INTERNET SCAM GUIDE

Web of Lies:
How to protect yourself on the Infohighway

The New York City Department of Consumer Affairs

WEB OF LIES: How to protect yourself on the Infohighway

The Internet is becoming a big part of our everyday lives. But there are no gatekeepers on the "information superhighway."

New, unregulated technology means new opportunities for consumers, investors, businesses — and for scam artists.

The rise of Internet use brings more deceptive and misleading promotions, bogus travel offers, contests, lotteries, and other illegal practices on the Web.

The scams aren't new, but on the Internet, scams can be more dangerous than ever. Unlike print advertising, impressive-looking Web sites can be designed relatively easily and affordably. Remember, just because an advertisement on the Internet appears to be professional does not mean it's legitimate.

The bottom line: don't believe Internet ads. Consumers are just as likely to be scammed online as through more "traditional" types of advertising.

Anti-scam rules

- Don't judge a Web site by how it looks.
- Remember that people in cyberspace are not always what they seem.
- Take your time to decide.
- Understand the offer.
- Check out the company's track record.
- Be careful about giving out your financial or other personal information.
- Do not respond to bulk e-mails. If they don't know you, keep your distance.
- Beware of investing money in an opportunity you learn about over the Internet.
- Make sure the company has a phone number and a physical address – not just a post office box or e-mail address.
- Always use common sense. If you have a gut feeling that something is not legitimate, you're probably right.
- Instruct your children NEVER to give out any personal information over the Internet, such as whole names, addresses, phone numbers, school names or photographs.
- Instruct your children to tell you about — and not respond to — any messages they read that make them feel uncomfortable.
- Do not take other users' identities for granted. Online user profiles and personal information provided by others could be more fiction than fact.
- When first joining a chat room or news group, read along for a while before joining the conversation to get a feel for the discussion and participants. If the newsgroup or chat room has a charter or FAQ ("Frequently Asked Questions"), read it before joining in.

- E-mail is not always private. Most e-mail is read by the sender and recipient only, but in rare cases others may have access to it. Also, one incorrect letter in an e-mail address can send the message to the wrong recipient. Your message can be forwarded on to others intentionally or inadvertently. Unless you are encrypting your e-mail, it's no more private than a postcard.

- When providing credit card information, make sure it is sent to a secure server. Use of secure servers is automatic in major Web browsers, and most Web sites that support them will clearly mark that option. Make sure you get a message that a secure server is in use before sending information.

- Protect your password. People can use your online password to log on to your Internet account, send mail from it or otherwise run up expenses. Use a combination of letters, numbers and symbols for your password, change it frequently and do not share it with anyone.

- Be careful about making purchases with ATM/Debit cards — they are not afforded the same protection as a credit card.

WATCH OUT FOR THESE POPULAR SCAMS ON THE INTERNET:

Computer Equipment Sales

An Internet site may offer great deals on computers, RAM, hard drives and multimedia equipment — and deliver shoddy material, or nothing at all.

DON'T BE FOOLED BY TECHNO-TALK. Sellers will often try to intimidate you with useless information, or comparisons that don't make sense. Sometimes they fail to disclose that certain vital components, such as the monitor, are not included in the advertised price. The better the deal, the more wary you should be.

Do some research to LEARN COMPUTER TERMS. Many magazines and newspapers run articles with up-to-date advice for computer buyers. Talk with friends and coworkers who may have recently purchased computers.

If you buy online, be sure to SEE THE WARRANTY before you buy. It contains important information about your rights if a problem does arise.

"Free Trial" Offers

Watch out for "free trial" evaluation period offers. You may incur charges during the "free trial." And when the "free" membership period ends, YOU MAY BE AUTOMATICALLY CHARGED a monthly fee. If you don't want to continue the service, be sure to cancel it at the end of the trial period!

Read the fine print before signing up for "free hours." Often those "free hours" must be used within the first 30 days — then they expire. WATCH OUT FOR "PREMIUM SERVICES," such as stock transactions, for which you may be charged during your "free trial" period.

The membership fee does not cover the telephone charges for connecting to the service. Contact your telephone company to CONFIRM THAT YOUR "DIAL-UP" CONNECTION IS A LOCAL NUMBER.

Pyramid scams

When on the Web, you can protect yourself against multilevel marketing ("pyramid") schemes.

Check to be sure the promotion is based on the SALE OF A PRODUCT AT THE RETAIL LEVEL, which is legitimate, or if it's based on RECRUITING MORE AND MORE DISTRIBUTORS to help you increase your income, which is illegal.

