Phishing Red Flags

Every day, money is lost to online phishing scams. Learn how to spot shady emails, phone calls and texts by knowing the things no bank would ever ask.

TEXT MESSAGE SCAMS

Phishing text messages attempt to trick you into sharing personal information like your password, PIN or social security number to gain access to your bank account.

Slow down and think before you act

Acting too quickly when you receive phishing text messages can result in unintentionally giving scammers access to your account and your money. Scammers want you to feel confused and rushed, which is always a red flag.

Don't click links

Never click on a link sent via text message—especially if it asks you to sign into your bank account. Scammers often use this technique to steal your username and password. When in doubt, visit your bank's website by typing the URL directly into your browser or login to your banking app.

Never send personal information

Your bank will never ask for your PIN, password or one-time login code in a text message. If you receive a text message asking for personal information, it's a scam.

Delete the message

Don't risk accidentally replying to or saving a fraudulent text message on your phone. If you are reporting the message, take a screenshot to share, then delete it. As long as you don't respond to the messages and delete them, your information is safe.

What to do if you fall for a phishing text message

1. Change your password If you clicked on a link and entered any sort of username and password into a fake site.
2. Contact your bank directly to notify them you may have fallen victim to a phishing text message.
3. If you have lost money, file a report with the local police department.
4. File a complaint with the Federal Trade Commission or call 877.382.4357.