Safeguarding Your Information

Tennessee Employees Credit Union

In today's high tech world, we are able to do things more quickly and conveniently electronically whether it is to send a letter via email, pay bills or even go shopping online. With this increase in speed and convenience also comes increased risk. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public. At Tennessee Employees Credit Union, the security of member information is a priority. We are strongly committed to the safety and confidentiality of your records. One of the best ways to avoid fraud is to become an educated consumer. Please take a moment to read this important information on steps in keeping you safe when conducting business online.

How to Keep Yourself Safe in Cyberspace

1. Set good passwords - A good password is a combination of upper and lower case letters and numbers not easily guessed. Change your password frequently. Do not write it down or share it with others.

2. Do not reveal personal information via email - Scammers will send email and text messages appearing as though they are coming from a trusted sender, when actually they are from someone else. Do not send personal information such as account numbers, social security numbers, passwords etc. via email or texting.

3. Do not download an attached file - Opening files attached to emails can be dangerous especially when they are from someone you do not know. Harmful malware or viruses could possibly be hidden and then downloaded onto your computer. Have a reliable and up to date antivirus program on your computer.

4. Links are not always what they seem - Never log in from a link embedded in an email message. Criminals use fake email addresses and fake web page that mimics a website. To avoid falling into their trap, type the URL address directly in your browser and then log in.

5. Web sites are not always what they seem - Be aware when you click a web site link you do not type as you may end up at a site which looks correct but in fact it is not. Take time to verify the Web page you are visiting matches exactly with the URL of an embedded link.

6. Logoff from sites when you are done - When you are ready to leave a site you have logged in to, logoff rather than just closing the page.

7. Monitory account activity - Monitor your account activity regularly either online or by reviewing your monthly statements and report any unauthorized transactions right away.

8. Assess your risk - We recommend periodically assessing your online banking risk and put into place increased security controls where weaknesses are found. Some items to consider when assessing your online risk are:

- Who has access to your online accounts?
- How and where are user names and passwords stored?
- Where do I log in from (work/home)?

What to Expect From TNECU

- TNECU will NEVER call, email or otherwise contact you and asking for your user name, password or other online credit union credentials.
- TNECU will NEVER contact you and ask for your credit or debit card number, PIN or 3-digit security code.

TNECU Credit Cards

Our card provider FIS, will identify themselves as Card Member Services. They will never ask for your card number, expiration date or CVC (security) code on the back of the card.

They will:

- Verify your street address.
- Verify the last four digits of your Social Security Number.

They may:

- Ask for the last four digits of your card number.
- Ask to verify the amount of your last transaction or payment.

If you are uncomfortable with the call, hang up and call the 800 number on the back of your card.

TNECU Check Card

Card providers Fiserv will identify themselves as TNECU Fraud Prevention Center.
They will:

- Verify your street address, zip code
- Verify your last name, and last four of your social
- Ask for a reference number should a voice message been left

If you are uncomfortable with the call, hang up and call TNECU.

Rights and Responsibilities

With respect to online banking and electronic fund transfers, the Federal government has put in place rights and responsibilities for both you and the credit union. These rights and responsibilities are described in the Account Information Disclosures you received when you opened your account with TNECU. You can also find them on our web site www.tnecu.org/join.html. Failure in promptly report a lost/stolen card could cause a denial in charge back rights and a loss of your funds. Ultimately, if you notice suspicious account activity or experience security-related events, contact the credit union immediately at 1-800-235-0403.