bought from these sites.
6. **Use common sense.** If the website advertises a drug as a "miracle cure" for a disease or pushes a drug that guarantees weight loss, the claims are probably false.
7. **Report any website for a pharmacy that you think is illegal or any drug you purchased that you suspect is counterfeit.** If you bought the drug by mail, telephone, or in person, contact the FDA's Medwatch program at 800-332-1088 or at www.fda.gov/medwatch/. To report a counterfeit drug that you bought on the Internet, visit www.fda.gov/oc/buyonline/buyonlineform.htm or call the Medwatch number.



National Crime Prevention Council
1000 Connecticut Avenue, NW • 13th Floor • Washington, DC 20036 • www.ncpc.org

SHOPPING SAFELY Online



You just found the perfect antique lamp at an online auction site. You send off the check to the seller, but never receive the merchandise. Your mother has decided to begin purchasing her medicine online. Is it safe to do so?

The Internet is an exciting tool that puts a vast amount of information at your fingertips. With the click of a mouse you can buy the latest bestseller, make travel arrangements, rent a video, or purchase a gift for a friend.

Convenience, good deals, and choices are all good things that the Internet offers. But before you use it, be cybersmart and make your online experience a safe one.

- **Shop with companies you know.** Anyone can set up an online shop under almost any name. If you are not familiar with a merchant, ask for a paper catalog to get a better idea of the merchandise and services. Also be sure to determine a company's return and refund policies before making your purchase.
- **Keep your password private.** Never give your password to anyone. Avoid using a birthday or a portion of your Social Security number. If possible, use a combination of letters and numbers.
- **Use a secure browser.** This is the software you use to navigate the Internet. Your browser should comply with all industry security standards. These standards encrypt or scramble purchase information you send over the Internet. Most computers have a browser installed. Some browsers may be downloaded from the Internet free of charge.
- **Pay by credit card.** If you pay by credit card, your transaction will be protected by the Fair Credit Billing Act. Under this law, you have the right to dispute charges under certain circumstances and temporarily withhold payment while the creditor investigates them.
- **Keep personal information private.** Do not give out your Social Security number, email address, telephone number, or address unless you know who is collecting the information, why it's being collected, and how it will be used.
- **Save all transaction information,** including e-mails and records of any phone conversations.



NATIONAL CRIME
PREVENTION COUNCIL

National Crime Prevention Council
1000 Connecticut Avenue, NW • 13th Floor • Washington, DC 20036 • www.nccpc.org

If Someone Rips You Off

- **Report con games to the police,** your city or state consumer protection office, state Attorney General's office, or a consumer advocacy group.
- **File an online complaint** with the National Fraud Information Center at www.fraud.org or call the Fraud Hotline at **800-876-7060**, 9:00 a.m. to 5:00 p.m., eastern standard time, Monday through Friday.
- **File an online complaint** with the Federal Trade Commission (FTC) Bureau of Consumer Protection at www.consumer.gov/sentinel/.
- **If the scam occurred over the Internet,** file an online complaint with the Internet Crime Complaint Center (IC3), a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI), at www.ic3.gov.

For More Information

Federal Trade Commission: www.ftc.gov
 Internet Crime Complaint Center: www.ic3.gov
 National Consumers League: www.nclnet.org
 National Do Not Call Registry: www.donotcall.gov/
 National Fraud Information Center: www.fraud.org
 National White Collar Crime Center: www.nw3c.org
 U.S. Administration on Aging: www.aoa.gov
 U.S. Department of Justice:
www.usdoj.gov/criminal/fraud/telemarketing/



Crime Prevention Tips From

NATIONAL CRIME PREVENTION COUNCIL
 1000 Connecticut Avenue, NW
 Thirteenth Floor
 Washington, DC 20036-5325
 202-466-6272
www.nccpc.org

and

Use Common Sense To Spot a Con Artist



The National Citizens' Crime Prevention Campaign, sponsored by the Crime Prevention Coalition of America, is substantially funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.



Production made possible by a grant from ADT Security Services, Inc., a unit of Tyco Fire & Security Services.

NATIONAL CRIME
PREVENTION COUNCIL

It's not always easy to spot con artists. They are smart, extremely persuasive, and aggressive. They invade your home through the telephone, the Internet, and the mail; advertise in well-known newspapers and magazines; and knock on your door. They're well-mannered, friendly, and helpful—at first. Most people think they're too smart to fall for a scam. But con artists rob all kinds of people—from investment counselors and doctors to teenagers and senior citizens—of billions of dollars every year. Cons, scams, and frauds disproportionately victimize seniors with false promises of miracle cures, financial security, and luxury prizes. One easy rule to remember: If it sounds too good to be true, it probably is.

You Can Protect Yourself

- **Never give a caller your credit card, phone card, Social Security, or bank account number over the phone.** It's illegal for telemarketers to ask for these numbers to verify a prize or gift.
- **Beware of 900 numbers.** Remember, if you call a 900 number to claim a "prize," you'll end up paying for the call. Make sure you understand all charges before making a call.
- **Take your time and shop around.** Don't let an aggressive con artist pressure you into making a decision. Demand information in writing by mail. Get a second opinion. Ask your family, friends, and neighbors what they think about certain offers.
- **Stay informed about current scams in your area.** Contact your state Attorney General's office, the Better Business Bureau, or local consumer affairs office for more information.

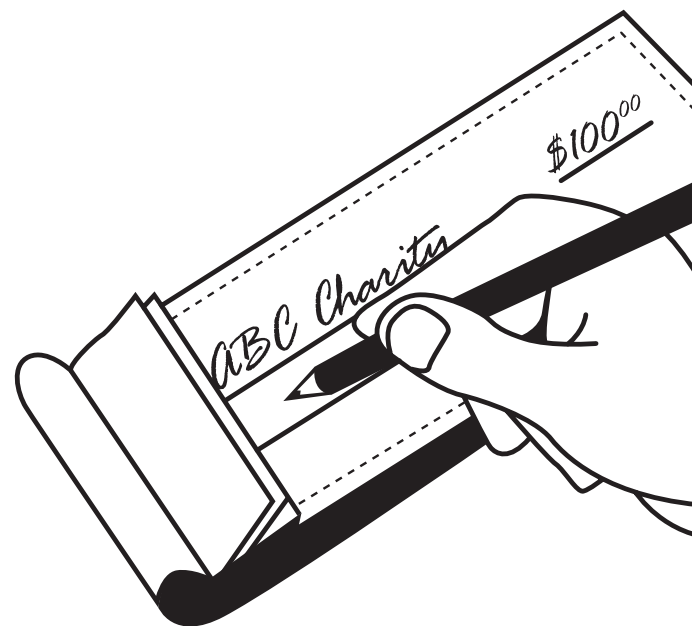
reliable, they'll come back after you check them out. who "just happen" to be in the neighborhood. If they're with cash. Never accept offers from drive-up workers simply take your deposit and never return. Never pay work, use shoddy materials and untrained workers, or *be expensive.* The con artist may do only part of the *Beware of cheap home repair work that would otherwise*

- **Register your phone number with the National Do Not Call Registry** at www.donotcall.gov to stop telemarketing calls.
- **Remember, you have the right, the ability, and the power to say no!** If the caller makes you wary, be assertive and end the conversation. Cons know that the longer they keep you on the phone, the higher their chance of success. By saying no and hanging up the phone, you can prevent a crime from taking place.
- **Don't buy health products or treatments that promise a quick and dramatic cure or that are promoted with testimonials, imprecise and nonmedical language, or emotional appeals.**
- **Look closely at offers that come in the mail.** Con artists often use official-looking forms and language to lure victims into signing up or sending payment. If you receive items in the mail that you didn't order, you are under no obligation to pay for them. You are free to throw them out, return them, or keep them.
- **Be wary of emails promising "free" vacations, foreign lotteries, work-at-home offers, get-rich-quick investments, and other schemes or that ask for donations to charities you've never heard of.** If you're interested, call the company directly. Never provide your personal information in a return email.
- **Beware of cheap home repair work that would otherwise be expensive.** The con artist may do only part of the work, use shoddy materials and untrained workers, or simply take your deposit and never return. Never pay with cash. Never accept offers from drive-up workers who "just happen" to be in the neighborhood. If they're reliable, they'll come back after you check them out.

