Our Commitment to Your Security.

At Guadalupe Bank, we're committed to keeping your accounts and personal information as secure as possible. Our online banking system uses various methods, tools, and processes to accomplish this, including:

Encryption: Once you begin the login process, the exchange of information over the Internet is encrypted. This means the information is scrambled in such a way that it cannot be read by anyone other than you and Comerica.

Automatic Logoff: If no action is taken for a preset interval, your session will be automatically terminated and you will be logged off.

Authentication: Some systems may require enhanced authentication from time to time to verify a user's credentials or activity.

Dual approval: Some systems may require one individual to initiate a payment and a second individual to approve it.

Constant Monitoring: We monitor our systems to prevent any potential problems that could compromise security or privacy.

Protect Yourself Online: What can you do to maximize your online security?

User ID and Password Guidelines

- Create a "strong" password with at least 8 characters that includes a combination of mixed case letters, numbers, and special characters.
- Change your password frequently.
- Never share username and password information with third-parties.
- Avoid using an automatic login feature that saves usernames and passwords.

General Guidelines

- Do not use public or other unsecured computers for logging into online banking.
- Check your last login date/time every time you 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 your financial institution.
- View transfer history by viewing account activity information.
- Whenever possible, use Bill Pay instead of checks to limit account number dissemination exposure and to obtain better electronic record keeping.
- Take advantage of and regularly view system alerts; examples include:
    - Balance alerts
    - Transfer alerts
    - Password change alerts
    - ACH Alerts (for cash management users)

    - Wire Alerts (for cash management users)

- Do not use account numbers, your social security number, or other account or personal information when creating account nicknames or other titles.
- Whenever possible, register your computer to avoid having to complete authentication procedures with each login.
- 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 online banking.
- Never conduct banking transactions while multiple browsers are open on your computer.

Tips to Protect Online Payments & Account Data

- Take advantage of transaction limits.
- When you have completed a transaction, ensure you log off to close the connection with the financial organization's computer.
- Use separate accounts for electronic and paper transactions to simplify monitoring and tracking any discrepancies.
- Reconcile by carefully monitoring account activity and reviewing all transactions initiated by your company on a daily basis.

Guard Against Email Fraud

- Do not open e-mail from unknown sources. Be suspicious of e-mails purporting to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes, and similar 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 hyperlink 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 your financial organization seems suspicious, checking with your financial organization may be appropriate.
  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 an online banking session in order 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.

ATM Security

- Always keep your card in a safe place.
- Safeguard your Personal Identification Number (PIN).
- Never lend your card to anyone and never share your PIN.
- Do not carry your PIN in your wallet or purse. Never write it on your card.
- Never give out your card information or PIN over the telephone.
- Report your card lost or stolen as soon as you become aware it is missing.
- Be aware of your surroundings. Avoid ATMs that have places nearby to hide, such as shrubs or corners.
- Have your card in your hand and ready to use when you approach the ATM.
- Visually inspect the ATM for possible skimming devices. Look for sticky residue or evidence of an adhesive used by criminals to affix the device to the machine. Scratches, damaged or crooked pieces and loose or extra attachments on the card slot should all be considered suspicious.
- Make sure no one can see you enter your PIN. Shield the keyboard with your body if necessary.
- Be wary of strangers offering to help you at the ATM.
- Always take your receipts with you.
- Do not count or display your money at the ATM. Place it out of sight and count it later.
- When using a drive up ATM, keep your passenger windows rolled up and your doors locked. Leave enough room to maneuver between your car and the car ahead of you in line.
- Reconcile your monthly bank statements and report any questionable withdrawals to us.
- When using the ATM at night take someone with you when possible.
- Park close if you must walk up to the ATM.
- If the ATM is not well lit, don’t use it.