LINKBANK
A DIVISION OF THE GRATZ BANK

THE GRATZ BANK

Security Standards

We understand that the confidentiality and security of your personal information and account information are of utmost importance. Therefore, we protect your information from unauthorized access by maintaining high security standards. Information that may be collected is used to administer customer accounts, provide uncompromising service and offer products and services that we believe will be of benefit to you based on your financial habits.

Data Encryption

When you use The Gratz Bank online banking, you are conducting business over a secured connection using encrypted data transmissions. Your data is encoded by Transport Layer Security (TLS), which is the Internet's most secure encryption protocol. This means the financial information you send to and receive from us is not visible or available on the Internet in a form that could be read. Following Banking standards (PCI DSS), passwords are always hashed (encoded) and never accessible to any person or system.

Best Practices for Security

Please note that we will never send you an email or text message requesting you to provide or confirm your username and password. Do not provide this information if you are asked to do so.

Online Banking

Our online banking system provides you with the date and time of your last session ("last login") located in the upper right corner when you sign in. This allows you to verify the most recent online session. If you notice a date and time when you believe you did not sign in, someone may have been accessing your information.

The Gratz Bank's website or Online Banking should only be accessed by typing www.GratzBank.com or www.linkbank.com into your web browser's URL bar, and should never be accessed from a link provided by a third party.

Username and Password

Please follow these guidelines to protect your confidential information:

1. Never disclose your username or password to anyone.
2. Memorize your username and password; do not write them down.
3. Use a mix of capital and lowercase letters, numbers, and symbols.
4. Change your password regularly.
5. Do not use birth dates, names, or other easily guessed information.

Log Out of Your Session

When you have completed your Online Banking session, always click “Sign Out” using the link in the upper right corner of the portal.

Email

Do not use an email account to send us sensitive information, such as social security numbers and account numbers. Emails are not secure and leave your information vulnerable to theft. You may send us a secure message through our Contact Us form.

Public Computers, Internet Access

Do not use public computers or public Internet access such as “Internet Cafes” or “Free Wi-Fi” to conduct online banking.

Phishing, Spoofs, Hoaxes and Other Deceptive Emails

Be careful when responding to email messages that appear to be from us, a regulator or an auditor. Thieves or hackers send email messages that direct you to click on a link which redirects you to a fraudulent website or pop-up window where you may be asked to “confirm, verify, update” or otherwise provide sensitive information. These links, websites and pop-up windows may look like ours with the same logo and colors and may falsely threaten that your account will be shut down if you do not act quickly. Do not be intimidated by these threats. Clicking a link in one of these emails can expose your computer to viruses and spyware, even if you do not supply the sensitive information thieves want. If you have any doubts about whether an email from us is authentic, do not reply to it, do not open any attachment, and do not use the link in the email. Instead, send us a message through our Contact Us form, or call us at (855) 569- 2265.

Spam

Do not open attachments in email messages if you do not know the sender. Attachments can contain viruses and spyware. Delete unwanted or suspicious email.

Links to Other Websites

If you click a link to another website, that website may collect, use, and disclose information about you in ways that are different from what we do. You should review that website’s policies. We are not responsible for what the operators of other websites do with your information.

Security for Your Own Computer

Protect your own computer with regular maintenance:

1. Keep your operating system and browser updated.
2. Install anti-virus software, including firewall and malware protection, and keep it updated.
3. Scan your computer for spyware regularly.
4. Do not download programs or files from unknown sources.
5. Install a pop-up blocker from a trustworthy source.