

Internet Frauds and Scams Tip Sheet

The Internet has become a widely used method of selling and purchasing items. Many legitimate companies sell products and services online. However, because it is inexpensive and affords a level of anonymity, there are also many fraudulent companies and individuals using the Internet as a vehicle to lure and scam people.

Here are some of the most common scams and frauds you may face when using the Internet.

“Get-Rich-Quick” Schemes

The Internet is full of claims to get rich quickly and easily. If it sounds too good to be true, it most likely is!

Business Opportunities/Work-at-Home Offers

These offers promise quick, maximum income for minimal labor at no risk—and the convenience of working from home. Often you are enticed to send money for products to sell, or instructional materials, but you never receive the goods. You may also be required to pay hidden costs to place newspaper ads, make photocopies, or buy supplies, software, or equipment to do the job. Once you complete your assignment, you may find that your employers refuse to pay you, claiming that your work isn't up to their “standards.”

Foreign Lotteries

Foreign lottery e-mails boast incredible odds and large payouts. The e-mail may even claim that you've already won, and all you must do is pay to collect your winnings. It's illegal for a company to require you to buy something or pay a fee in order to win or claim a prize. Besides being terribly risky, participating in a foreign lottery violates U.S. law.

Online Auctions

You can find almost anything at an online auction. However, sellers may not hold up their side of the bargain, or merchandise may have been misrepresented.

Charity and Disaster-Related Scams

Fraudulent charities often appeal to your patriotism and take advantage of disasters to trick people who want to help victims. Some crooks try to fool people by using names similar to those of well-known charities to tug at your heart strings and convince you to help the less fortunate.

Nigerian E-mail Scam

These e-mails are from crooks in Nigeria, or another country, who claim they need your help accessing money being held in a foreign bank. Their purpose is to steal your money or commit identity theft. If you assist them in accessing their money, they will transfer lots of money into your bank account in payment for assisting them. Inevitably, emergencies come up requiring more of your money and delaying the “transfer” of funds to your account. Ultimately, the scam artist vanishes with your money.

Medicare Rx Drug-Coverage Scam

Con artists are trying to cash in on the new Medicare discount drug card program by offering phony Medicare prescription plans. Their main objective is to steal your money or personal information.

Medical Scams

E-mails claiming that a product is a quick and effective cure for ailments or diseases, and that there's a limited availability, require payment in advance and offer a no-risk, money-back guarantee. Most include testimonials from customers or doctors verifying its effectiveness. All are intended to steal your money or identity.

Credit Card Fraud

Fraudulent credit card offers often promise to repair credit reports for a “fee” or to get credit cards for persons with credit problems. If your credit history is bad, your best bet is to use a well-known bank and get a “secured” credit card to rebuild your credit rating. You can correct inaccurate data on your credit report by contacting the credit-reporting agencies.

Travel Fraud

Fraudulent companies often offer free or low-cost trips to lure people into buying their products or services. A “free” or incredibly cheap trip may have hidden costs or restrictions, require you to use a specific company whose costs are higher, or take your money and never actually place the reservations for your travel.

Internet Frauds and Scams Tip Sheet

i-SAFE has created this list of tips to help you avoid and respond to Internet fraud and scams.

- **Never respond to unsolicited e-mails.**

To stop communications from a company or charity, contact the sender by phone or by going directly to the web page to request that you be removed from their contact list. Never click on links within e-mails or hit reply. Replying often verifies that your e-mail is valid and results in even more unwanted messages from strangers. The best approach may be to delete the e-mail.

- **Beware of imposters.**

Fraud e-mails often pretend to be connected with a business or charity, or have a Web site that looks just like a legitimate company or charitable organization. Contact the legitimate company or charity directly if you are interested in the offer or request.

- **Guard your personal information.**

Never provide personal information, including credit card or bank account numbers, to anyone unless absolutely necessary. Revealing your social security number should never be necessary unless you are applying for credit. Businesses with whom you already have an account will never request information that they should already have. They should not have to verify any information from you via e-mail.

- **Be cautious of file attachments.**

Opening file attachments and downloading files puts you at risk for viruses, spyware, and identity theft. Fraudsters often use spyware to obtain your personal information or download code that connects your modem to a foreign telephone number, resulting in expensive phone charges.

- **Know with whom you're dealing.**

Do your homework: Check out the company or charity by contacting the consumer-protection agency and the Better Business Bureau. Try to get the physical address and phone number in case there is a problem later. Check with Medicare to make sure that the plan you're considering is approved. If buying on an auction site, read the buyer feedback responses to gain useful information about other people's experiences with particular sellers.

- **Stay on guard.**

Be aware that "no complaints" does not mean that a business is legitimate. Fraudulent companies often don't stay in business under one name for long. The fact that there has been no complaint made against a company does not mean it is legitimate.

- **Resist pressure and time-sensitive appeals.**

Legitimate companies and charities don't use pressure or scare tactics to force you to make a decision. If a company or charity demands that you act immediately or is too persistent, it is most likely a scam.

- **Think twice before entering contests.**

Fraudulent marketers sometimes use contest entry forms to identify potential victims.

- **Do not believe promises of large sums of money for your cooperation.**

Why would a total stranger want to make you rich?

- **Monitor your credit report!**

Periodically, check your credit report for accuracy. Maintain a list of all your credit cards and account information along with the card issuer's contact information. If anything looks suspicious or you lose your credit card(s), you should contact the card issuer immediately.

To determine where to report specific Internet crimes, visit <http://www.cybercrime.gov/reporting.htm>, and forward all suspected fraud e-mails to spam@uce.gov.