Be a Wise Consumer

- **Register your phone number with the National Do Not Call Registry** at www.donotcall.gov to stop telemarketing calls.
 - **Remember, you have the right, the ability, and the power to say no!** If the caller makes you wary, be assertive and end the conversation. Cons know that the longer they keep you on the phone, the higher their chance of success. By saying no and hanging up the phone, you can prevent a crime from taking place.
 - **Don't buy health products or treatments that promise a quick and dramatic cure or that are promoted with testimonials, imprecise and nonmedical language, or emotional appeals.**
 - **Look closely at offers that come in the mail.** Con artists often use official-looking forms and language to lure victims into signing up or sending payment. If you receive items in the mail that you didn't order, you are under no obligation to pay for them. You are free to throw them out, return them, or keep them.
 - **Be wary of emails promising "free" vacations, foreign lotteries, work-at-home offers, get-rich-quick investments, and other schemes or that ask for donations to charities you've never heard of.** If you're interested, call the company directly. Never provide your personal information in a return email.
 - **Beware of cheap home repair work that would otherwise be expensive.** The con artist may do only part of the work, use shoddy materials and untrained workers, or simply take your deposit and never return. Never pay with cash. Never accept offers from drive-up workers who "just happen" to be in the neighborhood. If they're reliable, they'll come back after you check them out.
- Some Typical Scams Targeted at Seniors
- **Register your phone number with the National Do Not Call Registry** at www.donotcall.gov to stop telemarketing calls.
 - **Remember, you have the right, the ability, and the power to say no!** If the caller makes you wary, be assertive and end the conversation. Cons know that the longer they keep you on the phone, the higher their chance of success. By saying no and hanging up the phone, you can prevent a crime from taking place.
 - **Don't buy health products or treatments that promise a quick and dramatic cure or that are promoted with testimonials, imprecise and nonmedical language, or emotional appeals.**
 - **Look closely at offers that come in the mail.** Con artists often use official-looking forms and language to lure victims into signing up or sending payment. If you receive items in the mail that you didn't order, you are under no obligation to pay for them. You are free to throw them out, return them, or keep them.
 - **Be wary of emails promising "free" vacations, foreign lotteries, work-at-home offers, get-rich-quick investments, and other schemes or that ask for donations to charities you've never heard of.** If you're interested, call the company directly. Never provide your personal information in a return email.
 - **Beware of cheap home repair work that would otherwise be expensive.** The con artist may do only part of the work, use shoddy materials and untrained workers, or simply take your deposit and never return. Never pay with cash. Never accept offers from drive-up workers who "just happen" to be in the neighborhood. If they're reliable, they'll come back after you check them out.
- Many cons choose to victimize seniors. Con artists devise complex offers that confuse their targets and eventually persuade them to take up these offers. Don't let this happen to you:
- **The phone rings and the caller tells you that you've won a new car.** In order to claim the prize, you need to mail a check to cover the taxes and delivery costs. Weeks later, the phone rings again. You learn that the original prize company has gone out of business, but the caller tells you not to worry because his or her company has purchased the assets of the defunct company. All you need to do now is send another check to the new company to cover the costs of the legal transactions and for immediate delivery of the car. The check gets mailed but the prize never arrives.
 - **A mail offer or an ad in a newspaper or magazine or on television catches your eye.** It promises a quick cure for cancer, arthritis, memory loss, back pain, or other ailments. "It's an absolute miracle," one testimonial reads. "I feel a million times better." You mail your check for a six-week supply of this miracle cure and wind up with a jar of Vitamin C, placebos, or, even worse, pills or tonics that have not been medically tested.
 - **You get an email that promises that you can make \$1,000 a week working out of the comfort of your own home.** All you have to do is send a check for \$500, and you will receive everything you need to start your "home" business. You send a check, but all you get is a kit with some craft materials and printed instructions. The kit does not include a client list or any instructions on how or where to sell your products, and the craft materials are worth \$50, not \$500!

Preventing Charity Fraud



- The Internet Crime Complaint Center, online complaint form: www.ic3.gov
- The National Fraud Information Center, online complaint form: www.fraud.org



Crime Prevention Tips From

NATIONAL CRIME PREVENTION COUNCIL
1000 Connecticut Avenue, NW
Thirteenth Floor
Washington, DC 20036-5325
202-466-6272
www.ncpc.org

and



The National Citizens' Crime Prevention Campaign, sponsored by the Crime Prevention Coalition of America, is substantially funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.



Production made possible by a grant from ADT Security Services, Inc., a unit of Tyco Fire & Security Services.

NATIONAL CRIME PREVENTION COUNCIL

Charitable giving has never been easier. With a few clicks of a computer mouse, you can connect with causes you care about, learn how your support will make a difference, and put your money where your heart is—by making an instant online donation or pledge on a charity's website. But watch out! Fraudulent fundraisers know that "giving" is an emotional act, and they're good at pulling heartstrings—and pocket strings too.

How Charities Operate

All charities begin with a cause or mission. Next, they develop a program or service to promote the cause. Then they solicit funds to cover administrative costs (salaries, rent, and supplies), program costs (all services they will provide), and fundraising costs (mailings, advertisements, etc.).

Fundraising is how most charities stay alive. Common fundraising techniques include mailing letters, calling potential donors, posting requests for donations on websites, using emails to solicit funds, going door-to-door, selling products, and conducting telethons.

"Red Flags" and Illegal Fundraising Techniques

Charity fraud occurs when an individual or group deliberately misrepresents its fundraising intentions or solicits funds for phony causes. Fraudulent fundraisers use many of the same techniques as reputable fundraisers, but they may do so in a questionable or illegal way (e.g., a telephone call with a high-pressure appeal, a mailing that promises special favors from local firefighters in exchange for a donation).

Some charities operate just inside the law but outside of ethical boundaries, spending an excessive amount on fundraising and administrative costs but still

contributing a legally acceptable percentage of donated funds to the programs. The following fundraising techniques are questionable and, in some cases, illegal:

- **Prize offers:** Potential donors are told that they have won a contest and are eligible for a prize (usually worthless) if they make a donation to a charity.
- **Donated-back tickets:** Potential donors are encouraged to buy tickets and then donate them back so that they can be passed on to those who could not otherwise attend the event. Often the tickets never reach the needy.
- **Chain letters:** Unsolicited appeals, usually in the form of emails, ask potential donors not only to contribute to an organization but also to forward the email to friends and family members.
- **Unsolicited gifts:** Usually just tokens, these "gifts" are enclosed in direct mail solicitations to make the recipient feel obligated to give something back.
- **Emotional appeals:** Either verbal or written, they often involve graphic descriptions of need to play on sympathy of potential donors.
- **High-pressure tactics:** A solicitor urges the potential donor to give money (usually cash) immediately, before he or she has a chance to review information.
- **Spam email:** These unsolicited emails are sent to many people at once and often contain an emotional appeal and links to a website where potential donors can make an instant online donation using a credit card.
- **Sound-alike names:** Fraudulent charities take names that are very similar to those of high-profile charities that are known and trusted by the public.

that are known and trusted by the public.

- **Give directly to the charity if possible,** rather than to an organization claiming it will forward your donation to the charity.
- **Don't be fooled by a name** that closely resembles the name of a respected and well-known charity. Make sure you know who you are dealing with.
- **Don't give in to high pressure or emotional appeals** that urge you to donate on the spot. If you are unsure, don't be afraid to ask for more information.
- **Check out any charity** you don't know with the local charity watchdog group such as www.charitywatch.org, Better Business Bureau, or a charity registration office, www.give.org, and www.guidestar.org.
- **Request written information** that gives the full name, address, and phone numbers of the organization as well as a description of the programs it supports.
- **Check out any charity** you don't know with the local charity watchdog group such as www.charitywatch.org, Better Business Bureau, or a charity registration office, www.give.org, and www.guidestar.org.
- **Ask how your money will be used.** What percentage will go to the actual programs versus the administrative and fundraising costs?

How To Prevent Charity Fraud

- **Deceptive bills and invoices:** These claim that an amount is owed or promised to a particular charity when no such commitment was made.
- **Promises of special treatment by the local police or fire department:** Fundraisers claiming to be collecting on behalf of the police or fire department promise special treatment in return for a contribution.
- **Hasily constructed website:** Often set up within hours of a large-scale tragedy, these websites claim to be collecting for victims or victims' families.

What To Do If You're a Victim

If you're a victim of identity theft, the Federal Trade Commission (FTC) recommends that you do the following:

- **Contact the fraud department** of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts.
- **Close the accounts** that you know or believe have been tampered with or opened fraudulently. Use the ID Theft Affidavit (available on the FTC website and accepted by the three major credit bureaus) when disputing new unauthorized accounts.
- **File a police report.** Get a copy of the report to submit to your creditors and others who may require proof of the crime.
- **File your complaint with the FTC** at www.consumer.gov/idtheft. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. Filing a complaint also helps the agency learn more about identity theft and the problems victims are having so that it can better assist you.



Crime Prevention Tips From

NATIONAL CRIME PREVENTION COUNCIL

1000 Connecticut Avenue, NW
Thirteenth Floor
Washington, DC 20036-5325
202-466-6272
www.ncpc.org

and

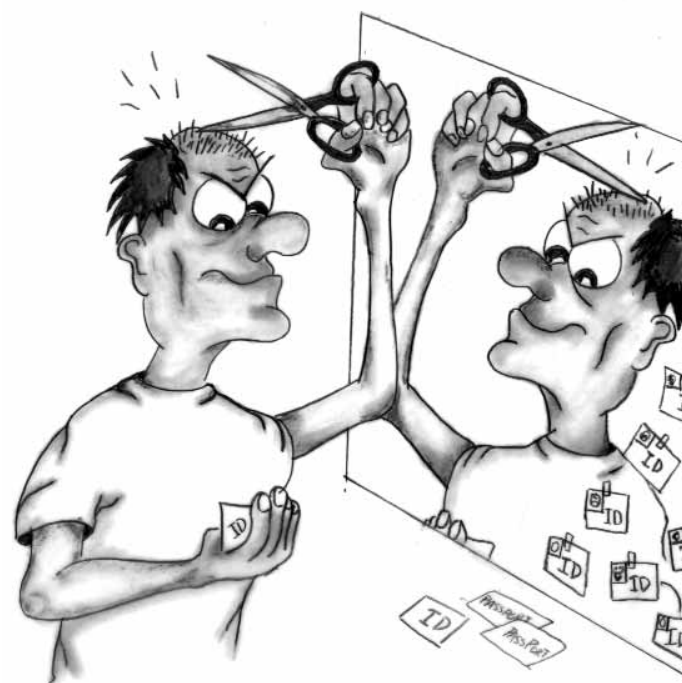


The National Citizens' Crime Prevention Campaign, sponsored by the Crime Prevention Coalition of America, is substantially funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.



