**Security Tips**

**Using e-Banking: Online Banking, Mobile Banking, Telephone Banking**

The Online Banking service has several effective security techniques that we encourage you to implement when you use the Online Banking service:

* Never reveal your password to anyone or leave your password anywhere that someone else can obtain and use it.
* Change your password on a regular basis.
* Use the Exit button to end each Online Banking session. Do not use the Back button to exit the site.
* Balance your account on a regular basis. Online Banking makes it easy!
* Protect your computer & prevent unauthorized access: Use secure passwords.
* Password tips: Use complex passwords; Never share passwords with anyone; **Do Not** write passwords down for others to see.
* Protect your computer from Cyber Threats: Install virus protection, a firewall, and enable automatic updates.
* Protect mobile devices from unauthorized access.  Plan ahead for the possibility of the device being lost or stolen: Lock your cell phone or tablet when not in use and require a pass-code or fingerprint to unlock.  Enable "time-out" feature that auto locks your device when left unused for a certain period of time.
* Protect mobile devices from Cyber Threats: Enable auto updates.
* Educate yourself about Cyber Awareness: Example: Cyber-criminals use e-mails to download spyware and malware on your computer or device.  Be suspicious of unsolicited e-mails asking you to click a link or download an attachment.
* Cyber-criminals use social networking sites to gather details about individuals such as date of birth, mother's maiden name, and other personal info so be careful what you put on the internet.
* Bank of Brewton will never call, text or e-mail you asking for your private information so beware of imposers and con-artists.

**ATM / Debit Card Security**

* Treat your card like cash. Keep it in a safe place.
* Keep your personal identification number (PIN) a secret.
* Do not disclose card information over the phone to anyone. No one needs to know your PIN, not even your financial institution.
* Report a lost or stolen card at once.
* Carefully review your account statements.
* Do not write your ATM PIN on your card or anywhere near the card.  Commit the number to memory.

**Security Tips at Walk-Up ATMs**

* Observe the ATM surroundings before approaching a walk-up ATM. If anyone or anything appears to be suspicious, cancel your transaction and leave the area at once.
* If an ATM is obstructed from view or poorly lit, go to another ATM. It is a good idea to take along a companion when using an ATM, especially at night.
* Minimize time spent at the ATM by having your card out and ready to use. Do not let anyone see how much money you withdrew, and never count your money at the ATM.
* Never allow a stranger to assist you in conducting an ATM transaction, even if you have trouble or if your card is stuck.
* Stand between the ATM and anyone waiting to use the terminal so that others cannot see your PIN or transaction amount.
* Look for possible fraudulent devices attached to the ATM. If the ATM looks different or appears to have any alterations or attachments to the card slot or PIN pad, do not use it.

**Security Tips at Drive-Up ATMs**

* Keep the doors locked, windows up and engine running at all times when waiting in line.
* Leave enough room between cars to allow for a quick exit should it become necessary.
* Before lowering the window to use a drive-up ATM, observe the entire surrounding area. If anyone or anything appears to be suspicious, cancel your transaction and drive away at once.
* Minimize time spent at the ATM by having your card out and ready to use. Once your transaction is complete, take your money, card and receipt and immediately drive away from the terminal.
* If anyone follows you after you have completed your ATM transaction, go immediately to a crowded, well-lit area and call the police.

**Point-of-Sale (POS) Security**

* Never allow the cashier or anyone else to enter your PIN for you, even if they are assisting you with the transaction.
* Block the view of others when using a POS terminal.
* Be sure the transaction is complete and you have received a receipt before leaving.
* If you received cash back, put it away before leaving the terminal.
* When using an outdoor POS terminal such as at a gas station, observe your surroundings before making a transaction. If anything looks suspicious, leave the area at once.
* It is a good idea to take someone with you when using an outdoor POS terminal at night.
* If anyone follows you after you have completed your POS transaction, go immediately to a crowded, well-lit area and call the police.

**Preventing Debit Card Fraud**

* Sign immediately. Sign the signature panel on your debit card as soon as you receive it.
* Memorize your PIN. Don't carry your PIN (Personal Identification Number). Memorize it or keep the number at home.
* Verify your card. Be sure your debit card is returned after a purchase, and that it is indeed your card.
* Wait for your card receipt. Don't leave your debit card receipts at the checkout counter. Always take your charge slips and tear up any carbons.
* Save your receipts. Check them against your monthly billing or account statements to make sure you can identify all of your transactions. Report any unauthorized transactions immediately. After you have reconciled your billing statements, tear up all receipts and discard them at home.
* Check statements and watch your charges. Verify that your monthly statement reflects the amount you authorized. Be cautious when giving your card number over the phone. Also, watch for multiple charges.
* Keep it private. Keep your statements in a safe place.
* Out of sight. Never leave your purse or wallet unattended and always keep your cards out of plain sight.
* Never lend your card. Your debit card is your responsibility. Also, periodically check to make sure you have all your cards.
* Keep a list. In a separate location, keep a list of account numbers and telephone numbers to call if your cards are lost or stolen.