Nascoga Federal Credit Union
Federal Financial Institutions Examination Council (FFIEC)
MEMBER EDUCATION

Nascoga Federal Credit Union (NFCU) is committed to preserving your privacy and security. In today's high tech world, we are able to do more things electronically, whether it is to send a letter via email, pay bills or shop 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 Nascoga Federal Credit Union, the security of our member's information is a priority. One of the best ways to avoid fraud is to become an educated consumer; we would like to help you in this endeavor. Please take a moment to read this important information on how to keep yourself safe when conducting business online.

Protections under Regulation E

Regulation E, also known as the Electronic Funds Transfer Act, outlines the rights, liabilities, and responsibilities of consumers that use electronic services as well as the financial institutions that offer electronic services. Electronic Fund Transfer services include, but are not limited to, debit card, Home Banking, Bill Pay, Mobile Banking, Automated Clearing House (ACH), and ATM transactions. These rights, liabilities, and responsibilities are described in the Account Agreement and Disclosures that you received at account opening.

Contact with NFCU

Nascoga Federal Credit Union is committed to preserving your privacy and security. Please remember, NFCU and its affiliate partners will **NEVER** request your sensitive account information via text, phone or email. NFCU will **NEVER** contact you and ask for your user name, password, other online banking credentials, credit or debit card number, or PIN.

Our Fraud Prevention provider may contact you on behalf of NFCU to verify unusual credit or debit card transactions. However, they will **NEVER** ask for your card number, expiration date, security code, PIN number or online banking credentials. They may ask to verify your address, the last four digits of your Social Security Number, the last four digits of your card number, and/or the amount of your last valid transaction or payment. If you are uncomfortable with the call, please hang up and call them back at one of the following numbers:

Debit and ATM Card: 1-800-472-3272 Credit Cards: 1800-791-2525

How to Keep Yourself Safe in Cyberspace

An important part of online safety is knowledge. The more you know, the safer you'll be. Here are some great tips on how to stay safe in cyberspace.

- **Set good passwords.** A good password is a combination of upper and lower case letters and numbers, and one that is not easily guessed. Change your password frequently. Don't share your password with others.
- **Safeguard your PIN.** Never keep your PIN with your debit or ATM card, as you may be liable for unauthorized use.
- **Don't reveal personal information via email.** Emails and text messages can be masked to look like they are coming from a trusted sender when they are actually from someone else. Play it safe, do not send your personal information such as account numbers, social security numbers, passwords, etc. via email or text.
- **Don't download that file!** Opening files attached to emails can be dangerous especially when they are from someone you don't know, as they can allow harmful malware or viruses to be downloaded onto your computer. Keep your home computer safe with current virus/malware/spyware detection software, which will help prevent virus infections and warn you when you are attempting to access a known phishing site.
- **Links aren't always what they seem.** Never log in from a link that is embedded in an email message. Criminals can use fake email addresses and make fake web pages that mimic the page you would expect. To avoid falling into their trap, open a new browser page, type in the URL address directly and then log in. Ignore emails or pop-up messages that request personal or financial information.
- **Web sites aren't always what they seem.** Be aware that if you navigate to a website from a link you don't type, you may end up at a site that looks like the correct one, when in fact it is not. Take time to verify that the web page you're visiting matches exactly with the URL that you would expect.
- **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.
- **Monitor account activity.** Monitor your account activity regularly – either online or by reviewing your monthly statements, and report any unauthorized transactions right away.
- **Assess your risk.** We recommend periodically assessing your online banking risk and put into place increased security controls where weaknesses are found, particularly for members with business accounts. Some items to consider when assessing your online banking risk are:
    - Who has access to your online business accounts?
    - How and where are user names and passwords stored?
    - How strong are your passwords and how often are they changed? Are they changed before or immediately after terminating an employee who had access to them?
    - Do you have dual controls or other checks and balances with respect to access to online banking transactions?
    - Do you have antivirus protection on your computer?

Additional Resources

If you've been scammed, visit the Federal Trade Commission's Identity Theft Website at www.ftc.gov/idtheft for assistance. Also, file a complaint on the Federal Bureau of Investigations Internet Crime Complaint Center Website.

If you should notice any suspicious account activity or experience any information security-related events, please contact Nascoga Federal Credit Union immediately at (940) 665-1797.