



Internet Fraud



Many legitimate companies sell their products or services through the Internet. Charities use the Internet to ask for donations. Unfortunately, fraudulent companies and individuals also understand that the Internet is a great way to reach people—and use it to rob them.

- **Know who you're dealing with.** If the seller or charity is unfamiliar, check with your state or local consumer protection agency and the Better Business Bureau. Some Web sites have feedback forums, which can provide useful information about other people's experiences with particular sellers. Get the physical address and phone number in case there is a problem later.
- **Look for information about how complaints are handled.** It can be difficult to resolve complaints, especially if the seller or charity is located in another country. Look on the Web site for information about programs the company or organization participates in that require it to meet standards for reliability and help to handle disputes.
- **Be aware that no complaints is no guarantee.** Fraudulent operators open and close quickly, so the fact that no one has made a complaint yet doesn't mean that the seller or charity is legitimate. You still need to look for other danger signs of fraud.
- **Don't believe promises of easy money.** If someone claims that you can earn money with little or no work, get a loan or credit card even if you have bad credit, or make money on an investment with little or no risk, it's probably a scam.
- **Understand the offer.** A legitimate seller will give you all the details about the products or services, the total price, the delivery time, the refund and cancellation policies, and the terms of any warranty. For more information about shopping safely online, go to www.nclnet.org/shoppingonline.
- **Resist pressure.** Legitimate companies and charities will be happy to give you time to make a decision. It's probably a scam if they demand that you act immediately or won't take "No" for an answer.
- **Think twice before entering contests operated by unfamiliar companies.** Fraudulent marketers sometimes use contest entry forms to identify potential victims.
- **Be cautious about unsolicited emails.** They are often fraudulent. If you are familiar with the company or charity that sent you the email and you don't want to receive further messages, send a reply asking to be removed from the email list. However, responding to unknown senders may simply verify that yours is a working email address and result in even more unwanted messages from strangers. The best approach may simply be to delete the email.
- **Beware of imposters.** Someone might send you an email pretending to be connected with a business or charity, or create a Web site that looks just like that of a well-known company or charitable organization. If you're not sure that you're dealing with the real thing, find another way to contact the legitimate business or charity and ask.
- **Guard your personal information.** Don't provide your credit card or bank account number unless you are actually paying for something. Your social security number should not be

necessary unless you are applying for credit. Be especially suspicious if someone claiming to be from a company with whom you have an account asks for information that the business already has.

- **Beware of “dangerous downloads.”** In downloading programs to see pictures, hear music, play games, etc., you could download a virus that wipes out your computer files or connects your modem to a foreign telephone number, resulting in expensive phone charges. Only download programs from Web sites you know and trust. Read all user agreements carefully.
- **Pay the safest way.** Credit cards are the safest way to pay for online purchases because you can dispute the charges if you never get the goods or services or the offer was misrepresented. Federal law limits your liability to \$50 if someone makes unauthorized charges to your account, and most credit card issuers will remove them completely if you report the problem promptly. There are new technologies, such as “substitute” credit card numbers and password programs, that can offer extra measures of protection from someone else using your credit card. For more information about paying safely online, go to www.nclnet.org/shoppingonline and www.nclnet.org/essentials/security.html