CYBERSECURITY FOR
SMALL BUSINESS

PLANTERS FIRST BANK
MEMBER FDIC

PHISHING

You get an email that looks like it's from someone you know.

It seems to be from one of your company's vendors and asks that you click on a link to update your business account. Should you click? Maybe it looks like it's from your boss and asks for your network password. Should you reply? In either case, probably not. These may be phishing attempts.

HOW PHISHING WORKS

You get an email or text

It seems to be from someone you know, and it asks you to click a link, or give your password, business bank account, or other sensitive information.

It looks real

It's easy to spoof logos and make up fake email addresses. Scammers use familiar company names or pretend to be someone you know.

It's urgent

The message pressures you to act now — or something bad will happen.

What happens next

If you click on a link, scammers can install ransomware or other programs that can lock you out of your data and spread to the entire company network. If you share passwords, scammers now have access to all those accounts.

WHAT YOU CAN DO

Before you click on a link or share any of your sensitive business information:

Check it out

Look up the website or phone number for the company or person behind the text or email. Make sure that you're getting the real company and not about to download malware or talk to a scammer.

Talk to someone

Talking to a colleague might help you figure out if the request is real or a phishing attempt.

Make a call if you're not sure

Pick up the phone and call that vendor, colleague, or client who sent the email. Confirm that they really need information from you. Use a number you know to be correct, not the number in the email or text.