Luther Burbank®
Savings

Protect yourself from identity theft and fraud.

Luther Burbank Savings has invested in the technologies, processes and people necessary to safeguard the privacy of customer information. To learn how to secure your personal and financial information, please read the following:

Equifax Data Breach

For general information regarding the Equifax data breach and how to protect yourself, visit the Federal Trade Commission (FTC) Consumer Information website at https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

Online Activity

Email and Text Security: Verify unexpected emails or texts through a trusted channel, such as a published phone number, before clicking links or downloading attachments. Personal and business email accounts should have effective spam and virus filtering. Never respond to an email or text message with personal or financial information, as these are not secure methods for transmitting sensitive information.

Computer Security: All computers connected to the internet should have a host-based firewall and effective anti-virus software, plus the operating system and all applications should have current patches and security updates installed. Avoid accessing online banking services on public computers like those found in libraries or hotels.

Password Security: Passwords should be complex – no less than eight characters in length and composed of numbers, letters (both upper and lower case) and special characters. Never share passwords and always store them securely. *Important: Luther Burbank will never ask you for your password.*

For more tips on email, computer and password security, visit the Department of Homeland Security website at https://www.us-cert.gov/ncas/tips.

Trusteer Rapport: For additional security, Luther Burbank offers all online banking customers access to IBM® Trusteer Rapport. To learn more, visit the Security page on our website at https://www.lutherburbanksavings.com/banking-resources/security.

Protect Sensitive Documents

Keep sensitive documents in a secure location. Hard copies with personal or financial information should be shredded before being recycled.

Secure Mobile Devices and Computers

Access Controls: Require passwords, PINs or biometrics (e.g. thumbprints) to log into mobile devices and computers to access your information. Configure mobile devices and computer screens to automatically lock after a period of inactivity and require a password, PIN or biometric to log back into the device.

Monitor Accounts

Monitor financial and credit accounts, including online banking activity, bank statements (eStatements), retirement account statements and credit reports. Suspicious account activity should be reported immediately. For more information about annual credit reports, visit https://www.annualcreditreport.com.

Additional Information

For more information regarding privacy and security, visit the Banking Resources page on our website at https://www.lutherburbanksavings.com/banking-resources.

Member FDIC