



Security

Privacy

Protecting the privacy of our customers is very important to Central State Bank. We take our responsibility to protect confidential consumer information seriously.

Central State Bank has implemented a security program to address the Standards for Safeguarding Customer Information Codified in 16 CFR 314 of the Gramm-Leach-Bliley Act. It is the policy of Central State Bank to 1) assure the security and confidentiality of our customers information, 2) protect against anticipated threats or hazards to the security or integrity of such information and 3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

We will maintain physical, electronic and procedural safeguards that comply with federal standards to guard the nonpublic personal information to those employees who may need to know that information in order to provide the customers products or services.

In addition, as per our Information Security Policy, we will only retain those critical vendors capable of maintaining appropriate safeguards for nonpublic financial information of employees and other third parties. We will further try to incorporate contractual protections, which will require such providers to implement and maintain appropriate safeguards.

Protecting Information

We maintain physical, electronic and procedural safeguards to guard your nonpublic personal information. Our operational and data processing systems are contained in a secure environment and that environment is access-controlled.

We use various authentication technologies, including passwords, to authenticate visitors to the portions of our website that may allow access to private or confidential information. We have implemented other security controls such as firewalls, intrusion detection and intrusion prevention to protect our systems and networks and your information. Our security systems constantly monitor the web server to ensure your accounts are safe and secure.



Email

Email messages are not secure. We are not responsible for the security or confidentiality of communications sent to us via Internet email messages. Generally, our security software does not encrypt email messages, unless we specifically send you an encrypted email message. Email messages traveling through the Internet are potentially subject to viewing, alteration and copying by anyone on the Internet. Be cautious when submitting personal or financial information via email. Send confidential information through the secure email portal located inside of our home banking, postal service or use the telephone to speak directly to our employees.

Internet Fraud

Central State Bank wants to protect clients by warning them about a growing form of Internet fraud called “phishing.” Fake email messages are disguised to look like requests from real businesses. These emails request private information. The information is then used to access financial records and steal identities.

You should not respond to emails from Central State Bank that request validation of personal information or link to Web sites requesting validation of personal information. Those receiving suspicious emails that appear to be from Central State Bank should immediately contact Central State Bank at (563) 245-2110.