

March 19th, 2007 - Important E-Mail Fraud Alert

We have just become aware of a scam e-mail that looks like it is from the National Credit Union Association (NCUA) asking you to click a link and enter your Social Security Number and PIN. If you received this e-mail, **it is important that you do not respond.** This e-mail is not from NCUA or Market USA Federal Credit Union. **Market USA Federal Credit Union and any organization affiliated with credit unions will never e-mail you to request your personal information.** The NCUA has posted a response on their web site at www.ncua.gov (under Alerts).

If you have any questions, please contact our Member Service Call Center at 301-586-3400 or 800-914-4268.

Please read the following consumer interest article titled *How to Expose Fraud*. It is full of important information that can help you identify telephone and email scams and keep you safe from fraud.

How to Expose Fraud

There was a time when most scams were quite unsophisticated – an obvious hodgepodge of information that didn't take a rocket scientist to crack. Scammers now send authentic looking emails – complete with professional graphics and authoritative language – designed to dupe you into disclosing pertinent personal information. You will receive an email or even telephone call from what you think is a credible financial institution – it could be your credit union, PayPal, etc. The email or call could also be “from” any store that you shop with like Ebay. Among other things, scammers will request that you verify your email address, password, credit card and pin numbers. Scammers want this information so they can log onto your online account (be it your bank, credit union, Ebay, etc.) drain your account, charge items to your credit card and/or purchase items online.

Email and telephone scams are easy for crooks to orchestrate – they send out hundreds of thousands of emails, make tons of calls and sit back and hope an unsuspecting victim will fall for their ruse. Arm yourself with the following information and avoid becoming a victim.

Detecting email fraud

- **Requesting too much information.** A company that you do business with already has access to needed information. Email is not secure, so no one should ask you for your password, social security number or credit card information in an email.
- **Links to Web sites.** Check to make sure links to Web sites are the same as the name displayed. A scam site could look very similar to the official site and you may not notice you aren't at the official site. To verify the link, click the link; if you are redirected to another Web site, this should be an indication that you have received a fraudulent email.

- **Not enough valid information.** Does the email have important information listed, such as dates, or indicate in any other way that it is not a random email? Is the email addressed directly to you in the body of the email? If not, the same email was probably sent to thousands of other people.
- **Double check with organizations.** Does the email mention a regulatory agency? Find out if the organization listed even exists and, if so, confirm that they are aware of the situation. It is also a good idea to check with official government agencies for known scams. Visit with the Federal Trade Commission and Better Business Bureau Web sites to see what scams are listed there.
- **Give us a call.** Some scam emails ask that you call a telephone number to speak to a representative. Scammers hope you will feel more at ease giving your information to a live person. Before calling a number that is listed on an unsolicited email, go to what you know to be the organization's official Web site and call their official hotline. If the person you reach on the other end knows nothing of the email – you've received a scam email.
- **Multiple emails.** Did you get multiple copies of the email, indicating that it is spam? Spam hits thousands of accounts randomly, and if you get duplicate copies of the same email – it probably isn't legitimate.

Common telemarketing scams

- **Information Requested.** You may receive a call from someone claiming to be from a reputable company. The caller will ask you to verify your sensitive personal information. They may claim to have a special offer for you, as in the case with the bogus Visa Card fraudulently offered to Market USA members.
- **Prize Offers.** You usually have to do something to get your "free" prize, like attend a sales presentation, buy something, pay a fee or give out a credit card number. But the prizes are worthless or overpriced.
- **Travel Packages.** "Free" or "low cost" vacations can end up costing a bundle in hidden costs. You may pay a high price for some part of the package — like hotel or airfare. The total cost may run two to three times more than what you'd expect to pay, or what you were led to believe. Some "bargain" vacations may never happen at all.
- **Investments.** People lose millions of dollars each year to "get rich quick" schemes that promise high returns with little or no risk. These can include movies or cable television production deals, Internet gambling, rare coins, art, or other "investment opportunities." The schemes vary, but one thing is consistent: Unscrupulous promoters of investment fraud rely on the fact that investing may be complicated, and many people don't research the investment process.
- **Charities.** Con artists often push you for an immediate gift, but won't send written information so you can check them out. They also may try to confuse you by using names that sound like well-known charitable organizations or even law enforcement agencies.
- **Recovery Scams.** If you buy into any of the above scams, you're likely to be called again by someone promising to get your money back. Be careful not to lose more money to this common practice. Even law enforcement officials can't guarantee they'll recover your money.

- **Foreign Lotteries.** Scam operators are using the telephone and direct mail to entice consumers to buy chances in high-stakes foreign lotteries from as far away as Australia and Europe. These lottery solicitations violate U.S. law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail. And you may never see a ticket.
- **Direct Mail.** Finally, some crooks initiate further contact through direct mail. You may get a letter or postcard saying you've won a prize or a contest. This often is a front for a scam. The instructions tell you to call or email the promoter with certain information. If you do, you'll be called by someone who may use persuasive sales pitches, scare tactics and false claims to deceive you and take your money.

In general, you should beware of any email or caller requesting information from you. It is better to be safe than sorry – so when in doubt, pick up the phone and call the institution in question to confirm any contact you receive. Reputable companies want you to feel secure, so they will have no problem helping you. By calling a company, you may even alert them to scams involving their good names. They can then take measures to protect their customers, such as issuing press releases and notifying authorities. And remember, if you happen to get an offer that sounds too good to be true – it probably is.

Source: Federal Trade Commission