

Secure Your Mobile Device!

Passcode Lock: Lock your devices like you do the doors of your home! Make code **unique**.
Never leave your device unattended when it isn't locked!

Apps: Skip downloading apps that ask for unnecessary permissions. Install app updates!

Device : Your device's operating system and security software should be kept up to date.

AVOID storing personal information on your mobile device such as PIN #'s, Social Security Numbers or Passwords!

Monitor your accounts!!!

TAKE CHARGE of your accounts and use our eBanking services to protect yourself! Don't wait on your monthly statements to review the transactions on your accounts. Our eBanking services allow you to review your accounts **DAILY**. Download our Mobile App and have your account information at your fingertips no matter where you go.

Call us at 615-446-3732 for detailed information on how to take advantage of these services!!

Internet Safety:

Websites: Only shop on reputable sites that are secure. Look for the https in the web address.
LOG OUT when finished on the site!

Pop-ups: Malware and viruses hide in screens that pop up or also in "flashy" ads when you are on sites. Resist clicking on them! Consider installing a pop-up blocker program.

Mobile Devices: Treat your mobile device like a computer. It is also vulnerable to viruses and malware. Keep devices updated! Use the device's security settings.

Truth or Scam!

Email: NEVER open an attachment or click on a link in an email unless you **BOTH** trust the sender **AND** are expecting the email. NO "get rich quick" offer is legit! **DELETE!!**

Phone Call: No matter how convincing the story..NEVER agree to wire money, deposit a check or pay fees for a "prize you won", or for a threat of "legal action" against you. NEVER give out personal info over the phone!

Remember:

If you didn't enter, you for sure didn't "WIN"!!

Public Wi-fi & Social Media:

Public Wi-fi: Avoid performing financial transaction activity or use of passwords while on public wi-fi. Use only reputable hot spot providers or your data plan for such activity. Be aware of who may be looking over your shoulder as you use your phone!!

Social Media: Hackers use whatever info they can get from your public profiles. Limit the amount of personal info you post! Private messages disguised as being from a known friend can include attacks hidden in links. Beware of friend requests and make sure you know the request is real before accepting. Change your password often!

Social Media accounts are powerful tools in the wrong hands!