



CANTON POLICE DEPARTMENT
1150 S. Canton Center Road, Canton, MI 48188
www.canton-mi.org/publicsafety

Crime Prevention Unit
734/394-5424

Internet Fraud

Criminals are recognizing the vast potential of cyberspace. Many of the same scams or frauds that for years have been conducted by mail or phone can now be found on the Internet.

The following are examples of the most frequent types of Internet fraud:

- **Internet and Online Services**

Free Internet access was promised with the purchase of software that was never provided. Consumers paid for a password to access pictures but never received it. Or people downloaded a viewer to see pictures and were hit with undisclosed international telephone charges. A breeder paid to place ads on a Web site for dogs she raises, never got the ads, and the company is now out of business.

- **General Merchandise**

Sales via unsolicited e-mails, newsgroup postings, chat room discussions, Web sites, online classified advertisements for everything from T-shirts to toys, calendars to collectibles: the merchandise was not delivered, arrived in damaged condition, was defective or was misrepresented. I wouldn't buy from a company online whose good reputation I didn't know from other sources of information.

- **Auctions**

Offers through Internet auction Web sites for antiques, new and used computer equipment, videos, games, etc.: the sellers never delivered the items or misrepresented their value. "Shills" were used to drive up bids. Sellers tried to raise prices after the highest bids were made.

- **Pyramids and Multilevel Marketing**

Pyramid schemes are similar to multi-level marketing. Pyramid schemes provide financial incentives to recruit new distributors. They are generally prohibited because it is a mathematical certainty that the pyramid will collapse when no new distributors can be recruited. When that happens, most people lose their money. The Internet offers a fast lane for pyramid builders by facilitating a large-scale recruitment pool in little or not time.

- **Business Opportunities and Franchises**

Investments are made in "Internet malls" that advertise goods or services in cyberspace. The buyer may purchase ATM machines that will supposedly be leased back to the seller and generate profits for buyers. The potential earnings from this scheme are misrepresented or unsubstantiated; promised business assistance is never provided.

- **Work-at-Home Schemes**

In the old "envelope stuffing" schemes, consumers are told they will be paid for addressing envelopes, but they actually receive instructions on how to sell others information on how they can make money stuffing envelopes. There are false promises of working as an answering service or approving credit card applications. Computer-related

- work-at-home scams may require the purchase of equipment or software to produce things like computer graphics that will supposedly be bought by companies.
- **Prizes and Sweepstakes**
Win a free trip with payment of a registration fee, but you are required to buy a companion ticket at full price. The prize in an online contest turns out to be a discount price on a satellite service package. The consumer supposedly wins cash but is asked for his or her bank account number. Alleged “sweepstakes” winnings require an advance fee to collect.
 - **Credit Card Offers**
Credit cards are offered on Web sites and via unsolicited e-mail despite bad credit, if the consumer pays an advance fee. Fees of as much as \$100 are paid, but the credit cards are never received.
 - **Books**
Manuals on how to hypnotize people; listings of celebrities’ phone numbers and addresses; books on how to stop paying taxes, speed reading kits, and other self-help guides that are never delivered.
 - **Magazine Subscriptions**
Magazines are never received from companies falsely representing themselves as subscription services for well-known magazine publishers. Consumers outside of the U.S. are offered club memberships to get magazines at lower prices than normal foreign rates. Vendors make other false claims of discounts and sometimes debit consumers’ bank accounts more than once when only one debit was authorized.
 - **The Hijack**
The “Hijack” is a relatively new form of Internet-related fraud. Consumers are prompted to download a purported “viewer program” to see computer images for free. Once downloaded, the consumer’s computer is “hijacked” by the viewer program which turns off the consumer’s modem speakers, disconnects the computer from the local Internet provider, dials an international number and connects the consumer to a remote site. The expensive international costs are charged to the consumer’s telephone bill until the telephone is turned off.

Tips for Avoiding Internet Fraud

- **Do business with those you know and trust.** Be sure you know who the company or person is and where it is physically located. Businesses operating in cyberspace may be in another part of the country or in another part of the world. Resolving problems with someone unfamiliar can be more complicated in long-distance or cross-border transactions.
- **Understand the offer.** Look carefully at the information about the products or services offered, and ask for more information, if needed. A legitimate business will be glad to provide it; a fraudulent telemarketer won’t. Be sure you know what is being sold, the total price, the delivery date, the return and cancellation policy, and the terms of any guarantee. The federal telephone and mail order rule, which also covers orders by computer, requires goods or services to be delivered by the promised time or, if none was stated, within thirty days. Print out the information so that you have documentation.
- **Check out the company’s or individual’s track record.** Ask your state or local consumer protection agency if the business has to be licensed or registered, and check to see if it is. Call to check for complaint records with consumer agencies and the Better Business Bureau in your area. But keep in mind that fraud artists can appear and disappear quickly, especially in cyberspace, so lack of a complaint record is no guarantee of legitimacy.
- **Never give your bank account numbers, credit card numbers or other personal information** to anyone you don’t know or haven’t checked out. And don’t provide information that isn’t necessary to make a purchase. Even with partial information, con

artists can make unauthorized charges or take money from your account. If you have a choice between using your credit card and mailing cash, check, or money order, the League recommends using a credit card. You can always dispute fraudulent credit card charges, but you can't get cash back.

- **Take your time.** While there may be time limits for special offers, high-pressure sales tactics are often danger signs of fraud.
- **Don't judge reliability by how nice or flashy a web site may seem.** Anyone can create, register, and promote a web site; it's relatively easy and inexpensive. And just like any other forms of advertising, you can't assume that someone has screened and approved it.
- **Know that people in cyberspace may not always be what they seem.** Someone who is sharing a "friendly" tip about a moneymaking scheme or great bargain in a chat room or on a bulletin board may have an ulterior motive: to make money. Sometimes friendly people are crooks!
- **Know that unsolicited e-mail violates computer etiquette and is often used by con artists.** It also violates most agreements for Internet service. Report "spamming," as unsolicited e-mail is called, to your on-line or Internet service provider.
- **Don't download programs to see pictures, hear music, or get other features from web sites you're not familiar with.** You could unwittingly download a virus that wipes out your computer files or even hijacks your Internet service, reconnecting you to the Net through an international phone number, resulting in enormous phone charges.