CYBERSECURITY FOR

SMALL BUSINESS

PLANTERS FIRST BANK

MEMBER FDIC

PROTECT YOUR WIRELESS NETWORK

Secure your router

Change the default name and password, turn off remote management, and log out as the administrator once the router is set up.

Use at least WPA2 encryption

Make sure your router offers WPA2 or WPA3 encryption, and that it's turned on. Encryption protects information sent over your network so it can't be read by outsiders.

MAKE SMART SECURITY YOUR BUSINESS AS USUAL

Require strong passwords

A strong password is at least 12 characters that are a mix of numbers, symbols, and capital lowercase letters.

Never reuse passwords and don't share them on the phone, in texts, or by email.

Limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

Train all staff

Create a culture of security by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. If employees don't attend, consider blocking their access to the network.

Have a plan

Have a plan for saving data, running the business, and notifying customers if you experience a breach. The FTC's *Data Breach Response: A Guide for Business* gives steps you can take. You can find it at FTC.gov/DataBreach.