Business Online Banking Information Security Selected Best Practices

Business Online Banking has several effective security techniques that we encourage you to implement, some of which are outlined below. 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 Business Online Banking account.

ADMINISTRATOR

The Administrator for the Business should use Administrative access for setting up and resetting sub users. Segregation of duties is important for both internal control and avoiding compromising credentials that have the overarching power of the Administrator.

COMPUTER

The Business should designate one computer strictly for Business Online Banking transactions. This computer should not be used to surf the internet, check email, etc. Certain criteria for an Administrator dedicated computer are:

- The computer should be physically secured
- The computer should be behind a securely configured firewall
- The computer should be placed on its own subnet
- The computer's operating system and browsers 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 using a wireless connection, follow the manufacturer's security instructions

These best practices are also encouraged for any computer that can initiate and/or approve Business Online Banking transactions such as Bill Pay, ACH, wire transfers, etc.

LOGIN/LOGOUT

To access Business Online Banking, procedures should include:

- Boot the computer and do not open other applications or additional browser windows before initiating Business Online Banking or while using Business Online Banking
- Access the Business Online Banking website 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 the 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 Business Online Banking session is completed, we recommend you click the LOGOUT button. This will securely close your Business Online Banking session

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.