Luther Burbank®

Savings

Security Reference Guide

Luther Burbank Savings (the "Bank") requires the use of a token, user ID and personal identification number ("PIN") to access Business Online services. You and your employees are responsible for safeguarding the confidentiality and security of tokens, user IDs and PINs used to access the Business Online. Do not share account information or passwords. If you or one of your employees has any reason to believe that the security and/or confidentiality of any account has been compromised, or that there has been a significant security event, you are required to notify the Bank immediately by calling 888.578.4495, Monday – Friday, 9am to 5pm (PST) or emailing onlineaccounthelp@lbsavings.com.

For additional security, the Bank recommends the following:

- Install Firewalls and set them to automatically update.
    - Firewalls are an electronic brick wall that helps keep hackers from intruding into your system. A firewall is like a guard, watching for outside attempts to access your system and blocking communications to and from unpermitted sources.
- Use one computer exclusively for online banking activities and assure its physical security. This computer should not be accessible to the general public, customers or vendors.
- Use password protection to access your computer and lock your computer when stepping away from your desk.
- Use automatic timeouts for additional security to automatically lock your computers after a period of inactivity.
- Set up your users with dual control requirements. Dual control is accomplished when one user initiates an external transfer and the second user verifies and approves the transaction.
- Periodically review your users and update your controls, passwords and procedures.
- Do not include sensitive information such as social security numbers, account numbers and log in credentials in an unsecured email even if it is sent to a trusted email address.

Refer to the Schedule B of the Business Banking Services Suite Agreement for additional information on security procedures.

It is important that you protect your business and customers' information by educating yourself and employees when using internet connected systems. The internet has become a primary source for criminals to obtain personal identifying information, passwords and banking information and use these to gain unauthorized access to financial accounts to perpetrate identity theft and other illegal acts. Awareness of existing threats will enable you and your employees to employ practices and behaviors that limit your risk. Please be advised that these are just a few of today's threats and security measures. There are numerous security measures available and new threats being created every day.

Viruses

Viruses are harmful computer programs that can be transmitted in a number of ways but mainly travel through email. Although they differ in many ways, all are designed to spread from one computer to another through the internet and cause havoc. Most commonly, they are designed to give the criminals who create them some sort of access to infected computers.

- To protect against computer viruses, the Bank recommends that you use anti-virus software and set it to automatically update.
    - Anti-virus software scans your computer as well as incoming email and attachments for viruses and will alert you if threats exist, giving you the option to delete them.

Spyware/Malware

Two important things to know about spyware and malware programs are:

- They can be downloaded onto your computer without your permission when visiting unsafe websites; bundled in with other downloads such as applications or games; included in an email attachment; or installed on your computer by someone with physical access.
- They can cause your computer to do unwanted things. This might be as simple as opening an advertisement or pop-up you did not authorize. In the worst cases, spyware and malware programs can track your online movements; log your keystrokes to steal your passwords and compromise your accounts and systems; send copies of emails and other documents to third parties; launch attacks such as sending infected emails and attachments to people in your contact lists; or redirect you to websites you never intended to visit. To protect against spyware and malware programs, the Bank recommends that you:
    - Use anti-malware software and set it to automatically update. We offer Trusteer Rapport as an anti-malware solution to safeguard your banking sessions. Simply download it when prompted upon log in to Business Online.
        - Anti-malware software periodically scans your computer for spyware and malware programs and gives you the opportunity to remove any harmful surveillance software it finds on your computer.
- Use a web filter to monitor and regulate internet surfing of employees.
- Do not open unsolicited email messages.
- Do not open a program or file attachment unless you know it is legitimate.

Phishing, Vishing and Smishing

Phishing attacks typically use fraudulent emails, phone calls (vishing) or text messaging (smishing) to trick consumers into sharing their personal data such as Social Security numbers, credit card account numbers, user names, passwords, etc.

If you receive a suspicious and/or unexpected email, phone or text, do not click any links right away and use the following techniques to protect yourself from potential attacks:

- Do not respond to emails or phone calls asking for personal information.
- Hover your mouse over the link to observe the URL details without clicking the link. This will allow you to validate where the link will take you. If the URL is unrecognizable or there are any doubts, delete the email promptly.
- If the suspicious email is from a company or a bank, open a new browser, go to the organization's website directly and log in to check the status of your account and/or make monetary transactions.
- Be cautious of telephone numbers when receiving phone calls or text messages. If you receive a text that looks genuine but the text is an unexpected form of communication from that company/person, contact the company/person directly by alternate methods and do not reply to the text.
- Use security software that interacts with your web browser to help identify websites that are generally known to be unsafe and used in phishing attacks.

For additional information on security measures and current fraud trends, please visit the following websites:

FDIC.gov
ftc.gov
nacha.org
achrulesonline.org (ACH Originators)