PINNACLE BANK
REACH HIGHER

Online Banking Fraud Prevention Best Practices

The following are best practices that you can implement to protect your personal information.

User ID and Password Guidelines

- Create a "strong" password that is difficult to guess.
    - Create an acronym from an easy-to-remember piece of information. For example, pick a phrase that is meaningful to you, such as My son's birthday is 12 December, 2004. Using that phrase as your guide, you might use Msbi12/Dec,4 for your password.
    - Substitute numbers, symbols, and misspellings for letters or words in an easy-to-remember phrase. For example, My son's birthday is 12 December, 2004 could become Mi$un's Brthd8iz 12124 (it's OK to use spaces in your password).
    - Relate your password to a favorite hobby or sport. For example, I love to play badminton could become ILuv2PlayB@dm1nt()n.
- Change your password frequently.
- Never share username and password information with anyone. Pinnacle Bank will never contact you on an unsolicited basis and request customer provisions of electronic banking credentials.
- Avoid using an automatic login feature that saves usernames and passwords

General Guidelines

- Do not use public or other unsecured computers for accessing your account or services through internet banking.
- Check your last login date/time every time you log in.
- Review account balances and detail transactions regularly (preferable daily) to confirm payment and other transaction data and immediately report any suspicious transactions to us at 888-485-7050.
- View transfer history through viewing account activity information.
- Whenever possible, use Bill Pay instead of checks to limit the account number dissemination exposure and to obtain better electronic record keeping.
- Take advantage of and regularly view systems alerts; examples include:
    - Balance alerts
    - Transfer alerts
    - Password change alerts
- 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 re-enter challenge questions and other authentication information with each login.
- Never leave your computer unattended while using online banking or any internet banking product.
- Never conduct banking transactions while multiple browsers are open on your computer.
- Immediately contact us at 888-485-7050 for all customer information security-related events.
- For business banking clients, perform a related risk assessment and controls evaluation periodically.

Tips to Protect Online Payments, Wires, Transfers & Account Data

- Take advantage of transactions limits.
- When you have completed a transaction, ensure you log off to close the connection with the online banking application.
- Utilize applicable transaction alerts.

Administrative Users

- Limit administrative rights on user's workstations to help prevent the inadvertent downloading of malware or other viruses.
- Limit the number of computers used to complete online banking or internet transactions; do not allow Internet browsing or e-mail exchange and ensure these computers are equipped with the latest versions and patches of both anti-virus and anti-spyware software.
- Delete online user IDs as part of the exit procedure when employees leave your company.
- Assign dual system administrators for online cash management services, e.g. wire transfers.
- Use multiple approvals for monetary transactions and require separate entry and approval users.
- Establish transaction dollar limits for employees who initiate and approve online payment such as wire and account transfers.