BIPPUS STATE BANK

DIGITAL BANKING PASSWORD/SECURITY BEST PRACTICES

PASSWORDS

- Choose longer passwords, such as a phrase rather than a single word.
- Use a mix of upper and lowercase letters.
- Include numbers and special characters.
- Avoid common sequences, such as "1234."
- Avoid using personal information, such as your name, pets' names, date of birth, etc.
- Do not use the same password for multiple online applications.
- Never share your username and password with anyone.

SECURITY

- Do not use public or other unsecured computers for logging into Online Banking.
- Review account balances and transaction details regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to Bippus State Bank.
- Sign up for balance and transaction alerts by email, text, or both.
- Be wary of Phishing scams. We will never call or email you requesting your username, password, Personal Identification Number (PIN), or answers to your security questions.
- If attachments and links in email are unexpected or suspicious for any reason, do not click on them.
- Keep anti-virus/anti-malware software installed and up to date on computers accessing online banking.
- Never leave devices unattended unless they are locked so no one else can use them.
- Protect your mobile device by:
  - Adding a PIN or Touch/FaceID to unlock
  - Only install apps from trusted sources (such as Apple AppStore or Google Play)
  - Keep the operating system up to date
  - Use Apple's Find my iPhone or the Android Device Manager tools to help prevent loss or theft