

“Buy Your Prescription Drugs Online And Save Big Dollars”

Although there are many legitimate mail order pharmacy services, beware of the ones that dispense prescription drugs without a valid prescription. The Federal Food and Drug Administration (FDA) cautions that this is in violation of the Federal Food, Drug and Cosmetic Act and could lead to your receiving counterfeit, tainted or diluted pharmaceuticals.

“We Give You Rock Bottom Prices On Merchandise”

The most common fraud associated with Internet auctions is non-delivery of the merchandise ordered. Try to find out as much information as you can about the seller before bidding, including his physical location. Be cautious about dealing with individuals or companies outside your own country.

Examine comments from past customers who have dealt with the seller, and avoid those with negative feedback.

It's safest to use a credit card for online purchases, or to go through a reputable alternate payment service such as PayPal. But make sure you are on a secure Web site when transmitting credit card information.

The best advice is ... if it seems too good to be true, it probably is!



Presented by the National Association of Federal Credit Unions, an independent trade association representing federally chartered credit unions nationwide.

© 2007 National Association of Federal Credit Unions.

PROTECT YOURSELF FROM INTERNET FRAUD



Internet fraud is on the rise, and scammers are getting more and more resourceful in their methods of trying to dupe the public. Although many scams are obvious, there are other, more subtle fraudulent activities being conducted on the Internet which trap unsuspecting persons every day. The FBI estimates that billions of dollars are being bilked from the public each year through fraud.

The very anonymity of the Internet makes it a popular vehicle for con artists. It can be difficult to trace the source of an e-mail or to determine if a Web site is from a legitimate business.

Here's how to protect yourself from some of the most common Internet scams:

“We Need To Verify Your Financial Information”

If you receive an e-mail that looks like it's from your credit union asking you to verify financial information, don't click on the link to reply. The message probably isn't from your credit union at all! Scammers have become adept at mimicking the look of communication from financial institutions, right down to the financial institution's logo. And the e-mail can be so cleverly worded that it appears you have to reply immediately to protect your assets.

It's best to err on the side of caution and initiate the contact to your credit union through a phone call, using the number provided on your statement. They'll want to know about fraudulent e-mail so they can alert other members.

“A Hot Stock Tip You Can't Afford To Pass Up”

The U.S. Securities and Exchange Commission (SEC) cautions you to do your homework before you invest in any securities or commodities online. Resist pressure from individuals to invest your money before you have the opportunity to investigate it thoroughly. Remember, promise of a high rate of return typically means a high risk.

There is a proliferation of investment newsletters online offering free advice. But beware . . . some companies pay the writers to recommend their stock. The writer's tips are often touted as being based on independent research, when in truth the writer stands to profit from convincing investors to buy or sell particular stocks.

You can find out more information about U.S. companies on the SEC's EDGAR Database at www.sec.gov before making an investment decision.

“Update Your Social Security Information Now To Protect Your Benefits”

That urgent e-mail asking you to update your personal information for a cost-of-living increase is not from the Social Security Administration (SSA) as it says. This is a particularly vicious scam directed at the elderly who tend to be more trusting than younger generations and are more likely to provide the information requested so they don't risk losing their benefits.

In this scam, a link takes you to a phony Web site where you are asked to confirm your identity by providing personal information such as your Social Security number, financial institution account information and credit card information. Don't fall for it. The SSA has all of this information already on file.

“Here's Your Dream Vacation For An Unbelievable Price”

The Federal Trade Commission (FTC) cautions that unsolicited e-mails for deeply discounted travel packages are from companies that rarely deliver on their promises. Buy your vacation package from a business with a proven track record. Call the resort or airlines direct to verify your reservations and arrangements, and get the details of your vacation in writing.

