Lake City Bank

Protect Your Financial Information

PASSWORDS

- Use a 10 digit combination of letters and numbers for your passwords, and change them periodically.
- Use different passwords and challenge questions for non-financial sites (e.g. online stores, games, social media, etc.) and your financial accounts. If you use the same information for all sites you access, the potential to compromise your bank accounts is higher.
- When creating passwords and PINs (personal identification numbers), don't use any part of your Social Security number, birth date, middle name, wife's name, child's name, pet's name, mother's maiden name, address, consecutive numbers, or anything that a thief could easily deduce or discover.

ATM/ DEBIT CARD

- Keep your ATM/Debit card in a safe place and treat it just like you would cash, credit cards or checks.
- Keep your Personal Identification Number (PIN) a secret. Never write it down anywhere, especially on your ATM/ Debit card.
- Never give any information about your ATM/Debit card or PIN over the telephone. If you receive a call, supposedly from your bank or possibly the police, wanting to verify your PIN, do not give that information.
- Always take your receipts or transaction records with you.

> ***TIP - Set up ATM/Debit Card Alerts***
> Receive email or text alerts for specific transaction types and card status changes.

E-MAILS/ PHISHING

- Never give out your personal financial information in response to an unsolicited phone call, fax or email, no matter how official it may seem.
- Do not respond to email that may warn of dire consequences unless you validate your information immediately. Contact the company to confirm the email's validity using a telephone number or web address you know to be genuine.
- Check your credit card and bank account statements regularly and look for unauthorized transactions, even small ones. Some thieves hope small transactions will go unnoticed. Report discrepancies immediately.
- When submitting financial information online, look for the padlock or key icon at the bottom of your internet browser. Also, many secure internet addresses, though not all, use "https" to signify that your information is secure during transmission.
- Don't open email from unknown sources. Use virus detection software.

> **What is *Phishing*?**
> Con artists can use email to try to hijack your personal financial information in a scam known as "phishing." Swindlers claim to be from a reputable company and send out fake emails (often with logos and banners copied from the company's website) telling you that their security procedure has changed or that they need to update/validate your information. Then they direct you to a look-alike website. If you respond, the thieves use your information to order goods and services or obtain credit.

CELL PHONE/ MOBILE BANKING

- Avoid storing sensitive information like passwords and social security numbers on your mobile device.
- Password protect your mobile device and lock it when you're not using it.
- Be aware of your surroundings. Don't type any sensitive information if others around you can see.
- Log out completely when you complete a mobile banking session.
- Protect your phone from viruses and malware just like you do for your computer by installing mobile security software.
- Download the updates for your phone and mobile apps.
- Use discretion when downloading apps.
- If you change your phone number or lose your mobile device, let your financial institution know right away.

MAILBOX

- Do not leave bill payment envelopes clipped to your mailbox or inside with the flag up. Criminals may steal your mail and change your address.
- Know your billing cycles and watch for any missing mail. Follow up with creditors if bills or new cards do not arrive on time. An identify thief may have filed a change of address request in your name with the creditor or the post office.
- Carefully review your monthly accounts, credit card statements and utility bills (including cell phone bills) for unauthorized charges as soon as you receive them. If you suspect unauthorized use, contact the provider's customer service and fraud departments immediately.

TIP - Switch to online bill payment!
In addition to being secure, you'll save money on postage!

PURSE/ WALLET

- Never leave your purse or wallet unattended ... even for a minute.
- Protect your PINs and passwords ... don't carry them in your wallet!
- Carry only personal identification and credit cards you actually need in your purse or wallet. If your ID or credit cards are lost or stolen, notify the creditors immediately and ask the credit bureaus to place a "fraud alert" in your file.
- Keep a list of all your credit cards and bank accounts along with account numbers, expiration dates and credit limits, as well as the telephone numbers of customer service and fraud departments. Store this list in a safe place.

Lake City Bank
Member FDIC

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