

SECURITY

The convenience of banking through the Internet is sometimes overshadowed by concerns that your private account information could fall into the wrong hands. At Little Horn State Bank, security is our top priority. To this end, we have a firewall between the Internet and our customer information preventing unauthorized access; we only communicate through web browsers that support Secure Socket Layer (SSL) 3.0 or higher. As a final security measure, we encrypt all data communications using state-of-the-art encryption technology and Message Authentication Code (MAC).

GUARANTEE

At Little Horn State Bank, we are so confident in our security measures that we guarantee you will be covered against 100% of losses for any funds improperly removed from your accounts due to a breach of our security measures, as long as you fulfill your customer responsibilities. This guarantee does not apply to small business, commercial, or other non-personal accounts and does not cover transactions by persons to whom you disclose your online Access Credentials, such as user IDs and passwords.

CLIENT RESPONSIBILITY

As you would expect, our security measures are only effective if customers fulfill their responsibilities as outlined in the terms and conditions of our online and mobile banking agreements. For example, our guarantee does not cover losses resulting from the following:

- Customer's input errors.
- Customer's negligent selection, handling, or sharing of Access Credentials leading to unauthorized access to accounts, and/or unreported theft of Access Credentials.
- Customer's failure to complete the banking sessions by logging/signing off before leaving a computer unattended.
- Customer's failure to review account activity and statements and report errors as set forth in account agreements.
- Customer's failure to report known incidents of Access Credential theft and/or unauthorized online account access within two business days of discovery.
- Customer's failure to protect their system's security.
- Customer's equipment/systems have been infected with malicious code (including but not limited to: viruses, trojans, spy ware, malware, etc.) through no fault of the bank.
- Customer's failure to use compatible web browsers and/or operating systems during online sessions.

Remember, you can contact us by phone at 406-665-2332 in our Hardin Branch or 406-656-5148 in our Billings Branch (Monday - Friday 8:00am-5:00pm) to report any unauthorized event.

SECURE SOCKETS LAYER (SSL)

Secure Sockets Layer 3.0 provides a way for your browser to ensure that you are in fact logging on to the Little Horn State Bank server and not a site that is attempting to impersonate our server. Before you log on to the Little Horn State Bank server, SSL sends our public key to your browser program. SSL lets your browser verify the identity of our server by viewing the site's certificate. A certificate is a way of associating a public key to a name.

DATA ENCRYPTION

Once SSL has authenticated the server, your browser and our server will create an individual symmetric key. This key will allow our server to communicate with your browser through encrypted transmissions of data. The symmetric key is valid for a single use only. If you log out and log in again at another time, the server and your browser will create a new unique symmetric key.

MESSAGE AUTHENTICATION CODE

With all data between our server and your browser scrambled, no outside party can understand our communications, though it is still possible to intercept a message. To verify that a message has not been tampered with, SSL uses a message authentication code (MAC). A MAC is a piece of data that is derived using pieces of the symmetric key and the message itself. Your browser will always check the MAC before decoding a message from our server. If the message from our server is not authentic, the MAC will not compute correctly and your browser will alert you of a possible security breach. The chances of someone encrypting a message and providing a correct MAC are next to impossible, about 1 in 18,000,000,000,000,000,000 using 128-bit encryption.

If you have any other questions about our Personal Online Security Guarantee, please contact us by phone at 406-665-2332 in our Hardin Branch or 406-656-5148 in our Billings Branch (Monday - Friday 8:00am-5:00pm).