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.

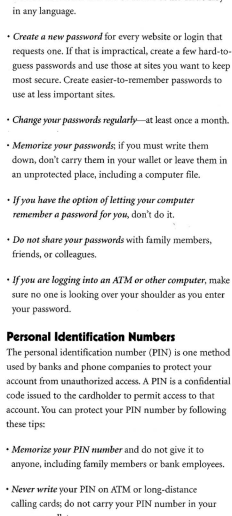
Using a technique called phishing, criminals send spam emails to consumers asking them to update their account information by clicking on a link to the company's website. The website looks like the real thing but is bogus and allows the criminals to steal any personal information that a consumer enters. 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.

Internet Crime Complaint Center
www.ic3.gov

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.

Protecting Your Private Information



NATIONAL CRIME PREVENTION COUNCIL

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

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.

Personal Identification Numbers

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.

Social Security Numbers

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.

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.

NCPC

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

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.

tyco Fire & Security ADT

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