TEXAS GULF BANK, N.A.

ONLINE BANKING SECURITY

Texas Gulf Bank is committed to keep your Online Banking information safe and secure. In doing so, we employ security measures that comply with Federal Regulations. As mandated by the FFIEC (Federal Financial Institutions Examination Council), Texas Gulf Bank has incorporated Multi-Factor Authentication since 2006. Multi-Factor Authentication incorporates multiple technologies to create a customer profile, including IP information, geographical location and transactional data and patterns.

When you initially set up your online banking, our system will monitor such things as the URL and computer you are using to access our system. If, at some point in the future, you happen to use another computer, access from a different URL, or are performing an activity which has been classified as high risk, our monitoring system may require additional information other than user ID and password, to further verify your identity. You will randomly be asked two of the three questions you supplied at your initial set up to further verify your identity.

Please keep in mind that we will never ask for or email you requesting your Online Banking password. We may on occasion call to verify other information regarding your online activity should we see something of concern in your login patterns. If you plan to travel and use your Online Banking or debit card, it is very helpful to call us in advance to avoid your account being temporarily disabled for security purposes.

Texas Gulf Bank values the protection of your information. The information and resources below are provided to help you safeguard your personal information.

Phishing Scams

Phishing refers to attempts to steal personal financial information, such as credit card numbers, account usernames/passwords, and social security numbers, through fraudulent e-mails, phone calls (vishing), text messages (smishing) and websites that will be used for fraudulent purchases.

How phishing works:

1. You receive an e-mail or text message which appears to originate from a financial institution, government agency or other well-known or reputable entity.
2. The fraudulent message usually provides a number to call where they must verify or update personal information, such as passwords, credit card, social security number and bank account numbers which the legitimate organization already has.
3. The website, however, is bogus and set only to steal the user’s information.

How to Avoid Phishing:

- Do not reply to these messages or visit websites include in e-mails warning that your account will be shut down unless your information is confirmed
- Do not send sensitive data such as passwords, account numbers or social security numbers in response to an e-mail or text message
- Do not reveal a personal/financial information or site password to anyone. Your bank has this information
- Do not click on links in an e-mail. Go directly to the company main website
- Contact the company in the e-mail by using a telephone number or website address you know to be genuine
- Before submitting financial information through a website, look for the "lock" icon on the browser status bar to ensure your information is secure during transmission
- Report suspicious activity to the Federal Trade Commission at www.ftc .gov

Identity Theft

You often don't know you've become a victim until the fraudulent activity shows up in your bills or bank statements. Protect yourself from identity theft.

Identity Theft often occurs when someone steals your personal information (such as bank and credit card numbers, your Social Security number, name and address) to commit fraud or theft. You often don't know you've become a victim until fraudulent activity shows up in your bills, bad credit reports, and more. It is recommended that you review your credit report annually. You can do so by visiting www.annualcreditreport.com to order an annual free credit report.

Safeguard personal information from being stolen:

- Use secure personal identification numbers (PIN)/passwords and a secure Web browser
- Do not use obvious passwords (birth date, mother's maiden name, telephone, social security number, etc.)
- Review all statements upon receipt and shred any unneeded documents with personal information
- Do not store financial information on a laptop computer, which can be easily stolen
- Beware of solicitors – do not give out information unless you have initiated the contact
- Do not leave outgoing mail in your mailbox and collect your incoming mail daily

If you are a victim of identity theft:

- Contact Texas Gulf Bank immediately if you feel your accounts have been affected
- Contact each of your creditors to determine if there has been any unauthorized activity or any new accounts have been opened that are fraudulent. Keep records of communications
- Immediately file a report with your police department and keep a copy of the report in case your creditors request it
- File a complaint with the Federal Trade Commission online at www.ftc.gov or call 1-877-IDTHEFT

- Contact each of the three credit reporting agencies to have a fraud alert placed on your account; creditors will then be instructed to obtain your authorization before opening any new accounts:
    - Equifax 800-525-6285
    - TransUnion 800-680-7289
    - Experian 888-397-3742

Business Accounts

Unfortunately business accounts are also targets of identity theft and other fraudulent activity. Information to help prevent this fraudulent activity is provided below.

