reliant
CREDIT UNION
achieve life

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.