Production made possible by a grant from ADT Security Services, Inc., a unit of Tyco Fire & Security Services.

Identity Theft

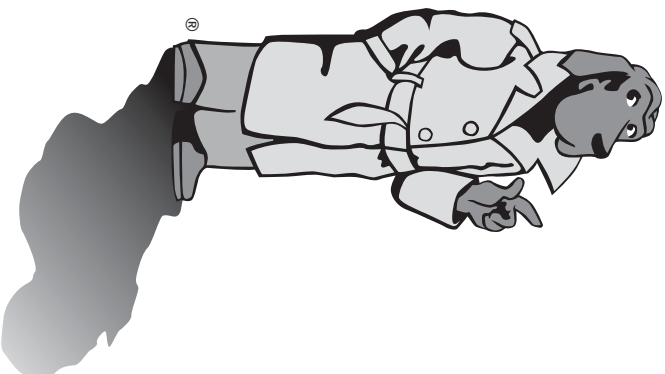


NATIONAL CRIME
PREVENTION COUNCIL

Don't Be Scammed!

Scams and schemes are a criminal's "bread and butter." If you have a computer, a telephone, or a mailbox, you could become a victim. Your best defense is to know a scam when you see (or hear) one. Following are a few common scams that criminals pitch to innocent people every day:

- **Credit-related Schemes:** You are promised a credit card regardless of your credit history, for an advance fee. Or you are promised credit card protection or credit repair services, also for a fee. You pay, but the card or service is never delivered.
- **Magazine Sales Scams:** You are offered a magazine subscription at a very low price by someone who claims to work for the magazine company. The price is misrepresented and is actually much higher, or the magazine is never delivered.
- **Investment Fraud:** You are invited to participate in an investment opportunity and promised spectacular profits with no risk. Instead of making money you lose it.
- **Overpayment Scams:** You advertise something you want to sell, and a potential buyer offers to purchase it. The buyer sends a check for more than the asking price and asks you to wire back the difference. You do, but later the buyer's check bounces.
- **Work-at-home Scams:** Advertisements promise big earnings for people who want to work at home. You send a check for training or materials and receive a kit with cheap craft materials and discover there are no clients to pay for your work.
- **Vacation/Travel Fraud:** You accept an offer for a free or very cheap travel package but end up paying hidden costs, such as reservation fees or taxes, or listening to a high-pressure sales pitch for a timeshare or club membership.
- **Phishing:** You get an email or pop-up message that says your account must be updated immediately or it will be closed. You click on a link to a website that looks like it belongs to your bank or other institution and "update" your account by entering personal identifying information. Soon you discover you are a victim of identity theft.
- **Pharming:** Also called domain spoofing, this technique is used by criminals to redirect Web traffic from a legitimate server to their own server, where they can steal any personal information that the user types in. Pharmers "poison" the Domain Name Service in order to "fool" a user's browser into linking to a bogus website.
- **Nigerian Money Scam:** You are contacted by someone from Nigeria and offered millions of dollars if you will transfer money from a foreign bank to your bank account for safekeeping. When you agree, you are asked to pay huge transfer fees or legal expenses but receive no money.
- **Prize and Sweepstakes Scam:** You are told that you have won a fabulous prize but must buy something or pay taxes up front in order to claim it. The prize is a cheap trinket, worth far less than the money you paid to claim it.
- **Foreign Lotteries Scam:** You are offered tickets to enter a foreign lottery and send money, but either the lottery doesn't exist or the tickets never arrive. It is illegal to promote a foreign lottery by telephone or mail in the United States.
- **Pyramids and Multilevel Marketing:** For a fee, you are promised big profits in exchange for recruiting new members. Plans that promise profits for recruitment of members rather than for selling goods and services are illegal and usually collapse.
- **Scholarship Scams:** A company guarantees scholarship money for an upfront fee, but it only helps locate scholarships rather than awarding them.
- **Charity Scams:** A natural disaster is dominating the news and you get a letter/email/phone call asking you to donate funds to help its victims. You send money, but the victims never receive your donation or receive only a tiny portion—the rest goes to cover administrative costs like salaries.
- **Bogus Merchandise Sales:** You purchase something advertised for sale on the Internet or through a telemarketing call. You pay for the merchandise but never receive it or receive an inferior or counterfeit product in its place.
- **Telephone Cramming:** Unauthorized charges for goods or services appear on your phone bill, but you miss seeing them because your phone bill is complicated with authorized charges such as voice mail and Internet service.
- **Telephone Slamming:** Your telephone service is switched from your current company to another one without your knowledge or permission, resulting in higher charges for long distance and other services.



Scams and schemes are a criminal's "bread and butter." If you have a computer, a telephone, or a mailbox, you could become a victim.



NATIONAL CRIME PREVENTION COUNCIL

National Crime Prevention Council
1000 Connecticut Avenue, NW • 13th Floor • Washington, DC 20036 • www.ncpc.org

In the course of the day you may write a check at the drugstore, charge tickets to a concert, rent a car, call home on your cell phone, or apply for a credit card. Chances are you don't give these routine transactions a second thought. But others may.

Identity theft is the fastest growing crime in America, affecting half a million new victims each year.

Identity theft is the taking of a victim's identity to obtain credit and credit cards from banks and retailers, steal money from a victim's existing accounts, apply for loans, establish accounts with utility companies, rent an apartment, file for bankruptcy, or obtain a job using the victim's name. Thousands of dollars can be stolen without the victim knowing about it for months or even years.

How Identity Theft Occurs

All an identity thief needs is any combination of your Social Security number, birth date, address, and phone number. This makes it possible to create a fake driver's license and then pose as you in order to apply for credit. The identity thief might put in a change of address with a credit card company so you will not know that someone else is running up charges. Once an identity thief opens one account, opening a second and a third is easier.

Identity thieves can get information about you from doctors, lawyers, schools, health insurance carriers, and other places. They may pick up your discarded personal information, such as utility bills, credit card slips, and bank statements. They may hack into your computer and

steal your Social Security or account numbers and credit card information. They may send you an email message asking you to "update" your account information and link you to a bogus website so they can steal your personal information.

How To Prevent Identity Theft

- **Do not give out personal information** over the phone, through the mail, or over the Internet unless you have initiated the contact or know with whom you're dealing.
- **Shred all documents**, including preapproved credit applications, insurance forms, bank checks and statements you are discarding, and other financial information.
- **Protect your computer from Internet intruders**—use "firewalls." Also use anti-virus software and keep it up-to-date.

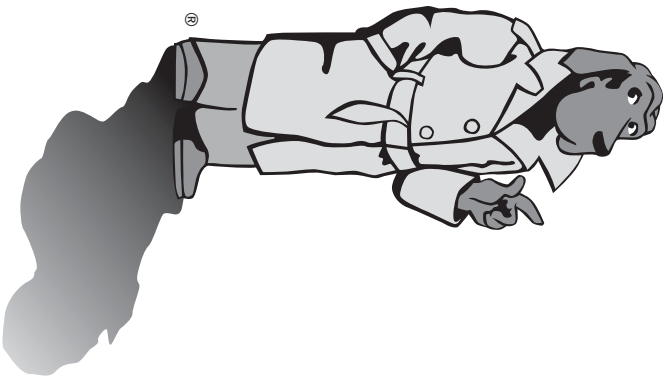
- **Create hard-to-guess passwords** that cannot be found in any dictionary. Select passwords with at least eight characters and that include a mix of numbers and both uppercase and lowercase letters.
- **Minimize the identification information** and the number of cards you carry. Take only what you'll actually need.
- **Do not put your Social Security number** on your checks or your credit receipts. If a business requests your Social Security number, give an alternate number.
- **Be careful when using ATM machines and long-distance phone cards.** Someone may look over your shoulder and get your PIN numbers.

- **Make a list** of all your credit card account numbers and bank account numbers with customer service phone numbers, and keep it in a safe place.

- **If you request a new credit card** and it doesn't arrive in an appropriate period of time, call to make sure someone has not filed a change of address for you.
- **Never submit your credit card number** to a website unless it is encrypted on a secured site. Look at the bottom of the screen for a padlock symbol. Do not select to save your information on the site for future transactions.
- **Pay attention to your billing cycles.** Follow up with creditors if bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your credit account and changed your address.
- **Cancel all credit cards** you have not used in the last six months.

- **Order your credit report** at least twice a year from the three major credit bureaus: Equifax (www.equifax.com), Experian (www.experian.com), and Trans Union (www.transunion.com). The Fair Credit Reporting Act allows you to get one free credit report from each of the three major credit bureaus once per year. Visit www.annualcreditreport.com.
- **Correct all mistakes on your credit report in writing.** Send a letter to the credit reporting agency identifying the problems item by item, include a copy of the credit report, and send the letter return receipt requested.

