PINNACLE BANK

Did you know that sharing Credentials, Passwords and Debit Card PINs can increase your chances of becoming a victim of fraud?

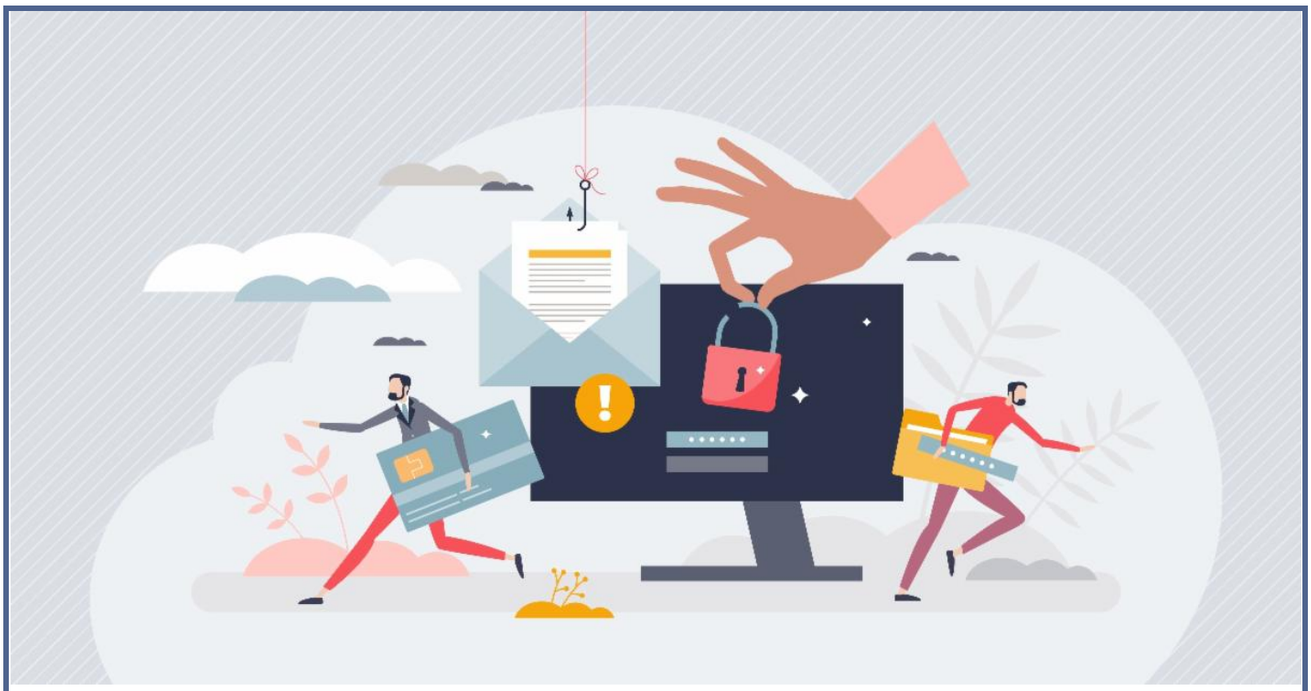
Pinnacle Bank takes client data protection seriously. Part of our efforts in combating fraud is educating our clients on effective and easy-to-implement security measures to avoid fraudulent activity on their accounts.

Why Should You Avoid Sharing Credentials, Passwords & PINs?

Passwords and Debit Card PINs have been the long-standing guardians keeping unauthorized persons from accessing your accounts and any related confidential data. However, these unique pieces of information are only truly secure when the owner keeps them private.

Sharing confidential account access information can increase the chances of fraudulent activity. Whether you share the information with your spouse or your most trusted coworker, confidential information could be at risk when credentials, a password or PIN fall into the wrong hands.

Below are some of the dangers that come with sharing credentials, passwords and PINs; as well as PIN and password management best practices that can be easily implemented to avoid becoming a fraud victim.



The Dangers of PIN & Password Sharing

Malicious Usage

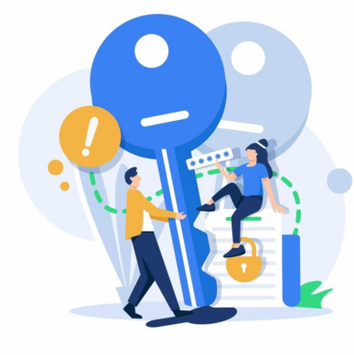
Traceability for important transactions is diminished when multiple users share a debit card or system credentials.

Account Loss

Shared Passwords increase the risk of account lockouts when credentials are updated and shared Debit Cards can decrease your detection of fraudulent activity.

Account Takeovers & Risks to Additional Systems

If a Password is entered into a malicious site by a shared user, the account owner risks greater account vulnerability if they are reusing passwords, leading account take overs on other accounts where the credentials may be the same.



Improving Password Management:

- Enable Multi-Factor Authentication
- Restrict Administrative Access
- Take Advantage of Multi-User Systems. Each authorized person should have their own access credentials.

Improving PIN Security & Management:

- Take advantage of card controls made available.
- Do not write down your PIN
- Assign a unique PIN, avoid having your PIN be a partial SSN, DOB, Anniversary date, etc.

- Businesses: Introduce a required procedure to remove access for terminated employees within a predetermined timeframe after their termination or notice of absence.

- Businesses: Ask about issuing each authorized person a debit card and take advantage of the card controls available.

Important! When sharing credentials, passwords and PINs, always keep in mind that by providing these secure pieces of information you are authorizing the person to act on your behalf.

To learn more about how to protect you and your business click on:

Online Banking Fraud Prevention Best Practices

Contact us right away if there's a problem!

If you believe you have been the victim of a fraud scheme, detected illegitimate activity on your account, or something just doesn't seem right — contact us immediately.

We will work with you to review your transactions to understand the extent of the issue.

Pinnacle Bank

(888) 485-7050

Get in Touch

PINNACLE BANK