CYBERSECURITY FOR
SMALL BUSINESS

PLANTERS FIRST BANK
MEMBER FDIC

PHYSICAL SECURITY

Cybersecurity begins with strong physical security.

Lapses in physical security can expose sensitive company data to identity theft, with potentially serious consequences. For example:

An employee accidentally leaves a flash drive on a coffeehouse table. When he returns hours later to get it, the drive — with hundreds of Social Security numbers saved on it — is gone.

Another employee throws stacks of old company bank records into a trash can, where a criminal finds them after business hours.

A burglar steals files and computers from your office after entering through an unlocked window.

HOW TO PROTECT EQUIPMENT & PAPER FILES

Here are some tips for protecting information in paper files and on hard drives, flash drives, laptops, point-of-sale devices, and other equipment.

Store securely

When paper files or electronic devices contain sensitive information, store them in a locked cabinet or room.

Limit physical access

When records or devices contain sensitive data, allow access only to those who need it.

Send reminders

Remind employees to put paper files in locked file cabinets, log out of your network and applications, and never leave files or devices with sensitive data unattended.

Keep stock

Keep track of and secure any devices that collect sensitive customer information. Only keep files and data you need and know who has access to them.