Reporting Crime Online



The Internet offers you many ways to notify law enforcement of criminal activity. Online complaint forms are available on the websites of government agencies and other organizations that are working to fight certain types of crime. These complaints go into secure online databases that are available to hundreds of civil and criminal law enforcement agencies worldwide.

Any crime that is dangerous or life threatening should be reported directly to local law enforcement. Credit card companies and financial institutions should be notified by phone as soon as fraud is suspected. But crimes such as identity theft, computer hacking, spam, and telemarketing fraud may be best addressed by agencies that specialize in these problems. Here is a list of online reporting portals, emails, and phone numbers for the following complaints:

- CHARITY FRAUD**
 - www.bbb.org: Better Business Bureau (BBB)
 - www.ic3.gov: Internet Crime Complaint Center (IC3)
 - www.fraud.org: National Fraud Information Center (NFIC)
 - NFIC hotline at **800-876-7060**
- CHILD PORNOGRAPHY OR SEXUAL EXPLOITATION**
 - www.cyberipline.com: National Center for Exploited and Missing Children (NCEMC)
 - NCEMC Hotline **800-THE-LOST (800-843-5678)** 24 hours a day
 - www.ic3.gov: Internet Crime Complaint Center (IC3)
- COMPUTER INTRUSIONS AND CYBER THREATS**
 - www.ic3.gov: Internet Crime Complaint Center (IC3)
 - www.treas.gov/uss/net_intrusion_forms.shtml: U.S. Secret Service
 - www.us-cert.gov: U.S. Computer Emergency Readiness Team
- IDENTITY THEFT**
 - www.ic3.gov: Internet Crime Complaint Center (IC3)
 - www.consumer.gov/idtheft/: Federal Trade Commission (FTC)
 - FTC's Identity Theft Hotline: **877-IDTHEFT (438-4338)**
 - www.bbb.org: Better Business Bureau (BBB)
- INTELLECTUAL PROPERTY RIGHTS**
 - www.ic3.gov: Internet Crime Complaint Center (IC3)
 - www.ice.gov/graphics/cornerstone/ipr/PPIForm.htm: U.S. Immigration and Customs Enforcement
 - www.sba.org: Software Business Alliance
- INTERNET-RELATED FRAUD**
 - www.ic3.gov: Internet Crime Complaint Center (IC3)
 - www.consumer.gov/sentinel/: Federal Trade Commission (FTC)
- MAIL FRAUD**
 - www.usps.com/postalinspectors/fraud/MailFraudComplaint.htm: U.S. Postal Inspection Service
- OBSCENITY CRIMES**
 - <http://www.fcc.gov/cgb/complaints.html>: Federal Communications Commission (FCC)
 - Email: fccinfo@fcc.gov
 - www.obscenitycrimes.org: Morality in the Media
- ONLINE SECURITIES FRAUD**
 - www.sec.gov/complaint.shtml: U.S. Securities and Exchange Commission (SEC) (Investment-related SPAM email)
 - Email: enforcement@sec.gov
- ONLINE TRANSACTION INVOLVING A FOREIGN COMPANY**
 - www.econsumer.gov: Agencies from 19 nations
- PHISHING**
 - reportphishing@antiphishing.org: Anti-Phishing Working Group
 - www.ic3.gov: Internet Crime Complaint Center (IC3)
 - www.consumer.gov/sentinel/: Federal Trade Commission (FTC)
- PRIVACY VIOLATIONS**
 - www.privacyrights.org: Privacy Rights Clearinghouse
 - www.bbb.org: Better Business Bureau (BBB)
- SUSPICIOUS ONLINE PHARMACIES**
 - www.deadiversion.usdoj.gov/: Drug Enforcement Administration (DEA)
 - **877-Rx-Abuse (877-792-8273)**
 - www.fda.gov/oc/buyonline/buyonlineform.htm: Food and Drug Administration (FDA)
- TELEMARKETING FRAUD**
 - www.fraud.org: National Fraud Information Center (NFIC)
 - NFIC hotline at **800-876-7060**
 - www.consumer.gov/sentinel/: Federal Trade Commission (FTC)
- TERRORIST ACTIVITY**
 - www.fbi.gov/contact/fo/fo.htm: To find local FBI office
 - <https://tips.fbi.gov>: Federal Bureau of Investigation (FBI)
- UNSOLICITED COMMERCIAL EMAIL (SPAM)**
 - Email: SPAM@UCE.gov: Federal Trade Commission (FTC)
 - www.sec.gov/complaint.shtml: Investment-related spam email
- VIOLATION OF DO NOT CALL REGISTRY**
 - www.donotcall.gov/: National Do Not Call Registry
- WIRELESS AND WIRELINE PHONE FRAUD**
 - www.fcc.gov/cgb/complaints.html: Federal Communications Commission (FCC)
 - **888-CALL-FCC (888-225-5322)**
 - Email: Stamming@fcc.gov (when your phone service has been switched without your authorization)

Beware of International Modem Dialing

If you use a dial-up modem to connect to the Internet and download a "viewer" or "dialer" computer program (usually offered for free to access a site), the program may disconnect your modem and then reconnect it to the Internet through an international long-distance number without your knowledge or authorization. You will then receive a large international phone bill.

Tip: Install a dedicated phone line for your computer that is restricted to local calls. If that is not possible, watch out for any program that allows your modem to redial to the Internet without your direction. Cancel the connection, and check the number your modem is dialing.

The Federal Communications Commission (FCC) is the federal agency responsible for regulating your telephone services. Go to its website, www.fcc.org, for information on how to review your telephone bill, how to spot cramming charges, and other telephone-related consumer issues.

You can file a complaint by email (fccinfo@fcc.gov), the Internet (www.fcc.gov/cgb/complaints.html), or telephone (**888-CALL-FCC [888-225-5322]**).



Crime Prevention Tips From

NATIONAL CRIME PREVENTION COUNCIL
 1000 Connecticut Avenue, NW
 Thirteenth Floor
 Washington, DC 20036-5325
 202-466-6272
www.ncpc.org

and

Protect Yourself From Telephone Fraud



BJA Bureau of Justice Assistance
 Office of Justice Programs ■ U.S. Department of Justice

The National Citizens' Crime Prevention Campaign, sponsored by the Crime Prevention Coalition of America, is substantially funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.



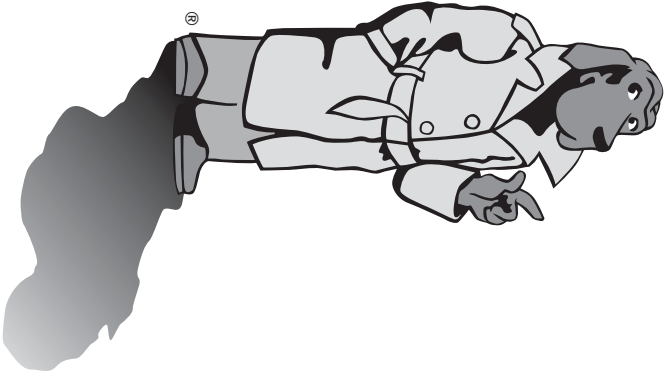
Production made possible by a grant from ADT Security Services, Inc., a unit of Tyco Fire & Security Services.

NATIONAL CRIME PREVENTION COUNCIL



NATIONAL CRIME PREVENTION COUNCIL
 National Crime Prevention Council
 1000 Connecticut Avenue, NW • 13th Floor • Washington, DC 20036 • www.ncpc.org

Kids: Be a Good Cyber Citizen!



Like a car, the computer is a complex machine that needs your care and attention in order to perform well. It can take you places on your own; some of these places are familiar to you and some are not.

You've heard the expression "surfing the Internet." In many ways, spending time on the Internet is more like driving a car than riding a wave. Like a car, the computer is a complex machine that needs your care and attention in order to perform well. It can take you places on your own; some of these places are familiar to you and some are not. And whether you're behind the wheel or at the keyboard, your personal safety and the safety of those around you depend on your willingness to use common sense, behave courteously, and obey the law.

In other words, driving a car and exploring the Internet mean the same thing: freedom and responsibility.

TAKE CARE OF YOUR COMPUTER

Protect your computer from viruses that could destroy your files and make it difficult or impossible to use. If your computer becomes infected, you might pass these viruses on to other computer users without realizing it.

- If your computer doesn't have anti-virus software, install it and keep it up-to-date.
- Don't open an email from someone you don't know. It might contain a virus.
- If you open an email by mistake, don't click on links or download files that came with it.
- Don't pass along joke emails or chain letters, as they may contain viruses.
- Use hard-to-guess passwords, and keep them secret—even from your friends.
- Make sure that your family has installed a firewall to keep your computer safe from hackers.
- If your computer operating system allows file sharing, disable it. File sharing could be used by others to infect your computer with a virus or to look at the files on your computer.
- Disconnect your computer when you're not on the Internet.
- Help your family by backing up your computer files onto CDs or diskettes.

