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.

PHONE CALL SCAMS

Scammers will impersonate the bank over the phone—some times acting friendly and helpful and other times threaten or scare—asking for personal information or get you to send them money.

Watch out for a false sense of urgency

Scammers count on getting you to act before you think, usually by including a threat. A scammer might say "act now or your account will be closed" or "we've detected suspicious activity on your account". Don't give into the pressure.

Never give out sensitive information

Never share sensitive information like your bank password, PIN or one-time login code with someone who calls you unexpectedly—even if they say they're from your bank. Banks may need to verify personal information if you call them, but never the other way around.

Don't rely on caller ID

Scammers can make any number or name appear on your caller ID. Even if your phone shows it's your bank calling, it could be anyone.

Hang up, even if it sounds legit

Whether it's a scammer posing as your bank or a real call, stay safe by ending unexpected calls and contact your bank directly.

What to do if you fall for an phone scam

1. If you gave out personal information, go to IdentityTheft.gov to see what steps to take, including how to monitor your credit.
2. Change your password if you shared any sort of username or password.
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.