



UNION STATE BANK

SECURITY STATEMENT

Union State Bank's Online Banking product utilizes the latest computer and security technology to ensure that all customer account information remains secure and accurate. All hardware components reside in secure locations with strict security controls implemented.

ACCOUNT ACCESS CONTROLS

Union State Bank maintains control of the way in which each customer may access accounts. These controls are maintained through settings on the host software and within the Online Banking interface. Restrictions may be placed on account access and transfer rights.

PASSWORD PROTECTION

A customer is only allowed to access account information on our Online Banking with a valid login using multi-factor authentication. Multi-factor authentication requires a username and at least two of the following:

- Something the user knows
- Something the user has
- Something the user is

Only customers who have been enabled for Online Banking will be allowed access and only data for these customers will be transferred to our Online Banking Network. After five simultaneous invalid username and/or password entries for a customer, access will be disabled for the customer preventing unauthorized access by a third party. Once disabled, only bank personnel may re-enable access through the Online Banking interface.

SECURE COMMUNICATION

All communication between the customer and the Online Banking Network are conducted using the Secure Socket Layer (SSL) protocol. SSL provides data encryption, server authentication, and message integrity for the entire banking session. This assures that somebody will not be able to eavesdrop on the session, that the customer is connected with the Online Banking Network and not an imposter, and that all information received will be accurate.

NETWORK SECURITY

The Online Banking Server Network is comprised of several components including Firewalls, Screening Routers, Web Servers, and Database Servers. The Firewalls and Screening Routers work in tandem ensuring that only authorized requests are allowed to reach the Web Servers. Any suspicious activity will result in access being denied and is logged for later review. All requests are passed to the Web Servers on behalf of the client and back to the client on behalf of the Web Servers. This ensures that access directly to the Web Servers is not possible, significantly reducing the possibility of unauthorized access. The Database Servers, where all account information is stored, is only accessible through request made by the Web Servers. Access to account information is only allowed through the Web Server Banking interface.