FOLLOW THE RULES OF THE ROAD

The best tool you have for screening what you find on the Internet is your brain. If you come across websites that are pornographic, full of hate literature, or have excessively violent content, move on. Here are a few reminders for safe traveling on the Internet:

- Never give out your name, address, telephone number, password, school name, parents' names, pictures of yourself, parents' credit card numbers, Social Security number, or any other personal information to others online.
- Never agree to meet face to face with someone you've met online without discussing it with your parents. If your parents decide that it's okay to meet your "cyber-friend," arrange to meet in a familiar public place and take an adult with you.
- Never enter an area that charges for services without first getting your parents' permission.
- If you receive pornographic material or threatening email, save the offensive material, tell your parents, and contact your Internet service provider and your local law enforcement agency.
- Beware of emails that are trying to sell you something. It is probably best not to respond to them. If you do, you are confirming that you have a valid email address and the sender will continue to email you with offers.
- If you have your parent's permission to order something over the Internet, go directly to the company's website. Never link to it from an email.

RESPECT THE RIGHTS OF OTHERS

Some things you do on the computer may seem okay to you, but they are actually crimes. Even if these cyber crimes are never prosecuted, your actions can have a serious financial and emotional cost to your victims. Remember, if you harass or threaten another person on the Internet, you are no different from the bully on the playground. The U.S. Department of Justice describes three ways computers are used to commit crimes:

- The computer as a target (using a computer to attack other computers): If you hack into school computer networks to view or change grades, shut down or deface websites, or create or send computer viruses, you are committing a crime.
 - The computer as a weapon (using a computer to commit a crime): If you use email and chat programs as harassment by saying things to other kids that you would never say face to face, steal passwords in order to read other peoples' emails, or send emails in their name, you are committing a crime.
 - The computer as an accessory (using a computer to store illegal files or information): If you download and share copyrighted music, games, and other software without the permission of the owner or plagiarize copyrighted information and pass it off as your own, you are committing a crime.
- If you have any questions about what is legal or illegal behavior on the Internet, talk to your teacher, parent, or other caregiver. You can also visit the U.S. Department of Justice website, www.cybercrime.gov/rules/kidinternet.htm, for more information about good cyber citizenship.



National Crime Prevention Council
1000 Connecticut Avenue, NW • 13th Floor • Washington, DC 20036 • www.ncppc.org

The telephone is among the greatest inventions of the modern age. From the days of the party line to the days of wireless and Internet phones, they have connected us with loved ones, made our lives more convenient, and given us peace of mind. But telephones are also prone to fraud. Don't be a victim. Educate yourself about phone fraud, and know how to spot—and prevent—a telephone scam.

Beware of voice mail fraud.

Hackers can compromise your voice mail system to make collect, third-party, or direct-dial calls at your expense. Voice mail vendors provide new customers with a default password—usually an easily-guessed combination such as 1-2-3-4. If you don't change it, hackers can guess it quickly and break into your phone system. Once a hacker knows your password, he or she can use it to make international calls at your expense.

Beware of cell phone subscriber fraud.

A criminal who obtains your personal information can use it to set up a cell phone account in your name. Charges can go on for years without your knowledge. People who are victims of identity theft often find that they are also victims of cell phone subscriber fraud.

Tip: Keep personal information (Social Security number, credit card number, bank account number, mother's maiden name, birth date, etc.) private so it cannot be used by someone else.

Tip: Always change your default password immediately. Choose a complex voice mail password of at least six digits, and change it frequently.

Tip: Always check your phone bill carefully to make sure you are paying only for services you authorized.

bill, figuring that you will not notice. charges—those you never authorized—onto your phone advantage of confusing phone bills by sneaking other a long and complicated statement. "Crammers" take calling cards added to your phone bill. This may result in charges for services such as voice mail, paging, and Like many consumers, you may choose to have legitimate

Beware of phone "cramming."

Tip: Read your phone bill carefully each month, and make sure you still have the long-distance company you selected.

A fraudulent carrier may change your long-distance phone service without your permission or knowledge. This usually results in higher charges for long-distance calls on your phone bill. Or you may be deceived into agreeing to switch your service by entering a contest and not reading the fine print, which authorizes the switch.

Beware of phone "slamming."

Tip: Check your phone bill carefully, and call your carrier if you think your cell phone has been cloned.

Criminals can clone your cell phone by illegally monitoring radio wave transmissions to determine your unique electronic serial number (ESN) and your cell phone number (mobile identification number [MIN]). The cloned cell phone is reprogrammed to transmit your ESN and MIN numbers. The cellular system will not be able to tell the difference and will bill you for the cloned phone's calls as well as your own.

Beware of calling-card number scams.

A criminal posing as a telephone company representative may call you and ask for verification of your calling-card number to check for unauthorized charges, and then use it to make international calls.

Tip: Never give out personal information on the telephone. Call your phone company directly to verify that there is a problem with your calling card.

Call splashing can happen when you place a call from a public phone. You may believe that you are using your preferred long-distance carrier, but your call is actually routed first to a distance call center. As a result, you will be billed as if you made the call from the distant location rather than from your actual location, resulting in higher rates.

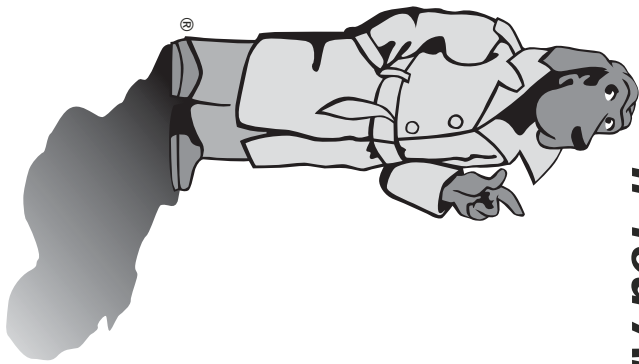
Tip: Call splashing is only legal if you request that the call be transferred to a different carrier's operator or you consent to this practice. Don't consent to any call transfers unless you understand what the operator is asking.

Beware of the 809 Area Code Scam.

You may receive an urgent message on your answering machine or pager requesting that you call a number immediately, usually because of a "family emergency." When you call the number, you discover that the call has nothing to do with your family. The 809 area code is actually the country code for the Dominican Republic, and later an expensive phone charge shows up on your phone bill.

Tip: Always know where you're calling before you dial. While it is usually necessary to dial 011 to reach an international location, some international locations have telephone numbers that resemble domestic long-distance calls.

How To Avoid Being Stalked in Cyberspace (and What To Do If You Are)



Like physical stalking, cyberstalking can lead to physical violence. Victims suffer psychological trauma, often resulting in anxiety, depression, insomnia, and even loss of employment.

Cyberstalking is a serious crime. A cyberstalker is someone who uses the Internet, email, or other electronic communications devices to repeatedly threaten and harass another person. Cyberstalking is similar to physical stalking in that most victims are women and most stalkers are men, the person being stalked usually knows the stalker, and the stalker's motivation is to exert control over the victim.

Cyberstalking is different in that the stalker and victim can be located in different geographic areas, the stalker generally relies on the Internet to send harassing or threatening communications, and the stalker can easily encourage other Internet users to harass and threaten the victim by posing as the victim in chatrooms or posting inflammatory messages on Internet bulletin boards.

Like physical stalking, cyberstalking can lead to physical violence. Victims suffer psychological trauma, often resulting in anxiety, depression, insomnia, and even loss of employment. The lack of direct contact between the cyberstalker and the victim can make it difficult for law enforcement to find and arrest the offender.

HERE ARE SOME TIPS TO PREVENT CYBERSTALKING:

- Make a list of safe sites (those sites that adopt an anti-harassment policy and follow through with it). Only visit those sites.
 - Never give out any personal information about yourself to strangers in emails and chatrooms or on Internet bulletin boards.
 - When you are online, only type things you would actually say to someone face to face. Think about how what you say might be interpreted without the context of body language and voice.
 - Make sure that your screen name is neutral; never use your real name, nickname, or any type of "suggestive" name.
 - Be very cautious about meeting an online acquaintance in person. If you choose to do so, always take someone with you and meet in a public place.
 - If you experience contact with someone that is unpleasant or hostile, log off immediately. Report the incident to your Internet Service Provider (ISP). Most chat/bulletin boards also have a reporting system for unpleasant encounters.
- HERE ARE SOME THINGS YOU CAN DO IF YOU ARE BEING CYBERSTALKED:**
- If you are under 18, immediately talk to your parents or an adult you can trust about the situation. You may be in physical danger.
 - If your email program has filtering capabilities, use them to block or filter email from the stalker. Sometimes you can block chatroom contact as well.
 - Inform your ISP of the situation and request a new log-on name and password. If your ISP is not responsive, get a new account.
 - Keep a log of all communications from the stalker. Make copies of every email, and do not alter them in any way. This is your only evidence.
 - Make it absolutely clear to the stalker that you would like him or her not to contact you again.
 - If the harassment does not stop, contact your local police department and tell them the situation.

For more information, contact the National Center for Victims of Crime (NCVC). You can call the Victim Assistance Hotline at 800-FYI-CALL Monday through Friday, 8:30 a.m. to 8:30 p.m. EST, or send an email to gethelp@ncvc.org. Visit NCVC's Stalking Resource Center at www.ncvc.org/src/.



NATIONAL CRIME PREVENTION COUNCIL

National Crime Prevention Council
1000 Connecticut Avenue, NW • 13th Floor • Washington, DC 20036 • www.ncpc.org

Protección de su información privada



NATIONAL CRIME PREVENTION COUNCIL

Tarjetas de crédito

Si hace compras en línea o por teléfono, puede pagar con su tarjeta de crédito. Ya que no puede usar la tarjeta misma, probablemente proporcionará el número de su tarjeta de crédito, incluyendo la fecha de caducidad, por teléfono o Internet. Si estos números llegan a manos equivocadas podría descubrir cargos no autorizados en el siguiente estado de cuentas de su tarjeta de crédito.