Pyramid scams may be disguised as games, chain letters, buying clubs, motivational companies, mail order operations, or investment organizations. The entrance fee into the pyramid usually is very high. The pyramid collapses when new people stop coming in. Those who join later in the scheme take the loss. In many cases, your money is lost the moment you pay.

The Traditional "Work-at-Home" Scam

Work-at-home opportunities on the Internet are no way to make money.

Flashy Internet ads typically promise a "large income" for working on projects "in great demand."

Here are the telltale signs of a work-at-home swindle:

- They never offer you regular salaried employment.
- They promise you huge profits and big part-time earnings.
- They use personal testimonials but never identify who made them.
- They require money for instructions or merchandise before telling you how the plan operates.
- They assure you of guaranteed markets and a huge demand for your handiwork.
- They tell you that no experience is necessary.

In the most common work-at-home scheme — envelope stuffing — all you get for your money are instructions to place an ad like the one that was answered. Once recruited, the only way workers make any money is to recruit other would-be workers.

Some schemes don't really offer work in the home, but sell ideas for setting up home businesses. This often involves selling you materials for making low-demand items that you will have to sell on your own. THE PROMOTERS TAKE YOUR MONEY BUT NEVER RETURN THE PROMISED "EMPLOYMENT OPPORTUNITIES."

Avoid them. They will rip you off.

Internet Telephone Scams

Are you finding huge international call charges on your long distance bill? Some Web sites, offering special software programs in order to see content, fleece customers through international dialing. The sites claim to be "free" or advertise that "no credit card is needed," then prompt the user to download a "viewer" or "dialer" program.

Here's the catch: Once the program is downloaded to the user's computer, it disconnects the Internet connection and reconnects to an international long-distance phone number, at rates between $2 and $7 a minute.

These scams, typically associated with adult sites, don't require a credit card number for access. That means they are available to children, who can click onto them without their parents' knowledge or permission. Even if parents disable international calling from their phone lines, many modem dialers are programmed to circumvent the "block," and initiate international calls using a "10-10 dial-around" prefix.

Follow these guidelines:

1. If you see a dialog box on your computer indicating that it's dialing when you didn't direct it to, cancel the connection and hang up. Check the number you're dialing and continue only if it's a local call.
2. Be sure your Internet Service Provider uses dial-up numbers in your area code.
3. Read online disclosures carefully. They may be buried several clicks away in pages of small print. In addition, carefully scroll through the language in the typical gray boxes on your screen. Don't click on "OK" unless you know exactly what you're agreeing to.
4. Talk to your children. They are obvious targets of international modem dialing scams. Tell them why they can't download "viewer" or "dialer" programs on the computer.
5. Monitor your children's Internet use. Keep track of the Web sites your child visits by checking the Web browser history files and cache.
6. Remember that on the Web, "free" offers can cost you plenty.
7. Take action if you find charges on your phone bill that you didn't authorize. Contact the Federal Trade Commission, toll-free, at 1-877-FTC-HELP (1-877-382-4357), or use the complaint form at **www.ftc.gov.**
8. Save your phone bill. If you think you've been a victim of international modem dialing, it may help identify the scammers.

Web Auction Scams

Look out for these Internet auction frauds:

Non-delivery – The seller places an item up for bid when in fact there is no item at all. If you buy by credit card, the seller obtains your payment, name and credit card number and you get nothing.

Misrepresentation – The seller lists false information about the item that is up for bid.

Triangulation – The perpetrator buys merchandise online using stolen identities and credit card numbers. Then, the perpetrator sells the merchandise at online auction sites to unsuspecting bidders. Next, the perpetrator has the buyer wire-transfer him the money and then sends the merchandise to the buyer. Later the police question the unsuspecting buyer and collect the stolen merchandise to keep for evidence. The buyer pays and loses the merchandise, and the merchant gets nothing.

Fee stacking – The seller adds hidden charges to the item after the auction is over. Instead of a flat rate for postage and handling, the seller adds separate charges for postage, handling and the shipping container.

Black-market goods – Some sellers offer black-market software, music CDs, videos, etc., for sale on Internet auction sites. The goods are delivered without a box, warranty or instructions.

Multiple bidding – A buyer using different aliases places many bids, some high and some low, on the same item. The multiple high bids by the same buyer cause the price to escalate, which scares off other potential buyers from bidding. Then in the last few minutes of the auction, the same buyer withdraws the high bids, only to purchase the item at a much lower price.

