Recognizing Online Scams
Phishing Tactics Explained

FIRST FEDERAL
Community Bank

CAPTCHA asking for your login?
What it is: A phishing trick that disguises itself as a CAPTCHA to appear legitimate.
How it works: After completing the CAPTCHA, you're asked to enter your email and password.
Why it matters: Real CAPTCHA tools never ask for login credentials. If one does, it is a scam.

A clean PDF isn’t always safe.
What it is: A phishing attempt hidden inside a PDF file.
How it works: You receive a PDF with no links in the email, but it contains a QR code. Scanning it takes you to a malicious website.
Why it matters: It bypasses email filters and tricks you into scanning something you did not request.

“It’s just a picture!” — Not always.
What it is: A deceptive tactic using image files like SVGs.
How it works: The image contains hidden links. Clicking it opens a fake login page that looks real.
Why it matters: You think you are just viewing a picture, but you are actually being redirected to a phishing site.

Recognizing Online Scams

Phishing Tactics Explained

Copy → Paste → Compromised
What it is: A clipboard hijack that changes what you paste.
How it works: You copy a command from a website, but when you paste it, something else appears — often malicious.
Why it matters: You might unknowingly run harmful code. Always double-check before pasting commands.

Looks like Google. Definitely isn't.
What it is: A phishing link that looks like a trusted URL.
How it works: You see something like accounts.google.com.security-check.fake.site — it looks legit but it is not.
Why it matters: Scammers use familiar-looking domains to trick you into entering credentials.