Safeguarding Your Information

In today's high tech world, we are able to accomplish tasks more quickly and conveniently using electronically transmitted data. Whether it's sending a letter via email, paying bills on line or internet shopping; we all enjoy the convenience electronically transmitted data provides. But, 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 Greater New Orleans Federal 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 and we would like to help you in this endeavor. Please take a moment to read this important information on how to keep your information safe when conducting business online.

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:

1. 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 write it down or share it with others.

2. 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.

3. 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. Make sure you have a good antivirus program on your computer that is up-to-date.

4. 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, type in the URL address directly and then log in.

5. Web sites aren't always what they seem. If you navigate to a Web site from a link you don't type, you may end up at a site that looks like the correct one, when in fact it's not. Take time to verify that the Web page you're visiting matches exactly with the URL that you'd expect.

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. Monitor 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 banking risk are:

- Who has access to your online accounts?

- How and where are user names and passwords stored?
- How strong are your passwords and how often are they changed?

What to Expect From GNOFCU

- GNOFCU will NEVER call, email or otherwise contact you and ask for your user name, password or other online banking credentials.
- GNOFCU will NEVER contact you and ask for your credit or debit card number, PIN or 3-digit security code. Please see below for more information about how our card provider PPS (Payment Processing Solutions), may approach customer service calls.

  Credit Cards

  Our card provider, PPS (Payment Processing Solutions), will identify themselves as PPS calling on behalf of GNOFCU.

  They will NEVER ask for your card number, expiration date or CVC (security) code.

  They may VERIFY card information such as:

  - Your street address.
  - The last four digits of your Social Security Number.

  They may also VERIFY certain transactions such as:

  - Ask you to confirm the amount of your last transaction or payment.

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

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 Electronic Funds Transfer Agreement and Disclosure you received when you opened your account with GNOFCU. Ultimately, if you notice suspicious account activity or experience security-related events, you should contact the credit union immediately at 504-454-8224 or 1-800-458-5041 (out of state).