Online Security

OVERVIEW

Bank of the Ozarks' Online Banking system brings together a combination of industry proven security technologies to protect data for the bank and for you, our customer. Some of these features include transmission security, which addresses the need to keep unauthorized agents from intercepting and/or deciphering the transmission of customers' encrypted data while it travels between the customer's computer and the Bank of the Ozarks ("Bank") server environment and various other state of the art security technologies working behind the scenes to help insure your data remains safe.

"End user" will be used to signify an authorized customer using software for the benevolent purposes it was intended and "agent" will be used to signify a person whose goal it is to exploit a software application for some negative end.

THREE STRIKES AND YOU'RE OUT!

If an agent attempts unauthorized entry into a customer's account by trying to guess a Login ID and password, the customer's Bank of the Ozarks' Online Banking account will be disabled on the third incorrect login attempt, thus invalidating the Login combination. The disabling and/or destruction of the password keeps an unauthorized agent from running a brute force attack, which uses an application that will run through millions of possible passwords eliminating the invalid ones until it arrives at a match. In this scenario, to guard against unauthorized use of a customer's Login ID and password, Bank of the Ozarks' Online Banking system disables the password indefinitely until the customer calls the Bank and requests the associated Login ID and password to be reset, or the customer clicks the "receive a new password" link to have a temporary password sent to the email address on file with the Bank. A customer will also trigger this security feature by unintentionally miss-keying a password three times. In this situation the customer will need to call the Bank to reestablish the password for the locked account(s). For example, a common mistake made by end users is having the caps-lock on while keying in a password. Since the password is case sensitive and an end user cannot actually see the characters being typed, it is easy to think the password is being typed correctly when the caps-lock is engaged.

SUGGESTIONS FOR PASSWORDS

A password and Login ID provide security against unauthorized entry and access to customers' accounts. Passwords should not be easy to guess; for example, children's or pet's names, birth dates, addresses or other easily recognized identifications should be avoided. Combining cases (utilizing upper and lower case) within your password as well as combining alpha, numeric, and special characters is a good security precaution in selecting a password.

Member FDIC

TRANSMISSION SECURITY

End-users must use later versions of Mozilla Firefox, Safari, Google Chrome and Microsoft Internet Explorer to access the Bank's Online Banking application. The later versions come equipped with Netscape developed encryption technology known as Secure Sockets Layer, commonly referred to as SSL. SSL's specific function is to manipulate data into an unreadable format as it leaves the end user's computer. The temporary scrambling of data in transit is referred to as 'encryption.' In the unlikely case that an agent should intercept the data in transit, the encryption makes the data unreadable to a human. Furthermore, data in transit is split up into packets that travel separately and are not reorganized until they filter through the Bank's router and firewall. The Bank also uses multiple measures to ensure data is encrypted and subsequently decrypted in a secure fashion. The use of electronic keys that lock data as it is transmitted and unlock the data once received and passed successfully through the Bank's firewalls is just one example.

EMAIL

Public email is not always a secure process, as data is not always encrypted as it travels over the public Internet, and it can be intercepted by third parties. Please be careful not to provide information in a single message that would allow an agent to log onto your account. Full account numbers should not be included in an email. If an account must be referenced, reference it by only the last four digits. Bank of the Ozarks will never request a customer's password for any system and encourages customers to never share passwords.

Member FDIC