Lake City Bank

Business Online Fraud Prevention

With the increase of computer viruses, we would like to update you on some ways to protect yourself against fraud when using internet banking.

Set Up Business Online Alerts

- Lake City Bank recommends activating the following alerts:

  ACH Template Activity – Notifies you when an ACH template has been added, edited, or deleted.

  Outgoing Wire Status Change – Notifies you when an outgoing wire's status from the selected account changes.

  Wire Transfer Template Activity – Notifies you when a Wire Transfer template has been added, edited, or deleted.
- To set up alerts in Business Online, go to the Administration tab and select "Manage Alerts" under the Communications heading. For more information about managing alerts, refer to page 10 of Lake City Bank's Business Online User Manual (www.lakecitybank.com/bizmanual).

Avoid Phishing, Spyware and Malware

- Do not open e-mail from unknown sources. Be suspicious of e-mails purporting to be from a financial institution, government agency, or other organization requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes, and similar information. Lake City Bank will never ask you for this information. Opening file attachments or clicking on web links in suspicious e-mails could expose your system to malicious code that could hijack your computer.
- Never respond to a suspicious e-mail or click on any link embedded in a suspicious e-mail. Call the purported source if you are unsure who sent an e-mail.
- If an e-mail claiming to be from Lake City Bank seems suspicious, check with us to confirm it is legitimate.
- Install anti-virus and spyware detection software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
- Update all of your computers regularly with the latest versions and patches of both anti-virus and anti-spyware software.
- Ensure computers are patched regularly, particularly operating system and key application with security patches.
- Install a dedicated, actively managed firewall, especially if using a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to your network and computers.
- Check your settings and select, at least, a medium level of security for your browsers.
- Clear the browser cache before starting any Business Online session to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared depends on the browser and version you are using. This function is generally found in the browser's preferences menu.
- Be advised that Business Online will never present you with a maintenance page after entering login credentials. Legitimate maintenance pages are displayed before entering login credentials.
- Business Online does not use pop-up windows to display login messages or errors. They are displayed directly on the login screen.
- Business Online never displays pop-up messages indicating that you cannot use your current browser.

Practice The Following General Guidelines

- Do not use public or other unsecured computers for logging into Business Online.
- Users should check and verify the last login date/time every time they log in.
- Review account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to Lake City Bank.
- View transfer history available through viewing account activity information.
- Do not use account numbers, your social security number, or other account or personal information when creating account nicknames or other titles.
- Review historical reporting features of your online banking application on a regular basis to confirm payment and other transaction data.
- Never leave a computer unattended while using Business Online.
- Never conduct banking transactions while multiple browsers are open on your computer.
- Prohibit the use of “shared” usernames and passwords for Business Online.
- Limit administrative rights on users’ workstations to help prevent the inadvertent downloading of malware or other viruses.
- Dedicate and limit the number of computers used to complete online banking transactions. For computers dedicated to Business Online, do not allow Internet browsing or e-mail exchange and ensure the latest versions and patches of both anti-virus and anti-spyware software are installed.
- Delete online user IDs as part of the exit procedure when employees leave your company.
- Assign dual system administrators for online cash management services.
- Use multiple approvals for monetary transactions and require separate entry and approval users.
- Establish transaction dollar limits for employees who initiate and approve online payments such as ACH batches, wire transfers, and account transfers.

Lake City Bank
Member FDIC

One Call Center • 888-522-2265
www.lakecitybank.com