PINNACLE BANK

Online Banking Fraud Prevention Best Practices

Online safety is Pinnacle Bank's number one priority when it comes to Online Banking.
The following are best practices that you can implement to protect your personal information.
Immediately contact Pinnacle Bank at 888-485-7050 for all customer security-related events.

User ID and Password Guidelines

- ✓ **Create a "strong" and unique password that is difficult to guess.**
  - o Create an acronym from an easy-to-remember phrase or piece of information. Such as birthdays, favorite sports, or hobby.
    Example: My son's birthday is 12 December 2004.
    Using that phrase as your guide, your new password might be Msbi12/Dec,4.
  - o Substitute numbers, symbols, and misspellings for letters or words in an easy-to-remember phrase.
    Example: I love to play badminton could become ILuv2PlayB@dm1nt()n.
- ✓ **Change your password frequently.**
- ✓ **Avoid using an automatic login feature that saves usernames and passwords.**
- ✓ **Never share username and password information with anyone. Including family, friends, and colleagues.**
  Pinnacle Bank will never contact you on an unsolicited basis and request customer provisions of electronic banking credentials.

General Guidelines

- ✓ **Avoid using shared computers and public Wi-Fi for accessing your online banking services.**
- ✓ **Check your last login date/time every time you sign in.**
- ✓ **Keep up on updates.**
  Your devices and web browsers should always be updated to the latest versions to reduce security risks.
- ✓ **Review account balances and transaction details regularly (preferable daily) from a safe location, to confirm payment and other transaction data is valid.**
  Immediately report any suspicious transactions to us at 888-485-7050.

- ✓ **Take advantage of multi-factor authentication methods when available.**
- ✓ **Never leave your computer unattended while using online banking products.**
- ✓ **Once you have completed a transaction, ensure you log off to close the connection with the online banking application.**
- ✓ **Ensure your computers are equipped with the latest versions and patches of licensed anti-virus and anti-spyware software.**
- ✓ **Do not provide account details over email.**
- ✓ **Avoid the use account numbers, your social security number, additional banking or personal information when creating a username, account nickname or other titles.**
- ✓ **Keep the bank informed on any changes to your personal information.**
  Such as, but not limited to:
  - o Phone number
  - o Email address
- ✓ **Utilize and regularly view systems alerts.**
  Examples include:
  - o Transfer Alerts
  - o Balance Alerts
  - o Password Change Alerts
  - o Personal Information Change Alerts

Protect Online Payments, Transfers & Account Data

- ✓ **Take advantage of transactions limits and utilize transaction alerts.**
- ✓ **Whenever possible, use Bill Pay instead of checks to limit the account number dissemination exposure and to obtain better electronic record keeping.**
- ✓ **Avoid conducting banking transactions while multiple browsers are open on your computer.**
- ✓ **Report Lost/Stolen cards right away.**

Business 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.**
- ✓ **Delete online user IDs as part of the exit procedure when employees leave your company.**

- ✓ **Assign dual system control for online cash management services and monetary transactions.** *e.g., wire transfers and ACH Payments.*

- ✓ **Establish transaction dollar limits for employees who initiate and approve online payments.** *e.g., wire and account transfers.*

- ✓ **Perform a related risk assessment and controls evaluation periodically.**