



## 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.**

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](http://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).

## 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 bestsellers, 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 cyber-smart 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 birthdate 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 emails and records of any phone conversations.



Crime Prevention Tips From

### NATIONAL CRIME PREVENTION COUNCIL

1000 Connecticut Avenue, NW  
Thirteenth Floor  
Washington, DC 20005-5325  
202-462-6272  
[www.ncpc.org](http://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



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