

Online Security

Internet Banking

HNB National Bank considers the security of your financial information a top priority. We take extensive security measures to ensure a safe and reliable online experience for our customers.

The first level of security is password protection. To gain access to accounts, users verify their identity with a password.

The second level of security is firewall protection. All HNB National Bank systems are protected with firewalls that limit access to only those customers providing the proper passwords.

The third level of security is 128 bit key SSL encryption. Before data is exchanged between the customer and HNB National Bank, it is encoded or scrambled with 128 bit key SSL encryption.

Additionally, the federal government provides significant protection. The same law protecting you from fraudulent credit card usage also protects you from unauthorized online banking activity.

Security Tips

Even with all the security precautions we have in place, we need your help in making your accounts as secure as possible. To that end, HNB National Bank recommends customers practice the following security measures:

- Keep Ids and passwords confidential
- Use passwords that include letters and numbers that are not easily discernable
- Change your passwords frequently
- Use different passwords for each online service

Firewall Protection

The Internet was not originally designed for open access by the general public. However, the popularity and acceptance of the Internet created the demand for more and more companies to make information available from internal computer systems. One of the ways to meet this need is for HNB National Bank to install and maintain a security firewall on the computer network.

Firewalls provide that every request for information is authenticated and provided only to the authorized individual. In addition all activity passing through the firewall is documented.

128 Bit Key SSL Encryption

All data exchanged over the Internet is divided into small units and sent in envelope packets. Upon arriving at the computer that requested the information, the packets are reassembled into the original message.

For Internet transactions and communications, you must employ a method of securing these packets as they travel across the Internet. Secure Socket Layer, or SSL, is a method for encrypting and decrypting packets of data as they are exchanged using a known only to the data's sender and recipient. SSL locks the data so that regardless of the path the data takes as it passes across the Internet, it only can be opened at the end with the proper key or combination to the lock on the data.

SSL technology is widely accepted today because the combination needed to unlock encrypted data is 128 characters long.