Steps you can take to ensure your Online Banking security:

- Conduct reconciliation of banking transactions on a daily basis
- Initiate ACH and wire transfer payments under dual control
- Familiarize yourself with Texas Gulf Bank's account agreement
- Immediately escalate any suspicious transactions to Texas Gulf Bank, particularly ACH or wire transfers—there is a limited recovery window for these transactions and immediate escalation may prevent further loss.

Best Practices to help secure computer system:

- For businesses that transact high value or large numbers of online transactions, it is recommended that all commercial online banking activities be carried out from a stand-alone, hardened and completely locked down computer from which email and web browsing are not possible
- 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 emails could expose your system to malicious code that could hijack your computer
- Install a dedicated firewall; a firewall limits the potential for unauthorized access to a network and computers
- Create a strong password with at least 8 characters that includes a combination of mixed case letters, numbers and special characters
- Prohibit the use of "shared" usernames and passwords for online banking systems
- Use a different password for each website that is accessed
- Change the password at lease several times each year
- Never share username and password information for online services with anyone
- Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses
- Install commercial anti-virus and desktop firewall software on all computer systems
- Ensure virus protection and security software are updated regularly
- Make sure certain computers are patched regularly
- Consider installing spyware detection programs
- 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
- Verify use of a secure session (https not http) in the browser for all online banking

- Avoid using automatic log-in features that save usernames and passwords for online banking
- Never leave a computer unattended while using any online banking or investing service
- Never access bank, brokerage or other financial services information from internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign on information leaving you vulnerable to possible fraud.

Viruses, Spy Ware and Firewalls

A virus is a type of software that “infects” computers. It’s typically inserted into a program, and when that program is executed, the virus activates. Viruses can infect immediately, or on a specified date. They can affect single desk tops, or spread to entire networks, servers and Websites. While many viruses are just pranks or annoyances, others are more complex. Viruses can destroy data, corrupt programs so that they no longer run, steal passwords and infect address books.

Spyware is like a virus in that it is an unwanted program that runs on your computer. However, it does not try to replicate itself to other machines. Infection usually occurs when it is installed alongside another program such as a peer to peer file sharing application. However, increasingly, spyware is blending with viruses making it harder to eradicate and harder to avoid.

There are different types of spyware; some are more damaging than others.

Spyware can do a lot;

- Pop-up unwanted advertisements, including offensive material
- Block access to certain websites
- Try to get you to shut down anti-virus or anti-spyware defenses
- Block updates to these defenses
- Scan your hard disk for private data such as credit card numbers
- Log the keys you type scanning for passwords or credit card numbers
- Take screen shots of the sites you visit to capture personal information
- Upload this information to criminals over the internet.

Prevention tips:

- Keep your Antivirus/Spyware software up-to-date
- Avoid running attachments (especially .EXE files) that come in your e-mail, even if they come from your friends, relatives or colleagues
- Use a firewall
- Get the latest windows updates
- Make frequent backups of your data files and keep some of your backups out of your computer
- Conduct Information Technology Risk Assessments.

Firewalls help keep you safe

Because the internet is a public network, any connected computer can find and connect to any other connected computer. A firewall is a barrier between the public internet and your private computer system. A firewall isn’t sufficient on its own to guarantee security, but it is the first line of defense.

- A firewall provides limited or no protection against:
- If you give permission for other computers to connect to yours
- If it is switched off, disabled or contains many exceptions or open ports
- Against most viruses
- Against spam against spyware installation
- Against any kind of fraud or criminal activity online
- If you or a virus has created a back door through the firewall
- If a hacker has the password for the firewall
- Against people with physical access to your computer or network
- Against malicious traffic that does not travel through it, for example via a poorly configured wireless network
- Against attacks after a network has been compromised
- Against traffic that appears to be legitimate.