

## SCAM ALERT

Always check your debit card purchase store receipts very carefully. There have been rumors in our area of possible store cashiers who are using the "cash back" option and pocketing the money. These may be just rumors, however; it is always a good idea to promptly view your store receipts to make sure you are being charged correctly.

## SCAM ALERT

The Department of Homeland Security's Computer Emergency Readiness Team (CERT) is warning Internet users to be on guard against a convincing **e-mail virus scam** disguised as a message from auditors at the Internal Revenue Service.

CERT recently reported: "The attacks arrive via an unsolicited email message concerning an inquiry by the IRS and may contain a link or attachment. If users click on this link or open the attachment, they may be infected with a malicious code, including the Zeus Trojan." The Zeus Trojan steals sensitive data, and it is especially interested in on-line banking credentials.

**A word to the wise: Do not click on attachments included in unsolicited e-mails, especially those that encourage you to act quickly or else suffer some scary fate. These are attempts to plant malicious software on your computer.**

*Also, note that the IRS has stated emphatically that it does not communicate with businesses or citizens via e-mail.*

## SCAM ALERT

New South members along with other area residents are receiving calls from a company claiming to be their credit or debit card issuer. The company informs the member that their card has been canceled, but explains that if the member would provide them with certain card information they would be glad to assist them in reissuing a new card, or reactivating their current one. **Do NOT** give any information to this company. Please be aware that neither New South nor any other legitimate business would ever initiate a call and request personal information from you. **This is a scam to obtain your private cardholder information.** This company is not believed to have any legitimate information on NSCU members, but is solely making these calls in a random pattern.

## FRAUD ALERT

There is a new fraud scheme in Tennessee. A letter from a company called Manpower is asking people to be mystery shoppers and will pay \$200 for the assignment.

Manpower includes a check (which is fraudulent) and asks the person to contact them immediately for detailed instructions. The assignment is to go to Walmart/Moneygram to complete a transaction within 48 hours.

Also included is an actual page with questions the individual is supposed to complete and fax to a toll free number. At the bottom of the letter they have placed logos of their affiliates which include Macy's, Circuit City, Sams, Walmart, Best Buy, JC Penney and TJ Maxx.

**Use caution when you receive any type of letter and/or check that requires you to send money back to them as a "service" or "delivery" fee.**

## **Ways to Avoid being a Scam Victim:**

The following are guidelines recommended by New South and other financial institutions as steps to avoid being a victim of a phone or e-mail scam:

1. Never provide your personal information in response to an unsolicited request, whether it is over the phone or over the Internet. If you did not initiate the communication, NEVER provide any personal information.
2. If you believe the contact may be legitimate, contact the financial institution yourself by phone or in person. The key is that YOU should be the one to initiate the contact, using contact information that you have verified yourself.
3. Never provide your password over the phone or in response to an unsolicited Internet request. A financial institution will never ask you to verify your account information online.
4. Review account statements regularly to ensure all charges are correct. Periodically review activity online to catch suspicious activity as soon as possible.