Reliant Community Credit Union
Online Security

Reliant Community Credit Union is committed to protecting your personal information and your financial accounts. A part of that commitment is to provide timely information on the many scams and fraud schemes that criminals use in an attempt to steal your money or your identity. Having that knowledge will help each member avoid being a victim of fraud.

Important Information for All Reliant Members

1. Reliant will NEVER contact you by email, phone, or text messages to ask you for your account number or other account information. It is important that you never respond to phone calls, text messages, or emails that ask you to provide, validate, or update any account information.

2. If you receive a suspicious email regarding your Reliant account, contact us immediately at 800-724-9282.

3. If you have provided your Reliant account information to an unknown source, please contact us immediately at 800-724-9282.

4. If you use Reliant's online banking program and find anything unusual when you login such as a change from the screen you normally see, the page format, inaccurate account information/balances, or if are asked to enter confidential account information, NEVER respond. Close out of the program and contact us immediately at 800-724-9282.

5. If you receive a call regarding activity on your Reliant debit or credit card, the representative will identify themselves as Card Member Services and may ask to verify: your address, last four digits of your Social Security Number, last four digits of your card, and the amount of recent transactions. They will never ask you for your card number, expiration date, or CVC (security) code. Visit our website and go to the Visa credit card page for additional information.

Protect Yourself With These Online Security Tips

1. **Install anti-virus and spyware-detection software, and a firewall.** Update on a regular basis, as recommended by the software providers.

2. **Keep your PC and browser updated**. Be sure to download patches only from official vendors' websites, and not from third-party websites.

3. **Ensure that the "anti-phishing" option is "on"** in Firefox, Chrome or Internet Explorer browsers. This will check for "blacklisted" websites. This option can generally be found under the Tools menu.

4. **Do not respond to e-mails, Web pages or telephone inquiries** requesting you to verify your account information.

5. **Delete e-mails from unknown senders** with nonsensical information or typos in the subject lines.

6. **Use your e-mail spam filter**.

7. **Type URLs, don't click**. If opening a suspicious e-mail, don't click on any links. Even if you think the e-mail is legitimate, type web addresses into your browser instead of clicking on links.

8. **Look beyond the logo**. Scammers often include actual logos and images they have stolen from official websites. They also convey a sense of urgency, stating that if you fail to provide, update or verify your personal or account information, access to your accounts will be suspended.

9. **Use "strong" passwords and NEVER share your password** with anyone. Choose an alphanumeric password that contains a mix of numbers, random characters and upper and lower case letters. Do not use numbers or words that can be easily guessed. It is good practice to change all your passwords every 30-60 days.

10. **Protect your personal information**. Limit the amount of personal information you give online, including when using social networking sites such as Facebook and MySpace. Be sure to read the site's privacy statement.

11. **Protect your credit card when shopping online**. Make sure there is an "s" (for secure) after the http in the web address (i.e., https). Secondly, check to see if there is a locked padlock on the screen (usually in the lower right corner). Lastly, if you're not familiar with the company, try to confirm a physical address, not just a P.O. Box.

12. **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 texting.

13. **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.

14. **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.

15. **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.

16. **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.

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

With respect to online banking and electronic funds transfers, the Federal government has put in place rights and responsibilities for both you and the credit union. These rights and responsibilities are outlined in the Electronic Funds Transfer disclosure you received when you opened your account. You can also find the disclosure on our website.