Shill bidding – This is intentional fake bidding by the seller to drive up the bidding price of his/her own item.

Travel Scams

If you get an e-mail that you've won a dream vacation, it may be a "trip trap."

The "bargain-priced" luxury travel package you are offered over the telephone or Internet may ruin your vacation.

Travel scams usually originate out of "boiler rooms," fly-by-night operations devoted to telephone sales rip-offs. Skilled salespeople will offer you travel packages that may sound legitimate, but often are not. These pitches usually include:

- written misrepresentations
- high pressure/time pressure tactics ("You must buy now")
- "affordable" offers
- contradictory follow-up material

The word "offer" can be a clue to hidden charges. The salesperson may ask for your credit card number to bill your account for the travel package. Once you pay, you receive the details of the "package," which usually include instructions for making trip reservation requests.

You may then be asked to pony up yet another fee. Many offers require you to pay upgrade costs to receive the actual destinations, accommodations, cruises or dates you were promised. Some offers may require you to pay more for port charges, hotel taxes or service fees.

Bottom line: do your homework before responding to promises that pop up on the Internet.

Credit Fixing Scams

By federal law, any offer made by an Internet credit repair or analysis service must be written in detail before you make any agreement. This law applies to state or interstate companies, operating by telephone or any other means. (This does not apply to nonprofit organizations, banks and credit unions, and creditors themselves.)

No agreement is binding unless there is a written contract signed by the buyer.

You have three business days to cancel.

The company cannot ask for payment before the promised services have been fully performed.

Chain Letters and Urban Legends

E-mail is a new frontier for con artists.

You get an e-mail asking you to send a small amount of money (or some item) to each of four or five names at the top of a list, and then forward the message, including your name at the bottom, via bulk e-mail. Then you never hear from them again.

Nearly everyone who participates in these chain letters loses money.

Another scam is the "urban legend" e-mail about people in need (usually children) who are crippled or have been injured in a horrible accident and "need your help." They usually ask you to send money to a certain address in order to help the child. The letters seem like real tragic stories, but more often than not are completely false.

NEVER RESPOND TO AN INTERNET APPEAL FOR MONEY FROM STRANGERS.

Medical Rip-offs

Consumers who have serious or chronic illness should be wary of Internet ads and Web sites hawking therapeutic products or services.

Watch out for:

- Claims that a product is a "scientific breakthrough," "miraculous cure," "secret ingredient" or "ancient remedy."
- Claims that the product is an effective cure for a wide range of ailments. No product can cure multiple conditions or diseases.
- Claims that use impressive-sounding medical terms. They are often covering up a lack of good science.
- Undocumented case histories of people who have had amazing results. These are easy to make up, and even if true, they cannot be generalized to the entire population. Anecdotes are not a substitute for valid science.
- Claims that the product is available from only one source, and payment is required in advance.
- Claims of a "money-back" guarantee.
- Claims that the medical profession or research scientists are conspiring to suppress the advertised product to keep their market share.
- Web sites that fail to list the company's name, physical address, phone number or other contact information.

Report anything suspicious you see on the Internet or any online service location to:

The National Fraud Information Center
PO Box 65868
Washington, DC 20035
(800) 876-7060

What to do if you're scammed

If you have been scammed, call **3-1-1** or contact:

New York City Department of Consumer Affairs
42 Broadway
New York, NY 10004

Federal Trade Commission
www.ftc.gov
(877) FTC-HELP

New York State Attorney General
120 Broadway
New York, NY 10271
(212) 416-8345

If you have been scammed through the mail, contact:

United States Postal Inspection Service
James A. Farley Building
PO Box 2762
New York, NY 10116-2762
(212) 330-3900
fax (212) 330-3355

If you have been victim to an online investing scam, contact:

U.S. Securities and Exchange Commission
www.sec.gov
(202) 942-7040

Michael R. Bloomberg
Mayor

Department of Consumer Affairs

Jonathan Mintz
Commissioner

The New York City Department of Consumer Affairs works to ensure that consumers and businesses benefit from a fair and vibrant marketplace.

If you would like more information about the work of the agency or our new strategic initiatives, please call **3-1-1** or contact:

New York City Department of Consumer Affairs
42 Broadway, New York, NY 10004-1617
www.nyc.gov/consumers

If you have a consumer-related complaint, call DCA at 311 or (212) NEW-YORK.

New York City employees are not allowed to ask for or accept anything of value, such as money, gifts, or tips for doing their job. To report corruption, contact the NYC Department of Investigation at www.nyc.gov/doi.