THE SOLO CHAPTER | 50 AND BEYOND

Your Scam-Spotting Checklist

A quick reference to help you pause, verify, and protect your money.

1 RED FLAGS: STOP AND CHECK

☐ An unexpected message says your account, payment, benefits, or computer has a problem.

☐ Someone demands immediate action, secrecy, or payment to avoid a threat.

☐ You are told to pay with gift cards, cryptocurrency, a wire transfer, or a payment app.

☐ A stranger asks for passwords, verification codes, or remote access to your device.

☐ An online acquaintance asks for money or offers guaranteed investment returns.

2 BEFORE YOU CLICK OR PAY

☐ Pause. Do not use links, phone numbers, or attachments in an unexpected message.

☐ Open the company's official app or type its known website address yourself.

☐ Call your bank or organization using a number from your card, statement, or verified website.

☐ Ask a trusted person for a second opinion if the request feels unusual.

3 YOUR FIVE-MINUTE ACCOUNT CHECK

☐ Review transactions on ALL accounts, including credit cards you rarely use.

☐ Turn on transaction alerts where available; still review your statements.

☐ Use unique passwords and multifactor authentication on important accounts.

4 IF SOMETHING WENT WRONG

☐ Contact the bank or card issuer immediately through an independently verified channel.

☐ Change exposed passwords through the real website or app; secure affected accounts.

☐ For credit-card billing errors, ask about written dispute requirements and the 60-day deadline.

☐ Report fraud at ReportFraud.ftc.gov; get identity-theft recovery help at IdentityTheft.gov.

REMEMBER: A familiar logo is not proof. Urgency is a warning sign. Verify first.