Bank of Washington Online Banking Security Statement

Multi Factor Authentication

In order to make your online banking experience as secure as possible we have introduced a new security feature that detects uncharacteristic or unusual behavior involving your online account. If anything out of the ordinary is detected, you may be asked a security challenge question. When a customer logs into online banking, the user is prompted to register the computer, and answer 3 security challenge questions. Advanced device forensics seamlessly authenticates your computer and various devices. The Extended Validation (EV) Certificate triggers web browsers to display a green address bar and our site provider's name (Fiserv, Inc.)

Bank of Washington Online Banking Security Practices

The Bank of Washington Online Banking System brings together a combination of industry-approved security technologies to protect data for the bank and for you, the customer. It features password-controlled system entry, a VeriSign-issued Digital ID for the bank's server, Transport Layer Security protocol for data encryption, router, and firewall to regulate the inflow and the outflow of all server traffic.

Secure Access and Verifying User Authenticity

To begin a session with the bank's server the user must key in a Log-in ID and a password. Our system, the Online Banking System, uses a "3 strikes and you're out" lock-out mechanism to deter unauthorized users from repeated login attempts. After three unsuccessful login attempts, the user is locked out of the system. A consumer customer can either call the bank to be reset or use the 'Forgotten Password' link, which will require them to enter the last four digits of their social security number, their Access ID and the email address that the bank has on file. The Senior Administrator of the business is required to call the bank and verify their identity before re-entry is permitted back into the system.

Secure Data Transfer

Public Internet Banking traffic is, at a minimum, encrypted with, Transport Layer Security 128bit, RC4 SHA 1 encryption. With, Transport Layer Security data that travels between the bank and the customer is encrypted and can only be decrypted with the public and private key pair. In short, the bank's server issues a public key to the end user's browser and creates a temporary private key. These two keys are the only combination possible for that session. When the session is complete, the keys expire and the whole process starts over when a new end user makes a server session.

Router and Firewall

Requests must filter through a router and firewall before they are permitted to reach the server. A router works in conjunction with the firewall, to block and direct traffic coming to the server. The configuration begins by disallowing ALL traffic and then only allows the traffic necessary to process acceptable data requests, such as retrieving web pages or sending customer requests to the bank.

Bank of Washington
is committed to the security
of your Online Banking experience!

Revised 3/17