Online Security Policy

Security is a common and logical concern with banking on the Internet. That is why Online Banking utilizes the latest technology, which was developed to safeguard data through encryption or coding of information. This creates barriers between systems that can only be crossed with authorized passwords, and by creating safe pathways to and from each system.

Multiple layers of advanced security tools including cryptography, firewalls and trusted operating systems are used to prevent tampering and ensure the privacy of your account information. Before gaining access to any account information, everyone is authenticated by a personal Access ID, Password, a private Authentication Image and a private Authentication Pass Phrase. Business Online Banking PLUS customers, performing higher risk transactions, will use a Security Token in addition to their personal Access ID number and Personal Identification Number. A Security Token is a small portable device that generates a one-time password to use each time the customer logs in. The password is unique to their account and it changes every 32 seconds.

You will personally select your own 8 - 10-digit alphanumeric case-sensitive password. This means your password should contain numbers and both upper- and lower-case letters. No one else will be able to access your accounts because your password is known only to you. Using a combination of numbers, and upper- and lower-case letters (as opposed to numbers only) provides maximum security for the protection of your individual account information.