



Online Banking Security

Servicelst Bank of Nevada understands that the security of your personal account information is important to you. We also understand that our continued success as a financial institution relies on both our ability to offer banking services to you in a secure manner as well as your responsibility in keeping any access codes, passwords or PINs secure. To assist us in offering these Web-based banking services in a secure manner, we employ a number of measures, which are described below. These measures allow us, among other benefits, to properly authenticate your identity when you access these services and protect your information as it travels between your PC and Servicelst Bank of Nevada. With the proper safety measures in place, your online banking transactions remain safe and secure. The following measures have been taken to ensure your privacy, as well as some steps you can take.

Information Encoding

We use the latest encryption technology to ensure that your private information cannot be intercepted. Encryption is a way to rewrite something in code, which can be decoded later with the right "key." A minimum 128-bit RC4 encryption technology is required. When you request information about your accounts, the request is sent encrypted to Servicelst Bank of Nevada. We decrypt your request and send the requested information back to you in an encrypted format. When you receive the information, it is decoded so that you can read it.

Personally Selected Account Names

Servicelst Bank of Nevada does not display your account numbers over the Internet. Instead, we ask you to choose a "pseudo" name for each of your accounts. Example of pseudo name would be personal checking account, operating account, payroll account, and savings account. You can change your "pseudo" account name under the "Options" section of our online banking service.

Unique ID and Personal Identification Number (PIN)

In order to access your accounts online, you must enter a unique User ID and PIN number. We strongly recommend that you choose a PIN that you can remember (without writing it down) but does not use information that can be easily guessed by someone. Avoid the use of birthdays, children's names, etc. Do not reveal your User ID or PIN to anyone.

Three (3) strikes and you're out

If an unauthorized person attempts entry into an end user's account by trying to guess a Log-In ID, the bank will disable the password on the third incorrect attempt, thus invalidating the Log-In combination. If you accidentally activate this security feature by unintentionally mis-keying a password three times, you would need to contact the Bank to reestablish the password for that account. For example, a common mistake made by the end user is having the CAPS-LOCK on while keying in a password.

To further protect you, a timeout feature is used. This feature will automatically log you out of your current financial service session after a 10-minute inactivity period on our site.

180 Day PIN Expiration Interval

Servicelst Bank of Nevada requires that you change your PIN every 180 days. This step provides additional security should someone guess your current PIN.

Email Communications

Please remember that e-mail is not secure against interception, and you should be cautious when sending e-mail with personal information. If your information is very sensitive, or includes personal or confidential information-such as your bank account, charge card or Social Security number-you may want to contact us by our secure email connection utilize the [Contact Us](#) option or by postal mail or telephone.

How You Can Protect Your Internet Security

While Servicelst Bank of Nevada works to protect your banking privacy, you will also play an important role in protecting your accounts. There are a number of steps you can take to ensure that your Servicelst Bank of Nevada account information is protected, including:

- Keep your PIN to yourself.
- Change your PIN frequently.
- Remain at your computer until your Online Banking transactions are completed and log out. Log out of Online Banking prior to visiting other Internet sites.
- Don't use obvious numbers or easily accessible information for your log-in ID and Password.
- Ensure that no one is watching when entering your log-in ID and Password.
- Don't record your log-in ID and Password on paper. Try to memorize them, if possible.
- If you do record your log-in ID and Password, keep them in a safe, secure location.
- Do not share your log-in ID and Password with anyone.
- Review your account information often. Report any unusual activity immediately.
- Never give account information to anyone over the telephone unless you initiated the call.

If you notice suspicious or unusual activity on your Online Banking accounts, call the bank immediately.

Member FDIC | Equal Housing Lender

© 2010 Servicelst Bank of Nevada www.servicelstnevada.com