Consumer Online Banking Information Security Selected Best Practices

Wood & Huston Online Banking uses Enhanced Login Security with Multi-factor authentication that verifies your identity in two ways. We verify your Login Credentials (unique Username and Password created by you) and a One-Time Passcode (OTP) sent via email, voice call or text message to your phone, computer or smart device. To further increase your security, we require a periodic change of password. As always, balancing your account on a regular basis is one of the best ways to avoid major problems with your account.

Contact us at 660-886-6825 immediately if you suspect someone else has been in your Online Banking account.

ENCRYPTION

To ensure password protection, Online Banking uses the latest techniques in data encryption for server authentication for you. Data encryption is a way of translating data into a format that is unintelligible without a deciphering mechanism.

COMPUTER

- Your computer should be physically secured
- Your computer should be behind a security configured firewall
- Your computer's operating system and browser should be up to date and securely patched
- Anti –virus software should be active and up to date
- Anti-spyware/anti-malware should be active and up to date
- If you are using a wireless connection, follow the manufacturer's security instructions
- Never leave your computer unattended with financial date displayed

LOGIN/LOGOUT

To access Online Banking, procedures should include:

- Boot the computer and do not open other applications or additional browser windows before initiating Online Banking or while using Online Banking
- Access the Online Banking web site by typing the URL directly into the address bar
- Look for anything unfamiliar, unprofessional, or out of place on the website. If you see anything different, call us and do not use the website.
- Be sure the website URL is proceeded by "HTTPS" indicating an encrypted communication

- Check for browser “lock” icon, but understand that this only signifies a secure communication channel, not necessarily a legitimate website
- Upon successful login, you will see the date and time of your last successful login. This will help you monitor usage for any unauthorized access attempts
- When the current Online Banking session is completed, we recommend you click the LOGOUT button. This will securely close your Online Banking session

SECURE EMAIL

We offer the ability to send and receive secure email messages using our Secure Email feature located at the top of each page within your Online Banking.

AUTHENTICATION/PASSWORD

Multiple levels of authentication are recommended, with the best including something you know (a strong, complex password) and One-Time Passcode. Use a strong, complex password with a combination of letters, both upper and lower case; symbols and numbers. A few best practices for your password are:

- Do not use the same password for multiple online accounts. Your Online Banking password should be exclusively used for your Online Banking account. In this way, if one password you use is somehow compromised, your other passwords are not exposed.
- Keep your password safe. Do not leave your password in a file on your computer or on a sticky note on your monitor.
- Do not share your password with anyone. If you have a joint account, each of you can setup your own login for Online Banking.
- We will never call or email you asking for login ID or password. If you are contacted, do not respond to the request and contact us immediately.
- Contact us immediately if you suspect someone else has been in your Online Banking account.