- Haga negocios sólo con compañías que conoce; no dé el número de cuenta de su tarjeta de crédito para hacer una compra o una reservación, a menos que usted haya iniciado la transacción.
- Compre sólo de sitios web seguros que usen software de encriptación para transferir datos de su computadora al comerciante y que tengan políticas estrictas de privacidad y seguridad.
- No responda a mensajes electrónicos que parecieran provenir de la compañía que emitió su tarjeta de crédito pidiéndole una "actualización" de su información. Llame directamente a la compañía para verificar la información que se necesite.
- Si recibe ofrecimientos de tarjetas de crédito preaprobadas por correo, no los tire en la basura sin antes hacerlos pasar por una máquina desfibadora.
- Si está esperando recibir por correo nuevas tarjetas de crédito y éstas demoran en llegar, o si no recibe sus cuentas de cobro en el período de tiempo esperado, llame inmediatamente a la entidad emisora de la tarjeta de crédito.
- Después de realizar compras por Internet, revise cuidadosamente los estados de cuenta de sus tarjetas de crédito durante varios meses. Si descubre compras que no hizo, póngase en contacto inmediatamente con la compañía que emitió la tarjeta de crédito y formule un reclamo por los cargos.
- Obtenga una copia de su reporte de crédito una vez al año y revíselo buscando cualquier actividad no esperada.

Notificación de un problema

Si descubre que hay cargos no autorizados en el estado de cuentas de su tarjeta de crédito o retiros de su cuenta bancaria, notifique inmediatamente a la policía y a la institución financiera correspondiente. Si es víctima del delito de robo de identidad, formule una denuncia policial; presente una denuncia en línea a la Comisión de Comercio Federal (Federal Trade Commission) en www.consumer.gov/idtheft/; notifique a las tres agencias de crédito más importantes: Equifax (www.equifax.com), Experian (www.experian.com) y Trans Union (www.transunion.com) y cierre su cuenta.



Consejos para prevenir delitos del

NATIONAL CRIME PREVENTION COUNCIL

1000 Connecticut Avenue, NW
Thirteenth Floor
Washington, DC 20036-5325
202-466-6272
www.ncpc.org

y de



La Campaña Nacional de los Ciudadanos para la Prevención del Crimen (The National Citizens' Crime Prevention Campaign) patrocinada por la Coalición Estadounidense para la prevención del Crimen (Crime Prevention Coalition of America) y financiada principalmente por la Dirección de Asistencia Judicial (Bureau of Justice Assistance), Oficina de Programas de Justicia (Office of Justice Programs), Departamento de Justicia de los EE.UU.



La producción de este folleto fue posible gracias a una subvención de ADT Security Services, Inc., Tyco International Ltd. Company.

- Cree una nueva contraseña para cada sitio web o para ingresar a un sistema de computadoras que lo solicite. Si eso es poco práctico, cree unas cuantas contraseñas difíciles de adivinar y úselas en los sitios en los que desee mantener más seguridad. Cree contraseñas fáciles de recordar para usarlas en sitios menos importantes.
- Cambie sus contraseñas con regularidad, por lo menos una vez al mes.
- No use ninguna palabra que pueda hallarse en el diccionario de cualquier idioma.
- No use Social, nombres de sus hijos o mascotas, ni la fecha de su nacimiento.
- No use el nombre de soltera de su madre, el nombre de su cónyuge, los últimos cuatro dígitos de su número de Seguro Social, nombres de sus hijos o mascotas, ni la fecha de su nacimiento.
- Seleccione por lo menos ocho símbolos, incluyendo una combinación de letras, números y signos que usted pueda recordar pero que otros no puedan adivinar fácilmente.
- No use el nombre de soltera de su madre, el nombre de su cónyuge, los últimos cuatro dígitos de su número de Seguro Social, nombres de sus hijos o mascotas, ni la fecha de su nacimiento.
- No use ninguna palabra que pueda hallarse en el diccionario de cualquier idioma.
- Cree una nueva contraseña para cada sitio web o para ingresar a un sistema de computadoras que lo solicite. Si eso es poco práctico, cree unas cuantas contraseñas difíciles de adivinar y úselas en los sitios en los que desee mantener más seguridad. Cree contraseñas fáciles de recordar para usarlas en sitios menos importantes.
- Cambie sus contraseñas con regularidad, por lo menos una vez al mes.

Contraseñas

El correo electrónico, Internet, los cajeros automáticos (automated teller machines – ATM), la banca en línea, los teléfonos celulares, las compañías telefónicas de larga distancia e incluso las tarjetas de crédito hacen nuestra vida más eficiente. Sin embargo, a medida que nos integramos más con la tecnología, se hace más difícil mantener nuestra información privada confidencial. Las transacciones electrónicas pueden dejarlo vulnerable al robo de identidad y a otros tipos de fraude. Los siguientes consejos sencillos le pueden ayudar a mantener segura su información privada.

- Memorice sus contraseñas; si tiene que escribirlas, no las lleve escritas en su billetera ni las deje en lugares sin protección, incluyendo archivos de la computadora.
- Si su computadora le brinda la opción de recordar su contraseña, no elija esa opción.
- No comparta sus contraseñas con miembros de su familia, amigos o colegas.
- Si ha ingresado su clave de acceso a un cajero automático o está comenzando la sesión en una computadora, asegúrese de que nadie esté mirando mientras ingresa su contraseña.
- Memorice sus contraseñas; si tiene que escribirlas, no las lleve escritas en su billetera ni las deje en lugares sin protección, incluyendo archivos de la computadora.
- Si su computadora le brinda la opción de recordar su contraseña, no elija esa opción.
- No comparta sus contraseñas con miembros de su familia, amigos o colegas.
- Si ha ingresado su clave de acceso a un cajero automático o está comenzando la sesión en una computadora, asegúrese de que nadie esté mirando mientras ingresa su contraseña.
- El número de identificación personal (personal identification number – PIN) es uno de los métodos usados por los bancos y las compañías telefónicas para proteger su cuenta del acceso no autorizado. Un PIN es un código privado emitido al titular de la tarjeta para permitirle el acceso a esa cuenta. Usted puede proteger su número PIN siguiendo estos consejos:
- Memorice su número PIN y no se lo dé a nadie, incluyendo a miembros de la familia o empleados del banco.
- Nunca escriba su PIN en las tarjetas de los cajeros automáticos (ATM) o tarjetas para hacer llamadas de larga distancia; no lleve su número PIN en su cartera o billetera.
- Cuando use un cajero automático (ATM) o un teléfono público, sitúese frente al teclado del cajero automático o del teléfono público para evitar que nadie observe su PIN mientras lo ingresa.
- No deje su recibo en la máquina cuando use el cajero automático; los delincuentes pueden usarlo para obtener su número de cuenta.
- Si un banco u otra institución le asigna un número PIN que consta de los cuatro dígitos finales de su número de Seguro Social, pida que se los cambien por otros números.

Números de identificación personal

- Algunas empresas y agencias del gobierno afirman que usar su número de Seguro Social (Social Security number – SSN) es la manera más precisa de almacenar y recuperar información. Su número de Seguro Social es, sin embargo, el objetivo principal de delincuentes interesados en cometer robo de identidad y otros delitos más. Por lo tanto, es esencial que proteja su SSN.
- Dé su SSN sólo cuando sea absolutamente necesario. Los empleadores necesitan su SSN para informar al Servicio Interno Fiscal (Internal Revenue Service – IRS) sus ingresos, pero las agencias del orden público no lo necesitan para emitirle un permiso de estacionamiento.
- No lleve su tarjeta de Seguro Social en su billetera o cartera a menos que lo necesite para una situación específica, como por ejemplo el primer día en un trabajo nuevo.
- No imprima su SSN en cheques o tarjetas profesionales de presentación.
- De ser posible, no incluya su SSN en los formularios de aplicación para puestos de trabajo.
- Si le piden su SSN en línea, busque el símbolo de candado cerrado en la parte inferior de la página y lea las normas de privacidad de la compañía con respecto a la forma en que protege su información personal.
- No responda a mensajes electrónicos no solicitados que pidan su SSN y otra información personal. Ninguna compañía acreditada ni agencia gubernamental envía mensajes electrónicos no solicitados para pedir datos personales confidenciales.
- Si una empresa privada le pide su SSN, sugiera alternativas como su número de licencia de conducir (a menos que su número de licencia de conducir sea el mismo que su SSN).
- Si la Dirección General de Tránsito de su estado usa el SSN como el número de licencia de conducir, pida un número diferente.

