The First State Bank of Kiowa

Customer Newsletter

Customer Fraud Awareness
Volume 2

Online Banking Security

Each year, more and more Americans have their identity stolen and the staff and management at The First State Bank of Kiowa want to give you the information you need to help protect yourself against identity theft.

The First State Bank of Kiowa's Online Banking will allow you to enter your password incorrectly a limited number of times; too many incorrect passwords will result in the locking of your online banking account until you call to reinitialize the account. We monitor and record "bad login" attempts to detect any suspicious activity.

The First State Bank of Kiowa is committed to protecting your information. All information within our Online Banking uses the Secure Socket Layer (SSL) protocol for transferring data. SSL is a cryptosystem that creates a secure environment for the information being transferred between your browser and First State Bank. All information transferred through Online Banking has a 128-bit encryption which is the highest level of encryption. In addition to the security features put in place by The First State Bank, here are some tips to keeping your information secure.

- Never give out personal information including Usernames, Passwords, SSN, Date of Birth
- Create difficult passwords which include letters, numbers & symbols
- Don't use personal information for your username or passwords.
- Avoid using a public computer to access your online banking.
- Don't give any of your personal information to any web site that does not use encryption or other secure methods to protect it.

Phishing

Phishing is the latest form of identity theft. It's when thieves pose as your financial institution and try to hook the customer into providing personal or financial information. Once the consumer is hooked, the thieves can do lasting damage to a consumer's financial accounts. They can dupe customers into providing their Social Security numbers, financial account numbers, Online Banking passwords, mother's maiden names and other personal information.

Clues to identifying a "Phishing" e-mail

1. Awkward greeting: a phish may address the customer with a nonsensical greeting or may not refer to the customer by name.
2. Typos & incorrect grammar- this is a technique used by phishers to avoid email filters. The errors are intentional.
3. Source code points to a different website- the link looks official, but when you when your mouse cursor rolls over it, the link's source code points to a completely different website.
4. Urgent call to act- Different approaches include things such as "We're updating our records", "We've identified fraudulent activity on your account", to encourage people to act immediately, or they may even threaten to close your account. **DO NOT respond to these attempts.**

Privacy

The privacy of communications between you (your browser) and our servers is ensured via ***encryption***. Encryption scrambles messages exchanged between your browser and our online banking server

How Encryption Works

- When visiting online banking's sign-on page, your browser establishes a secure session with our server.
- The **secure session** is established using a protocol called **Secure Sockets Layer (SSL)** Encryption. This protocol requires the exchange of what are called public and private keys.
- Keys are random numbers chosen for that session and are only known between your browser and our server. Once keys are exchanged, your browser will use numbers to scramble (encrypt) the messages sent between your browser and our server.
- Both sides require keys because they need to descramble (decrypt) messages received. The SSL protocol assures privacy, but also ensures no other website can "impersonate" your financial institution's website, nor alter information on it.
- To learn whether your browser is in secure mode, look for the lock symbol in the box at the top of your browser window where the web address shows.

Encryption Level

The numbers used as encryption keys are similar to combination locks. The strength of encryption is based on the number of possible combinations a lock can have. The more possible combinations, the less likely someone could guess the combination to decrypt the message.

For your protection, our servers requires the browser to connect at 128-bit encryption. Users will be unable to access online banking functions with lesser encryption levels. This may require end users to upgrade their browser to the stronger encryption level.

The First State Bank of Kiowa

is committed to protecting your personal information

If you feel your account has been jeopardized or you have questions regarding your account, please call or visit a customer service representative at any of our branch locations.

First State Bank of Kiowa
546 Main St. /PO Box 105
Kiowa, KS 67070-0105

Phone: 620-825-4147
Bookkeeping: 620-825-4100
Fax: 620-825-4790

Lobby Hours

9:00-3:00	Monday, Tuesday, Thursday, Friday
9:00-6:00	Wednesday
Closed	Saturday

Drive-thru

8:00-4:00	Monday, Tuesday, Thursday, Friday
8:00-6:00	Wednesday
8:00-12:00	Saturday