PFB

PLANTERS FIRST BANK

MEMBER FDIC

RANSOMWARE

Someone in your company gets an email.

It looks legitimate — but with one click on a link, or one download of an attachment, everyone is locked out of your network. That link downloaded software that holds your data hostage. That's a ransomware attack.

The attackers ask for money or cryptocurrency, but even if you pay, you don't know if the cybercriminals will keep your data or destroy your files. Meanwhile, the information you need to run your business and sensitive details about your customers, employees, and company are now in criminal hands. Ransomware can take a serious toll on your business.

HOW IT ——— HAPPENS

Criminals can start a ransomware attack in a variety of ways.

Scam emails

with links and attachments that put your data and network at risk. These phishing emails make up most ransomware attacks.

Server vulnerabilities

which can be exploited by hackers.

Infected websites

that automatically download malicious software onto your computer.

Online ads

that contain malicious code — even on websites you know and trust.