Números del Seguro Social

Para más información visite:

- Federal Trade Commission: www.ftc.gov
- Internet Crime Complaint Center: www.ic3.gov
- National Consumers League: www.nclnet.org
- National Do Not Call Registry: www.donotcall.gov/
- National Fraud Information Center: www.fraud.org
- National White Collar Crime Center: www.nw3c.org
- U.S. Administration on Aging: www.aoa.gov
- U.S. Department of Justice: www.usdoj.gov/criminal/fraud/telemarketing/



Consejos para prevenir delitos del

NATIONAL CRIME PREVENTION COUNCIL
 1000 Connecticut Avenue, NW
 Thirteenth Floor
 Washington, DC 20036-5325
 202-466-6272
www.ncpc.org

y de



La Campaña Nacional de los Ciudadanos para la Prevención del Crimen (The National Citizens' Crime Prevention Campaign) patrocinada por la Coalición Estadounidense para la Prevención del Crimen (Crime Prevention Coalition of America) y financiada principalmente por la Dirección de Asistencia Judicial (Bureau of Justice Assistance), Oficina de Programas de Justicia (Office of Justice Programs), Departamento de Justicia de los EE.UU.



La producción de este folleto fue posible gracias a una subvención de ADT Security Services, Inc., Tyco International Ltd. Company.

Use el sentido común para detectar a un estafador



NATIONAL CRIME PREVENTION COUNCIL

- No siempre es fácil detectar a los estafadores. Son inteligentes, muy persuasivos y agresivos. Invaden su hogar a través del teléfono, Internet y el correo; ponen sus anuncios en periódicos y revistas muy conocidos; y tocan su puerta. Son corteses, afectuosos y serviciales, por lo menos al principio. La mayoría de personas piensa que son demastado inteligentes para caer en una estafa. Pero los estafadores roban a todo tipo de personas — desde asesores financieros y médicos hasta adolescentes y ancianos — de miles de millones todos los años. Las estafas, los engaños y los fraudes afectan a los ancianos en forma desproporcionada ofreciendo esperanzas falsas de curas milagrosas, seguridad económica y premios de lujo. Una regla fácil de recordar: si suena demastado bueno para ser cierto, probablemente lo sea.
- **Usted puede protegerse a sí mismo**
- Cuando reciba una llamada de ventas telefónicas, nunca de ninguno de los siguientes números: tarjetas de crédito, tarjetas telefónicas, Seguro Social o cuentas bancarias. Es ilegal pedir estos números para verificar un premio o regalo.
- Tenga cuidado de los números telefónicos que comienzan con 900. Recuerde, si llama a uno de estos números para reclamar un "premio"; terminará pagando por la llamada. Asegúrese de entender todos los cargos antes de hacer la llamada.
- Tómese su tiempo y compare precios y productos. No deje que un estafador agresivo lo presione para tomar una decisión. Pida que le envíen por correo información por escrito. Obtenga una segunda opinión. Pregunte a su familia, amigos y vecinos lo que piensan sobre ciertos ofrecimientos.
- Manténgase informado sobre ciertas estafas que están ocurriendo en su área. Póngase en contacto con la oficina del Fiscal General, la Oficina de Mejores

- **Sea un consumidor educado**
- No compre productos de salud o tratamientos que prometan una cura rápida y sensacional o aquellos que se presentan con testimonios de terceros, lenguaje impreciso y no médico, o que recurran a las necesidades emocionales.
- Observe detenidamente las ofertas que lleguen por correo. Frecuentemente, los estafadores usan formularios que tienen una apariencia oficial y un lenguaje que atrae a las víctimas para firmar o enviar pagos. Si recibe artículos por correo que no ha pedido, no tiene ninguna obligación de pagarlos. Está en libertad de desecharlos, devolverlos o quedarlos con ellos.
- Tenga cuidado de mensajes que prometen vacaciones gratis, loterías en el extranjero, ofrecimientos de trabajo en el hogar, inversiones para enriquecerse rápidamente y otros ardidés que pidan donaciones a instituciones de caridad de las cuales nunca ha escuchado. Si está interesado, llame directamente a la compañía. Nunca proporcione información personal en un mensaje electrónico de respuesta.
- Tenga cuidado de ofertas de ofertas baratas de trabajos de reparación en el hogar que de otra forma serían muy costosos. El estafador podría hacer sólo parte del trabajo, usar materiales de baja calidad y trabajadores no capacitados, o simplemente aceptar su depósito y nunca regresar. Nunca pague en efectivo. Nunca acepte ofrecimientos de trabajadores que "justo estaban conduciendo por el vecindario". Si son confiables, regresarán después de que usted verifique sus credenciales.
- Algunos engaños típicos dirigidos a ancianos
- Muchos estafadores eligen a los ancianos como víctimas. Los estafadores urden ofrecimientos complejos que confunden a los destinatarios y finalmente los convencen de aceptar estas ofertas. No deje que lo siguiente le suceda:
 - El teléfono suena y la persona que llama le dice que se ha ganado un automóvil nuevo. Para reclamar el premio necesita mandar por correo un cheque que cubra el monto de los impuestos y el costo de envío. Semanas después, suena nuevamente el teléfono. Usted se entera de que la compañía que originalmente otorgaba los premios ha cerrado, pero la persona que llama le dice que no se preocupe porque su compañía ha adquirido el capital de la compañía que ha dejado de existir. Todo lo que ahora necesita hacer es enviar otro cheque a la nueva compañía para cubrir los costos de las transacciones legales y para que le entreguen inmediatamente el automóvil. Se envía el cheque pero el premio nunca llega.
 - Una oferta por correo o un aviso publicitario llama su atención. Promete una cura rápida para el cáncer, la artritis, la pérdida de memoria, el dolor a la espalda u otras dolencias. Se leen testimonios como "Es un milagro absoluto", "Me siento un millón de veces mejor". Usted envía su cheque por correo para adquirir un suministro para seis semanas de esta cura milagrosa

negocios (Better Business Bureau) o su oficina local de asuntos del consumidor para obtener más información.

Registre su número telefónico en la Lista Nacional de Teléfonos para No Recibir Llamadas de Telemarketeo (National Do Not Call Registry), en www.donotcall.gov.

Recuerde, usted tiene el derecho, la capacidad y el poder de decir ¡no! Si la persona que llama le inspira desconfianza, sea firme y termine la conversación. Los estafadores saben que entre más tiempo permanezca usted en el teléfono, más alta es su probabilidad de éxito. Al decir "no" y colgar el teléfono, está impidiendo la comisión de un delito.

- Corrija por escrito todos los errores que encuentre en su reporte de crédito. Envíe una carta a las agencias de reporte de crédito identificando los problemas, uno por uno. Incluya una copia del reporte de crédito y envíe la carta solicitando un comprobante de entrega.
- **Qué hacer cuando usted es la víctima**
- Si usted es víctima de robo de identidad, la Comisión Federal de Comercio (Federal Trade Comisión – FTC) recomienda que haga lo siguiente:
 - Póngase en contacto con el departamento de fraude de las tres agencias de crédito principales para colocar una alerta de fraude en su archivo de crédito. La alerta de fraude pide a los acreedores que se pongan en contacto con usted antes de abrir alguna cuenta nueva o de hacer cambios a sus cuentas existentes.
 - Cierre las cuentas que sepa o crea que han sido adulteradas o abiertas fraudulentamente. Use la Declaración Jurada de Robo de Identidad (disponible en el sitio web de FTC y aceptada por las tres agencias de crédito principales) cuando se dispute cuentas nuevas no autorizadas.
 - Presente una denuncia policial. Obtenga una copia de la denuncia para presentarla a los acreedores y a otras personas que puedan necesitar prueba del delito.
 - Presente su queja a la FTC en www.consumer.gov/idtheft. La FTC mantiene una base de datos de casos de robos, que es usada por las agencias del orden público en sus investigaciones. Presentar una queja también ayuda a la agencia a saber más sobre el robo de identidad y los problemas que enfrentan las víctimas para que puedan ayudarlo de una mejor manera.

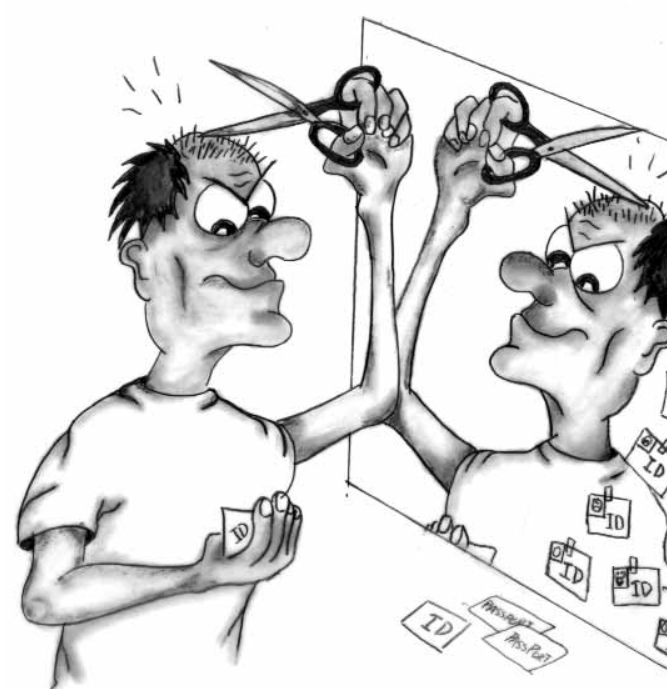


Consejos para prevenir delitos del

NATIONAL CRIME PREVENTION COUNCIL
 1000 Connecticut Avenue, NW
 Thirteenth Floor
 Washington, DC 20036-5325
 202-466-6272
www.ncpc.org

y de

Robo de identidad



La Campaña Nacional de los Ciudadanos para la Prevención del Crimen (The National Citizens' Crime Prevention Campaign) patrocinada por la Coalición Estadounidense para la Prevención del Crimen (Crime Prevention Coalition of America) y financiada principalmente por la Dirección de Asistencia Judicial (Bureau of Justice Assistance), Oficina de Programas de Justicia (Office of Justice Programs), Departamento de Justicia de los EE.UU.



