Online Banking Security

Ridgewood provides a number of additional security features.

Encryption

The numbers used as encryption keys are similar to combination locks. The strength of encryption is based on the number of possible combinations a lock can have. The more possible combinations, the less likely someone could guess the combination to decrypt the message.

For your protection, Ridgewood's online banking servers require the browser to connect at 128-bit encryption (versus the less-secure 40-bit encryption). Users will be unable to access online banking functions at lesser encryption levels. This may require some end users to upgrade their browser to the stronger encryption level.

To determine if your browser supports 128-bit encryption:

- Click "Help" in the toolbar of your Internet browser
- Click on "About [browser name]"
- A pop-up box or window will appear.
  - ◊ For Internet Explorer: next to "Cipher strength" you should see "128-bit"
  - ◊ For Netscape: you should see "This version supports high-grade (128-bit) security with RSA Public Key Cryptography"

If your browser does not support 128-bit encryption, you must upgrade to continue to access Ridgewood's Website secure pages.

Time Out Security

Ridgewood's Online Banking will "timeout" after a specified period of inactivity. This prevents curious persons from continuing your online banking sessions if you left your PC unattended without logging out. You may set the timeout period in Ridgewood's Online Banking's User Options screen. We recommend that you always sign off (log out) when done banking online.

Enhanced Multifactor Authentication (EMFA)

Authentication is the process used to allow access to only the correct customer. Without effective authentication controls, it is possible for fraudulent users to access your account. Ridgewood authenticates customers by issuing challenges that only the true customer should be able to pass.

Multifactor Authentication means two or more different types, or factors of authentication must be passed. By using two different factors of authentication, we get a higher assurance that the customer is the correct intended user. EMFA is commonly used to protect transactions at ATMs, where your card is something you have, and your PIN code is something you know. Similarly with EMFA, your phone or e-mail is something you have, and your password is something you know.

For your convenience, after you successfully authenticate with your password and One-Time Access code, you may enroll your computer for use in authentication. If you choose to enroll your computer, a special Browser Cookie will be present on the system, which will act in place of your phone or e-mail for something you have in your possession.