Protecting Yourself Online

Conducting Your Transactions Online

Federal financial regulators are reporting that Internet threats have changed significantly over the past several years. Sophisticated hacking techniques and growing organized cyber-criminal groups are increasingly targeting financial institutions, compromising security controls, and engaging in online account takeovers and fraudulent electronic funds transfers.

In order to help ensure the security of your online transactions, we want you to know that:

- We will never email, call, or otherwise ask you for your user name, password, or other electronic banking credentials
- You can help protect yourself by implementing alternative risk control processes like:
    - Making sure you choose an adequate user name and password that, at a minimum, mixes in small case letters, upper case letters, and numbers
    - Periodically changing your password
    - Safeguarding your user name and password information
    - Having current anti-malware and anti-virus software
    - Making sure you have a firewall in place when conducting your financial transactions
    - Logging off the system when you're done conducting business (don't just close the page or "X" out of the system)
    - Monitoring your account activity on a regular basis

In addition, we may require owners of commercial accounts to perform their own risk assessments and controls evaluations. For example:

- Make a list of the risks related to online transactions that your business faces including:
    - Password being written down and left out in the open
    - The use of old or inadequate passwords
    - The possibility of internal fraud or theft
    - Delays in terminating the rights of former employees
    - The lack of dual control or other checks and balances over individual access to online transaction capabilities
- An evaluation of controls your business uses may include:
    - Using password protected software to house passwords in
    - Conducting employee background checks
    - Initiating a policy and process to terminate access for former employees
    - Segregating duties among two or more people so no one person has too much access or control

- Conducting internal or third party audits of controls
- Using firewalls to protect from outside intrusion or hackers

Federal regulations provide consumers with some protections for electronic fund transfers. These regulations generally apply to accounts with Internet access. For example, these federal laws establish limits on a consumer's liability for unauthorized electronic fund transfers. They also provide specific steps you need to take to help resolve an error with your account. Note, however, that in order to take advantage of these protections, you must act in a timely manner. Make sure you notify us immediately if you believe your access information has been stolen or compromised. Also, review your account activity and periodic statement and promptly report any errors or unauthorized transactions. See the Electronic Fund Transfer disclosures that were provided at account opening for more information on these types of protections. These disclosures are also available online (or ask us and we will gladly provide you with a copy).

If you become aware of suspicious account activity, you should immediately contact the authorities and contact us at the number listed below.

DILLEY STATE BANK
830-965-1511

Personal Security Guidelines

Security Guidelines - Do's & Dont's

Security and privacy are of paramount importance to Dilley State Bank. While we do our utmost to ensure security and confidentiality, there are steps you should take to enhance your security and to protect yourself against identity theft.

The following information is provided as a guide to assist you in protecting the information on your computer. It is not an exhaustive list and is intended for informational purposes only.

Do's

- Do keep your computer user ids and passwords confidential and secure.
- Do choose your password carefully. Choose a password that uses a combination of characters, numbers, and symbols. See our guidelines for creating strong passwords.
- Change your password regularly.
- Be alert when using a PC for online banking and other transactions in public areas such as Internet cafes.
- Install reputable anti-virus software and ensure that it is updated regularly. Check with your local software supplier on the best software for you. Remember that you get what you pay for when downloading “Free” anti-virus software.
- Install reputable anti-spyware software and ensure this software is regularly updated. Check with your local software supplier on the best software for you.

- Install a personal Internet firewall to provide extra protection for your computer.
- When you've finished using the Internet Banking service, make sure you click on Logout to exit.
- Close your Internet browser after logging out of each Internet Banking session.
- Turn off your computer when it is not in use.
- Check the 'Last Logged In' information in each internet banking session - report promptly any irregularities to us.
- Report suspected security breaches immediately. If you are concerned that another person has ascertained your password, you should immediately change it and advise us by calling 830-965-1511.
- Check your statements for any transactions that look suspicious.
- Cancel any card that has been used fraudulently.

Don't

- Do not access banking sites from a link in an email.
- Never, in response to any email, provide your personal or security details, including debit card PIN or Internet Banking user id or password.
- Do not open, run, install or use programs or files obtained from a person or organization you do not know or is not a reputable vendor.
- Do not open email attachments from unknown sources. Email is one of the prime movers for malicious viruses. Delete any emails you think are suspicious. Delete the email from your 'Inbox', and delete it again from your 'Deleted' folder, or 'Sent' folder if you have forwarded the email.
- Never open an executable (.exe file) retrieved or received online unless you are expecting it from a trusted source.
- Do not leave the screen idle for long periods or leave your PC unattended.

Ways to Protect Your Accounts

Protect Your Identity

1. Never provide your personal information in response to an unsolicited request, whether it is over the phone or over the Internet. E-mails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you did not initiate the communication, you should not provide any information.
2. If you believe the contact may be legitimate, contact the financial institution yourself. You can find phone numbers and websites on the monthly statements you receive from your financial institution, or you can look the company up in the phone book or on the Internet. The key is that you should be the one to initiate the contact, using contact information that you have verified yourself.
3. Never provide your password over the phone or in response to an unsolicited Internet request. A financial institution would never ask you to verify your account information

online. Thieves armed with this information and your account number can help themselves to your savings.

4. Review account statements regularly to ensure all charges are correct. If your account statement is late in arriving, call your financial institution to find out why. If your financial institution offers electronic account access, periodically review activity online to catch suspicious activity.

Report all suspicious contacts to the Federal Trade Commission through the Internet at www.consumer.gov/idtheft, or by calling 1-877-IDTHEFT.

Protect Your ATM / Debit Card

1. **Never disclose your PIN number and reset it regularly.** Only you have your PIN - not even the bank or card processors know your PIN. It is best to memorize your PIN. If you write it down, store it in a safe place that is not accessible to others. Protecting your PIN is your first and most important line of defense.
2. **Carefully select your PIN.** Do not use obvious codes when selecting a PIN. If you suspect someone knows your PIN, then reset it.
3. **Protect your PIN.** Use your hand or body to shield the PIN pad to prevent "shoulder surfers" from observing your PIN.
4. **Monitor your account activity regularly.** Access your account via your Dilley State Bank Online Banking account to monitor your latest account activity.
5. **Swipe your card yourself.** If you have your card, a thief does not. Insist on retaining physical control of your card to prevent skimming. Always safeguard your card and never lend it to anyone.

If you discover fraud on your card, report the fraud to the police as soon as possible. Then, inform the bank. The bank will cancel your card and issue you a new one (with a different number, of course) immediately. You may also call the Federal Trade Commission at 877-FTC-HELP.

Your personal financial security is important to Dilley State Bank. Please take these precautions to protect your family's and business' financial well being. We appreciate the opportunity to be your bank!