La producción de este folleto fue posible gracias a una subvención de ADT Security Services, Inc., Tyco International Ltd. Company.

NATIONAL CRIME PREVENTION COUNCIL



LET US KNOW WHAT YOU THINK!

CRIME PREVENTION MONTH ACTION KIT

Please take a moment to answer these questions. Then fold this card, tape it, and mail it. Your comments will help us prepare for Crime Prevention Month 2006 and you will also receive a coupon for 25 percent off your total next order.

WHAT IS THE POPULATION OF YOUR COMMUNITY?

- Less than 25,000 25,000–100,000
 100,000–200,000 More than 200,000

WHAT TYPE OF GROUP IS USING THIS KIT?

- Business Community Group Government
 Law Enforcement Library Neighborhood Watch
 School Youth Service Other

DO YOU LIKE THE CALENDAR?

- Very much A lot Somewhat
 A little Not very much Not at all

HOW HELPFUL ARE THESE FEATURES?

	SLIGHTLY HELPFUL		EXTREMELY HELPFUL		
	1	2	3	4	5
Monthly Strategies	1	2	3	4	5
Reproducible Brochures	1	2	3	4	5
Web Resources	1	2	3	4	5
NCPC Resources	1	2	3	4	5
McGruff Licensing Program	1	2	3	4	5
Common Scams and Schemes	1	2	3	4	5
Press Release	1	2	3	4	5
Proclamation	1	2	3	4	5

WHICH CAMERA-READY MATERIALS INCLUDED IN THIS YEAR'S CALENDAR DO YOU THINK YOU WILL REPRODUCE AND DISTRIBUTE?

EXPECT TO USE?

YES NO # OF COPIES

- _____ Protecting Your Private Information
 _____ Ten Tips To Secure Your Personal Computer
 _____ Working Safely at Home
 _____ Online Auction Fraud
 _____ A Family Guide to Using the Internet
 _____ Protecting Yourself From Counterfeit Drugs
 _____ Shopping Safely Online
 _____ Use Common Sense To Spot a Con Artist
 _____ Preventing Charity Fraud
 _____ Identity Theft
 _____ Don't Be Scammed!
 _____ Reporting Crime Online
 _____ Protect Yourself from Telephone Fraud
 _____ Kids: Be a Good Cyber Citizen
 _____ How To Avoid Being Stalked in Cyberspace
 _____ Protección de su información privada
 _____ Use el sentido común para detectar a un estafador
 _____ Robo de identidad

Cómo ocurre el robo de identidad

El robo de identidad es la apropiación de la identidad de la víctima para obtener crédito y tarjetas de crédito de los bancos y comerciantes al por menor, robar dinero de las cuentas existentes de una víctima, pedir préstamos, establecer cuentas con compañías de servicios públicos, alquilar un departamento, declararse en bancarrota u obtener un empleo usando el nombre de la víctima. Se pueden robar miles de dólares sin que la víctima se entere por meses, e incluso por años.

Todo lo que necesita el ladrón de identidad es cualquier combinación de número de Seguro Social, fecha de nacimiento, domicilio y número de teléfono. Esto hace posible crear una licencia de conducir falsa y luego presentarse como si fuera usted para pedir crédito. El ladrón de identidad puede presentar un cambio de domicilio a una compañía de tarjetas de crédito, de manera que usted no sabrá que otra persona está acumulando cargos. Una vez que un ladrón de identidad abre una cuenta, es más fácil abrir una segunda y una tercera.

Los ladrones de identidad pueden obtener información sobre usted de médicos, abogados, escuelas, compañías de seguros de salud y otros lugares. Pueden recoger la información personal que tiró a la basura, como cuentas de servicios públicos, recibos de tarjetas de crédito y estados

Cómo impedir el robo de identidad

- Proteja su computadora de intrusos de Internet usando sistemas como cortafuegos (firewalls). También use software antivirus y manténgalo al día.
- Pase por la máquina desbarradora todos los documentos que esté desechando, incluyendo aplicaciones de crédito preaprobadas, formularios de seguros, cheques bancarios, estados de cuenta y cualquier otra información financiera.
- Reduzca los documentos de identidad y el número de tarjetas que lleve con usted. Lleve consigo sólo lo que realmente necesite.
- No incluya su número de Seguro Social en sus cheques o recibos de crédito. Si alguna compañía le pide su número de Seguro Social déle un número alterno.
- Sea cuidadoso cuando use las máquinas ATM y tarjetas telefónicas para llamadas de larga distancia. Alguien puede estar observándolo y obtener sus números PIN.
- Haga una lista de todos sus números de cuentas de tarjetas de crédito y números de cuentas bancarias incluyendo los números telefónicos de servicio al cliente, y manténgalos en un lugar seguro.
- Si solicita una nueva tarjeta de crédito y no llega dentro de un período adecuado de tiempo, llame para asegurarse de que nadie haya presentado un cambio de dirección en su nombre.
- Nunca proporcione su número de tarjeta de crédito a un sitio web a menos que esté codificado criptográficamente en un sitio seguro. Busque el símbolo de candado en la parte inferior de su pantalla. No seleccione la opción de guardar su información en el sitio para transacciones futuras.
- Preste atención a sus ciclos de facturación. Haga llamadas de seguimiento a los acreedores si las facturas no llegan a tiempo. Una factura extraviada de alguna tarjeta de crédito podría significar que un ladrón de identidad ha tomado posesión de su cuenta de crédito y ha cambiado su dirección.
- Cancele todas las tarjetas de crédito que no ha usado en los últimos seis meses.
- Por lo menos dos veces al año solicite su reporte de crédito de las tres principales agencias de crédito: Equifax (www.equifax.com), Experian (www.experian.com), and Trans Union (www.transunion.com). La Ley del Reporte Justo de Crédito (Fair Credit Reporting Act) le permite obtener un reporte de crédito gratis de cada una de las tres principales agencias de crédito una vez al año. Visite www.annualcreditreport.com.

ARE THERE OTHER CRIME PREVENTION MATERIALS YOU
WOULD LIKE TO SEE IN NEXT YEAR'S KIT?

ADDITIONAL COMMENTS:

FOLD
HERE

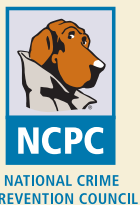
FOLD
HERE

FOLD
HERE

FOLD
HERE

PLACE
STAMP
HERE

ATTN: CRIME PREVENTION MONTH ACTION KIT 2006
NATIONAL CRIME PREVENTION COUNCIL
1000 CONNECTICUT AVENUE, NW
THIRTEENTH FLOOR
WASHINGTON, DC 20036 -5325



The National Crime Prevention Council (NCPC) is a private, nonprofit tax-exempt [501(c)(3)] organization whose primary mission is to enable people to create safer and more caring communities by addressing the causes of crime and violence and reducing the opportunities for crime to occur. NCPC publishes books, kits of camera-ready program materials, posters, and informational and policy reports on a variety of crime prevention and community-building subjects. NCPC offers training,

technical assistance, and a national focus for crime prevention: it acts as secretariat for the Crime Prevention Coalition of America, a nonpartisan group of more than 300 national, federal, state, and local organizations committed to preventing crime. It hosts a number of websites that offer prevention tips to individuals, describe prevention practices for community building, and help anchor prevention policy into laws and budgets. It operates demonstration programs in schools, neighborhoods, and entire jurisdictions and takes a major leadership role in youth crime prevention and youth service; it also administers the Center for Faith and Service. NCPC manages the McGruff® "Take A Bite Out Of Crime®" public service advertising campaign. NCPC is funded through a variety of government agencies, corporate and private foundations, and donations from private individuals.



This publication was made possible through Cooperative Funding Agreement No. 2002-DD-BX-K004 from the

Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. Opinions are those of NCPC or cited sources and do not necessarily reflect U.S. Department of Justice policy or positions. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.



Distribution was made possible in part by a generous grant from ADT Security Services, Inc. (a unit of Tyco Fire & Security Services, a corporate partner of the National Crime Prevention Council).

ACKNOWLEDGMENTS

Principal Writer: Caroline Barnes
Design: MediaPlus Design
Crime Prevention Coalition of America
Reviewers: Tibby Milne, Robert Douglas,
Patrick Harris, Ernest Long, Nancy
Matson, Daryl Pearson, and Robert Rowe

SPECIAL THANKS

A special thanks to Donald Cook, NCPC vice president; Darryl Jones, NCPC vice president; and Paul Steiner, senior policy advisor for crime prevention, Bureau of Justice Assistance, for their expertise and continued support in the writing and publication of this document.

Copyright© 2005 National Crime Prevention Council. All rights reserved, except that this calendar and the accompanying single-sheet materials may be reproduced in whole or in part with proper attribution so long as the reproductions are for nonprofit use and not for sale or resale.

Printed in the United States of America, July 2005.

L-4729-06
ISBN 1-59686-008-1

