Authentication in an Internet Banking Environment

Safeguarding Your Information

TEXAR Federal Credit Union is always committed to ensuring the safety of our member's information. In today's fast pace world, it seems more and more things are done electronically from paying our bills to online shopping. With this increase in speed and ease also comes increased risk. Unscrupulous individuals are working harder than ever before to find new ways to scam unsuspecting individuals. One of the best ways to avoid becoming a victim of fraud is to educate yourself and try to stay one step ahead of the scammers, hackers, and identity thieves. Please take a moment to read this important information on how to keep yourself safe when conducting business online.

How to Keep Yourself Safe in an Internet Environment

1. **Make passwords long and strong.** The longer the password the tougher it is to crack. Use at least 10 characters with a mixture of upper and lowercase letters, numbers and special characters. Do not use something that could be easily guessed. Change your password frequently, do not give anyone your password or allow anyone else to use your password. Do not use the same password for many accounts. If it is stolen from you – or from the companies in which you do business – it can be used to take over all your accounts.

2. **Keep your personal information private.** Be careful before you reveal personal information through email or text messages. Fraudsters are known for making email and text messages to look like they came from a trusted sender. If you are banking or shopping online, stick to sites that use encryption to protect your information as it travels from your computer to their server. Make sure the web address starts with https:// (the "s" is for secure). Http:// is not secure.

3. **Connect with care.** Links in emails, tweets, posts and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it is best to delete. These links could allow harmful malware or viruses to be downloaded on your computer if you open them.

4. **Always logoff.** Make sure you logoff when you are ready to leave a site you have logged in to. Do not just close the page or "X" out of the system.

5. **Monitor account activity.** Make sure you monitor your account activity regularly either online or by reviewing your monthly statements. You should report any unauthorized transactions as soon as possible.

6. **Assess your own risks.** We recommend every member do their own risk assessment on their online banking security controls they have in place. This should include but not limited to: storage of online banking information (user names, passwords, answers to security questions, account numbers etc.) and what

security software is on your computer and if you keep it up-to-date. If possible, set your security software to update automatically to help protect you against the latest threats.

Contact from TEXAR Federal Credit Union

TEXAR Federal Credit Union's employees will **NEVER** call, email or send you a text message and ask for your user name, password, or any other online banking credentials. Nor will an employee contact you and ask for your credit card or debit card account number, pin or security code. If someone from the credit union calls you and you are suspicious of the caller, tell them you will call them back using the main credit union phone number.

Credit Cards

Our card provider, Vantiv, will identify themselves as Card Fraud Security calling on behalf of TEXAR Federal Credit Union. For outbound calls, the representative will never ask for your credit card number, expiration date or CVC (security) code. They will ask you to verify activity on your credit card. If you are uncomfortable with the call, please hang up and call them back on the number provided on the back of your card.

For inbound calls, the representative may ask for two pieces of information to verify your identity. If you are returning their phone call, they will ask for the telephone number at which you were contacted. This will allow them to pull up your card account information. If you were transferred directly from the credit union or customer service then the representative may ask for your credit card account number.

Debit Cards

Our debit card provider will identify themselves as Risk Management calling on behalf of TEXAR Federal Credit Union. They will ask you to verify the transaction(s) in question. If they have to leave a message and you have to return their call they may ask you for your last four digits of your social security number or you date of birth just to verify they are speaking to the correct member. They will never ask for your card number, expiration date, or CVC code.

Additional Resources:

www.ftc.gov
www.idtheft.gov
www.onguardonline.gov
www.staysafeonline.com