Website Privacy Policy

Pelican State Credit Union respects the personal and financial privacy of all of its members. We are committed to protecting the information on and within our website with the same safety and confidentiality standards utilized in the transaction of all credit union business. Information obtained from our website is kept secure, and access to that information is limited within the credit union. Pelican State Credit Union may collect information such as user name, email addresses, Internet Service Provider addresses, access time and date and failed logon attempts.

Information Collected From Online Banking

When you conduct an online transaction through Online Banking, such as obtaining account information, transferring funds between accounts, paying a bill or completing an application, we request information from you online at our Online Banking site. This information is needed so that we can follow your instructions or review your request or application or so that you can perform a transaction. In these cases, we only collect the information necessary to interact with you and to respond to your requests or instructions. We may keep track of the number of times you log on per month to Online Banking. We do not gather or sell this information to any third parties.

Cookies

Pelican State uses small text files called cookies to collect anonymous website traffic data. This information helps improve our Web services. Our cookies do not collect or store any personally identifiable information.

Third Party Links

We are not responsible for practices employed by websites linked to or from our site, nor the information, content, accuracy, or opinions expressed in such websites, and such websites are not investigated, monitored or checked for accuracy or completeness by us, nor do we maintain any editorial or other control over such websites. Inclusion of any linked website on our site does not imply approval or endorsement of the linked website by us. This remains true even where the linked site appears within the parameters or window/frame of our site. Often, links to other websites are provided solely as pointers to information on topics that may be useful to users of our site. Please remember that when you use a link to go from our site to another website, our Privacy Policy is no longer in effect. Your browsing and interaction on any other website, including websites which have a link to our site, is subject to that website's own rules and policies. We are not responsible for the data collection and practices of third parties linked to our website. Please read the rules and policies of the third-party sites before proceeding. If you decide to leave our site and access these third-party sites, you do so solely at your own risk.

Email
Email is not a secure form of communication. 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 texting.

Children
Pelican State Credit Union does not knowingly solicit data from children. We recognize that protecting children's identities and privacy on-line is important and the responsibility to do so rests with both the online industry and parents.

Interruption of Service
At certain times, Pelican State Credit Union's website may not be available due to system maintenance or circumstances beyond our control. Pelican State Credit Union conducts frequent and regular backups of your information and utilizes redundant information practices to protect your information from being erroneously altered due to unintentional errors and equipment malfunctions.

Confidentiality and Security
The security of your account information is our top priority. We have employed the most comprehensive measures available to ensure your financial and personal information is kept private. Pelican uses industry-standard SSL encryption to protect data transmissions within Pelican@Net, our online banking program.

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 Pelican State Credit Union. Ultimately, if you notice suspicious account activity or experience security-related events, please contact the credit union immediately at 1-800-351-4877.

Safeguarding your Information

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 Pelican State 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 ways to try and stay safe when conducting business online. (*continued*)

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 long combination of upper and lower case letters, symbols 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. This is called phishing. Play it safe, do not send your personal information such as account numbers, social security numbers, passwords etc. via email or texting.

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. Be aware that 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; 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?